TANET2013 臺灣網際網路學術研討會

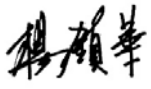
序　言

臺灣學術網路研討會(TANET)已邁入第十九屆，中興大學是繼臺灣大學之後成為第二個二度承辦此盛會的學校。本研討會除了強調網際網路應用技術與學術研討，也著重網路管理與數位內容建置等實務導向議題的經驗交流。今年研討會的主題訂為「樂活雲端、智慧臺灣」，希望能透過此研討會，邀集產官學研各界的專家學者、臺灣地區的資訊網路服務人員，共同探討先進的技術及應用，將資料轉換成可分析、可再使用的格式，透過雲端的分享，提高資料的附加價值，達到全球性、即時性及透通性，以奠定我國資訊化社會發展之基石。

TANET2013 研討會有專家學者及研究人員的論文發表，也有產業界從資訊應用技術層面探討網路應用發展的趨勢。會議主題包含雲端技術應用與服務、綠能通訊與資訊技術、數位內容與數位學習、數位落差數位關懷及數位機會、生物資訊、資通安全技術與管理、教育雲的技術及應用、個人資訊管理、校園數位化與校務行政、智慧生活科技、TWAREN 與未來網路規劃與設計等 22 個領域。大會透過線上投稿系統收到的論文計 314 篇，作者涵蓋產官學研等多方面的專家學者，參與面之廣為其他研討會少見。經過相關領域的學者專家審查，共收錄 239 篇論文，分 46 個場次進行發表。除了豐富的論文發表外，大會更安排一系列的學術活動，包含 2 場大會演講(Keynote Speeches)、21 個短期課程(Workshops)及 16 個現場展覽攤位。內容精彩，展現近年來各界研究與發展的豐碩成果。

今年 TANET2013 研討會之籌辦在有限的時間內能圓滿順利，首先要感謝指導委員會及籌備委員會的委員，並感謝所有論文投稿者、所有的論文審查委員以及議程委員會為大會所規劃的精彩論文議程，也要感謝行政院國家科學委員會、財團法人國家實驗研究院國家高速網路與計算中心、臺灣網路資訊中心及所有贊助廠商對大會的熱情參與與贊助。本次研討會能順利舉辦，主要是國立中興大學計算機及資訊網路中心全體同仁無怨無悔的付出，是同仁們團隊合作及專業能力再次展現的成果。最後，再次感謝各位先進參與此次盛會。

臺灣網際網路學術研討會(TANET 2013)　　大會主席





教育部資訊及科技教育司司長　　國立中興大學計算機及資訊網路中心主任

委 員 名 錄

榮譽主席

蔣偉寧／教育部長
朱敬一／國家科學委員會主任委員
李德財／國立中興大學校長

大會主席

楊鎮華／教育部資訊及科技教育司司長
呂瑞麟／國立中興大學計算機及資訊網路中心主任

指導委員會

楊鎮華／教育部資訊及科技教育司司長
吳瑞北／財團法人資訊工業策進會執行長
曾憲雄／財團法人台灣網路資訊中心董事長
謝錫堃／國家高速網路與計算中心主任
蔡進發／亞洲大學校長
李新林／國立中正大學副校長
周文光／靜宜大學副校長
王金龍／銘傳大學副校長
劉安之／逢甲大學資訊工程學系講座教授
曾黎明／國立中央大學資訊工程學系教授
蘇木春／國立中央大學電子計算機中心主任
李錫智／國立中山大學圖書與資訊處處長
王大為／國立中央研究院計算中心主任
呂瑞麟／國立中興大學計算機及資訊網路中心主任
官大智／國立中興大學圖書館館長
孫雅麗／國立臺灣大學計算機及資訊網路中心主任
蔡錫鈞／國立交通大學資訊技術服務中心主任
蔣榮先／國立成功大學計算機與網路中心主任
黃振榮／國立東華大學圖書資訊中心主任
楊亨利／國立政治大學電子計算機中心主任
賴尚宏／國立清華大學計算機與通訊中心主任
郭達源／國立臺東大學電子計算機中心主任
楊竹星／國立成功大學電腦與通訊工程研究所教授

籌備委員會

劉文惠／教育部資訊及科技教育司副司長
呂愛琴／財團法人台灣網路資訊中心副執行長
張顧耀／大葉大學電子計算機中心主任
蔡興國／中國醫藥大學資訊中心主任
林俊榮／弘光科技大學資訊管理系主任
楊朝棟／東海大學電子計算機中心主任
朱延平／東海大學資訊工程與科學系教授
蔡清欉／東海大學資訊工程與科學系教授
范俊逸／國立中山大學資訊工程學系教授兼圖資處副處長
朱彥煒／國立中興大學基資所副教授兼計資中心研究發展組組長
歐陽彥杰／國立中興大學電機工程學系教授
官大智／國立中興大學圖書館館長
陳文淵／國立勤益科技大學電子工程系教授兼電資學院院長
白能勝／國立勤益科技大學電子計算機中心主任
陳良瑞／國立彰化師範大學電子計算機中心主任
蔡月霞／國立臺中科技大學資訊與流通學院院長
林春宏／國立臺中科技大學電算中心主任
李維斌／逢甲大學資訊處處長
陳榮靜／朝陽科技大學資訊學院院長
楊伏夷／朝陽科技大學電子計算機中心主任
許孝麟／彰化縣教育網路中心主任
蔡英德／靜宜大學計算機及通訊中心主任
王孝熙／靜宜大學資訊學院院長

議程委員會

莊育秀／教育部資訊及科技教育司高級分析師
王旭正／中央警察大學資訊管理系教授
陳錦杏／中臺科技大學資訊管理學系教授兼圖書館館長
張怡君／弘光科技大學資訊工程系助理教授
周永振／亞洲大學資訊工程學系助理教授
楊朝棟／東海大學電子計算機中心主任
張志宏／修平科技大學資訊管理系副教授
姜文忠／修平科技大學資訊網路技術系助理教授
邱日清／國立中山大學電機工程學系副教授
江爲國／國立中正大學資訊工程學系副教授兼電算中心研究發展組組長
吳賢明／國立中興大學計資中心資訊網路組組長
朱彥煒／國立中興大學基資所副教授兼計資中心研究發展組組長
廖宜恩／國立中興大學資訊科學與工程學系教授兼主任
高勝助／國立中興大學資訊科學與工程學系教授
王丕中／國立中興大學資訊科學與工程學系副教授
吳俊霖／國立中興大學資訊科學與工程學系副教授
詹永寬／國立中興大學資訊管理學系教授兼主任
林詠章／國立中興大學資訊管理學系教授
許志義／國立中興大學資訊管理學系教授
楊朝成／國立中興大學資訊管理學系教授
蔡孟勳／國立中興大學資訊管理學系教授
林冠成／國立中興大學資訊管理學系副教授
蔡蕙芳／國立中興大學法律學系教授
丁一賢／國立高雄大學資訊管理學系副教授
蕭漢威／國立高雄大學資訊管理學系助理教授
柯博昌／國立高雄應用科技大學資訊管理系教授
黃天受／國立高雄應用科技大學資訊管理系副教授
陳昭宏／國立雲林科技大學資訊管理系教授兼主任暨所長
施學琦／國立雲林科技大學資訊管理系教授兼資訊中心主任
陳文淵／國立勤益科技大學電子工程系教授兼電資學院院長
張庭毅／國立彰化師範大學工業教育與技術學系副教授
李佩君／國立暨南國際大學電機工程學系教授
陳同孝／國立臺中科技大學資訊工程系教授兼主任
陳世穎／國立臺中科技大學資訊工程系副教授
王讚彬／國立臺中教育大學資訊工程學系教授兼主任
邱淑惠／國立臺中教育大學幼兒教育學系副教授
黃一泓／國立臺中教育大學數學教育學系副教授
逄愛君／國立臺灣大學資訊工程學系教授
黃秀芬／逢甲大學資訊工程學系主任
李榮三／逢甲大學資訊工程學系副教授
柯秀佳／朝陽科技大學資訊管理系助理教授
江茂綸／朝陽科技大學資訊與通訊系助理教授
李建緯／朝陽科技大學資訊與通訊系助理教授
洪啓舜／僑光科技大學資訊管理學系副教授兼主任
林家禎／靜宜大學資訊管理學系教授

Session 分類索引目錄

上　冊	頁次	下　冊	頁次
A1 網際網路技術與營運管理	1	K2 物聯網(IOT)	681
A2 網際網路技術與營運管理	37	L1 數位內容與數位學習	722
A3 網際網路技術與營運管理	72	L2 數位內容與數位學習	758
B1 雲端技術、應用與服務	107	L3 數位內容與數位學習	790
B2 雲端技術、應用與服務	133	M1 資通安全技術與管理	822
B3 雲端技術、應用與服務	163	M2 資通安全技術與管理	860
B4 雲端技術、應用與服務	193	M3 資通安全技術與管理	892
C1 網路犯罪與數位鑑識	220	M4 資通安全技術與管理	928
C2 網路犯罪與數位鑑識	244	M5 資通安全技術與管理	946
C3 網路犯罪與數位鑑識	267	N1 社群網路	964
D1 無線通訊與行動計算	297	N2 社群網路	975
D2 無線通訊與行動計算	327	O1 生物資訊	1011
D3 無線通訊與行動計算	345	O2 生物資訊	1041
E1 綠能通訊與資訊技術	376	P1 數位匯流技術與政策	1080
E2 綠能通訊與資訊技術	404	Q1 數位落差、數位關懷及數位機會	1111
F1 多媒體訊號處理	432	R1 校園數位化與校務行政	1143
G1 鏈結開放資料與巨量資料理	470	R2 校園數位化與校務行政	1174
H1 資料探勘	502	S1 智慧生活科技	1209
H2 資料探勘	526	S2 智慧生活科技	1245
I1 個人資訊管理	556	S3 智慧生活科技	1276
J1 教育雲的技術及應用	591	T1 數位學習與系統應用	1307
J2 教育雲的技術及應用	621	U1 TWAREN 與未來網路規劃與設計	1328
K1 物聯網(IOT)	645	V1 電子商務	1359

目　　錄

Session　A1：網際網路技術與營運管理　　10 月 23 日(三)13:20-15:00　Room 1

1. 鏈路故障時群播保護之備用重新供給問題-以漢彌頓環保護…… *黃仁伸　丁德榮*　1
2. 使用於 OpenFlow 網路架構下的網路狀態更新監錄機制…… *蔡逸祥　曾黎明　陳翔詠*　7
3. 開發與建置交通大學異地備份儲存系統…… *楊詠仁　王英鼎　陳昌盛*　13
4. 建置校園可擴充之輕量化網路身分認證系統：以交通大學爲例 … *林明樺　陳昌盛　王英鼎*　19
5. 基於 Wi-Fi 無線網路技術之工具機廠區監控系統建置…… *陳嚮亮　陳明皇*　25
6. 可變多工伺服器管理電源…… *連嘉宏　董瑞洋*　31

Session　A2：網際網路技術與營運管理　　10 月 23 日(三)15:20-17:00　Room 1

1. 多路徑環境下具預測與回饋機制之 VoIP 路徑決策系統…… *張家力　高勝助*　37
2. IPv6 與 NAT 網路傳輸之效能分析……*陳懷恩　鄭仕遠　邱俊傑*　44
3. An Adaptive RAR Tree-Based Diagnosis System for Rule Anomalies among Network Firewalls
   ……*趙啓時　邱振添*　49
4. 開放性 DNS 解析伺服器之防治…… *謝木政　陳怡碩*　55
5. 基於雲端虛擬化技術之無線化遠端監控管理系統架構設計-以射出成型機台爲例
   ……*陳嚮亮　蕭應涵　陳韻堯*　60
6. 封包分類器之二維衝突偵測…… *饒昕芳　張毓騏　方斐仙　王丕中*　66

Session　A3：網際網路技術與營運管理　　10 月 24 日(四)09:00-10:40　Room 1

1. 一個在半透明分波多工網路下的再生器配置演算法……*張弘毅　王靖宇　熊群傑*　72
2. 實現具有速寫演算法來源識別碼回溯機制之 OpenFlow 網路流量變異偵測系統
   …… *黃柏勳　賴裕昆*　78
3. 有效率的多維度分類規則衝突偵測演算法……*林冠宇　李春良　陳耀宗*　84
4. 限制理論思維應用於整合型郵件系統之建構—以核能研究所爲例…… *鄭勝璋　賴昱達*　89
5. 支援大型多人線上遊戲伺服器叢集之基於地域性的負載分配策略
   …… *李政翰　夏啓賢　黃俊鈞　姜美玲　陳弘勳*　95
6. 基於內容核心網路實現資料命名網路－以即時通訊爲例… *廖上全　曾繁勛　趙涵捷　周立德*　101

Session　B1：雲端技術、應用與服務　　10 月 23 日(三)13:20-15:00　Room 2

1. 具負載平衡與容錯機制的雲端魯班陽宅評估系統…… *陳裕升　高勝助*　107
2. 基於時間預估之雲端算圖系統…… *范登凱　蔡建麟　許家彰　袁嘉彬*　113
3. 設計與實作一基於虛擬化技術之網路及網路安全雲端測試平台
   …… *蔡邦維　賴瑀庭　羅孟彥　楊竹星*　119
4. 植基於 GCM 技術適合銀髮族使用之處方箋、用藥說明、醫療資訊的
   Android 訊息推播 APP 設計……*楊慶隆　蔡欣晏　吳志成　林哲佑　蔡松叡　陳政樺　謝祈樂*　127

Session B2：雲端技術、應用與服務 10 月 23 日(三)15:20-17:00 Room 2

1. 雲端彈性虛擬資料中心服務平台之安全性提升……*陳劭睿 李忠信 楊睿豪 王尉任* 133
2. 分散式檔案系統於虛擬化環境下效能比較……*呂泓縉 賴仲哲 葉俊雄 李盛安* 139
3. 基於 Hadoop 雲端運算架構之平行基因演算最佳化學習障礙診斷輔助系統
……*許晉瑜 許貫傑 高秀婷 吳東光 孟瑛如* 145
4. 品質控制流程應用於雲端服務監控機制之研究…… *陳奕明 楊采薇* 151
5. 叢集式虛擬機器磁碟系統之優化研究……*蘇偉哲 林佳辰 徐啓閎 蔡德明* 157

Session B3：雲端技術、應用與服務 10 月 24 日(四)09:00-10:40 Room 2

1. 雲端服務個人化應用之研究…… *黃建維、吳傳春、吳建興* 163
2. 以虛擬技術提升校園資訊系統的效能…… *呂建德、葉俊雄、王永鐘、李盛安* 172
3. 雲端服務環境之程序隱藏型 Rootkit 偵測機制研究…… *曹偉駿、吳佳鑫、杞承樺* 178
4. 雲端上可調式雙門檻的虛擬機器遷移策略…… *許俊傑、王逸民* 184
5. 雲端行動避難系統之設計與實作…… *周立德、劉家豪、劉登壹、郭凱威、潘偉誠* 188

Session B4：雲端技術、應用與服務 10 月 24 日(四)13:20-15:00 Room 2

1. 雲端虛擬桌面系統之分散式架構及負載平衡改進…… *湯凱崴* 193
2. 以 Linux 系統爲基礎之插件式雲端桌面架構…… *王國肇* 198
3. The Virtual Desktop and Application Sharing System for Cloud Computing
……*林佑青、王順泰、陳盈銓* 204
4. 設計並實現以建構 Windows 核心驅動方式之分散式資料儲存架構..*邱日清、楊承澔、高志宏* 209
5. 高效能遠端桌面系統之實作與評估…… *詹沛明、王皓立* 215

Session C1：網路犯罪與數位鑑識 10 月 23 日(三)13:20-15:00 Room 5

1. Simple Man-in-middle Attack, Investigation, and Defense
……*Tzu-Chi Huang, Kuo-Chih Chu, Jun-Ming Liang* 220
2. 學習動機與滿意度分析報告: 101 年度資通安全學程爲例……*黃玉枝、郭文中、官大智* 223
3. 低速阻斷服務攻擊之偵測與防禦……*陳哲鋒、賴義鵬* 227
4. 使用雙僞裝影像之可逆式資訊隱藏與機密分享技術
……*許俊萍、邱川峰、詹森仁、陳以裕、劉正意* 233
5. 多層式可逆資訊隱藏技術應用邊緣敏感度分析方法……*呂慈純、黃英軒、許永明* 239

Session C2：網路犯罪與數位鑑識 10 月 23 日(三)15:20-17:00 Room 5

1. Evidence Investigations in Forensics in Case of Clouding Access with Data Synchronizations
……*鐘敏如、王旭正* 244
2. 開發應用程式以保護社群網站影像之浮水印機制…… *廖惠雯、張士勳、孫全澍* 250
3. Watch Your Money：A Solution to Protect Your Android from Sending Unknown SMS Messages
……*廖緯玲、陳世仁、蘇育生、許富皓、吳敏豪* 256

4. Applying EPCglobal Architecture Framework for Criminal Physical Evidence Safety Monitoring System
…… *Chia-Chun Chen, Chua-Huang Huang* 261

Session C3：網路犯罪與數位鑑識 10 月 24 日(四)09:00-10:40 Room 5

1. TRAM: A Traceback Method using RAndom Moonwalks in AMI Meter Networks
……*徐詩淳、徐雅琦、徐彬海、陳耀鑫、鄭伯炤* 267
2. Enhancing the security of dynamic CSC with visual secret sharing technique
…… *Jung-San Lee, Kuo-Jui Wei, Shin-Jen Chen, Bo Li, Yuan Xue* 274
3. Cryptanalysis of a Certificateless Signature Scheme without Bilinear Pairings
…… *Kuo-Hui Yeh, Kuo-Yu Tsai, Chuan-Yen Fan* 281
4. 以觸控手勢爲基礎之 CAPTCHA 設計…… *陳昱翰、徐豐明* 285
5. 在車載網路上有效之金鑰分配實現遠距離與安全之推播訊息傳遞……*吳威震、陳奕明* 291

Session D1：無線通訊與行動計算 10 月 23 日(三)13:20-15:00 Room 6

1. 基於車輛網路動態路徑規劃之節能共乘配對演算法與 Android 平台上的實作
…… *張英超、洪似妮、厲秉忠、李建德、 邵盈智、王傳啓* 297
2. A Utility-based Resource Allocation and Scheduling Scheme…*胡誌中、陳振庸、楊峻權、麥毅廷* 303
3. 利用 NS-2 創建 PLC 模組於異質網路效能分析
……*王炯竣、陳國成、黃文祥、林政翰、鍾勝民、陶明宏* 310
4. A Relay Station Deployment with Particular K-means Strategy for Multi-hop Relay Network Systems
……*Jau-Yang Chang, Yun-Wei Chen* 315
5. An Enhanced Sorting Tree Energy-Efficient Routing Scheme for Wireless Sensor Networks with Mobile Sink……*Jau-Yang Chang, Ting-Huan Shen* 321

Session D2：無線通訊與行動計算 10 月 23 日(三)15:20-17:00 Room 6

1. 基於微控制器之工具機訊號擷取裝置設計與實作……*陳響亮、陳奕伶、陳韻堯* 327
2. ZigBee 無線感測技術應用於自走車之定位-增廣卡爾曼濾波器研究……*林鴻興、楊曜任* 333
3. 整合 ZigBee 與加速規之汽車路考系統…… *林揚凱、王丕中* 339

Session D3：無線通訊與行動計算 10 月 24 日(四)09:00-10:40 Room 6

1. LTE 上行鏈路中基於用戶滿意度之資源分配演算法研究
…… *Yu-Shun Liu, Jiun-Yu Tu, Wei-Ting So, Jung-Shyr Wu, Jehn-Ruey Jiang* 345
2. 一個在 LTE 中具即時行進方向預測及動態權重調整的換手機制……*蕭中一、高勝助* 351
3. LTE 系統之動態分配資源的下行 QoS 機制…… *陳俞樺、蔡智強、張詠勝、柯勤彥* 358
4. 以分散式 Tracker 爲基礎之 P2P 傳輸區域化機制……*李昭賢、童曉儒、林佳彥* 364
5. 應用於行動 P2P 串流網路之統計式多來源資料下載策略……*童曉儒、林思宏* 370

Session E1：綠能通訊與資訊技術 10 月 23 日(三)13:20-15:00 Room 7

1. 無線感測網路之可應變式多點跳躍 MAC 排程機制 ……*簡碩瑤、張林煌、吳忠宏、林青、鍾銘山、李宗翰、徐嘉佑* 376
2. 在 WiFi 與 ZigBee 共存網路中考量緊急訊息需求並提昇 Zigbee 傳輸機會之共存媒介傳輸協定… *Tse-Yuan Wang, Shih-Shun Hsu, Tzu-Lin Wang, Chao-Tsun Chang, Chih-Yung Chang* 382
3. QoS-Based Fairness-Aware Downlink Scheduling in LTE-Advanced …… *Ying-Hong Wang, Chih-Hsiao Tsai,Hao-Yi Huang, Yi-Jia Tong* 388
4. 植基於 IP 技術的環境光度監控系統…… *王柏翔、林嬿雯* 394
5. 利用網際網路傳遞觸覺回饋資訊之研究……*李宗翰、王朝仕、張林煌* 399

Session E2：綠能通訊與資訊技術 10 月 23 日(三)15:20-17:00 Room 7

1. 節能的動態連結式無線插座系統……*謝嘉維、紀光輝、江季翰、何前程* 404
2. 資訊設備耗能網路監測系統……*鄭嘉緯、包蒼龍* 409
3. 機房主機虛擬化管理之建置實務……*梁瑞崧、邱清鴻、林育民、陳青文* 414
4. 利用協同傳輸設計有效多重速率媒體存取控制協定… *陳柏岳、江庭輝、邱清鴻、陳青文* 418
5. Cooperative Localization with Energy Minimization in Vehicular Long-Thin Networks ……*Lien-Wu Chen, Chia-Chen Chang* 424

Session F1：多媒體訊號處理 10 月 23 日(三)13:20-15:00 Room 8

1. 應用棒球運動視訊之棒球軌跡追蹤研究…… *林家緯、張元翔、鄭立德* 432
2. 植基於距離測量之影像檢索系統……*黃國峰、黃慧鳳、林嘉文* 438
3. 一種實作於影像區塊截短編碼之可逆式資料隱藏技術……*林昱宏、仲維德、謝仕杰* 444
4. 多光源影像白平衡演算法之研究……*官怡秀、吳俊霖* 451
5. 結合人臉偵測之接縫雕刻法於內容感知影像不等比例縮放之研究 ……*莊靜芬、周佳毅、李孟桓、吳俊霖* 458
6. 以物件爲基礎的高動態範圍機密圖像分享研究 *黃金本、蘇昱軒、許孟妤、曾奕傑、徐竹君* 464

Session G1：鏈結開放資料與巨量資料理 10 月 23 日(三)15:20-17:00 Room 8

1. 具語意鏈結能力之文化領域政府開放資料服務設計…… *陳純美、廖峻鋒* 470
2. 在 Hadoop 中以 Failover Controller 改進 AvatarNode 可用性的架構…… *李滄智、高勝助* 476
3. 斷詞系統對於 Queried keywords 的影響…… *陳宜惠、呂瑞麟、黃政傑* 482
4. 海量資料基於 Multipath TCP 之 40Gb 網路傳輸……*楊哲男、古立其、周大源* 487
5. 預測分析運用於資料儲存建置成本之研究……*朱金城、趙原宏、彭煥淇* 492
6. 鏈結開放資料爲基礎之 Web API 服務--以觀光旅遊資訊爲例…… *陳良駒、張有志、余丁榮* 497

Session H1：資料探勘 10 月 24 日(四)13:20-15:00 Room 1

1. 利用正規化概念分析探勘分類關聯法則之研究……*黃錦法、彭浩政、徐博恩* 502
2. 應用資料採礦技術於中途輟學線上預警系統之實現……*翁秉逸、謝明哲* 508

3. 英文文本詞彙多樣性自動化指標發展與探討……*徐詩媛、白鎧誌、郭伯臣、邱毓芳* 514
4. MapReduce 架構下循序樣本探勘演算法之效能分析
……*陳世穎、魏秀蕙、蔡岳峻、許珉豪、郭立辰* 520

Session H2：資料探勘 10 月 24 日(四)15:20-17:15 Room 1

1. 基於 MapReduce 技術之時間區段性的網頁瀏覽樣式偏好度探勘…*賴鈺芬、葉介山、林彩雯* 526
2. 以 WOS 檢索與灰色理論探討行動商務相關文獻間的關聯…… *王信智、葉祐辰* 534
3. 以 SEO 概念維度爲基礎的 Google 搜尋結果之分群…… *陸承志、黃挺立、林昱呈* 544
4. 關鍵字爲基礎的多主題概念飄移學習……*林熙禎、林文羽* 550

Session I1：個人資訊管理 10 月 24 日(四)15:20-17:15 Room 2

1. 全球化下個人資料管理之研究-----從個資法分析相關法律議題…… *張文蘭* 556
2. 整合新版個資法與 ISO 27001&27011 於電信業客戶個資管理探討 *林哲民、陳致穎、林宜隆* 559
3. 從稽核觀點探討資訊系統對法令遵循之研究—以個人資料保護法爲例……*張明森、陳志誠* 564
4. 大學因應個人資料保護法的具體做法與成果評估-以臺北醫學大學爲例
……*萬序恬、蔡宛真、李佩珊、林建煌、邱泓文* 571
5. 基於 3D 人臉辨識之使用者數位版權管理方案…… *詹昭文、莊政儒、林詠章* 574
6. 個人資料保護法「目的拘束原則」對新聞報導的限制……*田炎欣* 579
7. 學校機關個人資料風險評鑑與控管系統之設計與開發……*李姵璇、洪新原* 585

Session J1：教育雲的技術及應用 10 月 24 日(四)13:20-15:00 Room 5

1. 雲端社群化電子書環境之發展及其在商業資訊工程協同流程再造教育課程之應用…*王信文* 591
2. 企業導入開源軟體與執行成效之分析……*陳志達、郭建明、吳昱伸* 597
3. 支援多重服務品質考量的教育雲服務選擇使用基因演算法……*唐東暘、朱正忠、黃建華* 603
4. 分散式檔案系統 Hadoop 與 Ceph 效能比較……*卓志遠、楊朝棟、張廣欽、李偉業* 609
5. 桌面雲建置及效能比較……*李偉業、楊朝棟、張廣欽* 615

Session J2：教育雲的技術及應用 10 月 24 日(四)15:20-17:15 Room 5

1. 亞洲大學教學雲規劃與建置經驗……*陳偉嵩、黃仁德、陳柏凌、鍾仁宗、劉嘉政* 621
2. 國中校園虛擬化系統規劃與設計之探討……*林宜隆、曾志忠* 627
3. 教育雲端應用及服務平台建置與整合……*曾憲雄、陳君銘* 632
4. 實作於修平科大之校園雲端網路服務教學平台……*高國峯、麥毅廷、王鵬程、陳東宏* 638

Session K1：物聯網(IOT) 10 月 24 日(四)13:20-15:00 Room 6

1. 基於比特幣加密演算法之跨平台物聯網系統裝置身份辨識服務……*劉祐安、賴槿峰* 645
2. 使用微型叫號器改善醫院門診叫號系統……*塗庭輝、王丕中* 651
3. Implementation of a Greenhouse Crop Remote Monitoring System with IOTs Technology
……*Joy Iong Zong Chen,Yuan-Chen Chen, Shien-Dou Chung* 657

4. 具即時與耗能考量的感測網路路徑產生方案
……鄧宇喬、盧永豐、郭錦福、汪新隆、郭弘翊、林金昇 662
5. Applying RFID Technology in Tracking and Tracing of Pallets in Supply Chain Management
……Ming-Wei Huang, Chua-Huang Huang 668
6. 感測節點上的混合式任務排程機制……郭錦福、盧永豐 675

Session K2：**物聯網**(IOT) 10 月 24 日(四)15:20-17:15 Room 6

1. 基於物聯網架構之電器導向雲端能源管理平台
…… 林偉益、陳瑋哲、賴槿峰、黃悅民、鄭鈺霖 681
2. 物聯網之電器感知活動識別方法於雲端能源管理平台
…… 陳瑋哲、林偉益、賴槿峰、黃悅民、鄭鈺霖 687
3. 使用粒子群最佳化演算法尋找無線人體區域網路低特定吸收率路徑
…… 吳庭育、李維聰、林承翰、吳昱緯 693
4. 以 RFID 爲主的 IoT 之研究－以 N 博物館文創商品管理爲例……姜國輝、翁瑞聲 699
5. 基於 Wi-Fi 之無線化廠區雲端機台遠端監控平台設計……陳響亮、王欣如、陳韻堯 705
6. 機器型態通訊於下一代行動通訊網路之挑戰……曾啓維、陳 灝 711
7. 以 OpenStack 建立可擴充式物聯網系統雲端平台……蘇俊憲、陳昌盛 716

Session L1：**數位內容與數位學習** 10 月 24 日(四)09:00-10:40 Room 7

1. 基於拼圖式合作學習融入國小閱讀理解與寫作成效之研究
……章淑貞 林秋斌 潘炯凱 黃孟鈴 林根煌 謝東諭 722
2. Moodle 融入國小高年級藝術與人文教學之研究--以戲偶天地爲例……張維娟 王麗雁 729
3. 將模擬系統移轉至視覺化程式語言環境之建置對照—以 StarLogo TNG 爲建置工具
……...林均恒 洪文麟 張智凱 735
4. 多人腦波遊戲系統架構設計探究……王曉璿 紀明良 林含諭 741
5. 在平板電腦上漢字部件悅趣學習系統建置……許政穆 邱孝義 葉玭瑄 747
6. 圖書館利用教育數位課程系統化設計與發展…… 劉 杰 752

Session L2：**數位內容與數位學習** 10 月 24 日(四)13:20-15:00 Room 7

1. 學生編擬題目卷學習系統的建置與使用分析…… 于富雲 蘇嘉鈴 758
2. 互動式 3D 電腦輔助學習應用於正投影視圖教學……洪明顯、游耿能、許永洲 760
3. 運用社群網站與行動載具輔助護生進行衛教護理實習之課程…… 吳婷婷、宋天文 766
4. 行動擴增實境於同儕互評上的應用—以基礎設計課程爲例…… 趙國宏、藍中賢、王冠傑 772
5. 國中學生英語閱讀電腦化測驗之編製與發展…廖麗珍、邱毓芳、郭伯臣、白鎧誌、白宗恩 778
6. 結合三段式 IRF 教學對話之英語文法學習系統
…… 蔡維軒、蘇建元、趙偉智、張家瑋、王宗一 784

Session L3：數位內容與數位學習 10 月 24 日(四)15:20-17:15 Room 7

1. 整合變易理論之物件導向程式設計語法導正系統.....*黃子峰、蘇建元、張証欽、王宗一* 790
2. 行動載具之個人化學習歷程應用程式研發初探.....*王仕祺、王怡萱、楊叔卿* 796
3. 具自動出題與診斷能力的實體關係模型轉換關聯表學習輔助系統.....*邱瑞山、蘇桓沂* 801
4. A Study on the Integration of Online Learning into English Course Design
..... *Hui-Chih Wang, Harry Shih* 806
5. 應用校園文化地景主題網站進行知識移轉之研究.....*李宜蓁* 811
6. 全人雲端網課程活動 App 對品格與關懷能力影響之研究
..... *廖慶榮、李清義、潘正德、陳鶴元、李明訓、劉致緯* 816

Session M1：資通安全技術與管理 10 月 24 日(四)09:00-10:40 Room 8

1. 一個高效率的擬亂數產生方法與平行化加速的研究與分析
.....*鄭毓融、林昀德、林芳邦、黃詠詳、蕭一豪* 822
2. 醫療影像之可逆式資訊隱藏技術應用邊緣敏感度分析預測方法 *呂慈純、曾俊雅、黃俊智* 830
3. 使用 URL Routing 與 Web Storage 防禦跨站冒名請求攻擊..... *劉書宇、吳其哲、丁建文* 837
4. ARP Spoofing 偵測及防護機制-以 Arcai Netcut 軟體爲例.....*王永鐘、王宜秀* 843
5. 基於 P2P-OSGi 服務取得機制之數位版權管理機制.....*林宸堂、張志鴻* 848
6. 全球行動網路服務之匿名性認證機制..... *楊仁和、溫柏旻* 854

Session M2：資通安全技術與管理 10 月 24 日(四)13:20-15:00 Room 8

1. 因應個資法規範建構 PDF 文件資料遮罩之低成本工具組合.....*蔡敦仁、欒家祥* 860
2. 智慧電網家庭閘道器資安驗證標準之制定與應用--資訊安全與實體安全整合評估
.....*林佳瑩、易俗、范金鳳* 866
3. 基於預測值與鄰近像素差值的標準差的可逆式資訊隱藏..... *冷輝世、張維剛、曾顯文* 872
4. 保持邊緣特性的可逆式資訊隱藏..... .*冷輝世、余奕憲、曾顯文* 878
5. 以網頁驗證碼爲基礎的側錄程式密碼防禦機制.....*許玉芳、沈慧宇、金 馳* 884
6. 網格計算之通訊安全設計..... *劉正義、黃慧鳳、詹昭文、程瑞芳* 888

Session M3：資通安全技術與管理 10 月 24 日(四)15:20-17:15 Room 8

1. 鑑識會計應用於政府審計之初探..... *林宜隆、林慄麗* 892
2. 結合邊緣特性與人類視覺系統的高藏量資訊隱藏法... *冷輝世、張維剛、余奕憲、曾顯文* 898
3. 雲端安全儲存系統 .....*林華鵬、周國森、郭志勇、單張麟、陳彥仲、林宗毅* 904
4. 主動式傳播殭屍網路防禦機制..... *葉奇鑫、曾黎明、彭博涵* 910
5. 基於 OpenFlow 交換機之跨雲端安全管理機制研究.....*陳奕明、朱永彤* 916
6. Min-Max 可逆式資料隱藏技術之安全性分析.....*林志麟、胡宸浩、婁德權* 922

Session M4：資通安全技術與管理 10 月 25 日(五) 09:00-10:40 Room 1

1. 結構化惡意程式資料庫系統.....*劉奕賢、蔡舜智、江啓賓、張家瑋、安家駒、李忠憲* 928
2. 植基於 Google 雲端訊息推播技術的行動認證機制..... *楊慶隆、邱創昱、蔡松叡* 934
3. 基於資料外洩的行動惡意程式行爲分析
..... *陳嘉玫、江玫璟、陳怡靜、張明達、吳惠麟、曾昭銘* 939

Session M5：資通安全技術與管理 10 月 25 日(五)11:00-12:40 Room 1

1. 應用蟻群最佳化與模糊分群演算法於資料隱私保護之研究..... *邵敏華、鄭仁豪* 946
2. 以合理輸入值驗證爲基礎之預存程序組合型 SQL 指令植入式攻擊防禦... *陳威霖、田筱榮* 953
3. 使用靜態分析與機器學習以偵測 Android 惡意程式.....*蘇民揚、張文銓* 959

Session N1：社群網路 10 月 25 日(五) 09:00-10:40 Room 3

1. 以代理人機制爲基礎的社群網路資料搜尋之研究..... *李佳菁、賴宥呈、陳明僑* 964
2. LOM：領隊導向多人連線遊戲自動匹配演算法 ..... *宋管翊、江振瑞* 970

Session N2：社群網路 10 月 25 日(五)11:00-12:40 Room 3

1. 行動虛擬社群科技壓力之研究.....*洪爲璽、蘇永松* 975
2. 智慧型手機即時通訊軟體使用行爲之調查研究.....*蔡瑋哲、蔡英德* 981
3. 以 Facebook 爲基礎之社群服務系統.....*王民翰、張焜翔、江清泉* 987
4. 網路社群之社會支持：以大學生 Facebook 使用者爲例...*鍾才元、楊政穎、陳明終、劉晏廷* 993
5. 人格特質、Facebook 使用動機對人際關係之衝擊研究—以台灣地區大學生爲例
.....*劉勇伸、張青桃* 999
6. 運用社群網路技術之主題式資訊整合服務：以校園社團資訊應用爲例
..... *詹孟穎、吳嘉峰、方慕堯、馬尙彬* 1005

Session O1：生物資訊 10 月 25 日(五) 09:00-10:40 Room 2

1. 腦波儀研究在各領域之應用.....*陳昆顯、何淑君* 1011
2. DNA 序列浮水印技術之強化設計.....*林琨祐、陳建銘、林韓禹、白敦文* 1017
3. 細胞自動機與 RFID 之基因密碼辨識與管理資訊系統-以 miRNA 爲例
..... *林守羿、蔡孟勳、吳協昌* 1023
4. 利用高通量定序資料預測老鼠微核醣核酸轉錄起始位置
..... *方浩宇、許郁彬、朱虹瑄、謝立青* 1029
5. 鈣離子通道基因剔除小鼠微陣列資料分析.....*林守羿、蔡孟勳、何宜霖* 1035

Session O2：生物資訊 10 月 25 日(五)11:00-12:40 Room 2

1. 挑選具有非線性關聯性之基因選取機制：以演化式計算模式搭配多目標決策作法
..... *唐瑋君、蔡毓舜、鍾翊方* 1041
2. 演化式計算輔助整合特徵模型預測蛋白質瓜胺酸化位置.....*陳啓瑋、洪慧芝、朱彥煒* 1047

3. 使用機器學習與特徵選擇預測明膠酶的受質切位……*張浩禎、朱彥煒* 1053
4. 標準化病人自動化動作分析訓練系統……*林志豪、吳建勳、林雨慶、陳治華* 1059
5. 個人健康紀錄的醫學建議知識庫系統……*林志豪、張家維、林俊成、鄭稚翰* 1067
6. 人類蛋白質在細胞內位置的預測……*徐筱姍、游景盛* 1075

Session P1：數位匯流技術與政策 10 月 25 日(五) 09:00-10:40 Room 4

1. 數位匯流技術應用於到院前緊急救護服務平台……*顧皓翔、林鴻逸、黃思淵* 1080
2. A Multimedia Sharing Scheme on IMS-based Digital Convergence Platform
……*李建緯、邱研倫、張怡君* 1086
3. 急診即時查詢與導航服務系統之研發……*曹祐誠、李昭賢、陳昭文、王冠傑* 1090
4. 行動視訊播放與管理系統……*葉耀明、鄭皓中* 1095
5. 從現行著作權法制談封鎖外國網站政策的可能性……*陳秉訓* 1101
6. 整合異質性資料來源成爲行動網站的方法……*周椽家、翁瑞元、王祥安、黃翰隆* 1105

Session Q1：數位落差數位關懷及數位機會 10 月 25 日(五)11:00-12:40 Room 4

1. 網路與手機雙重成癮者之人格特質分析……*鍾才元、陳明終、賴阿福、楊政穎、林慧婷* 1111
2. 偏遠地區國中學生資訊素養之變遷-以嘉義縣某國中爲例…… *游淑惠、尤國任、王偉達* 1117
3. 利用網路學習平台實施補救教學之可行性研究－以偏遠國小爲例……*沈保信、陳昌盛* 1123
4. 語意網在偏鄉遠距課輔教材分享上的應用……*溫敏淦、樂美邑、陳博智* 1129
5. 家庭傳播型態與父母介入對於兒少網路隱私關注與態度影響之研究……*黃琬翎* 1135

Session R1：校園數位化與校務行政 10 月 25 日(五) 09:00-10:40 Room 5

1. iTNUA 校園資訊入口及單一帳號登入整合之實作……*林明灶、劉仲凱* 1143
2. 選課系統問題分析及其解決方案……*賴秀香、蔡錫鈞* 1149
3. 應用 QR Code APP 在校園 E 化教室服務和管理之研究……*陳明芳* 1153
4. 改良式準隨機亂數株落演算法之組裝平行測驗……*胡芸菁、張庭毅、呂易鄙、鄭培成* 1158
5. 校外租屋資訊微軟 APP …… *嚴本嘉、陳鵬先* 1164
6. 利用社群網路建構程式設計同儕學習與測驗環境……*劉朝中、林忠億* 1168

Session R2：校園數位化與校務行政 10 月 25 日(五)11:00-12:40 Room 5

1. 誘導式結構發展彈性 ITI 建置校園 e 化雲端服務之研究-以臺灣藝術大學爲例……*梅士杰* 1174
2. 非試不可（Facebook）--另類的幼兒園親師交流…… *童巧雯、邱淑惠* 1180
3. 多媒體影音部落格於幼兒教育親師生關係與互動提升之研究……*梁佳蓁、吳俊霖* 1186
4. 亞洲大學協同合作辦公室建置經驗……*潘信宏、陳家妍、陳柏淩、鍾仁宗、劉嘉政* 1192
5. 學生學習成效分析－以國立臺北藝術大學爲例……*黃國倫、張翠琳* 1198
6. 網路電話系統在行動節費之應用……*陳家祿、楊世偉* 1203

Session S1：智慧生活科技 10 月 25 日(五) 09:00-10:40 Room 6

1. 下一代台灣電子發票系統與載具之評估與開發
……*賴源正、黃淑容、陳韋如、陳彥宏、馮壽元、林榮輝* 1209
2. 基於影像分析技術之自動化水位偵測警戒系統
……*曾建澔、羅世瑋、陳倫奇、吳志泓、林芳邦* 1215
3. I Know You: 智慧型家庭網路影音傳送系統
……*黃宏宗、林正倫、阮明英、胡誌麟、蘇奕宇、劉炳傳* 1221
4. 影像查詢技術應用於展場導覽系統設計之研究……*黃國峰、施成憲、林善智、游耿能* 1227
5. 中醫症狀詞庫的研製……*葉明憲、郭慧翔、林迺衛* 1233
6. 中醫病因及臟腑辨證系統的研製……*葉明憲、林育欣、林迺衛* 1239

Session S2：智慧生活科技 10 月 25 日(五)11:00-12:40 Room 6

1. 環境災害管理資訊系統行動通訊軟體之建置……*吳效遵、羅榮華* 1245
2. 基於 Wi-Fi 與 Bluetooth 混合式無線識別技術門禁控制系統之設計與實作
……*徐茂馨、劉嘉惟、高駿嘉、廖子翔、蘇暉凱* 1251
3. 虛擬實境結合網頁體感用於家具擺設之研究……*張晉豪、徐豐明* 1257
4. 基於 Wi-Fi 之家庭環境監控系統建置……*陳嚮亮、張書愷* 1263
5. 綠色農場遠端自動化監控系統之研究……*陳嚮亮、陳廷宗、林昆輝* 1269

Session S3：智慧生活科技 10 月 25 日(五) 09:00-10:40 Room 7

1. Android 平台之旅遊規劃與事故偵測系統……*吳思陳、羅壽之* 1276
2. 無鼠不在-Android 系統上的無線滑鼠……*謝瑞宏、張博誠、李昱穎* 1281
3. 建立於 Android 系統之鑰匙自動辨識系統……*王建仁、沈英謀、蔡哲民、鄭承淵* 1286
4. 以智慧型手機之定位功能結合微控裝置實現節能家電控制……*程榮祥、廖健智、林家鵬* 1291
5. 雲端同步通訊錄與防詐騙系統……*廖子萱、李貞穆、劉名皓、盧聖軒、方文聘* 1297
6. 基於智慧手機的室內 PDR 定位系統模組化快速開發平台
……*林恭煥、石佳雯、許雅婷、簡嘉瑩、廖峻鋒* 1301

Session T1：數位學習與系統應用 10 月 25 日(五)11:00-12:40 Room 7

1. 融入基因演算法進化演算特性之進化式教師介聘多角調作業
— 以臺閩地區公立國民中小學暨幼兒園教師介聘他縣市爲例……*王修、李文堂* 1307
2. 我國「資訊素養與倫理」數位教材融入國小教學學習成效之研究
……*李治慧、林宜隆、陳志穎* 1311
3. 中小學網路霸凌防治課程之教學：教學省思之內容分析研究……*徐敏容、周倩* 1316
4. 海洋污染防治管理系統 App 軟體之建置……*游哲凱、羅榮華* 1322

Session U1：TWAREN 與未來網路規劃與設計 10 月 25 日(五) 09:00-10:40 Room 8

1. 在 BSN 網路上建立與重組可靠反向路由樹的機制……*蕭智仁、許蒼嶺* 1328

2. 應用於校園網路與監控系統網路整合之 CAN 與 TCP/IP 閘道器之設計
…… *邱日清、王子昂、侯建和* 1334
3. 軟體定義網路下(SDN)跨網域之端對端自動拓樸與流量檢視…… *黃文源、胡仁維、劉德隆* 1338
4. 使用隧道技術實現網路虛擬化……*曾惠敏、胡仁維、劉德隆* 1344
5. TWAREN 網管 Flow 監控機制之設計與實作…… *梁明章* 1350
6. Cross domain VM migration over TWAREN OpenFlow testbed…*李慧蘭、劉德隆、胡仁維、陳敏* 1355

Session V1：電子商務 10 月 25 日(五)11:00-12:40 Room 8

1. 半導體業以 ETL 方式建構 B2B 系統方法之開發及應用…… *張永昌、范金鳳* 1359
2. 基於 3D 列印技術與社群工藝的文化創意產業生態系
…… *周忠信、張哲綜、陳丁加、楊尚仁、謝翰誼、王立志、陳怡文* 1365
3. 相容於 NFC 之匿名行動付款協定…… *羅嘉寧、楊明豪、黃思穎、蔡卓倫* 1369
4. 結合安全測試與異常偵測之防範架構降低電子商務安全風險……*賴森堂、羅翊萱* 1375
5. 以科技接受模式探討智慧型手機與 QR Code 結合的購買行為意圖之研究
…… *王俊嘉、陳美鐘、曾珈儒、周珉如* 1381

下

冊

基於物聯網架構之電器導向雲端能源管理平台

林偉益[1] 陳瑋哲[1] 賴槿峰[2] 黃悅民[1] 鄭鈺霖[3]
[1]國立成功大學 工程科學系
[2]國立中正大學 資訊工程系
[3]財團法人資訊工業策進會 雲端系統軟體研究所
cinfon@ieee.org

摘要

近年來由於物聯網議題逐漸受到重視，政府與研究單位已積極合作進行物聯網基礎架構之建置，同時隨著智慧聯網與雲端能源管理系統議題之興起，而透過電器識別之技術將可有效地協助使用者了解現正使用中的電器，進一步改善自我用電決策。然而針對一般雲端用戶之用電習慣，同時開啟與關閉多台電器的可能性是存在地，因此本研究探討於平行狀態進行多電器辨識，亦即提供多台電器同時開啟與關閉之電器辨識。本研究提出基於物聯網架構之電器導向雲端能源管理平台的設計，利用電器偵測得知電器使用狀況進而提供能源管理的能力進而提供異質裝置整合的服務，同時，本研究透過建立資料庫機制、電器特徵分群與波形辨識方法，解決當前電器辨識系統大資料量的問題。且相對於其他電器辨識系統，本研究採用低階嵌入式系統晶片提供低功耗的優勢，同時具備高度擴充性與易用性。在實驗過程有別於其他電器辨識系統之研究環境，考量到並行式多電器辨識與普遍使用者之用電習慣，本研究在實驗於一般日常用電習慣下，總系統辨識率可達 86.14%，而單一電器總辨識率可達 96.14%，顯示本研究具有高度可行性。

關鍵詞：物聯網，雲端能源管理平台，電器辨識。

1. 前言

近年來由於雲端運算(Cloud Computing)與智慧聯網(Internet of Things)技術的日漸茁壯，智慧雲端發展趨勢儼然進入另一個嶄新階段，各國產業界與專家學者開始著眼於智慧電網(Smart Grid)、雲端服務(Cloud Computing Service)與綠色建築(Green Building)等方向發展，而適逢能源危機與全球暖化的問題不斷被提出，能源議題亦成為各國迫切解決的國際性問題。

以智慧電網領域而言，主要可以區分為三階段探討：城鎮地區建置智慧型電錶基礎建設(Advanced Metering Infrastructure, AMI)，其中包括能源生產、管理與運輸之系統建設。配電站與雲端之間則提供自動化電錶讀取系統(Automatic Meter Reading, AMR)，取代人工抄錶造成的人為錯誤及成本。而在雲端方面則透過智慧電錶(Smart Meter)的技術，將智慧雲端控制與能源議題整合，提供一般雲端用戶即時了解雲端能源使用情況與家電控制服務，也就是所謂的雲端能源管理系統(Home Energy Management System, HEMS)。其中 HEMS 主要提供雲端之能源管控，目前產業界已有相關研究團隊進行智慧電錶開發，然而這類電錶產品多半以能源管理與控制為主且單價較高，無法受到使用者青睞，造成雲端能源管理系統無法普及。

針對智慧雲端 IoT 服務的問題，在我們先前的研究[6, 7]中，所提出的電器識別技術可對家電裝置提供一項有效且無須額外裝置的識別方式. 然而，這些技術不適合用於並行式多電器的辨識，也無法使用在輕量級的嵌入式系統上. 因此本研究中，為了克服之前研究所遇到的問題，自行設計與實作了智慧電錶與其控制軟體. 另外，也提出了一套電器導向的 IoTs 能源管理平台，該系統除了具有整合底層異質裝置的能力之外，透過智慧電錶能提供電器的使用資料，這些資料能進一步提供給能源管理或行為辨識模組使用.

此研究工作共有三項貢獻. 第一，所提出的系統能單純利用電器偵測得知電器使用狀況進而提供能源管理的能力. 該系統也符合 IoT 架構，透過服務導向的標準與設計，使得雲端使用者方便管理電器. 第二，系統能提供異質裝置整合的服務. 對於現今物聯網系統之實現，其最大的挑戰在於如何有效地整合各種不同協定之裝置，達到物與物溝通之服務，本系統將設計包含現今家用裝置如何加入物聯網路以及提供各種不同協定之溝通機制. 第三, Smart meter 的設計與實作. 在硬體方面，為了提供簡易安裝與低成本之特性，智慧電錶的設計以延長線為基礎; 採用較低階的嵌入式系統為核心架構來提供低功耗，低成本的特性. 採用低階嵌入式系統硬體後，系統必須面對運算量與空間相關的問題. 此研究提出了輕量化的並行式多電器辨識演算法於中介軟體中實作，使得智慧電錶上的少量電器能同時有效地被辨識. 另外，因為電器的辨識在智慧電錶中進行，所以電能感測的資料不需要一直送往能源管理平台分析，平台僅需要儲存辨識後的結果. 完整的波形資料庫只會放置在平台伺服器中, smart meter 只會儲存最近使用到的電器波形.

2. 相關文獻

美國牛津大學的氣候變遷協會研究指出「當使用者有辦法取得家中用電資訊，可節省 5%~10%能源」。在 T. Ueno et al. [8] 的研究中提出一能源消耗資訊系統(Energy Consumption Information System)，根據統計可省下 12%能源消耗。J. E. Petersen et al. 的研究[9]指出當使用者可即時獲得監控系統之能源訊息,可節省 32%的能源消耗. C. Fischer et al. [10]的研究也再次驗證若使用者可以了解用電資訊，可省下約 12%的能源消耗。由此可見，因不同地域環境與用電習慣下對於能源的損耗量略有不同，然而當使用者有效掌握用電資訊，將可有效降低能源的損耗。故適時地提供使用者用電資訊，可有效改善使用者的用電習慣，進而達到節約能源的效果，因此智慧電錶的議題也就成為能源研究趨勢之一。除了能源管理議題,由於目前感測器的發展越趨進步，無論是在居家照護[18,19]、無線感知網路的相關應用[20]以及感測器網路的安全性[21]等均有許多探討。

智慧電錶(Smart Meter)是智慧電網的最後一層，藉由電錶的自動化可提供使用者更詳盡的用電資訊，直接影響到使用者的用電狀況，並且提供自動抄錶的服務。現今智慧電錶的研究可分為兩大方向，第一電力線設計，現今一般雲端用戶所使用的無熔絲開關總錶可承受 50A 之電流源，此類設計由於針對的是大功率的總線，故需要高階儀錶進行測試。第二種是延長線設計[11,15,16,17]，延長線設計又稱智慧插座(Smart Socket)，此類電表有單個或多個插座並包含電壓以及電流的感測器，有的亦具有網路傳輸模組可將量測資料透過有線或無線網路傳遞，而有的則具有控制功能，可藉由繼電器來控制插座上的電器。但如果要精確地達成電器控制，那麼藉由智慧電表來實現電器辨識將是必須的。智慧電表有三項主要設計目的. 第一，提供延長線的家電控制服務，包括繼電器(Relay)控制、紅外線遠端控制。第二，降低電流感測範圍，提供更完善且安全的能源資訊系統。第三，與環境無縫整合，電力線電錶設計由於裝設不易，因此擴充性較差，反之，延長線設計提供智慧雲端更大的擴充彈性。而這類智慧電錶通常會內建一組 LCD 顯示幕，提供使用者較簡略之用電資訊與相關建議內容。

針對智慧插座設計, Hyun Sang Cho et al.[11]提出了智慧型多電源插座(Smart Multi-Power Tap, SMPT)來取得智慧插座之位置資訊，以備往後情境感知系統可以使用.在 Seunghyun Park et al.[12]的研究針對智慧電錶因其資料量大，進行資料簡化並進行預測以減少資料傳遞之負擔，並驗證其準確率. Smart Energy-saving Power Module (SEPM) 於 YE Yingcong et al.[13]的研究工作中發表，該模組設計由一低成本邏輯電路實作並配合微處理器來讀取電能資訊，針對量測到之電能資訊進行相關分析. 同時也設計了 Self-Locking loop，當電器進入待機狀態或使用者設定之門檻值時，系統會自動關閉微處理器與電器的運作，藉此降低待機時間所消耗之電能。

另外一類智慧插座提供有線/無線輸出設備將資訊輸出至網頁伺服器、智慧型手機端或電腦系統中。Naoyuki Morimoto et al.提出智慧插座的研究[14]，其中插座內提供電器控制與能源感測器，收集到的資訊將會透過 Wi-Fi 或乙太網路回傳至 Server 端處理，藉此讓使用者可以遠端查看家中能源管理系統資訊.

本研究所提出的非侵入式智慧電表除了感測電能資訊之外也進行資料分析以取得插座上的電器的資訊. 透過無線傳輸模組,少量的資訊會送往能源管理平台儲存, 這能避免大量 raw data 的傳送, 降低傳輸層的壓力. 這智慧電表不僅能整合進 iot 架構的系統也提供低成本與易安裝的特性.

3. 系統架構

為了有效整合 IoT 與 HEMS, 在本研究中, 我們提出了一項以 OSGi 為中介軟體的 Appliance-oriented HEM Platform (AOHEMP) 設計. 系統架構如圖 1 所示. 系統採用 Service-Oriented Architecture (SOA)模型標準, User Client 非常容易存取系統資訊. 系統的底層能連結各種協定的末端裝置; 在本研究中，將以 ZigBee、Bluetooth 和 TCP/IP 的溝通協定的裝置為主.

依據功能與架構, 系統能視為由三層結構所組成. 第一層結構是 Heterogeneous Network Packet Model. 現今許多裝置的網路傳輸界面都各自不同, 其中有些裝置同時擁有多種界面. 異質網路裝置是指一群擁有不同傳輸界面的裝置. 這些裝置透過此模型將可有效轉換其傳輸封包及格式，以方便向上遞送至中介軟體模組，進行註冊及協定溝通。Appliance-oriented Middleware (AOM) 是第二層結構, 包含中介軟體模組、隨插即用系統的處理 Bundle、異質網路協定轉換 Bundle, Smart Meter Module, Service Bundle. 這些元件是系統的核心軟體, 能使上下層結構正常協同運作. 最後一層結構是應用與服務中介軟體模組. 它能提供一個軟體開發框架和雲端電器應用服務.

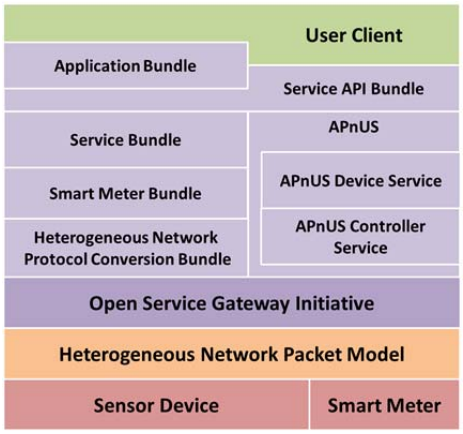


圖 1 系統元件架構

3.1 Heterogeneous Network Packet Model

Heterogeneous Network Packet Model 的功能對末端裝置與 AOM 兩者在相容性整合方面有非常大的效用。根據 iot 架構，圖 1 中的 sensor device & smart meter 屬於感知層. 感知層上的物件其資料匯整與控制由 AOM 指揮或協調. 感知層與 AOM 之間的資料傳輸由此模型定義封包規範. 傳輸層中的同質網路裝置能自行互相交換資料，而異質網路裝置則需要透過 AOM 的交涉來連結. 因此，在各種不同異質網路的通訊前，必須根據模型封包規範來轉換封包格式. 模型目前定義三種封包格式: 初始化封包(Init Packet)，命令接收封包(Command Packet)，狀態回傳封包(Respond Packet).

圖 2 為其封包格式，初始化時會傳送五個最基本內容，分別為 State、Protocol、Addr、Device name、Service 以及 Description。State 為此封包的用途，Protocol 是為無線通訊模組溝通協定，Addr 是無線通訊模組自述位置，若以 Zigbee，其夾帶就會是 PanID、Address、Channel 之類。Device name 則是此末端裝置名稱。Service 則是敘述此末端裝置是屬於何種服務，Description 為比較常一串描述裝置的資訊。除了上述基本內容，其後面還會有 Number of Action 和 Action，來敘述此末端裝置可以有的服務控制。Action 封包裡面有控制名稱(name)、控制描述(Description)、控制資料流向(Dir)、控制參數與參數數量(Arg)、控制狀態數值(Val)。初始化封包是此三個最長的，這是因為跟 OSGI Framework 註冊時須告知其裝置詳細資訊，因此在命令接收封包則會減少，基本只保留 State、Addr 跟 Device name，後面一樣為 Number of Action 和 Action，Action 減少為 name、Dir、Arg。在狀態回傳封包基本跟命令接收封包一樣，後面的 Action 不一樣，改為 name、Dir、Val。

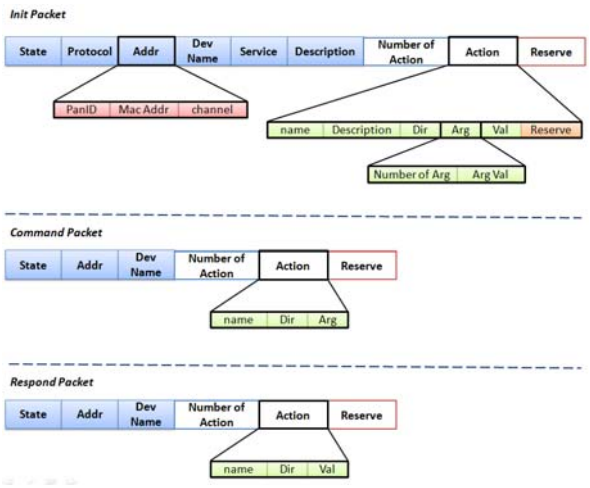


圖 2 傳輸封包格式

3.2 Appliance-oriented HEM Platform

在 iot 三層架構中，AOM 屬於應用層與傳輸層的 middleware，所以 AOM 在整個 AOHEMP 中扮演著核心的角色. 由於目前 iot 裝置使用的網路協定眾多，缺乏共同依循的標準，會造成不同網路協定互通性的問題。對於要讓物與物之間能夠互相溝通，這種不相容的情形不僅會造成相當多困擾。因此，讓這些網路協定與控制方法能夠協同運作，必須要設計 Middleware 來處理此項事務。除了建構中介軟體之外，還需考慮提到 AOHEMP 的特性，例如可彈性客製化加入中介軟體、末端裝置的服務告知等。因此在 AOHEMP 與末端裝置間會有裝置的註冊，事件處理，命令控制等相關功能.

3.2.1 Heterogeneous Network Protocol Conversion Bundle

異質網路協定轉換 bundle 負責配接傳輸層中的網路界面，提供非 TCP/IP 通訊協定的異質網路溝通. AOM 採用 UPnP 技術來連接感知層，其他的傳輸協定使用虛擬 APnUS 裝置支援. 異質網路裝置由 AOM 中的虛擬裝置配接傳輸界面並遞送資料. 此 bundle 需與異質網路末端裝置整合，根據末端裝置與 AOHEMP 的溝通制定其相關的溝通協定。由於一般末端裝置使用的網路協定可以分為長距離有線通訊、長距離無線通訊、短距離有線通訊、短距離無線通訊，由於為數眾多，為了長途發展，在異質網路協定轉換 bundle 會規劃保留其擴充性，以便未來可以相容更多的網路通訊協定。異質網路協定轉換 bundle 將以 OSGI Framework 為基底，開發異質網路協定轉換 bundle，其特性有底下幾點：

1. AOHEMP 支援接收傳輸網路通訊協定的驅動程式。
2. 需持續監聽 iot 末端裝置狀態，提供註冊服務功能。
3. 可讓與 AOHEMP 相連的末端裝置變成虛擬的 APnUS 裝置。
4. 匯集末端裝置的資訊與功能，提供生成 APnUS 控制點需要的 description.xml 檔案。
5. 對於 UPnP 控制點的控制命令轉換成與 iot 末端裝置可溝通的封包欄位。

圖 3 是整個異質網路協定轉換 bundle 的基本架構，為了保留擴充性，在 bundle 中設計了幾個功能. 核心為 Device Management Service，提供兩大應用程式介面功能，一是對 iot 末端裝置提供 Device Plug-In API，其二是對 APnUS AV bundle 提供描述功能與控制方式服務的 Virtual APnUS Device API。Device Management Service 主要是針對物聯網末端裝置提供註冊功能，當末端裝置對異質網路協定轉換 bundle 註冊時，服務包會把末端裝置所提供的資訊紀錄於其表單上，並且對末端裝置有監聽(Listen)功能，來監看目前末端裝置的狀態，除此之外還會對 Device Plug-In Bundle 做出呼叫控制功能.

Device Plug-In Bundle 是額外的 bundle，主要是給之後要擴充的末端裝置不同的網路協定來使用，本研究會為之設計其功能介面以及 Device Plug-In API 開發介紹，讓之後開發者可以對自己的末端裝置開發其符合本計畫架構的 bundle 並與 AOHEMP 相容，所開發完的 Device Plug-In Bundle 可以透過系統的網路管理模組來進行載入。

Virtual UPnP Device API 的用途就如同前文所敘述，非 TCP/IP 的裝置將透過 Device Management Service 進行註冊後模擬成 APnUS 裝置，在這裡會將 APnUS 中的定址(Addressing)和探索(Discovery)重新設計，取代掉 TCP/IP 的傳輸方式，匯集末端裝置描述檔，並儲存成 description.xml 檔案，釋出 Virtual APnUS Device API 提供 APnUS AV bundle 呼叫。

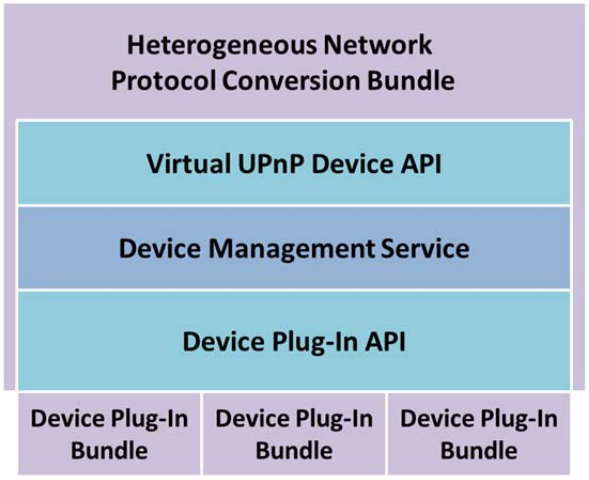


圖 3 異質網路協定轉換 bundle

3.2.2 Smart Meter Bundle

此 bundle 除了處理 smart meter 要求的相關事務之外，還要負責波形特徵分群與波形資料庫管理. smart meter 要求的事務有波形特徵學習與搜尋波形資料. 當 smart meter 在學習流程時，會擷取出當下的電器波形與特徵資料，這兩種資料會送給 Smart Meter Bundle 進行波形特徵學習. Smart Meter Bundle 會把收到的波形資料合併已儲存的其他波形，並判斷是否需要重新建立特徵索引. 如果要重建特徵索引，就會接著進行波形特徵分群，並儲存新的索引值到資料庫. 在辨識流程時, smart meter 會要求 database proxy 回傳波形比對目標. 如果 proxy 找不到目標，就會要求 Smart Meter Bundle 去搜尋波形資料庫.

3.3 Application and Service Middleware Module

該模組在系統設計中是最高階層的結構，包括 Service Bundle, Service API Bundle, Application Bundle. 其功能是提供電器應用服務與軟體開發框架給使用者. Application Bundle 主要負責裝置應用服務，包含裝置的管理與節能建議. Service Bundle 匯集所有的服務，像是系統原生服務和雲端裝置服務. Service API Bundle 提供類似軟體開發框架的功能. 透過 API，使用者能存取 AOHEMP 中的資源或是與 Bundle 互動.

由於在設計服務導向中介軟體平台時考慮到 SOA，SOA 主要目的是降低異質系統整合成本的分散架構，其包含了五種特性：

1. 具有模組性架構。
2. 模組可以達到跨平台使用。
3. 定義服務介面以及模組溝通。
4. 服務介面(Interface)與服務實現(Implement)須分離。
5. 服務可被不同系統呼叫應用，具有分享性。

SOA 最普遍的架構即是 Web Service 的架構. 在 Web Service 規格中, UDDI (Universal Description, Discovery, and Integration)是核心標準之一. 它是一個基於 XML 的跨平台的描述規範，可以使世界範圍內的企業在網際網路上發布自己所提供的服務，也使企業在網際網路上可以互相發現並且定義業務之間的交互. 互動流程 Service Provider 使用 Web Services Description Language (WSDL) 發佈服務到 Discovery Agencies，Discovery Agencies 用 UDDI 規範提供服務描述，讓 Service Requestor 可以找到，之後 Service Requestor 和 Service Provider 會建立起互動關係，並透過 SOAP 去完成服務交易。

軟體開發框架根據 SOA 標準模型來定義設計，它可以開發系統未來可擴充的特性。為了達到 SOA 的特性，系統由 Service API Bundle 來曝露相關的功能，讓使用者透過 web Service 做終端開發，其架構如同圖 4. 本系統的軟體發開框架 API 規格有 AOHEMP 資訊設定 API, AOHEMP 隨插即用 API, 裝置服務描述 API, 裝置服務控制 API 這四類.

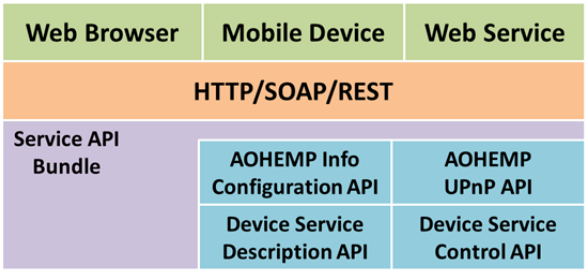


圖 4 Service API Bundle

AOHEMP 資訊設定 API 主要是針對 AOHEMP 本身機器的設定或是取得其本身資訊. AOHEMP 隨插即用 API 則是針對在中介軟體中的隨插即用的功能，而裝置服務描述 API 與裝置服務控制 API 為在 AOHEMP 上註冊的裝置描述與控制方法。此 API 在未來乃會針對需求做擴充。

在資料交換標準方面，通常會以 SOAP 或者是 REST 為主。但考慮末端裝置的即時性與 footprint 的大小較高，一般通常使用 REST，REST 是使用 HTTP、URI 在加上請求方式，像是 GET、PUT、POST、DELETE。

4. 智能電錶

本研究設計的 smart meter 主要由電能感測模組, Microcontroller Unit (MCU), transmitter 組成，其架構設計如圖 5, 依功能可區分為三種的層狀結構. Smart meter 最大的能力只在電器辨識，如果有更高階的功能，如智慧雲端與智慧電網的應用，會在 AOHEMP 中設計，由 service Bundle 提供.

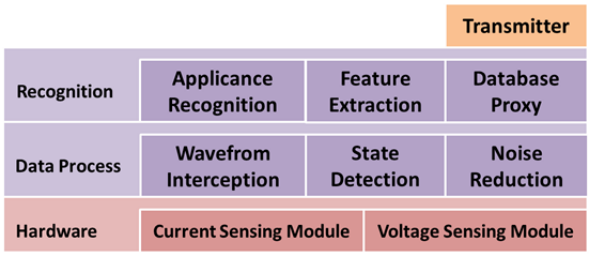


圖 5 異質網路協定轉換 bundle

硬體層為 smart meter 的硬體設計層面，主要負責電能訊號之處理，包含完整電能訊號感測，訊號擷取、資料調整等方法，提供資料處理層初步之原始電壓與電流訊號. 資料處理層與辨識層兩者皆在 Microcontroller Unit (MCU)內部進行運算. 資料處理層是進階處理硬體感測資料的部分，包括內部電流波形擷取方法、雜訊抑制與狀態偵測三大部分。主要負責提供電器辨識演算法所需要之電器特徵的前處理，藉由此階段的資料處理可大幅降低硬體層所造成之雜訊，同時增加系統之辨識率與準確度。辨識層為本論文之核心方法，包括波形辨識演算法、資料庫代理與特徵擷取. 其主要負責從資料處理層遞交的電器波形中擷取出電器特徵，這些特徵能視為波形資料的索引透過資料庫代理來取得要比對的波形類型. 資料庫代理是波形資料庫的快取，這是為了提供核心波形辨識演算法有較佳的辨識對象，也藉此降低辨識運算之時間複雜度。

4.1 Smart Meter Working Process

Smart Meter 的運作有兩種工作流程，學習流程與電器辨識流程,. 這兩種流程有部份步驟是相同的，即電能訊號感測，波形資料處理，特徵擷取. 完成整套的學習流程需要 Smart Meter 與 smart meter bundle 一起參與; smart 只參與前部份，而其餘部份會在 AOHEMP 上完成. 在學習流程中, smart meter 從感測電能訊號一直到擷取波形特徵的運算，都是它的工作. 接著會把完整電器波形與波形特徵透過 transmitter 送往 AOHEMP 進行後續的學習流程, smart meter bundle 會把學習的結果存放在 AOHEMP 中的資料庫. 電器辨識流程就如 smart meter 三層結構，在 hardware layer 感測電能訊號，在 data process layer 進行電器波形處理與校正，最後在 recognition layer 處理電器特徵和辨識電器種類.

電器辨識流程基本上所有步驟都在 smart meter 中完成，除非在 database proxy 中沒有可比對的波形資料時，才會去跟 AOHEMP 要求比對目標(target). database proxy 儲存著最近比對過的波形資料與其特徵索引; 而完整的波形資料庫只放置在 AOHEMP 中的資料庫. 圖 6 描述了辨識流程的詳細步驟. 當電器插進 smart meter 後，meter 將擷取到的電壓值作為觸發取出電流瞬間值集合，並將其儲存至滑動視窗的視窗區間中。接著透過滑動視窗進行狀態偵測與雜訊抑制的過程，得到取樣的電流波形與波形特徵。根據波形特徵值在 database proxy 中找出要比對的目標. 最後, smart meter 利用 Dynamic Time Warping algorithm 完成電器辨識.

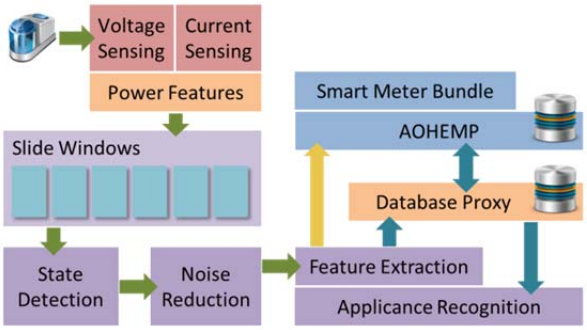


圖 6 電器辨識流程

5. 實驗結果

5.1 實驗環境

本研究採用下列五種電器作為分析資料組，如表 5.1 所示，分別為循環扇、筆記型電腦、LCD 螢幕、檯燈與熱熔槍。

表 5.1 實驗用電器列表

Type	Status			
Recirculation Fan	Close	Weak	Medium	Strong
Notebook	Close	Power saving	High performance	N/A
LCD Monitor	Close	Open	N/A	N/A
Bulb	Close	Open	N/A	N/A

5.2 平行式多電器辨識

為了測試本研究提出之電器辨識系統於平行式多電器環境之準確度，此章節將針對所有電器狀態之組合進行分析。而為了模擬電器在同時間開關之情況，本研究透過市面販售之多孔延長線進行輔助，透過多孔延長線所附之開關可以同時開啟多台電器。其中本研究使用之數據驗證部分是採用資料探勘之正確性評估法。

精確率(precision)代表在"所有被判定為 a 電器類別之集合中，取出真正為 a 電器的資訊"，精確率越高表示誤判率越低，如式 5.1 所示。

p=TP/((TP+FP))……..……..(式 5.1)

回復率(recall)則代表"實際為 a 電器的取樣中，同時也被判斷為 a 電器之比率"，定義如式 5.2 所示，在此本研究採用回復率為樣本空間中辨識率(Recognition Rate)的依據。

r=TP/((TP+FN))……..……..(式 5.2)

平行式多電器辨識測試中，本研究將透過隨機抽取不同電器組合的方式，並且透過本研究採用之電器辨識演算法進行電器的判斷。

此階段由四種電器中隨機抽取兩部進行辨識，本研究於此進行 174 次電器辨識過程，結果分析如下表 5.3 所示，其中評估法採用二元分類方式，也就是當兩部電器完全被辨識到時就是 TP，反之就是 FN。

表 5.2 兩電器組合辨識結果

No.	Combination	TP	FN	FP	TN	Recognition Rate (%)
1	Fan (Strong) Monitor	13	2	1	158	86.67
2	Fan (Medium) Monitor	18	3	2	151	85.71
3	Fan (Weak) Monitor	15	0	3	156	100.00
4	Bulb Monitor	14	1	0	159	93.33
5	Monitor NB(Power saving)	12	3	0	159	80.00
6	Fan (Strong) Bulb	12	3	2	157	80.00
7	Fan (Medium) Bulb	13	2	4	155	86.67
8	Fan (Weak) Bulb	15	1	0	158	93.75
9	Bulb NB (High performance)	10	5	0	159	66.66
10	Fan (Strong) NB (High performance)	12	3	0	159	80.00
11	Fan (Weak) NB (Power saving)	16	1	0	157	94.12
Total						86.21

從表中可以看出筆記型電腦與循環扇中的狀況較差。經過分析後發現，循環扇中等狀態的電流波形與波幅與循環扇弱狀態相差十分微小，推斷其為造成循環扇誤判的主要原因。

此外，由於此階段採用之電器辨識是同時針對兩部電器進行辨識，然而整體辨識率為 86.21%，為了分析影響整體系統辨識率之原因，其個別之辨識率也是本論文所感興趣的結果。

6. 結論

本論文提出基於物聯網架構之電器導向雲端能源管理平台，透過 SOP 協定可以快速且方便地將訊息在物與物之間進行傳遞，電器辨識方面，由於等量分割分群演算法可能因為特徵密度不均衡導致 Skewed cluster tree, 就算使用一般的分群演算法也無法避開這個問題, 此研究未來待解決的議題.

致謝

“本研究依經濟部補助財團法人資訊工業策進會「 102 年度雲端運算系統及軟體技術研發計畫 (2/3) 」辦理“以及國科會編號”102-2219-E-194-002”, “101-2628-E-194-003-MY3” 計畫

參考文獻

[1] Appliance-aware Activity Recognition Mechanism for IoT Energy Management System

[2] An Intercommunication Home Energy Management System with Appliance Recognition in Home Network

[3] Multi-appliance Recognition System with Hybrid SVM&GMM Classifier in Ubiquitous Smart Home

[4] Home Energy Management System for Interconnecting and Sensing of Electric Appliances

[5] An Intercommunication Home Energy Management System with Appliance Recognition in Home Network

[6] Multi-appliance recognition system with hybrid SVM/GMM classifier in ubiquitous smart home

[7] T. Ueno, R. Inada, O. Saeki, and K. Tsuji, “Effectiveness of Displaying Energy Consumption Data in Residential Houses: Analysis on how the residents respond,” In Proceedings of European Council for an Energy-Efficient Economy Summer Study, pp. 1289-1299, 2005.

[8] J. E. Petersen, S. Vladislav, K. Janda, G. Platt and K. Weinberger, “Dormitory residents reduce electricity consumption when exposed to real-time visual feedback and incentives,” Sustainability in Higher Education, Vol. 8, No. 1, pp. 16-33, 2007.

[9] C. Fischer, “Feedback on household electricity consumption: a tool for saving energy?,” Energy Efficiency, Vol. 1, No. 1, pp. 79-104, 2008.

[10] H. S. Cho, M. Hahn, T. Kato and T. Yamazaki, “Simple and robust method for detecting the electrical appliances using markers and programmable logic devices,” In Proceedings of the IEEE 13th International Symposium on Consumer Electronic, pp. 334-338, 2009.

[11] S. Park, H. Kim, H. Moon, J. Heo, and S.Yoon, “Concurrent Simulation Platform for Energy-Aware Smart Metering Systems,” IEEE Transactions on Consumer Electronics, Vol. 56, No. 3, pp. 1918-1926, 2010.

[12] Y. Yingcong, L. Binqiao, G. Jing and S. Yehui, “A Design of Smart Energy-saving Power Module,” In Proceedings of the IEEE Conference on Industrial Electronics and Applications, pp. 898-902, 2010.

[13] N. Morimoto, M. Tanaka, T. Akehi, M. Yoshida, H. Yoshimizu, M. Takiyamada and Y. Kamimura , “The Design and Implementation of a Smart Tap for Policy-based Power Management,” In Proceedings of the IEEE Consumer Communications and Networking Conference, pp. 280-284, 2012.

[14] H.Serra, J.Correia, A.J. Gano, A.M. de Campos, and I.Teixeira, “Domestic Power Consumption Measurement and Automatic Home Appliance Detection”, Proceedings of the IEEE International Workshop on Intelligent Signal Processing, pp.128–132, September 2005.

[15] M. Ito, R. Uda, S. Ichimura, K. Tago, T. Hoshi, and Yutaka Matsushita, “A Method of Appliance Detection Based on Features of Power Waveform”, Proceedings of the International Symposium on Applications and the Internet, pp. 291-294, August 2004.

[16] J. Heo, C.S. Hong, S.B. Kang, and S.S. Jeon, “Design and Implementation of Control Mechanism for Standby Power Reduction”, IEEE Trans. Consumer Electronics, Vol. 54, No. 1, pp. 179–185, February 2008.

[17] 18. Y. M. Huang, M. Y. Hsieh, H. C. Chao, S. H. Hung, and J. H. Park, “Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks”, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 27, NO. 4, MAY 2009.

[18] C. F. Lai, Y. M. Huang, J. H. Park, and H. C. Chao, “Adaptive Body Posture Analysis for Elderly-Falling Detection with Multisensors”, IEEE Journal on Intelligent System , Vol.25, No.2, pp.20-30, March 2010.

[19] H. C. Huang, Y. M. Huang, and J. W. Ding, “An implementation of battery-aware wireless sensor network using ZigBee for multimedia service”, Proceedings of the IEEE International Conference on Consumer and Electronics, pp. 369-370, February 2006.

物聯網之電器感知活動識別方法於雲端能源管理平台

陳瑋哲[1]　林偉益[1]　賴槿峰[2]　黃悅民[1]　鄭鈺霖[3]
[1]國立成功大學 工程科學系
[2]國立中正大學 資訊工程系
[3]財團法人資訊工業策進會 雲端系統軟體研究所
cinfon@ieee.org

摘要

物聯網其主要是將各種的末端裝置通過識別訊息傳遞將設備與網際網路建立其連結網路，其不僅是延伸和拓展網際網路的範疇，並可建構出現實生活中物件與網際網路通訊的橋梁。隨著能源危機的意識抬頭，智慧節能成為目前各界發展的新趨勢，本論文主要提出一套物聯網之電器感知活動識別方法於雲端能源管理平台，其主要對於現今家電裝置整合性問題提出一中介管理服務層，其不僅解決其各電氣間溝通服務，透過其以服務導向架構提供上層服務應用程式，並進一步地根據現今使用中之電器及其狀態之變化推論出其行為識別與進行其電器能源管理服務。

關鍵詞：電器感知活動識別, 雲端能源管理平台。

1. 前言

物聯網其精神為透過運用無線射頻辨識技術、全球衛星定位系統、掃描儀、紅外線及各種訊息感測裝置進行資訊擷取與交換。主要解決物與物(Thing to Thing)、人與物(Human to Thing)、人與人(Human to Human)之間的互聯並提供資訊的交換及眾多的服務。在 2008 年時，美國總統歐巴馬提出『物聯網振興經濟戰略』，確定將物聯網列入國家發展重點之一，並積極推動感測裝置技術與智慧型基礎設施建設。歐洲方面，在 2009 年，從歐盟聯網領域的專業研究組，先後公佈多份規劃歐洲物聯網未來發展動向報告。如『歐盟物聯網行動計畫』、『物聯網戰略研究路線圖』、『未來物聯網戰略』、『物聯網戰略研究路線圖』。內容包括物聯網管理體制制定、資安問題以及通訊標準化等重點。歐盟第七框架計畫(7th Framework Programme，FP7)也在 2011 年工作計畫，確立在 2011 年至 2012 年期間 ICT 產業領域優先發展項目。日本方面，2009 年八月提出 i-Japen 國家藍圖中，成立一個國家級的專任 CIO 職務，負責推動日本電子化政府的所有事務，社會資訊服務。同年韓國也通過『物聯網基礎設施構建基本規劃』。而中國大陸也提出『感知中國』，積極發展傳感網應用以及其關鍵技術，達到『全面感知，可靠傳遞，智慧處理』。

物聯網隨著技術的發展，新的感測器類型也不斷產生，常見的感測器有速度、溫度、濕度、壓力、位置、液面、能源消耗、輻射線、震動等等。不同感測器能達成不同的應用，如航空技術、能源管理、環境保護與生物科學等。感測器偵測到訊號之後，經過數位訊號處理器對訊號進行相對應之分析及比對之後，再將其結果輸出。「辨識」在智慧聯網中扮演著舉足輕重的角色，其判定智慧聯網設備之身分屬性，除了提供給訊息處理系統做分析處理之相關動作，也可透過身分認證加強智慧聯網系統安全性。

然而現今對於開發物聯網將會面臨一些問題：

1. 管理制度問題：由於各領域服務性質不同，其管理的層級也會有所不同，其通用性相對來講較低，很難建立起全球可互用的管理系統。
2. 安全性問題：由於要達到萬物皆可連網可達到智慧控制，因此，須有技術性解決方面來確保人與物之安全隱私。
3. IP 不足及設定困難度：物聯網基礎設施建設，使得未端裝置皆可上網，有可能導致全球 IP 不敷使用，並且對尚未支援網路功能之裝置將產生無法相容之問題或需透過額外識別裝置所造成之成本負擔。
4. 標準化問題：物聯網目前尚未有一個全球認同之標準，加上物聯網技術標準眾多，如通訊網路傳輸、設備操作、資安問題、中介軟體等。

其中針對於第三項挑戰，我們在先前的研究中[1, 2]透過電器識別之技術可對於現今大多數的家電裝置提供一項有效且無須額外裝置的識別方式，在本研究中將延續此電器識別技術作為基礎，進一步提出一套電器導向之 IoTs 能源管理系統，藉由一中介層將其識別完成之裝置加入此管理系統並提供各種不同通訊協定之整合服務，讓其不同通訊協定之裝置能藉由其中介系統達到彼此溝通之服務。

本研究根據現今電器使用之狀態及其變化推論其現今使用者行為狀態，透過此方式進一步對於不需要之電器關閉提供節能服務亦或者自動開啟使用者所需之電器裝置以提供更便利之控制應用。

2. 相關文獻

家庭能源管理系統（ Home Energy Management System, HEMS)為一基於智慧家庭環

境下所發展出的一套技術，其目的是為了減少並管理家用能源的損耗，其中整合了智慧電表、家庭用電控制系統。美國、歐盟以及日本等國家皆極力推行 HEMS。其中包括日本日立、松下、東芝、三菱電機等公司在 1997 年 12 月成立 ECHONET(Energy Conservation and Home Network)協會，目標是建立標準化家庭網路規格，並開發聯網功能的家電，實現家庭能源管理的服務。歐盟亦投入 HEMS 的發展，於 2006 年 1 月成立了「Econ' home」計劃，其中參與國為英國、法國、德國、葡萄牙、義大利及比利時，主要標榜住宅節能為目的，該計畫著重於家庭用電習慣、運輸用電與綠能建築三大方向，有效率降低能源耗損。美國方面則導入專家系統用於建置 HEMS，開發出 Home Energy Saver 網站，提供使用者了解自身用電資訊、相關用電決策與環境狀況診斷等服務。

現今的學術界已有相當的研究在探討 HEMS [3, 4]，其中包括能源管理系統平台設計、通訊協定設計以至於軟體解決方案，其主要探討方向約略可區分為：針對家用電器的耗電控制、省電模組的設計等方向。Young-Sung Sonp [5]提出使用電力線網路(Power Line Communication)建置家用能源管理系統，藉此監測智慧電表量測之耗電量，同時使用者可以藉由網路進行遠端控制，並可依據電費需求進行之用電決策的調整與自動控制機制。這類系統最大的問題就是在於，最初必須明確定義插座上的電器種類，使用性與擴充性較差。Ana Rossell´o-Busquet [6]所設計的機制為透過 OSGI 達到家電器的管理，但由於家用電器的通訊協定不盡不同，所以經由知識挖掘的規則引擎機制進行分析，決策出最適合的決策機制。

除了學術研究外，產業界也開始著手投入 HEMS 結合智慧電表與雲端技術之相關計畫的相關開發計畫與研究，如 Google PowerMeter [7]、Greenbox、The Power Tab，OPower, 其中 Google 所推出之 PowerMeter 服務，由於現今使用者對能源管理系統的並不強烈，同時也沒有獲得電力公司的輔助無法有效地融入使用者的用電習慣中，已於 2011 年 9 月終止服務。相較之下 OPower 擁有電力公司的合作關係，將能源管理資訊透過電費帳單的型式提供給消費者，因此獲得較多數使用者的認同。

3. 方法架構

本研究的整體使用架構如圖所示，其透過 IP 可以連結至網際網路，而底下可以連結各種協定的末端裝置，在本研究中，將以 ZigBee、Bluetooth 和 TCP/IP 的溝通協定的裝置為主，本論文將介紹智慧型中介軟體，提供可開發系統架構與設計、Android 終端管理介面系統、情境感知系統

3.1 電器導向中介軟體模組

本分項模組是整個系統核心架構，由於物聯網的裝置網路協定眾多，缺乏共同依循的標準，會造成不同網路協定互通性的問題。對於要讓物與物之間能夠互相溝通，這種不相容的情形不僅會造成相當多困擾。因此，讓這些網路協定與控制方法能夠協同運作，必須要設計中介軟體(Middleware)來處理此項事務。除了建構中介軟體之外，還需考慮上文提到物聯網路由閘道器的特性，例如可彈性客製化加入中介軟體、末端裝置的服務告知等。因此在物聯網路由閘道器與末端裝置間會有裝置的註冊，事件處理，命令控制等相關功能圖 1 是整個溝通的的循序圖。

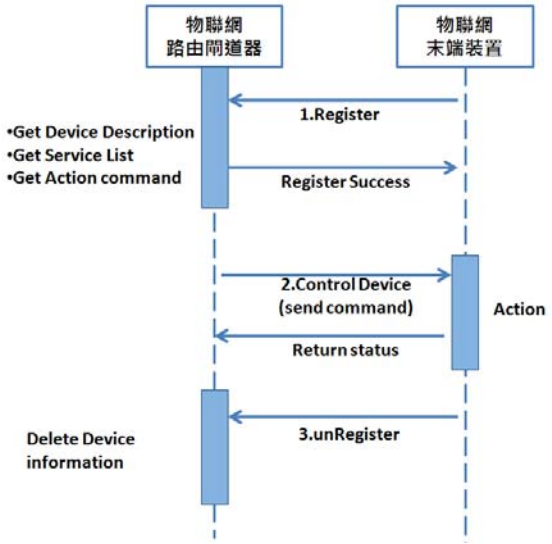


圖 1 物聯網訊息溝通循序圖

3.2 電器活動辨識模型

電器的使用可反映人的行為活動，尤其在 HEMS 中，家裡環境所使用的電器與人在家裡進行的活動是息息相關，而家電並非常常更換，建立活動辨識模型是有其可行性的。在此模型中建立電器使用與人為活動的關聯性，並利用它辨識目前家庭所進行的活動，進一步得知哪些電器是有可能處於不被使用的狀況下，這些目前活動的非參與性電器資訊可以反饋給使用者(client)進行後續的處理。

藉由電器辨識模型可以獲知目前物聯網路由閘道器(IOT router gateway)底下正在使用的電器，活動辨識模型由閘道器中的情境資料庫中收集相關的情境感知(context-aware)資訊，這些資訊由情境提供者服務包(bundle)分析並整合其他感應器服務包所產生的。混合電器與情境感知資訊，活動學習系統從中定義與計算出活動和電器的關聯性，並儲存於活動資料庫中。模型架構可參考圖 2。

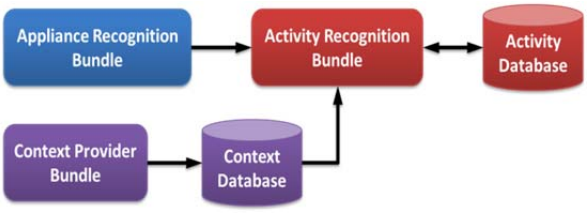


圖 2 電器活動辨識模型架構

在活動辨識系統中，如圖 3，電器設備(device)的使用資料會被群組成活動，根據這些活動與其中的設備產生關聯性資料。群組成活動的步驟稱為設備區塊選擇(device block selection)，關聯性產生的步則稱為設備活動相關性計算(device activity similarity calculation)。查詢的輸入資料是一群電器，一般是目前家裡正在使用的電器；這些資料輸入到學習辨識系統中會先與相關性模型進行活動的相似性比較，也就是計算出輸入資料中的設備是屬於模型中的那一個活動。相關性計算後會產生結果列表(list)，這列表可依相關性或非相關性排序，再由排名(ranking)門檻值選取前 N 筆具有相關性的結果。排名結果會和情境資料一同輸入到活動分類器中，該分類器會依情境資料決定查詢資料到底屬於哪一種活動。這裡使用活動分類決定活動歸屬而不單純使用相關性計算後的結果是因為相關性是一種活動與家庭設備之間的關聯，但在實際上的家電使用還牽扯到一些外在情境的因素。情境的因素可以影響活動中電器的使用。例如，當季節為夏天時，活動中的設備可能會多了電風扇或空調。所以，活動分類可以增加容錯性和提高辨識的準確率。

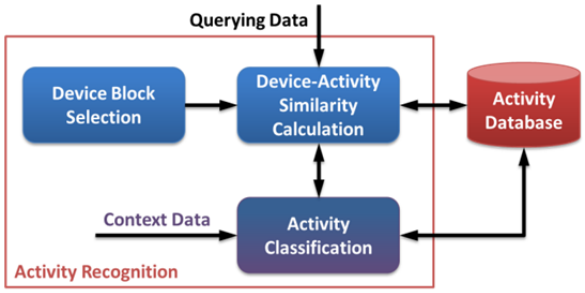


圖 3 電器活動辨識模型架構

3.2.1 Device Block Selection

在計算活動與電器設備之間的相關性之前，需要先定義好一個活動內所包含的電器。從電器辨識服務包過來的資料依單位時間可視為一筆活動片段(segment)，片段內容是目前使用的電器。連續片段是指在連續時間上其片段內容皆相同，這些片段能形成一區塊(block)，區塊分成穩定區塊與暫時區塊。判斷區塊是否穩定的方式是由穩定性門檻值(threshold) HS 決定；區塊時間長度大於門檻值則該區塊是一穩定區塊(stable block)。若區塊時間小於等於門檻值則該區塊被視為暫時性的區塊(impermanent block)。獨立片段是指該片段與其前後片段內容不相同。

利用圖 4 來詳細說明資料區塊，其圖用矩形框線標示了四個區塊和兩個片段，橫軸線代表時間(t)，區塊時間以 T 代表並用區塊名稱做為下標，如 TB1 代表區塊 1 的時間長度。因為 TB1 為 10，所以區塊 1(B1)由 10 個片段組成；B1 中的每個片段內容皆相同為 D1，D2 和 D3。接著，假設穩定性門檻值為 3 時間單位，則 B1, B3,和 B4 都是穩定區塊；B2 是暫時區塊，因為 B2 的區塊時間為 2，兩個片段。在 B1 前面有兩個獨立片段，S1 和 S2，無法形成區塊。

一般來說，暫時性區塊或獨立片段是因活動轉移或停止所造成。活動轉移可由區塊狀態，也就是指區塊內容，劇烈變化可得知活動正在轉移；在圖 3.22 中，B1 到 B4 是一種活動轉移，但 D1 在兩區塊內同時存在，可推導出 D1 是種長效型運作的電器，如日光燈，空調之類的設備。活動停止可視為區塊內容消失至長效設備狀態的行為，如 B1 到 B3 的過程，D3 與 D2 在區塊中消失，因此可以由 B1 所代表的活動正在停止。為了讓區塊與活動有更好的反映性，在決定穩定區塊後會將獨立片再與暫時性區塊合併到穩定區塊中。合併法則是依據區塊或片段的大小(size)，也就是指片段或區塊內容的電器個數，如 S1 片段大小是 1，而 B1 的是 3，B2 的是 2。進行合併時，從穩定區塊的左右開始找比自己大小還小的獨立片段或暫時性區塊並且它們的內容是自己的子集，直到另一個穩定區塊。以圖 3.22 為例，B1 往右找到 B2 是個暫時區塊且 B2 的內容是 B1 的子集，所以 B2 是個被合併到 B1 的候選集，往 B2 的右邊找到了 B3 是個穩定區塊，因為就停止往右合併，並把 B2 合併到 B1 中。從 B1 的左邊找到 S2 是個獨立片段且內容是 B1 的子集，所以 S2 加入到候選集中；S2 的左邊找到 S1 是個獨立片段且內容是 S2 的子集，所以 S1 也加入到候選集中。在上述的合併過程中，S1, S2, B1 和 B2 合併成一個活動區塊 A1，它反映了一個活動的狀態。

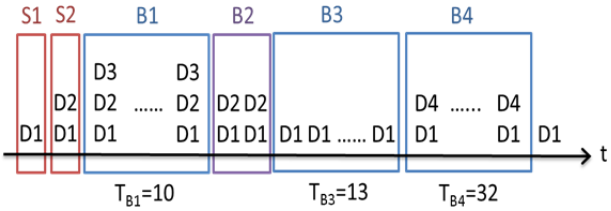


圖 4 電器活動資料區塊

活動辨識模型對從電器辨識服務包獲取的資料是有一些假設條件。第一個條件是活動不會同時發生，也就是指一個活動區塊僅僅代表一項活動，而不是多項活動同時進行。然後，可以把活動組視為一項活動，並能由使用者去標注活動組中的每項活動所擁有的電器，但前提是活動組中的活動是同時開始與同時結束，這也意謂著一項活動不會跨多個區塊。第二項條件是電器狀態的切換，如風扇的送風的強度，與電器同時運作的數量，如三個燈泡，仍被視為同一種設備。第三個條件是每個被辨識的電器設備必須是開啟獨立(open independent)或關閉獨立，一項電器的開關不會自動地開關另一項電器，這是為了計算電器與活動之間相關性的必要條件。

3.2.2 Device-Activity Similarity Calculation

在區塊選擇之後，活動與電器的關係就建立起來。接著要建立關聯性模型，以便計算某一種電器與所

有活動的相關度。為了快速計算與動態新增活動，將在活動辨識服務包中建立資訊擷取領域中常用的推論網路模型，該模型的另一項特性是方便進行查詢推論。推論網路模型的架構如圖 5；在網路中，每項活動與設備都是一個節點(node)，同樣也，一筆查詢資料也是一個節點。節點間的連結代表節點間的關係，活動節點指向設備節點代表該活動包含被指向的設備。查詢節點由設備節點指入，代表該查詢資料中由指入的節點設備所組成。多個查詢節點指向另一個查詢節點代表查詢是可以由其他子查詢組合。如節點 I 是節點 q 與節點 q1 的聯集。

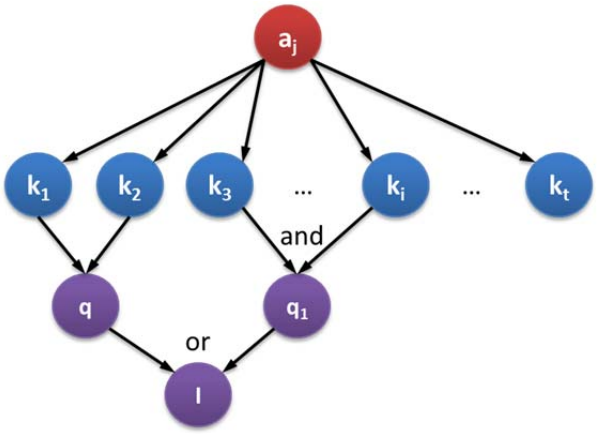


圖 5 推論模型

所有描述模型的符號定義在 Table 3.1 中。

一個 t 維的向量 k 是由所有設備所定義，即(k1, k2,…,kt) where k1, k2, …, kt 隨機二元變數.

表 1 參數定義

Notation	Definition
t	the number of devices in activity recognition system
k_i	a device, a binary random variable
$\vec{k} = (k_1, \ldots, k_t)$	t-dimensional vector defined by $k_1, k_2, \ldots,$ and k_t
q	a user query, a binary random variable
a_j	an activity, a binary random variable
g_i	a function returns the weight associated with the device k_i

有關於一筆查詢 q 的活動排名(ranking)是一種觀察的測量，而此觀察是指一項活動有多少明顯的支持提供給查詢 q。在一個推論網路中，活動排名是由 $P(q \wedge a_j)$所計算，其中 q 和 aj 是 q=1 和 aj=1 的簡短表示。因此，排名公式如下所示

$$
\begin{aligned}
P(q \wedge a_j) &= \sum_{\forall \vec{k}} P(q \wedge a_j | \vec{k}) \times P(\vec{k}) \\
&= \sum_{\forall \vec{k}} P(q | a_j \times \vec{k}) \times P(a_j \times \vec{k}) \\
&= \sum_{\forall \vec{k}} P(q | \vec{k}) \times P(\vec{k} | a_j) \times P(a_j) \\
&= \sum_{\forall \vec{k}} P(q | \vec{k}) \times \left(\prod_{\forall i | g_i(\vec{k})=1} P(k_i | a_j) \times \prod_{\forall i | g_i(\vec{k})=0} P(\overline{k_i} | a_j) \right) P(\vec{k} | a_j) \times P(a_j) \\
P(\overline{q \wedge a_j}) &= 1 - P(q \wedge a_j)
\end{aligned}
$$

其中 $P(\overline{k_i}|a_j) = 1 - P(k_i|a_j)$。$P(q|a_j \times \vec{k}) = P(q|\vec{k})$ 是因為 ki 節點使查詢節點 q 從活動節點 aj 分散。

接著利用 tf-idf 機制來完成排名機率的計算。根據觀察到的活動 aj，一設備 ki 的關聯性(relevance)是由 normalized term-frequency factor 所決定，如下式

$$P(k_i|a_j) = f_{i,j} = \frac{freq_{i,j}}{\max_l freq_{i,j}}$$

設備節點在查詢節點上的影響由 influence of idf factors 決定；定義一設備反應(active)向量如下

$$\overrightarrow{k_i} = \vec{k} \mid (g_i(\vec{k}) = 1 \wedge \forall_{j \neq i} g_i(\vec{k}) = 0)$$

The active vector $\overrightarrow{k_i}$ 是對向量 $\vec{k}$ 的狀態參考，即節點 ki 對 $\vec{k}$ 有反應而其他的節點則是無反應(inactive)。根據反應向量，the influence of the device node in the query node q 如下

$$P(q|\vec{k}) = \begin{cases} idf_i & if\ \vec{k} = \overrightarrow{k_i} \wedge g_i(\vec{q}) = 1 \\ 0 & if\ \vec{k} \neq \overrightarrow{k_i} \vee g_i(\vec{q}) = 0 \end{cases}$$

$$idf_i = \log \frac{N}{n_i}$$

套用上述方程式可產生完整的排名公式

$$
\begin{aligned}
P(q \wedge a_j) &= \left(\prod_{\forall i} P(\overline{k_i}|a_j) \right) \times P(a_j) \times \sum_{\forall \overrightarrow{k_i}} P(k_i|a_j) \times P(q|\overrightarrow{k_i}) \times \frac{1}{P(\overline{k_i}|a_j)} \\
&= C_j \times \frac{1}{|\overrightarrow{a_j}|} \times \sum_{\forall i | g_i(\overrightarrow{a_j})=1 \wedge g_i(\vec{q})=1} f_{i,j} \times idf_i \times \frac{1}{1 - f_{i,j}}
\end{aligned}
$$

3.2.3 Activity Classification

透過查詢資料與推論網路模型的相關性計算後，活動分類器會接收到活動排名列表(ranking list)，在進行分類前可以使用排名門檻值 HR 過濾或減少分類類別。活動分類的模型採用 Naïve Bayes 分類，使用活動發生時的 context data 當作 class features，包含溫度，光度，濕度，時段，季節等等。ranking list 中的每個活動都視為一個類別，貝式分類器依查詢設備的 feature 計算事後機率。

4. 系統實現及實驗分析

本章節則實現其整體架構之雛形系統，並針對於其 appliance-aware activity recognition 方法進行實驗分析。

4.1 識別實驗及分析

本研究將對於 appliance aware activity Recognition 進行實驗及分析，包含對於關聯性排名、時間區段及活動分類等相關參數進行實驗測試，而對其測試結果我們分別採用 recall(Rec)及 precision(P)的評估

指標來評斷對於此方式結果。

$$Pre = \frac{|Ra|}{|A|}$$

$$Rec = \frac{|Ra|}{|R|}$$

其中 Ra 表示 relevant activities in answer set，A 則為 answer set，R 則 relevant activities. 而為了在眾多活動中進行下述實驗，我們將對於其中包含看電視、使用電腦、作菜及打掃行為分類定義其活動，其中其前兩項為相類活動而核心電器的不同之區別，而作菜則是在一段時間區段中有不同的電器進行相關變化。而打掃則是主要核心電器搭配其他變動電器的產生。

4.1.1 關聯性排名分析

此本實驗則是對於資料關聯性排名進行相關實驗，當系統偵測到現今電器使用的時候，其會將電器組丟進 Device-Activity Similarity Model 找出相關關聯度排名，而本實驗將首先針對於上述四種活動中各挑出一種核心電器來作行為關聯度排名前二十之準確率及涵蓋率。其結果如下表所示，

表 2 電器使用關連度(1)

	電視	電腦	抽油煙機	吸塵器
precision	93.5%	83%	97.5%	74%
recall	75%	80%	40%	85%

再結果我們發現因為使用者往往在電腦開啟的時候進行不同之活動，因此，針對於其 precision 偏低，然而伴隨著 recall 則為較高之行為。而對於 cooking 的時候，使用者使用的電器變化則為較少之變化，其對於 precision 則有較高的表現，然而在 recall 部分則出現較低之現象。而接續我們則請受測者針對於上述的動作進行一個小時的測試，其結果如下圖所示，其中因為當使用者在看電視及打掃的時候，容易有周邊電器的狀態改變，因此，關連涵蓋率有較佳的表現。而用電腦及煮菜則為使用者較專注之工作。因此，其電器變化度較少導致有較高 precision。

表 3 電器使用關連度(2)

	看電視	用電腦	煮菜	打掃
precision	93.5%	83%	97.5%	74%
recall	75%	80%	40%	85%

4.1.2 門檻值

在本實驗中我們採用不同的 ranking 門檻值來進行活動識別，其相關結果如下圖所示，由結果顯示，當門檻值過低的時後，將會有非相關的活動進入其分類門檻，導致其整體分類準確率偏低的現象。然而當門檻值過高，則需進一步觀察其 precision 的值，假若 precision 有較佳表現的活動，則對於準確率並不會造成太大影響，但假設 precision 不佳的活動，則可能正確的活動被排除於門檻之外，造成整體識別率急速下降的現象。

4.1.3 電器個數對於行為識別率

而考慮對於整體環境電器數對於單一行為識別的影響度，考慮上述活動中，其看電視活動較容易有周遭電器發生變化，因此我們採用看電視進行識別，其相關結果如下圖所示，當電器數少於五個時候，其當使用者暫時離開進行別的活動的時候，因其主核心電視的開啟，導致將造成一持續識別為看電視之行為。而電器數超過 15 個的時候，其因周邊過多電器發生變化，造成整體關聯性排名較為降低導致整體識別率也將發生下降的現象。

4.3 節能實驗

而對於能源管理的部分，本實驗則以一家庭為實驗環境，其測試者為經過兩天之相關裝置之使用訓練，其測試裝置如下表所示，其測試時間為期十天，其中對於節能方式分為兩種，一種則為透過之前所設計之 smart socket 達成自動控制部分，另一種對於像電腦等較精密之家庭裝置，則透過行動裝置以建議的方式告知使用者，修正使用者用電習慣，如下圖為在使用前與使用後的用電量實驗對照，其可發現可大約節省其電源 12%。

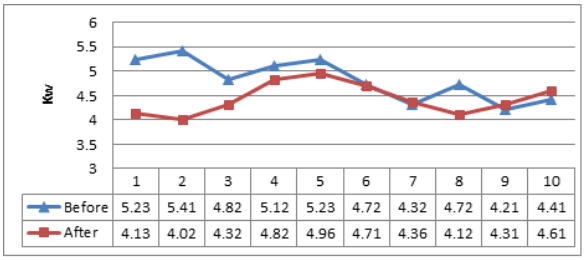


圖 6 十日書房用電量

5. 結論

針對於現今物聯網的發展與節能概念的提升，本研究提出了一套電器導向之物聯網能源管理系統，藉由著電器識別之技術讓現今一般家電無需透過額外識別裝置
便能加入物聯網系統，並利用電器區塊選擇之機制找出可能發生之活動，根據推論網路模型建立活動與電器之關聯性，最後採用 Naïve Bayes 對 context data 進行活動分類。而系統將對其最終之分類結果採用自動開關或者提醒使用者關閉不需要之電器，藉以達到能源管理之貢獻。對於單純以電器導向之識別而言，其行為仍需伴隨著電器使用才能達到識別之成果，為了增進其活動數量，對於未來，我們將進行結合 image 或者 location 等資料進行混合式識別，並嘗試進行其活動預測之推論來達到智慧控制之成果。

致謝

“本研究依經濟部補助財團法人資訊工業策進會「 102 年度雲端運算系統及軟體技術研發計畫 (2/3) 」辦理“以及國科會編號”102-2219-E-194-002”, “101-2628-E-194-003-MY3” 計畫

參考文獻

[1] Lai, Y.-X., Lai, C.-F., Huang, Y.-M. and Chao, H.-C. (2011) Multi-appliance Recognition System with Hybrid SVM/GMM Classifier in Ubiquitous Smart Home. information sciences. In press.

[2] Lai, Y.-X., Rodrigues, J. J., Huang, Y.-M., Wang, H.-G. and Lai, C.-F. (2012) An Intercommunication Home Energy Management System with Appliance Recognition in Home Network. Mob. Netw. Appl. 17(1) 132-142.

[3] Chu-sing, Y., Ming-yi, L. and Chao-xing, C. (2009) Design and implementation of HEMS based on RFID and OSGi. Anti-counterfeiting, Security, and Identification in Communication, 2009. ASID 2009. 3rd International Conference on.

[4] Dae-Man, H. and Jae-Hyun, L. (2010) Design and implementation of smart home energy management systems based on zigbee. Consumer Electronics, IEEE Transactions on. 56(3) 1417-1425.

[5] Young-Sung, S. and Kyeong-Deok, M. (2010) Home energy management system based on power line communication. Consumer Electronics (ICCE), 2010 Digest of Technical Papers International Conference on.

[6] Rossello-Busquet, A., Soler, J. and Dittmann, L. (2011) A Novel Home Energy Management System Architecture. Computer Modelling and Simulation (UKSim), 2011 UkSim 13th International Conference on.

[7] Redmer, J. (2010) Google's powermeter IET conference, 2 March 2010. Smart Metering 2010: Delivering a Smart UK, IET Seminar on.

[8] Chao, C., Das, B. and Cook, D. J. (2010) A Data Mining Framework for Activity Recognition in Smart Environments. Intelligent Environments (IE), 2010 Sixth International Conference on.

[9] Tapia, E., Intille, S. and Larson, K. (2004) Activity Recognition in the Home Using Simple and Ubiquitous Sensors

[10] Pervasive Computing. In Ferscha, A. and Mattern, F. (eds). Springer Berlin / Heidelberg.

[11] Kasteren, T. v., Noulas, A., Englebienne, G., Kr\, B., \#246 and se. (2008) Accurate activity recognition in a home setting. Proceedings of the 10th international conference on Ubiquitous computing, 1409637 ACM pp. 1-9.

[12] Harris, C. and Cahill, V. (2005) Exploiting user behaviour for context-aware power management. Wireless And Mobile Computing, Networking And Communications, 2005. (WiMob'2005), IEEE International Conference on.

[13] Liao, L., Fox, D. and Kautz, H. (2005) Location-based activity recognition using relational Markov networks. Proceedings of the 19th international joint conference on Artificial intelligence, 1642417 Morgan Kaufmann Publishers Inc. pp. 773-778.

[14] Singla, G., Cook, D. and Schmitter-Edgecombe, M. (2010) Recognizing independent and joint activities among multiple residents in smart environments. Journal of Ambient Intelligence and Humanized Computing. 1(1) 57-63.

[15] Duong, T. V., Bui, H. H., Phung, D. Q. and Venkatesh, S. (2005) Activity recognition and abnormality detection with the switching hidden semi-Markov model. Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on.

[16] Ben-Arie, J., Zhiqian, W., Pandit, P. and Rajaram, S. (2002) Human activity recognition using multidimensional indexing. Pattern Analysis and Machine Intelligence, IEEE Transactions on. 24(8) 1091-1104.

[17] Luhr, S., Bui, H. H., Venkatesh, S. and West, G. A. W. (2003) Recognition of human activity through hierarchical stochastic learning. Pervasive Computing and Communications, 2003. (PerCom 2003). Proceedings of the First IEEE International Conference on.

[18] Intille, S. S., Larson, K., Tapia, E. M., Beaudin, J. S., Kaushik, P., Nawyn, J. and Rockinson, R. (2006) Using a live-in laboratory for ubiquitous computing research. Proceedings of the 4th international conference on Pervasive Computing, 2094967 Springer-Verlag pp. 349-365.

[19] Patterson, D. J., Fox, D., Kautz, H. and Philipose, M. (2005) Fine-grained activity recognition by aggregating abstract object usage. Wearable Computers, 2005. Proceedings. Ninth IEEE International Symposium on.

[20] Ito, M., Uda, R., Ichimura, S., Tago, K., Hoshi, T. and Matsushita, Y. (2004) A method of appliance detection based on features of power waveform. Applications and the Internet, 2004. Proceedings. 2004 International Symposium on.

[21] Gu-yuan, L., Shih-chiang, L., Hsu, J. Y. J. and Wan-rong, J. (2010) Applying power meters for appliance recognition on the electric panel. Industrial Electronics and Applications (ICIEA), 2010 the 5th IEEE Conference on.

[22] Ruzzelli, A. G., Nicolas, C., Schoofs, A. and O'Hare, G. M. P. (2010) Real-Time Recognition and Profiling of Appliances through a Single Electricity Sensor. Sensor Mesh and Ad Hoc Communications and Networks (SECON), 2010 7th Annual IEEE Communications Society Conference on.

[23] Chin-Feng, L., Yueh-Min, H., Jong Hyuk, P. and Han-Chieh, C. (2010) Adaptive Body Posture Analysis for Elderly-Falling Detection with Multisensors. Intelligent Systems, IEEE. 25(2) 20-30.

使用粒子群最佳化演算法尋找無線人體區域網路低特定吸收率路徑

吳庭育[1] 李維聰[2] 林承翰[2] 吳昱緯[1]
[1]國立宜蘭大學資訊工程學系
[2]淡江大學電機工程學系
tyw@niu.edu.tw; wtlee@mail.tku.edu.tw; u45jc@hotmail.com; steven000083@hotmail.com

摘要

無線人體區域網路中的感測器節點被裝置在人體皮膚表面或嵌入至皮膚裡，當傳送端發送封包時，訊號會經由人體皮膚表面或皮膚內傳輸至接收端，而發送封包時所產生的電磁波輻射會對人體健康造成危害。特定吸收率(Specific Absorption Rate，SAR)是電磁波輻射對人體影響程度的重要指標，特定吸收率的數值愈高，代表人體所吸收的電磁波輻射量愈多，對人體健康造成的危害程度也愈大。本論文使用粒子群最佳化演算法尋找中繼節點合適的佈建位置，使得感測器節點透過此中繼節點轉傳封包到集中裝置這段路徑的特定吸收率較小且封包傳送成功率也能有所提升。

關鍵詞：無線人體區域網路、特定吸收率。

Abstract

The IEEE 802.15.6 sends the signals will reach the receiver through human body or skin. Nevertheless, the step to send packets will generate electromagnetic radiation, which may affect human body negatively. The specific absorption rate (SAR) is an important index that measures the electromagnetic radiation absorbed by human body: the higher the level of SAR means the more harmful effects of the electromagnetic radiation on human body. In our proposed method regulates the power of nodes according to the distances between nodes and therefore allows a node to complete the packet transmission with the minimum power.

Keywords: WBAN, SAR

1. 前言

近幾年來，隨著無線網路的普及與微型感測器製造技術的提昇，人們開始關注到各式各樣的生理資訊且相關的應用也愈來愈多元化。因此，隨時監控與取得生理訊號就顯得更加重要。為了人們對於生理健康資訊的需求，電機電子工程師學會制定一種適合在人體運作的網路協定，即 IEEE 802.15.6，以因應未來生理訊號監控之服務。IEEE 802.15.6 網路協定應用在人體，故又稱為無線人體區域網路(Wireless Body Area Network, WBAN)，為當前一個重要的技術，和無線個人區域網路(Wireless Personal Area Network，WPAN)、無線感測網路(Wireless Sensor Network, WSN)以及移動通訊(Mobile Communication)都有著密切的關係，並且具有非常廣泛的應用和巨大的市場潛能。

無線人體區域網路中的感測器節點被裝置在人體皮膚表面或嵌入至皮膚裡。當傳送端發送封包時，訊號會經由人體皮膚表面或皮膚內傳輸至接收端，而發送封包時所產生的電磁波輻射會對人體健康造成影響。電磁波輻射的強弱與感測器節點的運作頻率、功率及距離有關，而產生的電磁波輻射會被人體吸收轉化成熱能，而人體的體溫調節是藉由流汗和血液循環來散熱，當人體在短時間內吸收大量的電磁輻射時，會讓人體無法即時散熱，導致體溫瞬間增高，造成皮膚灼傷、心律不整、呼吸困難，嚴重的話會導致人體內的細胞產生突變，進而增加罹患癌症的機率。特定吸收率(Specific Absorption Rate, SAR)是電磁波輻射對人體影響程度的重要指標，高的特定吸收率數值，表示人體吸收較多的電磁波輻射量，對人體健康造成的危害程度也愈大。

而無線人體區域網路的相關研究中，大多數的學者都著重在解決封包碰撞避免[1][2]、提高傳輸成功率[3]、增加網路的生命週期時間[4]等問題；從未探討傳送封包時電磁波輻射對人體所造成的影響。所以本論文根據文獻[5]將 SAR 對人體的影響劃分成數個區域，每個區域各有其權重值，並利用粒子群演算法尋找中繼節點合適的佈建位置，使得感測器節點透過此中繼節點轉傳封包到集中裝置這段路徑的特定吸收率較小且封包傳送成功率也能有所提升。

2. 背景知識與相關文獻探討

本章首先會概括描述無線人體區域網路，接著針對電磁波輻射影響的指標-特定吸收率做介紹，最後說明粒子群最佳化演算法的由來與做法。

2.1 無線人體區域網路

相較於無線個人區域網路與無線感測網路，無線人體區域網路是一種具有短距離通訊、低功率消耗、高資料傳輸速率之特性的無線通訊技術[6]，通常用於醫療用途。在無線人體區域網路中，感測器節點被裝置於人體皮膚表面上(穿戴式)或嵌入於人體皮膚內(植入式)[7]，感測器節點負責蒐集各種生理訊號，並經由單躍(One hop)或兩躍(Two hops)的無線傳輸方式將封包上傳至人體上的集中裝置儲存。集中裝置可透過Wi-Fi或3G將所儲存的資料上傳至遠端的電腦。醫院或相關研究單位可透過所蒐集到的資料來分析人體的健康狀況和相關的醫療生理資訊研究。

2.2 特定吸收率

特定吸收率(Specific Absorption Rate, SAR)[8]是電磁波能量吸收的比值，如公式所式，其定義為單位時間內單位質量的人體組織所吸收的電磁輻射功率，單位為 W/Kg。

$$SAR = \frac{d(\frac{dW}{dm})}{dt} \quad (2.1)$$

其中

W：功率，單位為瓦(W)

m：質量，單位為公斤(Kg)

t：時間，單位為秒(Sec)

國際上各國對於 SAR 於人體上的限制值各有不同，又有區分人體全身與人體局部的 SAR 限制值。目前全世界所公認的 SAR 標準值是由美國聯邦通訊委員會(FCC)[9]制定的 1.6W/kg 標準值；而國際非游離輻射防護委員會(ICNIPR)[10]則對人體全身和局部位有不同的 SAR 限制，頭部和軀幹的標準值為 2W/kg、人體四肢為 4W/kg。

2.3 粒子群最佳化演算法

粒子群最佳化演算法[11](Particle Swarm Optimization, PSO)是由 Kenned 和 Eberhart 兩位學者於 1995 年所提出，Kenned 和 Eberhart 觀察鳥群的覓食行為，發現牠們具有和人類相同的群體智慧。鳥在尋找食物的過程中會傳遞訊息給牠的同伴，彼此形成資訊的共享。因此，鳥會根據自己目前的方向、個體最佳經驗方向和群體最佳經驗的方向來改變自己尋找食物的方向，最後將使得整個鳥群都往同一個方向前進。在粒子群演算法的過程中，初始化粒子是由電腦隨機產生的，目的是使眾多粒子能均勻的散佈在欲搜尋之空間。透過適應函數苦以判斷粒子在整個空間中的優劣程度。粒子在搜尋的過程中會記錄適應值較好的位置，並根據自己目前的速度、區域最佳解的位置和全域最佳解的位置來更新自己的速度與位置，其數學表示如下：

$$V_i^{k+1} = wV_i^k + c_1r_1(P_i^k - X_i^k) + c_2r_2(P_g^k - X_i^k) \quad (2.4)$$

$$X_i^{k+1} = X_i^k + V_i^{k+1} \quad (2.5)$$

公式2.4可以分成三個部分解釋。若$V_i^{k+1} = V_i^k$，則表示該粒子堅持己見，仍依上一次迭代的速度作為前進的方向；若$V_i^{k+1} = V_i^k + c_1r_1(P_i^k - X_i^k)$，表示該粒子稍具智慧，會參考自己過去的經驗作為方向改變的依據；若$V_i^{k+1} = V_i^k + c_1r_1(P_i^k - X_i^k) + c_2r_2(P_g^k - X_i^k)$，表示該粒子具群體智慧，除了參考自己過去的經驗，還會參考別的粒子的經驗來改變粒子前進的方向。

3. 以粒子群最佳化演算法尋找中繼節點佈建位置

3.1 問題描述

在無線人體區域網路中，單躍傳輸模式下的封包傳送成功率普遍偏低[18]。圖 3.1 為[18]的實驗場景，共有四個感測器節點與一個置於腰部的集中裝置。圖 3.2 為實驗場景在單躍傳輸下的封包傳送成功率。由圖 3.2 可以發現，在單躍傳輸模式下，節點 1、節點 2 與節點 3 的封包傳送成功率皆不到 20%，對於負責監控人體生理狀況的網路型態而言是相當不可靠的。而本論文為了減少封包在傳輸時對人體的傷害，以文獻[7]SAR 對人體影響的權重值為基準，使用粒子群演算法求解中繼節點的佈建位置，使得感測器節點透過中繼節點轉傳封包至集中裝置時，該路徑對人體的影響程度較小且封包傳送成功率也有顯著地提高。

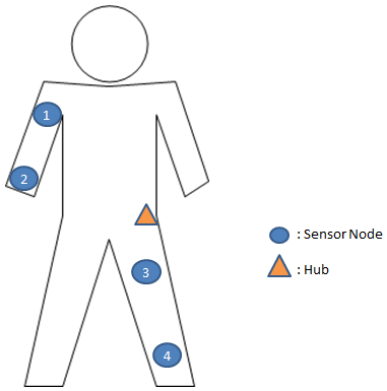


圖 3.1 網路節點佈建示意圖

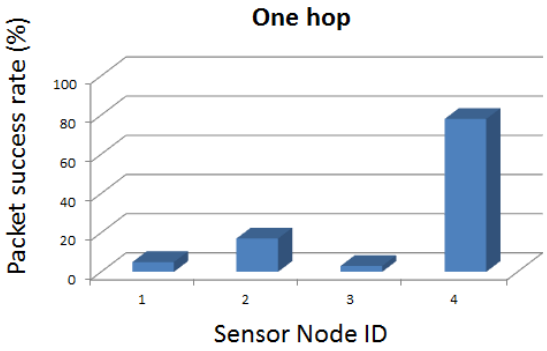


圖 3.2 封包傳送成功率

3.2 特定吸收率權重值

本論文根據文獻[7]中的SAR數值分布圖，將人體劃分數個區域，並給予不同的權重值，如圖所示。權重值表示電磁波輻射對於人體該部位傷害影響程度的大小，權重值愈大表示電磁波輻射對於該部位損害的程度愈大，要避免節點在此部位上運作。

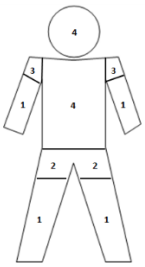


圖 3.3 SAR 對人體局部影響之權重分布圖

3.3 使用粒子群最佳化演算法求解

3.3.1 粒子編碼

為了使粒子群演算法能在本論文正常運作，須先將問題轉換成粒子的形式。在本篇論文中，每一個粒子是極座標系中的一個點，若有 20 個粒子則代表極座標系中有 20 個不同的座標點在運作，這 20 個座標點在經過多次迭代後會趨近於一個座標點，此點即是本論文中繼節點佈建的位置。本論文定義粒子的形式為：

$$X_i^k = \left(a_i^k, b_i^k\right),\ \forall i = 1, \dots, n \quad (3.1)$$

$$\begin{cases} a_i^k = r_i^k \cos\theta_i^k \\ b_i^k = r_i^k \sin\theta_i^k \end{cases} \quad (3.2)$$

X_i^k為第 i 個粒子在第 k 次迭代在極座標系上的座標，$\left(a_i^k, b_i^k\right)$即空間中解的位置，是在第 k 次迭代後，由集中裝置與中繼節點的距離和旋轉角度所組成的座標點。r與θ是速度參數，透過r與θ可改變粒子前進的速率與方向並改變下一次迭代的位置。r_i^k是第 k 次迭代後與集中裝置的距離，θ_i^k是第 k 次迭代後與集中裝置偏離的角度。所以粒子 i 的初始速度與位置可由公式 3.3、3.4 得到：

$$V_i^0 = (r_i^0, \theta_i^0) \quad (3.3)$$

$$X_i^0 = (a_i^0, b_i^0) = (r_i^0 \cos\theta_i^0, r_i^0 \sin\theta_i^0) \quad (3.4)$$

3.3.2 適應函數

在本論文的問題中，目標是要求一個中繼節點的佈建位置，使得感測器節點透過此中繼節點轉傳封包到集中裝置這條路徑的特定吸收率最小。在只有一個感測器節點的情境下，欲求一條由感測器節點透過中繼節點轉傳封包到集中裝置的最小特定吸收率路徑為各節點的最小發送功率乘上該節點所在區域的 SAR 權重值。而最小發送功率可由公式 3.5 訊號衰減公式計算得到。

$$10\log_{10} P + 95dB - 25dB = 32.45 + 20\log_{10} D + 20\log_{10} F \quad (3.5)$$

其中

P：功率，單位為毫瓦(mW)

D：兩個節點之間的距離，單位為公里(Km)

F：節點運作的頻帶，單位為赫茲(MHz)

$95dB$：節點接收靈敏度

$25dB$：空氣造成的訊號衰減

由公式 3.5 可得到感測器節點 s 發送封包給中繼節點的最小發送功率P_s以及中繼節點轉傳封包到集中裝置的最小發送功率P_R，如公式 3.7、3.8 所示：

$$P_s = 10^{\frac{32.45+20\log_{10}2400\sqrt{(x_S - r_i^k\cos\theta_i^k)^2 + (y_S - r_i^k\sin\theta_i^k)^2}}{10}} \quad (3.6)$$

$$P_R = 10^{\frac{32.45+20\log_{10}2400\sqrt{(r_i^k\cos\theta_i^k - 0)^2 + (r_i^k\sin\theta_i^k - 0)^2}}{10}} \quad (3.7)$$

如圖 3.6 所示，本論文假設在極座標系中，集中裝置的座標為原點(0,0)，若某個感測器節點 s 的座標為(x, y)欲求一個中繼節點座標為(a, b)，使得從(x, y)發送封包到(a, b)，再從(a, b)轉傳到(0,0)這條路徑的特定吸收率最小。

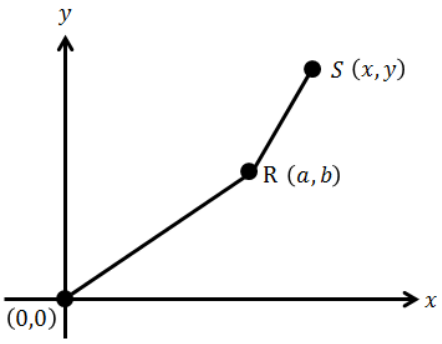


圖 3.4 平面直角坐標系節點示意圖

因此，問題的適應函數f如公式 3.8 所示：

$$f = P_s \times w_s + P_R \times w_R \quad (3.8)$$

其中

P_s：感測器節點 s 最小發送功率

P_R：中繼節點最小發送功率

w_s：感測器節點 s 的 SAR 權重值

w_R：中繼節點的 SAR 權重值

本論文中感測器節點個數有 4 個，故整個網路系統的適應函數f為：

$$f\left(X_i^k\right) = \frac{\sum_{s=1}^{4} P_s \times w_s}{4} + P_R \times w_R \quad (3.9)$$

3.3.3 更新粒子速度與位置

粒子會根據r與θ這兩個參數來更新下一個世

代中繼節點與集中裝置的距離與旋轉角度，然後透過新世代的r與θ更新粒子在極座標系上的座標值。速度更新公式如公式 3.8、3.9。

$$r_i^{k+1} = wr_i^k + c_1 rand_1(Pr_i^k - r_i^k) + c_2 rand_2(Pr_g^k - r_i^k) \quad (3.10)$$

$$\theta_i^{k+1} = w\theta_i^k + c_1 rand_1(P\theta_i^k - \theta_i^k) + c_2 rand_2(P\theta_g^k - \theta_i^k) \quad (3.11)$$

由公式 3.10、3.11 得到r_i^{k+1}與θ_i^{k+1}後即可得到第 i 個粒子在第 k+1 迭代的位置X_i^{k+1}，如公式 3.12 所示：

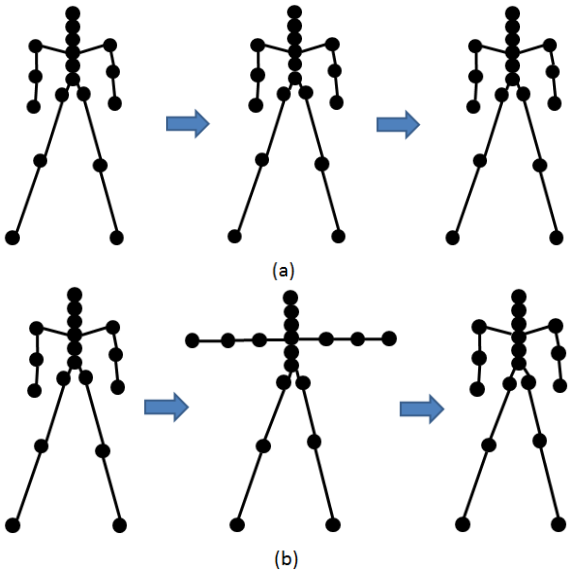
$$X_i^{k+1} = (a_i^{k+1}, b_i^{k+1}) = (r_i^{k+1}\cos\theta_i^{k+1}, r_i^{k+1}\sin\theta_i^{k+1}) \quad (3.12)$$

4. 模擬環境與結果分析

在這個章節中，使用粒子群最佳化演算法對本文所提出的方法進行模擬與分析並以[12]作為模擬對照組。4.1 節為模擬場景說明。4.2 節中探討在兩躍傳輸的情況下，中繼節點佈建的位置與各個感測器節點之特定吸收率的關係，並比較加入中繼節點後，各個感測器節點的傳輸封包效能。

4.1 模擬場景與參數設定

模擬場景分為三種情境，分別為(a)兩手臂向下伸展、(b)兩手臂向左右伸展與(c)兩手臂向上伸展。每個情境皆有 4 個感測器節點和置於腰部的集中裝置，節點運作頻段為 2.4GHz。



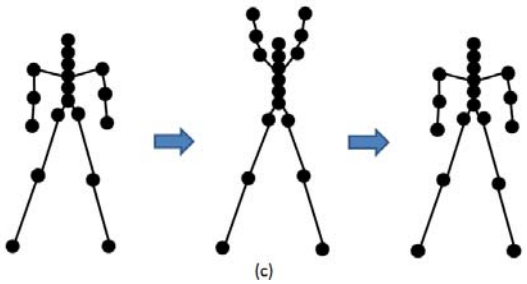


圖 4.1 模擬情境

表 4.1 參數設定

參數名稱	參數內容
粒子數	30
慣性權重值	1
區域最佳解權重值	2
全域最佳解權重值	2
迭代次數	100
封包大小	1024 bytes
資料傳輸率	500 kbp/s
時間延遲	250 ms
發送次數	100

4.2 結果分析

在情境(a)的狀況下，相較於[12]的最小覆蓋演算法，本論文透過粒子群最佳化演算法所得到的中繼節點佈建位置較具有較低的特定吸收率，降低的幅度約為 3 到 6 倍。在情境(b)的狀況下，特定吸收率有稍微增加，這是因為手臂向左右伸展，增加了節點與中繼節點的距離，導致節點需要更大的運作功率來發送封包，但是和[18]比較起來，仍是一個較低的特定吸收率網路。情境(c)為手臂向上伸展，可以明顯看出節點 2 的特定吸收率高於節點 1，這是因為在此情境下，節點 2 與中繼節點的距離大於節點 1，因此須調整為較大的運作功率。由圖 4.2、4.3 與 4.4 可說明本論文所提出的方法能有效降低電磁波輻射對人體的影響。

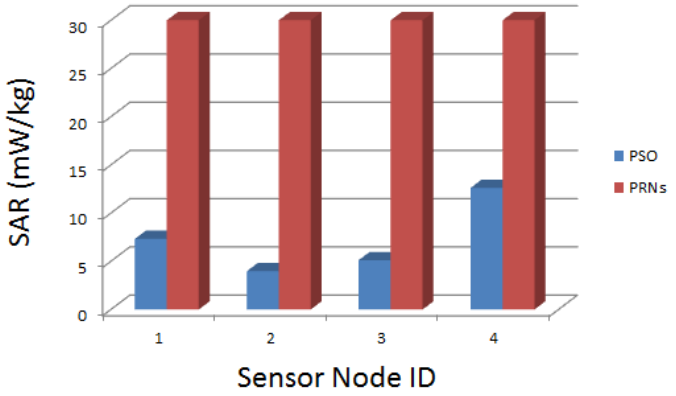


圖 4.2 情境(a)特定吸收率

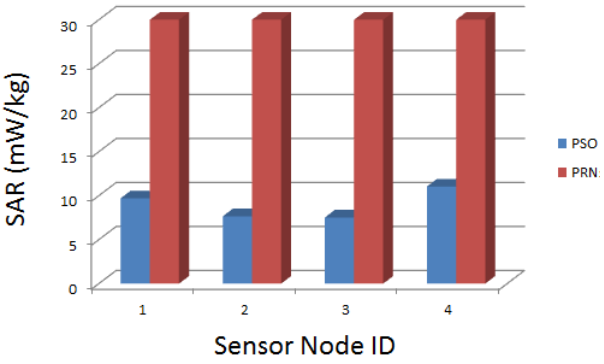


圖 4.3 情境(b)特定吸收率

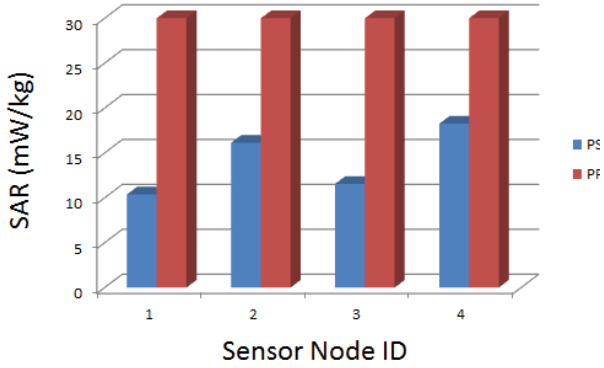


圖 4.4 情境(c)特定吸收率

接著比較加入中繼節點後，各節點的封包傳送成功率。在各種情境下封包傳送皆有 90%至 95%的成功率，相較於以提高封包傳送成功率為訴求的 PRNs，本論文提出的方法不僅能減少電磁波輻射對人體的傷害，對於網路的可靠度也能有效提升。

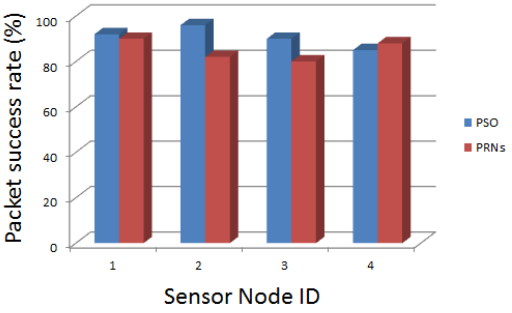


圖 4.5 情境(a)封包傳送成功率

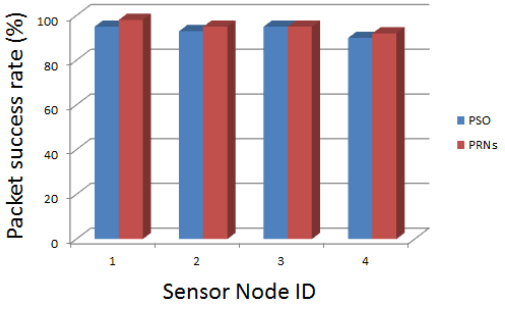


圖 4.6 情境(b)封包傳送成功率

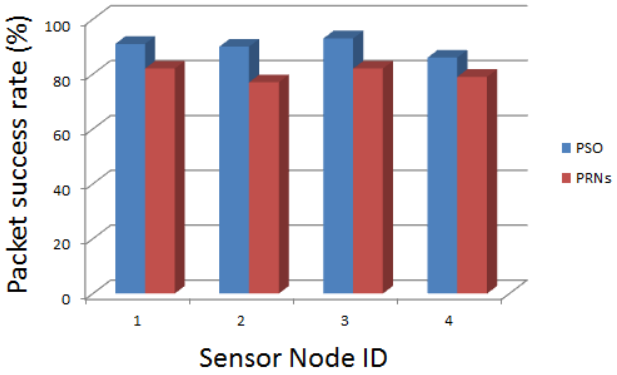


圖 4.7 情境(c)封包傳送成功率

5. 結論與未來工作

在本論文之中提出利用粒子群演算法尋找中繼節點合適的佈建位置，讓各個感測器節點在傳送封包時，能減少電磁波輻射對人體造成的影響。由於電磁波輻射與節點運作的功率有關，我們根據感測器節點與中繼節點之間的距離，讓節點只需提供小的傳輸功率即可滿足封包在此段距離之間的傳輸，這麼做的好處不但可以降低電磁波對人體的傷害也能延長節點的運作時間。對於中繼節點的佈建位置，本研究建議將中繼節點放置在人體的右手腕至右手臂這段區域。模擬結果顯示，將中繼節點佈建在右手腕至右手臂的部位上能有效降低特定吸收率且封包傳送成功率也有顯著提升。

在未來的工作中期望依服務品質區分感測器節點的服務類型，將相同優先權值的感測器節點歸類在同一群，以分群的方式來考慮中繼節點佈建的位置，讓每個群都有一個專屬的中繼節點，以提升無線人體區域網路的服務品質。

參考文獻

[1] R P Findlay and P J Dimbylow. "Effects of posture on FDTD calculations of specific absorption rate in a voxel model of the human body," INSTITUTE OF PHYSICS PUBLISHING, Phys. Med. Biol. 50 2005, pp.3825-3835.

[2] Timmons, N.F. and Scanlon, W.G., " An adaptive energy efficient MAC protocol for the medical body area network," Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, 2009. Wireless VITAE 2009. 1st International Conference on, 2009 , pp. 587-593.

[3] Marinkovic, S., Spagnola C. and Popovici, E., "Energy-Efficient TDMA-Based MAC Protocol for Wireless Body Area Networks," Sensor Technologies and Applications, 2009. SENSORCOMM '09. Third International Conference on, 2012 , pp. 247-248.

[4] Ortiz, A.M., Ababneh, N., Timmons, N. and Morrison, J. "Adaptive routing for multihop IEEE 802.15.6 Wireless Body Area Networks, " Software, Telecommunications and Computer Networks, 2012 20th International Conference on, 2012 , pp.1-5.

[5] Eberhart, R.C. and Shi, Y., "Parmeter Selection in Particle Swarm Optimization," Lecture Notesin Computer Sceince Evolutionary Programming VII, 1998, 591-600.

[6] Arif Onder ISIKMAN, Loris Cazalon, Feiquan Chen, and Peng Li, "Body Area Networks," Group 6 of the course SSY145 Wireless Networks.

[7] W. Astrin, Huan-Bang Li, Ryuji KOHNO, "Standardization for Body Area Networks, " IEICE TRANS. COMMUN., 2009, vol.E92-B.

[8] Findlay, R.P. and Dimbylow, P.J., "SAR in children from exposure to wireless local area networks (WLAN)," Electromagnetic Compatibility (APEMC), 2012 Asia-Pacific Symposium on, 2012 , pp.733-736.

[9]"FCC OET BULLETIN 65 SUPPLEMENT C 01-01.", IEEE Std 1528-2003 and 1528a-2005, 2013. http://infam.antville.org/static/infam/files/google-glass-fcc-4-15-2013.pdf

[10] ICNIRP: “Guideline for limitting exposure to time-varying electric,magnetic, and electromagnetic fields (up to 300 GHz), ” Health Physics, 1998, vol. 74, pp. 494-522

[11] Eberhart, R.C. and Shi, Y., " Particle Swarm Optimization," IEEE International Conference On neural networks, vol 4. 1995, pp.1942-1948.

[12] 張宜穎, "無線人體區域感測網路之中繼節點佈建方法" 國立清華大學資訊工程學系碩士論文, 2010 年 09 月.

以 RFID 為主的 IoT 之研究－以 N 博物館文創商品管理為例

姜國輝 [1]　翁瑞聲 [2]
[1,2] 國立政治大學資訊管理學系
[1]jkchiang@nccu.edu.tw
[2]kendiso@gmail.com

摘 要

IoT 被各國視為未來發展的目標，RFID 已廣泛被各界應用且被視為實現 IoT 的關鍵技術。而 IoT 的定義不明確一直是 RFID 與 IoT 發展的阻礙。本研究藉由探討 IoT 和 RFID 系統組成，付予 IoT 明確的定義，並進一步以資訊服務觀點建立以移動式 RFID 為主的 IoT 服務架構，以實現人啟動服務、設備啟動服務及物件啟動服務。其中，移動式 RFID 設備上的軟體可將唯一識別碼轉換成 DNS 系統查詢的完整網路名稱(FQDN)，然後依循 DNS 系統查詢方式，找到特定 ONS 伺服器，ONS 伺服器回傳 FQDN 所對應的服務網址以啟動服務。本研究並以 N 博物館為個例，利用此一 IoT 服務架構設計文創基金商品設計、銷售、管理的 IoT 服務。

關鍵詞: RFID，物聯網(IoT)，DNS，ONS，服務

Abstract

While Internet of Things (IoT) is considered as the most important technological development by the most countries, RFID technology is widely applied and becomes the key mechanism for IoT implementation. However, the unclear definition of IoT is a barrier to the aggregation of RFID and IoT. Through an investigation by means of literature review on the evolution of IoT and RFID, this paper at first clarifies the definition of IoT and further constructs a RFID-based IoT service framework from the information service perspective. This paper classifies the IoT services into three categories, viz. human-enabled service, device-enabled service and object-enabled service. To realize aforementioned services, the software on mobile RFID devices has to translate the unique ID into the FQDN in the form of DNS URL and then finds the specific ONS server according to the DNS URL. After that, the ONS server feeds back the URL of the service corresponding to the FQDN to activate the service。Last but not least, this paper presents the IoT service framework for solving problems in the field of creative-cultural product management with examples from the N museum and shows the potential IoT applications.

Keywords: RFID, Internet of Things. DNS, ONS

1. 前言

無線射頻辨識(Radio Frequency Identification, RFID)技術起源於二次世界大戰，戰機的敵我識別(Identification, Friend or Foe, IFF)系統用來偵測並確認飛向機場的飛機是否為己方所有，是為最早的 RFID 技術運用(Banks et al. 2007)。在 2008 年後 RFID UHF 標籤價格降至 5 美分，使得 RFID 技術被大量導入企業的相關應用領域(高志中 2009)。

隨著無所不在的聯網(Ubiquitous Network)之概念的發展，在 2005 年國際電信聯盟(ITU)將物件的概念加入無所不在的聯網中。也就是在網路化的時代，在任何時間與地點，人跟人之間得以透過網路相互聯繫、人透過網路取得物件的資訊，以及物件和物件之間相互通訊，形成一個未來網際網路的新概念，物聯網(Internet of Things, IoT)(Chaouchi 2010)。

在 RFID 被廣泛的應用下，不難理解其具有達成 IoT 的優勢，然而 RFID 該如何與 IoT 作結合，以及結合後又該如何應用？要回答這兩個問題，必須要先了解 RFID 組成、IoT 概念與 IoT 物件為何，以及資通訊設備間如何做溝通與互動。

2. 主要內容

2.1 RFID

2.1.1 RFID 系統組成

RFID 系統由標籤(Tag)、天線(Antenna)、讀取器(Reader)、中介系統(Middleware)，和資訊系統(Information System)等五個單元所組成，讀取器利用電磁波的方式與標籤溝通，在一問及一答間達到辨識標籤上的資訊(高志中 2009)。RFID 系統組成可參考圖 1，以下分述之：

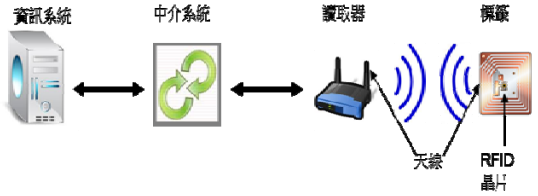


圖 1 RFID 系統組成 [2]

(1) 標籤

EPCglobal 將 RFID 標籤分成主動和被動式兩種(Armenio et al. 2010)。EPC 編碼系統中的通用識別碼(General Identifier, GID)，可因應不同產業需求調整編碼設計，使得商品物件能有全球獨一無二的編碼；GID 編碼格式分成四個區塊分別為 EPC 標頭(Header)、通用管理者代碼(General Manager Number)、物件類別(Object Class)，和序號(Serial Number)(EPCglobal 2011)。

EPC 標頭定義 EPC 的長度、識別類型和標籤的編碼結構；通用管理者代碼為組織代號或公司代碼，需向 EPCglobal 註冊取得；物件類別用來辨識物件的商品與類型，共有 24 bit 可區分 16,777,216 種商品；序號賦予特定物件類別每個物件一個唯一序號，有 36 bit 代表同種類商品，最多可賦予 68,719,476,736 個商品全球唯一代碼。

(2) 讀取器與天線

讀取器通常包含無線通訊模組(RF Module)和控制模組(Control Module)。而讀取器主要的功能就是透過無線通訊模組，以電磁感應或射頻共振的方式，與標籤通訊並取得資料，再透過控制模組以有線或無線的方式將取得的資料傳輸給主控制器。通常讀取器必須具備與標籤通訊、防碰撞、透過標準介面與後端系統連接傳遞資訊、讀取的標籤相關資訊與時間、識別固定或移動中的標籤等。

根據使用的場合不同讀取器可分為固定式和手持式兩種。固定式讀取器通常設置於停車場入口、倉庫出入口及門禁入口等受管制的閘門，讀取通過出入口貨品、人員、車輛…等上面的標籤。手持式讀取器因機動性高移動性佳之特點，方便倉儲管理人員做行動式物品清點與盤點作業。

(3) 中介軟體

中介軟體的用處在於橋接前緣設備與應用程式或系統間的接口，其功能主要有二；其一是做為從應用系統傳達指令給前緣設備的命令轉譯器，其二係做為整理從前緣設備取得的資料，並轉譯成對應用系統有意義的資料之轉換功能。通常可以分為三個模組，分別為讀取器介面、標籤訊息處理，和應用系統介面(高志中 2009)。以下則分述：

(3.1) 讀取器介面

提供讀取器硬體中介軟體通訊的介面，透過這個介面可以設定參數(讀取器參數、天線參數)、讀寫標籤編號，並透過有線或無線的方式聯結遠端監控讀取器。

(3.2) 標籤訊息處理模組

a. 標籤訊息過濾：過濾無法辨識、無關聯、多餘或重複的標籤資料。
b. 事件資料整合：接收來自不同讀取器的標籤資料，並利用演算法群組、歸類或分析統計成事件。
c. 自動控制：監控事件變化，並且致動其他設備進行自動控制，例如：商品 RFID 標籤未消磁通過閘門則觸發警報器。
d. 資料轉換：依照後端資訊系統需求，將資料轉換成不同格式。

(3.3) 應用系統介面

提供後端資訊系統取得經過過濾、整合和轉換後的標籤資料。

(3.4) 資訊系統

資訊系統例如企業資源系統、供應鏈系統、顧客關係管理系統、庫存管理系統…等，接收與處理讀取器取得的資料，透過使用 RFID，使得資訊系統能夠與實體世界連接，對於事件發生能快速的知覺並且做出反應，增進現存資訊系統能力。

2.2 IoT

2.2.1 IoT 的定義

由於 IoT 涵蓋領域甚廣，IoT 的定義目前並沒有一個統一的觀點，相關 IoT 定義整理如表 1。

表 1 IoT 相關定義

定義	作者
IoT 可被概念地定義為：擁有自我配置能力的動態全球網路基礎設施，且利基於標準和可互相運作的通訊協定，讓實體和虛擬的物件(Things)有身份、實體屬性，和虛擬人格，並且利用智慧界面無縫地整合進資訊網路中。	Vermesan et al. (2011)
未來的 IoT 使得可唯一識別的物件與其虛擬表示形式，透過網際網路作連接，或連接物件的身份、狀態、位置到額外資訊，或連接物件任何其他商業、社交或私人相關資訊。無論是否有財務支付，這樣的連接形式超過原本提供資訊的成果，並提供預先定義以外的參與者存取資訊。在正確的數量、條件、時間，和地點，提供準確和適當的資訊存取，並要求合適的價格。IoT 不是無所不在/普式運算(Ubiquitous/ Pervasive Computing)的代名詞，它包含了 IP 協定、通訊科技、內嵌設備、應用程式、人聯網(Internet of	Uckelmann et al. (2011)

People)，或組織內/跨組織(Intranet/Extranet)物聯網等所有方法。	
IoT是未來Internet不可分割得一部份。可被定義成擁有自我配置能力的動態全球網路基礎設施，且利基於標準和可互相運作的通訊協定，讓實體和虛擬的物件(Things)有身份、實體屬性，和虛擬人格，並且利用智慧界面無縫地整合進資訊網路中。在IoT中，物件(Things)被期許成為在商業、資訊，和社交等流程中的主動參與者；它們能彼此互動溝通，透過交換資料和感應(Sensed)環境資訊，在有人或無人的介入下，自動的反應真實世界中的事件，甚至藉由執行觸發動作和創造服務影響事件。介面以服務的形式促進與智慧物件(Smart Things)在Internet上互動(查詢、改變狀態，以及任何與其相關的資訊)並考慮安全和隱私問題。物聯網是一套讓真實世界中的任何物體隨時連結的網絡，透過網際網路技術讓各種實體物件、自動化裝置彼此溝通和交換資訊。…讓任何物體可以隨時和其他物體溝通…交換資訊，達到控制和通訊的目的。	CERP-IoT (2009, 2010) IoT-EUROPE (2009)
一個全球網路基礎設施，透過開發資料捕捉和通訊能力，連接實體和虛擬物件。這基礎設施包含現存且發展中的Internet與網路建設。它會提供特定的物件識別、感測器，和連接能力，作為發展獨立合作服務和應用的基礎。具有高度自動化資料捕捉、事件傳遞、網路連接性，和互相運作性等特性。	CASAGRAS (2010)

2.2.2 IoT 中的物件

ITU (2005)認為IoT的發展有賴於四個關鍵技術的進步，分別是RFID、感應器(Sensor)、內嵌智能(Embedded Intelligence)、奈米科技(Nanotechnology)；物件要能被識別，使物件的資料能被收集和處理，RFID在這方面是關鍵技術；物件要能感測實體環境的改變、資訊，或狀態，這要依靠感應器的發展；內嵌智能技術能更進一步的賦予物件網路通訊和資訊處理能力；另外為使資訊科技物件體積更小增加可攜性，需仰賴奈米科技；結合這些關鍵技術的發展可以創造IoT世界。

2.2.3 RFID 技術於 IoT 的應用

使用RFID技術使標示物成為所謂的智慧物件是否就是IoT應用，這其實可以從RFID技術如何被應用來看，Chiang et al.[2007]認為RFID的應用遷移可分做四個階段：

(1) Proprietary：企業或政府組織使用 RFID，設計特定系統追蹤特定資產，這些追蹤資訊通常只被使用和保留於企業和政府組織內部。
(2) Compliance：企業為配合重要的合作顧客或符合監管機構要求，而使用RFID技術，但通常企業內並未使用RFID相關資料。
(3) RFID-Enabled Enterprise：企業使用RFID資訊改善企業內部流程；此階段使用RFID的企業會與其他夥伴，在穩固的標準、安全與穩固的網路上分享RFID資訊。
(4) Internet of Things：RFID技術使用將要邁向的階段；RFID技術和其他能達成IoT的技術，與高度標準化和顧客所需求的獨特產品相結合，在這個基礎上會使人們對資訊、實體物件，和地點之間所認知的關係，產生巨大的改變。

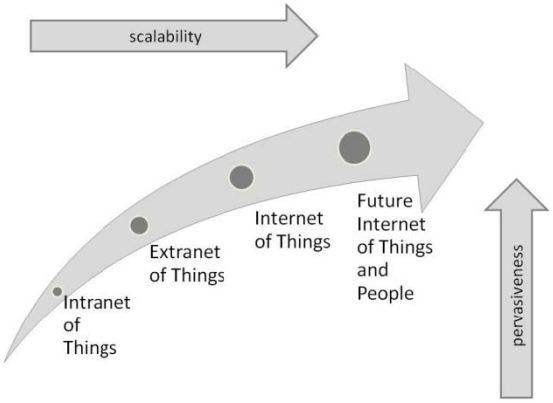


圖2：從IoT至未來IoT願景的階段區分 [21]

另外可以從IoT的角度來看其發展如圖2所示，大致上可分成三個階段Intranet of Things、Extranet of Things，和Internet of Things [Uckelmann et al.，2011；Zhou，2012]，概念上與RFID使用型態的遷移相類似，像是企業使用RFID技術，追蹤定位產品或資產等物件，和改善企業流程等，將RFID技術應用於組織內部管理屬於Intranet of things，而進一步擴大RFID技術應用，串連企業上下游甚至整個供應鏈，將RFID資訊分享於企業間屬於Extranet of Things，再進一步延伸既有應用支援開放Internet架構就可達IoT的範疇。

2.3 服務架構

Michael (2007)認為服務領域有三個重要的角色，分別為物件(Thing)、設備(Device)、人(Human)，並認為移動式RFID服務(Mobile RFID Services)依

照其啟動型態作區別可分為三種，分別是人啟動服務(Human Initiated Services, HIS)、設備啟動服務(Device Initiated Services, DIS)，和物件啟動服務(Thing Initiated Services, TIS)等，以下分述：

(1) 人啟動服務: 通常使用者利用裝載 RFID 讀取器的手機(Mobile RFID)，啟動在手機裡的應用程式，讀取物件上的 RFID 標籤並獲取相關資訊。
(2) 設備啟動服務：網路內的 Mobile RFID 或其他設備啟動的服務，而非透過人或物件啟動服務。
(3) 物件啟動服務：在無人為介入的情況下，行動設備讀取到標籤所啟動的服務。例如當保全人員帶著 Mobile RFID 手機經過貼有 RFID 標籤的門，Mobile RFID 手機裡的服務會啟動，並識別門上的 RFID 標籤，作為保全人員的巡察紀錄。

2.4 IoT 與 RFID

ITU 對於 IoT 物件所描述的相關能力包括被識別、資料傳輸(通訊)、感應環境資訊、資訊處理等，此節探討 RFID 相關限制與如何架構 RFID 為主的 IoT 服務架構。

2.5 RFID 標籤應用上的限制

本研究將 RFID 與 IoT 作結合，RFID 標籤可附加在物件上，然而 RFID 技術應在 IoT 中有些限制整理如表 2 所述：

表 2 RFID 標籤在 IoT 應用中的限制

	被動式 RFID 標籤	主動式 RFID 標籤
識別	具備	具備
資料傳輸(通訊)	有限能力 說明：標籤需靠讀取器的電波獲取所需電源，才能回應標籤資訊，為被動通訊能力，不具備主動通訊和與其他物件通訊的能力。	有限能力 說明：無法與其他物件直接通訊，需透過中介媒體如讀取器、中介軟體，或後端資訊系統等輔助。
感應環境資訊	不具備 說明：根據 EPCglobal 定義，不具備此能力。	有限能力 說明：根據 EPCglobal 定義，此功能為選擇性具備。
資訊處理	說明：受限於電源，標籤內晶片資訊處理能力有限，無法執行複雜運算。	說明：電源的使用為支援長距離與主動通訊，標籤內晶片資訊處理能力有限，無法執行複雜運算。

2.6 RFID 為主的 IoT 應用

綜合上述，要設計 RFID 為主的 IoT 應用需具備三個要素，如下分述：

(1) 智慧系統(Smart System)：RFID 標籤需要智慧系統支援。
(2) 物件命名服務(Object Name Service, ONS)：為了要在 RFID 標籤離開企業資訊系統範圍時，能將標籤裡的 EPC 與服務作對應。
(3) 記錄標籤被讀取器讀取的資料：像是標籤 X 被天線 Y 在時間 T 讀取到，並轉換成高階事件資料，再利用如 EPCglobal 架構中定義的伺服器如 EPCIS(EPC Information System)，捕捉、儲存和提供查詢，透過事件資料啟動相關的程式或服務。

2.7 IoT 服務架構

在了解本研究的 IoT 物件後，接著我們要了解 IoT 物件如何透過服務相互運作，基於 Michael (2007)的服務架構，我們設計了 IoT 服務架構，如圖 3 所示。

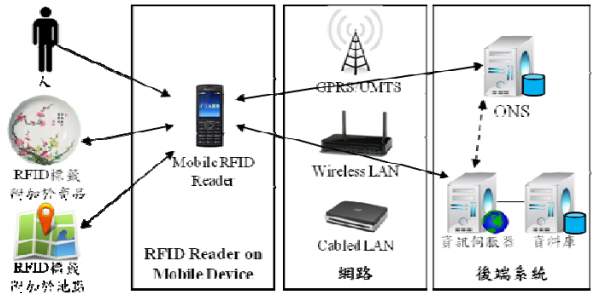


圖 3 IoT 服務架構

資料來源：本研究整理

3. IoT 服務案例設計

本研究之個案單位為 N 博物館，N 博物館典藏歷史悠久的中華瑰寶，收藏珍貴藏品總數超過六十五萬件。N 博物館各式文創基金商品(以下簡稱基金商品)，目前由文化行銷處基金管銷科(以下簡稱基金科)負責，營運基金商品進貨、出貨、儲存、經銷…等作業，基金商品材質如銅器、瓷器、塑膠、絲綢、紙張等，共計約 300 餘種，每年平均商品流通量 100 萬件，基金商品出入庫頻繁。

本研究以 N 博物館的基金商品銷售情形為個案，並以本研究 IoT 服務架構設計應用案例三種，以下分述：

3.1 物件啟動服務案例：

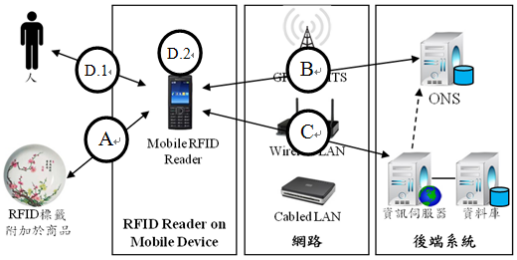


圖 3 IoT 服務架構－TIS

商品和地點有附加上 RFID 標籤，消費者可以利用裝有 RFID 讀取器的移動裝置(如具有 NFC 功能的手機)感應 RFID 標籤啟動服務，本研究設計感應產品和地點等標籤的物件啟動服務案例，如下分述：

3.1.1 感應產品 RFID 標籤

(1) 參考圖 3，移動式 RFID 設備感應產品 RFID 標籤後(A)，取得產品唯一識別碼(例：urn:epc:id:gid.0614141.3.0)。

(2) 移動式 RFID 設備上的程式將唯一識別碼轉換成可透過 DNS 系統查詢的完整網路名稱(Fully Qualified Domain Name，FQDN，例如：0.3.0614141.gid.id.onsepc.com.)，依循 DNS 系統查詢方式，找到特定 ONS 伺服器(B)，ONS 伺服器回傳 FQDN 所對應的服務網址(例：http://www.example.com/product/12345)。

(3) 得到 FQDN 所對應的服務網址後，移動式 RFID 設備上的程式會做兩件事情，以下分述：

(3.1) 開啟基金商品介紹網頁並儲存查詢紀錄移動式 RFID 設備上的程式依此服務網址(例：http://www.example.edu.tw/product/12345)向伺服器提出請求，伺服器回傳網頁資訊(C)，其中包括基金商品相關資訊，以及所對應的文物資料(如：文物的數位圖像)，在移動式 RFID 設備上開啟(D.1)，並同時傳送查詢紀錄給伺服器。



圖 4 移動裝置開啟網頁

3.1.2 啟動移動式 RFID 設備上程式的服務

使用 FQDN 所對應的其他服務網址，購買商品網址，和使用者活動網址，移動式 RFID 設備上的程式在取得這兩個網址後，改變程式的使用者介面(D.2)；購買商品網址的使用，會在人啟動服務的部分描述，而使用者活動網址的使用，會在設備啟動服務的部分描述。

3.2 人啟動服務案例

基金商品銷售量多，常使得結帳櫃台大排長龍，造成營運上的困擾；此案例使用 IoT 方式解決商品購買問題，讓消費者可以透過移動裝置直接購買商品，減少排隊時間。感應過地點標籤後，如圖 5 的購買商品按鈕進入購買畫面，步驟如下分述：



圖 5 更新程式畫面

(1) 使用者操作移動式 RFID 設備程式的使用者介面，進入自助購買基金商品使用者介面(A)。

(2) 移動式 RFID 設備利用感應商品上的 RFID 標籤得到商品唯一識別碼(B)，移動式 RFID 設備上的程式將唯一識別碼轉換成可透過 DNS 系統查詢的 FQDN，依循 DNS 系統查詢方式，找到特定 ONS 伺服器(C)，ONS 伺服器回傳 FQDN 所對應的服務網址。

(3) 移動式 RFID 設備的程式依此服務網址向伺服器取得商品資訊(D)，並更新使用者介面裡的基金商品清單與交易金額，第二和第三步驟會一直重複直到使用者確定欲購買基金商品清單。

(4) 當使者確定欲購買基金商品清單，然後點擊購買按鍵，交易的相關資訊會傳遞至伺服器(E)，並存取第三方金流服務，交易的結果會回傳至移動式 RFID 設備給使用者知道(A)，完成自助交易流程。

3.3 設備啟動服務案例

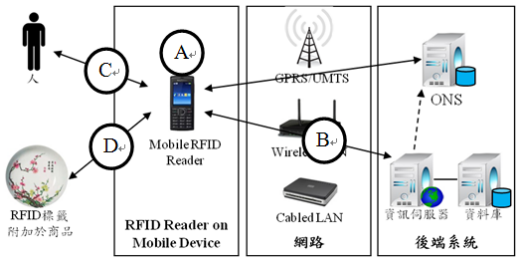


圖 6 IoT 服務架構－DIS

參考圖 6，感應過附加在地點的標籤後，移

動裝置上的程式會以定時的方式,每 10 秒向使用者事件伺服器發出請求更新事件，若有新事件會通知使用者，步驟如下分述：

(1) 使用者操作移動式 RFID 設備程式的使用者介面，進入自助購買基金商品使用者介面(A)。
(2) 移動式 RFID 設備的程式向後端系統請求使用者活動資料(B)。
(3) 得到後端系統回覆後，移動式 RFID 設備更新使用者介面和活動資料，若有新事件則提醒使用者查閱(C)。
(4) 當使者確定欲購買基金商品清單，然後點擊購買按鍵，交易的相關資訊會傳遞至伺服器(E)，並存取第三方金流服務，交易的結果會回傳至移動式 RFID 設備給使用者知道(A)，完成自助交易流程。

4. 結論與討論

本論文整理了 IoT 相關的定義，我們發現：RFID 技術和其他能促進 IoT 的技術可以與高度標準化和用戶所需求的獨殊物件相結合；在這個基礎上 IoT 會促成人們對資訊、實體物件，和地點之間關係的認知。基於此一觀點，我們建構了一個 IoT 服務架構，它包括了人、附於地點和附於物件之 RFID 標示，行動裝置之 RFID 讀取器，網路及後端系統。其中，移動式 RFID 設備可將唯一識別碼轉換成 DNS 系統查詢的完整網路名稱，然後依循 DNS 系統查詢方式，找到特定 ONS 伺服器，ONS 伺服器回傳網路名稱所對應的服務網址。透過上述設計，我們倡議考量人、設備，以及物件間的互動方式設計相關 IoT 創新服務。

在前述 IoT 服務架構的基礎上，本研究以 N 博物館為個案，設計相關 IoT 應用，驗證架構的正確性與可行性，並解決基金商品在設計鏈、務流及銷售管理方面的問題。由於在此一個案上之成功，本研究所提出之 IoT 服務架構及相當技術實可供 IoT 的設計與服務應用做為參考，並更進一步之發展。

5. 參考文獻

[1] 高佑嘉，2010，下一波資訊發展浪潮：物聯網時代即將降臨，資策會 FIND，Retrieved September 15, 2011。

[2] 高志中，2009，RFID 資訊應用系統之設計實務，台北縣：博碩文化.。

[3] 陳瑞順，2009，RFID 概論與應用，台北縣：全華圖書。

[4] 張琳一，2012，晶隼科技推出可內建手機超低價 UHF RFID 讀取器模組，DIGITIMES，Retrieved September 25, 2012，取自：http://www.digitimes.com.tw/tw/iot/shwnws.asp?cnlid=15&cat&packageid=5920&id=0000278515_G2C4KHR02FGKSX4PQUC3Y。

[5] 鍾曉君，2011，智慧聯網商業模式發展評析，資策會 FIND，Retrieved May 30, 2012。

[6] Armenio, F., Barthel, H., Dietrich, P., Duker, J., Floerkemeier, C., Garrett, J., Harrison, M., Hogan, B., Mitsugi, J., Preishuber-Pfluegl, J., Ryaboy, O., Sarma, S., Suen, K., and Williams, J. "The EPCglobal Architecture Framework," EPCglobal, Dec. 15 2010 (avaible online at http://www.gs1.org/gsmp/kc/epcglobal/architecture/architecture_1_4-framework-20101215.pdf).

[7] Banks, J., Hanny, D., Pachano, M. A., and Thompson, L. G. RFID Applied John Wiley & Sons, New Jersey, 2007.

[8] CASAGRAS "RFID and Inclusive Model for the Internet of Things," CASAGRAS, 2010 (avaible online at http://www.grifs-project.eu/data/File/CASAGRAS%20FinalReport%20(2).pdf).

[9] CERP-IoT "Internet of Things Strategic Research Roadmap," CERP-IoT, Sep. 15 2009 (avaible online at http://www.grifs-project.eu/data/File/CERP-IoT%20SRA_IoT_v11.pdf).

[10] CERP-IoT "Vision and Challenges for Realising the Internet of Things," CERP-IoT, Mar. 2010 (avaible online at http://www.internet-of-things-research.eu/pdf/IoT_Clusterbook_March_2010.pdf).

[11] Chaouchi, H. The Internet of Things: Connecting Objects ISTE Ltd and John Wiley & Sons, Inc., London and Hoboken, 2010.

[12] EPCglobal "GS1 EPC Tag Data Standard 1.6," EPCglobal, Sep. 22 2011 (avaible online at http://www.gs1.org/gsmp/kc/epcglobal/tds/tds_1_6-RatifiedStd-20110922.pdf).

[13] EPCglobal "EPCglobal Standards Overview," EPCglobal, 2012 (avaible online at http://www.gs1.org/gsmp/kc/epcglobal).

[14] IoT-EUROPE "Introduction," IoT-EUROPE, 2009 (avaible online at http://www.internet-of-things.eu/introduction).

[15] ISO/IEC "Standards and projects under the direct responsibility of JTC 1/SC 31 Secretariat," ISO/IEC, May, 8 2012 (avaible online at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45332).

[16] ITU "The Internet of Things," ITU, Oct. 28 2005 (avaible online at http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf).

[17] Michael, M. P. "Architectural solutions for mobile RFID services for the internet of things," in: Computer Science, Helsinki, Helsinki, 2007.

[18] NCC "認識頻率," NCC, 2012 (avaible online at http://freqdbo.ncc.gov.tw/Portal/NCCB01Q_.aspx).

[19] NEC "RFID 頻段," NEC, 2012 (avaible online at http://tw.nec.com/zh_TW/solutions/rfid/outline02.html).

[20] Uckelmann, D., Harrison, M., and Michahelles, F. Architecting the Internet of Things Springer-Verlag New York Inc, New York, 2011.

[21] Vermesan, O., and Friess, P. Internet of Things-Global Technological and Societal Trends From Smart Environments and Spaces to Green ICT River Publishers, London, 2011.

[22] Ward, M., Kranenburg, R., and Backhouse, G. "RFID: Frequency, standards, adoption and innovation," JISC Technology and standards Watch, May 2006 (avaible online at http://www.rfidaa.org/upload/documents/PDF/RFID%20explained.pdf).

[23] Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., Balazinska, M., and Borriello, G. "Building the internet of things using RFID: the RFID ecosystem experience," Internet Computing, IEEE (13:3) 2009, pp 48-55.

基於 Wi-Fi 之無線化廠區雲端機台遠端監控平台設計

Design of a Cloud Platform for Machine Wireless Remote Monitoring Based on Wi-Fi Technology

*陳響亮 王欣如 陳韻堯
國立成功大學 製造資訊與系統研究所
* slchen@mail.ncku.edu.tw

摘要

製造業生產線上的機台是否能維持正常運作，對於製造廠之競爭力有非常大的影響。當機台無預警的發生故障，除了機台停止生產外，往往需要工程師花費時間故障排除、重新調整製程參數。若能降低線上機台停機時間，則可以縮短製程時間，降低製造成本，提升製造廠之產業競爭力。因此，本研究提出規劃機台服務製造雲，以Wi-Fi 為基礎擷取廠區機台製造資訊，實現廠區機台M2M(Machine to Machine)之概念，並設計一雲端機台遠端監控平台，解決上述問題。研究中所設計之平台可即時蒐集機台製造生產資料於雲端資料庫。當發生機況時，工程師能夠立即透過Wi-Fi使用行動裝置查看機台資訊，也可透過機台服務製造雲完整回溯機台歷史狀態，有效釐清問題與排除機況。預計未來實作成果可達成廠區無線化且隨時隨地監控的功能，維持廠區機台生產效率和品質。

關鍵詞： Wi-Fi、M2M、遠端監控、製造雲、雲端運算

Abstract

Maintenance of inline machines is an important issue for vendors or industries. When machines failed without warning, for stopping production, engineers need to spend time on equipment troubleshooting and process parameters readjustment. We can reduce equipment idle time by reducing the down status time of it. Therefore, a design of cloud-based platform for machine wireless remote monitoring based on Wi-Fi technology is proposed. By adapting the concept of M2M (Machine to Machine) for designing cloud-based remote monitoring platform, The proposed platform is able to collect manufacturing data real-time and can be saved in cloud manufacturing database. When machine error occurred, engineers can immediately using mobile devices to view manufacturing information via Wi-Fi in the factory. Engineers can also check the equipment history records for effectively clarifying problems and troubleshooting machine errors. The future implementation of the design in this study can improve the efficiency and quality of machine production in factories.

Keywords: Wi-Fi、M2M、Remote monitoring、Cloud manufacturing、Cloud computing

1. 前言

以往的機台製造業僅於販售機台與售後維修保固服務，隨著資訊通訊技術的發展，物聯網(Internet of Things, IOT)與雲端科技(Cloud Technology)概念的興起，機台製造業可提供的服務也從單純的產品交易延伸至後方機台的整合管理以建立緊密顧客關係。在 2006 年，Google 提出 Google101 計劃，雲端運算便開始蓬勃發展[1]，其透過雲端伺服器進行運算，用戶可在任何地方透過不同的終端獲雲端取服務，用戶不再需要耗費大量的成本於本地端伺服器的管理並可彈性取得雲端上提供的各種服務，且雲端伺服器比起本地端的伺服器具有較高的可靠度及擴展性[2]。Xun Xu[3]也提及製造企業若能將雲計算引入製造企業之生產管理系統中，將對企業帶來全新的商業服務模式，建立智慧型工廠。

2012 年行政院經濟建設委員會提出之三業四化方案[4]，其一為「製造業服務化」，經由線上遠端監控軟體，擷取製造機台的各項機械性能與軟體功能所產生的資訊，進行服務與管理，進一步協助客戶掌握工廠的加工資訊，加入雲端概念以雲端平台技術，加值製造服務作為企業競爭之優勢，以別於一般的差異化商業服務快速拓展業務。未來製造業服務化將成為企業競爭力的指標。

當廠區生產線上的機台無預警發生故障時，除了機台停止生產外，往往需要耗費工程師時間進行故障排除、重新調整製程參數，若能使產線機台接近零停機時間，則可縮短機台製程時間，降低製造成本，進而提升製造業之產業競爭力。本研究提出基於 Wi-Fi 之無線化廠區雲端機台遠端監控平台，以 Wi-Fi 為基礎擷取廠區機台製造資訊，實現廠區機台 M2M 之概念，解決上述問題。透過本研究架構能夠即時蒐集廠區製造生產數據，當故障發生時，工程師能夠完整回溯機台歷史狀態，達到問題有效釐清與故障排除。並且能夠隨時隨地監看機台狀況，維持廠區機台生產效率和品質，協助製造廠區達到機台整合管理。

2. 研究目的

本研究主要目的為建構一 Wi-Fi 之無線化廠

區雲端機台遠端監控平台與機台服務製造雲，包含下述四項之開發指標：

1. 規劃製造廠區 Wi-Fi 設備之佈建，透過 Wi-Fi 擷取廠區機台生產資訊。
2. 規劃機台服務製造雲，延伸機台製造業提供的商業服務至後端製造資訊之整合性管理。
3. 基於機台服務製造雲規劃雲端機台遠端監控平台，提供製造廠區人員整合管理。
4. 實際測試 Wi-Fi 與機台連接，並分析 Wi-Fi 預計佈署效益與預計廠區導入本研究架構前後效益比較。

3.文獻探討

3.1 廠區機台資訊擷取佈建

以往廠區機台聯網佈建多採取有線乙太網路方式進行，近年來行動裝置普及，使得企業開始重視無線網路環境的佈建。安全的無線網路，需具備 End to End 加密，End To End 加密方式使無線網路具備擴充性、安全性、移動性與低成本優點，而目前技術也已發展完備。以網路佈建之成本、設備、後端管理、應用性、安全性考量，有線網路不再是最佳考量[5][6]，本研究也將加入 End To End 加密考量至 Wi-Fi 設備選擇的條件中。

部分遠端監控系統提出以 ZigBee 方式進行資料蒐集[7][8]，雖然 ZigBee 體積小、低成本、也具可靠性，但其傳播距離短(相鄰節點之間的距離 10-100m)，雖提高功率可延長傳播距離，但會縮短其內部電池的壽命。對於一般製造廠區而言，機台數量眾多且線上製造機台動輒數百萬，需要能夠提供穩定可靠且不需經常更換的聯網設備，因此本研究採用 Wi-Fi 做為製造機台之聯網設備。

3.2 M2M (Machine to Machine)應用

M2M 概念為設備與設備之間的溝通，透過網路作為橋樑，將設備的資訊傳遞至遠端的系統平台處理，設備之間傳遞資料可透過伺服器與系統進行溝通處理。M2M 系統被廣泛應用於各種領域，目前市場約有 100 萬無線 M2M 連接點，而未來預計市場 2016 年將達到 359 萬個連接點[9]，應用領域廣大包含智慧家庭系統、遠端監控系統、醫療保健、機械設備、貨物追蹤等[10]。

國家實驗研究院-科技政策研究與資訊中心(STPI)[11]與 RCG[12]皆提及提出 M2M 應用系統包括以下三點：

(1)現場設備的數據收集和監控

(2)設備可透過網路與伺服主機聯繫

(3)透過伺服主機之系統平台進行資料分析、反應與處理

歐洲電信標準協會 (The European Telecommunications Standards Institute, ETSI) 提出對於 M2M 服務模型提出定義[13]，ETSI 將 M2M 服務模型分為兩大部分，一為設備間的溝通，二為設備連網後所提供應用之服務，其架構如圖 1：

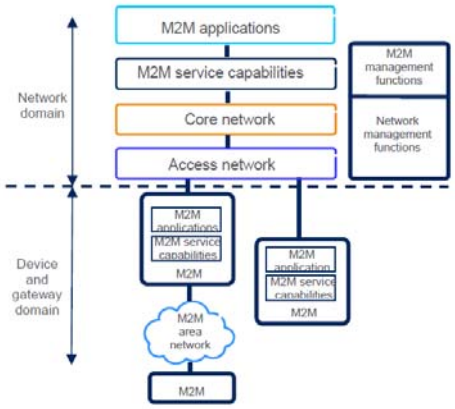


圖 1 ETSI 提出之 M2M 服務模型[13]

隨著雲端運算的興起，透過雲計算可提供大規模的設備管理和服務，解決以往複雜的 M2M 應用，集中管理和決策數十億的設備將成為 M2M 重要的精隨[14]。由 Geng Wu 等人提出一 M2M 架構結合雲端運算概念[15]，其將 M2M 伺服器與服務建置於雲端，並提供一行動化系統提供使用者取用服務，如圖 2 所示。

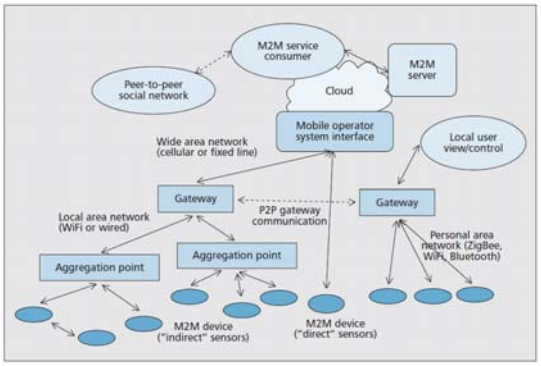


圖 2 M2M 架構結合雲端運算概念[15]

綜合以上所述，本研究規劃一應用於製造廠區機台遠端監控之 M2M 架構，如 4.1.1 所示。

3.3 雲端運算技術之應用

3.3.1 雲端運算模型定義

NIST (National Institute of Standards and Technology, 國家標準與技術研究院)提出對雲端運算的定義[16]，並說明符合雲端運算之系統，必須具備此定義之五項基本特徵。表 1 為 NIST 定義雲端運算之描述。

表 1 NIST 對雲端運算模型之定義[16]

Five **Essential Characteristics** (五項基本特徵)	On-demand self-service. Broad network access. Resource pooling. Rapid elasticity. Measured Service.
Three **Service Models** (三種服務模式)	Software as a Service (SaaS). Platform as a Service (PaaS). Infrastructure as a Service (IaaS).
Four **Deployment Models**	Private cloud. Community cloud.

(四種佈署模式)	Public cloud. Hybrid cloud.

依照 NIST 對雲端運算模型之定義，本研究之平台將使平台具備以下五項特徵－隨需自助服務、隨時隨地用任何網路裝置存取、多人共享資源、快速重新佈署靈活度、可被監控與量測的服務，提供 PaaS、IaaS、SaaS 的服務，本研究將採用私有雲方式建置製造雲後端伺服器環境。

4.3.2 IaaS 於廠區機台遠端監控

IaaS 提供後端製造雲基礎設施與建置虛擬環境，於虛擬環境中，可提供快速重新佈署的靈活度。雲端伺服器佈署平台與服務讓多使用者能夠共享資源，雲端資料庫則存放機台製造資訊與雲端平台相關資料。

4.3.3 PaaS 於廠區機台遠端監控

PaaS 提供雲端製造服務平台，使用者可根據自己的需求選擇平台所提供的服務，支援雲端應用，平台需仰賴 IaaS 雲端基礎設施資源。製造雲可透過 PaaS 平台整合服務，使用者只需利用任何網路裝置聯網，即可隨時隨地存取平台之服務。

4.3.4 SaaS 於廠區機台遠端監控

Bernhard Holtkamp 等人[17]對於 SaaS 層提出以下定義，SaaS 層將運算、儲存及網路等資源轉化為標準化服務，提供使用者在網路環境下進行操作。本研究將轉化 PaaS 規劃之平台功能為雲端服務，設計一行動化 APP 應用程式存取服務。

在本研究規劃 IaaS 層為雲基礎設施與虛擬環境建置；PaaS 層規劃為雲端機台遠端監控平台與製造雲服務整合開發；SaaS 層規劃將提供製造廠區一行動化 APP 應用程式取用雲端所佈建的服務，讓廠區人員使用行動裝置即可操作。

3.4 遠端監控系統

由陳響亮等人[18]提出之工具機智慧型遠端加工及診斷與維修軟體系統，在遠端監控模組功能規劃，遠端主機連線、機台遠端運動控制及加工參數傳輸、機台資料紀錄及遠端讀取、檔案傳輸、文字即時訊息交談視窗等功能，本研究將參考其功能並加入行動化 APP 概念使本研究平台服務加值，平台功能規劃如 4.3.2 所示。

Dragan Djurdjanovic 等人[19]提出以 Web 建構一遠端監控平台應用於機床主軸的診斷預測，此研究之架構如圖 3，此遠端監控平台在後端 Server 部分採 P2P 架構建置。作為一個可提供廠區給多用戶使用的製造管理平台若採用 P2P 架構會有速度過慢且資訊安全不夠嚴謹的問題，因此在本研究將加入雲端的概念並以私有雲的架構去建置一個廠區生產機台之雲端機台遠端監控平台。

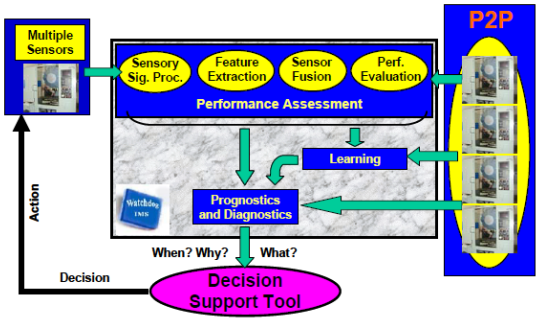


圖 3 Dragan Djurdjanovic 等人提出之遠端監控平台架構[18]

4.研究方法

4.1 製造廠區 Wi-Fi 模組佈署

4.1.1 本研究之 M2M 架構

本研究 M2M 架構分為兩大部份共 5 層，第一部份為 Device domain 有 M2M device Layer、M2M hardware Layer、Middleware Layer，第二部份為 Communication network Layer、Cloud service Layer，架構如圖 4 所示。

以下將對本研究 M2M 架構分層敘述：

(1) M2M device Layer：實現 M2M 的第一步就是將機器設備中獲得的數據，透過網路發送出去，使機器具有 talk 的能力。方法有兩種，一為生產機器設備的時候即嵌入 M2M hardware；二為對現有機器進行加裝，使其具備聯網能力。本研究以製造廠區機台為研究對象，為現有機器。因此本研究將於 M2M hardware 層規劃對廠區機台加裝之設備。

(2) M2M hardware Layer：M2M hardware 是使機器具備通訊和聯網能力的設備。本研究採用 Wi-Fi Node 組裝於製造機台，使其具備聯網能力。

(3) Middleware Layer：主要負責數據收集，為 M2M 架構中的"翻譯員"。收集來自機台的數據，將數據傳送給訊息處理系統。本研究於此採用陳響亮等人[20]開發之 i-line 32 software 擷取製造機台控器上的製造資訊，並傳遞至雲端資料庫儲存。

(4) Communication network Layer：將蒐集的數據傳送至 Cloud service Layer，Communication network 在整個 M2M 架構扮演重要角色。本研究架構通訊網路將會通過無線網路 Wi-Fi(IEEE 802.11)與有線網路 Ethernet (IEEE 802.3)傳遞數據。

(5) Cloud service Layer：將雲端資料庫中的數據進行處理，將結果呈現給觀察者和決策者，並進一步建置雲端服務或應用程式。本研究於此層將建構一製造雲，其中包含雲端伺服器、雲端平台、App 應用程式、製造雲端服務等，提供 PaaS、IaaS、SaaS 服務。

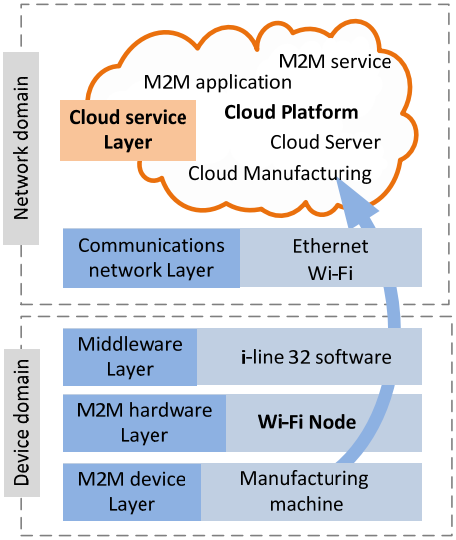


圖 4 本研究之 M2M 架構

4.1.2 廠區 Wi-Fi 模組佈署架構

本研究於廠區機台 Wi-Fi 模組佈署架構如圖 5 所示，在廠區內在每台機台上都裝上一台 Wi-Fi 傳輸模組，如圖 5 中 Wi-Fi Node。Wi-Fi Node 透過 RJ-45 Port 加裝於機台上，再透過網路設定使機台擁有無線功能，Wi-Fi Node 與 AP 連接透過無線網路將機台資訊傳至伺服器儲存。

在跨廠區佈建，透過 Switch/Router 串接，若廠區距離較遠可透過佈署 AP Node 將無線網路串起，其佈署架構如圖 5。

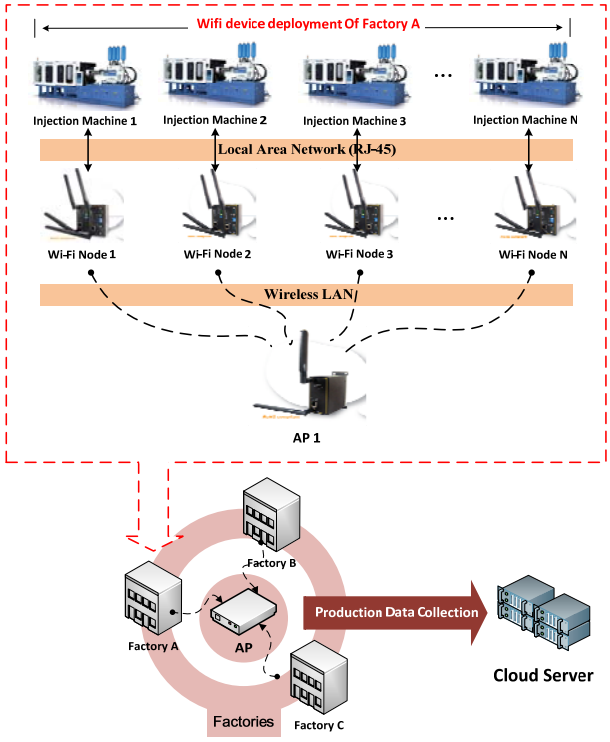


圖 5 廠區機台資訊收集 Wi-Fi 模組佈署

4.2 機台服務製造雲之建置規劃

本研究規劃之雲端伺服器環境，將規劃私有雲方式建置，圖 6 為本研究之規劃佈署架構。使用者只須透過可聯網之載具，經由網路通過防火牆進入本研究之私有雲雲端服務環境，即可取得服務。在雲端伺服器佈署部分，本研究規劃使用兩台實體伺服器，一台利用虛擬化技術分割成三台虛擬伺服器分別做為平台服務佈署、備份雲佈署、資料庫佈署、平台機制佈署(身份辨識、負載平衡等)；另一台實體伺服器則用來資料備份。於此，為本研究規劃提供之 IaaS 服務。

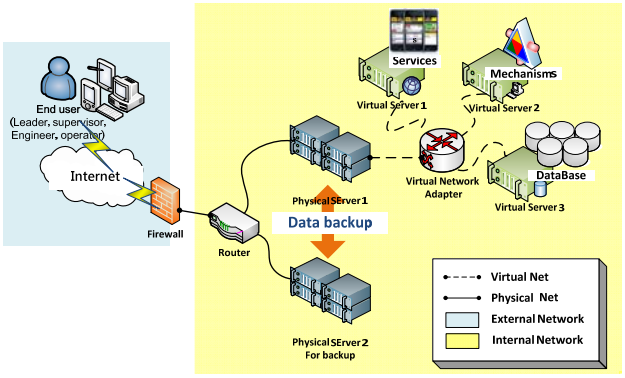


圖 6 雲端伺服器網路設備佈署架構

4.3 行動化雲端製造服務平台之規劃

4.3.1 行動化雲端製造服務平台架構

本研究平台架構如圖 7，廠區機台透過 RJ-45 Port 連接 Wi-Fi 模組，將機台生產資訊傳遞至廠區所架設的 AP，AP 再透過 TCP/IP 協定將生產資訊傳至伺服器，進入 Database 儲存。本研究所規劃之雲端機台遠端監控平台即可從雲端資料庫撈取資料以建置雲端服務。最後呈現的界面則有 Web 瀏覽器與行動版機台資訊應用 APP 兩種方式。於此，本研究透過平台提供廠區 PaaS 服務。

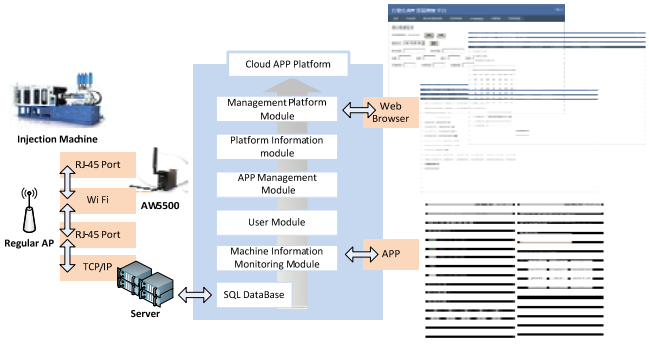


圖 7 行動化雲端製造服務平台架構圖

4.3.2 行動化雲端製造服務平台功能規劃

本研究規劃使用 ASP.NET 建置平台，平台以 Web Browser 方式呈現，提供用戶能夠上傳下載自

行設計之機台 App，平台功能包含使用者模組、APP 管理模組、訂閱模組、管理者模組，雲端機台遠端監控平台。

研究中雲端機台遠端監控平台主要規劃五大服務模組，分別說明如下。

(1)機台資訊監看模組：經由抓取雲端資料庫機台之資訊，顯示於平台上供使用者查看監測，提供機台生產統計表、多機狀態監看、加工資訊表、機台稼動率表等資訊。

(2)使用者管理模組

a. 使用者註冊認證服務：基於企業內部資訊安全，平台的使用者註冊後，須透過平台管理者二次認證後才能夠使用平台。

b. 使用者分群管理服務：註冊時依據不同身分別將使用者分成不同的群組管理，給予不同權限。

使用者資料維護/檢閱服務：提供使用者維護個人資料、變換群組申請。提供管理者查詢使用者基本資料。

(3)APP 管理模組

a. APP 上傳/下載服務：規劃雲端空間供使用者能夠上傳自行開發之 APP，與下載其他使用者設定公開的 APP 程式，並加強規劃不同使用者存取之區塊將使用戶資料隔離。

b. 權限設定服務：使用者透過此功能可將 APP 設定不同的公開程度，或是設定特定群組下載或閱覽。

c. 分類服務：平台提供多使用者上傳 APP，因此具備 APP 分類功能能讓使用者方便找尋 APP 程式。

d. 訂閱申請/取消服務：提供使用者訂閱其他使用者之 Windows/Android APP，當被訂閱者上傳新的 Windows/Android APP 則會透過平台通知功能來提醒訂閱者。

e.訂閱認證服務：透過此認證來告知被訂閱者其帳戶被訂閱，被訂閱者須確認許可後，訂閱者才能夠訂閱以保障被訂閱者之權益。

(4)平台資訊服務模組

a. 雲端空間與傳輸量資訊：提供查詢雲端空間使用狀況以及平台資料傳輸量的查詢。

b. 平台基本資訊服務：提供平台模組功能介紹、平台版本更新以及系統公告等資訊。

c. 平台通知服務：用戶能在此功能查詢由平台所發出之個人重要通知。

d. 平台用戶備忘錄服務：提供平台用戶紀錄個人重要資料或發出公告。

(5)管理平台權限模組

a.帳號管理服務：提供平台管理者管理平台所有的帳號、查詢帳號資訊、登入紀錄。

b.安全性管理服務：提供可連線之 IP 設定。

4.4 測試環境測試與效益分析

4.4.1 廠區機台 Wi-Fi Node 佈署

本研究採用佈署於機台之 Wi-Fi 模組，如表 2:

表 2 Wi-Fi 模組規格與功能

Atop AW5500	**設備規格**	相容標準	IEEE802.11 a/b/g/n
		傳輸率	300Mbps
		加密類型	TKIP, AES
		支援通訊協定	IPv4, TCP, UDP, DHCP Client, SNMP, SMTP, HTTP, DNS, RADIUS, RFC2217, WPS
		主要特點	可做為 Access Point, WDS Bridge, AP Client
	功能	於本研究作為 AP，串聯各個機台之 Wi-Fi Node。並作為跨廠區 Wi-Fi 佈署時的橋接設備。	
Atop SW5501	**設備規格**	**相容標準**	IEEE802.11 a/b/g/n
		傳輸率	300Mbps
		加密類型	TKIP, AES
		支援通訊協定	IPv4, TCP, UDP, DHCP Client, SNMP, SMTP, HTTP, DNS, RADIUS, WDS, WPS
		主要特點	具有串列傳輸功能
	功能	於本研究作為機台之 Wi-Fi Node，透過網路線(RJ-45)即可與工具機台連接，使機台具有無線傳輸功能。	

4.4.2 Wi-Fi 模組連接機台測試

Wi-Fi 模組連接機台測試畫面，如圖 8 所示使用者能夠成功使用平板電腦查看到機台製造資訊，圖 9 為本研究所採用之 Wi-Fi Node-SW5501，SW5501 透過 RJ-45 Port 與機台連接。



圖 8 使用 Windows 作業系統平板電腦讀取機台生產參數



圖 9 連接機台之 Wi-Fi 模組

4.4.3 無線網路預計佈署效益分析

廠區佈署 Wi-Fi 無線網路與乙太有線網路效益比較，如表 3 所示：

表 3 Wi-Fi 無線網路與乙太有線網路效益比較

	Wi-Fi 無線網路	乙太有線網路
佈署成本	低	高
變動成本	無	有
移動便利性	高	低
穩定度	一般	高
安全性	高	高
速度	視 Wi-Fi 設備而定	高
服務多樣性	高	一般

由表 3 可知採用若 Wi-Fi 無線網路佈署於製造廠區，比起以往採用有線網路有著更大的效益。以下將對於本研究架構預計導入製造廠區之前後做出比較，如表 4 所示：

表 4 本研究架構預計導入製造廠區之前後比較

	導入前	導入後
系統整合性	低	高
雲端基礎設備	有	完備
機台訊息即時性	低	高
廠區資訊整合性	低	高
資訊功能多樣性	低	高

5. 結論與未來展望

本研究提出無線化製造廠區，透過 Wi-Fi 設備佈建廠區，擷取機台製造資訊，並規劃機台服務製造雲，延伸機台製造業提供的商業服務至後端管理，規劃雲端機台遠端監控平台，提供製造廠區機台整合性管理。使製造廠區能夠透過 Wi-Fi 立即以行動載具接收機台資訊，完整回溯機台歷史狀態，有效釐清問題與排除機況。

本研究規劃採用私有雲方式建置雲端服務，對於企業內部資料提供安全的環境，使廠區能夠放心的讓客戶透過雲端機台遠端監控平台使用服務。本研究未來將進行平台開發、製造雲(IaaS、PaaS、SaaS)建置與廠區實際佈建，預計研究成果可達成無線化且隨時隨地監控的功能，使廠區機台維持生產效率和品質。

誌謝

感謝高科技設備前瞻技術發展計畫編號 302205501 與國科會編號 NSC 102-2221-E-006-107- 之計畫對本研究之經費提供與技術支援，由於國科會與賜福科技公司的支持，使本研究得以順利進行，特此致上感謝之意。

參考文獻

[1] Shuai Zhang, Shufen Zhang, Xuebin Chen, and Xiuzhen Huo, “Cloud Computing Research and Development Trend,” Second International Conference on Future Networks, 2010.

[2] Ning Liu, Xiaoping Li, and Qian Wang, “ A resource & capability virtualization method for cloud manufacturing systems,” IEEE International Conference , 2011.

[3] Xun Xu, “From cloud computing to cloud manufacturing,” Robotics and Computer-Integrated Manufacturing, Volume 28, Issue 1, pp. 75–86 , 2012.

[4] 行政院經濟建設委員會，工具機製造業服務化，[Online]. Available: http://www.cepd.gov.tw/m1.aspx?sNo=0018051 , 2012.

[5] DIGITIMES, http://www.digitimes.com.tw/tw/dt/n/shwnws.asp?cnlid=13&cat=50&id=0000329449_22736ACO590NM38OG6PBE#ixzz2bkxWyhdy

[6] ARUBA, 網路佈建新思維-無線與有線比重之考量, http://www.ecomsoft.com.tw/solution/s_02.html.

[7] Zhang Xiang-li, Yan Kun, Ye Jin, Li Jian, “A Remote Manufacturing Monitoring System Based on the Internet of Things,” International Conference on Computer Science and Network Technology, pp. 221 - 224, 2012.

[8] Qiang Ruan, Wensheng Xu, Gaoxiang Wang, “RFID and ZigBee Based Manufacturing Monitoring System,” Electric Information and Control Engineering (ICEICE), pp. 1672 – 1675, 2011

[9] Berg Insigth, The Global Wireless M2M Market, M2m Research 2012.

[10] Shih-Hao Hung, Chun-Han Chen and Chia-Heng Tu, “Performance Evaluation of Machine-to-Machine (M2M) Systems with Virtual Machines,” pp. 159 – 163, 2012.

[11] ETSI TS V1.1.1, Machine-to-Machine communications(M2M); M2M service requirements.

[12] Regal Cyber Group, M2M 技術簡介, http://www.rcg.tv/zh_tw/industry-technology/m2m-overview.html

[13] 科技產業資訊室，機器與機器的溝通-看 M2M 產業發展趨勢 http://cdnet.stpi.org.tw/techroom/analysis/2008/pat_08_A021.htm

[14] Željko Popović, Vanesa Čačković, “Cloud Based Service for M2M Communication”, International Symposium on Telecommunications, pp. 1-6, 2012.

[15] Geng Wu, Shilpa Talwar, Kerstin Johnsson, Nageen Himayat, and Kevin D. Johnson, Intel , “M2M: From Mobile to Embedded Internet,” IEEE Communications Magazine, vol. 49, pp. 36-43, 2011.

[16] Peter Mell, Timothy Grance, "A NIST Definition of Cloud Computing," National Institute of Standards, 2011.

[17] Bernhard Holtkamp, Sebastian Steinbuss, Heiko Gsell, Thorsten Loeffeler, Ulrich Springer "Towards a Logistics Cloud" 2010 Sixth International Conference on Semantics, Knowledge and Grids, PP.305-309, 2010.

[18] 陳響亮，林鼎皓，何季璋，”工具機智慧型遠端加工及診斷與維修軟體系統之開發研究,” NSC Project, 2004.

[19] Dragan Djurdjanovic, Jihong Yan , Hai Qi , Jay Lee and Jun Ni, “Web-Enabled Remote Spindle Monitoring and Prognostics“, 2007

[20] 陳響亮、郭晟宏、蕭應涵、王欣如、李庚學,” 基於射出成型機之雲端 e 化監控管理系統,” PMMT, 2013

機器型態通訊於下一代行動通訊網路之挑戰

曾啟維　　陳 灝
國立台灣大學資訊工程研究所
d95922034@ntu.edu.tw　　r01922111@ntu.edu.tw

摘要

機器對機器通訊(Machine-to-Machine Communication, M2M Communication)提供無須人為介入的自動化應用通信服務。3GPP 定義名為機器型態通訊(Machine-Type Communication, MTC)之標準作為 M2M 通訊之技術規範。本論文首先描述 3GPP MTC 網路架構，並提出 3GPP MTC 必須關注的挑戰議題，同時我們也提出目前解決這些關鍵議題的相關技術。

關鍵詞：機器對機器通訊、機器型態通訊、長程演進

Abstract

Machine-to-Machine (M2M) communication provides communications services for automation application without human intervention. 3GPP defines standards, namely Machine Type Communications (MTC), for M2M communications. In this paper, we first describe the general network architecture for 3GPP MTC. We discuss the challenges that should be notices in 3GPP MTC. Following by that, we survey the existing works to resolve the issues.

Keywords: Machine-to-Machine Communication Machine-Type Communication, Long-Term Evolution

1. 前言

第三代合作夥伴計畫(Third Generation Partnership Project, 3GPP)提出名為機器型態通訊(Machine-Type Communication, MTC) [1]之技術，作為下一代行動通訊網路長程演進(Long-Term Evolution, LTE)中，機器對機器通訊(Machine-to-Machine Communication, M2M Communication)之標準規格。

有別於傳統人對人(Human-to-Human, H2H)通訊模式，MTC 通訊具備幾項特徵，例如：較低的資料傳輸量、較低的移動性、極低的電耗量，及非經常性資料傳輸等。3GPP 制定 LTE 標準流程時，針對 MTC 特性所衍生之重要技術議題包含 MTC 裝置觸發(MTC Device Triggering)及壅塞控制(Congestion Control)等亦有探討[2, 3]。

由於 MTC 裝置的數量預計將比傳統 H2H 裝置大上許多，以現有提供 H2H 通訊所設計之標準，用在提供 MTC 通訊服務時，行動通訊網路架構的各個階層都可能面臨頗為嚴重的壅塞。例如，在無線電接取網路(Radio Access Network, RAN)的層面，若有大量的裝置同時嘗試要與基地台(eNB)連結，就會發生大量的隨機存取(Random Access, RA)碰撞，造成 Physical Random Access Channel (PRACH)壅塞及封包延遲等降低整體服務品質(Quality of Service, QoS)的情形。因此，行動網路標準技術[3]需要作一些強化，以因應這種新型態的通訊模式。

本論文將針對 MTC 通訊於 LTE 網路中所面臨的挑戰與可能的解決方案。本文各節安排如下：第二節將說明 3GPP MTC 系統架構；第三節說明 MTC 重要研究議題與挑戰；第四節說明 RA 壅塞控制可能解決方案；第五節介紹 MTC 的其他關鍵議題；最後是結論。

2. 3GPP 機器型態通訊系統架構

圖 1 為 3GPP 提出之 LTE 行動通訊網路 MTC 系統架構圖[2]。MTC 裝置透過 LTE-Uu 介面連接 3GPP LTE 網路。幾個重要的網路元件及介面說明如下：

- MTC Interworking Function (MTC-IWF): 可獨立作為一個網路元件或是存在於 HPLMN 的一個功能單元，透過 Tsp 介面接收外部應用服務之信令(例如：MTC 裝置觸發信令)。
- Service Capability Server (SCS):經由 MTC-IWF 連接行動通訊核心網路，與 MTC 裝置進行通訊。MTC 裝置可使用一個或多個應用服務，不同的應用服務則是透過外部 Application Server (AS)作控制與管理。
- Tsp reference point: SCS 與 MTC-IWF 間用來傳遞裝置觸發信令之介面。
- S6m reference point: MTC-IWF 與 HSS 間之介面，作為國際行動用戶識別碼(International Mobile Subscriber Identity, IMSI)與行動用戶識別碼(Mobile Subscriber Integrated Services Digital Network Number, MSISDN)或外部識別

碼對應之用。

- T4 reference point: MTC-IWF 透過本介面，以簡訊服務(Short Message Service)方式傳送觸發訊息至簡訊服務中心(SMS-SC)。

依照電信營運商的網路架構，3GPP 提出三種 MTC 應用服務連線模式，分別為間接連線模式(Indirect Mode)、直接連線模式(Direct Mode)及混合模式(Hybrid Mode)。AS 需透過 SCS 連接核心網路稱之為間接連線模式；倘若 AS 可直接連接核心網路則為直接連線模式；電信營運商也可同時提供直接與間接連線模式供外部 AS 連接核心網路，則稱之為混合模式。3GPP 亦定義幾項 MTC 通訊的特徵，描述如表 1。

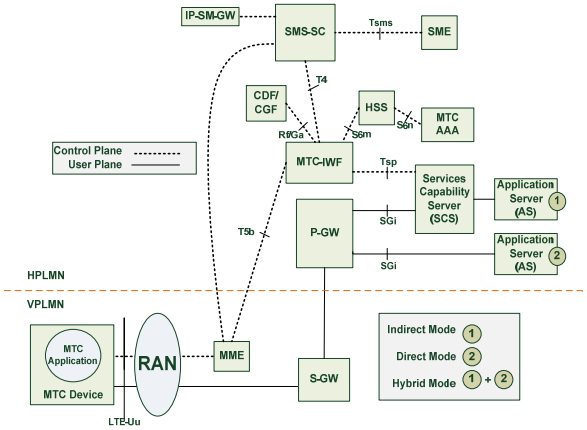


圖 1　3GPP MTC 系統架構

表 1　MTC 特徵

MTC 特徵	描述
Low mobility	MTC 裝置具備低移動性，或是在特定區域移動。
Time controlled	MTC 裝置在特定時間區間內進行資料傳輸。
Small data transmissions	少量的資料傳輸或接收。
Mobile originated only	由 MTC 裝置發起通訊呼叫。
Infrequent mobile terminated	非經常性由 MTC 裝置接收通訊呼叫，主要是由 MTC 裝置發起通訊呼叫。
MTC monitoring	監控 MTC 裝置之行為與事件。
Priority Alarm	發出告警之功能，例如：MTC 裝置遭竊或是遭破壞。
Group based MTC features	系統以群組化來達到最佳化掌握 MTC 裝置

3. 關鍵議題與挑戰

在 3GPP TR 23.887[3]中，特別提到幾項關鍵議題，本節說明兩項目前較主要關注的研究議題及其面臨的挑戰。

3.1 MTC 裝置觸發(MTC Device Trigger)

MTC 裝置具備非經常性的小資料傳輸，為節省 MTC 裝置電力消耗，AS 若有需要與 MTC 裝置通訊時，會發送觸發訊息，利用 MTC 裝置觸發的方式，啟動 AS 與 MTC 裝置間的通訊連線，用以執行特定的指令。

圖 2 為 3GPP 標準制定之 MTC 裝置觸發程序。SCS 會先向 Domain Name Server (DNS)詢問 MTC 裝置所對應服務之 MTC-IWF 在哪裡，然後再將觸發訊息發送至正確的 MTC-IWF。MTC-IWF 會向 HSS 取得用戶資訊，並依據用戶資訊，選擇適當的觸發方式。MTC-IWF 透過 T4 介面與 SMS-SC 介接，用以傳遞裝置觸發簡訊。除了利用簡訊觸發方式，MTC-IWF 也可透過 T5 介面連接 MME 來傳遞裝置觸發信令。當 MTC 裝置收到觸發訊息後，則會開始進行觸發訊息所要求執行之指令。

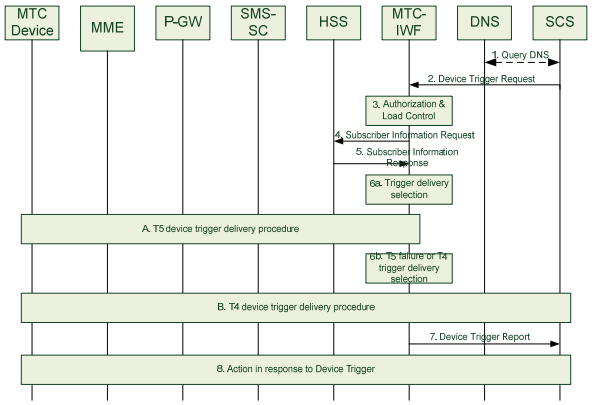


圖 2 MTC 裝置觸發程序

因應未來大量 MTC 裝置使用裝置觸發方式用來觸發裝置執行對應的應用服務，可能會造成網路的壅塞，3GPP 已將裝置觸發列為關鍵議題進行研究。在 3GPP TR 23.887[3]中提出幾項有關 MTC 裝置觸發關鍵議題，包含裝置觸發造成網路過載處理、T5 介面支援裝置觸發及如何將無效之裝置觸發信令召回等。

由於同一個觸發訊息可能會再同一時間傳遞給大量的 MTC 裝置，因此，如何有效率的發送大量的觸發訊息，並減少 MTC 裝置觸發後對於網路負載之影響將會是 MTC 裝置觸發關鍵議題中的一項研究挑戰。

3.2 基於隨機存取之 MTC 通訊(RA-Based MTC Communication)

MTC 裝置開機或接收到觸發訊息後，會嘗試透過無線電接取網路與 AS 連接。在 MTC 裝置建立 PS 連線之前，必須要先透過 RA 程序，取得無線電資源後方能進行 Packet Switch Domain(PS)連線程序。

圖 3 為 LTE 隨機存取程序 [4]。MTC 裝置首先由 64 個 preamble sequences 中隨機選一個，送出 Random Access Preamble 訊息，經由 PRACH 送至 eNB。當 eNB 正確收到 preamble 後，會回傳 Random Access Response (RAR) 訊息給 MTC 裝置。MTC 裝置收到 RAR 訊息後，透過 Physical Uplink Shared Channel (PUSCH)傳送 RRC Connection Request 訊息。當 MTC 裝置收到 RRC Connection Setup 訊息後，即完成隨機存取程序。

當有兩個以上的 MTC 裝置同一時間選擇相同的 preamble sequence 送給相同的 eNB 進行隨機存取程序，則會發生 preamble 碰撞。當此碰撞情形發生時，MTC 裝置則會隨機選一個 backoff 時間，並開始等待 back-off 時間結束後，再嘗試進行 RA 程序，直到成功完成 RA 程序或是 RA 重送次數到達上限後，RA 程序便宣告失敗。

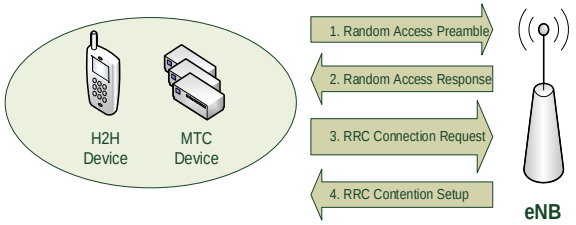


圖 3　LTE Random Access Procedure

MTC 裝置傳輸的資料量通常很小，然而在一個 eNB 涵蓋範圍下的 MTC 裝置數量可能很多，且其進行通訊連線的頻率也會大於一般 H2H 裝置。當大量的 MTC 裝置同時嘗試接取行動網路，將會造成 RA 成功機率降低，以及 PRACH 壅塞，使得封包傳輸延遲變長，甚至造成服務中斷。

若 MTC 裝置於 RA 程序發生碰撞後，重複發出接取需求，PRACH 將會面臨過載的問題。因此，如何有效控制 PRACH 過載，將會是基於隨機存取 MTC 通訊中最重要的研究挑戰。

4. 可能之解決方案

有許多文獻[5-10]主要都在探討 MTC 通訊對於行動通訊網路所造成的壅塞現象，以下分別說明目前文獻中提出解決 RAN 壅塞之可能解決方案。

4.1 限制存取層級機制(Access Class Barring, ACB)

ACB [5]的作法是由 eNB 廣播系統存取機率 p，及存取層級限制時間 τ。當 H2H 裝置開始進行 RA 程序前，會從 0 到 1 之間，隨機取一個數值 q，並與 p 比較。若 $q \le p$，則 H2H 裝置可以與 eNB 開始進行 RA 程序；若 $q > p$，則 H2H 裝置必須等待 τ 時間後方得再嘗試執行 RA 程序。在目前 3GPP LTE 標準中也開始討論，於 ACB 機制中提供多種存取層級(指定不同 p 與 τ)給 MTC 裝置，藉以降低大量 MTC 裝置同時執行 RA 程序時，對 PRACH 所造成的負載。

4.2 PRACH 資源分配 (PRACH resource separation)

將 PRACH 的 RA preamble 分別配置給 H2H 裝置及 MTC 裝置。在[10]中，作者提出兩種分配方式。第一種分配方式是將 RA preamble 分成兩個部分，分別專屬於 H2H 裝置及 MTC 裝置，彼此間的資源不會互相影響。另一種分配方式也是將 RA preamble 分成兩個部分，第一部分的 preamble 是給 H2H 裝置專用，另一部分是給 H2H 裝置及 MTC 裝置共享。藉以降低 MTC 裝置接取網路對原有 H2H 裝置的影響。

4.3 MTC 回退 (MTC Specific Backoff)

當 RA 過程中發生碰撞時，裝置會等待一個 backoff 時間後再重新嘗試執行 RA 程序[10]。在 H2H 通訊通常會設定一個較小的數值，然而在 MTC 裝置則會設定一個較大數值。目的在於希望利用延展 backoff 時間來緩解重新執行 RA 時對於 PRACH 造成的負載。

4.4 群組 MTC 裝置 (Grouping MTC Device)

MTC 裝置可依據應用型態與實際地理位置來建立群組，如圖 4 所示，並在群組中選擇一個 MTC 裝置作為 group head，用以代表其他全組成員與 eNB 通訊。在同一個群組之下的成員則利用 LTE 所提供的 peer-to-peer 通訊模式互動，由 group head 來接收群組成員的需求，並傳遞給 eNB。

近期有研究利用感知無線電(Cognitive Radio, CR)作為群組間相互通訊的方式。在[8]中作者分析，隨著群組增加可有效降低 MTC 裝置對於 eNB 的負載。但隨著群組增加，對於 eNB 之下的干擾影響會增加，使得封包傳輸速率降低。

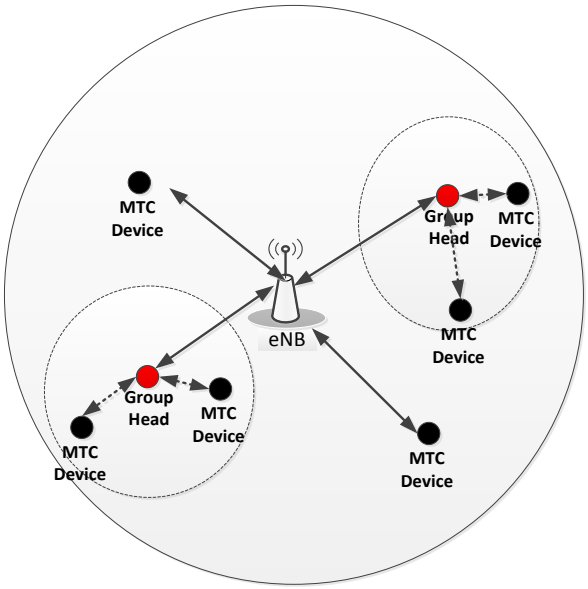


圖 4　MTC Grouping Architecture

4.5 詢問機制 (Pull-based)

當 AS 需要與 MTC 裝置建立通訊連線時，透過 eNB 對 MTC 裝置進行傳呼(Paging) [7]。當 MTC 裝置收到 paging 訊息之後，方得進行 RA 程序。以集中控制方式，由 eNB 依據 PRACH 的負載及可用之無線電資源，來決定是否要對 MTC 裝置進行 paging。本方案可能需要額外的控制通道資源來支援大量 MTC 裝置的 paging 訊息

5. 其他關鍵議題

在 3GPP TR 23.888[11]中也提及了其他關鍵議題，本節對這些關鍵議題進行簡單的介紹。

5.1 IP 地址 (IP Addressing)

在部分 MTC 應用中，MTC 伺服器需要主動嘗試與 MTC 裝置通訊。故 MTC 裝置需要一個通訊地址提供 MTC 伺服器聯絡

在 Rel-11 [11]中，MTC 使用者與 MTC 伺服器所使用的地址預計為 Internet Protocol version 6 (IPv6)地址。因為在 IPv6 地址中可用的前綴數量非常多，IPv6 地址空間的大小是幾乎沒有限制的，所以兩者可以處於相同的路由地址空間。

而在使用 IPv4 地址的情況下，由於 IPv4 公用網路的地址有限，加上未來 MTC 裝置數量的快速增加，可能無法配給所有 MTC 裝置一個專屬的 IP 地址，固給予 MTC 裝置的是 IPv4 專用網路的地址。而 MTC 伺服器則是使用與 MTC 裝置一樣的 IPv4 專用網路地址或是 IPv4 公用網路的地址。若是前者，則 MTC 裝置與 MTC 伺服器是位於同一路由地址空間，後者則否。

5.2 小量資料傳輸 (Small Data Transmission)

小量資料傳輸特徵是指 MTC 裝置只傳送或接收非常小量的資料，而小量的定義則需要各個系統更進一步的定義。線上的小量資料傳輸須滿足無論 MTC 裝置原是處於連線或是離線的狀態，都能在任何需要傳送資料的時刻進行傳送並且完成傳送。

5.3 低移動性 (Low Mobility)

部分 MTC 裝置擁有低移動性 (Low Mobility) 之特徵。在[11]中提出了擁有此特徵之 MTC 裝置使用場景，其中又可根據移動行為做初步區分，例如：小區域內不頻繁的移動行為、大範圍不頻繁的移動行為與幾乎沒有移動行為等。若實際舉例，前者可以是家用健康監測裝置，後者則為智慧型水電錶。

5.4 時間控制 (Time Controlled)

時間控制是透過訂定之可以傳送與接收資料的時間區間來控制 MTC 裝置對網路存取的行為。這些時間區間可由營運商事先訂定，或是事後以網路傳送通知的方式告知 MTC 裝置時間區間的相關資訊。此議題主要描述如何透過限制 MTC 裝置對網路的存取來避免不必要的網路負擔。

5.5 MTC 監控 (MTC Monitoring)

許多 MTC 裝置可能裝設在有安全風險區域，像是容易發生裝置被破壞、被竊盜之區域。當狀況發生時，網路需要能及時偵測並且回報狀況，以便採取對應的措施，例如限制該裝置對網路資源的存取。

5.6 信令壅塞控制 (Signaling Congestion Control)

MTC 相關信令的壅塞與過載是極需面對的問題。不只是提供 MTC 服務的電信營運商會受到影響，使用該服務的裝置所漫遊使用的網路之電信營運商也會受到 MTC 相關信令壅塞與過載的影響。一些情況容易造成信令壅塞與過載，例如：有事件觸發大量的 MTC 裝置同時進行連線行為、應用程式頻繁的進行時間同步行為等等。

為了解決信令壅塞的狀況，網路節點需能拒絕特定的連線要求。要能夠拒絕造成壅塞狀況的 MTC 應用資料傳輸，同時不影響其他 MTC 甚至是非 MTC 使用者的資料傳輸則是此議題的困難所在。專用的 Access Point Name (APN)或 MTC 群組識別雖然可以協助標明特定的 MTC 應用，要如何分辨出造成網路壅塞的 MTC 應用仍是一大挑戰。

6. 結論

本論文中，我們於 MTC 通訊的系統架構及關鍵議題與可能解決方案提出描述，相關關鍵議題在 3GPP 標準組織持續制定中。對於大量的 MTC 裝置執行 RA 程序，造成 eNB 無線電資源壅塞，是目前 MTC 研究的主要議題。文中所提的可能解決方案皆是目前 H2H 通訊已存在之解決無線電資源壅塞之作。這些解決方案也需要作適當修改，方能適用於 MTC 通訊的特性。

參考文獻

[1] 3GPP, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for Machine-Type Communications (MTC); Stage 1 (Release 12),” 3GPP, Tech. Spec. 3G TS 22.368, Dec. 2012.

[2] 3GPP, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements to facilitate communications with packet data networks and applications (Release 11),” 3GPP, Tech. Spec. 3G TS 23.682, Dec. 2012.

[3] 3GPP, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Machine-Type and other Mobile Data Applications Communications Enhancements (Release 12),” 3GPP, Tech. Spec. 3G TS 23.887, Feb. 2012.

[4] 3GPP, “3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 11),” 3GPP, Tech. Spec. 3G TS 36.300, March. 2013.

[5] Lien, S.-Y., Liau, T.-H., Kao, C.-Y., and Chen, K.-C., "Cooperative Access Class Barring for Machine-to-Machine Communications," IEEE Trans. on Wireless Comm., Vol. 11, No. 1, Jan 2012.

[6] P. Jain, P. Hedman, and H. Zisimopoulos, “Machine Type Communications in 3GPP Systems,” IEEE Comm. Magazine, Vol. 50, No. 11, pp.28-35, Nov. 2012.

[7] M. Hasan, E. Hossain, and D. Niyato, “Random access for machine-to-machine communication in LTE-advanced networks: issues and approaches,” IEEE Communication Magazine, Vol. 51, No. 6, pp.86-93, June 2013.

[8] Lee, H-K, Kim, D.-M. and Hwang, Y., Yu, S.-M. Yu and Kim, S.-L., “Feasibility of cognitive machine-to-machine communication using cellular bands,” IEEE Wireless Communications, Vol. 20, No. 2, pp.97-103, April 2013.

[9] T. Taleb and A. Ksentini, “On alleviating MTC overload in EPS,” Ad Hoc Networks (in press).

[10] Lien, S.-Y., Chen, K.-C., and Lin, Y., “Toward Ubiquitous Massive Accesses in 3GPP Machine-to-Machine Communications,” IEEE Communication Mag., vol. 49, no. 4, pp.66-74, Apr. 2011.

[11] 3GPP, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System improvements for Machine-Type Communications (MTC) (Release 11),” 3GPP, Tech. Rpt. 3G TR 23.888, Sept. 2012.

以 OpenStack 建立可擴充式物聯網系統雲端平台

蘇俊憲　　陳昌盛
國立交通大學 資訊技術服務中心
chsu@mail.nctu.edu.tw　cschen@mail.nctu.edu.tw

摘要

本論文旨在探討運用 OpenMTC 物聯網平台軟體結合 OpenStack 以建置可自動擴展雲端運算平台之相關課題。本論文以 OpenStack 為 IaaS 基礎架構，整合 fokus 公司的物聯網系統軟體 OpenMTC，利用 OpenStack API 指令，控制虛擬機的開關機以及 Load Balancer 成員的加入與刪除，達成自動擴展(auto scaling)物聯網服務的目的。由於在本研究進行期間，本實驗系統尚未有大量物聯網感測元件運作，因此本論文使用 Jmeter 測試軟體模擬多個連線同時存取所建置的物聯網系統，加以測試其效能。透過效能的模擬測試，可以得知當 NSCL(Network Service Capability Layer)的個數增加時，平均回應時間可以有效地下降，提升系統的效率，尤其是在同時有許多連線數的情況之下，更能夠顯著地提升效能，降低平均反應的時間。

關鍵詞：物聯網、OpenStack、OpenMTC、負載平衡、M2M、雲端運算。

Abstract

This paper aimed to explore the issues on developing an auto-scalable M2M service on the NCTU OpenStack private cloud (with OpenStack' load balancer module, LBasS, installed) by using the OpenMTC software platform. For performance evaluation, we adopted the Apache JMeter benchmark program for conducting the stress test. From the simulation results, we could find that the average response time could be greatly reduced as the number of NSCLs (Network Service Capability Layer) had been increased (i.e., changed from one to eight) gradually.

Keywords: JMeter, LBaSS, M2M, OpenMTC, OpenStack, Private cloud.

* 本論文由國科會計劃(編號 NSC NSC102-2218-E-009-002)提供部分補助，僅此致謝。

1. 物聯網簡介與研究動機

隨著網際網路與行動裝置的普及與發達，雲端運算與物聯網(Internet of Thing；IOT)結合的議題是未來研究的重要課題。2005 年，國際電信聯盟((International Telecommunication Union；ITU)發布了網際網路年度報告《ITU 網際網路報告 2005：物聯網》，報告中具體描述物聯網的概念，資訊與通訊技術的適用範圍已經從任何地點、任何時間連接任何人，演變成連接任何物品的階段，所有的物品透過網路相連，就形成了物聯網[1][2]。

物聯網擁有廣泛發展空間，尤其是在交通、環境、政府機構、全球安防、居家安全、環保節能、運輸和物流領域、健康醫療領域、智能環境（家庭、辦公、工廠）領域，物聯網中所有的感應裝置收集數據資料後，皆透過網路傳回數據中心，數據中心再提供資料掘取分析的平台給各個應用使用。每個人周圍的設備可以達到一千至五千個，所以物聯網可能要包含 500 萬億至一千萬億個物體[1]，因此隨之而來的挑戰為將會有成千上萬以上的裝置從各地不斷地回傳感測資料回資料中心，資料中心內部的物聯網系統將會承受大量的網路流量，大量的網路流量流入將會造成系統 CPU 使用率過高、連線數過高而導致系統失效。

基於以上所遇到的挑戰，本研究擬將物聯網系統導入雲端運算的概念，善用雲端運算具有彈性、可擴展的特性來建立物聯網的雲端服務。本論文以 OpenStack 建立 IaaS 與 PaaS 雲端運算私有雲平台，並使用德國 fokus 公司[3]所開發的 OpenMTC 物聯網系統軟體，將本研究之物聯網系統架設在 OpenStack 上，並額外加入負載平衡(Load Balancer)功能，結合系統的監控，整合成為一個自動擴展的物聯網雲端服務，藉此解決當系統負載過重時，需人工手動調整系統架構的缺點。

由於在本研究進行期間，本實驗系統尚未有大量物聯網感測元件運作，因此本論文使用 Jmeter 測試軟體模擬多個連線同時存取所建置的物聯網系統，加以測試。透過效能的模擬測試，可以得知當 NSCL 的個數增加時，平均回應時間可以有效地下降，提升系統的效率，尤其是在同時有許多連線數的情況之下，更能夠顯著地提升效能，降低平均反應的時間。

本篇論文後續的內容如下：第 2 節介紹物聯網、雲端運算與 OpenStack 的相關研究，第 3 節介紹 NCTU OpenStack 建置與 OpenMTC 與 OpenStack 之整合，第 4 節為系統建置成果與效能分析，第 5 節是結論與未來工作。

2. 相關研究

2.1 物聯網

圖 1 為歐洲電信化標準協會(European Telecommunications Standards Institute；ETSI)所定義的物聯網標準化架構，圖中文字 M2M 的解釋為 Machine to Machine(機器對機器)，亦即代表物聯網的意思。ETSI 把物聯網分成三個部份，物聯網的系統架構分別為圖 1 左邊的 Device Domain，中間部分稱之為 Network Domain；而左邊部分定義為 Application Domain。

- Device Domain：此 domain 又稱之為物聯網的感知層，感測器感測資料(例如溫濕度、位置、速度、RFID、條碼等資料)，透過有線網路或短距離低速的無線網路(例如 Zigbee/ RFID/ NFC/ Bluetooth/ WiFi)將所收集到的資料透過 Gateway 進行匯集，再經由 Network Domain 進行傳輸。
- Network Domain：此為物聯網的網路層，是 M2M 在通訊中傳輸資料的關鍵，在串連 Device Domain 與 Application Domain 中扮演重要的角色。在此 domain 所運用到的網路傳輸技術為有線網路(如 Ethernet/ Fiber/ Cable /xDSL 等)、無線網路(如 2G/ GPRS/ 3G/ HPSA/ LTE/ WiMAX 等)、衛星等技術。然而在 Network Domain 中，還有一個重要的部分，那就是 service capability，可視為 M2M 應用與網路的整合平台，儲存 Device Domain 所送進來的感測資料，並提供資料給 Application Domain 使用。
- Application Domain：Application Domain 則是代表著不同的 M2M 應用，例如智能交通、居家照護、物流監控、公共安全等等應用，皆是未來物聯網發展是否成功的重要關鍵。訊息收集、分析與管理技術在此層是一門重要的學問，因此最近火紅的巨量資料(Big Data)也是屬於物聯網的研究範圍之內。

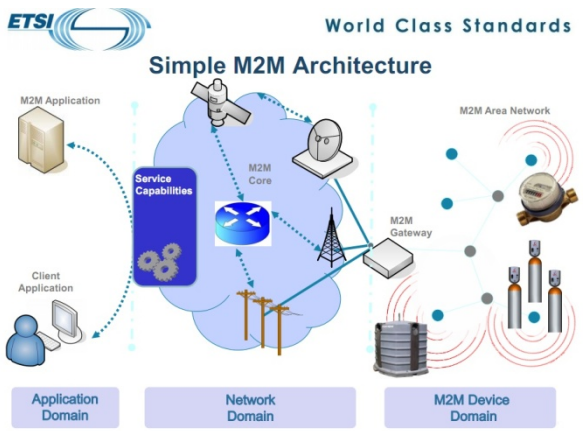


圖 1 ETSI Simple M2M Architecture

2.2 雲端運算

雲端運算是一種依需求，可從網路便利地存取使用設定好的共享運算資源池(例如 CPU、Memory、Storage、Network、Application、Services 等等)，以最少的管理負擔與減少與雲端服務供應商的頻繁互動，來達成快速配置和發佈。如表 1 所示，美國國家技術標準局（National Institute of Standards and Technology；NIST）定義雲端運算五個基礎特徵、三個服務模式及四種佈署模型[4]。

表 1 雲端運算之基礎特徵、服務模式及佈署模型

項目	內容
五大基礎特徵	(1). On-demand self-service (2). Broad network access (3). Resource pooling (4). Rapid elasticity (5). Measured Service
三個服務模式	(1). Software as a Service。 (2). Platform as a Service。 (3). Infrastructure as a Service。
四個佈署模型	(1). Private cloud (2). Community cloud (3). Public cloud (4). Hybrid cloud

本論文的雲端平台以 OpenStack 架設，屬於 Private Cloud 部屬模型，符合以上五大基礎特徵，下一節將會介紹 OpenStack 詳細的內容。

2.3 雲端作業系統 - OpenStack

OpenStack 為 2010 年 NASA 與 Rackspace 共同推出的系統，以 Python 語言撰寫，並使用 Apache 授權開放原始碼，讓所有人都可以利用這套系統自由的部署自己的私有雲與儲存環境[5]。OpenStack 內部包括了運算模組、網通模組和儲存模組，如圖 2 所示，再搭配一個可以集中管理上述三大類模組的儀表板模組，最後組合而成一套 OpenStack 共享服務，並且可以提供虛擬機器的方式，對外提供運算資源以便彈性擴充或調度。

應用程式的開發者，只要透過 API 的呼叫就可以和 OpenStack 溝通，例如用 API 來調整虛擬機器的數量、開機或關機等等，OpenStack 內部再負責運算資源的管理還有各元件內部溝通與協調。

目前 OpenStack 一共有 9 個不同的專案套件，9 個不同的專案套件分別提供虛擬化技術、網路、認證、儲存、管理介面、映象檔管理等功能，每個專案皆有專屬的專案名稱，分別說明如下[6]：

I. **Nova**：提供部署、排程與管理虛擬機之功能。
II. **Keystone**：提供不同種類的驗證方式，能查看哪位使用者可存取哪些服務。
III. **Neutron**：2013/6 由 Quantum 改名為 Neutron，管理的 OpenStack 的網路架構，支援多種網路

相關的 Plug-in。

IV. **Cinder**：負責管理區塊儲存容量，具有快照能力。

V. **Glance**：提供映象檔蒐尋、註冊以及服務交付等功能。

VI. **Horizon**：圖形化的網頁管理介面，讓雲端運算使用者管理雲端服務的所分配的資源。

VII. **Swift**：分散式儲存平臺，可存放非結構化的資料，類似於亞馬遜的 S3[7]服務。

VIII. **Heat(開發中)**：編制(Orchestration)的套件整合元件，提供雲端服務流程自動化引擎。

IX. **Ceilometer(開發中)**：計算雲端服務所使用的資料量，作為日後收費參考依據。

OpenStack 版本資訊如圖 3[8]所示，交通大學所使用的版本有 Essex 與 Grizzly，目前正在致力於再 OpenStack 開發新服務，例如本論文的物聯網服務，就是一項在 OpenStack 所使用的應用。未來新版本 Havana 釋出之後，我們將會更新 OpenStack 之版本。

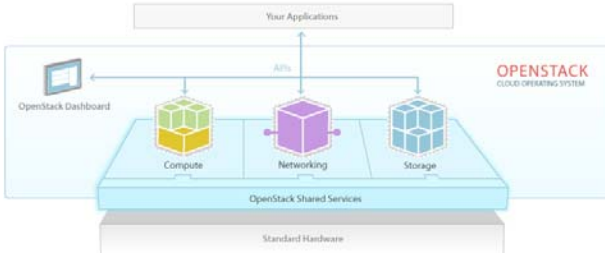


圖 2 OpenStack 模組示意圖

Series	Status	Releases	Date
Havana	Under development	Due	Oct 17, 2013
Grizzly	Current stable release, security-supported	2013.1	Apr 4, 2013
		2013.1.1	May 9, 2013
		2013.1.2	Jun 6, 2013
		2013.1.3	Aug 8, 2013
Folsom	Security-supported	2012.2	Sep 27, 2012
		2012.2.1	Nov 29, 2012
		2012.2.2	Dec 13, 2012
		2012.2.3	Jan 31, 2013
		2012.2.4	Apr 11, 2013
Essex	EOL	2012.1	Apr 5, 2012
		2012.1.1	Jun 22, 2012
		2012.1.2	Aug 10, 2012
		2012.1.3	Oct 12, 2012

圖 3 OpenStack 版本資訊

3. 系統架構說明

3.1 交通大學 OpenStack 系統架構

交通大學資訊技術服務中心於 2013 年 4 月建立新版的 OpenStack Grizzly，並於 Grizzly 上開發新的服務，例如 Hadoop 服務與物聯網雲端平台服務，後續將會持續開發其他之服務。

我們使用了多台伺服器來架設 OpenStack，分別為 1 台 Controller Node、4 台 Compute Node 與 1 台 Network Node，如圖 4 所示。另外儲存方面，使用了分散式檔案系統 Ceph 來負責 Object Storage(類似於亞馬遜 S3)服務，使用 iSCSI 儲存設備存放虛擬機器的檔案與區塊儲存(Cinder)的檔案。OpenStack 實體伺服器規格如表 2 所示，Compute Node 因為需要開啟虛擬機，因此需要規格較好的 CPU 與容量較大的記憶體空間，而 Controller Node 與 Network Node 相較於 Compute Node，所需要的記憶體比較少，CPU 規格也不需跟 Compute Node 一致。

交通大學資訊中心與資工系於 2012 年一起建立版本名稱為 Essex 的 OpenStack，接著於 2013 年 4 月建置了 Grizzly 版本之 OpenStack，提供一個 IaaS 架構的私有雲於交通大學中使用，目前主要使用於研究計畫、雲端運算課程、實驗室以及資訊中心同仁測試使用，提供老師與學生在 OpenStack 平台上開發雲端服務，而本論文就是在 OpenStack 上開發物聯網雲端服務，開發人員可以透過網頁介面登入 OpenStack，並管理被分配的 IaaS 資源，開發人員登入 OpenStack 之畫面如圖 5 所示。

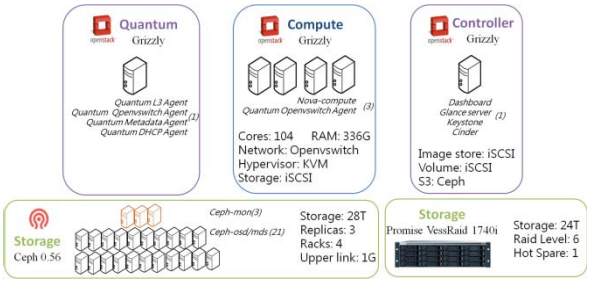


圖 4、NCTU Grizzly OpenStack 架構

表 2 OpenStack 伺服器規格

	CPU	Core	Memory
Controller	Intel X5130 2.00GHz	8	32GB
Compute-1	Intel E5-2620 2.00GHz	24	64GB
Compute-2	Intel E5-2620 2.00GHz	24	64GB
Compute-3	Intel E5-2620 2.00GHz	24	64GB
Compute-4	Intel E5-2620 2.00GHz	32	144GB
Network	Intel X5130 2.00GHz	8	8GB

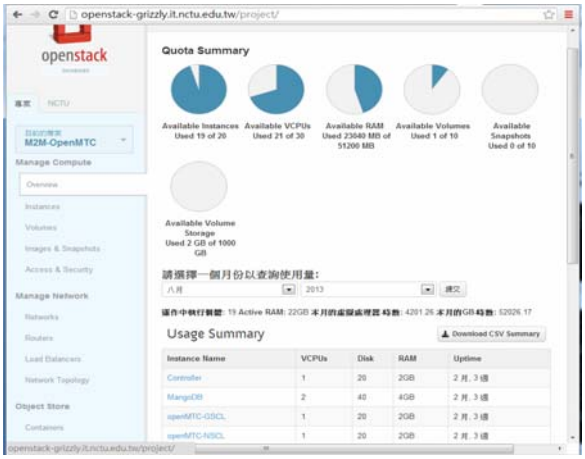


圖 5 OpenStack 登入畫面

3.2 OpenStack Load Balancer - LBaaS

OpenStack 提供了負載平衡器的插件，協助建立一個高可靠度的雲端服務，以避免因單一伺服器當機而停止服務或是流量過高超過單台伺服器的負荷，本論文使用此插件提供負載平衡的服務，此插件名稱稱之為：LBaaS(Load Balancer as a Service)。

LBaaS 安裝與設定之後，使用畫面如圖 6 所示，使用者可以透過 Dashboard 建立 Load Balancer 的 Pool、Member、Health Monitor 與 VIP。除了以 GUI 介面設定之外，我們還可以透過呼叫 API 的方式設定 Load Balancer 的服務，呼叫方式如圖 7 先建立一個名為 webpool 的 Load Balancer 服務。接著再透過 quantum lb-member-create 指令加入 2 台 web server 到 webpool 中，如圖 8。另外可以建立 health monitor 以監控後端的 web server 是否正常，建立的方式(quantum lb-healthmonitor-create)如圖 9，最後需再建立對外服務的 Virtual IP Address(VIP)，最後達成負載平衡的目的，如圖 10 所示。

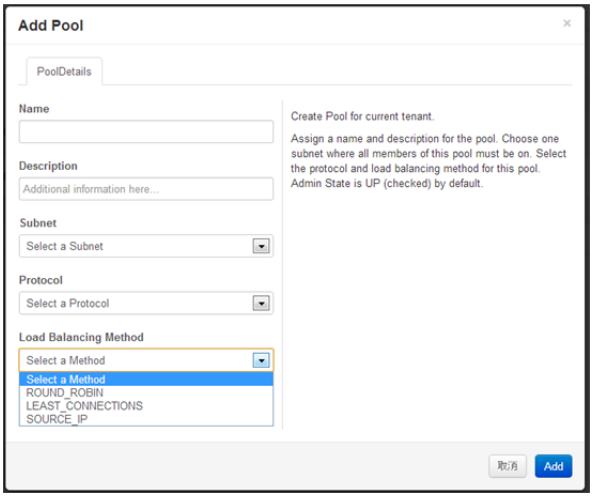


圖 6 LBaaS in OpenStack

```
chsu@OpenStack-Grizzly:~$ quantum lb-pool-create --lb-method ROUND_ROBIN --name webpool --protocol HTTP --subnet-id ea0750c7-8293-4755-9e29-e86cbeff41c5
Created a new pool:
+------------------+--------------------------------------+
| Field            | Value                                |
+------------------+--------------------------------------+
| admin_state_up   | True                                 |
| description      |                                      |
| health_monitors  |                                      |
| id               | fd659cf5-499b-4a25-8329-dcf1d061224f |
| lb_method        | ROUND_ROBIN                          |
| members          |                                      |
| name             | webpool                              |
| protocol         | HTTP                                 |
| status           | PENDING_CREATE                       |
| subnet_id        | ea0750c7-8293-4755-9e29-e86cbeff41c5 |
| tenant_id        | fa5dd1ac50664703af87853599db1544     |
| vip_id           |                                      |
+------------------+--------------------------------------+
```

圖 7 LBaaS API 建立 pool API

```
chsu@OpenStack-Grizzly:~$ quantum lb-member-create --address 172.16.1.14 --protocol-port 80 webpool
Created a new member:
+----------------+--------------------------------------+
| Field          | Value                                |
+----------------+--------------------------------------+
| address        | 172.16.1.14                          |
| admin_state_up | True                                 |
| id             | 94f52676-98ac-480a-be23-a4f4a849fd3d |
| pool_id        | fd659cf5-499b-4a25-8329-dcf1d061224f |
| protocol_port  | 80                                   |
| status         | PENDING_CREATE                       |
| tenant_id      | fa5dd1ac50664703af87853599db1544     |
| weight         | 1                                    |
+----------------+--------------------------------------+
chsu@OpenStack-Grizzly:~$ quantum lb-member-create --address 172.16.1.15 --protocol-port 80 webpool
Created a new member:
+----------------+--------------------------------------+
| Field          | Value                                |
+----------------+--------------------------------------+
| address        | 172.16.1.15                          |
| admin_state_up | True                                 |
| id             | 42b6c20f-46bc-4c64-92c9-36b671ce8ac9 |
| pool_id        | fd659cf5-499b-4a25-8329-dcf1d061224f |
| protocol_port  | 80                                   |
| status         | PENDING_CREATE                       |
| tenant_id      | fa5dd1ac50664703af87853599db1544     |
+----------------+--------------------------------------+
```

圖 8 LBaaS API 加入 member

```
chsu@OpenStack-Grizzly:~$ quantum lb-healthmonitor-create --delay 3 --type HTTP --max-retries 3 --timeout 3
Created a new health_monitor:
+----------------+--------------------------------------+
| Field          | Value                                |
+----------------+--------------------------------------+
| admin_state_up | True                                 |
| delay          | 3                                    |
| expected_codes | 200                                  |
| http_method    | GET                                  |
| id             | c74f5f64-a574-49ba-b0e6-60b3d8491fad |
| max_retries    | 3                                    |
| status         | PENDING_CREATE                       |
| tenant_id      | fa5dd1ac50664703af87853599db1544     |
| timeout        | 3                                    |
| type           | HTTP                                 |
| url_path       | /                                    |
+----------------+--------------------------------------+
```

圖 9 LBaaS API 建立 health monitor

```
chsu@OpenStack-Grizzly:~$ quantum lb-vip-create --name webvip --protocol-port 80 --protocol HTTP --subnet-id  ea0750c7-8293-4755-9e29-e86cbeff41c5 webpool
Created a new vip:
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| address             | 172.16.1.18                          |
| admin_state_up      | True                                 |
| connection_limit    | -1                                   |
| description         |                                      |
| id                  | 51851952-33fd-4321-8591-3968174cef98 |
| name                | webvip                               |
| pool_id             | fd659cf5-499b-4a25-8329-dcf1d061224f |
| port_id             | 7e61b503-2ed3-48ae-86c6-284a5fa53564 |
| protocol            | HTTP                                 |
| protocol_port       | 80                                   |
| status              | PENDING_CREATE                       |
| subnet_id           | ea0750c7-8293-4755-9e29-e86cbeff41c5 |
| tenant_id           | fa5dd1ac50664703af87853599db1544     |
+---------------------+--------------------------------------+
```

圖 10 LBaas API 建立 VIP

3.3 物聯網整合 OpenStack 雲端作業系統

本論文使用 fokus 公司所開發的 OpenMTC 物聯網平台軟體建置，此軟體所需的作業系統與安裝的軟體套件如表 3，OpenMTC 資料庫採用 MongoDB[9]，程式語言使用 node.js 撰寫，OpenMTC 的資料存取支援 RESTful APIs 提供以 GET 或 POST 交換資料。

表 3 OpenMTC software requirement

OS.	Ubuntu 12.04 64bit
Software	NodeJS 0.8.16
	MongoDB 2.0.4
	GNU make 3.81

4. 系統建置成果與分析

4.1 物聯網雲端平台平行擴展(Scale Out)

在物聯網中，遍佈於世界各地的感測裝置為了傳回資料，將會產生成千上萬甚至上億個連線，若只靠傳統的方式使用單一台伺服器接收回傳的資料，系統可能會因架構無法平行擴展，很快地遇到效能的瓶頸。然而雲端運算強調的是快速有彈性的平行擴展，因此本論文將 OpenMTC 建置在 OpenStack 上，並使用 OpenStack 的負載平衡 LBaaS，當連線數到達一定的門檻值後，搭配 OpenStack API 的呼叫，彈性地擴充或縮減後端服務的伺服器，建置一個可平行擴充的物聯網雲端平台。

圖 11 為本論文的物聯網雲端平台架構圖，在圖裡的 Device Domain 中，我們可以想像有成千上萬的 DA(Device Application)節點透過 GSCL 傳送回 Network Domain，本論文將 OpenMTC 架設在 OpenStack 的平台上，負載平衡器使用 OpenStack 提供的 LBaaS，如圖 12 所示，本論文建立了 2 個負載平衡器於 NSCL 上使用，分別為提供 Device Domain 回傳資料的 Load Balancer A 與提供給 Application Domain 使用的 Load Balancer B，而每

台 Load Balancer 後端有 2 台 NSCL 負責服務，如圖 13 所示。

在雲端平台平行擴展方面，當連線數超過一定的門檻值後，本論文使用 OpenStack Nova API 指令”nova boot --flavor=1 --image=NSCL_Orig NSCL-3”(如圖 14)呼叫開啟新的虛擬機，虛擬機內自動執行 OpenMTC 軟體的 NSCL 程式，再呼叫 OpenStack Quantum LBaaS API 指令” quantum lb-member-create --address 172.16.1.26 --protocol-port 15000 NSCL-mia-15000-LB”(如圖 15)將新的虛擬機加入到 Load Balancer 的 Pool 中(172.16.1.26 為虛擬機 NSCL-3 所取得的 IP 位址)，此時後端就有 3 台 NSCL 伺服器服務了。另一個情況是當連線數降低時，系統會以 API 指令自動將虛擬機關閉(使用 nova delete 指令)，並移除 Load Balancer 的 pool 中停止使用的 IP(使用 quantum lb-member-delete 指令)，平行擴展之演算法如下方文字方塊所描述。

```
max_VM_size =8
min_VM_size =2
current_VM = min_VM_size

while (check LBaaS incoming connection session every 1 second)
{
 if number of session > 30*current_VM and current_VM   <
max_VM_size
    {
          OpenStack API boot new VM
          OpenStack LbaaS API add VM as a member to openMTC Load
Balancer Pool
          current_VM++
    }
 else if number of session < 30*(current_VM - 1) and current_VM >
min_VM_size
    {
           OpenStack API terminate new VM
          OpenStack LbaaS API remove VM as a member to openMTC
Load Balancer Pool
          current_VM++
    }
 else
    exit
}
```

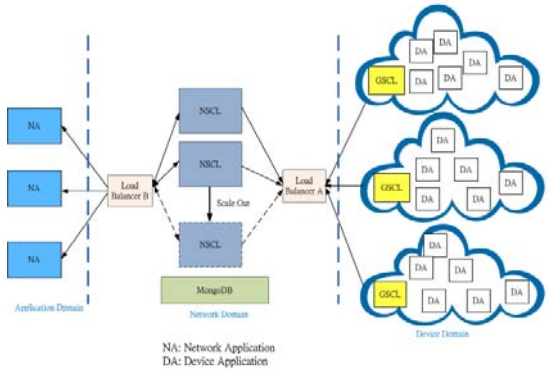


圖 11 物聯網雲端平台架構圖

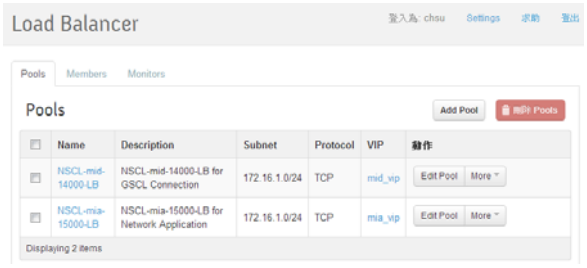


圖 12 物聯網 OpenMTC LBaaS

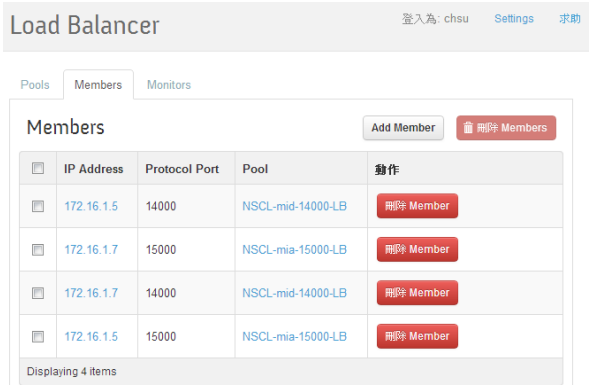


圖 13 LBaaS Member – NSCL

```
chsu@OpenStack-Grizzly:~$ nova boot --flavor=1 --image=NSCL_Orig NSCL-3
+-----------------------------+--------------------------------------+
| Property                    | Value                                |
+-----------------------------+--------------------------------------+
| status                      | BUILD                                |
| updated                     | 2013-08-22T13:41:06Z                 |
| OS-EXT-STS:task_state       | scheduling                           |
| key_name                    | None                                 |
| image                       | NSCL_Orig                            |
| hostId                      |                                      |
| OS-EXT-STS:vm_state         | building                             |
| flavor                      | m1.tiny                              |
| id                          | b2615ea7-9158-4f3b-8055-e62e657e8464 |
| security_groups             | [{u'name': u'default'}]              |
| user_id                     | b49b710a33fa429ba5fdbb7a5456279a     |
| name                        | NSCL-3                               |
| adminPass                   | ZyCBCYX4MdiH                         |
| tenant_id                   | fa5dd1ac50664703af87853599db1544     |
| created                     | 2013-08-22T13:41:06Z                 |
| OS-DCF:diskConfig           | MANUAL                               |
| metadata                    | {}                                   |
| accessIPv4                  |                                      |
| accessIPv6                  |                                      |
| progress                    | 0                                    |
| OS-EXT-STS:power_state      | 0                                    |
| OS-EXT-AZ:availability_zone | nova                                 |
| config_drive                |                                      |
```

圖 14 OpenStack Nova boot API

```
chsu@OpenStack-Grizzly:~$ quantum lb-member-create --address 172.16.1.26 --protocol-port 15000 NSCL-mia-15000-LB
Created a new member:
+----------------+--------------------------------------+
| Field          | Value                                |
+----------------+--------------------------------------+
| address        | 172.16.1.26                          |
| admin_state_up | True                                 |
| id             | c4293871-a470-4c08-addc-9c9e4aab26f7 |
| pool_id        | 11fcc873-1986-44f8-a37f-71b0ed5e896f |
| protocol_port  | 15000                                |
| status         | PENDING_CREATE                       |
| tenant_id      | fa5dd1ac50664703af87853599db1544     |
| weight         | 1                                    |
+----------------+--------------------------------------+
```

圖 15 OpenStack Quantum LBaaS API

4.2 效能測試模擬結果

因本實驗系統尚未有大量的物聯網感測元件回傳感測資料以及大量的應用(i.e., Network Application)，因此本論文採用 Jmeter 軟體執行壓力測試，Jmeter 參數設定如表 4 所示，本論文建立兩個測試項目，第一個項目是針對 OpenMTC 的埠 15000 進行 HTTP Request(Get)，同時送出 100 個 request，重複 100 次，總共取樣 10000 次。第二個改為同時送出 1000 個 request，重複 10 次，取樣總數一樣為 10000 次。我們將會比較此系統於 Load Balancer 後端不同的 NSCL 個數之平均回應時間與

每秒鐘可以處理要求的數量。

圖 16 為 NSCL 個數與系統平均回應時間之比較圖，當後端只有 1 台 NSCL 服務時，同時有 1000 個連線存取的平均回應時間遠大於同時指有 100 個連線的時間，當 Load Balancer 後端後端陸續增加了 NSCL 的個數之後，平均反映時間很快地將低了，代表著當連線數較多的時候，使用 Load Balancer 的效果越明顯。

圖 17 表示每秒鐘系統可以處理 request 的數量，每秒可處理的數量，會隨著後端的 NSCL 數量增加而變多。在同時有 8 個 NSCL 時，因為 8 個 NSCL 可以較快處理完成同時 100 個連線，因此執行緒 100 比執行緒 1000 有較高的吞吐量(每秒可處理數量)。

表 4 Jmeter 參數

Jmeter 參數				
測試 ID	**取樣數**	**執行緒數量**	**迴圈數**	**HTTP**
1	10000	100	100	GET
2	10000	1000	10	GET

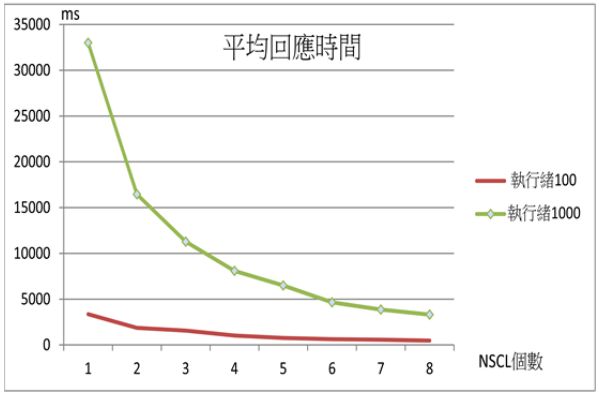


圖 16 平均回應時間

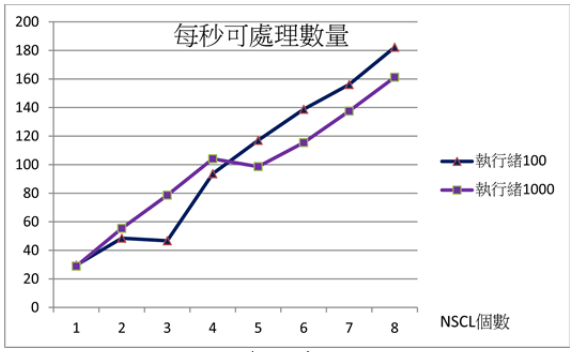


圖 17 每秒處理個數

5. 結論與未來工作

本論文以 OpenStack 為 IaaS 基礎架構，整合 fokus 公司的物聯網系統軟體 OpenMTC，利用 OpenStack API 指令，控制虛擬機的開關機以及 Load Balancer 成員的加入與刪除，達成自動擴展(auto scaling)物聯網服務的目的。此系統透過效能的模擬，可以得知當 NSCL 的個數增加時，平均回應時間可以有效地下降，提升系統的效率，尤其是在同時有許多連線數的情況之下，更能夠顯著地提升效能，降低平均反應的時間。

由於目前尚未有大量的感測節點於網路上運作，因此本論文使用 Jmeter 軟體以模擬的方式，模擬物聯網的運作，後續待校內系所開發許多應用之後，將可以預期有大量的資料量使用本系統，有可能會遇到不可預知的問題發生。未來我們模擬時，Jmeter 將使用不同之參數來模擬更多大量的連線需求，以利了解更多大量連線需求時，系統所可能遭遇到的問題。

OpenMTC 使用 Mongo 儲存感測端所送回的資料，當儲存的資料量變多時，MongoDB 效能可能會將低，因此 MongoDB 支援自動擴展之功能相形重要，未來將會開發 MongoDB as a Service 於 OpenStack 上。

參考文獻

[1] 維基百科-物聯網, http://zh.wikipedia.org/zh-tw/物聯網

[2] 電子時報 - 雲端運算加速物聯網市場發展, http://www.digitimes.com.tw/tw/iot/shwnws.asp?CnlID=15&id=0000280390_MQB4PCGM8HZOUK1TCINNU&ct=1

[3] Fraunhofer Fokus, http://www.fokus.fraunhofer.de/en/ngni/index.html

[4] The NIST Definition of Cloud Computing, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[5] OpenStack, "OpenStack Open Source Cloud Computing Software", http://www.openstack.org/

[6] OpenStack 是一套打造 IaaS 服務的開源軟體, http://www.ithome.com.tw/itadm/article.php?c=81091&s=2

[7] Amazon Simple Storage Service, http://aws.amazon.com/s3/

[8] OpenStack 版本 history

[9] mongoDB, http://www.mongodb.org/

[10] node.js, http://nodejs.org/

基於拼圖式合作學習融入國小閱讀理解與寫作成效之研究

章淑貞　林秋斌　潘炯凱　黃孟鈴　林根煌
國立新竹教育大學
數位學習科技研究所
{memily、chiupin.lin、panjiongkai、moring4560、comboday }@gmail.com

謝東諭
臺中市太平區
長億國民小學
tskeshbbg@gmail.com

摘要

本研究旨在發展出一套適合「高年級學生結合課程、課外閱讀的寫作教學方案」，並探討此方案對受試學生寫作時，在立意取材、結構組織、遣詞造句、錯別字、格式與標點符號等方面表現的影響，及以「拼圖式的合作學習」模式，利用平板電腦與互動學習軟體，對國小六年級學童閱讀理解與寫作成效；課程內容分為三個主題，主題配合康軒版六下國語教材單元，每個主題都包括課本教材、課外閱讀、寫作。本研究以台中市某國小六年級25名學生為例，方案實施前先對受試學生進行前測，結束後進行後測，比較前後測成績作為研究結果依據。本研究發現採拼圖式合作學模式，讓學生更能理解閱讀的內容，提升寫作的成效，幫助同儕之間的合作與溝通。

關鍵詞：閱讀理解、拼圖式合作學習、一對一

1. 前言

閱讀是學習最基礎的能力，人類從「學習閱讀的能力」(learn to read)，到「透過閱讀學習知識」(read to learn)，這樣的能力決定他是否具備了「學會如何學習的能力(learn to learn)」的能力，閱讀能力也是所有學習能力的基礎，在學好英文、數學、科學之前，最重要的就是「學會閱讀」[1]。然而，在目前國民小學教育現場，學生閱讀理解能力低落，因此很多學生害怕寫作，教學上，教師受限於語文科教學時數的縮減、教學內容的增加、學生程度的落差，因此，如何讓學生在小學階段就培養閱讀習慣，並能從文本內容推論出作者的寫作動機，以訓練其理解及寫作能力就變得很重要。

為提升教育品質及學生的學習能力，教育部提出「活化教學～分組合作學習的理念與實踐方案計畫」[2]，實施分組合作學習，以落實與推展分組合作學習的理念及活化國中之教學。十二年國教重視的是讓每個學生都可以適性發展，在常態編班的情況之下，合作學習是最有效的教學策略，不但可以提升學習成就、增進學習動機，更可以發展合作及溝通的技巧。本研究配合語文領域教學單元主題，導入與主題相關之課外讀物，以拼圖式合作學習進行閱讀，再以課程及閱讀的內容為題材，進行主題寫作。藉由拼圖式合作學習理論設計出來的閱讀學習活動，促使小組成員間頻繁的相互討論，激發學生高層次的思考，並有效提升閱讀理解與寫作之能力，增進學生之學習興趣與合作學習之效益。因此本研究的目的有三：

1. 探討電腦輔助拼圖式合作學習下，對學生閱讀理解能力之學習成效。
2. 探討電腦輔助拼圖式合作學習下，對學生寫作能力之學習成效。
3. 探討電腦輔助拼圖式合作學習下，學生之學習興趣與合作學習之效益

2. 文獻探討

2.1 閱讀理解

閱讀理解是一種複雜、包含多種能力交互作用而成的心智運作過程，從不同的角度切入有許多不同的看法[3]。例如從心理語言學的角度，認為閱讀理解建立於交互作用本質（interactive nature）及理解建構本質（constructive nature）上，建立已知到未知之間的橋樑，是極為主動的過程。任何影響一般思考或問題解決的能力亦會影響閱讀理解的內容 [4]。

又或者從傳統的角度來看，陳淑娟(1997)認為閱讀是一個複雜、動態的過程，讀者一方面從閱讀物件中獲取意義，另一方面把本身所既有之的意義帶入讀物中，所以閱讀理解可視為讀者從書面材料中提取意義的過程[5]。

不同的閱讀者所具備的閱讀技巧不同，因此就會產生不同層次的閱讀理解程度，擁有愈佳的閱讀技能，對文本的理解的程度也就會愈高。而閱讀理解則可依不同程度分為以下四種[6]：

1. 字義理解（ Literal Comprehension）指閱讀者從字句的語意就能瞭解文章中所陳述的主題及思想。
2. 推論理解（Inferential Comprehension）指閱讀者能根據文章所描述的訊息，再以本身的經驗去推論其隱含的意義。
3. 評鑑理解（Evaluative Comprehension）指閱讀者依據文章所傳達的訊息而產生了自己 的觀點。
4. 批評理解（Critical Comprehension）指閱讀者能分析文章的格式與內容。

2.2 拼圖式學習法

拼圖式學習法是由Elliot Aronson和他的學生於

1971年在德克撒斯大學及加州大學所開發出的一種合作學習的方法。(Elliot Aronson, 2000-2013)最初的開發目的是為了解決學生間種族不平等概念所產生的爭執、衝突以及學習環境等問題[7]。

其實施方法是先將全班學生進行分組，組內每一位同學分別負責一小題題目，負責相同小題的各組代表先成立「專家小組」並共同研讀此題題目，待完全理解之後回到原小組之中，向組內組員報告自己本身所負責的題目內容，組員可以在此時提出問題，以澄清學習概念。老師在學生討論的期間，巡視各組發展的狀況，當小組有疑問時可以適時地介入，並且於評量之前加入教師回饋階段，解答學生所提出之疑難問題，最後再給予每一位學生評量，檢視學習的成果[8]。

2.3 一對一數位學習

「一對一數位學習」，指的就是一位學生可以使用至少一台以上的數位學習輔助工具來從事學習[9]。國外學者 Penuel(2006)將「一對一數位學習」概念分別歸納出四大研究領域，(1) 用科技增進學生的學習成效。(2) 解決數位資源取得的不平等問題。(3) 為了讓學生熟悉在未來科技環境下工作。(4) U-Learning 環境對於教學產生的質變[10]。對於非正式學習的學習輔助工具應具有下列特性：(1) 可攜帶性 (2) 支援社會互動 (3) 個人化 (4) 情境感知 (context sensitivity) (5) 連結性 (6) 整合虛擬與真實世界 (Chan, Roschelle,His, & Kinshuk, 2006)。數位學習輔具的無線行動運算能力，可以讓學習輔助工具互傳資料，或存取網際網路上的數位資源。也因此在一對一數位學習的教室中，學生的學習模式、互動關係，都將變得更加多元[9]。

3. 研究方法

3.1 研究對象

研究對象為臺中市某國小六年級 25 位學生(男生 14 位，女生 11 位) 及該班導師。

3.2 相關設備：

本實驗計畫提供每位學生及教師一台平板電腦 (ASUS_TF101_wifi 版)，採用 Android 系統，教學場域則有單槍投影機、無線基地台、無線網路行為記錄及認證伺服器各一台。

3.3 研究工具：

1. 平板電腦 (Android 作業系統)
2. 電子書閱讀軟體
3. 平板電腦內建筆記軟體

3.4 結合教學模式：

1. 結合平板電腦以拼圖式合作學習方式進行閱讀及寫作
2. 結合本學期語文領域教學單元主題
3. 透過即時反饋系統(Interactive Response System，IRS)，進行線上閱讀測驗
4. 以小組共讀分享閱讀心得

3.5 研究設計：

結合本學期語文領域教學單元主題，進行主題式教學，循環三次。前、後測以同一篇題目進行寫作。

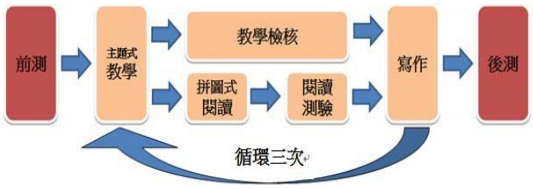


圖 1.融合閱讀、寫作之主題式教學模式

3.6 從閱讀理解進入寫作的具體模式：

配合語文領域教學單元主題，導入與主題相關之課外讀物，以拼圖式合作學習進行閱讀，再以課程及閱讀的內容為題材，進行主題寫作。

表 1.從閱讀進入寫作的具體模式表

期程	具體模式	週次
主題教學	1. 確認教學文體	第一週—第三週
	2. 內容深究教學：問題探究、主題思考。	
	3. 形式深究教學：句型、修辭、文章佈局、寫作技巧。	
	4. 運用 IRS 檢核主題教學目標	
主題閱讀	1. 依據教學主題、內容及形式深究進行閱讀	第一週—第三週
	2. 以拼圖式合作學習方式進行閱讀	
	3. 運用平板電腦及心智圖進行閱讀寫作(如下圖 2.)	
	4. 運用 IRS 檢核主題閱讀目標 (閱讀測驗，如下圖 3.)	
主題寫作	1. 小組利用心智圖討論並分享	第四週
	2. 完成寫作	
	3. 分享寫作內容	

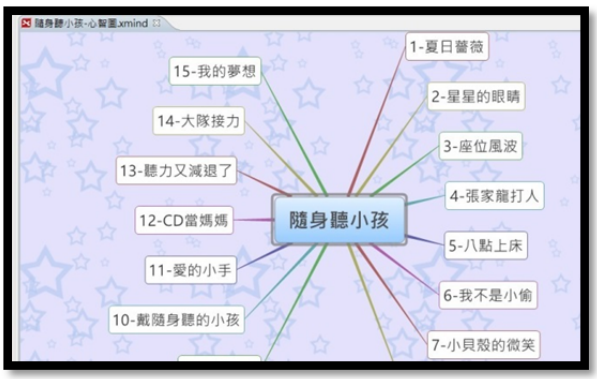


圖 2.利用心智圖討論閱讀寫作

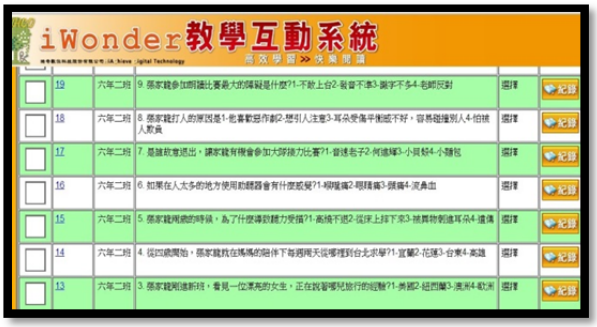


圖 3. IRS 進行閱讀測驗

3.7 研究實驗流程：

1. 前測（作文，開學第一週）
   - ◆ 測驗學生起始能力
2. 拼圖式合作學習方式閱讀模式導入（共三輪，102.02~102.06）
   - ◆ 每月共讀 2 本，給予成就感並協助參與。
   - ◆ 學校給於固定閱讀時間。
   - ◆ 運用 IRS 進行閱讀測驗，以檢核學生閱讀成效。
   - ◆ 同時要求課後閱讀，並與家長溝通，期能規劃學生課後閱讀時間，養成課後閱讀習慣
   - ◆ 鼓勵學生增加課外閱讀數量並登錄，透過班級經營方式加強（正增強）。
3. 後測（作文，畢業前完成）
   1. 測驗學生以此模式完成閱讀及寫作的學習成效差異

3.8 閱讀及寫作方式：

1. 閱讀：在校培養閱讀概念及導入方式，閱讀以課後及課餘時間進行。
2. 寫作：以電子作文為主，前後測及寫作練習均以平板電腦打字進行。文體以說明文為主。(如下圖 4)。

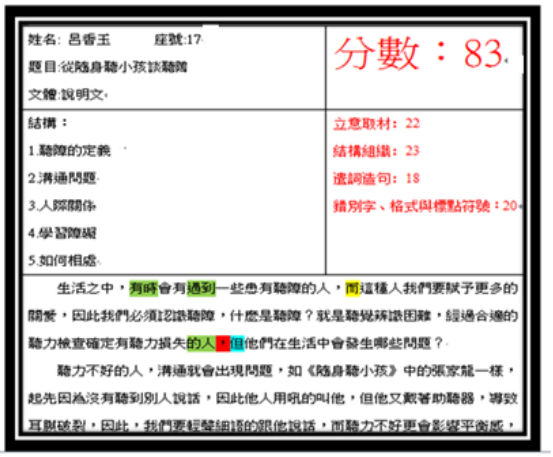


圖 4.電子作文

3.9 導入書單：

實體書為主、電子書為輔，每月共讀 2 本。

表 2. 導入書單

實驗期程	教學主題	實體書書單	電子書書單
102.02~102.03	人間角落	隨身聽小孩	假如給我三天光明
102.03~102.04	海天遊蹤	鐘樓怪人	小公主
102.04~102.05	童年故事	少年噶瑪蘭	苦兒流浪記

3.10 從閱讀進入寫作單一主題流程：

1. 一個主題教學為期四週，教學內容包含國語課本教材四課，閱讀兩本課外讀物，主題寫作一篇。
2. 拼圖式閱讀：
   ①將共讀書內容分作五等分，小組成員每人一等分。
   ②原屬小組各組相同範圍的成員聚集共同討論及分享。補充及整理所負責的閱讀部分，以便回原屬小組分享。
   ③將過專家小組的精進討論，各自回原屬小組，透過分享與報告的形式完成完整的閱讀與精讀。(如圖 5)

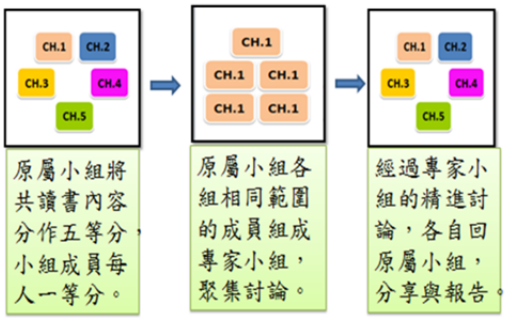


圖 5.拼圖式閱讀討論模式

表 3. 從閱讀進入寫作－單一主題教學流程表

第一週	1.閱讀開始
	2.專家小組內容分配
第二週	1.專家閱讀報告開始製作
	2.完成閱讀
第三週	1.專家閱讀報告製作完成
	2.線上閱讀測驗
	3.專家小組分享
	4.原屬小組分享
第四週	1.原屬小組統整
	2.班網公布作品
	3.進行主題寫作

4. 研究結果與討論

4.1 學生問卷調查結果：

背景資料統計，有效問卷 25 份（男生 14 人、女生 11 人）

表 4.平板電腦課後用途

選項	人數	比例
從沒帶回家過	0	0.0%
閱讀電子書	15	57.7%
評量測驗	5	19.2%
資料查詢	21	80.8%
線上聊天	13	50.0%
線上遊戲	6	23.1%
個人娛樂	6	23.1%
其他：寫功課	3	11.5%

從以上數據顯示，學生把平板電腦帶回家的課後用途，主要在資料查詢，其次是閱讀電子書。

表 5.利用平板電腦閱讀的時間

選項	人數	比例
幾乎沒有	0	0.0%
課堂教學	13	52.0%
下課時間(含早、午休)	17	68.0%
回家使用	16	64.0%
其他	0	0.0%

從以上數據顯示，學生利用平板電腦閱讀的時間大部分是在校的早、午休時間，其次是回家使用。

表 6.課後使用平板電腦閱讀次數

選項	人數	比例
幾乎沒有	2	7.7%
1~2 次	4	15.4%
3~5 次	12	46.2%
5~10 次	5	19.2%
10 次以上	3	11.5%

從以上數據顯示，學生課後使用平板電腦閱讀的次數以 3~5 次居多。

4.2 前後測成對樣本 T 檢定

依據六上國語學期成績，將學生分成低、中、高三組，學期成績 68 分以下的為低分組，共有 6 人；學期成績 68 分以上 82 分以下的為中分組，共有 10 人；學期成績 82 分以上的為高分組，共有 9 人，全班共 25 人。

表 7.全班、低、中、高分組前後測成對樣本 T 檢定

(全班)	標準差	t 值	顯著性
前測成績	12.884	-4.189	.000***
後測成績	8.114		
(低分組)	標準差	t 值	顯著性
前測成績	8.64292	-2.527	.053
後測成績	6.92820		
(中分組)	標準差	t 值	顯著性
前測成績	10.17022	-3.042	.014*
後測成績	5.56177		
(高分組)	標準差	t 值	顯著性
前測成績	11.91055	-1.605	.147
後測成績	7.1589		

*P<.05，**p<.01，***p<.001

由表 7.可知，全班及中分組的前後測作文成績均達顯著性，顯示透過電腦輔助拼圖式合作學習有助於全班學生寫作成效的提升。

表 8.全班、低、中、高分組前後測平均數與進步度

項目 (全班)	最小值	最大值	平均數	進步度
前測成績	40	95	66.6	7.84
後測成績	60	90	74.44	
項目 (低分組)	最小值	最大值	平均數	進步度
前測成績	40	65	55.5	11.5
後測成績	60	80	67	
項目 (中分組)	最小值	最大值	平均數	進步度
前測成績	52	82	64.9	8.7
後測成績	65	82	73.6	
項目 (高分組)	最小值	最大值	平均數	進步度
前測成績	52	95	75.89	4.44
後測成績	70	90	80.33	

由表 8.可知，無論是全班或是低、中、高三組學生，寫作的成效均有提升，以低分組的進步最多。而針對課程主題，進行電子書及紙本課外讀物主題式的閱讀，除了讓學生從中獲取更多的寫作題材，進而降低主題寫作的困難度之外，亦期望協助學生建立平時閱讀習慣。

4.3 依據《國民中學學生基本學力測驗寫作測驗評分規準》四大評分項目進行前後測成

對樣本 T 檢定：

作文分數以國民中學學生基本學力測驗寫作測驗評分規準來評分，嚴謹的評分機制和一致的評分標準，得以區分學生的寫作能力[11]。

四大評分項目為：①立意取材②結構組織③遣詞造句④錯別字、格式與標點符號。

表 9.全班四大評分項目前後測成對樣本 T 檢定

評分項目	標準差	t 值	顯著性
立意取材	4.06735	-2.803	.010*
結構組織	3.72245	-5.050	.000***
遣詞造句	3.31311	-3.501	.002**
錯別字、格式與標點符號	3.29292	.790	.438

*P<.05，**p<.01，***p<.001

由表 9.可知，電腦輔助拼圖式合作學習對全班的寫作，在「立意取材」、「結構組織」、「遣詞造句」等評分項目均達顯著性，其中以「結構組織」前後測的差異最大。

分析第四項「錯別字、格式與標點符號」前後測的分數幾乎沒有差異的原因，在於學生用平板電腦打字寫作並非手寫，因此降低寫字的錯誤率。

表 10.低分組四大評分項目前後測成對樣本 T 檢定

評分項目	標準差	t 值	顯著性
立意取材	4.58984	-1.245	.268
結構組織	3.20416	-4.332	.007**
遣詞造句	2.88097	-2.976	.031*
錯別字、格式與標點符號	5.62139	.000	1.000

*P<.05，**p<.01，***p<.001

由表 10.可知，電腦輔助拼圖式合作學習對低分組的寫作，在「組織結構」、「遣詞造句」方面有顯著性。

表 11.中分組四大評分項目前後測成對樣本 T 檢定

評分項目	標準差	t 值	顯著性
立意取材	3.99444	-2.533	.032*
結構組織	4.47338	-2.616	.028*
遣詞造句	2.70801	-3.503	.007**
錯別字、格式與標點符號	2.57331	1.475	.174

*P<.05，**p<.01，***p<.001

由表 11 可知，電腦輔助拼圖式合作學習對中分組學生的寫作在「立意取材」、「結構組織」、「遣詞造句」等三項在前後測均有顯著性。

表 12.高分組四大評分項目前後測成對樣本 T 檢定

評分項目	標準差	t 值	顯著性
立意取材	4.02423	-.911	.389
結構組織	2.87711	-2.665	.029*
遣詞造句	3.89801	-.599	.566
錯別字、格式與標點符號	2.08833	.160	.877

*P<.05，**p<.01，***p<.001

由表 12 可知，電腦輔助拼圖式合作學習對高分組學生的寫作，在「結構組織」方面有顯著性。綜上來說，全班的寫作能力除了有顯著提升之外，再依據四大評分項目比較，高、中、低分組學生在部分項目之中亦有不同的顯著進步，顯見教學實驗對於低、中、高分組學生寫作能力的提升皆有所不同程度的助益。

4.4 形成性評量

根據 100 年 4 月修正國民中小學九年一貫課程綱要語文學習領域—國語文及重大議題。[3]

相關的能力指標如下:

5-1-7-2 能理解在閱讀過程中所觀察到的訊息。

5-3-5 能運用不同的閱讀策略，增進閱讀的能力。

6-2-4-3 能練習利用不同的途徑和方式，蒐集各類可供寫作的材料，並練習選擇材料，進行寫作。

6-2-7-4 能配合閱讀教學，練習撰寫心得、摘要等。

6-4-4-1 能確立主旨，擬定大綱，並完成寫作。

表 13. 全班閱讀測驗與課後作文成績平均

全班平均	分數 1	分數 2	分數 3
閱讀測驗	88.4	85.2	83.6
作　　文	71.12	72.84	75

由表 13 可知，閱讀測驗成績都在 80 分以上，作文成績都有進步，拼圖式合作學習能增進閱讀及寫作的能力。

表 14.低、中、高分組閱讀測驗與作文成績統計

測驗別	高分組	中分組	低分組
	平均	平均	平均
閱讀測驗 1	95.6	85	83.3
閱讀測驗 2	89	86	78
閱讀測驗 3	90	83	75
作文別	高分組	中分組	低分組
	平均	平均	平均
作文 1	78.78	72.4	60
作文 2	76.22	76	62.5
作文 3	82.11	75.6	63.3

由表14可知，拼圖式合作學習有助於低、中、高各組學生閱讀理解及寫作能力的提升。

透過表 13、14 可知，透過閱讀策略能增進閱讀能力，能理解在閱讀中所觀察到的訊息，提升閱讀理解能力；利用電子書及紙本課外讀物，蒐集寫作材料，提升寫作能力。閱讀測驗結果三組分數大部分都在 80 分以上，而作文分數三組都有進步，顯示閱讀能力與寫作能力之提升。

4.5 使用現況調查

為瞭解學生在此實驗教學中的學習狀況，分做合作學習、學習應用成效及學習感受等三大主題進

行問卷調查，每大主題各五小題，問卷結果如下：

表 15 使用現況調查統計表-合作學習

主題	面向和內容	平均值	主題平均
合作學習	1.透過專家小組學習方式，讓我可以更深入了解閱讀內容。	4.76	4.50
	2.在專家小組中我會自由的表達自己的意見及想法。	4.40	
	3.透過原屬小組的學習方式讓我可以更快的完成整本閱讀。	4.48	
	4.與同學分享溝通的過程中，所得到的訊息能幫助我閱讀。	4.48	
	5.在小組分享過程中，我會專心聽取同學的內容。	4.40	

由表 15 可知，使用平板電腦進行拼圖式合作學習效果顯著，透過專家小組及原屬小組的討論與分享，學生能更快、更深入的了解閱讀內容。

表 16 使用現況調查統計表-學習應用成效

主題	面向和內容	平均值	主題平均
學習應用成效	6.透過這種小組討論學習方式，讓我增加了閱讀速度。	4.00	4.19
	7.透過這種小組討論學習方式，讓我養成每日閱讀的習慣。	3.88	
	8.透過這種小組討論學習方式，讓我提升寫作的能力。	4.16	
	9.我覺得使用平板電腦進行討論，可以更快理解閱讀內容。	4.76	
	10.我認為使用平板電腦閱讀，對我的寫作能力有幫助。	4.16	

由表 16 可知，在電腦輔助拼圖式合作學習下，可提升學生閱讀的理解能力，對寫作能力也有明顯的幫助。

表 17 使用現況調查統計表-學習感受

主題	面向和內容	平均值	主題平均
學習感受	11.我覺得使用平板電腦，可以很快和同學分享閱讀心得與感想。	4.32	4.43
	12.我覺得使用平板電腦，可以幫助我和同學合作與溝通。	4.32	
	13.我覺得使老師使用平板電腦的閱讀理解教學，讓閱讀更有趣。	4.48	
	14.我希望有更多的電子書可以閱讀。	4.24	
	15.我覺得使用平板電腦，能提升我學習軟體操作的能力。	4.80	

表 17 可知，教師透過平板電腦的閱讀教學，讓學生覺得閱讀更有趣，同時提升學生學習軟體操作的能力。

5. 結論與建議

5.1 結論

經過一個學期的實驗，結合國語課程的主題，進行閱讀與寫作，建立了主題式教學模式，此教學模式豐富了學生的寫作內容，即使是最害怕的說明文，也能言之有物。利用平板電腦進行拼圖式的合作學習，讓學生比以往快速的閱讀並理解閱讀的內容，有效的提升學生閱讀的興趣及習慣的養成。就教師而言，配合國語課程訓練閱讀及寫作，不會增加太多備課及教學負擔，是一種有效益的教學策略，希望藉此教學模式，提供有興趣提升學生閱讀力及寫作力的老師，作為教學參考。透過這種教學模式，我們發現：

一、 電腦輔助拼圖式合作學習，可以提升學生的閱讀理解能力及閱讀的興趣。

二、 電腦輔助拼圖式合作學習，可以提升學生寫作的成效。

三、 電腦輔助拼圖式合作學習，可以增進學生溝通的能力，促進同儕之間的合作。

四、 電腦輔助拼圖式合作學習，讓學生樂於學習。

5.2 建議

一、 學生的閱讀習慣養成不易，除了要提供學生在學校固定的閱讀時間外，課後閱讀也很重要，因此需要與家長溝通，請家長協助督促學生在家也要有固定時間閱讀的習慣。

二、 作文宜採取紙本寫作，學生用平板電腦打字寫作，因非手寫而降低了寫字的錯誤率，導致無法辨識學生識字、寫字的能力。

三、 以拼圖式合作學習方式進行閱讀討論時，須注意小組之間座位的安排，組與組之間的距離要拉開，避免各組在討論的聲音互相干擾。

參考文獻

[1] 柯華葳 (2006). 教出閱讀力，天下雜誌。

[2] 教育部(2013)「活化教學～分組合作學習的理念與實踐方案計畫」取自 http://www.coop.ntue.edu.tw/index.php，檢索日期：2013.07.10

[3] 黃雅玲（2010）。國小六年級學童融入式自我發問策略教學研究。國立屏東教育大學教育心理與輔導學系碩士論文。

[4] 張郁婕（2010）。國小國語文教學指引內容深究之問題探討──以低年級為例。國立臺中教育大學語文教育學系碩士論文。

[5] 陳淑娟（1997）。「指導－合作學習」策略應用於國小閱讀教學之理論探討。台中師院學報，11，65-112。

[6] 邢淇淇（2009）。行進情境模擬下手機動態文本閱讀之研究。銘傳大學設計管理研究所碩士論文。

[7] Elliot Aronson (2000-2013)。取自: http://www.jigsaw.org/

[8] 簡妙娟（2000）。高中公民科合作學習教學實驗之研究。國立高雄師範大學碩士論文。

[9] 童志榮（2008）。運用一對一數位學習於小組合作概念構圖之研究--以國小六年級社會科單元為例。國立新竹教育大學數位學習科技研究所碩士論文。

[10] 姜善迪（2009）。一人一機合作學習環境的學習效益探討。國立臺灣師範大學資訊教育研究所 碩士論文。

[11] 寫作測驗評分規準修訂說明(99.08)。取自 http://www.bctest.ntnu.edu.tw/(2013.07.10)

[12] 中華民國 100 年 4 月 26 日修正國民中小學九年一貫課程綱要語文學習領域—國語文及重大議題。(2011)取自 http://140.111.34.54/EJE/content.aspx?site_content_sn=15326，檢索日期：2013.07.10

Moodle 融入國小高年級藝術與人文教學之研究-以戲偶天地為例

張維娟　　王麗雁
國立彰化師範大學美術系藝術教育碩士班
jessieart999@yahoo.com.tw　　lywang@cc.ncue.edu.tw

摘要

本研究旨在探討 Moodle 網路平台融入國小五年級藝術與人文之戲偶天地教學，學生在學習態度與成效的改變，並瞭解學生對平台之接受度，以做為教學上之參考。研究採「不等控制組設計」，隨機分派實驗組與控制組各一班。研究工具包括 Moodle 網路平台，及自編之「學生學習態度問卷」、「學生對 Moodle 網路平台接受度問卷」、「戲偶天地學習測驗」，將透過單因子變異數分析及 t 檢定（t-test）等方式進行統計分析。

從研究結果顯示，融入 Moodle 網路平台學習之學生在整體學習態度上，顯著優於一般講述法學習之學生、學生對 Moodle 網路平台的接受度上具有正面功能性、學生在學習過程與認知上，顯著優於一般講述法學習之學生。

關鍵詞：Moodle、學習態度、接受度、學習成效。

1. 緒論

本研究主要希望藉由 Moodle 網路平台，提昇學生在藝術與人文上的學習興趣，及彌補講述教材不足之處；進而分析一般講述教學及融入 Moodle 網路平台教學，此二種模式於藝術與人文教學，學生在學習態度與成效的改變，並瞭解學生對平台之接受度，以作為教學上之參考。

1.1 研究動機與目的

隨著網路蓬勃興盛，以網路做為輔助的教學逐漸受到重視，學習的主導性亦回歸學習者本身，學習模式漸轉為「學生本位」。在這樣的時代，需要符合這個世代的學習工具，「網路教學平台」即是在網路世界中，開闢一個屬於教師與學生學習交流的空間，透過它我們可以瞭解學生的成長及轉變歷程，也能紀錄每一筆具有意義的知識建立過程，這樣的學習過程是充滿著價值的探究與追尋。

網路學習環境囿於時空限制與虛擬互動的媒體特質，使得其歷程本質在在反映出主動學習的實質內涵，進而促進學習者自主性的認知歷程，以建構個人化的知識結構，在不停建構、探索知識與解決問題過程中，亦時時刻刻觸動著反思的行為；社會化的合作學習更為網路學習的核心，異質性分工及討論，形成社群間彼此互助合作的機能與本質，讓每一個參與成員都有貢獻著一己所長的機會，這種知識共構模式，恰是網路學習的最佳寫照。

結合網路學習具體呈現之主動、合作、反思及共構歷程本質輔助，讓學習者無形中有著情意的主動、社群的合作、問題的反思、知識的共構等學習態度的改變，因此研究者想探究在教學中，如何融入網路這些特性、功能、優點，來精進學習成效、改變學習態度及提昇教學品質，或是可更進一步的建置網路學習課程與學習環境，培養學生具備使用網路自主學習的能力。而在進行具體學習成效評估的同時，網路學習所具體呈現之主動、合作、反思、知識共構等重要歷程本質[1][2]，在無形中啟發的學習態度改變，亦是值得探討。

教育部近年來積極推動國民中小學九年一貫化與資訊融入課程教學，更於藝術與人文學習領域課綱之國小五、六年級課程目標中（探索與表現、審美與理解、實踐與應用），納入了資訊教育指標[3]。且為縮短資訊科技所造成的城鄉落差，教育部亦致力推廣校園自由軟體的應用，成立校園自由軟體應用諮詢中心；同時，建置了一個免費之數位化課程服務平台 Moodle（Modular Object-Oriented Dynamic Learning Environment），讓教師透過此平台呈現教學方法與概念，協助教師建置數位課程。

目前，國內之中小學教育經費對課程資訊化融入之補助普遍不足，間接造成系統或軟體上的缺乏，Moodle 網路平台恰可提供教學者與學生一個免費數位化課程建置的學習平台。有鑑於網路的發達、國小課程資訊化的缺乏、藝術與人文教學模式及課程目標逐漸導向數位化的趨勢下，研究者期望能借由國小藝術與人文教學活動，融入 Moodle 網路平台，成為學生學習的輔助工具，進而分析學生在藝術與人文領域中探索與表現、審美與理解、實踐與應用課程目標之有形學習成效及主動、合作、反思、合作等無形的學習態度，提供藝術教師在資訊時代中，另一種可運用之教學方式，並瞭解其網路平台應用的有用性及易用性等接受度，給於未來國小推展網路教學平台之參考。為瞭解融入 Moodle 網路平台在藝術與人文領域各項課程目標所提昇之學習成效，在學校既定之教材中，擇以完整涵蓋課程目標的「戲偶天地」單元，為融入 Moodle 網路平台之題材，以利對所有課程目標研究與分析。

基於上述研究動機，研究者以學習者為中心的 Moodle 網路平台，融入國小高年級藝術與人文之戲偶天地教學活動中，讓學生透過網路教學平台互動學習、取得藝術與人文資訊、啟發美感認知、加深

對文化的理解，並研究探討比較目前課堂上所使用之講述、分組學習，與融入 Moodle 網路平台學習的過程、成果之間的差異。因此，本研究目的：

(1) 瞭解 Moodle 網路平台融入國小高年級藝術與人文之戲偶天地教學，學生在過程中學習態度上的影響及改變。
(2) 瞭解學生對 Moodle 網路平台融入教學之接受度。
(3) 瞭解 Moodle 網路平台融入國小高年級藝術與人文之戲偶天地教學，學生在學習上的成效。

1.2 研究問題

(1) 分析 Moodle 網路平台融入國小高年級藝術與人文之戲偶天地教學，學生在學習態度上之影響及改變為何？
(2) 分析學生對 Moodle 網路平台融入教學之接受度為何？
(3) 分析 Moodle 網路平台融入國小高年級藝術與人文之戲偶天地的教學模式與傳統講述教學模式，學生在學習成效上的差異為何？

2. 文獻探討

2.1 網路教學

網路教學是以現有的資訊技術，融會講述教學的優點，所以能突顯了數位學習帶來的優勢，亦成就了網路教學的優點[4]。但縱使網路學習帶來了便利與滿足，也勾勒出未來學習的方向與希望。但在現今藝術學習過程中還是無法完全取代整個師生教學的全部，只能視為教學工具的應用，而學生運用網路學習增進對藝術知識的了解、體驗及行為改變的過程與結果才是重要的。教師想透過網路增進學生對知識的探索經驗與改進視覺藝術教學策略、方法以提昇學習成效，不在於網路資訊的填充，而是在於能否了解及活用網路學習的特性。所以，就進行網路教學時應根據網路學習的特性進行下列幾點思考：

(1) 學習態度的轉變：由於網路學習管道通暢，學生學習由被動的接受轉變為主動的建構，在態度上也應隨之調整改變、積極投入與參與整個學習。
(2) 合作關係的建立：與團體的分組分工競爭方式不同，透過網路上的互動機制，學生必須在同儕之間建立合作之夥伴關係，進行分享及交流，學習才能有效的達成目標。
(3) 重視反思的過程：知識的探索不再是追尋固定而且唯一的答案，而是由同儕間學習互動而成，所建構的學習內容是否正確或者是具有意義價值，需藉由反思的過程來應證。
(4) 教師角色的調適：網路資訊廣擴帶來學習的便利，網路學習中的教師不再是知識的唯一提供者，但應具有多重性與帶領引導的角色與功能，協助學生主動共構學習的知識體系。

2.2 Moodle 網路平台

Moodle 主要是由開放原始碼自由軟體發展而成的課程管理系統。由澳洲創始人（Martin Dougiamas）運用教學原理並以 PHP 所撰寫。Moodle 可以透過它強大的功能來幫助教學者將知識資訊傳遞的更廣、服務更為透徹，並且跳脫以往教學輔助平台價格昂貴、複雜功能設計的缺點，並且還允許使用者根據個別的需求修改程式[5]。

2.3 學習態度

在網路學習的歷程中，顏榮泉與陳明溥（2002）對線上學習歷程本質建構四項歷程：主動學習、合作學習、反思、知識共構的歷程；許紹真（2006）在運用網路互動式學習介面對藝術知識的探索研究中，更歸納主動、合作、反思與共構是網路學習所具體呈現之重要歷程本質。學習的歷程中，學習者是最具關鍵性的成員，Sternberg[6]認為態度、經驗、認知及學習型態等四個重要指標是可以增強學習者本身學習的歷程，當中態度是為最重要的指標。學習態度不是天生而來的，而是後天習得的，不同的學習環境，不同的學習態度，對於學習的具體呈現亦有不同，相對於網路的環境，主動、合作、反思與知識共構等學習態度對網路學習更能具體呈現，本研究依據網路學習特性分析及針對網路學習歷程本質與內涵，將以主動、合作、反思及知識共構學習態度等層面，分析 Moodle 網路平台融入國小高年級藝術與人文之戲偶天地教學，學生學習態度上之影響及改變。

2.4 學習成效

學習成效可以從許多方面來衡量，綜合相關學者的看法[7]-[9]，如學習績效、學習的自我評估、學習興趣、作業表現、學習者的態度等。本研究以國小高年級為研究對象，參照上述這些衡量學習成效的指標，再依據教育部（2008）國民中小學九年一貫藝術與人文學習領域課程綱要，第三階段國小高年級之探索與表現、審美與理解、實踐與應用等課程目標中之學習能力指標，經由學習測驗，瞭解學生在藝術與人文之戲偶天地教學中，探索傳統戲偶起源資料之認知能力，理解傳統戲偶美感、形式、特徵及要素之辨能力，應用傳統戲偶角色之欣賞能力等學習成效。

2.5 Moodle 網路平台接受度

Moodle 乃為電腦資訊系統之一種，而科技接受模式（Technology Acceptance Model，TAM）為使用者對於電腦資訊系統接受度的決定性因素提供理論基礎[10]；在科技接受模式中有兩個重要的信念：「知覺有用性」與「知覺易用性」，其認為影響使用者接受資訊科技行為的外在變數，是透過知覺

有用性與知覺易用性這兩個信念，再經由對使用態度與使用行為意向的影響，然後產生實際系統使用行為。該模型當中的「知覺有用性」與「知覺易用性」為形成態度的關鍵，而影響到使用者的意圖，最後影響使用者實際使用的行為。所以知覺有用性與知覺易用性亦衡量資訊系統接受度的指標。知覺有用性會影響使用態度與使用意願；知覺易用性會影響知覺有用性、使用態度與使用意願；使用意願會影響實際使用行為。如下圖 1：

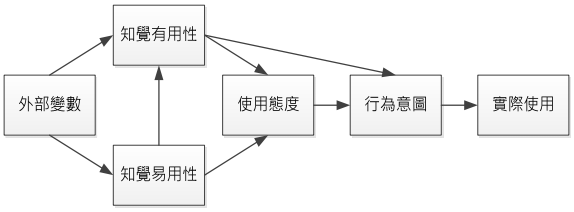


圖 1 科技接受模式[11]

3. 研究設計與實施

本研究為實驗研究法，採以班級為單位之實驗研究，結合學校課程教學進行實際教學實驗，並針對研究內容中的各個變項進行分析及界定。

3.1 研究設計

整個研究架構如圖 2 所示：

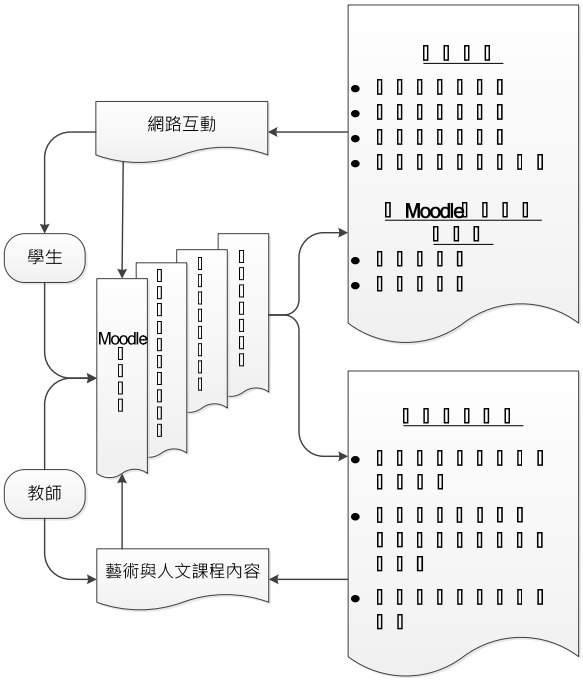


圖 2 研究架構圖

教學實驗為實驗研究法中之不等控制組設計[12]：以五年級學生為實驗對象，將現有的班級建制中，隨機各選擇一班為實驗組及控制組，每班（組）學生各 23 人。對實驗組進行 Moodle 網路平台操作應用之實驗處理，兩組間同時採取前、後測設計，用以分析之間的差異性，以了解融入 Moodle 網路教學平台與學習態度、學習成效及平台接受度的關係。模式如圖 3：

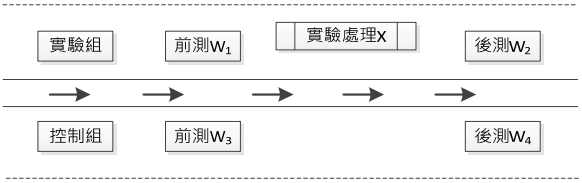


圖 3 實驗設計模式

(1) W_1、W_3 ，W_2、W_4：實驗前、後，兩組均接受「學生學習態度問卷」、「學生對 Moodle 網路平台接受度問卷」及「戲偶天地學習測驗」測驗。

(2) X：實驗組接受講述教學及 Moodle 網路平台操作與線上互動交流的實驗處理。控制組接受講述教學及一般課堂討論及分組合作方式進行學習。

本研究主要探討的自變項及依變項如圖 4：

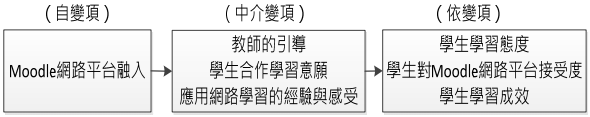


圖 4 變項關係圖示

3.2 研究工具

(1) 學生學習態度問卷

本問卷採用 Likert-type scale 四點量表，內容分為：主動學習、合作學習、反思學習及知識共構學習的態度等四個面向，每個面向各七題，包括一題反向題。並針對學習態度內容之符合程度填答，每題得分範圍為 1-4 分，每個面向得分範圍為 7-28 分；得分愈高，表示學習動機強，態度愈積極、正面。題目由研究者參考資料文獻自行設計編訂，先經「專家效度分析」，再經信度分析檢核，各個面向 Cronbach's α 系數達 0.8 以上、整體之 Cronbach's α 系數為 0.972，顯示其一致性是可被接受。

(2) 學生對 Moodle 網路平台接受度問卷

本問卷採用 Likert-type scale 四點量表，內容依網路平台使用之知覺有用性與知覺易用性二個面向，每個面向各 6 題。並針對內容之符合程度填答，每題得分範圍為 1-4 分，每個面向得分範圍為 6-24 分；得分愈高，表示平台之有用性、易用性愈高，接受度愈正面。知覺有用性與知覺易用性題目由研究者翻譯自 TAM 原始問卷，再經信度分析之檢核。信度分析檢核後，各個面向及整體之 Cronbach's α 系數達 0.9 以上， 顯示其一致性是可被接受。

(3) 戲偶天地學習測驗

戲偶天地學習測驗，以文字描述為主，為研究者參考資料文獻及藝術與人文教學之目標與能力而自行設計，先經「專家效度分析」後，再經信度分析檢核，整體信度值為 0.773，顯示本試題內容具有內部之一致性。編製目的主要用來評量學習者

對學習主題的認知程度，其測驗面向依教學之學習目標共分為探索、理解與應用知識三個面向。

4. 結果與討論

4.1 學生整體學習態度之分析與討論

本節主要為分析本研究中融入 Moodle 網路平台學習之實驗組與進行一般討論學習之控制組學生，在戲偶天地課程之整體學習態度情形。分析中，以組別（實驗組、控制組）為自變項，「主動學習的態度」、「合作學習的態度」、「反思學習的態度」及「知識共構學習的態度」為依變項，進行「學習態度之平均數與標準差」如表 1、「學習態度之單因子變異數」如表 2、「學習態度之 t 檢定（t-test）」如表 3 等相關分析。

表 1 學習態度之前、後測驗平均數與標準差分析

統計		控制組			實驗組		
項目		個數	平均數	標準差	個數	平均數	標準差
整體學習的態度							
前測		23	90.70	11.79	23	91.91	18.15
後測		23	92.22	13.30	23	100.30	10.09
1.主動學習的態度							
前測		23	21.39	4.30	23	21.43	3.85
後測		23	22.83	3.60	23	25.17	2.87
2.合作學習的態度							
前測		23	23.00	3.66	23	23.61	4.93
後測		23	23.00	3.72	23	25.04	3.05
3.反思學習的態度							
前測		23	22.48	3.17	23	23.09	5.33
後測		23	23.09	3.48	23	24.96	2.53
4.知識共構學習的態度							
前測		23	23.83	3.50	23	23.78	4.81
後測		23	23.30	3.31	23	25.13	2.56

上表統計資料，無論在「整體學習態度」或是在其分向度之前、後測驗平均數差異，都以實驗組之差異較大，相對表示融入 Moodle 網路平台教學之實驗組在這些方面均有較多的成長。

表 2 學習態度之前、後測驗單因子變異數分析

		平方和	自由度	平均平方和	F 值	顯著性 P
整體學習的態度						
前測	組間	17.043	1	17.043	.073	.789
	組內	10302.696	44	234.152		
後測	組間	752.087	1	752.087	5.398	*.025
	組內	6130.783	44	139.336		
1.主動學習的態度						
前測	組間	.022	1	.022	.001	.971
	組內	733.130	44	16.662		
後測	組間	63.391	1	63.391	5.978	*.019
	組內	466.609	44	10.605		
2.合作學習的態度						
前測	組間	4.261	1	4.261	.226	.637
	組內	829.478	44	18.852		
後測	組間	48.022	1	48.022	4.152	*.048
	組內	508.957	44	11.567		
3.反思學習的態度						
前測	組間	4.261	1	4.261	.221	.640
	組內	847.565	44	19.263		
後測	組間	40.196	1	40.196	4.348	*.043
	組內	406.783	44	9.245		
4.知識共構學習的態度						
前測	組間	.022	1	.022	.001	.972
	組內	779.217	44	17.709		
後測	組間	38.348	1	38.348	4.377	*.042
	組內	385.478	44	8.761		

***P＜.05**

上表資料顯示，後測在其分向度皆具顯著性，綜合「整體學習態度」亦具有顯著性。

表 3 學習態度之前、後測驗 t 檢定（t-test）分析

		平均數相等的 t 檢定			
		t	自由度	顯著性 P(雙尾)	平均差異
整體學習的態度					
前測	假設變異數相等	-.270	44	.789	-1.21739
	不假設變異數相等	-.270	37.768	.789	-1.21739
後測	假設變異數相等	-2.323	44	*.025	-8.08696
	不假設變異數相等	-2.323	41.031	*.025	-8.08696
1.主動學習的態度					
前測	假設變異數相等	-.036	44	.971	-.04348
	不假設變異數相等	-.036	43.459	.971	-.04348
後測	假設變異數相等	-2.445	44	*.019	-2.34783
	不假設變異數相等	-2.445	41.918	*.019	-2.34783
2.合作學習的態度					
前測	假設變異數相等	-.475	44	.637	-.60870
	不假設變異數相等	-.475	40.562	.637	-.60870
後測	假設變異數相等	-2.038	44	*.048	-2.04348
	不假設變異數相等	-2.038	42.395	*.048	-2.04348
3.反思學習的態度					
前測	假設變異數相等	-.470	44	.640	-.60870
	不假設變異數相等	-.470	35.851	.641	-.60870
後測	假設變異數相等	-2.085	44	*.043	-1.86957
	不假設變異數相等	-2.085	40.211	*.043	-1.86957
4.知識共構學習的態度					
前測	假設變異數相等	.035	44	.972	.04348
	不假設變異數相等	.035	40.170	.972	.04348
後測	假設變異數相等	-2.092	44	*.042	-1.82609
	不假設變異數相等	-2.092	41.417	*.043	-1.82609

***P＜.05**

上表資料再一次驗證，後測在其各分向度皆具顯著性，「整體學習態度」亦具顯著性。因此，我們認為融入 Moodle 網路平台學習對於實驗組「整體學習態度」提昇是有成效的，且以「主動學習的態度」前、後測平均數差異值為最大，所以提昇為最多。

4.2 學生對 Moodle 平台接受度之分析與討論

本節主要為分析本研究中融入 Moodle 網路平台學習之實驗組與進行一般討論學習之控制組學生，在戲偶天地課程之學生對 Moodle 網路平台接受度情形。分析中，以組別（實驗組、控制組）為自變項，「知覺有用性」及「知覺易用性」為依變項，進行「對 Moodle 網路平台接受度之平均數與標準差」如表 4、「對 Moodle 網路平台接受度之單因子變異數」如表 5、「對 Moodle 網路平台接受度之 t 檢定（t-test）」如表 6 等相關分析。

表 4 對 Moodle 平台接受度之前、後測驗平均數與標準差分析

統計		控制組			實驗組		
項目		個數	平均數	標準差	個數	平均數	標準差
對 Moodle 網路平台接受度							
前測		23	35.70	4.50	23	36.26	6.80
後測		23	35.70	6.65	23	42.30	6.31
1.知覺有用性							
前測		23	18.09	2.39	23	18.39	3.81
後測		23	17.87	3.49	23	21.39	3.43
2.知覺易用性							
前測		23	17.61	2.37	23	17.87	3.33
後測		23	17.83	3.39	23	20.91	3.29

上表統計資料，無論在「對 Moodle 網路平台接受度」或在其分向度之前、後測驗平均數差異，都以實驗組之差異較大，相對表示融入 Moodle 網路平台教學之實驗組在這些方面均有正面的改變。

表 5 對 Moodle 平台接受度之前、後測驗單因子變異數分析

		平方和	自由度	平均平方和	F值	顯著性 P
對Moodle網路平台接受度						
前測	組間	3.674	1	3.674	.111	.741
測	組內	1461.304	44	33.211		
後測	組間	502.261	1	502.261	11.960	*.001
測	組內	1847.739	44	41.994		
1.知覺有用性						
前測	組間	1.065	1	1.065	.105	.747
測	組內	445.304	44	10.121		
後測	組間	142.630	1	142.630	11.884	*.001
測	組內	528.087	44	12.002		
2.知覺易用性						
前測	組間	.783	1	.783	.094	.761
測	組內	368.087	44	8.366		
後測	組間	109.587	1	109.587	9.818	*.003
測	組內	491.130	44	11.162		

*P＜.05

上表資料，後測在「知覺有用性」及「知覺易用性」等向度皆具顯著性，綜合「對 Moodle 網路平台接受度」亦具顯著性。

表 6 對 Moodle 平台接受度之前、後測驗 t 檢定（t-test）分析

		平均數相等的 t 檢定			
		t	自由度	顯著性 P(雙尾)	平均差異
對 Moodle 網路平台接受度					
前測	假設變異數相等	-.333	44	.741	-.56522
測	不假設變異數相等	-.333	38.162	.741	-.56522
後測	假設變異數相等	-3.458	44	*.001	-6.60870
測	不假設變異數相等	-3.458	43.877	*.001	-6.60870
1.知覺有用性					
前測	假設變異數相等	-.324	44	.747	-.30435
測	不假設變異數相等	-.324	37.002	.747	-.30435
後測	假設變異數相等	-3.447	44	*.001	-3.52174
測	不假設變異數相等	-3.447	43.987	*.001	-3.52174
2.知覺易用性					
前測	假設變異數相等	-.306	44	.761	-.26087
測	不假設變異數相等	-.306	39.701	.761	-.26087
後測	假設變異數相等	-3.133	44	*.003	-3.08696
測	不假設變異數相等	-3.133	43.956	*.003	-3.08696

*P＜.05

上表統計資料再一次驗證，後測在「知覺有用性」及「知覺易用性」等向度皆具顯著性，綜合「對 Moodle 網路平台接受度」亦具顯著性。因此，我們認為實驗組對 Moodle 網路平台接受度的改變具正面功能性。

4.3 學生整體學習成效之分析與討論

本節主要為分析本研究中融入 Moodle 網路平台學習之實驗組與進行一般討論學習之控制組學生，在戲偶天地課程之整體學習成效情形。分析中，以組別（實驗組、控制組）為自變項，「傳統戲偶起源資料之探索能力」、「傳統戲偶美感、形式、特徵及要素之理解能力」、「傳統戲偶角色之應用能力」為依變項，進行「傳統戲偶認知能力之平均數與標準差」如表 7、「傳統戲偶認知能力之單因子變異數」如表 8、「傳統戲偶認知能力之 t 檢定（t-test）」如表 9 等相關分析。

表 7 認知能力之前、後測驗平均數與標準差分析

統計	控制組			實驗組		
項目	個數	平均數	標準差	個數	平均數	標準差
整體傳統戲偶認知能力總分						
前測	23	7.57	1.90	23	7.39	1.95
後測	23	11.91	2.70	23	14.39	1.03
1. 傳統戲偶起源資料之探索能力						
前測	23	1.13	0.76	23	1.09	0.85
後測	23	3.13	1.36	23	4.74	0.45
2. 傳統戲偶美感、形式、特徵及要素之理解能力						
前測	23	3.30	1.06	23	3.26	0.92
後測	23	4.22	1.00	23	4.91	0.29
3. 傳統戲偶角色之應用能力						
前測	23	3.13	0.92	23	3.04	0.82
後測	23	4.30	1.06	23	4.96	0.21

上表統計資料，無論在「整體傳統戲偶認知能力」或其各分向度之前、後測驗平均數差異，都以實驗組之差異較大，相對表示融入 Moodle 網路平台教學之實驗組在這些方面均有較多的進步。

表 8 認知能力之前、後測驗單因子變異數分析

		平方和	自由度	平均平方和	F 值	顯著性 P
整體傳統戲偶認知能力						
前測	組間	.348	1	.348	.094	.761
	組內	163.130	44	3.708		
後測	組間	70.630	1	70.630	16.954	*.000
	組內	183.304	44	4.166		
1.傳統戲偶起源資料之探索能力						
前測	組間	.022	1	.022	.034	.855
	組內	28.435	44	.646		
後測	組間	29.761	1	29.761	29.071	*.000
	組內	45.043	44	1.024		
2.傳統戲偶美感、形式、特徵及要素之理解能力						
前測	組間	.022	1	.022	.022	.883
	組內	43.304	44	.984		
後測	組間	5.565	1	5.565	10.315	*.002
	組內	23.739	44	.540		
3.傳統戲偶角色之應用能力						
前測	組間	.087	1	.087	.114	.737
	組內	33.565	44	.763		
後測	組間	4.891	1	4.891	8.333	*.006
	組內	25.826	44	.587		

***P＜.05**

由上表資料，後測在其各分向度能力皆具顯著性，綜合「整體傳統戲偶認知能力」亦具有顯著性。

表 9 認知能力之前、後測驗 t 檢定（t-test）分析

		平均數相等的 t 檢定			
		t	自由度	顯著性 P(雙尾)	平均差異
整體傳統戲偶認知能力					
前測	假設變異數相等	.306	44	.761	.17391
	不假設變異數相等	.306	43.976	.761	.17391
後測	假設變異數相等	-4.118	44	*.000	-2.47826
	不假設變異數相等	-4.118	28.327	*.000	-2.47826
1.傳統戲偶起源資料之探索能力					
前測	假設變異數相等	.183	44	.855	.04348
	不假設變異數相等	.183	43.444	.855	.04348
後測	假設變異數相等	-5.392	44	*.000	-1.60870
	不假設變異數相等	-5.392	26.749	*.000	-1.60870
2.傳統戲偶美感、形式、特徵及要素之理解能力					
前測	假設變異數相等	.149	44	.883	.04348
	不假設變異數相等	.149	43.049	.883	.04348
後測	假設變異數相等	-3.212	44	*.002	-.69565
	不假設變異數相等	-3.212	25.641	*.004	-.69565
3.傳統戲偶角色之應用能力					
前測	假設變異數相等	.338	44	.737	.08696
	不假設變異數相等	.338	43.485	.737	.08696
後測	假設變異數相等	-2.887	44	*.006	-.65217
	不假設變異數相等	-2.887	23.690	*.008	-.65217

***P<.05**

上述資料再一次驗證，後測在其各分向度能力皆具顯著性，綜合整體傳統戲偶認知能力亦具有顯著性。因此，我們認為融入 Moodle 網路平台學習對實驗組「整體傳統戲偶認知能力」的提昇是有成效的，其中以「傳統戲偶起源資料之探索能力」前、後測平均數差異值為最大，所以成效提升為最多。

5. 結論

本研究從藝術與人文的發展可能性為起點，突破了時間空間限制，架構了以學習者為中心的 Moodle 網路平台，使學生能透過網路平台互動學習並發現美感知識，而非僅於一般的課堂。研究者透過對網路平台的研究實驗比較此一學習過程和結果與一般教學的過程和結果之間的差異做出結論。

經探討對於學生在學習態度、學習成效與對 Moodle 網路平台的接受度都是具有正向的功能性及顯著性。在學習態度方面，尤以主動學習的態度提昇為最多，顯示透過網路平台學習，可讓學生的學習更為積極。在平台的接受度方面，知覺有用性及知覺易用性都為顯著，可見得學生非常樂於接受網路平台的學習方式。在學習成效方面，與傳統講述教學相較，使用 Moodle 者皆顯著提昇學習上探索、理解、應用等課程目標能力，尤以傳統戲偶起源資料探索能力提昇為最多。經此等實驗與分析，皆呈正向性，希望可提供學界為教學上之參考。

參考文獻

[1] 顏榮泉、陳明溥、葉嵩生（2002）。網路學習之歷程分析與知識探索模式，第六屆全球華人學習科技研討會（GCCCE 2002），中國，北京，北京師範大學，2002 年 6 月。

[2] 許紹真（2006）。情緒誘導表現於互動式學習介面之創作與研究－以藝術知識探索為例。國立臺灣師範大學設計研究所在職進修碩士班。未出版。台北市。

[3] 教育部（2008）。國民中小學九年一貫課程綱要藝術與人文學習領域。台北市：教育部。

[4] 趙惠玲、丘永福、張素卿、傅斌暉、曹筱玥、鍾政岳(2006)。高中藝術領域課程輔助教學參考手冊 1－美術。台北市：國立臺灣藝術教育館。

[5] 歐展嘉（2008）。Moodle 馬上就會。台北市：松岡。

[6] Sternberg, R. J. (1999). A propulsion model of types of creative contributions. Review of General Psychology, 3(2), 83-100.

[7] Alavi, M. (1994). Computer-mediated collaborative learning: An empirical evaluation. MIS Quarterly, 18, 159-174.

[8] Piccoli, G., Ahmad, R., & Ives, B. (2001). Web-based virtual learning environments: A research framework and a preliminary assessment of effectiveness in basic it skills training. MIS Quarterly, 25, 4, 401-426.

[9] Schutte, J. G. (1997). Virtual teaching in higher education: The new intellectual superhighway or just another traffic jam. Northridge, CA: California State Univerity.

[10] Davis, F. D. (1989a). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-340.

[11] Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989b). User acceptance of computer technology: A comparison of two theoretical models. Management Science, 35(8), 982-1003.

[12] 王文科、王智弘（2007）。教育研究法：研究與方法。台北市：五南。

將模擬系統移轉至視覺化程式語言環境之建置對照—以 StarLogo TNG 為建置工具

林均恒 洪文麟 張智凱
國立臺南大學 數位學習科技學系
chihkai@mail.nutn.edu.tw

摘要

模擬學習(simulation-based learning)與「從設計中學習」理論皆提出，學習者在自行進行操作或設計的過程中，可高度融入學習情境，以個人方式累積經驗，將有助於所學知識的靈活運用。基於以上觀點，NetLogo 豐富而完整的模型庫可視為良好的學習教材，其中每個模擬系統都被清楚地分類且橫跨多個領域，但由於 NetLogo 裡的模擬系統是以文字型程式語言(text-based programming)進行編寫，對於程式能力不精熟的學習者，需花費時間在克服程式識讀與編寫的問題。為了降低學習者程式能力的門檻，本研究選擇以具視覺化程式編寫環境的 StarLogo TNG 作為模擬系統建置工具，將 NetLogo 中的模型進行移轉，並整理出移轉工作可依循的對照及轉換方針，搭配實際移轉範例做說明，期望藉此提供於 NetLogo 中遭遇程式問題的學習者另一個建置模擬系統的管道。

關鍵詞：模擬學習、模擬系統、NetLogo、StarLogo TNG、模型移轉

Abstract

In light with two theories of simulation-based learning and learning by design, learners are expected to enjoyably participate in learning task and developed a high order thinking skills to apply the prior knowledge they acquired to solve the problems. Based on the above concept, NetLogo which provides rich models library could be seen as a great learning materials. There're many simulations being specifically classified and the types include variety of fields. However, learners are required to dedicate themselves to master programming because NetLogo is a platform of text-based programming that low proficiency programmer needs to spend lots of time editing and debugging code. In order to lower the threshold of programming, the research adopted a visual programming language StarLogo TNG to transfer NetLogo models and listed principles and guidelines for transferring. Through a demonstration from a transferring example, the research offered an alternative for low-proficiency learners of programming to establish a simulation-based learning system.

Keywords: simulation-based learning, simulation, NetLogo, StarLogo TNG, simulation transferring.

1. 前言

目前視覺化程式語言相較於一般的程式語言在編寫上雖然較缺乏彈性，但其程式的排列及編輯方式能夠讓即使不是電腦相關科系的學習者亦可輕易理解程式內容與結構。因此在以學習為主要目標的基礎上，選擇以視覺化程式語言做為模擬系統建置的環境，且在模擬系統建置的過程，將欲模擬的現象進行分析，並轉化為抽象概念，嘗試以程式語言將其完整地表達出來，接著運作模擬系統，不斷地進行測試、修正符合真實情況，在每一次的程式修改中，都將更清楚了解程式編寫的結構、規則以及實際問題抽象化的技巧，重複地面對問題、解決問題，將進行處理的經驗內化，進而應用於生活中，達到融會貫通的學習境界。

2. 文獻探討

2.1 模擬學習(Simulation-Based Learning)

根據體驗式學習理論(experiential learning theory)，藉由實作、思考並以自身經驗的方式進行學習將可以得到較好的學習效果[1]，學習者是主動地、完全地投入在學習的過程中[2]，以自己的學習方法吸收經驗。在 Kolb 的體驗學習圈(experiential learning cycle)中將學習過程分成四階段：具體經驗、反思性觀察、抽象概念化、主動進行實驗[3]。

而模擬系統的建置與運用可分為以下六步驟[4]：分析特定系統、發展概念雛形、將雛型轉為程式架構、完成初步模擬系統、進行實驗驗證模擬系統、進行模擬以解決問題或找出原因。對照後可發現模擬系統建置與運用的部分過程恰能與體驗學習圈的四個階段相互呼應。

學習者由實際情況進行觀察分析，再依據分析的結果發展出模擬的概念雛型，經歷了具體經驗與反思性觀察兩階段；接著將其中概念抽象化，設法以程式指令表達，進而完成模擬系統，進入了抽象概念化階段；且在模擬系統中，學習者可以調整變因，運行模擬系統，即為主動進行實驗；由不同的

變因組合觀察到模擬的可能結果，同時亦檢視模擬系統是否合理，再對模擬系統的設計進行微調，回到了具體經驗與反思性觀察的階段；最後參考模擬結果對實際情況做出相應行為，此乃為學習效果的呈現。經歷這些過程使得學習者充分將接收訊息消化，更能將所學融會貫通。

2.2 從設計中學習(Learning by Design)

為使學習者有能力去融會貫通學習內容並進行應用，在過去有研究對學習者日常行為模式的產生進行相關資料的蒐集，發現在處理生活中的各項事務時，第一時間通常會從以往的記憶中找尋類似事件，根據經驗著手進行思考解決方式，即為案例式推理(Case-Based Reasoning)的基本原理[5]，同時也是問題導向學習(Problem-Based Learning)理論的目的[6]。

「設計」是提供實際經驗的過程，需要學習者完全地投入思考，其中會使用到分析問題、蒐集資料、訂定方法、評估可行性等技巧，最後找出最好的解決方法[7]，Gee 認為設計能促使學習行為的發生[8]。「從設計中學習」理論依據以上所述，希望學習者在找出問題答案的過程中，運用「設計」發展出解決方法。

案例式推理與問題導向學習的概念融合在「從設計中學習」的理論中呈現[9]，以學習者的角度出發，引導學習者主動、積極進行學習活動，Kolodner、Gray 以及 Fasse 所提出 LBD's Cycle[10]的活動包含兩個部分：設計／再設計(design/redesign)與研究&探討(investigate & explore)。

設計部分由瞭解挑戰、運用科學知識進行規劃設計、驗證、建構與測試、分析與解釋、展示與表達想法，這幾個程序進行循環，而研究部份的循環則是由清楚明白疑問、做出假設、設計調查、指導調查、分析結果、海報展示所組成。兩個循環間的關係為：從設計的結果得到知識與面臨問題而進行研究，再將研究的成果實際應用進行規劃設計。在 LBD's Cycle 中可見，「設計」在學習行為中扮演著重要的角色，與研究的過程相輔相成。

「設計」的動作可以使學習者全心投入學習的狀態中，而在此同時，學習者也能藉由「設計」的行為，以自己的方式累積個人經驗，使學習者能靈活運用所學的成果，擺脫傳統教學的單一性(即由教師主導的單一教學方式)，達到更佳的學習效果。

2.3NetLogo 與 StarLogo TNG 之比較

先前所提到的模擬學習理論表示，由模擬系統的建置進行模擬現象的學習能有較深刻的學習經驗。因此模型庫中具有眾多模擬系統且橫跨多個領域[11]的 NetLogo 便被納入考量中，NetLogo 是以 Java 為基底所開發，由美國西北大學 The Center for Connected Learning(CCL) and Computer-Based Modeling 所開發的模擬建置環境，以 Logo 語言進行編寫，多被使用於建置須長時間觀察或結果不可逆的模擬系統[12]，使用者可依自己的需求在環境中建立模型進行模擬。

由 MIT Scheller Teacher Education Program 所開發的 StarLogo TNG 在程式編輯方式與 NetLogo 全然不同，改以視覺化程式語言進行模擬系統的程式編寫，發展概念乃基於以下兩點：(1)降低使用者建立模擬系統的門檻，以及(2)增加模擬場景的生動感[13]。各式指令以不同顏色及形狀的程式塊(programming blocks)替代，運用拼圖拼接、拖拉的方式來編輯組合，爾後在其程式編輯視窗(Workplace)中依背景分類區塊進行擺放，使得即使不精通程式編輯的人也能輕易進行程式編寫，而模擬系統則以 3D 方式呈現，除了符合現今視覺傳達的趨勢，亦給予模擬建置者一個機會更精確地呈現模擬系統，地面可進行高低起伏的設計，生動的場景呈現更能吸引目光，提升使用者的興趣；學習者能利用可從任意角度檢視的鏡頭，更清楚地進行觀察。

NetLogo 與 StarLogo TNG 皆以 StarLogo 為基礎發展而來[14][15]，繼承 StarLogo 大部分的特性，NetLogo 承接了 StarLogo 的簡單語法[16]，程式編寫較具彈性，因多了跨平台之便利性，大幅降低了系統上的限制問題，使得大多數使用者選擇以 NetLogo 建置模擬系統，而 StarLogo TNG 則一改 StarLogo 原有的文字型程式語言(text-based programming)，轉而發展視覺化程式語言，以具有繽紛色彩的程式塊替代了文字型指令，但由於同承接自 StarLogo 系列且兩者之開發目的相同，因此在設計上仍有許多雷同之處，如：部分指令的名稱、使用介面的形式，以及皆提供多個 Agent 同時運作的功能，這些使得使用者在操作上只要熟悉其中一個環境，對另一個就不會感到陌生。

本研究以學習為主要考量，為使學習者即使不精通程式編輯也不受影響，視覺化程式語言具有的幾項屬性：具體性、直接性、清晰性和立即性[17]，以及不必費心思顧慮指令拼法與程式語法的編寫過程可以減少學習者在建立模擬系統時程式編輯上的困難，而當學習者進行模擬系統的觀察及程式識讀時，以 3D 方式呈現模擬系統再搭配色彩繽紛且按照分類排放的程式指令，不但能清楚表現模擬系統，亦可提升學習者的興趣。

有鑑於以上原因，本研究選擇 StarLogo TNG 做為模擬系統建置的工具，但發現目前在 StarLogo TNG 的模型庫中可供使用的模擬系統範例仍不足，多需使用者自行建置，在模型庫豐富的 NetLogo 則因為文字型程式編寫方式而有可能產生編寫與識讀上困擾的問題(表 1)，為此本研究決定從 NetLogo 移轉模型至 StarLogo TNG，並於建置的經驗中為使用者整理出規則，供使用者於模擬系統建置過程中參考使用。

表 1 Starlogo TNG 輔助解決 Netlogo 使用上之問題

Netlogo 使用上所遭遇的問題	問題描述	Starlogo TNG 可提供的輔助
需要具有程式語法的先備觀念以及留心程式的拼字細節	Netlogo 仍是以文字型程式語言(text-based programming)進行程式編寫，使用者需花時間了解語法結構，並且注意指令拼法，以避免小小的拼字錯誤造成整個模擬系統無法運行。	以視覺化的程式塊為最小單位，且不同類型的程式塊有特定的接口形狀，符合形狀的連結才可接上，不必費心於注意程式結構及拼字上的錯誤。
程式碼識讀不易	Netlogo 的程式編寫十分彈性，但程式碼若未經整理並進行註解，則在識讀上易造成混亂，對程式初學者更是一大障礙。	Starlogo TNG 的程式編輯視窗(Workplace)有針對各個 agent 及運行階段進行區域劃分，編寫者可依此排列程式，識讀者可依此理解程式。
必須自行創建與連結模擬系統的控制項(control)	Netlogo 中需在介面上自行產生控制項，再進行程式碼的連結設定，若連結錯誤指令將影響系統運行結果。	於程式編寫中自動產生相應控制項。

3. 移轉動機與方針

NetLogo 與 StarLogo TNG 皆可將環境分成兩個區塊：程式編寫及模擬呈現，程式編寫區塊即學習者主要學習程式概念的部分，亦為影響模擬系統可否順利運作的核心，StarLogo TNG 中此區域在左側設有程式指令的分類，點擊後可出現各分類下的程式指令；在模擬呈現區塊中學習者可以看到自己編寫出來的模擬系統，藉由調整控制項，觀察運行結果及數據結果來輔助對於程式部分的理解。以下將針對這兩部分，分別解釋指令移轉對照與控制介面轉換方法，最後輔以流浪狗範例進行解釋說明。

3.1 指令對照

StarLogo TNG 與 NetLogo 大多數的指令名稱相同，此與兩者之發展皆參考自同一軟體 StarLogo 有關，指令的命名顯現了簡短、直覺的特點，主要是希望使用者不必在理解指令的過程中花費太多心力。StarLogo TNG 中可進行相似對照的指令分類主要有 Setup & Run、Movement、Logic、Trait 與 Math。

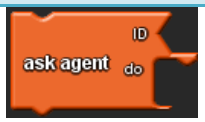
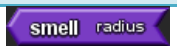
在 Setup & Run 分類中的指令會直接對模擬呈現介面(Spaceland)造成改變，包含按鈕與圖表的產生，這部分也是 StarLogo TNG 的特點之一，特別規劃程式塊供使用者進行模擬系統的初始條件設定(Setup)與運行過程設計(Run)，此分類中只有與清除物件相關的指令能進行相似對照，例如：clear all(clear-all) 、 clear patches(clear-patches) ； 而 Movement 分類中的指令主要在使 Agent 產生位置移動，除去 NetLogo 中沒有的三維空間之上下移動指令，其餘基本的指令 forward(forward)、towards(towardsxy x y)以及 set heading(set heading)等皆有相似指令可進行呼應。

Logic 分類中的指令以邏輯判斷式為主，為程序間進行連接的重要指令，大多數的程式塊都能找到相似的指令，譬如：if(if)、and(and)、true(true)、hatch(hatch)，少部分程式塊即使無相似對應，仍能由其他程式塊組合而成生相同的效果，例如 StarLogo TNG 的 switch 指令於 NetLogo 中無相似對應，而其功能為判斷多個性質相同的不同條件，依條件分別進行相應的動作，此即為結合多個 if 指令的結果。

Trait 分類，顧名思義即為對各項 agent 的特性做調整的指令集，拿掉對於 agent 高度(altitude)與場景轉換(level)的設定，其他指令幾乎都能相應，至於 Math 分類，其中包含所有數學相關的指令，例如：數字、運算子與各類常見之數學符號(sqrt、abs、log 等)，每一個程式塊都能找到近乎完全相同的指令。

少部分的指令因視覺化程式塊單位內容的設計，使得程式指令名稱產生差異，再加上 StarLogo TNG 在模擬系統的呈現上較 NetLogo 多了一個維度的呈現方式，甚至還可以自由調整鏡頭，從不同角度呈現模擬結果，因此 StarLogo TNG 的指令還多了 Terrain 分類與 Control 分類，Control 內部的指令可用來控制鏡頭，而 Terrain 分類裡主要是控制地形的起伏，另有與地面相關之判斷式以及場景轉換動作(level)的指令。表 2 內容即針對部分相異但仍可以進行對照的指令做整理。

表 2 部分相異指令名稱對照範例

相異	
StarLogo TNG	NetLogo
Setup & Run	
	set xy random-xcor random-ycor
	to *setup* *cmds* end
Procedure	
	to *name* *cmds* end
Terrain	
	pcolor
Logic	
	ask *agent* [*cmd*]
OtherAgents	
	in-radius *num*
Colors	
	one-of base-colors

3.2 模擬系統之控制介面轉換

除了程式的編寫外，模擬系統的呈現與互動亦是本研究重點之一，在 StarLogo TNG 中，各個模擬系統的控制項會經由程式的編寫相應產生，而於 NetLogo 中則須自行於介面上創建，再與程式指令進行連結。NetLogo 常用的模擬控制項目(control)有：Button、Slider、Switch、Chooser、Monitor 與 Plot。以下將針對 NetLogo 各控制項列出使 StarLogo TNG 產生相應項之方法。

Button 通常應用在模擬系統的初始設定與運行，在 StarLogo TNG 中選擇 setup、forever、run、run once 皆能自動於介面出現按鈕，可於程式編輯時變更按鈕名稱，運行部分的按鈕在運行其間會發亮，而當 forever 按鈕發亮時只須再點選一次即可結束其運行的狀態。

Slider 用於調整輸入數值，StarLogo TNG 中有相應程式塊 slider，接上程式塊 shared number，便可於控制面板產生 Slider，程式塊 shared number 的命名即為控制面板上 Slider 的名稱，同時亦會產生一組能使此變數供其他程序使用的程式塊，另外，Slider 的數值範圍可直接於控制面板上進行設定。

當決定某項情況是否發生或是否納入考慮時可使用 Switch，在 StarLogo TNG 中可利用 run once 結合 set shared boolean 造成相同效果，要產生 set shared boolean 前必須先宣告一個 shared boolean，宣告方法為拉出一個 shared boolean 的程式塊放置在任意區塊，最後對 run once 程式塊重新進行命名，以點選按鈕的方式對預先設定的布林值做改變，來達到與 NetLogo 的 Switch 一樣的結果。

Chooser 可藉由下拉選單設定不同情況，於 StarLogo TNG 中並無發現相應的程式塊，它的移轉方式與 Switch 十分相似，只是把 set shared boolean 改成執行 procedure，procedure 內為該情況下之條件設定，這樣的作法即為把 Chooser 中的各種情況分成多個按鈕，藉由按鈕的點選造成與選取動作相同的效果。

Monitor 與 Plot 為數據呈現的部分，Monitor 會產生顯示數值的方塊於控制介面，有相應程式塊 monitor，Plot 則產生數值動態變化之圖表，亦有相應程式塊 line graph、bar graph，皆與內容形式為數值之程式塊結合即可，其中 monitor 只能接一個程式塊，而 line graph 及 bar graph 可與多個數值結合。

3.3 移轉範例

為更清楚解釋指令對照與控制介面的轉換，此節將以流浪狗模擬系統[18]的移轉為範例，對照其於 NetLogo 與 StarLogo TNG 環境下的程式碼以及產生之結果(圖 1 與圖 7)，並對上兩節所整理出來的移轉方法進行對應與說明。



圖 1 NetLogo 流浪狗問題模擬系統

建置一個模擬系統，首先要對其模擬環境進行設定，在 StarLogo TNG 中，特別為系統設置部分設計了 setup 程式塊(如表 5 之內容所示)，而在執行部分另有 forever、run、run once，這些程式塊會自動於模擬呈現介面(Spaceland)產生相應的控制項，供使用者控制模擬系統，此部分可參考 3.2 的 Button。

NetLogo 中部分程式指令會被 StarLogo TNG 進行改寫或結合成一單位的程式塊，如圖 2 的對照所示，將左邊 NetLogo 的程式指令(設定 X 與 Y 座標為任意 X 座標、Y 座標)簡短地以 scatter 代表，這部分可參考表 2 的相異指令名稱對照表。

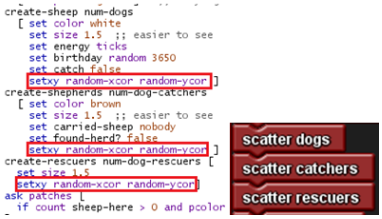


圖 2 隨意散布 agent 的程式寫法對照

完成了模擬系統設定，接下來要對系統的事件進行設計。經觀察發現，NetLogo 中程式架構主要以函式(function)組合而成，由 to 後接函式名稱(圖 3 中函式名稱為 wiggle)為一個函式的開頭，最後以 end 結束函式內容，需要運用該函式時，在執行函式中寫入函式名稱即可。



圖 3 wiggle 函式對照

我們可以根據事件，將內容分成多個函式，圖 3 的 wiggle 函式可使物件進行左右擺動的行為，在 StarLogo TNG 中，可以使用 procedure 這個程式塊進行函式編寫，每個 procedure 會自動產生如圖 3 右上角的程式塊，可與執行部分的程式塊連結，讓 procedure 中的內容得以運行。

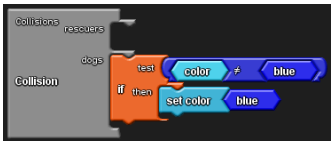


圖 4 StarLogo TNG 中偵測碰撞的程式塊

流浪狗問題模擬系統中有一事件為動保團體將流浪狗結紮並於原地放養，在此事件中會使用到 StarLogo TNG 的程式塊 Collision，碰撞偵測，動保人士一旦接觸到狗便會替狗結紮，圖 4 範例中將已結紮的流浪狗顏色設為藍色。程式塊 Collision 為前面所提到，NetLogo 程式指令被 StarLogo TNG 結合成一單位程式塊的例子。

在 NetLogo 中解決碰撞偵測問題時，會倚靠 patch 進行判斷，以指令 *agent*-here 編寫，對周遭 8 塊 patch 上的 agent 進行偵測，但是在 StarLogo TNG 裡，會依所建立的 agent 項目，自動倆倆產生一個 Collision 程式塊，使用者只需要選擇進行碰撞的對象，而後對碰撞所造成的結果進行設定即完成。



圖 5 Slider 控制項之對照與 StarLogo TNG 中 Slider 程式塊

除了程式部分，可與模擬系統進行互動的控制介面也是建置的重點，圖 5 下方紅色區塊為編輯 Slider 的程式塊，須與粉紅色的 shared number 程式塊結合才能出現對應的 slider 於控制面板上(圖 5 中)，可做數值變化的調整，面板上 slider 的命名將隨著粉紅色程式塊的名稱做變化。

相對於 StarLogo TNG 的自動產生控制項，NetLogo 必須要在控制面板上自行創建完 Slider(圖 5 上方)後，於其上按右鍵，叫出編輯視窗，輸入參數名稱以及設定數值範圍，須注意在程式碼編寫部分要對參數名稱進行全域變數宣告，否則便無法進行連結，以上可對照著 3.2 的 Slider 部分進行理解。

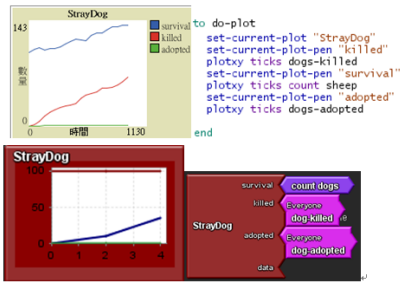


圖 6 折線圖對照

模擬系統中產出的各項數據亦是分析的素材，StarLogo TNG 在這方面亦有能自動產生相應圖表的程式塊，而 NetLogo 同樣需要再從編輯視窗中進行程式連結以及各數據呈現方式的設定。從圖 6 的呈現，StarLogo TNG 在程式碼的編寫上明顯地較 NetLogo 簡單、直覺。圖 6 的內容為流浪狗模擬系統之控制介面的折線圖，可參閱 3.2 的最後一段 Plot。

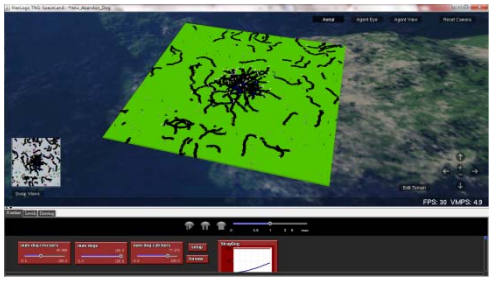


圖 7 StarLogo TNG 流浪狗問題模擬系統

由模擬環境設定開始，接著將模擬系統中的事件內容分割成一段段函式進行編寫，而後產生能影響系統的控制項以及模擬結果呈現的圖表。3.3 之內容以流浪狗問題模擬系統作為輔助，依據建置模擬系統的大致流程進行說明，希望可以幫助使用者了解 3.1 與 3.2 所整理之規則，在移轉的過程中更迅速、更輕鬆。

4. 結論與未來展望

由模擬學習(Simulation-based Learning)與從設計中學習(Learning by Design)兩個理論可推知，學習者能藉由建置與使用模擬系統，在其中投入高度的專注力，進而達到將所學習之概念內化的效果；另一方面，有鑑於視覺化程式語言的易讀性以及程式編寫上的容易性，搭配著色彩繽紛的程式塊，還有立體的模擬呈現方式，可以增加使用者在學習上的樂趣。根據以上兩點，本研究將 NetLogo 中的模型移轉至 StarLogo TNG 中建置，並將移轉過程中所獲得之經驗進行整理，產生部分指令的對照範例以及模擬系統之控制項目的轉換方法，同時帶入流浪狗模擬系統範例，對移轉方式進行解釋，期望以上移轉規則能幫助其他曾經在 NetLogo 的使用中遭遇程式障礙的學習者，轉而以 StarLogo TNG 做為模擬系統建置工具，為他們提供一份可依循的模式，便於完成模擬系統的移轉，讓 StarLogo TNG 中的模擬系統可以日漸豐富，更進一步使得學習者在 StarLogo TNG 中進行更有效率與輕鬆的模擬學習。

致謝

本研究承蒙臺灣行政院國家科學委員會專題研究計畫贊助，計畫編號：NSC 100-2628-S-024-001-MY3，以及計劃贊助，計畫編號：NSC 101-2511-S-024-007-MY2。

參考文獻

[1] Fanning, R. M., & Gaba, D. M. (2007). The role of debriefing in simulation-based learning. *Simulation in Healthcare, 2*(2), 115-125.

[2] Horton, W. (2012). Games and Simulations: Learning by Playing and Pretending in Virtual Worlds. *E-Learning by Design, 2nd Edition*, 323-398.

[3] Kolb, D. A. (1984). *Experiential learning : Experience as the source of learning and development* (Vol. 1). Englewood Cliffs, NJ : Prentice-Hall.

[4] Landriscina, F. (2013). Simulation-Based Learning. In *Simulation and Learning*(pp. 99-146). Springer New York.

[5] 蕭碧茹、洪振方。2000。《案例式推理與科學教學》。*Chinese Physics*, , 3.2： 57-74.

[6] 鄭宇樑。2006。《問題導向學習的課程與教學》。*致遠管理學院學報*，(1), 177-195.

[7] Kolodner, J. L. (1997). Educational implications of analogy : A view from case-based reasoning. *American Psychologist, 52*(1), 57-66.

[8] Gee, J. P. (2004). Learning by design: Games as learning machines.*Interactive Educational Multimedia*, (8), 15-23.

[9] 黃志豪。2006。《「從設計中學習」與網路學習社群對學習成效關係之研究》。臺南大學資訊教育研究所碩士論文。

[10] Kolodner, J. L., Gray, J., & Fasse, B. B. (2003). Promoting transfer through case-based reasoning：Rituals and practices in learning by design classrooms.*Cognitive Science Quarterly*, *3*(2), 119-170.

[11] Tisue, S., & Wilensky, U. (2004, May). NetLogo：A simple environment for modeling complexity. In *International Conference on Complex Systems* (pp. 16-21).

[12] Sklar, E. (2007). NetLogo, a multi-agent simulation environment. *Artificial life,13*(3), 303-311.

[13] Wendel, D. J. (2006). *Design and editing 2.5-dimensional terrain in StarLogo TNG* (Doctoral dissertation, Massachusetts Institute of Technology).

[14] Thiele, J. C., Kurth, W., & Grimm, V. (2011). Agent-and individual-based Modelling with NetLogo：introduction and New NetLogo Extensions. *Die Grüne Reihe, 22*, 68-101.

[15] McCaffrey, C. (2006). StarLogo TNG： the convergence of graphical programming and text processing. *Massachusetts Institute of Technology Master's Thesis*.

[16] 朱江、伍聰。2005。《基於 Agent 的計算機建模平台的比較研究》。*系統工程學報*，20(2)，頁 160-166。

[17] Chang, S. K., et al. (1999).Future of visual languages. IEEE SYMP VISUAL LANG PROC,58-61.

[18] 張智凱、郭文鱗、王士瑋、李詩婷、林育伶、何昱穎 (2011)。建立探究學習的模擬環境：以流浪狗問題為例。第七屆數位內容國際學術研討會 (ICDC2011)，臺灣。

多人腦波遊戲系統架構設計探究
The Study of Architecture Design about Multi-player Brain Computer Interface Game System

王曉璿　　紀明良　　林含諭
國立台中教育大學數位內容科技學系
hswang@mail.ntcu.edu.tw

摘要

近年來，隨著科技的日新月異，在大腦人機介面裝置(Brain Computer Interface, BCI)之應用有不少的突破與進步，惟獨較少研究針對多人腦波遊戲進行探討。為了能達成多人線上腦波遊戲的目標，本研究結合大腦人機介面裝置、多人連線等技術，開發一套基於多人腦波偵測與遊戲的多人腦波遊戲系統，遊戲的模式從基本的「單人練習」模式，擴展出可供多人線上即時互動的「多人練習」與「雙人競賽」模式，並經由實際系統測試，提供相關未來多人腦波遊戲系統開發的參考與建議。

關鍵字：大腦人機介面、腦波、多人遊戲、MindSet。

Abstract

The purpose of this study is using the Brain Computer Interface (BCI) devices to develop a multi-player BCI game system (MBCIGS). The BCI devices in this study uses MindSet as game equipments, Electro Sever as sever platform, and Flash software as client to develop a system. So, in order to achieve multi-player interact each other, the MBCIGS includes two skills that are the multi-user management system and three modes of BCI games.

Keywords：Brain Computer Interface, Brainwaves, Multi-player Game, MindSet

1.前言

近年來，在資訊科技的蓬勃發展下，大腦人機介面(Brain Computer Interface, BCI)技術有很大的進展與突破。發展至今十餘年的大腦人機介面，隨著科技的進步，在傳統上用來量測腦波的機器不再局限於空間和大小的限制，而是著重於使用的方便性與舒適性。最初，大腦人機介面的主要目的是幫助殘疾人士，使他們透過大腦傳遞指令，不需要依靠周圍神經和肌肉就能與外界溝通[1]；現今已有許多研究將大腦人機介面技術加以應用，將其裝置作為新的輸入設備，並利用 MindSet 腦波意念耳機為研究工具，應用於娛樂或學習用途。因此本研究主要結合腦波偵測設備以及多人技術，開發以腦波偵測為基礎的多人線上互動系統，期能提升此方面的運用經驗與效益。

2.文獻探討

2.1 大腦人機介面

大腦人機介面(Brain Computer Interface, BCI)指的是經過大腦的運作，能夠用意念來控制特定裝置。根據第一次國際腦機介面會議的定義為「腦機介面提供使用者一個與外界溝通的替代管道，而不需要依賴周圍神經及肌肉當媒介」[2]。大腦人機介面裝置系統其基本架構有三個部份[3]，分別為訊號的接收(Signal Acquisition)、訊號的處理(Signal Processing)及訊號的輸出(Device Commands)。如圖 1 所示：

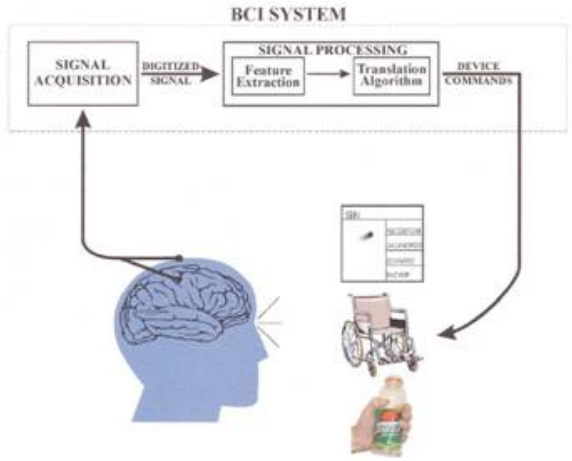


圖 1 腦機介面裝置的基本架構

早期的應用主要為身體不便的人，提供另一種溝通介面，如電子輪椅、電子義肢等，偏向於醫療方面；後期隨著應用領域更加廣泛，目前已有技術運用駕駛汽車中。

2.2MindSet 腦波意念耳機

MindSet 腦波意念耳機是美國 NeuroSky 公司開發的一種腦電波設備，為非侵入性的量測腦波方法，可以測量出人體的專注和放鬆狀態，它的準確度與價值四萬美元的醫療設備 Neuroscan 腦波儀有 96%的相似度[4]。

基於大腦人機介面技術，MindSet 帶有一個乾電極傳感器放在頭部的前額處，參考電極和電路接地系統放在左耳處，用來採集大腦產生的生物電信號(α、β、γ、δ、θ 波)，並將這些信號送入至 ThinkGear™晶片，使混雜在信號中的噪音進行濾除，最後，透過 NeuroSky eSense™專利演算法解讀出使用者專注及放鬆狀態的 eSense™參數，再經由藍芽輸出到電腦、手機等裝置[5]，完成腦波訊號的偵測。如圖 2 所示：

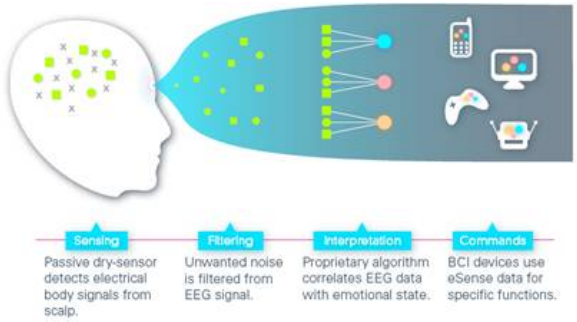


圖 2 MindSet 腦波意念耳機運作機制

2.3 多人遊戲

多人遊戲為玩家透過伺服器及通訊協定，在遊戲中直接和其他玩家進行互動[6]。在網路連線中，用戶彼此間主要可以藉由點對點架構(Peer to peer, 簡稱 P2P)及主從式架構(Client-Server)兩種方式來達到互動與同步。點對點架構在任何一個用戶端都是其他用戶端的伺服器，不僅用戶可以互相傳遞訊息，也不需要透過特定伺服器來傳遞資料，但用戶數過多時，此架構很可能讓子網路超載。主從式架構則是區分用戶端和伺服器端，屬於集中管理的網路連線架構，單一用戶傳送資料至伺服器，再經由伺服器傳送資料至各個用戶。此種架構又可分為輪詢(Polling)和持續性的伺服器連結兩種方式，前者為不斷地詢問伺服器有無更新資料，會很佔頻寬；後者則有 Socket 伺服器，用戶端與 Socket 伺服器建立連結後，會形成一個持續性的連結，但當無事件發生時，不會佔任何的頻寬。

Socket 伺服器是一台存在於遠端的實體伺服器，此伺服器會等待用戶端連結請求，伺服器接受請求後，就能在用戶之間傳遞訊息[7]。常見的 Socket 伺服器有 ElectroServer、SmartfoxServer、Red5、Union 和 Adobe Flash Interactive Server 等。在開發多人遊戲時，必須要考量到採用哪種方式去決定遊戲的決策權，否則便會影響遊戲的結果。遊戲的決策權分成用戶主控型(Authoritative Client)及伺服器主控型(Authoritative Server)兩種。

2.4 總結

回顧過去的文獻發展，大腦人機介面技術從醫學方面發展至電玩遊戲應用，在近幾年新的技術加值下，已有許多研究案例將 MindSet 裝置作為遊戲的設備，使用腦波意念訊息與使用端系統進行互動，有別於用滑鼠、鍵盤或是搖桿控制，帶給使用者新奇的體驗。同時配合多人遊戲設計環境的成

熟，如何將腦波訊號互動介面、使用者遊戲學習內容與多人互動環境進行結合應用，將是預期可提供學習者或使用者新的學習體驗與學習效益，因此，本研究嘗試發展多人腦波遊戲系統，以提供未來多人互動娛樂與學習的應用參考。

3.系統架構與設計

3.1 系統目標

針對文獻探討，本研究主要設計多人腦波遊戲系統，提供使用者即時觀測自己腦波狀態，並能進行線上多人腦波訊息偵測，以及多人腦波互動遊戲功能，以達成結合腦波訊號偵測與多人互動遊戲介面設計功能。本系統在腦波互動遊戲規劃中設計為「單人腦波互動練習」、「多人腦波互動練習」和「雙人腦波互動遊戲競賽」三種模式，供使用者進行腦波互動練習與多人競賽遊戲進行。在遊戲進行中，透過點選遊戲中的物件，系統就會依據玩家當時腦波專注(attention)或放鬆(meditation)的數值而產生不同的變化效果。除了即時偵測和即時互動的功能之外，本系統也使操作環境更簡單易懂，並提供文字傳遞訊息，使得多人互動性連結更為快速有效。

3.2 系統運作模式

本系統運作流程為主要先啟動使用者配戴的MindSet 腦波意念耳機、藍芽與 ThinkGear Connector 連線設定，然後透過 MindSet 傳感器擷取使用者的腦波訊號，並利用藍芽連線將腦波訊號數位化及傳送到個人及多人互動遊戲系統。當使用著進入多人腦波互動遊戲系統後，Client 端會與 Server 端進行遠端連線登入，之後所有的訊息交換與同步動作都將透過 Client 端與 Server 端將網路訊息封包傳給各個用戶，使得每個用戶能透過本系統進行多人腦波遊戲和觀測多人腦波即時動態。

3.3 系統架構

本系統採用 NeuroSky 公司提供的 API，將 MindSet 腦波意念耳機與互動遊戲軟體連結，平台連線技術採用主從式架構(Client-Server)；後端伺服器使用 ElectroServer 5，目前使用可同時連線 25 位使用者的版本；用戶端平台使用 Flash CS6 ActionScript 3 的程式語言撰寫；遊戲的決策權則屬於用戶主控型，作為遊戲系統的平台。

其多人系統架構可分為區域(Zone)、房間(Rooms)與使用者(Users)。區域是房間的集合，「多人腦波遊戲區」為本系統唯一的區域，區域內主要又分成「大廳」及「遊戲大廳」兩個房間，遊戲大廳內有三個房間可讓玩家進行遊戲，即遊戲規劃中的三種模式，同個房間內的玩家可以互相交談聊天，而各個房間內則會有一群使用者。如圖 3 所示：

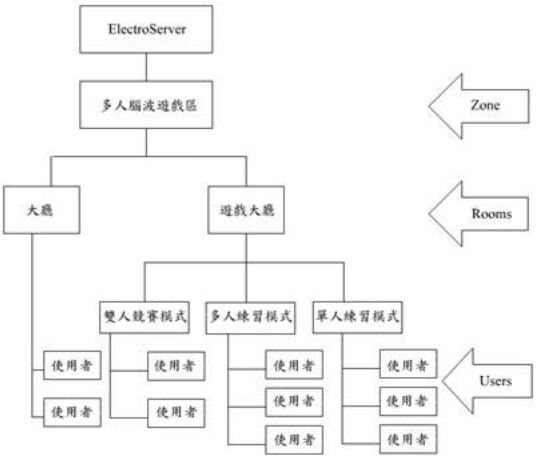


圖 3 系統架構圖

3.4 系統功能設計

本系統建置的功能主要規劃成「使用者登入介面」、「大廳」與「遊戲大廳」三個部分。在使用者登入介面中，分為「輸入帳號區」與「使用者登入訊息區」，分別用為提供使用者登入本系統，其帳號可自行輸入喜愛的名稱，限制 7 個字元，無須經過註冊；以及顯示目前使用者與系統連線的狀況。本系統也加以運用 Electro Server 內建過濾功能，在伺服器端進行帳號過濾設定，直接排除不雅的帳

號名稱。

當使用者經過登入認證後，就會進入到本系統的「大廳」房間，此房間規劃分成「房間資訊區」、「使用者資訊區」、「輸入聊天訊息區」、「系統訊息與玩家聊天區」和「進入遊戲大廳」五個區塊。房間資訊區是用來顯示伺服器上所有使用者目前所存在的房間資訊；使用者資訊區是所有線上使用者的資訊清單，包含帳號、專注值、放鬆值及意念耳機的訊號值；輸入聊天訊息區是線上使用者互相交談的管道；系統訊息與玩家聊天區是系統和使用者的互動與使用者彼此間的互動，包含使用者登入系統的問候語、使用者進出房間狀況和使用者討論聊天的文字內容訊息；進入遊戲大廳則是協助玩家進入遊戲練習與競賽的地方。

當使用者進入遊戲大廳，即能選擇「單人練習」、「多人練習」與「雙人競賽」這三種遊戲模式進入遊戲。在進入遊戲之前，會有遊戲說明影片以及介紹操作方法，玩家如果不進行遊戲，點選「離開遊戲大廳」即可返回至大廳。

在「單人練習」的遊戲模式中，主要訓練單一個玩家的專注與放鬆的控制情形，將其規劃成「紅色球」、「藍色球」、「專注數值條」及「放鬆數值條」。當玩家進入遊戲後，專注和放鬆的數值條分別會顯示玩家當下的狀態，玩家可以使用滑鼠點選紅色球與藍色球，這兩顆球便會隨著玩家當前的專注和放鬆進行漂浮，再點選一次球後則會停止漂浮。

在「多人練習」的遊戲模式中，主要訓練多個玩家的專注與放鬆的控制情形，將其規劃成「木桶」、「藍色球」、「專注數值條」及「放鬆數值條」。在遊戲的設定規劃中，可進行多人遊戲互動，當玩家進入遊戲後，玩家可以使用滑鼠點選木桶與藍色球，木桶會隨著玩家當前的專注進行著火燃燒，而藍色球則隨著玩家當前的放鬆進行漂浮，再點選一次球後便會停止。

在「雙人競賽」的遊戲模式中，主要規劃為雙人專注力競賽遊戲。當玩家進入遊戲後，可以開始蹺蹺板遊戲，點選人物後便隨著玩家當前的專注與對手的專注進行比較，在比賽過程中，人物會隨著專注高低進而升起或下降。

當進入任意一個遊戲模式之中，每個模式裡都會有使用者資訊區、輸入聊天訊息區、離開遊戲這三項功能。使用者資訊區會顯示目前同樣在該模式中的所有玩家；輸入聊天訊息區可以和同樣在該模式中的玩家進行交談；離開遊戲則是返回至大廳。

4.系統展示

本系統架構分成 7 個區塊，分別為「系統登入運作模式」、「使用者列表運作模式」、「房間資訊列表運作模式」、「系統訊息與玩家聊天區運作模式」、「單人練習運作模式」、「多人練習運作模式」及「雙人競賽運作模式」。各個模式皆有其分工合作的運行方式，使本系統能夠順利運作。

本研究所發展的多人腦波遊戲系統中，操作流程為使用者進入登入頁面後，經過系統驗證後便來到大廳，之後進入遊戲大廳選擇遊戲模式即可進入遊戲，當遊戲結束後，則會返回至大廳。

4.1 大廳展示

初次進入大廳，將會顯示歡迎字幕迎接使用者，此後使用者進出房間都會在此區顯示訊息；而利用多人連線技術，Client 端將資料傳送給 Server 端，Server 端再將資料傳給每位使用者，使得透過「使用者列表區」，所有使用者皆可觀測到線上其他人的專注與放鬆的即時狀態，進而達到多人腦波即時觀測之目的。如圖 4 所示：



圖 4 系統大廳介面展示

4.2 遊戲大廳展示

當使用者從大廳點選進入到遊戲大廳，遊戲大廳將提供三種遊戲模式給玩家選擇。如圖 5 所示：



圖 5 遊戲大廳介面展示

4.3 單人練習模式展示

當使用者進入單人練習模式遊戲中，會有一段遊戲操作說明影片，介紹相關知識後，即可進入單人練習模式遊戲。如圖 6 所示：

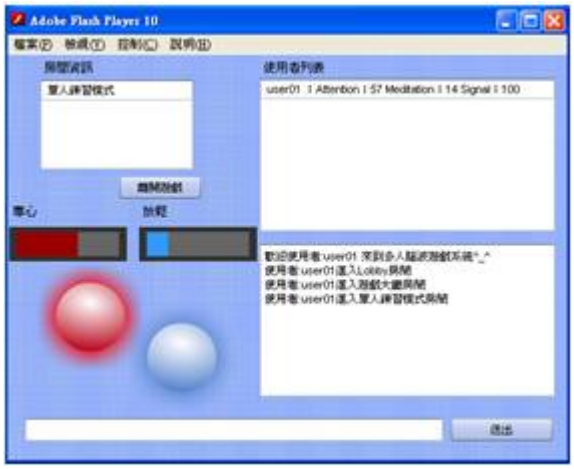


圖 6 單人練習介面展示

4.4 多人練習模式展示

當使用者進入多人練習模式遊戲中，會有一段遊戲操作說明影片，介紹相關知識後，即可進入多人練習模式遊戲。如圖 7 所示：



圖 7 多人練習介面展示

4.5 雙人競賽模式展示

當使用者進入雙人競賽模式遊戲中，會有一段遊戲操作說明影片，介紹相關知識後，即可進入雙人競賽模式遊戲。如圖 8 所示：



圖 8 雙人競賽介面展示

5.結論與建議

5.1 結論

本研究整合 MindSet 腦波意念耳機、Flash 遊戲系統與 Electro server 伺服器於系統平台，建構一套多人腦波遊戲系統，主要特色為能夠即時偵測個人與多人腦波訊號，並進行多人腦波訊號與遊戲介面系統互動與遊戲競賽。經由使用者實際系統使用發現，對於新介面應用的體驗具有新奇性，同時經由本研究設計的腦波互動遊戲中，讓使用著能依據自身的腦波狀態，調整自我的專注度與放鬆度，對

未來學生使用著的學習專注力具有潛在的發展應用效益。

5.2 建議

依據本系統的實際測試發現，未來可針對使用者的特性發展多人腦波互動學習遊戲，以系統化提升學習者的學習專注力。同時記錄不同環境下使用者的腦波資料變化狀況，以作為數位遊戲領域的內容發展規畫修正參考。

配合行動載具的快速發展與使用，後續研究建議朝向不同媒介平台發展，例如：手機即時腦波互動遊戲、個別化適性腦波學習系統、以及多人行動腦波互動遊戲，以提升腦波介面與行動載具連結應用效益。

參考文獻

[1] Pfurtscheller,G., Guger,C., Müller,G., Krausz, G., & Neuper,C., “Brain oscillations ontrol hand orthosis in a tetraplegic,” Neuroscience letters, vol. 292, pp.211-214, 2000.

[2] Wolpaw, J. R., Birbaumer, N., Heetderks, W. J., McFarland, D. J., Peckham, P. H., Schalk, G., Donchin, E., Quatrano, L. A., Robinson, C. J., & Vaughn, T. M., “Brain-computer interface technology : A review of the first international meeting,” IEEE transactions on rehabilitation engineering, vol. 8(2), pp.164-173, 2000.

[3] Wolpaw, J. R., Birbaumer, N., McFarland, D. J., Pfurtscheller G., & Vaughan, T. M., “Brain-computer interface for communication and control,” Clinical Neurophysiology, vol. 113, pp.767-791, 2002.

[4] NeuroSky, Research, 2011 Retrieved from http://neurosky.com/Academics/Research.aspx

[5] NeuroSky, Thinkgear Chipsets, 2011 Retrieved from http://neurosky.com/Business/ThinkGearChipsets.aspx

[6] Kim, K.H., Park, J.Y., Kim, D.Y., Moon, H.I., and Chun, H.C., “E-lifestyle and Motives to Use Online Games,” Irish Marketing Review, vol. 15(2), pp.71-77, 2002.

[7] 陳亦慧譯, 2010, ActionScript多人互動遊戲與虛擬世界製作, 台北市, 上奇資訊股份有限公司。

在平板電腦上漢字部件悅趣學習系統建置

許政穆　邱孝義　葉玭瑄
國立嘉義大學資訊工程學系
{hsujm, s0983001, s0983025}@mail.ncyu.edu.tw

摘要

漢字部件教學是一種以部件組裝的漢字單字學習方式，能幫助學習者以部件圖像進行漢字單字學習認知過程，特別是初識漢字學習者有其學習成效。然而以漢字部件教學進行學習識字需要合適的媒體介面，以協助部件組裝識字。平板電腦攜帶方便且具直覺操控特性，隨著平板電腦逐漸普及，已有不少以平板電腦作為教學輔具與學習平台、甚至電子書與電子書包載具等應用，皆有不錯教學與學習成效。本論文將利用平板電腦的直覺觸控操控特性，設計一套以漢字部件學習的悅趣學習系統，透過平板電腦進行漢字部件拼接識字，並以遊戲模式進行同儕學習競爭，讓學習者能於遊戲中學習漢字識字。

關鍵詞：漢字部件教學、平板電腦、悅趣式學習

Abstract

Chinese component instruction is a method to learn the Chinese words through the combination of graphical components. It is especially useful for the beginners of learning Chinese words by using the Chinese component instruction. Nevertheless, it is necessary to prepare a user-friendly interface to easily learn the Chinese words through Chinese component instruction. A Tablet PC equipped with a touch screen can provide intuitive and touchable operations to assist the learners to easily combine the various word components to spell Chinese words. Therefore, this paper will try to design and implement a game-based combination of word components for Chinese radical recognition on Tablet PCs. Through the learning feature of game-based learning, the learners will compete against other learners to enhance their learning effects of Chinese radical recognition via the combination of word components.

Keywords: Chinese Component Instruction, Tablet PCs, Game-based learning.

1. 緒論

閱讀是人類用以傳遞訊息技能，透過閱讀人們能夠理解事務與建構知識，甚至可作為人類間訊息傳達方式。為了要與新事物與不斷變動的環境做接軌，因此閱讀已轉變成人類適應群體生活所不可或缺的一項重要能力，而單字學習是構成閱讀與寫作的重要基礎。在華人世界中，有許多漢字教學法，主要如字源、字根與部件等教學，其中以部件教學法的成效較為顯著。

漢字部件是指由筆劃組成具有組配的構字單位，可透過部件組合來構成漢字。對於漢字構成部件及部件配置位置來看，大多可藉由六書中組字法的形聲字來解釋。在中文漢字中約 81%的漢字為形聲字[9]，故在學習中文漢字歷程中，形聲字構字原則的了解也成為一個重要課題。由於漢字部件教學與形聲字是相輔相成，會成為一項具有教學優勢的漢字教學工具。

目前已有多套漢字部件教學系統也已實作於電腦上，透過電腦輔助教學(computer assisted instruction，CAI)機制來輔助漢字教學[5]。然而電腦正朝向迷你、攜帶便利方向發展，例如平板電腦和智慧型手機，而此類裝置的攜帶方便、直覺觸控操作方式、Wi-Fi/3G 無線上網等特點，很適合作為下一代 CAI 電腦輔助教學平台。在[1]中已將平板電腦結合建構鷹架活動於輔助國小英語主題教學上與主題式教學課程促進多原技能整合[2]，其研究結果指出平板電腦的可攜特性有助於解決原先教學過程中跨時間與空間問題。參與研究教師亦指出平板電腦易操作、即時互動、方便存取等特性，確實可增進學生學習動機。然而在學習過程，即使有了最新學習科技設備導入，要使學習者全心全意持續投入於課程學習活動中是件不大可能事情。就如同工廠作業員一樣，每天面對著同樣產線流程、同樣作業手續；同樣對人而言，因為只要長時間面對於同一事物，終究會有興趣疲乏一刻、失去熱忱，甚至是開始產生抗拒。因此對於事物看法的調適是很重要，或者以異曲同工方法去達到同一項目的。

近年來，悅趣式學習[10][11]是一種新式教材設計與自學方式，其主要是導入遊戲的愉悅與樂趣，來進行教學與學習，以達到教育目的。其作法是提供學習者在充滿樂趣與挑戰的環境，達到「沉浸」之效，進而從中達到提高學習動機與學習歷程支持。雖然學習方式是以遊戲為主，但其遊戲方式又與平常所見之遊戲有所不同。悅趣式學習是以遊戲之娛樂性結合教領域之學習的「非休閒遊戲」(serious game)，如此組合方式，便可透過遊戲本身吸引學習者之學習動機，以達到較高效率之整體學習效果。也因為如此設計理念受到認可，已經逐漸成為學習課程設計之趨勢，這也是數位學習的新模式。

綜合上述各項理論之特點，本論文將在平板電腦

上設計一個融入悅趣式學習的漢字部件學習系統，其功能包括同儕互動的部件拼字遊戲競賽模式，透過同儕互動來提高學習動力，也能與同儕分享學習成果，促使學習者能達到「沉浸」之學習效果。

對於本論文架構，第二節介紹相關文獻探討，第三節為本論文所設計的悅趣式漢字部件學習系統之系統架構與實作畫面，最後一節則是結論與未來展望。

2. 文獻探討

2.1 漢字部件教學

所謂漢字部件教學法，可分為兩部分：教材編纂與教學流程設計，在[3]中所介紹教學法依循步驟為：學習詞語、認識單字、掌握該單字的部件、學習字形特點、掌握字形、學習其他單字等循環步驟重複執行擴充字庫；而教材編纂步驟為：統計字頻、列出高頻漢字、找出高頻部件、組成單字、組成詞語、編成課文或是補充教材。而此教學法經過多次試驗，已顯示有相當成效。

然而在閱讀障礙相關研究中，有些學者認為閱讀障礙學生在短期記憶及工作記憶能力上有缺陷存在，閱讀障礙學生在有關字的資訊處理過慢，以致於難以達到有效的閱讀理解[4]。因此，如何讓閱讀障礙學生從大量重複練習中獲得自動化的識字技巧是很重要課題。例如圖 1 為典型以漢字部件學習漢字單字的衍伸流程，首先將漢字單字進行部件拆解後，教導部件組字組合教學，進而達到漢字單字學習之效。

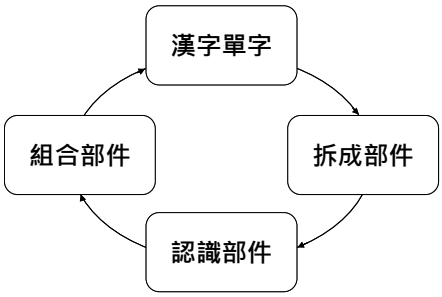


圖 1 漢字部件學習流程

2.2 平板電腦應用於學習與教學

在目前教育現況中，多數中小學教學授課方式仍然是基於老師為中心教授方式，近年來將平板融入教學課程的嘗試者也逐漸增加。以平板電腦結合建構鷹架活動輔助國小英語主題課程學習[1]為例，藉由平板電腦多媒體影音功能，將英語學習的聽、說、讀等學習流程給予適當輔助，甚至能讓學習者順著學習課程中不知不覺具備新式科技操作能力。其實驗結果顯示，將平板電腦融入教學之中，學習者的英語能力、學習認知、學習情意與技能等面向皆持正向肯定態度。而該研究亦指出，平板電腦用於學習課程中可分為學習動機引發、自我學習引導以及即時教、學分享中介等三種角色，假若能適當搭配教育類別 App 應用程式，將可成為教育現場輔助、引導、強化學習之最佳工具，為學習者增加多元自主的學習機會。

2.3 悅趣式學習

以教育理念建構於遊戲之上且具有較教育價值與意義的遊戲，被稱作為「悅趣式學習」。遊戲設計的初衷，主要是讓學習者們透過遊戲方式競賽，使學習者能從中獲得學習效果[6][7]。近幾年來，把遊戲建構於教育學習方式一直是熱門話題，也在早些時候有研究發現，使用者透過玩遊戲是瞭解自我的最好方式[8]。由於遊戲是一種現實的模擬，透過遊玩遊戲，人可以較容易的與他人進行互動。透過遊戲，人可以為了達成較高的目標或成就而有效的自我處理個人需求和解決問題。即使使用者在遊戲中失敗了，使用者也不會因此輕易受到心靈挫敗，較常見的反而是激起競爭的意識，促使自己學習得更多，再次參與競賽，直至達到目標。

在[10]中，其研究以迷宮與中文詞句組合來構成遊戲主軸，配合探索性質的任務以吸引學習者興趣，並搭配學校老師課程與可編輯題庫，實作出變化性十足的中文詞句迷宮遊戲，使其讓學生達到「沉浸」之效果。另外[11]也將認識昆蟲等想法透過遊戲引擎實作出來，其中配置完善劇情、可愛角色與場景設計、冒險挑戰等種種要素，用以引出學生好奇心，給予學生十足的學習動機。因此融入悅趣遊戲等因素來建構教學，確實能促使學習者的學習動機提升。

依據上述所列，漢字部件教學是由從一系列步驟重複循環所構成，如學習詞語、認識單字、掌握該單字的部件、學習字形特點、掌握字形及學習其他單字等。假若將漢字部件教學透過平板電腦的簡單易懂且直覺的觸控操方式，讓學習者更能直接體會漢字部件拼字的學習精要，相信在漢字教學會有相當大的教學助益提升。此外，加入悅趣學習的同儕競遊模式，不僅可讓學習過程更具趣味，更能引發學習動機，讓學習者浸潤於遊戲之中進行學習。因此，本論文將在平板電腦上建置一套具同儕競遊的漢字部件悅趣學習系統用以輔助教師漢字部件教學與同儕間競遊的漢字部件學習。

3. 系統設計

3.1 漢字部件建構

本論文所用漢字部件總數為 439 個，主要是參考國立臺灣師範大學所建置「漢字、部件五項查詢平台」網站[12]所設計。該網站提供相當完整「部件查詢系統」、「短文析字部件拆解系統」、「真字查詢系統」、「假/非字產出系統」、「相似自查詢系統」等，提供不同的部件查詢功能，其中以圖片形式來

顯示無法靠輸入法輸出部件較為特別。此外，其「短文析字部件拆解系統」還提供漢字單字部件拆解結構，共有 11 種類型，可了解漢字部件組合的空間關係結構。然而此 11 類型的漢字部件空間結構，對於謝、倒、並、幸等漢字部件表示並不完備，故本論文自行曾加兩種漢字部件的空間關係結構來補足 11 種結構不足之處，詳細結構如圖 2 所示。在圖中的結構編號 a 至 k 為該平台提供結構，而 p 與 m 為本論文所新增空間關係結構。

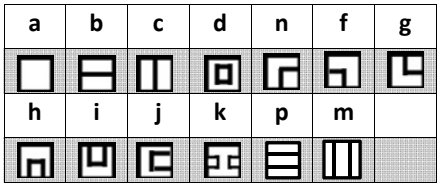


圖 2 空間關係結構圖

表 1 紀錄漢字單字的資料庫

_id	#序號
Sum	部件總數
Number	單字的部件編號結合空間關係結構組成
Word	漢字單字
Frequency	康軒版國小國文課本附加的漢字字頻

本論文目前所建的漢字單字總量約為 1000 筆，參考康軒版國小國文課本所使用的漢字。為了方便系統處理漢字單字與其所對應的漢字部件，以資料庫方式作資料管理，資料庫表單如表 1 所示。除了 Word 欄位是以漢字單字外，其餘部件是以編號組成作為儲存內容。Word、Frequency 的內容來源是康軒版國小國文課本單字，而 Sum、Number 的來源是參考師範大學「短文析字部件拆解系統」來拆解 Word 的內容而得到。例如，『和』字(Word(和))的部件總數為 2(Sum(2))，其所組成的部件編號分別為 220(禾)與 063(口)，而其空間關係結構為 c，故在資料庫內儲存值為 220c063 (Number(220c063))，圖 3 為『和』字的漢字部件組成空間結構關係。

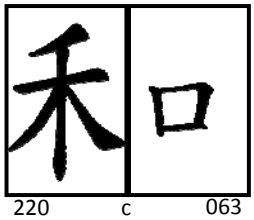


圖 3『和』字與其部件空間關係結構與編號設計

3.2 系統架構

本論文所設計的漢字部件學習系統主要分成兩部分：漢字部件學習伺服器端與平板電腦上漢字部件學習客戶端。伺服器端一次可以對應兩台客戶端的連線請求，將兩台客戶端匹配並形成漢字部件拼字遊戲競賽。客戶端透過伺服器端的中介溝通來進行互動式的部件拼字操作，其中伺服器與客戶端之間是以 TCP 進行連線與資料傳輸，而互相傳送資訊訊息格式則以 JSON 方式加以封裝與解析，其系統架構如圖 4 所示。

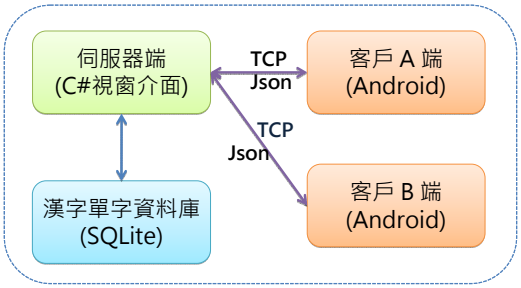


圖 4 系統架構圖

3.3 同儕部件拼字競賽流程

本論文的漢字部件學習系統中，設計了組別競賽遊戲方式，讓學習者分別派分到不同角色的組別，一邊是扮演老師出題角色，而另一邊是學生解題角色，兩邊互相提出部分部件來組成一個漢字單字，最後系統作為中介裁判來根據兩方對於拼組出來的漢字單字是否正確來給予得分，其流程如圖 5 所示。

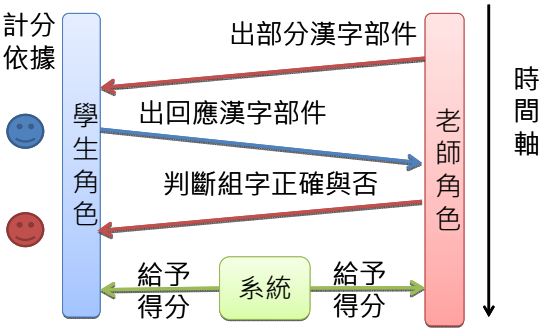


圖 5 分組拼字競賽的一回合流程圖

全競賽的賽程一輪共為 10 個回合，出題的漢字部件題目由伺服器端的資料庫中隨機抽取，然後將題目的漢字單字拆成等分數量漢字部件，再加以參雜非答案之隨機部件，分別指派給兩邊。在設計漢字拼字競賽時，有考慮到角色立場優勢問題，故設置了五回合後交換角色設定，使得兩個小組都能夠輪到老師角色與學生角色，輪流出題與解題。圖 6 為全競賽賽程的總運作流程，其中外部框圈為伺服器端運作流程，而內部框圈為客戶端運作流程。

本論文中的伺服器端除了扮演轉達各個客戶端間的溝通橋樑和管理資料庫的角色外，伺服器還要負責分組拼字競賽的轉播員，也就是可以透過伺

服器的視窗介面，透過投影機將競賽情況投影於布幕上，讓同樣在場而沒參與競賽人員也能清楚知道目前比賽進度與比分為何。此外，伺服器端也須負責測驗紀錄工作，測驗紀錄是將客戶端所傳輸內容記錄且存進資料庫，以利未來解析學習者在競賽期間的識字歷程，透過資料分析能較清楚了解學習者在漢字單字上的學習成長曲線。

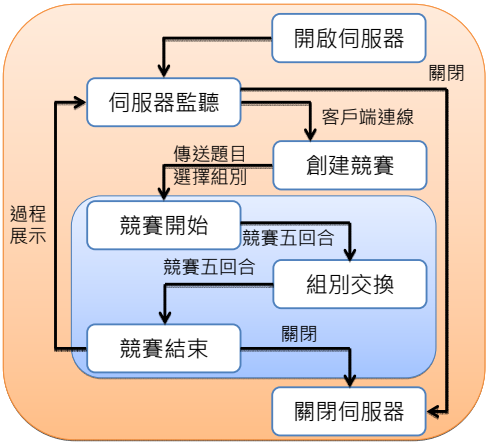


圖 6 全競賽賽程的總運作流程

3.4 系統實作與漢字部件拼字競賽執行過程

本論文所設計的漢字部件學習系統，伺服器端是以 C#語言開發並以 SQLite 作為漢字資料庫，而且在 Android 平板電腦上開發部件學習客戶端供學習者使用。圖 7 為學習者在平板電腦上選擇老師組與學生組的畫面，而圖 8 為伺服器端上顯示參與漢字部件拼字競遊的兩組學習者資訊與所伴演角色。



圖 7 學習者在平板電腦上選擇漢字部件拼字競賽角色設定

圖 9 為扮演學生組的學習者在平板電腦上依據老師組所出的部件從右邊部件清單選取合適部件進行組字競賽，而圖 10 為扮演老師組的學習者評斷學生組依據其所出題部件所出的部件組成漢字正確與否的判斷處理。同樣圖 11 為在學習者所持用的平板電腦上顯示該回合漢字部件拼字的競賽結果畫面，而圖 12 則是在伺服器端上顯示該回合漢字部件拼字的競賽過程畫面。透過伺服器端的畫面顯示，讓尚未參與漢字部件拼字競遊的學習者，能感受到同儕競遊的情境，更能促進學習者參與學習動機與意願。



圖 8 在伺服器端顯示學習者在漢字部件拼字同儕競遊中所選定角色



圖 9 扮演學生組學習者在平板電腦上進行漢字部件拼字畫面



圖 10 扮演老師組學習者在平板電腦上進行漢字部件拼字正確檢查畫面

圖 13 為在學習者所持用的平板電腦上顯示漢字部件拼字競遊的得分結果，圖 14 則是在伺服器端上顯示最終的同儕競遊結果與漢字部件拼字的學習歷程。可透過伺服器端的結果顯示了解該次漢字部件拼字競遊中所拼過的漢字部件與組字正卻與否的過程，由教師再次指導參與漢字部拼字競遊的學習者正確的漢字部件組合。



圖 11 全競賽賽程的總運作流程



圖 12 在伺服器端上顯示學習者進行同儕漢字部件拼字競遊過程



圖 13 在平板電腦上顯示同儕間漢字部件拼字競遊得分結果

4. 結論與未來展望

漢字部件教學法是一個簡而易學的漢字識字學習法，本論文在平板電腦上設計一套融入同儕競遊的漢字部件悅趣學習系統，使學習者透過操作便利的平板電腦，以直覺觸控的拖拉方式進行部件拼組學習。



圖 14 在伺服器端上顯示同儕間漢字部件拼字競遊得分結果與過程中部件拼字學習歷程紀錄

對於本論文所設計的系統，現階段已完成分組拼字競賽，雖然同儕競遊功能完整，但畫面美工與內容呈現仍須加強，未來將加入單人自我學習(self-learning)、漢字連詞強化學習等功能，讓此系統更能符合教師在漢字教學所需。

未來也將尋求小學教師或華語教師合作，透過完整的漢字部件教學的教材設計、同儕部件拼字競遊教學活動等一系列的教學設計，以系統化對本論文所建置的系統進行質量化分析研究，以檢驗本系統在漢字教學上的學習成效。

參考文獻

[1] 王怡萱、楊叔卿、李珮瑩。平板電腦結合建構鷹架活動輔助國小英語主題課程學習，TANET 2012。

[2] 蔣宗廷、楊叔卿、林君徽、張博裕。融入平板至國小主題式教學課程促進多元技能整合，TANET 2012。

[3] 溫瓊怡。電腦多媒體漢字部件教學系統對國小閱讀障礙學生識字學習成效之研究。碩士論文。國立嘉義大學特殊教育研究所。2003。

[4] 廖彩萍。單字呈現的部件識字教學法及以文帶字的部件識字教學法對國小輕度智能障礙學生識字教學成效之研究，碩士論文，國立屏東教育大學特殊教育學系，2007。

[5] 李嘉玲、張裕淇、李佳穎、劉昭麟。結合認知理論之電腦輔助漢字教學遊戲，TANET 2010。

[6] 施力瑋。數位遊戲類型對學習者的影響，ICDC 2012。

[7] M. Prensky, Digital Game-Based Learning, New York: McGraw-Hill, 2007.

[8] 數位遊戲式學習系統，http://web1.nsc.gov.tw/ct.aspx?xItem=14115&ctNode=1031。

[9] 林佩怡。漢字辨識中的部首部件處理歷程：一般與弱讀兒童的比較，碩士論文，國立中正大學臨床心理學研究所，2011。

[10] 陳曉鳳。迷宮多路徑融入國語詞句悅趣學習之設計式研究，碩士論文，國立新竹教育大學數位學習科技研究所，2011。

[11] 陳勇全。國小自然科「認識昆蟲」單元之虛擬實境式悅趣學習設計與成效研究，碩士論文，國立新竹教育大學數位學習科技研究所，2012。

[12] 國立臺灣師範大學。Cool Chinese 能力導向之全方位華語學習計畫 – 漢字部件五項查詢平台(http://140.122.109.78/COOL/)。

圖書館利用教育數位課程系統化設計與發展

劉 杰
行政院原子能委員會核能研究所圖書館
國立臺灣大學圖書資訊學系博士班
jj610026@iner.gov.tw

摘要

隨著時代演進，圖書館的角色逐漸由資訊保存者轉變為資訊中介者，如何將豐富的館藏資源提供給讀者使用便成為圖書館的首要任務之一。在網際網路興起之後，便利的搜尋工具和豐富的電子資源，改變讀者使用圖書館的習慣。然而諸如圖書檢索系統、電子資料庫查詢系統等服務，如果沒有相關使用經驗，確實會出現許多問題和阻礙，因此圖書館利用教育的重要性便不言而喻。本研究採用網路教材系統化設計模式，透過分析、設計、發展、實施與評鑑等階段開發相關課程，以求所開發之「圖書館利用教育」課程能真切符合所需，並發揮數位網路化學習的優勢。希望透過相關課程，讓讀者更瞭解圖書館提供的各項服務，使圖書資源被充分利用，進而增進知識流通。本研究之成果將可提供圖書館或其他機構在課程設計上之參考。

關鍵詞：圖書館利用教育、數位學習、網路教材系統化設計。

Abstract

As time goes by, the role of libraries have changed, from the preserver of information to the mediator. Then, the primary task of libraries is to provide the resources to the patrons. As the popularity of the Internet, the convenient search tools and the rich electronic resources have changed the users' behavior. However, users find it difficult to use the IR system and all kinds of electronic platforms if they have no experience. So, the importance of library-use instruction goes without saying. In view of this, this study used the instructional design model to build "library-use instruction" courses . By way of incurring analysis, design, development, implementation and evaluation phases, we successfully develop such courses in order to meet users' needs. Thus, the resources of library can be fully utilized, and the circulation of knowledge will be enhanced as well. Last, the results of this study can also provide for other course developer as reference materials.

Keywords: Library-use instruction, e-learning, Instructional design.

1. 前言

由於網際網路之普及與資訊科技的進步，學習的習慣也隨之改變。數位學習不受到時間和空間的限制，並可充分發揮電腦多媒體的特性，尤其是在非正式教育的應用上，數位學習更可以發揮其優勢。而自古以來，圖書館是人們獲取知識的主要來源之一，而隨著時代的演進，圖書館的角色逐漸由資訊的保存者轉變為資訊的中介者，如何將豐富的館藏資源提供給讀者使用便成為圖書館的首要任務。在網際網路興起之後，便利的搜尋工具和豐富的電子資源，促使讀者改變使用圖書館的習慣，由實體的圖書館逐漸轉向使用數位資源。然而諸如圖書檢索系統、電子資料庫查詢系統等多元之服務，若沒有相關使用經驗，確實會有許多操作上的問題和阻礙，因此，圖書館利用教育的重要性便不言而喻。

然而，圖書館雖會定期舉辦教育講習，但是礙於場地與時間的限制，並不是所有讀者皆能參與。有鑑於此，圖書館可嘗試採用系統化的教材設計模式，透過分析、設計、發展、實施與評鑑等階段來開發課程，以求所開發之「圖書館利用教育」課程能真切符合所需，並充分利用數位學習的優勢，達到加乘的效果。而在導入數位學習的過程中，教材的設計與開發佔有舉足輕重的地位，唯有針對所教授的課程內容發展適合的教材，才能真正達到「教」與「學」的效果。因此要建構一個數位化的網路學習環境，首先應該瞭解「教學」的本質，然後再來檢視教學環境應包含哪些功能項目。基本上，「教」與「學」是一體之兩面。所謂「教」，是教學者依據學習者的需求將知識傳送出去的行動；而「學」則是有系統的瞭解吸收知識的過程[1]。因此本研究在教材開發上係以網路教學理論為架構進行規劃設計，並以學習者的角度來考量整體教材的建製。希望透過相關課程的增設，讓讀者更瞭解圖書館提供的各項服務，使圖書館資源被充分利用。

2. 文獻回顧

以下將從「圖書館利用教育」與「網路教材系統化設計」兩個面向，探討相關理論與實證研究之結果。

2.1 圖書館利用教育

依據美國圖書館學會圖書館暨資訊科學詞彙的定義，任何一種型態的活動，只要是被設計用來教導使用者有關圖書館的服務、設施、組織、資源及查詢策略等皆可視為圖書館利用教育。其中包含指導一種或多種參考資源的利用，例如：參考服務、圖書館利用講習、書目指導等[2]。換句話說，圖書館利用教育係為透過正式與非正式的教學活動指導讀者如何有效善用圖書館資源[3]。而此定義便為本文所指之圖書館利用教育。

圖書館利用教育可分為三個層次[4]：

(1) 認識圖書館環境：包含介紹圖書館的沿革、組織、環境，簡介服務項目、閱覽規則等，使讀者對圖書館有一個概括性的認識。

(2) 圖書館利用指導：介紹館藏檢索方式、線上公用目錄、電子期刊查詢等，讓讀者學會各種參考資料的取得方式。

(3) 書目指導：指導讀者如何利用圖書館資源進行獨立研究，大多以研究指引、專題選目等方式進行，目的在節省讀者查詢資料的時間。

而圖書館利用教育可以利用多元方式進行。具體來說，常見的方式如下所述[3]：

(1) 參考服務：館員於服務台接受讀者諮詢。

(2) 說明指標：以淺顯易懂文字指引方向、標示操作說明等。

(3) 圖書館手冊：較完整的圖書館相關說明，如閱覽規則。

(4) 研討會、演講：邀請學科專家舉辦研討會或專題演講。

(5) 正式課程：開設課程，有系統地進行教學。

而各種圖書館利用教育進行的方式皆有其必要性及相對應的服務項目，而本研究後續探討之圖書館利用教育主要係針對正式課程而言，此正式課程並非專指學校開設之必修或選修課程，而是泛指經過課程設計，有一定教學目標之教學活動，不論是嵌入於網站中的服務，或是圖書館開設的常態課程，皆在本研究討論的範圍之中。

2.2 網路教材系統化設計

教學設計是解決問題的系統方法，設計者以有系統的步驟，經由一系列的活動，產生並實施各種教學計畫或教學材料，以便從事教學，並有效且經濟地解決教學問題[5]。其中，網路教學系統設計需與教育情境設計融合，其功能設計也需配合網路媒體的特有屬性。而數位化、網路化之課程在發展時有既定之教學設計程序可供依循。一般而言，普遍被接受的模式為 ADDIE 模式，此一模式將教學設計的過程分為分析 (Analyze)、設計 (Design)、發展 (Develop)、實施 (Implement) 與評鑑 (Evaluate) 等五個階段。而此五階段的內涵大致可以歸納如下圖所示[6]：

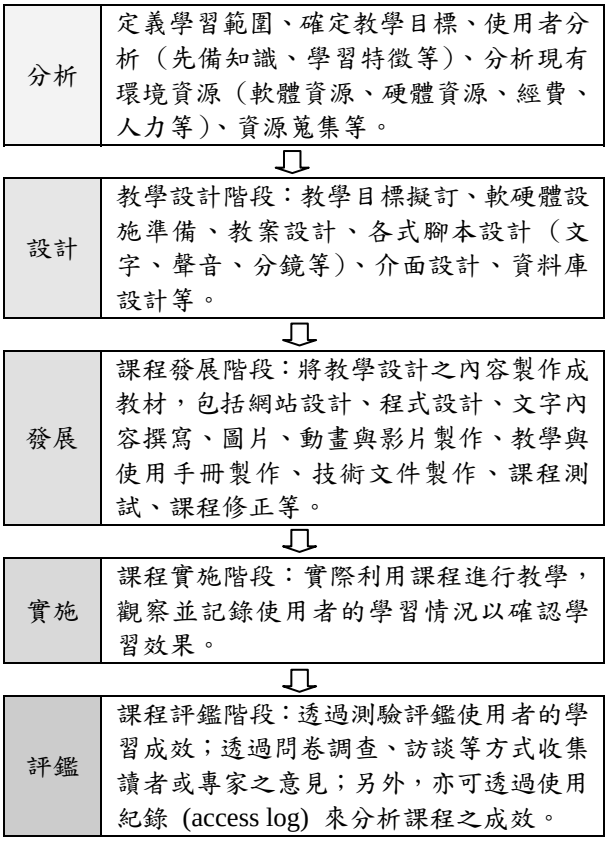


圖 1 教材設計之 ADDIE 流程圖

3. 研究設計與成果

本研究以系統化教學設計模式 - 「ADDIE」(Analysis, Design, Development, Implementation, Evaluation) 為主軸，以下將針對研究方法、課程架構與教學設計等層面進行說明。

3.1 研究方法

本研究採用之研究方法為「設計本位研究法」（Design-based research）。設計本位研究是一種系統化且較具彈性的研究方法，透過反覆的分析、設計、發展與實施來增進教育的實踐[7]。本研究針對讀者的需求，發展圖書館利用教育課程，課程開發採用「ADDIE」模式，研究架構圖如下：

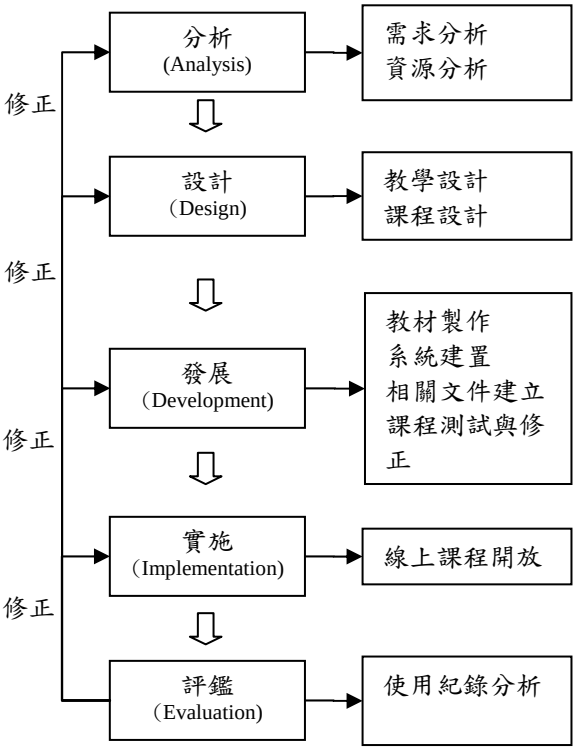


圖 2 研究架構圖

3.2 課程架構與教學設計

根據「ADDIE」課程設計程序，以下將從「分析」、「設計」、「發展」、「實施」與「評鑑」等五個階段進行說明。

3.2.1 分析階段

為了瞭解圖書館推展利用教育的需求，並探究此數位教材在現有環境之下的發展性，可從「需求分析」和「資源分析」兩個層面進行。

首先，在需求分析部分，本研究以圖書館各項服務之使用統計數據為依據進行分析，結果發現使用電子期刊服務之數量居所有服務之冠，且有持續增加的趨勢。由此可知，本館讀者使用電子期刊服務的情形相當踴躍，且隨著使用人數的增加，圖書館接到使用者詢問操作方式的電話數量也相對成長許多。雖然圖書館會定期舉辦實體教育訓練，但礙於場地和時間的限制，能夠參與的讀者有限。如果在操作過程中遇到阻礙，無法取得解答或回應，很可能影響他讀者再次使用的意願。有鑑於此，圖書館應採取更積極的作為，利用數位課程的方式，讓每一位讀者都有機會接觸相關的課程講習，讓圖書館的資源能充分被利用。

而本館目前採用「SFX 智慧型檢索系統」作為電子資源服務的整合式平台，使用者透過這個系統可以跨平台及資料庫去檢索電子資源，有效節省讀者在各個期刊資料庫探索的時間，對於利用電子資源有很大的助益。因此本研究便決定以「SFX 智慧型檢索系統」為主題，開發相關的圖書館利用課程。

另外，在資源分析的部分，主要在分析發展與實施教材的軟硬體設施，探究符合需求並兼具經濟效益之環境，使課程能正常運作，又不至於造成圖書館在人力與物力上過大的負擔。而藉由資源分析的結果，可以作為發展其他課程之參考。另外，本研究教材之開發以兼顧讀者使用上的便利性、互動性與一致性為原則，因此採用 Microsoft Powerpoint 編製教學簡報內容；再以開放原始碼軟體 -Wink ，錄製教學簡報，並製作課程動畫與互動內容；再將以上素材透過 Macromedia Dreamweaver MX 製作成網頁的形式加以彙整，最後將製作完成之教材上傳至 Moodle 平台 (本研究採用之數位學習平台，為一開放原始碼軟體)，進行課程測試與實際教學。

以下針對本研究所採用之軟硬體資源，分別從開發者端與使用者端兩個面向加以說明：在開發者端使用之硬體為本館目前現有之硬體資源，包含多媒體電腦一部以及內部網路，不需另外購置設備，硬體需求大致分析如表 1。其中相關規格說明僅為建議，不一定要完全符合條件才可以進行課程製作，僅表示在此硬體規格下，可以順暢地進行課程開發的作業：

表 1 開發者端硬體資源

硬體項目	說明	備註
多媒體電腦一部	■ Intel Pentium Ⅲ 以上或其它相容規格之 CPU ■ 512MB 以上記憶體 ■ 40G 以上硬碟 ■ 彩色螢幕，可支援 1024 X 768，65536 色以上解析度 ■ 網路卡 ■ 錄音裝置（麥克風）	一般等級之個人電腦
內部網路	■ 下載速度：大於 2M ■ 上傳速度：大於 512K	

軟體規格的部分，本研究所使用之軟體，除 Microsoft Windows XP、Microsoft office 2003 以及 Macromedia Dreamweaver MX 為付費套裝軟體，其餘皆為開放原始碼之免費軟體。而 Microsoft Windows XP 並非必要之軟體，與其他開發所需軟體相容之作業系統皆可，而 Microsoft office 2003 亦同。開發者端軟體資源需求詳列如表 2：

表 2 開發者端軟體資源

軟體項目	說明	備註
Microsoft Windows XP	作業系統	Windows Me 以上作業系統皆可

(續表 2)

軟體項目	說明	備註
Macromedia Dreamweaver MX	網頁製作軟體	
Wink	螢幕錄製與課程編輯軟體	Freeware
Internet Explorer 8	網頁瀏覽器	其它相容於 Windows 作業系統之瀏覽器皆可
Microsoft office 2003（Powerpoint）	文書處理軟體	其他相容之版本皆可

相較於開發者端，使用者端之軟硬體需求相對單純。由於是線上網路課程，因此個人電腦與內部網路是必須的硬體需求，建議需求資源如表 3。軟體部分必須要有支援 Flash Player 的瀏覽器，由於一般使用 Windows 作業系統之個人電腦皆內含 IE 瀏覽器，因此建議使用安全性較佳之 Internet Explorer 8 來瀏覽課程即可，建議需求資源如表 3 所述。

表 3 使用者端硬體資源

硬體項目	說明	備註
多媒體電腦一部	■ Intel Pentium Ⅱ 以上或其它相容規格之 CPU ■ 128MB 以上記憶體 ■ 彩色螢幕 ■ 可支援 1024 X 768，65536 色以上解析度 ■ 網路卡 ■ 音效卡 ■ 喇叭	喇叭可以耳機取代
內部網路	■ 下載速度：大於 2M ■ 上傳速度：大於 512K	

表 4 使用者端軟體資源

軟體項目	說明	備註
Microsoft Windows XP	作業系統	相容於 Windows Me 以上作業系統皆可
Internet Explorer 8	網頁瀏覽器	其它相容於 Windows 作業系統之瀏覽器皆可
Flash Player	Flash 動畫播放軟體	Flash Player 6 以上版本

3.2.2 設計階段

在設計此圖書館利用課程時，比較強調功能介紹與應用，而非專業的知識。因此在規劃學習目標時，也依循此原則，依據教育目標分類原則，將本教材的學習目標分成以下三個主要範疇：(1) 認知學習領域：瞭解圖書館目前提供之電子資源服務。(2) 情意學習領域：提升使用電子資源服務的意願，增進本所研究動力。(3) 技能學習領域：熟悉電子資源相關介面的操作方式與程序。另外，依據分析階段的結果將本課程定名為「圖書館電子資源使用教學」，其中又可分成六個小單元，課程大綱與學習目標整理如表 5：

表 5 課程架構與學習目標

課程名稱	課程大綱	學習目標
圖書館電子資源使用教學	圖書館電子期刊網頁位置說明	瞭解如何取得圖書館電子期刊的服務
	所外連線使用說明	瞭解如何在所外使用電子期刊服務
	圖書館電子期刊檢索頁面介紹	瞭解電子期刊檢索的界面與功能
	SFX 檢索系統介紹	瞭解 SFX 檢索系統的介面與功能
	SFX 檢索方式說明	瞭解如何使用 SFX 檢索系統
	SFX 與 Google Scholar 整合式運用	瞭解如何運用 Google Scholar 來取得本所訂閱的電子全文

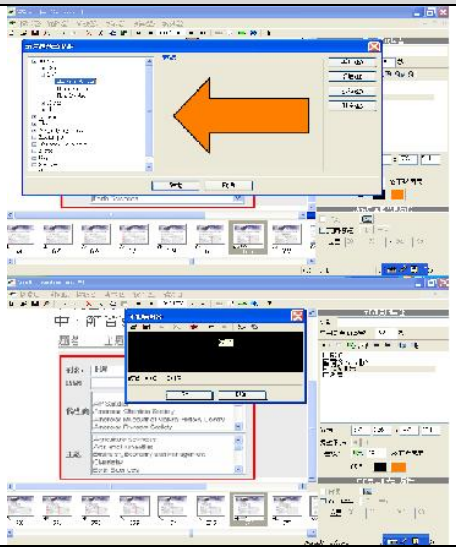
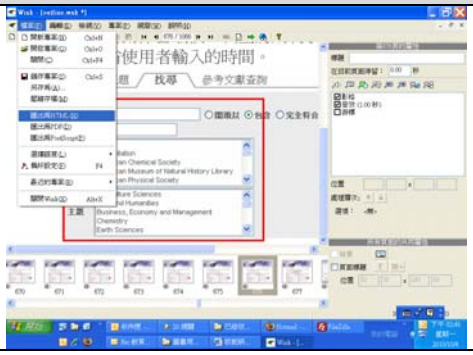
3.2.3 發展階段

依據上一節所設計的課程大綱與學習目標，本節將說明如何進一步發展成為數位課程。本研究所使用的課程編輯工具，除了文書編輯軟體之外，其餘皆為開放原始碼的免費軟體，這些軟體基本上已經可以滿足本課程製作的全部需求，因此不需額外編列經費購置軟體。課程發展的程序與使用之軟體說明如表 6：

表 6 課程發展階段程序

製作教學簡報


(續表 6)

錄製教學畫面
 使用軟體與說明： ● 使用免費軟體 Wink 錄製教學畫面 ● 需準備麥克風設備 ● 配合提字腳本，增進錄製效率
教學畫面編輯
 使用 Wink 軟體編輯錄製好的教學畫面： ● 調整時間軸：刪除多餘的畫面。 ● 調整音訊：加上背景音樂及調整音量大小。 ● 編輯工具：加上註解文字和其他效果。
數位課程匯出
 使用 Wink 軟體匯出功能將課程匯出： ● 匯出成網頁格式 ● 可符合 SCORM 規範

3.2.4 實施階段

數位課程製作完成後即進入實施階段，本圖書館利用課程將上傳至本館之數位學習平台，並開放給所有讀者使用，課程時間為一個小時。而本館之數位學習平台系以「Moodle」建置而成，Moodle 為一種課程管理系統(Course Management System)，其兼具「開放原始碼」及「模組化」的特性，能幫課程設計者或管理者快速且有效地建立線上教學平台、進行客製化調整並節省建置成本，對於目前經費普遍不足的圖書館而言，無疑是一個可善加利用的解決方案。本館之數位學習平台簡介如表 7：

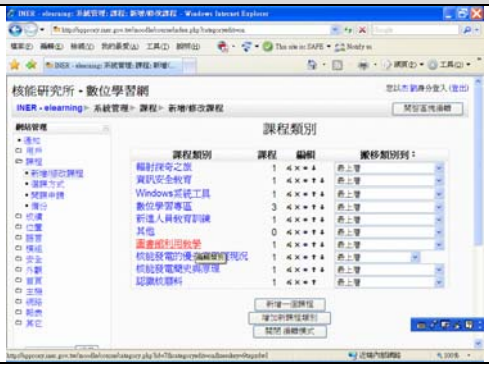
表 7 數位學習平台系統與架構

項目	說明	備註
系統介紹	Moodle ● 完整使用存取控制機制 ● 布告欄、討論區互動功能 ● 作業繳交 ● 學習測驗 ● 個人學習歷程記錄	開放原始碼數位學習平台
取得方式	網站首頁→數位學習→線上學習專區	
運作現況	數位學習平台營運現況： ● 九大類別（包含新進同仁教育訓練、輻防講習、資訊安全講習等） ● 十一門課程（課程中又可再細分為數個單元） ● 僅開放本館讀者使用	使用個人資訊系統帳號等入

此數位學習平台有完善的管理功能，透過圖形化介面，讓管理者可以輕鬆建立課程與測驗，並檢視課學現況與學習者的參與情形，對於不具資訊背景的圖書館館員而言，亦相當容易上手，不致造成過大的工作負擔。而本研究所利用之 Moodle 數位學習平台，係為本館所屬母機構之共用數位學習平台，因此其中除了圖書館利用教育相關課程之外，亦包含許多母機構的其他相關教育訓練課程，因此若圖書館將設計之課程放在一個教學平台中讓讀者使用，並非一定要自行建置，若母機構已有類似平台，便可直接利用。另一方面，若圖書館已自行建置平台，亦可以開放讓母機構之其他單位共同利用，除了豐富平台上的資源之外，亦可達成單一入口、資源整合的目標，便於管理與讀者利用。而本研究即透過母機構的數位學習平台管理介面建立圖書館利用課程專區，並上傳此課程，相關的程序如表 8 所示：

表 8 課程上傳及開放程序

登入系統

● 課程管理者使用管理權限帳號登入
建立課程類別及課程

● 建立課程類別（圖書館利用教育） ● 建立課程（圖書館電子資源使用教學）
上傳課程及測試

● 上傳課程於檔案伺服器 ● 編輯課程參數，設定課程連結 ● 以一般使用者權限登入進行課程測試

3.2.5 評鑑階段

在評鑑階段，一般可透過問卷調查、訪談等方式收集讀者、專家之意見，另也可透過使用紀錄來分析課程之成效。而依據本課程案例之觀察，在圖書館利用教育課程正式上線之後，該服務平均每月之使用量增加約 2.15 倍，並有持續升高之跡象。可見此課程除了讓讀者更瞭解該項服務的利用方式與功能之外，更兼具推廣效果。而其他評鑑作業尚待未來相關研究繼續進行之。

4. 討論與建議

隨著時代變遷，圖書館利用教育也需有所變革，以因應新世代學習者的需求。而改變是目前圖書館所面臨最重要的挑戰，在資通訊科技的進步之下，以網路進行教學的線上課程，可提供多元學習管道，並不受時間、空間限制。而透過系統化教學設計模式，可以循序漸進地形成一門課程，對於缺乏教學設計專業背景之館員或資訊人員來說，確實為一可遵循之方式。在標準化的程序之下，依據圖書館之各項服務與目的，建置相應的課程，使得讀者能更瞭解並進而使用各項資源，達到「Every Resource Its User」的目標。希望本研究能達到拋磚引玉的效果，作為其他圖書館建立利用教育課程之參考，在此模式之下，不需要教育背景也能進行課程設計，不需要資訊人員亦能開發數位課程。圖書館員應充分發揮自己的專業，挺身而出，不可妄自菲薄、畫地自限，因為唯有圖書館員才能設計出符合該圖書館資源以及讀者需求的圖書館利用教育，嘉惠圖書館與每一位使用者。

另外，獨有個別課程尚嫌不足，若能再搭配一個網路學習平台，統整各式課程，並提供個人化功能，例如社會書籤、個人學習檔案等，作為讀者學習的單一入口網站，將更能發揮課程之功效以及加值效益。而這些功能都能夠透過免費的資源來達成，且技術門檻亦不高。因此，從本研究的內容可以得知，數位課程之建立並不困難，技術上的問題其實相當容易解決，而且有許多現成的、免費的工具可以利用，再加上系統化的教材設計程序，將使得每一個圖書館都可以自行開發相關課程，而不假他人之手。總而言之，圖書館利用教育是圖書館服務的重要項目之一，尤其在數位時代中，更應充分利用數位化優勢，打破時空的限制，採取主動積極的態度，提供更符合經濟效益的課程，以吸引更多讀者使用圖書館的豐富資源。

參考文獻

[1] 楊家興，虛擬學校：資訊網路下整合性的教學環境。**教學科技與媒體，47**，1999，pp.12-23。

[2] Y. Heartsill, ed. A. L. A. Glossary of Library and Information Science.(Chicago: American Library Association). 1983, p.237.

[3] R. A. Hall, “Beyond the Job Ad: Employers and Library Instruction,” College & Research Libraries Pre-Print, 2012.

[4] J. Rice, “Teaching library use: a guide for library instruction,” Greenwood press, 1981.

[5] C. B. Leshin, , J. Pollock and C. M. Reigeluth, “Instructional Design Strategies Ant Tactics,” Educational Technology, 1992.

[6] M. Molenda, “In search of the elusive ADDIE model,” Performance improvement 42(5), 2003, pp.34-37.

[7] F. Wang and M. J. Hannafin, “Design-based research and technology-enhanced learning environments,” Educational Technology Research and Development, 53(4), 2005, pp.5-23.

[8] 徐新逸、許家卉。大學圖書館利用教育設置線上課程之需求分析。**教育資料與圖書館學，44**(1)，2006，pp.83-99。

學生編擬題目卷學習系統的建置與使用分析

于富雲* 蘇嘉鈴
國立成功大學教育研究所
*fuyun.ncku@gmail.com

摘要

近年已有不少支援學生出題活動的線上學習系統問世。有鑑於學生出題與編擬題目卷應會促發不同的認知歷程，本研究旨在發展一套學生編擬題目卷學習系統，並分析學習者使用情形。配合每周教師教學進度，針對54名修課學生進行學生編擬題目卷學習活動，以瞭解編擬學生題目卷對學生的知識整合及知識精緻化等的影響。以描述統計分析瞭解個別學生編擬題目卷中之題目跨章節以及修改的情形。主要研究發現：一、超過七成以上的參與學生能經由題目卷編擬活動，連結兩個以上的章節進行出題；二、題目卷編擬的過程中，幾乎所有參與者會再針對原先已編擬好的題目進行不同程度的編修，以增加題目精緻程度。文末，針對研究發現，提出教學建議。

關鍵詞：使用分析、知識統整、知識精緻化、網路學習系統、學生編擬題目卷

1.前言

允許學生自己探索及建構問題，以「個人觀點去選定哪些研讀主題或教材屬相關、重要及有趣之學習內容」的論點逐漸受到學者與現場教師的重視[1]。至今，學生出題對學習的效應已累積許多實徵研究證據，研究多支持其對認知、情意與社交發展上可產生的學習效果[1、2-10]。

有鑑於網路科技的優勢，目前國際間已成功建置十數個支援學生出題的線上學習系統[11]；然而，目前已有系統僅著眼於支援個別出題的學習活動，未支援編擬題目卷的相關功能。有鑑於編制題目卷與單獨出題牽涉不同的認知歷程[12]，而迄今尚未有系統支援學生編擬題目卷之學習活動，本研究旨在發展一套學生編擬題目卷學習系統並就使用情形進行分析，以瞭解編擬學生題目卷對學生知識整合與精緻化的情形。

2.學生編擬題目卷學習系統的建置

學生編擬題目卷系統發揮了網路科技的眾多優勢，如：大儲存空間、無時空限制、立即展現性、無平台限制、多媒體等。目前主要包含三大功能：題目卷編擬、題目卷評估與題目卷瀏覽，各簡述如下。

題目卷編擬功能：在決定新建置題目卷的架構（包括：涵蓋題型與各題型順序、各題型題數與配分）後，學生就可以拖曳的方式，自行挑選已編寫完成的題目為題目卷內容，或以新增新題目方式出題。送出前，學習者可針對任題目卷內的任一道題目進行修改，並調整不同題型內各題目編排的順序、題數及計分方式。

題目卷評估功能：評估功能以列表方式將目前班上已編擬完成的題目卷，依送出時間排列，讓評估者自由選擇擬評估的題目卷。評估者主要就整體品質、理解性、難度、內容涵蓋適切性與鑑別度等向度給予量化評比，並參考線上評估表的內建評量指標，給予修改建議。

題目卷瀏覽功能：目前該功能不僅提供學習者檢視同儕編擬題目卷過程中的不同版本，也能一窺題目卷編制者與評估者間的互動內容，以營造一個觀察學習的環境。

3.學生題目卷學習系統的使用分析

3.1研究對象與實施過程

本研究參與對象為南部某國立大學教育學程修習「教學原理」一課的師資培育生，共計54名。

本研究分兩階段進行。第一階段，教學者主要讓學生配合教師教學進度，以每一章為單位，進行學生出題活動。在教學者以範例講解出題須知與系統操作使用後，學生則利用 20 分鐘課內時間進行至少兩題的出題活動，並於課後另要完成至少四題的同儕評估活動。

第二階段，開放題目卷編擬、評估與瀏覽功能，讓學生可就其已編寫完成的題目為題目卷的基礎，視需要進行題目內容修改，或直接出新題目。

3.2 資料分析

研究者逐一審視與分析題目卷內各題目所含的章節內容與題目修改版次情形，以瞭解編擬學生題目卷對學生的知識整合及精緻化的情形。其中，知識整合情形會以描述統計分析個別學生編擬題目卷中是否有題目跨章節的情形。知識精緻化會以以描述統計分析個別學生編擬題目卷中是否有題目修改的情形。

4.研究結果

4.1 知識整合—題目跨章節情形

為瞭解學生編擬題目卷對知識整合的情形，研究者分析每份題目卷中各題目取材內容涉及不同教學原理的情形。結果發現，近四分之三的學生（74%）有題目內涉及不同教學原理的情形，僅有約四分之一（26%）的學生題目卷內各題目來自各獨立章節。

4.2 知識精緻化—題目修改情形

為瞭解題目卷編擬對觸發題目卷內各題目精緻化的影響，研究者統計題目卷功能開放後，其下各題目的修改情形。結果發現，幾乎所有學生(98%)在題目卷編擬過程會有將題目再進行修改的情形。事實上，僅有 1 位學生沒有進行題目卷內的題目編修動作。

5.結論

5.1 小結

本研究旨研發學生編擬題目卷系統，並瞭解編擬題目卷對知識統整度與精緻化的可能影響。本研究重要研究發現包括：超過七成以上的參與學生能經由題目卷編擬活動，連結兩個以上的章節進行出題，以進行不同程度的知識統整。跨章節題目的編擬，有賴不同教學原理間概念的連結建立，以串連成知識網絡。經此，以增加並促使學習者將思考運作拉抬至較上層、整體全面性的視角，以統合、處理各重要概念間的異同。

此外，綜觀參與學生題目卷內各題的修改版次記錄發現，經由題目卷編擬的過程，幾乎所有參與者會針對原先已編擬好的題目進行不同程度的編修，以增加題目精緻程度。

5.1 教學與未來研究建議

本研究所建置的學生編擬題目卷系統，結合數位科技眾多優勢，以建置編擬題目卷以及相關功能。使用資料分析支持題目卷的編擬有利學生知識統整以及知識精緻化的表現。有鑑於此，建議採用學生出題的教師，能考量後續加上題目卷的編擬學習活動，以促成學生更上層的個人知識網絡之建立。

致謝

本研究感謝國科會計畫補助（計畫名稱：網路學生出題目卷學習系統：建置、教學適用性與學習效益，NSC 102-2511-S-006 -003 -MY3）。

參考文獻

[1] F. Y. Yu, “Learner-centered pedagogy + adaptable and scaffolded learning space design—online student question-generation,” International Conference on Computers in Education, pp. 26-30, November 2012, Singapore.

[2] S. Abramovich, and E. K. Cho, “Technology as a medium for elementary preteachers’ problem-posing experience in Mathematics,” Journal of Computers in Mathematics and Science Teaching, vol. 25, no. 4, pp. 309-323, December 2006.

[3] A. Barlow, and J. M. Cates, “The impact of problem posing on elementary teachers' beliefs about mathematics and mathematics teaching,” School Science and Mathematics, vol. 106, no. 2, pp. 64-73, February 2006.

[4] S. L. Brown, and M. I. Walter, The art of problem posing, 3rd ed. New Jersey: Lawrence Erlbaum Associates, 2005.

[5] C. Chin, D. E. Brown, and B. C. Bruce, “Student-generated questions: A meaningful aspect of learning in science,” International Journal of Science Education, vol. 24, pp-521-549, December 2002.

[6] B. Rosenshine, C. Meister, and S. Chapman, “Teaching students to generate questions: a review of the intervention studies,” Review of Educational Research, vol. 66, no. 2, pp. 181-221, June 1996.

[7] D. J. Whitin, and P. Whitin, “New visions for linking literature and mathematics urbana,” VA: National Council of Teachers of Mathematics, March, 2004.

[8] B. Y. L. Wong, “Self-questioning instructional research: A review,” Review of Educational Research, vol. 55, no. 2, pp. 227–268, June 1985.

[9] F. Y. Yu, Y. H. Liu, and T. W. Chan, “A Web-based learning system for question-posing and peer assessment,” Innovations in Education and Teaching International, vol. 42, no.4, pp. 337-348, February 2005.

[10] F. Y. Yu, and Y. H. Liu, “Potential values of incorporating multiple-choice question-construction for physics experimentation instruction,” International Journal of Science Education, vol. 27, no. 11, pp. 1319-1335, June 2005.

[11] F. Y. Yu, and C. P. Wu, “Student question-generation: The learning processes involved and their relationships with students’ perceived value,” Journal of Research in Education Sciences, vol. 57, no. 4, pp. 135-162, December 2012.

[12] J. M. Chamoso, and M. J. Ca’ceres, “Analysis of the reflections of student-teachers of mathematics when working with learning portfolios in Spanish university classrooms,” Teaching and Teacher Education, vol. 25, no.1, pp. 198-206, January 2009.

互動式 3D 電腦輔助學習應用於正投影視圖教學

洪明顯　　游耿能　　許永洲
國立臺中科技大學多媒體設計系碩士班
evia918@gmail.com, gny@nutc.edu.tw, openbigeyes@gmail.com

摘要

在技職教育的機械、建築與設計等類科的圖學課程，是學生學習空間概念的基礎課程之一，其中正投影視圖單元更是學生踏入空間領域所需具有的先備知識。

隨著科技進步，應用電腦輔助教學的方式逐漸多樣化，藉由影音動畫的輔助與 3D 互動技術的發展，圖學學習不再只能依靠傳統授課模式。本研究設計一套輔助教師與學生認識正投影視圖的電腦輔助學習工具，將互動式 3D 模型的操作與觀察融入到學習內容中，以協助學生了解正投影視圖。本文中將著重於敘述此輔助學習工具之設計依據與發展流程。

關鍵詞：正投影視圖、互動式 3D、電腦輔助學習

Abstract

Graphics is a basic course in vocational high school for students to acquire skills in machinery, architecture or design. In most graphics-related courses, orthographic projection is an important prior knowledge for the development of spatial concepts.

As rapid improvement in computer graphics technology, the approaches for the application of computer-aided instruction have been more versatile. With the development of animation and 3D-based graphics and interactive techniques, learning is no longer based only on traditional teaching. This study designs a Computer-Aided Instruction (CAI) prototype for teaching and learning orthographic projection. The prototype integrates the 3D-based interaction with visualization tools to help students understand orthographic projection. This paper focuses on the description of the design rationale and the development of the CAI prototype.

Keywords: orthographic projection, 3D-based interaction, computer-aided instruction

1. 前言

在現今日常生活中，眾多實體的生產過程往往需要透過製圖與視圖來做為設計發想、研究開發與執行製造之間的共通語言[1]。因此，在技職體系的機械群、土木與建築群、設計群，將圖學列為重要基礎學科，並依不同科系的屬性，開設基礎圖學、機械製圖、工程製圖、建築製圖等相關課程，以教授學生應具備製圖與視圖的溝通能力[2]，而其中一單元是關於正投影（orthographic projection）立體圖的學習。在教學上的研究發現學生對於立體圖的識圖能力與空間能力呈現正相關，尤其在立體圖旋轉、二度空間旋轉及空間組織能力、空間整體能力等皆有顯著提昇[3]。

然而，具有標準化準則的正投影視圖，在繪製時僅以特定角度的 2D 白底黑色線條、尺寸標註符號呈現，學生在學習過程中，容易受困於圖形符號與立體空間轉換。其一問題是空間線索不明確，有名的例子是奈克立方體（Necker cube），由於奈克立方體單純以線條描述一立方體造型，在毫無任何深度線索下，人類視覺上容易產生含糊不明確的圖像。其二是視圖投影的差異性，透過人眼觀察實體後所解讀的是透視投影（perspective projections），繪製時則必須再轉換成具有平行投影（parallel projections）的等角立體圖。

因此本研究設計一套配合教學進度的電腦輔助學習工具，讓學生藉由互動式 3D 虛擬模型的操作與觀察，達到正投影視圖的解題訓練，並從中讓學生逐漸建立起解讀正投影視圖的空間觀念。

2. 互動式 3D 電腦輔助學習工具之發展

在本節中將針對學生學習正投影視圖常遇到的一些盲點，進行相關文獻整理，作為設計本輔助學習工具的參考依據。

2.1 空間知覺

在人類的視覺作用中，是由 2D 的視網膜成像獲取 3D 空間的訊息，在這 3D 實體空間投射到 2D 平面的過程中，是一種遺漏訊息的轉換過程（lossy transform），因此大腦需要透過一些線索、根據，來彌補探索空間深度的立體（深度）知覺（depth perception）。其中，圖畫線索（pictorial cues）指的是在平面上以各種手法營造出深度層次感[4]。

在本研究中的平行投影與透視投影皆是由圖畫線索中的直線透視繪製，直線透視靠的是線條的交錯與消失點來傳達空間深度資訊[4]。在繪製投影圖像的技術上，又可依觀察者的視點所在位置而分。當觀察的物體如圖 **1** 距離視點越遠，視點觀看物

體上各點的視線幾乎形成平行線，此時稱為平行投影；反之，物體越靠近視點時，物體上各視線便會集中落於視點上，因此形成如圖 **2** 的透式投影。

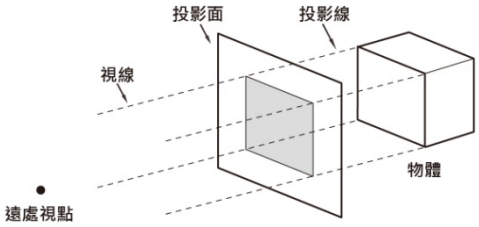


圖 1 平行投影

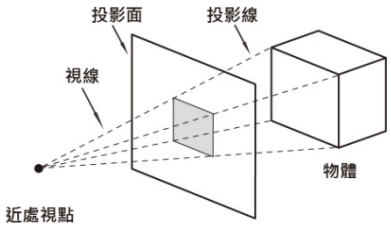


圖 2 透視投影

如表 **1** 所示，此二類型投影圖在繪製的功能上各有其特點，但在視覺上仍有可能造成如矛盾圖形（Paradoxical Figure）的錯視效果，因此本研究擬以具有互動式 3D 之輔助學習工具來協助學生釐清正投影視圖所產生的一些矛盾現象，為解題能力減少不必要的錯視誤判。

表 1 平行投影與透視投影比較表

類型	平行投影	透視投影
特性	前後大小一致	前景大、後景小
尺寸標註	較準確	依等比縮放，易產生誤差
空間知覺	不具有空間感	具有空間感
用途	工程製圖	建築外觀 室內空間
圖樣	正投影視圖 等角立體圖	一點透視圖 二點透視圖 三點透視圖

2.2 應用電腦輔助教學於圖學教學

自從 1970 年代個人電腦普及化之後，電腦輔助教學（Computer-Aided Instruction, CAI）不斷地被擴大研究範圍以運用到各個學習領域。尤其 90 年代後網路與多媒體的興起，快速地提昇了流通性與使用率[5]。在相關的研究發現，一套好的輔助教學工具需要具備使用的效果、便利與自主性，並透過電腦繪圖、動畫與虛擬實境的整合已達成學習目標[6]。

時至今日，由於電腦硬體設備與網路傳輸速度大幅提升，原先運用於遊戲育樂的 3D 遊戲引擎，開始將 3D 圖形顯像技術開發於網路線上遊戲，此類型軟體較常見的有 Quest 3D、Unity 3D、EON 與 Cryengine 等。近幾年來，陸續有其他學者在研究圖學相關的電腦輔助工具開發時，嘗試將 Cult 3D 軟體製作操作平台，提供網路學習版本[7]；而國外亦有將視覺化軟體系統地可視化機制運用在實體對象的正投影隱喻[8]，以及用遊戲引擎軟體 Unity 3D 製作，在軟體系統加入定向指標的概念，以協助視圖者觀看立體物件[9]。

3. 輔助工具之使用性設計

本研究為提供學生亦能在課後自我學習的互動性，在操作性與支援平台的考量下選擇以 Unity 3D 作為研究開發工具，並以普及性較高的網頁 Flash 互動模式做為本輔助學習工具，開發前端選擇以 3Ds Max 軟體建置模型，運用 Unity 3D 遊戲引擎的特點，整合成虛擬互動，並參考空間知覺的使用經驗，設計成更具有辨識力的 3D 輔助學習工具，最後再透過網路平台呈現。

3.1 學習正投影視圖的問題點與解決方法

正投影視圖的繪製內容必須包含一個等角立體圖（圖 **3a**）與三個面的視圖（圖 **3b**），在傳統教學過程中，常將圖 **3b** 三個視圖抽離其中一視圖，訓練學生從其他二個面與等角立體圖的關聯線索推理與解題，亦有讓學生觀察僅提供的等角立體圖再繪製出其他三面視圖（正視圖、俯視圖、右側視圖）；或是由三面視圖反推思考正確的等角立體圖。

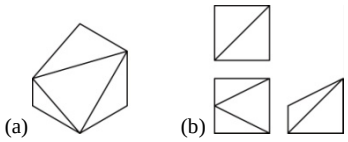


圖 3 正投影視圖，包含等角立體圖(a)、三視圖(b)

根據授課教師的經驗，初學者觀察單純以黑色線條勾勒出的立體圖，不易對該圖像產生立體空間的知覺，尤其如遇到圖 **3** 中一個立體圖包含有單斜面與複斜面的元素時，更容易在深度感知上產生混淆。因此教師在教授時常使用的手法有塗色、代號標註等方式，讓學生了解立體圖與各視圖之間的對應面向。

因此本研究在使用設計上亦加入教師們的經驗，將立體圖的各面向以顏色做出明確區隔，並加上文字標註，以正確對應各面的關係。圖 **4** 為操作視窗，視窗左邊提供一般標準的等角立體圖，視窗右邊則是以製作虛擬實境為專長的 Unity 3D 軟

體產生具互動效果的學習視窗。在學習策略上請學生從視窗左邊觀察並繪製三視圖，在推理過程中如對空間深度或對應關係有所疑惑時，即可操作視窗右邊的學習工具，運用滑鼠拖拉以旋轉立體圖像，或是點擊下方各視圖選項，找尋答案並立即釐清問題點。

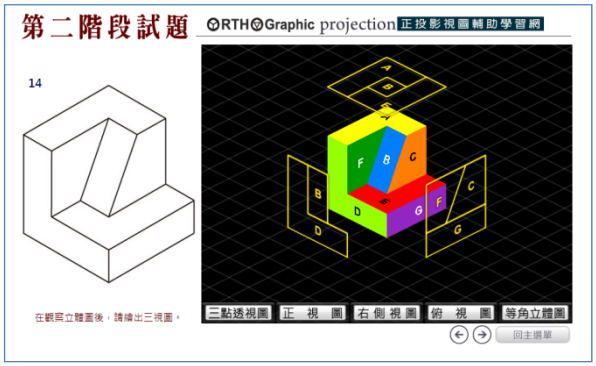


圖 4 輔助學習工具的操作視窗

3.2 輔助工具發展程序

在本研究所開發之 3D 輔助學習工具流程如圖 5 所示，是以 2D 正投影視圖（設計題型、繪製 2D 線稿）、3D 模型製作、虛擬互動式 3D 製作（場景與燈光安排、互動腳本撰寫）、網頁編輯等四項技術做整合。

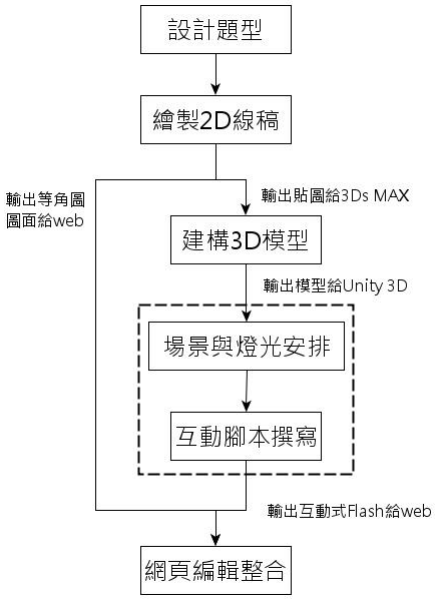


圖 5 輔助學習工具之開發流程

一、2D 正投影視圖繪製：在工業上，繪製正投影視圖講求精準、正確，因此較常使用 AutoCAD、Inventor、Pro/E 或 Solidworks。然而本研究最終是以網頁呈現，基於網頁通用格式之考量則需要選用 Illustrator。在繪製線條時，由於 Illustrator 具有智慧型參考線的輔助功能，因此很適合畫出優美正確的線條以提供給網頁圖形格式。

二、3D 模型製作：配合正投影視圖之圖面資料，以 3Ds MAX 製作出一立體模型，並在各面設定不同材質顏色與文字代號作為各面之間區隔，輔助參考的三視圖則以透空貼圖貼上事前在 Illustrator 繪製好的影像檔，最後再將各式模型輸出 OBJ 檔案格式，OBJ 檔為 Unity 3D 可接受之 3D 模型通用格式，其特點是可以連同具時間動態之動作（animation 選項）一併完整輸出。

三、虛擬互動式 3D 製作：以 Unity 3D 將製作好的 3D 模型匯入，原則上匯入的 OBJ 檔案，亦可將 3Ds MAX 設定之模型貼圖、燈光與鏡頭位置等關聯性一併完整地帶入，然而本研究為統一各模型的鏡頭、燈光位置，僅將模型與貼圖一起匯入，鏡頭與燈光的設定選擇另外在 Unity 3D 裡重新放置。Unity 3D 完成的互動式 3D 模型，可選擇匯出給不同的使用平台例如 PC 電腦、網頁、行動裝置等，本研究中考量受測試者為高中學生，使用電腦上網比其他行動裝置有較多的機會，因此選擇以一般網頁方式呈現。

四、網頁彙整：已完成之圖面資料如 2D 正投影視圖以 JPEG 影像檔呈現、虛擬互動式 3D 則以 Flash 播放檔（.swf 格式）呈現，再使用 Dreamweaver 軟體配合 HTML 與 CSS 之網頁規範，建立網頁形式之正投影視圖資料與操作介面，並嵌入具有互動效果的 swf 檔案進行整合，以製作互動式多媒體網頁。

4. 實例：輔助學習工具之規劃與設計

本節中將藉由一模型實例介紹其設計與製作過程中，各軟體間不同特性與使用方式。

4.1 圖樣設計與選定

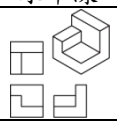
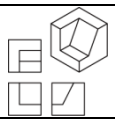
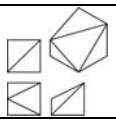
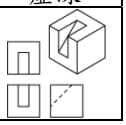
本研究在設計題型的難易度是依實驗對象作為考量，因此擬定受測試者為某縣立高級職業商業學校廣告設計科一年級學生，學生需對正投影視圖具有基本的先備知識，內容包含：空間三維、空間座標、第一與第三角投影法、正投影六視圖、線條虛實的意義、中心線畫法、繪圖的程序等。

教學目標則是針對正投影視圖單元的讀圖與視圖，著重在讓學生對只有黑白線條所構成的等角立體圖（如圖 3），如何在心理產生立體感，進而對立體模型的三個面（正視、右側視、俯視）有正確的投影觀念，以提升正投影圖的解題能力。

在教學策略設計上是以正投影視圖的線條特徵、意義做四大分類（表 2）：(1)具有直角特性的垂直、水平線；(2)斜角特性的單斜面；(3)斜角特性

的複斜面；(4)隱藏特性的隱藏虛線。

表 2 正投影視圖特性分類

分類	垂直線 水平線	單斜面	複斜面	隱藏 虛線
圖例				

4.2 2D 圖面繪製

透過 Illustrator 軟體的線條繪製，可以分別將等角立體圖之原型圖樣輸出.JPG 檔案給網頁編輯使用（如圖 **6a**）；三視圖則是在各面標註文字代號後，另外輸出具有透明背景的.PNG 格式，提供給 3Ds MAX 做為透空貼圖使用（如圖 **6b**）。

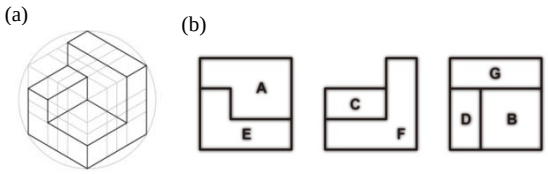


圖 6 等角立體圖與三視圖之 2D 線條稿

4.3 3D 模型製作

為協助學生增強對模型的空間知覺，依據設計原型之尺寸在 3Ds MAX 重新建置模型（圖 **7**），並在模型的各面設定不同的顏色貼圖作為明確區隔，以及在模型外圍貼上 Illustrator 繪製的透空貼圖，做出模擬投影面的效果，對照貼圖上之文字編號，亦在模型上賦予相同編號，如此即可讓學生了解各面的投影關係。完成後輸出.OBJ 格式，作為 Unity 3D 軟體之 3D 物件使用。

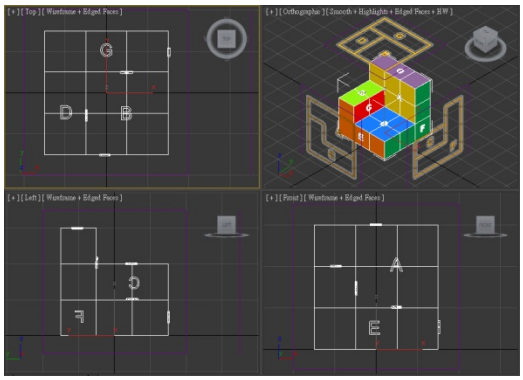


圖 7 在 3Ds MAX 之模型建置

4.4 虛擬互動整合

Unity 3D 原是為開發遊戲引擎之 3D 互動設計軟體，透過腳本（Script）撰寫達到控制 2D 或 3D 物件的互動效果，腳本所使用的程式語言可以選擇 Javascript 或是 C 語言來撰寫。本研究目的為提供學生正確地觀察模型的三面向，因此主要是撰寫程式以提供滑鼠對攝影機的方向、角度做正確的控制來圍繞模型觀察。其中，亦在攝影機的旋轉角度加入範圍限制，以避免在心理上，學生對物體的心象旋轉造成額外的負荷[10]。

由於 Unity 3D 提供遊戲玩家能以擬真的透視角沉浸在遊戲場景中，或是提供以概觀的直射角總覽整體場景，因此在攝影機的投射方式提供如圖 **8** 之正射投影（Orthographic）與圖 **9** 透視投影（Perspective）兩種視角選擇。

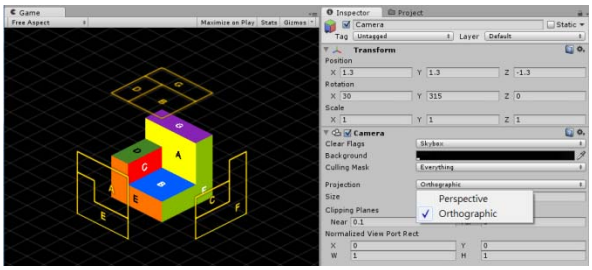


圖 8 在 Unity 3D 中，攝影機的正射投影視角

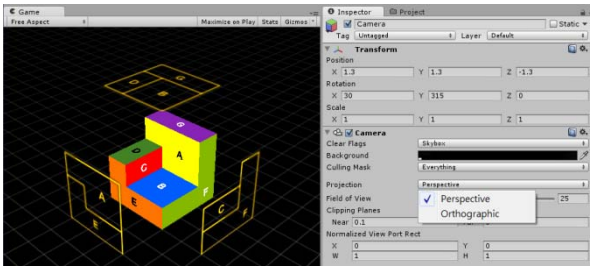


圖 9 在 Unity 3D 中，攝影機的透視投影視角

本研究為協助學生排除視覺錯視的困擾，提供學生除了正射視角以外，另一具有空間感的透射視角觀察，因此在 UI 介面設計時，加入切換攝影機視角的選項：三點透視圖、正視圖、右側視圖、俯視圖、等角立體圖，做為不同面向的觀察比較。

燈光設定方面，Unity 3D 則提供各式具有逼真效果的光源應用（Light），其項目包含：(1)聚光燈（Spot Light）；(2)平行光源（Directional Light）；(3)點光源（Point Light）；(4)區域光源（Area Light）。本研究中考量使學生清楚觀察模型的正視、俯視、右側視三個面向，因此分別於此模型的三面各以一盞平行光源垂直投射到模型（圖 **10**），使其三面能均勻受光。

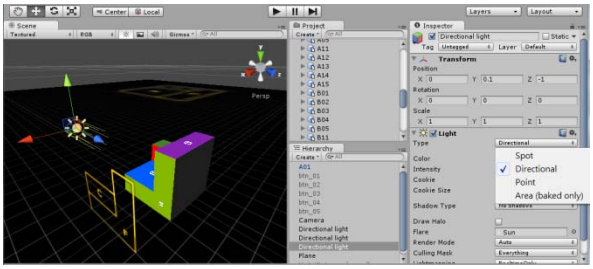


圖 10 Unity 3D 之燈光控制

最後，Unity 3D 提供多類型平台的輸出格式

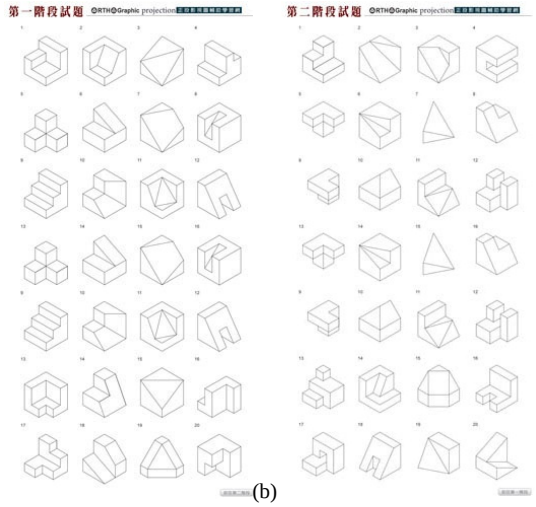
（圖 **11**），其包含了 Web Player、PC and Mac、Flash Player、iOS、Android、Xbox 360、PS3、Wii，因此本研究選擇以 Flash Player 格式輸出，以利後續網頁編輯。



圖 11 Unity 3D 之輸出介面

4.5 網頁視覺編輯

最後，在網頁整合時配合研究者與教師討論之教學策略，在網頁首頁提供二階段實驗之選擇，第一階段由授課教師操作示範（圖 **12a**），每階段呈現 20 個不同樣式的等角立體圖，點選後即可進入到如圖 **4** 之等角立體圖操作介面；第二階段亦為 20 個不同樣式的等角立體圖（圖 **12b**），由學生自行操作觀察與練習。



(a) (b)

圖 12 網頁之二階段實驗畫面

5. 研究分析

為了解本研究所開發之 3D 輔助學習工具是否對學生的學習產生影響，選定以廣告設計科一年級學生為實驗對象，學生需對正投影視圖具有基本的先備知識，將學生分二組進行實驗，研究期間共有 76 位學生參與實驗，在實驗組有學生 36 位，對照組學生 40 位，在男女生比例分配上女生人數比男生多，女生有 60 人、男生共有 16 人。其中實驗組男生 8 人、女生 28 人，對照組男生 8 人、女生 32 人（表 **3**）。

表 3 研究受測人數統計一覽表

性別	組別	
	實驗組	對照組
男生	8	8
女生	28	32
合計	36	40

5.1 學習成效分析

本研究採用獨立樣本單因子共變數分析（one-way analysis of covariance; ANCOVA）將兩班學生的前測成績（代表學習前的視圖能力）做為共變項以進行差異校正，探討並將後測成績設為依變項，不同的教學方式的班級則是自變項，以使用 3D 輔助學習工具的班級訂為實驗組，而使用傳統課程教學做為學習方式的班級設為對照組。

在實驗分組自變項與前測成績共變項之間的交互作用中（表 **4**），F 值為 2.442、顯著性 p 值 = .123 > 0.05 並未達顯著水準，這表示共變數（前測成績）與依變數（後測成績）之間的關係並不會因為自變項（不同教學方式）各自處理水準的不同而有所差異，因此可以繼續進行共變數分析。

表 4 組內迴歸係數同質性檢定

	SS	df	MS	F	Sig.
分組*共變項	370.117	1	370.117	2.442	.123
誤差	10912.101	72	151.557		

經過前測成績調為 67.5 的共變量之後，在不同教學方式的分組影響下，原始的後測成績平均數分別為 79.86 與 74.87，調整後平均數分別為 80.747 與 74.078（表 **5**）。

表 5 不同教學方式的後測成績描述性統計量

實驗分組	人數	後測原始分數		後測調整後分數
		平均數	標準差	平均數
實驗組	36	79.86	18.07	80.747
對照組	40	74.87	19.56	74.078

註：共變量為前測成績 = 67.5

其中，觀察自變項（實驗分組）對依變項（後測成績）所造成的實驗效果（表 **6**），在實驗分組項目的 F 值為 5.433，顯著性 p 值為.023（<.05），達到顯著水準，表示後測成績的高低受到不同教學方式的實驗分組影響而有所不同。因此採用本研究的 3D 輔助學習工具的實驗組確實比使用傳統教學的對照組更有助於學生對識圖能力的提升。

表 6 學習成效之共變數分析摘要表

變異來源	SS	df	MS	F	Sig.
前測成績	15066.463	1	15066.463	97.485	0
實驗分組	839.721	1	839.721	5.433	.023
誤差	11282.218	73	154.551		
總數	480200	76			

6. 結語

本研究依據輔助教學工具的實驗發現，實驗組使用互動式 3D 電腦輔助學習工具後，有助於受測試學生在正投影視圖的解題表現。

雖然市面上已有簡易且免費的 3D 繪圖軟體如 Google 公司出品的 SketchUp 軟體可供學生進行塑模練習，然而本研究的優勢則是提供教師與學生無需學習新軟體即可輕鬆容易地操作學習，以協助學生克服正投影視圖學習的障礙。

隨著數位媒體的迅速發展，將遊戲引擎的操作模式融入到傳統教學中，將是突破傳統黑板上單一平面的教學方式，讓學生有更多機會從虛擬 3D 模型的互動觀察中，逐漸建構起心中的空間知覺。

參考文獻

[1] 康鳳梅、戴文雄、李金泉、吳煥昌、簡慶郎、陳憲章，「機械製圖交線與展開提昇學生空間能力之研究」，全國技術及職業教育研討會論文集，第十六卷，第一期，第 313-322 頁，2001。

[2] 職校群科課程綱要 97 年版，取自高級職業學校群科課程資訊網：http://course.tchcvs.tc.edu.tw。

[3] 簡慶郎，「學習正投影對提昇高工學生空間能力之研究」，碩士論文，國立臺灣師範大學工業教育研究所，台北，2000。

[4] 陳一平，視覺心理學，雙葉書廊，台北，2011。

[5] 李亞蘭，「電腦輔助教學釋義」，國家教育研究院雙語詞彙、學術名稱暨辭書資訊網：http://terms.naer.edu.tw。

[6] 張萬子，「圖學網路學習系統之發展」，國立虎尾科技大學鼓勵性研究計畫成果報告 No. TCS-9204，雲林，2003。

[7] 趙世範、方榮爵，「應用立體電腦動畫技術建置高職製圖課教學網站研究」，高雄師大學報，第十五卷，第一期，第 55-83 頁，2009。

[8] C. Atkinson, C. Tunjic, D. Stoll, and J. Robin, “A prototype implementation of an orthographic software modeling environment”, Proceedings of the 1st Workshop on View-Based, Aspect-Oriented and Orthographic Software Modelling, Article, No. 3, July 2, 2013, Montpellier, France.

[9] T. Ziemek, S. Creem-Regehr, W. Thompson, and R. Whitaker, “Evaluating the effectiveness of orientation indicators with an awareness of individual differences,” Journal ACM Transactions on Applied Perception, 9(2), Article, No. 7, 2012.

[10] 趙世範，「基於圖學原理量化心像旋轉空間維度之實徵研究」，博士論文，國立高雄師範大學工業科技教育學系，高雄，2010。

運用社群網站與行動載具輔助護生進行衛教護理實習之課程

吳婷婷* 宋天文
嘉南藥理科技大學 資訊管理學系
國立成功大學 電腦與通信工程研究所
*wutt0331@mail.chna.edu.tw, tienwen.sung@gmail.com

摘要

網際網路的普及，突破了實體社交活動的限制，除提供人們快速獲取資訊、知識的管道外，更提供人際間互動、溝通、分享等多元化的應用。而行動載具的發展，更為社群網站提供了多元化的聯繫管道，虛擬社群中豐富的資源、即時的回饋與資訊的分享，促使許多研究將其應用於教學環境中。本研究則運用上述環境之優勢，將平板電腦結合Google+導入於衛教實習課程中，透過虛擬社群中豐富的資訊分享與便利的回饋機制，激發護生潛在的學習技能，提高實習過程的學習動機，且藉由高機動性與高便利性的載具輔助，更能為實習課程帶來嶄新的學習方向。經研究結果分析可知，透過社群網站的輔助，確實能有效提升師生與同儕彼此的交流互動；此外，多數護生與老師對這樣創新的學習方式皆表正向且滿意的態度，並期望未來相關課程也可繼續使用這樣的學習方式。

關鍵詞：社群網站、學習社群、虛擬社群、Google+、行動載具、護理實習課程。

Abstract

Nowadays, the prevalent Internet technology has diminished the limitations on the way of real-life social interaction, which facilitates not only the acquisition of information or knowledge for people, but also the development of diverse applications in interpersonal interaction, communication, and sharing. The advances of mobile devices also have contributed to the ways of contact for social networks. The rich resources, immediate feedback and information sharing in virtual communities facilitate the inclusion of their applications in the teaching environments. This study utilized these advantages and introduced tablet PC with Google+ into a health education practice course. The convenient information sharing and feedback mechanisms in the social network were used to stimulate potential learning skills of nursing students, and the mobility and convenience of mobile devices brought a novel way of learning within social networks. According to the analysis of the experimental results, learning interaction between the participants can be improved effectively with the assistance of the social network. In addition, the majority of the nursing students and the teacher expressed positive and satisfactory attitude for such an innovative learning method. They also look forward to using this approach in the future courses.

Keywords: social network, learning community, virtual community, Google Plus, mobile device, nursing practice.

1. 前言

資訊科技的普及與網際網路的便利，突破了實體社交活動的限制，而 Web2.0 概念的興起，也促使社群網路的蓬勃發展，社群網路除提供人們快速獲取資訊、知識的管道外，更提供人際間互動、溝通、分享等多元化的應用[1, 2]。在這虛擬空間中，每個人都可能是知識的給予者或接受者，藉由不同專業背景的個體，在知識互動與交流的過程中將知識建構，從而建立一個學習社群，並提供學習者正式或非正式參與的學習機會[3]。

隨著網路行動化與行動科技服務的迅速發展，載具多元與行動共享之概念逐漸崛起，間接發展網路社群跨界平台的整合實力。多數使用者透過載具的便利性與立即性，快速存取網路上的資源，並運用虛擬社群中知識分享的功能，擴大知識的價值[4, 5]，進而發展個人與組織的相對利益與組成目標。近年來，應用行動載具支援護校學生進行實習課程之研究也愈加蓬勃發展[6, 7, 8]，行動載具的引入，不僅節省人力、降低錯誤，更能提升護校學生的專業知識與技能[9, 10]。

有鑑於此，本研究也以行動載具為主要學習工具，為避免載具本身硬體限制造成學習上的挫折與壓力[11]，於學習載具的選擇上，則採用輕薄、易操控且大螢幕的 Pad 最為合適，並運用 Google+作為虛擬社群知識分享、回饋交流的學習平台，Google+可結合 Google 相關的應用軟體，能讓使用者以簡易的操作方式，迅速地將資訊分享到不同的軟體上[12]；此外，Google+也提供了其他社群網站所未見的軟體元件[13]，而這些元件正適合用於虛擬學習社群中。藉此，本研究則將其導入於衛生教育護理實習課程中，透過行動載具即時性的支援與服務，以及虛擬社群中資源共享的特性與優勢，將其理論與實務建立關聯，並讓抽象概念具體化，使其知識結構意義化，有效提升護校學生公衛理論之應用性，且藉由新興資訊的融入，能減少護生衛教實習之困難，提升護生實習過程之興趣，有效落實

習課程之目標，進而協助護生發展後設認知、批判性思考及解決問題的能力。

2. 相關文獻

學習是一種社群與集合的成果，為達到如此成果則需透過互動溝通、知識分享與社群連結[14]。而學習社群中知識的來源，不僅來自於教師或學習教材，也可能分散並存在於社群成員或情境脈絡的過程中，可經由討論、溝通、協商、分享與交換過程，使原本分散在各處的知識得以集中，社群成員的知能水平因知識分享而提升[15]。Quinn, Anderson & Finkelstein 也認為，知識分享能創造價值，因知識愈經使用，會不斷更新與創造，組織中的智慧資產因此而提升[16]。Tan 則強調分享的必要性，且認為分享行為是一種交換，透過有效率的溝通，終將促成組織目標的達成[17]。Hendricks 更指出，知識分享是一種溝通的過程，當向他人學習新知或分享知識時，其必須有知識再建構之過程，進而達到有意義之學習目的[18]。

而虛擬社群(Virtual Community)中豐富的資訊分享與便利的回饋機制，促使現階段許多相關研究，將虛擬社群網路之特性導入於傳統的教學活動中，更為學習型態帶來嶄新的方向[4, 5, 19]。如：Bruckman 研究發現，在虛擬環境中，透過學習者彼此的互動交流，可激發潛在的學習技能[20]；Wasko and Faraj 的研究則提出，虛擬社群中高互動的知識分享，可提高學習者的學習動機[21]；而 Zhang and Tanniru 所建置的代理人虛擬學習社群，經長時間的研究發現，在分享概念強大的環境中進行學習，能促使學習者由被動的觀看者逐漸轉化為主動的知識擷取者[22]。另外，Eales-Reynolds, Gillham, Grech, Clarke & Cornell 基於 Web2.0 之概念建置了 WRAP 系統，並將其用於護校學生之課程中，經研究發現虛擬社群環境中，多元且跨領域的資源，能有效提高護生的批判性思考、問題分析與解決問題之能力[23]。

隨著行動載具的普及與便利，亦使學習更加多元[24, 25]。而行動載具的立即性(Immediacy)與無間斷性(Seamless)[24]，讓身處在高機動性的醫療護理人員，能立即獲取所需之資源，解決當下所面臨之問題，並能隨時掌握各種突發狀況且給予立即性之支援[5, 8, 10, 19, 26, 27]。除應用於一般醫療院所，護理相關課程也逐漸導入行動載具於護校學生實習課程中，如：臨床實習(Clinical Practice)、藥物管理追蹤(Tracking Medication Administration)、醫療門診(Outpatient Clinics)、療養院(Nursing Homes)及居家照顧(Home Health)等等[6, 7, 8, 28]。

行動載具導入於護理實習課程，不但節省人力、降低錯誤、提供迅速且立即的資訊搜尋外[26, 27, 28]，即時的回饋與核心知識的支援，更加提升護校學生的專業知識與技能使用[29]。Skyscape 於研究中發現，行動載具導入後，能有效降低醫療疏失之問題，並提升整體實習學習之成效[30]。Carroll and Christakis 的研究中也指出，行動載具的導入確實提升實習程序上的準確性[31]。而 White, Allen, Goodwin, Breckinridge, Dowell, and Garvy 也發現，透過行動載具的輔助，能有效提高學習者於專業知識運用上的自信[29]。Jeffries 學者的研究也證實，於臨床實習環境中導入新興技術與科技，將能提供學生更多的學習機會，並提升既有資料擷取系統之精確性[32]。此外，美國護理大學協會(American Association of Colleges of Nursing)、醫學研究院(Institute of Medicine)與澳洲護理聯盟(Australian Nursing Federation)也都認為，應將資訊技術導入於護理課程教育中，以提供護理人員良好的終身學習之機會[33, 34, 35]。

3. 學習情境

於創新的學習環境中，為符合衛教實習之教學目標，且達到資訊導入之有用性，並符合傳統教學之活動內容，以及擴展護理之實務經驗，本研究則以原本護校所制定的教學策略(專題導向學習)為基礎，透過平板電腦，護生以小組分工方式對個案資料進行分析與探討，且藉由團隊合作之方式，自行規劃探索方向、蒐集所需資料、建立決策行動，最後進行家訪衛教與發表研究作品，於實習活動過程中，學習者不但「從做中學」更要「從研究中學」，並運用科技的輔助促進資訊搜尋技能、有效掌握工作進度，進而協助護生發展團隊技能、衝突管理、溝通管理與決策管理，並培養問題解決的能力與多元思維的技能，以下則針對 Google+導入於衛教實習課程之過程進行解說與描述。

在整體實習過程中，護理教師藉由引導，讓護生透過 Google+的相關應用軟體進行組內的溝通、協調與討論，並運用問題的探討與剖析，獲得知識與技能，且進一步培養護生高層次的認知能力。Google+可結合多樣的應用軟體(Google Picasa、Google Docs、Google Map、Google Location、Hangouts…etc)，護生只需申請使用帳號，即可享用各項應用軟體的服務，且能快速地對資訊進行公告、存取與操作，提高資訊的流通性與使用性。

於衛教實習家訪前，護理教師可利用 Google Circle，進行實習小組的分組活動，且運 Google Map 規劃訪視路線、Google Docs 編輯文件資料，並將相關資訊分享於平台上，透過學習社群之概念，護生相互分享知識、溝通互動，藉由協商後的共識建立，強化個人學習進而促進團體知識的成長。而在衛教家訪過程中，透過平板電腦則可觀看、查詢預先規劃之路徑及表單，並能利用定位拍照及影音錄影之功能，將實習相關過程進行記錄、分享與保存，而這些學習歷程，除讓護理教師能夠瞭解各組護生實習家訪之狀況，也可提供護生課後檢討、複

習之用。此外，當護生於家訪過中遇到無法解決之問題，透過此平台則可同時向護理教師與同儕請求的協助，或透過多樣的網路資源獲得資訊。家訪實習結束後，所有相關資料與文件，都可透過 Google+上傳繳交，藉以強化資訊儲存、傳輸、管理及運用之效能，其系統使用介面如圖 1 所示。此外，透過 Google+的社群網路之概念，各組護生皆可觀看平台上所分享之資訊，藉由資訊的分享與心得的交流，增加實習過程的互動性與趣味性。



圖 1 系統使用介面圖

而在整體實習過程中，透過 Google+的各項輔助功能，護理教師可隨時監控、管理各組護生之學習情境與進度，甚至透過定位拍照與影音上傳，讓護理教師更能立即掌控實習狀況與活動過程；藉由資訊為輔，實習為主的學習模式，促使護理教師轉為輔助者之角色，對於被動之學習者，可主動給予關懷、引導，而對於主動求知者，則採被動協調之方式給予輔助。於學習社群網路中，運用適當的輔助與安排，能強化護生理論與實務的連結，有效落實衛生教育相關知識之應用與整合，達到公衛護理實習學習之目的。

4. 研究設計

4.1 受試者

本研究之受試者為護校五專四年級之學生，且皆有修習衛教實習之課程，實習活動依學校安排，共分為兩梯次，每一梯次有 18 位護生，故兩梯次的護生人數共為 36 人。第一梯的實習護生為控制組，第二梯則為實驗組；控制組之護生採傳統的實習方式，在活動過程中皆以紙本方式進行記錄、交流與資料繳交；而實驗組之護生則以平板電腦作為實習活動之工具，並運用 Google+作為學習社群之平台，透過平台上多樣化的功能與服務，讓護生在實習活動的過程中，能方便的操作與應用。藉由兩組不同的實習工具之輔助，來探討學習社群網路對護生實習行為之影響，以及護生對使用學習社群平台之觀感與滿意度。

兩梯次之實習教師皆為同一人，且教學方面已有多年經驗，對於運用科技融入護理實習之課程相當感興趣，因而自願配合本研究參與實驗。另外，為確保每位受試者在實驗中都有良好的執行能力與學習過程，此成績將列入受試者此課程科目之在校成績中。

4.2 實驗流程

依學校課程規劃，衛教實習之課程共 4 週，每天上課時間為 7 小時，前兩週護生則待在地區性衛生所中，以了解基層醫療保健的工作內容與功能，且針對外出家訪的衛教資料進行整理與準備，而後兩週則開始進行外出實習家訪之活動與參加社區衛生護理之實務工作。實習課程之第一天，護理教師將針對實習課程之目標與實習活動之流程進行解說，並讓護生進行分組(一組兩人)，而其中實驗組之護生，將會發放平板電腦，以熟悉了解載具與 Google+之操作介面。隨後，不論實驗組或控制組，將針對所被分配到的個案，進行衛教資料的蒐集、整理，組內各護生皆會相互討論，並透過有效率的溝通，促成效果的達成；而衛教家訪時，各組護生則攜帶先前所準備的衛教資料，到各個案家中進行衛教實習之活動。實習課程之最後一天，實驗組將填寫系統滿意度問卷並進行深入訪談。整體實驗流程如圖 2 所示。

實習活動過程中，所有護生皆須完成家訪目的單、家訪路線單、家訪記錄表、個案管理卡以及家訪心得；而控制組之護生，則採傳統紙本方式進行課程活動、資料準備、與衛教家訪，而實驗組之護生則以平板電腦與 Google+進行相同的實習活動，且所有的學習行為都記錄於後端資料庫中。



圖 2 實驗流程圖

4.3 評估工具

系統滿意度問卷

系統的有用性與易用性將會影響學習者使用系統的意願與意圖，進而將影響學習者之學習成效[36]。藉此本研究針對學習系統的有用性與易用性進行滿意度之評估，並依此結果作為系統後續改善之參考依據。問卷設計上參考了 Chen 學者發展的問卷，問卷內容共為 6 個面向，包含：軟硬體服務、學習興趣、學習模組、師生互動、學習態度、學習成效，6 個面向之題項共有 25 題[37]，問卷採用 Likert 五等量表，最正向之意見給予 5 分，最負向之意見則給予 1 分，問卷問項的陳述方式均採正向問法，並經由兩位專家協助修正使其具備準則效度與建構效度。

實習課程之成績

不論是實驗組或控制組，在家訪實習期間，所有相關成績，將列入此課程科目之成績中。為瞭解護生在透過平板電腦並使用 Google+輔助後，對於衛生教育實習課程之理解力與操作能力是否有所提昇？以及更進一步瞭解，運用社群網站的溝通、討論、交流，和行動載具的便利、即時、多元等機制，對於外出實行家訪是否有所助益？本研究則依據實習課程之評分標準，對實驗組與控制組之護生進行學習成效之評估，而各評分面向包含：實習表現 30%、團體活動 25%、討論參與 15%、專業精神 15%、作業 15%。

訪談

訪談內容主要目的在於了解，衛教實習課程中融入了資訊與社群網路的輔助，是否能有效提升實習活動之效益，且與傳統式的實習方式有何差異，此外，更想了解，護理教師與護生對平板電腦的運用與 Google+的導入其接受程度與想法。

5. 研究分析與結果

5.1 系統滿意度分析

滿意度評估部分，各構面之 Cronbach's α > 0.7，如表 1 所示，故顯示本研究所回收之問卷皆達到一致性(Consistency)、穩定性(Stability)和可靠度。依據問卷回收後之統計分析結果可知，大多數的護生對於在平板電腦上運用 Google+進行衛教實習課程感到有趣，並認為互動式的學習社群模組，能方便且即時的分享資訊，進而提升同儕間、師生間的互動性；此外，由於 Google+所提供的相關輔助工具，能適當地滿足衛教實習活動的需求，因而能減輕護生實習上的壓力，給予即時性的輔助，增強運用專業技能之信心，提升學習過程之態度，並有效達到理論與實務整合之學習方式。

表 1 問卷信度之評估值

系統滿意度之 Cronbach's α	
軟硬體服務	0.769
學習興趣	0.889
學習模組	0.869
師生互動	0.906
學習態度	0.896
學習成效	0.824

另外，由於大多數之護生皆為初次使用平板電腦，在介面與軟體的操作上，還需多點時間去熟悉。因此軟硬體服務面向部分分數較為低一些，但整體而言，均為正向回應，由此可知，護生對於在平板電腦上運用 Google+進行衛教實習課程皆感到滿意。

5.2 學習成效分析

學習成效分析部分，則針對實驗組與控制組活動後的共同評量成績進行探討，並採用獨立樣本 t 檢定(t-test)進行分析，且運用描述統計對兩組的學習成效關係進行說明。

由表 2 統計分析結果可知，Levene = .548 > .05，故變異數具同質性，實驗組與控制組達常態分佈且具相似離散狀態；p =.000 (p<.05)達顯著水準，因而實驗組與控制組其學習成效達顯著差異，再進一步探討兩組之平均值，其實驗組之平均分數 88.888 明顯高於控制組 84.166，由此可了解，兩組護生雖都進行衛教實習之課程，且實習活動之內容相同，但採用平板電腦結合 Google+之護生，其學習成效之表現較優控制組。藉此可知，於傳統公衛護理實習課程中，導入資訊科技，確實能改善傳統學習上之缺失，並能有效提高公衛實習課程之成效。另外，再針對標準差之結果可知，實驗組之護生其學習成效間之差距高於控制組，經實驗過程之觀察與訪談可發現，在如此高互動、高合作的學習環境中，系統平台或護理教師應給予適時且適當的輔助與監控，以避免後段或被動之護生，產生搭便車(Free riding)、閒逛(Stroll)、迷失(Disorientation)的問題，進而影響學習成效。

表 2 學習成效評估之獨立樣本 t 檢定

	Mean	N	Std. Deviation	Levene	t	df	p
E	88.888	18	2.654	.548	-5.780	34	.000*
C	84.166	18	2.229				

*p < .05

再細部觀察實驗組與控制組，各評分面向之差異，可發現各面向之成績差異較大的部份是「討論參與」。實驗組的護生透過平板電腦與 Google+，即使組員未處於同一地點或位於課後時間，都還可以

透過社群網路之便利，進行同步或非同步的溝通、協商、與交流，即使在進行外出家訪的過程中，也可透過 Google+ 平台即時的向同儕與護理教師，尋求幫忙與協助，相較於使用紙本進行實習的控制組護生，其討論參與部分確實較為便利，並也解決了傳統護理家訪實習上的困處。

5.3 訪談結果分析

訪談對象除一位護理教師外，也以隨機方式，由實驗組中隨機挑選 3 位護生進行深入訪談。訪談的資料內容經人工方式整理分析後，歸納出數個主重要點，其陳述如下。

就護理教師而言，資訊的導入能有效幫助教師進行管控，傳統的學習方式，各組護生都分散於不同地區，教師只能採用電話進行追蹤，一位教師是無法同時兼顧各組學生所遇到的突發狀況，當學習者迷路、遇到突發問題或是資料遺失，教師更是疲於奔波、耗時耗力；然而，當運用平板電腦並結合 Google+平台後，不但增加師生間的互動性，教師也可透過無縫的資訊傳遞功能，可隨時掌握護生目前討論的狀況、外出家訪的情形，並於適當的時機給予回饋與輔助，以提升教師監控、管理、輔助之功能。

就護生來說，平板電腦與 Google+的導入，增加了實習過程的互動性、有趣性、即時性與便利性，護生不再需要隨身攜帶厚重的紙本資料，所有衛教資訊皆可存放在平板電腦上，透過載具中多元且豐富的衛教資料，更能提升個案對於資訊的吸收，也能減輕護生在資料準備上的負擔；此外，Google+強大的共享與流通機制，促使同儕間、師生間交流、互動更為頻繁，運用溝通互動的討論方式，促使組織目標達成，進而達到有意義之學習目的。另外，Google+上定位與路徑規劃的功能，能減少護生找尋家訪個案位置所耗費之時間，而影音錄製的家訪過程，可用於課後複習以加深護生學習印象。

訪談的回應與建議，大都抱持著樂觀與正向的態度，對於本研究所規劃的學習方式與學習載具，也都給予高度推崇。然而，護理教師認為這樣的學習方式較自主與開放，對於後段或較為被動的學習者，需要建置適當的引導機制與妥善的教學策略，來輔助學習者進行學習，惟有給予完善的輔助與規劃，才能達到學習本質的理想。

6. 結論與未來工作

本研究採用平板電腦並結合 Google+，並將其導入於衛生教育護理實習課程中，透過 Google+上多項應用與社群軟體，可達到個人化、多元化之學習效益，無論是家訪前的行前規劃、家訪時的各項活動或是家訪後的資料統整，皆可透過 Google+的輔助迅速、即時地完成，而 Google+的高互動性與應用性，能有效強化資料的共享、儲存、傳輸及運用，另外，其社群互動的各項應用功能，則增加了師生間或是同儕間資訊分享與交流的行為模式。

透過實驗分析可知，無論護理教師或是護生，對與採用這樣新興的學習方式均表示正向的態度，並認為平板電腦的行動性，能符合實習課程之所需，而 Google+上的各項應用功能，提高的師生與同儕間交流互動的機制，特別針對討論參與之面向。另外，針對訪談內容的彙整可瞭解，資訊的導入能提升護理教師，在實習活動過程中監控、管理、輔助的行為，而對護生可減少傳統實習上的困難，增加溝通、討論、互動的機制。整體而言，社群網路上的多元化互動方式，是以護生為中心，在共同參與學習活動時，會相互溝通討論，分享彼此的知識與經驗，達到資源共享、資訊互通、知識分享、經驗交換與情感交流，其成果不僅表現上的合作學習，也包括協商後的共識建立和共享成果，並強化個人學習進而促進團體知識管理。

本研究初步導入平板電腦與 Google+於護理實習課程中，目前僅針對系統滿意度以及學習成效進行分析與探討，未來可再融入合作學習之教學策略進行分析，也可針對護生之學習歷程或認知負荷進行進一步的分析；另外，Google+可結合相當多元且豐富的應用軟體服務，於後續研究上，則可再針對不同實習課程進行分析，並深入探討不同實習課程較適用於那些應用軟體於學習過程中。本研究之實驗還持續進行中，期望這些研究結果可作為相關研究學者之參考，也希望透過不斷的研究創新，能帶給護生與護理教師更完善且便利的學習環境與策略。

致謝

本研究由國科會計畫 NSC-102-2511-S-041-002 和 NSC 102-2511-S-041 -003 部份經費補助。

參考文獻

[1] J. Kolbitsch, and H. Maurer, “The transformation of the Web: How emerging communities shape the information we consume,” Journal of Universal Computer Science, vol.12, no.2, pp. 187–213, 2006.

[2] F. T. Rothaermel, and S. Sugiyama, “Virtual Internet communities and commercial success: Individual and community-level theory grounded in the atypical case of TimeZone.com,” Journal of Management, vol. 27, no 3, pp. 297-312, 2001.

[3] J. Lave, and E. Wenger, “Situated learning: Legitimate peripheral participation,” New York: Cambridge University Press, 1991.

[4] S. Bennett, K. Maton, and L. Kervin, “The “digital natives” debate: A critical review of the evidence,” British Journal of Educational Technology, vol. 39, no 5, pp. 775–786, 2008.

[5] T. T. Wu, C. S. Wang, S. H. Huang, and M. Y. Chung, “Using Google+ to Conduct High Interaction and Interdependence Learning Environment Based on Group Investigation Strategy,” Journal of Internet Technology, vol. 13, no 6, pp. 997-1004, 2012.

[6] J. Brian, and S. Jamieson, “Post-surgical cardiac patients receive new level of care,” Caring, vol. 21, no 3, pp. 28-29, 2002.

[7] D. J. Edwards, “Help is at hand(held): Meet the new personal digital assistants that will keep you informed,” Nursing Homes Long Term Care Management, vol. 50, no. 4, pp. 52-54, 2001.

[8] P. H. Wu, G. J. Hwang, C. C. Tsai, Y. C. Chen, and Y. M. Huang, “A pilot study on conducting mobile learning activities for clinical nursing courses based on the repertory grid approach,” Nurse Education Today, vol. 31, pp. 8-15, 2011.

[9] S. Huffstutler, T. H. Wyatt, and C. P. Wright, “The use of handheld technology in nursing education,” Nurse Educator, vol. 27, no. 6, pp. 271-275, 2002.

[10] T. T. Wu, “Using Mobile Annotation System in Public Health Practice Course based on Project-Based Learning,” International Computer Symposium 2012 (ICS 2012), Dec. 12-14, 2012.

[11] C. Tang, and S. Carpendale, “Evaluating the Deployment of a Mobile Technology in a Hospital Ward In Proc. CSCW 2008,” ACM Press, pp.205-214, 2008.

[12] B. W. Fitzpatrick, and J. J. Lueck, “The case against data lock-in,” Communications of the ACM, vol. 53, no. 11, pp. 42–46, 2010.

[13] S. Ovadia, “An Early Introduction to the Google+ Social Networking Project,” Behavioral & Social Sciences Librarian, vol. 30, no. 4, pp. 259-263, 2011.

[14] J. S. Brown, and P. Duguid, “Organizational learning and communities-of-practice: toward a unified view of working, learning, and innovation,” Organization Science, vol. 2, no. 1, pp. 40–57, 1991.

[15] P. Goodyear, “Situated action and distributed knowledge: A JITOL perspective on EPSS,” Innovations in Education and Training International, vol. 32, no. 1, pp. 45-55, 1995.

[16] J. B. Quinn, P. Anderson, and S. Finkelstein, “Managing professional intellect: Making the most of the best. Harvard Business Review,” vol. 74, pp.71-80, 1996.

[17] M. Tan, “Establishing Mutual Understanding in Systems Design: An Empirical Study,” Journal of Management Information Systems, vol. 10, no. 4 , pp. 159-182, 1994.

[18] P. Hendricks, “Why Share Knowledge? The Influence of ICT on the Motivation for Knowledge Sharing,” Knowledge and Process Management, vol. 6, no. 2, pp. 91–100, 1999.

[19] T. T. Wu, and S. H. Huang, “Investigation of Google+ with Mobile Device Implement into Public Health Nursing Practice Course,” The 6th FTRA International Conference on Human-centric Computing (HumanCom2013), Aug. 23-25, 2013.

[20] A. Bruckman, “The future of e-learning communities,” Communications of the ACM, vol. 45, no. 4, pp. 60–63, 2002.

[21] M. M. Wasko, and S. Faraj, “Why should I share? Examining social capital and knowledge contribution in electronic networks of practice,” MIS Quarterly, vol. 29, no 1, pp. 35–57, 2005.

[22] Y. Zhang, and M. Tanniru, “An agent-based approach to study virtual learning communities,” In: Proceedings of the 38th Hawaii International Conference on System Sciences, 2005.

[23] L. J. Eales-Reynolds, D. Gillham, C. Grech, C. Clarke, and J. Cornell, “A study of the development of critical thinking skills using an innovative web 2.0 tool,” Nurse Education Today, vol. 32, no. 7, pp.752–756, 2012.

[24] Y. L. Jeng, T. T. Wu, Y. M. Huang, Q. Tan, and S. J. H Yang, “The Add-on Impact of Mobile Applications in Learning Strategies: A Review Study,” Educational Technology & Society, vol. 13, no. 3, pp. 3–11, 2010.

[25] T. T. Wu, T. W. Sung, Y. M. Huang, C. S. Yang, and J. T. Yang, “Ubiquitous English Learning System with Dynamic Personalized Guidance of Learning Portfolio,” Educational Technology & Society, vol. 14, no. 4, pp. 164-180, 2011.

[26] D. F. Criswell, and M. L. Parchman, “Handheld computer use in U.S. family practice residency programs,” Journal of the American Medical Informatics Association, vol. 9, no. 1, pp. 80-86, 2002.

[27] D. L. Fowler, N. J. Hogle, F. Martini, and M. S. Roh, “The use of personal digital assistant for wireless entry of data into a database via the Internet,” Surgical Endoscopy, vol. 16, pp. 221-223, 2002.

[28] M. Hassett, “PDAs: Leading the information revolution,” Nursing, vol. 32, no. 2, pp. 66, 2002.

[29] A. White, P. Allen, L. Goodwin, D. Breckinridge, J. Dowell, and R. Garvy, “Infusing PDA technology into nursing education,” Nurse Educator, vol. 30, pp. 150-154, 2005.

[30] Skyscape, Skyscape Survey: 50 percent of medical professionals who use handhelds significantly reduce their medical errors. Retrieved April 18, 2008, from http://www.skyscape.com/Company/PressRelease.aspx?id=184, 2004.

[31] A Carroll, and D. Christakis, “Pediatricians' use of and attitudes about personal digital assistants,” Pediatrics, vol. 113, pp. 238–242, 2004.

[32] P. R. Jeffries, “Guest editorial: Technology trends in nursing education: next steps,” Journal of Nursing Education, nol. 44, no. 1, pp. 3-4, 2005.

[33] American Association of Colleges of Nursing, Nursing education’s agenda for the 21st century, Washington, DC: Autho, 2002

[34] Institute of Medicine, Health professions education: A bridge to quality (A.C. Greiner & E. Knebel, Eds.), Washington, DC: National Academies Press, 2003.

[35] Australian Nursing Federation, National consensus statement on nurses and lifelong learning, Canberra, Australia: Author, 2005.

[36] F. D. Davis, “Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology,” MIS Quarterly, vol. 13, no. 3, pp. 319-340, 1989.

[37] C. M. Chen, “Intelligent web-based learning system with personalized learning path guidance,” Computers & Education, vol. 5, no. 2, pp. 787-814, 2008.

行動擴增實境於同儕互評上的應用 —以基礎設計課程為例

趙國宏　　藍中賢　　王冠傑
國立師範大學資訊教育研究所
桃園創新技術學院
stefan@tiit.edu.tw
chlan@tiit.edu.tw
nanya1226129@gmail.com

摘要

本研究主要是將行動擴增實境(Augmented reality , AR)技術融入同儕互評系統，其突破藝術性創作課程作品評量時的時間與空間的侷限性，並提供學生更多元且豐富的資訊。藉由行動載具科技與擴增實境技術整合起來的特質，美術設計相關科系的學生作品可以依照所處的位置與情境來呈現不同的樣貌。而研究中建構的同儕互評系統結合擴增實境技術於檢視與評量同儕的藝術創作作品，這個機制強化了學生闡釋作品、分享創作想法、切磋製作技術時的互動行為，並將獲得的認知知識反饋回自己的作品。再者，行動 AR 系統提供個人化與位置導向的適性化內容，會讓個別的使用者與真實環境中的虛擬資訊進行互動，並讓學生在不同的觀點與情境中觀賞作品，從中獲取不同角度的觀點與設計理念，從而培養深度思考與認知的能力，進而增進創意設計。

關鍵詞：擴增實境，同儕互評，行動學習。

1. 背景簡介

教育界採用同儕互評的例子越來越多，只因其具備支援小組學習以及強化學習效能的因素。在執行同儕互評的過程中，學生參與了許多的認知活動，包括做作業、分解作業項目、討論、整理、釐清疑問、提供反省回饋、診斷錯誤、找出遺漏的知識以及互相評量作品的價值[1][2][3]。早期關於同儕互評的研究大多強調在互評時的實況、方法與產出，並且專注於學生作品的品質、專業技能與互評的技巧 [4] 。 近幾年來，行動科技展現了提供學生經歷創意學習的潛力；學生可以藉由手上的手持式裝置隨時隨地即時取得學習的素材、分享想法創意，以及建構出所需的知識。為了降低空間與時間上限制，利用行動裝置進行同儕互評立即對過程中互評的方法與結果產生了正面的影響，並且能讓學生可以很方便地隨時呈現自己的作品，互相觀摩同學的作品，最後彼此給予建議回饋。

然而，在互評的過程中若是可以讓學生隨時取得彼此想要呈現的正確資訊，對於互評活動會有更好的助益。擴增實境技術提供了在合適的時間與地點提供正確資訊的功能，而將此技術植入於行動裝置後，藉由整合位置導向與情境感知式學習的方法，行動式 AR 可以將虛擬的物件與訊息重疊在真實世界的影像上，因此提供學生豐富的有用資訊與有意義的作品展現情境。研究也發現，在利用行動式 AR 技術觀賞過其他同學的作品之後，學生將吸收到的知識與體驗反映到自己的作品上，會有正面的成長。

為了對整個同儕互評過程有個有效且全面性的觀察，受評作品的呈現內容與互評的方法也需要更多的關注。因此，本研究呈現一個概念性的架構，其藉由結合 AR 技術來強化作品的展示與提升同儕互評的效率，使人工智能與行動載具的加入能更具效果。在這個架構中，學生可以用許多不同的方式來觀賞同學的作品，並且立即取得互評的結果。如此，如何了解同儕設計作品時的理念並給予評量所遇到的困難，都可以藉此解決，而充分且合適的資訊呈現將使互評的工作更加的準確。最重要的是，合宜對應的互評機制及對作品的回饋，將使學生將這些正面的認知反映到自己的作品，在家以精緻化，提升作品的品質。

2. 行動學習與同儕互評

在教學活動中讓學生彼此評量作品並給予回饋意見，這種同儕互評的方式已經被公認為具有教育效能的機制[5]，並且在合作學習的領域中，也是一種改善學生學習效能的學習工具[6]。在高等教育中，於各種關於教育、商業、醫療與科學等領域的個人評量與同儕互評的研究紛紛被提出[7][8][9][10]。這些研究都提到學生若融入這種互動性很高的互評活動之中，可以提升學生表達與即時反應的能力。考量到如何讓學生有效率的融入到互評活動當中，互評程序中必須包含評量標準的訂定、作品的展示活動、評量的方法、評量與取得回饋意見之間的循環…等等[11][12]。 大多數的研究著重於互評的狀態、方法與結果[4]，並且都提出了數位導向的互評系統來支援同儕互評的過程[13]

[14]。適當的科技應用於同儕互評系統中可以協助觀察與評量的這兩個工作。而電腦網路則是提供了學生在任何時間與地點來參與評量的活動，而老師則可以藉此觀察到學生互評的整個過程與進展。線上即時互評系統可以消除在教室中舉行互評時無法同時舉行多種互評的限制，如此可以縮減互評活動所需要的時間，降低與同學們溝通、列印成果與列印評分表格等所需的成本。

近幾年來，學生們嘗試在各種地方進行學習的活動，因此行動學習的方式越來越廣泛。行動載具中的科技具有提供任何地方任何時間可行的創新學習方式的潛力[15] 。由於行動載具科技的特性，例如體積小、隨處可用、學生買的起、具有無線網路，使得越來越多的研究者在行動手持系統上，例如智慧手機、平版電腦與 PDA，開發了可以協助學習活動的應用程式。一些研究已經提出如何利用行動載具來增進評量效率的關鍵議題 [16][17]。 學生可以在教室內或戶外靈活地利用行動載具來實施專案導向(project-based)的學習活動。數個研究也提出如何應用行動科技於個人或同儕互評的發現[11]。陳認為結合行動科技與小組展示概念(round-table presentations)，行動評量系統可以協助老師更穩定的管理評量的活動，並讓學生更願意在互評的過程中展示他們自己的作品、參與互動與回饋意見。然而，大部分的研究著重在探查評分標準的項目、評分過程與宣傳回饋的結果，藉此提升評量的效能與回應。事實上，在互評的過程中可以讓學生仔細的解說與展示他們的作品是很重要的關鍵。經由觀賞別人的作品，學生可以瞭解如何評量自己的作品並把別人的回饋意見對應至自己的作品上，並做修正。

藉由行動科技的特性，學生可以依照所處的不同地點與情境，用不同的方式來展示自己的作品，並且可以與同學在任何時間地點一同溝通討論作品的好壞。本研究提出一個整合擴增實境技術至互評與展示過程的行動同儕互評系統，這個機制可以讓學生容易地展示作品、增加互動的機會、重複說明自己的製作理念，並將回饋反應回自己的作品。經過這樣的觀察與互動的過程，評量的正確性與品質都相對提昇。整體來說，整個過程讓學生培養深度思考技巧與提升有意義的學習，都更加的容易了！

3. 行動擴增實境在同儕互評的應用

擴增實境技術可以針對某個特定的人在特定合適的時間地點對於適當的設備展示正確的資訊[18][19]。此技術可以將虛擬物件疊合在真實物件的影像上，讓使用者產生沈浸融入的效果，並讓人們的日常生活也可以藉由設備而充滿了數位的資訊、影像、聲音及其他可以獲取到的訊息。簡單來說，藉由在現實世界影像上置入一層虛擬數位資訊的圖層，擴增實境技術可以將虛擬的物件擬真化，就如同這物件在正確的地方真實的呈現。廣泛對於擴增實境的定義如下：“擴增實境讓使用者看見真實世界中，具有虛擬的物件疊合或合成於其中。AR 讓真實世界中增加資訊，而不是將真實物件完全移除取代[20][21]。擴增實境技術與傳統方法比較起來，被認為是取得與呈現數位資訊的好方法[22]。

在行動學習方面，定位科技的發展讓追蹤到學生的即時位置是可行的，並針對學生所處地點立即提供量身訂做的學習內容。更進一步來說，位置導向式(location-based)學習提供學習者個人化的學習經驗並協助學習者融入學習的活動與學習情境當中，藉此提高學習的效率[23]。先前的研究指出，結合位置導向式(location-awareness)學習與環境導向式學習(contextual learning)的教學策略，能讓學生更有能力地將各種知識概念有意義的整理建構起來[24][25]。為了能讓教學情境中的虛擬資訊能在真實世界正確的地方出現，可供辨識位置用的標籤或標誌是需要的。 AR 技術會辨識出這些標籤後將這些標籤的位置當作虛擬資訊該出現的位置。而這些標籤大略分成兩大類：一個是 “AR ToolKit marker”，它是一個由正四方框所圍起來的黑白圖形；另一類則是全圖像辨識。當“AR ToolKit marker”的正四方形框在真實世界依不同觀察角度而投射到拍攝畫面時會變形成平行四邊形，藉由反轉這樣的程序，將平行四邊形轉變成正四方形的方式，這個四方形標籤位於真實世界的位置與方向就可以推測計算出來，因此虛擬資訊便可以在行動裝置的螢幕上，依所拍攝的真實世界影像中出現在正確的方位了。然而，真實物件可以依不同的角度被觀察，所以利用真實物件當作全圖標籤的方式，是比較困難的。因此，在現階段利用真實物件全圖標籤技術偵測物件方位的技術尚未被廣泛使用，但已經有研究正在進行當中。由於真實物件全圖標籤偵測不需要製作額外的標籤放於真實的世界，在過不久的將來，這方法成熟後應該是會成為主流的虛擬物件位置偵測技術。

在幾年前，如果有人想要在真實物件上顯示虛擬的資訊，必須在身上穿戴許多設備。其中包含一台相機來擷取真實世界的影像，一台無線網路路由器來傳送影像到資料庫，並把相關資訊從資料庫傳送回使用者身上的機器，再把這些數位虛擬訊息與真實世界的影像確實無誤的整合在一起，再有一台投影機將這些虛擬訊息投射到真實世界的物件上。然而，這樣的裝備實在是不方便操作。近幾年來，在行動科技與無線網路通訊科技的長遠進展助益之下，讓具備許多實用功能的手持式系統成了展示 AR 技術最方便與合適的平台。手持系統上的攝影鏡頭可以擷取真實世界的即時影像，電子羅盤可以偵測使用者所面對的方向，衛星定位系統 GPS 可以定位使用者所處的位置，而裝置上的螢幕可以顯示 AR 系統與真實世界合成完畢所要展示的虛擬資訊，其可以是文字、影像、表格、影片，甚至是多媒體的整合。更甚的是，例如按鈕或互動式表格等

額外的元件也可以加入做為互動時的人機介面。這樣的行動擴增實境系統提供了流暢的行動性功能，並且絕不限制使用者在某些固定的地點才可以獲取學習的服務資訊，隨時隨地都可以進行學習的活動。根據 NMC Horizon Report 2012 年 K-12 的版本，AR 技術在教育領域提供了視覺上與學習活動的互動性上有了很好的支援。藉由使用者輸入資料與系統互動後系統相對應產生的即時虛擬資訊，學生可以因這些資訊建構出新的認知基礎[26]。許多的研究也支持 AR 技術是可以協助學生的學習，例如教育遊戲、語言學習、電子書、故事講演、駕駛導引…等等 [20] [11] [27]。如此一來，AR 技術成為數位資訊在人們眼前展示的革命性技術的可能性，並且在客製隨選、內容感知及合作式訓練的領域上，都具有很大的潛力[28]。另外，行動擴增實境技術提供個別學生個人化與位置導向的適性化學習內容，使其可以在行動瀏覽環境上做互動式的學習，而且觀賞自己的作品在現今的位置上未來可以與這環境如何的融合在一起。

根據上面所述，行動擴增實境技術明顯可以支援學生在同儕互評的過程中檢視同儕的作品。在以前傳統的設計課程，學生在檢視作品時只在意評量的準則，例如獨創性、製作技巧、色彩表現等等，卻沒能讓評量者在當地觀察到在這環境中此作品未來能有什麼可用之處、能否合適的裝飾這個空間。一個位置導向行動擴增實境技術的最大功能，就是依照使用者所處的位置提供合適的資訊。當學生手持此系統走進某些特定區域，行動擴增實境系統便會自動將切合學習主題的資訊呈現出來。舉例來說，一張作品圖是當作一幅畫掛在牆上亦或當成一幅巨大壁畫，或者一個手工勞作被重建成巨大雕塑可否融入這個空間環境，系統都可以利用 AR 技術在現場呈現出來。「整合了 GPS 定位系統、無線網路接收、羅盤方向偵測、加速度器感應動作、聲音與影像辨識等豐富的偵測裝置於現今的智慧型手機當中，便啟動了人們與環繞於其四周世界萬物互動的新方法」[29]。行動擴增實境技術將可以連接數位資訊與實體世界，使得位置、內容與事件導向的情境教學可以無縫的整合創建出來。在本研究，在同儕互評的過程裡，評量者不只評量放在眼前的實體作品，更可以看見作品未來的應用與前景。因此，評量者評斷的不只是設計者製作作品的技巧與功力，更需要評判這作品的實用性與未來的可能性。

4. 系統實作與範例說明

4.1 系統架構

擴增實境可以定義為在現實環境中，部分的成分是由電腦感應器感觸輸入而產生，例如聲音、影像或 GPS 定位系統的資料。在教育的領域，有許多操作或展示的過程是無法在實體教室中讓學生直接體驗的，而擴增實境技術則是現有可以針對學生特殊需求而允許並修改學生學習經驗的方式。到底擴增實境技術能做到什麼，簡單說就是在攝影機與顯示器的協助下，在現實環境中可以觀賞到虛擬的數位物件。接下來，藉由擴增實境技術強化的行動同儕互評系統是探討的重點。描述的過程將展示擴增實境技術在互評的過程中如何強化觀察作品與評量作品的效能。

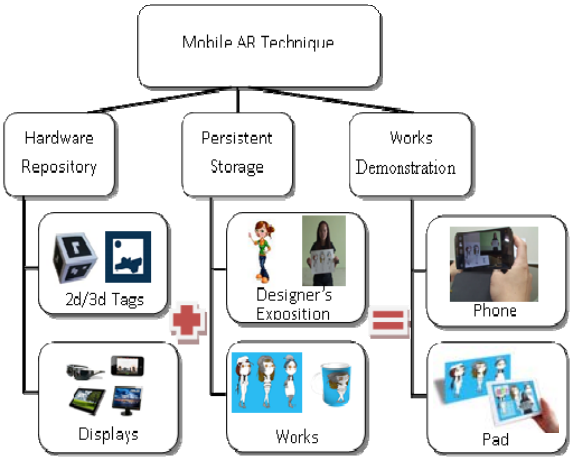


圖 1 行動 AR 系統架構

這個行動擴增實境技術的架構包含了三大部分，其為硬體平台、資料儲存單元與作品展示單元，如圖 1 所示。在硬體平台部分，辨識與展示虛擬物件的正確位置所必需的平面或立體標籤是需要的，並加上要將其展示出來的螢幕裝置。學生的作品及設計者對此作品的介紹，全都數位化與系統化的儲存在資料儲存單元中。這些素材將提供虛擬物件額外的展示訊息。在作品展示的部分，疊合虛擬訊息的真實環境影像可以呈現在手持系統的螢幕之上，例如智慧型手機或平版電腦。經由整合行動擴增實境技術與同儕互評系統，圖 2 中展示了行動擴增實境同儕互評系統 (mobile-AR peer-assessment system，MARPAS) 的執行流程與系統框架。.

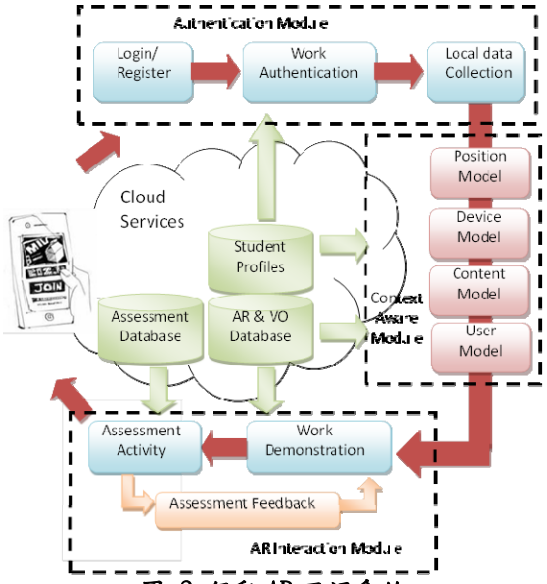


圖 2 行動 AR 互評系統

圖 2 中在雲端共有三個資料庫，包含學生資料庫、擴增實境虛擬資訊資料庫與互評結果資料庫。在互評的活動一開始，學生必需登入系統來辨識身份並決定自己要扮演的角色，是學生上傳作品相關資料，還是評量者參與評量活動，另或是老師進入系統進行評量或觀察評量活動，而所有與學生相關的資料都已經事先建立於學生資料庫中。接下來目標作品將會呈現在評量者的面前，而 MARPAS 系統持續進行收集與使用者相關的資訊，包括評量者的位置、面向方位以及在室內或戶外等等狀況。這些即時的在地訊息將由手持式裝置收集獲得後傳送到系統之中。在進行同儕互評的過程中，程序會分成三個模組，包含身份鑑別模組、內容感知模組與 AR 擴增實境互動模組。身份鑑別模組讓正確的人獲得正確的資訊來評量正確的作品。內容感知模組讓評量者使用正確的工具取得正確的資訊來做評量的工作；在內容感知模組中，系統判別與過濾當地資訊之後在虛擬物件資料庫中選擇合適的資訊呈現給評量者。所有的資料將會準備齊全之後交由 AR 擴增實境互動模組，讓這些虛擬資訊疊合在真實環境的影像之上，因此評量者的評分工作將會更方便與直覺，也更加正確。最後在 AR 擴增實境互動模組讓評量者方便且直覺地觀看同儕的作品，並可以讓評量的方式與主題更具多樣化與彈性，最後給予回饋的意見，讓每個受評者可以在這過程中學習更多，更加認識自己與別人的作品。

4.2 實例操作

同儕互評系統大多以三到四人的小群組方式在推行。這些參與的學生將會更加的能夠從同儕的回饋意見中找到作品與主題或目標的關連性[29]。因此在本研究中，50 位視傳系的大一學生在基礎設計課程中參與了這項實驗，並隨機被分成了數個小組。課程教師指定了一個會話主題的作業之後，學生會在自己的手機或平版電腦上收到相關的訊息與通知。學生會有三個星期的時間製作作品並錄製對作品設計理念的介紹與說明，這些全部要上傳到行動擴增實境同儕互評系統(MARPAS)當中。其中，AR 擴增實境技術建立了作品與解釋說明影片之間的連結與互動關係。 接著，在互評的過程，教師設計兩個情境讓學生在室內與戶外兩個環境作評量的活動。學生的作品數位化之後會縮小印出當成判別虛擬物件呈現位置的標籤，並貼在一個室內的展示會場與一個戶外的牆上。這兩個室內與戶外的互評活動情境與行動擴增實境同儕互評系統(MARPAS)呈現在下面圖 3。

在室內的情境，評量者到達展示會場並利用自己的手持式系統上的攝影機辨識會場中個別的作品標籤，然後就可以在螢幕中看見此作品在真實環境中真實的呈現出來。過程中，受評者對自己作品

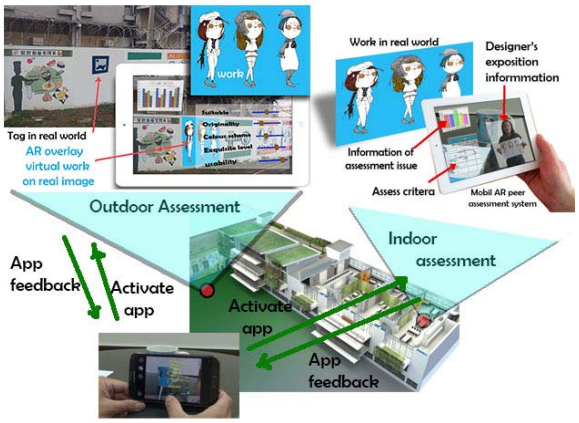


圖 3 MARPAS 系統操作

的說明與設計理念介紹會在作品旁出現，而評分標準以及已經完成的評分與回饋意見也會在系統中當成虛擬訊息在真實環境中展示出來。在戶外的情境中，評量者到戶外場地的牆上擷取作品標籤，則學生作品將會在真實環境中的牆面上呈現出來。評量者依然可以像室內情境一般看見受評者的介紹與評分標準等訊息。但是，評分標準將會依照所處的不同情境而有所不同。舉例來說，室內情境的標準是切題性、創意、色彩表現，然後評分者在各項目給予分數。在戶外的情境，評分標準則改為切題性、精緻度以及在此環境的合適度，藉由這種方式，評量者可以在現場評量作品是否搭配周遭的環境而畫在這面牆上。另外，所有針對這個作品的評量結果都在完成後同步顯示在 AR 擴增實境系統中以虛擬物件的方式出現於真實環境之上，如圖 4 所示，因此評量者可以參考到其他不同評量者的意見，受評者則可以收到大家給予的回饋意見與評量結果。

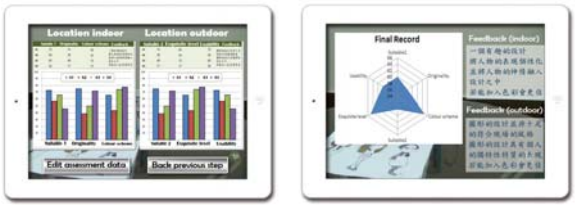


圖 4 評量結果展示與提供回饋

依據四周環境的不同，學生不只可以隨時取得與作品相關的介紹與展示，還可以依不同但情境合適的評分標準來評量其他同學的作品，產生不同的評量結果與回饋意見。行動擴增實境同儕互評系統(MARPAS) 增進了學生觀賞其他同儕的作品的意願與評量後的回饋意見，因此，學生便能依照所獲得的正向回饋意見反映到自己的作品，再修改自己的作品，這種方式將使學生更加能學習到不同面向的知識。

5. 結論

本研究提出了一個具備智能與行動力的架構來強化同儕互評系統，使得在時間上、空間上與設備上常見的限制都可以消除了。在這個架構中學生可以利用擴增實境技術將虛擬訊息與真實環境結合的協助來檢視與評量同儕的作品。行動擴增實境技術提供穩定的行動科技以及位置導向的適性化資訊，讓個別的學生們可以因此與許多的作品在真實環境中互動，學生可以利用自己的手持式裝置在合適的情境中來擷取標籤並在正確的位置正確的時間點取得正確的訊息。藉由整合 AR 擴增實境技術，前面所提的架構讓學生可以在不同的情境下檢視作品並立即取得互評的結果與回饋，所以檢視同儕作品並瞭解設計者原先設計理念的瓶頸都逐一解決了，而且充足的資訊更讓整個互評的結果更加的正確與具有更高的效能。另外，合適的評分標準與充分的回饋意見促使學生將這些正向意見回應到自己的作品上，再繼續增進作品的品質。雖然這個架構證明了在同儕互評系統中加入 AR 擴增實境技術的許多正面影響，其中仍有許多工作需要去執行，包括大量的樣本實驗實作與適性化資料能自動分析與記錄。

參考文獻

[1] Liu, E. Z., Lin, S. S., Chiu, C. H., & Yuan, S. M. (1999). Student Participation in Computer Sciences Courses via the Network Peer Assessment System, *Advanced Research in Computers and Communications in Education*, *2*, 744-747.

[2] Sitthiworachart, J., & Joy, M. (2003). Web-Based Peer Assessment in Learning Computer Programming, *Proceedings of IEEE International Conference on Advanced Learning Technologies*, 180-184.

[3] Van Lehn, K. A., Chi, M. T., Baggett, W., & Murray, R. C. (1995). Progress Report: Towards a Theory of Learning during Tutoring, Learning Research and Development Center, Univ. of Pittsburgh.

[4] Van Zundert, M., Sluijsmans, D., & Van Merriënboer, J. (2010). Effective peer assessment processes: Research findings and future directions. *Learning and Instruction*, *20*(4), 270–279.

[5] Van den Berg, B. A. M., Admiraal,W. F. & Pilot, A. (2006) Peer assessment in university teaching: evaluating seven course designs, *Assessment & Evaluation in Higher Education*, *31*, 19-36.

[6] Topping, K. J., Smith, E. F., Swanson, I., & Elliot, a. (2000). Formative Peer Assessment of Academic Writing Between Postgraduate Students. *Assessment & Evaluation in Higher Education*, *25*(2), 149–169.

[7] Ballantyne, R., Hughes, K., & Mylonas, A. (2002). Developing procedures for implementing peer assessment in large classes using an action research process. Assessment & Evaluation in Higher Education, *27*(5), 427–441.

[8] Price, M., & O'Donovan, B. (2006). Improving performance through enhancing student understanding of criteria and feedback, *Innovative Assessment in Higher Education*, 100–109.

[9] Prins, F. J., Sluijsmans, D. M. A., Kirschner, P. A., & Strijbos, J.-W. (2005). Formative peer assessment in a CSCL environment: A case study, *Assessment and Evaluation in Higher Education*, *30*(4), 417–444.

[10] Searby, M., & Ewers, T. (1997). An Evaluation of the Use of Peer Assessment in Higher Education: A Case Study in the School of Music, Kingston University, *Assessment and Evaluation in Higher Education*, *22*, 371-383.

[11] Chih-Ming Chen, C. M., & Tsai, Y. N. (2010). Interactive Location-based Game for Supporting Effective English Learning, *International Journal of Intelligent Information Technology Application*, *3*(1), 44-50.

[12] Lan, C., Lai, K. R., Chou, C., & Chao, K. (2012). A Study in Negotiation-based Peer Assessment : Natural Language Applied in Assessment Representation. *International Conference on Computers in Education(ICCE).*

[13] Davies, P. (2000). Computerized Peer Assessment. *Innovations in Education & Training International*, *37*(4), 346–355.

[14] Lin, S. S. J., Liu, E. Z. F., & Yuan, S. M. (2001). Web-based peer assessment : feedback for students with various thinking-styles. *Journal of Computer Assisted Learning*, *17*, 420–432.

[15] Chang, W., & Tan, Q. (2010). Augmented Reality System Design and Scenario Study for Location-Based Adaptive Mobile Learning, *Proceedings of IEEE International Conference on Computational Science and Engineering*, 20–27.

[16] Penuel, W. R., Lynn, E., & Berger, L. (2007). Classroom assessment with handheld computers, *Ubiquitous Computing in Education*, 103–125.

[17] Shin, N., Norris, C., & Soloway, E. (2007). Findings from early research on one-to-one handheld use in K-12 education, *Ubiquitous Computing in Education*, 19–39.

[18] Chang, W., Tan, Q., & Tao, F. W. (2010). Multi-Object Oriented Augmented Reality for Location-Based Adaptive Mobile Learning, *Proceedings of IEEE International Conference on Advanced Learning Technologies*, 450–451.

[19] Chen, C. (2010)..The implementation and evaluation of a mobile self- and peer-assessment system. *Computers & Education*, *55*(1), 229–236

[20] Azuma, R. T. (1997). A Survey of Augmented Reality, *Presence: Teleoperators and Virtual Environments*, *6*(4), 355–385.

[21] Azuma, R., Baillot, Y., Behringer, R., Feiner, S., Julier, S., & MacIntyre, B. (2001). Recent advances in augmented reality, *IEEE Computer Graphics and Applications*, *21*, 34–37.

[22] Anastassova, M. (2007). User-Centred Design and Evaluation of Augmented Reality Systems for Industrial Applications: Some deadlocks and breakthroughs, *Proceedings of IEEE International Conference on Virtual Reality*, 215-224.

[23] Chen, C., Li, Y., & Chen, M. (2007). Personalized Context-Aware Ubiquitous Learning System for Supporting Effectively English Vocabulary Learning, *Proceedings of IEEE International Conference on Advanced Learning Technologies*, 1–3.

[24] Michie, M. (1998). Factors influencing secondary science teachers to organise and conduct field trips, *Australian Science Teacher's Journal*, *44*(4), 43-50.

[25] Patten, B., Sanchez, I. A., & Tangney, B. (2006). Designing collaborative, constructionist and contextual applications for handheld devices, *Computers & Education*, *46*, 294–308.

[26] NMC Horizon Report (2012). *NMC Horizon Report: 2012 K-12 Edition*, http://www.nmc.org/publications/2012-horizon-report-k12.

[27] Van Krevelen, D. W. F., & Poelman, R. (2010). A Survey of Augmented Reality Technologies, Applications and Limitations, *The International Journal of Virtual Reality*, *9*(2), 1-20.

[28] Hollerer, T., Feiner, S., Hallaway, D., & Bell, B. (2001). User Interface Management Techniques for Collaborative Mobile Augmented Reality, *Computers and Graphics*, *25*(5), 799-810.

[29] Nokia Research Center, NRC. (2009). Mobile Mixed Reality: The Vision, *Nokia Technology Insights Series*.

國中學生英語閱讀電腦化測驗之編製與發展

廖麗珍[1] 邱毓芳[2] 郭伯臣[3] 白鎧誌[3] 白宗恩[3]
亞洲大學 資訊工程研究所[1]
國立臺中教育大學 教師教育研究中心[2]
國立臺中教育大學 教育測驗統計研究所[3]
lich@gm.cajh.chc.edu.tw, yvonnechiou65@gmail.com, kbc@mail.ntcu.edu.tw, minbai0926@gmail.com, smallwhite219@hotmail.com

摘要

本研究目的為依據國中英語教材和「九年一貫課程綱要」英語科中「讀的能力指標」，編製與研發仿教育會考的國中學生英語閱讀電腦化測驗，以彰化縣一所國中的 345 位三年級學生為樣本，檢驗其信度與效度。以試題反應理論分析，平均鑑別度為 1.40，平均難度為 0.066，平均猜測度為 0.243，屬於難易適中的測驗，並且鑑別度良好；在測驗信度考驗方面，內部一致性信度 α 係數為 0.896；效度採專家效度，請英語系教授審題，因此本測驗具良好信度與效度。此外，本研究以真實測驗資料模擬電腦化適性測驗施測程序，比較最大概似估計法、最大後驗估計法與期望後驗法在電腦化適性測驗評估的成效，研究結果顯示使用期望後驗法成效教佳。

關鍵詞：英語閱讀、電腦化測驗、電腦化適性測驗評估。

Abstract

The purposes of this study were to develop an English reading computer-based test for junior high school students imitated from Education Examination based on junior English textbooks and English reading ability index for Nine-year Curriculum Outline. Three hundred forty-five ninth grade students sampled from an junior high school in Changhua participated in this study to verify the reliability and validity of the test, which was the main instrument in this study. Analyzing items with IRT, 3PL model, the mean of discrimination (a), difficulty (b), and guessing(c) are 1.40, 0.066 and 0.243 respectively. Therefore, it could be called a test with moderate difficulty and good discrimination percentage. According to the result of the reliability examination, the Cronbach value of internal consistency was 0.896. Moreover, criterion validity was based on expert validity. The researcher asked the English professors to revise the items. As a result, the English reading computer-based test for junior high school students has good reliability and validity. Besides, this study simulated computerized adaptive testing (CAT) measuring program with real test data and compared the effects of computer adaptive testing assessments for MLE(maximum likelihood estimation), MAP(maximum a posteriori), and EAP (expected a posteriori). In the end, EAP turned out to be the most efficient in assessing the effects of CAT according to the findings of this study.

Keywords: English Reading, computer-based test, computer adaptive testing assessment.

1. 前言

隨著地球村時代的來臨，全球人類社會的互動更加頻繁，國際間政治、經濟、文化的交流愈為密切，被公認為世界共通語的英語，遂成為國際交流的重要溝通工具。此外，透過學習英文，學習者可以適切回應英語為母語的國家之社會文化活動並增進多元文化的瞭解與尊重。根據英國文化協會的報告，全世界約有八成以上的文獻資料是英文，而且大部分學者和科學家習慣以英文來閱讀。對許多學生來說，提昇英語閱讀能力和英語溝通能力成為適應當前競爭劇烈社會最迫切的需要。足見英文已是 e 世代吸收知識的關鍵能力，也讓政府意識到，英語能力之良窳，將決定下一代擷取知識的深度與廣度。在這樣的社會殷切期待下，自九十四學年度起英語教學已提早至國小三年級全面實施。

1.1 研究動機

教學與評量並非兩條平行線，評量是教學當中不可或缺的重要部分，成功的教學，需透過評量的「程序」才能判定。教師能由評量的結果，瞭解教學的成果，以做為修正教學進度與掌握學生學習成效的參考，另一方面，具優良信效度的評量能提供學生適當的回饋，有助於瞭解自己的能力，藉此判斷需加強哪些單元的學習，足見評量之於教學的重要性。

國中教育會考(以下簡稱教育會考)是評量國中學生三年學習成果的重要測驗，教育會考的成績也是國中畢業生申請免試入學時作為超額比序的主要依據。而今年試辦的國中教育會考和國中基測一樣，受試學生仍需畫卡，然後再運用電腦讀卡與計

算成績，而此種測驗方式從出題、讀卡、到成績分析統計等，部分作業仍需靠人工完成。因此，隨著電腦科技的發達，愈來愈多的測驗，都改以電腦化測驗(computer-based test, CBT)進行，目前大型測驗如 GRE 和 TOEFL 已採行 CBT 或 IBT 模式施測。由於 CBT 和 IBT 具有不少優點，例如：(1)測驗的效率提高，能立即得知分數，快速處理相關的資料；(2)減少測驗時間，根據 Olsen、Maynes 和 Slawson [1]等人的研究指出，以電腦來實施同一版本的紙筆測驗，測驗時間只有紙筆測驗的 57%；(3)受試時間彈性大，受試者可隨時進行線上評量；此外，(4)可記錄解題歷程，CBT 能夠記錄受試者閱讀題目所需的時間、是否更改過答案、作答的順序等，讓教師瞭解學生的解題技巧以及困難所在，可幫助改進測驗或瞭解學生的障礙。

現行所有國中英語版本中，內容涵蓋很多重要的文法知識與艱深的句型，如關係代名詞、現在完成式、假設語氣…等較難理解的句型，使得多數學生覺得準備不易，對國三學生來說，教師教授新課程的時間已很緊湊，而教育會考時間約在國三下學期第二次段考後（5 月中旬），教師必須在此時間點之前教授完國三下學期課程並複習完國一、國二的課程實不容易！因此啟發研究者思考，若能編製一份符合教育會考英語科命題方向的試題並建置電腦化評量系統，讓學生可於課餘時間練習，又能得到立即回饋，有助於學生及時發掘自己的學習困難所在，亦利於教師實施補救教學。

1.2 研究目的

基於上述研究動機，研究目的如下；

I 仿教育會考的命題架構編製「國中英語閱讀成就」測驗試題，檢驗其信度與效度。

II 發展「國中英語閱讀學習成就」線上測驗系統。

III 根據實徵資料分析最大概似估計法、最大後驗估計法與期望後驗法等三種能力估計法的電腦化適性測驗成效。

2. 文獻探討

本研究目的旨在依照「國民中小學九年一貫課程綱要」英語科第二階段能力指標編擬一份仿教育會考國中英語閱讀成就測驗的試題，對一群國三學生進行電腦化測驗，而電腦化測驗是以試題反應理論為基礎的測驗模式，故在本章分別就教育會考的試題編製、教育會考英語科的試題編製、試題反應理論及電腦化評量進行探討。

2.1 國中教育會考的試題編擬

教育當局為適度舒緩國中學生學習壓力，自 103 年起十二年國民基本教育政策將正式實施，中央及地方主管機關為了解及確保國中畢業生學力品質，將辦理「國中教育會考」，作為我國國中畢業生學力檢定之機制，而這項入學考試變革的宗旨即為在「降低壓力以活化學習」和「確保品質以維持競爭力」兩個目標之間求得平衡，換句話說，教育會考將在十二年國教的改革過程中，扮演適度降低壓力和維持競爭力的角色[2]。

2.1.1 國中教育會考的試題編製

教育會考各學習領域試題之取材以學生學習及生活經驗為主要來源。每個題目都依明確的能力指標設計，並經過審查，以確保題目可以反映該能力指標。各學習領域一般命題原則如下：

1. 以能經由紙筆測驗評量的能力指標為主。
2. 以能有效檢測學生能力水準為目的。
3. 以符合綱要不涉及素材（版本）之選取為方針。

教育會考和國中基測一樣，試題係依據九年一貫課程綱要國中階段能力指標來命題，採教材（內容）、能力之雙向評量方式研發，測驗的精神在評量學生基本、核心、重要的知識與能力，但測驗試題難度以「難易適中」為原則[3]。

教育會考為一標準化測驗，依「闈外建置題庫，闈內依組題計畫抽組試題」為試題研發方式，茲說明組題計畫如下：

教育會考的題本由闈場的組題電腦系統來選題，無法事先得知系統組成的測驗試題，其組題的原則為評量需符合教育會考目的，目的為能精確區分「基礎」與「精熟」能力等級的學生；試題取材均勻分布；生活化、統整化素材優先；試題平均通過率為 .5～.6，另外，林世華指出試題難度低於 30%的不可出現，因為通過率低於 30%時，就不算是基本的試題[4]。

題庫中的測驗組合系統可使選題程序電腦化，以避免人工選題產生的疏失與不公正的現象。在選題策略上，國中教育會考使用 0-1 線性規劃來作為選題程式的主幹，依據題目的各種屬性（例如：題目的類型、認知層次、所屬的章節範圍…等），以及各項統計上的指標（例如：題目的難度、鑑別度、訊息量…等），設計出線性方程組的限制條件，再配合線性規劃求取目標函數的極大（小）值進行組題。相較於隨機選題或是人工組題，經由這樣的組題程序所獲得的題本，在難度及類型的題數分布上，較為客觀[5]。

2.1.2 國中教育會考英語科試題的編製

教育會考英語科試題的研發係以「國民中小學九年一貫課程綱要」英語科國中階段能力指標為依據，試題編寫以一千兩百基本字彙為主，考生在一

般學習狀況下習得基本英語聆聽及閱讀能力，不論使用哪一版本，均能夠作答，不須習讀所有版本。

依據課程綱要，國民中小學英語課程目標為：

1. 培養學生基本的英語溝通能力，俾能運用於實際情境中。
2. 培養學生學習英語的興趣與方法，俾能自發有效地學習。
3. 增進學生對本國與外國文化習俗的認識，俾能加以比較，並尊重文化差異。[6]

在課程綱要中，英語科課程分為國小和國中兩個階段，兩階段之教學重點是不同的。國小以聽、說為主，讀、寫為輔；國中則聽、說、讀、寫並重。

有關英語國中階段讀的能力指標為：

3-2-1 能辨識英文字母的連續書寫體。
3-2-2 能用字典查閱字詞的發音及意義。
3-2-3 能看懂常用的英文標示和圖表。
3-2-4 能用適切的語調、節奏朗讀短文、簡易故事等。
3-2-5 能瞭解課文的主旨大意。
3-2-6 能瞭解對話、短文、書信、故事及短劇等的重要內容與情節。
3-2-7 能從圖畫、圖示或上下文，猜測字義或推論文意。
3-2-8 能辨識故事的要素，如背景、人物、事件和結局。
3-2-9 能閱讀不同體裁、不同主題的簡易文章[6]。

國中教育會考英語科閱讀測驗主要是評量基本重要概念，非片斷的記憶，試題編寫重視真實語言使用的整體自然情境，呈現多種體裁及主題。

國中教育會考英語科聽力與閱讀測驗合計共60題，其中前20題為聽力試題，後40題為閱讀試題。本研究範疇為閱讀學習成就測驗試題。題本架構包括單題和題組兩種題型，其中單題部分主要在評量語言知識，如字彙、語意和語法；題組則是評量篇章理解能力，包括克漏字和整段式閱讀測驗文章。以102年試辦國中教育會考英語科閱讀測驗的題組選文而言，除了文章及對話等一般體裁，也有電子郵件、圖表、詩歌、網頁廣告及新聞報導等各式體裁[7]。

2.2 試題反應理論

為了改進古典測驗理論的缺失，因而產生當代測驗理論[8]，當代測驗理論以試題反應理論為基礎，是一具有合理與嚴謹的立論與假設的學說，採用複雜艱澀的計算公式，所適用的測驗資料種類雖屬有限，但深受測驗學者的青睞，有後來居上之勢。

試題反應理論(item response theory, IRT)又稱作潛在特質理論，建立在兩個基本概念上：(1)受試者的答對機率受到本身潛在特質或能力的影響[9]。(2)受試者的表現與潛在特質間的關係可由一條連續性的試題特徵曲線來加以詮釋[10]。

試題反應理論為試題獨立的能力估計值，不會受不同測驗種類的影響；其次，它是樣本獨立的試題參數估計值，不會受到不同族群考生的影響。

IRT有四項基本假設：單向度、局部獨立性、非速度測驗與知道—正確假設[11]。而IRT的試題參數模式可分為單參數模式（Rasch模式）、二參數模式和三參數模式[12]，都只適用於二元化的反應資料。教育會考和基測一樣，測驗題庫均採用Rasch模式，在此模式中影響受試者答對率的試題參數只考慮難度參數，未考慮鑑別度與猜測度等參數，較無法呈現試題的內部一致性信度，故本研究將採三參數模式做試題分析。

三參數模式(three-parameter logistic model)可用公式1表示：

$$P_i(\theta) = C_i + (1 - C_i)\frac{e^{a_i(\theta - b_i)}}{1 + e^{a_i(\theta - b_i)}} \qquad i = 1,2,\ldots,n \qquad (1)$$

其中，$P_i(\theta)$表示能力為θ的考生在試題i上正確反應的機率；b_i表示試題難度(difficulty)參數；a_i表示試題鑑別度(item discrimination)參數；c_i表示猜測度參數(pseudo-chance parameter)；n是該測驗的試題總數；e代表以底為2.718的指數；且$P_i(\theta)$是一種S形曲線，其值介於0與1之間[12]。

2.3 電腦化評量系統

電腦化測驗已是世界發展的趨勢，除了可運用多媒體科技，讓試題以色彩、聲音、動畫、互動、操作等方式呈現，測驗資料可進行試題分析及信度與效度估計，此外，近年來由於網路頻寬加大及資料傳輸速度提高，透過網路實施電腦化適性測驗也漸漸增加。目前電腦化測驗系統的建置多以IRT模式做為理論基礎，較複雜的模式也引進到電腦化測驗系統中，如：CAT (Computer Adaptive Testing)。目前國外已經發展電腦化評量系統的如美國軍方電腦化職業性向測驗系統、英國劍橋大學英文考試院（Cambridge ESOL）發展出的BULATS英語能力檢定和ETS(Educational Testing Service)所承辦的TOEFL、GRE等測驗；國內則包含TOEFL測驗、交通部公路局的汽機車駕照考試和考選部的航海類專技人員考試都已實施電腦化測驗。

3. 研究方法

本研究旨在編製仿教育會考國中英語閱讀成就測驗試題和發展線上測驗系統。根據研究動機、研究目的，透過文獻與國中現行教科書其中四個版本的分析與探討，並參考教育會考的題本架構，編製適合國三學生的閱讀學習成就測驗試題，並建置電腦化測驗系統以作為學生自我評量的工具。

3.1 電腦化測驗研發

本研究蒐集近兩年的模擬考題本和歷年基測試題，諮詢領域專家與國中現職英語教師之意見，決定以 1,200 基本字彙為可命題的字彙，接著根據教育會考英語科的命題原則和國中階段讀的能力指標之檢核重點，從模擬考題本和基測試題中挑選基本、核心概念和重要知識的試題，與國中現職英語教師就題目內容進行討論，並請英語學者幫忙修審試題，以確保試題品質和可行性。表 1 為正式組卷的試題分布情形如下：

表 1 試題分布

能力指標	分佈題號
3-2-1	第 2, 3 題
3-2-3	第 27, 28, 29, 30 題
3-2-5	第 24, 26, 39 題
3-2-6	第 4, 5, 8, 11, 13, 14, 16, 19, 25 題
3-2-7	第 1, 6, 7, 9, 10, 12, 15, 17, 18, 31, 32, 35 題
3-2-8	第 20, 21, 22, 23, 33, 36 題
3-2-9	第 34, 37, 38, 39 題

其中能力指標 3-2-2 和 3-2-4 實務上無法透過電腦化評量系統施測，需耗費很多人力當面施測，是故，不適合研發相關題目。

組卷完成後，本研究直接開發「電腦化測驗系統」，提供使用者由 IE 瀏覽器進入系統施測。以下為系統介面步驟說明和執行畫面：

一、登入系統

每位受試者會有自己的帳號、密碼登入系統施測，如圖 3.1 所示。



圖 3.1 登入系統畫面

二、進行電腦化測驗，如圖 3.2 所示。



圖 3.2 進行電腦化測驗畫面

3.2 測驗資料分析

為瞭解試題品質，研究者採用測驗的實徵資料進行試題分析，在估計過程中無法收斂者、試題通過率偏低等情況的試題予以刪除，重新估計後所餘試題為 39 題。

為了顧及測驗資料品質，本研究參考國外大型測驗的檢核程序，訂定仿教育會考國中英語閱讀成就測驗的無效樣本檢核準則，簡述如下：

(1) 考生的作答反應有疑似亂答情況（規則性作答）
(2) 考生整份測驗作答時間在 30 秒內，且答對率低於 0.25

關於不良試題的檢核準則，參考 IRT 估計之參數值，訂定標準如下：

1. IRT 的試題鑑別度參數小於 0.4 ($a < 0.4$)
2. IRT 的試題難度參數小於 -2（$b < -2$）；或者大於 2（$2 < b$）[12]

本研究使用 SPSS 進行內部一致性信度分析，藉著信度估計來檢定測驗中試題之一致性或關聯性，若 Cronbach's α 值很低，表示試題之間的關連性很低，也就是測驗不具信度。針對一般性的研究來說，內部一致性估計可接受數值為 .80，標準化成就測驗 α 係數最好在 .9 以上；至於效度分析方面，本研究透過專家學者對於內容上的專業知識，進行題項與形式之審查，是故，本研究是採專家效度。

本研究以 BILOG-MG 軟體進行 IRT 各模式之試題參數估計，由於本測驗採選擇題的方式，含猜測成分，因此採三參數的估計，即鑑別度、難度和猜測度參數。此外，利用 IRT 來分析本研究之測驗資料，需滿足 IRT「局部獨立」的假定。本測驗資料分析包括 39 道試題，每道題目均測量不同的語意或句型，亦即每一題的答對機率不會因受試者在其他題目的表現所影響。

3.3 電腦化適性測驗評估

電腦化適性測驗（Computer Adaptive Testing, CAT）的原則是依照受試者的作答反應估計出其能力值，然後提供適合受試者能力的題目進行施測，然而在測驗開始時，並不知受試者能力值，所以必須先決定測驗的起始點，以選擇試題供受試者施測。常用的選題法如：依受試者能力選題、中等難度題目選題、自由選題、隨機選題等。本研究目的為建置一個完整的電腦化測驗系統(computer-based test, CBT)，不過目前電腦化適性測驗已是教學評量的發展趨勢，啟發研究者思考，使用測驗的實徵資料進行電腦化適性測驗評估，而為了進行適性測驗評估，採用較常見的能力估計方法，例如：最大概似估計法（maximum likelihood estimation, MLE）與貝氏估計法（Bayesian procedure）中的最大後驗估計法（maximum a posteriori, MAP）與期望後驗法

（expected a posteriori, EAP），以下分別介紹：

a. 最大概似估計法（MLE）

假設測驗共有 n 道試題，試題間彼此獨立，概似函數（likelihood function）如下式（2）所示：

$$L(u|\theta)=L(X_1 \ldots\ldots X_n|\theta)=\prod_{i=1}^{n} P_i^{X_i} Q_i^{1-X_i} \quad (2)$$

◆為所有作答反應的向量，$L(X_1 \ldots X_n|\theta)$為概似函數；θ 為受試者的真實能力；X_i 指受試者在第 i 題的作答反應，答對為 1，答錯為 0；P_i 指受試者在第i題的答對機率；Q_i 指受試者在第 i 題的答錯機率[13]。

b. 期望後驗估計法（EAP）[14]

Bock 與 Mislevy 主張 EAP 是尋找能力值的事後機率密度函數的期望值，如公式（3）所示：

$$\theta_{EAP}=\sum_{q=1}^{k_q}\theta_q f(\theta_q|\mathrm{U})=\sum_{q=1}^{k_q}\theta_q \frac{L(\mathrm{U}|\theta_q)f(\theta_q)}{\sum_{q=1}^{k_q}[L(\mathrm{U}|\theta_q)f(\theta_q)]} \quad (3)$$

u 為所有作答反應的向量，$L(\mathrm{U}|\theta_q)$為概似函數；θ_q 為受試者的真實能力；q是計算能力的期望值時所切割成的分割點，共有 k_q 點，k_q 愈大，計算愈精確。

c. 最大後驗估計法

MAP 是以受試者的事前能力分布 $f(\theta)$作為加權值，形成事後機率密度函數，並找出能使此事後機率密度函數最大化的程度值。事後機率密度函數的計算式（4）如下：

$$\mathrm{f}(\theta|\mathrm{U})=\frac{\mathrm{L}(\mathrm{U}|\theta)\mathrm{f}(\theta)}{\mathrm{f}(\mathrm{U})} \quad (4)$$

$\mathrm{L}(\mathrm{U}|\theta)$是受試者$\theta$的概似函數，$\mathrm{f}(\mathrm{U})$是受試者的邊際機率，是由$\mathrm{L}(\mathrm{U}|\theta)\,\mathrm{f}(\theta)$從$-\infty\sim\infty$積分所得，若要加速找到事後機率密度函數的最大值，通常以 Newton-Raphson 法來進行迭代。

本研究以上述之能力估計法進行參數估計值誤差評估以診斷出能最快達到適性目的的能力估計法；而參數估計值誤差評估的過程為視原始生成參數為真值，以真值產生作答反應，再以作答反應進行參數估計後得到估計值，計算真值與估計值的均方根誤差（root mean squared error, RMSE）。當均方根誤差值在0.2以下時，測驗即可終止，因為此種情形就是適性測驗。以上三種能力估計法估RMSE是根據能力值計算。其數學式為：

$$RMSE(\theta)=\sqrt{\frac{1}{N}\sum_{i=1}^{N}(\theta_i-\hat{\theta}_i)^2}$$

$\hat{\theta}_i$：第 i 位能力值估計值

θ_i：第 i 位能力值真值

N：受試者人數

3.4 研究對象

本研究以彰化縣一所國中三年級 14 個班級的學生為研究對象，共計 410 位，其中有效樣本為 345 人。

3.5 研究工具

a. 基測和教育會考試題

本研究利用四個版本國中英語教科書的基本、核心、重要的教材內容來檢核試題，並配合九年一貫國中英語科讀的能力指標以分析基測試題及試辦教育會考考題的命題原則，以上述分析的結果作為依據，評估本研究編製的試題內容、認知層次是否符合國中教育會考的方向，然後形成線上測驗的正式組卷。

b. 線上測驗系統

研究運用的線上測驗系統是由國立臺中教育大學教育測統所研發的「電腦化測驗診斷系統」，針對研究對象進行線上電腦化測驗與成效評估。

c. 各項統計分析軟體

BILOG-MG 軟體

本研究使用 BILOG-MG 軟體能夠估計測驗試題的參數值，包括難度、鑑別度、猜測度及受試者的能力值[15]。

SPSS 統計分析軟體

統計分析軟體 SPSS 是用於大量資料的統計分析，本研究以 SPSS 分析測驗的信度及相關係數。

MATLAB 軟體

利用 BILOG-MG 估計的試題參數值和受試者能力值，再透過 MATLAB 軟體撰寫 MLE、 EAP、和 MAP 等三種能力估計方式，以分析出何種方法可使本研究的電腦化測驗最快達到適性的效果。

4. 研究結果

依據前述之研究方法，本章以研究對象施測之資料為基礎，透過測驗理論和研究工具針對測驗結果進行分析和估計，此外，研究者利用不同能力估計方法評估電腦化適性測驗成效。以下為研究結果的分析與討論。

4.1 測驗結果描述

本研究測驗信度 Cronbach's α 值為 .896，顯示測驗信度佳；而效度檢定採專家效度，研究者邀請兩位國立臺中教育大學英語系教授依據自身在學科上之專業知識，進行試題內容與題型之審查。

實施電腦化測驗後，依自訂的無效樣本指標，刪除 65 位無效樣本，共 345 位有效樣本；並依據 IRT 的不良試題檢核標準，刪除試題，剩餘試題共 39 題。接著，以 BILOG-MG 軟體做 IRT 之試題參數估計，顯示平均難度參數為 0.066，符合教育會考「難易適中」原則；試題平均通過率為 0.601，大致符合教育會考試題平均通過率 0.5～0.6 的標準；平均鑑別度參數為 1.395，顯示測驗具良好鑑別度；平均猜測度值為 0.243，符合 IRT 猜測度參

數小於 0.3 的指標，而受試者的能力估計值為 -2.248～2.215 之間，在正常值 -4～+4 範圍。

4.2 電腦化適性測驗評估結果

本研究以真實測驗資料模擬 CAT 施測程序，比較最大概似估計法（maximum likelihood estimation, MLE）、最大後驗估計法（maximum a posteriori, MAP）與期望後驗法（expected a posteriori, EAP）不同能力估計法在電腦化適性測驗評估的成效，三種能力估計法模擬 CAT 施測成效如圖 4-1。

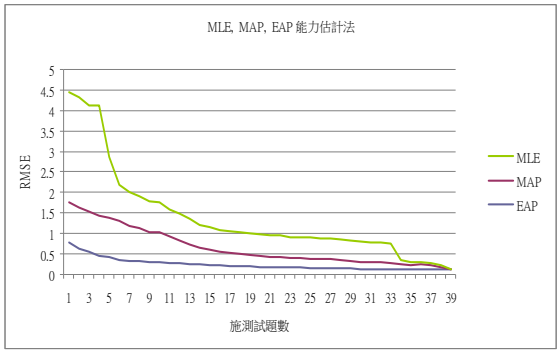


圖 4-1 不同能力估計方法之精確度

圖 4-1 為使用三種能力估計方法在不同測驗長度下與施測全部試題 RMSE 的變動情形，圖 4-1 顯示不論使用哪一種估計方法，當施測題數累積愈多，RMSE 的下降就愈明顯。從估計結果顯示 MLE 估計法測驗題數在 30 題之前，RMSE 都大於 0.5；總題數達到 34 題時，RMSE 小於 0.2；MAP 估計法施測總題數在 12 題以前，RMSE 都大於 0.5；當總題數達 29 題時，RMSE 小於 0.2。EAP 估計法施測總題數達 4 題時，RMSE 小於 0.5；總題數達 19 題時，RMSE 小於 0.2。在這三種估計法中，EAP 估計法得到較低的 RMSE，此結果與陳柏熹提出的研究結果類似，因此在適性功能的評估中，使用 EAP 估計法成效較佳〔16〕。

5. 結論與未來研究方向

透過研究樣本測驗資料分析結果顯示，本研究研發之測驗信度介於 0.890～0.903 間，且具有良好的效度，整份試題都經過領域學者專家縝密修審，具有一定的品質，未來可做為一般國三學生英語閱讀能力測驗檢測之工具。

本研究使用 IRT 三參數模式能改善 CTT 模式的諸多缺點，且和教育會考測驗題庫僅採用 Rasch 模式分析測驗資料比較，本研究較能呈現內部一致性信度。

本研究研發之仿教育會考英語閱讀成就測驗配合英文電腦化評量系統進行施測，教師可透過系統介面管理者得知學生的施測成績，作為補救教學的依據；使用者可隨時登入系統介面，以帳號和密碼註冊回傳即進行線上測驗，施測完可立即看測驗結果報告得到回饋；管理者能夠在試題庫管理介面隨時新增或修改試題，也可取得受試者作答反應。

未來將視教科書內容變動，更新或增修試題，也計劃擴充試題規模建立題庫，以國立臺中教育大學教育測統所建構的適性化評量系統為平台，使用者由 IE 瀏覽器進入平台並註冊帳號、密碼，即可開始測驗。經由此適性評量系統，使用者可依個別能力差異進行不同長度的測驗，達到省題和省時的目標。

參考文獻

[1] Olsen, J. B., Maynes, D. D., & Slawson, D., Comparison and equating of paper-administered, computer-administered, and computerized adaptive tests of achievement, San Francisco: Paper presented to the annual meeting of the American Educational Research Association, 1986.

[2] 教育部，十二年國民基本教育落實國中教學正常化、適性輔導及品質提升方案，中央及地方主管機關，2012。

[3] 臺灣師大心測中心，國中教育會考試題取材與命題原則，（台北市，2012）。

[4] 林世華，國民中學學生基本學力要如何走下去，（飛揚月刊，第九期，2008），取自 http://www.bctest.ntnu.edu.tw

[5] 宋曜廷、許福元、曾分蘭、蔣莉蘋、孫維民，國民中學學生基本學力測驗的回顧與展望，（台北：教育研究與發展期刊，第三卷第四期，2007），pp. 34-38。

[6] 教育部，國民中小學九年一貫課程綱要語文學習領域（英語），（台北市，2008）。

[7] 教育部，國中教育會考英語科加考聽力測驗說明，台北市，2012。

[8] 王寶墉，現代測驗理論，臺北：心理出版社，1995。

[9] Hambleton, R. K., & Cook, L. L., Latent trait models and their use in the analysis of educational test data. Journal of Educational Measurement, 14, 1977, 75-96.

[10] Lord, F. M., Practical applications of item characteristic curve theory. Journal of Educational Measurement, 14, 1977, pp. 117-138.

[11] 余民寧，試題反應理論的介紹（二）－ 基本概念和假設，研習資訊 9 卷 1 期，1993，pp. 5-9。

[12] 余民寧，試題反應理論的介紹（三）－ 試題反應模式及其特性，研習資訊 9 卷 2 期，1993，pp. 6-10。

[13] Bock, R. D., & Aitkin, M., Marginal maximum likelihood estimation of item parameters: Application of an EM algorithm. *Psychometrika, 46,* 1981, pp. 443-459.

[14] Bock, R. D. & Mislevy, R. J., Adaptive EAP Estimation of Ability in A Microcomputer Environment, Applied Psychological Measurement, 6, 1982, p.431-444.

[15] Birnbaum, A., Some latent trait models and their use in inferring an examinee's ability. In F. M. Lord and M. R. Novick, Statistical theories of mental test scores, 17-20. Reading, MA: Addison-Wesley, 1968.

[16] 陳柏熹，能力估計方法對多向度電腦化適性測驗測量精準度的影響，教育心理學報，38 (2), 2006, pp.195-211.

結合三段式 IRF 教學對話之英語文法學習系統

蔡維軒　蘇建元　趙偉智　張家瑋　王宗一*
成功大學工程科學系
pa015596@gmail.com ; bredysu@gmail.com
n98981161@mail.ncku.edu.tw ; jaiweichang@gmail.com ; *wti535@mail.ncku.edu.tw

摘要

在課程教學中，透過教學對話的方式能幫助學生糾正錯誤觀念並快速建構知識。其中 Initiation, Response, Follow-up or Feedback（IRF）教學對話模式已被證明為有效的教學策略且應用在許多學科之中，本研究嘗試設計並開發一結合 IRF 教學對話模式之智慧型英語文法學習方式，並建構出具策略效用的國中英語文法數位學習環境，提供學習者學習並強化國中英語文法觀念。該系統具自動發問與回饋機制，並根據不同程度學習者的答題情況，適性地引導學習者改正英語文法的錯誤概念。

為證明導入 IRF 教學對話模式於英語文法學習系統的效果，本研究實驗採準實驗設計(quasi-experimental design)中「不等組前後測」設計方式，共有 85 位國二學生參與，分為實驗組及兩組控制組，分別參與使用具 IRF 模式及分層次回饋的系統，進一步探討運用不同層級的回饋機制，在 IRF 模式與不使用 IRF 模式下，學生對英語文法學習的效果。實驗採單因子共變數分析方式，由三組的前後測結果得知，藉由不同層次回饋的情形下，使用 IRF 模式的學生顯著優於不使用 IRF 模式的學生；在 IRF 模式下，整體上使用分層次回饋的學生與不使用分層次回饋的學生則無顯著差異，然而在簡單的文法概念下則有顯著差異。

關鍵詞：電腦輔助語言學習；英語文法學習；三段式教學對話；文法檢查。

1. 前言

多媒體與網路普及下，藉由電腦來輔助語言學習（Computer Assisted Language Learning，CALL）以已成為許多人日常生活中語言學習的方式之一，其不受時間、地點限制的優勢外，數位語言教材亦可提供高互動性、立即回饋、適性安排教材，並允許與各種不同的學習輔具或學習平台進行搭配，營造出個人化的數位化語言學習環境。

我們知道語言的學習要有效果，適當的學習策略與數位教材或資源的配合亦顯重要[1]，只單單將教材放置到學習系統上任由學習者自由瀏覽，並無法有效提高學習者的學習效率及效用。因此，妥善的結合學習策略或教學方法，將使得整個學習發揮最大效果。Woodill 與 Officer [2]的研究中也主張數位教材設計或學習平台應融入適當的教學方法並考量到不同學習者的學習能力與經驗。而過去在知識建構與教學方法的應用上，透過教學對話（exchange）是教師有效檢測並了解學習者能力與錯誤概念的重要方法之一，藉由師生教學對話的內容與教學情境中的實際互動，有效幫助學生釐清錯誤與建構新知識 [3]。Initiation, Response, Follow-up or Feedback (IRF)教學對話模式便是其中應用最廣的策略之一，因為這個理由，本研究將嘗試結合 IRF 教學對話模式，建構出一適性化的國中英語文法學習系統，讓學生在語言學習時就像擁有虛擬老師般，能從旁協助與引導學生進行學習。

2. 相關研究

基於上述，本章節分三個小節對相關研究進行歸納與探討。

2.1 電腦輔助英語文法學習系統

近幾年亦有不少關於電腦輔助英語文法學習系統的相關研究，針對運用技術而有不同的設計做法：

(1) 適性化難度調整的英語文法學習系統[4]

該系統運用知識網路的概念，將英文文法的概念的學習，由簡單到複雜建構出一像網絡般的知識網路，讓學習者從最簡單的概念開始學習，並依據學習者的回答情形適性調整後續的學習概念。

(2) 自動生成問題之英語文法學習系統[5]

該系統透過語法剖析的技術以及字詞間的關係，從英語文章中自動生成英語練習題目，檢測學生對於文章的理解度以及英語文法的概念，並依照學習者的學習情形或需求產生適合學習者的題目。

(3) 自動解析文法錯誤之英語文法學習系統[6]

該系統會對學習者提出中翻英問題，問題皆有預設的參考答案，學生回答問題之後，系統則會自動檢查拼字、文法和關鍵字的錯誤情況，而針對錯誤情形給予回饋。

2.2 發問與回饋

過去研究已證實，課堂中透過教師進行發問，由學生進行作答的模式可以提升學生的專注力及學習效果[7]。發問亦能刺激學生思考、理解，而學生的回答情況也能同時讓教師了解學生的認知情形

[8]。Chin[3] 認為在學生作答後，教師能依據學生的答題情況進行推論，並根據不同學生的程度進行各種回饋，其做法能引導學生進行再思考、再矯正，不單單只是純粹性的告知學生答案的對錯，而是更深入的鼓勵與激發學生思考答案背後的含意。Shute [9]亦將回饋應用於電腦測驗中，以類型(type)及時間性(timing)作為區別，依據內容複雜程度進行不同程度的劃分，並指出雖然回饋越詳盡越好，但是如果回饋太長或太複雜也可能同時降低學習者的學習專注力。

2.3 IRF 教學對話模式

IRF 教學對話的運作模式通常是教師在 Initiation（I）階段以測驗或提問的型式進行；接著學生回答（R）已知的資訊；之後教師可以選擇評估（E）學生的回答是否正確，或是在評估後提供適當的回饋（F）[10]。該教學對話模式源自於科學教育，但由於 IRF 亦能提升學生在對話表達上的能力，不少研究將它用於語文的教學上，尤其是第二外語的學習，已有相當不錯的成果，例如 Gourlay[11]用於經濟學的字彙學習並進一步提出 IRFEE (Initiation, Response, Follow-up and Embedded Extension) 的教學對話模式，強化第三步驟 Follow-up 型式的延伸對話內容與程度。Hardman 與 Abd-Kadir 等人[12]研究小學教師課堂上應用 IRF 的情形，探討各種不同學科如英語、數學及科學的應用情形。Temmerman[13]則針對兩間國小高年級學生採用 IRF 模式以幫助學生學習第二外語。

3. 系統設計

要能適性的引導與矯正每位學生的文法錯誤概念，研究人員與英語教學專家教師共同討論出結合 IRF 教學對話模式於英文文法教學互動中可能發生且適用的對話策略情節，並嘗試建置於所開發的三段式英語文法學習系統，以因應針對學生各種不同的文法錯誤，設計出多樣性且具策略效用的英語文法教學對話情景。

3.1 IRF 教學對話模式運作流程

本研究所採用之 IRF 教學對話模式，初步分為 Initiation, Response, Feedback/Follow up 三個階段，分別設計至該學習系統的主要運作流程如圖 1 所示。於 Initiation 階段，首先對學生提出一個新問題，問題採問答或翻譯形式，並針對問題難度分成難、中和易三個難度等級，系統題目的難易程度是由專家教師事先所訂定，一開始給予中等難度的題目，而後根據學生的回答情形適性調整問題難度。Response 階段為學生的答題結果，並由系統自動檢測學生輸入答題句子所犯的文法錯誤類型。Feedback/Follow up 階段會根據學生所犯的文法錯誤類型以及錯誤次數給予相對應的回饋內容，亦會根據學習者作答情形決定出下個問題的難易程度，而回饋機制的運作亦分成三種不同程度的回饋作法(如圖 1)，若學生在接受到第三層回饋前即答對，則系統會加深下個問題的難度。反之，則系統會降低之後所問問題的難度。為避免學習者產生厭倦並降低學習意願，系統設定學習者連續答對三題難度等級為難的題目且是在接受第三層回饋前即答對，則該學習者即可前往下個更深入的英語文法概念進行學習，亦表示學習者對該文法概念已充分瞭解，否則須將該概念中的全部題目做完。

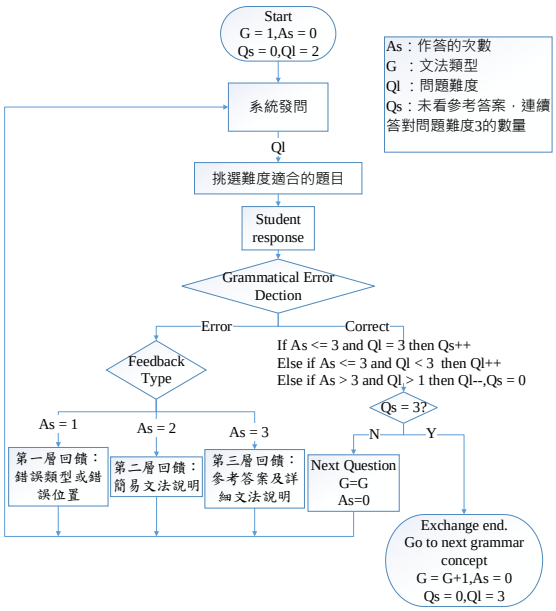


圖 1 IRF 教學對話模式流程圖

3.2 英語文法檢測機制

本系統主要配合國二程度的學生所需學會的英語文法概念進行設計，共涵蓋現在式、頻率副詞與次數表達、過去式、未來式、過去進行式、不定詞、動名詞和連綴動詞等八種不同難易程度的文法概念，當中包含冠詞與介系詞的錯誤檢查，系統所設計的自動檢測與文法錯誤判別共計有 28 種。為了能提高與有利於系統的自動判別與偵錯，前置作業則需先將學生的答題結果轉成詞性節點序列，如圖 2 所示，詞性節點有：主詞、動詞、受詞、形容詞、介系詞、地方副詞片語和時間副詞片語…等等，每個詞性節點皆有其對應的單字，而動詞節點則另外包含該動詞的時態。並透過正規表示法將詞性節點序列與學生輸入的句子進行比對，即可抓出學生答題結果上的語法錯誤。

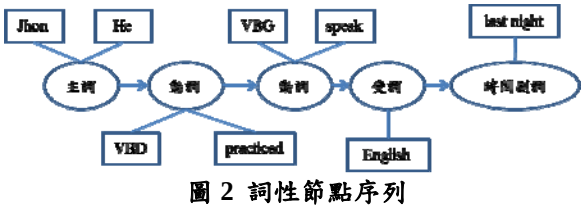


圖 2 詞性節點序列

3.2.1 句型轉換成詞性節點序列

本研究使用 Stanford Parser 語法工具來剖析系統中所用到的所有英文句型，藉以標註出句子的語法結構，該工具是由史丹佛大學所開發[14]，只要置入英文句型，即能輸出為一樹狀的語法結構，如圖 3，語法樹規則即所建立出的上層節點可用來表示較大的概念，第一層代表 ROOT，第二層是 S，代表整個句子結構，將句子劃分成幾個較大的概念，依序為副詞片語、逗號、名詞片語和動詞片語等。

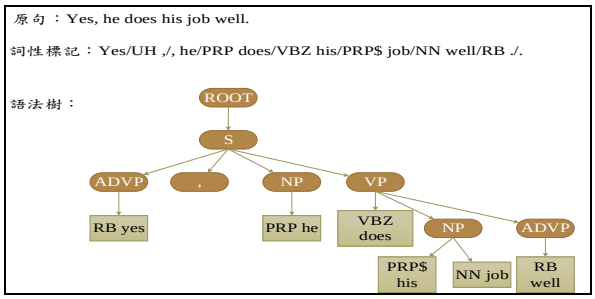


圖 3 語法樹

依照語法樹結構特性，主詞資訊會在第一個名詞片語中，透過正規表示法設計比對樣板，如表 1，或主要動詞資訊會在第一個動詞片語中，則將依序進行拆解，直到找出該標註的詞語特性，如圖 4，在第二步驟中則先取出副詞，像 always, often, usually…等頻率副詞，以簡化語法樹的結構，方便系統進行判斷；而地方副詞及時間副詞則因為這些副詞在語法樹中被標記為介係詞片語或名詞片語，而無法從名詞片語及介係詞片語判斷出該詞組為地方副詞或時間副詞，因此系統建置時會先將常用的時間副詞和地方副詞優先存入資料庫；步驟三會將取出副詞後的句子交由語法剖析工具處理，之後會得到一顆語法樹；步驟四會將樹的結構作簡化；步驟五則會將已經前處理過的語法樹轉為陣列的形式，以利後續處理；步驟六則透過索引值的標註下，由小到大依序將其轉為詞性節點序列。

表 1 抓取主詞的正規表示式樣板

樣板	抓取範例
NP \(NNP (\w+)\) \(CC and\) \(NNP (\w+)\)	NP (NNP Lisa) (CC and) (NNP Kelly)
DT (.*)\) \(NN[S]? (.*)\) \(NN[S]? (.*)\)	NP (DT The) (NN history) (NN lesson)
DT (.*)\) \(NN[S]? (.*)\)	NP (DT the) (NNS boys)

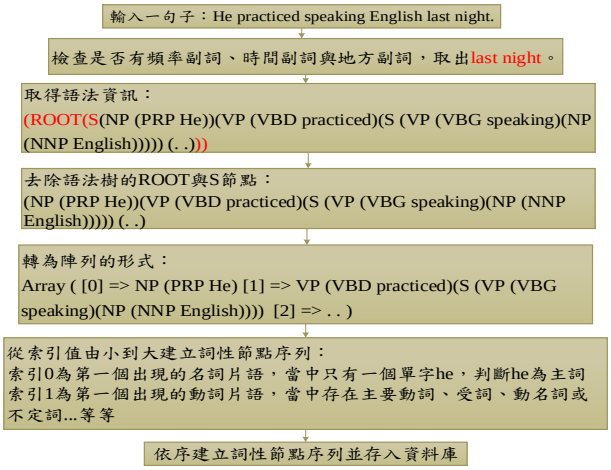


圖 4 句子轉為詞性節點序列化流程

3.2.2 英語文法檢測流程

由於在進行英語文法檢測之前，已完成文法句型的詞性節點序列轉換，因此，便可透過正規表示法將學生的答題語句與系統中優先建立的正確答案詞性節點序列進行比對，找出文法錯誤的地方，其運作流程如圖 5 所示。

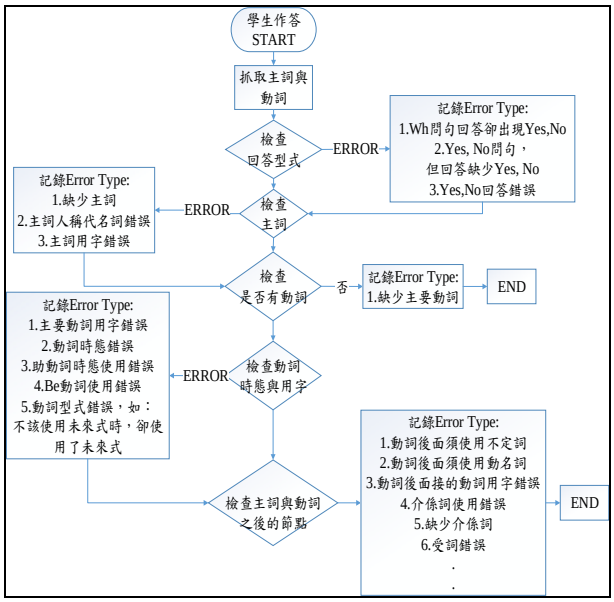


圖 5 文法檢測錯誤流程

系統將學生所輸入的語句經由 Stanford Parser 處理後轉化成語法樹，並從中抓出主詞與動詞資訊。首先檢查學生句子的回答型式，依照系統所設定的問題型式主要分為 wh 問句與非 wh 問句，非 wh 問句的回答型式則需要有 yes, no，在此共分為三種錯誤型態。接著檢查學生的主詞，比對學生句子的主詞與詞性節點序列的主詞節點，在此更細分為三種錯誤型態。接著檢查學生的動詞，首先檢查學生的句子是否有動詞，若沒有動詞則記錄缺少動詞，並停止之後的檢查，因為學生的句子相當不完整，接著透過比對學生的動詞型式與詞性節點序列

的動詞節點，檢查動詞的時態與用字是否正確，在此共分為五種錯誤型態。但主要動詞之後沒有固定的詞性序列，因此這邊採取的檢查方法是結合正規表示法將答案的詞性節點序列與學生句型進行比對，系統檢查的範圍包含：介係詞、受詞、冠詞、頻率副詞、連綴動詞使用、動名詞使用、不定詞使用、時間副詞、地方副詞。最後由系統實際判別出各種錯誤的情形，如表 2。

表 2 系統針對錯誤的英語文法判別情形

學生的句子	參考答案	錯誤類型
No, he will go camping every day.	Yes, David goes camping every week.	Yes, No 錯誤、動詞形式錯誤、時間副詞錯誤
We always studies English on the weekend.	We often study English on the weekend.	動詞時態錯誤、頻率副詞錯誤
Tom and James are sleeping at nine yesterday.	They were chatting at nine yesterday.	Be 動詞錯誤、動詞用字錯誤
He needs to reading the magezine every morning.	He needs to read the magazine every morning.	應使用不定詞、受詞錯誤

3.3 回饋機制設計

為了能符合 IRF 教學對話模式中 feedback 的本質並提供給不同學習者適合的回饋訊息，系統所設計的回饋內容則事先由兩位教學經驗豐富的國中英語教學老師所設計，並參考過去學者們對回饋設計的相關研究，考量到太複雜或長度太長的回饋會降低學生的學習專注力，因此本研究決議採取分層次回饋的方式進行，提供學習者由淺入深的回饋內容，如表 3 所示，第一層回饋會告知學習者文法的錯誤類型或錯誤位置，第二層回饋則提供簡易的文法說明，第三層回饋將提供參考答案和完整詳細的文法說明，其各層回饋的描述如表 4，配合學生的答題情況由系統進行自動的適性調整，如該概念使用的時機與用法、單字放置的位置或詞性的變化規則…等。。

表 3 錯誤類型及其回饋

錯物類型	第一層回饋	第二層回饋	第三層回饋
Yes, No 回答錯誤	答句與圖意不合	Yes, No 使用錯誤	顯示參考答案、句型、文法說明
主詞用字錯誤	主詞錯誤	句子主詞___錯誤，應用___	顯示參考答案、句型、文法說明
動詞時態錯誤	動詞時態錯誤	題目的時態為___式，所以動詞應該用?	顯示參考答案、句型、文法說明
動詞後應用不定詞	動詞___使用錯誤	動詞___後須使用不定詞	顯示參考答案、句型、文法說明

表 4 文法概念的詳細說明

頻率副詞文法概念	頻率副詞放置的位置	(1) Be 之後 EX：They are sometimes at home on Sundays.
		(2) 一般動詞之前 EX：I always go to school on time.
		(3) 助動詞+頻率副詞+動詞 EX：I don't always go to school late.
	常見的頻率副詞	always（總是）, usually（經常）, often（常常）, sometimes（有時候）, seldom（很少）, never（從不）

4. 實驗與結果討論

4.1 實驗設計

實驗對象為台南市某國中二年級三個班級的學生，採用「準實驗設計」方式分成實驗組與兩組控制組，以非等組前後測方式進行實驗，其學習成效評估則採用研究者與專家教師所設計之「英語學習成就測驗卷」做為三組的學習成效評估工具。自變項為分層次回饋與 IRF 機制，依變項則設定為後測成績，共變項為前測成績。

表 5 為各組所接受的教學法，實驗組設定使用 IRF 教學對話模式及接受分層次回饋機制；控制組 A 使用 IRF 教學對話模式及接受最詳細回饋(第三層)和完整參考答案；而控制組 B 則不使用 IRF 教學對話模式，並隨機給予不同難度的題目，且同時接受分層次回饋。其實驗設計流程如圖 6，而整個實驗預計以二周共計 90 分鐘的學習時間進行。

表 5 實驗分組

組別 / 自變項	實驗組 (28 人)	控制組 A (31 人)	控制組 B (26 人)
回饋方式	分層次回饋	直接第三層次的回饋	分層次回饋
題目給予方式	結合 IRF 調整問題難易度	結合 IRF 調整問題難易度	隨機給予不同難度題目

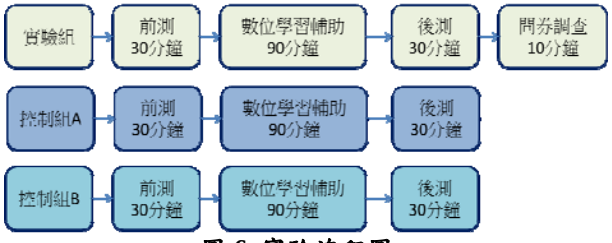


圖 6 實驗流程圖

4.2 實驗結果與討論

為了能確實掌控與引導學生的答題情形，系統

中所建置的試題類型將不採用選擇題形式而完全採用問答方式進行，也因如此，為落實系統能自動且完整、正確地判別出每位學生在回答英語文法的語句，該系統語句的正確判別情形將更顯重要，為此特別針對系統語句判斷的準確度進行分析。

4.2.1 語句檢測準確度驗證

為了評估語句檢測的正確率，本研究採如[6]的 Accuracy 檢測方式進行，以句子為單位，而不是以錯誤類型為單位，以要人工與系統的判斷皆須有相同錯誤或正確才算正確，只要人工與系統判斷的結果不相符則歸為判斷失誤，其計算公式如下：

$$\text{Accuracy}=\frac{\text{系統與人工判斷相同的句數}}{\text{全部的句數}}$$

所採用的分析語句來自於系統所收集的學生作答語句共 12,843 句，依其錯誤類型劃分共 3,502 個不同的句子。並透過上述公式驗證所得的準確性達到 95.09%。

4.2.2 前後測分析

為了檢驗結合 IRF 教學對話模式及分層回饋機制對國二學生於英語文法學習上的影響，實驗數據分析將收集到的前後測分數，採 T 檢定與共變數分析方式進行。其前後測 T 檢定分析結果如表 6 所示，實驗組前後測的 T 檢定結果為 t=6.055(p < .05)，達到顯著差異，顯示實驗組使用結合 IRF 教學對話模式可以有效增進英語文法學習，控制組 A 前後測 T 檢定結果為 t=3.197（p < .05），亦達到顯著差異，顯示出控制組 A 在無分層次回饋機制下，單純運用 IRF 教學對話模式，仍優於控制組 B，顯示出隨機的提供試題方式並無法有效引導學生學習。

表 6 各組前後測成績之成對樣本 T 檢定表

	實驗組		控制組 A		控制組 B	
	前測	後測	前測	後測	前測	後測
平均數	18.0000	22.46	17.54	21.10	18.11	18.42
標準差	6.57	6.27	7.90	7.66	8.80	7.40
觀察值個數	28	28	31	31	26	26
差異的 95% 信賴區間	下界	上界	下界	上界	下界	上界
	-5.98	-2.95	-5.81	-1.28	-2.20	1.59
T 檢定	6.055		3.197		0.33	
P 值(雙尾)	0.000**		0.003**		0.74	

*表示 p<0.05　**表示 p<0.01

表 7 為共變數分析結果，實驗組與控制組 B 達到顯著差異(p<.05)，說明透過 IRF 教學對話模式策略，並幫助學生挑選適合他們程度的題目，能有效幫助學生學習英語文法。而實驗組與控制組 A 未達到顯著差異水準(p>.05)，則表示有無使用分層回饋機制對於學生英語文法學習則沒有顯著差異，猜測所造成的原因為控制組 A 接受的回饋內容與實驗組在第三次錯誤接受的回饋內容皆相同，而實驗組多數學生皆進行到第三層回饋。

表 7 成對比較表

(I)教學法	(J)教學法	平均差	標準誤差	顯著性[a]
實驗組	控制組A	1.053	1.203	0.384
	控制組B	4.114*	1.256	0.002*
控制組A	實驗組	-1.053	1.203	0.384
	控制組B	3.062*	1.227	0.015*
控制組B	實驗組	-4.114	1.256	0.002*
	控制組A	-3.062*	1.227	0.015*

儘管從初步的統計結果得知該分層回饋機制的運用並沒有達到預期效果，但為了更深入探討分層回饋機制的效果，根據實驗組與控制組 A 的學生作答紀錄進行後續分析，整個實驗中共有八種難度不同的文法概念。系統預設若學生在該概念連續答對三題難度高的題目，即可提前完成該概念並轉換下個較難的概念，否則須完成該概念中所有試題。根據系統收集的數據，可看出實驗組未接受到第三層回饋即答對題目的比例，如表 8，發現將近有一半以上的完成題數，學生未接觸到第三層回饋即可完成題目，表示第一層與第二層的回饋訊息確實能提供學生修改文法上的錯誤。由圖 7 可看出實驗組的學生對於每個概念提前做完的人數比例遠比控制組 A 高出許多，甚至學習後四個較難的概念時，控制組幾乎沒有提前完成該概念的學生，實驗組的學生因接受分層回饋機制的影響，較控制組學生能夠反思所犯的文法錯誤，而控制組的學生則因直接接受完整參考答案的回饋訊息，修正錯誤後便直接送出答案，可能造成並沒有真正理解錯誤的主因，而形成大部分學習者都出現概念內全部的題目的情形。

表 8 實驗組未接受第三層回饋即答對題目的比例

完成的題數	未看參考答案即答對的題數	比例（%）
1,286	614	47.74

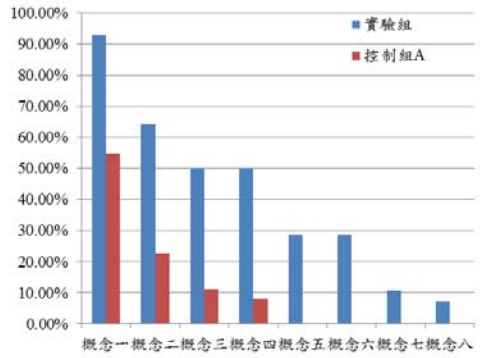


圖 7 提前做完該概念的人數佔全班比例

另一個可能影響分層回饋機制效果的因素在於在實驗時間（90 分）內，學生並無法全然完成八個文法概念的題目，而可能影響其學習效果（後測的分數）。為此，特別針對操作完成度較高的前四個概念與操作完成度較低的後四個概念進行特定前後測共變數分析。分析結果如表 9 和表 10，實驗組與控制組 A 學生在前四個概念的比較有達到顯著差異(p<.05)，然而在後四個概念中則沒有顯著差異(p=.324>.05)，可推論出當學習者在概念完成度高或概念難度較低的情況下，分層回饋機制對於學生英語文法學習上仍具一定的效用。

表 9 前四概念實驗組與控制組 A 共變數分析摘要

變異來源	SS	df	MS	F	Sig. of p
對比	33.608	1	33.608	4.550	0.037*
誤差	406.210	55	7.386		

*p<0.05

表 10 後四概念實驗組與控制組 A 共變數分析摘要

變異來源	SS	df	MS	F	Sig. of p
對比	2.951	1	2.951	0.324	0.572
誤差	501.452	55	9.117		

*p<0.05

5. 結論與建議

本研究探討整合 IRF 教學對話模式及運用分層回饋方式於國二學生英語文法學習的效果，透過系統自動剖析英語文法的結構，檢查出學生所犯的文法錯誤，並依照使用者的文法錯誤適性調整問題難度與回饋內容。實驗結果顯示出 IRF 教學對話模式的運用能有效幫助學生學習英語文法；而分層回饋方式的運用雖然初步統計上並沒達成顯著差異，然而深入分析學生的學習歷程，說明分層給予回饋的方式確實能夠增加學生自我反思的機會，進而讓學生對該文法概念有較深刻的瞭解。

未來研究上除了持續提升文法偵錯的準確度外，將考量利用 IRF 教學對話模式設計更多樣化的文法概念題目，而不僅限於國中範圍，然而越複雜的文法概念其規劃由系統自動判別文法與提供各項適性機制的建立，其設計的複雜度也相對提高許多[15]，而如何有效設計與簡化各項判別與文法偵錯的方法亦將是未來需要克服的重要課題。

致謝

本研究承蒙台灣國科會經費之補助，計畫編號為 NSC99-2511-S006-003-MY3，特此致謝。

參考文獻

[1] Mooij, Ton. (2007). Contextual learning theory: Concrete form and a software prototype to improve early education. *Computers & Education, 48*(1), 100-118.

[2] Woodill, Gary, & Officer, D Chief Learning. (2004). Where is the Learning in E-learning? *Educational Psychology Interactive. Valdosta, GA.*

[3] Chin, Christine. (2006). Classroom interaction in science: Teacher questioning and feedback to students' responses. *International Journal of Science Education, 28*(11), 1315-1346.

[4] Goto, Takuya, Kojiri, Tomoko, Watanabe, Toyohide, Yamada, Takeshi, & Iwata, Tomoharu. (2008). *English grammar learning system based on knowledge network of fill-in-the-blank exercises.* Paper presented at the Knowledge-Based Intelligent Information and Engineering Systems.

[5] Sung, Li-Chun, Lin, Yi-Chien, & Chen, Meng Chang. (2007). *The Design of Automatic Quiz Generation for Ubiquitous English E-Learning System.* Paper presented at the Technology Enhanced Learning Conference (TELearn 2007), Jhongli, Taiwan.

[6] Lee, Kong Joo, Choi, Yong-Seok, & Kim, Jee Eun. (2011). Building an automated English sentence evaluation system for students learning English as a second language. *Computer Speech & Language, 25*(2), 246-260.

[7] Campbell, Julie, & Mayer, Richard E. (2009). Questioning as an instructional method: Does it affect learning from lectures? *Applied Cognitive Psychology, 23*(6), 747-759.

[8] Dantonio, Marylou, & Beisenherz, Paul C. (2001). *Learning to question, questioning to learn: Developing effective teacher questioning practices:* Allyn & Bacon.

[9] Shute, Valerie J. (2008). Focus on formative feedback. *Review of educational research, 78*(1), 153-189.

[10] Giordan, Marcelo. (2003). The role of IRF exchanges in the discursive dynamics of e-mail tutored interactions. *International Journal of Educational Research, 39*(8), 817-827.

[11] Gourlay, Lesley. (2005). OK, who's got number one? Permeable Triadic Dialogue, covert participation and the co-construction of checking episodes. *Language Teaching Research, 9*(4), 403-422.

[12] Hardman, Frank, Abd-Kadir, Jan, & Smith, Fay. (2008). Pedagogical renewal: Improving the quality of classroom interaction in Nigerian primary schools. *International Journal of Educational Development, 28*(1), 55-69.

[13] Temmerman, Martina. (2009). Communicative aspects of definitions in classroom interaction: Learning to define in class for first and second language learners. *Linguistics and Education, 20*(2), 126-144.

[14] Klein, Dan, & Manning, Christopher D. (2003). *Accurate unlexicalized parsing.* Paper presented at the Proceedings of the 41st Annual Meeting on Association for Computational Linguistics-Volume 1.

[15] Siddiqi, Raheel, & Harrison, Christopher J. (2010). Improving teaching and learning through automated short-answer marking. *Learning Technologies, IEEE Transactions on, 3*(3), 237-249.

整合變易理論之物件導向程式設計語法導正系統

黃子峰　蘇建元　張証欽　王宗一*
國立成功大學工程科學所
n96001177@mail.ncku.edu.tw, bredysu@gmail.com, johnc680106@gmail.com,
wti535@mail.ncku.edu.tw*

摘要

物件導向程式設計是資訊軟體專業領域中十分受到重視的課程，但初學者往往在程式撰寫的過程中，對程式語法、語意或指令敘述的程式設計概念一知半解而在真正面對程式實際撰寫的過程中感到挫折，甚至害怕接觸程式。本研究提出整合變易理論策略並建構出用以輔助與導正初學者物件導向程式語法的學習系統。以變異理論其讓學習者體驗與分辨特徵及差異的學習方式下，讓學習者在撰寫 C++物件導向程式、編譯程式碼的過程中，給予學習者更有效的語法導正回饋訊息，以幫助他們學習。

為了探討變易理論應用於物件導向程式設計輔助語法導正的學習成效，本研究以實驗設計方式進行，共有 90 位大一新生參與實驗，以 S 型分組方式將參與學生分派為「具變易理論策略組」(實驗組）與「無變易理論策略組」(對照組)，以單因子變異數分析進行統計分析；並結合問卷分析以及訪談，探討本研究的輔助語法導正機制對於學習者的影響。實驗結果顯示使用「具變易理論模式的語法導正策略」在學習成效表現上優於使用「無變易理論模式的語法導正策略」，證明應用變易理論於物件導向程式設計的語法導正學習能夠幫助學習者撰寫及練習物件導向程式，並且能解決在學習程式設計的過程中，對程式語法、語意或指令敘述的不了解而感到挫折的問題。

關鍵詞：變易理論；物件導向程式設計；語法導正輔助

1. 前言

程式設計一向是資訊技術人員不可或缺的技能之一，要能應用、撰寫出合用的程式，是需要不斷的自我練習、撰寫以及除錯，許多人寫不好程式，或害怕接觸程式，在於對程式的基本概念不瞭解或有所混淆，以致於學習感到挫折[1]-[4]，甚至逃避或放棄學習[5]。因此，本研究採用變易理論（Variation Theory）方法，於學生在編寫程式設計的過程中，以特殊的類比、對比、區別、融合四種不同模式的學習輔助，提供針對語法錯誤以及錯誤程式概念的矯正，來幫助學習者釐清或分辨程式概念間的差異，達成矯正錯誤程式觀念的目的。

2. 相關文獻

2.1 程式設計教學策略

為了有效促進程式設計的學習，過去一些有效的教學策略被廣泛應用在程式設計的教學中，例如使用類比教學方法於程式設計教學[6]；或透過動態視覺化程式碼的呈現方式來幫助學習者學習程式設計[7]；於遞迴程式設計教學中運用雙碼理論建構概念模型的學習策略等[8]。

雖然這些策略皆有助於程式語言的學習，但有文獻指出學生對程式設計的撰寫上仍深感困難[9][10]，推敲其原因在於對程式概念及程式語法不熟悉或產生誤解。針對該問題，有學者認為應透過許多淺顯易懂的例子來幫助學習者釐清程式概念中容易混淆的部分[11]。另也有學者認為在程式教學中，應針對易混淆的概念善用區別、對比等方式以突顯出概念的關鍵屬性，讓學習者更有效率、有效的掌握概念的核心意涵[4]。

2.2 變易理論教學模式

源自於現象圖析學（phenomenongraphy）的變易理論（variation theory），強調體驗事物的變化和差異才是認知的開始，透過分辨現象或概念的特徵及差異，才能習得事物或概念的本質[12]。並將整個變易理論細分成四種不同的變易模式[13]，由淺入深分別為「類比」、「對比」、「區別」以及「融合」，分述如下：

1. 類比（generalization）：要了解某事物的普遍性，就必須經歷此事物在不同情況下的呈現。例如教某個概念時，透過列舉不同的例子，讓學習者辨識例子之中相同的地方，以認識此概念。
2. 對比（contrast）：要清楚瞭解某事物，就必須把此事物和其他事物進行對比。更具體而言，若是你想知道什麼是 X，就必須知道什麼不是 X，例

如要認識「甜味」，就要經歷苦味及鹹味，才能知道什麼「是甜味」，什麼「不是甜味」。

3. 區別（separation）：要審辨事物某方面的特徵，就必須經歷此事物在某方面的改變，而保持其他方面不變，如讓學習者思考同一問題的不同答案或同一現象的不同解釋。
4. 融合（fusion）：某事物需要我們綜合考慮各方面因素時，我們必須經歷多個關鍵性特徵的改變，同時察覺到各方面的轉變。

該策略曾廣泛應用於各個學科領域來幫助學生釐清迷思概念，其中亦包含程式設計的教學。例如 Suhonen 等人在教學時就運用變易理論來突顯程式設計概念差異[14]。Eckerdal 利用變易理論讓學習者觀察二段相似的程式碼，讓學習者透過對比與區別程式碼及比對執行結果的差異來幫助學生習得正確概念[15]。Thota 等人運用變易理論於 OOP 課堂教學，協助學習者學習 OO 概念[16]。

3. 研究方法

本研究針對初學者建構一物件導向程式設計的概念與語法導正學習系統，以變易理論的類比、對比、區別及融合為基礎，該系統主要涵蓋兩個層級，分別為語法導正機制與變異理論回饋策略。

3.1 語法導正機制

本研究採行的語法導正機制流程如圖 1 所示，在系統中讓學習者實際進行程式碼的撰寫，當學習者輸入的程式碼經編譯器剖析之後發生編譯錯誤，將啟動語法導正機制進行語法導正，而在學習者反覆修正及編譯程式碼的過程中，語法導正機制會依照變易理論的教學模式，逐步地給予學習者適當的回饋訊息。

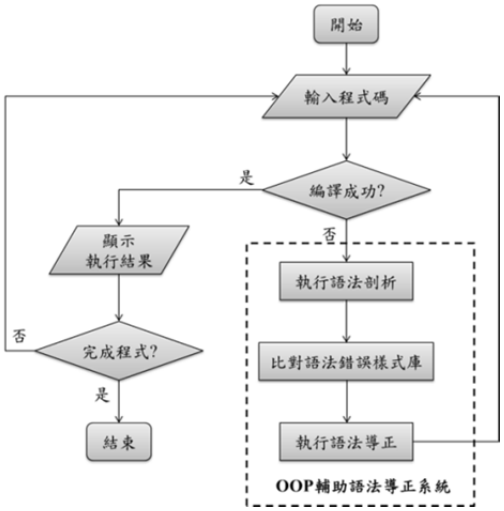


圖 1 初步擬定的語法導正機制流程圖

本研究所建置之語法導正方法主要參考自[17]針對協助學習者程式除錯，所提出的虛擬助教機制（Virtual Teaching Assistant，VTA）。本研究經適度調整該 VTA 機制並用以結合變易理論，並使用語法錯誤樣式庫的錯誤樣式內容來啟動語法導正知識庫所對應之導正教學。其修改後的方法如表 2 所示。

表 2 修改後的 VTA 機制

提示層級	提示方法
hint 1	告訴學習者程式中「哪裡有錯」與「程式錯誤類型」。
hint 2	針對錯誤，提供相關的語法知識或語法導正教材，即**啟動「變易理論語法導正模組」**。

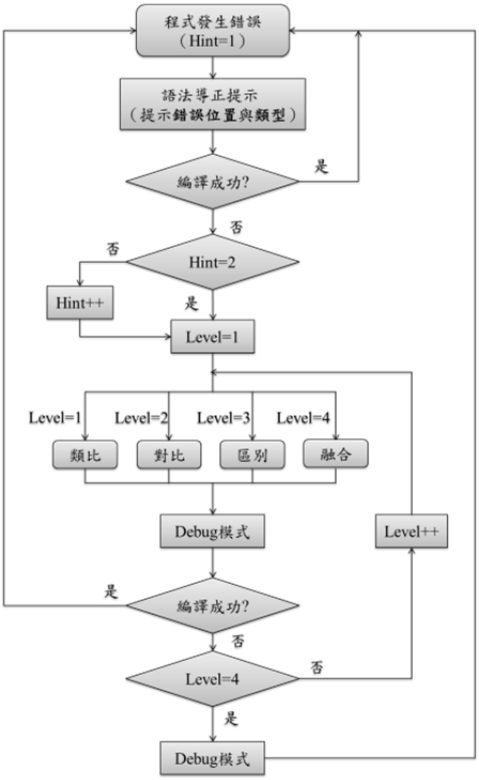


圖 2 變易理論的語法導正流程圖

所新設計之詳細語法導正流程如圖 2 所示。當程式發生編譯錯誤時，給予學習者 hint 1 的提示，告訴學習者程式「錯誤的位置」以及「程式錯誤類型」；若學習者仍無法完成修正語法，接著將依照變易理論模式，給予類比模式（Level=1）的回饋教材，並回到 debug 模式讓學習者修正程式，若糾正錯誤後仍發生同樣錯誤修正程式，若糾正錯誤後仍發生同樣錯誤情形，則系統進一步給予對比模式（Level=2）的回饋訊息，當學習者一再地遇到同樣的程式錯誤情形，系統將依序以類比、對比、區別、融合等四個模式的回饋，逐一予以提示。

3.2 變易理論的回饋策略

在此以物件導向程式概念中的私有區存取錯誤案例為例（如圖 3），該程式錯誤乃是因為物件呼叫到私有區的成員函式所導致，在C++的語法定義中，如果某類別內的成員被定義在私有區（private），則這些成員僅能透過類別內的成員函式對其進行存取。針對發生此錯誤情形，則設定依照特定狀況提供變易理論四種模式的語法導正教材內容，說明如下：

```
1  #include <iostream>
2  using namespace std;
3  class Circle
4  {
5  private:
6     double radius;
7     double Area();
8  };
9
10 double Circle::Area()
11 {
12    return radius * radius * 3.14;
13 }
14
15 int main()
16 {
17    Circle C1;
18    cout << "Area of Circle C1 is " << C1.Area();
19
20 return 0;
21 }
```

成員函式「Area()」為私有區的成員

圖 3 私有區存取錯誤實例

表 3 類比模式的範例

(1)

```
#include <iostream>
using namespace std;
class MyClass
{
private:
   void display();   // private member function
};

void MyClass::display()
{
    cout << "print from the member of MyClass";
}

int main()
{
   MyClass obj;
   obj.display();  // Call a private member function, Error!

return 0;
}
```

(2)

```
#include <iostream>
using namespace std;
class MyClass
{
private:
   double data;     // private data member
};

int main()
{
   MyClass obj;
   obj.data = 1.1;  // Access the private data member, Error!

return 0;
}
```

(3)

```
#include <iostream>
using namespace std;
class MyClass
{
   void display();   // 若未指定成員之權限，則預設為 private
};

void MyClass::display()
{
    cout << "print from the member of MyClass";
}

int main()
{
   MyClass obj;
   obj.display();    // Error!
return 0;
}
```

■ **Level 1 – 類比模式**

變易理論強調要讓學習者了解某事物的普遍性，就必須讓其學習者經歷此事物在不同情況下的過程體認。因此以私有區存取錯誤實例（如圖 3）為例，透過觀視不同的例子，讓學習者辨識不同例子之中相同的地方來認識此概念，藉此反思所撰寫的程式發生的錯誤在哪，該回饋資訊如表 3。

■ **Level 2 – 對比模式**

對比模式主要強調要讓學習者清楚了解某事物，就必須把此事物和其他事物進行對比，藉以突顯某事物的特徵。如表 4，便是讓學習者透過經歷「私有區成員」與「公有區成員」兩者關鍵特徵的變化與異同，以幫助學習者瞭解程式為什麼發生錯誤。

表 4 對比模式的範例

1. 「private 成員」大多為**資料成員**，**只能**透過**類別本身**的成員函式之程式命令對其做存取，其他外部程式命令皆**不允許透過「.」直接存取私有成員**。
2. 「public 成員」大多為**成員函式**，**除了**可透過**類別本身**的成員做存取之外，公開的成員**可任意為外部程式命令透過「.」直接存取**。

■ **Level 3 – 區別模式**

要釐清事物某方面的特徵，就必須經歷此事物在某方面的改變，而同時保持其他方面不變，如讓學習者思考同一問題的不同答案或同一現象的不同解釋。因此針對該私有區存取錯誤的實例（如圖 3），區別模式所給予的回饋訊息如表 5 所示，系統提供學習者 2~3 個此錯誤類型的正確程式範例，亦即讓學生經歷「程式」某方面改變（由錯誤改為正確），而「錯誤類型保持不變」，讓學生能比較自己的錯誤程式與正確範例差別後，瞭解該部分正確的程式應如何撰寫，以導正程式錯誤。

表 5 區別模式的範例

(1)

```
#include <iostream>
using namespace std;
class MyClass
{
public:
   void display();   // public member function
};

void MyClass::display()
{
    cout << "print from the member of MyClass";
}

int main()
{
   MyClass obj;
   obj.display();    // Correct!

return 0;
}
```

(2)

```
#include <iostream>
using namespace std;
class MyClass
{
public:
   double data;     // public data member
};

int main()
{
   MyClass obj;
   obj.data = 1.1;    // Correct!

return 0;
}
```

■ **Level 4 – 融合模式**

某事物需要綜合考慮各方面因素時，我們必須經歷多個關鍵性特徵的改變，以察覺其各項轉變，

如讓學生透過同一現象的不同感知，以開啟他們思辨和學習的空間，來習得相關知識或概念。因此，融合模式將如表 6，系統將以一個同時包含「正確範例」與「錯誤情形」的程式碼作為該階段的回饋，當學習者經歷過前面三個階段，已將事物的學習特徵逐一區別出來之後，再將這些特徵於同一情境當中融合表示，可以提升學習者對於程式語法的理解，更能全面、完整的掌握正確的程式語法。

表 6 融合模式的範例

```
#include <iostream>
using namespace std;
class MyClass
{
private:
   void testing();     // private member function
public:
   void display();     // public member function
};

int main()
{
   MyClass obj;
   obj.testing();     // Error!

   obj.display();     // Correct!

return 0;
}
```

3.3 系統架構

本研究所建置的系統共包含六個部分，其架構如圖 4 所示。

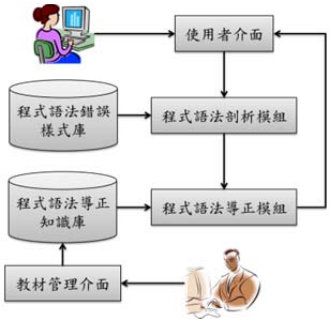


圖 4 系統架構圖

學習者可以透過「使用者介面」進行 C++物件導向程式的撰寫、編譯及除錯，並在程式發生編譯錯誤時，系統將予以程式語法導正幫助學習者進行除錯。

「程式語法剖析模組」主要功能為剖析、分析學習者輸入的程式碼，透過比對「程式語法錯誤樣式庫」以得知該程式的錯誤類型。「語法錯誤樣式庫」則存放學習者於程式撰寫時常犯的語法錯誤樣式。而「程式語法導正模組」則協助學習者進行除錯，將語法剖析模組剖析後之結果結合「程式語法導正知識庫」內的變異理論模式回饋資訊進行語法導正。其可能發生的所有錯誤樣式處理規則，本研究聘請三位具 OOP 教學經驗的專家教師，於「教材管理介面」中以變易理論之類比、對比、區別與融合等模式為原則製作相對應的變易理論語法導正回饋教材。

4. 實驗設計

為驗證所開發出的「整合變易理論之 OOP 語法導正學習系統」的效果，實驗設計將以期中考試成績透過 S 型分派學生為實驗組和控制組，使其兩組學生具有相同的程式設計先備知識。自變項為語法導正策略，依變項為學習成就測驗結果。其中，實驗組使用「具變易理論模式的語法導正策略」的導正教材；控制組則使用「無變易理論模式的語法導正策略」的教材，而控制組修改後的 VTA 機制如表 7 所示，在提示層級 1 中同樣告訴學習者程式之「錯誤位置」及「錯誤類型」；而在層級 2 中則使用原始編譯器資訊做為回饋。

根據課程進度，我們將測驗的範圍訂定為「物件與類別」及「繼承」兩單元，讓學生使用本系統實際進行 OOP 程式的撰寫，並依測驗範圍分為兩次實驗活動，將在實驗 1（物件與類別單元的上機測驗）之後間隔一個月，執行實驗 2（繼承單元的上機測驗）。每次各提供 2 題程式問題，學生須於規定時間（120 分鐘）內完成所要求的程式撰寫。學生完成、提交後的結果將由人工進行批改，做為學習成就測驗的結果。

表 7 控制組之修改後的 VTA 機制

提示層級	提示方法
hint 1	告訴學習者程式中「哪裡有錯」與「程式錯誤類型」。
hint 2	提供原始編譯器回饋資訊（使用 Microsoft Visual C++編譯器）。

4.1 實驗對象

實驗對象是以台灣南部某大學工程科學系之必修程式設計課的 90 位修課學生，分為實驗組與控制組各 45 人，兩組均同時接受過程式設計課程講授。我們利用實驗分析以及問卷、訪談方式來檢驗變異理論於物件導向程式設計語法導正系統中的效果。相關分析結果如下:

4.2 統計分析結果

扣除無效樣本得第一次實驗活動的有效樣本數為 82 人，第二次實驗活動則為 81 人。本研究採單因子變異數分析（ANOVA），進行變異數差異的顯著性考驗。於正式實驗前先執行 Levene’s 變異數同質性檢定來初步評估實驗組與控制組是否具同質性（如表 8），其結果得知二組沒有顯著差異（$p = .891$ 與 $p = .976$），顯示兩組學生具同質性。

表 8 先備知識變異數同質性檢定

	df1	*df2*	*Sig.*

實驗 1	1	80	.891
實驗 2	1	79	.976

其針對學習成效測驗進行單因子變異數分析，結果如表 9 所示，第一次實驗分析結果為 F(1,80) = 4.255，p = 0.042；第二次實驗結果為 F (1,79) = 4.165，p = 0.045，兩次不同單元的實驗均達顯著差異。可推論出實驗組學生使用具變易理論模式的 OOP 語法導正的學習系統，比無學習變易理論模式的 OOP 語法導正策略的學習系統的學生，在學習成效上有較好的表現。

表 9 學習成效之變異數分析

實驗1	組間	4842.375	1	4842.375	4.255	0.042*
	組內	91054.076	80	1138.176		
	總和	95896.451	81			
實驗2	組間	4240.400	1	4240.400	4.165	0.045*
	組內	80420.879	79	1017.986		
	總和	84661.279	80			

*$p < 0.05$

為進一步了解具變易理論模式的語法導正策略對不同程度學生的影響，我們進一步從收集到的數據資料中將參與實驗的學生依照先備知識成就測驗結果（學期第一次期中考試成績），分成高、中、低成就三群，並從兩次實驗的成就測驗分數觀察發現，本研究所建置之整合變易理論的 OOP 語法導正系統對於中成就的學生幫助較大，對於低成就學生次之，而對於高成就的學生則較小。

4.3 問卷結果分析

為深入了解變異理論輔助語法導正機制對於學習者的使用意見，由三位熟悉物件導向程式設計教學的專家教師共同編制「變易理論語法導正學習系統使用問卷」，所有試題以李克特五點量表分成非常同意、同意、無意見、不同意與非常不同意五個選項，其問卷具備一定程度之專家效度，該問卷針對實驗組的學習者進行調查，且僅針對問卷進行描述性分析，用以了解實驗組學習者於使用該語法導正系統後，對於該應用變易理論於語法導正回饋的看法與意見，問卷內容共分為「類比模式」、「對比模式」、「區別模式」、「融合模式」及「整體經驗」等五個部分進行調查。其問卷統計結果如表 10 所示，對於「整體經驗」向度中的分析結果為贊同（平均數=3.65、3.50、3.78），而對於變易理論中四種變易模式的語法導正回饋也大多表示贊同，其中大部分填答者較贊成「對比模式」的回饋有幫助（平均數=4.03、3.75），而其次為「區別模式」（平均數=3.85、3.65）及「融合模式」（平均數=3.70、3.63），最末為「類比模式」（平均數=3.58、3.40、3.45）。

表 10 問卷之平均數與標準差統計表

	題目	平均數	標準差
類比模式	1 有助於辨識程式錯誤的地方。	3.58	.68
	2 有助於清楚釐清相關程式語法的特徵。	3.40	.71
	3 有助於未來遇到相同語法錯誤時，辨識相同的錯誤類型。	3.45	.75
對比模式	4 有助於瞭解程式「為什麼發生錯誤」。	4.03	.48
	5 有助於清楚釐清相關程式語法的特徵。	3.75	.59
區別模式	6 有助於瞭解正確的程式語法。	3.85	.66
	7 有助於分析程式錯誤的地方。	3.65	.80
融合模式	8 有助於更全面、更完整地理解程式錯誤，並能進一步修正該錯誤。	3.70	.65
	9 有助於更全面地掌握正確的程式語法。	3.63	.74
整體經驗	10 有助於釐清以往程式語言語法上的模糊觀念，得到正確的語法概念與認知。	3.65	.62
	11 以「逐層、漸進」方式提供回饋有助於對程式語言語法觀念進行更深入思考。	3.50	.72
	12 整體而言有助於「導正」程式語法錯誤。	3.78	.66

4.4 訪談結果

從實驗組學生的訪談結果可以發現到，學生樂於透過該系統進行程式撰寫，主要能針對編譯錯誤的部分，得到更完整的回饋訊息。該組學生也反應 hint 1 回饋提示的「錯誤位置」與「程式錯誤類型」，在已經領悟到是屬於哪種錯誤情形或糾錯方式時，相較於一般的程式編譯方式，該系統所提供的回饋資訊將更有助於他們糾正程式錯誤。其中，學生表示所系統所提供的「類比」回饋訊息能幫助思考與判斷較簡單的程式錯誤，當程式出錯的內容較為複雜或難解時，「區別」回饋則能幫助思考與反思較複雜、困難的程式問題。「對比」回饋主要是提供錯誤的關鍵特徵，讓學生進行比較，不少學生皆反應該方式對他們的學習助益最大；「融合」回饋亦能提供完整的例子，幫助學生解決錯誤與提供詳細的程式錯誤論述訊息。

在控制組的學生訪談中，一些學生認為原始編譯器的回饋資訊較不容易讓人理解；而尤其當所撰寫的程式發生多種錯誤情形時，原始編譯器回饋資訊可能過度複雜，而造成學習者無法糾正他們的程式錯誤；也有學生表示若回饋資訊能提供更好的程式例子來參考，將會有很好的幫助。

整體而言，整合變異理論的四種模式於物件導向程式設計語法導正學習中，對於學生語法的釐清

及糾正程式錯誤有正向的助益。

5. 結論與建議

本研究開發整合變易理論於物件導向程式語言語法導正學習系統，為了檢驗該變異理論應用於語法導正學習系統之成效，讓已學過程式設計的初學者進行實際的程式撰寫，並以兩階段的上機進行程式撰寫實驗進行，結果顯示使用「具變易理論模式的語法導正策略」的學生於學習成效表現上優於「無變易理論模式的語法導正策略」的學生，推論出變易理論應用於物件導向程式設計語法導正能有益於學習者釐清程式語法、語意或指令敘述的錯誤概念。未來將持續延伸至其他物件導向程式設計單元，或針對不同程度的學習對象，進一步印證與深入探討該變異理論策略中不同模式與不同學習單元對學習者的影響。另外，對於系統的使用建議，亦可強化系統的自我操作性，如提供程式編輯區中關鍵字顏色分別、自動對齊、自動縮排等等的編排功能，以提供更完整、妥善的物件導向程式設計語法導正學習系統。

致謝

本研究承蒙台灣國科會經費之補助，計畫編號為 NSC 101-2511-S-006-011-MY2，特此致謝。

參考文獻

[1] G. Stavroula and S. R., "Using Educational Tools for Teaching Object Oriented Design and Programming.," *Journal of Information Technology Impact*, vol. 7, pp. 111-130, 2007.

[2] A. Ebrahimi and C. Schweikert, "Empirical study of novice programming with plans and objects," *SIGCSE Bull*, vol. 38, pp. 52-54, 2006.

[3] A. Eckerdal and M. Thun'e, "Novice Java programmers' conceptions of "object" and "class", and variation theory.," *Proceedings of the 10th Annual SIGCSE Conference on Innova-tion and Technology in Computer Science Education (ITiCSE'05)*, pp. 89-93, 2005.

[4] S. Holland, R. Griffiths, and M. Woodmanw, "Avoiding object misconceptions.," *In Proceedings of the 28th SIGCSE Technical Symposium on Computer Science Education(SIGCSE'97)*, pp. 131-134, 1997.

[5] 陳怜秀、郭英峰, 學生程式設計能力影響因素之研究—以崑山技術學院資訊管理系為例, *技術學刊*, vol. 13, pp. 661-668, 1998.

[6] J. Whittle, A. Bundy, and H. Lowe, "Supporting programming by analogy in the learning of functional programming languages.," presented at the The 8th International Conference on AI in Education (AIED), 1997.

[7] H. Ramadhan, "An intelligent discovery programming system.," in *SAC '92 Proceedings of the 1992 ACM/SIGAPP Symposium on Applied computing: technological challenges of the 1990's*, New York, USA, 1992, pp. 149-159

[8] 陳明溥, 雙碼理論於遞迴程式設計教學之概念模型設計研究, 第八屆電腦輔助教學國際研討會, 逢甲大學, 1999.

[9] J. Bennedsen and M. E. Caspersen, "Revealing the Programming Process," *Proceedings of 36th SIGCSE Technical Symposium on Computer Science Education (SIGCSE2005)*, pp. 186-190, 2005.

[10] V. Shanmugasundaram, P. Juell, G. Groesbeck, and M. Makosky, "Evaluation of Alice World as an introductory programming language.," in *Proceedings of the ED-MEDIA 2006-World Conference on Educational Multimedia, Hypermedia & Telecommunications*, 2006, pp. 1976-1982.

[11] 陳明溥, 程式語言課程之教學模式與學習工具對初學者學習成效與學習態度之影響, *師大學報*, vol. 52, pp. 1-21, 2007.

[12] F. Marton, "Phenomenography-describing conceptions of the world around us.," *Instructional Science*, pp. 177-200, 1981.

[13] 祁永華, 謝錫金, and 岑紹基, *變易理論與學習空間*. 香港: 香港大學出版社, 2005.

[14] J. Suhonen, E. Thompson, J. Davies, and Kinshuk, "Applications of variation theory in computing education," in *Proceeding Koli Calling '07 Proceedings of the Seventh Baltic Sea Conference on Computing Education Research*, Koli National Park, Finland, 2007, pp. 217-220.

[15] A. Eckerdal and M. Thun'e, "Variation Theory Applied to Students Conceptions of Computer Programming.," *European Journal of Engineering Education*, vol. 34, pp. 339-347, 2009.

[16] N. Thota and R. Whitfield, "Holistic Approach to Learning and Teaching Introductory Object-Oriented Programming.," *Computer Science Education*, vol. 20, pp. 103-127, 2010.

[17] C.-Y. Chou, B. Huang, H., and C. J. Lin, "Complementary Machine Intelligence and Human Intelligence in Virtual Teaching Assistant for Tutoring Program Tracing," *Computers & Education*, vol. 57, pp. 2303-2312, 2011.

行動載具之個人化學習歷程應用程式研發初探

王仕祺
國立清華大學資訊系統與應用研究所
colocolo317@gmail.com

王怡萱
國立清華大學資訊系統與應用研究所
annywang12345@hotmail.com

楊叔卿
國立清華大學學習科學研究所
scy@mx.nthu.edu.tw

摘要

本研究為一多階段研究之初探研究，目的為了解行動載具應用於國小教學情境中學習者對於行動載具應用 App 的需求與期待以及學習者對於在行動學習載具上進行個人化學習歷程記錄之需求與看法。本研究以問卷與半結構式訪談蒐集學習者反饋並進行資料分析，研究結果顯示學習者對於行動載具融入課堂情境之期待科目主要以國語、數學、自然與科技等科目為主，而學習者對於透過行動載具 App 功能將作品收集整理為學習歷程並進行學習分享之功能抱持著正面的態度。另外，本研究亦發現，學習者的性別亦會影響學習者使用行動載具 App 功能進行學習互動的關鍵之一，最後，本研究歸納本階段之初探研究結果，提出擬建置行動載具學習 App 之三大面向做為下階段系統建置之依據。

關鍵詞：行動載具；學習歷程；國小教學；應用 App 開發

1. 前言

隨著一對一手持式行動載具 (One-to-one handheld technology and learning devices)的高度普及與受歡迎，其不僅是人們日常社交通訊之主要工具，也具良好「教」與「學」之優勢與潛力，乃因手持式行動載具有融會文字、聲光、影像之多媒體特性、具手寫辨識功能可結合人們使用傳統科技之既有行為，再加上其輕便易攜等特性，一對一手持式行動載具可提供個人化、主動式的學習管道與多元功能，近年來高度普及的手持式行動載具之教育情境應用融入，已使得「教」與「學」漸由傳統的「教學者為中心 (Teacher-centered instruction)」轉而成為以「學習者為中心（Learner-centered learning)」。若行動載具可合宜地規劃、應用、融入教學，將使得學習可在教室內與教室外的任何情境進行，因而提供任何時、地（Anytime & Anyplace）的個人化（Personalized）、自我調適學習進度（Self-paced learning）之學習方式，已成為現今教學的新派典（Paradigm shift）與全球教學發展趨勢，並且已受到各國政府、教育單位的重視而在各國制定推動科技融入教學之相關政策或白皮書(Office of Educational Technology, U.S. Department of Education, 2010)。為迎接個人化、自我調適學習進度、以學習者為中心的學習新派典與趨勢，如何設計一應用於手持行動載具上的學習應用工具程式 (application, App) 在不同的教學情境中，支持各教師之教學需求與輔助學生進行個人化、主動學習如今更顯出其重要與必要性。

本研究分為多階段性研究，本第一階段研究擬針對學習者之實際教學需求考量，進行應用於手持行動載具之學習 App 建置前的初探研究。本論文首先針對手持式行動載具應用於學習之相關文獻進行探討，接著針對國小學習者對於使用行動載具中學習 App 的實際使用期待與態度等面項進行資料蒐集與分析，最後，歸納本階段的行動載具學習 App 初探結果，做為下階段系統建置之依據。

1.1 研究目的與研究問題

本研究擬從學習者使用端部分切入，探討學習者對於使用手持式行動載具中之學習 App 於課堂學習之需求與期待性分析，本研究問題如下：1. 國小生學習者對於使用行動載具學習應用 App 進行學習的功能與期待為何? 2.國小生學習者對於利用手持式行動載具學習應用 App 進行個人化學習歷程紀錄之需求與看法為何?

2. 文獻探討

2.1 行動載具學習

資訊科技近年來在教學情境中的發展越來越多的應用，隨著行動載具日趨普及，更為課堂中的科技輔助學習之媒介增添選擇，帶給老師及學生創新形式的學習機會與教學模式。行動載具可以使數位資訊更加隨手可得，也不必受固定地點以及座位的限制，有研究認為這樣的特性可以避免桌上型電腦的使用方式對學習活動造成的限制[1]，而行動載具科技發展相當多的個體應用程式，其雖然非為課堂教學設計，卻可用在教學的情境之中，亦有教師帶入課堂中進行教學，但使用範圍仍僅限於個別活動和教學設計的使用。行動學習載具融入於課堂不僅可給予學生創新之教學活動，其可紀錄性，可以幫助學生彙整個人的學習歷程，其資訊之便利傳遞特性，亦可被教師所借重用以追蹤學習者學習的步伐進度，同學間的資訊交流，以及課堂教學材料的傳

遞和管理都是資訊科技所能發揮之處[2]，利用教學活動的模組化設計資訊平台也可以提供教師教學設計上的協助；在行動載具的融入之下，平台與載具的整合性、互動性也將會是重要的議題。

2.2 資訊科技融入學習情境

在運用資訊科技載具融入教室協助教學的過程中，其目的除了讓學習者達到更好的學習成效外，如何有效協助教師從準備到執行教學活動也是重要須考量的層面，過去國內外皆有相關研究朝此目標整合資訊科技融入課堂教學中[2][3]，綜合相關文獻，本研究歸納出科技對於教師輔助的兩個要點：1.科技的融入與教學活動彼此緊密的結合:為了讓學生達到更有效的學習教學活動的設計對教師來說是相當重要的，但也同時會使教學執行更為複雜，資訊科技融入課堂可以增強訊息的傳遞，針對不同的教學活動設計，發揮適合的輔助功能，因此科技融入的角色往往會與教學活動有密切關聯。2.科技的融入幫助教師更有效了解學習者的狀態，從[2]的研究結果可發現，透過社群標籤的平台，學生必須在閱讀完外文(英文)文章後，條列出適合描述主旨的標籤，並且會有一系列的討論和篩選。在這個過程中，教師可以透過學生所提出和取捨的標籤，更了解學生個別的學習狀態，以及系統也設計了智慧評分機制，幫助教師有效的了解學習者的學習進度。透過資訊平台的記錄與分享功能，可以讓學生更多欣賞彼此在學習上的作品，也提供便利的交流管道。

2.3 數位學習歷程 (E-portfolio)

近年來數位學習歷程可見於各種學習平台上也扮演重要的角色。數位學習歷程幫助學習者建構個人化的學習紀錄，學習者可以保存與取得學習過程中的個人作品、閱讀自己的學習經歷以及可以作為個人學習成效的評量[4]。數位學習歷程扮演一個建構式學習工具的角色，藉由數位學習歷程學習者可以自我主導學習過程紀錄的收集、彙整和選擇紀錄媒體的形式[5]。數位學習歷程也被認為具有提升學習者反思能力[6]和深層學習[7]的潛力。因而，本研究針對學生對於使用行動載具學習應用 App 紀錄與分享自我學習的歷程的態度與看法進行探討。

2.4 回饋建議促進學習

研究指出回饋建議是個人所接受到的學習資訊中最能幫助其修正錯誤觀念、更新知識結構、推動後設認知運作、增進學術成就以及促進動機的項目[8]。回饋建議的來源包括三大部分：自我本身、教學科技產品、其他人。Johnson 和 Johnson[9]研究指出在不同類型的回饋建議中，他人所給予的回饋建議最能有效增進自我學習。本研究希望藉由使用科技載具融入課堂活動以促進同儕間與師生間彼此的回饋與互動，以利學生在課堂與課後得到深層的學習，因而，本研究亦針對學習者對於使用行動載具學習應用 App 給予同儕學習回饋進行學習互動等面向進行學習者相關看法與態度探討。

3. 研究方法

本研究經由 Informant Design[11]方式，透過問卷法先了解目標學習者的個人科技操作背景，接著探討探討學習者對於使用行動載具學習 App 的期待功能與看法，並從建置個人化學習歷程服務、增強課堂參與等面向蒐集學習者使用手持式行動學習載具進行學習之意見與反饋進行歸納分析。

3.1 研究對象

本研究的對象為台灣北部一所國小的 26 位中年級學生，研究過程中發放 26 份問卷，有效問卷為 26 份，其中，有 11 位女生與 15 位男生參與本研究。在接觸新式數位科技使用經驗部分，有高達 96.1% (25 人)的學童家中擁有個人電腦可進行上網，約有 50% 的學童家中擁有平板電腦如：iPad 可供課後使用。此外，約有 42% (11 人) 的學生每天能使用電腦半小時，35% (9 人) 的學生每天能使用電腦一至二小時，而有 12% (3 人) 的學生在家完全被禁止使用網路。其中，學習者最常使用網路進行的行為主要分別為：查詢資料 22.7%、玩遊戲 22.7%、使用社群網站 16.5% 與撰寫作業 14.4%。此資料結果顯示，目前國小學童數位化的程度相當高，從個人電腦到觸控式的智慧型數位裝置皆有所涉略。

3.2 研究問卷內容與訪談

本研究將 Pintrich 與 Schunk [10] 之學習者動機量表項目融入研究問卷設計並酌量修改，問卷共包含三大部分：7 題為學習者的基本資料，18 題為李克特式五點量表及 9 題複選題與兩題開放問答題。填寫問卷時間為 40 分鐘，於填答問卷結束後，研究者隨機選擇十名學生，進行學習者對於使用行動載具之學習 App 需求與使用態度之半結構性訪談，訪談內容包含了解學習者對於使用手持式行動載具融入課堂學習以及使用行動載具學習 App 紀錄個人學習歷程的看法與態度。

4. 資料分析

本研究資料分析以量化為主質化為輔之方式，探討學習者使用行動學習載具 APP 進行個人學習之需求分析，研究者首先針對使用行動載具學習 App 進行學習的功能與期待作分析，第二部分探討利用手持行動載具學習 App 進行個人化學習歷程紀錄之需求分析。

4.1 行動載具學習應用 App 之功能與期待

本研究首先針對學習者對應用行動載具之學習App 於課堂情境之科目進行期待調查，根據數據統計顯示，學習者希望將行動載具學習App融入之九年一貫課程前三名分別為: 國語課 (20.3%)、數學課(19.0%)與自然與科技課 (16.7%)，學習者亦針對行動載具融入不同科目提出不同的看法與需求原因，如：”*因為可以讓自然課多元，可以認識更多東西*-S14”、”*因為上英語課可以聽老師說英文，聽不懂的我可以直接用iPad查*-S15”、”*因為自然課程有許多實驗要做，可以上網查怎麼做*-S18”等（表2 A）。其中，學習者認為經由使用行動載具上的學習App可以幫助學習的原因前三名為：行動載具具有撥放影音之功能（26.5%）、透過使用行動載具上之學習App可完成屬於個人的數位學習成品（21.7%）以及行動載具之學習App具有互動（18.1%）。研究者亦想了解國小學習者在使用行動載具App進行課堂學習紀錄的方式，多數學習者習慣在載具上用虛擬鍵盤打字記下筆記 （29.2%），其次為在載具上進行手寫筆記（27.7%）與使用照相功能紀錄筆記（23.1%），最後則為使用錄音功能紀錄筆記（20.0%）。

另外，研究者更進一步針對兩門學科：數學科及藝文課程中的音樂科等兩門課，從學習者角度探討其希望行動載具學習App能融入課程進行輔助學習的單元項目，在數學課部分，學習者最期待能透過行動載具的App學習數學單元中的:七巧板拼圖之形狀學習(25%)、積木類立體概念(21%)、平面圖形單元之面積計算(15 %) 以及量尺單元之測量長、寬、高(15%) 等內容（圖1A），學習者在質性訪談中也提到行動載具可以輔助圖形的視覺呈現，幫助學習者理解原本抽象的三維圖形，學習者反饋如:”*有立體圖片可以看形狀，計算面積可以比較快完成*-S08”;在音樂課程部分，學習者期待透過行動載具App進行：音樂賞析課程（21.7%）、樂器演奏練習（20.8%）、節奏學習（17.9%）等內容（圖1B），質性訪談中學習者提到希望行動載具App幫助自己將音樂音符標示出來，讓自己能了解音高的變化，相關反饋如:“*希望他可以標上 do ,re, mi, fa, sol，自動撥放音樂然後告訴我 do, re ,mi, fa, sol他是怎麼排列的*-S06”。研究者亦將學習者對於將學習App融入數學與音樂課程的部分手寫反饋整理歸納於表2B與表2C。

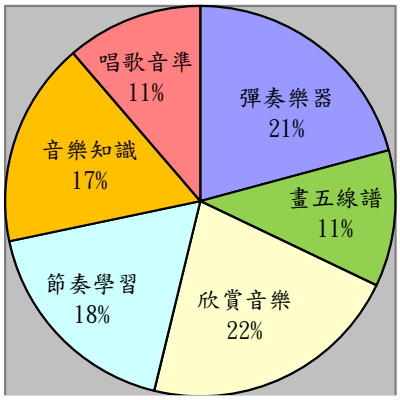


圖 1A 數學課程：學習者期待融入行動載具 App 學習單元

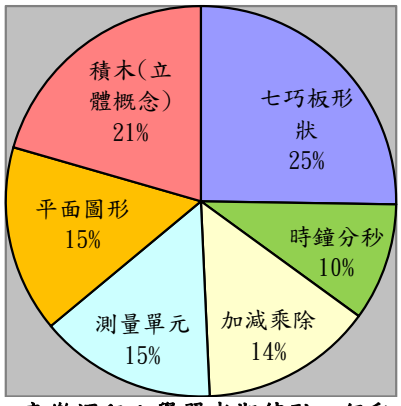


圖 1B 音樂課程：學習者期待融入行動載具 App 學習單元

4.2 行動載具學習應用 App 之學習歷程功能分析

研究者針對使用行動學習載具學習應用App做為記錄學習歷程工具的看法與需求進行分析（表1），經由問卷統計後發現，根據學習者過往的經驗而言，多數學習者在遇到學習困難時皆願意透過請教同學來解決問題（表1,Q2），而學習者也願意透過同儕間的意見交換進行學習（表1,Q10 & Q11）。

在使用App記錄學習歷程的看法部分，學習者期待自己使用行動載具學習App的學習行為與學習過程能被紀錄下來（表1,Q1），且學習者願意主動分享自己的數位學習歷程（表1,Q14），並同意經由觀看自己不同階段的學習過程能有助於學習（表1,Q4），此外，學習者亦認為教師若能針對使用App個別的學習過程給與自己學習建議，將能有助於課程理解與進步（表1,Q6）。整體而言，學習者對於在行動載具上使用學習App記錄自我學習歷程的功能具有正向支持反饋（表1,Q15）。

然而，在數據分析的過程中，本研究亦發現了學習者的性別會影響學習者使用行動載具學習App進行學習分享或學習紀錄的意願，根據表1發現，男性學習者對於使用行動載具學習App紀錄下自己的學習過程有較高的意願且亦較女性學習者肯定

其對於學習帶來的正向幫助（表1，Q1 & Q3），同時，男性學習者希望同儕能給予自己的學習作品意見或利用學習App進行同儕互評，並經由同儕互評的過程了解自己學習成品的優缺點（表1， Q5,Q9 & Q17），學習者亦從質性訪談中提出關於透過行動載具學習App紀錄自己學習歷程的看法，如：”*因為這樣就可以知道我上課的時候有沒有認真、進步，可以給爸爸媽媽看*-S25”；”*因為我們這樣可以把他寄回家，給媽媽，可以和他討論，把他弄到我們家的drobox*-S28”。

表 1 問卷分析結果

題項	整體平均	性別平均
Q1 我願意我的學習過程被ipad記錄下來	4.27	男4.47 女4.00
Q2 在學習上遇到問題時，我會主動請問別人	4.58	男4.47 女4.73
Q3 我覺得記錄下自己學習過程，對學習有幫助	4.04	男4.20 女3.82
Q4 我覺得觀看自己的學習過程，對學習有幫助	4.15	男4.20 女4.09
Q5 我覺得觀看別人的學習過程，對學習有幫助	3.77	男4.00 女3.45
Q6 老師針對學習過程給建議，對學習有幫助	4.62	男4.40 女4.91
Q7 同學針對學習過程給我建議，對學習有幫助	4.04	男4.07 女4.00
Q8 我會想要在ipad上分享自己的學習過程	4.00	男4.00 女4.00
Q9 我會想要在ipad上觀摩同學的學習過程	4.15	男4.33 女3.91
Q10 我希望同學能依據我的學習過程給我建議	4.27	男4.20 女4.36
Q11 我願意給與同學的關於她們學習過程建議	4.42	男4.53 女4.27
Q12 我希望能常常閱讀自己的學習過程檔案	4.12	男4.13 女4.09
Q13 我會和同學分享學習成果(如繪畫、作文)	4.00	男3.80 女4.27
Q14 我喜歡和同學分享我的學習成果	4.15	男4.13 女4.18
Q15 如果有一個iPad軟體可以和同學分享學習成果，我會想使用它	4.12	男4.00 女4.27
Q16 我願意讓同學對我的上課作品進行評分	3.54	男3.93 女3.00
Q17 我喜歡透過和同學互相打分數方式，來了解他們對我作品的喜好程度	3.92	男4.20 女3.44
Q18 我希望課堂上能有一個排行榜，即時顯示哪位同學的作品獲得最高評分	3.73	男4.20 女3.09

另一方面，女性學習者卻有不一樣的反饋，數據顯示，相較於男性學習者而言，女性學習者願意分享自己的學習成品給予其他同學進習觀摩 （表1，Q13），但較不同意使用學習App紀錄自己的學習歷程對於學習有幫助（表1，Q3），且較不願意讓其他學習者對於自己的成品進行同儕評分（表1，Q6 &Q17）。研究者從部分訪談中歸納不同性別學習者之建議，女性學習者提出由於擔心自己的作品隨意被不熟悉的同學批評，因此，女性學習者僅願意讓班級的幾位好朋友進行評分，而不願意分享自己的成品讓同儕進行評分，相關回應如：”*希望和比較好的朋友分享就好，因為我比較常跟比較好的朋友在一起，所以我們本來就會各自分享，跟比較好的朋友不會害羞，跟全班會害羞*-S13; ”*我想和我的朋友分享，我不想給其他人看，因為有時候我給不喜歡的人看，他會批評我的作品，因為我自己努力做出來的作品，我不想要被別人批評*-S20”，另外，研究者亦發現，不同性別對於在App上使用學習排行榜的意願亦有不同，相較於女性學習者而言，男性學習者較喜愛使用學習排行榜來促進上課學習的競爭氣氛（表1，Q18）。

表 2 部分學習者開放問答

A.將行動載具融入不同學習科目反饋
S12 融入行動載具可以讓課程進行更有趣
S14 因為可以讓自然課多元，可以認識更多東西
S15 因為上英語課可以聽老師說英文，聽不懂的我可以直接用 iPad 查
S16 因為上數學課需要許多算式，但有了 iPad 就不用這麼麻煩了
S19 因為可以在上課的時候，直接練習今天教的東西
S18 因為自然課程有許多實驗要做，可以上網查怎麼做
B. 學習者期待將行動載具 App 融入數學學習
S15 希望能計算面積，因為面積用圖形算比較簡單。而加減乘除可以用課本計算比較好
S08 計算面積
S09 學除法、容量、毫米毫升
S12 想學除法，然後要考試前幫我複習
C. 學習者期待將行動載具 App 融入音樂學習
S15 打節奏，因為節奏需要準確的機器來測量，如果只用口說的可能會不準確
S03 吹直笛，因為我直笛都按不好
S05 我想要認識音符
S08 打節奏
S23 查詢音樂知識，查詢音樂名人傳記

5. 討論與結論

5.1 討論

學習者期待行動載具可以發揮其豐富多媒體呈現以及編輯的特質，如行動載具的多媒體可以延伸紙本課本以及課堂教材在視覺上的訊息傳遞、提供創新的作業創作方式給予學習者成就感並且在互動性介面的設計給予學習者新奇的感受。根據資料分析顯示，學習者對於行動載具融入課堂情境之期待科目主要以國語、數學、自然與科技等科目為主，此三科目皆為學校教學的主要科目，由此結果可發現將行動載具融入課堂協助學習者學習時，可以設計符合九年一貫主要課程學科教學的學習應用App做為首要設計，此外，在對照訪談資料亦可

更深入發現，在將行動載具融入數學科目學習的功能設計中，學習者的期待能在數學課中有更多視覺化圖形的教材呈現，以幫助測量、面積計算及三維圖形等思考。學生期望行動載具可以幫助自己在這些科目中解決遇到的困難或者延伸不同學習的機會，並期待能透過行動載具輔助自己在圖形思考上遇到的困難。可見學習者對於行動載具融入課堂抱持正面的態度，並且相信此科技產品可以幫助課堂學習。音樂課部分，學習者期待行動載具能夠在示範音樂的演奏、協助了解樂曲的音符進行以及協助演奏樂曲和節奏的練習。由於音樂演奏屬於程序性知識，學習者透過反覆練習以習得演奏的技巧，學習者會希望在練習中得到行動載具的指引，這種指引像是一個虛擬教師一般可以長時間並且讓學習者可以根據自己的進度自主進行練習。

另一部分，根據學習者對於使用行動載具中的學習應用App進行個人化學習歷程紀錄之需求問卷分析可發現，學習者喜歡透過使用行動載具上之學習App可完成屬於個人的數位學習成品，利用載具創作個人的數位作品的同時，學習者對於將作品收集整理為學習歷程以及分享抱持著正面的態度；學習者對於來自老師以及同儕的回饋建議都抱持正面的態度，樂於接受並相信從中可以得到學習上的助益。此外，學習者的性別亦是影響學習者使用載具的關鍵之一，從學習者的回饋發現男生較願意學習歷程被記錄下來，並且較女生相信記錄學習歷程有助於學習，男生也較喜歡觀摩他人的學習歷程，相信可以藉此幫助學習；而女生較喜歡分享自己的學習的成果。男女較大反差的部分，在以評分的方式給予彼此學習歷程回饋以及將作品的評比作排行比較，在此項目上男生顯現較高的偏好，而女生則回應較無興趣。

5.2 結論

本研究為一多階段性研究，本論文針對學習者使用問卷以及半結構式訪談進行初步的學習者需求與期待看法分析，根據研究結果，研究者將會針對國小主要學習科目：數學進行後續的行動載具學習App開發，將會針對七巧板拼圖、積木立體圖形及測量與面積計算等學習單元進行學習教材設計。此外，在學習歷程紀錄部分，將會著重在學習成果紀錄以及分享的功能，以增進學習者與同儕、與教學者間的互動，讓學習者在彙整自我的學習歷程中，更進一步反思與深入思考；也透過外來的回饋建議達到修正認知並更新知識架構的學習成效。

最後，本研究提出未來將設計的行動載具學習App的三大面向，包含:「學生個人化學習」，「增強課堂參與」以及「個人化學習歷程建置與分享」。

在「學生個人化學習」中，預期提供學生能自由簡易的將教師提供的教學材料進行編排註記，注重在介面的易用性以及學生對於教材的紀錄、管理的自主性，藉以提升個人化的學習要素；「增強課堂參與」主要為開發提升學生課堂的參與的機制，此模組注重在教學中間階段性的要求學生在活動中進行小組互動，達到學習者與同儕、與師生間之互動並記錄於資料庫中；「個人化學習歷程建置與分享」將學生在課堂上的筆記以及課堂活動中的回饋彙整成個人的學習歷程，可以整理自己已知的知識，也可以和同儕分享。本研究將根據所歸納之資料與結果進行下階段行動載具應用 App 開發，相關的研究成果將會在近期分享。

致謝

本研究由台達電子補助研究經費，特此感謝。

參考文獻

[1] J. Roschelle and R. Pea “A walk on the WILD side: How wireless handhelds may change CSCL.” G. Stahl (Ed)., Proceedings of CSCL 2002, Boulder, CO, January 7-11

[2] J. M. Chen, M. C. Chen and Y. S. Sun, “A novel approach for enhancing student reading comprehension and assisting teacher assessment of literacy.” Computer & Education, 55 (3), 2010, pp. 1367-1382,

[3] 張謙楣，”行動載具在支援高中國文科教室教學情境的應用。”未出版碩士(Master)，國立臺灣師範大學資訊教育學系，2005，台北市

[4] C. Grace, “The Portfolio and Its Use: Developmentally Appropriate Assessment of Young Children”, Eric, 1992.

[5] M. F. Baris and N. Tosun, “E-portfolio in Lifelong Learning Applications.” In H. I. Yalin, F. Adiloglu, H. Boz, S. Karatas & F. Ozdamli (Eds.), World Conference on Educational Technology Researches-2011 (Vol. 28). Amsterdam: Elsevier Science Bv.

[6] J. A. Moon, “Reflection in learning and professional development.” New York: Routledge, 2004.

[7] L. Stefani, R. Mason and C. Pegler, “The educational potential of e-portfolios: Supporting personal development and reflective learning.” New York: Routledge, 2007.

[8] J. W. Lin and Y. C. Lai, “Online formative assessments with social network awareness.” Computers & Education, 66(0), 40-53. doi: http://dx.doi.org/10.1016/j.compedu.2013.02.008

[9] D. W. Johnson and R. T. Johnson”Cooperative learning and feedback in technology-based instruction.” In J. Dempsey & G. C. Sales (Eds.), Interactive instruction and feedback. Englewood Cliffs, NJ: Educational Technology Publications, 1993.

[10] P. R. Pintrich and D. H. Schunk, “Motivation in education: theory research, and applications.” NJ: Prentice Hall Merrill., 2002.

[11] Scaife L., M. Scaife, Y. Rogers, F. Aldrich, M. Davies. “Designing for or designing with? Informant design for interactive learning environments”. Proceedings of CHI’97: Human Factors in Computing Systems ACM, New York pp. 343-350, 1997.

具自動出題與診斷能力的實體關係模型轉換關聯表教學輔助系統

邱瑞山　　蘇桓沂
大葉大學資訊工程系
jschiu@mail.dyu.edu.tw

摘要

資料庫課程為資訊相關科系的重要課程之一。關聯式資料庫是目前最廣為使用的資料庫類型，而實體關係模型也是在概念設計階段常用的模型。學生學習如何設計資料庫，除了須學會設計實體關係模型外，也要學會將實體關係模型正確的轉換為關聯式資料庫。本研究設計的實體關係模型轉換關聯式資料模型教學輔助系統具有下列的功能：(1)自動產生各種不同組合的實體關係模型，並繪製成實體關係圖，供學生練習；(2)自動產生解答；(3)自動判斷學生作答的結果是否正確，並給予適當的指引訊息，以協助學生完成作答；(4)動態展示逐步轉換教學；(5)記錄學習歷程，除了分析學生常犯錯誤，也顯示學生的學習成就。教師可以指定學生使用教學輔助系統完成課後作業，提昇學習成效。

關鍵詞：實體關係模型、關聯式資料模型、資料庫、智慧型教學系統、自動出題、自動診斷

Abstract

The database course is one of the important courses in computer-related fields. The relational database is currently the most widely used type of database. The entity-relationship model (ER model) is commonly used in the conceptual design phase. Students learn how to design a database, apart from having to learn to design ER model, they need also to learn to map an ER model into a relational database correctly. In this research, a tutoring system is implemented with the following features: (1) automatically generates a variety of different combinations of ER model which will be drawn as entity-relationship diagrams for students to practice; (2) automatically generates answers; (3) automatically determines whether the answers are correct or not and gives proper guidance messages to help students complete exercises; (4) dynamically shows the problem solving process step-by-step; (5) records learning portfolios for analyzing the common mistakes students make and demonstrating accomplishments. Teachers can request students to complete homework by using the system in order to enhance learning.

Keywords: Entity Relationship Model, Relational Data Model, Database, Intelligent Tutoring System, Automatic Item Generation, Automatic Diagnosis

1. 前言

資料庫普遍應用於各行各業的資訊系統中。資料庫課程為資訊相關科系的重要課程之一。資料庫課程主要內容包括：概念設計(Conceptual Design)，邏輯設計(Logical Design)，實體設計(Physical Design)，以及資料庫語言 SQL 等主題。其中，概念設計以介紹實體關係模型(Entity-Relationship Model)為主，邏輯設計包含關聯式資料模型(Relational Data Model)，實體關係模型對關聯式資料模型的轉換方法，以及正規化(Normalization)等[1]。關聯式資料庫是目前最廣為使用的資料庫類型，而實體關係模型也是在概念設計階段常用的模型。學生學習如何設計資料庫，除了須學會設計實體關係模型外，也要學會將實體關係模型正確的轉換為關聯式資料庫。這些課程主題不但需要理解其概念，更需要實作練習，才能深入了解其意涵，進而融會貫通。

隨著高等教育的日益普及，學校所招收的學生的素質越見參差不齊。在學習的過程中有些學生得心應手，而有些學生則會出現困難。學習成效不佳的原因，有些是由於學生本身的資質較差，需要花較多的時間才能學會；而有些則是學習意願較低，旁騖太多，花太少的時間在學習上。前者需要有老師或同學提供適時的幫助，後者需要有人督促與激勵。

以往學生修習資料庫課程之所以會感到所需理解的概念太過抽象而難以理解，除了缺乏抽象思考與邏輯推理能力外，往往是因為缺乏實作練習所導致的。如果要強化實作練習，必須有足夠多的題目可供練習，且學生自我練習遇到困難或錯誤時，需有即時且適當的指引來幫助學生解題。而要達到這樣的需求，其所需付出的時間與心力，並不是任課教師所能負荷的。

智慧型教學系統（Intelligent Tutoring System，ITS），能夠針對課程各項主題，提供多樣化的實作題目供學生練習，且學生在解題時，能判斷其作答是否正確，並能針對其所犯的錯誤，提出適當的指引以幫助學生繼續作答。這樣一個全年無休的自動化系統，對於提昇學生的學習成效及減輕任課教師的負擔將有莫大的幫助。

不過，即使有了 ITS 的輔助，如果學生不去使用，也是枉然。陳金奇[2]利用問卷方式調查我國的公務員使用數位學習系統的情況，調查結果顯示被

動學習占了 50.8%，主動學習占 39.6%，應付了事的人占了 9.3%。數位學習在沒有人監督的情況之下，認真主動使用的人數約只占了 40%。因此如何讓學習者持續的使用數位學習系統是目前主要的瓶頸之一。

解決之道其一是將 ITS 與作業結合，而 ITS 必須能自動產生多樣化的作業題目。其二是推動同儕學習(Peer Learning)。每位學生對於每門課的理解程度不一樣，理解程度較好的學生可以協助帶領理解程度較差的學生學習，相對的也可減少教師在教學上的負擔。

根據美國國家訓練實驗室(National Training Laboratories)之學習金字塔(Learning Pyramid)，學生在2週以後還記得的學習內容，會因為不同的學習方式而有很大的差異，如圖 **1**所示。光是聽教師用講述的方式，2週以後記得的內容只剩5%，因為這是最被動的學習方式，學生的參與度最低。如果用範例展示的方式，可記得30%，群組討論可達50%。但如果能動手練習則可達75%，教別人則可達90%。

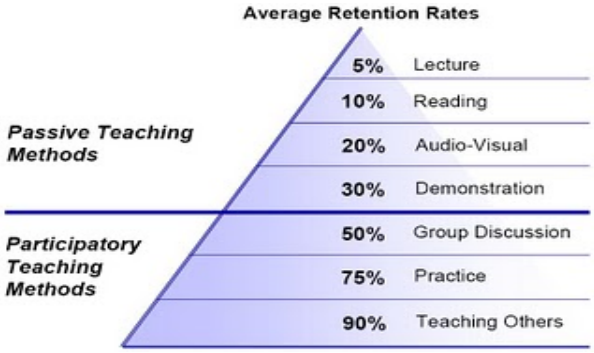


圖1 學習金字塔 (取自 National Training Laboratories. Bethel , Maine)

本研究所開發的擴充實體關係模型轉換關聯式資料模型學習輔助系統(Extended Entity Relationship Model to Relational Model Mapping Tutor)具有下列的功能：(1)自動產生各種不同組合的實體關係模型，並繪製成實體關係圖，供學生練習；(2)自動產生解答；(3)自動判斷學生作答的結果是否正確，並給予適當的指引訊息，以協助學生完成作答；(4)動態展示逐步轉換教學；(5)記錄學習歷程，除了分析學生常犯錯誤，也顯示學生的學習成就。學生可利用此一系統來自我學習，教師也可利用此系統來進行範例動態展示教學，並指定學生使用此系統完成課後作業。

此外，我們結合社群網站與教學輔助系統，透過任務合作的機制，來促進學生之間的互動，發展同儕學習，同時賦予成就動機，強化教學輔助系統的使用，以提昇學習成效[3]。為了促使學生相互學習，我們將課後作業轉換成任務的形式，學生要完成任務，除了必須使用教學輔助系統完成指定的練習外，也必須相互邀請同學一起來完成練習。透過相互邀請，相互幫忙的方式，期望能發揮相互教學與相互督促的作用。透過任務的獎勵，來增強學習的動力與成就感。藉由定期的任務來強化教學輔助系統的使用與持續的學習。希望藉此能全面的提昇學生的學習效能。

2. 相關文獻

布魯姆分類法(Bloom's Taxonomy)將認知領域區分為六個層級[4]，包括(1)知識層級(Knowledge Level)，(2)理解層級(Comprehension Level)，(3)應用層級(Application Level)，(4)分析層級(Analysis Level)，(5)綜合層級(Synthesis Level)，(6)評鑑層級(Evaluation Level)等。層級越高表示學習的效果越好。資料庫課程的目標是要讓學生有能力設計、運用及管理資料庫，也就是要達到應用層級以上，而要達到這樣的目標，學生須做足夠多的練習。

Keller[5]提出教學設計應把握ARCS四個要素，分別為注意(Attention)、相關(Relevance)、信心(Confidence)以及滿足(Satisfaction)。Carroll[6]提出影響學習模式(Model of School Learning)，認為學習成就與所做的努力，以及所需的時間密切相關。資質較差的學生，其學習所需的時間較多，需格外的努力才能學好。而現今被動學習的學生居多數，因此要提昇學習的成效，須有辦法讓學生願意花足夠多的時間在學習上，不但能學得會，且能從中得到成就感。

教學輔助系統已發展多時，許多的學者在研究如何讓學生使用教學輔助系統更有效率。智慧型教學系統(ITS)在學生練習解題時，不需人為介入，即能提供有效的指導或回饋[7]。ITS具體實現了從做中學的理論。從1990年後，ITS有日益普及的趨勢。

紐西蘭Canterbury大學的Intelligent Computer Tutoring Group(ICTG)自1998年起陸續開發了一系列資料庫課程相關的智慧型教學系統，包括KERMIT[8]，EER-Tutor[9]，ERM-Tutor[10]，SQL-Tutor[11]，和NORMIT[12]等。這些教學系統除了供Canterbury大學修習資料庫課程的學生使用外，也授權給Addison Wesley的DatabasePlace[13]，供購買該出版社資料庫書籍的讀者以Web-based的方式使用該系統。實驗顯示，這些教學系統對學習資料庫有顯著的幫助[14]。

西班牙 Girona 大學自 2005 年起陸續開發了一系列的線上資料庫教學系統 ACME-DB，包括Entity-Relationship Model[15]，Relational Database Schema[16]，Normalization[17]，SQL 和 Relational Algebra[18]等主題。實驗顯示，從 2002-2004 年尚未使用 ACME-DB，到 2005-2008 使用之後的比較，成績明顯提升，而不及格率從 2002 年的 56.3%降到 2008 年的 22.2%，成效顯著[19]。

過去這些ITS為Constraint-based的系統，題目和解答須手動產生，並由專家撰寫推論規則。本研究所開發的系統，則具有自動產生題目和解答，自動檢查作答是否正確，並提供漸進式提示的能力。ICTG所開發的ERM-Tutor僅包含實體關係模型對關聯式資料模型轉換方法的教學與練習。本研究所

開發的系統，除了擴增為擴充實體關係模型對關聯式資料模型轉換方法的教學與練習，還具有動態展示逐步轉換教學的功能。如此除了可節省大量人力外，也可增加系統的用途，例如用於教學展示、作業練習或測驗。

本研究所開發擴充實體關係模型轉換關聯式資料模型的學習輔助系統是一個整合的資料庫教學與實作練習系統的子系統，其他還包括：Extended ER Modeling Tutor、Relational Algebra Tutor[20]、SQL Tutor[21]和Normalization Tutor[22]等子系統。系統根據資料庫的定義和資料內容，進行反向工程(Reverse Engineering)，並實作各種資料庫設計和轉換的演算法，因此授課教師只需要將資料庫匯入，做簡單的設定，系統就能夠自動產生練習題目與解答。

3. 研究方法與進行步驟

本研究所開發的教學輔助系統與社群平台結合運作。圖 2 為教學輔助系統的架構。出題模組能自動產生各種不同組合的實體關係模型，並繪製成實體關係圖，供學生練習、作業或測驗。診斷模組能自動根據系統產生的解答，判斷學生作答的結果是否正確，並給予適當的指引訊息，以協助學生完成作答。通訊模組負責與社群平台互動交換訊息，而成就模組則在學生完成作業時，透過通訊模組在社群平台發佈訊息。

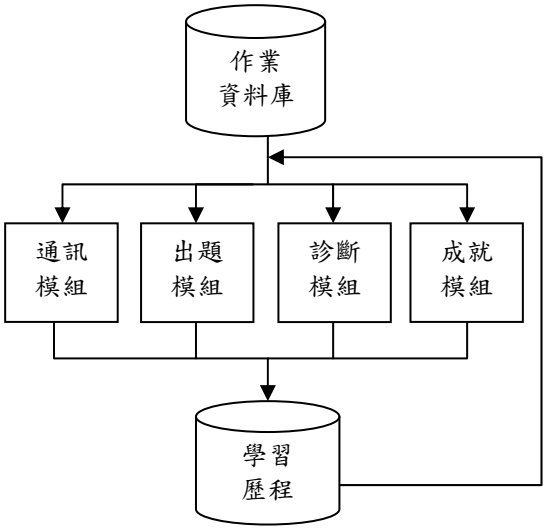


圖2 教學輔助系統架構。

系統提供四種模式。(1)教學模式：除了包含課程教學內容外，也能自動展示解題的逐步過程，以幫助學生理解。(2)練習模式：系統能自動產生不同難度的題目供學生練習，也能自動診斷作答結果是否正確。如果作答有誤，將提供診斷訊息、提示與教學連結，以協助學生完成作答。(3)作業模式：學生須在無提示下，正確解答系統指派的題目。如果答錯，也必須修正到答對為止，否則下一題即使答對也不列計。(4)同步學習模式：數位學生可透過網路合作方式，同步使用教學輔助系統，共同操作以完成解題練習[23]。。

系統以C#、ASPX與JSP共同開發Web-based的教學輔助系統，使用HTML5、Ajax技術及Javascript來處理及時互動。後端使用 MySQL 資料庫。修課學生可透過瀏覽器來做課後練習。

3.1 自動出題

擴充實體關係模型轉換為關聯式資料模型，共分為九個步驟[2]，包括：

(1). 轉換一般實體型態(Regular Entity Type)為資料表，

(2). 轉換弱實體型態(Weak Entity Type)為資料表，

(3). 轉換一對一的二元關係型態(Binary Relationship Type)，

(4). 轉換一對多的二元關係型態，

(5). 轉換多對多的二元關係型態為資料表，

(6). 轉換多值屬性(Multivalued Attribute)為資料表，

(7). 轉換多元關係型態(N-ary Relationship Type)為資料表，

(8). 轉換特殊化(Specialization)或一般化(Generalization)，

(9). 轉換聯集型態(Union Type)。

題目共分為五個等級，等級一包含步驟(1)到(2)，等級二包含步驟(1)到(5)，等級三包含步驟(1)到(7)，等級四包含步驟(1)到(8)，等級五包含步驟(1)到(9)。其中步驟(3)又分三種不同的情況與轉換方式，步驟(8)也有四種不同的情況與轉換方式。

自動出題分兩類，一類是資料庫出題，另一類是隨機出題。資料庫出題是系統利用所匯入的各種範例資料庫，以反向工程技術將關聯式資料庫定義轉換為實體關係模型，再產生實體關係圖。資料庫出題方式所產生的實體、關聯和屬性名稱均具有實質意義，較具真實感。但所能產生的題型組合較有限。

隨機出題是由系統自動根據題目等級所需組合，隨機產生包含實體型態、弱實體型態、主鍵屬性、複合屬性、簡單屬性、多值屬性、一對多二元關係、一對一二元關係、多對多二元關係、多元關係、特殊化和聯集型態等的實體關係模型，然後利用Graphviz套件產生實體關係圖。Graphviz是一種開放源碼的圖形視覺化軟體，由一種被稱為DOT的圖形描述語言與一組可以產生和處理DOT檔案的工具所組成[24]。系統會自動產生實體關係圖的DOT檔案。

3.2 自動診斷

系統實作了轉換的演算法，會將實體關係模型

轉換成關聯表，以做為檢查答案正確與否的依據。系統會逐一比對關聯表及其屬性，屬性除了逐一比對名稱，以檢查是否有多餘或缺少的屬性外，還比對是否為主鍵和是否為外來鍵。由此可診斷出哪些轉換步驟有錯及錯誤的原因。

在練習模式下，系統會顯示錯誤診斷訊息和教學網頁連結，以協助學生找出錯誤和完成作答。透過連結可連到該轉換步驟的教學網頁。而在作業模式下，系統只顯示錯誤，不提供作答提示與教學網頁連結。

系統會記錄學生的作答歷程，包括題目的等級、作答時間、是否完成、答錯次數、答錯的步驟和原因等。系統會針對個別學生及全體學生分別統計、分析並顯示下列資訊，包括作答次數、各題目等級與步驟答對率及升降趨勢、各題目等級平均作答時間及升降趨勢、完成題目等級加權平均與各種排名等。一方面可供學生參考，了解和比較自身與全班的學習狀況，也可做為適性化出題的依據，另一方面也可讓教師了解多數學生常犯錯誤，可以在課堂上再加強。

3.3 動態逐步轉換教學

在教學模式下，選擇題目的等級後，系統會隨機產生一個該等級的實體關係圖，並顯示步驟1的轉換結果。系統也會顯示該步驟的教學網頁連結，裡面有詳細範例解說。可透過下一步或上一步，逐步學習每一轉換步驟。圖 **3**為實體關係圖逐步轉換教學的第2步驟，即弱實體型態的轉換。實體關係圖中和已處理的步驟有關的部份會以藍色顯示，和目前步驟有關的部份以紅色顯示，尚未處理的部份以黑色表示。轉換所產生的關聯表和屬性也會以顏色區別。屬性前面星號表是主鍵，屬性後面括弧關聯表示外來鍵及其所參照的關聯表。教師可利用此功能進行動態範例教學，學生也可於課後自我學習。

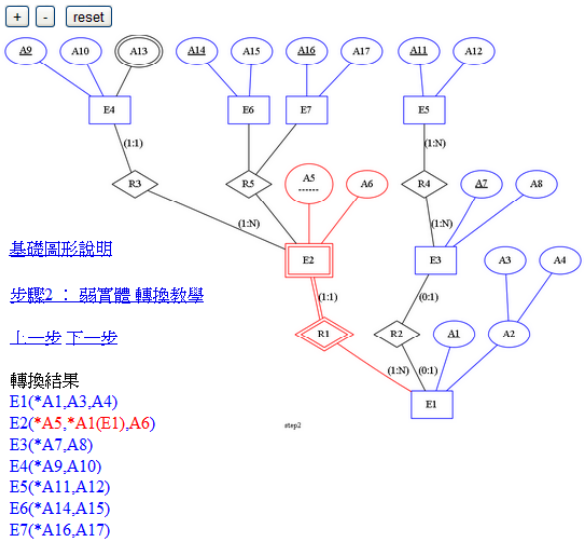


圖 3 實體關係圖逐步轉換教學

3.4 同步與非同步學習

本系統可在同步學習環境下使用，具有同步操作、視訊、音訊、和文字聊天室等功能。學生可透過網路合作方式，同步使用教學系統，共同操作以完成解題練習。學生之間可利用此一環境相互教學。

此外，學生（和教師）也可以儲存解題步驟，並發佈於社群網站的塗鴉牆。其他同學可藉由重播來學習。

同步操作與非同步解題步驟儲存與重播採用事件觸發與重演的方式，視訊語音傳播採用P2P方式，大幅降低伺服器的負擔。

本研究採用HTML5的Websocket技術[25]來進行雙向通訊，並以PostMessage配合javascript處理跨網域網頁間的訊息交換。以WebRTC技術[26]進行瀏覽器間的點對點影音資訊傳輸。使用者只需連上網站，不需安裝外掛程式，即可進行同步學習。系統不但具有跨各種平台的優點，且使用頻寬較少，伺服器的負擔也較輕。

4. 實驗計劃與預期成果

資料庫教學輔助系統已完成且已使用的子系統包括SQL、關聯代數和正規化等。擴充實體關係模型轉換關聯式資料庫的子系統已完成但尚未正式使用。擴充實體關係模型的教學輔助子系統則仍在開發中。後面兩個子系統預計於102學年度正式使用。

實驗計劃與中部某大學資訊工程系“資料庫系統”課程結合。依課程進度，以作業(任務)形式要求修課學生於指定期限內，使用資料庫教學輔助系統相關單元，完成一定題數的練習。預計約每隔兩週發佈一次作業。

計劃於學期末實施無記名問卷調查，以評估各項成效。問卷選項分為非常不同意、不同意、部份同意、同意以及非常同意共5項，分數從非常不同意的1分到非常同意的5分。

SQL、關聯代數和正規化三個子系統已於100學年度正式使用。修課人數共91人，問卷回收率91%。表 **1**為學習成效問卷統計結果，顯示多數學生認同資料庫教學輔助系統有助於提高學習成效。此外，學生完成作業能得到成就感。傳統課後作業抄襲一直是令教師頭痛的問題。為了防範學生抄襲，系統每次所出的題目都不一樣，這使得學生無法互相抄襲答案，即使要幫忙作答，所需花費的時間也難以負荷。問卷結果也顯示多數的學生都認同，相較於傳統作業，本系統的自動出題機制可以減低作業抄襲的風氣。

我們預期擴充實體關係模型子系統和擴充實體關係模型轉換關聯式資料庫的子系統正式使用後，能顯著提升資料庫概念設計與邏輯設計的學習成效。

表 1 學習成效問卷統計結果

單元	問卷題目	平均
SQL	使用SQL教學系統對熟悉SQL語法有幫助	4.2
	使用SQL教學系統對正確運用SQL語法寫出查詢有幫助	4.1
關聯代數	使用關聯代數教學系統對熟悉關聯運算有幫助	4.0
	使用關聯代數教學系統對正確運用關聯運算寫出查詢有幫助	4.0
正規化	使用正規化教學系統對找出Candidate Key有幫助	3.7
	使用正規化教學系統對找出Partial/Transitive Functional Dependency有幫助	3.8
	使用正規化教學系統對找出2NF, 3NF, BCNF 有幫助	3.7
全部單元	完成作業有成就感	4.0
	相較於傳統作業，系統的自動出題機制減低了作業抄襲的風氣	3.9

5. 結論與未來方向

本研究所開發的擴充實體關係模型轉換關聯式資料模型學習輔助系統是一個整合的資料庫教學與實作練習系統的子系統，其他還包括：Extended Entity Relationship Modeling Tutor、Relational Algebra Tutor、SQL Tutor和Normalization Tutor等子系統。系統具有下列的功能：(1)自動產生各種不同組合的實體關係模型，並繪製成實體關係圖，供學生練習；(2)自動產生解答；(3)自動判斷學生作答的結果是否正確，並給予適當的指引訊息，以協助學生完成作答；(4)動態展示逐步轉換教學；(5)記錄學習歷程，除了分析學生常犯錯誤，也顯示學生的學習成就。

本研究所開發的系統除了可供學生於課後自我學習外，同儕之間也可用利用此系統進行同步或非同步教學。教師可利用此系統進行動態示範教學，也可分配作業或測驗。我們預期系統將有助於提昇學生的學習成效。

本研究尚在開發中的擴充實體關係模型子系統除了可自動產生資料需求文字敘述，供學生練習設計擴充實體關係模型外，也可自動產生各種典型的表單和報表格式與內容。學生可學習如何從表單與報表中擷取出有用的資料需求。這是設計資料庫所應具備的重要能力。

參考文獻

[1] R. Elmasri and S. B. Navathe, Fundamentals of Database Systems, 5th Ed., Addison Wesley, 2007.

[2] 陳金奇，“我國地方政府公務人員參與數位學習態度與行為之研究”，國立臺灣師範大學社會教育學系社會教育與行政文化行政碩士在職專班碩士論文，2011 年。

[3] 邱瑞山、呂岳訓和張佳豪，“以任務合作機制發展同儕學習”，TANET 臺灣網際網路研討會，2012 年。

[4] B. Bloom, Taxonomy of Educational Objectives: The Classification of Educational Goals, London: Longman Group United Kingdom, 1969.

[5] J. M. Keller, “Development and Use of the ARCS Model of Instructional Design,” Journal of Instructional Development, vol. 10(3), pp. 2-10, 1987.

[6] J. B. Carroll, A model of school learning. Teachers College Record, 64, 723-733, 1963.

[7] J. Psotka, L. Massey, S. A. Mutter, and J. S. Brown, Intelligent Tutoring Systems: Lessons Learned, L. Erlbaum, 1988.

[8] P. Suraweera and A. Mitrovic, KERMIT: A Constraint-Based Tutor for Database Modeling, Lecture Notes in Computer Science, 2002.

[9] K. Zakharov, A. Mitrovic and S. Ohlsson, Feedback Micro-engineering in EER-Tutor. In Proc. Artificial Intelligence in Education AIED, IOS Press, pp. 718-725, 2005.

[10] Milik, N., Marshall, M. and Mitrovic, A. (2006), Responding to Free-Form Student Questions in ERM-Tutor, Lecture Notes in Computer Science.

[11] A. Mitrovic, An Intelligent SQL Tutor on the Web, International Journal of Artificial Intelligence in Education, Vol. 13 No. 2-4, pp. 173-197, 2003.

[12] A. Mitrovic, NORMIT: A Web-Enabled Tutor for Database Normalization, Proceedings of the International Conference on Computers in Education, 2002.

[13] Database Place, http://www.aw-bc.com/databaseplace/.

[14] A. Mitrovic and the ICTG team, Large-Scale Deployment of Three Intelligent Web-based Database Tutors, Journal of Computing and Information Technology – CIT, Vol. 14, No. 4, pp. 275–281, 2006.

[15] F. Prados, I. Boada, J. Soler, and J. Poch, “A web based tool for entity relationship modeling,” Proceedings of International Conference on Computational Science and its Applications (ICCSA), Glasgow, UK, LNCS 3980, pp. 364-372, 2006.

[16] F. Prados, I. Boada, J. Soler, and J. Poch, “An automatic correction tool for relational database schemas,” Proceedings of International Conference on Information Technology based higher Education and Training (ITHET), Santo Domingo, Dominican Republic, 2005.

[17] F. Prados, I. Boada, J. Soler, and J. Poch, “A web based problem solving environment for database normalization,” Proceedings of 8th International Symposium on Computers in Education (SIIE), Leon, Spain, 2006.

[18] F. Prados, I. Boada, J. Soler, and J. Poch,, “An automatic correction tool for relational algebra queries,” Proceedings of International Conference on Computational Science and its Applications (ICCSA), Kuala Lumpur, Malaysia, LNCS 4706, pp. 861-872, 2007.

[19] J. Soler, I. Boada, F. Prados, J. Poch, J., and R. Fabregat, “Database design using a web based e-learning tool,” Department of Computer Science and Applied Mathematics, University of Girona, Spain, 2008.

[20] 邱瑞山和呂文凱，“具自動出題和診斷能力的關聯代數學習輔助系統”，KC2011 知識社群研討會，2011。

[21] 邱瑞山和呂文凱，“具自動出題和診斷能力的 SQL 學習輔助系統”，DLT2011 數位生活科技研討會，2011。

[22] 邱瑞山，“具自動出題與診斷能力的資料庫正規化學習輔助系統”，EITS2010 數位教學暨資訊實務研討會，2010。

[23] 邱瑞山、呂岳訓和呂文凱，“結合社群網站與教學系統的協同合作學習環境”，Taiwan CSCL & AIED SIG Conference，2012。

[24] Graphviz, http://www.graphviz.org/.

[25] I. Hickson, The WebSocket protocol, Retrieved from http://www.whatwg.org/specs/web-socket-protocol/.

[26] W3C, Real-time communication between browsers, http://dev.w3.org/2011/webrtc/editor/webrtc.html.

A Study on the Integration of Online Learning into English Course Design

Hui-chih Wang
Dept. of Applied Linguistics and Language Studies
Chung Yuan Christian University
Chung -Li, Taiwan
Corresponding author's e-mail: laura@cycu.edu.tw

Harry Shih
Dept. of Business Administration
Chung Yuan Christian University
Chung-Li, Taiwan

摘要

本研究的主要目的是要檢驗以整合線上學習教材與線上測驗為主的教學策略是否能融入大二英文課程並幫助高學習動機之學生提升他們的英文閱讀、聽力、文法及字彙程度。樣本共 76 人，取樣在台灣北部一所大學，分為實驗組及對照組，於 2011 年學期初進行需求評估，同時使用具國際公信力之 Michigan Test 進行前測，整學年結束前進行 Michigan Test 後測，由學生表現得知此一教學策略確能幫助學生的英文學習，實驗組在融入線上學習教材與線上測驗自學練習之後，閱讀、聽力、文法及字彙均有進步，前、後測總平均進步 3.83 分，對照組也有進步，但於閱讀項目則是退步。

關鍵詞: 期初需求評估，線上測驗

ABSTRACT

The purpose of this study was to examine if the integration of online learning into sophomore general English class was effective to advance students' learning performance regarding listening, reading, grammar usage, and vocabulary.

A needs analysis questionnaire was constructed and distributed to 76 Sophomore who were taking a required **Sophomore General English class** in a northern university in Taiwan. These students were divided into an experimental group and a control group. For experimental group, Internet learning resources adapted from Studio Classroom, Live ABC, New TOEIC, and GEPT vocabulary test bank play an important role in the course design and learning activities in and out of class. Throughout the fall of 2011 and spring 2012, four thematic teaching units, each using a theme-based structure were given to both groups of students as they join Sophomore English class. During the initial stage of this course, Michigan Test, a well-established achievement test served as a pretest for examining the participants' English learning performance was conducted; the posttest of Michigan Test was again given at the end of the following semester in 2012. A SPSS sampling t-test was run in this study. The Michigan Test results indicated that students in both experimental and control groups made progress in **vocabulary, listening,** and **grammar** learning. For the overall performance, with the assistance of the integration of online learning materials and the practices of online mock tests, the experimental group outperformed the control group by 1.10 points.

Key words: initial needs assessment, online test

I. INTRODUCTION

In Taiwan, English course has always been one of the major content areas from elementary school up to college level. Following with the advancement of technology, computer-assisted language learning in TESL (Teaching English as Second Language) field has become a teaching trend. To create a more interactive, learning at ease, self-paced, and authentic English learning environment for today's Taiwanese students, many English teachers feel struggled to dominate the teaching-and-learning time with mainly lectures, instead, they are willing to provide a learner-centered, performance-based as well as self-motivated learning atmosphere in the school setting. In other words, learning English should not be "forced" or "required" responsibility which demand students to succeed in academic achievement only. Moreover, the increasing usage of Internet-driven or online learning as part of the formal instructional strategy and self-study learning tool help Taiwanese students to eliminate their "fear" toward leaning English. In order to have high competition ability in their future career or work environment, nowadays, Taiwanese students understand the importance of self-engaged motivation, autonomous learning and their association with online learning. To get more specific, for these so called "Internet generation" youngsters, the integration of online learning into English learning is, no doubt, a priority.

For non-English major, science-oriented college students in this study, communicative trainings of English are really important and the training usually takes integrated instructional approaches to achieve the goal. In an integrated/thematic, Internet-assisted approach to learning, students become active participants in the learning and assessment process. As Walker and Soltis (2009) stated students' learning records on website and other progress of learning, all can be valuable tools when teachers designing their own curricula, many teachers find much enjoyment in thinking about new ways to integrate multiple or

various strategies into their class. As a matter of fact, integrated thematic instruction calls for a non-traditional approach to assessing the effectiveness of the instruction and student learning performance (Etim, 2005).

II. PURPOSE OF THE STUDY

This study was designed to explore if the integration of online learning into Sophomore English course was effective regarding participating students' performance in listening, reading, grammar, and vocabulary.

III. LITERATURE REVIEW

It is not surprising to find that many of today's foreign language texts are designed to be theme/topic-based materials and instruction in their chapters or units. The emphasis of foreign language learning has moved from a traditional approach to an integrated-skill communicative approach, including a variety of online learning strategy, in which learners acquire both linguistic and cultural competence (Lee, 2001).

Furthermore, with the assistance of Internet learning, a structured theme/topic-based five skill (reading, speaking, listening, writing, and communication) class could provide the learners more authentic reading materials as well as up-to-date global information from different forms such as online test and online learning resources. To be more specific, today's college students need to be more equipped with wide reading through Internet and its practice of self-expression, which builds language fluency, large vocabulary, syntactical knowledge, and culture appreciation ability (Wang & Shih, 2007).

Education in the 21st century should be more inspiring and full of flexibility; however, it has been criticized for being overwhelmed by the "test-driven" orientation in English education (Chu, Wang, & Shih, 2013). Under the circumstances, students learn the materials unavoidably put stress on gaining good grades at the expense of students' real interests and needs. However, as TESL teachers, one of the unavoidable missions still is to help students pass proficiency test in order to survive in today's highly competitive society. With a new perspective, today's English teachers feel that most students may enjoy learning at their own pace if only they have better or full control of the way they learn. Facing reality, taking proficiency test is necessary for their future, but they no longer have to be caught up in dilemma. English teachers serve as the facilitators who find out what students' goals are and what topics they want to learn about, then built these into the curriculum as much as possible. Students would be motivated to learn as long as they think the material is worth learning. However, teachers should keep in mind that the existence of materials is to strengthen learning and teaching, not just enhance students' workload in learning. Many studies suggested that teachers add issues about society and contemporary life in the class according to Taiwanese students' needs and local culture to reach the ultimate goal of learning.

As we all know, students' needs, abilities, and interests should be taken into consideration in the selection process of learning materials to reduce students' learning burden and help students achieve the objectives set for each unit or lesson provided in the class. In order to motivate students, language teachers need to offer something authentic to them, and something that corresponds to their students' practical needs along with passing tests. Apparently, English magazines as well as online English learning materials are good authentic materials which are worth being adapted to the classroom to bring the best out of each student.

IV. DEFINITION OF TERMS

Initial needs assessment. In the first week of the class, students will answer survey questions about their learning background, learning needs, and possible goals for the course to prepare teachers to write or modify their own goals and objectives (Graves, 2001).

Online test. Standardized GEPT, New TOEIC, and 5,000 vocabulary list adapted from GEPT website serve as the basis and test bank which facilitate a self-paced online learning and online mock test for college students in general (Wang & Shih, 2012).

V. RESEARCH DESIGN, DATA ANALYSIS AND FINDING

Part One.

Implementation of Needs Analysis and Its Significant Results

At the first week of class in fall 2011, 76 sampling students in **Sophomore English** class were distributed a "needs analysis" questionnaire to understand the following questions: (1) age to start learning English, (2) motivation in learning English (3) motivation in learning online learning materials (4) difficulty in learning English, (5) with the assistance of online learning, the specific needs for them in learning English for a specific field of study (i.e. the professional subject taught in whole English), (6) with the assistance of online learning, the needs of using authentic English, (7) the needs for them in learning Internet English, and (8) perception about online learning and proficiency test. Seventy-one valid needs analysis questionnaires were collected.

As for the starting point, 40.8% of the sampling subjects started learning English at the 3rd grade in elementary school. Moreover, 22.5% began to study English since kindergarten. The answer for "having motivation to learn English" was encouraging to the researchers. 51 (71.7%) of the sampling students expressed that they have motivation learning English.

To probe for a more clear answer, 74.6% of these students voice out their opinions which further confirmed that they “have motivation in learning online learning materials.” Regarding the biggest challenge they face in learning English, 84% of them pointing out that they have had very limited vocabulary; they expect teachers help them enlarge the vocabulary span in Sophomore English class. To get more specific, 74.6% of those participants indicated that they need to enhance their language ability in taking a whole English class in their professional field of study. As we all know that Ministry of Education put emphasis on “Whole English Class for Learning Professional Subjects” as one of the most important policy enforced in Taiwan today. Sampling subjects here do have a strong need to get used to or pass these professional subjects taught in English. Table 1 showed that 53 among 71 participants indicated that they need to improve their ability in taking a whole English class offered from their professional subject or specific field of study.

Most importantly, as Table 2 showed, 62 participants expressed they need to improve communication skills in utilizing authentic English. In Table 3, 81.3% of these sampling subjects expressed clearly that they need to learn how to read materials (e.g. Internet reading materials including magazines or other articles) written in English. When the choice “somewhat important” is included, 97.3% sampling subjects believe there is a need for them to build up their reading skills based on the trainings learned in class, so they can read and understand English magazines such as Studio Classroom and other Internet learning materials now.

Many participants (78%) recognize that performance in English proficiency test plays a very important role in their future, especially for future career development in the work place. They understand proficiency test is associated with general language skills (i.e. reading, listening, grammar, and vocabulary). Moreover, students understand proficiency test is to examine how good their language skill currently is and how much efforts they need to put into the learning progress to strengthen these language skills. A need to integrate online learning materials into sophomore English class was indicated by the sampling students from this needs analysis questionnaire.

TABLE 1. WITH ONLINE LEARNING, BE ABLE TO TAKE A WHOLE ENGLISH CLASS IN PROFESSIONAL SUBJECTS

	Frequency	Percent	Valid Percent	Cumulative Percent
not important	4	5.6	5.6	5.6
somewhat important	14	19.7	19.7	25.3
important	37	52.1	52.1	77.4
very important	16	22.5	22.5	100.0
Total	71	100.0	100.0	

TABLE 2. WITH ONLINE LEARNING, BE ABLE TO COMMUNICATE WITH OTHERS USING AUTHENTIC ENGLISH

	Frequency	Percent	Valid Percent	Cumulative Percent
not important	1	1.4	1.4	1.4
somewhat important	8	11.2	11.2	12.6
important	33	46.4	46.4	59.0
very important	29	40.8	40.8	100.0
Total	71	100.0	100.0	

TABLE 3. WITH ONLINE LEARNING, BE ABLE TO READ ENGLISH INTERNET RESOURCES

	Frequency	Percent	Valid Percent	Cumulative Percent
not important	2	2.8	2.8	2.8
somewhat important	12	16.9	16.9	19.7
important	44	62.0	62.0	81.7
very important	13	18.3	18.3	100.0
Total	71	100.0	100.0	

Part Two. Implementation Stage
Research procedure illustrated below:

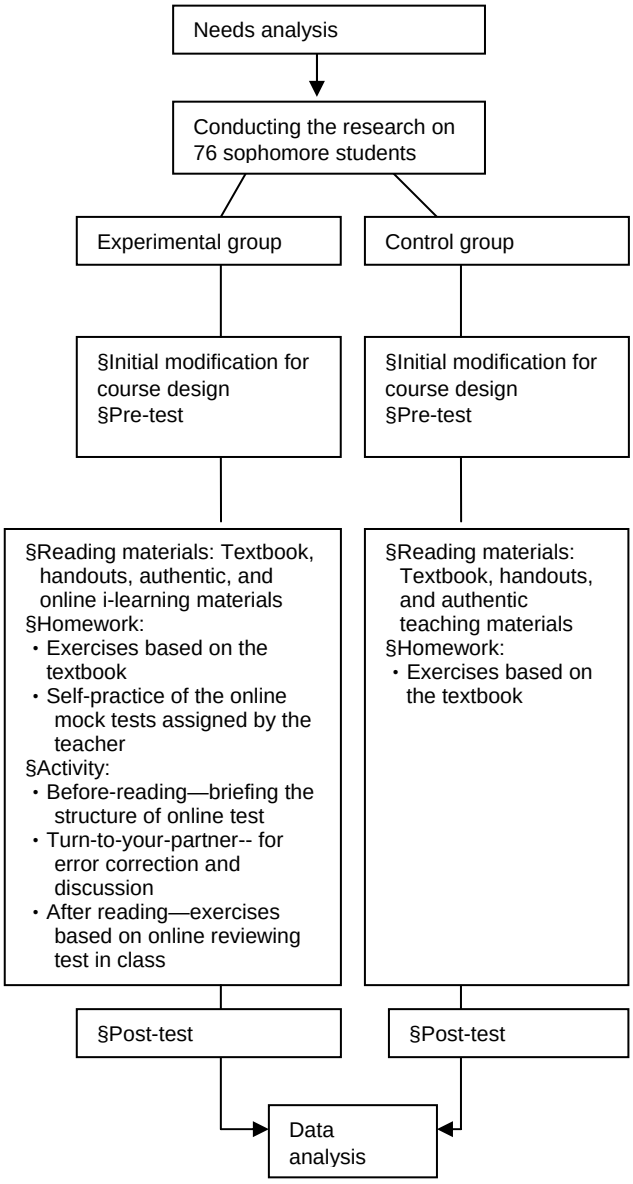


Figure 1. Course design framework

In this study, the researcher and her co-workers recognized that one of the most important features of course design for both groups was developing opportunities for students to fully understand what they know, how well they master course materials or how well they could use skills they were developing in the course and from the course. Vocabulary list and context provided form online Studio Classroom, Live ABC, Teacher vision (Tyler, 2005), New TOEIC and GEPT were added into experimental group.

The basic course design framework for both groups are stated below:

1. Syllabus checklist. A well-organized syllabus, included course goals, objectives, descriptions, required textbooks, homework assignments, assessment rubrics, class rules, weekly schedule, and a clear guideline for individual and small group participations in group activities, discussions, presentations, and individual test schedule was given to each student. From the first week of the class, each student of both groups understood clearly that this class required students **come to class prepared**.

2. Learner-centered, Theme-based Design. A theme-based, learner-centered instructional design served as the core. The learner-centered thematic teaching units were implemented in sequence, they were: (1) Technology Units – including "Internet Ethics" and "Internet as social media" units. (2) Culture Appreciation Units – including "friendship across culture" and "education around the world" units. (3) Contemporary Concern Units – including "global concerns" and "earth green" units. (4) Critical Thinking Units – including "controversial issues for debating" and "movie viewing for reflective thinking" units.

Part Three. Ongoing Process for the Application of Online Learning and Online Mock Test in Experimental Group

1. Online test integrated as part of class learning activity – in class online reviewing test which was composed by The Language Center in the university.

(1) Schedule: two times in one semester; first one was given before midterm exam, second one was given before final exam

(2) Content related to thematic units of sophomore English, GEPT, New TOEIC, and the format was presented as (A) vocabulary and structure (items 1-10), (B) cloze (items 11-15), and (C) reading comprehension (items 16-25). Items were selected from the aforementioned test bank as to help sophomore in the experimental group to be familiar with English proficiency test.

2. Online mock tests were given as self-learning practices. This part was assigned as homework which allowed students to finish it within a certain period of time.

(1) Schedule

(A) Four GEPT intermediate level mock tests open to test- takers (biweekly)

(B) Two GEPT high-intermediate level mock tests open to test-takers (biweekly)

(C) Two New TOEIC mixed level mock tests open to test-takers (biweekly)

(2) Test contents cover both reading and listening sections

(3) Test-taking procedure

(A) Log in:http://easytest.lib.cycu.edu.tw

(B) Select GEPT or New TOEIC test bank, then select "course code" to begin the mock test

(C) Go over answer sheet to self-correct errors.

Part Four. Results of Pretest and Posttest on Learning Performance

This study applied SPSS sampling t-test. A noticeable increase was found on the sampling students' listening, reading, as well as vocabulary performance. The total mean for experimental group improved 0.14 points for listening, 1.38 for grammar, 2.28 for vocabulary, and 0.03 for reading. For control group, they gain 0.03 for listening, 1.24 for grammar, 1.65 for vocabulary; they had regression on reading. As for the total mean, overall progress for experimental group improved 3.83 points; control group gained 2.73 only. The result turned out to be that experimental group outperformed control group by 1.10 points.

For experimental group, listening, reading, even the usage of grammar all improved. In the beginning of this study, both groups voiced out their serious concern for a lack of vocabulary; at the end of the study, the results revealed the fact both groups have improved their performance in vocabulary learning. The regression in reading score for control group revealed that the integration of online learning and online test was needed for this group; both online learning and online mock test help college students read more and prepare better in terms of English proficiency.

TABLE 4. LEARNING PERFORMANCE IMPROVED IN THE STUDY

Sophomore from Department of Chemical Engineering (Experimental group)
Sophomore from Department of Industrial Engineering (Control group):

	Experimental group	Control group
Sampling subjects took pre-and-post test:	29 students	37 students
Total mean score improved	+3.83	+2.73
Listening mean score improved	+0.14	+0.03
Grammar mean score improved	+1.38	+1.24
Vocabulary mean score improved	+2.28	+1.65
Reading mean score improved	+0.03	- 0.19

VI. CONCLUSION AND RECOMMENDATION

In this study, the repeatedly practice of online mock test and the large amount of time spent on reviewing online reading materials indeed help individual students in the experimental group to be more self-engaged in learning and better equipped with test-taking skills. The results of learning performance indicated that students in experimental group made impressive progress on listening, reading, grammar, and vocabulary; for them, the total mean between pretest and posttest improved 3.83 points. Additionally, the results of needs analysis enabled the teacher to be more informed while designing class learning activity, and put more emphasis on the use of online learning. However, limited by the number of sampling size of this study, more studies and an in-depth interview should be taken on both groups; more observations and follow up study should be done in the near future.

ACKNOWLEDGMENT

This study is sponsored by the Teaching Excellence Project, between 2011-2012, from Ministry of Education, R.O.C.

REFERENCES

[1] D.F.Walker, and J.F. Soltis, Curriculum and aims. N.Y.: Teachers College, Columbia University, 2009.
[2] J. S. Etim, Curriculum integration K-12. Lanham, Maryland: University Press of America, Inc, 2005..
[3] L, Lee, "Online readings and discussions." In G. Brauer (Ed.), Pedagogy of language learning in higher education. London: Alex Publishing., 2001.
[4] H. C. Wang, and H. Shih, "Integrating online learning strategies into classroom teaching," In Leung, Y. N. (Ed.), Selected papers from the Sixteenth International Symposium on English Teaching. Taipei: Crane Publishing Company Ltd., 2007, pp. 556-562.
[5] M.C Chu, H.C. Wang, and H. Shih, The use of needs assessment in designing practical English course. Proceeding of Oversea Chinese University (OCU) Tourism & Hospitality, Language, and Culture Conference, Taichung, Taiwan, 2013, in press.
[6] K. Graves, Designing a language course. N.Y.: Heinle-Thompson Publisher, 2001.
[7] H. C. Wang, and H. Shih, "The use of focused discussion learning strategies in teaching college high achievers," In Leung, Y. N. (Ed.), Selected papers from the 21st International Symposium on English Teaching. Taipei: Crane Publishing Company Ltd., 2012, pp. 348-356.
[8] M.Tyler,."Belly Slide" and "Toboggan: No Brakes" (http://wallyandosborne.com/2005/08/10) Wally and Osborne. http://www.teachervision.fen.com/creative-writing/printable/34492.html, 2005.

應用校園文化地景主題網站進行知識移轉之研究

李宜蓁
高雄市大寮區忠義國民小學　教師兼任教務主任
ichen.lyn @gmail.com

摘要

本研究旨在探討國小學生應用文化地景主題網站進行知識移轉，並了解其知識移轉的覺知。在本研究中，以 12 位國小六年級學生為研究個案，透過主題網站，進行「校園文化地景」知識的移轉。

本研究採取質性研究法，透過文件蒐集與訪談法，將獲得資料歸納及分析。本研究的發現有三項，分別是（一）學生應用資訊科技(電腦)學習知識；（二）透過主題網站移轉校園文化地景知識；（三）學生透過主題網站認識校園文化地景，有助於產生認同感。

依據研究發現，本研究的結論有三項，分別是（一）學生可善用資訊科技學習知識；（二）主題網站的知識移轉策略具有效能；（三）學生運用主題網站的知識移轉更認同學校。本研究供了學生知識移轉方式的經驗；此外，校園文化地景主題網站知識的知識移轉設計，獲得學生喜愛；學生亦透過主題網站學得綜合能力。依據上述結論，可以作為日後國小應用主題網站進行知識移轉的參考。

關鍵詞：地景、校園文化地景、知識移轉

1. 緒論

在知識經濟時代，資訊科技扮演重要的角色，每個組織也相當重視資訊科技環境的建置[8,10]。資訊科技有助於知識的獲得與分享，也可以提升知識移轉的效能。

目前在台灣，國小非常重視實施資訊教育，融入鄉土教學之中。尤其，使用電腦技能與熟悉軟體應用更是列為重點。相關的研究[9,11]認為數位學習方式與主題網站學習顯得日益重要。

電腦在成功的教學扮演重要的角色，研究顯示，當網路資訊資源與連網設施增加時，學生會常使用網際網路[15,19]。

Joshi, Sarker 和 Sarker（2004）指出知識轉移能透過社會化、教育和學習的過程展開。知識可能被有目的轉移，或者它可能作為一種其他活動的結果發生[14]。知識移轉是知識接受者經由與知識提供者間的互動，透過各種方式或資訊設備來達到移轉知識的目的。

因此，本研究欲在國小教育現場，規劃校園文化地景知識，作為知識移轉內容。在本研究中，以 12 位國小六年級學生為研究個案，透過 6 週的主題網站知識設計，進行「校園文化地景」知識的移轉。在應用電腦部分，則包括使用電腦資訊設備、網際網路、製作網頁相關軟體、學校主題網站等。

綜上所述，本研究目的是探討國小學生應用電腦進行校園文化地景知識移轉的過程，以及探討應用主題網站進行知識移轉的覺知。

2.文獻探討

2.1 地景與校園文化地景

王鑫（1997）認為地景（landscape）是人對環境特徵所感受的景像，它屬於高價值的非再生性資源，對人為管理所產生的變化也缺少抗拒性，一旦遭到了破壞，就很難再復原[1]。再者，何立德（2009）認為地景是指地表上一切視覺可見的有形景物，也可稱為景觀。一般而言，有些地景是經由自然作用產生，有些則為人類利用資源造成的結果，前者可稱為「自然地景」，後者則稱為「文化地景」。自然地景的概念多著重於對自然物質與作用的認識與探討；文化地景方面，則多研究形塑地景背後的社會、文化、經濟、政治等驅動力[2]。

關於文化地景一詞，Sauer(1925)提出，認為是某一文化群體利用自然地景的產物。文化是驅動力，自然區是媒介，而文化地景則是結果[18]。全國科學技術名詞審定委員會（2007）指出文化地景（cultural landscape）是在特定文化背景下和具體的自然環境基礎上，在人的作用下形成的地表文化型態的地理複合體[3]。此外，劉敏和方如康（2009）認為文化地景，是自然地景的對稱。是地表各種文化現象或人文現象的複合體，是文化賦予一個地區的特徵。組成文化地景的要素有農田、城鎮、道路、建築、古文化遺址等可以透過地景照片或實地觀察直接看到的事物；也有不可見，但置身其中卻能感覺到的非物質內容，如語言、宗教、生活習俗等。還有一種不可見，但可感到的氣氛，如人們的文化氣質、精神面貌、生活習慣等[5]。

地景透過了人與土地的互動方式，因而形成了文化地景。李宜蓁（2013）認為校園地景是指學校校園中一切視覺可見的有形景物，亦即校園的自然環境；而所謂校園文化地景，則係指學校校園環境原屬於自然環境，經由課程規劃與設計，與學生透過了閱讀、學校本位課程與校園環境探索之互動學習，因而產出學校環境與學生學習生活之學習文化模式，並賦意學校環境 [4]。

2.2 知識與知識移轉

對於知識的特性，Polanyi（1966）將知識的類型分為隱性的或非正式的知識以及顯性的或正式的知識[17]；此外，Nonaka和Takeuchi（1995）將知識分為外顯知識、與內隱知識二種，並進一步詮釋外顯知識（explicit knowledge）是一種客觀、形上，可以用語言、文字來記錄、描述與傳遞，及數字表達的知識；內隱知識（tacit knowledge）則是一種主觀、實質，無法用文字或句子表達的知識，亦是個人經由經驗，所感受、累積的經驗知識，內隱知識深深地根源於個體的行動和經驗，而且包括他們的想法、價值、主觀洞察、直覺以及情感[16]。

Buckley和Carter（2000）認為知識移轉有三個內涵，包含資訊移轉、思考（反應、判斷、評價），以及經過試驗瞭解的經驗[7]。此外，在知識經濟時代，資訊科技扮演重要的角色，每個組織也相當重視資訊科技環境的建置[8,10]。資訊科技有助於知識的取得與分享，也可以提升組織知識的移轉效能。關於影響知識移轉效能的相關研究，Johannessen、Olaisen 和 Olsen （2001），認為組織成員的信任關係是重要的[13]。至於知識移轉，Polanyi（1966）認為透過見習與體驗學習隱性知識[17]；其相關研究[13, 20]也認為隱性知識屬於練習型的知識，必須在執行工作中習得。組織中的知識移轉，被認為是組織創新及維持競爭優勢的方法。

綜上所述，知識移轉重視移轉知識的應用，透過實際練習及體驗，達成特定任務或完成工作，並且能獲致滿意的覺知。

在本研究中，顯性的知識就是學生需要學習的校園文化地景知識及應用電腦技術性的知識，諸如使用網頁能力、資料蒐集能力、物件取材能力、網際網路基本能力等。以上這些都是有關實際運用方面，讓學生可以了解並且能實際運用的一些工具，以及閱覽主題網站的必要觀念。關於隱性知識，則是透過學習的過程中，由潛移默化中生成的一些非自覺性的知識，如合作學習、認同校園、統整能力、自主學習等。

2.3 校園文化地景主題網站的知識

本校師生形塑校園文化地景，運用校園豐富生態環境，累積學校文化資產。Stephenson（2008）認為地景的意義是建立豐富的互動，地景的重要性則是經驗、知識和記憶的互動結合[12]；蘇美如（2008）文化地景的內涵包括人與土地的互動、明顯的場域、持續性的活動、歷史性及延續性等四項特性[6]。李宜蓁（2013）研究顯示學生透過學校本位閱讀課程，學子有了基本環境--自然資源認知之後，再搭配自然植物圖鑑，藉由學校植物地圖的路徑導引，學子進行校園植物基礎調查；透過了實作與閱讀理解認知互動，建置了學子環境--自然資源認知，並理解校園豐富生態環境、大自然時序、生物互動等關係。並在探索的過程中，學子發現了原有之學校植物地圖以外之自然資源，透過知識管理系統，進行知識擴散與分享，除了重整建置校園生態環境資料庫，也累積成為學校的文化資產[4]。

透過學校植物地圖之路徑導引，學生發現學校植物地圖以外的植物，豐富了校園生態環境資料庫，進而形塑校園綠活之文化地景。如蘇美如（2008）研究顯示文化地景具有變動的特質，而人為作用力是形塑文化地景的主因。校園四大區域，包括前庭（A 區）、中央花圃（B 區）、廚房（C 區）、後操場（D 區），繪製圖示於主題網站，並且鍵入基礎知識。

在本研究中，則透過師生共塑的校園文化地景主題網站的知識移轉（校園文化地景主題網站內容舉隅，如附錄 1 及 2 所示），讓學生能從各項教學活動中，積極參與及觀察記錄，能轉化學生為主動式學習者，也更認同校園。

3. 研究設計與實施

3.1 研究對象

本研究旨在探討國小學生應用電腦進行知識移轉的方式，並評估知識移轉的效能。在本研究中，以 12 位國小小六年級學生為研究個案，透過 6 週的主題網站知識設計，進行「校園文化地景」知識的移轉。

從文獻探討中，團隊學習是獲得有效能知識移轉的策略。此外，團隊學習重要的因素，包括團隊的良好互動、成員彼此信任的感覺，以及資訊科技的輔助。許多學者認為透過策略聯盟的組織學習，可以從同伴獲得新的能力[19]。因此，在本研究中，12 位國小六年級學生是同班同學，彼此熟悉，有助於團隊的知識分享與移轉。

3.2 研究方法

本研究採取質性研究法，透過文件蒐集與訪談法蒐集資料，將獲得資料歸納及分析。在研究進行之前，學生已具備電腦基本操作、簡易文書處理、使用網際網路的基礎能力。

3.3 研究流程

本研究的流程，如圖 1 所示。

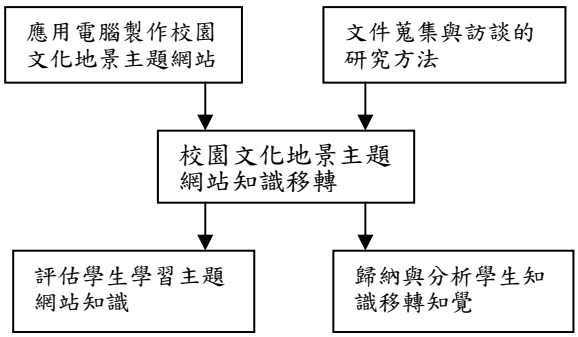


圖 1　研究流程圖

在圖 1 中，學生移轉校園文化地景主題網站知識，學生經過 6 週進行主題網站知識的移轉，研究者透過資料的蒐集與分析，歸納出學生知識移轉方式，學生的知識移轉覺知。

3.4 製作主題網站教學課程設計

本研究校園文化地景主題網站知識移轉的內容設計，如表 1 所示：

表 1 校園文化地景主題網站知識移轉的內容

週次	主題網站移轉知識內容
一	網站架構及其組成介紹、網頁應用教學
二	主題網站圖檔及鍵入文獻資料
三	學習校園文化地景知識植物篇
四	學習校園文化地景知識鳥類篇
五	學習校園文化地景知識建物篇
六	學習校園文化地景知識人文篇

資料來源：由研究者自編

由表 1 可知，主題網站知識設計共分為 6 週，每週各有知識移轉的內容。

4. 研究發現與討論

本研究探討 12 位國小學生應用電腦，以 6 週進行校園文化地景主題網頁的知識移轉。研究者透過蒐集相關文件及訪談學生，將所得資料的蒐集與分析，歸納學生知識移轉方式，學生知識移轉覺知。訪談的資料，12 位學生則分別以 S1、S2、S3、S4、S5 表示，S1-4-1 表示學生 S1 的觀點，歸納在 4-1 的結果中，以下由此類推。茲將研究結果分述如下。

4.1 學生應用資訊科技(電腦)學習知識

在本研究所設計的主題網站知識，必須使用電腦（能連結網際網路）設備。教導學生使用網際網路基本技能應用是必要的，老師採用講解方式傳達知識，並指導學生操作電腦。

在創作綠地圖當中很辛苦，又怕哪個小細節出錯，所以我們都非常小心。繪畫綠活圖當中我們都非常小心字體大小和顏色等。完成綠地圖的那個時刻，我們大家都高高興興的喝采，做了那麼久的綠地圖終於完成了（S1-4-1-1）。

在活動前我們做了許多的準備，包括繪圖、準備資料，還有要背植物的特性、文化景觀的由來。（S10-4-1-2）。

在本研究中，學生實地踏查，親自在自己校園蒐集資料，以學習主題網站。Polanyi（1966）透過見習與體驗，去學習隱性知識[17]。相關研究[如13,20]也認為隱性知識屬於練習型的知識，在完成工作中習得。

根據觀察學生實際操作，移轉主題網站的知識。此外，根據學生表達的學習感受，顯示透過本次主題網站知識，學到相關的知識，操作技能也增強許多。因此，學生應用資訊科技(電腦)學習知識。

4.2 學生透過主題網站移轉校園文化地景知識

個案學生在校園文化地景主題網站中，除了知識的移轉外，對於學生的學習態度，亦相當重視。尤其，學生在知識移轉的過程中，具有學習的興趣。以下的訪問內容，可以得知學生學習的歷程及學生的態度覺知。

以前我根本不知道這些植物的位置和特徵，現在參加了這個活動，我終於知道這些植物的位置和特徵了（S1-4-2-1）。

對於認識校園有很大的幫助，以及對植物和地點的資料更深的去研究，讓我們知道那棵樹，或那座建築是有甚麼樣的意義和作用（S6-4-2-2）。

認識學校的植物，增加我們的知識。讓我們認識學校大大小小的植物，如大花紫葳、阿勃勒、大王椰子等；還有也能加深植物和地點的資料，讓學生們的知識（S7-4-2-3）。

學生在學校文化地景主題網站，逐步移轉學校豐富的植物及地景知識，對學校也更加了解，如同 Buckley 和 Carter（2000）認為知識移轉有三個內涵，包含資訊移轉、思考（反應、判斷、評價），以及經過試驗瞭解的經驗[7]。

我們大家都更深入的了解學校的景觀、人、事、物（S8-4-2-4）。

了解環境與植物的特性或者是作用。也能讓他們對學校更深層的了解更具有意義與特色，並加以解說和認知，這也是對我有很好的經驗（S9-4-2-5）。

本次應用電腦主題網頁的學生相處融洽，學生間互動良好，從訪談中，學生學習校園文化地景知識。

4.3 學生透過主題網站認識校園文化地景，有助於產生認同感

在研究過程中，學生都相當投入，學生也會自動地利用許多課餘時間在使用主題網站學習。以下是訪談學生的內容：

參加這個活動讓我瞭解到我以前不懂的植物的特性，也讓我瞭解學校有許多我不懂的植物，更讓我瞭解到同心協力的重要（S2-4-3-1）。

大花紫葳因為他跟我們學校的運動服顏色一樣，看起來很醒目，感覺就像會和我們運動服互相

對應（S7-4-3-2）。

我對這個校園有濃厚的感情，在這個校園我看到了老師們的用心、學生們的努力，這些都是學校的驕傲（S8-4-3-3）。

Stephenson（2008）認為地景的意義是建立豐富的互動，地景的重要性則是經驗、知識和記憶的互動結合[12]。透過主題網站知識移轉，學生與校園文化地景有了互動。

我現在才發現原來要了解學校的所有的一切是那麼困難的一件事啊！如果我有可以為學校服務的機會的話，我一定會全力以赴的把事情儘量做到最完美（S10-4-3-4）。

我覺得學校所有的人文歷史，包括藝術、地形、動植物、還有在校所有的每位老師以及學生，都讓我印象深刻，牢牢的記在心裡（S11-4-3-5）。

蘇美如（2008）文化地景的內涵包括人與土地的互動、明顯的場域、持續性的活動、歷史性及延續性等四項特性[6]。

因此，應用移轉的知識進行實際操作練習，可以瞭解學生移轉的學習覺知，也可以藉此檢視移轉的效能，本研究顯示有正向的移轉效能，學生對校園也更具有認同感。

5. 研究結論

本研究透過文件蒐集及訪談，將獲得資料歸納及分析，依據研究發現，本研究的結論有三項，分別是（一）學生可善用資訊科技學習知識；（二）主題網站的知識移轉策略具有效能；（三）學生運用主題網站的知識移轉更認同學校。

本研究供了學生知識移轉方式的經驗；此外，校園文化地景主題網站知識的知識移轉設計，獲得學生喜愛；學生亦透過主題網站學得綜合能力。依據上述結論，可以作為日後國小應用主題網站進行知識移轉的參考。

參考文獻

[1] 王鑫。地景保育。台北：明文書局，1997。

[2] 何立德。地景多樣性與地景保育。科學發展，439 期，2009，22-29 頁。

[3] 全國科學技術名詞審定委員會。地理學名詞。全國科學技術名詞審定委員會審定--二版。北京：科學出版社，2007。

[4] 李宜蓁。國小學生參與校園文化地景之行動研究：以閱讀校園地景課程為例。載於 2013 年南臺灣教育學術研討會，2013，1-23 頁。

[5] 劉敏、方如康主編。現代地理科學詞典。北京：科學出版社，2009。

[6] 蘇美如，蘭陽平原散村文化地景之形塑與特質--以礁溪玉田地區「竹圍」為例。中國文化大學地學研究所博士論文，2008，未出版。

[7] Buckley, P. J., & Carter, M. J., Knowledge management in global technology markets-applying theory to practice. Long Range Planning, 33(1), 55-71, 2000.

[8] Chien Chou & Chin-Chung Tsai , “Developing web-based curricula: issues and challenges”, Journal of Curriculum Studies, 34, 6, 623-636, 2002.

[9] Cornell, R. , “Web-based courseware tools: where is the pedagogy”? Educational Technology, 39 (3), 60-64, 1999.

[10] Hamel G., Competition for competence and inter-partner learning within international strategic alliances. Strategic Management Journal, 12(Specil Issue), 83-103, 1991.

[11] Harrison, N. & Bergen, C., “Some design strategies for developing an online course”, Educational Technology, 40 (1), 57-60, 2000.

[12] Janet Stephenson, The Cultural Values Model: An integrated approach to values in landscapes. Landscape and Urban Planning, 84, 127–139, 2008.

[13] Jon-Arild Johannessen, Johan Olaisen, & Bjorn Olsen, ”Mismanagement of tacit knowledge- the importance of tacit knowledge the danger of information technology and what to do about it”, International Journal of Information Management, 21(1), 3- 20, 2001.

[14] Joshi, K. D., & Sarker, Saonee, & Sarker, Superateek, “Knowledge Transfer Among Face-to-Face Information Systems Development Team Members: Examining the Role of Knowledge, Source, and Relational Context”, Proceedings of the 37th Hawaii International Conference on System Sciences, 2004.

[15] Miriam J. M., Andrew J. F., & Lara Zwarun, “College student Web use, perceptions of information credibility, and verification behavior”, Computers & Education, 41, 271-290, 2003.

[16] Nonaka, I., & Takeuchi, H., The knowledge-creating company: How Japanese companies create the dynamics of innovation. New York: Oxford University Press, 1995.

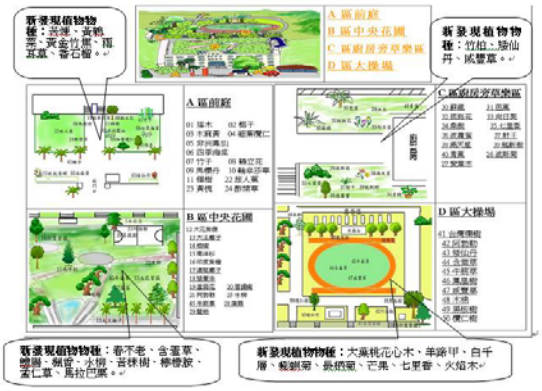
[17] Polanyi, M., The Tacit Dimensio. Doubleday & Company, Garden City, New York, 1966.

[18] Sauer, C. O., "The Morphology of Landscape". University of California, Publications in Geography, 2(2): 19-53, 1925.

[19] Shackleford, J., Thompson, D. S., & James, M. B., “Teaching strategy and assignment design: assessing thequality and validity of information via the Web”, Social Science Computer Review, 17(2), 196–208, 1999.

[20] Sveiby, K. E., “The new organizational wealth: Managing & measuring knowledge-based assets”, San Francisco:Berrett-Koehler Publisher, 1997.

附錄 1 校園文化地景主題網站舉隅之一



附錄 2 校園文化地景主題網站舉隅之二

學生發現之植物種類、植物特性，以及書寫的校園地景故事

	植物名稱	植物特性	由學生書寫的校園地景故事
A 區	黃鵪菜	根生葉簇性，倒披針形，葉下半部羽狀深裂，柄、莖生葉較少。	它生長在大門口的花圃中，它不容易被發現，它有開黃花，靠近看黃黃的花朵，那就是它了。
A 區	兩耳草	花為白色偏淡綠色，有的為穗狀花序，果實為頴果而兩穗上有綠狀毛。	因為長相只長莖，而且長得很像耳朵，所以名為兩耳草。
A 區	番石榴	成熟的蕃石榴為淺綠色，果皮脆薄，食用時一般不用削皮，果肉厚輕甜脆爽。	番石榴因外形像石榴(即安石榴)是屬安石榴科，卻因產自外地，所以叫番石榴。
B 區	春不老	全年枝葉均綠密翠綠，開花及果實累累，具高度觀賞價值，也可以吸引野生動物前來採蜜覓食。	在校園一角中，一年四季總是翠綠迎人。
B 區	含羞草	每個羽片有小葉 14-48 片，邊緣及葉脈有刺毛，碰觸即閉合下垂。	含羞草很怕別人傷害它，所以別人摸它的時候，它會閉合起來，我覺得含羞草很聰明，它會防備敵人到來。
B 區	鱧腸	鱧腸是頂頂有名的救荒野菜，別名是「旱蓮草」、「墨菜」、「鴨菜」，在夏季時是盛花期。	它長在校園的大草皮上，每天雖然都被我們踩在腳底下，但它還是很努力的成長，陪我們度過許多歲月。 要認得鱧腸最容易的方法，便是折一段莖葉，其斷面處會很快變黑，因此又稱為墨菜。
B 區	楓香	落葉大喬木、互生，葉基圓形或心形，通常掌狀三裂葉，長寬各約 4-8 公分，果實為圓刺刺的小球。	它在幼稚園的前面，只要看到星形的形狀，那就是它了。因為它的葉子長得很像楓樹，所以叫楓香。
B 區	水柳	樹皮縱向溝裂，幼枝略有短柔毛。	溼地的大池週邊有大量的水柳，水柳雖不若垂柳之葉柔軟飄逸，然其滿樹新綠及雪白柳絮，亦別具風情。
B 區	苦楝樹	落葉喬木，樹高 10-20 公尺，傘形樹冠，樹皮灰褐至灰黑色，有明顯的縱裂紋。	因為苦楝樹靠近種子的樹根，很像鍊子一樣一節一節的所以要叫苦楝樹。
B 區	檸檬桉	果實有很多功用，如可當醬料和泡茶用。	它的葉子很香，細細搓揉有檸檬香味哦，它就長在我們最愛踢球的大草皮旁邊。
B 區	盃仁草	莖直立，基部呈毯狀，具分枝，節處生根。	它原產於東亞熱帶地區或熱帶美洲，由於適應力極強，引入台灣後便迅速擴展，它所到之處無不構成顯著的群聚現象。目前在校園中也是呈現群聚面貌。
C 區	矮仙丹	常綠小灌木，高 1-3 公尺，枝條由基幹附近密生。用途可做為綠籬、庭園賞花、誘蝶植物。	它的位置在廚房前方，每次抬餐筍回廚房時，會看到蝴蝶停在上頭，老師曾說過因為它的蜜源很豐富，

全人雲端網課程活動 App 對品格與關懷能力影響之研究

廖慶榮[a] 李清義[b] 潘正德[b] 陳鶴元[c] 李明訓[d] 劉致緯[d]
[a]中原大學資訊管理學系 [b]中原大學通識教育中心 [c]東海大學師資培育中心
[d]中原大學資訊管理研究所
{cjliao, cylee, jender}@cycu.edu.tw; {huc140, johnsonlee.vqti, taiwanliu}@gmail.com

摘要

本研究以數位學習（e-Learning）的方式，透過全人發展網設計能夠以課餘時間參與的網路活動 App，藉此希望能提升職場所需的核心能力。數位學習改變了傳統教與學的方式，但是一般的數位學習系統較常針對單一主題進行學習，對於跨學科、跨領域整合的學習機會也比較少。因此，本研究透過全人發展網，設計一個和品格與關懷有關的 App「品品禮 2.0」，以活潑有趣的方式來嘗試提升學生的品格與關懷能力。實驗設計以單組前後測的方式進行，共計 103 位同學完成八週的活動。實驗結果發現，使用課程活動 App 的同學在「品格認同」、「關懷與服務」、「App 使用者品格與關懷活動延伸」等三個構面並未達顯著影響；而在「誠實與負責」、「尊重與態度」，以及「品格認知」等三個構面則達到顯著影響。

關鍵詞：雲端運算、全人發展網、手機應用程式、品格、關懷、核心能力。

Abstract

In this study, the e-HO activities Apps are designed for students' participation during their spare time and wish to improve the core capabilities which are necessary at workplace by means of e-Learning. e-Learning have been changed the traditional way of teaching and learning, but the general learning management systems are usually designed for some specific disciplines with little opportunities for more integrative and cross-disciplinary learning exposures. Therefore, this study intends to design an App “PinPinLi 2.0” related to character and caring through the holistic learning environment "e-HO", which tries to improve students' character and caring capacities in a lively and interesting way. Experimental design participants surveying a one-group pretest-posttest design, there are 103 students finish all of the activities after eight weeks. The results show that the participants don’t have significant influence in “Character cognition”, “Care and services”, and “Character and care activities extension of App users” dimensions; but in the “Honesty and responsibility”, “Respect and attitude”, and “Character recognition” dimensions achieve significant influence.

Keywords: Cloud Computing, e-HO, App, Character, Caring, Core Capability.

1. 前言

現代的大學生除了自我的專業領域學有專精外，也需要培養資訊公民素養以及建立職場所需的核心能力，如此才能有助於未來的工作。各家人力銀行對企業徵才所注重的職能需求進行調查時發現，現代的企業選才時，特別重視應徵者的品格、團隊精神、主動積極、溝通協調能力、工作熱誠、負責任、工作具效率等特質，專業能力反而是可以學習的。

近十幾年來，網際網路已經成為這新時代教學與學習的重要工具之一 [10]，在新興的 Web2.0 時代[28]，數位學習也從早期的 1.0 時代演進現在的 e-Learning 2.0。然而傳統的師生教學模式及學習內容也隨著以往的課堂講授漸漸發展成光碟多媒體學習、遠距教學（Distance Instruction）、數位學習，以及行動學習（Mobile Learning），以及無所不在的學習（Ubiquitous Learning）等，這些學習模式的演進均是利用資訊平台及網路設備不斷進步，讓學習者可以藉由相同的學習目標進行學習，但目前普遍學習模式都是針對單一主題進行學習，無法跨學科、跨領域的整合。傳統的網路學習系統由於結構性較強，互動多以 BBS 的方式進行，容易使學生在學習上感到乏味，導致學習意願降低，因而無法達到所期待的學習效果。但是全人發展網（e-HO）實現一個全人學習環境適合大規模的「數位居民」使用，使他們可以常常徘徊在此平台來進行學習，此環境具互動性，且可以快速的讓同學在學習中接觸其他領域，達到多元化的學習 [17]。由於 e-HO 的用量越來越高，因此我們將 e-HO 建置到雲端運算的環境成為全人雲端網。

使用智慧型手機的人越來越多，Nielsen 在 2012 年的一份調查報告指出，今年第一季使用智慧型手機的人佔了 49%，但到了第三季，已成長到了 56% [24]。另一項根據資策會 FIND 在 2012 年 4 月針對智慧型手機與平板電腦的使用調查報告，顯示在使用智慧型手機的使用者當中，有將近八成的低頭族用戶（76%）曾經在一個月內到應用軟體商店下載 App，App 應用程式下載者則以相對較年輕、收入較低、且以學生族群為主 [5]。為了讓同學提升就業時的核心能力，再加上希望以他們時下所喜歡的方式來進行學習，本研究透過全人發展網的特性，設計 e-HO 活動 App 來吸引同學使用，提升品格和

關懷能力，希望在未來就業時有好發展，也藉此探討不同院別、年級、性別，以及是否修習相關課程等背景變項的學生，透過 e-HO 活動 App 融入學習後，對於學生的品格與關懷能力有何影響。

2. 文獻探討

透過有趣的 App，讓同學在學習中無形提升自我的核心能力，研究相關的議題與技術計有雲端運算、全人發展網、核心能力、品格能力，以及關懷能力等，以下將分述之。

2.1 雲端運算

透過 Google Trends 的關鍵字搜尋次數統計功能，可知雲端運算（Cloud Computing）這個名詞是自 2007 年第 3 季開始興起。雲端運算這個名詞是 Google 的執行長 Eric Schmidt 於 2006 年提出，其重要的概念是「透過網際網路運算」[6]，之後就出現各式各樣不同的定義。Foster 等人指出雲端運算是一個大規模的分散式運算模式，它具有經濟規模，並透過網際網路提供外部客戶資源的需求，在一個抽象、虛擬化、動態可擴展的資源池，其可管理運算能力、儲存、平台以及服務 [12]。Weiss 說明雲端運算將虛擬化（virtualization）技術運用於運算及儲存上，建立下一代數據中心，以提供可靠的服務，使用者可依需求在世界的任何地方進入應用程式[32]。Hayes 指出雲端運算是一個提供基礎設施的新模式，這個模式將基礎設施移轉至網際網路上，以降低管理硬體和軟體資源的成本 [14]。Sun 於 2009 年提出的白皮書中將雲端運算架構部署模式分為公用雲（Public Cloud）、私有雲（Private Cloud）及混合雲（Hybrid Cloud）[31]。依據服務的層次可分為軟體即服務（Software as a Service, SaaS）、平台即服務（Platform as a Service, PaaS）、基礎設施即服務（Infrastructure as a Service, IaaS）三個部份（Jones, 2008），在過去的經驗裡，我們曾經成功以 Eucalyptus [26][27]和 OpenNebula 建置私有雲端（private cloud）運算環境 [19][20]，本研究也採用國網中心的 Formosa cloud (http://formosa5.nchc.org.tw) 來建置 e-HO cloud。

2.2 全人發展網

近五年中原大學發展全人教育，導入數位化，成立全人發展網（e-HO, http://ge.cycu.edu.tw），e-HO 是以跨領域的學習環境，以使用者生成內容（UGC）的概念助於學習者激勵學習和互動，提供一個自主學習環境。當中學校以成果導向概念發展學生能力基本地圖（C-map），透過能力指標系統衡量學生基本能力，制定八大能力指標，有四項指標為品格教育的能力，透過品格教育數位化，以全方位整合跨領域學習，藉此學生能學習不同類型的教學內容和課餘學習，達到全方位教育的目的。

2.3 核心能力

Spady 認為學生學習的成效重點不在於學業分數，而強調學生學習後的學習成果，以學習成效和明確制定畢業生能力，學生畢業後能達成任務性質所該具備的能力 [30]。King & Evans 指出，成果導向教育是一種能促使學生在傳統教學內容上學習，增長能力和行為發展的課程方式，其基本教育的理念是假設所有學生均是卓越的，能互相學習合作，學校能幫助學生找到成功的方式 [16]。Brandt 認為成果導向教育實施應掌握明確的學習成果、擴展學習機會、高期待，以及回歸基本課程設計等四項原則 [9]。成果導向是為學生學習後的成果，以往傳統的衡量學生能力方式是以學生學業分數作為能力之參考，而成果導向著重的是學習後的學習成效和明確制定畢業生之能力，學生畢業後能達成任務性質所該具備能力，依學習成效之成果決定所具備的制定能力。王玉麟等人將核心能力解釋為依學校規劃發展方向與產業需求訓練個體在各領域中需要的關鍵能力 [2]。核心能力一詞國內外有許多學者對其論述，個體若具備核心能力，可以比其他競爭者具較多的技能 [18]，這種獨特的特徵對於潛在事業具極大的幫助。Long & Mary 則認為核心能力是一種技巧、知識、技術兼備的能力，具有特殊的特質優勢 [23]。核心能力通常需要在就業前養成 [13]，王保進將核心能力視為乃學生畢業時所具備的專業知識、技能及態度 [1]；李坤崇也說明核心能力是就業前應具備的中心、主要、重要且具競爭力的才能，是學生畢業時所具備的專業知識、技能及態度 [3]。綜上所述，在高等教育中，培養「一般能力」與「專業能力」使個人能力增強，不論是個人發展或組織合作關係皆具重要的影響力。因此本研究引導學生使用 App 參與 e-HO 活動，希望能提升品格指標的核心能力。

2.4 品格能力

近年來政府積極推導品格教育以及社會關懷服務，透過學習與活動發展良好的道德以及培養社會和生命關懷的價值觀。Lickona 認為品格教育追求的是助於學生表現出有禮的行為 [21]。品格教育是指教導學生從事善良的活動，透過教育的教導與傳授品格的理念，促使學生發展品格論理與關懷情懷的一個歷程，著重於品格素質與內涵。Lickona 認為品格教育是以善良、道德和行善協助學生內化良好行為之認知和習慣，就由教育的過程促進個人發展倫理責任與人文關懷教育活動 [22]。品格是個人習慣的總和，因此品格教育是培養個人成長中的習慣歷程。而品格教育目的是教導學生建立自我的「核心價值」，核心價值界定了個人與民主社會中應盡的義務與責任，促進個人與群體向「善」發展，

藉以增進人類福祉。Berkowitz 等人研究讓學生實踐認識善良、喜愛善良，以及做出善良 [7]。Otten 認為品格教育含有多元的意義，是個人成長中，透過教育與學習改變的歷程，主要含有發展道德認知、情緒學習、道德教育、生活技能、健康教育，以及解決衝突等方面 [29]。綜上所述，品格教育追求的是幫助學生表現仁慈、有禮與持續的自律行為，學習善良的習慣，以多元道德認知、情緒學習與道德教育促使個人學習成長中的一個歷程。品格教育目的是教導與告訴學生如何從事善良，是透過師與生之間的互動傳達，而本研究所指的品格教育是透過網路活動和 App 進行互動，透過品格相關的議題引導學生對品格認知看法的評論與討論，激發出不同的認知與認同看法，促進品格之能力。因此本研究設計品格與關懷能力量表來觀察學生參與 e-HO 活動 App 後的品格能力影響。那麼品格能力如何衡量呢？衡量品格的能力，可以利用有效的量表來衡量品格教育的相關活動。Kinnamon 認為品格的核心包含誠實、尊重、責任、信賴、素養和關懷的能力 [15]。Barlow 等人以領導者所具備的品格特質研究中，衡量完整性、誠實、忠誠、無私、同情、能力、尊重、公平、決定性、負責和自律、決斷，以及讚賞和合作等 12 個構面 [8]。潘正德與李清義在中原大學品格教育的實踐與反思研究中，衡量品格的態度、認知、認同，以及培養等四個構面。本研究採用「誠實與負責」、「尊重與態度」，以及「認知與認同」為主要衡量指標 [4]。

2.5 關懷能力

Davies 認為關懷是一種生理、心理及情緒上的型態，必須委託他人在身體及成長的方面撫養或照料 [11]。關懷與參與從事活動可透過服務學習課程幫助於他人，除了志工服務學習之外，透過日常生活中對周遭事物的關懷照護和朋友間的關懷，可促使社會發展與增進福祉。關懷除了自己以外，對於周遭事物的關心也是一種關懷，周遭事物包含親人、朋友、陌生人，以及動植物等，關懷可使對方感受到溫暖與關心。Noddings 提出六項關懷主題，分別是關懷自己、關懷親密與周遭熟識之人、關懷不熟識之人、關懷動植物及自然環境、關懷人為世界，以及關懷理念 [25]。使得對自我的理解，了解被關懷者的感受，發展出關懷的關係。也能使不相識的人能感受到關懷，讓自己感同身受。除此之外，對於世界上的生物與環境抱持關懷的角度，也能觀察人類文明的價值，培養以人為出發點的關懷，最後使人體會人生的道理。所以關懷可以是一種生理、心理及情緒上的型態，以愛為主傳遞，因此本研究設計的活動以關懷議題傳達學生產生同理心與認同，促進對事物的關心與朋友間相互的關懷，達到和諧幸福的感受。

3. 研究方法

本研究透過前、後測量表與訪談分析，來了解學生使用 e-HO 活動 App 後，是否可以提升品格和關懷能力。

3.1 全人雲端網（e-HO Cloud）

為了讓全人發展網運作順暢以及克服負載問題，首先將全人發展網建置在雲端運算環境上，行程新的全人雲端網。採用 IaaS 的架構方式，之前我們曾經成功以 Eucalyptus 和 OpenNebula 建置私有雲端運算環境，這一次則採用國網中心的 Formosa Cloud 來建置。

3.2 課程活動 App

在學習活動設計上，我們發展出品格與關懷的學習活動共計八周，每周提供一個主題，透過 App 和全人雲端網回應發表，讓同學可以親身經歷，了解品格與關懷的意義，活動設計舉隅可以如表 **1** 所示，內容可以是文字、影片、動畫、漫畫、擴增實境、遊戲等不同多媒體型式的呈現，兩個活動 App 畫面擷取如圖 **1** 所示。

表 1 品格與關懷能力活動 App 內容舉隅

主題	活動內容	預期目標
品格與生活（自拍影片）	在某個聚餐的夜晚，眾人齊聚一堂，當一陣寒暄過後，點菜上桌後，大家的動作似乎是先拍照標記打卡，後面就開始埋首在低頭族的行列中，但也忽略的以往與人對談時的尊重，整個聚餐卻是一半時間以上在當低頭族。	了解品格對於日常生活的影響
典範人物不凡的慷慨（影片）	典範人物陳樹菊的故事，平民英雄陳樹菊被美國時代雜誌列為百大影響人物，她默默行善數十年。當年她母親難產，醫院說如果沒繳保證金就不開刀，等到父親籌到錢時，媽媽已經斷氣了，死前緊握平民英雄陳樹菊的手，因此陳樹菊發誓長大有能力一定要幫助別人。請問你從陳樹菊身上有學習或感受到甚麼？	讓學生從典範人物身上，了解品格的意義。



圖 1 活動 App 畫面擷取

3.3 實驗設計

在實驗設計方面，以「品格與關懷能力量表」來衡量學生使用 e-HO 活動 App 後，是否對品格和關懷能力有幫助；並且探討不同年級和性別等背景變項的學生，透過 e-HO 活動 App 融入學習後，對於學生的品格和關懷能力有何影響？根據研究問題，提出四個假說：

H_1：品格活動 App 可以提升學生的品格能力。

H_2：關懷活動 App 可以提升學生的關懷能力。

H_3：學生的年級和性別等不同背景變項，對於品格能力有影響。

H_4：學生的年級和性別等不同背景變項，對於關懷能力有影響。

經過課程活動設計後，採取實驗前與實驗後的方式探討課程活動與品格與關懷能力間的影響，以中原大學修習通識課程學生為實驗對象。自變項為教學活動與學生的性別、年級等背景變項，依變項為實驗後量測所得之分數。實驗前，學生先填寫「品格與關懷能力量表」，藉此得知學習者進行活動前的量表分數。經過八周使用智慧型手機 App 的活動實施後，再讓學生接受一次「品格與關懷能力量表」衡量，得到實驗後的量表分數。本研究的實驗設計分成實驗前測、實驗處理，以及實驗後測三個部分，採用前實驗設計（pre experimental design）中的「單組前後測設計（one-group pretest-posttest design）」以單一組的方式進行實驗。在研究工具方面，使用量表、學生回饋問卷，以及質性訪談。其中「品格和關懷能力量表」係參考文獻自行發展，品格能力衡量「誠實與負責」、「尊重與態度」、「品格認知」，以及「品格認同」四個構面；而關懷能力主要是衡量「關懷與服務」構面。在質性的資料蒐集上，採事後半結構式訪談法和學習者進行面對面訪談，由前、後測中各個不同分數組別的同學隨機抽取。

資料分析與詮釋則對量化資料與質性資料進行分析。實驗對象為中原大學學生，年級、性別皆不同，提供實驗的參與者使用 e-HO 活動 App，藉此觀察學生在使用此 App 後對品格與關懷能力的影響。

實驗的前測與後測成績以成對樣本 t 檢定統計分析，來了解實驗組經過八周的活動之後，學習成效是否有達到顯著差異；接著以多變量分析探討年級和性別對於學生品格與關懷能力是否有影響。在差異性分析部分，進行敘述性統計、不同性別對各個構面的差異分析（使用 ANOVA 分析男女間能力的差異）、不同年級對各個構面的差異分析（達顯著的因子再進行 Scheffe 事後檢定），以及透過手機發表次數多寡對各個構面的差異分析。這些分析均包含前-後測資料，前-後測資料的敘述性統計分析，主要計算量表填寫後各個構面的平均值（Mean）和標準差（SD），後測資料的敘述性統計表再加上和前測資料的差。

4. 實驗結果與討論

4.1 因素分析

本研究在 254 份有效樣本中，男性為 83 位，佔 33%，女性為 171 位，佔 67%，以此進行因素分析，去除獨立和因素負荷量小於 0.5 的問項後，共計 29 個問項，如表 **1** 所示。其中 Cronbach's α 值為 0.85，在 0.7 以上表示問卷具有好的可靠性，而問卷效度採用專家效度，編製專家意見調查表，由六位專家針對各題項給予適度修改，以提升內容效度。

表 1 因素分析後之品格與關懷能力量表問項

誠實與負責
1. 與人接觸時，我通常會誠實面對他們。
2. 不論碰到什麼事，我通常會誠實面對事情。
3. 人的成功需要誠實面對每一件事，而不是以應付的方式完成。
4. 我通常會以負責的態度完成每一件事情。
5. 即使需要付出一些代價，我也願意完成我應該做的事。

尊重與態度
6. 與人接觸時，我通常會尊重對方的感受。
7. 與人說話時，我通常會專心傾聽對方。
8. 日常生活中，我會尊重任何人。
9. 與人相處時，我通常會以正向的態度面對他們。
10. 人的成功需要以一個好的態度完成事情，而不是草草應付。

品格認知
11. 我了解成功條件不在聰明，而是人格特質。
12. 大多數品格典範人物都有他們的理想或目標。
13. 了解品格的意義，使我更樂於貢獻自己的力量給社會。

品格認同
14. 了解品格的意義，使我對自己的未來和潛力有更大的期許。
15. 我同意品格對我現今求學與未來工作都有很大的幫助。
16. 我認同品格與態度對人生的重要性。
17. 我認同品格對我生命成長具有正面的意義。
18. 良好品格的人常常帶給我的人生重要啟發和影響。

關懷與服務
19. 我常常會主動關心周圍的人。
20. 我做任何事時，通常會事先考慮他人的感受。
21. 我常常樂於幫助別人。
22. 我常常希望別人生活過得更幸福。
23. 我常常願意去減輕別人的負擔。
24. 我會透過報章雜誌去關心社會事件

App 使用者品格與關懷活動延伸

25. 透過 App 參與「品格與關懷」活動，讓我對 e-HO 的其他活動更感興趣。
26. 透過 App 參與「品格與關懷」活動看到他人的留言，即使不同意也不任意謾罵，會予以尊重。
27. 透過 App 參與「品格與關懷」活動對我有正向的意義。
28. 我會透過 App 關心朋友的近況。
29. 我會透過 App 了解社會時事。

4.2 資料分析與討論

後測階段之有效樣本共 103 位，男女比例為男生 36.89%、女生 63.1%，年級比例分別為大一 16.5%、大二 26.21%、大三 32.03%、大四 11.65%、大五 0.97%、研究所 12.62%，學院比例分別為人育學院 11.65%、商學院 40.77%、理學院 14.56%、工學院 9.7%、設計學院 3.88%、電資學院 17.47%、法學院 1.94%。分析前測構面的平均數與標準差，在「誠實與負責」平均數為 3.98、「尊重與態度」平均數為 4.10、「品格認知」平均數為 4.06、「品格認同」平均數為 4.16、「關懷與服務」平均數為 3.85、「App 使用者品格與關懷活動延伸」平均數為 3.53；後測則分別增加 0.18、0.20、0.28、0.12、0.15，以及 0.15，顯示在「品格認同」、「關懷與服務」、「App 使用者品格與關懷活動延伸」等三個構面成長幅度不大，受試者在品格的認同並不會因為短期活動而有大幅度的成長。

經 ANOVA 分析後，性別的差異在「關懷與服務」之構面具有顯著影響，以平均數比較後發現女生平均數大於男生，顯示在「關懷與服務」構面中，女生對於關懷與服務的議題具有感受上的影響。在年級差異上，「品格認知」具有顯著差異，以 Scheffe 事後檢定後，發現在受測者顯著為大一及大四，表示這兩個年級的受測者經過學校提倡的通識課程與全人教育後，對於六個構面上具有差異。透過手機發表次數越高者，則有助於自己在品格與關懷能力上有所影響，在「品格認知」及「App 使用者品格與關懷活動延伸」中，有顯著的影響，反之另四個構面則影響較不顯著。

以成對樣本 t 檢定來比較前後測之差異，在「誠實與負責」之後測平均數高於前測 0.24，達顯著性；在「尊重與態度」之後測高於前測 0.30，達顯著性；「品格認知」之後測高於前測 0.31，達顯著性；「品格認同」之後測高於前測 0.17，未達顯著性；「關懷與服務」之後測高於前測 0.17，達顯著性；「App 使用者品格與關懷活動延伸」之後測高於前測 0.56，達顯著性。結果說明，在受測者參與活動前後比較後，「品格認同」、「關懷與服務」，以及「App 使用者品格與關懷活動延伸」未達顯著性，並未因為參與活動後而有明顯的影響。以成對樣本 t 檢定來比較前後測男生的差異，在「誠實與負責」之後測的平均數高於前測 0.01，未達顯著性；在「尊重與態度」之後測高於前測 0.17，未達顯著性；「品格認知」之後測高於前測 0.06，未達顯著性；「品格認同」之後測低於前測 0.01，未達顯著性；「關懷與服務」之後測低於前測 0.06，未達顯著性；「App 使用者品格與關懷活動延伸」之後測高於前測 0.04，未達顯著性。結果說明，在受測者參與活動前後的比較，品格與關懷能力並未因為參與活動後而有明顯的影響。以成對樣本 t 檢定比較前後測女生的差異，如表 **1** 所示。在「誠實與負責」之後測平均數高於前測 0.38，達顯著性；在「尊重與態度」之後測平均數高於前測 0.38，達顯著性；「品格認知」之後測平均數高於前測 0.46，達顯著性；「品格認同」之後測平均數高於前測 0.27，達顯著性；「關懷與服務」之後測平均數高於前測 0.3，達顯著性；「App 使用者品格與關懷活動延伸」之後測平均數只略高於前測 0.07，未達顯著性。結果說明，女生參與活動前後的比較上，在「App 使用者品格與關懷活動延伸」上未達顯著性，「品格認同」也未能因參與活動後而有明顯的影響。

表 1 前後測女生成對樣本 t 檢定差異表

構面	平均數	標準差	顯著性(雙尾)
誠實_前	3.88	0.67	0.001***
誠實_後	4.26	0.56	
尊重_前	4.00	0.69	0.000***
尊重_後	4.38	0.50	
認知_前	4.00	0.67	0.000***
認知_後	4.46	0.54	
認同_前	4.11	0.72	0.014**
認同_後	4.38	0.57	
關懷_前	3.81	0.62	0.002**
關懷_後	4.11	0.51	
APP_前	3.61	0.79	0.598
APP_後	3.68	0.75	

*p<0.05; **p<0.01; ***p<0.001

在受測樣本中，「App 使用者品格與關懷活動延伸」在參與活動後未達顯著，經過性別差異分析後，發現在「誠實與負責」、「尊重與態度」、「品格認知」、「品格認同」、「關懷與服務」上女生是有顯著差異的，顯示經由參與活動後影響了女生，且男生在參與活動後皆未達顯著性，顯示在參與活動後男生並未有太大的影響。

4.3 質性資料

在質性訪談方面，歸納使用者表示的「*參與活動中，透過觀看了同學的發表與迴響討論，透過活動後更加了解品格與關懷的觀念是多麼重要。*」、「*在陳樹菊的故事中，樂於助人的精神，讓我覺得認同他的理念與理想，也期勉自己能夠開始幫助需要幫助的人。*」、「*印象最深刻的是志工服務，因為*

我現在的志工服務也許只是為了升學或工作，並非出於自願的，感覺自己應該要更加的積極參與關懷弱勢及志工。」，以及「*手機發表在使用上，因為需要輸入所以便利性，會成為我使用發表或參與活動便利性考量因素。*」這四點，對照量化的實驗結果可以當成強化的資料說明。

5. 結論

本研究探討透過「品品禮 2.0」活動 App 對品格與關懷能力的影響，在不同的背景變項對「誠實與負責」、「尊重與態度」、「品格認知」、「品格認同」、「品格關懷」，以及「App 使用者品格與關懷活動延伸」等六個構面的影響。透過成對樣本 t 檢定分析八周活動的前後測樣本，發現參與者在「誠實與負責」、「尊重與態度」、「品格認知」等三個構面具顯著影響。其中發現性別對於品格與關懷能力具有差異，男生參與活動後，在這三個構面的表現皆不顯著；而女生參與活動後，在「誠實與負責」、「尊重與態度」、「品格認知」、「品格認同」，以及「品格關懷」等構面均有顯著影響。透過手機發表次數越高者，則有助於自己在品格與關懷能力上的提升，對於「品格認知」和「App 使用者品格與關懷活動延伸」這兩個構面會有顯著的影響。透過活動 App 中的影片與漫畫傳達關懷與服務的重要性，可以了解品格與關懷對自我成長是有意義的；而活動 App 傳達理念與觀念，在日常生活中就可以執行，更能提升自我品格和道德。

致謝

本研究承蒙國科會計畫部分補助，計畫編號 NSC 102-2511-S-033-003，特此致謝。

參考文獻

[1] 王保進, "引導學生學習成效品質保證機制之推動與落實-論第二週期系所評鑑之核心內涵," *評鑑雙月刊*, vol. 32, pp. 36-40, July 2011.

[2] 王玉麟, 黃以玫, 李光華, and 楊鎮華, "以核心能力為基礎之學生學習成效評量機制: 以中央大學為例," *教育研究月刊*, vol. 207, pp. 42-52, July 2011.

[3] 李坤崇, "大學基本素養與核心能力意涵及其建置," *教育研究月刊*, vol. 211, pp. 114-126, Nov. 2011.

[4] 潘正德 and 李清義, "中原大學品格教育的實踐與反思," 通識教育學刊, vol 4, pp. 97-123, Dec. 2009.

[5] 資策會. (2012). 智慧型手機與平板電腦的使用調查報告 [Online]. Available: http://www.find.org.tw/find/home.aspx?id=332&page=many

[6] F. M. Aymerich, G. Fenu, and S. Surcis, "An approach to a cloud computing network," *Proc. First International Conf. Applications of Digital Information and Web Technologies*, Ostrava, 2008, pp. 113-118.

[7] M. W. Berkowitz and J. H. Grych, "Early character development and education," *Early Education & Development*, vol. 11, no. 1, pp. 55-72, Jan. 2000.

[8] C. B. Barlow, M. Jordan, and W. H. Hendrix, "Character assessment: An examination of leadership levels," *Journal of Business and Psychology*, vol. 17, pp. 563-584, June 2003.

[9] R. Brandt, "On outcome-based education: A conversation with Bill Spady," *Educational Leadership*, vol. 50, pp. 66-70, Dec. 1992.

[10] W. Cheung and W. Huang, "Proposing a framework to assess Internet usage in University education: an empirical investigation from a student's perspective," *British Journal of Educational Technology*, vol. 36, pp. 237-253, Mar. 2005.

[11] E. Davies, "Reflective practice: A focus for caring," *The Journal of Nursing Education*, vol. 34, p.167, Apr. 1995.

[12] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and grid computing 360-degree compared," in *Grid Computing Environments Workshop (GCE)*, Austin, TX, 2008, pp. 1-10.

[13] K. Hafeez, Y. Zhang, and N. Malak, "Core competence for sustainable competitive advantage: a structured methodology for identifying core competence," *IEEE Trans. Eng. Manag.*, vol. 49, pp. 28-35, Feb. 2002.

[14] B. Hayes, "Cloud computing", *Communications of the ACM*, vol. 51, no. 7, pp. 9-11, July 2008.

[15] R. Kinnamon, "The importance of character development: An interview with Ron Kinnamon," *Camping Magazine*, vol. 76, no. 1, pp. 38-42, Jan-Feb 2003.

[16] J. A. King and K. M. Evans, "Can we achieve outcome-based education?," *Educational Leadership*, vol. 49, pp. 73-75, Oct. 1991.

[17] C.-Y. Lee, P. J. D. Pan, and C.-J. Liao, "Impacts and preferences study for e-HO as a holistic learning environment complementary to e-Learning," *Computers & Education*, vol. 56, no. 3, pp. 747-759, Apr. 2011.

[18] D. Leonard, "Core capabilities & core rigidities: A paradox in managing new product development," *Strategic Management Journal*, vol. 13, no. 1, pp. 111-125, Feb. 1992

[19] C.-J. Liao,, M.C. Chung, Y.W. Lai, W.C. Tseng, and C.H. Lin, "The construction of an i-Social learning system in the cloud computing environment," *Proc. 2nd International Conf. Future Computers in Education (ICFCE)*, ShangHai, China, 2012.

[20] C.-J. Liao, C.-J. Yang, and J.-T. Yang, "The Construction of a Social Learning Environment for Individuals in the Cloud Computing Environment," *Proc. World Conf. Educational Multimedia & Technology (EdMedia)*, Denver, Colorado, USA, pp. 1694-1700, 2012.

[21] T. Lickona, "The return of character education," *Educational Leadership*, vol. 51, pp. 6-11, Nov. 1993.

[22] T. Lickona, Character matters: How to help our children develop good judgment, integrity, and other essential virtues. New York: Simon and Schuster, 2004.

[23] C. Long and V. K. Mary, "Using core capabilities to create competitive advantage," *Organizational Dynamics*, vol. 24, no. 1, pp. 7-22, June 1995.

[24] Nielsen (2012). [Online]. Available: http://blog.nielsen.com/nielsenwire/online_mobile/nielsen-tops-of-2012-digital/

[25] N. Noddings, The challenge to care in schools: An alternative approach to education. advances in contemporary educational thought, Volume 8. New York: Teachers College Press, 1992.

[26] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, Eucalyptus: A Technical Report on an Elastic Utility Computing Archietcture Linking Your Programs to Useful Systems. Tech. Rep. 2008-10, University of California, Santa Barbara, 2008.

[27] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The Eucalyptus Open-source Cloud-computing System," in *Cloud Computing and Applications (CCA)*, Chicago, IL, 2008

[28] T. O'reilly. (2005, Sep. 30). *What is Web 2.0 Design patterns and business models for the next generation of software* [Online]. Available: http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html

[29] E. H. Otten, *Character education*. ERIC Digests, 2000. *(ERIC Document Reproduction Service No. ED 444932)*. [Online]. Available: http://www.eric.ed.gov/PDFS/ED444932.pdf

[30] W. G. Spady, Outcome-based instructional management: a sociological perspective. Arlington, VA: American Association of School Administrators, 1981.

[31] Sun Microsystems, Inc. (2009). *White Paper: Introduction to Cloud Computing Architecture (1st ed.)* [Online]. Available: https://www.sun. com/offers/details/CloudComputing.xml

[32] A. Weiss, "Computing in the clouds," *netWorker*, vol. 11, no. 4, pp. 16-25, Dec. 2007.

一個高效率的擬亂數產生方法與平行化加速的研究與分析

鄭毓融[1] 林昀德[2] 林芳邦[2] 黃詠詳[2] 蕭一豪[2]
[1]資訊工業策進會雲端系統軟體研究所
thisisyujungcheng@gmail.com
[2]國家高速網路與計算中心
{ lsi,fplin,1203086,ihow }@narlabs.org.tw

摘要

亂數產生器可以產生一連串無法預測的數值，產生的數值是在有限的數值或有限的資料範圍內，產生出來的一連串數值通常具有分佈平均、隨機、獨立及不可預測的特性。良好的亂數產生器必須是長週期的，並具有良好的統計性質及有效率的電腦執行。本研究提出一種以亂數基底的計算方法來產生擬亂數值，節省的使用記憶體資源即可產生大量的擬亂數，並且產生的亂數不會重複，再導入多線程的平行化方法，有效利用多核心處理器的優勢來加速巨量的擬亂數產生。

關鍵詞：亂數，擬亂數產生器，平行化，多線程。

錯誤! 找不到參照來源。.關於亂數產生器與平行化的重要性

亂數產生器可以產生一連串無法預測的數值，產生的數值是在有限的數值或有限的資料範圍內。產生出來的一連串數值通常具有分佈平均、隨機、獨立及不可預測的特性，也就是每個數值出現的機率大致是相同的，且產生出來的數值無法由其他數值推導而得，每次所產生的數值之間沒有關係，即下一個數值無法由前一個數值推導出來[1][4]。

良好的亂數產生器必須是長週期的，並具有良好的統計性質及有效率的電腦執行。具有長週期的亂數產生器不容易發生重複性的亂數序列，經過很長一段時間後亂數才會再度循環；良好的統計性質則是指產生的亂數序列是具有獨立且連續分布均勻的性質；有效率的電腦執行是指電腦在使用相同的亂數種子下不論重覆演算幾次都會產生相同的亂數序列，此外演算法的速度必須夠快，執行的時間和占用的記憶體越少越好[2][6]。

各個科學研究領域中時常運用亂數產生器來進行各類應用的模擬與測試，例如：雜訊模擬、雜湊搜尋、抽樣、數值分析、決策等皆使用亂數產生器來實現。亂數產生的方法可分成物理性及軟體性兩種方法。物理性方法例如：擲骰子，擲硬幣和輪盤等是最簡單的產生方式；而利用更小的物質如原子或亞原子的不確定性物理現象也可用來產生物理亂數，雜訊、放射性、時鐘偏移等都是產生物裡亂數的來源。軟體性的亂數產生方法是運用特殊的演算法或人工方法來產生長週期性與隨機性的亂數序列，因為在軟體上所產生的亂數主要透過演算法所產生，並不是真實的隨機亂數，所以此類的亂數產生器一般也稱作為擬亂數產生器(Pseudo Random Number Generator)。常見的擬亂數產生器使用線性同餘法(Linear Congruential Method)、多階層餘法(Multiple Recursive Method)或梅森旋轉法(Mersenne Twister)等演算法來產生擬亂數[7]-[10]。

科學研究與實驗有時候需要大量的擬亂數來進行模擬，例如產生大量的二進位的亂數模擬檔案(符合0與1常態化分佈的Normal Distribution)或產生大量的正弦/餘弦波形來模擬一般常態的電子訊號。而在最近幾年很熱門的雲端計算環境裡面，實體機器與虛擬機器之間的關聯性與資源配置亦可使用亂數序列來做指定，如此一來除了可以加強避免容易被追蹤出來的安全性，也可以使資源分配更為平均。但是當我們所要產生的亂數序列數量越大且不能重覆及具備高維亂度時，其所需要的計算維度與執行時間也會跟著呈現指數般的遞增。

在高效能計算系統的發展中，由於半導體技術受到了物理限制的影響(包含：製程大小、散熱問題、電力消耗等)，使得電腦處理器的時脈速度面臨到瓶頸，所以處理器製造商轉以發展多核心的架構，在單一處理器中置入多顆運算核心來提升整體處理器的運算能力。多核心架構的發展提升了平行處理(Parallel Processing)的效能與優勢，所以近年來平行化運算因而被廣泛的使用與研究。

一般在單一台電腦上，將複雜計算進行平行化時可使用多線程(Multi-threading)的方式來實現；如果有多台電腦時，則可以使用訊息傳遞界面(Message Passing Interface, MPI) 的方式來實現。兩者都需要將原始程式進行改寫，通常我們會將計算與資料切割成多份較小的集合，然後分配到不同的

核心或各計算節點上進行運算，最後再將不同的核心或是各計算節點的結果收集起來做後續的處理，然後輸出最終的結果。本研究將使用多線程的方式來開發平行化版本的擬亂數產生器，並透過本研究所設計的亂數產生方法來分析產生大量擬亂數時的加速情形。

本研究所提出的亂數產生方法其執行效能比較快速同時也比較節省記憶體。但是當我們要產生非常巨量的亂數時，計算時間會隨著亂數數量呈現指數般的遞增，所以將會需要一段很長的計算時間。近年來，由於多核心技術越來越成熟，利用平行化的技巧可以加速超級巨量擬亂數產生器的執行速度，本研究我們是透過有效率地使用多核心處理器的計算資源來達到平行化的加速目標。

2.亂數序列的簡介與基本理論

亂數一般分成自然亂數與擬亂數。自然亂數基本上是無法逆推的真實亂數，也就是無法透過分析來推斷其下個或上個亂數值，一般來說，沒有人可以保證精準的猜測到下個亂數。一般只能透過物理性亂數產生器才能產生自然亂數。擬亂數則是透過人工或人為的演算法所產生出來的亂數，來模擬出自然亂數的隨機性，其亂數結果是根據種子來產生的，因此實際上是可以被計算出來的，不過透過使用越複雜的演算法與種子組合就可以讓人越難猜測到下個產生的擬亂數值，在應用上便可以達到自然亂數的特性[3]。

傳統產生擬亂數的方法通常會以電腦的實際時間(Timer Based)作為隨機種子並導入演算法來產生亂數，此方法所產生的亂數隨著時間單元的變化而產生不同的亂數，優點是快速且種子取得簡單，種子也不易重覆，足夠提供一般的亂數隨機性。然而此方法也有些缺點，例如：亂數的隨機性在高品質的亂數需求時，如加密的應用、統計或數值分析時就不適合；並且也可能會在數千萬次的亂數產生執行中遇到重覆的亂數。當透過以時間為種子的方式來產生不重覆的亂數時，擬亂數產生器需要提供一套重覆亂數的檢查機制，如果出現重複的亂數時，就必須捨棄此次產生的亂數，然後重新產生一個新的亂數，反覆執行直到獲得足夠且不重複的亂數數量為止。當以此方式來產生大量且不重覆的亂數，隨著已經產生的亂數數量越多，亂數重覆的機率就會越高，導致需要更多額外的亂數產生週期與亂數唯一性的比對時間，浪費大量的計算資源。

根據不同的需求及用途，擬亂數產生器可以被設計出產生多種不同類型的衍生亂數。例如產生0與1的亂數序列可用來模擬一般檔案的位元資料流；1與 -1 的亂數可用來模擬傳輸訊號的震盪波形；包含文字與數字組合的亂數字串可以用來進行加密；或者是產生近似自然亂數序列來模擬出蒙地卡羅隨機取樣統計法[5]。

為了提供非常大量且亂數雜度足夠，同時具備不會重覆的擬亂數序列，本研究提出一種高效率的擬亂數生成方法來產生一連串的自然數亂數序列，此方法透過使用極少的記憶體來達到快速產生亂數序列的目的，並且保證產生的亂數序列數值絕對不會重覆。此外，我們把使用者輸入的密碼字串作為亂數隨機種子，以便確保輸入相同的密碼一定可以產生相同的亂數序列。最後我們再導入平行化架構，來提升整個超級巨量擬亂數計算的執行速度。

3.我們所設計的 PRNG 亂數生成演算法

相較於一般傳統的擬亂數產生器來產生不重覆的亂數序列，如圖 1 所示，本研究所提出的擬亂數產生方法是利用多組從 0 到 31 且不重覆的亂數序列作為多項式的計算基底(以 32 進制作為底數，如同一個二維陣列，內維大小固定為 32 個，外維大小則為階層的數量，至於外維的層數編號剛好就是所對應之指數次方的大小數值)，把每個階層的亂數值當作是係數(Coefficient)，然後乘上該係數所對應之 32 的指數率(次方值)，如此遞迴循環地相加各階層的數值組合而成，最後組合出 32 的 K 次方個亂數值。亂數序列的需求個數取決於欲產生的最大擬亂數值 N，然後以 32 為基底來進行多項式分解，找出可包含這個最大擬亂數值的階層個數 K。階層索引的次序編號也代表其各組亂數序列所需乘上 32 的指數次方值，如第一層的指數率為 0，也就是 32 的 0 次方；第二層指數率為 1，代表 32 的 1 次方；依此類推．．．。透過這種方式即可快速地計算出以 32 為基底且完全不會重複的 32 的 K 次方個亂數值，最後再輸出符合使用者所指定範圍內的亂數值序列。以下圖示說明了本研究的擬亂數生成原理與演算方法。

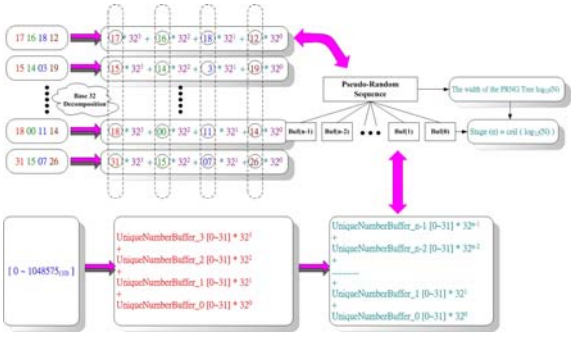


圖 1 以亂數基底方法產生亂數

如圖 2 所示，本研究的擬亂數產生器第一步先產生亂數基底序列。將使用者輸入的密碼字串做為亂數種子用來產生基底亂數序列。為了確保產生的亂數的雜度足夠，且每層的 Seed 種子數值能夠完全不同，首先將使用者輸入的密碼字串與預設的 128 個字元密碼字串做"替換"與"結合"的雙重組合，組合後的每個字元依序向前位移(Shifting)一個字元，使原本第一個字元循環左移至最後的字元，第二字元變為第一字元，最後再導入 MD5 Hashing Function 演算出第一層的 32 個 16 進制(Hex)的字元陣列(或稱字符陣列)。第二層依照第一層組合好的字串再進行一次字元循環左移，然後同樣再導入 MD5 Hashing Function 演算出第二層的 32 個 16 進制字元陣列，其他層也都依此方式來產生字元陣列，每層的字元陣列皆固定為 32 個字元長度。當產生所有需要的 16 進制的字元陣列(即陣列層數)後即可開始導出基底亂數序列。

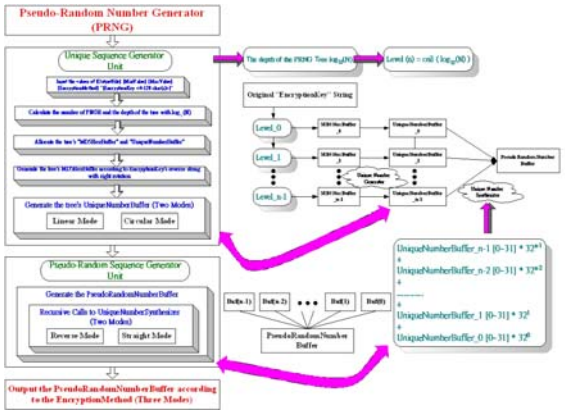


圖 2 本研究所設計之亂數產生流程

各層的字元陣列再透過本研究方法所設計的唯一數值(Unique Number)產生函數來轉換成 32 個 0 到 31 之間不重覆的亂數序列。由於數值的範圍不大，個數只有 32 個，因此可以快速比對是否存在重覆的數值，因此產生唯一數值的執行速度非常地快速。產生 MD5 基底亂數的方法是將字元以 16 進制先轉換成長整數(Long Integer)後做為起始位置，然後開始以起始位置(Start Position)的值加入計數值(Count)後與總字串長度(Key Length)相除取出餘數做為現在位置(Current Position)，現在位置帶入基底序列的 index 取出對應的位元，再做一次 16 進制的轉換，最後得到一長整數值(Value)。當最後得到的長整數值為偶數時，將長整數做放大處理，即是將字串長度減去長整數值再與字串長度相除取出餘數。透過上述的方法即可演算出 0 到 31 之間的數值，最後再檢查是否產生重覆的數值。當演算出 0 到 31 之間的亂數值發生重覆時，就進行雙向的鄰邊擴散演算(Bi-Direction Neighboring Diffusion)，搜尋最接近此數值可用的不重複數值。

雙向的鄰邊擴算演算以偏移(Offset)的方式進行向左或向右的擴散，也就是從周邊數值中取出尚未重覆的數值。當數值減去位移值後等於或大於 0 時或加上位移值後大餘總字串長度，則進行向左偏移擴散計算，反之則進行向右偏移擴散計算。透過這種持續的雙向偏移方式，檢查其值是否重覆，即可快速找出尚未重覆的數值。使用此雙向鄰邊擴散演算的優點是可以用最少的偏移(或搜尋)次數找出可用的不重複數值，無需再從頭開始檢查所有的數值(最壞的情況 O(n)=15，遠小於 O(n)=31)。

最後，當密碼字串轉換成計算亂數用的基底序列後即可開始產生 32 的 K 次方個擬亂數。當產生的亂數值越大時，所需的基底層數量則越多，以 32 的倍數來決定所需要的最大層數。例如當需要產生最小值為 1 至最大值為 100 萬的 100 萬個不重覆的擬亂數時，則至少需要 4 層基底，也就是至少產生 32 的 4 次方個亂數，再從中取出符合範圍內的所有亂數值。在進行每層的亂數值加乘組合時，每層的亂數值先乘以該層的 32 指數率後再開始做加法組合，層數越多，組合出來的亂數值就會越大。因為每層的亂數基底序列都沒有重複，所以將各層的亂數值相加後必然就可得到絕對不會重複的亂數序列。

利用本研究中所設計的擬亂數產生器所產生出來的亂數，也可以再轉換成 0 與 1 數量常態化分佈(Normal Distribution)的 0/1 亂數。所謂 0/1 亂數是指由 0 與 1 所組成的亂數，相當於計算機中的位元(Bit)0 與 1，所以可以用來模擬檔案資料或網路封包中的實際資料(Payload)。轉換為 0/1 亂數的方法有許多種，其中最簡單的方法是將亂數做餘數運算(Modulus)，將亂數值除以 2，即得到的餘數為 0 或 1，符合常態化均勻分佈的特性。

4.將亂數生成演算法進行平行化加速

亂數產生器產生亂數時，必須即時地儲存所有產生的亂數，一般都會使用陣列來暫存所有產生的亂數。使用陣列的方法需先定義一大小固定的陣列後，再開始將資料依序存入陣列中，資料不能儲存到陣列定義的大小範圍以外，否則就會發生溢位(Overflow)問題。本研究採用多線程的方式來實做平行化版本的擬亂數產生器，使用者能夠決定使用多少個線程數來執行平行化亂數產生，由於使用多線程後，每個線程所產生符合亂數需求範圍內的亂數數量將會不確定，無法有效地定義符合大小的陣列來暫存該線程所產生的亂數。本研究提出四種不同的方法來解決每個線程的亂數暫存問題，並比較四種方法的優缺點。

第一種方法是使用鏈結(Link List)的方法隨時依需求來增加或減少亂數暫存用的臨時空間。為了盡可能使用最少的記憶體，本研究設計了最簡單的結點(Node)資料型態，盡可能地讓結點資料型態使用最少的記憶體。結點型態中定義一個用來儲存亂數值的長整數(Long Integer)變數與一個用來指向下個結點位址的指標變數(Pointer)，透過該指標變數可實現單向鏈結(Single Link List)的方式來儲存亂數，每當一新的亂數值產生，則新增一鏈結點，用來儲存該亂數。使用單向鏈結的方式優點是能夠完全動態地依照產生的亂數個數來增加鏈結長度，但缺點是每個結點需要額外記錄下一個亂數結點的位址，一般來說在 32 位元的作業系統下，每個指標需使用 4 個位元組(Byte)來儲存記憶體位址，64 位元的作業系統則需 8 個位元組(實際大小依不同的作業系統與編譯器來做決定)。因此使用鏈結方法來儲存亂數值將會比使用陣列方法消耗更多的記憶體空間。

有介於鏈結的方法會使用較多的記憶體資源，因此使用陣列來暫存亂數序列，並透過 realloc()函數來動態調整該陣列的記憶體大小，即時地增加陣列的大小，避免產生溢位情形。其他三種方法分別使用了不同的 realloc()函數呼叫時機設計，第一種設計是每當產生一個新亂數時，便呼叫 realloc()函數，將陣列大小加一。第二種設計則是直接配置全部亂數數量大小的陣列，當亂數產生完畢後再呼叫 realloc()函數，來縮小陣列大小以符合實際產生的亂數數量。第三種設計是先將全部亂數數量除以線程數量後，得到一平均值 p(p=N/m)，各線程開始先配置 p 值大小的陣列，也就是將全部亂數數量大小的陣列先平均分配至每個線程中。當該線程產生的亂數數量超出預先配置好的陣列大小時，就開始使用第一種設計的方法，使用 realloc()函數來增加陣列大小；反之如果亂數產生完畢後，亂數數量低於陣列大小時，則使用第二種設計的方法透過 realloc()函數來縮小陣列，以符合實際亂數所使用到的陣列大小。

以上三種動態調整陣列的方法來暫存亂數值皆有其優點與缺點。第一種陣列方法的優點是可以完全動態的依照亂數產生數量來調整陣列大小，隨時保持最佳的記憶體使用率。然而，因為每產生一亂數時都需使用 realloc()函數來調整陣列大小，需頻繁地重新配置虛擬記憶體，因此會付出許多額外的時間在記憶體的配置上面，重新配置記憶體大小的執行次數大約等於亂數數量(N)。第二種方法的優點是使用 realloc()函數次數最少的，其次數大約等於多線程數量 m，但缺點是一開始就會佔用 m 個全部亂數陣列大小的虛擬記憶體(m*N)。第三種方法結合第一種與第二種方法的優點，一開始佔用的總虛擬記憶體空間為總亂數數量 N 的陣列大小(m*p=N)，至於 realloc()函數只有出現在亂數數量超出線程內的陣列大小時與最後在縮小陣列大小時才使用到，因此使用次數遠小於第一種方法。

本研究所設計的亂數產生器使用了多項式分解演算法，主要架構在多階層且長度固定的亂數基底陣列(Length = 32) 上面，因此在進行平行化時有多種方法可以將計算做拆解。最基本的方法為平行切割，將第一層的亂數計算基底進行切割。如圖 3 所示，例如當使用 4 個線程進行平行運算時，將第一層亂數基底陣列切割成 4 組亂數陣列(每組將會有 8 個亂數)，然後分別將各組亂跟底下各層(第 2 層至第 K 層)亂數基底陣列帶入各線程中進行運算。當各線程完成運算後，再按照順序從各線程中將產生的亂數序列組合後即可產生所有的擬亂數序列。不過使用這種切割方式的缺點是當使用的線程數量無法整除 32 時，則無法等量平均分配所有計算到各線程中；此外，由於每層只有 32 個亂數值，最多也只能使用 32 個線程。

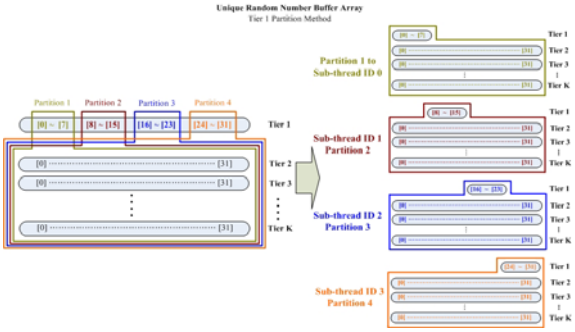


圖 3 第一層亂數基底序列切割

由於第一種平行化的計算切割方式有許多限制，因此本研究使用總量均分的方式來進行計算切割。進行總量均分切割時，直接將所有亂數計算基底陣列的組合進行切割，將切割出來的陣列範圍分配給各線程進行計算。所有亂數基底陣列組合相當於所有的亂數計算次數，如使用三層的亂數基底陣列時，亂數計算的總次數為 32 的 3 次方。總量均分切割後的各線程的計算範圍呈現一個垂直性的分割方式，以四個線程來說，第一個線程的陣列計算範為從[第一層的第 1 個/第二層的第 1 個/第三層的第 1 個]的開始計算，一直循序計算到[第一層的第 8 個/第二層的第 32 個/第三層的第 32 個] (相當於多維陣列[0][0][0] ~ [7][31][31])；第二個線程的計算範圍則從[第一層的第 9 個/第二層的第 1 個/第三層的第 1 個]開始計算到[第一層的第 16 個/第二層的第 32 個/第三層的第 32 個] (相當於多維陣列[8][0][0] ~ [15][31][31])。每個線程大致上都可以得到 8 * 32 * 32 個亂數計算組合，也就是大約產生的亂數個數。如圖 4 所示為上述之以總量均分的切割方法的意示圖。

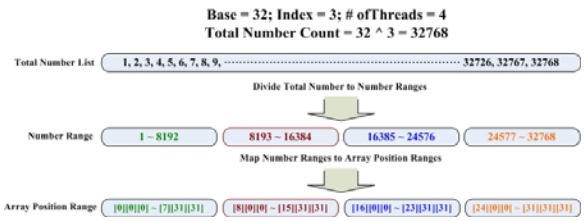


圖 4 總量均分的切割方法的意示圖

圖 5 所示為以總量均分方法的多線程詳細執行流程，根據所需的基底層數將亂數計算總量計算出來後，將總量以線程數量做均分，均分後每個線程得到在總量中的計算範圍，計算範圍再轉為陣列的中的開始與結束位置，即得到一陣列的計算範圍。每個線程再各自的陣列圍內計算出符合需求內的亂數後，將結果返回主線程，依序合併每個線程的亂數序列即可得到一完整亂數計算結果。

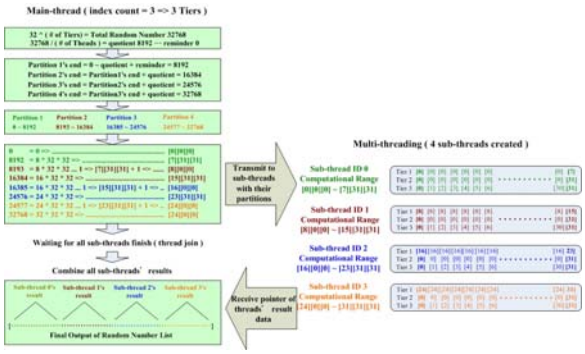


圖 5 總量均分的切割方法流程(4 線程)

當總量無法完全平均分配計算範圍到每個線程時(意即 m 無法完全整除 N)，我們將那些剩餘多出的計算分配給第一個建立的線程(通常線程 ID 為 0)。例如當所有亂數計算的次數為 32^4，使用線程數為 20 時，透過總量均分方式進行切割後，各線程平均分配到 52428 次計算，此時還有剩下的 16 次計算尚未分配，所以就將多出的 16 次計算加入到第一個產生的線程中，因此第一個線程會被分配到 52444 次的計算量，可轉換成 32 進位的 1 * 32^3 + 19 * 32^2 + 6 * 32^1 + 28 * 32^0 (相當於陣列組合從[0][0][0][0] ~ [1][18][5][27])。當總量均分無法完全平均切割時，多出來的計算次數一定會少於線程數量，所以把多出來的計算放入到任何一個線程對於整體執行效率而言幾乎沒有影響。但由於多線程的產生是依序執行的，一般來說當每個線程計算量一樣，越早產生的線程應該可以越早完成執行，所以將多出來的計算直接放入第一個建立的線程理論上是最有可能使全部的線程能夠同時完成計算的方法。

當使用總量均分切割方式來分割計算基底陣列除了可以有效地解決第一種分割方式中最多只能使用 32 個線程的限制；同時也能夠更均勻地分配亂數計算次數至各線程中，使平行化後的擬亂數產生器能夠更有效率地產生擬亂數序列。

5.平行化之實驗模型設計與實驗數據分析

針對本研究所設計的擬亂數產生方法與平行化的方式，我們從 1 個線程開始逐步增加線程數量（每次增加 4 個線程）來測試其擬亂數產生的加速效果，並針對四種亂數暫存方法測試其記憶體使用率。本實驗分成多線程加速測試及記憶體使用量測試兩個部分：(1).在多線程加速測試實驗中，分別以本研究中所設計的四種亂數暫存方法及亂數基底層數為 5 層、6 層及 7 層的亂數數量產生來做測試，記錄各層數的平均亂數產生時間。(2).在記憶體使用量測試中，使用 18 個線程，分別測試四種亂數暫存方法在產生約十億個(1G)擬亂數過程中的記憶體使用量，記憶體使用量的取樣間隔為 1 秒。表 1 所示為測試主機的硬體規格及實驗設計模型。

測試主機規格
CPU: Intel(R) Xeon(R) E7530 CPU @ 1.87GHz (true 24 cores CPU, HT enabled)
Memmory: 529322584 KB
OS: Linux 2.6.32-5-amd64 x86_64 GNU/Linux

測試準備
1. 快取清除 - "echo 3 > /proc/sys/vm/drop_caches"
2. 記憶體與硬碟資料同步 - "sync"

測試亂數數量
1. 多線程加速測試：產生擬亂數範圍從 1 開始到以下各層(index)的最大亂數值：
＊五層基底亂數{1048577, 2097152, 4194304, 8388608, 16777216, 33554432}
＊六層基底亂數{33554433, 67108864, 134217728, 268435456, 536870912, 1073741824}
＊七層基底亂數{1073741825, 2147483648, 4294967296}
2. 記憶體使用率測試：產生擬亂數範圍從 1 到 1073741824。

測試線程數量
1, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60

亂數暫存方法
1.Link List - Single Direction
2.Array Method 1 - Reallocate Array Size Random Number N Times
3.Array Method 2 - Reallocate Array Size T Threads Times
4.Array Method 3 - Reallocate Array Size 1 Time or size exceed N Times

記憶體使用率測試
1. 使用 ps -au 指令取得 VSZ 與 RSS 兩種記憶體使用量。
2. 測試 18 個線程數量的記憶體使用率。
3. 取樣間隔為 1 秒。
4. 從開始產生線程時開始記錄記憶體使用量直到所有線程完成計算。

表 1 測試主機硬體規格及實驗模型

本實驗之多線程加速測試部分，首先進行本研究所設計的原版擬亂數產生器(無多線程平行化之亂數產生測試。該擬亂數產生器為一般單線程程式，使用陣列來暫存所有產生的亂數，表 2 所示為其擬亂數產生時間之結果數據。相同層數(index)之亂數產生時間大致相同，最右側欄位為各層數的平均亂數產生時間。

Original PRNG Generation Time (seconds)				
Num of Index	Num of Values		Generation Time	Avg. Generation Time
index = 5	32 ^ 4 + 1	1048577	17.442	17.471
	32 ^ 4 * 2	2097152	16.973	
	32 ^ 4 * 4	4194304	17.375	
	32 ^ 4 * 8	8388608	17.670	
	32 ^ 4 * 16	16777216	17.809	
	32 ^ 5	33554432	17.559	
index = 6	32 ^ 5 + 1	33554433	698.639	703.980
	32 ^ 5 * 2	67108864	694.572	
	32 ^ 5 * 2	134217728	696.448	
	32 ^ 5 * 2	268435456	704.053	
	32 ^ 5 * 2	536870912	711.341	
	32 ^ 6	1073741824	718.831	
index = 7	32 ^ 6 + 1	1073741825	25948.942	26011.562
	32 ^ 6 * 2	2147483648	26010.398	
	32 ^ 6 * 4	4294967296	26075.346	

表 2 原版擬亂數產生器之結果數據

表 3 所示為本研究所設計的平行化版本擬亂數產生器的加速測試數據結果。其中左邊欄位為開啟的線程數量，由 1 個線程開始測試，逐次增加 4 個線程來測試直到 60 個線程。每種線程數量測試中也分別測試鏈結和三種使用陣列的亂數暫存方法。針對每種亂數基底層數（index = 5, 6, 7）內所有亂數測試的產生時間，加總計算取得該層的平均亂數產生時間。本實驗數據不包含亂數基底層數為 2、3 及 4，因為當亂數基底層數為 4 層及以下的亂數產生時間都遠低於 1 秒，所以無法有效地顯示出其加速效果。關於各基底層數的多線程加速曲線特性請參考表 4、5、6。

Num of Threads	Average Time of PRNG Generation (sec)											
	index = 5 {1048577, 2097152, 4194304, 8388608, 16777216, 33554432}				index = 6 {33554433, 67108864, 134217728, 268435456, 536870912, 1073741824}				index = 7 {1073741825, 2147483648, 4294967296}			
	Link List	Array Method			Link List	Array Method			Link List	Array Method		
		1	2	3		1	2	3		1	2	3
1	18.39	18.19	17.95	17.76	730.77	721.86	710.72	710.10	27411.18	27231.94	27206.41	27320.43
4	4.91	7.57	4.52	4.53	189.25	1525.99	177.73	177.40	6903.46	57735.83	6831.66	6843.92
8	3.02	4.98	2.30	2.30	106.20	1265.22	88.82	88.83	3482.71	10093.27	3419.55	3408.57
12	2.53	3.89	1.76	1.71	84.35	600.17	59.55	59.58	2356.13	16123.72	2279.62	2285.15
16	2.38	3.67	1.13	1.11	83.45	256.46	44.69	44.71	2027.33	12746.84	1786.12	1786.95
20	2.37	3.62	0.92	0.92	157.06	306.62	35.81	36.21	1653.19	7721.28	1431.27	1430.06
24	2.34	3.65	0.77	0.80	249.21	256.58	29.82	30.40	1414.60	11899.90	1199.95	1216.53
28	2.36	3.70	0.85	0.85	270.89	266.41	33.91	33.93	1420.65	6903.53	1366.39	1364.76
32	7.24	3.61	0.76	0.77	293.45	239.03	29.69	29.75	1417.06	6762.04	1202.81	1197.45
36	8.71	3.76	0.68	0.68	302.95	207.93	26.80	26.52	1475.52	6594.05	1073.29	1079.98
40	8.66	3.99	0.75	0.77	300.35	178.74	26.45	26.51	1739.71	5862.46	1108.14	1114.84
44	8.75	4.10	0.70	0.70	323.99	168.95	24.68	24.68	2150.40	5090.79	1035.14	1036.77
48	8.62	4.67	0.73	0.76	331.93	177.47	23.59	23.48	2267.76	5361.10	971.01	970.22
52	9.02	4.71	0.80	0.79	334.09	157.68	24.52	24.59	2657.33	4861.39	974.48	981.47
56	9.03	5.06	0.75	0.77	336.50	189.63	24.30	24.63	2756.16	3858.91	976.37	980.14
60	8.89	5.18	0.77	0.75	338.10	169.64	24.21	24.30	2832.96	4552.38	986.64	978.74

.表 3 多線程平行加速之實驗結果數據

表 4 所示為使用 5 層的亂數基底時，各線程數量的平均亂數產生時間曲線圖。以鏈結方法做為暫存亂數方法時，當使用線程數量為 24 時，會達到最佳的加速效果，但當線程數量為 28 時反而會開始降速，其後各線程數量的亂數產生時間約為 1 個線程時的一半時間（1 線程的平均亂數產生時間約 18 秒，36 至 60 線程的平均亂數產生時間約 9 seconds）。當以使用第一種陣列儲存方法時，多線程的加速效果大約在使用 12 個線程之後停止加速，之後開始緩慢降速。第二種和第三種陣列儲存方法比起之前兩種有更佳的多線程加速效果，但線程使用數量約達到 24 個之後就會停止加速。

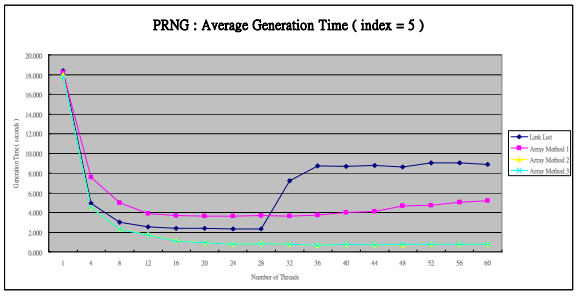


表 4 五層基底亂數平均亂數產生時間

表 5 所示為使用六層的亂數基底時，各線程數量的平均亂數產生時間曲線圖。鏈結的方法當線程數量為 16 達到最高的加速效果，當線程數量超過 16 之後加速效果開始緩慢下降。在使用第一種陣列儲存方法中，線程數量為 4 和 8 時，速度大幅下降，比 1 個線程約慢一倍左右，使用 16 個線程數量時加速效果最明顯，但是當線程數量大於 20 之後加速效果不明顯。使用第二種及第三種陣列儲存方法中，可以明顯看出有兩個階段的加速效果，當線程數量為 24 時得到第一階段最佳的加速效果，當使用 48 個線程時（第二階段）得到比第一階段更快的加速效果，之後加速效果趨近為零。

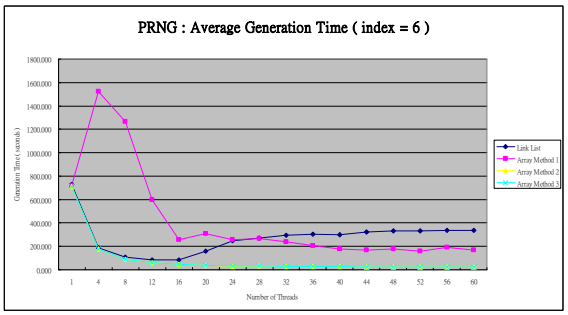


表 5 六層基底亂數平均亂數產生時間

表 6 所示為使用七層的亂數基底時，各線程數量的平均亂數產生時間曲線圖。當使用 40 個線程時，鏈結的方法達到最高的加速效果，之後開始緩慢降速。而使用第一種陣列儲存方法，加速效果是最低的，皆不如其他三種方法，使用四個線程時，加速效果為負的，當使用 8 個線程時開始逐漸有加速效果，但加速效果不穩定。使用第二種及第三種陣列儲存方法在第 24 個線程與 48 個線程數量可達到分別兩個階段的最佳加速效果。

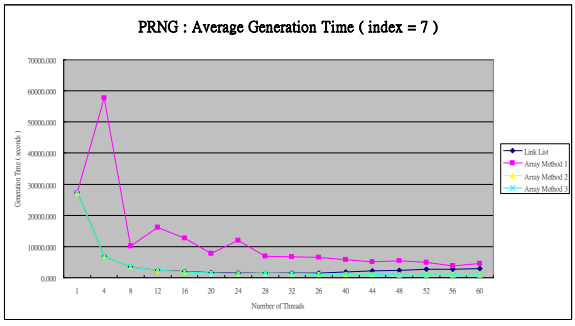


表 6 七層基底亂數平均亂數產生時間

將原始版擬亂數產生器與其平行化版本中之最短的亂數產生時間做比較，可得到平行化後的擬亂數產生器之最佳加速比率。表 7 顯示平行化版本的四種亂數暫存方法中，具有最佳加速效果的線程數量與加速比率。使用陣列儲存方法二和三，在六層亂數基底時，可得到 29.83 及 29.97 最佳的加速

比率。

		Link List	Array Method		
			1	2	3
index = 5	Num of Threads	24	32	36	36
	Best Speed Up Rate	7.46	4.83	25.35	25.50
index = 6	Num of Threads	16	52	48	48
	Best Speed Up Rate	8.43	4.46	29.83	29.97
index = 7	Num of Threads	24	56	48	48
	Best Speed Up Rate	18.38	6.74	26.78	26.80

表 7 最佳的多線程數量之加速比率

本研究所設計的四種亂數暫存方法解決了各線程無法配置準確的亂數暫存空間問題，使各線程能夠正常的暫存該線程所有產生的亂數。但根據測試結果，四種方法在不同數量的擬亂數產生，有些不同的加速情形，甚至降速。只使用 1 個線程時，四種方法的亂數產升速度差別不大，當增加線程數量後則開始產生差異。本研究中所使用的第二種與第三種陣列的亂數儲存方法的加速效果是幾近相同且最佳的。根據表 7，亂數基底數量為 5 時，第二種和第三種陣列儲存方法中使用 36 個線程時，最高可加速約 25 倍。亂數基底數量為 6 時，第二種和第三種陣列儲存方法中使用 48 個線程時，最高可加速至 29 倍 (近 30 倍)。亂數基底數量為 7 時，第二種和第三種陣列儲存方法中使用 48 個線程時，最高可加速 26 倍。另外可以明顯看到加速效果在 24 與 48 個線程時達到兩個最高的加速效果，這與我們所使用的測試主機規格有關，也符合了我們當初所預期的加速最佳理想值應當落在(a). 實際核心數量為 24 與 (b). 超執行緒 (Hyper Threading)所模擬出來的 48 核心之間。

以下為第二部分的實驗測試，針對四種亂數暫存方法中，測試在產生大量亂數時的記憶體使用率。記憶體使用率測試使用外部系統指令(ps -au)來取得兩種記憶體使用量；(1). 虛擬記憶體(VSZ) 、 (2). 實際使用記憶體(RSS)。VSZ 為行程(Process)執行時，向作業系統所提出的記憶體使用量需求;RSS 則為行程執行時實際所佔用的記憶體使用量。

表 8 為使用鏈結時的 VSZ 與 RSS 使用率，兩種記憶體的使用率同時緩慢穩定成長。VSZ 最高使用約 34347 MB，RSS 最高使用約 33477 MB。

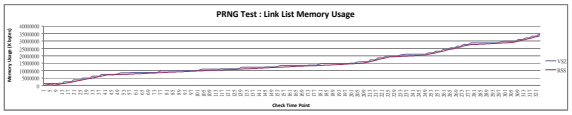


表 8 記憶體使用率之一(鏈結儲存)

表 9 為陣列儲存方法一的 VSZ 與 RSS 使用率。兩者記憶體使用率成反曲線成長，成長速度逐漸緩慢。VSZ 最高使用約 8647 MB，RSS 最高使用約 8360 MB。

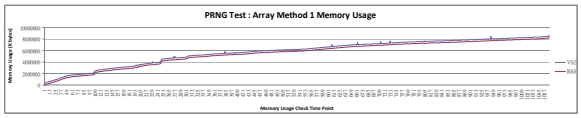


表 9 記憶體使用率之二(陣列儲存方法一)

表 10 為陣列儲存方法二的 VSZ 與 RSS 使用率。VSZ 全程固定使用大量的記憶體，RSS 的使用率慢速成長。VSZ 最高使用約 151300 MB，RSS 最高使用約 8329 MB。

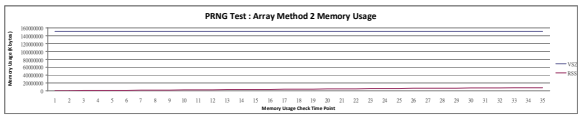


表 10 記憶體使用率之三(陣列儲存方法二)

表 11 為陣列儲存方法三的 VSZ 與 RSS 使用率。VSZ 全程的大小固定，RSS 則呈現線性成長。VSZ 最高使用約 8759 MB，RSS 最高使用約 8305 MB。

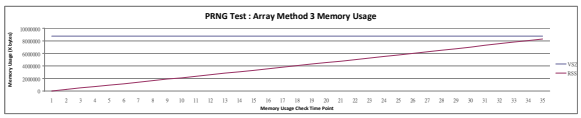


表 11 記憶體使用率之四(陣列儲存方法三)

四種亂數暫存方法中，使用鏈結的方法中 RSS 的使用量是最高，而使用第二種陣列儲存方法中 VSZ 的使用量是最高的，但這是由於使用多線程所導致的，因為每個線程自己都會配置一個全部亂數陣列大小的記憶體空間，因此使用量與線程數量成線性倍數成長。使用三種陣列的方法的 RSS 使用量都很相近，但測試結果中第三種的 RSS 使用量最低。

綜合多線程平行實驗的加速效果與記憶體使用率兩個部分的測試結果，使用第二及第三種陣列的儲存方法的加速效果最佳，而這兩者中，又以第三種的記憶體使用量較佳，因為 VSZ 的使用量遠小於第二種。換言之第二種陣列方法若是用在一些記憶體空間不大的主機中，很有可能會造成記憶體不足的窘境。

6.結論與未來工作

本研究所設計的擬亂數產生器可以有效地使用少量的記憶體來進行大量的擬亂數產生，確保產生的亂數絕對不會重覆，並且再透過多線程的平行化架構來提升擬亂數的產生速度，最高可達近 30

倍的加速效果。多線程以總量均分切割方式來將亂數計算更平均地分配至每個線程中，進而提升多線程的使用效率；同時也透過使用平均分配陣列大小再依實際使用量來調整陣列大小的亂數暫存方法提供了較佳的記憶體使用率。故我們所提出之擬亂數產生器具備了節省記憶體、執行效率快，可充分利用多線程平行化的方式來產生超大量的擬亂數等三大特色。

本研究已完成實作多層式亂數基底組合來產生大量擬亂數的方法與多線程版本的擬亂數產生器，未來我們可以更進一步地研究如何讓計算分佈更均勻的平行化切割方法與多線程之動態記憶體配置最佳化，最後也可以再導入 MPI 的平行化技術，透過網路串連多台電腦來計算更大量的擬亂數序列。

誌謝

[1] 資訊工業策進會雲端系統軟體研究所
This work is conducted under the "Cloud computing systems and software development project (2/3)" of the Institute for Information Industry which is subsidized by the Ministry of Economy Affairs (MOEA) of the Republic of China.

[2] 國家實驗研究院國家高速網路與計算中心

參考文獻

[1] A. De Matteis, S. Pagnutti, Long-range correlations in linear and non-linear random number generators, Parallel Computing 14, 1990, pp. 207-210.

[2] Charles W. O'Donnell, G. Edward Suh, and Srinivas Devadas, "PUF-Based Random Number Generation", Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, 2004

[3] D.E. Knuth, The Art of Computer Programming, Vol. 2, Addison-Wesley, Reading, Mass., 2nd ed., 1981.

[4] David K. Gifford, "Natural Random Numbers", Laboratory For Computer Science, Massachusetts Institute of Technology. 1998

[5] H. Niederreiter, Random Number Generation and Quasi-Monte Carlo Methods, SIAM, Philadelphia, 1992.

[6] P. Hellekalek, "Good random number generators are (not so) easy to find", Mathematics and Computers in Simulation 46, 1998, pp. 485-505

[7] P. L'Ecuyer, Random number generation, In Jerry Banks (Ed.), Handbook on Simulation, Wiley, New York, 1997.

[8] 李和家、傅振華與陳樂惠，"強化型 LCG 虛擬亂數機制亂數產生評量之研究"，台灣博碩士論文知識加值系統，2010。

[9] 林水木與黃宇中，"真實亂數產生器之設計"，台灣博碩士論文知識加值系統，2003。

[10] 謝國偉與盧鴻興，"增量選取在平行化線性亂數產生器的應用"，台灣博碩士論文知識加值系統，2006。

醫療影像之可逆式資訊隱藏技術應用邊緣敏感度分析預測方法

呂慈純[*]　曾俊雅[1]　黃俊智[2]
朝陽科技大學資訊管理系
[*]tclu@cyut.edu.tw
[1]s10033901@cyut.edu.tw
[2]opo1211@gmail.com

摘要

醫療影像是一種記錄病患資訊的重要資料，隨著資訊科技的進步，為了讓病患的資料能夠更為清晰，影像品質已經發展到 16 位元的 DICOM 高品質影像。本研究改良 Feng 和 Fan 學者提出的延伸 Lukac 方法並且使用於醫療影像，透過標準差分析影像區塊的複雜程度，進而決定不同的預測方式，提高預測的精確度。實驗結果證實本研究方法可以有效地提升影像品質，尤其是複雜型的影像及醫療影像有較佳的效果。

關鍵字：醫療影像、可逆式資訊隱藏、標準差、直方圖位移。

Abstract

Medical imaging is important data to record patient information. In this study, we improve Feng and Fan's method and use it in 16-bit DICMO medical imaging. The proposed scheme analyzes the complexity of image black by using image standard deviation to determine the prediction method for improving prediction accuracy. Experimental results show that the method can effectively improve image quality, especially in complex images and medical images with better results.

Keywords: Medical image; Reversible data hiding; Standard deviation; Histogram- shifting technique.

1. 前言

醫療影像是一種記錄病患重要資訊的資料，隨著資訊科技的發展，數位化的處理便持續受到關注，為了提升診斷時的精確度，醫師對影像品質的需求逐漸提升。隨著科技進步，醫療影像的記錄方式從 8 位元深度影像，演進到 16 位元和 32 位元影像，影像品質更為精細 [9]。圖 1–2 為 8 位元和 16 位元影像的像素分佈比較。醫療數位影像和通訊標準(Digital Imaging and Communications in Medicine, DICOM)是為了讓醫院各部門的醫療儀器產生出來的醫療影像進行整合，更完整建構出病患資訊。但是數位化醫療影像在網際網路上的儲存和傳輸的過程中可能會遭到第三者的攔截或篡改，導致醫師無法正確判斷病患的資訊。因此，學者們將資訊隱藏技術運用於醫療影像 [2, 5, 6]。隨著 16 位元影像的盛行，如何有效利用高階位醫療影像藏入機密訊息，已成為新一代資訊隱藏技術的挑戰。

醫療影像嵌入訊息後必須注意影像的變化，因為醫療影像是完整呈現出病患資訊的一種資料，假使影像失真太嚴重，可能會影響醫師的判斷 [1]。也有可能導致承載訊息的影像媒體被破壞，永遠無法復原回原始狀態。因此，學者們發展出可逆式資訊隱藏技術（Reversible Data Hiding, RDH），在取出機密訊息後，可以讓隱蔽影像完全恢復回原來的影像。



(a) 8-bit 影像

240	241	241	240	245	243	238
240	241	248	245	246	243	245
243	245	245	251	251	246	245
243	245	248	245	252	248	245
245	251	249	253	249	245	246
248	248	249	251	255	251	253
246	249	251	251	248	248	251
251	255	252	252	251	251	251

(b) 8-bit 像素值



(c) 16-bit 影

2843	2676	2559	2579	2606	2696	2894
2616	2458	2512	2655	2685	2881	3066
2420	2286	2414	2674	2727	2838	3161
2247	2163	2316	2759	2792	2865	3177
2120	2096	2226	2732	2788	2956	3156
2087	2091	2209	2593	2740	2950	3094
2249	2234	2270	2572	2707	2783	2910
2522	2457	2412	2520	2627	2722	2962

(d) 16-bit 像素值

圖 1 像素值比較

近幾年來 RDH 技術有許多的相關研究，其中一種類型是差異擴張法（Difference Expansion），是以像素與像素之間的差異進行擴張，將機密訊息藏於擴張後的差異中 [10, 11]。另外一種常用的方法是直方圖位移法（Histogram Shifting-based），該方法是先分析像素值之分佈情況，藉由產生出來的直方圖將機密訊息藏於峰值點中 [4, 8, 12]。

本研究提出一個改良 Feng 和 Fan 學者的方法，透過標準差評估各區塊的複雜度，不同複雜度的區塊用不同方式進行預測，並且以自適性的方式設定門檻值。最後分析預測誤差的分佈情形，利用直方圖位移的方式嵌入機密訊息，提升影像品質。

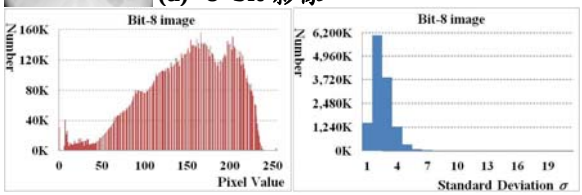
2. 文獻探討

2.1 預測方式

預測像素是 RDH 技術中很常用的一種方式，該方法利用預測像素與原始像素之間的差異距離進行訊息嵌入，如果被預測的像素越趨近於原始像素，則嵌入訊息後對影像失真程度越小。因此，預測方法的精準度會顯著影響到嵌入量和影像品質。學者們為了降低差異距離提出了以預測值進行差值運算的方法，預測值有些是利用鄰近像素值的平均值，有些使用加權概念，以減少預測值與原始像素之間的差異距離。然而，除了預測方法的修改外，選擇適當的像素個數和位置也可能會影響預測結果。



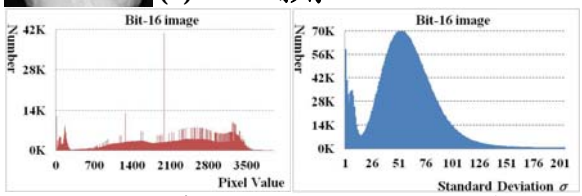
(a) 8-bit 影像



(b) 8-bit 像素值分佈　(c) 8-bit 標準差分佈



(d) 16-bit 影像



(e) 16-bit 像素值分　(f) 16-bit 標準差分佈

圖 2 影像分析

Yang 和 Tsai 學者將影像中的每個像素以棋盤方式分成 2 個類別（如圖 3 所示），並且以直方圖位移的方式嵌入機密訊息，該方法將灰階影像分類成互不相交的 2 個集合 [12]。

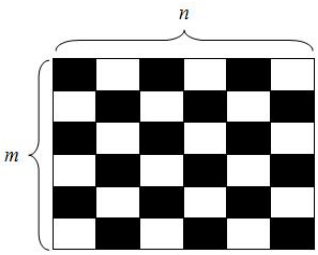


圖 3 棋盤式（交錯式）影像

Yang和Tsai學者的方法使用不同集合的4個鄰近像素進行預測，例如預測黑色棋盤格的 α 集合的 $x_{(i,j)}$ 像素時，會使用鄰近白色棋盤格的 β 集合的像素進行預測；反之，預測 β 集合的像素時，會透過 α 集合的像素進行預測。因此，在進行訊息嵌入和取出時，不會干擾到相同集合的數值。

2.2 直方圖位移

Ni 等學者於 2006 年提出直方圖位移技術與 RDH 進行結合 [8]，直方圖位移的概念是先分析整張影像像素分佈情形，並且得到一張直方圖表，接

著從直方圖表中尋找出現最多次的峰值點（Peak Point）和都沒有出現過的零值點（Zero Point），最後將機密訊息嵌入峰值點，嵌入流程如下。

(1) 分析像素分佈情形，並且產生直方圖表。

(2) 尋找峰值 P 和零值 Z。

(3) 位移直方圖像素值，位移條件如下：

I. 如果 $P<Z$，$[P+1,Z]$之間的像素 $x_{(i,j)}+1$。

II. 如果 $P>Z$，$[P-1,Z]$之間的像素 $x_{(i,j)}-1$。

(4) 將機密訊息嵌入峰值點，並且產生隱蔽影像，公式如下所示：

$$\begin{cases} x'_{(i,j)} = x_{(i,j)} + b, & if \quad P < Z, \\ x'_{(i,j)} = x_{(i,j)} - b, & if \quad P > Z. \end{cases} \tag{1}$$

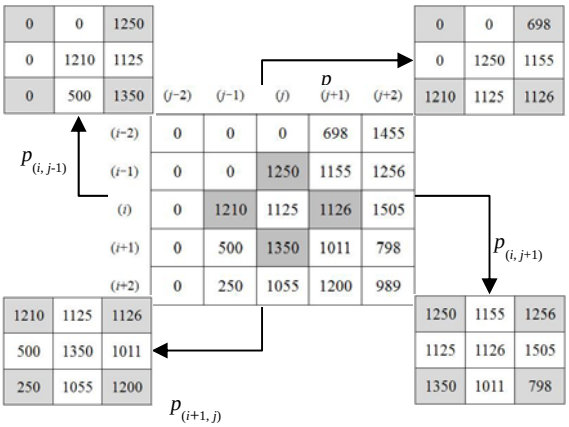


圖 4 演算法範例

令 $x'_{(i,j)}$為偽裝影像的像素值，b 為欲嵌入的機密訊息。當像素值 $x_{(i,j)}$分析完成後，找出峰值點 P 和零值點 Z，接著位移 P±1 和 Z 之間的像素並且對峰值點 P 嵌入訊息。

2.3 延伸 Lukac 演算法

Lukac 等學者使用周圍鄰近像素的邊緣敏感（Edge-Sensing）權重係數對彩色影像進行預測[7]。首先，計算鄰近像素的權重，其公式如下：

$$p_{(i,j)} = \left\lfloor \sum_{k=1}^{4} w_k r_k \right\rfloor, \tag{2}$$

令 $p_{(i,j)}$為預測像素值，w_k 為鄰近像素權重，r_k 為第 k 個鄰近像素值，i 和 j 為影像的 2 維索引位置，k 為鄰近像素集合 $k=\{r_{(i,j-1)}, r_{(i-1,j)}, r_{(i,j+1)}, r_{(i+1,j)}\}$。權重 w_k 的計算會透過鄰近像素的邊緣敏感係數 u_k 求得，其公式如下：

$$u_l = \left(1 + \sum_{k=1}^{4} |r_l - r_k|\right)^{-1}, \tag{3}$$

令 $l=k$，公式 (3) 加強邊緣像素 r_l 與其他 4 個像素 r_k 之間的關聯性，降低預測誤差。最後，利用下列公式正規化 u_k 的數值，即可得到鄰近像素的權重。

$$w_l = \frac{u}{\sum_{k=1}^{4} u_k}。 \tag{4}$$

以圖 4 為例，首先利用公式 (3)計算鄰近像素 $r_{(i,j-1)}$、$r_{(i-1,j)}$、$r_{(i,j+1)}$和 $r_{(i+1,j)}$的邊緣敏感係數 u_k。接著，透過公式 (4) 正規化，得到鄰近像素的權重值。最後，利用公式 (2) 即可得到預測像素值 $p_{(i,j)}$=1,231。

Feng 和 Fan 學者於 2012 年將 Lukac 等學者的概念運用於資訊隱藏中 [4]，他們假設 $r_{(i-1,j-1)}$、$r_{(i-1,j+1)}$、$r_{(i+1,j-1)}$和 $r_{(i+1,j+1)}$的鄰近像素對預測像素 $p_{(i,j)}$ 也會有貢獻。因此，首先計算 $p_{(i,j)}$的鄰近像素的預測值，其 u_k 和 w_k 的公式與 (3)-(4) 相同，但是鄰近像素集合改為 $f_k=\{r_{(i-1,j-1)}, r_{(i-1,j+1)}, r_{(i+1,j-1)}, r_{(i+1,j+1)}\}$。

最後對預測後的像素值 p_k 調整影響大小，其公式如下：

$$p'_k = \lfloor r_k - \eta_k \times (p_k - x_k) \rfloor, \tag{5}$$

令 η_k 為調整預測值的影響大小，η_k 決定該預測值 p_k 的影響大小，作者建議 η_k 值設為 0.1。

以圖 4 為例，透過公式 (2)-(4) 對 4 個鄰近像素進行預測，並且利用公式 (5) 得到調整後的預測

值 $p'_{(i,j-1)}$=1,146、$p'_{(i-1,j)}$=1,165、$p'_{(i,j+1)}$=1,003 和 $p'_{(i+1,j)}$=1,242。最後，再透過公式 (2)-(4) 即可得到 $p_{(i,j)}$=1,149。

從圖 4 中的範例可以發現，Feng 和 Fan 學者所提出的延伸 Lukac 方法對高複雜度區塊的預測更為精確。然而，本研究在分析延伸 Lukac 方法時，發現該方法在平滑區塊上的表現不比原始 Lukac 方法好，因此我們提出一個能夠依區塊特性調整使用的方法，用以改進 Feng 和 Fan 的方法。使提出方法更適用於醫療影像。

3. 研究方法

本研究利用 Feng 和 Fan 學者的延伸 Lukac 方法，提高複雜區塊的預測能力，針對平滑區塊，則使用傳統 Lukac 預測方法進行。因此，本研究將影像切割成數個區塊，並進行標準差計算，根據標準差門檻決定該區塊要使用的預測方法。最後，利用預測誤差進行直方圖位移並且將機密訊息嵌入，研究設計流程如圖 5 所示。

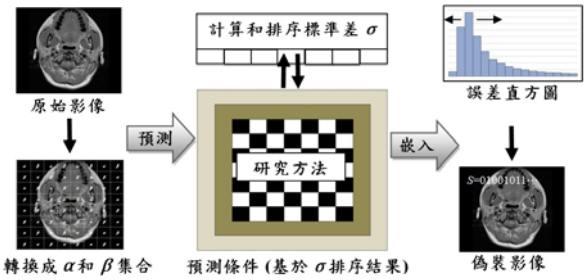


圖 5 所提方法示意圖

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	0	0	0	1398	1455	1456	0
2	0	0	0	0	698	1455	1546	1506
3	0	0	0	1250	1155	1256	1354	1355
4	0	0	1210	1125	1126	1505	1323	1444
5	0	0	500	1350	1011	798	1246	459
6	0	0	250	1050	1200	989	410	137
7	0	150	115	1320	1411	200	598	199

圖 6 研究範例

3.1 前置階段

首先，將影像分成 α 和 β 集合，每次取其中一個集合進行嵌入。如圖 6 所示。

Al-Qershi 和 Khoo 學者透過 Pearson 相關係數分析標準差與均方差（Mean Squared Error, MSE）之間的關係 [3]。經實驗分析後發現標準差與 MSE 呈現出顯著正相關聯。因此，本研究利用 Al-Qershi 和 Khoo 學者的概念，對每個 3x3 區塊進行標準差計算。以 $x_{(i,j)}$ 其鄰近 4 個像素計算標準差。最後，對標準差進行排序，數值越小會優先嵌入訊息。

3.2 預測階段

進行預測時，會先設定 2 個門檻值 T_1 和 T_2，門檻值主要是判斷使用的預測方式。如果該像素位置的標準差 $\sigma \leq T_1$，以傳統 Lukac 方法進行預測；如果該像素位置的標準差 $T_1 < \sigma \leq T_2$，則以延伸 Lukac 方法進行預測。

是延伸 Lukac 方法會有超出邊界的情形，因此對邊緣位置的像素會有不同的處理（如圖 7）。最邊緣的像素，如圖 7-(a)，會使用周圍 2 個鄰近像素進

行預測；靠近邊緣像素最外圍一圈的像素，如圖

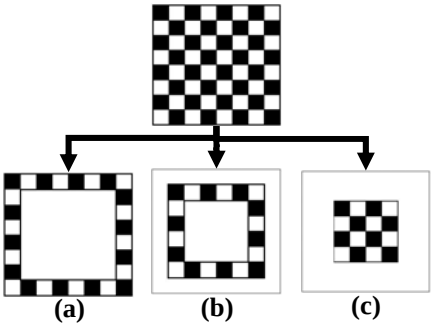


圖 7 不同位置使用的預測方法

7-(b)，因無法再向外擴展使用延伸 Lukac 方法，故統一採用傳統 Lukac 方法，即 $\sigma \leqq T_2$，即可進行藏入。

3.3 嵌入階段

本研究以預測誤差為基礎進行直方圖分析，最後將機密訊息嵌入峰值點中，嵌入流程如下：

(1) 建立預測誤差 $e_{(i,j)}$ 直方圖表。

(2) 尋找個數最多的誤差值，做為峰值（P）。

(3) 從 P 開始尋找零值點 Z。

(4) 位移 P 和 Z 之間的誤差值，將機密訊息嵌入峰值點 P，並且產生偽裝影像。

(5) 以此類推，直到所有屬於 β 集合都嵌入訊息後，改藏 α 集合，藏入方法相同。

3.4 提取階段

提取階段與前述嵌入流程相似，流程如下：

(1) 將影像分成 α 和 β 集合，並且對最後進行嵌入的集合開始進行取出。

(2) 計算像素標準差和排序。

(3) 取得嵌入時的門檻值，以第 3.2 節的方式對偽裝影像進行預測，並且產生直方圖。

(4) 取得嵌入時的峰值點 P 和零值點 Z。

I. 當 $P<Z$：

a. $e_{(i,j)}=P+1$，則 $e_{(i,j)}-1$，取出 $b=1$。

b. $e_{(i,j)}=P$，則 $e_{(i,j)}$ 不變，取出 $b=0$。

c. $P<e_{(i,j)} \leqq Z$，恢復誤差值 $e_{(i,j)}-1$。

II. 當 $P>Z$：

a. $e_{(i,j)}=P-1$，則 $e_{(i,j)}+1$，取出 $b=1$。

b. $e_{(i,j)}=P$，則 $e_{(i,j)}$ 不變，取出 $b=0$。

c. $P>e_{(i,j)} \geqq Z$，恢復誤差值 $e_{(i,j)}+1$。

(5) 最後，還原原始像素 $x_{(i,j)}=p_{(i,j)}-e_{(i,j)}$。

4. 實驗結果

本實驗使用 Matlab 7.10.0 (R2010a) 開發，實驗用 DICOM 醫療影像，來自於 aycan OsiriX^{PRO} 和 National Biomedical Imaging Archive (NBIA)免費醫療樣本影像，如圖 8 所示。

本研究使用 PSNR 為衡量機制進行比較。PSNR

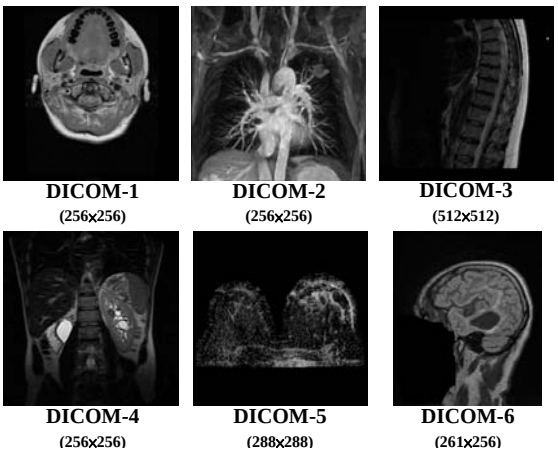


圖 8 測試影像

是用來測量藏入機密訊息後的影像和原始影像之間的差異，PSNR 數值越大，代表影像的品質越好。其公式如下：

$$PSNR = 10 \times \log_{10}\left[\frac{(ImageDepth)^2}{\frac{1}{mn}\times\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(x_{(i,j)}-x'_{(i,j)}\right)^2}\right] \text{(dB)}。\quad (6)$$

由於影像深度之不同，導致 PSNR 值的標準也會隨

著改變，就以往的經驗，8 位元影像的 PSNR 值要高於 28 dB 以上，偽裝影像品質才是可以被接受的。然而，16 位元影像的 PSNR 值標準就不再是 28 dB 以上，在實驗過程中發現，不同影像會有不同的 PSNR 值標準，有些偽裝影像在 PSNR 值低於 85 dB 以下時，已經與原始影像有些微的差異，像是白色部份會顯得更為光亮、胡椒點，或者是組織紋理的部份會被平滑化；但有些偽裝影像在 PSNR 值低於 80 dB 以下，仍然很難發現有被修改的跡象。因此，本研究假設醫療影像的 PSNR 值需要高於 90 dB 以上，才能被接受並且防止被第三者察覺。

4.1 自適性門檻值設定

為了提升預測的精確度，本研究利用標準差定義 2 個門檻值 T_1 和 T_2，以決定使用的預測方法。透過分析每張影像的標準差分佈情形，從圖 9 的醫療影像中可以發現，多數影像有較大的背景區，標準差峰值點會位於 0；而 DICOM-2 和 DICOM-4 屬於背景區較少的影像，因此標準差的峰值點分別落於 37 和 12。標準差越小，代表適合使用傳統 Lukac 方法進行預測。因此，本研究以此峰值點做為 T_1 的設定。而 T_2 會根據使用者需求決定，整張影像最多藏入多少訊息，即 T_2 設定其對應的標準差。

然而，所提方法會對同一張影像進行多次的嵌入，門檻值的設定會對不同的嵌入階段產生影響。故本研究假設 4 種門檻值設定方式，分別為：

(1) Method-1：以整張影像產生門檻值，並且使用於所有的嵌入階段。

(2) Method-2：以整張影像產生 T_1，T_2=100%。

(3) Method-3：各嵌入階段都重新計算門檻值，門檻值不會互相影響。

(4) Method-4：以首次嵌入得到的門檻值，使用於各嵌入階段。

上述方法除了 Method-2 會對所有像素值進行預測和嵌入外，即 T_2=100%，其他 3 種方法 T_2 都設定為 80%的像素個數。除了 Method-3 以外，其它 3 種方法都是使用相同標準差門檻值進行多次嵌入，為了避免提取時發生錯誤，必須額外記錄 T_1 和 T_2。

4.2 藏入量和影像品質

本實驗使用第 4.1 節的兩種門檻值設定方式與其他學者提出的方法進行藏入量和 PSNR 值比較，一種是影像品質較佳的 Method-1，另一種是藏入量

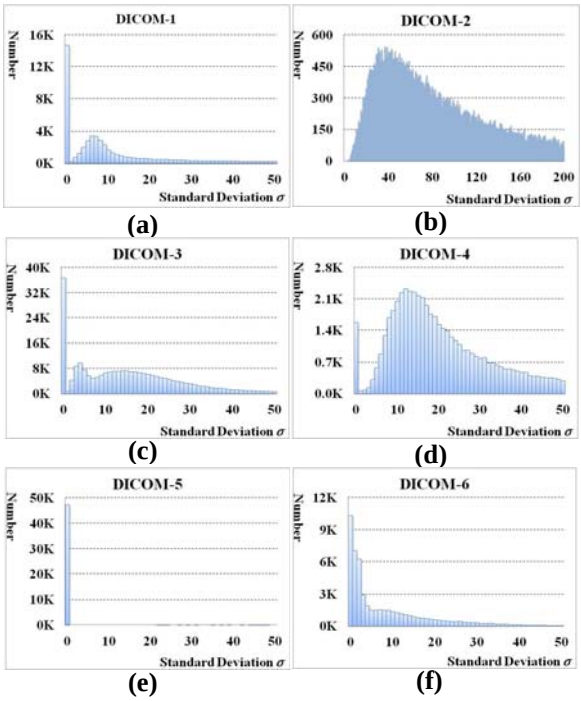


圖 9 DICOM 醫療影像之標準差分佈圖

表 1 嵌入 4 次訊息後的 PSNR 和藏入量比較

DICOM-1	turn-2		turn-4		Total bpp
	Capacity	PSNR	Capacity	PSNR	
Ni et al.	24,465	94.80	38,819	89.32	0.59
Tian	65,536	62.69	131,072	54.92	2.00
Lukac et al.	16,250	99.39	24,305	93.39	0.37
Feng & Fan	14,767	99.09	21,287	96.86	0.32
Method-1	16,240	102.24	24,415	96.35	0.37
Method-3	16,850	100.34	25,289	95.57	0.39
DICOM-2	turn-2		turn-4		Total bpp
	Capacity	PSNR	Capacity	PSNR	
Ni et al.	384	118.85	623	114.29	0.01
Tian	65,536	48.34	131,072	41.01	2.00
Lukac et al.	788	99.47	1,533	94.72	0.02
Feng & Fan	984	99.55	1,813	93.49	0.03
Method-1	759	102.33	1,397	97.73	0.02
Method-3	906	100.31	1,658	94.23	0.03
DICOM-3	turn-2		turn-4		Total bpp
	Capacity	PSNR	Capacity	PSNR	
Ni et al.	101,190	94.71	159,525	89.49	0.61
Tian	262,144	62.21	524,288	56.54	2.00
Lukac et al.	45,559	101.32	87,881	95.43	0.34
Feng & Fan	39,162	100.07	65,985	97.16	0.25
Method-1	44,884	105.87	87,768	100.15	0.33
Method-3	46,653	102.74	90,497	96.89	0.35
DICOM-4	turn-2		turn-4		Total bpp
	Capacity	PSNR	Capacity	PSNR	
Ni et al.	4,572	94.50	7,161	89.41	0.11
Tian	65,536	60.15	131,072	53.83	2.00
Lukac et al.	3,372	99.76	5,998	94.98	0.09
Feng & Fan	3,186	99.44	5,338	94.90	0.08
Method-1	3,040	102.75	5,556	96.85	0.08
Method-3	3,423	100.64	6,138	94.68	0.09
DICOM-5	turn-2		turn-4		Total bpp
	Capacity	PSNR	Capacity	PSNR	
Ni et al.	80,225	96.46	126,979	91.93	1.53
Tian	82,944	40.21	165,888	34.45	2.00
Lukac et al.	46,817	99.66	69,441	97.62	0.84
Feng & Fan	39,333	99.47	53,779	95.16	0.65
Method-1	47,441	101.44	70,072	96.27	0.84
Method-3	47,891	100.98	71,019	97.12	0.86
DICOM-6	turn-2		turn-4		Total bpp
	Capacity	PSNR	Capacity	PSNR	
Ni et al.	15,862	93.95	25,150	89.20	0.45
Tian	55,296	71.19	110,592	64.08	1.66
Lukac et al.	13,546	100.86	25,450	95.78	0.46
Feng & Fan	12,012	99.55	19,883	96.85	0.36
Method-1	12,743	105.39	24,162	99.46	0.44
Method-3	13,680	102.14	25,624	96.15	0.46

和 PSNR 值介於 Method-1 與 Method-2 的 Method-3。表表 1 為藏入 4 次後之比較。

在 DICOM 醫療影像的表現上，Ni 學者的方法在多數影像上能夠維持高藏入量和 PSNR 值，原因在於多數醫療影像的背景區非常多。Tian 學者的方法嵌入量非常高，因為溢位問題只會發生向下溢位，太多的區塊符合嵌入訊息的條件。Lukac 方法在多數影像下的藏入量會比 Feng 的方法還要好，但是當影像太過於複雜時（如圖 9-(b)），藏入量會比適合預測複雜影像的 Feng 方法還低。而本研究方法在 PSNR 值高於 95 dB 的情形下，藏入量明顯高於其他方法；然而，在 DICOM-4 影像的藏入量只有些微的贏過其他方法，主要原因在於該影像的複雜度過高（如圖 9-(d)），標準差的峰值點位於較為複雜的數值，故預測精確度降低導致藏入量變少；DICOM-2 影像也是相同的情況，藏入量的表現並不顯著。

5. 結論

本研究提出一個改良 Feng 和 Fan 學者的延伸 Lukac 方法，透過標準差分析每個區塊的複雜度，並且使用不同方法進行預測。然而，門檻值設定會受到不同標準差統計方式影響，故本研究將標準差統計分為 2 種類型，一種是以全部像素為基礎計算標準差，另一種是用一半像素為基礎計算標準差。實驗結果顯示，本研究方法可以有效提升複雜影像的 PSNR 值，並且維持一定水準的藏入量，尤其是在 16 位元醫療影像上的表現更為顯著，在預測越精確的情況下，可以提升預測峰值點和藏入量。

參考文獻

[1] O.M. Al-Qershi and K.B. Ee., "Authentication and Data Hiding Using a Reversible ROI-Based Watermarking Scheme for DICOM Images," *Proceedings of World Academy of Science: Engineering and Technology*, Vol. 50, pp. 801-806, 2009.

[2] O.M. Al-Qershi and B.E. Khoo, "High Capacity Data Hiding Schemes for Medical Images Based on Difference Expansion," *The Journal of Systems and Software*, Vol. 84, pp. 105-112, 2011.

[3] O.M. Al-Qershi and B.E. Khoo, "Two-Dimensional Difference Expansion (2D-De) Scheme with a Characteristics-based Threshold," *Signal Processing*, Vol. 93, pp. 154-162, 2013.

[4] G. Feng and L. Fan, "Reversible Data Hiding of High Payload Using Local Edge Sensing Prediction," *The Journal of Systems and Software*, Vol. 85, pp. 392-399, 2012.

[5] L.C. Huang, L.Y. Tseng, and M.S. Hwang "A Reversible Data Hiding Method by Histogram Shifting in High Quality Medical Images," *The Journal of Systems and Software*, Vol. 86, pp. 716-727, 2013.

[6] D.C. Lou, M.C. Hu, and J.L. Liu "Multiple Layer Data Hiding Scheme for Medical Images," *Computer Standards and Interfaces*, Vol. 31, pp. 329-335, 2009.

[7] R. Lukac, K. Martin, and K.N. Plataniotis, "Digital Camera Zooming Based on Unified CFA Image Processing Steps," *IEEE Transactions on Consumer Electronics*, Vol. 50, pp. 15-24, 2004.

[8] Z. Ni, Y.Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 16, No. 3, pp. 354-362, 2006.

[9] O.S. Pianykh, Digital Imaging and Communications in Medicine (DICOM): A Practical Introduction and Survival, *Springer*, 2012.

[10] J. Tian, "Reversible Data Hiding Using a Difference Expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 13, No. 8, pp. 890-896, 2003.

[11] W.J. Yang, K.L. Chung, H.Y. Liao, and W.K. Yu, "Efficient Reversible Data Hiding Algorithm Based on Gradient-based Edge Direction Prediction," *The Journal of Systems and Software*, Vol. 86, pp. 567-580, 2013.

[12] C.h. Yang and M.H. Tsai, "Improving Histogram-Based Reversible Data Hiding by Interleaving Predictions," *IET Image Processing*, Vol. 4, No. 4, pp. 223-234, 2010.

使用 URL Routing 與 Web Storage 防禦跨站冒名請求攻擊

劉書宇　　吳其哲　　丁建文
國立高雄應用科技大學 資訊管理研究所
{f126882231,jerryclass, jenwen.ding}@gmail.com

摘要

近年來網際網路資訊的發展與行動設備的普及，生活中越來越多的資訊與活動都在網路上流通與進行，以網站為基礎的網站應用程式(Web Application)更是蓬勃發展，但由於 HTTP 有著無狀態(stateless)的特性，因此易造成伺服器與用戶端(Broswer)之間的關聯薄弱與驗證不足等，使得網站經常為駭客攻擊的目標，其中的跨站冒名請求攻擊(Cross site request forgery)為最常見的攻擊方式之一，駭客將惡意程式碼嵌入攻擊者或被攻擊者的伺服器網頁中，使得瀏覽者遭到如 session riding 與 session hijacking 等冒用使用者身分的攻擊。

在本論文中將深入討論當前和未來網路的安全性，並針對跨站冒名請求攻擊提出了一套針對使用者的網址變化機制，研究中利用 HTML5 新制定的 Web Storage 來儲存多組使用者登入成功時所取得的多組 UUID API Key，並在使用者操時時將網址與 UUID API Key 結合後作為請求網址發送至伺服端，當伺服端接收到後便可透過 URL Routing 之機制將鍵值取出並與 Server 端的資料做比對，以此達到使用者 Cookie 與 UUID API Key 的雙重認證機制。

關鍵詞：跨站冒名請求、網址路由、通用唯一識別碼、HTML5、Web Storage

Abstract

In recent years, the development of Internet information and the popularity of mobile devices, more and more information and activities are working on the Internet and besides, web applications are booming in our life. However, HTTP is a stateless protocol. Therefore, the linking between the server and the client verifying is weak and inadequate to make the hackers target these sites. One of the most common attacks is Cross Site Request Forgery; Hackers would embed malicious code into the attacked person's web server. Then, viewers are attacked such session riding and session hijacking and other fraudulent attack by using of user identity.

In the research, we would discuss deeply the current and future network security and propose a set of URL change mechanism focusing on the Cross Site Request Forgery attack. Using newly Web Storage to store multiple UUID API Keys from many sets of successful user-login is based on HTML 5 in the research. Besides, while users operate to login into the sites, combining the site and UUID API Key is as a request URL which is sent to the server.

When the server receives the URL, it can compare the data from the server through URL Routing mechanism to achieve the two-factor authentication mechanism based on user cookie and UUID API Key.

Keywords: Cross site request forgery, URL Routing, UUID, HTML5, Web Storage

1. 前言

根據網路安全專家研究，跨站冒名請求攻擊(Cross site request forgery)為過去十年中最為嚴重和常見的威脅之一，並分被標註在 CWE(Common Weakness Enumeration)清單與 OWASP(Open Web Application Security Project)清單中(圖 1)，且多個主要網站包含 Facebook、Twitter、eBay、Google 和 McAfee 皆已成為跨站冒名請求攻擊的目標。

跨站冒名請求攻擊是屬於許多網頁應用程式所固有的弱點，主要發生原因為網站應用程式對於使用者的請求缺乏檢查或認證不足，且在任何不同的語言如 PHP、JSP 和 ASP.NET 等都存在著，攻擊者通過這些漏洞注入惡意代碼，而導致意想不到的惡意命令從客戶端瀏覽器執行[1,2]。

雖然許多研究人員已經提出了多種跨站冒名請求攻擊(Cross site request forgery)的緩解機制，包含請求方法的更改、使用者來源的認證與代理伺服器的使用等，但由於網頁應用程式開發者缺乏對跨站冒名請求攻擊的理解與技術上的侷限，跨站冒名請求攻擊的漏洞依然廣泛的存在。

本研究提出的安全機制主要以 HTML5 的 Web Storage 與伺服端網址路由(URL Routing)的技術為基礎，利用 HTML5 Web Storage 相較於 Cookie 擁有更高安全性與更大儲存空間的特性來儲存多組獨一無二的 UUID API Key，並與請求網址(URL)做結合以產生使用者專用的請求連結位置，以達到每位使用者的網址獨特性，最後再透過 Server 端的網址路由(URL Routing)技術取出 UUID API Key，達到 UUID API Key 與 Cookie 的雙重認證，使得使用者的網路環境更加安全。

OWASP TOP 10 – 2013
A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control
A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards

圖 1 OWASP 十大網路威脅[3]

2. 文獻探討

2.1 Cookie

由於 HTTP 是基於請求與回應的無狀態協定，因此當客戶端每一次的請求與伺服端的回應結束之後伺服端便會遺忘曾與客戶端間有過的任何互動，若沒有 Cookie 與 Session 的概念存在的話客戶端每次連線到伺服端都會被當成是一個新的連接，因此 Cookie 與 Session 的發明便是為了保持客戶端與伺服端間的連續性與狀態儲存[4，5]。

如圖 2 所示，當客戶端造訪至一個擁有 Cookie 機制之網站時，伺服端便會透過 HTTP 標頭與瀏覽器將 Cookie 儲存至客戶端的硬碟或記憶體之中，接著在客戶端之後的 HTTP 請求中，伺服端便會透過瀏覽器送出的 HTTP 標頭檢索客戶端擁有之 Cookie 並取得相關訊息以進行後續之服務，而不要求相同之訊息。

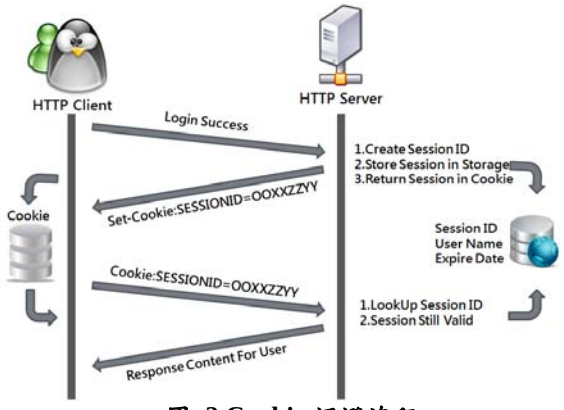


圖 2 Cookie 認證流程

2.1.1 Cookie 威脅

Cookie 的威脅主要有三種類型：網路威脅、系統威脅與竊取威脅，且三種威脅都相當容易實現[6]。首先網路威脅是由於大部分之 Cookie 是以明文的形式在網路上傳輸的，因此 Cookie 是相當容易遭到監聽與解讀，雖然 SSL[7]的出現能增加 Cookie 之安全性，但此安全性也僅限於在網路上傳輸時。其次系統威脅是由於 Cookie 是儲存在客戶端電腦之硬碟或記憶體中，因此夠在系統能夠輕易地修改內容或將其複製至其他電腦中，這使得攻擊者將能偽造訊息或冒充他人身分。最後竊取威脅為若攻擊者在網站中嵌入惡意之請求，該攻擊者便可透過此攻擊竊取使用者之 Cookie 以達到身分偽造之目的。

2.2 跨站冒名請求攻擊

跨站冒名請求攻擊(Cross site request forgery)是相較於跨站腳本攻擊(Cross site scripting)是屬於比較新的網路安全議題[8]，跨站冒名請求攻擊(Cross site request forgery)透過網站對客戶端下達任意有漏洞的 HTTP 請求以達到攻擊的目的，若此時受害者已通過該 HTTP 請求之認證，跨站冒名請求攻擊(Cross site request forgery)便能繞過該 HTTP 請求之身分認證機制並進行攻擊，根據攻擊的方式，將可能會造成受害者在不知情的情況下發布消息或郵件，而更嚴重時甚至會更改受害者之資料如姓名或密碼等，但不幸的是相較於跨站腳本攻擊(Cross site scripting)與隱碼注入(SQL Injection)攻擊，跨站冒名請求攻擊(Cross site request forgery)之防禦是網頁開發者中鮮少會去注意到的[9]。

2.2.1 跨站冒名請求攻擊方式

跨站冒名請求攻擊(Cross site request forgery)主要是利用伺服端透過 Cookie 儲存在客戶端的 Session ID，其原因為瀏覽器會自動在 HTTP 請求時加入 Cookie，因此在不論是在超連結的點擊或是網頁的重新導向情況下，該 HTTP 請求皆會正確的被觸發，相對的若遭跨站冒名請求攻擊的客戶端不包含驗證所需的 Cookie，則該跨站冒名請求攻擊(Cross site request forgery)便會失敗。

其中最常見的跨站冒名請求(Cross site request forgery)攻擊方式是利用 HTML 中如<Script>、<Image>或<iframe>等有能力發出 HTTP 請求之標籤，如圖 3 所示跨站冒名請求攻擊(Cross site request forgery)強迫使用者的瀏覽器自動對於該目標網址發出請求，導致該頁面的瀏覽者受到資料竄改(Web Content Manipulation)等攻擊，其他典型的跨站冒名請求攻擊(Cross site request forgery)方式還有透過超連結網址(URL)、表單(Form)、JavaScript、VBScript 和 Flash 等[1]。

與跨站腳本攻擊(Cross site scripting)相較之下，跨站冒名請求攻擊(Cross site request forgery)攻擊的目的不是為了取的使用者的資料，而是利用伺服端無法分辨用戶的請求真假特性，欺騙伺服器而導致使用者的行為與權限遭到濫用。

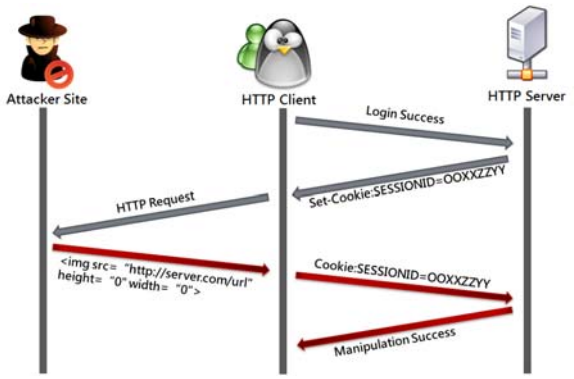


圖 3 跨站腳本攻擊流程

2.2.2 現存防禦跨站冒名請求攻擊機制

防禦跨站冒名請求攻擊(Cross site request forgery)最為簡單的方式便是將 HTTP 請求的方法由 GET 改為 POST，然而這種防禦的方式經實驗證明，只是提高了跨站冒名請求攻擊(Cross site request forgery)的攻擊門檻，如避免一些特定的攻擊方式如利用<image>、<iframe>標籤等，此外若想將網站的 HTTP 請求方式完全改為 POST 是不可能的，因為這將導致網站的程序複雜與網頁開發者的難以實現[9]。

另外防禦跨站冒名請求攻擊(Cross site request forgery)的方式還有透過驗證瀏覽器所產生的 HTTP 標頭 Referer，Referer 的內容為客戶端在發出此 HTTP 請求時瀏覽器所在的頁面網址，因此透過此 Referer 伺服端便可進一步判斷是否要接受來自此 Referer 的 HTTP 請求，以銀行的交易網站為例，若該 Referer 的網址不再伺服端接受的白名單內，則會拒絕此 HTTP 請求並中斷交易，但不幸的是由於此 Referer 是很容易偽造並有可能會洩漏個人隱私資料的，因此大部分的瀏覽器為了不洩漏該使用者的隱私資料，當客戶端發出 HTTP 請求時大多會以空值送出，導致開發者若採用此跨站冒名請求攻擊(Cross site request forgery)防禦機制，勢必會造成客戶端瀏覽器的限制，進而影響使用者的操作意願[11,12]。

而金鑰交換為迄今最常使用的跨站冒名請求攻擊(Cross site request forgery)解決方案，其為透過在伺服端與客戶端兩地儲存由應用程序產生不容易遭到猜測的共同金鑰代碼，並在客戶端 HTTP 請求發生時將此代碼包含在送出的變數中，以供伺服端比對是否與客戶端的金鑰代碼相同，若金鑰相同則執行正確的 HTTP 回應。而此方法的缺點為開發者所需投入的開發成本較高，因為採用金鑰交換機制須建立龐大且複雜的金鑰管理機制，且需修改每個採用金鑰交換機制的 HTTP 處理器，而若開發者還採用更加複雜的一次性密碼(One Time Password)機制，除了開發成本的更加提高外也會大幅將低客戶端操作之彈性[10]。

最後防禦跨站冒名請求攻擊(Cross site request forgery)的方式還有透過代理伺服器(Proxy)，此方式的防禦方法為透過另外一台伺服器去擴展原有伺服端的功能，進而達到伺服端對客戶端進一步的掌握，以阻絕所有開發者認為不正當或惡意的操作可能，而此減輕機制最為重要的條件為開發者需要建立代理伺服器與伺服端間的完整的關聯，因此相較於前幾項跨站冒名請求攻擊(Cross site request forgery)的防範機制，使用代理伺服器勢必也將造成開發者投入的開發成本更為增加[10]。

2.3 HTML5 Web Storage

HTML5 中提供了一個類似於 Cookie 的 HTML5 Web Storage 儲存機制，提供伺服器端能夠在客戶端儲存鍵值與變數，並且提供了簡單的函數來達成新增、修改、刪除和查詢之功能。然而不同於 Cookie 的是 HTML5 Web Storage 並不會透過 HTTP 請求而自動送出，如圖 4 所示 HTML5 Web Storage 所有的控制與儲存皆是透過 Javascript 腳本做操作。另外相較於 Cookie，最大的優點就是不需要持續地發送至伺服端做驗證。

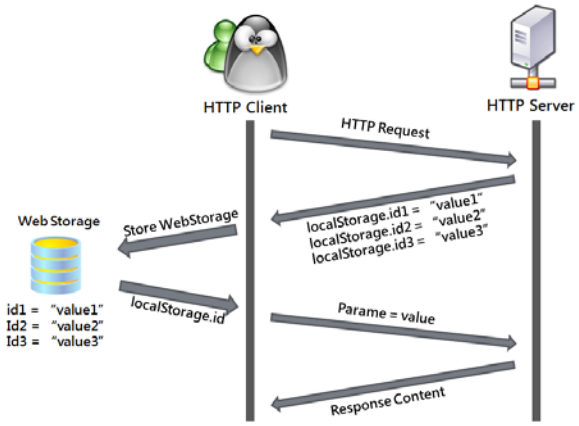


圖 4 HTML5 Web Storage 流程

2.3.1 HTML5 Web Storage 隱私

由於持久性的 Cookie 造成有關隱私上的相關問題，因此 HTML5 Web Storage 規範提供了相似於 Cookie 的替代品 Web Storage 使得客戶端能對資料能有更佳的控制。以網頁中呈現的背景顏色為例，若在沒有使用 HTML5 Web Storage 的情況下，伺服端需在資料庫中或 Cookie 中儲存使用者之偏好之背景顏色，並且在 HTTP 請求中不斷的送出與驗證該客戶端背景顏色之資料，此時便會有洩漏資料之

問題，但若改為使用 HTML5 Web Storage 來存取該背景顏色資料時，便能將修改與驗證之機制都留在客戶端處理，同時也能減少資料走漏之風險 [13]。

2.4 網址路由

網址路由在伺服端中主要有兩個目的，分別是比對並處理客戶端透過瀏覽器送出的 HTTP 請求與回應適當的回應給瀏覽器，以 MVC 架構為例，瀏覽器會將 HTTP 請求轉換成封包並發出 HTTP 請求到伺服端上，此時伺服端之網址路由便會取得該請求之路由值，並由上而下比對網址路由表中所有路由規則來選擇最適合之路由規則後交由網址路由模組判定此請求要交由哪個 HTTP 處理器處理，如伺服端判定是由 MVC 處理器來處理，那就會讓 HTTP 請求進入 MVC 的執行週期，最後再提供適當的回應給客戶端[14]。

此外網址路由中也可以自行定義路由參數與路由值，如圖 5 所示，開發者在路由表中定義了 Controller、Action 與 Parame 之路由參數，但由於 Parame 在路由表中非屬於 MVC 處理器的路由參數之一，因此 Parame 所屬的路由值"123" 就會自動被轉換成查詢參數的一部分。

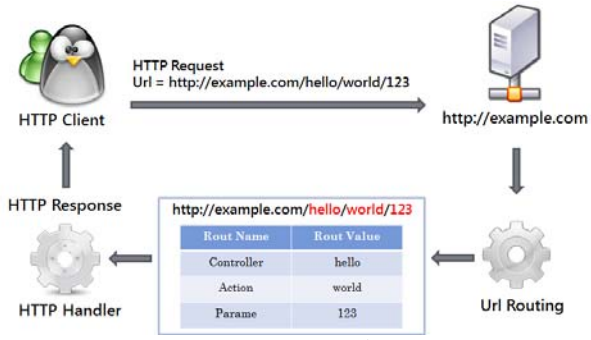


圖 5 網址路由流程

2.5 通用唯一識別碼 UUID

通用唯一標識別碼 UUID(Universally Unique Identifier)也被稱為全局唯一識別碼 GUID(Globally Unique Identifier)，是一種在沒有中央系統的情況下還能保證唯一性之規範。使用通用唯一標識別碼 UUID 主要的原因之一是希望在沒有權利管理其他系統的情況下，能產生獨立之鍵值並用於各種用途如做交易之鍵值等，如此一來每個人都可以不與其它人衝突，進而解決名稱或 ID 重複之問題[15]。

一組通用唯一標識別碼 UUID，是由一串 16 位元組(128 位元)的 16 進位數字所構成，是故通用唯一標識別碼 UUID 的總數為 2 的 128 次方，也就是說若每奈秒產生 1 兆個 UUID，則要花 100 億年才會將所有的 UUID 用完，其中通用唯一標識別碼 UUID 的標準型式包含 32 個16 進位數字，以連號分為五段，形式為 8-4-4-4-12 的 36 個字元如 08dac2f1-e4c4-4cea-a202-7e480affe859，而其他重要的應用，則有 Linux ext2/ext3 檔案系統、LUKS 加密分割區、GNOME、KDE 和 Mac OS X 等。

3. 系統架構與設計

本研究提供一套跨站冒名請求攻擊(Cross site request forgery)防禦機制，以網址路由(URL Routing)與 HTML5 Web Storage 為基礎，首先在使用者登入成功時於伺服端 Session 和客戶端 HTML5 Web Storage 儲存多組使用者專屬之 UUID API Key，這些 UUID API Key 主要目的為供使用者用於敏感性之連結如有關資料庫新增、修改、刪除、查詢等，使用者在後續的操作時將會將此些 UUID API Key 加入 API 網址並作為請求的網址中送出 HTTP 請求，傳送至伺服端後伺服端便可透過網址路由(URL Routing)之機制從路由值中取得使用者之 UUID API key 與所對應之 API，再透過 Cookie 機制取得使用者之 Session 做兩者 UUID API Key 之比對，若使用者 Session 之內容 UUID API Key 與使用者 HTTP 請求之 UUID API Key 相同，便做出正常的 HTTP 回應，反之若兩者不同則 HTTP 回應請求失敗，並於伺服端執行比對失敗時之機制如清除 Session 等。

3.1 客戶端登入機制

圖 6 為當使用者在登入成功後，伺服端會除了建立使用者所需的 Session 外還會建立使用者專用之 UUID API Key 並儲存於伺服端之 Session 與客戶端之 HTML5 Web Storage 中，以供客戶端在之後的 HTTP 請求中做為 UUID API Key 使用。

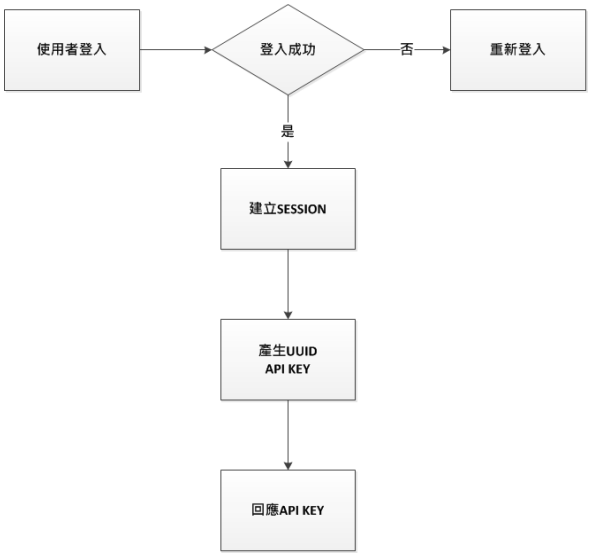


圖 6 客戶端登入流程

3.2 伺服端認證機制

圖 7 為當客戶端發出 HTTP 請求時，伺服端會除了使用 Cookie 驗證使用者的身分外，還會透過網址路由判斷客戶端 HTTP 請求所使用的 API 網址是否包含正確的 UUID API Key 以達到雙重認證的效果，以本流程圖為例，若當使用者的 UUID API Key 未通過伺服端認證時，便會清除該 Cookie 所屬之 Session，並導客戶端導向致重新登入之介面。

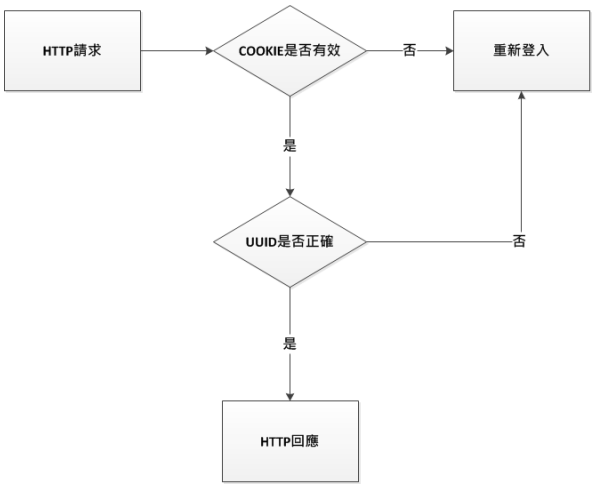


圖 7 伺服端認證流程

3.3 客戶端對伺服端請求機制

圖 8 為在本研究架構下，客戶端登入成功時伺服端除了以傳統 Cookie 認證之機制建立 Session 之外，也將創建符合敏感 API 數量之 UUID API Key 並儲存於伺服端 Session 與客戶端的 HTML5 Web Storage 中，接著在客戶端之後的 HTTP 請求裡，若有用到需要 UUID API Key 之 API 網址時，便會將該 API 網址與專屬之 UUID API Key 做結合做作請求之網址，當該請求被送至伺服端時，伺服端便會透過網址路由之機制，判斷該 UUID API Key 是否為該客戶端所屬，並根據認證之情形回應內容。

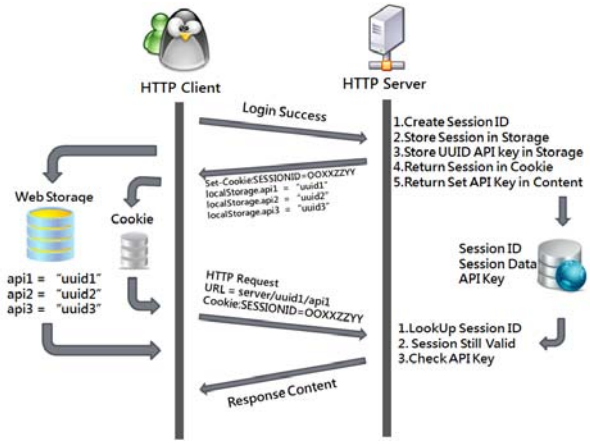


圖 8 HTTP 請求流程

3.4 跨站冒名請求攻擊之防禦

圖 9 為客戶端以正常之方式登入並驗證成功後，取得受認證之 Cookie 與多組 UUID API Key，接著在登入成功並取得認證後雖然遭遇到跨站冒名請求攻擊(Cross site request forgery)，但由於跨站冒名請求攻擊之攻擊者並無法事先得知客戶端之專屬 UUID API Key，而導致雖然 Cookie 認證通過了而 UUID API Key 認證卻失敗的結果，進而導致跨站冒名請求攻擊失敗。

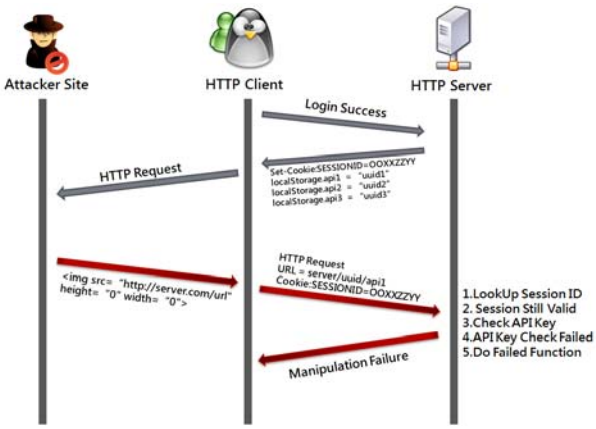


圖 9 跨站冒名請求防禦流程

4. 安全與效能評估

在安全與效能評估中，主要探討在本研究架構與舊有架構相比之下，對客戶端與伺服端所造成之效能影響與安全之改善。

4.1 效能評估

4.1.1 優點

由於 HTML5 Web Storage 不同於 Cookie 不會將資料附加在每一個 HTTP 請求中，而是只在被使用時才被截取並傳送至伺服端，因此相較於將資料存在 Cookie 上的方法對於伺服端與客戶端的流量都將有相當大幅度之改善，另外由於同時也減少伺服端之資料處理量。

4.1.2 缺點

1.由於本研究架構在伺服端加入了網址路由之機制(URL Routing)，因此對於伺服端來說增加了實體路徑搜尋與路由表對照之處理時間，但此時間消耗能透過對於網址路由機制的搜尋順序進行優化。而在本研究中，透過實驗比較正常實體路徑搜尋與網址路由(URL Routing)的機制，在同樣回傳空白網頁的情況下網址路由(URL Routing)機制大約

只比實體路徑搜尋多了 1m 秒的延遲。

2.本研究系統架構在使用者登入成功的當下，將會產生所有需認證之 API 所需的 UUID API Key，因此當採用本機制之 API 網址逐漸增加時，伺服端之運算量也會隨之增加。其圖 8 為本研究實驗在伺服端 CPU 為 Intel(R) Core(TM)2 Quad CPU Q9500 的條件下，當客戶端請求發生時，伺服端產生 UUID 從 0 到 50000 筆並回應客戶端所需之時間。

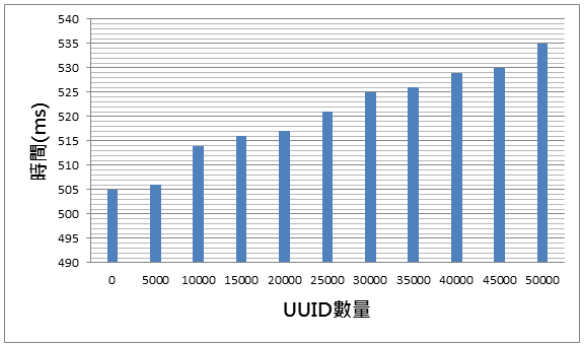


圖 8 UUID 數量與時間之影響

3. 本研究系統架構在使用者登入成功之後，會將所有產生之 UUID API Key 儲存一份在 Session 以供後續之認證與比對，因此當採用本機制之 API 網址逐漸增加時，伺服端 Session 所需之容量負擔也將會隨之成長。

4.2 安全性評估

4.2.1 優點

1.造成跨站冒名請求攻擊(Cross site request forgery)主要的原因為所有的網站使用者皆使用相同之 API 網址，因此導致駭客能在網頁中嵌入指定之 API 網址以進行特定之攻擊，而本研究系統架構則利用 HTML5 Web Storage 與網址路由企圖改善此本漏洞，期望能阻絕大部分之跨站冒名請求攻擊(Cross site request forgery)。

2.本研究系統架構遭駭客監聽時，由於每組 UUID API Key 是無關聯並且獨一無二的，因此若駭客想取得該使用者完整的控制，勢必需要投入更長的時間與心力。

4.2.2 缺點

由於 HTML5 Web Storage 可供所屬之 Domain 網站存取與控制，因此採用本研究架構之網站若擁有跨站腳本攻擊(Cross site scripting)等重大網頁漏洞，則本研究架構將極有可能遭到破解。

5. 結論

隨著網路技術的快速發展，網路安全的議題也勢必會變得更加重要，而在常見的網路攻擊上，跨站冒名請求攻擊(Cross site request forgery)相較於跨站本攻擊(Cross site Scripting)和隱碼注入攻擊(SQL Injection)，是網站開發者較為陌生或尚未注意的部分，故本研究預期在網路安全越來越重要的未來，跨站冒名請求攻擊(Cross site request forgery)必定會會到更高的重視，因此提出此系統架構。

本研究系統架構相較於其他相關研究的不同主要在於開發者實作的容易性上，大部分過去的相關研究大多都存在的開發成本與實作難度較高的問題，因此本研究從跨站冒名請求攻擊(Cross site request forgery)的原理著手，透過建立每位使用者的網址獨特性，提出了一個架構簡單的解決方案，試圖大幅減少客戶端遭受跨站冒名請求攻擊之機率，希望能為網路的安全盡一份心力。

參考文獻

[1] Siddiqui, M. S., & Verma, D. (2011, May). Cross site request forgery: A common web application weakness. In Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on (pp. 538-543). IEEE.

[2] Shahriar, H., & Zulkernine, M. (2010, November). Client-side detection of cross-site request forgery attacks. In Software Reliability Engineering (ISSRE), 2010 IEEE 21st International Symposium on (pp. 358-367). IEEE.

[3] Open Web Application Security Project,accessed on May 2013 from https://www.owasp.org/https://www.owasp.org/index.php/Top_10_2013

[4] Kristol, D. M., & Montulli, L. (2000). HTTP state management mechanism.

[5] Moore, K., & Freed, N. (2000). Use of HTTP state management. RFC 2964, Network Working Group.

[6] Nescape. Persistent Client State: HTTP Cookies. http://wp.netscape.com/newsref/std/cookie\ _spec. html.

[7] Wagner, D., & Schneier, B. (1996, November). Analysis of the SSL 3.0 protocol. In The Second USENIX Workshop on Electronic Commerce Proceedings (pp. 29-40).

[8] Schreiber, T. (2004). Session riding-a widespread vulnerability in today's web applications. Whitepaper, SecureNet GmbH.

[9] Chris S. (2003). Foiling Cross-Site Attacks. PHP Architect Magazine.

[10] Jovanovic, N., Kirda, E., & Kruegel, C. (2006, August). Preventing cross site request forgery attacks. In Securecomm and Workshops, 2006 (pp. 1-10). IEEE.

[11] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., & Berners-Lee, T. (1999). Hypertext transfer protocol–HTTP/1.1.

[12] Johns, M., & Winter, J. (2006, May). RequestRodeo: Client side protection against session riding. In Proceedings of the OWASP Europe 2006 Conference.

[13] West, William, & Pulimood, S. Monisha. (2012). Analysis of privacy and security in HTML5 web storage. J. Comput. Sci. Coll., 27(3), 80-87.

[14] Sanderson, S. (2010). Pro Asp. net MVC 2 Framework. Apress.

[15] Leach, P. J., Mealling, M., & Salz, R. (2005). A universally unique identifier (uuid) urn namespace.

ARP Spoofing 偵測及防護機制-以 Arcai Netcut 軟體為例

王永鐘　王宜秀
國立臺北科技大學　計算機與網路中心
國立臺北科技大學　電機工程系
ycwang@ntut.edu.tw　t100318117@ntut.edu.tw

摘要

Address Resolution Protocol (ARP)是電腦主機用以轉換網路位址(IP Address)至實體位址(MAC address)的網路協定，ARP spoofing 則藉由 ARP 沒有防護機制的弱點而產生的網路攻擊手法，例如在區域網路發動 Denial of Service (DoS) 及 Man In The Middle (MITM)攻擊，ARP 的缺點所造成的網路攻擊不但可能會癱瘓網路運作，甚至個人資料也會透過 ARP spoofing 而被竊取。本論文以 ARP spoofing 軟體為研究對象，分析 Arcai Netcut 軟體運作原理及其造成的網路影響，並建立一套分散式架構、快速、有效、低成本的自動偵測及防護 Arcai Netcut 解決方案，本研究整合 Command-Line Interface (CLI) 功能及各式 Linux scripts，本系統已成功運作於學生宿舍網路及校園網路並有效偵測及防護 Arcai Netcut。

關鍵詞：ARP spoofing、DoS、MITM、Arcai Netcut

Abstract

Address Resolution Protocol (ARP) is one of heavily used protocols by computers for mapping network address (IP address) to physical address (MAC address). ARP spoofing is a deception within the LAN caused by ARP flaws, which is used to launch Denial of Service (DoS) and Man In The Middle (MITM) by attackers. ARP flaws could cause the network paralyzed and even worse personal information stolen through ARP spoofing attack. In this paper, we analyzed the process and the effect of the common ARP spoofing software called Arcai Netcut. A distributed, swiftly, effective, and low cost solution, which could automatically detect and defense the Arcai Netcut is implemented on Linux Mini PC. We combined the functions of Command-Line Interface (CLI) and some different Linux scripts to develop the software, which succeed in detecting and defensing the Arcai Netcut in the student dormitory network and campus network.

Keywords: ARP Spoofing、DoS、MITM、Arcai Netcut

1. 前言

隨著網路應用服務愈來愈多元，其中影音訊務頻寬需求愈來愈大，當網路壅塞時，不少網路使用者便嘗試上網尋求可提高網路連線速度的方法，或者使用可影響其他網路使用者的軟體；若是採用調整區域網路架構、從集線器(hub)改用交換器(switch)或者調整作業系統設定值等方式都是正確且不影響他人的作法，但是對電腦網路運作知識不了解的人，可能會誤用含有網路惡意行為的軟體，例如 Arcai Netcut 軟體便是其中之一[1]，該軟體運作機制即是 ARP spoofing[2]，程式啟動後對同網段中其他電腦發動 Denial of Service (DoS)[3]攻擊，使其他電腦無法取得正確 gateway MAC 位址而無法上網，但是 Arcai Netcut 軟體使用者卻可以正常上網，原作者還提供 Netcut Defense 軟體來防禦 Arcai Netcut 攻擊，如此矛盾的兩款軟體，造成骨幹網路充斥大量 ARP 封包，使骨幹網路設備 CPU 使用率快速上升，在骨幹網路設備相當忙碌的狀態下產生 packets drop 及網路斷斷續續的現象。

Arcai Netcut 使用者大多位於共享網路頻寬的學生宿舍網路及校外租屋環境，有時為了保障自身使用網路頻寬的權益，有時為了阻止其他佔用網路頻寬進行大量下載的使用者，不管是以何種原因安裝 Arcai Netcut 軟體，一旦在區域網路內運行 Arcai Netcut，立即會使區域網路變得壅塞及忙碌。

目前已有不少針對 ARP spoofing 弱點而提出的解決方案[4]，大致上分為三類，一、加密式 IP/MAC[5]、二、Host-based[6]、三、Server-based[7]；不論是以非對稱式加密將 ARP 封包進行交換，或是在個人電腦安裝 Agent 程式，甚至以集中式控管所有 ARP 封包的方式，大多需要在 PC 端安裝程式或進行電腦參數的調整；本研究以不影響住宿學生的電腦環境，卻又能在短時間發現 Arcai Netcut 的運作，並且有效阻止 Arcai Netcut 所造成的網路不良影響為目標，著手進行各種可能的解決方案。

本文之架構如下：第二章簡介 Address Resolution Protocol(ARP)的運作原理；第三章簡介數個可以有效防禦 ARP spoofing 的系統，以及這些系統的優缺點；第四章為系統設計，詳細介紹本研究的作法及運作流程，並且展示實際應用於學生宿舍網路及校園網路的成果。

2. 地址解析協定簡介

地址解析協定 Address Resolution Protocol(ARP)網路協定是用於將 32 位元的 IP 位址與 48 位元的

MAC 位址之間進行轉譯[8]，是 IPv4 中網路層必要的協定，ARP 運作流程如下：首先，若電腦 A 想與電腦 B 進行通訊，電腦 A 會先在自身的 ARP table 中查詢電腦 B 的 IP 位址及 MAC 位址對應紀錄，若該對應紀錄存在，則電腦 A 將電腦 B 的 MAC 位址填入 Data Link 層的封包表頭，再將封包發送出去，若該對應不存在，則電腦 A 會以 broadcast 方式，對同網段所有電腦發送 ARP 請求封包，電腦 B 收到該 ARP 請求封包後，將自身的 MAC 位址填入 Data link 層封包表頭，再用 unicast 方式將封包回送給電腦 A，電腦 A 將封包中電腦 B 的 IP 位址及 MAC 位址對應更新 ARP table，由於 ARP 請求封包的發送端只管接收回應的封包訊息，無法對封包內容真偽進行分辨，所以利用此 ARP 網路協定的弱點就可以在區域網路中發動 Denial of Service(DoS)及 Man In The Middle(MITM)[9]等網路攻擊。

3. 防範 ARP 網路攻擊相關研究

列舉數個已發表且可以有效防護 ARP spoofing 的解決方案內容及其優缺點：

3.1 基於 SNMP 及 WinPcap 之 ARP Spoofing 即時偵測及恢復

此研究整合 SNMP 及 WinPcap 功能達到 ARP spoofing 即時偵測及恢復的效果[10]，該研究於 Windows 平台安裝 WinPcap 程式，由於 WinPcap 程式具有讀取封包及解析封包的能力，可藉由撰寫 WinPcap filter 程式，不斷監聽區域網路中所有網路封包，然後判斷區域網路中是否有 ARP spoofing 事件，即時發現 ARP spoofing 來源的 MAC 位址，將判斷結果交給 Linux 平台，以 SNMP 指令查找 ARP 攻擊者所在 switch port，再以 SNMP 指令關閉該 switch port，可立即阻絕 ARP spoofing 運作；此研究需協同二種作業系統平台，且 mirror 大量區域網路資料流，此作法恐對 Windows 平台造成效能衝擊，而在 switch 開放 SNMP 寫入的作法方面，若 switch IP 及 SNMP community 名稱被發現，則 switch 可能被有心人士進行操作，恐造成資安事件。

3.2 動態 ARP spoof 問題防護系統

該研究於 DHCP 網路環境中架設 Linux 平台伺服器當作 gateway，將所有 DHCP 封包中 IP/MAC 對應紀錄保存，並於同網段中各個電腦安裝 Agent 程式，在電腦開機時，由 Agent 程式向 gateway 取得所有電腦的 IP/MAC 對應紀錄，並寫入自身 static ARP table 中，可防止 ARP spoofing 攻擊[11]，一旦 Agent 程式收到 ARP 請求與回應封包時，Agent 程式將與自身的 static ARP table 比對，比對結果有差異時，就是發生 ARP 攻擊事件，此時再通過數位簽章的方式將訊息傳達給同網段的監控伺服器，該伺服器以簡訊、MSN 訊息、Email 及 log 四種方式告警網路管理員，以達到自動化監控及防護機制；此解決方案適用於小型 DHCP 的網路環境，且需要於所有電腦主機安裝 Agent 程式，用以向 gateway 取得同網段中所有電腦的 IP/MAC 對應紀錄，然後寫入自身的 static ARP table 中，安裝 Agent 程式的作法對於校園網路或企業網路為數眾多且作業系統不一的電腦主機來說，將是一種管理負擔。

3.3 輕量化 IP-ARP Spoofing 偵測及預防系統

此解決方案以分散式架構運作，以達成輕量化 IP-ARP spoofing 偵測及預防目的[12]，首先，在各個閘道器架設流量監控伺服器，各網段的電腦設備均需安裝 Agent 程式，在電腦開機後，Agent 程式發送本機 IP/MAC 對應紀錄給流量監控伺服器，同時 Agent 程式在背景不斷將本機發送的 ARP 請求封包、ARP 回應封包、ARP 封包數量及發送時間間隔等資訊給流量監控主機，各流量監控主機擁有各網段所有電腦正確的 IP/MAC 對應紀錄，一旦與 Agent 程式比對送來的 ARP 訊息有差異時，即可確定發生 ARP 攻擊事件，流量監控主機即時將所有的正確 IP/MAC 對應資料傳送給被攻擊電腦，以確保被攻擊的電腦可以重新取得所有正確的 IP/MAC 對應紀錄及恢復正常網路運作，在 ARP 攻擊事件發生時，同時以防火牆阻擋異常流量，如此可使被攻擊電腦恢復正常網路連線及防止 ARP 攻擊流量擴散；此解決方案有分散式管理及快速有效的優點，但是無法找到 ARP 攻擊者的所在網路位置，且需要在不同作業系統平台安裝 Agent 程式，若電腦數量眾多，也有管理及安裝 Agent 程式的困難。

4. ARP Spoofing 偵防系統設計

本研究整合網路設備 Command-Line Interface (CLI) 功能[13]，定時運作 Linux minicom script 連接網路設備 console 介面[14]，並下達 debug arp 及 no debug arp 指令，建置 Linux syslog server 蒐集網路設備 ARP log[15]，使用 Linux shell script 解析及排序 ARP log 內容[16]，即可找出 Arcai Netcut 使用者的 IP 及 MAC 位址，再透過 Linux shell script 對學生宿舍所有 Layer-2 switch 下達 SNMP 指令，查詢 Arcai Netcut 使用者所在 switch port No. [17,18]，最後透過 Linux telnet script 關閉 Arcai Netcut 使用者所在網路節點，以達到自動偵測及防護 Arcai Netcut 的目標[19]。

本研究的 ARP spoofing 攻擊偵測及防禦系統實作目標以分散式架構、快速、有效、低成本等前提下進行，可發動 ARP 攻擊的常見軟體有：用於中間人攻擊的 Cain & Abel[20]，用於修改封包內容然

後使用的 Packet Builder[21]，以及用於發送大量 ARP 阻斷封包造成 Denial of Service (DoS)攻擊的 Arcai Netcut 等，其中以 Arcai Netcut 最常被學生使用於宿舍網路，使自己可以佔用網路頻寬，同時造成其他同學無法上網及骨幹網路設備 CPU 使用率瞬間提高等現象，為阻絕 Arcai Netcut 所造成的影響，本研究針對 Arcai Netcut 進行自動偵測及防禦系統實作，詳細實作內容於下列各節說明。

4.1 Arcai Netcut 網路剪刀手運作原理

網路攻擊者常用 Arcai Netcut 發送大量 ARP 回應封包至區域網路中所有電腦，這些 ARP 回應封包都是包含偽造的 gateway MAC 位址，由於 ARP 協定的弱點，被攻擊的電腦收到 ARP 回應封包時，無法驗證真偽，所以即使收到偽造的 gateway MAC 位址，也會取用並更新自身的 ARP table，如此一來，在收到大量惡意的 ARP 回應封包後，被攻擊者將無法與正確 gateway MAC 位址聯繫而無法上網。

圖 1 為 Arcai Netcut 開始執行運作時畫面，該軟體會先掃描同網段所有 IP，得知各電腦是否於網路上運作，並向同網段所有 IP 發送 ARP 請求封包，以 broadcast 方式發送每秒鐘約 60 個 ARP 請求封包，以取得同網段所有 IP 的 MAC 位址，如下圖 2 所示，再以 Arcai Netcut 選擇發動 Denial of Service(DoS)攻擊的對方 IP 後，隨即針對該 IP 發送大量內含偽造 gateway MAC 的 ARP 回應封包，由於被攻擊者無法取得正確的 gateway MAC 位址而無法上網。



圖 1 Arcai Netcut 程式啟動畫面



圖 2 Arcai Netcut 顯示同網段各電腦 IP/MAC

4.2 CISCO Layer-3 switch 功能

本校校園網路以常見的三層式網路架構建置而成，其中核心層為 CISCO 6509，匯聚層為 CISCO 3750，而存取層為 CISCO 2960；當有電腦開始運作 Arcai Netcut 時，不斷以 broadcast 的方式發送每秒鐘約 60 個 ARP 請求封包，向同網段所有 IP 送出 ARP 請求，此時由於 CISCO 3750 收到大量 ARP 廣播封包而使 ARP Input 程序 CPU 使用率立即提高，下圖 3 為執行 Arcai Netcut 後，CISCO 3750 CPU 即時使用率，而下圖 4 為一日之中各時段使用 Arcai Netcut 對 CISCO 3750 CPU 使用率的統計圖。

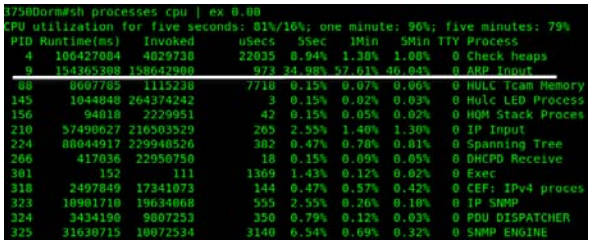


圖 3 CISCO3750 CPU 即時使用率

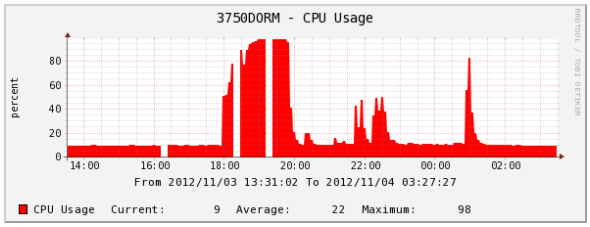


圖 4 CISCO 3750 CPU 使用率統計圖

在 CISCO 3750 的 CLI 指令裡，可用下表 1 所示指令查看即時 ARP 請求及回應封包細節，ARP 相關訊息都會被儲存於 CISCO 3750 log 之中，如下表 2 所示，透過 syslog server 自動收集 CISCO 3750 log，並以 Linux shell script 自動解析並排序 log 內容，即可找出發送大量 ARP 請求封包的來源 IP/MAC 位址。

表 1 CISCO ARP 封包查看指令

指令	用途
debug arp	開啟 ARP debug mode
no debug arp	關閉 ARP debug mode

表 2 CISCO ARP debug log 內容

log 類型	log 內容
ARP 請求封包	IP ARP : rcvd rep src 140.124.135.122 b888.e3a0.d88f, dst 140.124.135.254 Vlan134
ARP 回應封包	IP ARP : sent rep src 140.124.135.254 0026.0ba1.fec2, dst 140.124.135.122 b888.e3a0.d88f Vlan134

4.3 Arcai Netcut 偵測及防護機制運作流程

由於 CISCO 3750 提供 debug arp 指令功能，所以無需使用 Windows 平台的 WinPcap 軟體對區域網路所有流量進行即時分析，就可以透過收集、解析及排序 ARP log 找到大量發送 ARP 請求封包的來源 IP/MAC 位址；本系統使用一台 Mini PC，安裝 Linux CentOS 6 作業系統，使其與 CISCO 3750 的 console 及 LAN 相接，如下圖 5 所示。

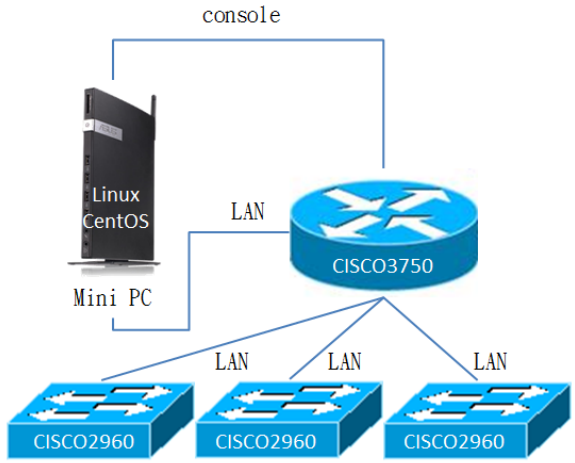


圖 5 Mini PC 與 CISCO 3750 架構圖

Mini PC 每 10 分鐘執行 Linux minicom script 連接 CISCO 3750 console 介面，使 CISCO 3750 執行 10 秒鐘 debug arp 指令，將 ARP log 以 syslog 的方式在 LAN 環境下傳送給 Mini PC，再使用 Linux shell script 解析及排序 log 內容，即可自動化得到大量發送 ARP 請求封包的來源 IP/MAC 位址，如圖 6 所示。

```
20130110-13:32:18
  count request-IP      request-MAC
    838 140.124.131.17:0024.1da6.d3e8
     11 140.124.141.155:50e5.493e.f1db
      9 140.124.147.251:001d.6054.469b
      7 140.124.135.43:bcf6.85a8.2f96
      6 140.124.135.31:5404.a61f.5990
      5 140.124.147.107:bcae.c51d.0723
      5 140.124.135.164:3085.a918.b7cd
      4 140.124.144.194:000e.c6f0.2090
      4 140.124.141.165:c860.0021.f3dc
      4 140.124.141.154:dc0e.a11f.f630
```

圖 6 10 秒鐘內 ARP 請求封包統計 TOP 10

經過多次實驗後得到的統計結果，我們發現在 10 秒鐘內發送超過 500 筆 ARP 請求封包者，即是使用 Arcai Netcut 使用者，我們可以從 ARP log TOP 10 統計結果得知 Arcai Netcut 使用者的 IP/MAC 位址，接著 Mini PC 傳送 SNMP 指令給 CISCO 3750 底下所有 CISCO 2960 的 FDB (forwarding database) table，查找 Arcai Netcut 使用者 MAC 位址所在 switch port No.，相關的 MIB(Management Information Base)值分別為：dot1dTpFdbAddress OID, 1.3.6.1.2.1.17.4.3.1.1 及 dot1dTpFdbPort OID, 1.3.6.1.2.1.17.4.3.1.2，Mini PC 得到 Arcai Netcut 使用者所在 CISCO 2960 switch port No.後，再執行 Linux telnet script，將該 switch port 關閉，即可阻絕 Arcai Netcut 使用者，完整自動化偵測及防護流程如下圖 7 所示。

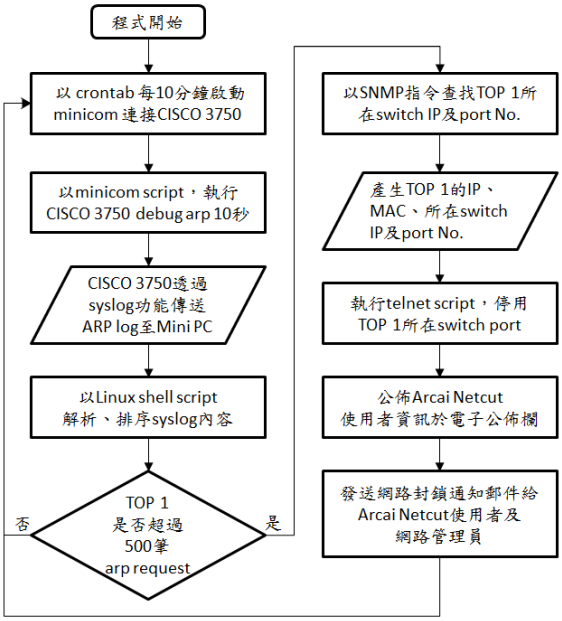


圖 7 自動化偵測及防護 Arcai Netcut 流程

本系統自動封鎖 Arcai Netcut 使用者網路後，立即透過電子郵件方式通知使用者及網路管理員，並且公佈部分使用者個人訊息於液晶電視公佈欄，如下圖 8 所示，待使用者移除 Arcai Netcut 並回覆電子郵件後，再由網路管理員解除網路封鎖限制。

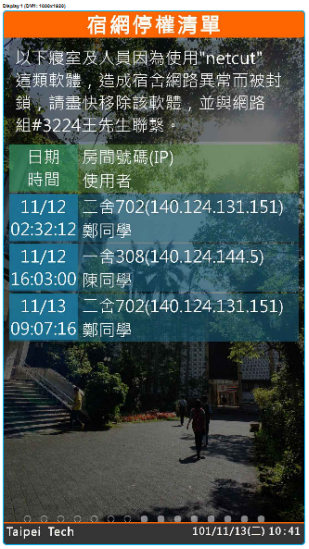


圖 8 公告 Arcai Netcut 使用者資訊

4.4 系統運作成果

本系統於學生宿舍自動偵測及防範 Arcai Netcut 使用者的成效顯著，因此複製相同的網路架構至全校校園網路，如下圖 9 校園網路架構圖，經由統計全校每月 Arcai Netcut 事件，得到如表 3 統計結果，本系統於全校運行後，雖然仍有少數使用 Arcai Netcut 事件，但已無法對校園網路造成影響，以及不再發生因 Arcai Netcut 而使學生無法上網的情形，以 8 個月的系統運作成果顯示，可驗證本系統具有效偵測及防範 Arcai Netcut 於校園網路中運作的能力。

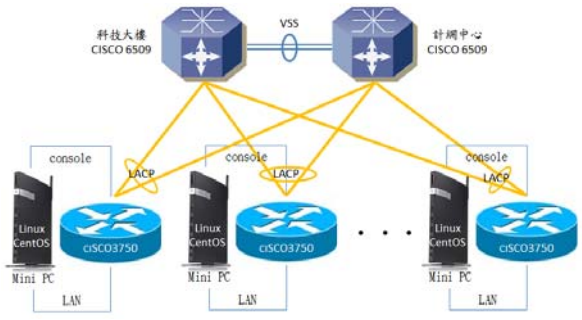


圖 9 擴大本系統至全校網路架構

表 3 全校 Arcai Netcut 事件統計表

民國年/月	101/10	101/11	101/12	102/1	102/2	102/3	102/4	102/5	102/6	102/7
全校Arcai Netcut 事件總數	1	7	4	7	5	5	4	6	0	0

5. 結論

本研究整合網路設備提供的 CLI 指令，debug arp 功能，搭配一台 Linux CentOS Mini PC，透過撰寫各式 scripts，以達到自動偵測及防護 Arcai Netcut ARP spoofing 網路攻擊，本研究初期於學生宿舍網路運作，因為成效良好，接著擴及全校校園網路，成功達到分散式架構、快速、有效、低成本的目標；由於 ARP 網路攻擊日新月異，本研究未來可朝以下幾個方向發展：

(1)具備對各廠牌 Layer-3 switch 進行 ARP spoofing 網路攻擊偵測及防護的能力。

(2)縮短偵測時間，達到即時偵測及防禦大量使用者同時進行 ARP 網路攻擊的能力。

參考文獻

[1] “Arcai Netcut,” http://arcai.com/

[2] http://en.wikipedia.org/wiki/ARP_spoofing, accessed Sep. 2012.

[3] Kumar, S., “Impact of distributed denial of service (DDoS) attack due to ARP storm,” Lect. Notes Comput. Sci., 2005, 3421, pp. 997–1002.

[4] M. Oh, Y.-G. Kim, S. Hong, S. Cha, “ASA: agent-based secure ARP cache management,” IET Communacation., vol. 6, no. 7, 2012, pp. 685-693.

[5] Bruschi, D., Ornaghi, A., Rosti, E., “S-ARP: a secure address resolution protocol,” Proc. 19th Annual Computer Security Applications Conf. (ACSAC2003), Las Vegas, NV, USA, December 2003, pp. 66–74.

[6] Xing, W., Zhao, Y., Li, T., “Research on the defense against ARP spoofing attacks based on WinPcaP,” Proc. Second Int. Workshop on Education Technology and Computer Science (ETCS2010), Wohan, China, March 2010, pp. 762–765.

[7] Gouda, M.G., Huang,C.T., “A secure address resolution protocol,” Comput. Netw.: Int. J. Comput. Telecommun. Netw., vol. 41, no. 1, 2003, pp. 57–71.

[8] RFC-826, “An ethernet address resolution protocol,” 1982.

[9] “Man In The Middle,” http://en.wikipedia.org/wiki/Man-in-the-middle_attack,

[10] L. Wang, Y.-S. Li, L.-wei Hu, “Real-time detection and recovery of ARP Spoofing based on SNMP and WinPcap,” 2012 IEEE Internation Conference on Cyber Technology in Automation, Control, and Intelligent System(CYBER), 2012, pp.1-4.

[11] S. Puangpronpitag, N. Masusai, “An Efficient and Feasible Solution to ARP Spoof Problem,” IEEE, 2009, pp.2-3.

[12] S. G. Bhirud, V. Katkar, “Light Weight Approach for IP-ARP Spoofing Detection and Prevention,” 2011, pp.3-4.

[13] Cisco Systems, “Configuring Dynamic ARP Inspection,” Catalyst 6500 Series Switch Cisco IOS software Configuration Guide, Release 12.2SX, chapter 56.

[14] “Linux/UNIX minicom Serial Communication,” http://www.cyberciti.biz/tips/connect-soekris-single-board-computer-using-minicom.html

[15] “Configuring a syslog server on RHEL/CentOS 6,” http://people.opencomputingsolutions.com/?p=53

[16] “Linux Shell Scripting Tutorial v1.05r3 A Beginner’s handbook,” http://freeos.com/guides/lsst/

[17] “Cisco SNMP Object Navigator,” http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

[18] “SNMP Command Examples,” http://docs.oracle.com/cd/E19201-01/820-6413-13/SNMP_commands_reference_appendix.html

[19] “Telnet Scripting with Bash-Linux,” http://amilasurendra.info/telnet-scripting-with-bash-linux/

[20] “Packet Builder, ” http://www.colasoft.com/packet_builder/

[21] “Cain&Abel, ” http://www.colasoft.com/packet_builder/

基於 P2P-OSGi 服務取得機制之數位版權管理機制

林宸堂　　張志鴻
國立嘉義大學資訊管理系
{ ctlin, s0981497 }@mail.ncyu.edu.tw

摘要

隨著資訊科技的發展，讓數位家庭的概念也越來越熱門，OSGi 聯盟提出以家庭閘道器整合家電設備，讓各式各樣的設備間可以相互溝通、提供服務；因而有一些研究結合 OSGi 平台與傳輸更快速的 P2P 網路架構，來達到家庭間多媒體服務的共享。但在 P2P 的分享架構下卻一直存在著盜版的問題，因此我們必須有一套完整的機制，來幫助解決盜版的問題。

在過去已經有針對 P2P 的分享機制提出了數位版權管理機制，它們雖然提供了一定程度的安全性，但相對也讓版權控制系統伺服器的負載過於龐大，因此本研究在基於一 P2P-OSGi 服務取得機制的研究上，整合了數位版權管理機制，在本機制中，利用密碼學系統，為分享檔案的過程提供了一個安全的保護，也減輕了過去研究中版權控制系統伺服器的負載，更讓使用者可以很方便的利用本機制來販售其數位內容。

關鍵詞：OSGi、P2P、DRM。

Abstract

The concept of digital home becomes popular with the development of the information technology. The OSGi Alliance proposes the idea of integrating the household appliances with home gateway, in that case, the communication among appliances becomes possible. Many researches integrated of OSGi platforms and the P2P networking to share multimedia services. However, a digital rights management (DRM) mechanism is needed to solve the piracy problem due to P2P sharing system.

Although some DRM mechanisms for P2P sharing systems have been proposed, they often caused the DRM server overloaded. Therefore, in this paper, we propose a new DRM solution based on the P2P-OSGi system. Our solution uses PKI system involved in the OSGi standard to protect communication security and user authentication. Our DRM system is built on OSGi service gateways, hence, it is convenient for OSGi users to sell or buy the digital contents. In addition, the proposed DRM system is more efficiency since we do not need a central DRM server to encrypt content.

Keywords: OSGi、P2P、DRM

1. 前言

現今家庭中有越來越多的家用設備，而不同的設備各有不同的功能，若欲整合這些功能，一般使用者通常欠缺專業的知識來處理這些整合的問題，因此實現一個自動化設定硬體環境也就顯得更重要，家庭環境中的不同的多媒體裝置間之通訊就變成了一個很重要的議題。現在有許多廠商提出了各種家庭應用環境的標準，如 ECHONET、OSGi、UPnP、DLNA...等[1][2][3]，有了這些標準的支援，讓家庭環境中的各種設備間得以相互通訊，達到一個有助於發展家庭網路的環境。

其中 OSGi 的應用十分廣泛，從醫療照護至家庭娛樂，都可利用 OSGi 來達成自動化的環境，以方便使用者之使用。過去已有研究[4]利用 OSGi 平台建置 P2P 分享機制，以提升多媒體檔案的分享速度，透過 P2P，讓每個不同的家庭間可以透過該機制互相分享多媒體數位內容，使數位內容更容易地在不同家庭的 OSGi 平台間做更快速的共享，且達到自動化的視聽環境設定以及多媒體的播放。P2P 提供了一個很快速的檔案分享技術，但 P2P 也一直被認為是盜版的溫床，其原因是 P2P 本身就缺乏安全機制—其並未提供付款（Payment）、限制非授權存取…等相關機制。過去已有一些研究針對此議題提出基於 P2P 的 DRM 系統[5][6][7]，雖然這些研究都可以解決傳統 DRM 系統在數位內容在傳輸上的效率問題，且也提供了一定程度的安全性，但它們都過於依賴中心伺服器來提供每個使用者的加解密金鑰，如此會讓中心伺服器對於金鑰上的管控變得過於複雜，所以我們希望可以分散加解密的運算負載以及金鑰的管控到各個欲販售數位內容的使用者上，達到一個安全又有效率的 P2P 分享環境。

因此本研究在基於 OSGi 平台上設計一套 DRM 系統，目標是讓創作者可將自己欲販售之數位內容加密後再予以發佈至 P2P 網路上，下載完數位內容的使用者可在付費後向創作者要求使用執照（License），拿到使用執照後方可存取所下載的數位內容。而 License 會依使用者對數位內容的權限（如存取次數、存取時間等）來製作。同時，我們會對 License 做一完整的保護，其中包括：License 使用者的身份驗證、License 的完整性驗證、以及 License 的來源驗證。

2. 文獻探討

過去已有許多針對 OSGi 平台的研究，但由於 OSGi 的標準中缺乏自動化的 Content（多媒體）服務取得機制，所以有研究提出了一套以 Content 導向的 OSGi 服務取得機制[4]，且此研究為顧及 Content 的傳輸效率，因此又加入了 P2P 的網路架構，以加速服務的傳輸速度以及可靠度。由於本研究是以該機制為基礎來設計 DRM 系統，因此底下先簡略介紹該機制的內容。

2.1 P2P-OSGi 服務取得機制

該研究設計一個 Content 導向的相關服務取得機制，且將該機制整合於 OSGi 平台上，該機制內有 2 種主要的 Bundle，分別為：影音 Bundle（Content Bundle）以及相關服務 Bundle（Device Bundle），為了建立 Content Bundle 與 Device Bundle 間的關連性，以達到一個自動化的設定環境，作者重新設計了 OSGi 原始的 Bundle，但並未更動其結構，而是將 Content 放入原始 Bundle 的 Other Resource 欄位中，利用了原始 Bundle 的閒置空間，並且將關連性資訊設計成 Relationship Header（RH），分別放入 Content Bundle 以及 Device Bundle 中，以建立 Content Bundle 和 Device Bundle 的關聯。

而在 Content Bundle 的分享方面，因為 Content Bundle 中包含多媒體影音檔案，其檔案大小通常很大，若只單純透過 Client-Server 架構來傳送，會讓系統效率受阻，可能會降低使用者的使用意願，因此，該研究採用純分散式 P2P 的架構來做 Content Bundle 的分享，利用 P2P 傳輸速度上的優勢，讓 Content 的分享效率提升。

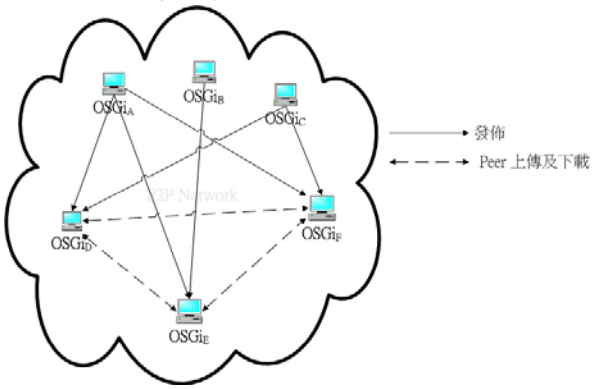


圖 1 P2P-OSGi 服務取得機制架構圖

2.2 P2P-DRM 系統相關研究探討

目前有許多知名的 P2P 分享軟體，如 BT、eMule…等，它們提供了分享檔案上的便利性，但這些分享軟體並未提供數位版權保護的機制。因此，Zhang 學者等人在 BT 的分享機制上提出了一套 DRM 系統[6]，其使用非對稱式加密來保護數位內容。

Zhang 等人所提出的雖然方法可以保證每一個資料區塊在網路上傳送的安全性，以及保護了其數位版權，但相對上也有一些缺點。該系統需要一個集中式的 Server 幫各個 Peer 產生 Re-Encryption Key，且從每一個 Peer 到其它 Peer 都會需要重新重送 Re-Encryption Key，如此 Server 的負載會過於龐大，以至於無法顧及其效率。Server 還需要保留每一次交換後的資訊，因為所有的 Public Key 和 Re-Encryption Key 都保留在 Server 中，這樣會嚴重拖累到 Server 的延展性。再者，將數位內容使用不同金鑰重新加密，在實質上並不會增加安全性，攻擊者只要能截走其中一個 Peer 的 key 攻擊即可，並不需要拿走所有 Peer 的 Key 才可破解，因此在實質上與只用一把金鑰加密的安全性並無差異。

3. P2P-OSGi DRM System

此章節我們將對我們所提出的 P2P-OSGi DRM 機制做一個介紹。

3.1 系統環境與假設

DRM 系統中最關鍵的要素為客戶端的平台中，需要有一個可信任的內容播放器（Player）或瀏覽器（Browser），主要預期它在解密的過程中不會將解密過後的明文外流，意即保護資料流，以及正確地強制執行並套用明定在 License 裡的使用權限[8][9]。本系統內的播放器或瀏覽器會自行判斷 Client 對於他拿的 License 是否具有讀取權限，若 License 中的資訊與其 OSGi 平台的 ID 不符，則不予讀取。意即，使用者收到其購買 License 後只能在其自己的系統上使用，無法移轉。因此本研究做了四個基本的假設：第一、用戶端的 OSGi 平台是可信任、且安全的，即在 Client 端的 OSGi 平台（使用者端的 OSGi 閘道器）內的播放器或瀏覽器，它們只負責解密 License，並且讀取出權限使用規則，且在播放期間不會將解密 Content 的金鑰以及解密後的 Content 外流；第二、我們假設我們架構內的 PMG 的角色是公證的第三方，可以很正確協助交易事宜，但本研究不干涉 PMG 及銀行間的金流方式，只確保交易雙方交易是否完成；第三、因本研究是架構在 OSGi 平台上，OSGi 的規格[2]中，就具有 PKI 的架構，因此本研究之後的協定會使用 PKI 機制，來達成本研究的交易協定；第四、使用者在加入 P2P-OSGi 分享機制之前，都需要取得一個 Token，其目的是提供使用者自身具唯一且唯讀的機密資訊，Token 的取得方式有許多種，而目前較常見的有 Smart Card（IC Card）、RFID、與手機的 SIM 卡[11]…等，都可以用來提供唯一性的資訊當作 Token 使用，在本研究中為了保持系統設計的彈性，不指定使用何種方式來取得 Token 資訊。

本研究基於以上之假設，為 P2P-OSGi 服務取得機制[4]設計了 DRM 系統（如下圖 2 的系統架構圖），架構中共包含了四個角色：

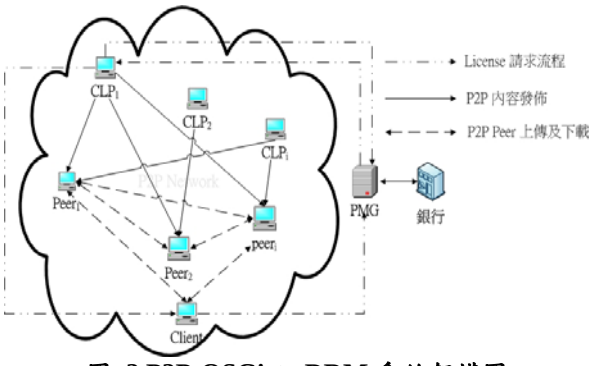


圖 2 P2P-OSGi 之 DRM 系統架構圖

- 原始檔案擁有者（Content and License Provider，簡稱 CLP）：在 P2P 分享機制下，任何一個 OSGi User 想透過本 DRM 機制販售商品，都可以成為 CLP 的角色。它同時也掌控消費者對 Content 的使用規則，意即每個 CLP 都是 DRM Server。
- 已擁有檔案的使用者（$Peer_1$~$Peer_{i-1}$,$Peer_i$）：已經經由 P2P 分享機制下載到 Content Bundle 區塊的 OSGi 平台，其在 DRM 的機制下並未參與任何角色，除非它想購買此 Content 的 License，若想購買，即成為上圖 2 中的消費者（Client）的角色。
- 消費者（Client）：即想購買 Content 的 Peer，它會向 PMG Server 請求付款，在做完付款動作後即可向 CLP 拿到 Content 的 License 來解密、存取 Content。
- 付款中心（Payment Gateway，簡稱 PMG）：協調買賣雙方交易的中介角色，負責與銀行處理雙方交易流程，但本研究不干涉 PMG 及銀行間的金流方式，只確保交易雙方交易是否完成。

3.2 符號定義

在詳細介紹 P2P-OSGi DRM 系統之前，為了簡化協定的表示方法，將之後所使用的每個符號加以定義，以提升可讀性，如表 1 所示：

表 1 符號說明表

符號	說明
ID_x	角色 X 的唯一識別碼
$Name_{Bundle}/ID_{Bundle}$	Content Bundle 的名稱及 ID，即商品的名稱以及商品的 ID。
PK_User/PR_User	在 PKI 機制下，User 的公開金鑰（Public Key）與私密金鑰（Private Key）
Token	硬體特徵碼，可經由多種方式取得，如 IC 卡、CPU 序號…
TS	時戳 (Time Stamp)，以 TS_1~TS_k 代表不同的時間
H()	單向雜湊函數
$E_{PK\_User}(M)$	使用公開金鑰 PK_User 對 M 做非對稱式加密
TID	交易單號碼
TD	詳細交易資訊，如 ID_{Bundle}、購買之存取等級、數量…等
PA	付款總金額
N	Nonce，以 N_1~N_k 代表不同的 Nonce
BA_{Client}	Client 的付款帳戶資訊
BA_{CLP}	CLP 在販售商品後的收款帳號資訊
$CERT_{OSGiUser}$	OSGi User 向 CA 註冊後，所得到的憑證（Certificate）
DR	PMG 所簽發給付款者的數位發票（Digital Receipt），用來記錄成功付款後商品的項目以及金額

3.3 系統流程與協定設計

在本節我們將詳細介紹本研究的交易機制。下圖 3 為系統流程圖，共分成 5 個階段。系統實際流程 5 個階段中的 P2P 下載階段，為第二章文獻探討中所提到之 P2P-OSGi 服務取得機制[4]，因此在下面的協定介紹中並不會針對此一階段多做說明，以下僅針對本研究中所新增 4 個新設計的流程做說明。因為本研究是架構在 PKI 的環境上，因此我們假設在交易開始前，不論是 CLP、Client 或是 PMG，都已經向 CA 取得各自的憑證（Certificate），供後面的交易過程中可驗證身份、以及加密交易資訊。憑證的時效性檢驗，也都會利用 PKI 的機制去處理，所以接下來的處理流程都不包括憑證的正確性與時效性的檢驗。

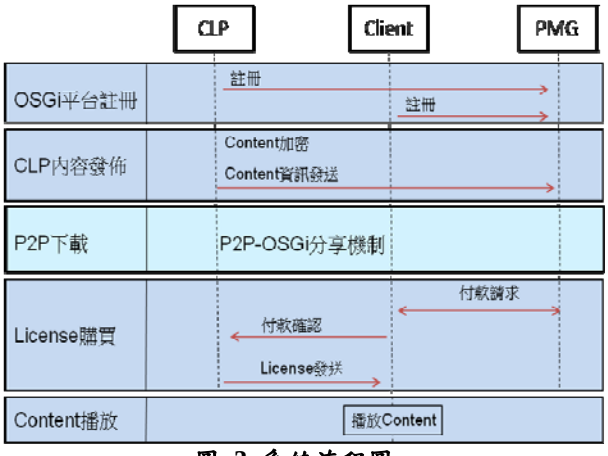


圖 3 系統流程圖

3.3.1 OSGi 平台註冊階段

CLP 或 Client（以下合稱 OSGiUser）要販售或購買商品前都必須向 PMG 註冊，註冊的動作主要是為了讓 PMG 可以知道有這一個使用者（Client/CLP）的存在，下圖 4 為 OSGiUser 註冊協

定）。

步驟1. OSGiUser 利用 Token 做雜湊運算，將運算結果當成自己的 ID。

步驟2. OSGiUser 利用上一步驟中利用 Token 所計算出來的 ID 向 PMG 做註冊的動作，並在訊息內會帶入 OSGiUser 的憑證，供 PMG 可利用憑證辨識第一次註冊的使用者，同時也將憑證與 $ID_{OSGiUser}$ 做關聯，讓日後 PMG 可依 ID 來查找對應的公開金鑰（PK_User）。訊息會使用 PMG 的公開金鑰加密，以保有其機密性。我們是利用密碼學的擴散（Diffusion）特性來達成訊息的完整性驗證[12]，我們將密文內第一個欄位 CLP/Client 的資訊，以明文的方式，附加在訊息中，讓 PMG 可以利用此明文來驗證解密後的訊息是否正確，以此判斷訊息是否有遭到竄改。同時，我們在訊息內會加入一 Time Stamp TS_1，讓 PMG 可依此 TS_1 來確認該訊息是即時訊息，不是重送攻擊。

步驟3. 註冊成功後，PMG 會回應一個成功註冊的訊息，告知 OSGiUser 註冊成功。PMG 會使用其私密金鑰將 N_1 加密，N_1 為上一步驟中，OSGiUser 所產生的一個 Nonce，OSGiUser 收到後利用 PMG 的公開金鑰解密訊息，比對 N_1 是否正確，若比對無誤，即表示此回覆訊息的發送者確實為 PMG，藉此達到身份確認，以及防止重送攻擊的問題發生。

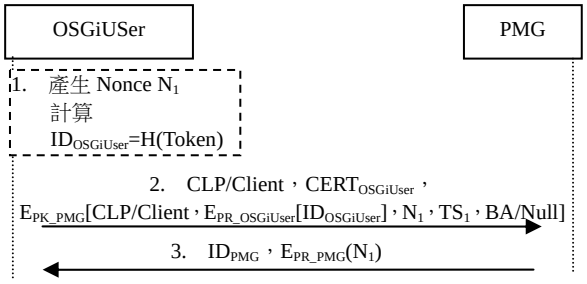


圖 4 OSGiUser 註冊協定

3.3.2 CLP 內容發佈階段

若 CLP 有 Content 欲販售前，CLP 會對欲販售的各個 Content，各自使用不同數位內容加密金鑰（Content Encryption Key，CEK）加密，一個 Content 僅加密一次，不會因使用者不同而再重新加密，完成加密後，再封裝成 Content Bundle。封裝完成後，其必須將商品（Content Bundle）的資訊告知 PMG，日後，若 Client 想購買商品時，即可向 PMG 要求商品資訊，下圖 5 為 CLP 商品資訊更新協定。

步驟1. 計算 H(CB_Manifest)，其為欲販售之 Content Bundle 的 Manifest 的雜湊值。

步驟2. 將商品資訊以及 CB_Manifest 雜湊值，傳送給 PMG，更新商品資訊。協定的設計也允許 CLP 在一次的流程中，傳送多筆商品資訊，在訊息中，$[ID_{Bundle}、H(CB\_Manifest)]_i$ 就代表某一筆商品的資訊，所以假定 CLP 同時間有 10 筆商品資訊欲更新，則 i 就會以 1 到 10 來表示。訊息會利用 CLP 的私密金鑰加密，讓 PMG 可以驗證訊息來源，PMG 可以使用 CLP 的公開金鑰正確的解密訊息，即可以確認是 CLP 所送過來的資訊，不是他人假造。

步驟3. 商品資訊更新成功後，會回傳更新成功訊息通知 CLP。

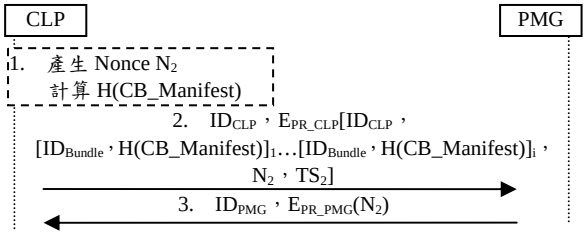


圖 5 CLP 商品資訊更新協定

3.3.3 License 購買階段

在 License 購買階段，Client 取得 Content Bundle 後，若 Client 有意購買 License，則 Client 的 OSGi 平台依 Bundle 的 Manifest 資訊，向 PMG 請求查詢正確的 Content Bundle Manifest 資訊，查詢成功後，即可向 CLP 購買 License，下圖 6 為 License 購買協定。

步驟1. Client 利用所下載的 Content Bundle，從 Content Bundle Manifest 中取出 Bundle 的擁有者 ID（ID_{CLP}），以及 Bundle 的 ID（ID_{Bundle}），向 PMG 發送「查詢 Content Bundle Manifest 的雜湊值」的請求，我們會將訊息利用 PMG 的公開金鑰加密，以保有該訊息的機密性，此步驟還未正式發出購買請求，所以不需要做身份的驗證，但我們需要做訊息的完整性驗證。

步驟2. PMG 收到 Client 的查詢請求訊息後，會依 ID_{CLP} 以及 ID_{Bundle} 開始查找資料庫內是否有符合之項目，若找到符合之項目，會回傳 Content Bundle 的 Manifest 雜湊值給 Client。此步驟 Client 需要去驗證該訊息是否是 PMG 所送過來，並檢驗訊息的來源以及完整性，因此 PMG 會將訊息以自己的私密金鑰加密，以達到來源驗證與訊息完整性。

步驟3. Client 收到訊息後，即可向 CLP 告知欲購買的商品資訊（包含 ID_{Bundle}、購買之存取權限名稱，統稱 TD），請求購買 License。Client 會將訊息利用 CLP 的公開金鑰加密，讓其購買訊息保有機密性，達到保護 Client 隱私的目的。

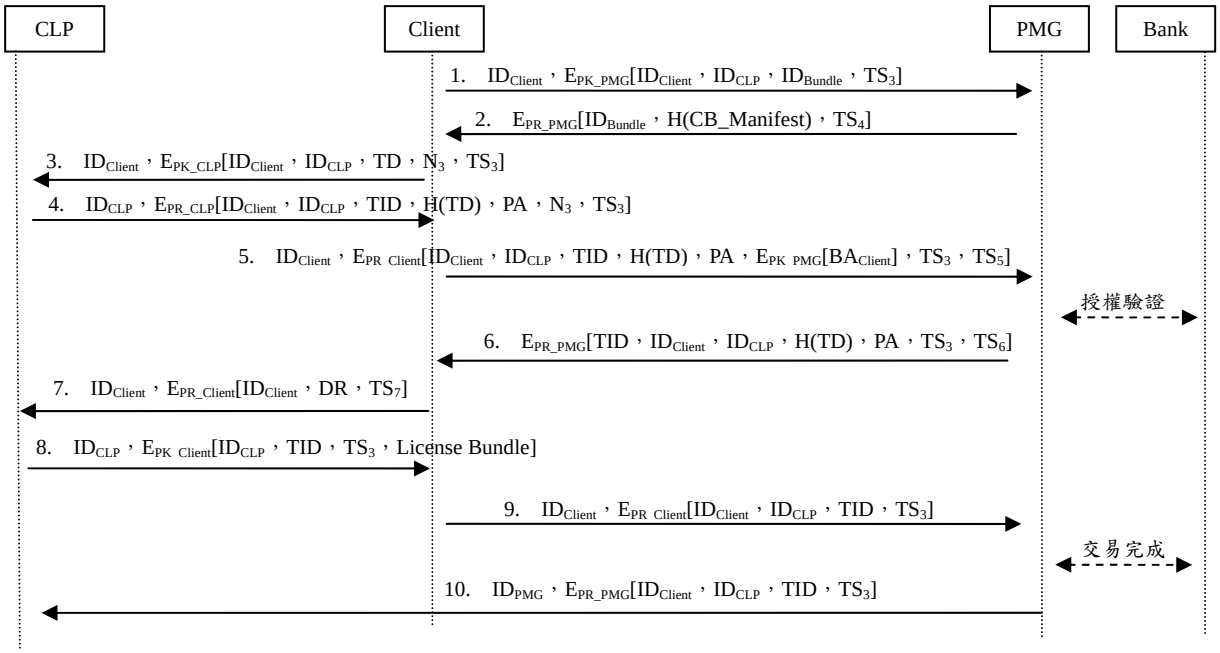


圖 6 License 購買協定

步驟4. CLP 收到 Client 的購買請求後，會依 Client 的購買需求，產生相對應的訂單號碼（TID），並將訂單編號 TID 以及訂單總金額 PA 回傳給 Client，讓 Client 做最後的訂單確認動作。CLP 會利用自己的私密金鑰將訊息加密，做簽署的動作，讓 Client 可以利用 CLP 的公開金鑰來檢驗訊息的來源以及完整性，同時 Client 也需要留存此訊息，若日後訂單上有爭議時，可利用此訊息來解決爭議。由於任何人都可以用 CLP 的公開金鑰來解密此訊息、並得知內容，而商品資訊（即 TD）為較私密的資料，因此我們是將 TD 做雜湊運算後，再加入密文中，如此 Client 仍可驗證其正確性，又不用擔心第三方知曉商品內容。

步驟5. Client 收到訂單資訊後，即會比對商品項目以及商品價格、總額是否正確，若比對無誤，則向 PMG 發送付款請求，同時會附上自己的付款帳號資訊（BA_{Client}）。我們會利用 PMG 的公開金鑰將付款帳號加密（BA_{Client}），因此無須擔心 Client 的付款帳號這種敏感資料會被他人竊知，並將訊息利用 Client 的私密金鑰加密，對訊息做簽署的動作，讓 PMG 收到訊息後，可以利用 Client 的公開金鑰解密訊息，來驗證訊息的完整性以及來源。

步驟6. PMG 收到付款帳號資訊後，即會向銀行確認 Client 所給的帳號是否具有付款能力。若 PMG 在向銀行確認付款帳號正確，即會向 Client 送出付款帳號確認成功的訊息。該訊息會使用 PMG 的私密金鑰加密，做簽署的動作，本系統將整個經 PMG 簽署過的訊息當作是一個數位發票（代稱 DR），Client 即可使用 DR 來證明自己所給的付款帳號確實是有付款能力，可以支付此次交易。

步驟7. Client 在收到 PMG 利用其私密金鑰所簽發的 DR 後，即可利用 DR 向 CLP 要求 License。Client 利用其私密金鑰加密做簽署的動作，讓 CLP 可以驗證此筆交易付款者（Client）的身份，證明 DR 確實是他本人的。

步驟8. CLP 收到 Client 所送來的 DR 後，即會依 Client 的購買需求，將對應的存取權限以及 Content 解密金鑰（CEK）封裝成 License。為了讓 Client 可以去檢驗 License 的來源以及完整性，CLP 必須對 License 做簽章，再一同寫入 License 中，產生 License 檔案，再將 License 檔案，封裝成完整的 License Bundle，再發送給 Client。為了保護 License，我們會使用 Client 的公開金鑰加密，以達到訊息的機密性。

步驟9. 在比對資料無誤後，Client 會傳送收到商品的確認訊息給 PMG，之後 PMG 再向銀行確認此筆交易已經完成，得以轉帳。

步驟10. PMG 確認交易都完成後，會再送一個轉帳成功的訊息給 CLP。

3.3.4 Content 播放

第五階段為 Content 播放階段，Client 已經擁有 Content Bundle 以及完成 License 購買的動作。

步驟1. OSGi 平台內的播放器或瀏覽器，會以 Client 自己的 Token 計算出 ID_{Client}，然後去讀取 License 的資訊，看是否與 License 內所記錄的 ID_{Client} 相符，相符則再繼續第 2 步驟的檢驗，否則不允許存取 License。

步驟2. 在完成第一階段的檢驗後，OSGi 平台即會

開始檢驗 License 的完整性，以確認其未被修改過。OSGi 平台是利用 License Bundle 裡的 CLP 簽章來驗證 License 的來源以及完整性，若驗證無誤，即表示 License 未被竄改過且來源是正確的，OSGi 平台即會再利用 Client 的私密金鑰解密 Content Encryption Key（CEK）取得 CEK，利用 CEK 將 Content Bundle 中的 Content 解密，同時播放器會配合 License 中所記載的存取權限來控制 Content 的存取。

4. 分析評估

本章節中，我們將會分析本研究中之協定，是否有達到一個交易機制所需要的各個安全需求，以及交易公平性問題。

- 訊息機密性
  在訊息機密性上，本研究採用了雜湊函數以及 PKI 的機制來達成。較機密的資料、如 License 購買協定訊息 5 中的付款帳號、訊息 8 傳送商品（License），或者在註冊協定中 OSGiUser 的 ID，我們會以訊息接收者的公開金鑰將訊息加密，以確保只有擁有相對應私密金鑰的接收者才可解密、取得訊息內容。若資訊是需要給第三方知道的（如使用者所購買的商品資訊，TD），我們會將 TD 使用雜湊函數計算，再將訊息傳送給第三方，用以保護使用者的隱私。
- 訊息來源驗證
  我們使用傳送者的私密金鑰將欲傳送的訊息加密，讓訊息接收者可以利用傳送者的公開金鑰來驗證訊息的來源，若可以成功解密，則表示訊息來源是正確的，例如 License 購買協定中訊息 1 即是採用此法。
- 訊息完整性
  在訊息完整性部分，我們分別以 PKI 機制，以及利用密碼學擴散（Diffusion）[12]的特性來達成訊息的完整性驗證。在 PKI 機制的完整性驗證部分，我們使用傳送者的私密金鑰將欲傳送的訊息加密，讓訊息接收者可以利用傳送者的公開金鑰來驗證訊息的來源，若可以正確的解密，則表示訊息是未被竄改的；利用密碼學擴散（Diffusion）的特性，讓攻擊者在不知解密金鑰的情況下，無法準確的修改密文中的資訊。而本研究協定設計中，每個訊息都會有一固定的欄位格式，若密文在傳送的過程中被修改，接收者可以很容易判斷出欄位是否有符合協定設計中的格式，因此，我們利用密文中可辨別身份或內容的欄位，以明文的方式放在訊息中，再一併傳送給訊息接收者，接收者就可透過該明文來間接驗證密文的完整性，比如 License 購買協定訊息 8 即是用此方法。
- 不可否認性
  我們利用簽章的技術來達成這個目的，當買家付款完成或者賣家送出的商品，都會利用其各自的私密金鑰將訊息加密，即對訊息做簽署的動作，若日後交易雙方有爭議時，即可使用這些經過簽署的訊息來證明，以解決爭議，藉此來達到不可否認性。
- 交易公平性若
  一套具公平性的交易機制，必須考量到交易雙方的利益，在交易公平性部分，即買方在付完款給賣方後，可以確實的收到商品；而賣方在收到錢後要確實的將商品送給買方。本系統在這點考量下，在加入了 PMG 這個角色，來協調雙方的交易。在 License 購買協定訊息 9 中，PMG 會待 Client 向他發送商品收到的訊息後，再向銀行確認此筆交易，再進行轉帳的動作；轉帳完成後，PMG 即會再向 CLP 告知轉帳成功，讓 CLP 可以確認帳款是否收到，以此來保證交易雙方的權益。

5. 結論

本研究提出一個整合了 P2P-OSGi 平台的 DRM 機制，不但解決了 P2P 架構分享機制的版權的問題，也讓家庭中的使用者以及創作者，有更便利的管道去存取、販售數位商品。因此，本研究提出的方法，不僅能確保買家的購買商品時的隱密性，也提供一套能有效解決交易上爭議的方法，以確保買賣雙方的權益。

參考文獻

[1] EchoNet. [Online]. Available: http://www.echonet.gr.jp/

[2] OSGi. [Online]. Available: http://www.osgi.org/

[3] DLNA. [Online]. Available: http://www.dlna.org/

[4] 陳一翔，基於 P2P 網路架構下 Content 導向 OSGi 服務取得之設計與實作，國立嘉義大學，2010。

[5] T. Kalker, H. J. Dick, H. Pieter, R. Hartel, L. Lagendijk, and V. S. Maarten, “Music2Share-Coypright-Compliant Music Sharing in P2P Systems,” Proceedings of the IEEE, Vol. 92, pp. 961-970, 2004.

[6] X. Zhang, D. Liu, S. Chen, and R. Sandhu, “Towards Digital Rights Protection in BitTorrent-like P2P Systems,” George Mason University, Fairfax, VA, USA.

[7] 林奕如，P2P 網路之可追蹤與公平交易的數位版權管理機制，國立中興大學，2011。

[8] J. Park, R. Sandhu, and J. Schifalacqua, “Security architectures for controlled digital information dissemination,” Proceedings of 16th Annual Computer Security Application Conference, pp. 224-233, 2000.

[9] J. E. Cohen, “DRM and Privacy,” Communications Of The ACM, Vol. 46, pp. 46-49, 2003.

[10] T. Lindholm and F. Yellin, “Java Virtual Machine Specification,” Addison-Wesley, 1999.

[11] K. U. Chen, C. Y. Lin, and T. W. Hou, “A Low-cost Secure Schemes for Authentications and Access Control with the Use of Multiple Public IC Cards,” 3rd International Conference on Advanced Computer Theory and Engineering, Vol. 3, pp. 609-613, 2010.

[12] S. Claude, “Communication theory of secrecy systems,” Bell Systems Technical Journal, Vol.28, pp. 656-715, 1949.

全球行動網路服務之匿名性認證機制

楊仁和　　溫柏旻
開南大學多媒體與行動商務學系
{ jenhoyang, m10108007}@mail.knu.edu.tw

摘要

本論文研究在全球行動網路下之漫遊服務的匿名性認證，因為先前學者所提出的相關匿名認證機制仍存在安全性的弱點，因此本文將提出全新的全球行動網路服務之匿名性認證機制。在我們的方法中，主基地台於認證時不需維護認證相關的資料表格，可降低設備負擔及搜尋成本。此外我們也利用互斥或及單向雜湊函數運算來降低計算量，因此本文所提出的方法將比先前相關研究更加安全以及有效率。

關鍵字：全球行動網路、行動漫遊服務、匿名性、交互認證。

Abstract

In this paper, we propose an anonymous authentication mechanism for roaming services in global mobility networks. Because the related works still have some security problems, we propose a new anonymity authentication mechanism for roaming services in global mobility networks. The proposed mechanism does not need to maintain a verification table, and thus the authentication time and the storage loads can be greatly reduced. In addition, we use exclusive-or operations and one-way hash functions to reduce the computation cost of the mobile device. According to the above reasons, the proposed authentication mechanism is securer and more efficient than the related works.

Keyword: Global mobility networks, mobile roaming service, anonymity, mutual authentication.

1. 前言

在 1997 年 Suzuki and Nakada [1]學者提出適用在全球通訊的分散式安全管理，在全球行動網路下提供行動用戶進行漫遊服務的認證機制，使行動用戶漫遊在外部基地台就能夠存取主基地台提供之服務，並與基地台間進行交互認證，以防止惡意攻擊。於 2003 年，Hwang and Chang [2]學者接著提出具匿名性的認證機制。隨著行動裝置的進步與行動網路服務的發展，企業也逐漸由電子商務轉型為行動商務，行動用戶能隨時隨地的存取各種資訊服務，為通訊界中快速增長的市場。然而行動裝置與行動服務提供者之間的認證有別於傳統的有線網路，是透過開放式的無線訊號，只要行動用戶在基地台電波的涵蓋範圍之下就能夠接聽到傳輸的資訊，該特性也使得行動裝置面臨資訊安全相關的潛在威脅。行動網路安全始終是一個重要的問題，由於無線電波的本質，只要在無線電波的廣播範圍內，任何人都能夠將已發送出去的資訊封包攔截[3]，因此使用無線通訊技術進行資料傳輸時，比有線網路更容易有被竊聽或未經授權的存取行為[4]。

近年來，已有許多的學者提出利用全球行動網路的認證機制來提供行動用戶漫遊相關服務[5]，且對於行動用戶的身分進行認證是非常重要的，以防止非法使用者存取資源。另外行動用戶越來越看重個人的隱私，達到匿名性認證將會是認證機制的重點之一[6, 7]。

在 2011 年，Mun 等學者[8]指出雖然已有學者強化 Wu 等學者[6]架構之弱點，不過仍有如未達成匿名性、合法用戶密碼洩漏、完備前向機密性不完全等弱點存在，於是 Mun 等學者提出強化的匿名認證機制，在交談金鑰的協議過程中使用許多單次隨

機亂數達到匿名性認證，並於協議金鑰部分使用橢圓曲線加密法(ECDH)[9]，使金鑰破解難度建立在解離散對數的問題上。但是我們發現 Mun 等學者架構仍有弱點存在，如行動用戶與外部基地台間使用的交談金鑰可能被竊取的威脅，因此我們在本文中的第二章節回顧 Mun 等學者之認證機制，並展現出其機制之弱點，接著於第三章提出我們的方法，並修正這些弱點，我們使用低運算成本的單向雜湊函數以及互斥或運算保護重要資訊，且主基地台不需要儲存行動用戶認證的相關資訊，能夠降低硬體負擔，減少搜尋成本。最後於第四章則提出安全性分析。

2. Mun 等學者之增強全球行動網路漫遊服務之安全匿名認證機制

本節將介紹 Mun 等學者[8]提出之增強全球行動網路漫遊服務之安全匿名認證機制。有三個參與者：行動用戶、外部基地台以及主基地台，且分為註冊、認證與協議交談金鑰及更新交談金鑰三個階段，其所使用的符號如表 1 所示：

表 1、Mun 等學者的方法之符號說明

符號	敘述
MU	行動用戶
FA	外部基地台
HA	主基地台
PW_x	角色 x 的密碼
ID_x	角色 x 的身分識別碼
$h(.)$	單向雜湊函數
N_x	角色 x 所產生的單次使用隨機亂數 N
$\|\|$	字串連接運算
$\oplus$	互斥或運算
f_k	用秘密金鑰 k 做訊息鑑別碼函數運算
K_{XY}	於角色 x 與 y 之間所使用的交談金鑰
E	橢圓曲線方程式
P	橢圓曲線方程式上的一點
$*$	橢圓曲線的乘法運算

註冊階段

步驟一、 行動用戶產生的單次隨機亂數 N_{MU} 後，與身分識別碼一同傳送給主基地台。

步驟二、 主基地台收到行動用戶的資訊後，產生單次隨機亂數 N_{HA} 並計算行動用戶密碼 $PW_{MU} = h(N_{MU} \| N_{HA})$以及 $r_{MU} = h(ID_{MU} \| PW_{MU}) \oplus ID_{HA}$。

步驟三、 主基地台將註冊完成資訊$\{ID_{HA}, N_{HA}, PW_{MU}, h(.), r_{MU}\}$ 回傳給行動用戶儲存。

認證與協議交談金鑰階段

步驟一、 行動用戶將完成註冊的$\{ID_{HA}, N_{HA}, r_{MU}\}$傳送給外部基地台，當外部基地台收到$\{ID_{HA}, N_{HA}, r_{MU}\}$後會將其儲存，作為之後交互認證使用，並產生隨機亂數 N_{FA}，將$\{ID_{FA}, N_{FA}, N_{HA}, r_{MU}\}$一起傳送給主基地台。

步驟二、 主基地台驗證行動用戶之身分，計算 $r'_{MU} = h(ID_{MU} \| PW_{MU}) \oplus ID_{HA}$ 並與收到的 r_{MU} 比較，假若行動用戶認證失敗，則拒絕提供服務給非法用戶。若比較結果相等，則認證成功且行動用戶為合法用戶。接著，主基地台計算 $P_{HA} = h(PW_{MU} \| N_{FA})$ 及 $S_{HA} = h(ID_{FA} \| N_{FA}) \oplus r_{MU} \oplus P_{HA}$ 後將$\{S_{HA}, P_{HA}\}$回傳給外部基地台。

步驟三、 外部基地台收到$\{S_{HA}, P_{HA}\}$，計算 $S'_{HA} = h(ID_{FA} \| N_{FA}) \oplus r_{MU} \oplus P_{HA}$ 並與收到的 S_{HA} 比較，以確認主基地台是否合法。如果比較結果不同，則認證流程終止。當結果相同，外部基地台計算 $S_{FA} = h(S_{HA} \| N_{FA} \| N_{HA})$後選擇隨機亂數$a$，使用 Elliptic Curve Diffie-Hellman (ECDH) [9]計算出在橢圓曲線方程式 E 上的一點 $a*P$，$a*P$ 可表示為 aP，後將$\{S_{FA}, aP, P_{FA}=(S_{HA} \| ID_{FA} \| N_{FA})\}$傳送給行動用戶。

步驟四、 行動用戶計算 $S'_{HA} = h(ID_{FA} \| N_{FA}) \oplus r_{MU} \oplus P_{HA}$，且與收到的 S_{HA} 比較。接著計算 $S'_{FA} = h(S_{HA} \| N_{FA} \| N_{HA})$，並與收到的 S_{FA}

比較是否相等，如比較結果皆相等，則行動用戶可以認證主基地台與外部基地台為合法的，否則流程終止。之後，行動用戶選擇隨機亂數 b 計算出橢圓曲線方程式 E 上的一點 $b*P$，$b*P$ 可表示為 bP 且 $aP*bP$ 可表示為 abP，行動用戶使用 aP 與 bP 計算出交談金鑰 $K_{MF} = h(abP)$，與 $S_{MF} = f_{KMF}(N_{FA} \| bP)$後，將$\{bP, S_{MF}\}$傳送給外部基地台。

步驟五、 外部基地台收到$\{bP, S_{MF}\}$後，使用 aP 與 bP 計算 $K_{MF} = h(abP)$，再計算 $S'_{MF} = f_{KMF}(N_{FA} \| bP)$，並與收到的 S_{MF} 比較，如果不相同那麼該 K_{MF} 於行動用戶與外部基地台間並不合法，則流程結束。若比較結果相等，則外部基地台可以認證行動用戶為合法的。

交談金鑰更新階段

步驟一、 行動用戶選擇新的隨機亂數 b_i，計算出 b_iP (i = 1, 2, …, n)將$\{b_iP\}$傳送給外部基地台。

步驟二、 外部基地台收到$\{b_iP\}$，選擇新的隨機亂數 a 並計算 a_iP (i = 1, 2, …, n)，產生新的 $K_{MFi} = h(a_ib_iP)$，計算 $S_{MFi} = f_{KMFi}(a_ib_iP \| a_{i-1}b_{i-1}P)$將$\{a_iP, S_{MFi}\}$傳送給行動用戶。

步驟三、 行動用戶收到$\{a_iP, S_{MFi}\}$，使用 a_iP 計算出新的 $K_{MFi} = h(a_ib_iP)$，再計算出 $S'_{MFi} = f_{KMFi}(a_ib_iP \| a_{i-1}b_{i-1}P)$，並與收到的 S_{MFi} 比較。若結果相等，則行動用戶使用新的 $K_{MFi} = h(a_ib_iP)$。若結果不同，則不使用此把 $K_{MFi} = h(a_ib_iP)$，並通知外部基地台與主基地台此結果。

根據以上步驟，我們在此提出 Mun 等學者機制[8]的弱點，他們的方法在認證與協議交談金鑰階段可能存在著非法用戶冒用合法行動用戶存取服務的可能性，說明如下。

離線資訊破解

於此節將呈現 Mun 等學者架構交談金鑰洩漏之弱點。首先，攻擊者於與行動用戶相同之外部基地台註冊完成後，可以在認證與協議交談金鑰階段之步驟一至四中，取得其他合法行動用戶的$\{ID_{HA}, N_{HA}, r_{MU}\}$、$\{ID_{FA}, N_{FA}\}$、$\{S_{HA}, P_{HA}\}$、$\{aP\}$和$\{bP\}$。攻擊者透過這些資訊可以計算出 $K_{MF} = h(abP)$，並計算出行動用戶回合交談金鑰 $S_{MF} = f_{KMF}(N_{FA} \| bP)$。為了解決上述弱點，我們將在下一章節提出我們的方法。

3. 我們的架構

本文所提出的方法分為行動用戶註冊與交互驗證兩個階段。三個主要參與者：行動用戶、外部基地台及主基地台。本方法所使用的符號如表 2。

表 2、我們的架構之符號說明

符號	敘述
MU	(Mobile User)行動用戶
FA	(Foreign Agent)外部基地台
HA	(Home Agent)主基地台
ID_a	角色 a 的身分識別碼
PWa	角色 a 的密碼
$h(.)$	單向雜湊函數
A_a	驗證角色 a 的資訊
N_x	角色 a 的大隨機亂數
$\oplus$	XOR 運算
$\|$	字串連結運算
X_a	角色 a 的私密金鑰
T	時間戳記
$A \stackrel{?}{=} B$	比較 A、B 是否相等

行動用戶註冊階段

在這個階段中，行動用戶 MU 透過安全通道向主基地台 HA 註冊，以取得身分認證相關資訊，詳細說明如下：

步驟一、 行動用戶將自身的身分識別碼 ID_{MU} 以及密碼 PW_{MU} 傳送給主基地台。

步驟二、 主基地台產生隨機亂數 N_{HA}，計算 $SID = h(ID_{MU} \| N_{HA})$ 及 $r_{MU} = h(SID \| X_{HA}) \oplus PW_{MU}$，將$\{SID, r_{MU}\}$透過安全通道(Secure channel)傳送回去給行動用戶。

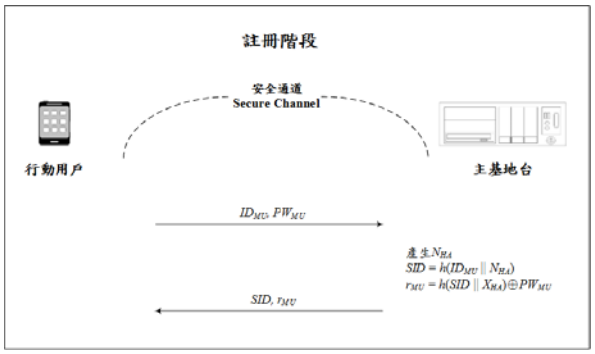


圖 1、行動用戶註冊階段

交互認證階段

此階段中，行動用戶已於外部基地台(FA)服務範圍內漫遊，外部基地台將行動用戶認證資訊轉送至主基地台並透過主基地台的協助來認證行動用戶身分，同時行動用戶也可以透過主基地台來認證外部基地台，步驟詳細說明如其下。

步驟一、 行動用戶輸入密碼 PW_{MU}，計算 $h(SID \| X_{HA}) = r_{MU} \oplus PW_{MU}$，產生亂數 N_{MU} 和時間戳記 T，計算 $A_{MU} = h(h(SID \| X_{HA}) \| T) \oplus N_{MU}$ 與 $C_{MU} = h(SID \| N_{MU}) \oplus ID_{MU}$，並將$\{SID, A_{MU}, C_{MU}, T\}$傳送給外部基地台。

步驟二、 外部基地台收到$\{SID, A_{MU}, C_{MU}, T\}$，將$\{SID, A_{MU}, C_{MU}, T, ID_{FA}\}$轉送至主基地台。

步驟三、 主基地台收到$\{SID, A_{MU}, C_{MU}, T, ID_{FA}\}$後為驗證用戶身分，計算 $N_{MU} = A_{MU} \oplus h(h(SID \| X_{HA}) \| T)$、$ID_{MU} = C_{MU} \oplus h(SID \| N_{MU})$與 $SID' = h(ID_{MU} \| N_{HA})$。比較 SID' 是否與 SID 相等。如果相等則 SID 為真，且與 ID_{MU} 為同一組，A_{MU} 與 C_{MU} 於傳送過程中沒有被竄改，行動用戶是合法用戶。

步驟四、 主基地台計算出 $A_{HA} = h(SID \| X_{HA}) \oplus h(ID_{FA} \| ID_{MU})$與 $C_{HA} = h(h(ID_{FA} \| SID) \| ID_{FA})$以及交談金鑰 $SK = h(ID_{FA} \| SID \| N_{MU})$和 $C_{SK} = h(SK \| h(ID_{FA} \| ID_{MU}))$之後將$\{A_{MU}, C_{HA}, C_{SK}\}$傳送給外部基地台。

步驟五、 外部基地台收到$\{A_{MU}, C_{HA}, C_{SK}\}$後，將$\{A_{MU}, C_{HA}, C_{SK}\}$回傳行動用戶。

步驟六、 行動用戶收到$\{A_{MU}, C_{HA}, C_{SK}\}$後計算 $h(ID_{FA} \| ID_{MU}) = A_{HA} \oplus h(SID \| X_{HA})$，接著計算 $C'_{HA} = h(h(ID_{FA} \| SID) \| ID_{FA})$，並比較 C'_{HA} 與 C_{HA} 是否相等，若相等則主基地台是有效的，且外部基地台也可以被認證。

步驟七、 接著計算 $SK = h(ID_{FA} \| SID \| N_{MU})$以及 $C'_{SK} = h(SK \| h(ID_{FA} \| ID_{MU}))$，之後核對 C'_{SK} 與 C_{SK} 是否相等，若相等則完成交互認證，並產生出行動用戶與主基地台之間加解密的回合金鑰 SK。

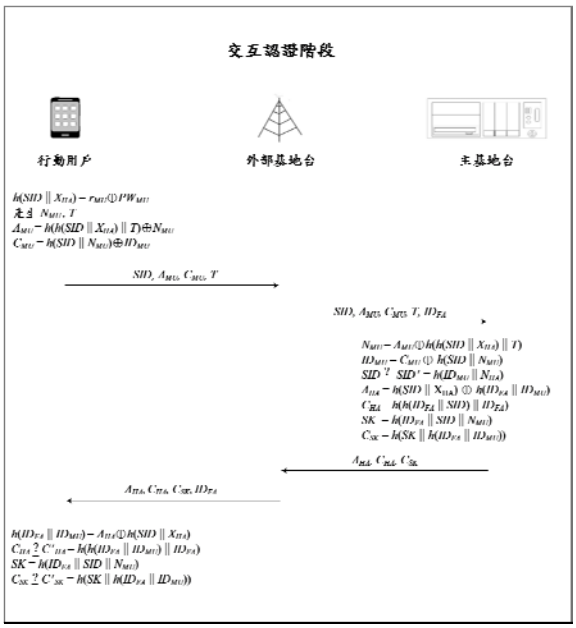


圖 2、交互認證階段

根據上述步驟，主基地台不需要將 SID、行動用戶身分識別碼或是其他相關資訊另外儲存在資料庫中。

4. 討論與分析

在此節中，我們對本文所提出的方法做安全性的分析，以下我們提出幾種攻擊方法來分析安全性

以及與 Mun 等學者的架構作計算成本之比較。安全性分析如下。

外部攻擊(Outsider attack)

假設有一攻擊者想要計算主基地台之秘密金鑰 X_{HA}，攻擊者可以從行動用戶傳送給外部基地台的$\{SID, A_{MU}, C_{MU}, T\}$中，擷取 SID, A_{MU} 做分析。假設一，若攻擊者想計算 $SID = h(ID_{MU} \| N_{HA})$，那麼攻擊者需要 ID_{MU} 及 N_{HA}，但於認證過程中並不會傳送 N_{HA}，因此攻擊者無法計算出 SID。假設二，若攻擊者想分析 $A_{MU} = h(h(SID \| X_{HA}) \| T) \oplus N_{MU}$，首先得知道 N_{MU} 才能夠和取得的 A_{MU} 一起運算得到 $h(h(SID \| X_{HA}) \| T)$，再經過分析得到 X_{HA}，但認證過程中並不會明文傳送 N_{MU}，因此攻擊者無法取得，即使攻擊者取得 N_{MU}，X_{HA} 也有單向雜湊函數所保護，因此攻擊者無法計算出主基地台的私密金鑰 X_{HA}。根據上述的推斷可以顯示出我們的方法能夠抵檔攻擊者發出的外部攻擊。

內部攻擊(Insider attack)

假設有 N 個惡意的行動用戶企圖逃避主基地台認證，並試圖計算主基地台之秘密金鑰 X_{HA}，當攻擊者取得 $A_{MU} = h(h(SID \| X_{HA}) \| T) \oplus N_{MU}$，但是 X_{HA} 使用了單向雜湊函數保護，因此即使利用 SID、T 及 N_{MU} 想要計算出來是不可能的。因此根據上述分析，我們的方法可以防止內部攻擊。

偽裝攻擊(Impersonation attack)

假設有一攻擊者想要偽裝成合法的行動用戶，並擷取行動用戶與外部基地台以及外部基地台與主基地台之間傳送的$\{SID, A_{MU}, C_{MU}, T, ID_{FA}\}$，來偽裝成是一個合法行動用戶嘗試騙取主基地台的認證，但是 A_{MU} 內包含有時間戳記，一但時戳過期即無法通過認證且 SID、A_{MU} 和 C_{MU} 皆有單向雜湊函數所保護，攻擊者無法竄改其內容或計算出更多的訊息，也因此攻擊者是無法偽裝成合法用戶的。根據上述之原因，可以證明我們的方法能夠防止攻擊者的偽裝攻擊。

重送攻擊(Replay attack)

假設有一攻擊者想要透過攔截合法使用者交互認證階段傳輸的資訊，並且透過將資訊重送來達到騙取服務或者破解相關資訊的目的。以上述流程來看，若攻擊者竊取 $A_{MU} = h(h(SID \| X_{HA}) \| T) \oplus N_{MU}$ 與 $C_{MU} = h(SID \| N_{MU}) \oplus ID_{MU}$，$X_{HA}$ 皆有單向雜湊函數保護且僅有主基地台知道，N_{MU} 並未公開傳輸且僅有行動用戶知道、主基地台可解出，且若直接將$\{A_{MU}, C_{MU}\}$重新傳送給外部基地台，將會因時戳過期而被捨棄，而修改 A_{MU} 則會使與 SID 無法相互認證，讓我們判定為攻擊者所傳送。根據上述的推斷可以顯示出我們的方法能夠抵檔攻擊者發出的重送攻擊。

驗證表竊取攻擊(Stolen-Verifier attack)

現今行動用戶的認證的主體主要是行動裝置本身或是 SIM 卡，在這種情況下當手機遺失被撿取，合法用戶即有被冒用的風險，我們假設有一合法使用者不小心遺失其手機，而被攻擊者拾獲，當攻擊者想要存取服務時，由於不知道合法用戶之密碼，因此無法通過基地台認證，進而存取行動漫遊服務的，且主基地台與外部基地台並不會存放驗證表，當攻擊者攻擊主基地台時無法竊取行動用戶驗證過程的相關資訊，根據上述理由，我們的方法能夠抵擋驗證表竊取攻擊。

計算成本分析

在本節中，我們將分析 Mun 等學者的方法與本文所提出的方法之計算成本。表 3 顯示出行動用戶與主基地台方面之計算成本，根據表 3 可以顯示出我們所提出的方法相對於 Mun 等學者的方法，其計算成本降低許多。我們的方法並無使用橢圓曲線加密法或是非對稱式加密法，而是採用運算量較低的互斥或運算以及單向雜湊函數來保護驗證資訊，所以我們的方法更加的有效率。

表 3、兩種方法之計算成本比較

方法 / 參與者	MUN 等學者的方法	我們的方法
行動用戶	5*Hash* + 2*XOR* + 1*Asym* + 2*ECDH*	5*Hash* + 4*XOR*
外部基地台	4*Hash* + 2*XOR* + 1*Asym* + 2*ECDH*	12*Hash* + 4*XOR*
主基地台	5*Hash* + 3*XOR*	13*Hash* + 4*XOR*
總計	14*Hash* + 7*XOR* +2*Asym.* + 4*ECDH*	30*Hash* + 12*XOR*

Asym:非對稱式加密法
ECDH:橢圓曲線加密法
Hash:單向雜湊函數
XOR:互斥或運算

5. 結論

於本篇論文中，我們提出了一個全新的行動網路服務匿名性認證機制，主基地台不需要儲存行動用戶認證過程的驗證表，能降低設備負擔，也能夠避免驗證表被竊取的風險。行動用戶於漫遊時，外部基地台並不會直接取得用互相關資訊，能夠保障行動用戶之隱私，且我們的方法有著低計算成本的優勢，因為它不需要作橢圓曲線系統或公開金鑰系統的加解密運算。因此相較於先前學者所提出的相關方法，本文所提出之方法更符合現實環境且更有效率，可應用於網路服務提供者所提供之服務，且認證方式更適用於行動裝置之使用。

參考文獻

[1] S. Suzuki, and K. Nakada, “An authentication technique based on distributed security management for the global mobility network”, *IEEE Journal on Selected Areas in Communications.* , Vol. 15, No. 8, pp. 1608-1617, Oct. 1997.

[2] K. F. Hwang and C. C. Chang, “A self-encryption mechanism for authentication of roaming and teleconference services”, *IEEE Transactions on Wireless Communications*, Vol. 2, No. 2, pp. 400-407, Mar. 2003.

[3] J. Zhu and J. Ma, “A new authentication scheme with anonymity for wireless environments”, *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 1, pp. 231-235, Feb. 2004.

[4] X. Yi, C. K. Siew, and C. H. Tan, “A secure and efficient conference scheme for mobile communications”, *IEEE Transactions on Vehicular Technology*, Vol. 52, No. 4, pp. 784-793, Jul. 2003.

[5] T. F. Lee and T. Hwang, “Provably secure and efficient authentication techniques for the global mobility network”, *The Journal of Systems and Software*, Vol. 84, No. 10, pp. 1717-1725, Oct. 2011.

[6] C. C. Wu, W. B. Lee and W. J. Tsaur, “A secure authentication scheme with anonymity for wireless communications”, *IEEE Communications Letters*, Vol. 12, No. 10, pp. 722-723, Oct. 2008.

[7] P. Zeng, Z. F. Cao, K. K. Choo and S. B. Wang, “On the anonymity of some authentication schemes for wireless communications”, *IEEE Communications Letters*, Vol. 13, No. 3, pp. 170-171, Mar. 2009.

[8] H. Mun, K. Han, Y. S. Lee, C. Y. Yeun and H. H. Choi, “Enhanced secure anonymous authentication scheme for roaming service in global mobility networks”, *Mathematical and Computer modeling*, Vol. 55, No. 1–2, pp. 214-222, Jan. 2012.

[9] D. Hankerson, A. J. Menezes and S. Vanstone, “Guide to elliptic curve cryptography”, Springer-Verlag Inc., Berlin, Germany, 2004.

因應個資法規範建構 PDF 文件資料遮罩之低成本工具組合

蔡敦仁　　樂家祥
中國文化大學資訊管理學系研究所
pw3215@pchome.com.tw

摘要

個人資料保護法（個資法）[1]已於 2012 年 10 月 1 日正式施行。由於該法不分行業一體適用，對於為數眾多的小型企業及個人，如何處理及利用含有個資之電子文件，問題亟待解決，已形成相當壓力與負擔。因應個資法規範之安全需求，資料遮罩（Data Masking）[2]不失為根本解決方法之一。目前提供類似功能之商業軟體頗多，惟因價格偏高，使用成本負荷較重，不易普及。

本研究針對 PDF[3]文件，嘗試運用網路上可取得之免費軟體及試用軟體，搭配建立一套幾近零支出之工具組合，使之具備完整必要功能，供使用者自行下載且易於使用，提升電子文件處理及利用之安全性，符合個資法規範。

關鍵詞：個資法、資料遮罩、PDF 文件、免費軟體、試用軟體

Abstract

Personal Information Protection Act had already implemented formally on October 1st , 2012. Without discrimination to all vocations, the new law has been getting public department and numbers of Individual enterprises into trouble with looking for a legal way using e-documents with personal information. In order to follow rules of Personal Information Protection Act, data masking is one of the radical methods to solve the anxieties. Because of a high price, several software with data masking function haven't been popularized so far.

In this search, we will focus on PDF documents. Trying to find out Freeware or Trialware which you can get it easily from the internet and combines them to mask data perfectly. We expect these user-friendly data masking software' sets shall be a law-abiding method to keep e-documents with personal information confidential.

Keywords：Personal Information Protection Act, Data masking, PDF documents, Freeware, Trialware

1. 前言

現行個資法對於公務或非公務機關乃至個人對於個人資料之蒐集、處理及利用，規範更加嚴謹[4]。由於新法不分行業一體適用，且要求各公、民營單位及個人必須舉證說明無過失或無故意違反法律[5]。

網路媒體 iThome[6]於 2012 年 10 月 1 日至 8 日，就個資法問題，透過網路問卷和電子郵件問卷，針對國內五千大企業或營收規模相當的企業 IT 主管進行調查，結果顯示，其中只有約 45.9%企業開始執行因應措施。在防護措施方面，大部分公司採用較熟悉的備份、加密、銷毀、稽核、資料庫防火牆等作法，僅 17.7%企業表示已經或預計採用資料遮罩[7]。大型企業尚且如此，中、小型企業恐難以樂觀，遑論個人。就承辦人或檔案持有人立場而言，最困擾與擔心的問題，無非是含有個資之檔案外洩所衍生之法律責任，資料遮罩因可避免原始文件之個資明示於文件，個資不露白，相關的訴訟就不會產生[8]。

歸納承辦人或檔案持有人在前述情境中之主要作業需求為「資料遮罩」；為保護資料不被篡改，則需具「文件保全」功能；為使遭遮蔽之資料仍能取得，須有「內容回復」功能。

PDF 文件格式因不受作業系統平台限制，可將文字、字型、格式、顏色及獨立於設備和分辨率的圖形影像等封裝在一個文件中，加密後可限制文件內容不受未經授權者存取，避免作者或送件者任意修改文件，復因大多數文件、表格、圖形和網頁均可轉換為 PDF 文件，遂廣為各公、民營單位及個人採用。

個資法規範無可迴避，意謂大多數承辦人員（文件保管者）均存在作業需求，而坊間相關商業軟體工具因單價不低（每套至少新臺幣三千元以上），對機關及個人造成一定負擔。

本研究就個資法相關規範，從承辦人（文件保管者）角度，針對 PDF 文件之安全及內容控管，建構功能完整之低成本工具組合，其應具備以下條件：

一、 組合所含之工具易於合法取得及使用（易取可用）。
二、 功能須符合個資法規範之需求（合用）。
三、 成本低廉（免費）。
四、 工具操作方式簡易，無需先經繁複學習過程（易用）。
五、 文件經組合處理後具相當安全性（文件安全）。
六、 文件經工具非更改內容之處理後仍可回復原始文件內容（文件回復）。
七、 組合具可調整性，視需求可增減或更換工具

（彈性）。

研究就前述方向，針對「資料遮罩」、「文件保全」、「內容回復」三項作業需求，參考 Acrobat Professional XI 相關功能，選取網路上之免費軟體及試用軟體，搭配建構接近需求之工具組合，再比較優劣利弊，擇取較合宜者，做為本研究推薦組合。供廣大公務或非公務機關承辦人員、資料保管人員及個人，在符合該工具開發商（設計者）授權範圍內的一個選項，以符合個資法規範。

2. 文獻探討

2.1 個資法簡介

個資法前身為「電腦處理個人資料保護法」，於 2010 年 4 月 27 日經立法院三讀通過，同年 5 月 26 日由總統公布，計分 6 章共 56 條條文；除第 6、54 條條文之施行日期由行政院另定，其餘條文已自 2012 年 10 月 1 日起施行。

個資法與資料遮罩相關條文[8]包括第 9 條第 2 項第 4 款、第 16 條第 5 款、第 19 條第 4 款、第 20 條第 5 款（概為：基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者。）及第 41 條（罰則）。

2.2 資料遮罩

資料遮罩[2]是在資料儲存區中，將特定資料遮蔽起來的一種處理技術，目的在確保敏感資料被看似逼真的資料所取代或將敏感資料遮蔽。資料遮罩技術依執行時機與執行方式而異，現行常見資料遮罩技術，依執行方式可分為資料錯置（Shuffling）、資料遮蔽（Masking）、資料加密（Encryption）、資料移除（Nulling Out Or Deletion）及資料變異（Number and Date Variance）5 類[7]。

2.3 PDF 文件

PDF(Portable Document Format 簡稱，意謂「攜帶型文件格式」)[3]係美國 Adobe 公司於 1993 年開發之檔案標準，其副檔名即為 PDF。PDF 格式發展過程主要有三項技術，包括衍生自 PostScript 之系統、字型嵌入系統、資料壓縮及輸入、輸出系統。初期由 Adobe 公司發行之 Adobe Acrobat 製作檔案，該公司並推出僅具閱讀、列印等非編輯功能之免費軟體 Adobe Reader，以利推廣 PDF 格式。由於 PDF 格式具備跨平台、能保留文件原有格式(layout)、開放標準，且能免版稅(royalty-free)自由開發 PDF 相容軟體等優點，加上 Adobe 公司持續研發，使 PDF 檔案加入讓使用者編輯、注釋、審閱檔案、擷取網頁、設定密碼限制存取、數位簽章等功能，PDF 格式逐漸為使用者所接受而普及。至 2007 年，由美國家標準協會 ANSI 公布有關列印內容的 PDF 標準，包括適用於封存的 PDF/A，適用於工程的 PDF/E，以及適用於列印的 PDF/X，同年 12 月，PDF 成為 ISO 32000 國際標準。

2.4 免費軟體

免費軟體（Freeware）[9]指一切不需使用費用購買的電腦軟體。開發者通常是因為興趣、名氣等原因而主動分享。亦有部分係因為不滿足或想改善現有軟體而修改某些程式、更有自行開發另一替代程式等等。某些自由軟體(Free Software)或開放源碼軟體(Open Source Software)並非免費軟體，反之亦然。

2.5 試用軟體

試用軟體（Trialware）[10]又稱共享軟體(Shareware)或演示軟體（Demoware），是一種以限制使用期限、使用次數或縮減功能之形式，免費發布的商業軟體，目的讓使用者試用後產生購買意願。因此，許多軟體開發商為爭取使用者支持，即使試用期屆滿，仍維持試用狀態。

試用軟體除限制時間、用量或縮減功能外，其中某些對於試用後匯出時的檔案，會強制加入浮水印或字幕，通常是軟體開發商的商標、軟體名稱或其他文字聲明，另有某些試用軟體則是加入廣告，一旦使用者付費購買後，即可獲得授權而取消廣告。

3. 研究方法

為符合個資法規範，對於使用者端有關 PDF 文件編輯之「資料遮罩」、「文件保全」、「內容回復」三項作業需求，參考 PDF 編輯工具 Adobe Acrobat 具備之相關功能，建立文件處理工具組合模型（如圖 1），據以搜尋下載、測試篩選所需之免費軟體及試用軟體，作為實驗所需之基本工具，並嘗試建構文件處理工作流程，達成研究目標。

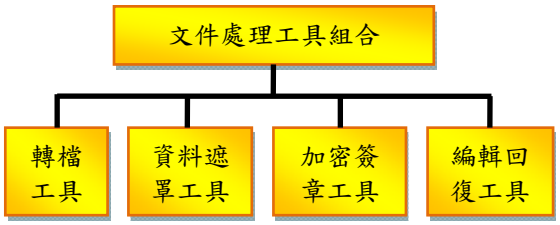


圖 1 文件處理工具組合模型圖

考量實務上承辦人員作業時使用 PC 之組態，

本研究工具軟體測試環境如次：

硬體設備：PC 一台（CPU:Intel Pentium Dual-Core E5700 3.0 GHz；RAM:2G Byte）

作業系統：Windows 7 sp1；連接網際網路。

各類工具軟體測試比較表如表 1 至表 5：

表 1 轉 PDF 檔工具測試比較表

工具名稱	軟體種類	被轉檔案類型	設定 PDF 檔密碼	其他限制
PDF Creator	免費	不限	V	
Doro PDF Writer	免費	不限	V	
doPDF	免費	不限	×	
PDFill PDF Tools	免費	Image	V	
Foxit PDF Creator	試用	不限	V	試用期限 30 日
Gaaiho PDF Driver	試用	不限	V	試用期限 30 日
PdfFactory Pro	試用	不限	V	PDF 檔每頁下方有訂購此軟體文字提示

表 2 PDF 檔轉影像檔工具測試比較表

工具名稱	軟體種類	轉出影像檔類型	其他功能與限制
PDF To JPG Converter	免費	png、gif、bmp、jpg、tif	可逐頁或指定某頁轉為圖檔且支援多檔案批次轉檔
PDFill PDF Tools	免費	png、gif、bmp、jpg、tif、pcx、	可逐頁或指定某頁轉為圖檔；轉檔遇中
		wmf、emf	文部分易出現亂碼

表 3 資料遮罩工具測試比較表

工具名稱	軟體種類	遮蔽內容回復選項		其他限制
		可回復	無法回復	
VeryPDF PDF Editor	試用	V	×	輸出檔頁角有浮水印（浮水印較易清除）
Foxit Phantom PDF	試用	×	V	試用期限 60 日
Gaaiho PDF Doc	試用	V	V	試用期限 30 日

表 4 加密（簽章）工具測試比較表

工具名稱	軟體種類	功能			其他限制
		加密	解密	簽章	
PDFill PDF Tools	免費	V	V		
Doro PDF Writer	免費	V			
VeryPDF PDF Editor	試用	V		V	輸出檔頁中有文字提示浮水印
PDFCreator	免費	V			
PDF-XChange Viewer	免費	V	V	V	使用簽章需先提升版本且輸出檔頁角有浮水印

表 5 編輯及回復工具測試比較表

工具名稱	軟體種類	編輯及回復選項		其他限制
		編輯	回復	
PDF-XChange Viewer	免費	V	V	
Foxit Phantom PDF	試用	V	V	試用期限 60 日
Gaaiho PDF Doc	試用	V	V	試用期限 30 日

初步篩選工具組合及評估其符合部分條件如表 6：

表 6 文件處理工具組合部分條件表

工具名稱	軟體種類		符合條件			
	免費	試用	易取可用	合用	免費	易用
PDF Creator	V		V	V	V	V
PDF To JPG Converter	V		V	V	V	V
VeryPDF PDF Editor		V	V	V	V	V
PDF-XChange Viewer	V		V	V	V	V
PDFill PDF Tools	V		V	V	V	V

文件處理工作流程如圖 2：

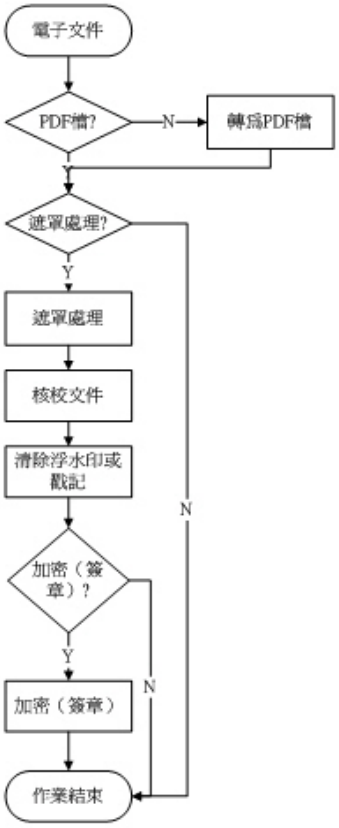


圖 2 文件處理工作流程圖

4. 實驗設計、結果與分析

4.1 實驗設計

一、實驗環境：如前「研究方法」所述。

二、實驗工具：自文件處理工具組合（如表 6）挑選。

三、實驗檔案：snake.doc（自建 word 文件）

四、實驗流程：本研究之實驗概分為 4 個，說明如次：

（一）實驗 1：依文件處理工作流程圖（如圖 2），選擇工具軟體，透過不同的工具軟體執行相關功能，以找出待解決之關鍵步驟。

（二）實驗 2：針對關鍵步驟建構新的實驗流程，續行實驗，以解決問題並持續改進實驗流程。

（三）實驗 3：針對實驗 2 流程之弱點，重新設計實驗流程，改善解決問題方式。

（四）實驗 4：針對實驗 2、實驗 3 之結果，進行檔案回復及安全性測試並提出改善方法，以滿足文件處理之各類需求狀態。

4.2 實驗結果分析

一、實驗 1：

（一）步驟：依文件處理工作流程圖，分別選擇 PDF Creator（轉檔）、VeryPDF PDF Editor（遮罩）、PDF-XChange Viewer（核校、加密），結果 VeryPDF PDF Editor 在輸出檔案加上浮水印，餘皆正常。

（二）分析：由前項結果，關鍵步驟應係資料遮罩作業時或作業後，編輯過之檔案頁面，均存在浮水印，乃重新設計實驗流程如圖 3，作為實驗 2 之流程。

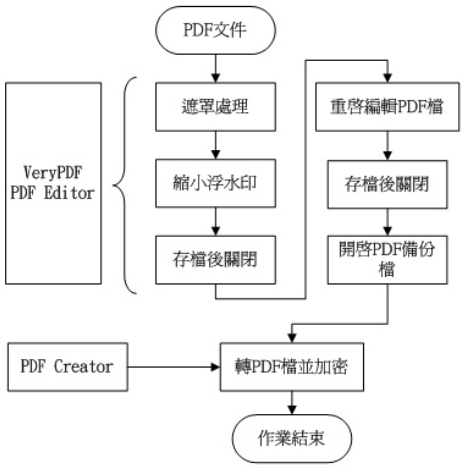


圖 3 實驗 2 流程圖

二、實驗 2：

（一）步驟：依圖 3，分別選擇 VeryPDF PDF Editor（遮罩）、PDF Creator（轉檔及加密）進行實驗，以 Adobe Acrobat 檢視實驗結果，確認最終之 PDF 文件無浮水印，符合需求。

（二）分析：此實驗結果雖符合需求，但過程略為繁複，恐一般承辦人員不易操作，另透過 PDF Creator 之類轉檔工具設定密碼亦嫌複雜。乃重新設計實驗流程如圖 4，作為實驗 3 之流程。

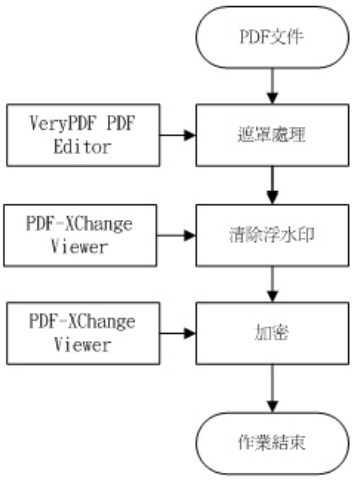


圖 4 實驗 3 流程圖

三、實驗 3：

（一）步驟：依圖 4，分別選擇 VeryPDF PDF Editor（遮罩）、PDF-XChange Viewer（清除浮水印及加密）進行實驗，以 Adobe Acrobat 檢視，確認實驗結果符合需求。

（二）分析：此實驗結果符合文書處理需求且步驟簡要，允為較佳方法。

四、實驗 4：

（一）步驟：自網路下載破解 PDF 密碼軟體（如 AP PDF Password Recovery、PDF Password Remover、Appnimi PDF Unlocker、Advanced PDF Password Recovery Pro 等）測試破解加密 PDF 文件；另針對需 PDF 文件遮蔽資料無法回復者（畢竟數位加密方式無法完全防範破解），設計實驗流程如圖 5，製作無法回復資料遮罩之 PDF 文件，實驗結果略如表 7。

（二）分析：以本研究實驗 2 及實驗 3 製作之 PDF 文件，其資料遮罩可回復，因此製作之 PDF 文件應予加密，以確保資料遮蔽作用。而設定雙密碼（開啟密碼及變更權限密碼）之 PDF 文件安全性較高；單一密碼之 PDF 文件易遭破解。若希望文件遮蔽資料不可回復，可採圖 5 之 PDF→影像→PDF 方式建立 PDF 文件。

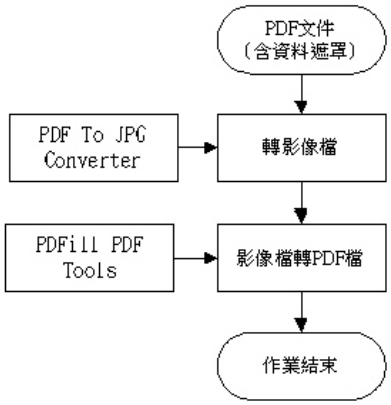


圖 5 製作遮蔽資料不可回復 PDF 文件流程圖

表 7 PDF 文件加密狀態及安全性比較表

文件狀態	回復方式	回復難易	安全性
未設密碼	直接編輯	易	最弱
一道密碼	破解或轉檔	易	弱
二道密碼	逐道破解	難	強
PDF 檔轉圖形檔再轉 PDF 檔	無	最難	最強

4.3 實驗結果探討

本研究規劃進行的 4 個實驗，其結果大致符合預期目標，使研究進展順利，得以建構符合需求之工具組合（文件處理工具組合條件表如表 8），綜合實驗過程及結果之成效如次：

一、選用之工具組合符合實驗需求。

二、實驗結果足以解決文書處理問題。

三、實驗流程設計簡要易於操作。

四、工具組合成本極低且大致符合預期目標。

表 8 文件處理工具組合條件表

工具名稱	符合條件						
	易取可用	合用	免費	易用	文件安全	文件回復	彈性
PDFCreator	V	V	V	V	V	V	V
PDF To JPG Converter	V	V	V	V	V	X	V
VeryPDF PDF Editor	V	V	V	V	V	V	V
PDF-XChange Viewer	V	V	V	V	V	V	V
PDFill PDF Tools	V	V	V	V	V	V	V
備註	PDF To JPG Converter 主要作用在防止文件內容回復。						

5. 結論

通過本研究，我們成功得出 2 種 PDF 文件資料遮罩之執行方法（實驗 2、實驗 3），主要差別在於前者係以操縱滑鼠縮小浮水印方式，使備份檔保有資料遮罩且去除浮水印；後者則直接經由編輯方式去除浮水印。實驗結果顯示此兩種方法均符合文件處理之需求。

因該二法之資料遮罩均可回復內容，本研究更提出「遮蔽資料不可回復」之製作方式，兼顧 PDF 文件之安全性，充分滿足「資料遮罩」、「文件保全」、「內容回復」3 項需求。更由於各項工具易於取得，易於使用，且均屬免費或試用性質，幾近零支出，大幅提高使用者接受度。

本研究雖以 PDF 檔案為研究主體，但在實驗過程中，透過雙向轉檔之執行與測試，事實上已包含大多數電子文件及影像檔案格式的處理技巧，幾乎不受限於檔案格式。可以說，我們提供的是一整套免費的全方位解決方案。

本研究之主要貢獻，在介紹可免費取用之作業工具組合，供廣大公務或非公務機關承辦人員、資料保管人員及個人，在符合該工具開發商（設計者）授權範圍的一個選項。因個資法已正式施行，全臺民眾幾皆面臨個資處理及利用問題。由於坊間具文件處理相關功能之商業軟體，最廉價者每套仍需三千餘元，假設全國有十分之一人口有此需求，則其潛在商機達數十億元。若採用本研究所推薦之免費工具，將可大幅減輕經濟負荷，亦可符合個資法規範。

參考文獻

[1] 個人資料保護法（2010-5-26）。臺北市：法務部。

[2] Wikipedia(2013). Data masking. 2013-3-15, From http://en.wikipedia.org/wiki/Data_masking

[3] Wikipedia(2013). Portable Document Format. 2013-2-2, From http://en.wikipedia.org/wiki/Portable_Document_Format

[4] 呂丁旺（2010）。淺析修正「個人資料保護法」。月旦法學雜誌，183，131-146。

[5] 羅一倫（2012）。論個人資料保護法對產業之影響與因應（未出版碩士論文）。東吳大學法律學系，臺北市。

[6] 李宗翰、吳其勳、王宏仁、張景皓、黃彥棻(2012)。iThome 2012 年個資法大調查。2013 年 4 月 10 日，From iThome 電腦報 http://www.ithome.com.tw/itadm/article.php?c=77042

[7] 賴威慎、許嘉家(2012)。應用系統之資料遮罩技術實作分享。財金資訊季刊，71，56-64。

[8] 李宗翰（2012）。運用個資遮罩，為重要個資穿上金鐘罩—既保護個資，也讓作業流程不打結。2013 年 3 月 6 日，From iThome 電腦報 http://www.ithome.com.tw/privacylaw/article/77886

[9] 維基百科(2013). 免費軟體. 2013-3-11, From http://zh.wikipedia.org/wiki/免費軟體

[10] 維基百科(2013). 試用軟體. 2013-3-11, From http://zh.wikipedia.org/wiki/試用軟件

智慧電網家庭閘道器資安驗證標準之制定與應用
--資訊安全與實體安全整合評估

林佳瑩[1]　易俗[2]　范金鳳[1]
[1]元智大學資訊工程系　[2]健行科技大學資訊工程系
csfanc@saturn.yzu.edu.tw　swuyih@uch.edu.tw

摘要

智慧電網家庭閘道器不僅需考慮資訊安全（security）議題，亦需考慮到資訊安全漏洞可能引起之實體安全（safety）影響。後者在此類應用上尚未廣被重視。本研究針對此現象，制定以能處理資訊安全及實體安全兩方面需求的智慧電網家庭閘道器資安驗證標準。作法首先延伸德國 BSI 之智慧電網閘道保護剖繪，為其新增及修正了實體安全相關的章節及元件；接著根據此延申之保護剖繪制定了一套對照的驗證準則；最後以一商用之閘道器為個案，顯示我們所提之資安驗證標準之有效性。

關鍵詞：智慧電網、家庭閘道器、實體安全、資訊技術安全評估共同準則、保護剖繪。

Abstract

Smart grid home gateway needs to consider both the information security and the physical safety issues. However, the safety issue has not yet been widely emphasized. This research project developed an information security certification standard for smart grid home gateway, and the standard emphasizes both of the information security and physical safety requirements. First, we extended the newest Gateway Protection Profile (PP) of a Smart Metering System by German BSI [4] to include safety-related information and to develop safety-related CC components. Then we defined a corresponding certification standard for this proposed PP. Finally, a case study was conducted to demonstrate the effectiveness of the proposed certification standard.

Keywords: smart grid, home gateway, safety, common criteria, protection profile.

1. 緒論

智慧電網[1]將傳統的電力系統與現代資通訊技術結合，整合發電、輸電、配電、及用戶端裝設智慧電表，搭配電腦監控、診斷及修復等功能，可提升電力的使用效率。世界各國為因應節能減碳之趨勢，皆積極推動「智慧電網」之研究。

資訊安全（security）為智慧電網的核心議題；若連上電網的用戶端為工業控制系統、智慧家電控制系統等，智慧電網進一步涉及實體安全（safety）議題。傳統資安議題旨在防止攻擊者經由系統漏洞竄改資訊(例如少付電費)、或是竊取用戶之個人隱私資料；實體安全議題（safety）則需考量因資安漏洞導致電力系統遭入侵破壞，以至系統故障(例如不運作、引起不安全後果等)。

資訊技術安全共同評估準則(ISO/IEC 15408, Common Criteria，簡稱 CC）[2-4]，是現今資訊產品資安評估及驗證的通用國際標準。CC 原針對資訊系統（IT）所制定，並未考慮工業控制系統（Industrial Control System, ICS）可能延伸之實體安全問題。近年來先進的電腦病毒事件已影響重大基礎建設的安全:例如，2013 年南韓首爾媒體及銀行遭受 APT (Advanced Persistent Threat)攻擊[5]，損失嚴重。2010 年 6 月伊朗鈾濃縮工廠遭受 Stuxnet 病毒攻擊[6]，損失重大。

消費者可透過網路控制及監測智慧型家電；智慧家電通常具有溫度、濕度等控制系統；若具有獨立的 IP，亦可進行資訊收集、監測，可視為小型的 ICS。然而現今智慧電網家庭閘道器的安全需求(即保護剖繪 Protection Profile， PP[2])，多數尚未考慮實體安全（safety）。本研究針對上述議題，發展了一套智慧電網家庭閘道器保護剖繪標準及其檢測技術規範，能兼顧資訊安全及實體安全，本研究並提出處理 APT 的機制。最後，以一商用智慧電網閘道為例，評估此標準之適用性。本研究成果可提升智慧電網之資訊安全及實體安全等級。

2. 相關背景

2.1 智慧電網家庭閘道器（Smart Grid Gateway）

「閘道器」（Gateway）為連接兩種網路的一種通訊裝置；可連接兩個不同通訊協定的網段，處理通訊協定間的轉換包括：訊息格式轉換、位址轉換、協定轉換。目前國內已有多家廠商正進行智慧電網家庭閘道之開發，包括資策會開發之智慧型能源閘道器（Intelligent Energy Gateway）[7]，此為家庭能源管理控制器之系統核心，透過智慧家電應用層控制通訊協定（SAANET），可即時蒐集各家電設備及電表之資訊，並透過網際網路上傳至資料庫。

家庭網閘道器可連接並控制許多家電用品，因

此若有心人士利用惡意程式碼入侵或攻擊閘道，讓電暖爐或是烤麵包機等家電運轉不停，可能產生溫度過高引發火災等問題。因此，未來智慧電網閘道器在避免及偵測惡意攻擊上應扮演一重要角色，需具備防火牆、存取控制及監控等功能外，還需包含以下功能：收集、處理電表資料、保護區域網路中的裝置、提供其通訊、加密等功能。

2.2 資訊技術安全評估共同準則及保護剖繪

資訊技術安全評估共同準則(ISO/IEC 15408，即 Common Criteria，簡稱 CC）[2-4]，是現今各國為資通安全產品評估及驗證時所遵循的一個國際標準。此標準包含三個部分：第一部分：介紹和一般模型[2]、第二部分：安全功能需求[3]、第三部分：安全認證需求[4]。CC 定義了七個評估保證等級（EAL1-EAL7）用以判斷產品的安全等級。CC 將資訊科技產品之安全功能需求（Security Functional Requirement）分成十一大類，除此之外，尚還介紹保護剖繪（Protection Profile, PP）、安全標的（Security Target, ST）以及九大類安全保證需求（Security Assurance Requirement）。

十一大類型（class）之安全功能需求分別為:安全稽核(FAU: Security Audit)、通訊(FCO: Communication)、密碼學支援(FCS: Cryptographic Support)、使用者資料保護(FDP: User Data Protection)、識別及認證(FIA: Identification and Authentication)、安全管理(FMT: Security Management)、隱私(FPR: Privacy)等。每一個類別(Class)皆可以再細分為幾個家族(Family)，每個家族又可以分為幾個元件(Component)，每一個元件也可以分為幾個元素(Element)。

保護剖繪（Protection Profile, PP）[2,8]是根據 CC 為資通產品類型所撰寫的基本安全需求文件，主要包含以下部分(見圖一)：

- PP 介紹
- TOE（Target of Evaluation）描述
- TOE 資訊安全環境
- 資訊安全目標（Security Objective）
- 資訊科技產品（IT）資訊安全需求
- 理由闡述

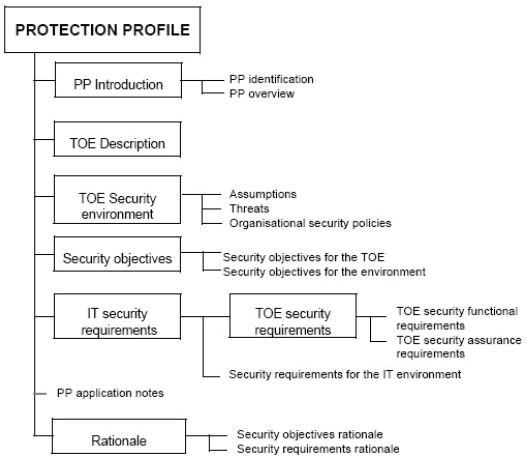


圖 1 保護剖繪內容

2.3 德國 BSI 智慧電網閘道保護剖繪

德國聯邦信息安全辦公室（BSI）於 2011 年根據 CC 製作了智慧電網閘道保護剖繪[9]。本研究已將其第六章之安全需求翻譯為中文，並延伸此 PP 作為智慧電網之家庭閘道器之資安驗證標準；延伸部份將在第三節章中介紹。

在 BSI 之 PP 中所用到的安全功能需求類別包含了安全稽查（FAU）、加密支援（FCS）、用戶資料保護（FDP）、身分識別及認證（FIA）、安全管理（FMT）、隱私（FPR）、保護評估標的安全功能（FPT）以及可信任之路徑／頻道（FTP）類別。以 FAU 為例，FAU 為安全稽查及產生稽查日誌類別，其下有數個元件，例如：FAU_ARP/SYS.1，為「系統日誌的安全警報」，指 TOE 的之安全功能應偵測潛在的違規行為並通知已授權之閘道管理員。

3. 家庭閘道器保護剖繪特殊需求分析

本研究進行步驟如下:

(1) 比較工業控制系統(ICS)與 IT 系統之差異性
(2) 翻譯並分析德 BSI 之 PP 主要技術章節
(3) 制定新的、符合控制系統之安全(safety)元件
(4) 綜合 BSI 原有的以及我們新制定的元件以撰寫更完整之智慧電網家庭閘道器保護剖繪
(5) 制定此保護剖繪之資通安全檢測技術規範
(6) 用一實際商用閘道器作為個案以評估所制定之保護剖繪績效

首先，資訊(IT)系統與工業/智慧家電控制系統(ICS)不同在於前者主要保護的是邏輯性（logical）資訊資產，而後者關注的則是實體（physical）資產，因此，攻擊此兩者的機制與損害亦不相同。例如，IT 系統遭攻擊可能不會立即發生作用，且可利用系統備份還原，因此較注重攻擊來源的分析、預防、偵測與回復。然而針對控制系統的攻擊(例如 APT 等)通常具有破壞性，若遭攻擊可能引起實體安全上之後果，如何控制損失規模則是 ICS 所要關注的[10]。

我們建議智慧電網家庭閘道器保護剖繪應如圖 2 所示，新增和延伸部分以紅字標註並加註編號。新增和延伸部分為 TOE Security and Safety environment (圖 2 編號 1)、Safety and security objective(編號 2) 及 IT security and safety requirements(編號 3)；原來資訊安全相關章節皆延伸為 資訊安全與實體安全(safety)，包含實體安全相關資訊、需求、及其下的子項目。

針對圖 2 編號 1, 我們建議在 PP 組織安全策略（OSP）內新增 OSP.System 策略，意旨 TOE 設

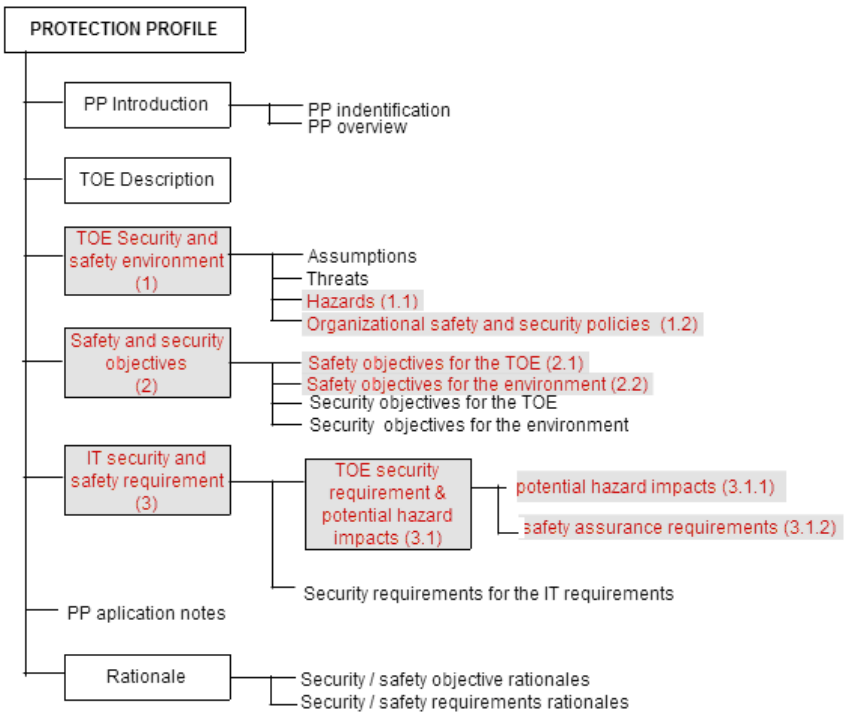


圖 2 建議之保護剖繪結構（修正及新增部分有加註編號）

計需要考慮安全因素；包含多套（N-version）設計，避免單一元件失誤造成全系統失效（single failure criteria）、深層/多層防禦等，以避免後續之實體安全影響（Hazard impact）(見表 1)。 另外，針對 APT、Stuxnet 等進階潛伏病毒，我們並建議修正原 BSI PP 中之 OSP.Log 內容為如下：TOE 應將正常使用的行為模式（patterns）和正常工作區間（envelope）儲存於另一同步監控處理器（co-processor）中(見表 2)。Co-processor 可動態對封包比對及偵測可能有的進階持續性滲透攻擊或 Stuxnet 等病毒。

針對圖 2 編號 2，我們建議 BSI PP 中 TOE 之資訊安全與實體安全目標中 O.Protectd 可移至編號 2.1 安全目標；而操作環境目標中之 OE.PhysicalProtection 移至編號 2.2，因其內容都考慮到實體安全（例如 fail-safe）及資訊安全失效後續影響。

針對圖 2 編號 3，我們制定了一新的安全功能需求類別 FSP，主要內容為避免系統失效。此新增的類別可進一步分為家族名為 FSP_SYP(system protection)，其下包含數個元件以對照上述組織安全策略 OSP.System（見表 3），包含不同設計之多套系統（N-diverse version）、置於不同地點、電源之多套系統及多層次的防禦機制等。

此外，針對編號 3，我們亦建議於原 BSI PP 之安全稽核 FAU 類別中新增一家族 FAU_APT（Advanced Persistent Threat），內容即是偵測或阻止 APT 或 Stuxnet 之類病毒的攻擊威脅方法。其下包含三個元件：設定正常時間之家電使用之溫度、壓力、通風等正常範圍；利用同步處理器做分析與監控；如發生異常狀況，需有警示或是能夠立即切斷電源 （見表 4）。

原 BSI PP 安全保證需求下（圖 2 編號 3.1.2）中，包含了一 ADV 類別，為 TOE 開發時每一項安全功能皆須提供安全評估所需的資訊。本研究建議 ADV 下新增家族 Safety functional specification (ADV_SF) 和 Safety design (ADV_SAF)。ADV_SF 加強實體安全功能，例如故障亦安全（fail-safe）[11],及監控（monitoring）等。即時監控可分析可疑行為如 APT 攻擊，以立即偵測並隔離，此家族與 FAU_APT 相關。ADV_SAF 家族則說明產品在設計時是否使用不同設計之多套系統（N-diverse version）、置於不同地點、電源之多套系統及多層次的防禦等安全機制；其下的元件見表 5。

針對圖 2 編號 3.1.2 下之 ATE，我們建議新增一安全分析家族 Safety analysis(ATE_SAF)。此家族之可利用錯誤植入（fault injection）方法進行側試，亦可採用故障樹分析（fault tree analysis）[12]方法，以驗證產品之安全性（safety），並進一步了解可能的不安全事件的過程及因果。

其中安全分析元件 ATE_SAF.1 可採用故障樹分析。故障樹採取由意外事件往前推導其可能之原因(backward)方法。舉一電器走火故障樹為例 (見圖 3):電器走火基本原因含電壓異常、溫度過高、或軟硬體故障；溫度過高則可能起因於電器過熱、短路等；電器過熱則可能因為不當使用、或被駭客端控制；駭客則可能非法取得密碼、或竄改訊息等。駭客可入侵的原因又可進一步推導，因網路釣

表 1 新增之組織安全策略

組織安全策略	描述
OSP.System	TOE 在系統的設計上需包含以下方法以降低系統故障所造成之後續安全影響： • 多套備份系統（Multiple version system） • 避免單點失效（single failure） • 避免共同失效模式（common mode failure） • 深層防禦（defense-in-depth）

表 2 修正 OSP.LOG 之內容

組織安全策略	描述
OSP.Log	TOE 應該要有下列四種記錄檔（log）：1～3 （同原始 BSI 智慧電網閘道保護剖繪） 4. 儲存正常使用型式（patterns）或正常工作區間（envelope）於 co-processor，包括時間、範圍、數值狀況等。

表 3 新增 FSP_SYP 家族之元件內容

元件名稱	內容描述
FSP_SYP.1	不同方式設計的多套系統(N-diverse version)，可用不同邏輯、平台、感應器及輸出等，以避免單點失效（single point of failure, SPOF）的發生，提高可用性及可靠性。
FSP_SYP.2	一多套系統置於不同地點、電源及基礎建設等，以避免共同失效之故障模式（common mode failure）。
FSP_SYP.3	多層次的防禦機（defense -in-depth）以增加安全性。

表 4 新增 FAU_APT 家族之元件內容

元件名稱	內容描述
FAU_APT.1	設定正常時間之溫度、壓力、通風等家電正常使用之範圍（即正常工作範圍）。
FAU_APT.2	利用 co-processor 做分析及監控－偵測器偵測並回傳值。
FAU_APT.3	異常警示、切斷電源

表 5 新增 ADV_SAF 家族之元件內容

元件名稱	內容描述
ADV_SAF.1	不同方式設計的多套系統(N-diverse version)，可用不同邏輯、平台、偵測器及輸出等，以避免單點失效（single point of failure, SPOF）的發生，提高可用性及可靠性。
ADV_SAF.2	一多套系統置於不同地點、電源及基礎建設等，以避免共同失效之故障模式（common mode failure）。

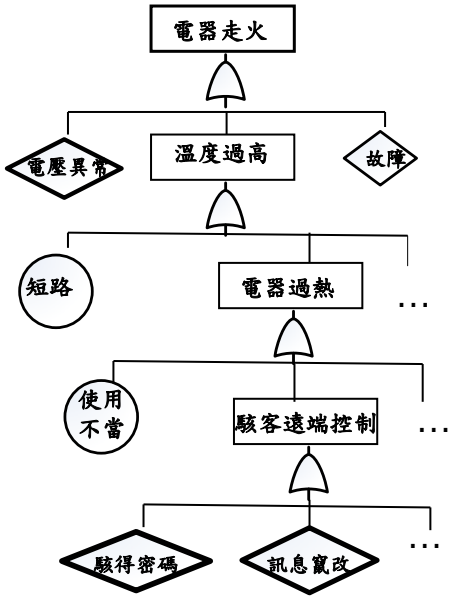


圖 3 電器走火部份故障樹

表 6 新增及修正的元件

編號（依照圖 2 之分類編號）			新增或修正內容
1：TOE 之資訊安全與實體安全環境	1.1：Hazards		T.Infrastructure
	1.2：組織資訊安全與實體安全策略		OSP.System
			OSP.Log
2：資訊安全與實體安全目標	2.1：TOE 實體安全目標		O.Protect
	2.2：環境之實體安全目標		OE.PhysicalProtection
3：資訊安全與實體安全需求	3.1 TOE 資訊安全需求及潛在實體安全影響	3.1.1：TOE 資訊安全與實體安全功能需求	FSP_SYP.1 FSP_SYP.2 FSP_SYP.3
			FAU_APT.1 FAU_APT.2 FAU_APT.3
		3.1.2：TOE 資訊安全與實體安全保證需求	ADV_SF.1 ADV_SF.2 ADV_SF.3
			ADV_SAF.1 ADV_SAF.2
			ATE_SAF.1

魚、訊息未加密簽章、網路設備安性不足等等。故障樹圖中長方形為事件，菱形為未進一步展開的事件，圓形為基礎肇因，不需再展開。從故障樹之一縱向分支可組成一因資訊安全問題導至實體安全效應的一情境。表 6 彙整本研究所增修之元件。

4. 制定家庭閘道器驗證標準及個案評估

本研究進一步根據上述智慧電網家庭閘道器 PP 制定驗證標準。方法為修改並延伸國內最新的相近驗證標準:電信技術中心（TTC）之「防毒閘道設備資通安全檢測技術規範」 [13]。其安全功能需求之審查內容包括稽核紀錄、使用者身分關

表 7 部份安全功能需求之書面審查內容[13]

項目	審查標準
1. 稽核紀錄	安全功能應具備以下稽核紀錄： (1)依下列事件類型產生其稽核紀錄並存於資料庫中： A. 啟閉稽核功能。 B. 存取稽核資料。 C. 使用者登錄成功或失敗、登錄權限變更及恢復。 D. 變更安全屬性。 E. 變更系統時間。 (2) 每筆稽核紀錄至少包含下列資訊：A. 事件識別碼。 B. 事件日期及時間。 C. 事件類型 D. 事件成功或失敗
…	…
8 防毒措施	(資訊)安全功能應具備以下防毒措施： (1) 清除病毒 (2) 隔離病毒 (3) 監控企圖透過遠端 TCP、UDP 或 SMTP 協定進行非授權之程序
9 防毒告警	(資訊)安全功能應具備以下防毒告警： (1) 偵測到病毒時，應發出警示訊息，內容應包含病毒資訊與處置措施 (2) 應持續提供警示訊息，直到使用者與管理者有所回應
10 密碼操作….	…
12 安全功能資料管理….	提供管理者設定查詢、更改或刪除下列事項： (1)病毒被偵測後所需行的動作 (2)病毒特徵檔 (3)稽核紀錄
14 ….	

聯、稽核審查等項目。此份技術規範可涵蓋大部分 BSI 之智慧電網閘道保護剖繪之項目且有具體檢查細項 (見表 7)，共 14 大項。例如第一項稽核紀錄之技術規範標準包含開啟關閉稽核功能、存取稽核資料等以產生稽核紀錄，且每筆紀錄需包含資訊如事件識別碼、日期時間等。

此一技術規範僅考慮一般防毒閘道器所需具備之功能，但未考慮智慧電網之實體安全或資安漏洞之後續危害效應。根據上述第三節之延伸實體安全功能需求、實體安全保證需求元件，我們新增了下面 15-18 項(見表 7)：

- 第 15 項－實體安全功能保護：
  (1)平時並在開機時執行安全功能測試，且應定期執行自我測試或由已授權使用者執行測試，以確認所有安全功能皆可正常運作。
  (2)當系統運作期間，應偵測本機之外盒是否被拆開，以確保不會遭受實體竄改。
  (3)當有任何故障發生時，評估標的應保持實體安全狀態。
- 第 16 項－可信任之通訊頻道：TOE 之安全功能應在自己與另一可信任之 IT 產品間提供可信任之通訊頻道，保護本身及頻道之資料不被修改或公開。
- 第 17 項－避免系統失效：為避免因系統失效而導致後續之實體安全影響，因此需事先準備多套系統便不時之需。
- 第 18 項－APT 攻擊偵測：預先設定家電正常使用時，溫度、溼度等的範圍，並利用一同步處理器（co-processor）動態監測並分析網路傳入之封包是否符合正常範圍，如未在正常範圍，則應發出警示，或是切斷其電源。

表 8 上表新增項目

項目 (元件)	審查標準
15 實體安全功能保護 (FPT_TST.1 FPT_PHP.1 FPT_FLS.1)	(1) 實體安全功能應在以下情況執行自我測試已確認安全功能之正常運作： A 開機初始化時 B.已授權之使用者要求時 C.正常操作期間定時做自我檢測 (2)實體攻擊之被動偵測 (3) 當故障發生時亦保持安全（safe）狀態
16 可信任之通訊頻道 (FTP_ITC/WAN.1 FTP_ITC/MTR.1 FTP_ITC/USR.1)	評估標的之安全功能應在自己與另一可信任之 IT 產品間提供可信任之通訊頻道，保護本身之端點及頻道之資料不被修改或公開。
17 避免系統失效 (FSP_SYP.1 FSP_SYP.2)	(1) 具有 redundant version 或 N-version programming，如偵測到有模組錯誤，方可以另一功能相同之模組做替換 (2)避免共同失效模式
18. APT 攻擊偵測 (FAU_APT.1 FAU_APT.2 FAU_APT.3)	(1)設定正常時間之溫度、壓力、通風等家電正常使用範圍。 (2)利用 co-processor 做分析及監控－偵測器偵測並回傳值。 (3)異常警示、切斷電源

本研究向合勤科技借了一項產品－整合式安全閘道器（ZyWALL USG 200）[14]，用以作為評估標的（TOE） 用上述驗證標準家以評估。此閘道器主要可應用於中小企業（25～50 個 PC 使用者），具有入侵偵測防禦系統，除了可防範來自外部的威脅，亦可防範內部之威脅。其主要優點並包含安全連線、主動防禦、容易管理、網路恢復力等。

評估結論為此台閘道器幾乎皆符合上述智慧電網家庭閘道器驗證標準，僅有少數項目未符合審查標準，包含：

- 第八項防毒措施之（3）監控企圖透過遠端

TCP、UDP 或 SMTP 協定進行非授權之程序：此閘道器主要支援 HTTP/FTP/SMTP/POP3/IMAP4 協定，因此並無支援審查標準中之 TCP 與 UDP。

- 第十五項安全功能保護之（2）實體攻擊之被動偵測：因此閘道器之最初目的為設計給中小企業使用，因而並未考慮到其實體可能遭受竄改。
- 第十八項 APT 攻擊偵測，目前較少閘道能夠偵測 APT 之攻擊，因其潛伏期長且難發現。

此個案之 15-18 項評估結論見表 9

表 9 合勤安全閘道器部份評估結果

項目	PP 相對應元件	TOE 符合否
15	FPT_TST.1 FPT_PHP.1 FPT_FLS.1	(1) V (2) X (3) V
16	FTP_ITC/WAN.1 FTP_ITC/MTR.1 FTP_ITC/USR.1	V
17	FSP_SYP.1 FSP_SYP.2	V
18	FAU_APT.1 FAU_APT.2 FAU_APT.3	X

5. 結論

智慧電網為未來之趨勢，藉由與智慧家電與家庭閘道器之結合，使用者可遠端遙控智慧家電之操作。因為電網所連結的多為工業或家電控制系統，此類系統具有對實體環境運作能力，一旦遭惡意攻擊，可能產生實體上的破壞。故此領域衍生了一新議題:如何預防與處理資訊安全(information security)漏洞可能引發之後續實體安全(physical safety) 問題。然而，目前智慧電網閘道相關標準多數尚未考慮實體安全新議題;並且多數未能處理 APT(或 Stuxnet)等進階病毒攻擊及其後對實體安全影響。

本研究針對此問題，將德國 BSI 的智慧電網閘道器 PP 第六章節翻譯為中文，並進一步修正及新增其內容，增加處理實體安全及 APT 之相關元件。本研究建議以此增定版為智慧電網家庭閘道保護剖繪標準；並依此標準，擴充了國內相關之安全檢測規範以做為智慧電網家庭閘道器檢測規範;最後再以一商用閘道器做為個案，評估本研究所制定標準之有效性。

本研究為智慧電網中結合資訊安全與實體安全之初步研究，希望能有拋磚引玉效果，日後能有更多研究人員投入相關技術開發。未來物聯網（Internet of Things）的興起，更需要資訊安全與實體安全之整合。本研究未來方向將擴充實體安全相關元件以達到完整性，亦將此類元件通用化(generalized)，用以修訂資訊技術安全評估共同準則（Common Criteria）內容。

誌謝

本研究部份接受國科會編號 NSC 101-3113-P-033-003，NSC 102-2221-E-155-030 計畫經費補助。

參考文獻

[1] 台灣智慧型電網產業協會，http://www.smart-grid.org.tw/index.aspx.

[2] ISO/IEC 15408-1, “Common criteria for information technology security evaluation, Part 1: Introduction and general model, ” Version 3.1, Release 4, September 2012, http://www.commoncriteriaportal.org.

[3] ISO/IEC 15408-2, “Common criteria for information technology security evaluation, Part 2: Security functional components, ” Version 3.1, Release 4, September 2012, http://www.commoncriteriaportal.org

[4] ISO/IEC 15408-3, “Common criteria for information technology security evaluation, Part 3: Security assurance components, ” Version 3.1, Release 4, September 2012, http://www.commoncriteriaportal.org

[5] 南韓大顆首爾(DarkSeoul)大規模 APT 攻擊事件，http://blog.xecure-lab.com/2013/03/darkseoul-apt.html.

[6] 惡意程式－Stuxnet 簡介，http://www.cert.org.tw/docfile/Stuxnet.pdf.

[7] 資策會，In-Snergy 雲端智慧綠能管理系統，http://www.insnergy.com/html/home.jsp.

[8] SANS Institute, “Protection Profile, A key concept in the Common Criteria”, 2003 http://www.sans.org/reading_room/whitepapers/standards/protection-profile-key-concept-common-criteria_1007.

[9] Germany Federal Office for Information Security (BSI), “Protection Profile for the Gateway of a Smart Metering System,” 2012, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf?__blob=publicationFile.

[10] 易俗、陳振楠、范金鳳、曾婉惠、陳明輝、鄭宗杰， 工業控制系統資訊安全問題及特性初步分析，資訊安全會議，2005。

[11] “Fail-safe,” http:// en.wikipedia.org/wiki/Fail-safe.

[12] Nancy Leveson, Safeware: system safety and computers, Addison Wesley, 1995.

[13] 財團法人電信技術中心，防毒閘道設備資通安全檢測技術規範，http://www.ttc.org.tw/index.html.

[14] 合勤科技，http://www.zyxel.com/tw/zh/homepage.shtml.

基於預測值與鄰近像素差值的標準差的可逆式資訊隱藏

冷輝世
國立彰化師範大學
lenghs@cc.ncue.edu.tw

張維剛
國立彰化師範大學
s9922119@mail.ncue.edu.tw

曾顯文
朝陽科技大學
hwtseng@cyut.edu.tw

摘要

近年來可逆式資訊隱藏逐漸受到重視，尤其是基於預測值的預測值與原始值的差值擴張方法。同樣是基於預測值，本研究改用預測值與鄰近像素值差值的標準差，其優點是減少影像結構的失真，使偽裝影像有更好的影像品質與藏量。一般使用預測值的方式會定義預測值與原始值差值的門檻值，本研究則是使用相對於預測值的鄰近像素差值定義標準差。實驗結果顯示本研究所提出的方法能有效的提高偽裝影像的藏量並具有較佳的影像品質。

關鍵詞：可逆式資訊隱藏、預測值、差值擴張、標準差。

Abstract

Reversible data hiding is paid great attention in recent years, especially for prediction-based difference expansion schemes. Different from other schemes, in traditional design, threshold is used to be the standard of whether the target pixel should embed secret bits or not. The proposed method uses the concept of the standard deviation replaces the original design. The experimental results show that the purposed method is effective in increasing payload and improving the image quality.

Keywords: Reversible data hiding, prediction-based, difference expansion, standard deviation.

1. 前言

隨著網路科技的發展，大量的資訊在網路間傳遞。因此，資訊安全也越來越受到重視。資訊隱藏是一門新興的資訊安全科學，將機密訊息藏入載體中不被發現，再傳送給接收方，接收方可藉由與傳送方協定的方法取出載體中的機密訊息。載體可以是文字、圖形、影像等類型，由於圖形被廣泛的使用在網路上，而且圖形具有龐大藏量的特性，所以大部份的研究都使用圖形為載體。

資訊隱藏法又分為不可逆式與可逆式。不可逆式是指機密訊息取出後無法還原原始載體。對於商業、醫療、軍事等資訊的傳遞，保持其原始載體的完整性非常重要，所以可逆式資訊隱藏逐漸成為研究的主流方向。

可逆式資訊隱藏又分為兩大類，一種是 Tian 學者提出的差值擴張法，一種是 Ni 學者提出的直方圖位移法。差值擴張法主要是以預測像素值與實際像素值的差值進行擴張藏匿，包括 Lee 等學者[1]利用目標像素 x 的鄰近像素 a、b，如圖 1 所示，將 $(a+b)/2$ 作為 x 的預測值，Chuan Qin 等學者[2]利用 x 鄰近像素 a、b、c 如圖 1 所示，將 $(a+b+c)/3$ 作為 x 的預測值，Vasiliy Sachnev 等學者[3]利用 x 鄰近像素 a、b、c、d，如圖 2 所示，將 $(a+b+c+d)/4$ 作為 x 的預測值，本研究基於 Lee 等學者的方法為基礎，改進實驗方法。

由於 Lee 等學者提出的預測值與原始值差值擴張必須設定一個門檻值，對於預測值差值大於門檻值的像素都必須加或減一個門檻值，因而造成失真。本研究使用了另一種方式減少此類的失真。

c	b
a	x

圖 1　目標像素 x 與其鄰近像素

	b	
a	x	c
	d	

圖 2 目標像素 x 與其鄰近像素

2. 相關研究

本章將介紹 Lee 等學者的預測值與原始值差值擴張法與冷等學者的 MMED 預測法。

2.1 Lee 等學者的預測值差值擴張法

在 Lee 等學者(2010)的方法中，對於一張長寬為 $M \times N$ 的影像，藏匿區域為影像中去掉的一行與第一列的部分如圖 3 白色部分：

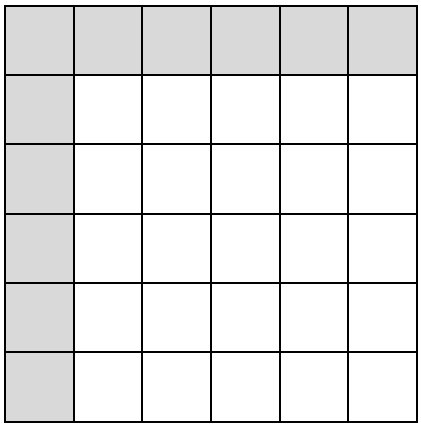


圖 3 藏匿區域示意圖

首先決定一個門檻值T，T 值愈小藏量愈低但影像品質好，T 值愈大藏量愈高但影像品質愈差。藏匿方法：

對於目標像素 $x_{i,j}$，使用其左上方的臨近像素進行預測，如圖 4 所示：

$x_{i-1,j-1}$	$x_{i-1,j}$
$x_{i,j-1}$	$x_{i,j}$

圖 4 臨近像素示意圖

則其預測像素 $x'_{i,j}=\lfloor (x_{i-1,j}+x_{i,j-1})/2 \rfloor$，預測誤差 $d=\left|x_{i,j}-x'_{i,j}\right|$。對於 d 值與門檻值有以下兩種情形：

一、若 d 值小於等於門檻值 T，則進行藏匿，隱蔽像素

$$\bar{x}_{i,j}=\begin{cases} x'_{i,j}+2\times d+s, & if\ x_{i,j}\geq x'_{i,j} \\ x'_{i,j}-2\times d-s, & if\ x_{i,j}<x'_{i,j} \end{cases},\ s\in\{0,1\}$$

二、若 d 值大於門檻值 T，則

$$\bar{x}_{i,j}=\begin{cases} x_{i,j}+(T+1), & if\ x_{i,j}\geq x'_{i,j} \\ x_{i,j}-(T+1), & if\ x_{i,j}<x'_{i,j} \end{cases}$$

取出與還原方法：

對於隱蔽像素 $\bar{x}_{i,j}$，因為 $x_{i-1,j}$ 與 $x_{i,j-1}$ 皆已經被還原，因此可以得到預測像素

$$x'_{i,j}=\lfloor (x_{i-1,j}+x_{i,j-1})/2 \rfloor \text{ 與 } d'=\left|\bar{x}_{i,j}-x'_{i,j}\right|$$

由 d'與門檻值 T 可分為下列兩種情形：

一、若 $d'\leq 2\times T+1$

所藏的機密信息 $s=d'\bmod 2$ 且原始像素為

$$x_{i,j}=\begin{cases} x'_{i,j}+\left\lfloor \frac{d'}{2} \right\rfloor, & if\ x'_{i,j}\leq \bar{x}_{i,j} \\ x'_{i,j}-\left\lfloor \frac{d'}{2} \right\rfloor, & otherwise \end{cases}$$

二、若 $d'>2\times T+1$

$$x_{i,j}=\begin{cases} \bar{x}_{i,j}-(T+1), & if\ x'_{i,j}\leq \bar{x}_{i,j} \\ \bar{x}_{i,j}+(T+1), & otherwise \end{cases}$$

以下舉例說明：

80	179	175
78	178	177

圖 5 示範影像

如圖 5，假設門檻值 $T=2$，機密訊息 $s=1$，對於目標像素 $x_{2,2}$，$x'_{2,2}=\lfloor (78+179)/2 \rfloor=128$，$d=\left|178-128\right|=50$。因為 $50>T=2$，屬於第二類型所以 $\bar{x}_{2,2}=x_{2,2}+(T+1)=178+3=181$。

對於目標像素 $x_{2,3}$，$x'_{2,3}=\lfloor (178+175)/2 \rfloor=176$，$d=\left|177\text{-}176\right|=1$。因為 $1\leq T=2$，屬於第一類型，所以 $\bar{x}_{2,3}=x'_{2,3}+2\times d+s=176+2+1=179$。

取出與還原步驟：

$\bar{x}_{2,2}=181$，則 $x'_{2,2}=\lfloor (78+179)/2 \rfloor=128$，$d'=\left|\bar{x}-x'\right|=\left|175-128\right|=47>2\times T+1=5$，屬於第二類型，所以 $x_{2,2}=181-3=178$。

$\bar{x}_{2,3}=179$，則 $x'_{2,3}=\lfloor (178+175)/2 \rfloor=176$，$d'=\left|\bar{x}-x'\right|=\left|179-176\right|=2\leq 2\times T+1=5$，屬於第一類型，$s=5 \bmod 2=1$，$x_{2,3}=176+1=177$。

2.2 冷等學者的 MMED 預測

冷等學者(2013)修改了 MED 預測方法[4]，依據不同影像的特徵得到一個特有的門檻值 T，令 c 為目標像素的對角像素，a 為目標像素的水平鄰近像素，b 為目標像素的垂直鄰近像素，若 c 與 $(a+b)/2$ 的差小於門檻值 T 的話，則取預測值為 a、b、c 的平均值，會有更準確的預測：

設 x 為目標像素，其鄰近三個像素為 a、b、c 如圖 1 所示，且由影像特徵所得到的門檻值 T，則目標像素 x 的預測值：

$$x' = \begin{cases} \min(a,b), \ if \ \ c \ge \max(a,b) \\ \max(a,b), \ if \ \ c \ge \min(a,b) \\ \dfrac{a+b+c}{3}, \ c \in (a,b) \ \left| c - \dfrac{a+b}{2} \right| < T, T \in N \\ a+b-c, \ otherwise \end{cases}$$

3. 研究方法

由於考慮到影像的切割、陰影等等對於影像邊緣的影響，因此我們將藏匿區域限制為去除四個邊的中間區域。首先我們依照 S.Geetha 等學者[5]的分割方式，將圖片分割為擁有共用邊的九宮格區塊，並且使用這些鄰近像素利用冷等學者提出的 MMED 預測方法對該像素進行判斷是否為'edge'或是'non-edge'，再根據判斷結果進而預測其像素值，接著計算此預測值與其鄰近像素的標準差(S)，並且利用此標準差(S)設為門檻值，根據不同的標準差，使用差值擴張可逆式資訊隱藏法進行分次藏匿。

3.1 影像分區與使用 MMED 預測像素

依照 S.Geetha 等學者(2011)的分割方式，每個像素的座標皆可用(o,o),(o,e),(e,o),(e,e)這四種座標來表達，其中 o 代表奇數，e 代表偶數，如圖 6 所示：

(o,o)	(o,e)	(o,o)	(o,e)	(o,o)
(e,o)	(e,e)	(e,o)	(e,e)	(e,o)
(o,o)	(o,e)	(o,o)	(o,e)	(o,o)
(e,o)	(e,e)	(e,o)	(e,e)	(e,o)
(o,o)	(o,e)	(o,o)	(o,e)	(o,o)

圖 6 區塊圖示

因此我們可以將影像去除外圍的中間部分區分為四類，分別為：

$$S_{UL} = \{x_{i,j} \mid i = 2k, j = 2k\}$$
$$S_{UR} = \{x_{i,j} \mid i = 2k+1, j = 2k\}$$
$$S_{DL} = \{x_{i,j} \mid i = 2k, j = 2k+1\}$$
$$S_{DR} = \{x_{i,j} \mid i = 2k+1, j = 2k+1\}$$

並且對這四類像素進行分次藏匿。

我們首先針對 S_{UL} 的像素進行藏匿。我們將影像分割為擁有共用邊的九宮格區塊，因此對於目標像素 $x_{i,j}$ 的鄰近像素集合

$$N_{i,j} = \{x_{i-1,j-1}, x_{i-1,j}, x_{i-1,j+1}, x_{i,j-1}, x_{i,j+1}, x_{i+1,j-1}, x_{i+1,j}, x_{i+1,j+1}\}$$

對 $x_{i,j}$ 的鄰近像素中的四個角落

$$N_{UL}(x_{i,j}) = \{x_{i,j-1}, x_{i-1,j}, x_{i-1,j-1}\}$$
$$N_{UR}(x_{i,j}) = \{x_{i,j+1}, x_{i-1,j}, x_{i-1,j+1}\}$$
$$N_{DL}(x_{i,j}) = \{x_{i,j-1}, x_{i+1,j}, x_{i+1,j-1}\}$$
$$N_{DR}(x_{i,j}) = \{x_{i+1,j+1}, x_{i+1,j}, x_{i,j+1}\}$$

使用 MMED 對 $x_{i,j}$ 判斷該像素是否為'edge'，並且利用此判斷進行預測。

判斷方式：

如圖 1，若 $c \ge \max\{a,b\}$ 或 $c \le \min\{a,b\}$，則該角落為'edge'，否則為'non-edge'。

預測方式：

若角落判斷為'edge'，則 $p_i = (a+b)/2$。若角落判斷為'non-edge'，則 $p_i = MMED(x_{i,j})$。

因此對於目標像素 $x_{i,j}$，可以得到四個預測結果 p_1、p_2、p_3、p_4，我們令 $x_{i,j}$ 的預測值

$$x'_{i,j} = \lfloor (p_1 + p_2 + p_3 + p_4)/4 \rfloor \text{。}$$

3.2 評估函數 $\sigma_N(x_{i,j})$

我們令

$$D(x_{i,j}) = (x_{i-1,j-1} - x'_{i,j})^2 + (x_{i-1,j} - x'_{i,j})^2 + (x_{i-1,j+1} - x'_{i,j})^2 + (x_{i,j-1} - x'_{i,j})^2 + (x_{i,j+1} - x'_{i,j})^2 + (x_{i+1,j-1} - x'_{i,j})^2 + (x_{i+1,j} - x'_{i,j})^2 + (x_{i+1,j+1} - x'_{i,j})^2$$

，且 $\sigma_N(x_{i,j}) = \left\lfloor \sqrt{D(x_{i,j})/8} \right\rfloor$，為 $x'_{i,j}$ 與鄰近九宮格像素的標準差，因此我們可以設立標準差 S 的大小來決定哪些像素點要藏入機密訊息。

3.3 藏匿方法與取出還原方法

藏匿方法：

對於目標像素 $x_{i,j}$，若 $\sigma_N(x_{i,j}) \le S$，則隱蔽像素

$$\bar{x}_{i,j} = \begin{cases} x'_{i,j} + 2 \times \left| x'_{i,j} - x_{i,j} \right| + b \text{，} for \ x_{i,j} > x'_{i,j} \\ x'_{i,j} - 2 \times \left| x'_{i,j} - x_{i,j} \right| - b \text{，} for \ x_{i,j} \le x'_{i,j} \end{cases}$$

其中 $b \in \{0,1\}$ 為機密訊息。

若 $\sigma_N(x_{i,j}) > S$，則不進行藏匿。

取出與還原方法：

對於隱蔽像素 $\hat{x}_{i,j}$，可以得到預測像素 $x'_{i,j}$，令 $d' = \left| \bar{x}_{i,j} - x'_{i,j} \right|$，若 $\sigma_N(x_{i,j}) \le S$，則機密訊息 $s = d' \bmod 2$，

$$x_{i,j} = \begin{cases} x'_{i,j} + \left\lfloor \dfrac{d'}{2} \right\rfloor, \ if \ x'_{i,j} < \bar{x}_{i,j} \\ x'_{i,j} - \left\lfloor \dfrac{d'}{2} \right\rfloor, \ otherwise \end{cases}$$

若 $\sigma_N(x_{i,j}) > S$ ，則不進行動作。

3.4 進行分次藏匿

將 S_{UL} 的像素藏匿完之後，我們對藏匿完的影像進行第二次、第三次與第四次藏匿，藏匿方法與上述方法一樣，但是目標像素分別更改為 S_{UR}、S_{DL}、S_{DR} ，如圖 7 所示：

	第一次目標	第二次目標	第一次目標	第二次目標
	第三次目標	第四次目標	第三次目標	第四次目標
	第一次目標	第二次目標	第一次目標	第二次目標
	第三次目標	第四次目標	第三次目標	第四次目標

圖 7 目標像素示意圖

3.5 溢位問題

對於影像中像素質較大或較小的像素點，經過藏匿之後有可能會發生溢位問題(over flow or under flow)，本研究將藏入後會產生溢位的像素點的座標使用 Location Map 記錄下來，不進行藏匿，取出時先判斷該像素點是否位於 Location Map 內，若否才執行取出動作。

3.6 藏匿與取出還原範例

以圖 8 為例：

80	179	175	175
78	178	177	177
79	175	173	179
77	177	175	177

圖 8 藏匿範例圖

灰色部分不進行藏匿，白色部分則為我們的藏匿區域。

藏匿步驟：

我們設門檻值 T=4，S=50，機密訊息 B='100'，$S_{UL}=\{x_{2,2}\}, S_{UR}=\{x_{2,3}\}, S_{DL}=\{x_{3,2}\}, S_{DR}=\{x_{3,3}\}$ ，首先我們對 $S_{UL}=\{x_{2,2}\}$ 進行第一次藏匿，

$p_1 = 78+179-80 = 177$

$p_2 = (179+177)/2 = 178$

$p_3 = 78+175-79 = 174$

$p_4 = (175+177)/2 = 176$

因此

$x'_{2,2} = \lfloor (177+178+174+176)/4 \rfloor = 176$

，$\sigma_N(x_{2,2}) = 59 > 50$ ，所以 $\bar{x}_{2,2} = 178$ 。

將 S_{UL} 藏匿完畢後，對 S_{UR} 進行第二次藏匿，

$p_1 = (178+175)/2 = 176.5$

$p_2 = (175+177)/2 = 176$

$p_3 = \lfloor (178+175+173)/3 \rfloor = 175$

$p_4 = (173+177)/2 = 175$

因此

$x'_{2,3} = \lfloor (176.5+176+175+175)/4 \rfloor = 175$

，$\sigma_N(x_{2,3}) = 2 \le 50$ ，且 $x_{2,3} > x'_{2,3}$

所以 $\bar{x}_{2,3} = 175+2\times|175-177|-0 = 179$ 。

將 S_{UR} 藏匿完畢後，對 S_{DL} 進行第三次藏匿，

$p_1 = (178+79)/2 = 128.5$

$p_2 = (178+173)/2 = 175.5$

$p_3 = (79+177)/2 = 128$

$p_4 = (173+177+175)/3 = 175$

因此

$x'_{3,2} = \lfloor (128.5+175.5+128+175)/4 \rfloor = 151$

，$\sigma_N(x_{3,2}) = 49 \le 50$ ，且 $x_{3,2} > x'_{3,2}$

所以 $\bar{x}_{3,2} = 151+2\times|151-175|+0 = 199$ 。

將 S_{DL} 藏匿完畢後，對 S_{DR} 進行第四次藏匿，

$p_1 = (179+199)/2 = 189$

$p_2 = (179+179)/2 = 179$

$p_3 = 199+175-177 = 197$

$p_4 = (175+177+179)/3 = 177$

因此

$x'_{3,3} = \lfloor (189+179+197+177)/4 \rfloor = 185$

，$\sigma_N(x_{3,3}) = 8 \le 50$ ，且 $x_{3,3} < x'_{3,3}$

所以 $\bar{x}_{3,3} = 185-2\times|185-173|-1 = 160$ 。

取出還原步驟：

第四次： $x'_{3,3}=185$ ，$\sigma_N(x_{3,3}) = 8 \le 50$ ，因此 $d' = |160-185| = 25$ ，機密訊息 $b = 25 \bmod 2 = 1$ ，$x_{3,3} = 185-12 = 173$ 。

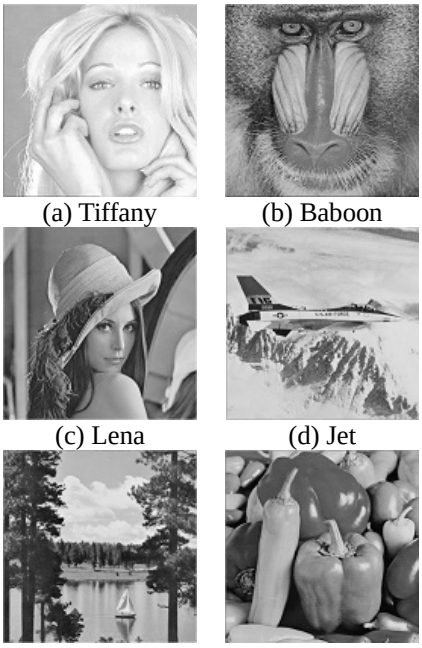
第三次： $x'_{3,2}=151$ ，$\sigma_N(x_{3,2}) = 49 \le 50$ ，因此 $d' = |199-151| = 48$ ，機密訊息 $b = 48 \bmod 2 = 0$ ，$x_{3,2} = 151+24 = 175$ 。

第二次： $x'_{2,3}=175$ ，$\sigma_N(x_{2,3}) = 2 \le 50$ ，因此 $d' = |179-175| = 4$ ，機密訊息 $b = 4 \bmod 2 = 0$ ，$x_{2,3} = 175+2 = 177$ 。

第一次： $x'_{2,2}=176$ ，$\sigma_N(x_{2,2}) = 59 > 50$ ，因此不執行動作。

4. 實驗結果

本實驗使用 SIPI 影像圖庫裡的'Tiffany'、'Baboon'、'Lena'、'Airplane'、'Scene'與'Peppers'，這 6 張，大小為 512×512 的圖片作為實驗樣本：



(a) Tiffany (b) Baboon (c) Lena (d) Jet (e) Scene (f) Peppers

圖 9 六張原始影像

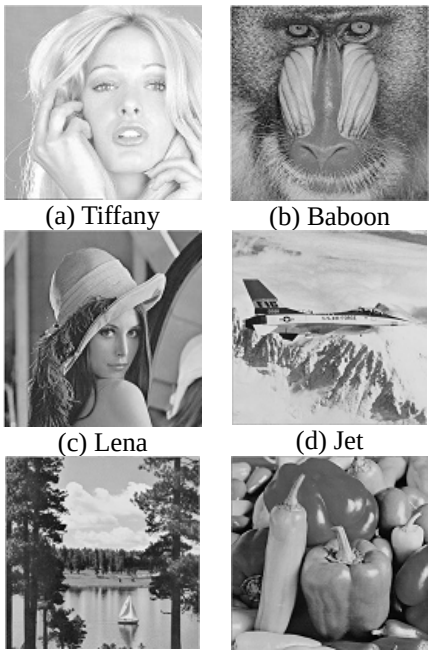
由於人類視覺系統(HVS)對於 PSNR 值大於 30db 的影像幾乎是無法分別出與原始影像的差異，因此本研究希望在 PSNR 值維持在 30 左右的情況下，盡可能的提高藏量，下面表 1 為這 6 張圖在 PSNR 值保持在 30 左右時的最高藏量：

表 1 最高藏量表

	標準差	PSNR	溢位	Payload
Tiffany (T=4)	51	32.493	4194	0.9738
Baboon (T=17)	19	30.738	63	0.5220
Lena (T=3)	74	32.770	11	0.9913
Jet (T=5)	74	33.623	8	0.9908
Scene (T=9)	27	29.742	34	0.8784
Peppers (T=11)	77	29.995	672	0.9881

註：第一欄的 *T* 值為 MMED 中對於不同的影像特徵所得到的 *T* 值。

藏匿後的結果如下圖：



(a) Tiffany (b) Baboon (c) Lena (d) Jet (e) Scene (f) Peppers

圖 10 六張藏匿後的影像

由表 1 可得知本實驗中在 PSNR 值保持在 30dB 左右時，有著極高的藏量。

下面表 2 為本實驗與 Lee 等學者的實驗數據在 PSNR 為 30dB 左右的數據比較：

表 2 與 Lee 等學者的比較表

Tiffany			
	Payload	PSNR	溢位
Lee 方法(T=86)	0.973804	31.228121	4822
本研究(S=51)	0.973850	32.493630	4194
Baboon			
	Payload	PSNR	溢位
Lee 方法(T=9)	0.515072	30.156863	10
本研究(S=19)	0.522045	30.738195	63
Lena			
	Payload	PSNR	溢位
Lee 方法(T=105)	0.991356	30.060167	222
本研究(S=74)	0.991364	32.770688	11
Jet			
	Payload	PSNR	溢位
Lee 方法(T=93)	0.990593	29.517609	422
本研究(S=74)	0.990883	33.623186	8
Scene			
	Payload	PSNR	溢位
Lee 方法(T=15)	0.870777	29.675332	6
本研究(S=27)	0.878490	29.742448	34
Peppers			
	Payload	PSNR	溢位
Lee 方法(T=123)	0.987999	29.428772	1102
本研究(S=77)	0.988117	29.995505	672

註：上表的 *T* 值為 Lee 方法中的門檻值。

由表 2 得知與 Lee 等學者的方法在相近的 Payload 比較之下，PSNR 值都明顯較高，表示本研究有較佳的影像品質。

5. 結論

由表 2 可得知本實驗方法在'Tiffany'、 'Lena'、'Jet'、'Peppers'等圖的 Payload 與 PSNR 值都優於 Lee 等學者的方法，Overflow/Underflow 的數量也明顯少很多。在'Baboon'與'Scene'這兩個比較複雜的圖形，如果扣除 Location Map，本實驗'Baboon'圖的 Pure Capacity 為 134834bits 仍優於 Lee 等學者的 134703bits; 本實驗'Scene'圖的 Pure Capacity 為 229202bits 仍優於 Lee 等學者的 228077bits。

關於本實驗能夠擁有這樣結果我們認為是有兩個因素所影響。第一個因素是預測方法，由於我們使用 MMED 的預測方式是對於預測'non-edge'擁有比較準確的結果，而對於'edge'的預測方法則是使用與 Lee 等學者的方法一樣，因此在預測方面我們的結果會比 Lee 等學者的預測來的準確，預測比較準確相對的失真就會比較少，藏量也會比較多。第二個因素是藏匿方法，因為本實驗的藏匿方法中，對於高於標準差 S 的像素我們不需要加減一個門檻值 T，因此有較少的失真。由此可知使用本實驗的方法可以獲得更高的影像品質。

此外，本實驗使用預測值與其鄰近像素的標準差來當作評估函數，並且由 MMED 中的影像特徵取門檻值，但是標準差小並不一定代表預測像素與實際像素的差值就會比較小，若是在像素差值較大的形況中，使用差值擴張法進行藏匿就會造成較大的失真，因此我們認為在這個部分是可以再更進一步改進的，另外由於我們使用 MMED 預測方法使我們對於'non-edge'的預測變得比較準確，但是對於'edge'的預測則是沒有多加琢磨，因此可以對'edge'使用更為準確的預測方法或是訂定更加完善的評估方法進而使實驗獲得更好的效果。

參考文獻

[1] Chin-Feng Lee, Hsing-Ling Chen, & Hao-Kuan Tso, “Embedding capacity raising in reversible data hiding based on prediction of difference expansion”, Journal of Systems and Software, 83, 2010, pp. 1864 – 1872.

[2] Chuan Qin, Chin-Chen Chang & Chang, Li-Ting Liao, “An adaptive prediction-error expansion oriented reversible information hiding scheme”, Pattern Recognition Letters 33, pp. 2166-2172, 2012.

[3] Vasiliy Sachnev, Hyoung Joong Kim,Jeho Nam Senior,Sundaram Suresh, and Yun Qing Shi, “Reversible Watermarking Algorithm Using Sorting and Prediction”, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 19, NO. 7, JULY 2009, pp. 989 – 999.

[4] 冷輝世、余奕憲，”改良 MED 邊緣檢測法以增加可逆式隱藏藏量的方法”，第七屆資訊科技國際研討會(2013)。

[5] S. Geetha, V. Kabilan, S.P. Chockalingam, & N. Kamaraj,” Varying radix numeral system based adaptive image steganography”, Information Processing Letters, 111, 2011, pp. 792 – 797.

保持邊緣特性的可逆式資訊隱藏

冷輝世
國立彰化師範大學
lenghs@cc.ncue.edu.tw

余奕憲
國立彰化師範大學數學系
s9922117@mail.ncue.edu.tw

曾顯文
朝陽科技大學
hwtseng@cyut.edu.tw

摘要

資訊隱藏技術是透過媒介，例如影像檔、視訊檔、文字檔、聲音檔等將機密訊息藏入，此技術可分為可逆式與不可逆式兩種，可逆式隱藏的主要技術有兩種，一是利用峰值點的直方圖位移技術，另一是利用差值擴張。近年來，許多學者以預測值與原始像素值差值擴張的方法得到很好的成果，如何使預測值更準確，則失真更少，進而提升藏量為本研究的主要目的。

本研究首先介紹 MMED(Modified Median Edge Detect)邊緣檢測法，藉由 MMED 檢測法結合區塊四角預測，經由實驗結果顯示，本研究所提出的方法能有效的提昇藏量與影像品質。

關鍵詞：可逆式資訊隱藏、預測值與像素值差值擴張、MMED。

Abstract

Data hiding is a technique that embed secrets message through the media, such as image files, video files, text files, audio files, etc. The main methods of reversible data hiding include histogram shifting and difference expansion. In recent years, many researchers focus on prediction-based scheme and use difference expansion. How to predict more precisely becomes an important issue. A good prediction method can reduce distortion, enlarge payload and obtain a better result.

In this study, modified median edge detection (MMED) was introduced as the proposed prediction method to reduce distortion, and the embedding area was designed to preserve edge characteristics. The experimental results show that the proposed method achieves higher payload and lower distortion.

Keywords: Reversible data hiding, prediction-based, difference expansion, modified median edge detection.

1. 前言

隨著科技的發展，網際網路縮短了人與人之間的距離，每天都有無數的資訊透過網路傳遞訊息。對於高度機密的資訊，其安全性更受到重視，進而發展出資訊隱藏技術。資訊隱藏技術是透過媒介，例如影像檔、視訊檔、文字檔、聲音檔等將機密訊息藏入，且不易被人所察覺出來。資訊隱藏技術又可分為可逆式與不可逆式，若藏入機密訊息後無法回復至原始影像稱的稱為不可逆式，可逆式則可回復至原始的影像。相較於不可逆式資訊隱藏，可逆式因為要保留還原的資訊所以藏量較低。近年來，許多學者以預測值與原始像素值差值擴張的方法得到很好的成果，如何使預測值更準確，則失真更少，進而提升藏量為本研究的主要目的。

這些預測方法中，包括 Lee 等學者[1]利用目標像素 x 的鄰近像素 a、b (如圖 1)，將 $(a+b)/2$ 作為 x 的預測值，Chuan Qin 等學者[2]利用 x 鄰近像素 a、b、c，將 $(a+b+c)/3$ 作為 x 的預測值，以及著名的邊緣預測方法 MED (Median Edge Detect)等等。在本文中，引用近期冷等學者[4]保留邊緣特性的 MMED 預測法，進而減少預測值與像素值的差值，並提高藏量。

本文其餘的部分安排如下：第二章介紹相關研究，研究方法則在第三章說明，實驗結果在第四章說明，最後是結論。

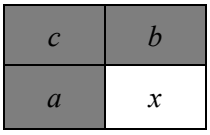


圖 1 目標像素 x 與相鄰像素

2. 相關研究

在本章節中將介紹：MED、MMED 與差值擴張。在底下的小節中，我們定義被預測像素值為 x，其預測像素值為 $\hat{x}$，如圖 1，陰影區域代表是 x 的相鄰像素，a、b、c 分別為相對位置的像素值。

2.1 MED

Weinberger(2000)[5]所提出的 MED 預測法：假設在原始影像中 a、b、c 為目標像素 x 的鄰近像素。則其預測值為

$$\hat{x}=\begin{cases}\min(a,b), & if\ c\geq\max(a,b)\\ \max(a,b), & if\ c\leq\min(a,b)\\ a+b-c, & otherwise\end{cases}$$

2.2 MMED

冷等學者(2013)[4]提出的保留邊緣特性的 MMED 預測法：假設在原始影像中 a、b、c 為目標像素 x 的鄰近像素，對於個別的影像特徵可找到一個門檻值 T，使其預測值在非邊緣區時更為準確。

則其預測值為

$$\hat{x}=\begin{cases}\min(a,b) & , \quad if \quad c\geq\max(a,b)\\ \max(a,b) & , \quad if \quad c\leq\min(a,b)\\ \dfrac{a+b+c}{3} & , \quad c\in(a,b) \quad \left|c-\dfrac{a+b}{2}\right|<T, \quad T\in N\\ a+b-c & , \quad otherwise\end{cases}$$

在此定義中，將目標像素定位在非邊緣區，如果 c 與 $\frac{a+b}{2}$ 的差小於個別的影像特徵找到的門檻值 T，則預測值可設為 $\frac{a+b+c}{3}$，修改後的 MMED 預測值經由數學式証明可減少預測的誤差，且可使單一或區域提高峰值點提高，增加其資訊隱藏的容量，進而判斷影像的特性選擇適用的可逆式資訊隱藏技術。

本研究使用 SIPI 影像資料庫的六張 512x512 灰階影像經由實驗可得到 MMED 的門檻值如表 1：

表 1 實驗圖形的 MMED 門檻值

	MMED Threshold
Tiffany	T=4
Baboon	T=10
Lena	T=3
F16	T=5
Boats	T=9
Peppers	T=5

2.3 差值擴張

Tian 學者(2003)[3]提出差值擴張的方法利用鄰近像素的相關性進行資訊隱藏，假設兩個預測像素分別為 u=3,v=6，藏入的機密訊息為 $b=(01)_2$，首先計算整數平均值 l 及預測像素差值 d

$l=\left\lfloor\frac{u+v}{2}\right\rfloor=\left\lfloor\frac{3+6}{2}\right\rfloor=4$

$d=v-u=6-3=3$

接著新的預測像素差值 d'得如下：

$d'=2\times d+b=2\times3+1=7$

最後，利用新的預測像素差值 d'和整數平均 l 完成嵌入

$$v'=l+\left\lfloor\frac{d'+b}{2}\right\rfloor=4+\left\lfloor\frac{7+1}{2}\right\rfloor=8$$

$$u'=l-\left\lfloor\frac{d'}{2}\right\rfloor=4-3=1$$

知道新的預測像素 v',u'，計算平均數 l'及預測像素差值 d'，可取出嵌入資訊且可還原。

平均數 ： $l'=\left\lfloor\frac{u'+v'}{2}\right\rfloor=\left\lfloor\frac{1+8}{2}\right\rfloor=4$

像素差值 ： $d'=v'-u'=8-1=7$

嵌入的資訊 ： $b=d'-\left\lfloor\frac{d'}{2}\right\rfloor\times2=7-6=1$

原像素差值 ： $d=\left\lfloor\frac{d'-b}{2}\right\rfloor=\left\lfloor\frac{7-1}{2}\right\rfloor=3$

還原後： $v=l'+\left\lfloor\frac{d+b}{2}\right\rfloor=4+2=6$

還原後： $u=l'-\left\lfloor\frac{d}{2}\right\rfloor=4-1=3$

在 2010 時，Lee 學者提出了利用預測值與原始像素值的差值進行可逆式隱藏，此方法不僅大大的增加嵌入量，且減少影像的失真。

原始影像為一個 MxN 的灰階影像圖，定義 $I(x,y)$為原始影像某一像素的座標(x,y)，被預測像素定義為 $\hat{I}(x,y)$，T 代表門檻值，用來控制影像失真，符號 δ 代表原始影像直方圖收縮的距離，且 $\delta=T+1$，機密訊息 $s=\{0,1\}$。

除了第一行和第一列外，首先以 raster-scan 進行掃描原始影像以得到預測像素 $\hat{I}(x,y)$，計算如下:

$$\hat{I}(x,y)=\left\lfloor\frac{I(x-1,y)+I(x,y-1)}{2}\right\rfloor$$

差值 d 計算如右: $d=\left|I(x,y)-\hat{I}(x,y)\right|$

在此方法中，差值 d 可能出現兩種情況：$d\leq T$ 和 $d>T$，前者可嵌入機密訊息，後者則不能。

嵌入機密訊息：

(1) 如果 $d\leq T$，機密訊息藉如下面的式子嵌入：

$$I'(x,y)=\begin{cases}\hat{I}(x,y)+2\times d+s, & if\ \hat{I}(x,y)\leq I(x,y)\\ \hat{I}(x,y)-2\times d-s, & otherwise\end{cases}$$

(2) 如果 d>T，則執行下面式子：

$$I'(x,y)=\begin{cases}I(x,y)+\delta, & if\ \hat{I}(x,y)\leq I(x,y)\\ I(x,y)-\delta, & otherwise\end{cases}$$

取出機密訊息：

除了第一行和第一列外，首先以 raster-scan 進行掃描含有機密訊息的影像影像以得到預測像素 $\hat{I}'(x,y)$，以及 $I'(x,y)$和 $I'(x,y)$的差值 d'

(1) $d'\leq2\times T+1$，機密訊息可被取出，且 $I(x,y)$ 回復如下:

$s=\mathrm{LSB}(d')$

$$I(x,y)=\begin{cases}\hat{I}'(x,y)+\left\lfloor\frac{d'}{2}\right\rfloor, & if\ \hat{I}(x,y)\le I'(x,y)\\ \hat{I}'(x,y)-\left\lfloor\frac{d'}{2}\right\rfloor, & otherwise\end{cases}$$

(2) $d'>2\times T+1$，I(x,y)回復如下:

$$I(x,y)=\begin{cases}\hat{I}'(x,y)-\delta, & if\ \hat{I}'(x,y)\le I'(x,y)\\ \hat{I}'(x,y)+\delta, & otherwise\end{cases}$$

3. 研究方法

在本章節中將介紹研究方法的嵌入程序、取出程序以及溢位的問題。

在本研究中，利用 MMED 的預測法，將嵌入的範圍限制在的灰色區塊中，如圖 2(a)，且利用鄰近像素對中間像素做預測，如圖 2(b)，此方法可保留邊緣特性並減少預測的誤差，且能使區域峰值點提高，增加資訊隱藏的容量。

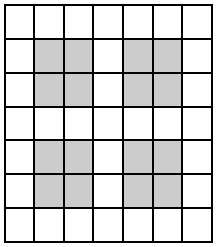


圖 2(a) 機密訊息的嵌入範圍

$I(i\text{-}1,j\text{-}1)$	$I(i\text{-}1,j)$	$I(i\text{-}1,j+1)$	$I(i\text{-}1,j+2)$
$I(i,j\text{-}1)$	$I(i,j)$	$I(i,j+1)$	$I(i,j+2)$
$I(i+1,j\text{-}1)$	$I(i+1,j)$	$I(i+1,j+1)$	$I(i+1,j+2)$
$I(i+2,j\text{-}1)$	$I(i+2,j)$	$I(i+2,j+1)$	$I(i+2,j+2)$

圖 2(b) 鄰近像素對中間區塊做預測

3.1 嵌入程序

原始影像為一個MxN的灰階影像圖，定義$I(x,y)$為原始影像某一像素的座標(x,y)，被預測像素定義為$\hat{I}(x,y)$，T 代表門檻值，用來控制影像失真，符號δ代表原始影像直方圖收縮的距離，且δ=T+1，機密訊息 s={0,1}。

如圖 2，$I(i,j)$、$I(i,j+1)$、$I(i+1,j)$、$I(i+1,j+1)$為被預測像素，

$\hat{I}(i,j)$是由左上角的三點鄰近像素透過 MMED 預測而得到；

$\hat{I}(i,j+1)$是由右上角的三點鄰近像素透過 MMED 預測而得到；

$\hat{I}(i+1,j)$是由左下角的三點鄰近像素透過 MMED 預測而得到；

$\hat{I}(i+1,j+1)$是由左下角的三點鄰近像素透過 MMED 預測而得到。

當個區塊的$\hat{I}(i,j)$計算好後，計算$I(i,j)$和$\hat{I}(i,j)$的預測誤差值d，計算式如下:

$$d=\left|I(i,j)-\hat{I}(i,j)\right|$$

差值d可能出現兩種情況：$d\le$T 和 $d>$T，前者可嵌入機密訊息，後者則不能。

嵌入機密訊息：

(1) 如果$d\le T$，機密訊息藉如下面的式子嵌入：

$$I'(x,y)=\begin{cases}\hat{I}(x,y)+2\times d+s, & if\ \hat{I}(x,y)\le I(x,y)\\ \hat{I}(x,y)-2\times d-s, & otherwise\end{cases}$$

(2) 如果$d>T$，則執行下面式子：

$$I'(x,y)=\begin{cases}I(x,y)+\delta, & if\ \hat{I}(x,y)\le I(x,y)\\ I(x,y)-\delta, & otherwise\end{cases}$$

以下將用更詳細的例子來說明嵌入程序，以 Tiffany 影像(修改 MED 的 T=4)，假設門檻值 T=4，δ=4+1=5，機密訊息s=1010。

圖 3(a)為嵌入前像素。

$\hat{I}_1(2,2)$=78+179-80=177

$\hat{I}_2(2,3)$=177

$\hat{I}_3(3,2)$=177

$\hat{I}_4(3,3)=\lfloor(175+177+179)/3\rfloor$=177

預測像素差值分別為:

$d_1=|178-177|$=1

$d_2=|177-177|$=0

$d_3=|175-177|$=2

$d_4=|173-177|$=4

因為d_1、d_2、d_3、d_4皆小於門檻值 T，透過差值擴張，將機密訊息藏入，

$\hat{I}_1(2,2)$=177+2x1+1=180

$\hat{I}_2(2,3)$=177+2x0+0=177

$\hat{I}_3(3,2)$=177-2x2-1=172

$\hat{I}_4(3,3)$=177-2x4-0=169

嵌入後像素I'如圖 3(b)。

	1	2	3	4
1	80	179	175	175
2	78	178	177	177
3	79	175	173	179
4	77	177	175	177

圖 3(a)嵌入前像素

	1	2	3	4
1	80	179	175	175
2	78	180	177	177
3	79	172	169	179
4	77	177	175	177

圖 3(b)嵌入後像素

3.2 取出程序

預測像素值 $\hat{I}'$，透過由左到右、由上到下的循序掃描得到，預測差值 d' 計算式如下:

$d'=\left|\hat{I}'(i,j)-I'(i,j)\right|$.

在取出與恢復的階段，主要有兩個判斷式進行取出機密訊息 s 以及恢復原始像素 $I(i,j)$.

嵌入機密訊息：

(1) $d'\le 2\times T+1$ 機密訊息可被取出，且 $I(x,y)$ 恢復如下:

$s=d'$ mod 2.

$$I(x,y)=\begin{cases}\hat{I}'(x,y)+\left\lfloor\frac{d'}{2}\right\rfloor, & if\ \hat{I}(x,y)\le I'(x,y)\\ \hat{I}'(x,y)-\left\lfloor\frac{d'}{2}\right\rfloor, & otherwise\end{cases}$$

(2) $d'>2\times T+1$，$I(x,y)$恢復如下:

$$I(x,y)=\begin{cases}\hat{I}'(x,y)-\delta, & if\ \hat{I}'(x,y)\le I'(x,y)\\ \hat{I}'(x,y)+\delta, & otherwise\end{cases}$$

以下將用更詳細的例子來說明取出機密訊息與恢復原始的程序，以'Tiffany'影像(MMED 取 T=4)，假設門檻值 T=4，δ=4+1=5，假設嵌入後的像素如圖 3(b).

I_1' (2,2)=180，其預測值 $\hat{I}_1'$(2,2)=78+179-80=177，預測誤差 $d_1'=\left|180-177\right|$=3，因為 $d_1'\le 2\times T+1=5$，

機密訊息 s=3 mod 2=1

原始像素值 I(2,2)=177+1=178

I_2' (2,3)=177，其預測值 $\hat{I}_2'$(2,3)=177，預測誤差 $d_2'=\left|177-177\right|$=0，因為 $d_2'\le 2\times T+1=5$，

機密訊息 s=0

原始像素值 I(2,3)=177+0=177

I_3' (3,2)=172，其預測值 $\hat{I}_3'$(3,2)=177，預測誤差 $d_3'=\left|172-177\right|$=5，因為 $d_3'\le 2\times T+1=5$，

機密訊息 s=3 mod 2=1

原始像素值 I(3,2)= $177-\lfloor 5/2\rfloor=175$

I_4' (3,3)=169，其預測值

$\hat{I}_4'$(3,3)= $\lfloor(175+177+179)/3\rfloor$ =177，預測誤差 $d_4'=\left|169-177\right|$=8，因為 $d_4'\le 2\times T+1=5$，

機密訊息 s=8 mod 2=0

原始像素值 I(3,3)= $177-\lfloor 8/2\rfloor=173$

3.3 溢位問題

在嵌入過程中，若像素值發生溢位(Overflow/Underflow)問題，則使用 Location Map 的方法，紀錄 x、y 的位置且不藏入機密訊息，再取出的過程中，先判斷是否存在於 Location Map 中，若否再進行取出的動作。

4. 實驗結果

本研究使用 SIPI 影像資料庫的六張 512x512 灰階影像進行測試(如圖 4)，並使用表 1 的 MMED 門檻：



(a)Tiffany (b)Baboon (c) Lena (d) F16 (e) Boats (f) Peppers

圖 4 六張測試圖

4.1 MED 與 MMED 差值比較圖

由圖 5-10 各圖的 MMED 與 MED 的差值比較可得知 MMED 可得到較精確的預測值。

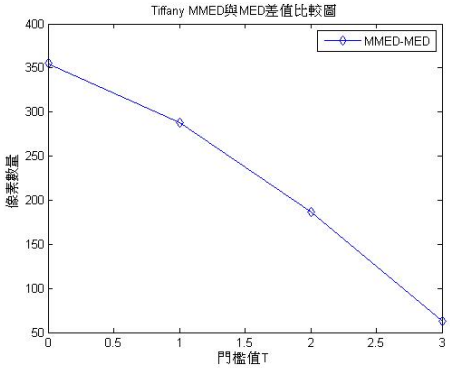


圖 5 Tiffany 圖 MMED 與 MED 的差值比較

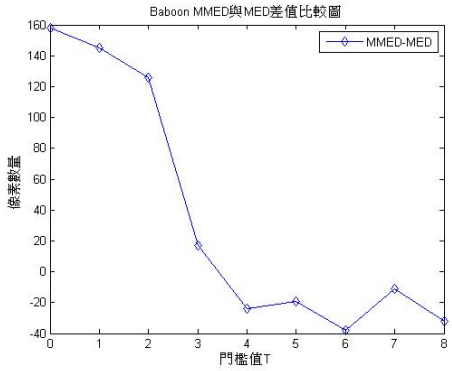


圖 6 Baboon 圖 MMED 與 MED 的差值比較

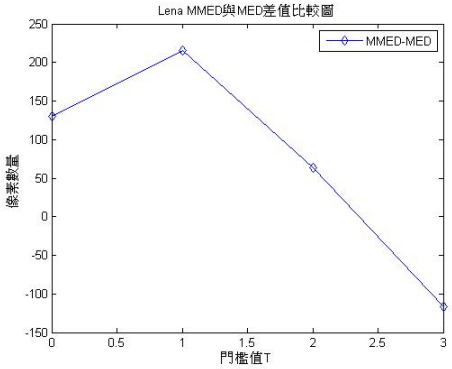


圖 7 Lena 圖 MMED 與 MED 的差值比較

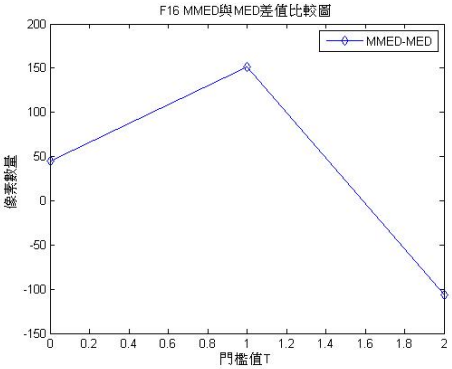


圖 8 F16 圖 MMED 與 MED 差值

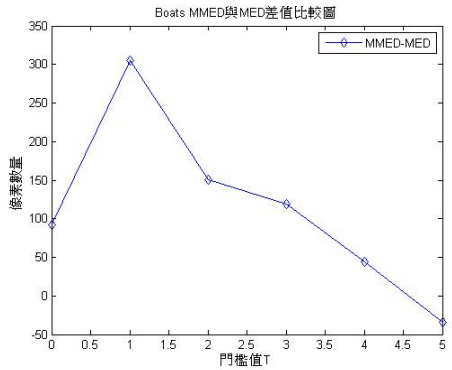


圖 9 Boats 圖 MMED 與 MED 的差值比較

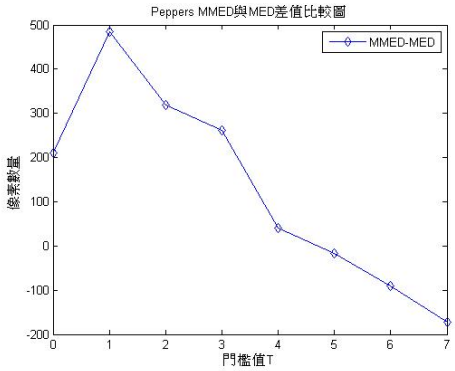


圖 10 Peppers 圖 MMED 與 MED 的差值比較

4.2 嵌入效果與品質

由表 2-7 各表的嵌入效果與品質，除表 2 與表 7 有溢位產生時另外計算 Pure Payload，其餘皆無溢位情形。當對偽裝影像品質要求較高時，必須取較小的門檻值，而本研究方法的預測精準度集中於較小的門檻值。在此情況下，本研究方法會有較大的藏入量。

表 2 Tiffany 圖嵌入效果與品質

Tiffany(T=4)		PSNR	Capacity	Payload	溢位	Pure Payload
proposed	T=0	45.83	14116	0.122	318	0.034
MED		45.91	13947	0.120	295	0.038
proposed	T<=1	41.90	39333	0.340	425	0.222
MED		41.89	38946	0.336	456	0.210
proposed	T<=2	40.02	59033	0.510	497	0.373
MED		40.05	58287	0.504	523	0.359
proposed	T<=3	38.74	73636	0.636	646	0.458
MED		38.77	73025	0.631	625	0.458

表 3 baboon 圖嵌入效果與品質

Baboon(T=10)		PSNR	Capacity	Payload
proposed	T=0	41.59	4045	0.034
MED		41.54	4025	0.034
proposed	T<=1	37.45	11889	0.102
MED		37.29	11885	0.102
proposed	T<=2	35.48	19509	0.168
MED		35.36	19361	0.167
Our method	T<=3	34.20	26905	0.232
MED		34.14	26633	0.230

表 4 Lena 圖嵌入效果與品質

Lena(T=3)		PSNR	Capacity	Payload
proposed	T=0	46.98	12301	0.106
MED		46.98	12237	0.105
proposed	T<=1	42.54	34021	0.294
MED		42.55	33733	0.291
proposed	T<=2	40.54	53213	0.460
MED		40.51	52777	0.456

表 5 F16 嵌入效果與品質

F16(T=5)		PSNR	Capacity	Payload
proposed	T=0	45.94	20193	0.174
MED		46.10	19917	0.172
proposed	T<=1	41.29	51505	0.445
MED		41.42	51381	0.444
proposed	T<=2	38.97	70961	0.613
MED		39.04	70765	0.612

表 6 Boats MED 嵌入效果與品質

Boats(T=9)		PSNR	Capacity	Payload
proposed	T=0	44.10	7349	0.063
MED		44.08	7053	0.061
proposed	T<=1	40.04	20605	0.178
MED		40.05	19921	0.172
proposed	T<=2	38.03	32541	0.281
MED		38.04	31673	0.273
proposed	T<=3	36.94	42949	0.371
MED		36.93	41949	0.362
proposed	T<=4	36.02	52165	0.451
MED		36.02	51197	0.44

表 7 Peppers 嵌入效果與品質

Pepper(T=5)		PSNR	Capacity	Payload	溢位	Pure Payload
proposed	T=0	46.32	7677	0.066	0	0.066
MED		46.33	7357	0.063	0	0.063
proposed	T<=1	42.08	22717	0.196	0	0.196
MED		42.14	21845	0.188	0	0.188
proposed	T<=2	40.19	36845	0.318	0	0.318
MED		40.26	35821	0.309	0	0.309
proposed	T<=3	38.91	50109	0.433	5	0.432
MED		38.91	48813	0.422	5	0.420

5. 結論

利用預測值與原始像素值的差值擴張技術主要差異在於預測方式。Lee 等學者、Chuan Qin 等學者使用平均值作為預測值，以數學的角度減少差值；MED 則是以邊緣特性的角度預測，MMED 則加強了 MED 對非邊緣區域的預測。

限制嵌入區域可以加強對邊緣區的預測，使用 MMED 則使非邊緣區的預測值更準確。經由實驗結果驗證了本研究使預測值更準確，失真更少，進而提升藏量。

參考文獻

[1] Chin-Feng Lee, Hsing-Ling Chenb & Hao-Kuan Tsoc, “Embedding capacity raising in reversible data hiding based on prediction of difference expansion”, Journal of Systems and Software, 83, pp. 1864–1872, 2010.

[2] Chuan Qin, Chin-Chen Chang & Chang, Li-Ting Liao, “An adaptive prediction-error expansion oriented reversible information hiding scheme”, Pattern Recognition Letters 33, pp. 2166-2172, 2012.

[3] Tian, J., “Reversible data embedding using a difference expansion”, IEEE Transactions on Circuits and Systems for Video Technology, 16(3), pp. 721–730, 2007.

[4] 冷輝世，余奕憲，“改良 MED 邊緣檢測法以增加可逆式隱藏藏量的方法”，第七屆資訊科技國際研討會，2013。

[5] Weinberger MJ & Seroussi G, “The LOCO-I lossless image compression algorithm:principles and standardization into JPEG-LS”, IEEE Trans Image Process, 9(8), pp. 1309-1324, 2000.

以網頁驗證碼為基礎的側錄程式密碼防禦機制

許玉芳[1] 沈慧宇[2] 金馳[3]
建國科技大學[1,3]電子工程系 [2]資訊與網路通訊系
[1]yfshi@cc.ctu.edu.tw , [2]wyshen@ctu.edu.tw, [3]robinpig46@yahoo.com.tw

摘要

傳統上，為防制駭客以側錄程式攻擊原使用者的帳號密碼登入，大部分多採用 OTP – One-Time Password 一次性密碼的保護機制，或軟體式動態鍵盤的輸入方式，以避免攻擊者有效攔截使用者的帳號密碼資料。但是 OTP 的缺點必須在使用者端的電腦內安裝相關的硬體讀卡設備；而動態鍵盤的程式仍存在被攻擊的風險，且往往需要另申請合法憑證。

本文嘗試提出一種全新的密碼登入方式，使用者無須再記住密碼的明文資料，相反的，使用者需記住的是密碼的產生方式，並利用登入驗證碼的亂數產生機制與圖形辨識難度，以防禦本地電腦的側錄程式攻擊，這樣的防禦機制完全不需要額外安裝任何硬體設備或軟體程式，而且每次登入的密碼也會完全不同，換言之，本文所提出的防護方式是更便捷且仍具有 OTP 所擁有一次性密碼的功能。

關鍵詞：側錄程式、動態鍵盤、一次性密碼

Abstract

Traditionally, in order to protect user password from eavesdropping program such as keylogger, One-Time Password (OTP) or software dynamic keyboard is always adopted to prevent password and user name from being intercepted. However, OTP solution needs additional hardware reader installation and software dynamic keyboard exist some exploit risks. Moreover, dynamic keyboard should still need additional requirement for valid certificate.

In this paper, we try to propose a new authentication approach. It is not necessary for user to remember his password context. Instead, user should only keep in mind how password is created. Additionally, in order to enhance the password hacking complexity, the graphical authentication code which varies with login times is inserted to mix with the password generation. In other words, the real password will be dependent on the authentication code. Therefore, the login password must be valid for only one time. Since the login password changes each time automatically, we are convinced that this approach will provide sufficient security for one-time password solution without any software package or hardware device involved.

Keywords: keylogger, dynamic keyboard, one-time password

1. 研究動機與目的

目前網際網路所存在的惡意程式 (Malware) 中，木馬程式可能是最為普遍，因為它可以輕易透過釣魚 (Phishing) 的方式就下載到使用者電腦。很多木馬程式 (Trojan) 往往會包裝側錄程式 (Keylogger)，側錄程式可以在背景過程讀取使用者所輸入的鍵盤資料，使用者將因此在不知不覺中輸入被攔截的帳號與密碼等相關重要資訊，攻擊者再將所攔截到帳號與密碼等資訊傳送到遠端駭客網站，而這也正是許多網路帳號被盜用日益嚴重的重要原因。

為能解決帳號密碼被盜用的問題，許多網站會提供動態鍵盤的軟體模擬方式以避免觸發敲打實體鍵盤，這個方式確實可以應付許多側錄程式，但是點選動態鍵盤的行為資訊仍可能在網路中被攔截，相關的密碼明文資料還是很可能會被分析出來，因此大部分的動態鍵盤網頁都會搭配 HTTPS [1][2][3]的通訊協定，以建立傳送端與接收端雙方的加密通道。

HTTPS 通訊協定可以建立瀏覽器與伺服器之間的加密通道，主要的基本原理是利用伺服器憑證 (Certificate) 內的公鑰 (Public Key)[4] 來傳遞後續加密與解密所需要的對稱鑰匙 (Session Key)，由於瀏覽器會主動透過憑證授權中心 (CA-Certificate Authority) 來驗證伺服器憑證是否合法，因此透過公鑰所加密傳送的對稱鑰匙將具備合法使用的有效性，換言之，瀏覽器可以依據對稱鑰匙將網路封包轉換為密文，而伺服器則可以利用該對稱鑰匙將相關的密文還原為明文資料，反之亦然。

由於上述 HTTPS 運作原理具有非常完備的理論基礎，而且破解其加解密過程需要很高成本與時間的代價，因此 HTTPS 不僅適用於帳號密碼的登入網頁或會員帳號的申請網頁，也普遍應用於金融銀行或電子商務的資金交易，但是，使用 HTTPS 通訊協定必須申請合法的憑證，若是沒有合法的憑證，瀏覽器會出現伺服器網站可能是偽造的警告網頁，事實上，許多網站基於成本考量，往往都不會申請合法的憑證。

OTP (One-Time Password) [5]是一次性的密碼的技術，密碼使用一次後立即失效，因此也可以用來防禦側錄程式的攻擊，然而，由於使用者需要再加裝相關的讀卡機才可以利用 OTP 的功能，因此，可能也無法全面性推廣。

本文所提出的方法完全異於動態鍵盤與 OTP 的防禦機制，第二節將說明本方法的設計理念；第三節則舉例說明系統運作細節；第四節說明本方法的相關重要特色；最後，本文會針對本論文做一簡要的結論。

2. 設計理念

本文的設計理念與 HTTPS 相近，如下圖 1，HTTPS 主要功能就是建立瀏覽器與伺服器的加密通道，因此，攻擊者無法從網路中攔劫任何有效的資料。一樣的道理，若是使用者與瀏覽器之間存在隨機組合的資料變化，攻擊者自然也無法執行任何側錄的動作。

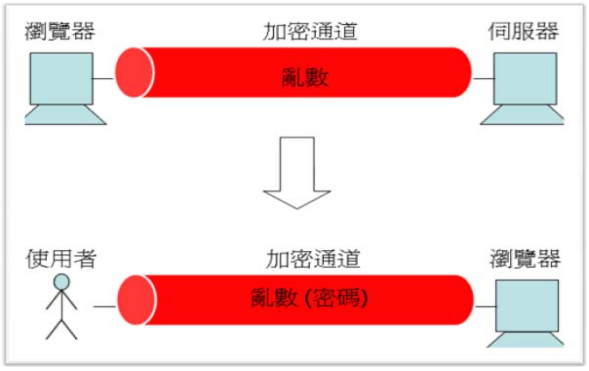


圖 1 可以避免被側錄的加密通道

本文設計方式就是利用網頁驗證碼的隨機明文資料，再透過適當的計算規則，產生密碼的隨機明文資料，密碼內容本身雖然是以明文的方式呈現，其內容卻是數字與文字的隨機組合，下圖 2 代表密碼產生方式運作的示意圖，其中，網頁驗證碼是一隨機的亂數字元，使用者只需要記住適當的計算規則，就可以產生各種不同的密碼。

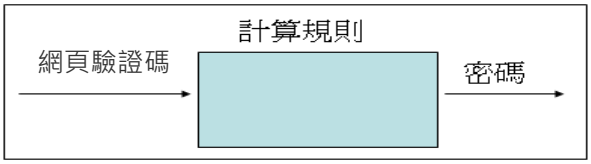


圖 2 登入密碼產生方式

網頁驗證碼主要是以圖形來顯示文字與數字的隨機組合 (如下圖 3 所示)，大部分是應用在帳號密碼的登入網頁或會員帳號的申請網頁，主要目的是用以防止機器程式將大量資料直接輸入網頁的相關欄位，來增加驗證的複雜性，由於大部分機器程式無法判讀以圖形所表示的文字或數字，(除非機器程式本身具備類似 OCR-Optical Character Recognition 光學字元辨識能力)，因此，網頁驗證碼確實可以在前端瀏覽器有效阻擋惡意的機器程式。



圖 3 網頁驗證碼範例

3. 本系統運作

伺服器依據使用者的帳號基本資料決定所要列舉的計算規則，使用者在申請帳號時就必須決定所使用的計算規則，一旦決定相關的計算規則，使用者就必須記住該規則的計算方式。如下圖 4 所示，使用者如果選擇替換式規則，他可以決定右起第 4 個位置要替換為 Z，第 6 個位置要替換為 9；使用者如果選擇循環式規則，他可以決定左移 3 個位置，然後右補 A5C。

在本系統架構中，使用者不再需要記住密碼，使用者只需要記住登入演算法所產生的計算規則，當使用者連線到登入網頁時，登入網頁一樣會出現帳號密碼的輸入欄位，同時也會出現一驗證碼圖示。它與傳統驗證碼不同的是本系統架構的密碼與驗證碼存在一定的計算規則，使用者必須依照記憶中的計算規則與驗證碼一同運算，才可以得出密碼的內容，換言之，使用者不再需要記住密碼，使用者只需要記住登入演算法的計算規則即可。

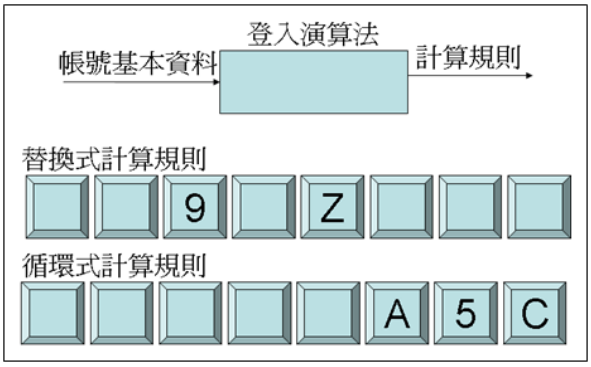


圖 4 計算規則範例

所謂計算規則可能是乘以 2 [*2], 加上 3 [+3], 右起第 3 個字元改為 p [p?3], 右移 2 位且左補 9k [9k>2], 或是左移 1 位且右補 m [1<m] 等類似的規則。

舉例來說，若是登入網頁所出現的驗證碼為 1234，那麼上述計算規則所換算出來的密碼如下。

[*2]	所對應的密碼為 2468，
[+3]	所對應的密碼為 1237，
[p?3]	所對應的密碼為 1p34，
[9k>2]	所對應的密碼為 9k12，
[1<m]	所對應的密碼為 234m。

由於計算規則並沒有任何特別的限制，而且計算規則不會提示於任何網頁內容 (但是使用者與伺服器會記住計算規則)，所以所對應的密碼不僅每一次登入都不相同，而且所對應的密碼也可以展現相當高的亂度 (因為驗證碼本身就是亂數產生器所建立)。

由於伺服器會記住使用者自由定義的驗證碼與計算規則，因此雙方一定都可以驗證密碼的正確性。

本系統實作範例介面如下圖所示，其中圖 5 代表系統登入畫面，每次登入的密碼內容都與驗證碼有關聯性，因此，密碼內容只有一次有效性。



圖 5 系統登入介面

另外，圖 6 是申請新帳號時所定義的密碼產生方式，使用者必須記住自己所勾選的密碼產生方式，依據驗證碼字元內容執行位移、取代或交換的字元操作運算以產生動態的密碼內容。由於每次登入系統時驗證碼都不會一樣，密碼的明碼內容也會隨之改變，因此，使用者無須記住密碼的明碼內容 ，僅須記住密碼的產生方式。

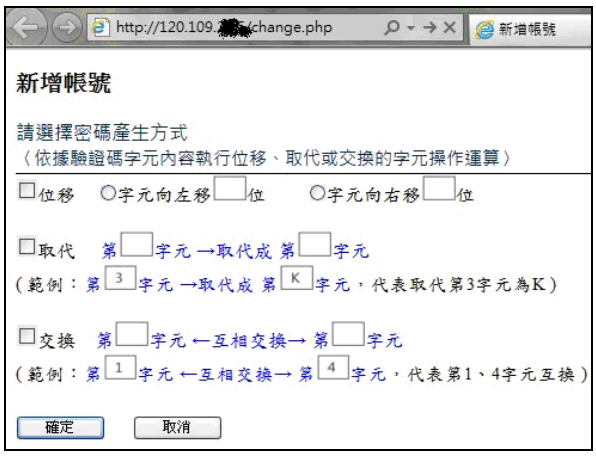


圖 6 密碼產生方式操作介面

4. 本系統特色

(1) 網路攔截密碼的安全強度高

本文提出的方法所產生的密碼是以明文的方式在網路上傳送，由於每次登入的密碼都不相同，所以即便攻擊者攔截相關的密碼資料也無法使用。但是，以明文方式表現的密碼可以被進一步分析，因為攻擊者會希望了解登入演算法的計算規則，然而，這一部份的分析過程還需要再搭配使用者的驗證碼規則，而驗證碼是以圖形的方式隨機呈現數字與文字的組合，因此破解的難度將大幅提高，而這也正是本文採用驗證碼的主要原因。

(2) 密碼方便性

本文所提出的密碼運作機制有別於傳統的密碼記憶方式，傳統上，使用者所背記的是密碼明文資料，然而，在本文所介紹的方式中，使用者需要記憶的卻是密碼明文的產生方式，密碼長度越長，就越能顯示出我們所提供的方法的方便性，事實上，以 15 個字元長度的密碼明文資料為例，若是採用 [+3] 的計算規則，使用者僅需記住 +3 這樣的規則即可。

(3) 本地攔截密碼的防禦入侵度高

即便攻擊者以側錄程式攔截使用者與瀏覽器之間所輸入的密碼資料，甚至以類似 OCR 的方式判讀驗證碼的內容，攻擊者依然無法入侵使用者的登入網頁，因為輸入演算法所產生的每一種計算規則都具有很高的變化性，入侵難度相對非常高。

(4) 一次性有效的密碼

本方式所提出的登入方式具有非常特殊的意義，尤其當伺服器主機受到某種程度的入侵時 (例如攻擊者可以利用 injection 的方式取得網頁內容的控制權，但是由於存取管控的機制，卻仍無法取得 root 管理者的密碼)，使用者瀏覽器所呈現的動態鍵盤網頁有可能是攻擊者所偽造的，攻擊者處心積慮希望能在伺服器端攔截到使用者的帳號密碼資料 ，但是，就如同前文所述，攻擊者所取得的仍屬一次性有效的密碼，因而無法以使用者的帳號執行入侵動作。

5. 結論

本文所建議的驗證系統方式不僅不需要額外安裝任何軟體或硬體，每次所產生的登入密碼也完全不同。此外，計算規則雖然簡易，卻容易記憶，如果再將日期或特殊紀念日等相關變數考慮進去，不僅依然有方便記憶的特性，同時也大幅提高其複雜度。

本系統的使用最大的改變是在於密碼的記憶方式，如果不必去記憶密碼的明文，改而從原始基礎去記憶密碼的產生方式，瀏覽器與使用者之間所傳遞的輸入資料就可以呈現亂數的組合，因此可以免除被攻擊者側錄到原始密碼的明文資料。

參考文獻

[1] RFC 2818, “HTTP over TLS”.

[2] Rescorla, E. SSL and TLS: Designing and Building Secure System. Reading, MA: Addison-Wesley, 2001.

[3] Cormen, T; Leiserson, C; Rivest, R; and Stein, C, “Introduction to Algorithm”, Cambridge, MA: MIT Press, 2001.

[4] RFC 2459, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”.

[5] RFC 2289, “A One-Time Password System”.

網格計算之通訊安全設計

劉正義 [1]
[1]環球科技大學 資訊管理系
chengyi6129@gmail.com

黃慧鳳 [2,*] 詹昭文 [3] 程瑞芳 [4]
[2,3,4]國立台中科技大學 資訊工程系
{phoenix, ccwen, s17013003}@nutc.edu.tw

摘要

由於日益成長的計算服務，資源分享已愈來愈普及化，網格運算（Grid Computing）有可能成為未來的資訊基礎建設，因此，資通安全於網格運算之環境的應用是愈來愈受重視。又目前大部份之網格運算的研究，在執行群組成員的金鑰協定時都必須透過驗證中心，如此易增加驗證中心在計算方面與傳送時之負擔。基於二次剩餘，本研究提出一個具低運算量與傳輸量的群組通訊安全於網格計算(Grid Computing)應用服務之協定， 除了保護資料在傳輸的過程中免於遭受它人的存取或修改以外，所提之技術中，其傳送端與接收端的計算量，隨著群組通訊成員的數量增加並沒有明顯的差異，且執行群組的金鑰協定時不須要依賴驗證中心的參與而產生，將可降低驗證中心的負擔，更能提升資訊服務的品質，並提供安全與高效能的運算平台，可加速重要研究之進行。

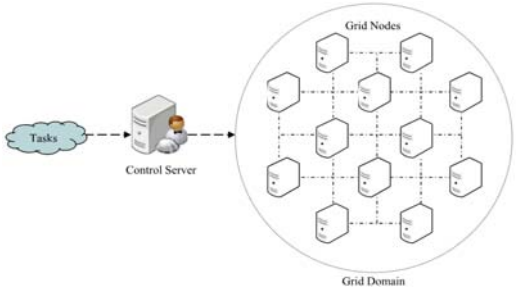
關鍵詞: 網格運算，二次剩餘 (Quadratic Residue) ，通訊安全

1. 前言

近數十年來網路科技的快速成長，人們逐漸習慣利用這些網際網路應用來處理一些日常工作，進一步享受便利的生活。舉凡郵寄信件、檔案分享、訊息交換、購物、醫療照護訊息等，使用者只需坐在電腦前即可完成。而網格計算 (Grid Computing)主要概念是將包括軟、硬體的分散伺服器資源、資料庫、儲存設備等，如(圖一)[14]，透過網路串聯以組成虛擬的超級電腦進而分享運算資源。以現今電腦科技進步，個人電腦的運算能力，早已遠遠超越當年計算主力之工作站電腦，然而一般大部份之桌上型電腦，其處理工作主要為「低運算需求」之文書處理、上網瀏覽、郵寄信件、與檔案分享等，因此可以想見，座落於校園內之「行政用電腦」，以及「電腦教室」之電腦，絕大多數時間，其 CPU 皆處於「閒置」的狀況。倘若能透過網路結集而充分運用其閒置資源，肯定能提供高效能之運算能力，且未來更能省下一筆可觀的軟硬體建置成本費用與預算。

而對企業而言，只需運用現有科技成本的一小部份，即能有效運用且聯結網路現有設備的資訊資源，隨而獲得更為強大的運算能力。網格運算還可讓分散於各地的虛擬組織，協調彼此的資源分享，同時滿足大量運算的需求。而集合分散的運算資源之外，Grid Computing 能夠經由網路管理組織內任何一個可使用的運算資源，進而降低伺服器的閒置時間。然而，為了防止非法入侵的存取或篡改以及保護系統資源的安全，所以散佈於網格計算(Grid Computing)中的節點通訊安全更顯得很重要。因此，近年來，陸續都有學者提出於網格運算之各節點間或群組通訊安全機制[1]，[2]，[4]-[7]，[17]，以確保資料在傳送的過程中免於遭受它人的存取或修改。但在這些方法中，有些學者所提之機制並不安全[3]，[8]-[11]，而在有些學者的方法中，其網格運算中很難動態刪除或加入新節點或群組成員[12]。

(圖一)



在2008年，Zhu-Wu[16]雖然提出網格運算之節點或群組成員可動態加入，但是各個成員須存有大量相關之資料量； 後來Yoon-Yoo[14]學者亦證明Zhu-Wu方法易遭受偽造攻擊並提出新的改進方式。因此，Yoon-Yoo [14]提出新的網格節點或群組成員之安全通訊機制，以改進Zhu-Wu等人的安全性與效能。 然而，我們發現在Yoon-Yoo與Zhu-Wu.等人之方法中，其傳送者與信賴驗證中心的運算量會隨著網格計算中之節點或群組成員之增加而明顯的增加。 除此之外，每次執行群組的金鑰協定都必須依賴驗證中心的參與而產生，因此，很容意增加驗證中心在計算方面與傳送時之負擔，如此一來，對日益成長的資訊服務，會使得效能易受影響而導致瓶頸。因此，為了克服因計算量及傳輸量所導致的瓶頸，本研究設計一個高效能且具安全的網格計算之通訊環境，除了保護資料在傳輸的過程中免於遭受它人的存取或修改外，所提之技術中，其傳送端與接收端的計算量，隨著群組成員

的數量增加並沒有明顯的差異，且執行群組的金鑰協定不須要依賴驗證中心的參與產生，將可減低驗證中心的負擔，因此，更能提升資訊服務的品質，並提供更好效能且安全的資源共享與合作分工的服務環境。

2. 相關研究的探討

由於目前網格計算(Grid Computing)的群組通訊安全協定中以 Yoon-Yoo [14]之方法較為安全，所以在提出本設計之前，以下先簡單介紹 Yoon-Yoo 之方法，其方法分為起始階段、訊息的廣播階段、與解密階段。

Yoon-Yoo 之方法主要是植基 RSA 密碼系統，在起始階段，信賴驗證中心(central authority system 簡稱 CAS)負責產生各個結點或使用者之參數與私鑰，CAS 先選擇兩個很大的質數 p 與 q 且令 $N=p\times q$，接著選擇一對數(e,d), 使得 $e\times d=1 \bmod \phi(N)$ [16],並選擇一加密函數 $f(x)=x^d \bmod \phi(N)$。如此一來, e及 N 即為CAS的公開金鑰,而 d 為CAS秘密金鑰; 同時地, p 與 q 亦是秘密參數，然後 CAS 選擇一個公開之單向雜湊函數 $h(\,)$。

假設目前參與群組有 n 個人為$U_1,U_2,...,U_n$，首先信任驗證中心 CAS 選擇私密參數K_0，r_c 與t_i，而 $i=1,2,...,n$。接著由信任驗證中心 CAS 產生 n 把私密金鑰，$K_i=K_0^{t_i}$，並透過安全通道配送K_i給使用者 U_i，而 $i=1,2,...,n$。另一方面，並公開 $P_i=t_i^{-1}r_c \bmod \phi(N)$，$i=1,2,...,n$。接著介紹 Yoon-Yoo 方法之訊息廣播階段與解密階段:

訊息廣播階段:

假設目前傳送者U_1欲將重要訊息傳送至網格計算(Grid Computing)中之某一群組$G=\{U_i\}_{i=1}^{a}, a\le n$, 以下為所執行之步驟:

1. U_1 先將目前之群組$G=\{U_i\}_{i=1}^{a}$傳於 CAS。
2. CAS 選擇一數 Z，並計算 $Z_i=E_{K_i}(Z)$ 而 $i=1,2,...,a$，$B=t_1t_2...t_a \bmod N$，$f(B)=B^d \bmod \phi(N)$，以及 $Y=h(z,f(B))$。然後，CAS 將 $Z_i=E_{K_i}(Z)$ 而 $i=1,2,...,a$，與 $f(B), Y$ 廣播於群組$G=\{U_i\}_{i=1}^{a}$中。
3. 當收到訊息後，U_1利用其私鑰K_1解開$Z=E_{K_1}(Z_1)$，並驗證$Y=h(z,f(B))$是否成立，若成立則接受其為合法之 CAS; 否則停止這次協定。
4. 接著U_1計算這次群組通訊之共同私鑰

$sk=K_1^{Z(f(B)P_1)e} \bmod N=K_1^{Z(Bt_1^{-1}r_c)ed} \bmod N=K_0^{ZBr_c} \bmod N$，並利用 sk 將重要資料 M 加密為密文$C=E_{sk}(M)$，並計算$V=h(sk,M)$，然後，將 C 與 V 廣播於群組$G=\{U_i\}_{i=2}^{a}$中。

解密階段:

當這次合法群組$G=\{U_i\}_{i=2}^{a}$收到U_1之訊息 C 與 V 後，則解密步驟說明於下:

1. 首先群組成員$G=\{U_i\}_{i=2}^{a}$由其私鑰K_i解開 $Z=D_{K_i}(Z_i)$，而$i=2,3,...a$，並驗證$Y=h(z,f(B))$是否成立，若成立則接受其為合法之 CAS; 否則停止這次解密階段。
2. 接著U_i，$i=2,3,...a$，計算這次群組通訊之共同私鑰

$sk=K_i^{Z(f(B)P_i)e} \bmod N=K_i^{Z(Bt_i^{-1}r_c)ed} \bmod N=K_0^{ZBr_c} \bmod N$，並利用 sk 將重要資料解密為$M=E_{sk}(C)$，並驗證$V=h(sk,M)$是否成立，若成立，則接受 M 為其合法者U_1所廣播之資訊; 否則停止這次解密階段。

而網格計算(Grid Computing)中之群組$G=\{U_i\}_{i=1}^{a}, a\le n$，可利用此共同私鑰 sk 來傳送重要資源與協同分工運算後之結果。

由上述 Yoon-Yoo [14] 兩人所提方法可知，當群組$G=\{U_i\}_{i=1}^{a}, a\le n$共有 a 位時，對傳送者U_1而言,須要執行一個指數運算、二次對稱式加密與二個雜湊函數運算，而對每位接收者而言,也須要執行一個指數運算、二次對稱式加密與二個雜湊函數運算，另一方面，信任驗證中心 CAS 仍須執行一個指數運算、a 次對稱式加密與一個雜湊函數運算。雖然 Yoon-Yoo 兩人所提方法比之前其它學者所提方法更具安全性，但是，其 CAS 的運算量會隨著網格計算中之群組成員之數量增加而明顯的增加。除此之外，每次執行群組的金鑰協定都必須透過驗證中心 CAS 的參與而產生,很容意增加 CAS 在計算方面與傳送時之負擔,對日益成長的資訊服務，會使效能易受影響而導致瓶頸。

3. 研究方法

由於日益成長的計算服務，資源分享已愈來愈普及化，網格運算（Grid Computing）有可能成為下一代的資訊基礎建設，又目前大部份之研究，在執行群組的金鑰協定都必須透過驗證中心 CAS，因此，本研究提出一個具低運算量與傳輸量的群組通訊安全於網格計算(Grid Computing)應用服務之協定。

為了降低各方面的傳輸量與計算量，以及提供更有效率之資訊服務與共享的平台，因此，本研究採二次剩餘(Quadratic Residue，簡稱 QR)的密碼系統方式，因為 QR 的加解密方式很明瞭簡單,其安全是建立在因數分解之難題上[15], 與 RSA 金鑰系統的安全性是一樣的[13]。在提出本研究之前，以下我們先簡單描述二次剩餘(QR)密碼系統之性質。$n\in N$，若一整數 a 且 $\gcd(a,n)=1$，滿足$x^2=a(\bmod n)$有解，則稱 a 為模 n 之二次剩餘((Quadratic Residue a modulo n)QR)，否則稱 a 為模 n 之非二次剩餘(Quadratic Nonresidue of n)。而滿足$x^2=a(\bmod n)$之解 x，則稱為模 n 之二次剩餘的根(modular square roots of quadratic residue a modulo n)。二次剩餘(QR)密碼系統之性質有下列之性質[15], [16]。

(1) 當 $p=3(\bmod 4)$ 且 a 為模 p 之二次剩餘($x^2=a(\bmod p)$,則有兩個模 p 之二次剩餘的根為 $r_{1,2}=\pm a^{\frac{p+1}{4}}(\bmod p)$，使得 $(r_{1,2})^2=a(\bmod p)$。

(2) $n = p \times q$ 且 $\gcd(a,n)=1$，a 為模 n 之二次剩餘（$x^2 = a(\bmod n)$），其中 p 和 q 為兩個質數，當 $p = q = 3(\bmod 4)$，則有四個模 n 之二次剩餘的根為 $r_{1,2,3,4}$，使得 $(r_{1,2,3,4})^2 = a(\bmod n)$，而 $r_{1,2} = \alpha \cdot q \cdot q^* \pm \beta \cdot p \cdot p^* (\bmod n)$，$r_{3,4} = -\alpha \cdot q \cdot q^* \pm \beta \cdot p \cdot p^* (\bmod n)$，其中 $\alpha = a^{\frac{p+1}{4}} (\bmod p)$，$\beta = a^{\frac{q+1}{4}} (\bmod q)$，$p^* = p^{-1} (\bmod q)$，且 $q^* = q^{-1} (\bmod p)$。

上述之性質(2)，若 p 和 q 兩個質數已知時，則 $x^2 = a(\bmod n)$ 之四個根均可在多項式時間內求出[15]，但 p 和 q 兩個質數未知時，要求出 $x^2 = a(\bmod n)$ 之四個根，則須先將 n 因數分解，在此情形下與 RSA 金鑰系統的安全性是一樣，都是建立在因數分解之難題上[15]。底下將針對所要設計的網格計算之安全通訊協定，分別說明其過程步驟。

在本協定剛開始階段，假設目前參與群組有 n 個人為 $U_1, U_2, ..., U_n$，首先信任驗證中心(central authority system 簡稱 CAS)挑選一個對稱式加解密系統如 AES 或 DES [15]，而 $E_K(.)$ 和 $D_K(.)$ 分別表示當秘密金匙 K 時之加密和解密之意義，然後，選擇一個公開之單向雜湊函數 $h(\,)$，CAS 接著計算並公開 $h(ID_i, x)$，而 $i = 1,2,...n$，其中 ID_i 為使用者 U_i 的辨識碼，x 為 CAS 之秘密私鑰。另一方面，每位 U_i 先選擇兩個很大的質數 p_i 與 q_i 且令 $N_i = p_i \times q_i$，其中 $p_i = q_i = 3(\bmod 4)$ 且 p_i, q_i 均為兩個很大的質數，接著選擇一對數 (e_i, d_i)，使得 $e_i \times d_i = 1 \bmod \phi(N_i)$，而 (N_i, e_i) 即為每位 U_i 之公鑰，d_i 為 U_i 之密鑰且 p_i 與 q_i 亦是 U_i 的秘密參數。接著介紹本研究中之訊息廣播階段與解密階段的步驟於下:

訊息廣播階段:

假設目前傳送端 U_1 欲將重要訊息 M 傳送至網格計算(Grid Computing)中之一某群組成員 $G = \{U_i\}_{i=1}^{a}, a \le n$，以下為所執行之步驟:

1. U_1 先選擇這次群組通訊之共同私鑰 sk。
2. U_1 計算 $C = E_{sk}(M)$，$S = (h(M))^{d_1} \bmod N_1$，與 $Z_i = (h(ID_i, x) \| sk)^2 \bmod N_i$，而 $i = 2,3,...,a$。
3. U_1 將 C，S，與 $Z_i = (h(ID_i, x) \| sk)^2 \bmod N_i$，$i = 2,3,...,a$，廣播於群組 $G = \{U_i\}_{i=2}^{a}$ 中。

解密階段:

當這次合法群組 $G = \{U_i\}_{i=2}^{a}$ 收到 U_1 之訊息 C，S，與 $Z_i = (h(ID_i, x) \| sk)^2 \bmod N_i$，$i = 2,3,...,a$，則解密步驟說明於下:

1. 首先 U_i，$i = 2,3,...a$，計算這次群組通訊之共同私鑰 sk，U_i 計算並取出滿足 $Z_i = (h(ID_i, x) \| sk)^2 \bmod N_i$ 之四個模 N_i 之二次剩餘的根為 $r_{1,2,3,4}$ 使得 $(r_{1,2,3,4})^2 = (h(ID_i, x) \| sk)^2 \bmod N_i$，並從四個根 $r_{1,2,3,4}$ 中挑出附有 $h(ID_i, x)$ 為開頭之私鑰出 $sk = r_{1,2,3,4} \oplus h(ID_i)$。
2. 接收者 U_i，$i = 2,3,...a$，利用 sk 將重要資料解密為 $M = D_{sk}(C)$，並驗證 $h(M) = S^{e_1} \bmod N_1$ 是否成立，若成立，則接受 M 為其合法傳送端 U_1 所廣播之資訊; 否則停止這次解密階段。

而網格計算(Grid Computing)服務中之群組 $G = \{U_i\}_{i=1}^{a}, a \le n$，可利用此共同私鑰 sk 來傳送重要資源與協同分工運算後之結果。由上述之訊息廣播階段與解密階段，可明顯看出協定機制中，目前授權合法之群組 $G = \{U_i\}_{i=1}^{a}, a \le n$ 通訊成員之數量 a，可以動態的加入或刪除成員，並不影響其它成員原本之參數與系統之通訊安全。

4 方法之討論與分析

由上一節所提之研究方法可知，系統協定的程序很簡單，可提高實際的應用價值，並提供安全與便利之網格運算環境的服務。基於安全考量，為了避免重送攻擊(replay attack)與每次網格運算環境的資訊安全，以上之群組通訊之私鑰 sk，都不可以重覆使用，以免導致資訊被不同之群組所竊取或修改。本研究採二次剩餘(簡稱 QR)的密碼系統，當使用者 U_1 先選擇這次群組通訊之共同私 sk，並計算 $C = E_{sk}(M)$，$S = (h(M))^{d_1} \bmod N_1$，與 $Z_i = (h(ID_i, x) \| sk)^2 \bmod N_i$ 並將其廣播於 $G = \{U_i\}_{i=2}^{a}$ 時，所以當群組 $G = \{U_i\}_{i=1}^{a}, a \le n$ 的私鑰 sk 被求出時，則網格運算環境的訊息隱私就被得知，這時就不具有使用者安全了，然而，由已知 $Z_i = (h(ID_i, x) \| sk)^2 \bmod N_i$ 要得到 sk 是很困難的，其安全是建立在因數分解 $N_i = p_i \times q_i$ 之難題上，與 RSA 金鑰系統[13]的安全特性是一樣，因此，本協定可提供網格運算中群組通訊之安全。除此之外還具備下列的安全性質:

1. 由於使用者可因目前之需求而決定網格運算之成員，而每次各個群組通訊之私鑰 sk 也不同，因此，機制中群組之成員可以動態的加入或刪除，不須更改原本成員之參數。
2. 信任中心 CAS 只須公開網格環境中，目前合法使用者之相關參數(包含新加入之新成員與被刪除之成員)，不須參與各個群組之私鑰產生。所以 CAS 無法得知各個群組之私鑰，因此，更可提高網格環境中群組通訊之安全。
3. 具 forward security 和 backward security 的安全性: 即使使用者的某回合私鑰 sk 被得知，因每次的 sk 都由傳送端任選且不重覆，又被保護於 $Z_i = (h(ID_i, x) \| sk)^2 \bmod N_i$，因此，惡意者很難得知使用者過去與未來之回合私鑰。所以本研究擁有 forward security 和 backward security 安全性。

另一方面，我們所提出之方法中,傳輸量方面只須一次(one round) 的傳輸次數, 比先前 Yoon-Yoo 學者的三次回合較少[14]。在計算量上，本研究將採二次剩餘(Quadratic Residue，簡稱 QR)的密碼系統方式，且系統在開始階段，信任中心 CAS 已計算並公開 $h(ID_i, x)$ 之值

且 $i=1,2,3,...n$，所以當群組 $G=\{U_i\}_{i=1}^{a}, a \le n$ 有 a 個使用者時，在傳送端的計算量只須一次高次的指數運算、一次對稱式加密運算、一個雜湊函數運算、與 a 次的乘法運算；而對每位接收者而言，只須一次二次剩餘根的計算、一次高次的指數運算、一次對稱式解密運算與一個雜湊函數運算；而信任中心 CAS 無須任何之計算，因此，本研究之方法其運算速度方面比 Yoon-Yoo 學者之方法更加快速，相對也減少很多傳輸量，所以可提高整體之計算速度，更能提供高效能的資訊服務品質且更適合於網格運算之環境。

有關計算效能方面我們與目前較安全的 Yoon-Yoo 之方法作比較，如下表(一)之敘述:其中 E 表示模之指數運算，h 為雜湊函數運算，Mul 為模之乘法運算，r 為二次剩餘根的計算，而 S 為對稱式加解密運算，又 XOR 計算在此省略不計。由表(一)可得知無論在傳送端 U_1、接收者(群組成員)、以及信任中心 CAS 方面，我們所提之方法都比 Yoon-Yoo 方法快速。雖然 Yoon-Yoo 兩人所提方法比之前其它學者所提方法更具安全性，但是，Yoon-Yoo 方法中 CAS 的運算量都須要 a 次對稱式加解密，其運算量會隨著網格計算中之群組成員之增加而明顯的增加。除此之外，Yoon-Yoo 方法每次執行群組的金鑰協定都必須透過驗證中心 CAS 的參與而產生，因此，很容意增加 CAS 在計算方面與傳送時之負擔，如此一來，對日益成長的資訊服務，會使得效能易受影響而導致瓶頸。

在我們所提之方法中，信任中心 CAS 無須任何之計算，雖然傳送者仍須 a 次的乘法運算，但是 a 次的乘法運算，隨著成員數量的增加比較沒有明顯的差異了。因此，由上述的安全分析與效能分析，本研究可以大幅改善傳送者和信任中心 CAS 的計算量，更適用於網格運算的環境，除此之外，CAS 亦無法得知群組 $G=\{U_i\}_{i=1}^{a}, a \le n$ 之回合私鑰 sk。透過本協定使用者可在任何時間、任何地點，藉由此安全通訊來達成存取與分享資源之理念，並提供安全與高效能的運算平台，進而加速各項重要研究之進行。

表(一)

成員有 a 位時	群組之成員	傳送者 U_1	信任中心 CAS
Yoon-Yoo 方法	$1E+2S+2h$	$1E+2S+2h$	$1E+aS+1h$
所提之本方法	$1E+1S+1h+1r$	$1E+1S+1h+aMul$	0

5 結論

基於二次剩餘(簡稱 QR)的密碼系統，本研究提出一個具低運算量與傳輸量的通訊安全於網格計算(Grid Computing)應用服務之協定， 除了保護資料在傳輸的過程中免於遭受它人的存取或修改以外，所提之技術其傳送端與接收端的計算量，隨著群組成員的數量增加並沒有明顯的差異。而機制中群組之成員可以動態的加入或刪除，不須更改原本成員之參數，且執行群組的金鑰協定時，不須要依賴驗證中 CAS 的參與而產生，將可減低 CAS 的負擔。

參考文獻

[1] W. Chung, R. Chang, "A new mechanism for resource monitoring in grid computing", *Future Generation Computer Systems*, Vol. 25, No. 1, 2009, pp. 1–7.

[2] M. Smith, M. Schmidt, N. Fallenbeck, T. Dornemann, C. Schridde, B. Freisleben, "Secure on-demand grid computing", *Future Generation Computer Systems* Vol.25, No. 3, 2009, pp. 315–325.

[3] J. Masque, A. Peinado, Cryptanalysis of improved Liaw's broadcasting cryptosystem, *Journal of Information Science and Engineering*, Vol. 22, 2006, pp. 391–399.

[4] X. Zou, Y. Dai, X. Ran, "Dual-level key management for secure grid communication in dynamic and hierarchical groups", *Future Generation Computer Systems*, Vol. 23, No. 6, 2007, 7pp. 76–786.

[5] D. Zou, W. Zheng, J. Long, H. Jin, X. Chen, "Constructing trusted virtual execution environment in P2P grids", *Future Generation Computer Systems*, Vol. 26, No.5, 2010, pp. 769–775.

[6] F. Martinelli, P. Mori, "On usage control for GRID systems", *Future Generation Computer Systems*, Vol. 26, No. 7, 2010, pp. 1032–1042.

[7] J. Perez, J. Bernabe, J. Calero, F. Clemente, G. Perez, A. Skarmeta, "Semantic-based authorization architecture for grid", *Future Generation Computer Systems*, Vol. 27, No.1, 2011, pp. 40–55.

[8] C. Chang, T. Wu, "Broadcasting cryptosystem in computer networks using interpolating polynomials", *Computer Systems Science and Engineering*, Vol. 6, No. 3, 1991, pp.85–188.

[9] G. Chiou, W. Chen, "Secure broadcasting using the secure lock", *IEEE Transactions on Software Engineering*, Vol. 15, No.8, 1989, pp. 929–934.

[10] H. Liaw, "Broadcasting cryptosystem in computer networks", *Computers & Mathematics with Applications*, Vol. 37, 1999, pp. 85–87.

[11] Y. Tseng, J. Jan, "Cryptanalysis of Liaw's broadcasting cryptosystem", *Computers & Mathematics with Applications*, Vol. 41, 2001, pp.1575–1578.

[12] M. Ramkumar, "Broadcast authentication with preferred verifiers", *International Journal of Network Security*, Vol. 4, No.2, 2007, pp. 166–178.

[13] R.L. Rivest, A. Shamir and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM*, Vol. 21, 1978, pp. 120-126.

[14] E. J. Yoon, K. Y. Yoo, "A secure broadcasting cryptosystem and its application to grid computing", *Future Generation Computer System*, Vol. 27, 2011, pp. 620-626

[15] S. S. Yan, "Number Theory for Computing", Berlin, Germany, 2000.

[16] W. Zhu, C. Wu, "Security of the redefined Liaw's broadcasting cryptosystem", *Computers & Mathematics with Applications*, Vol.56, 2008, pp. 1665–1667.

[17] K. Huang, D. Zhang, "DHT-based lightweight broadcast algorithms in large scale computing infrastructures", *Future Generation Computer Systems*, Vol.26, No. 3, 2010, pp. 291–303.。

鑑識會計應用於政府審計之初探

林宜隆[1]　林愫麗[2]
[1]元培科技大學資管系暨數位創新管理研究所
[2]國立宜蘭大學多媒體網路數位學習碩專班
cyberpaul747@gmail.com ; n0143028@ms.niu.edu.tw

摘要

目前鑑識會計在我國尚處於起步階段，鑑於社會變遷及資訊科技迅速發展，商業環境越來越複雜，舞弊的手法更是推陳出新，影響層面日漸廣泛，鑑識會計除可為舞弊之查核外，亦可為建立制度、加強公司治理，達到興利防弊之效果，與審計機關職司財務司法之功能相仿。

近年來，審計機關的內部研究，多以鑑識會計在分析案情及調查時所使用的觀念，應用在審計工作上，幫助查核人員確認查核目標後，快速的建立查核方向和重點，而本研究蒐集相關鑑識會計文獻加以探討，鑑識會計與政府審計工作流程相似，均包括證據的蒐集、分析及評估[1]，據以即時還原事件真相。除了將上述鑑識會計的觀念導入政府審計外，更進一步探討，政府職能擴張後，審計機關人少事繁責重，在投入成本受限之情況下，善用 E 化稽核工具為數位證據分析，快速挖掘不法案件，並經由實際案例應用分析，驗證導入鑑識會計，運用於政府審計工作上，有助於提升審計機關偵測及調查舞弊的能力，亦可協助建立制度、強化治理能量。

關鍵詞：鑑識會計、數位據證、政府審計

Abstract

Nowadays, business environment has become more and more complex; meanwhile, with fast-developing information technology, fraud also advances from day to day. In order to detect fraud, forensic accounting has emerged as one of the most effective approaches in the past decade. In recent years, the audit authority's internal research, mostly forensic accounting investigations in the analysis of the case and the concepts used, the application of the audit work, audit objectives to help inspectors confirmed after checking quickly establish direction and focus. This study collected literatures regarding forensic accounting and explored it. Forensic accounting procedures involve collecting, analyzing and evaluating evidential matter, which is similar to government auditing. In Taiwan, due to limited budget and workforce shortage, forensic accounting is considered as beneficial to integration into the audit authority, which can advanced investigation skills and discover fraud. The audit authority can improve abilities of detecting and investigating fraud by applying forensic accounting in aspects of government in Taiwan. Moreover, it can help government establish internal control system and enhance governance.

Keywords:Forensic Accounting、Digital Evidence、Government Auditing。

1. 前言

近年來，國際經濟犯罪事件頻傳，其金額越加龐巨、影響層面廣泛，如美國安隆事件，促成沙賓法案(Sarbanes Oxley Act)的制定，及鑑識會計的崛起，而在我國審計學術及實務上鮮少討論鑑識會計，95 年間行政院為因應總統所宣示之「有效開放積極管理」政策，研擬引進鑑識會計(Forensic Accounting)制度，期望藉由委託專業機構，赴大陸查核投資廠商的財務情況，達到監督管理之效。鑑識會計除可為舞弊之查核外，亦可為建立制度、加強公司治理，達到興利防弊之效果。

政府職能擴張後，政府審計業務量由 93 年度每一審計人員平均監督預算金額 190.03 億元，增加至 101 年度每一審計人員平均監督預算金額 280.20 億元，審計機關行使審計職權，在審計人力有限的情況下，如何善盡職責，扮演監督、洞察、前瞻之角色，審計機關職司財務司法，其功能與鑑識會計相仿，工作流程亦相似，包含規劃階段、蒐集證據、分析及評估、撰寫報告，如能導入鑑識會計於政府審計工作，有助於提升審計機關偵測及調查舞弊的能力，亦可協助建立制度、強化治理能量。

2. 鑑識會計與執行程序

2.1 鑑識會計

2.1.1 鑑識會計之定義

最早出現「鑑識會計(forensic accounting)」一詞，係美國學者皮洛貝(Maurice Peloubet)於 1946 年的 Journal of Accountancy 中，第一次用鑑識會計來敘述會計人員所提供的法律支援服務。其後在 1948 年美國學者班寧頓（Lee Pennington）在「調查性會計」一文中指出，美國政府在二次大戰期間 FBI 已有近 500 名的會計探員（Special Agent Accountant），當時的主要活動為監督軸心國在美國境內的融資與經濟活動，這是首次以「調查性會計」一詞描述會計人員所從事的有關調查舞弊之活動。近年研究者皆以會計人員對法庭提供之支援性

或調查性等服務工作，稱之為「鑑識會計」，以下茲略述主要機構或學者對其定義：

■ 美國會計師協會(AICPA)的定義

鑑識會計是應用會計原則、會計理論、會計訓練等各種會計知識到一法律紛爭上之事實問題及假設問題。鑑識會計包含運用會計、審計、財務金融、計量方法以及一些法律與研究之特殊技術及調查技巧，以收集、分析、並且評估可做為證據之事項，並解釋及傳達其發現，以供法院在斷案之依據。

■ Bologna and Lindquist 的定義

鑑識會計是一項在證據法（Rules of evidence）的範圍內，將財務會計上的知識以及調查性之心態應用到未解決之議題上。以一門學科而言，它結合了財務專業、舞弊學識、對企業現實環境的深切了解，以及法律系統的運作。

在會計專業中，鑑識一詞乃指運用財務上的專業知識來進行財務調查，法律上的問題與爭議以及在衝突上尋求可能的解決方案。鑑識會計即是在為法庭或其他與法律有關之目的下，所執行的會計專業工作，故鑑識會計涉及了適用於法庭中之證據的蒐集、提供會計上的分析等工作，以協助討論以及協商，並達成最終的爭議的解決方案。

綜合言之，可以定義鑑識會計是一項結合了會計、審計、調查能力，以及在法律訴訟的應用所衍生的專業。[2]

2.1.2 鑑識會計的功能

鑑識會計依據前述之定義，其主要功能包括兩大領域：

■ 調查性會計（investigative accounting）

鑑識會計人員通常會涉及非常廣泛的調查活動。調查性會計通常都與犯罪的調查相關。在調查性會計中，鑑識會計人員著重的重心，在於針對犯罪動機、機會或其可獲取之利益等蒐集相關證據。一般而言，社會大眾對調查性會計運用的場合，多聯想到白領階級的商業犯罪（white-collar crime，WCC）。包括了基層員工可能涉及的員工偷竊（embezzlements）或詐欺事件，例如將收到之現金款項予以挪用、偷竊公司之資產等行為；高階經理人員可能涉及的犯罪行為，主要為財務報表詐欺等。

鑑識會計在其發展的初期，在偵查舞弊上多屬被動（reactive）的型態。在舞弊的偵查過程中，首先由舞弊檢查人員（fraud examiners）或者舞弊查核人員（fraud auditors）主動偵查可能的舞弊。在上述人員發現舞弊之證據後，再由鑑識會計人員來進行後續的工作。另外，鑑識會計為會計專業人員所提供的服務；而舞弊調查則僅針對舞弊事件進行調查，且執行者也不一定必須非為會計專業人員不可[2]。然隨著鑑識會計近年來的發展，其所能提供的服務涵蓋的範圍也越來越廣。鑑識會計在偵查舞弊上的角色，從原先的被動型態轉變為也包括了主動的偵查舞弊之功能[3]。亦即就今日的鑑識會計的內容與型態而言，已經包括了所謂的舞弊偵查。

■ 訴訟支援（litigation support）

AICPA 認為，所謂的訴訟支援就是「任何非律師者在訴訟過程中，對律師所提供之專業協助」。訴訟支援主要是鑑識會計人員作為調查案件中，在法律之爭議或者是財務補償之要求等議題中，提供其專家之意見。在訴訟中，鑑識會計人員檢視個人或公司之帳冊以及相關紀錄等，以協助律師準備其手中之案件。

鑑識會計人員最常遇到的情況，就是對經濟損失之量化與分析。最典型的訴訟支援之委任，就是計算由於違反契約所造成之財務損失。其中可能必須衡量收益與利潤之損失，同時也有可能需要對企業之財產或業主權益等進行評價。在訴訟支援中使用鑑識會計的範圍可以十分廣泛，雖然一般都認為只有在進入審判的階段才會使用到鑑識會計，但事實上鑑識會計也可應用在審判前之支援，例如撰寫報告、確立因果關係、蒐集真相、翻譯術語等。同時，雇用鑑識會計人員者，有可能是在法庭中的任何一方，甚至包括法庭本身（如法官）。

此外，鑑識會計在訴訟支援中，另外一項十分重要的功能，即擔任專家證人（expert witness）。一般的情況下，證人是不允許在作證的過程中陳述其意見、或者是結論等。亦即，證人僅能就其感官知覺（視覺、聽覺、觸覺、嗅覺、味覺等），以及他們所知道的事實進行陳述。但若是一個在其專精之領域或學科上符合一定資格之專家，則可以對其所擁有專業知識之領域的範圍內，給予專家之意見。[2]

2.2 鑑識會計工作流程

通常鑑識會計人員從事舞弊(犯罪)鑑識的作業流程與方式如下[4]：

- 工作規劃及問題發現：查核工作有賴完善之事前規劃，以及先行就已取得的資料加以分析、研判，以求凡事能事半功倍。
- 分析性程序：鑑識人員需用分析性程序，以取得一家企業財務資料中異常變化的蛛絲馬跡，如：趨勢分析、比率分析及模型建構等。
- 與相關人員面談：面談也是查核的一項非常重要的活動，多數時候鑑識會計人員需由人員的面談中，找出矛盾或不合理的問題點。
- 撰寫舞弊(犯罪)調查報告：撰寫報告為鑑識會計工作的產出，其中論據皆須有證據，如此才能供法院之引用，作為判案之依據。

2.2.1 鑑識會計證據的特點

另外就一般經驗言，鑑識會計證據的特點如下：[4]

- 通常與財務、會計事項有關，如會計憑證、會計帳簿、會計報告。
- 形成於經濟活動的運算過程。

- 是以價值量化方式反映經濟活動的全貌。
- 同時具有書證與物證的意義。
- 具有較強的機密性，如：股東往來交易、商業機密或特別協議等，故鑑識人員需保密。

2.2.2 數位化鑑識會計執行步驟

數位鑑識(digital forensics)技術是關於如何在電腦內找到可供法庭上確認待證事實之證據資料；亦即是將電腦內的相關數位資料加以保存、識別、擷取以及文件化之過程。其目的在於如何於蒐證過程中，確保數位證據(digital evidence)之「不可否認性」與「完整性」，使數位證據具有絕對證據能力，而能成為呈堂證據。[5]

數位化鑑識會計主要的步驟，分為電子蒐證(e-Discovery)及數位證據分析。

- 電子蒐證(e-Discovery)：美國在 2006 年 11 月修法通過電子蒐證法，對「電子儲存資訊」(Electronically Stored Information；ESI) 定義了法律認定的相關發現程序和原則，簡化蒐證程序的要求。企業有責任保存與訴訟案件相關的證據，包含電子媒體中所有儲存的資料及紀錄。利用適宜的電子蒐證工具與技術，可精確地將證據複製留存，減少工作量與審查的成本，更能有效管理電子資料及紀錄。
- 數位證據的分析：鑑識會計的分析過程，比一般的電腦鑑識過程要來的複雜，因此鑑識人員需利用電腦輔助稽核技術(Computer Assisted Audit Techniques；CAATs)進行資料的分析，其分析程序中，須先設定查核分析目標後，決定可用的數位證據，擷取所需的資料後，並選擇有效的分析方法，進行數位證據的分析。[6]

2.3 數位證據

2.3.1 數位證據之定義

「數位證據」依據 Digital Evidence and Computer Crime 一書中定義為電腦及網路儲存媒體中，任何足以證明犯罪構成要件或關聯的電子數位資料，為物理證據的一種，包括有文字、圖片、聲音、影像等形態，具有可無限無差異性複製、原始作者不易確定、資料完整性不易驗證等性質，亦稱電腦證據。[2]

2.3.2 數位證據的特點

數位證據與傳統證據比較有下述特點：[7]

- 科技性：數位證據的搜集與審查，需要一定的科學技術、甚至是較尖端的技術，且伴隨科技的發展不斷的更新、變化。
- 易變性：數位證據因為儲存媒體多採電磁運作，故操作人員的差錯或供電系統和網路的故障等情況發生時，數位證據均有可能被輕易地盜取、修改勝甚至全盤毀滅而不留下任何證據。
- 無形性：進行電子交易的過程中，一切資訊都由經過編碼的電子訊號傳遞，這些電子訊號都是看不見的，因此數位證據也具有這種無形性的特點。

2.3.3 數位證據之分類

由上述定義與特點，可以將數位證據分類如下：(見表 1) [7]

表 1：數位證據分類

分類	屬性一	屬性二	例證	類比傳統書證
可列印	可閱讀		文字檔(Word 檔、LOGO 檔)	文字證據
	不可閱讀	可執行	執行檔(EXE 檔、COM 檔)	物證
		不可執行	應用程式擴充(DLL 檔、目的檔)	其他證據
不可列印	可執行		音樂檔、聲音檔	物證
	不可執行		加密檔、壓縮檔	其他證據

3.政府審計

3.1 政府審計之定義

政府審計係由國家設立獨立的審計機關，以有系統的方法，審核政府財務收支及決算、考核財務效能及核定財務責任對各機關財務上之違失或不當，及效能過低之情事，應依法為適當之處理，暨提供建議改善意見審計結果，應向國會提出報告，以提升及促進政府公共責任 (accountability) 之履行。

3.2 政府審計之功能

我國憲法第 59 條規定，行政院於會計年度開始 3 個月前，應將下年度預算案提出於立法院。第 63 條規定，立法院有議決預算案之權。第 60 條規定，行政院於會計年度結束後 4 個月內，應提出決算於監察院。又第 105 條規定，審計長應於行政院提出決算後 3 個月內，依法完成其審核，並提出審核報告於立法院。預算執行結果之考核，即決算之審核，由監察院審計長司理，屬財務司法。

審計為良好公部門治理架構之關鍵因素，可協助監督(over sight)、洞察(insight)及前瞻(foresight)

之治理角色。監督者角色包括打擊貪腐、促進行政機關之透明與確保課責機制之建立；洞察者角色則係針對查核施政計畫之經濟、效率及效果性，進而提出對行政管理之改進意見；前瞻者角色則聚焦未來的挑戰，如人口結構變化、經濟條件改變或安全之威脅，並從快速變遷之科技、複雜的社會及經濟環境中，確認風險及機會之所在。審計機關扮演監督之角色係其存在之基礎，惟發展愈趨成熟之審計機關，多朝向以洞察及前瞻角色為重，督促各機關提升施政績效，並協助其風險管理。

綜上，經依據憲法及審計法等相關規定，以及政府良善治理觀點，歸納我國政府審計三大核心功能如下：

（一）監督功能：

1. 審核財務收支及審定決算，提高財務資訊公信力及促進透明度

財務審計主要包括：查核分配預算、審核財務收支、隨時稽察採購案件、審定年度決算等，並於政府總決算提出後 3 個月內完成其審核，編造最終審定數額表，提出審核報告於立法院或議會，以為民意機關監督行政機關善盡責任與否之依據。

2. 稽察機關人員財務（物）上之違失，匡正財務紀律及致力於反貪腐

依據審計法第 17 條至第 19 條規定，審計人員發覺各機關人員有財務上不法或不忠於職務上之行為，應報告該管審計機關，通知各該機關長官處分之，並得由審計機關報請監察院依法處理；其涉及刑事者，應移送司法機關辦理，並報告於監察院。受通知處分之機關長官，不為緊急處分時，應連帶負責。如應負責者為機關長官時，審計機關應通知其上級機關執行處分。

3. 審查決定機關人員財務上行為應負之責任，落實課責機制

我國政府課責機制之設計，審計機關被賦予審查決定機關人員財務行為應負之責任，包括：審核各機關經管現金、票據、證券、財物之遺失、毀損或其他資產之損失，並決定損失責任；決定各機關違背預算或有關法令之不當支出之剔除、繳還、賠償責任；對於主管人員未盡善良管理財務（物）之責任、會計人員簽證支出有故意或過失或記錄不實、出納人員誤付款項等，而使公款或公有財物受到損失者，審計機關查明決定剔除、繳還、賠償責任後，各該機關長官應限期追繳，並通知公庫、公有營業或公有事業主管機關；逾期，該負責機關長官應即移送執行機關強制執行。

（二）洞察功能，考核財務效能，提供財務管理諮詢之服務

審計機關考核各機關之績效，如認為有制度規章缺失或設施不良者，應提出建議改善意見於各該機關；有未盡職責或效能過低者，除通知其上級機關長官外，並應報告監察院。審計機關於政府編擬年度概算前，應提供審核以前年度預算執行之有關資料及財務上增進效能與減少不經濟支出之建議意見。其功能在於藉由評估計畫政策達成與否、分享標竿性資訊，及各政府層級之橫向與縱向比較，提出對行政管理之改善建議；並提供持續性回饋資訊，協助行政機關將組織學習制度化，俾及時調整政策。審計結果除對未盡職責或效能過低案件，依法報告監察院外，並可提升個別施政計畫執行績效，啟發行政部門對類似問題之解決能力。

（三）前瞻功能，及時辨識關鍵趨勢與新興挑戰，提供預警服務前瞻功能

係指行政部門之關鍵趨勢與新興挑戰變成危機前，審計機關能及時辨識並提出預警性建議意見，分析重點轉為強調預計成果（results）及結果（outcomes），不侷限於過程（processes）與產出（outputs）。隨著政府公共服務的範疇及型態複雜且多樣化，歲入歲出規模持續擴增，我國審計相關法規雖無明文規範政府審計之前瞻者角色，惟在協助各機關辨認未來趨勢，提醒機關留意即將發生的挑戰，包括組織改造、穩健財政、金融監理、環境保護、社會福利、健保財務、經濟建設、公務人員退休制度等議題，或導入或採取新的查核方法，以發揮政府審計積極功能。

3.3 政府審計工作流程

政府審計工作流程依序為：1.確認查核目標，2.規劃查核計畫，3.執行查核工作，4.撰寫查核報告，5.繕發審核通知。

3.4 審計權之行使對象

審計權的行使對象，為中央至地方政府所屬全國各機關及有關人員。包括：

- 政府及其所屬機關
- 公私合營事業
- 受公款補助之私人團體
- 政府捐助財團法人
- 行政法人

4.鑑識會計於政府審計之案例應用

根據上述第 2 章鑑識會計流程與第 3 章政府審計流程做以下 2 個案例應用分析說明：

4.1 案例 1 之應用分析

○○會辦理「農漁民子女就學獎助學金補助計畫」，公務人員涉及重複申領多項補助、夫妻同為公教人員重複申領、或無申請資格、或與規定不符者，仍發給獎助學金等案例之應用分析如表 2 所示。

表 2：犯罪分析內容

1 犯罪時間	2005年~2006年
2 犯罪地點	臺中縣、臺中市、彰化縣、雲林縣等地
3 犯罪事實	1.公教員工兼領子女教育補助費及農

(過程)	漁民子女就學獎助學金：依農漁民子女就學獎助學金申請作業要點四（四）規定，申領資格為：「未領取政府各類學雜費就學減免優待補助者」。經核中央及地方政府94及95年度各機關學校公教員工兼領子女教育補助及農漁民子女就學獎助學金者計有11,655件，金額77,354,000元。 2.夫妻同為公教人員，重複申領公教員工子女教育補助費：依「全國軍公教員工待遇支給要點」附表九「子女教育補助表」說明7規定，「夫妻同為公教人員者，其子女教育補助應自行協調由一方申領」。經核中央及地方政府94及95年度公教員工重複申領公教員工子女教育補助費者計2,343人次。 3.無申請資格或與規定不符者，仍發給獎助學金：核有就讀公立學校卻以私立學校標準發給、成績不符合申請資格、逾所得標準仍發給獎助學金、農(漁)會未登錄身分證統一編號、延畢學生仍發給就學獎助學金、未符合農漁民資格、年齡逾25歲仍發給獎助學金、就讀高中職卻以大專標準發給、申請人已死亡仍受理申請。 4. ○○會未就獎助學金資訊系統進行稽核，亦未建立資訊系統輸入控制及檢核機制。
4 犯罪者分析	政府各項獎助學金申請時雖要求申請人具結僅能申領1項補助為限，惟未建立相關控管機制，致重複領取政府各類學雜費就學減免優待補助。
5 犯罪損害	1.涉及中央及地方政府94及95年度各機關學校公教員工兼領子女教育補助及農漁民子女就學獎助學金者計有11,655件，金額77,354,000元。 2. 夫妻同為公教人員，中央及地方政府94及95年度公教員工重複申領公教員工子女教育補助費者計2,343人次。 3.無申請資格或與規定不符者，仍發給獎助學金。
6 起訴移送	刑法(貪瀆)與「全國軍公教員工待遇支給要點」附表九「子女教育補助表」說明7規定等 行政院人事行政局於民國96年10月22日召開「研商公務人員涉及重複請領子女教育補助相關行政責任如何處理」會議決議如下： 1.有關公務人員涉及重複請領子女教育補助之情事，由各機關依個案情形，從嚴認定公務人員是否構成犯罪後，再考量函送檢調單位偵辦。
	2.本案原則上由各機關政風單位負責查證事宜，惟各機關亦可基於實際需要，由機關首長指定適當單位辦理。
7 偵辦過程	見圖1

資料來源：審計部內部網站

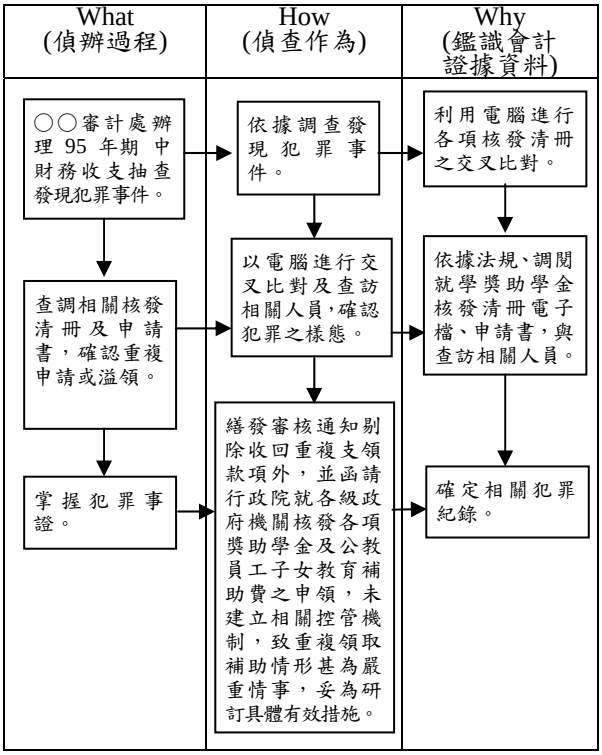


圖 1：偵辦過程

資料來源：本研究整理

4.2 案例 2 之應用分析

○○機關漏溢發退休當事人或遺族年終及三節慰問金、內控機制功能不彰等案例之應用分析如表 3 所示。

表 3：犯罪分析內容

1 犯罪時間	2007年~2012年
2 犯罪地點	台北市
3 犯罪事實(過程)	○○機關最近5年度年終慰問金暨三節慰問金之核發結果： 1.同一退休人員前後年度之年終慰問金發放金額不一。 2.已死亡之退休人員仍發給年終慰問金或發放比例有誤。 3.部分支領月退休金人員，未發給年終慰問金。 4.發放年終慰問金之退休金比例計算與規定未合。 5.已死亡或戶籍遷出國外之退休人員仍發給三節慰問金。 6.同1人重複發放三節慰問金。
4 犯罪者分析	承辦人於每年度三節及年終慰問金發放前，未能確實詳查各退休人員有無

	死亡等應注意情事，且相關發放作業，悉由承辦人員全程包辦，劃撥轉帳清冊亦由其製作，內控機制顯未落實；另各該業務主管及覆核人員均未確實審核。
5 犯罪損害	共計溢發年終慰問金250萬元、三節慰問金100萬元，計800人次；短發年終慰問金30萬元、三節慰問金10萬元，計100人次。
6 起訴移送	除承辦人員核有疏失責任外，機關相關人員亦未善盡職務上應有之注意，依審計法第17條及同法施行細則第16條規定報請監察院依法處理。嗣經監察院於○○年○○月○○日依監察法第24條提案糾正該機關之主管機關。
7 偵辦過程	見圖2

資料來源：審計部內部網站

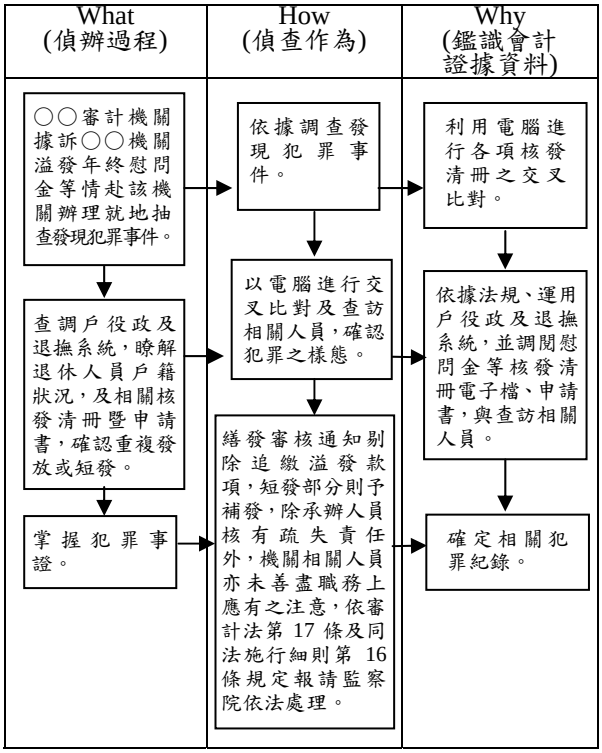


圖 2：偵辦過程

資料來源：本研究整理

5.結論與建議

5.1 結論

在本研究中將鑑識會計與電腦鑑識領域中相關專家對於鑑識會計與數位證據的定義，藉以釐清數位證據在鑑識會計領域之意義與概念，並經由案例驗證得知導入鑑識會計，善用 E 化稽核工具為數位證據分析，運用於政府審計工作上，對於跨機關資料之查核，實有相當的成效，有助於提升審計機關偵測及調查舞弊的能力，亦可協助建立制度、強化治理能量。由於舞弊手法不斷更新，並非千篇一律，亦會迴避偵測機制，如何歸納舞弊樣態，研擬標準化之作業手冊，讓舞弊無所遁形，達到預防之效，實為未來值得研究之課題。

5.2 建議

審計機關職司財務審計一職，導入鑑識會計為勢在必行之事，筆者任職於審計機關多年之經驗，提出以下建議：

(一)強化審計機關有關鑑識會計之知識與技巧：

審計機關人少事繁責重，在投入成本方面，受限於經費、人力不足及時間限制情況下，提升高風險案件之辨識，藉由例行財務收支抽查及隨時稽察等方式，導入鑑識會計強化調查技能，挖掘不法案件，提升審計人員的調查能力，以期精進審計人員掌握案情及審計證據之能力，並輔以數位證據分析，對大量交易資料(如稅捐)，進行資料萃取、比對、個化，即時還原事件真相，突破投入成本的限制，藉由職權行使，有效促進政府廉能政治。

(二)建置鑑識會計成功案例專區：

隨著雲端時代的來臨，審計機關應秉持著「創新」之核心價值，善加運用電腦輔助稽核軟體，創造審計價值。目前審計機關內部網站建置之審計知識庫，以系統化方式呈現各審計單位之查核經驗與成果，作為審計人員辦理查核業務之參考，惟尚未成立鑑識會計成功案例專區，將查核目標、範圍及證據資料，以條列式方式，建立紅旗警訊，藉由標準作業程序縮短新進人員的學習時間，激發資深人員的創新思維，供審計人員相互觀摩及交流，提高工作效率及審計成果。

參考文獻

[1] 審計部，「鑑識會計應用於政府審計之探討」，第 29 期審計人員訓練班，2007，頁 16。
[2] 林宜隆、李建裕、張志宋、楊期荔，鑑識會計數位證據鑑識標準作業程序建構之探討，雲林第 16 屆資訊管理暨實務研討會,2010。
[3] 陳紫雲、C. Pacini，談鑑識會計，會計研究月刊第 244 期，2006 年 3 月，頁 63-76。
[4] 錢緒鳴，財務舞弊與鑑識會計之研究，靜宜大學管理碩士在職專班論文，2009。
[5] 林宜隆，網路釣魚之 iPhone 數位證據鑑識標準作業程序，第 101 期，2011。
[6] 黃士銘、黃秀鳳、周玲儀，電腦稽核在舞弊查核與數位化鑑識會計的運用，會計研究月刊第 332 期，2013 年 7 月，頁 107-108。
[7] 林宜隆，數位證據標準作業程序(DESOP)之建構，電腦稽核第 16 期，2007 年 4 月。

結合邊緣特性與人類視覺系統的高藏量資訊隱藏法

冷輝世
國立彰化師範大學
lenghs@cc.ncue.edu.tw

張維剛
國立彰化師範大學
s9922119@mail.ncue.edu.tw

余奕憲
國立彰化師範大學
s9922117@mail.ncue.edu.tw

曾顯文
朝陽科技大學
hwtseng@cyut.edu.tw

摘要

數位化已是目前時代的潮流。因此，資訊安全亦受到重視。近年來許多學者從事資訊隱藏領域的研究，將機密訊息藏匿在媒介中。如何結合影像的特性以及符合人類視覺系統是一重要課題。本研究複製四份原始影像，再將這四份原始影像各別分割為 2×2 的區塊，分別使用 MED 邊緣檢測法判斷是否存在邊緣，進而以 LSB 結合 OPAP 的方式藏入機密訊息，最後再將四份藏入後的影像結合為偽裝影像。目的是儘可能在人類視覺系統可接受的影像品質下提高偽裝影像的藏量。實驗結果顯示本研究的方法不但符合邊緣特性且具有高藏量。

關鍵詞：人類視覺系統、MED 邊緣檢測法、LSB、OPAP。

Abstract

Nowadays, digitization is the current trend. Therefore, information security was paid great attention. In recent years, many researchers focus on data hiding, and how to combine the image feature under the human vision system (HVS) is an important issue.

In this study, the proposed method makes the cover image into four copies. For each copy, divide into 2-by-2 blocks, applied median edge detection (MED) to detect whether there is an edge or not, and embedding secret messages by the LSB method and the OPAP process. Finally, combine this four copies into one stego image. The aim is to enlarge payload and keep the good image quantity under the human vision system. The experimental results show that the proposed method not only keep the edge feature of cover image but also has higher payload.

Keywords: HVS, MED, LSB, OPAP.

1. 前言

數位化時代的來臨造成大量的資訊在網路間傳遞。因此，資訊安全受到重視並進而發展出資訊隱藏科學。資訊隱藏是一門新興的資訊安全科學，將機密訊息嵌入媒介中(文字、圖形、影像等)，再傳送給接收方，接收方可藉由與傳送方協定的方法取出媒介中的機密訊息。由於圖形被廣泛的使用於網路上，且圖形具有龐大藏量的特性，所以大部份的研究都以圖形為媒介。

資訊隱藏法又分為可逆式與不可逆式。可逆式可保持其原始媒體的完整性，主要有 Tian 學者(2007)[3]提出的差值擴張法、Ni 學者(2006)[5]提出的直方圖位移法，通常無法藏入大量的機密訊息；不可逆式是指機密訊息取出後無法還原原始媒介，通常可藏入大量的機密訊息，以 Chan 等學者(2001)[1]提出的最小位元藏匿法(LSB)為一個普遍的藏匿技術，Chan 等學者(2004)[2]對 LSB 另外提出了 OPAP 的最優化方法。

一般而言，人類視覺系統(HVS)對於影像平坦區內的變化之視覺敏感度高於複雜區的變化，且在 PSNR 值大於 30dB 時不具分辨性。本研究透過 MED 邊緣檢測法判別 2x2 區塊內是否有'edge'還是'non-edge'，並依上述的 HVS 特性決定藏入訊息的長度，利用 LSB 藏匿技術結合 OPAP 優化技術將機密訊息嵌入，使其偽裝影像在人類視覺系統可接受的範圍內(PSNR 為 30dB 左右)，有較大的藏量及好的影像品質。

本文其餘的部分安排如下：第二章介紹相關研究，研究方法則在第三章說明，實驗結果在第四章說明，最後是結論。

2. 相關研究

在本章中將介紹：MED、Least Significant Bit (LSB)與 Optimal pixel adjustment process (OPAP)。在底下的小節中，我們定義目標像素為 x，如圖 1，陰影區域代表是 x 的相鄰像素，a 為目標像素之水平鄰近像素、b 為目標像素之垂直鄰近像素、c 為目標像素之對角像素。

c	b
a	x

圖 1 目標像素 x 與其相鄰像素

2.1 MED

Weinberger(2000)[4]所提出的 MED 預測法：假設在原始影像中 a、b、c 為目標像素 x 的鄰近像素(如圖 1)。則其預測值為

$$\hat{x}=\begin{cases}\min\{a,b\}, & if\ c\geq\max\{a,b\}\\ \max\{a,b\}, & if\ c\leq\min\{a,b\}\\ a+b-c, & otherwise\end{cases}$$

其中若 $c\geq\max\{a,b\}$ 或是 $c\leq\min\{a,b\}$ 表示有'edge'，否則為'non-edge'。

2.2 LSB

Chan 等學者(2001)[1]提出 Least Significant Bit (LSB)藏匿法為一個普遍的藏匿技術，具有高藏量與低失真的特性，其方法如下：

設 P 為 8 位元像素的 $M\times N$ 原始影像的像素。

$$P=\{x_{ij}\mid 0\leq i<M, 0\leq j<N, x_{ij}\in[0,255]\}$$

設 s 為 n 位元的機密訊息。

$$s=\{s_i\mid 0\leq i<n, s_i\in\{0,1\}\}$$

假設將 n 位元的機密訊息 s 嵌入於原始影像 C 的最右邊 k 位元，首先，將機密訊息 s 排置成 k 位元的 s'。

$$s'=\{s'_i\mid 0\leq i<n', m_i\in\{0,1,...,2^k-1\}, n_i<M\times N\}$$

n 位元的機密訊息 $s=\{s_i\}$ 與嵌入訊息 $s'=\{s'_i\}$ 的關係如下：

$$s'=\sum_{j=0}^{k-1}s_{i\times k+j}\times 2^{k-1-j}$$

其中 n' 像素 $\{x_{l_1},x_{l_2},...,x_{l_{n'}}\}$ 從原始影像 C 預先定義的序列中選出。

嵌入過程：原始像素 x_{l_i} 嵌入 k 位元訊息 m'_i 後為隱蔽像素 x'_{l_i}，則

$$x'_{l_i}=x_{l_i}-x_{l_i}\bmod 2^k+s'_i$$

取出過程：使用和嵌入過程中相同的序列，隱蔽像素 $\{x'_{l_1},x'_{l_2},...,x'_{l_{n'}}\}$ 含有嵌入的訊息，嵌入訊息 m'_i 可透過下面的式子取出:

$$s'_i=x'_{l_i}\bmod 2^k$$

2.3 Optimal pixel adjustment process

Chan 等學者(2004)[2]提出 LSB 技術最佳化的方法 OPAP (Optimal pixel adjustment process)，利用 LSB 藏匿機密訊息再加以最佳化以減少失真。

在原始影像 C 中，假設, p_i，p'_i，p''_i 為第 i 個相對應的像素，透過 LSB 的藏匿方法和 OPAP 得到偽裝影像 C'，假設 d_i 為 p'_i 和 p_i 的嵌入誤差，在 2.2 節中，p'_i 是透過 LSB 取代 p_i 的 k 位元而得到的，因此，$-2^k<d_i<2^k$，d_i 可再進一步地分成三個區間：

第一區間: $2^{k-1}<d_i<2^k$

第二區間: $-2^{k-1}\leq d_i\leq 2^{k-1}$

第三區間: $-2^k<d_i<-2^{k-1}$

藉由三個不同的區間，將隱蔽像素 p'_i 透過 OPAP 修改為 p''_i，敘述如下：

例一($2^{k-1}<d_i<2^k$)：

若 $p'_i\geq 2^k$，$p''_i=p'_i-2^k$，否則 $p''_i=p'_i$。

例二($-2^{k-1}\leq d_i\leq 2^{k-1}$)：

$p''_i=p'_i$。

例三($-2^k<d_i<-2^{k-1}$)：

若 $p'_i<256-2^k$，$p''_i=p'_i+2^k$，否則 $p''_i=p'_i$。

假設 d'_i 為 p''_i 和 p_i 的嵌入誤差，d'_i 的計算如下：

例一($2^{k-1}<d_i<2^k$ & $p'_i\geq 2^k$)：

$d'_i=p''_i-p_i=p'_i-2^k-p_i=d'_i-2^k$

$\Rightarrow\quad 2^{k-1}-2^k<d'_i<2^k-2^k$

$\Rightarrow\quad -2^{k-1}<d'_i<0$

例二($2^{k-1}<d_i<2^k$ & $p'_i<2^k$)：

$d'_i=p''_i-p_i=p'_i-p_i=d_i$

$\Rightarrow\quad 2^{k-1}<d'_i<2^k$

例三($-2^{k-1}\leq d_i\leq 2^{k-1}$)：

$d'_i=p''_i-p_i=p'_i-p_i=d_i$

$\Rightarrow\quad -2^{k-1}\leq d'_i\leq 2^{k-1}$

例四($-2^k<d_i<-2^{k-1}$ & $p'_i<256-2^k$)：

$d'_i=p''_i-p_i=p'_i+2^k-p_i=d_i+2^k$

$\Rightarrow\quad -2^k+2^k<d'_i<-2^{k-1}+2^k$

$\Rightarrow\quad 0<d'_i<2^{k-1}$

例五($-2^k<d_i<-2^{k-1}$ & $p'_i\geq 256-2^k$):

$d'_i=p''_i-p_i=p'_i-p_i=d_i$

$\Rightarrow\quad -2^k<d'_i<-2^{k-1}$

由上面五例可知經由 OPAP，可將原始影像與偽裝影像的嵌入誤差的絕對值限制於 $0\leq|d'_i|\leq 2^{k-1}$。

3. 研究方法

本實驗中先將原始影像複製為四份相同的影像，再將這四張相同影像各別切割為 2x2 的區塊，這四張影像中的每個小區塊，分別在小區塊中的四個不同位置依 MED 邊緣偵測分為'edge'與'non-edge'，並且依照特性決定藏入訊息的多寡，最後再將這四張影像合併為一張偽裝影像(如圖 2)。

3.1 複製影像與影像切割

本實驗中先將原始影像複製為四張相同的影像，再將這四張影像分割為 2×2 的小區塊，並且將這四張圖在小區塊中的四個不同位置分別藏入機密訊息，如圖 3、圖 4、圖 5 與圖 6 所示：

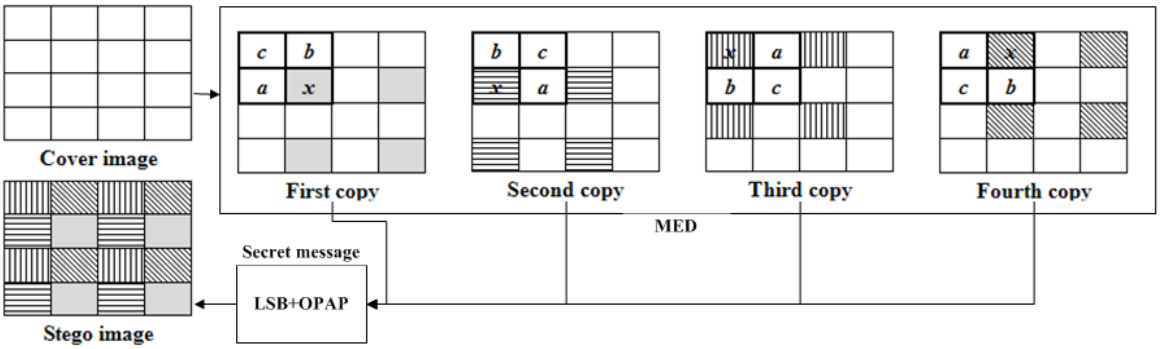


圖 2 藏入方法

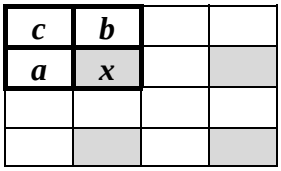


圖 3 First copy

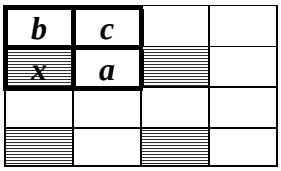


圖 4 Second copy

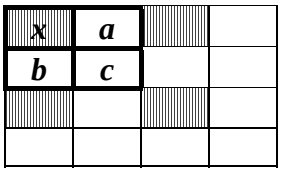


圖 5 Third copy

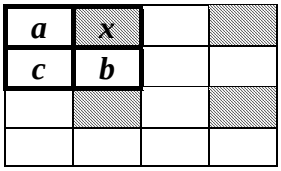


圖 6 Fourth copy

其中 x 為藏匿的目標像素，a 為目標像素的水平鄰近像素，b 為目標像素的垂直鄰近像素，c 為目標像素的對角近像素。

3.2 藏匿方法與取出方法

將 2x2 區塊分為'edge'與'non-edge'，並且根據其特性決定藏量大小。

判斷方法：

若 $c \geq \max\{a,b\}$ 或 $c \leq \min\{a,b\}$ ，則該區塊為'edge'，否則為'non-edge'。

依照人類視覺系統(HVS)，複雜區塊的改變較難察覺，因此在'edge'區藏入 n bits，在'non-edge'區藏入(n-1) bits。

藏匿方式使用 LSB+OPAP，如圖 3、圖 4、圖 5 與圖 6 之順序，依序藏入機密訊息。

藏匿方法：

對於目標像素 x 使用 LSB(n)+OPAP 藏入 n bits：

$$x_1' = [x - (x \mod 2^n)] + s$$

$$x_2' = \begin{cases} [x - (x \mod 2^n) + 2^n] + s \ if \ \left\lfloor \frac{x}{2^n} \right\rfloor \in even \\ [x - (x \mod 2^n) - 2^n] + s \ if \ \left\lfloor \frac{x}{2^n} \right\rfloor \in odd \end{cases}$$

隱蔽像素 $x' = \begin{cases} x_1' \ if \ |x_1' - x| \leq |x_2' - x| \\ x_2' \ if \ |x_1' - x| > |x_2' - x| \end{cases}$ ，其中 s 為 n bits 機密訊息。

四張圖接藏匿完成之後將藏匿完成的四張影像各自取其 x 像素，合併為一張偽裝影像(Stego image)，如圖 7：

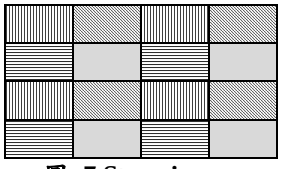


圖 7 Stego image

取出方法則是需要四張原始影像，並且將偽裝影像中每個小區塊的四個不同位置的像素，複製到四張原始影像中對應的位置，將偽裝影像還原回如圖 3、圖 4、圖 5 與圖 6，四張影像，接著將這四張影像依序使用 LSB 取出機密訊息(如圖 8)。

對於隱蔽像素 x' 使用 LSB(n)取出 n bits：

機密訊息 $s = x' \mod 2^n$ 。

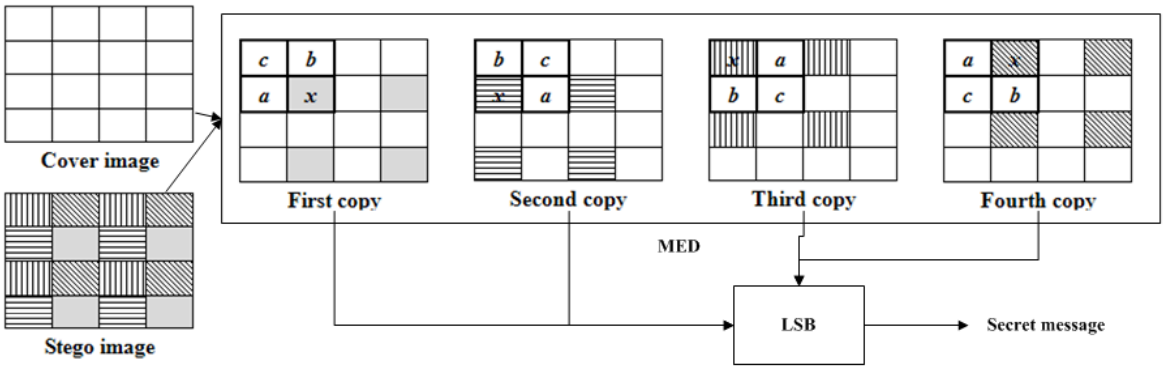


圖 8 取出方法

3.3 藏匿與取出範例

設 n=5，機密訊息串為'101011010000010011'以圖 9 為例：

80	179
78	178

圖 9 藏匿範例圖

藏匿步驟：

第一張圖：

目標像素 $x=178$，因為 $\min\{a,b\}<c<\max\{a,b\}$ 故藏入 4 bits，s=0011_2=3，則

$$x'=[178-(178 \bmod 16)]+3=179$$ 。

第二張圖：

目標像素 $x=78$，因為 $c\geq\max\{a,b\}$ 故藏入 5 bits s=00001_2=1，則

$$x'=[78-(78 \bmod 32)]+1=65$$

第三張圖：

目標像素 $x=80$，因為 $\min\{a,b\}<c<\max\{a,b\}$ 故藏入 4 bits，s=1010_2=10，則

$$x'=[80-(80 \bmod 16)]-16+10=74$$

第四張圖：

目標像素 $x=179$，因為 $c\leq\min\{a,b\}$ 故藏入 5 bits，s=10101_2=21，則

$$x'=[179-(179 \bmod 32)]+21=181$$

之後再將這四張圖有藏匿機密訊息的部分取出，合併為一張偽裝影像，如圖 10：

74	181
65	179

圖 10 藏匿完後的合併圖

取出步驟：

將圖 10 的偽裝影像中每個小區塊的四個部分各自取出，並且替換掉四張原圖相對應位置(灰色部分)的像素值，如圖 11-14：

80	179
78	179

圖 11 第一張替換圖

80	179
65	178

圖 12 第二張替換圖

74	179
78	178

圖 13 第三張替換圖

80	181
78	178

圖 14 第四張替換圖

第一張圖：

隱蔽像素 $x'=179$，因為 $\min\{a,b\}<c<\max\{a,b\}$ 故藏入 4 bits，$s=179 \bmod 16=3=0011_2$。

第二張圖：

隱蔽像素 $x'=65$，因為 $c\geq\max\{a,b\}$ 故藏入 5 bits，$s=65 \bmod 32=1=00001_2$。

第三張圖：

隱蔽像素 $x'=74$，因為 $\min\{a,b\}<c<\max\{a,b\}$ 故藏入 4 bits，$s=74 \bmod 16=10=1010_2$

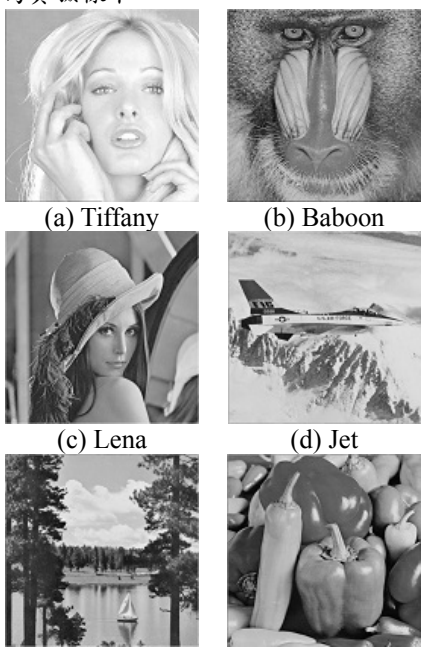
第四張圖：

隱蔽像素 $x'=181$，因為 $c\leq\min\{a,b\}$ 故藏入 5 bits

$s = 181 \bmod 32 = 21 = 10101_2$ 。

4. 實驗結果

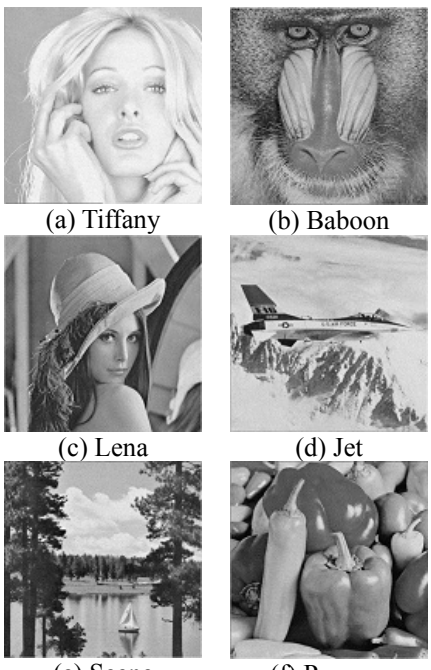
本實驗使用 SIPI 影像圖庫裡的'Tiffany'、'Baboon'、'Lena'、'Airplane'、'Scene'與'Peppers'，這六張圖為實驗樣本：



(a) Tiffany (b) Baboon (c) Lena (d) Jet (e) Scene (f) Peppers

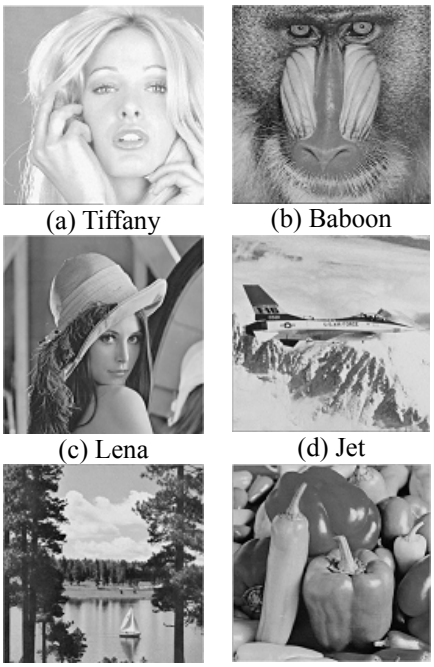
圖 15 六張原始影像

當 n=5 與 n=4 時，藏匿後的結果如圖 16、圖 17，由於 PSNR 值皆接近或大於 30dB，並無顯著差異：



(a) Tiffany (b) Baboon (c) Lena (d) Jet (e) Scene (f) Peppers

圖 16 n=5 六張藏匿後的影像



(a) Tiffany (b) Baboon (c) Lena (d) Jet (e) Scene (f) Peppers

圖 17 n=4 六張藏匿後的影像

由表 1、表 2 可知 n=5 時，平均 PSNR 值約為 29.86dB，接近人類視覺系統可接受的影像品質，平均藏入率高達 4.69 bpp。若取 n=4，平均 PSNR 值約為 35.90dB，其平均藏入率亦高達 3.69 bpp。

表 1 n=5 藏量表

	PSNR	Capacity	Payload
Tiffany	29.391660	1235456	4.712891
Baboon	30.215669	1214049	4.631229
Lena	29.957462	1229326	4.689507
Jet	29.891162	1233349	4.704853
Scene	29.930917	1230931	4.695629
Peppers	29.766402	1241229	4.734913

表 2 n=4 藏量表

	PSNR	Capacity	Payload
Tiffany	35.697580	973312	3.712891
Baboon	36.197437	951905	3.631229
Lena	35.964673	967182	3.689507
Jet	35.894131	971205	3.704853
Scene	35.908862	968787	3.695629
Peppers	35.755626	979085	3.734913

5. 結論

本研究利用複製四份原始影像，再將這四份原始影像各別分割為 2×2 的區塊，分別使用 MED 邊緣檢測法判斷是否存在邊緣，進而以 LSB 結合 OPAP 的方式藏入機密訊息，最後再將四份藏入後

的影像結合為偽裝影像。由實驗結果可以知道可知當 n=5 時，平均 PSNR 值約為 29.86dB，接近人類視覺系統可接受的影像品質，平均藏入率高達 4.69 bpp。

參考文獻

[1] Chi-Kwong Chan, L.M. Cheng, “Improved hiding data inimages by optimal moderately signifcant-bit replacement”, IEEElectron. Lett. 37 (16) ,pp1017–1018,2001.

[2] Chi-Kwong Chan, L.M. Cheng, “Hiding data in images by simple LSB substitution”,Patter Recognition,Vol.37,pp. 469-474,2004.

[3] Tian, J.,“Reversible data embedding using a difference expansion.” IEEE Transactions on Circuits and Systems for Video Technology, 16 (3), 721–730. 2007.

[4] Weinberger MJ & Seroussi G, “The LOCO-I lossless image compression algorithm:principles and standardization into JPEG-LS”, IEEE Trans Image Process, 9(8), pp. 1309-1324, 2000.

[5] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su, “Reversible Data Hiding.” IEEE Transactions on Circuits and systems for video technology, Vol. 16, No. 3, March 2006

雲端安全儲存系統

林華鵬　周國森　郭志勇　單張麟　陳彥仲　林宗毅
中華電信研究院　資通安全研究所　雲端運算研究所
walterlin@cht.com.tw、cksp@cht.com.tw、jason_kuo@cht.com.tw、zlshan@cht.com.tw、yzchen@cht.com.tw、ianlin@cht.com.tw

摘要

近年來雲端運算技術在資訊科技產業上已成為眾所皆知的技術，雲端技術服務提供了有效率及有彈性的資源分配，使用者可以依據自己的資源需求，動態的取得資源，如此使用者僅需依實際上使用資源量的多寡來支付費用。另一方面，許多企業因擁有大量的數位資料，原本可能需要花費龐大的成本來購買硬體儲存設備，然而因為雲端技術服務用多少付多少的特性，可有效的減少企業購買硬體儲存設備的成本。

雖然企業使用雲端儲存服務可有效降低成本，但將可能會有企業敏感性資料散佈在世界各地儲存設備上之安全性疑慮。

資料安全是企業及個人都相當重視的重要議題，且雲端資訊安全和實體資訊安全擁有不同的特質與需求，本文將提出一個雲端安全儲存系統，能夠有效解決雲端儲存服務所面臨的資訊安全議題，確保雲端儲存服務使用者的資料安全。

關鍵詞：雲端運算、雲端儲存服務、雲端儲存安全、資料安全、加密與解密

Abstract

In recent years, cloud computing has become the well-known technology in the information technology industry. The cloud-based services always supply great service performance and flexible resource allocation to the cloud users. Therefore, users can dynamically allocate the storage resources and computing according to the demands. It saves huge hardware costs and users only need to pay for what they really used. On the other hand, a number of companies plan to paper information data into digital data, so the data storage and backup requirements are highly valued. It would take considerable cost if the companies build their own storage. Although cloud storage services could effectively reduce the costs, users are afraid of the data to be stolen through the accessible Internet, especially for the sensitive data.

Data security in the cloud is an important issue for companies and personal users. In this paper, we will propose a cloud security storage system to solve those security issues to ensure that the user's data security.

Keywords: Cloud Computing、Cloud Storage、Security of Cloud Storage Services、Data Security、Encrypt and Decrypt

1. 前言

「雲端技術」已成為近年來最熱門的名詞，政府也投入龐大的經費，投入雲端運算的領域，當然中華電信也不缺席，在 2013 年 6 月耗資 130 億元打造的中華電信 IDC 雲端資料中心，預定 2015 年正式營運並提供服務，預估在四年之內就有上千億元的雲端建設投資將陸續進駐。

另一方面，由台灣雲端運算產業協會規劃建置的「台灣雲谷」已經在 2012 年 3 月 14 日正式啟用，未來能夠整合雲端產業資源並提供企業完整的雲端服務解決方案。

雲端儲存屬於雲端運算大架構中的一環，所謂雲端運算就是將具備擴充性及彈性化的 IT 資源，透過網路並以服務的型態分派給用戶的一種運算服務型態。相同的，所謂雲端儲存，也就是將具備高擴充性與高彈性化的儲存資源存放到網際網路上供用戶存取的一種服務型態。進一步而言，雲端儲存由儲存服務提供商(SSP；Storage Service Provider)所提供，雲端儲存擁有彈性的儲存空間池(Storage Pool)管理架構，比起傳統儲存架構或裝置，雲端儲存將會更加便宜。

為因應企業龐大的數位資訊，雲端儲存服務帶給企業更有彈性及更節省成本的解決方法，但相較於傳統儲存設備，原本企業擁有的個資或機敏資料是儲存於企業內部儲存設備，若遺失或遭竊都是企業本身的責任，但若企業將機敏資料或個資存放於雲端儲存服務提供商之儲存空間，企業便無法保證資料安全性問題，當資料毀損或遺失，又或是敏感性資料遭到公開散佈，將會面臨到各種的資訊安全性議題，導致企業及個人使用者對雲端儲存望而卻步。

企業將資料儲存於第三方雲端儲存服務提供商，將面臨到「資料是否會遺失」、「資料是否會遭駭客入侵竊取」、「資料是否會被第三方讀取甚至公開」、「資料是否會被複製或備份到其它未知的伺服器」、「若退租第三方是否會將資料確實移除」、「由檔案名稱判斷可能為敏感性資料」等等的安全議題，為了使雲端儲存能為企業所接受，使得企業願

意將敏感性資料存放在雲端儲存服務提供商儲存空間，必須解決前述的雲端儲存資訊安全之議題。

本研究將提出一個雲端安全儲存系統，可有效的解決上述提到之安全議題，使得雲端儲存達到資料機密性、資料完整性等安全優勢，進而增強使用者對雲端儲存之信賴度。

2. 相關研究

2.1 雲端儲存簡介

雲端運算基本上是使用網際網路的方式調配資源，使用者不需要知道雲端中底層基礎設施的詳細資訊，也不需要具備相關專業知識，即可透過網際網路動態的取得所需要的資源。

雲端儲存基於雲端運算的概念，由第三方雲端儲存服務提供商，提供雲端儲存空間，所有伺服器及儲存資源都由第三方代管，第三方提供像是儲存資源池的概念，使用者可依需求購買或租賃儲存空間，即可動態的取得所需的儲存資源，並將檔案資料存放到儲存空間中，而檔案資料可能被第三方利用分散式儲存的方式，分散儲存在多部的伺服器主機上。

一般使用者可以透過第三方雲端儲存服務提供商所提供的瀏覽器 Web 化介面，或是使用第三方所提供的服務應用程式介面(API)的方式，對後端雲端儲存空間進行存取，企業只需要依實際使用的空間量來支付相關費用，如此企業不需要負擔儲存設備的購買及管理成本，可有效減少企業數位資料的儲存成本。

2.2 雲端運算類型

根據雲端資訊安全聯盟(CSA: Cloud Security Alliance)[1]於雲端安全重點領域指引文件中的定義，雲端運算分為三種產業類型模式：

●基礎架構即服務(IaaS: Infrastructure as a Service)：使用者不需自行購買硬體建置基礎設施，即可透過租用的方式，使用虛擬化處理器、儲存容量、網路等基礎之運算資源。

●平台即服務 (PaaS: Platform as a Service)：可提供雲端軟體平台開發人員所需的程式語言工具或其它相關工具，使其能在基礎架構上部署及開發應用程式，建立自己的功能平台(如規畫設計、開發、測試、部署等)，使用者僅需要控制部署環境設定組態，不需要知道較底層的網路、處理器等基礎架構。

●軟體即服務(SaaS: Software as a Service)：使用者可以透過任何具有瀏覽器的設備，設備本身不需要強力的硬體效能，不需要下載或安裝額外的程式，亦不需瞭解或管理底層的雲端基礎架構，即可直接存取該應用軟體程式。

2.3 雲端儲存安全議題

2.3.1 雲端儲存安全調查報告

IT 研究與分析網站 InformationWeek Analytics[2]於 2011 年 6 月的一份調查報告指出，企業害怕使用公用雲端儲存最大的原因在於「雲端儲存安全性的顧慮」(73%)，企業內部可能擁有機敏性資料，或是個資相關資料，即使雲端儲存方案可以有效的降低企業購買及管理儲存設備的成本，但可能因擔心敏感性資料遭第三方使用或公開散佈，或儲存空間遭到駭客入侵等安全性議題，導致企業對雲端儲存服務的使用上仍有疑慮。

2.3.2 傳統儲存架構與雲端儲存架構

圖 1 為傳統儲存架構與使用雲端儲存架構之示意圖，說明如下：

●傳統儲存架構：傳統的儲存架構模式，是透過遠端磁碟或 FTP 的方式，對企業內部的儲存設備進行存取，缺點在於使用者必須安裝特殊協定的客戶端軟體工具，且企業必須自行負擔購買儲存設備成本，以及管理設備的成本。

●雲端架構-使用瀏覽器：用戶利用瀏覽器(如 Firefox、Internet Explorer、Chrome、Safari 等)對雲端儲存空間直接進行存取，但企業將內部機敏性資料存放於雲端儲存空間，將會有資料外洩的疑慮，一方面擔心是否會被雲端儲存服務提供商公開或使用，另一方面擔心是否會遭到駭客入侵而遺失資料。

●雲端架構-使用 Client 應用程式：用戶使用 Client 應用程式(如 CrossFTP、Dragon Disk、JetS3t 等)對檔案進行上傳的動作，雖然有部份 Client 應用程式有實作資料加密的功能，但因用戶必須依應用程式的類型安裝相對應的程式語言編譯器才可使用應用程式工具，相較起來其方便性較沒那麼友善。

●雲端架構-使用雲端安全儲存系統：用戶透過本研究所提供的雲端安全儲存系統進行檔案上下載，用戶可透過雲端安全儲存系統所提供的瀏覽器

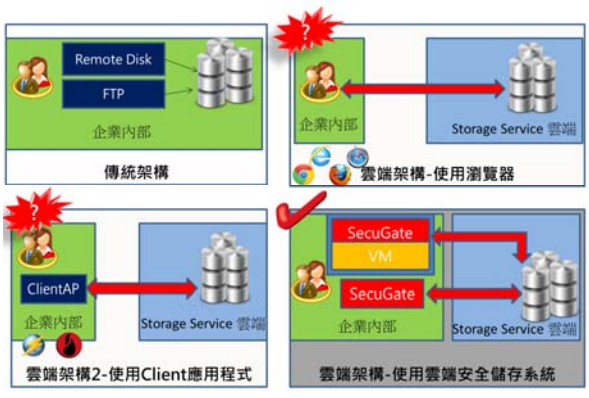


圖 1 傳統儲存架構與雲端儲存架構圖

介面或 WebDAV(VDisk/NFS)的介面進行檔案上下載的動作，當檔案經過雲端安全儲存系統時，將自動化實施資訊安全強化機制處理後，才可儲存到後端雲端儲存服務提供商儲存空間，因經過資安強化處理，所以雲端儲存服務提供商無法得知檔案正確內容，即使雲端儲存空間遭駭客入侵，同樣無法得到資料的正確內容。

2.3.3 雲端儲存安全問題

本研究經過資料蒐集匯整後，整理出企業使用雲端儲存服務可能會遭遇到的安全問題所列如下：

●雲端儲存服務身份認證安全性問題：若使用雲端儲存服務，一般雲端儲存服務提供商將會提供一組帳號密碼的金鑰給使用者，使用者則可以透過這組帳號密碼對雲端儲存空間進行存取，但一旦這組金鑰遭到有心人士竊取，則儲存空間上之敏感性資料也可能遭到取得。

●用戶所能掌控之安全範圍邊界問題：傳統上企業將機敏性資料存放在企業內部的儲存設備上，因此企業可以自行完全掌控其資料的安全範圍，但若使用雲端儲存服務，則企業必須信任第三方雲端儲存服務提供商不會使用或散佈企業內部的機敏性資料。

●檔案資料最終存放位置的疑慮：傳統上企業將機敏性資料存放在企業內部的儲存設備，企業可明確的知道檔案所在的位置，但若使用雲端儲存服務，檔案資料可能因為分散式檔案系統的特性，資料被複製或備份到未知的伺服器上，一旦用戶退租雲端儲存服務，也無法確定機敏性檔案資料是否已確實完全的被刪除。

●檔案資料完整性的疑慮：傳統上企業直接將資料存放在企業內部的硬體儲存設備上，不需要透過網際網路即可直接在企戶內部儲存設備上確認檔案的完整性，但若使用雲端儲存服務，必須透過網際網路將檔案資料上傳至雲端儲存空間，則可能會因網路穩定性或網路品質問題，造成封包資料的遺失，而檔案完整性出現問題。

●雲端儲存空間資料被駭客竊取並散佈：傳統上企業可使用安全設備，加強存放機敏性資料的儲存設備，若使用雲端儲存服務，則企業用戶必須全盤信任第三方雲端儲存服務提供商的安全性防護機制，可以有效防護駭客的入侵。

3. 雲端安全儲存系統架構

3.1 雲端安全儲存系統使用情境

圖 2 為雲端安全儲存系統使用情境示意圖，雲端安全儲存系統提供了瀏覽器介面(支援 HTTP/HTTPS 協定)，讓所有擁有瀏覽器的設備皆可以透過此介面，將檔案資料透過瀏覽器上傳至後端雲端儲存空間，另外使用者也可以透過 WebDAV(VDisk/NFS)的介面，使用類似網路芳鄰的方式，將檔案資料上傳至後端雲端儲存空間。

當檔案經由雲端安全儲存系統時，會將檔案資料進行資訊安全強化的特殊處理，處理完成後，才會將檔案資料送至第三方雲端儲存服務提供商，第三方雲端儲存服務提供商看到的只是沒有任何意義的資料片段，無法得知檔案實際的內容，因此雲端儲存服務提供商並無法得知檔案真正內容。

同樣的，使用者或企業可透過瀏覽器或 WebDAV(VDisk/NFS)的介面，來對檔案進行下載的動作，檔案經過雲端安全儲存系統後，將對原本沒有意義的資料片段實施還原的動作，使用者即可獲得原始的檔案資料內容。

3.2 雲端安全儲存系統架構

圖 3 為雲端安全儲存系統架構圖，使用者透過前端使用者介面，進行檔案的上傳及下載，雲端安全儲存系統中的資訊安全強化模組則負責接收前端使用者介面所傳送過來的資訊，並且對使用者準備傳送或接收的檔案進行資訊安全的強化，不論上傳或下載，資訊安全強化模組皆會與雲端儲存服務提供商進行溝通，並傳輸或取得檔案，而後端雲端儲存服務提供商可以是各種不同的 S3 Compatible 之服務提供商。



圖 2 雲端安全儲存系統使用情境示意圖

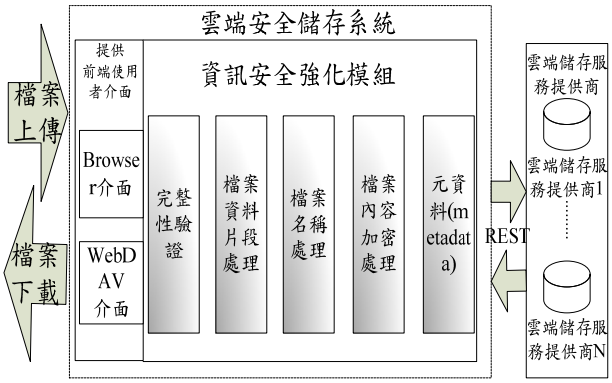


圖 3 雲端安全儲存系統架構圖

使用者可透過前端使用者瀏覽器介面或WebDAV 協定(VDisk/NFS)介面，選擇想要上傳至雲端儲存空間的檔案，檔案將透過介面被傳送到資訊安全強化模組，資訊安全強化模組將對檔案實施資安強化處理。

檔案資料於資訊安全強化模組中將實施完整性驗證、檔案資料片段處理、檔案名稱處理、檔案內容加密處理，最後將各個片段檔案名稱與原始檔案名稱實施對應，儲存在使用者可自行控管的元資料(MetatData)檔案中，如此即完成資訊安全強化模組對檔案實施強化的步驟。

資訊安全強化模組會再將資安強化後的檔案片段，利用多工的方式，將各個檔案片段使用 REST 協定傳送至後端各種支援 S3 Compatible 的雲端儲存服務提供商，也因各個上傳完成的檔案片段皆經過資訊安全強化模組的安全強化處理，所以後端的雲端儲存服務提供商無法得知實際檔案資料的內容。

同樣使用者也可透過前端瀏覽器或WebDAV(VDisk/NFS)介面，下載並取得原始檔案內容，存放於雲端儲存服務提供商的檔案片段，將被傳送至雲端安全儲存系統的資訊安全強化模組實施反向的處理，檔案將會被還原成原始內容，呈現在前端使用者介面上。

4. 雲端安全儲存系統功能

4.1 雲端安全儲存系統瀏覽器介面實作

圖 4 為雲端安全儲存系統瀏覽器介面功能圖，透過雲端安全儲存系統所提供的瀏覽器介面存取後端雲端儲存空間，其介面上所提到的功能，於表 1 雲端安全儲存系統瀏覽器介面功能介紹表上進行詳細說明：

表 1 雲端安全儲存系統瀏覽器介面功能介紹表

功能名稱	功能詳細說明
分享密庫	分享自己的密庫給其他雲端安全儲存系統的使用者
開啟或關閉密庫	開啟或關閉屬於自己的密庫
刪除密庫	將未使用的密庫刪除
進入密庫	顯示所有存在於該密庫中之檔案列表，並進一步對檔案進行操作。
編輯密庫說明	對該密庫的用途作描述
上傳檔案	在本機端，選擇想要上傳至雲端儲存空間之檔案，檔案傳送過程中，會經由雲端安全儲存系統之安全強化處理，所以成功傳送至雲端儲存空間之檔案是具備資料安全性的
刪除檔案	於檔案列表中刪除所選擇的檔案，檔案也隨之在後端儲存空間被刪除
重新命名檔案	檔案名稱將被重新命名
下載檔案	從雲端儲存空間中，取得原始檔案內容
分享檔案	分享自己的檔案給其他雲端安全儲存系統的使用者

4.2 雲端安全儲存系統 WebDAV 介面實作

雲端安全儲存系統除了實作瀏覽器介面外，也有另外實作 WebDAV 的介面，圖 5 為雲端安全儲存系統 WebDAV 介面圖，於表 2 雲端安全儲存系統 WebDAV 介面介紹表上進行詳細說明：



圖 4 雲端安全儲存系統瀏覽器介面功能圖



圖 5 雲端安全儲存系統 WebDAV 介面圖

表 2 雲端安全儲存系統 WebDAV 介面介紹表

Windows WebDAV	Mobile Device WebDAV
圖 5 左側為使用 Windows 內建的 WebDAV 協定，連接到雲端安全儲存系統提供之 WebDAV 介面，可以透過拖曳資料夾或拖曳檔案的方式，將檔案上傳至後端雲端儲存空間，上傳途中同樣的檔案會經過資訊安全強化模組的安全強化	同樣的可以在支援 WebDAV 的行動裝置上，使用 WebDAV 協定連接到雲端安全儲存系統的介面上，使用者可在行動裝置上，安裝 WebDAV 協定之 APP，圖 5 右側為使用 iPhone 行動裝置配合 WebDAV APP，對雲端安全儲存系統實施操作的展示

4.3 雲端安全儲存系統資訊安全強化結果

圖 6 為雲端安全儲存系統資安強化結果確認圖，使用者透過雲端安全儲存系統，上傳多個文字檔案，檔案經過資訊安全強化模組對檔案資料實施安全性強化後，才上傳至後端雲端儲存空間。我們利用開放原始碼的 S3 客戶端工具 JetS3t ，直接連接到後端雲端儲存服務提供商，實際檢視上傳後的檔案內容，可發現檔案內容已實施資安強化處理。

在經過雲端安全儲存系統資安強化處理後的檔案，不僅檔案名稱被置換成無意義的檔名，並且檔案也成為許多無意義的檔案片段。為了進行確認，將檔案片段下載後，直接開啟檔案片段內容，可以發現資料內容是呈現密文的情況，因此即使檔案是儲存於不信任的第三方雲端儲存服務提供商，或是後端儲存空間若不幸遭到駭客入侵，也無法還原其原始檔案的真正內容，因此可以確保在後端雲端儲存空間檔案的安全性。

同樣地，當使用者進行儲存空間退租時，因後端是經由資訊安全強化模組處理後的資料，所以即使實際上資料片段沒有被第三方雲端儲存提供商真正刪除，或是檔案被複製或備份至其它伺服器時，同樣不需要擔心機敏性資料外洩的問題。

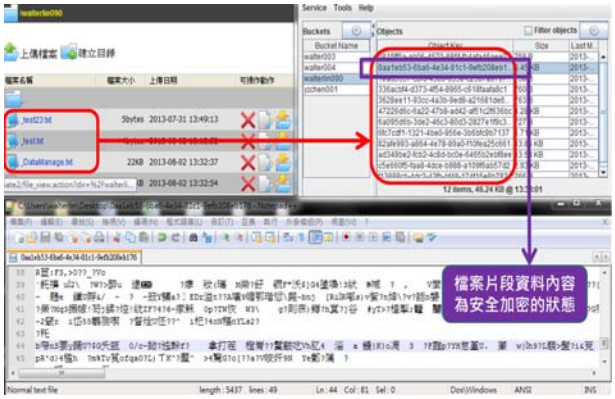


圖 6 雲端安全儲存系統資安強化結果確認圖

4.4 雲端安全儲存系統優勢

雲端安全儲存系統可確保檔案資料於雲端儲存空間之機密性、完整性、刪除確定性。綜合來說，雲端安全儲存系統具備的優勢於表 3 雲端安全儲存系統優勢列表進行說明：

表 3 雲端安全儲存系統優勢列表

優勢項目	功能詳細說明
雲端平台具高度獨立性	雲端安全儲存系統可運行於 XEN、VMWare、KVM…等平台之虛擬機器上
與作業系統之相容性	雲端安全儲存系統建置於 Tomcat Web 伺服器上，並使用 Java 程式語言所開發，可運行於 Linux、Windows…等作業系統上
使用者自行控管金鑰及安全性範圍	使用者可以自行保管加解密之金鑰，所有加解密過程在用戶端進行，可確保檔案資料之機密性
加密等級高	使用高強度之 AES-256 對稱式加密演算法並配合非對稱式加密演算法
通道安全	所有檔案傳輸過程，皆運行於 SSL 安全通道上
使用 Smart Card 認證	企業可選用 Smart Card 認證機制，透過 Smart Card 安全認證後才可使用雲端安全儲存系統
檔案操作權限控管	可限制雲端安全儲存系統使用者檔案操作權限，如可讀/寫、可瀏覽之副檔名
操作紀錄查詢	提供雲端安全儲存系統之操作紀錄查詢功能
標準化之存取介面	提供 HTTP/HTTPS 及 WebDAV 之存取介面，使得具備瀏覽器及支援 WebDAV 協定之機器及行動裝置設備，可透過此兩種存取介面進行檔案上下載之操作
分享機制	提供檔案目錄分享機制，以及限制下載次數之單一 URL 分享機制
片段分散儲存機制	具備將單一檔案進行若干片段處理並傳送至不同雲端儲存服務提供商儲存空間之機制

5. 結語

資訊科技與網路技術不斷的提升，促成了雲端服務時代的來臨，使得雲端服務成為近來最熱門的話題，隨著企業實體資料轉換為數位化資料的趨勢，企業必須購買更多的儲存設備來儲存龐大的數位資料，可能增加了企業購買儲存設備及維運的成本。

企業若使用雲端儲存服務，可視實際需求調整儲存空間的租用量，並依據租用量來計費，如此可有效降低購買實體儲存設備的資本支出及維運設備的人事成本，但雲端儲存是否會被企業所接受，企業主要考量仍在於能否解決雲端儲存資訊安全方面的議題。

雲端儲存服務所衍生的資訊安全問題與以往傳統資訊安全領域不盡相同，例如檔案資料最終存放位置的疑慮、檔案資料完整性的疑慮、檔案資料被駭客竊取並散佈的疑慮、若退租是否真的將檔案資料刪除的疑慮。若企業的機敏性檔案資料未實施安全強化處理，直接將檔案資料儲存於雲端儲存空間，若不幸重要資料被公開或外洩，將造成企業嚴重的損失。

本研究提出雲端安全儲存系統，使用者可直接使用任何具有瀏覽器之設備，或支援 WebDAV 協定之設備，對後端儲存空間進行存取，所有透過雲端安全儲存系統上載至雲端儲存空間之檔案資料內容，均經過資訊安全強化模組的處理，可確保後端雲端儲存空間資料的安全性，達到資料機密性、資料完整性、資料刪除確定性等安全儲存的目的。

雲端儲存服務帶給使用者及企業更大的便利，使用雲端安全儲存系統能夠解決使用者及企業所擔心的雲端儲存安全議題，並爲雲端儲存使用者提供更完整的安全保障，增強使用者對雲端儲存之信賴度，助益雲端儲存技術之推廣。

參考文獻

[1] Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing V3.0”, 2011.

[2] Michael Biddick, “Cloud Storage: Changing Dynamics Beyond Services”, 2011.

[3] Grant Bugher, “Secure Use of Cloud Storage”, USA: Blackhat Briefings 2010.

[4] Rampal Singh, Sawan Kumar, Shani Kumar Agraharii, “Ensuring data storage security in Cloud Computing”, International Journal Of Engineering And Computer Science, 2013, pp. 825-830.

[5] Amazon, “Amazon Web Services: Overview of Security Processes”, AWS Security Whitepaper, 2011.

[6] Google Developers, “Google Cloud Storage, https://developers.google.com/storage/”, 2013.

[7] Cloud Security Alliance, “Top Threats to Cloud Computing V1.0”, 2010.

[8] Ceph, “Ceph Storage File System, http://ceph.com/ceph-storage/file-system/”, 2013.

[9] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing”, CA: INFOCOM, 2010, pp. 1-9.

[10] S. Subashini, V. Kavitha, “A survey on security issues in service delivery models of cloud computing”, Journal of Network and Computer Applications, 2011, pp. 1-11.

[11] L.M. Kaufman, ”Data Security in the World of Cloud Computing”, Security & Privacy, IEEE, 2009, pp. 61-64.

[12] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou, “Security and Privacy in Cloud Computing: A Survey”, Beijing: Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on, 2010, pp. 105-112.

主動式傳播殭屍網路防禦機制
A Defense Mechanism for the Active Spread of Botnet

葉奇鑫　　曾黎明　　彭博涵
國立中央大學
candle576@dslab.csie.ncu.edu.tw
tsenglm@cc.ncu.edu.tw
natata@dslab.csie.ncu.edu.tw

摘要

殭屍網路是目前最嚴重的資訊安全威脅之一，原因在於殭屍網路是結合多種惡意程式特色的攻擊手法，攻擊者具有高度隱密性並能同時一對多來操控整個殭屍網路進行惡意行為。

主動式入侵方式是指攻擊者去利用漏洞入侵到受害者電腦，並取得權限去安裝惡意程式。我們將針對主動式入侵攻擊的方式提出防禦機制，利用動態延伸蜜罐誘捕系統(Dynamic Extensible Two-way Honeypot)機制提供連上特殊的偽造 C&C 伺服器來作為解毒的方法以防止主動式殭屍網路的傳播。

關鍵詞：殭屍網路、主動式入侵、誘捕系統、解毒、殭屍網路傳播

Abstract

Botnet is a combination of a variety of unique malware attack techniques. Victims install and execute the botnet malware by themselves, because they have a bad habit of network usage. Even if their computers have been cleared the malware, they are likely to be a bot again in a short time. It explains the passive decoy botnet is difficult to prevent. We will focus on the defense mechanism of active intrusion, and we use dynamic extensible honeypot system to provide a special connection to the server and remove malwares to prevent the active spread of botnet.

Keyword：Bot、Botnet、Active intrusion、Honeypot、Active spread of botnet

1. 前言

殭屍網路(Botnet)是目前最嚴重的資訊安全威脅之一[1][2][3]，它是指一群感染惡意軟體並受駭客控制的電腦，受感染的電腦(Botclient)將會猶如一個殭屍而任由擺佈，攻擊者可利用這些殭屍電腦來竊取使用者私人的資料和帳號密碼，特別是電子商務行為的重要資訊，或者用來發送垃圾郵件及釣魚郵件可以用來進行分散式阻斷服務攻擊癱瘓特定電腦[3]。

在偵測的手法上也都努力的發展出相對應的方式去檢測，像是透過部署誘捕系統[4]，如：蜜罐(Honeypot)，去找出經常性的不正常對外連線，這是利用 Botclient 必須定期的向 C&C Server 聯絡以便取得最新的配置檔或是所發佈惡意指令，相較於一般電腦的正常連線，這項特殊的特徵就能夠來作為偵測的因素之一，在利用統計方法或是演算法[5][6][7]來設定偵測門檻值，進而判斷是否有殭屍網路中毒的電腦個體。殭屍網路近來常使用新興的隱藏技術「fast-flux」[8]，來使的他們更難被偵測到，這是針對防禦方法：「封鎖特定 IP」的改良策略，這技術會不斷地輪流改變殭屍網路 C&C Server 的 DNS 紀錄，讓殭屍網路難以被查獲。

根據實際安裝者的差異，我們可以分成兩種情境：主動式攻擊漏洞與被動式誘騙攻擊。前者係因受害者電腦存在某些漏洞，使得攻擊者去利用這些漏洞入侵到受害者電腦，因此取得權限或利用程

式去下載程式檔及同時安裝。後者則是透過垃圾郵件、網頁誘騙或是將惡意程式嵌入一些應用軟體，讓粗心的使用者去將殭屍網路病毒的程式安裝起來，這類型的受害者是在無知或是相關知識較為不足的情況下，遭攻擊者透過誘騙的方式去裝設了殭屍網路程式。

對於被動式誘騙的攻擊型態而言，即便清除病毒之後，因為具有同樣的不良使用習慣，往往在短期間內又讓電腦感染了殭屍病毒程式，而又成為了殭屍病毒的其中一員，要真的隔絕此類攻擊行為並不容易。針對這些困擾，我們希望可以先針對主動式攻擊型的殭屍網路傳播來提出一個新的防禦機制。

本論文後續章節架構如下：章節二探討相關背景知識及研究；章節三分析相關研究並並提出新的防禦機制；章節四實作系統並討論防禦機制可行性；章節五結論與未來發展。

2. 相關研究

2.1 宙斯殭屍網路分析

宙斯殭屍病毒是使用 HTTP Protocol 的通訊協定[9][10]，透過網站伺服器來下達命令給 Botclient，隱藏其通訊流量於正常網頁瀏覽所產生的流量，因 HTTP web port 80 是經常開啟讓網頁可以瀏覽下載文件的管道，因此不易被防火牆偵測出來，所以隱蔽性極高。

一般使用者只要依照需要置入所需要的相關配置資訊以後，就可以產生具感染力的宙斯殭屍病毒程式。

2.2 惡意資料洩漏分析與檢測

[11]提出一種透過通訊流量來分析檢測的方法，並用宙斯殭屍網路病毒來驗證理論。宙斯殭屍網路雖然是以 HTTP 通訊協定來試圖隱藏殭屍網路通訊的訊息，但相較於一般正常使用的情況下，網路的流量仍會具有部分的差異性，這些差異就可以用來作為偵測的依據。

利用信息理論的夏農熵(Shannon's Entropy)來做特徵選取的計算，這可以對特定結果計算隨機變數的不確定性，不確定性越高，計算出來的 Entropy value 也會越高。作者將一般正常使用者電腦與感染宙斯殭屍網路病毒的電腦進行長時間的網路封包紀錄，使用夏農熵計算式去算出 Entropy value[12][13]。在使用不同的資料集去交叉比對找出誤判率較低的值來作為偵測的門檻值(threshold value)。

2.3 Openflow switch 分析偵測

在[14][15]中，透過 openflow switch 具有封包轉向的功能，來實作受害者的通知機制。整個系統架構中，除了控制封包導向的 NOX controller 與 openflow switch 外，還有一台替身的伺服器(substitute server)與一台網站伺服器(web server)。

1. 替身伺服器其功能主要作為一個偽造的 C&C Server，當中毒者向 C&C server 發送訊息，會由 openflow switch 導至這台替身伺服器，由其與中毒者電腦來回應。
2. 網站伺服器會將中毒者的網頁內容導向事先架好的中毒通知頁面，以便提醒中毒者電腦有異常行為，以便後續進行惡意病毒移除的動作。

2.4 動態延伸蜜罐誘捕系統

[16]中提出一種動態延伸雙向蜜罐誘捕系統(Dynamic Extensible Two-way Honeypot，簡稱 DEH)的架構，two-way 指的是提供進出蜜罐的雙向網路，相較於一般蜜罐怕被作為攻擊者對外攻擊的跳板，往往只提供連入蜜罐的對內網路，而由蜜罐對外的網路連線多半是禁止的，但這樣一來容易被識破且造成整體誘捕效率不佳，攻擊者當然不願在蜜罐中被記錄下攻擊手法與資訊，同時，這更是提供了攻擊者一個很好測試是否身處蜜罐系統中的方

法，因為只要針對由內對外的網路連線測試就能得知了。DEH 架構如圖 1 所示。

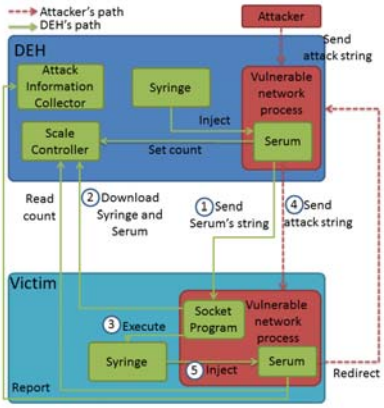


圖 1 DEH 系統結構流程圖

資料來源：[16]

3. 系統設計與架構

我們將提出的方法於虛擬機器中來進行實作，並且以宙斯病毒為測試對象，討論測試方法的可行性與實驗結果，我們期望中毒的受害者電腦可以透過我們提供的 Server 解毒，停止或降低受害者端的影響程度。

3.1 問題分析

我們利用 DEH 機制提供連上特殊的偽造 C&C 伺服器位置，由伺服器端來下指令給 Botclient 作為解毒的方法。

1. 解毒的行為從伺服器端來操作，這樣可更加快解毒的時程。
2. 若對於存在大規模需要解毒的情況下，從伺服器端解毒會是比較有效率的方式。

同時，我們會將 DEH 機制納入於系統設計中，DEH 是一個主動式注入通訊機制附帶於病毒惡意軟體跟隨著被執行的防禦方式，這正巧符合我們想提出主動式傳播殭屍網路的防禦功能，透過攻擊型態的區別，我們能避免一般的偵測機制常發生的問題：即便電腦多次完成清毒的行為，操作習慣不良的使用者往往容易在短時間內又成為殭屍網路受害者。

3.2 系統設計

系統主要包含四大部分，包括 DEH、Fake C&C Server、Switch 和 Victim PC。

DEH：

本系統設計以 DEH 作為一個基礎架構，由於 DEH 還提供動態延伸觀察範圍的機制，我們可藉此利用這項機制為來對受害者電腦對外網路進行控制，一旦感染的惡意程式嘗試與外部 C&C Server 作聯繫，DEH 便會自動注入 DLL 檔來修改建立 Socket 連線時所需的相關程式，並且更改封包傳送的目的端位置，如此一來，惡意程式便不會與真實的 C&C Server 有所聯繫。

Fake C&C Server：

Fake C&C Server 為本系統機制重要角色之一，因為它會接收惡意程式所送過來的封包訊息，並且可以對其下指令進行控制，受感染的電腦透過封包的導回作用，與此 Fake C&C Server 作聯繫，同時 Fake C&C Server 也會給予殭屍網路病毒的相關配置檔，進而修改原先殭屍網路設定值，方便後續解毒之用。

Switch：

我們將於 Switch 上裝設網路封包分析軟體 Wireshark。透過 Wireshark 去分析顯示出詳細的網路封包資料，目的在於我們希望可以得知 C&C Server 的 IP 位置，設定出 IP 黑名單作為封包導向的依據，黑名單中記錄的是來源端 IP，也就是哪些 PC 電腦曾經配置檔的請求。

Victim PC：

此為受害者電腦角色，它會被攻擊者入侵並安裝殭屍網路病毒。

透過流程圖來說明每個階段的運作機制，如圖 2 所示。



圖 2 主動式入侵防禦機制之系統運作流程

4. 實驗與討論

本章節為我們系統的實驗測試，將第三章所討論的架構採用 VMware 來進行環境的架設，所有 VM 環境皆為 Windows XP SP3，並以宙斯殭屍網路為例去實際測試提出方法的可行性。

4.1 實驗環境

在此實驗環境中我們安裝版本號: 1.2.7.19 的宙斯病毒，同時裝設 1.2.10.1 版本的 Control Panel 作為發佈命令的控制頁面。使用 XAMPP 工具程式架設網站，這是一個整合 Apache、PHP 和 MySQL 的工具套件，方便使用者輕易地建立網站。

4.2 黑名單的篩選機制

每個 Zbot 會依照配置檔內的 timer_config 設定值，定期的向 C&C server 發送 GET reques，我們可以利用宙斯殭屍網路的這項特性，一旦出現 GET config.bin 的訊息，我們將判定為是 Zbot 向 C&C Server 發送請求的訊息，因為在正常使用網路的情況下，並不會有這樣需求訊息出現。

4.3 DEH 系統修改

在原 DEH 設計中，Scale Collector 除了是一個 web server 提供相關的程式下載外，它是 DEH 控制觀察路徑長度的關鍵元件，每當有攻擊連線於 victim 端發送出前，Serum 會連至此處的相關網頁讀取 count 值作為參數，決定是否要修改 Inet_addr() 進行導回至 DEH。

在主動式攻擊防禦機制中，我們將修改導回的機制與導回的地點。Victim 端要發送連線之前，一樣會讀取相關網頁取值作為參數，而依照來源端的 IP 是否在 IP 黑名單中而得取不同的數值。1 表示來源端在 IP 黑名單中，故這個受害者電腦必定曾經發送出 GET config.bin 訊息而列為黑名單，它的連線請求都必須導回至 Fake C&C Server；0 則表示來源端 IP 正常，不需導向。

4.4 實驗測試與結果

4.4.1 實驗一：更新配置檔

測試是否可以利用偽造 C&C Server 配送更改的 config 檔來達到停止 ZBot 的行為。我們在 Fake C&C Server 放入了偽造的配置檔案，希望透過 ZBot 來更新此檔並且接受 Fake C&C Server 的特定指令。首先，更改配置檔中的 timer_config 的設定值，如此一來，雖然 ZBot 成功於受害者電腦啟動，但短期間內並不會執行任何惡意指令，這樣可以視同為暫時終止 ZBot 的行為模式。對 ZBot 而言，更新後的配置檔內新的 C&C Server 就是 Fake C&C Server。

以實驗結果來說，我們可以透過偽造的 config 檔來達到停止 ZBot 的行為。

4.4.2 實驗二：更改登錄值

測試是否可以停止 ZBot 的執行。ZBot 感染後會修改的登錄值，如果可以將此登錄值更改成正常數值，讓每次受害者開啟電腦時，ZBot 相關程式不會自動被執行，那麼就可以確實終止了 ZBot 的惡意行為。因此，我們將透過偽造的 C&C Server 去下特定指令，讓修改的登錄值還原回來。「rexec」是個可以「下載指定檔案並且執行」的指令，我們

需要「rexec」這個指令來修改登錄值，將修改登錄值的指令寫入檔案中，讓 ZBot 去下載並且執行，不過「rexec」指令有其限制性，它無法執行會顯示於視窗的執行檔，也代表下載並執行的功能具有限制條件。我們決定使用執行批次檔的方式去符合這項條件，同時批次檔(.bat file)內部的指令亦是設定為強迫執行，以避免出現警告視窗。

Fake C&C Server 所下之 command：

rexec http://URL/xxx.bat

實際測試後，在移除這些登錄值並且重新開機，sdra64.exe 並不會自動將自身植入 winlogon.exe，而 Fake C&C Server 所下的 command 一直未等到 ZBot 來執行，所以我們可以透過移除 ZBot 所修改的登錄值來終止 ZBot 的行為。

4.4.3 實驗三：測試其他版本 ZBot

測試其他版本 ZBot，並驗證上述方法之可行性。我們將在與 ZBot 相同的環境下測試驗證版本號: 2.0.8.9 的宙斯殭屍網路病毒(以 nZBot 代稱之)，在實驗一的部分，透過配送 config 檔可達到停止 nZBot 的行為，實驗效果與預期功能相符。

但在實驗二的部分經過實驗卻發現由 C&C Server 所下的「下載指定檔案並且執行」的指令無法發揮作用，原因在於原本預期的機碼名稱並非 userinit 而是改成一個亂數字串，如此一來我們便無法使用實驗二的方法達到終止 ZBot 的行為。

為此我們提出了另一個方法來處理這個問題：透過 C&C Server 下達更換首頁的指令[19]，目的在於透過原先殭屍網路想要用來綁架受害者網頁的功能，將它轉作為我們通知受害者的方式之一，受害者的瀏覽器首頁會被轉到我們預先設定好的中毒通知警告頁面，一方面讓受害者知道自己的電腦已遭到危害，二方面在網頁上可提供相關的解毒訊息供受害者參考。

Fake C&C Server 所下之 command：

user_homepage_set http://URL/xxx.htm

如果在無法終止其他版本 ZBot 情形下，我們可以使用更改首頁位置達到通知受害者的功能，雖然沒辦法對 ZBot 作有效的終止行為，但即時的通知受害者可降低整體的受害程度。

5. 第五章 結論與未來工作

5.1 結論

我們提出的主動式攻擊防禦機制可以有效的停止宙斯殭屍網路的惡意行為，並有效的降低受害者電腦的受害情況。同時，我們提出的方式適用於主動式的攻擊型態，相較不受限於使用者的上網使用習慣，比多數的防禦方法更能有效避免受害者電腦在清除病毒之後又發生多次人為不良操作而中毒的情況。我們透過Server端嘗試對受害者電腦進行直接進行解毒的行為，一來可以提升解毒成功率，二來我們可以有效的大規模進行解毒。面對不同的殭屍網路病毒，此防禦機制可以透過C&C Server指令的下達，來停止殭屍網路的行為與提供中毒頁面的通知，相較於只有單一方面的偵測機制，我們的防禦機制更能防止殭屍網路的蔓延。

根據不同需求的殭屍網路會有不同樣的功能設計，因此，依照我們的系統設計限制，可歸納出本論文提出的防禦機制所適用的範圍條件：

可否偽造出C&C Server

在系統設計中，偽造的C&C Server是扮演下達偽造命令的角色，提供受害者電腦停止惡意行為的命令，如果無法偽造出C&C Server來下命令，那麼此防禦機制會因為無法修改受害者電腦內部被攻擊者更改的設定而無法進行防禦，所以偽造的C&C Server是關鍵因素之一。

殭屍網路命令功能的限制

在偽造命令的下達方面，本防禦機制會使用到「下載檔案並執行」這個動作，如果殭屍網路命令列表並沒有提供這項功能，這會無法讓受害者電腦去載入我們指定檔案的執行工作，進而影響防禦機制的運行。

5.2 未來工作

本論文中我們以HTTP的殭屍網路為例實際測試，但是殭屍網路的型態並非只有這一種，尤其是以P2P作為通訊協定的殭屍網路其拓樸架構為隨機式的，每個Botclient也可能扮演C&C Server的角色，這會加深防禦上的難度。在未來，防禦機制的自動化將是未來的重點項目之一，在黑名單的篩選以及偽造命令的下達方面，若能夠自動化的進行處理，將可提高此機制的效率，同時也可在最短時間內可防止惡意行為的發生。

參考文獻

[1] Abu Rajab, Moheeb, et al. "A multifaceted approach to understanding the botnet phenomenon", Proceedings of the 6th ACM SIGCOMM conference on Internet measurement. ACM, 2006, pp. 41-52

[2] Davis, Carlton R., et al. "Sybil attacks as a mitigation strategy against the Storm botnet", Malicious and Unwanted Software, 3rd International Conference on. IEEE, 2008, pp.32-40

[3] S. Stankovic and D. Simic. "Defense Strategies Against Modern Botnets", IJCSIS, June 2009, Vol. 2

[4] Zou, C.C. and Cunningham, R., "Honeypot-Aware Advanced Botnet Construction and Maintenance", Proceedings of the 2006 International Conference on Dependable Systems and Networks (DSN'06), pp.199-208

[5] Masud, M. M., et al. "Flow-based identification of botnet traffic by mining multiple log files", Distributed Framework and Applications, 2008 First International Conference on. IEEE, 2008, pp.200-206

[6] Livadas, C., et al. "Usilng machine learning technliques to identify botnet traffic" Local Computer Networks, Proceedings 2006 31st IEEE Conference, 2006, pp.967-974

[7] Gu, G., Perdisci, R., et al. "BotMiner: Clustering analysis of network traffic for protocol-and structure-independent botnet detection", 17th conference on Security symposium, 2008, pp. 139-154

[8] Jose Nazario and Holz, T., "As the Net Churns: Fast-Flux Botnet Observations", 2008 3rd International Conference on Malicious and Unwanted Software(MALWARE), pp. 24-31

[9] Binsalleeh, H., "On the Analysis of the Zeus Botnet Crimeware Toolkit", 2010 Eighth Annual International Conference on. IEEE, 2010, pp.31-38

[10] Falliere, Nicolas, and Eric Chien, "Zeus: King of the Bots.", Retrieved from Security Response Whitepapers Symantec Corp, 2009. [online] http://www. symantec. com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots. pdf

[11] A. Al-Bataineh and G. White, "Analysis and detection of malicious data exfiltration in web traffic", Malicious and Unwanted Software (MALWARE), 2012 7th International Conference, p26 - 31

[12] Lesne, A., "Shannon entropy: a rigorous mathematical notion at the crossroads between probability, information theory, dynamical systems and statistical physics." (2011).

[13] Pharwaha, Amar Partap Singh, and Baljit Singh, "Shannon and Non-Shannon measures of entropy for statistical texture feature extraction in digitized mammograms", Proc World Congress Eng Computer Sci. Vol. 2. 2009, pp. 1-6

[14] 彭士家, "Botnet Victim Detection and Notificationbased on Openflow Switch", 國立中央大學資訊工程所碩士論文 民國 99 年

[15] 黃勝獅, " Botnet Traffic Analysis and Dectection by Using OpenFlow Switch", 國立中央大學資訊工程所碩士論文 民國 100 年

[16] 趙亞略, "DEH: Dynamic Extensible Two-way Honeypot", 國立中央大學資訊工程所碩士論文 民國 101 年

[17] Raghava, N. S., Divya Sahgal, and Seema Chandna, "Classification of Botnet Detection Based on Botnet Architechture" Communication Systems and Network Technologies (CSNT), 2012 International Conference on. IEEE.

[18] 銳傑科技威脅通報[online] http://www.eranger.com.tw/virus.php?v_id=811

[19] A Brief Look at Zeus/Zbot 2.0[online] http://www.symantec.com/connect/blogs/brief-look-zeuszbot-20

基於 OpenFlow 交換機之跨雲端安全管理機制研究

陳奕明　　朱永彤
國立中央大學資訊管理學系
cym@cc.ncu.edu.tw
100423052@cc.ncu.edu.tw

摘要

在跨雲端環境，使用者及雲端供應商可以對不同雲端上的資訊進行存取，然而隨之而來的則是必須面對資訊洩露和資訊安全政策等更多的挑戰，跨雲端環境下，封包轉送須經過網際網路，若缺少妥善的安全機制，很可能遭到攻擊者竊聽封包，另外也須確保使用者所接收資訊符合自訂安全政策。現有網路設備及協定在跨雲端來臨下已顯不敷使用，也因此 OpenFlow 成為研究重點。OpenFlow 於跨雲端安全管理之相關研究尚未多見，本篇希望以 OpenFlow 實現跨雲端安全管理機制，以 OpenFlow 建構出跨雲端運算的環境；結合 Secure in-packet Bloom Filter，將轉送路徑資訊儲存於跨雲端銜接的路徑節點及封包中，在進行跨雲端傳送時，得以隱藏雲端內部資訊，避免資訊洩漏；同時也可利用 OpenFlow 達到使用者自訂的安全控制，符合跨雲端運算的安全需求。

關鍵詞：跨雲端, OpenFlow, Secure in-packet Bloom Filter

1. 緒論

雲端運算的蓬勃發展，目前已經有許多服務及技術在其上成形，許多的雲端供應商則以各自的技術提供了多樣的服務選擇[1]。根據美國國家標準技術研究所(National Institute of Standards and Technology)[2]的定義，依照雲端運算環境的部署方式將其分為三種：私有雲、公有雲及混合雲。混合雲結合了公有雲及私有雲的好處，透過將兩個或以上的雲端設施互相連結，並根據其相關技術及協議達到彼此的互通。在這種架構下，企業可以將一部份資訊工作交給其他雲端，而保留核心部分在組織內部。如此，企業使用者可能會在不同的雲端上存取資訊，例如奇摩(Yahoo) 會去租用新聞雲、氣象雲的資料，因此跨雲端運算的環境及服務已逐漸成形。在跨雲端環境中，必須讓使用者及雲端供應商將不同雲端上的資訊互相存取和使用，然而，隨之而來的可能是資訊洩露及資訊安全控制的挑戰。隨著雲端環境互動的增加，將會帶給雲端使用者和服務供應商在安全上的挑戰[3][4]。

隨著雲端環境轉型為跨雲端環境，在安全性的考量也成為我們必須要注意的焦點，如圖 1 所示為跨雲端運算的安全需求[3][4]。在跨雲端環境的傳輸，必須要能確保發送端到目的端所經過的網際網路(Internet)的安全性，因為一般封包路由都是基於 TCP/IP 協定技術，難保會遭到有心人士擷取封包導致網路攻擊發生。

使用者的傳輸資料，為了要都能符合合格的資訊安全政策，必須允許使用者控制雲端運算安全機制的運作，例如使用者的安全政策之一是要防止分散式阻斷服務攻擊(Distributed Denial of Service, DDoS)，對於接收的資訊則必須加上額外的過濾器做檢查，以免雲端內之機器遭到攻擊而導致服務中斷。在此情況下，系統必須允許使用者可在資訊流的路徑上加入 MiddleBox (例如入侵偵測系統、防火牆等)，對接收資訊進行過濾或檢查。

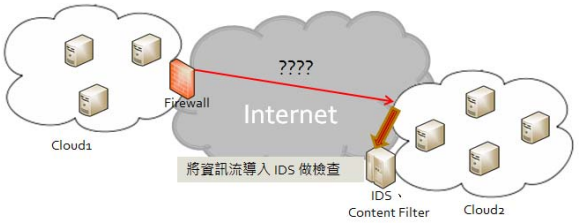


圖 1 跨雲端安全問題

除了上述的安全需求，跨雲端運算的環境中，也有效能上的需求[5]，下面為相關的描述：

(1) 流量需求的增加(Traffic between clouds)：

要能夠應付跨雲端之間增加的流量需求，因為在未來跨雲端運算環境的通訊流量會不斷地增加。

(2) 最小延遲(Minimum delay)：

隨著跨雲端環境擴大，其也會包含各種不同的雲端設施及服務，而有些服務可能會需要即時(real time)的溝通，所以即時通訊可能是必不可少的。

(3) 流量控制(Traffic control)：

跨雲端環境中包含有許多雲端設施，因此在傳輸封包時，不屬於通信兩端之網通設備、實體機器及使用者，就不應該收到封包，以免造成流量上的浪費或是安全疑慮。

近年來，面對不斷快速增高的網路需求，現有網路設備已瀕臨硬體傳輸效能的極限[6]，在跨雲端運算環境更顯不敷使用。因此，OpenFlow 已逐漸成為近年研究的重點項目。美國史丹佛大學所開發的 OpenFlow，已成功幫助 Google 處理急遽升高的網路流量需求，Google 將其佈署在跨雲端資料中心網路後，資訊傳輸流量不斷被擴大及優化[7]。本研究將使用 OpenFlow Switch 搭建出跨雲端環境，然而 OpenFlow 並未強調其安全性，因此我們將針對前述兩項安全需求，結合 OpenFlow 和 Secure in-packet Bloom Filter 方法，希望可以建構出跨雲端

環境的安全管理機制，同時利用 OpenFlow 來滿足跨雲端高速運算需求。

本篇後續章節如下：第二節探討本篇選用背景技術及相關研究；第三節描述系統的設計與架構；第四節為實驗與討論；第五節為結論及未來方向。

2. 相關研究

本節針對本篇所使用之相關技術進行探討，分別介紹 OpenFlow 專案與適用於跨雲端封包傳輸之 LIPSIN 和 Secure iBF 方法。

2.1 OpenFlow Switch

OpenFlow 可以讓研究人員測試自己設計的協定或政策，它是軟體定義網路的實現，將過去統一由設備執行的路徑控制與封包傳輸功能區分，讓路徑規劃以安裝 OpenFlow 控制軟體的控制伺服器（Controller）來進行，而封包傳輸則由 OpenFlow 交換器來執行。其以開放式網路管理架構來提高網路效能與彈性應用需求，協助網路管理員或服務供應商更為精確的網路管理能力。

OpenFlow 主要是透過 Controller 去管理底下的每台電腦的封包傳遞，OpenFlow Switch 主要包含了 Flow Table 以及 OpenFlow 相關軟體，Flow Table 負責封包查詢(Lookup)以及轉送(Forwarding)，其中的每個條目(Flow entry)都由表頭(Header)、統計資訊(Counter)以及對應動作(Action)所組成，表頭是用來比對封包用，包含有十個欄位。統計資訊用來維持此 Flow 的統計資訊。對應動作則指出符合此 Flow 的封包所應該做的動作；而 OpenFlow 相關軟體則負責與控制器(Controller)利用安全性通道(Secure Channel)互相交換資訊。

2.2 NOX – An OpenFlow Controller

NOX[8]為 OpenFlow 的控制器，當 OpenFlow Switch 面對未知流量時，NOX 控制器決定該流量的對應處理方式。

圖 2 為 NOX 網路組件圖，包含一台伺服器上安裝 NOX 軟體以及連接數台 OpenFlow Switch，使用者和網路管理者可以在 NOX 控制器上對底下任何一台 Switch 設定封包流向或是管理規則；其之上的管理元件(APP)，可以讓使用者自行選用或添加，根據需求設計控管策略或加入需要的功能或協定。

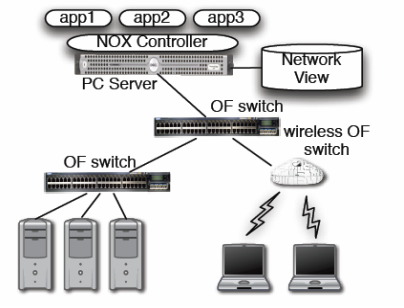


圖 2 NOX 網路組件圖

2.3 LIPSIN

LIPSIN(Line Speed Publish/Subscribe Inter-Networking)[9]為一個新興的多播轉發架構，很適合用在跨雲端傳輸中，它的運作機制是使用識別鏈結(Link)來取代節點，首先利用布隆過濾器的格式對每一個鍊結賦予一獨特鏈結編號(LinkID)，長度為 m 個位元(bit)長且其中的 k 個位元設為 1。LIPSIN 拓樸系統利用這些 LinkID 及可連接性的資訊，建立網路拓樸，如圖 3 示意。

圖 3 LIPSIN 網路拓樸及封包轉發

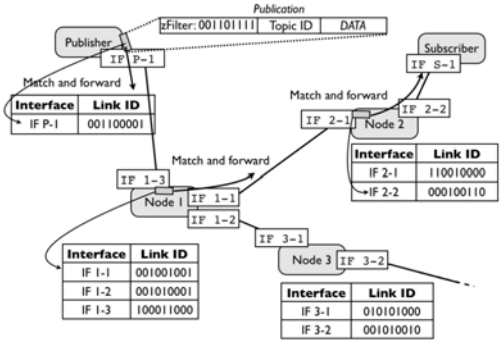


圖 3 為轉發示意，此情境中 Publisher 欲發送封包至 Subscriber，因此拓樸元件會生成轉送封包所需的 zFilter，而轉送路徑為透過 IFP-1、IF1-1 及 IF2-2 轉送，因此將路徑上 LinkID 利用二進制 OR 合併成為此轉送路徑的 zFilter。當各個轉送節點接收到封包時，便透過二進制 AND 比較 zFilter 和 LinkID 決定其傳出介面，演算法如圖 4 所示。

圖 4 LIPSIN 轉發演算法

Algorithm 1: Forwarding method of LIPSIN

Input: Link IDs of the outgoing links; zFilter in the packet header

foreach *Link ID of outgoing interface* **do**
  if *zFilter & Link ID == Link ID* **then**
    Forward packet on the link
  end
end

2.4 Secure in-packet Bloom Filter

LIPSIN 不具有管理機制，LinkID 一經決定好後就不會再更新，每個轉送節點都會紀錄一個固定的對映表。如此，攻擊者可能就可以偽造合法地 zFilter 對特定路徑注入流量或是以暴力法去分析破解 zFilter 進行攻擊。為了避免上述安全疑慮，Ghani [10][11] 提出 Secure in-packet Bloom Filter(SiBF)方法，又稱為 z-Formation。其方法設計上皆與 LIPSIN 的概念一致，唯其加入了加解密金鑰來動態計算 LinkID 和 zFilter，如圖 5 所示。

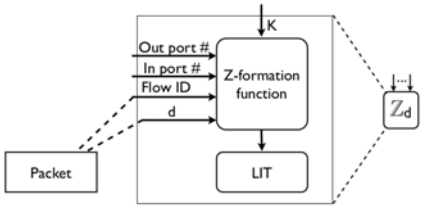


圖 5 Secure iBF function

比 LIPSIN 方法安全的原因是因為解密金鑰是由發送端發送的，只有指定的轉送點才有解密金鑰，當金鑰改變時，計算出來的資訊就會不同，也就是說 LinkID 是會變動的，zFilter 值也會跟著不同(依據金鑰不同而改變)，這種方式提供了更安全的保障(隱匿性)。

3. 系統設計與架構

3.1 目標

本篇目標為建立一適用於跨雲端的安全管理機制，因此針對以下兩點作為目標：1. 資訊加密：對封包進行加密，將封包內儲存之雲端內部資訊、位址加以隱蔽，避免成為攻擊者目標，使攻擊者僅能獲取有限的資訊，難以竊聽封包獲得雲端內部之相關資訊。2. 安全控制：讓使用者參與安全控制，允許使用者在雲端出入口加入 MiddleBox，在跨雲端傳送時將資訊流轉向做檢查，檢查後的正常資訊才可進入雲端內部。

3.2 系統架構

現有的研究方法中，於跨雲端運算皆有其不足之處，本篇提出的架構希望以截長補短的方式建立適用於跨雲端運算的系統架構。NetFPGA 搭建的 OpenFlow Switch 可以加速 Flow Table 查詢；透過控制器，方便建立跨雲端的網路拓樸及決定封包轉送路徑；金鑰則可透過控制器管理及向轉送路徑上的 OpenFlow Switch 進行分派；資訊加密方面，可利用 zFilter 將雲端內部及轉送資訊進行加密；安全控制方面，使用者則可以透過控制器，依需求對 OpenFlow Switch 制定安全政策。

依據上面描述，本篇之系統將以 OpenFlow 作為基底，圖 6 為 OpenFlow 網路示意圖，在各個雲端出入口皆放置一台 OpenFlow Switch，彼此之間透過網際網路連接，系統將結合 OpenFlow 和 SiBF 方法以達到資訊加密，保障在跨雲端傳輸時雲端內部之安全。而所有 OpenFlow Switch 皆透過 OpenFlow Protocol 接受一 NOX 控制器集中管理。

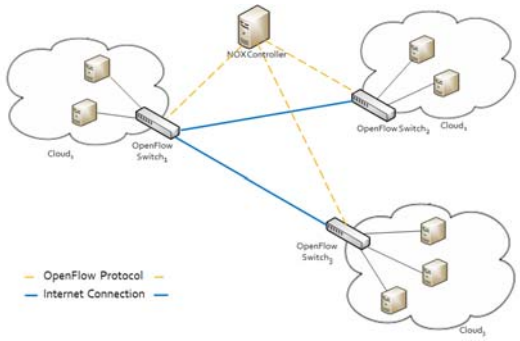


圖 6 OpenFlow 跨雲端網路示意

3.3 NOX 控制器

文獻中 zFilter 的生成倚靠的是其拓樸元件，在 OpenFlow 網路是透過 NOX 控制器集中管理底下所有的 OpenFlow Switch，因此適合用以維護網路拓樸、計算轉送路徑和產生 zFilter 及 LinkID，下面為相關功能描述：

(1) 建立 OpenFlow 網路拓樸：網路拓樸資訊用以作為封包轉送路徑的計算，NOX 控制器可透過發送封包探勘底下網路設備之連接資訊，建立 OpenFlow 網路拓樸。

(2) 找出封包轉送路徑：封包轉送路徑可藉由 NOX 控制器預設的 OSPF 路徑演算法進行計算。

(3) 產生 LinkID、zFilter：前項動作完成後，將路徑上所有 LinkID 進行二進制或(OR)，再以加密金鑰 K 進行 XOR 加密後作為轉送 zFilter。

(4) 回傳 LinkID、zFilter：LinkID 與 zFilter 的產生與回傳，皆是由 OpenFlow Protocol 來傳遞。NOX 發送命令寫入 LinkID 和 Key 至轉送節點上，以及將 zFilter 經由 OpenFlow Switch 再轉交至使用者。

3.3 OpenFlow 交換機

為了使 OpenFlow Switch 符合本篇之設計，能適用於跨雲端運算環境之中，下述為新增的功能：

(1) 增加 OpenFlow Switch 對 zFilter 的判斷：在接收到封包時，先提取封包標頭，將 zFilter 進行 XOR 運算解密後，再進行 Flow Table 查找，將儲存的 LinkID 與 zFilter 進行二進制 AND 後再依據結果對應之 actions 處理封包。

(2) 依據 Flow Table 查找結果進行對應動作：根據封包內 zFilter 與 LinkID 進行比對，比對後將封包透過指定介面傳出。

3.4 LinkID 與 zFilter

LinkID 與 zFilter 都在 NOX 控制器中完成，LinkID 產生方式為將一 64 位元變數，0 至 31 位元儲存來源端 IP 位址，32 至 63 位元儲存目的端 IP 位址，再用雜湊函數計算儲存位址，將變數中儲存位元設為 1 做為轉送路徑 LinkID。

zFilter 產生方式為將轉送路徑上所有的 LinkID 進行二進制或(OR)，再與金鑰(Key)進行邏輯異或(XOR)合併產生。

3.5 Flow Table

Flow Table 其上儲存的條目(Flow entry)比對項目僅為 LinkID 而行動(Action)為指定封包傳出介面。表 1 為 OpenFlow Switch 的 Flow Table 示意。

表 1 Flow Table 結構表

LinkID	Action
	Output:interface
10000100000001010101010010101010	1
10000100000001010101010011111111	2
00000100101000101110111010101101	3
00000000100000000001000000000000	4

3.6 系統運作流程

本節以情境闡述本篇系統運作流程。

3.6.1 網路拓樸更新

於文獻中，zFilter 的生成需仰賴拓樸系統，而在 OpenFlow 網路中，可利用集中控制的網路控制器來定期更新網路拓樸，以取得最新的封包轉送路徑。圖 7 為此情境之示意圖。其運作步驟如下：1.NOX 控制器對網路底下的 OpenFlow 設備送出 LLDP (Link Layer Discovery Protocol)探勘訊息。2.OpenFlow Switch 接收到訊息後會在傳遞此訊息至所連接設備，取得其連接情形。3.探勘完畢後，OpenFlow Switch 將探勘資訊回傳至 NOX 控制器，由控制器建立目前最新的網路拓樸。

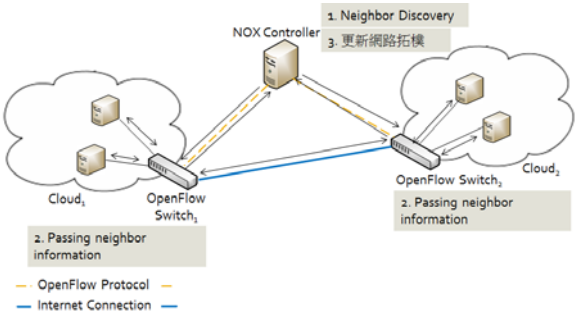


圖 7 OpenFlow 網路拓樸更新流程

3.6.2 LinkID 和 zFilter 值產生

本節假設於 OpenFlow 網路中，NOX 控制器已取得了最新 OpenFlow 網路拓樸，而使用者 $User_1$ 與 $Host_{1,1}$ 需取得彼此之間通訊所使用的 zFilter，圖 8 為此情境示意圖。步驟如下：1. $User_1$ 透過 OF $Switch_2$ 提出至 $Host_{1,1}$ 之間進行傳輸的 zFilter 要求。2. OF $Switch_2$ 將此要求轉送至 NOX 控制器。3. NOX 控制器根據網路拓樸找出可用之封包傳輸路徑，擇定具最小網路時延之 OpenFlow Switch 作為轉送端，於此情境中選擇了 OFS_2、OFS_1 作為轉送路徑。4. NOX 控制器將針對 OFS_2、OFS_1 更新其 Flow Table，生成 LinkID 及 zFilter($Host_{1,1}$,$User_1$)及指定 OF Switch 該使用哪個介面傳出封包。5. NOX 控制器計算出 LinkID，將路徑上所有 LinkID 進行二進制或(OR)，再與密鑰 K 進行邏輯異或(XOR) 生成 zFilter，將 K、LinkID 寫入至 OFS_1、OFS_2，並將 zFilter 經由 OFS_1 轉交至 $Host_{1,1}$ 完成 zFilter 產生流程。

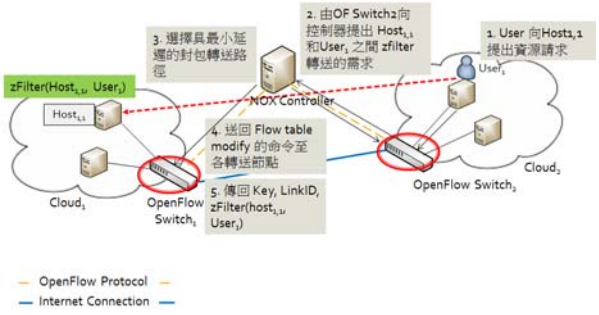


圖 8 zFilter 值產生流程圖

3.6.3 轉送封包

完成 zFilter 產生流程之後，此時 $Host_{1,1}$ 已可使用 zFilter 來完成與 $User_1$ 之間的通訊需求。圖 9 為此情境示意圖。步驟如下：1.$Host_{1,1}$ 將 zFilter 插入封包標頭中，傳送至 OFS_1。2.在此前 NOX 控制器已先將密鑰 K 及 LinkID 寫入至各轉送節點，OF $Switch_1$ 接收到封包後，提取封包 zFilter 值並與 K 進行邏輯異或(XOR)運算解密，接著進行 Flow Table 查詢，將儲存之 LinkID 與 zFilter 進行二進制 AND 運算後，依據結果依對應 actions 由指定介面傳出。3.OF $Switch_2$ 接收到封包後，同樣進行 zFilter 解密、Flow Table 查詢，比對 LinkID 與 zFilter 結果後依對應 actions 由指定介面傳出。4. $User_1$ 接收到封包，完成封包傳送。

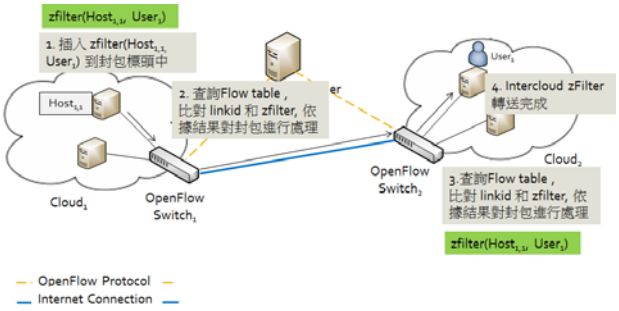


圖 9 封包轉送流程

3.6.4 安全規則制訂

使用者或公司行號於跨雲端環境進行運時，可能會面臨到不同的雲端彼此安全政策不一的形，使用者將無法確保自己的個人資訊，不會在雲端通訊時不經意的洩露。因此對於安全政策的統整管理可以利用 NOX 控制器對各個雲端出入口之 OpenFlow Switch 增設安全政策管理機制，使用者可依據需求去添加 MiddleBox 以符合安全規則。圖 10 為此情境示意圖。步驟如下：1.由控制器寫入規則指定接收封包的處理，須先由 Middle Box 做檢查。2.$Host_{1,1}$ 發送封包，OF $Switch_2$ 提取封包 zFilter 值並與 K 進行邏輯異或(XOR)解密，接著進行 Flow Table 查詢，將儲存的 LinkID 與 zFilter 進行二進制 AND，依據結果依對應 actions 由指定介面傳出。3.OF $Switch_1$ 接收封包後，依據 Flow Table 規則，將封包導向至 Middle Box，依據安全規則檢查封包，如果是不合法的內容則阻擋掉。4.正常封包再回傳至 OF $Switch_1$，再由 OF $Switch_1$ 轉送至目的端。

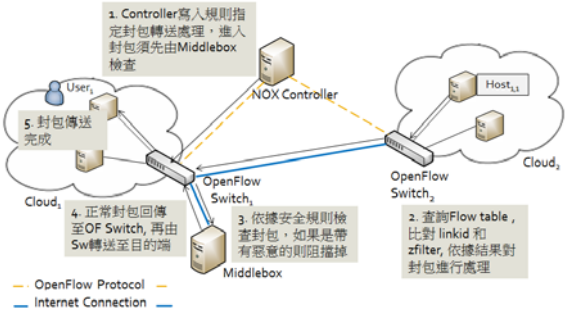


圖 10 自訂安全規則流程

4. 實驗與討論

本節以 SiBF 封包轉送、封包轉向至 MiddleBox 檢查兩項實驗評估系統可行性，來進行探討。

4.1 實驗環境

實驗環境如圖 11，依據第三章的系統架構及流程，分別架設了以下伺服器，兩台 Switch 皆連接到相同的控制器，OpenFlow Switch$_1$ 底下連接了一台 MiddleBox 主機用作封包轉向和過濾的測試。

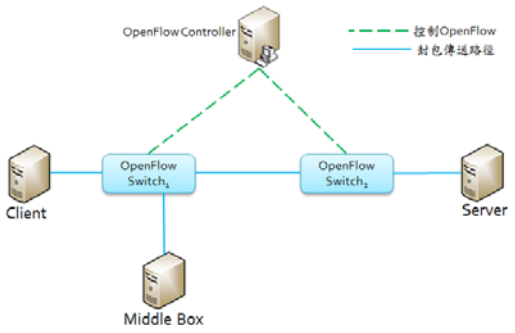


圖 11 實驗系統架構

4.2 系統架設及操作

OpenFlow Switch 及 NOX Controller 依照官方教學架設完成後，即可建立連線及開始測試，如圖 12。

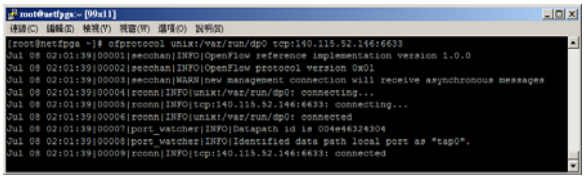


圖 12 OpenFlow 與控制器建立連線

4.3 封包轉送

4.3.1 NOX 程式流程圖

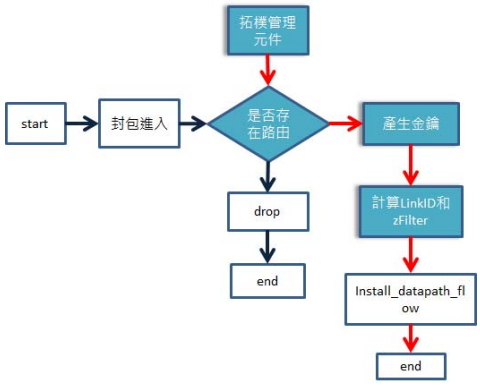


圖 13 程式流程圖

我們的目的是透過 LinkID 和 zFilter 來進行封包轉送，由 NOX 控制器負責計算和寫回 OpenFlow Switch，由 OpenFlow Switch 判讀接收的封包及轉送。圖 13 為 NOX 程式流程圖。白色的方塊是原有的程式，藍色的部分是新增上去的。新增的功能為管理及維護網路拓樸，當有封包進入後，會先找出封包轉送路徑，再產生加密金鑰計算 LinkID 和 zFilter，完成後透過 install_datapath_flow 將資訊寫回 Switch 上。而金鑰管理的部分，我們亦加入了時間參數，每 60 分鐘將進行金鑰的更新。

4.3.2 於 OpenFlow 轉送端上的處理

在 OpenFlow Switch 上要新增的功能為，查找 Flow Table 時，將 zFilter 值與 Key 作邏輯異或(XOR)，以及 zFilter 和 LinkID 做 AND 運算比較，此部份我們將修改原有的程式來達成此功能。

4.3.3 將封包轉向

要使封包轉向我們可以利用 OpenFlow Switch 提供的 dpctl 工具來新增、修改 Flow。我們要使得接收所有封包皆導向至連接的 MiddleBox 進行過濾，設定的指令範例如下：dpctl add-flow nl:0 in_port=1, actions=output:2。使得只要是來自這個網卡的封包，一律由 port2 出去，而 port2 底下所連接的是 MiddleBox，可以檢查封包。封包檢查完後會再回傳至 Open Flow Switch 上，由 Switch 進行 Flow Table 查找後再轉送封包至正確的目的端。

4.4 實驗一 SiBF 封包轉送

此實驗目的為針對 OpenFlow 結合 SiBF 方法後對封包轉送的功能進行測試，實驗中將運行兩台 OpenFlow Switch 和 NOX 控制器並進行連接，再透過 Server 向 Client 發送測試封包，並觀察其結果。

實驗採用的測試工具是 Colasoft 的 Packet Builder。Packet Builder 可以製造出 TCP、IP、ARP 封包，並且可以設定封包播送間隔及數量。我們以 Packet Builder 發送 1000 個封包，設定為 1 秒發送一次。發送完封包後，在 OpenFlow Switch 主機端打入指令查看封包統計，驗證封包是否正確從 Switch 轉送出去，以及使用 Wireshark 監聽封包轉送情形。

如圖 14 為 Switch 端之封包統計，而接收的封包數量不止 1000 個的原因是因為在 NOX 控制器上運行了 of_monitor 元件，該元件會定期地發送 LLDP 封包對底下連接的設備進行探勘，以保持最新網路拓樸。所以在 Switch 端查看封包統計時會有小量的額外封包。



圖 14 Switch 端封包統計

除了查看 Flow Table 的封包流量統計外，我們在以 Wireshark 查看封包轉送時的情形，以下為 Wireshark 監聽到的封包，tap0 即為 Switch 端，封包在轉送時會以 zFilter 取代封包 IP 資訊作為轉送的判讀資訊，可看到 IP 欄位是空的，如圖 15。

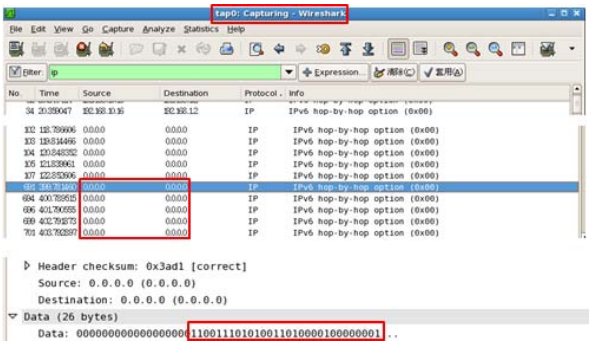


圖 15 Wireshark 監聽封包的情形

4.5 實驗二封包轉向至 MiddleBox

我們要讓封包在進入時被導到 MiddleBox 做檢查，在 MiddleBox 主機上同時有 eth1 和 eth2 兩張網卡，由 eth1 網卡去接收來自 OpenFlow Switch 的封包，eth2 則將過濾後的封包轉送回 Switch。MiddleBox 以安裝 Snort 及安全分析引擎（Basic Analysis and Security Engine, BASE）進行測試，而 Snort 主機為了考量安全性，避免遭受外部攻擊，因此以橋接(bridge)的方式將 eth1 和 eth2 連結，並不指定 IP，如此可避免 IP 資訊洩漏所導致的安全疑慮。接著由 PC2 使用 Nmap 掃描工具對 PC1 進行掃描，驗證是否可將封包流轉向至 Snort，並且進行攻擊來源主機的阻擋。當掃描完成後，如圖 16 查看 Snort 主機上的安全分析引擎可看到確實有封包進入。

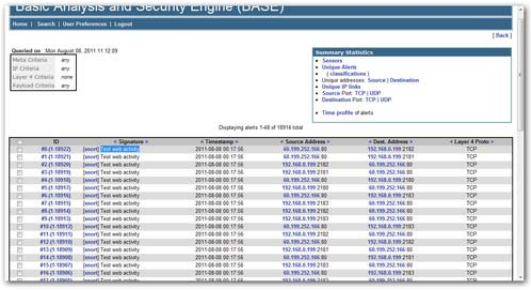


圖 16 封包紀錄至 BASE 資料庫

另外 Snort 也會記錄此 IP，並把 IP 傳遞至 iptables 的規則內，寫入一條新規則阻擋此來源位址的封包，如圖 17 所示。

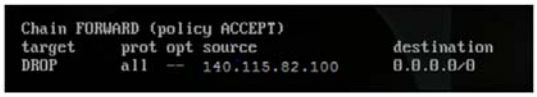


圖 17 iptables 阻擋攻擊主機

4.6 實驗結果討論

透過實驗證實了我們可以透過 NOX 控制器和 OpenFlow Switch 來控制封包的流動，我們可以利用 NOX 控制器找出轉送路徑及計算 zFilter 和 LinkID 並寫回 OpenFlow Switch 上，而在 OpenFlow Switch 也可以正確地透過 zFilter 轉送封包。也可以利用 OpenFlow Switch 將封包導向至 MiddleBox，達到封包過濾以及阻擋攻擊，保護雲端內部安全的目的。

5. 結論及未來研究

本篇所設計的系統結合了 SiBF 方法增強了 OpenFlow 於跨雲端上安全性，透過 zFilter，將封包轉送資訊加密避免雲端內部資訊洩漏，避免竊聽的攻擊。而對於使用者安全政策的統整管理則是利用 NOX 控制器對各個雲端出入口之 OpenFlow Switch 增設安全政策管理機制。使本篇系統更適於跨雲端環境之應用。

未來研究主要可往下列幾個方向：1.使用者會依不同需求配置不同的 MiddleBox，因此之後可測試更多的 MiddleBox 主機，評估是否適用於 OpenFlow 搭建的跨雲端網路中。2.只有一台控制器控管底下所有 OpenFlow Switch 可能會有效能上的問題，因此可將系統架構改為每一雲端皆有一台控制器控管雲內部，而所有控制器再交由一台集中控制器來掌管，負責對路徑、流量進行調配。未來若要整合不同地區的雲端設施，可嘗試將其改良為此種架構。3.對系統進行壓力測試，探討在高流量的運算需求下，是否能達到良好的效能表現，以及將封包轉向至 MiddleBox 檢查時，會不會因流量過大導致誤報或是遺失封包的情形，這是未來研究目標。

參考文獻

[1] 如何建構企業專屬的雲端運算平台,2010 年取自http://www.ringline.com.tw/

[2] Mell, Peter, Timothy Grance, "The NIST Definition of Cloud Computing (draft).", NIST special publication 800: 145, 2011

[3] Chen, Shiping, Suya Nepal, Ren Liu. "Secure Connectivity for Intra-Cloud and Inter-Cloud Communication", Parallel Processing Workshops (ICPPW), 40th IEEE International Conference on, 2011

[4] Kretzschmar, Michael, Mario Golling, Sebastian Hanigk. "Security Management Areas in the Inter-Cloud.", Cloud Computing (CLOUD), IEEE International Conference on, 2011

[5] Dayananda, M. S., Ashwin Kurmar. "Architecture for inter-cloud services using IPsec VPN." Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on. IEEE, 2012.

[6] McKeown, Nick, et al., "OpenFlow: enabling Innovation in Campus Networks.", ACM SIGCOMM Computer Communication Review 38(2): 69-74, 2008

[7] Google Sets New Internet Traffic Record, 2010 年取自 http://ddos.arbornetworks.com/2010/10/google-breaks-traffic-record/

[8] Gude, Natasha, et al., "NOX: towards an operating system for networks.", ACM SIGCOMM Computer Communication Review 38(3): 105-110, 2008

[9] Jokela, Petri, et al., "LIPSIN: line speed publish/subscribe inter-networking.", ACM SIGCOMM Computer Communication Review, 2009

[10] Ghani, A. and P. Nikander, "Secure in-packet Bloom Filter forwarding on the NetFPGA.", Proceedings of the European NetFPGA Developers Workshop, 2011

[11] Rothenberg, Christian Esteve, et al., "Self-routing Denial-of-service resistant capabilities using in-packet Bloom filters.", Computer Network Defense (EC2ND), 2009 European Conference on, IEEE 2009

Min-Max可逆式資料隱藏技術之安全性分析
Steganalysis of Min-Max Reversible Data Hiding Technique

林志麟 [1]
陸軍官校資訊系 [1]
davelin040@gmail.com [1]

胡宸浩 [2]
空軍航空技術學院航空通電系 [2]
chenhao.hu@gmail.com[2]

婁德權 [3*]
長庚大學資訊工程學系 [3*]
dclouprof@gmail.com [3*]

摘要

一般資料隱藏技術發展歷程中，鮮少考慮掩護媒體(Cover-Media)在機密資料嵌入後，遭受破壞的程度，故此類不可逆性資訊隱藏技術並不適用於軍事、情報及醫療影像。Tian 在 2003 年運用差值擴張法(Difference Expansion)提出可回復式資訊隱藏技術則可有效解決此一問題。2008 年 Lin 與 Hsueh 運用三個像素區塊來增加可回復式資訊隱藏技術的藏密量，但其對偽裝媒體的影響稍大，致可能影響其不可察覺性。2009 年 Hsiao 等人提出區塊為基礎的可回復式資訊隱藏技術，初步提升改良前述方法的 PSNR 值，惟提升的幅度亦有限。2010 年 Yang 與 Hu 提出一個基於 Min-Max 演算法之可回復式資訊隱藏技術，並加入係數調整的過程使得其在不可察覺性此一特徵有明顯的進步。考量當資訊隱藏技術遭違法人士濫用時，此一機密訊息傳遞技術勢必形成安全防護上的死角。因此本文即是以資訊隱藏技術之安全性分析為出發點，探討 Yang 與 Hu 提出之基於 Min-Max 演算法之可逆資料隱藏技術之優缺點，並初步說明可逆性資訊隱藏偵測技術的偵知與未來發展方向。

關鍵詞：可逆式資訊隱藏、資訊隱藏分析、Min-Max 演算法、χ^2 偵測、直方圖偵測。

Abstract

The changing of cover-media after embedding secret message is rarely considered in data hiding processes, such data hiding technology is not applicable to military, intelligence and medical imaging. In 2003, Tian proposed reversible data hiding technology using the difference expansion method and solve this problem effectively. In 2008, Lin and Hsueh used three pixel blocks to increase the embedding capacity of data hiding technology, but it make the larger impacts and decrease the imperceptible of cover media. In 2009, Hsiao *et al.* proposed reversible data hiding technology based on block to enhance the improvement of the foregoing methods initially PSNR value, but its enhancement also limited. In 2010, Yang and Hu proposed Min-Max reversible data hiding algorithm that adjusting the coefficients of blocks and getting better imperceptible. If the data hiding technique is abusing offenders, this confidential messaging technology will inevitably result in security on the corner. This paper analyzed the security of Min-Max reversible data hiding technology and trying to explore its advantages and disadvantages. Steganalysis and some future developments are also describe in this paper.

Keywords: *Reversible information hiding, steganalysis, Min-Max algorithm, χ2 detection, histogram detection.*

1. 前言

鑑於近年來資訊科技與網際網路的倍速發展趨勢，促使數位資料可不受時空限制，快速且便利地傳達至世界上任一地點，但隱藏著潛在的資訊安全疑慮與問題。植基於數論基礎的現代密碼技術雖可保障機密訊息傳遞時安全性，卻無法避免訊息傳遞過程遭人窺視之問題。資訊隱藏(Information Hiding)技術的發展與應用，使得人們可以將機密訊息嵌入於網際網路常見多媒體資料中，再用正常方式進行傳遞。不僅能提供訊息傳送雙方一個安全的通訊管道，亦可確保機密訊息得以不受攻擊者竊取、冒用與窺視，故資訊隱藏技術成為資訊安全領域中相當熱門的研究領域。

一般資料隱藏技術研究人員並未考慮掩護媒體(Cover-Media)在機密資料嵌入後，會遭受相當程度的破壞，故在訊息取出後，並無法還原成原來的形態。故此類不可逆性資訊隱藏技術並不適用於軍事、情報及醫療影像。Tian [6]在 2003 年運用差值擴張法(Difference Expansion)提出可回復式資訊隱藏技術則可有效解決此一問題。但 Tian 所提方法將因像素值溢位與複雜邊緣等問題而需要加入額外紀錄資訊，使其可藏容量稍嫌不足。

2008 年 Lin 與 Hsueh 運用三個像素區塊來增加可回復式資訊隱藏技術的藏密量，但其對偽裝媒體的影響稍大，致可能影響其不可察覺性。2009 年 Hsiao 等人提出區塊為基礎的可回復式資訊隱藏技術，初步提升改良前述方法的 PSNR 值，惟提升的幅度亦有限。2010 年 Yang 與 Hu [10]提出一個基於 Min-Max 演算法之可回復式資訊隱藏技術，另加入係數調整過程，使得其在不可察覺性與藏密量間取得較佳的平衡。

早在 2001 年 2 月美國 USA Today 報導中指出，1998 年東非美國大使館的恐怖炸彈攻擊事件中，恐怖份子疑似運用網站聊天室及成人貼圖網站當作媒介，將恐怖行動之指令及攻擊目標資訊嵌入

於圖片後，有效躲避各國情治單位的查核。而前述恐怖攻擊行動的首領，正是策劃 2001 年美國「911 恐怖攻擊事件」的奧薩瑪・賓拉登。而 2012 年賓拉登伏法及蓋達組織勢微後，執法單位在蓋達組織查獲的資料中發現，有大量攻擊計畫與資料被隱藏在色情影片，並以偽裝資料運用網路傳遞給組織成員。此間所透露出來的訊息，顯示了人們早時擔憂確實是其來有自，當資訊隱藏技術遭受違法人士的濫用時，此一保障個人隱私安全之機密訊息傳遞技術則將成為許多罪犯用以逃避檢調單位查緝的訊息傳遞工具，勢必形成安全防護的死角。因此，資訊隱藏偵測技術(Steganalysis)發展則有其必要性。

本文即是以資訊隱藏技術之安全性分析為出發點，探討 Yang 與 Hu 提出之基於 Min-Max 演算法之可逆資料隱藏技術。下一章節將說明可回復式資訊隱藏技術及 Min-Max 演算法。其次將介紹資訊隱藏偵測技術。第四部份探討 Min-Max 演算法之偵測方式。最後提出我們的結論與未來發展方向。

2. 可回復式資訊隱藏與 Min-Max 演算法

2.1 可回復式資訊隱藏

可逆性資訊隱藏技術主要運用人類感官的侷限性，將機密訊息透過偽裝處理的方式來傳遞，除以避開不當的窺視、存取或攻擊外，亦可讓取出訊息後的掩護媒體，還原成原始之偽裝媒體。在吳汶涓教授所發表的"可逆性資訊隱藏技術之發展趨勢"一文中[11]，將此類技術區分為三個種類，分別為差值擴張(Difference Expansion, DN)、直方圖位移(Histogram Shifting, HS)、與預測法(Prediction)。

2.1.1 差值擴張法(Difference Expansion)

Tian 在 2003 年提出之 DN 差值擴張技術係運用影像相鄰像素值間具有相似的特性[6]，以達到藏密的過程。傳送端首先將偽裝影像 I 區分為多個像素對，再逐一將像素對 Pi, Pj 的差值 d 及平均值 m 再將機密資料 s 藏於擴大後的差值 d'，最後計算出新的像素對 Pi'與 Pj'，再將所有的像素對組合成掩護媒體 C，整個嵌入步驟如式子(1)-(5)所示。

$$d = |Pi - Pj|, \tag{1}$$

$$m = \left\lfloor \frac{Pi + Pj}{2} \right\rfloor, \tag{2}$$

$$d' = 2 \times d + s, \tag{3}$$

$$Pi' = m + \left\lfloor \frac{d'+1}{2} \right\rfloor, \tag{4}$$

$$Pj' = m - \left\lfloor \frac{d'}{2} \right\rfloor. \tag{5}$$

接收端接收到藏密後的掩護媒體 C 後，可透過下列式子(6)-(11)取出內嵌機密 s 及原始偽裝影像 I。

$$d' = |Pi' - Pj'|, \tag{6}$$

$$s = d' \bmod 2, \tag{7}$$

$$d = \left\lfloor \frac{d'}{2} \right\rfloor, \tag{8}$$

$$m = \left\lfloor \frac{Pi' + Pj'}{2} \right\rfloor, \tag{9}$$

$$Pi' = m + \left\lfloor \frac{d'+1}{2} \right\rfloor, \tag{10}$$

$$Pj' = m - \left\lfloor \frac{d'}{2} \right\rfloor. \tag{11}$$

但 Tian 所提差值擴張方法可能會因取樣的像素值接近臨界 0 或 255 造成像素值溢位，因此其將像素值區分為可改變與不可改變兩類，另若取樣的像素對差異過大或是位於原圖複雜邊緣都將會使得影像品質嚴重降低。因此 Tian 又需將此類情況排除，鑑於前述 2 種須排除的嵌入狀況，DN 法須加入額外資訊以紀錄前述排除狀況，使得 DN 技術的藏密容量不到 0.5 bpp，可藏容量稍嫌不足。為了解決 DN 法的藏密量不足問題。

2004 年，Alatter 將多組像素值的向量組合取代 Tian 的像素配對方式[1]，並參考向量權重平均值來嵌入訊息，將整體藏密量提高至 0.75 bpp (bit per pixel)以上。2008 年 Lu 使用半字節配對方式，將每個像素切成兩個半節(Nibble)，並在相鄰像素的每個半節中分別藏入一個位元，將整體藏密量提高至 1 bpp。

2.1.2 直方圖位移(Histogram Shifting, HS)法

2006 年，Ni 等學者提出以統計概念完成可逆性資訊隱藏的技術[3]。此方法突破 Tian 的像素對藏密概念，而改以全圖像素統計特徵來進行藏密的方式。該方法將灰階偽裝影像 I 的所有像素值進行統計，並分別計算各別像素值的總數量，並繪製成直方圖(Histogram)。分別找出統計圖中出現次數最多的峰(Peak)值，及出現次數最少的零(Zero)值。將峰值與零值間的像素值位移出一個藏密位置，最後以藏密位元來判斷是否調整待藏密像素的像素值；遇 0 不調整，遇 1 則調整至藏密位置。如此會將藏密位置之像素值點數調整至大約等於峰值像素質點數的一半。

A. 藏密步驟

I. 統計偽裝媒體的像素直方圖，並找出其中的峰點 P 及零點 Z。

II. 將 P 到 Z 點間的所有像素值，向左($P<Z$)或向右($P>Z$)位移。

III. 依訊息 S 調整每個像素值等於 P 的數值。

i. $P>Z$，若藏入位元為 0，則像素值不變；若藏入位元為 1，則像素值減 1。

ii. $P<Z$，若藏入位元為 0，則像素值不變；若藏入位元為 1，則像素值減 1。

iii. 重複前述步驟，直至所有機密訊息都嵌入，並輸出掩護影像 S、峰值 P 與零值 Z。

B. 機密取出與偽裝影像復原步驟

I. 統計掩護媒體的像素直方圖，並依取得資訊找到峰點 P 及零點 Z。
II. 利用掩護影像的資訊來取出機密訊息。
  i. $P>Z$，若像素值為 P，則訊息為 0，若像素值為 $P-1$，則訊息為 1，並將像素值改回 P；
  ii. $P<Z$，若像素值為 P，則訊息為 0，若像素值為 $P+1$，則訊息為 1 並將像素值改回 P；
III. 重複前述步驟，直到所有機密訊息取出。
IV. 將 P 到 Z 點間的所有像素值，向左($P>Z$)或向右($P<Z$)還原回起始位置。

Ni 所提直方圖位移法若因找不到直方圖的統計零點，將無法進行藏密，此時可以統計值最低的像素值作為零點，另其整體的藏密量係以峰值像素點進行藏密，而此峰值像素的數量即為此法的藏密上限。2007 年，Hsieh 與 Tseng 等人提出一個峰點搭配兩個零點的直方圖改良技術，運用兩次直方圖位移，增強 Ni 藏密技術的可行性。2007 年 Fallahpour 與 Sedaaghi 提出區塊藏密方式改善 Ni 的直方圖位移藏密法的藏密容量偏低問題。

2.1.3 預測法(Prediction)

2004 年，Thodi [7]等人使用預測法產生之誤差來取代 Tian 方法的差值，其運用相鄰三個像素 Pa, Pb, Pc 來預測 Pi 的像素值，再使用差值擴張法將機密訊息嵌入於擴張後的預測差值中，將整體的藏密量提昇至 1bpp。預測公式：

$$\tilde{Pi}=\left\lfloor\frac{2\times Pa+1\times Pb+2\times Pc}{5}\right\rfloor,$$
$$Pj'=m-\left\lfloor\frac{d'}{2}\right\rfloor. \quad (12)$$

2009 年，Wu 使用 JPEG-LS 預測器，由於此預測器考量影像內容的邊走向，加上多基底的符號表示系統，可動態的提昇嵌入的訊息量。

2.2 Min-Max 演算法

Yang 與 Hu 為改善 Tian 等人提出可回復式資訊隱藏技術在不可察覺特性的不足[10]，故將機密訊息運用 Min-Max 演算法嵌入於空間域中，其次再運用頻率域係數調整(Coefficient-Bias)的方式來額外加入一個浮水印，可承受一般影像處理式的攻擊。該演算法運作方式說明如下。

A. 資料嵌入步驟
I. 將掩護影像區分為不重疊的影像區塊 P。
II. 設定控制參數 σ 及正乘數 k。
III. 計算區塊 P 的最大值 P_{max} 與最小值 P_{min}。
IV. 計算出可嵌入訊息的位置
  i. 若 $P_{min}\geqq 128$，則將區塊 P 所有像素 P_j 減掉 P_{min} 以得出暫存區塊 Q。
  ii. 若 $P_{min}<128$，則將區塊 P 所有像素 P_j 減掉 P_{max} 以得出暫存區塊 Q。
V. 若暫存區塊 Q 的像素值 $q_j\geqq$ 控制參數 σ，則將 q_j 加上 σ 得到 $q1_j$，並視為不可嵌入位置。
VI. 若暫存區塊 Q 的像素值 $q_j<$ 控制參數 σ，則將 q_j 乘上 k 以取得 $q2_j$，並依序嵌入訊息。
VII. 組合成偽裝媒體
  i. 若 $p_{min}\geqq 128$，則將暫存區塊 Q 所有像素 $q1_j$ 及 $q2_j$ 加上 P_{min} 以得到偽裝區塊。
  ii. 若 $p_{min}<128$，則將暫存區塊 Q 所有像素 $q1_j$ 及 $q2_j$ 加上 P_{max} 以得到偽裝區塊。
VIII. 重複執行步驟 I-VII，直到所有區塊完成。

表 1 為 Min-Max 演算法嵌入資料的範例[10]，其中控制參數 $\sigma=5$ 及正乘數 $k=2$，嵌入訊息為“11101001011”。我們先從表 1(a)找到 $P_{min}=163$，$P_{max}=168$。由於 $P_{min}\geqq 128$，所以將所有像素減去 163 得到表 1(b)。再依嵌入程序 V 及 VI 進行機密資料嵌入，表 1(c)淺網底為不可嵌入區塊，白色為可嵌入區塊，先乘上 2 再加下方括弧中的嵌入訊息資料。最後依步驟 VII 組合成偽裝區塊。

B. 資料萃取步驟
I. 將偽裝影像區分為不重疊的影像區塊 $P1$。
II. 計算區塊 $P1$ 的最大值 $P1_{max}$ 與最小值 $P1_{min}$。
III. 求出暫存區塊
  i. 若 $P1_{min}\geqq 128$，則將區塊 $P1$ 所有像素 $P1_j$ 減掉 $P1_{min}$ 以得出暫存區塊 $Q1$。
  ii. 若 $P1_{min}<128$，則將區塊 $P1$ 所有像素 $P1_j$ 減掉 $P1_{max}$ 以得出暫存區塊 $Q1$。
IV. 若暫存區塊 $Q1$ 的像素值 $q_j\geqq 2$ 倍的控制參數 σ，則將 q_j 減掉 σ 得到 $q1_j$。
V. 若暫存區塊 Q 的像素值 $q_j<$ 控制參數 σ，則先將嵌入訊息取出後，再除以 k 以取得 $q2_j$。
VI. 還原成原始區塊
  i. 若 $p_{min}\geqq 128$，則將暫存區塊 Q 所有像素 $q1_j$ 及 $q2_j$ 加上 P_{min} 以得到原始區塊。
  ii. 若 $p_{min}<128$，則將暫存區塊 Q 所有像素 $q1_j$ 及 $q2_j$ 加上 P_{max} 以得到原始區塊。
VII. 重複執行步驟 I-VII，直到所有區塊完成。

表1 Min-Max 演算法嵌入程序範例表

168	164	165	163
168	164	165	163
168	164	165	163
168	164	165	163

(a)原始區塊 P

5	1	2	163
5	1	2	0
5	1	2	0
5	1	2	0

(b)暫存區塊 Q

10	3 (1)	5 (1)	163
10	3 (1)	4 (0)	1 (1)
10	2 (0)	4 (0)	1 (1)
10	2 (0)	5 (1)	1 (1)

(c)位置區塊 P

173	166	168	163
173	166	167	164
173	165	167	164
173	165	168	164

(d)偽裝區塊

表 2 為 Min-Max 演算法萃取資料的範例[10]，其中控制參數 $\sigma=5$ 及正乘數 $k=2$ 為已知訊息。從表

2(a)找到 $P1_{min}$=163，$P1_{max}$=168。由於 $P1_{min}$≧128，所以將所有像素減 163 得到表 2(b)。依程序 III 算出暫存區塊 $Q1$，然後運用步驟 IV 及 V 取出機密資料“11101001011”。最後依步驟 VII 還原成原始區塊。

表2　Min-Max 演算法嵌入程序範例表

173	166	168	163
173	166	167	164
173	165	167	164
173	165	168	164

(a)偽裝區塊

10	3 (1)	5 (1)	163
10	3 (1)	4 (0)	1 (1)
10	2 (0)	4 (0)	1 (1)
10	2 (0)	5 (1)	1 (1)

(b)位置區塊

5	1	2	163
5	1	2	0
5	1	2	0
5	1	2	0

(c)暫存區塊 $Q1$

168	164	165	163
168	164	165	163
168	164	165	163
168	164	165	163

(d)原始區塊 P

2.3　係數誤差(Coefficient-bias)法

Yang 與 Hu 再利用 Min-Max 藏入機密訊息後，將再利用係數誤差法來嵌入一張浮水印資料，以有效增加訊息的嵌入量，其作法如下。

A. 資料嵌入程序
   I. 將偽裝影像進行整數小波轉換(Integer Wavelet Transform, IWT)轉換成頻率域係數，並將資料嵌入 LH (或 HL)等子頻帶。
   II. 將嵌入區塊分成 nxn 區塊 C，利用控制參數 β 進行係數調整，當係數 $C_r \leqq -\beta$，則將係數值減去 β；若係數 $C_l \geqq \beta$，則將其係數值加上 β，即完成係數調整作業。
   III. 將所有符合 $0 \leqq C_{dr} < \beta$ 間的係數值乘上乘數 k 後再加上浮水印資料 δ，可得到 $C1_{dr}$；另將符合 $-\beta < C_{dl} < 0$ 的係數，乘上乘數 k 後，再減去浮水印資料 δ，可得到 $C1_{dl}$。
   IV. 將浮水印資料依序嵌入調整之係數值後，即完成資料嵌入作業。

B. 資料萃取程序
   I. 將接收到掩護影像先進行 IWT 轉換，再從轉換後 LH (HL)子頻帶進行資料萃取。
   II. 當子頻帶係數值 D_c 滿足 $-k\beta < D_c < k\beta$ 此一條件時，則代表其為浮水印嵌入區塊，可進行資料萃取，先將其反向除以嵌入時的乘數 k，其相除運算之餘數即為原先嵌入之浮水印資料 δ。
   III. 另外將大於或等於 2β 的係數值減去 β，並將小於或等於 -2β 的係數值加上 β，即可還原成初始係數值。

C. 係數調整作業
   為避免浮水印嵌入(萃取)過程的運算影響影像可逆作業，故選擇適當的係數來進行嵌入與萃取即有其必要。Yang 與 Hu 在進行嵌入作業前，需先進行係數調整作業，方能順利進行浮水印嵌入。

3. 資訊隱藏偵測技術

Petitcolas 等人將資訊隱藏技術分為強調數位內容完整性之數位浮水印(Watermarking)技術，與重視訊息不可見性的資料隱藏(Information Hiding)技術。前常運用於智慧財產權與數位版權保護[4]，而後者則常用於機密訊息之發送與傳遞。對一設計良好的資訊隱藏技術來說，其須具備不可察覺性(Imperceptibility)、安全性(Security)、高藏密量(High Payload)及簡易有效性(Efficiency)等四大特性。但在實際進行資訊隱藏技術設計時，往往發現要同時滿足前述四項特性非常不易。因其彼此間隱藏有矛盾(Trade off)性質，假如提高嵌入資料之隱藏量時，將使影像的不可察覺性降低。故發展資訊隱藏技術來嵌入機密訊息時，即必須考量應用領域並針對前述特性應佔有之比例作出取捨。而透過實際應用需求考量後所做出的調整，往往即是資訊隱藏偵測技術可用來分析與研究的關鍵因素。

3.1　資訊偵測步驟

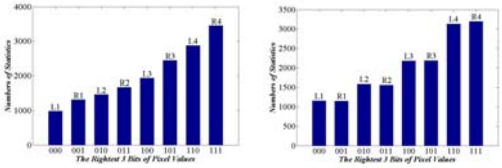
一般來說，若要能找出潛藏於多媒體影像中的機密訊息，並進一步解譯出嵌入訊息之內容，必須透過以下分析步驟的進行方能達成。

A. 藏密偵知：首先，要在浩瀚無涯的網際網路影像中，偵測出可能嵌入有機密訊息之偽裝影像，以供作為進一步分析之依據，此亦即為破密分析過程中最繁雜且最耗費資源的步驟。
B. 特徵萃取：從偵測出的可疑偽裝影像中，嘗試運用不同分析方式來萃取出嵌入訊息之資料特性，如訊息長度、訊息格式及使用之加密技術等特徵。
C. 訊息破解：嘗試從前一步驟所得出之特徵，更進一步地分析與解譯出嵌入之機密訊息原文內容，此即為藏密分析之最終目的。

3.2　常見資訊隱藏偵測技術

3.2.1 χ^2 偵測技術

由 Westfield 及 Pfitzamann [8]於 1999 年提出，其發現傳統 LSB 取代技術是以取代將影像像素值之最低位元達到訊息嵌入之效果。若於嵌入過程中取代掩護圖像中所有像素值之最低位元，則將無可避免地產生像素對(Pair of values; POV)問題，如圖 1 所示。圖 1(a)為未藏密之掩護影像其像素值出現頻率長方統計圖，圖 1(b)為 LSB 藏密之偽裝影像其像素值頻率長方統計圖，其中虛線代表像素對之平均值。由圖可知，偽裝影像之相鄰像素值的出現頻率統計量將趨近相同，而原始掩護圖像則無此現象。



(a) 原始圖像　　(b) LSB 嵌入後圖像

圖 1　相鄰像素對問題示意圖

χ^2 偵測技術演算流程如下。

I. 首先找出影像之可能像素對總數 k，如無調色盤影像像素值則使用調色盤影像索引值。

II. 先將像素值排序，再計算第 i 組像素值出現頻率之平均數：

$$n_i^* = \frac{|\{colour \mid sortedindexOf(colour) \in \{2i, 2i+1\}\}|}{2} \quad (13)$$

計算第 n_i 個像素值之出現頻率：

$$n_i = |\{colour \mid sortedIndexOf(colour) = 2i\}|. \quad (14)$$

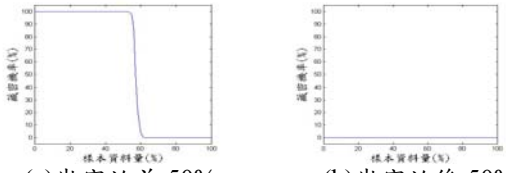
III. 以(15)式計算 χ^2 統計量：

$$x_{k-1}^2 = \sum_{i=1}^{k} \frac{(n_i - n_i^*)^2}{n_i^*}. \quad (15)$$

IV. 利用卡方分佈特性計算出影像藏密機率 p：

$$p = 1 - \frac{1}{2^{\frac{2k-1}{2}}\Gamma(\frac{k-1}{2})} \int_0^{x_{k-1}^2} e^{-\frac{x}{2}} x^{\frac{k-1}{2}-1} dx. \quad (16)$$

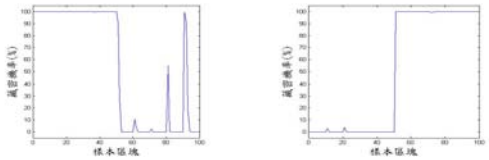
V. χ^2 偵測技術雖能有效地找出依序嵌入資料之影像；但若資料非以循序方式嵌入，則 χ^2 偵測技術將會失效，如圖 2 所示。



(a)嵌密於前 50%　　(b)嵌密於後 50%

圖 2　以 χ2 偵測不同 LSB 嵌入順序之結果

鑑於 χ^2 偵測技術只能偵測連續嵌入秘密訊息之影像，Provos [5]提出延展式 χ^2 偵測技術，其將統計樣本區分為多個獨立區塊，再分別計算個別區塊之統計值。使用 χ^2 偵測技術之偵測結果將如圖 3(a)所示，而運用延展式 χ^2 偵測技術之偵測結果如圖 3(b)所示。由實驗結果可知延展式 χ^2 偵測技術確實具有較佳的偵測效果。



(a)嵌密於前 50%　　(b)嵌密於後 50%

圖 3　延伸 χ2 不同 LSB 嵌入順序之結果

3.2.2 RS 偵測技術

Fridrich [2]於 2001 年將相鄰像素間區分多個群組 G，先運用鑑別函數 (Discrimination Function) f 來計算影像之平順性(Smoothness)，即像素群組之一般性(Regularity)，再透過遮罩(Mask)及翻轉函數(Flipping Function) F 的運算來將影像區分為 R、S 及 U 三個不同群組。

RS 攻擊法運作方式如下。

I. 將影像根據空間排列位置區分為多個群組 G，每一群組皆是由 n 個相鄰像素組成。

II. 運用鑑別函數 $\boldsymbol{f}$ 來分別找出影像中最平順(Smooth)與最雜亂(Noise)之像素群組，如(17)式所示：

$$\boldsymbol{f}(x_1, x_2, ..., x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i|. \quad (17)$$

III. 翻轉函數 F_1 與 F_{-1} 如(18)式及(19)式：

$$\mathbf{F}_1(x) = \begin{cases} x-1, x \bmod 2 = 1 \\ x+1, x \bmod 2 = 0 \end{cases} \forall x. \quad (18)$$

$$\mathbf{F}_{-1}(x) = \mathbf{F}_1(x+1) - 1 \ \forall x. \quad (19)$$

IV. 以-1，0，1 作為翻轉函數之遮罩參數，模擬加入不同雜訊對原始影像之影響。

V. 運用鑑別函數f與翻轉函數F將影像區分為三個不同群組：

R：$\boldsymbol{f}(\mathbf{F}(G)) > \boldsymbol{f}(G)$

S：f(F(G))<f(G)

U：f(F(G))=f(G)

VI. Fridrich 等人認定於一般未嵌入訊息之影像，(20)式必然會成立，若該式不成立代表其間可能嵌入機密訊息。

$$R_M \cong R_{-M} \text{ and } S_M \cong S_{-M}. \quad (20)$$

VII. 透過(21)式計算出可能訊息嵌入長度 p：

$$p = x/(x - 1/2). \quad (21)$$

圖 4 中可明顯看出，在測試影像進行不同比例的翻轉，將對 RS 偵測結果造成不同影響[2]。由於資料嵌入過程對影像 LSB 產生改變的機率只有 1/2，所以當翻轉比率達到 50%時，對影像所造成之影響則將接近於全影像嵌入機密之結果。運用 F_1 翻轉與 F_{-1} 翻轉過程對影像將造成不同影響，因此可用以估計出將機密訊息嵌入於影像之可能性。

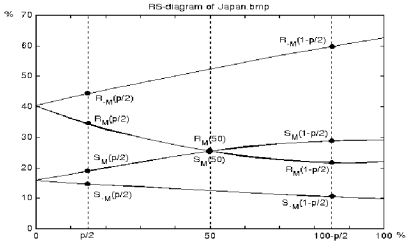
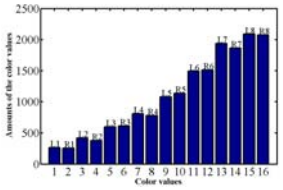


圖 4　RS 計算不同比率翻轉量之統計圖

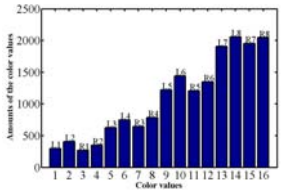
4. Min-Max 演算法安全性分析

χ2 與 RS 偵測技術均係針對 LSB 嵌入法將資料嵌入於最低位元平面所引發數值對(Pairs of Values, PoV)問題，如圖 5(a)所示，透過統計與機率計算方式來判斷求出可疑影像藏密機率。此兩種偵測技術可有效運用於絕大部分 LSB 系列之資訊隱藏技術之偵測。Tian 之 DE 擴張法因運用影像相鄰像素值間之相似特性，故無法抵抗前述技術之偵測。

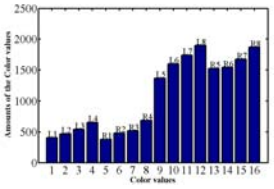
而 Yang 與 Hu 所提出之 Min-Max 演算法係將偽裝媒體待嵌入區塊之像素值與頻率係數，係運用乘數 *k* 來擾亂可能存在之相鄰像素對問題。當乘數 *k* 設定等於 2 時，經 Min-Max 演算嵌入之偽裝影像，雖存在像素對問題，如圖 5(b)所示，但已可有效躲過前述 χ2 與 RS 偵測技術仍可有效偵測及估算。若乘數設定為 4 時，則其像素對問題的區間將隨乘數增加而變大，且不再是以相鄰位置出現，將依乘數 k 的設定而形成不同群組，如圖 5(c)所示。因此 χ2 與 RS 偵測技術已經無法有效偵測運用 Min-Max 演算法所簽入之訊息及浮水印資料。



(a)一般 LSB 嵌入之相鄰像素對問題



(b) *k*=2 時之像素對問題



(c) *k*=4 時之像素對問題

圖 5　不同乘數 *k* 所衍生像素對示意圖

雖然目前 RS 與 χ2 偵測技術無法偵測經 Min-Max 演算法嵌入過程所使用的乘數 k 擾亂之像素對順序。但從圖 5 中仍可明顯看出，其仍具備之像素對特性，亦即其仍存在有規則性的特徵可供破密研究者進行探究。在 3.1 節所提到之資訊隱藏偵測的步驟中，本文目前已經發現 Min-Max 演算法的訊息嵌入特徵，後續即可有可能依循藏密偵知、特徵萃取及內容破解，有效分析與破解經 Min-Max 演算法嵌入訊息之偽裝影像資料。

5. 結論與未來發展方向

為避免原本用於保護個人隱私之資訊隱藏技術遭不法份子所利用，資訊隱藏偵測技術的研發係將隨資訊隱藏技術的發展而推陳出新。本文初步將資訊隱藏的偵知步驟區分為藏密偵知、特徵萃取及內容破解等三部分，即是希望能逐步強化資訊隱藏偵知技術的能力，以兼顧個人隱私不超過國家安全範疇之目標。

Yang 與 Hu 改良 Tian 可逆式資訊隱藏技術，運用 Min-Max 演算法提出一個可回復式資訊隱藏技術，雖然沒有出現明顯像素對，但從經其嵌入訊息的掩護媒體分析後，仍可看出一定之像素對規則。其雖能暫時抵抗現行 RS 與 χ2 偵測技術的探知，但是經由本文所揭露出的像素特徵，將可作為發展有效偵知技術之基石，經過持續的分析與研究，應可找出有效的偵知技術，以精進資訊隱藏偵知技術的發展。

誌謝

本研究為中華民國行政院國家科學委員會專題研究計畫部分成果，計畫編號：NSC 102-2221-E-182-013-。

參考文獻

[1] A. M. Alatter, “Resverible watermarking using the difference expansion of a generalized integer transform,” *IEEE Transaction on Imaging Processing*, vol. 13, no. 8, pp. 1147-1156, 2004.

[2] J. Fridrich, M. Goljan, and R. Du, “Detecting LSB steganography in color and gray-scale images,” *Magazine of IEEE Multimedia, Special Issue on Security*, vol. 8, no. 4, pp. 22-28, Oct.-Dec. 2001.

[3] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” *IEEE Transactions on Circuits and System for Video Technology*, vol. 16, no. 3, pp. 354-362, March 2006.

[4] F. A. P. Petitcolas, R. J. Anderson, and, M. G. Kuhn, “Data hiding - a survey,” *Proceedings of the IEEE*, vol. 87, no. 7, July 1999, pp. 1062-1078.

[5] N. Provos and P. Honeyman, “Detecting steganographic content on the internet,” *Proceedings of the Network and Distributed System Security Symposium*, San Diego, CA, Feb. 2002.

[6] J. Tian, “Reversible data embedding using a difference expansion,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890-896, Aug. 2003.

[7] D. M. Thod and, J. J. Rodriguse, “Reversible watermarking by predict-error expansion,” *Proceeding of the 6th IEEE SouthWest Symposium on Image Analysis and Interpretation*, NV USA, 2004, pp. 21-25.

[8] A. Westfeld and A. Pfitzmann, “Attacks on steganographic systems,” *Proceedings of the 3rd Data hiding Workshop*, Sept.-Oct. 1999, pp. 61-75.

[9] H.-C. Wu, C.-C. Lee, C.-S. Tsai. and, H.-R. Chen, “A high capacity reversible data hiding scheme with egde prediction and different expansion,” *Journal of System and Software*, vol. 82, no. 12. pp. 1966-1973, 2009.

[10] C.-Y. Yang and. W.-C. Hu, “Reversible data hiding in the spatial and frequency domain,” *International Journal of Imaging Processing*, vol. 3 Issue 6, pp. 373-382, 2010.

[11] 吳汶涓，可逆式資訊隱藏技術之發展趨勢，*資訊安全通訊*，vol. 18, no. 4 , pp. 84-66. Oct. 2012.

結構化惡意程式資料庫系統

劉奕賢　蔡舜智　江啟賓　張家瑋　安家駒　李忠憲
國立成功大學 電機工程學系 / 電腦與通信工程研究所
{dannyliu, sctsai, takumi, william, jjan}@hsnet.ee.ncku.edu.tw, jsli@mail.ncku.edu.tw

摘要

近年來惡意軟體急遽增加，特別是殭屍網路，對於資訊安全的危害甚鉅。由於駭客工具快速的發展與大量散播，加上經濟的誘因及網路犯罪防治的困難等因素。殭屍網路成為駭客用來作為分散式阻絕服務攻擊、發送垃圾郵件等犯罪工具。傳統上對殭屍網路的研究主要由本體論等方式著手，本研究有鑑於關聯式資料庫系統中資料探勘工具的成熟，故著手建置以關聯式資料庫系統為基礎的結構化惡意程式資料庫系統，以做為後續研究運用該類型工具的基礎。

關鍵詞：殭屍網路、資料探勘、關聯式資料庫、分散式阻絕服務攻擊、網路安全

Abstract

Recently, number of malwares surges dramatically, especially the botnet. It becomes a vast challenge to network security. Due to rapidly developed and massive spreading hacking tools and financial inducement, network crimes increase tremendously. Botnet is a powerful criminal tool for DDOS or SPAM. In contrast to the research of botnet mainly with ontology, this research is based on data mining technology with relational database.

Keywords: Botnet; Data Mining; Relation Database; DDOS; Network Security

1. 前言

不論是民間企業組織或政府單位，日常營運中對於資訊科技依賴程度與日俱增，資訊科技已是不可或缺的重要基礎建設之一。在建置資訊基礎設施的同時，主要以功能性及便利性為主要考慮，然而在個資法施行後，對機敏性資料及個人識別資訊的防護及管理，已成為另一個考量的重點。功能性、便利性的訴求，與安全性考量相對來說，是不同的角度，如何保護其資料的安全，並達到機密性、完整性與可用性的要求，已成為企業組織與政府單位的重要問題[17][18]。微軟[1]曾在 RSA 歐洲大會上發表的一篇研究報告，更顯示美國地區殭屍網路數量以 220 萬部居冠，由此可見其猖獗的程度。

近年惡意軟體的快速增長，對資訊安全的機密性、完整性與可用性已產生嚴重的威脅。這種趨勢已引起國外資訊界及企業組織、資訊業界與政府單位的重視。在眾多的惡意程式中，尤以殭屍網路(botnet)帶來的安全威脅最為嚴重。當前因網路連線型態的改變，撥接上網造成連線持續不一定的問題，在當前 ADSL、FTTB 等網路接取服務普及下，持續連網已成為網路上的常態。大多數的使用者資訊安全意識薄弱，故個人電腦容易淪為感染殭屍網路的受害者。新一代的惡意程式與傳統的電腦病毒最大的差異在於對宿主的行為。傳統上電腦病毒以破壞、干擾電腦運作、造成資料損壞為主要目的，使用者極易察覺其電腦運作不正常，而懷疑自身中毒；相較之下，殭屍網路以運用宿主做為跳板、竊取宿主的機敏資料為主要目的，在日常操作中，使用者極難察覺異常，進而讓殭屍網路這種新一代的惡意程式潛伏其中。加上經濟上的誘因及網路犯罪防治的困難等多種助因，促使駭客工具快速的發展與散播。殭屍網路慢慢成為駭客用來作為竊取帳號密碼、軟體序號或其他機敏資料的工具，甚至成為進行分散式阻絕服務攻擊(DDoS)[5][6]、發送垃圾郵件(SPAM)的跳板主機。

假若駭客運用殭屍網路對某特定企業網站進行分散式阻絕服務的攻擊行為，導致一般正常的使用者無法順利瀏覽該公司網站，或假冒某公司發出釣魚郵件進行詐騙犯罪，這種行為對商譽造成的影響，其潛在商業損失是難以估計的。由此可見殭屍網路對網路的服務供應商、企業形象與廣告商等產生的威脅及影響。殭屍網路主要是由個人電腦所組成的網路大軍，許多人由於電腦防護不足或缺少基本的資安觀念，往往在不知情的情況下成為殭屍網路的一員。在經濟利誘或網路軍備競賽的引導下，駭客們可以利用大量的殭屍電腦進行垃圾郵件發送或分散式阻絕服務攻擊等的惡意行為[5]，而這些非法行為透過殭屍電腦的隱蔽性和自我摧毀等功能，是很不容易被發現的[6]。從微軟的安全研究報告提到目前的殭屍網路大多用來進行網路金融犯罪，手段包含發送垃圾郵件，釣魚網頁，竊取個人機密資料等等。且自從網域快速轉換對應(fast-flux)技術出現之後，殭屍網路更加難以偵測，因為殭屍網路透過網域名稱系統(DNS)快速變換對應的網路位址(IP)，進而導致傳統以鎖定特定網路位址的防治措施無法奏效，甚致會對無辜使用者造成傷害。

有鑑於殭屍網路對資訊安全的嚴重影響及威脅，且產業界中不乏針對惡意程式分析的相關平台。唯當前相關研究主要是運用語意網、本體論等方式，鮮少運用在商業資料分析中較為成熟的關聯

式資料探勘工具，探究其原因，主要是惡意程式的分析報告，主要原始輸出格式即為延伸標記語言(XML)或網頁格式(HTML)，甚至為純文字格式(txt)，研究者因此受限於資料來源及轉換處理不易等限制。有鑑於此，本研究主要目的為建立一結構化惡意程式資料庫系統，運用第三方惡意程式分析平台的分析結果，開發相關轉換套件，將相關分析報告，轉換成為關聯式資料庫數據內容，以供後續相關研究得以運用關聯式資料探勘工具，進而試圖從中獲得更大的效益。

2. 文獻探討

本研究將運用惡意程式分析平台對殭屍網路惡意程式的範本進行分析，進而萃取其中重要的資料加以收集彙整，再以結構化的關聯式資料庫方式存取相關分析資料，故本研究將就惡意程式類型、殭屍網路原理及架構與惡意程式分析平台等進行相關探討，以做為本研究結構化惡意程式資料庫系統設計的基礎。

2.1 惡意程式類型

傳統上，惡意程式又常被稱為電腦病毒。早期依惡意程式行為的不同，主要可區別為病毒、特洛依木馬及網路蠕蟲三種[13]。其中病毒這種程式，具有自我複製能力。可能會對損毀檔案、格式化磁碟而造成損害。或消耗記憶體造成電腦效能低落，影響使用者正常作業等。特洛依木馬則不具備複製能力，以竊取受害者的資料為主要目的。網路蠕蟲則以其可透過網路連線、電子郵件、檔案分析或即時通訊等各種通訊管道，快速進行自我複製來傳播而得名。從趨勢科技的定義[14]來說，目前常見的電腦安全威脅主要分為垃圾郵件、間諜程式和廣告軟體、網路釣魚、病毒與其他惡意程式等六大類型。新一代的惡意程式，又稱為進階持續性滲透攻擊(APT)[12]其結合傳統的網路蠕蟲、特洛伊木馬及其他類型的相關技術，如 Rootkit 等，於後門工具的基礎上強化，並透過相互融合而發展成為目前最為複雜的攻擊模式之一。

當前常見的惡意程式傳播方式，有下列常見幾項[9]:

1. 主動式漏洞攻擊：
   攻擊者會先搜尋一般電腦作業系統或應用程式的缺陷，利用該漏洞，植入惡意程式。此一手法，又以零日攻擊(Zero-day Attack)[3]最為精典，即運用缺陷被發現後，相關廠商完成修補的時間差，對相關系統進行攻擊。
2. 跨網站腳本攻擊(XSS)：
   跨網站腳本攻擊(XSS)[8]即攻擊者在提供網頁服務的站台中，於特定超文件標記網頁中(HTML)嵌入惡意的程式腳本，當訪問者訪問這些網站時，使用者會被重新導向到惡意網站而執行惡意腳本，使得惡意程式被下載到主機上，並被自動執行。
3. 郵件病毒：
   許多常見的電腦病毒及其他惡意軟體係以電子郵件附件 (即與郵件訊息一同傳遞的檔案) 的形式散佈。如果附加至郵件訊息的檔案內含病毒。輔以社交工程的技巧，誘使不知情的使用者執行附件，而感染該惡意程式。
4. 網路蠕蟲：
   是一種電腦程式碼，會將自身附加到程式或檔案，在電腦之間散佈，同時感染途經的電腦。病毒會把自身附於母體程式，然後嘗試感染其他電腦。
5. 即時通訊軟體與社群網路：
   此一管道即運用 Facebook 等好友清單及個人訊息的功能，配合社交工程手法，誘使不知情的受害者好友，點選連結或執行程式而感染之。

2.2 殭屍網路

殭屍網路是從傳統惡意代碼形態包括網路蠕蟲、特洛伊木馬和後門工具的基礎上進化，並透過相互融合發展而成的目前最為複雜的攻擊模式之一。近年來隨著網路連線型態的改變，持續連網的連線服務如 ADSL、FTTB 等服務普及與連線速率的提昇，加上使用者缺乏危機意識，大量的個人電腦容易淪為受到殭屍網路感染的受害者，進行成為殭屍網路危害資訊安全的代罪羔羊。

殭屍網路是駭客出於惡意，大量傳播殭屍程式來感染並控制受害電腦，以形成一個連線的網路群體，駭客可以透過一對多的控制命令來指示受害電腦從事特定的行為。因受害電腦並不知情，故稱殭屍網路。殭屍網路主要由下列三大元件所組成：

- Master： 為駭客本身，主要目的為下達惡意程式指令、更新惡意程式碼給殭屍網路成員(bot)。
- Command and Control (C&C) Server： 有時會由 Master 本身來扮演這一個角色，其主要負責管理控制整個殭屍網路的伺服器，並將 Master 的指令傳遞給 bot。殭屍網路的通訊拓樸十分多元，包括星狀、階層式等多種不同的架構，且 C&C Server 也會經常變動以逃避追蹤及反制。
- Bot： 一群無辜受到殭屍網路程式感染而被遙控的受害者電腦。殭屍網路程式有別於傳統以破壞電腦正常運作為目的的電腦病毒不同，其反而不希望讓受害者察覺本身遭受感染，而成為殭屍網路的

成員，在依照 Master 的指令於特定時間進行特定的工作。

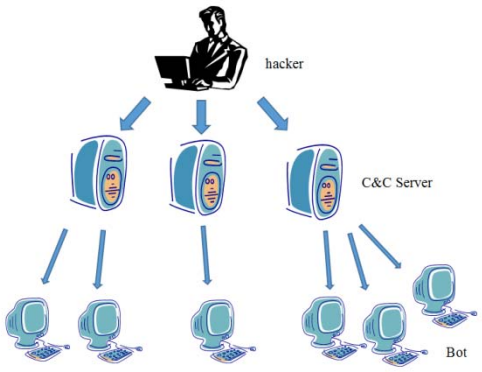


圖1. 殭屍網路的組成元件

故本研究亦會結合多種的惡意程式分析平台的分析結果，以取得殭屍網路在不同分析平台硬體上執行時的相關數據。並記錄如網路通訊行為、主機檔案存取行為等相關的系統操作情況。

2.3 惡意程式分析平台

本研究主要目的，即整合第三方惡意程式分析平台的分析結果，並整合成為一結構化的殭屍網路資料庫。故本研究主要將透過國家實驗研究院高速網路與計算中心(NCHC)及國立成功大學資通安全研究與教學中心(TWISC@NCKU)及 International Secure System Lab 的 Anubis 平台[7]等第三方專業資訊安全研究單位所提供的分析平台進行相關惡意程式範本的分析作業，以下將介其所擁有的惡意程式分析平台特色。

- 高速網路與計算中心(NCHC)國家實驗研究院下的高速網路與計算中心是國內重要的資訊安全研究單位之一，其主要具備了 TWMAN(抬丸郎)、Cuckoo 及 CWSandbox 等平台，並結合其自組開發提供的自由軟體 Clonezilla(再生龍)系統還原套件來強化用用實機作為分析平台硬體的能力。以下分別以這三大平台的特色進行介紹：

1. TWMAN(抬丸郎)[11]：由於現今的一些殭屍病毒已具備偵測當下環境是否為虛擬化，且具備偵測是否有沙盒在監視，為了解決此一問題 TWMAN 利用實際的電腦進行感染，執行惡意程式進行分析，並利用 Clonezilla[10]快速恢復的能力將受感染的電腦還原。此外更可進一步針對惡意程式樣本進行切片比對，與資料庫中已有的惡意程式進行相關的比對，找出變種或加殼的新型惡意程式。

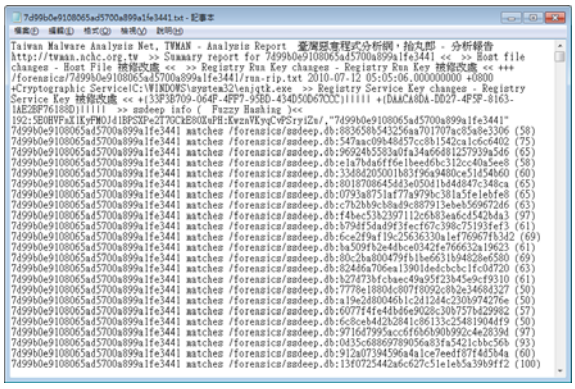


圖2. TWMAN 的惡意程式分析報告

2. Cuckoo[4]： 此一平台為二進制行為自動動態分析的工具，能夠呈現程序運行中詳細的關鍵應用程式介面和網路活動，也可以處理分析 PDF、office 和其他微軟的文件，在執行惡意程式時產生網路流量的儲存，並在分析的同時拍攝畫面和呈現程序運行中詳細的相關應用程式介面。此外該平台因有發現部分不同的惡意程式具有相同的 MD5 值，而無法區分，進一步加入 SHA1 及 SHA256 兩種的識別方式。



圖3. Cuckoo 的惡意程式分析報告

3. CWSandbox[16]：CWSandbox 以自動分析惡意程式為基礎，在虛擬的環境且有限的時間下，密切監控其所有的系統呼叫，並能夠自動生成一份詳細的報告，大大的簡化了惡意程式分析師的工作。其強大的能力可以讓使用者分析所有的微軟的應用程式介面其中包括感染的：office 文件、PDF 檔、惡意的 URL 和 Flash 廣告。



圖4. CWSandbox 的惡意程式分析報告

- 國立成功大學資通安全研究與教學中心(TWISC@NCKU)

  國立成功大學資通安全研究與教學中心主要具備 Malbed 及 CWSandbox 兩大分析平台，其特色在於分析作業並非是於虛擬的環境下進行，而是運用美國 Utah 大學所授權的 Emulab 軟體配合實體的系統來架構分析所需的環境。：

  1. Malbed[15]：以自動化惡意程式分析為基準，並利用自行開發、整合之 Malbed 進行分析記錄更動的檔案、註冊表以及在惡意程式在執行時所做的系統呼叫，在網路方面將來源端和目的端的 IP 位置、區域名及連接埠記錄下來，以觀察分析中的惡意程式，是否有對外連接的行為，並藉由上述的分析了解惡意程式發展的趨勢。

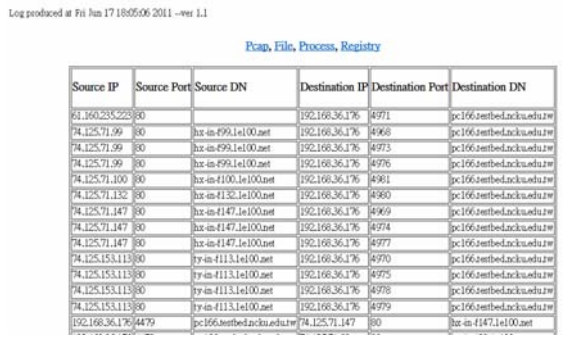


圖5. Malbed 的惡意程式分析報告

  2. CWSandbox：因 CWSandbox 與國網使用平台相同，唯分析的硬體系統改以 Testbed 方式進行分析而有所差異，平台本身特色就不再加以贅述。

- Anubis 惡意程式分析分台

Anubis[7]主要是在虛擬的環境下進行二進位文件的分析，並可及時觀察其分析和執行，分析的重點主要著重在安全相關方面程式的變動，也因為將範圍縮小所以可以得到更精確的結果，也讓分析程序更加簡單，藉由線上的沙盒執行與測試惡意程式，並記錄其執行時的系統呼叫與檔案和註冊表的更動藉以判斷此一惡意程式的目的。此外 Anubis 亦有提供介面供第三方上傳惡意程式樣本以進行分析，並於分析後提供相關數據以供研究參考。

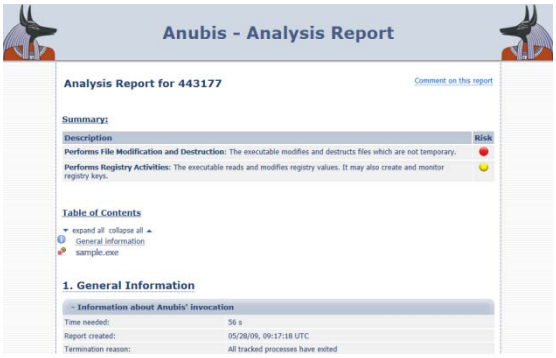


圖6. Anubis 的惡意程式分析報告

3. 系統架構

本研究所提出之結構化殭屍網路資料庫系統(SBDS)，主要分為殭屍網路報告擷取模組(BRGM)、殭屍網路資料整合模組(BDIM)、殭屍網路資料展示模組(BDPM)及殭屍網路資料庫(BotDB)等四大元件。本研究系統架構圖如下所：

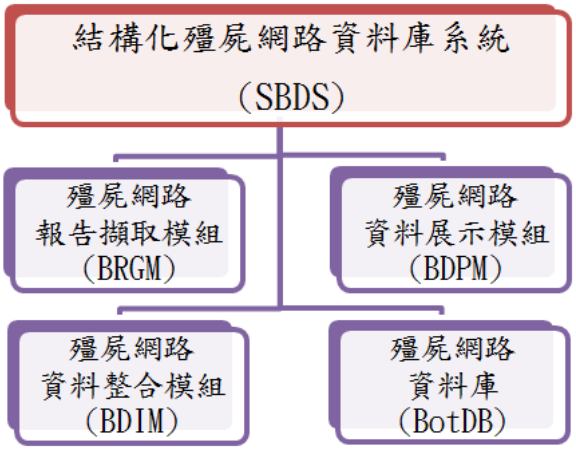


圖7. 結構化殭屍網路資料庫系統架構

以下針對本研究所提出之結構化殭屍網路資料庫系統(SBDS)之四大模組分別進行說明：

1. 殭屍網路報告擷取模組(BRGM)

   該模組主要功能在於負責將惡意程式樣本上傳至其他的惡意程式分析軟體進行相關分析，再取回其分析報告，以作為本研究後續作業的主要資料來源。透過惡意程式分析軟體的相關分析的結果，可令使用者更加清楚特定程式的意圖與行為。在此一模組中，將以批次及事件驅動兩種管

道來觸發該模組，以執行其負責之分析報告擷取的工作。

2. 殭屍網路資料整合模組(BDIM)
該模組主要功能在於負責整合來自於殭屍網路報告擷取模組(BRGM)所擷取的惡意程式分析報告，並加以處理轉換，最終輸入本研究所建置的結構化殭屍網路資料庫系統(SBDS)中。本研究將依惡意程式分析報告的資料項目及相關文獻回顧，訂定結構化殭屍網路資料庫的資料綱要，利用實體關係模型、資料型別和條件約束將其行為描述進行一個有系統化的整理架構，以提供相關分析數據整合的依據，同時保留原有資料，以供後續進一步比對的需求。

3. 殭屍網路資料展示模組(BDPM)
該模組主要功能在於將結構化殭屍網路資料庫系統(SBDS)中的相關資料透過網頁應用程式的方式加以顯示，可以提供使用者查詢相關的統計資訊或各惡意程式的分析結果及下載原始報告等功能。

4. 殭屍網路資料庫(BotDB)
該資料庫即本系統的主要核心，負責儲存所有惡意程式的分析報告內容。運用關聯式資料庫的設計規範加以實作。並輔以正規化的相關流程，確保資料儲存的一致性及避免重覆儲存的問題。

結構化殭屍網路資料庫系統(SBDS)系統環境圖如下所示：

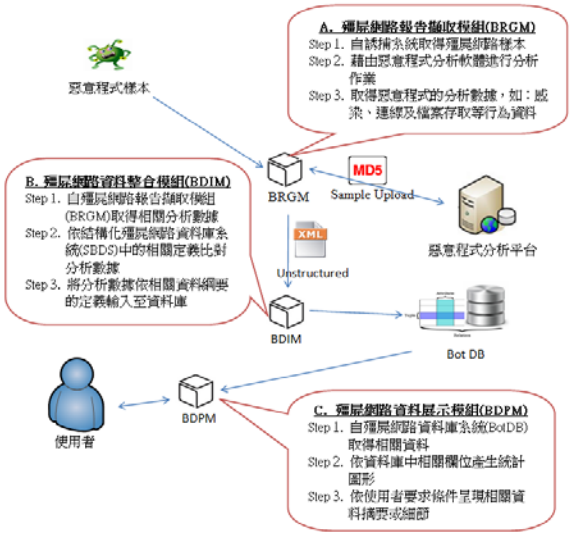


圖8. 結構化殭屍網路資料庫系統環境

本研究以關聯式資料庫系統為存儲所有分析報告的載具。在資料綱要及資料庫架構的設計上，本研究以正規化模型[2]為依據，依序進行第一正規化、第二正規化及第三正規化三項程序，確認資料中沒有重複值組、單一筆資料中沒有多重屬性、資料庫中可避免資料重覆儲存及更新可能造成資料不一致等問題。本研究設計之結構化惡意程式資料庫的實體關係圖(ERD)如下所示：

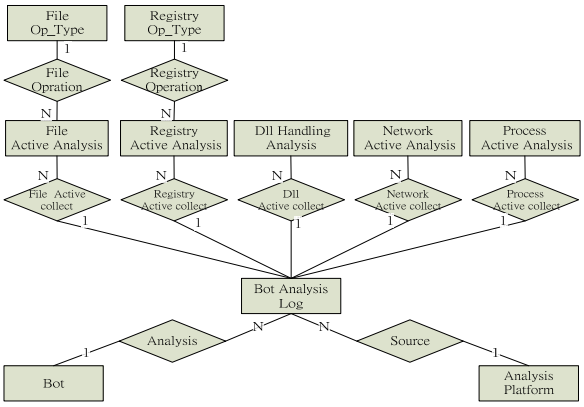


圖9. 結構化殭屍網路資料庫系統環境

本研究的設計中，以 Bot Analysis Log 這個資料表為紀錄每份惡意程式分析報告的核心，再由其與 Bot 資料表的關聯，來識別該份報告屬於每一隻惡意程式；並透過其與 Analysis Platform 的關聯說明該分析報告是由那一個惡意程式分析平台所產生的。此外惡意程式分析報告中會有關於執行緒(Process)、網路活動(Network Active)、動態連結函式庫(Dll)、註冊機碼(Registry)及檔案操作(File)等相關行為，再分別以關聯的型式，分別存放至對應的資料表中。同時在註冊機碼(Registry)及檔案操作(File)這兩種活動中，再以其操作行為類型，各別加以關聯。以此設計為藍圖，再結合關聯式資料庫管理系統加以實作這結構化惡意程式資料庫。

4. 結論

本研究有鑑於關聯式資料庫系統中資料探勘工具的成熟，唯當前相關研究主要是運用語意網、本體論等方式，而鮮少運用在商業資料分析中較為成熟的關聯式資料探勘工具。探究其原因，產業界中主要的惡意程式分析的相關平台，其分析報告主要原始輸出格式即為延伸標記語言(XML)或網頁格式(HTML)，甚至為純文字格式(txt)，研究者因此受限於資料來源及轉換處理不易等限制所致。有鑑於此，本研究主要目的為建立一結構化惡意程式資料庫系統，運用第三方惡意程式分析平台的分析結果，開發相關轉換套件，將相關分析報告，轉換成為關聯式資料庫數據內容，以供後續相關研究得以運用關聯式資料探勘工具，進而試圖從中獲得更大的效益。

誌謝

感謝國科會計畫 NSC100-2218-E-006-029-MY3 提供經費支持本研究的進行。

參考文獻

[1] Adrienne Hall, “In Pursuit of Cyber Crime,” RSA 2010, London, UK, Oct. 12-14, 2010.

[2] Catriel Beeri, Philip A. Bernstein & Nathan Goodman, 1978, “A sophisticate's introduction to database normalization theory,” Proceeding VLDB '78 Proceedings of the fourth international conference on Very Large Data Bases, Vol 4, pp. 113-124.

[3] Constantin Musca, Emma Mirica adn Razvan Deaconescu, 2013, “Detecting and Analyzing Zero-Day Attacks Using Honeypots,” 2013 19th International Conference on Control Systems and Computer Science (CSCS 2013), May 29-31, Bucharest, Romania

[4] Cuckoo, “Cuckoo Sandbox,” Retrieved 2012/03/15 from http://www.cuckoobox.org.

[5] Felix C. Freiling, Thorsten Holz & Georg Wicherski, “Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks,” ESORICS '05, Milan, Italy, Sep. 12-14, 2005.

[6] Guofei Gu, Junjie Zhang & Wenke Lee,2008, “BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic,” NDSS'08, San Diego, USA, Feb. 8-11, 2008.

[7] International Secure Systems Lab, “Anubis: Analyzing Unknown Binaries,” Retrieved 2011/10/15 from http://anubis.iseclab.org.

[8] Lwin Khin Shar & Hee Beng Kuan Tan, 2013, “Predicting SQL injection and cross site scripting vulnerabilities through mining input sanitization patterns,” Information and Software Technology, Vol. 55, Iss. 10, pp. 1767-1780.

[9] Mentor Wang, 2008, “Botnet 介紹,” , Retrieved 2010/11/26 from http://mentorwang.blogspot.com/2008/07/botnet.html.

[10] NCHC, “Clonezilla 再生龍,” Retrieved 2011/12/15 from http://clonezilla.nchc.org.tw.

[11] NCHC, “臺灣惡意程式分析網,” Retrieved 2011/12/10 from http://twman.nchc.org.tw.

[12] Sood A.K. & Enbody R.J., 2013, “Targeted Cyberattacks: A Superset of Advanced Persistent Threats,” IEEE Security & Privacy, Vol. 11, Iss. 1, pp. 54-61.

[13] Trend Micro, “病毒/特洛依木馬程式/網路蠕蟲網頁,” Retrieved 2013/08/13 from https://imperia.trendmicro-europe.com/tw/threats/home-user/common-threats/viruses/index.html.

[14] Trend Micro, “常見的電腦安全威脅,” Retrieved 2013/08/13 from https://imperia.trendmicro-europe.com/tw/threats/home-user/common-threats/index.html.

[15] TWISC@NCKU, “Malbed,” Retrieved 2012/03/30 from http://malbed.twisc.ncku.edu.tw.

[16] University of Erlangen-Nuremberg, “Malware Analysis System, CWSandbox: Behavior-based Malware Analysis,” Retrieved 2012/01/05 from http://mwanalysis.org/.

[17] Von Solms B., 2006, “Information security - The fourth wave,” Computers & Security, Vol. 25, No. 3, pp.165-168.

[18] Yeh, Q. J. & Chang, A. J. T., 2007, “Threats and countermeasures for information system security: A cross-industry study,” Information & Management, Vol. 44, pp.480–491.

植基於 Google 雲端訊息推播技術的行動認證機制
(Mobile Authentication Based on Google Cloud Messaging)

楊慶隆　　邱創昱　　蔡松叡
國立東華大學 資訊工程學系
cnyang@mail.ndhu.edu.tw

摘要

多數人習慣使用容易記的弱密碼當作自己帳號的通行碼，但是這些簡單的數字組合，容易遭破解。如果選擇數字與符號不具意義的長密碼，又容易遺忘。由於人對圖形的記憶比文字容易，很多點擊式的圖形密碼認證機制被提出，以代替文字密碼。但是圖形密碼需要大的資料庫容量來儲存圖片。本文以 Android 平台，結合 Google 雲端訊息推播技術 (Google Cloud Messaging; GCM)，設計完成一個行動認證機制。藉由智慧型手機以及一台具有視訊鏡頭的電腦，不需要記憶密碼就可以使用這套行動認證機制登入帳號。使用者登入時，會從 GCM Server 同步推播至手機一組亂數，再經具金鑰的雜湊函數，計算得雜湊值並轉換為 QR 碼。透過視覺通道(電腦的視訊鏡頭替代肉眼判斷影像內容稱之為視覺通道)，將雜湊值傳送到伺服器。最後使用者成功登入系統，而視覺通道讓我們不用手動輸入長串的雜湊值，也能防止側錄或偷窺攻擊。

關鍵詞：Google 雲端訊息推播技術、QR 碼、雜湊函數、認證、視覺通道。

Abstract

People often use weak passwords, such as the names, or combination of alphanumeric words, for their accounts. However, these weak passwords are easily cracked by malicious attackers. Choosing the strong password is secure, but it is not easy to remember. Since graphic picture is more memorable than text, graphical passwords are accordingly proposed. However, graphical password needs a large storage capacity to store the pictures. In this paper, we implement a mobile authentication scheme based on Google Cloud Messaging (GCM). Through the helps of smart phone and computer with a camera, one can login accounts without remembering password. Client's mobile device will receive a random number from GCM Server by push notification. By using the keyed hash function, a hashed value is determined from this random number and then transferred to QR code. Through the visual channel (composed of smart phone and computer with a camera), we can transmit this hashed value to the server. Finally, one can successfully login system. Meantime, the visual channel let users not keyin the long hashed value and meantime can avoid the peeping attack.

Keywords: Google Cloud Messaging (GCM), QR code, Hash function, Authentication, Visual channel.

1. 前言

網路服務千百種，現代人生活已經和網路脫不了關係，舉凡食衣住行都與網路有關，網路上使用者不計其數，就以 Facebook 來說，在 2012 年已超過十幾億名活躍用戶，為了要區別使用者，各大網站都有其登入系統，此類需要登入操作的網站本文稱作「登入網站」，目前主要登入方法為輸入一組帳號密碼[1]-[3]，但每天需使用到的服務繁多，帳號密碼不只一組，若註冊新帳號又須多記一組密碼，導致使用不便。一般而言，使用者會選擇短密碼，或者是自己的名字、生日、電話、寵物名字來當作密碼。若是這樣，惡意的攻擊者可使用密碼攻擊工具來破解。如果選擇數字與符號不具意義的長密碼增加安全強度，又容易遺忘。而且在不安全的環境中輸入密碼可能會被竊取，導致隱私暴露，為此若能有個統一且快速，安全性高又不需要記憶密碼的登入方法，必能有極多的應用場合。

如何讓使用者不需要記憶密碼就可以達到認證。當然可使用指紋、視網膜、聲音波型等個人的生物特徵，但是這增加了複雜度。或者是使用圖形密碼認證機制[4]-[5]，利用人對圖形的記憶比文字更容易，避免記憶長密碼。但是圖形密碼需要大的資料庫容量來儲存圖片。本文以 Android 平台，結合 Google 雲端訊息推播技術 (Google Cloud Messaging; GCM)，設計完成一個行動認證機制。藉由智慧型手機以及一台具有視訊鏡頭的電腦，不需要記憶密碼就可以使用這套行動認證機制登入帳號。由於智慧型手機的普及，幾乎人手一支，且有高度相容性。例如 Google 的 Android 手機智慧型手機以及一台具有視訊鏡頭的電腦平台，憑著完全開放原始碼免費的作業系統，任何人都能獲得及使用 Android 系統，越來越多的國內外開發工程師也競相投入 Android 手機開發行列，進而成為手機市占率最高的作業系統。使得現代人生活中擁有方便性絕佳的載具，讓我們的行動認證機更為可行。

綜合以上敘述，本文提供一種安全且方便的登入方式，使用者不再需要記憶密碼，且可快速的登入各個「登入網站」。使用者登入時，會從 GCM Server 同步推播至手機一組亂數，再經具金鑰的雜湊函數，計算得雜湊值並轉換為 QR 碼。透過視覺通道(電腦的視訊鏡頭替代肉眼判斷影像內容稱之

為視覺通道)，將雜湊值傳送到伺服器。最後使用者成功登入系統，而視覺通道讓我們不用手動輸入長串的雜湊值，也以能防止偷窺攻擊。

文章架構如下，第二部份是為相關背景，介紹 GCM 推播技術的使用方式及特色。第三部份為本文所提的植基於 Google 雲端訊息推播技術的行動認證機制。App 實作，則於第第部份說明，最後為本文結論。

2. 相關背景

GCM 為 Google 提供的一種訊息推播技術，可將伺服器上的資料推播給行動裝置(如手機、平板)上的 App。使用此技術的伺服器需向 Google 申請 API key，由 API key 可向 GCM Server 申請 Sender ID [6]。Android client 端的裝置要加入此推播的群組，只需將 Sender ID 傳送給 GCM 伺服器，並將收到的 Register ID (簡稱為 RegID) 傳送給應用程式伺服器，就完成加入此推播群組的工作。當應用程式伺服器要傳送訊息時，需將本身的 API Key 和使用者的 RegID 及欲發送的訊息傳送給 GCM 伺服器，就可由 GCM Server 推播給行動裝置上的 App[7]-[8]。

GCM 可幫第三方的伺服器端發送訊息，至該伺服器的使用者行動裝置上，且行動裝置不必維持運行狀態。當要傳送訊息時，伺服器會利用無線網路推播來喚醒行動裝置，再由手機中的 App 接收訊息資料。當行動裝置在無網路的環境下，無法收到訊息，這些通知訊息將會被存在伺服器中，而這些被暫存的訊息有數量上的限制，數量限值為一百則，當超過一百則時通知訊號將會被丟棄，直到行動裝置回到有網路的環境底下，行動裝置將會收到一條特殊的訊息通知，告知通知訊號的數量已達上限。

GCM 所傳輸的資料分為兩種，一種是輕量型的訊息，用來通知行動裝置上的 App 去擷取伺服器上的資料；另一種是含有裝載資料的訊息，訊息大小的限制為 4KB，大部分用在即時通訊上的簡單訊息交換。本機制採用第二種的方式，伺服器產生亂數後，藉由 GCM 的推播機制，將亂數推播給使用者，並由我們完成的 App 雜湊此亂數並產生 QR 碼。透過視覺通道，讓視訊裝置擷取 QR 碼，且送至伺服器端。

3. 植基於 GCM 的行動認證機制設計

使用者需要有智慧型手機，及擁有視訊鏡頭的電腦裝置。當使用者要登入一個「登入網站」時，可點選本機制提供的登入頁面，輸入完帳號後，本系統的認證伺服器會發送亂數，藉由 GCM Server 推播給使用者的手機，由手機中的 App，將亂數透過具金鑰的雜湊函數 (註: 此金鑰為使用者與登入網站所分享的秘密訊息)。產生的雜湊值則為此次登入的密碼，並轉成 QR 碼的形式在手機螢幕上呈現，使用視訊鏡頭擷取 QR 碼並傳回伺服器端。伺服器比對 QR 碼與亂數的雜湊值是否相同。若相同，使用者可以登入此網站。有別於傳統輸入密碼的方式，此種透過視訊鏡頭擷取畫面的方式，稱為視覺通道，不會有輸入密碼被側錄或偷窺的風險[9]-[10]。此亂數雜湊值為密碼，每次數值皆不相同，為一次性密碼，不需擔心密碼外洩或竊取的可能。透過 GCM 推播技術，使用者可以馬上取得此亂數，不需要記憶密碼。我們將此認證機制稱為行動認證，是因為過程中使用這需藉由行動裝置的幫忙。表 1 為行動認證機制與傳統登入方式的比較。

表 1. 本機制與傳統方式之比較

	本機制	傳統方法
安全性	採用亂數雜湊值為密碼，每次不同，只有該手機收到亂數。	每次密碼相同。需防止密碼被側錄或偷窺。
便利性	密碼被轉成 QR 碼後，透過視覺通道傳送雜湊值。	需手動輸入密碼，不同帳號密碼不同，有忘記密碼的疑慮

3.1 本機制架構

本機制架構如圖 1 所示，令 H，M，P，S，G 分別代表使用者，行動裝置(智慧型手機)，一台具有視訊鏡頭的電腦，認證伺服器，以及 GCM Server，詳細認證步驟說明如下:

(1) $H \rightarrow P \rightarrow S$: 輸入使用者帳號。
(2) S: 產生亂數 α。
(3) $S \rightarrow G$: 傳送{API key, RegID, α}至 GCM Serve。
(4) $G \rightarrow M$: 將 α 推播至使用者的智慧型手機。
(5) M: 計算 $\beta = H_K(\alpha)$，並用 β 產生 QR 碼，其中 $H_K(\cdot)$ 為具有金鑰的雜湊函數。H 與 S 分享金鑰 K。
(6) $M \rightarrow P \rightarrow S$: 透過視覺通道傳送 QR 碼。
(7) S: 從使用者帳號取得相對的金鑰 K 並由 QR 碼得 β，來確認 $\beta \stackrel{?}{=} H_K(\alpha)$。

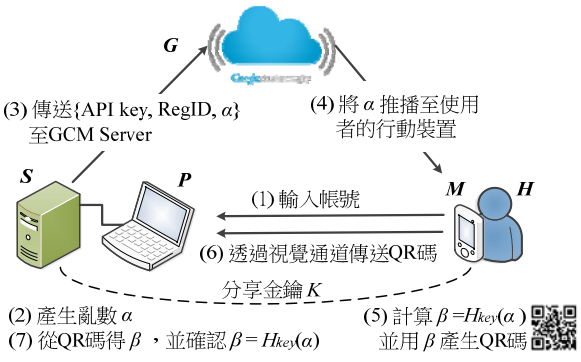


圖 1. 使用 GCM 推播技術的行動認證機制

一般的方法都是輸入帳號密碼，任何人只要有

密碼後即可登入。本方法的特色在於登入不需輸入任何密碼，藉由行動裝置(如智慧型手機)中的 App 接收由 GCM Server 傳送來的一組亂數 α。因為認證伺服器與使用者分享金鑰 K，當它由視覺通道收到 QR 碼後，驗證 $\beta \stackrel{?}{=} H_K(\alpha)$ 來決定是否為合法使用者。

3.2 伺服器端與行動裝置端之設計

本論文提供各種需要登入操作的網頁(如社群網站、信箱、...等)一種新的認證機制，採用此設計的網頁可在登入頁面提供連結，讓使用者選擇傳統的登入方式或此認證方式。本系統包含認證伺服器，及一個手機 App。該認證伺服器需先向 GCM 申請一組 API key，並擁有一個資料庫，記錄使用者的帳號，RegID，與雜湊時使用的金鑰 K。

當使用者從行動裝置中下載本系統的 App 後，App 會自動的向 GCM 申請一組 RegID，並傳送至認證伺服器端。認證伺服器收到後，產生一把雜湊用的金鑰，此金鑰需以“離線”方式通知使用者，並輸入至手機。完成後，App 會列出與本計畫合作的網頁，使用者可以選擇那些網頁要採取此方式登入，並進行綁定程序，因為當使用者在此網站採取本系統的認證登入方式，將不再需要輸入密碼，只需要使用者本人的手機。

在 App 中點選與本系統合作的「登入網站」後，會連結到該網站的綁定頁面中，過程中需填入此網頁使用者的帳號密碼，若為合法使用者，網頁會傳送帳號與 RegID 至本系統的認證伺服器。綁定過程是在網頁端處理，本 App 不會接觸到使用者在各網頁的密碼，確保使用者隱私。當使用者欲登入一採用此系統的網頁，可點選連結至本系統為此網頁設計的頁面，使用者輸入完帳號後，會進行圖 1 的認證過程，當認證伺服器確認是合法登入的使用者後，會向此「登入網站」發送使用者在此網頁的帳號與登入訊息，並由「登入網站」讓使用者轉跳至登入後的畫面，完成登入程序。

4. 系統實作

本部份介紹此行動認證系統的實作過程，包括以 Android 的環境下並配合 Eclipse 整合開發環境的 App，以認證伺服器的建置。

4.1 開發流程與技術

此系統分為兩個部分，認證伺服器與行動裝置上的 App。認證伺服器端需架設多個的認證服務網頁，提供每個需要登入網站的專屬頁面。認證伺服器需與各「登入網站」間有一個安全的 VPN 通道，並有傳送訊息給 GCM Server 的功能。所建置的網頁，可讓使用者填入帳號，藉由此帳號，在資料庫中尋找使用者的 RegID，並產生亂數，讓 GCM 推播至使用者的行動裝置中。當收到由視覺通道傳來之 QR 碼時，認證伺服器需解回 QR 碼並比對亂數雜湊值是否與 QR 碼的值相同。認證伺服器除需具備以上功能外，還需在新的使用者註冊時，需將對方的 RegID 寫入資料庫中，並產生一把金鑰，作為雜湊時共享的金鑰。上述，是我們開發一個認證伺服器所需的功能。

另一方面，手機端的 App 程式所需的功能說明如下。App 安裝完後，初次執行時要自動向 GCM 註冊一組 RegID，並傳送至認證伺服器中。之後，使用者可以選擇那些「登入網站」要啟用本系統的行動認證機制，點選後，程式要開啟連結至該網站的綁定頁面。當使用者填入帳號後，「登入網站」會將帳號與 RegID 發送至本系認證統伺服器，讓認證伺服器寫入資料庫中。Android 手機中具金鑰的雜湊函數，我們是使用 MD5，並採用 HMAC (Hash-based Message Authentication Code)方式，輸出雜湊值大小為 128 位元，並且轉換成 QR 碼的形式，在螢幕上呈現。

在認證網頁及手機 App 中，本文所需的 QR 碼編解碼程式，使用 ZXing 所提供的開放原始碼。ZXing 提供了多種不同一維及二維條碼的編解碼原始碼，如 Code 39、Code 93、Codabar...等，提供了各種語言所撰寫的開放原始碼，可以在不同的平台上執行。本文使用 Java 語言在網頁與 Android 平台上實作 QR 碼的編解碼，開發介面如圖 2，使用 Eclipse 撰寫程式碼，並匯入 ZXing 提供的 JAR 檔，以執行其提供的套件程式。

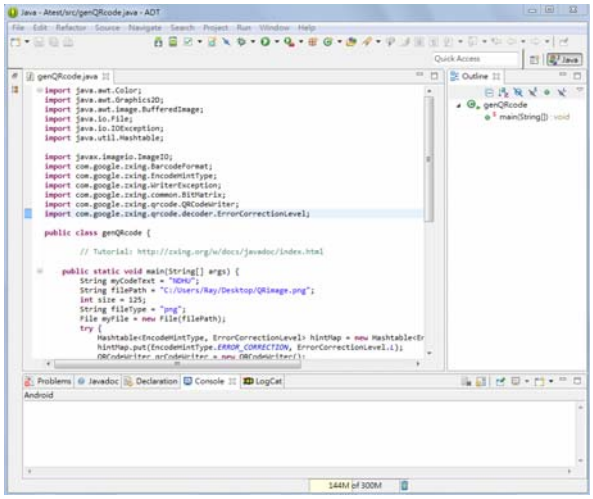


圖 2. QR 碼實作介面

圖 3 為 QR 碼產生器的部分指令，當亂數經過雜湊後，輸出為字串型態，大小為 128 位元，宣告參數 CodeText 及 Size 來儲存字串內容與大小，並產生錯誤控制碼編碼對應 ECCMap，以 QRCodeWriter 類別建立物件，輸入相關參數便可產生 QR 碼的二元矩陣，之後在由矩陣產生圖檔即完成 QR 碼。

```
String CodeText = hashValue;
int size = 128;
...
QRCodeWriter qrWriter = new QRCodeWriter();
BitMatrix matrix = qrWriter.encode (CodeText,
BarcodeFormat.QR_CODE, size, size, ECCMap);
...
```

圖 3. QR 碼部分程式

4.2 實作結果

實作本系統需撰寫一支手機 App 程式，以及架設一個進行認證伺服器，兩者皆須滿足上一節所提之功能。當使用者從 Android 平台中下載本系統的 App 後，初次執行時，系統會進入等待畫面，如圖 4(a)所示，此過程會向 GCM 註冊一組 RegID，當取得 RegID 後再發送給本系統認證伺服器。認證伺服器會產生一把雜湊時使用的金鑰，此金鑰需以“離線”方式通知使用者，以完成註冊程序。App 會進入主程式頁面，如圖 4(b)。使用者可以選擇那些「登入網站」要使用本系統的行動認證服務。



(a) (b)

圖 4. 本系統手機 App 執行畫面

當點選其中一個登入網站後，程式會自動開啟網頁，連結至該登入網站的綁定頁面，當登入網站與採用本系統的認證服務時，圖 5 為模擬的綁定頁面。連結此頁面時，程式會自動將 RegID 傳送至該登入網站。當使用者輸入完帳號密碼後，點選啟用，當網站確認帳號密碼無誤後，會將帳號與 RegID 一起發送至本系統伺服器，並完成綁定程序碼。



圖 5. 登入網站中啟用認證服務頁面

與本系統合作的「登入網站」，可以在原登入頁面放置連結，讓使用者可以進入本系統為此網站所架設的認證頁面。或是該網站直接採用本系統服務，作為該網站的登入方式。當一個經過綁定程序的使用者要登入網站時，會連結至本系統的認證網頁，如圖 6 所示。使用者輸入帳號後，按下確認鍵，伺服器端會在資料庫中查詢該帳號的 RegID，並產生亂數，由 GCM 推播至使用者的手機。



圖 6. 本系統認證服務網頁

手機端收到亂數後，App 透過金鑰將亂數雜湊，運算完的值以 QR 碼呈現在螢幕上，如圖 7 所示。



圖 7. 進行認證服務所需的 QR 碼

使用者將手機畫面對準視訊鏡頭，透過視覺通道掃描 QR 碼，如圖 8 所示。視訊畫面下方，會顯示發送訊息時間，當手機接收到後可以比對時間，確認是否為該次認證的 QR 碼。



圖 8. 透過視覺通道擷取 QR 碼

當伺服器取得 QR 碼中後，與亂數雜湊值比

對，確認使用者是否認證成功，並將結果回傳給「登入網站」，若使用者認證成功，網站便轉跳至登入後的畫面。若使用者在本系統認證網頁中，在收訊不好的情況下，輸入完帳號後，卻沒有收到由 GCM 推播來的亂數，無法產生 QR 碼時。使用者只需重新整理頁面，並再次輸入帳號，伺服器會重新發送亂數，不須擔心遺失封包而無法登入網頁的問題。傳送時，手機螢幕也會顯示發送時間，可以與網頁上顯示的比對，確認是否為該次認證的 QR 碼，以避免惡意第三者的重送攻擊。由於每次登入都會有不同的亂數，產生的 QR 碼也都不相同，所以手機 App 程式只會暫存顯示 QR 碼，當使用者掃描完按下確認後，會自動移除並將記憶體釋回給作業系統，使用者不需擔心使用本系統 App 造成儲存空間的負擔。

5. 結論

本論文採用 Android 開發，搭配智慧型手機及具視訊鏡頭的電腦，完成了能夠使建立在視覺通道的認證方法，登入過程無需記憶繁雜的密碼，也更有安全性保證。我們將此認證機制稱為行動認證，是因為過程中使用這需藉由行動裝置的幫忙。雖然本方法有硬體上的限制，但對於登入機制又多了一樣選擇。做這個專題開發此行動認證，我們學習了 JAVA 語言在 Android 平台的開發過程，及使用 Eclipse、模擬器等開發工具，並了解 QR 碼的轉換原理，透過 GCM 雲端推播技術，設計安全且方便的網站登入系統。

本行動認證機制，除了使用 GCM 訊息推播外，亦可自行架設推播伺服器，但此方法需要額外的硬體與通訊成本，另外，也可採用藍牙(Bluetooth)或其他通訊技術完成本機制。

參考文獻

[1] Morris, R., and Thompson, K. “Password security: a case history”, Commun. ACM, 1979, 22, (11), pp. 594–597.

[2] Seeley, D., “Password cracking: a game of wits”, Commun. ACM, 1989, 32, (6), pp. 700–703.

[3] Gait, J., “Easy entry: the password encryption problem”, ACM SIGOPS Oper. Syst. Rev., 1978, 12, (3), pp.54–60.

[4] J. Spitzer, C. Singh, and D. Schweitzer, “A security class project in graphical passwords,” Journal of Computing Sciences in Colleges archive, 2010, 26, pp. 7–13.

[5] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P.C. van Oorschot, “Persuasive Cued click-points: design, implementation, and evaluation of a knowledge-based authentication mechanism,” IEEE Tans. On Dependable and Secure Computing, 2012, 9, pp. 222–235.

[6] Google play,https://support.google.com/googleplay/android-developer/answer/2663269?hl=zh-Hant.

[7] Wikipedia, https://en.wikipedia.org/wiki/ISO/IEC_27001.

[8] Google Developers, https://developers.google.com/android/c2dm/?hl=zh-TW.

[9] McCune J., Perrig A., and Reiter M., “Seeing-is-believing: using camera phone for human-verifiable authentication,” IEEE Symposium on Security and Privacy, pp. 110-124, 8-11 May, 2005.

[10] Kao, Y.W., Zhang, X., Studer, A., and Perrig, A., “Mobile encryption for laptop data protection (MELP)”, IET Inf. Secur., 2012, 6, (4), pp. 291–298.

基於資料外洩的行動惡意程式行為分析

陳嘉玫　江玟璟　陳怡靜　張明達　吳惠麟　曾昭銘
台灣學術網路危機處理中心(TACERT)
chiamei.chen@gmail.com

摘要

行動裝置出現已經有一段時間，但其安全問題一直未受到大家注意，直到近來科技快速的進步下、行動裝置開始擁有不下於個人電腦的計算能力，越來越多人使用行動裝置進行各項活動，其中儲存的大量使用者資料，吸引了駭客們注意並對其開發並製作惡意軟體，這些惡意軟體以行動裝置上使用者資料為目標，造成使用者的資料外洩，被用來謀取利益，對使用者造成極大的損失。

本研究提出用敏感性資料洩露為特徵來偵測惡意程式的方法，利用封閉環境的模擬裝置來隔離並執行應用程式，透過行為分析的方式，監控並記錄應用程式執行過程中的行為，並對其相關行為進行深入分析，從檔案與網路連線等方面，來分析並追縱敏感性資料是否被送出行動裝置外面，同時也針對應用程式發送短訊息的行為是否異常等方式，來偵測惡意軟體。透過實際的惡意樣本進行實驗，結果證明在分辨惡意軟體的正確率上以及誤判率上各取得不錯的成果，比起現有的方式，像是以權限為基礎來進行分析或是透過系統呼叫繁率等方式，能夠擁有較好的惡意軟體偵測率，並擁有較低的誤判率。

關鍵詞：行動裝置安全、Android、行為分析、動態分析、惡意軟體偵測。

1. 前言

移動裝置又稱手持裝置，典型的裝置有個人數位助理、行動電話…等，隨著技術的進步、網路的普及，智慧型手機開始在市場上嶄露頭角，更整合行動電話和個人數位助理系統等，成為全方位的行動網上裝置，為了追求較好的效能與方便性，更出現平板電腦，漸漸形成個人與網際網路的不可分割性。這些移動裝置不只是能作為行動電話與朋友間聯絡之用、也可以用來上網、收發信件，以及進行娛樂影音用途。更甚之可以透過行動裝置來進行財務管理，也因為如此行動裝置上面儲存著大量的個人敏感資料，如：各類網站、信箱等服務之帳號密碼、個人通訊資料、金融轉帳資料等。這些重要的個資更吸引駭客們的注意，花費心思鑽研破壞行動裝置的安全性問題，透過獲取手機使用者的隱私資料、如通訊錄、個人資料，以及利用手機寄送付費簡訊或是進行不合法的行為，從中獲取利益。由於早期行動電話所使用的作業系統與應用程式，多由行動電話設備商自行開發或採取合作異同開發，因此不同手機所搭載的程式，具有相當大的差異性。對於這類型的裝置，較不受駭客青睞，因此早期手機的安全性問題較不受人們重視。

雖然近年來各家廠商已不斷改進行動裝置的安全性，但是從報告中可以發現，行動裝置的安全威脅不但沒有降低反而日益嚴重。目前除了官方的市場外還有第三方市場，對於開發者而言在第三方市場上發佈軟體是不需要付開發者費用的，吸引了部份開發者選擇在第三方市場上發佈軟體。這也導致了一些駭客利用這個方式散佈自己的惡意軟體。而一些使用者為了規避官方市場付費軟體的費用，選擇從第三方市場下載破解版本，結果反而下載到惡意軟體。有些熱門實用的軟體，官方只提供部份語言，使用者礙於語言障礙，透過第三方市場下載經過翻譯的版本，這也導致使用者可能下載到惡意軟體的風險。

目前應用於行動裝置的分析模式與基於個人電腦的分析方法類似，亦區分為靜態分析與動態分析兩種。靜態分析相較於動態分析，前者的優點在於不需要執行應用程式的情況下，透過程式的反組譯，由程式碼中找尋特徵值，分析時間短且快速、不會在分析期間造成感染擴散等問題。但缺點是，靜態分析必須能夠事先獲取其惡意程式特徵值，因此對於新威脅的應變能力較弱。此外，近來惡意程式使用了大量的程式碼混淆機制，造成靜態分析在解析程式碼上面臨困難。

動態分析方法的缺點是，因為需要執行應用程式來進行分析，在分析執行效率方面，則略遜於靜態分析。但是動態分析的優點則重於行為上的分析 ，即使攻擊者所採用的攻擊方式改變、使用新的漏洞或是利用混淆機制來阻礙分析，其惡意行為也不能夠被隱藏，因此在面對新的行動裝置平台上與新型態的攻擊模式上，動態分析比起靜態分析更能夠快速的應對這些安全威脅。

本研究利用現有動態分析，利用現有模擬裝置建置一個動態行為分析的系統平台。監控並記錄應用程式的行為，並對其相關行為進行分析，追縱應用程式執行過程資料的流向，來判斷良性與惡意程式。與現有重於權限與系統呼叫頻率的分析相比，能夠有效分辨良性與惡意程式，並擁有較低的誤判率。

2. 相關技術背景

2.1 行動裝置概況

近年來，智慧型手機開始出現，以蘋果(apple)公司所推出搭載 iOS 作業系統的 iPhone 智慧型手機谷哥(Google)公司所推出搭載 Android 作業系統的手機為市場的主流，其它還包括 Windows 的 Phone7 RIM 的 BlackBerry 等。根據 IDC 在 2012 年 5 月所公佈的統計數據[1]，如所示 Android 在 2012 年第一季市占率約 59%，緊接著 iOS 為 23%。為了推陳出新並迎合客戶的喜好，各家廠商各自釋出自己的 API，供程式人員開發相關行動裝置的應用程式，因此降低開發應用程式的難度，讓大多數的程式開發者可以共同參與開發應用程式的工作。在難度降低與多人使用的誘因之下，更是吸引大量的駭客的注意。

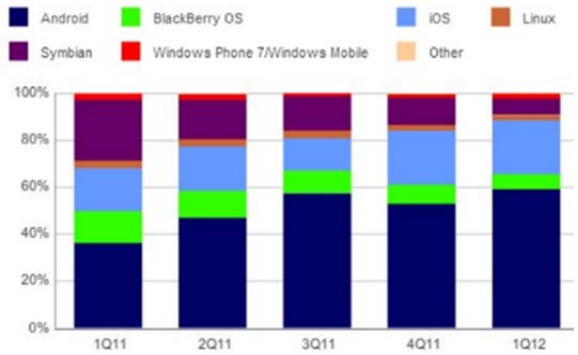


圖 1 全球行動裝置市佔率[1]

根據 McAfee2012 年威脅報告[2]指出，如圖 2 所示，McAfee 到 2012 年為止，其發展速度更是以幾何倍數的方式持續遞增成長。所收集的惡意樣本就高達了 8000 個，其樣本中有 7000 個屬於 Android 平台。如圖 3 所示，相較於其它平台來說 Android 的惡意軟體數量就佔了大部份，其次為諾基亞(Nokia)所使用的 Symbian 系統。

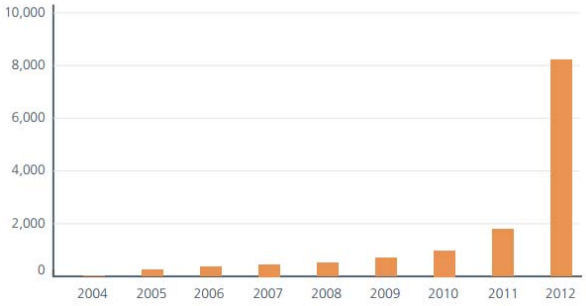


圖 2 行動裝置樣本數[2]

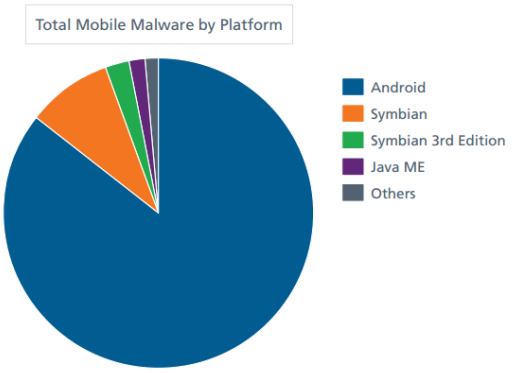


圖 3 平台樣本數[2]

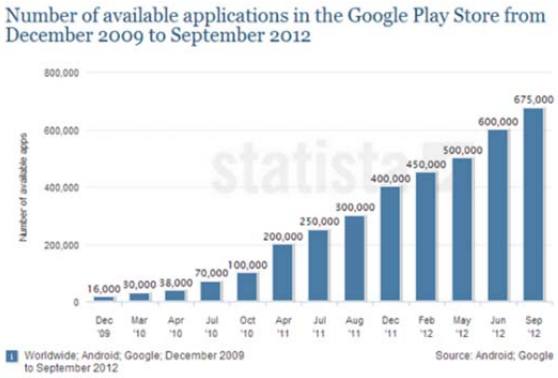


圖 4 Google Play 應用程式數量[3]

從 Google play 上的應用程式數量的增長率(圖 4)與惡意樣本數增長率相比，可以發現，應用程式數量從 2009 年 12 月的一萬六千個，到 2012 年 9 月的 67 萬個，呈現出倍數成長的趨勢，而惡意軟體樣本的增長率也自 2010 年起開始大幅度上升，到了 2012 年更是呈現爆炸性的增加。其原因可能是著眼於 2009 年 Google play 官方市場的正式營運並伴隨第三方市場的出現，Android 開放源碼的特性、語言上採用 java、使得開發與轉換平台難度降低，因此漸漸成為行動裝置的主流系統，駭客們也開始將攻擊重心轉往 android 平台，從而導致 2012 年惡意程式的數量大增。

2.2 惡意軟體

根據 F-Security 的 2013 第一季行動裝置威脅報告[4](如圖 5 所示)，可以發現 2011 年的惡意軟體種類中，以木馬程式的數量為最多，其次是病毒、蠕蟲與監視軟體等。報告指出，大量的惡意軟體會竊取行動裝置的資訊，包括行動裝置的國際行動識別碼、SIM 卡號碼、聯絡人資訊、作業系統資訊等，並透過簡訊服務(SMS，Short Message Service)、網路連線存取(如：透過網頁的 GET、POST)等方式將這些資料傳給遠端服務器或是利用被感染的手機發送付費 SMS、瀏覽網頁賺取點擊數等。

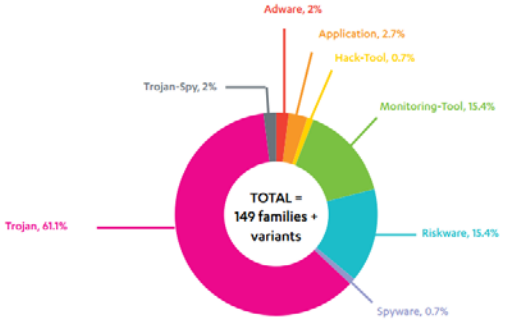


圖 5 惡意軟體種類[4]

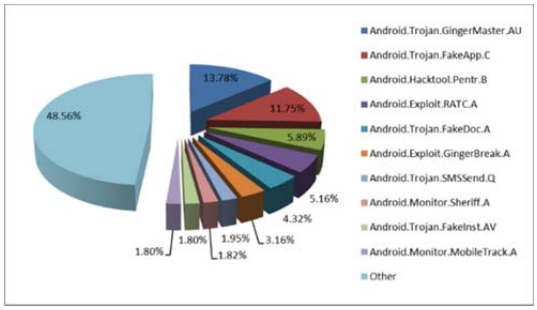


圖 6 前十大惡意軟體

如圖 6 所示，以前十大惡意軟體為例，像是偵測比例最大的 Android.Trojan.GingerMaster.AU 以及 Anroid.Trojan.FakeDoc.A 等木馬軟體，會收集使用者的行動裝置資料並傳送至遠端伺服器，造成使用者的資料外流並侵犯隱私。Android.Trojan.FakeApp.c 此木馬軟體，會顯現一些廣告讓使用者點擊之後，以賺取點閱數並秘密的收集使用者的資料。另外其它家族的 FakeAndroid.Trojan.SMSSend.Q 與 Android.Trojan.FakeInst.AV 則是會在使用者不知情的情況下，發送 SMS 訊息到付費號碼，來賺取使用者的金錢。

3. 系統架構

本系統的架構如圖 7 所示，共分為執行區塊(Execution Section)以及分析區塊（Analysis Section）兩大部份。Android 的.apk 檔案會送入執行區塊，這部份會進行模擬器的建置、啟用，並且進行應用程式的安裝與執行，隨後會對應用程式發出模擬操作行為，過程中應用程式在模擬器中的各種行為訊息會被記錄下來，同時會將所產生並被記錄下來的行為訊息傳送至分析區塊進行分析。分析區塊的部份本研究所提出的分析器（Analyzer）收到從執行區塊傳來的行為訊息記錄後會開始進行分析，如果行為訊息被辨識為惡意行為時，分析器會通知執行區塊中止執行階段，接著分析器會將訊息記錄進行統整後產生出行為分析報告（Behavior Report），此報告會顯示此應用程式是否有進行任何可疑的惡意行為，並根據其行為判斷是否為惡意程式。

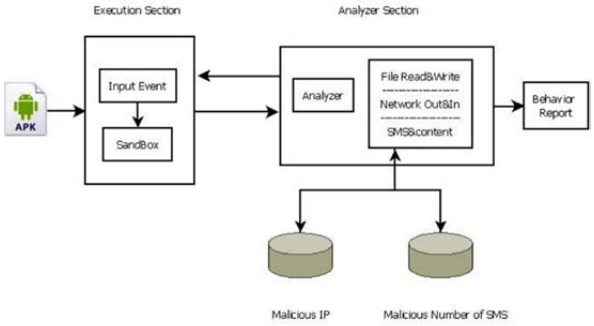


圖 7 系統架構

3.1 Execution Section

執行區塊（Execution Section）的部份主要被區分為兩個部分，(輸入產生器）Input Generator 以及（模擬器）Emulator 兩個區塊。進行分析的過程模擬器區塊會配置一個模擬器，當模擬器建置完成時，傳送過來的.apk 檔案會被送入模型器中，並進入安裝階段，此安裝過程與一般行動裝置上的安裝程序是相似的。當應用程式安裝完成一段時間後，輸入產生器區塊會開始對模擬器傳送輸入行為訊息，對應用程式自動產生輸入訊息以模擬使用者操作 Android 裝置的行為，藉此與應用程式進行互動。在模擬器運作的過程中，所有系統的訊息會被記錄下來，並同時傳送給分析區塊進行分析。

該虛擬機器每當執行完一個應用程式分析就會進行系統初始化的動作，分析結束時會將目前的虛擬機器刪除，在每次進行新的分析前會配置一個新的虛擬機器，以避免前次的實驗影響到本次實驗的結果而造成不必要的誤判。

3.2 Analysis Section

分析區塊(Analysis Section)部份的則有以下三個主要的分析重點：

- Read&Write
- Network Out&In
- SMS Content。

本研究的分析區塊是利用 Python 搭配 hell Script 共同篩寫而成，分析區塊會以上面三個部份為主要對象進行分析，其目的主要是在確認以上這三個部份有沒有出現惡意行為。執行區塊執行的期間，會不斷的將模擬器最新的行為記錄訊息傳到分析區塊區塊，每當分析區塊收到一筆行為記錄訊息，會將該行為訊息記錄傳至自行開發的分析器，會針對該行為記錄訊息以上三個部份進行分析，如果在行為記錄訊息中發現任何惡意的行為，分析器就會發出中止訊息停止執行區塊的運行，並對該應用程式的行為產生一份行為報告。之後會進行實驗環境的復原與初始化的動作，以供下一次的實驗進行。

要判斷是否有惡意行為，必須確認是否有將敏感性資料外洩的行為，行動裝置上的敏感性資料很多，依據其行動裝置規格與使用的應用軟體可能會

有差異，為了要鎖定重要的敏感性資料做為特徵，本研究除了前章所述研究所討論的敏感性資料，另外針對由相關研究單位 Android Malware Genome Project 與 contagion mobile 所提供的真實的惡意樣本進行研究、檢測與分析。所有的行動裝置都會共同擁有的資料為主，惡意應用程式會收集的目標進行探討，本研究定出四種敏感性資料（如表 1 所示）：

表 1 敏感性資料

名稱	敘述
國際移動設備辨識碼 (IMEI)	一般稱作行動裝置序列號、行動裝置唯一碼，由於每一個行動裝置都有其獨立的識別碼，因此又被稱為是行動裝置的身份證。其號碼的組成是由核准序號+產地序號+生產序號+檢驗序號組成。
國際移動用戶識別碼 (IMSI)	在電話網路中用來識別移動用戶的唯一識別碼，一般存在 SIM 卡中。由行動國家碼+行動網路碼+行動用卡識別碼組成。
系統訊息	各類系統裝置的訊息。如：系統版本、裝置型號等
通訊錄訊息	以往的行動裝置上又稱為電話簿，一般可以登記電話持有人的姓名、電話、住址、信箱等個人資訊。

File Read&Write 的部份，有部份的惡意程式會在執行的過程中，收集裝置上面的敏感性資訊並儲存在檔案中，如：xml 檔案。在應用程式執行的過程中在將存有敏感性資料的檔案傳送到遠端伺服器上。

分析重點：

- 追蹤帶有敏感性資料的檔案

Network In&Out 的部份，大部份的惡意程式會在對外網路連線過程中，透過各種方式將敏感性資料傳送到遠端伺服器。通常是以誘騙的方式或是在不通知使用者的情況下，在使用者操作應用程式的過程中，將敏感性資料藏在連線資料中傳送至遠端伺服器。

此外也有部份惡意程式會在程式的運行中誘導使用者操作下載其它的 APK 檔案。其方式有可能透過誘騙使用者該應用程式有新的更新可以使用，或是推薦使用者其它相似的工具來誘騙使用者下載，因此可能在原本的惡意程式中並沒有任何的惡意行為，但是下載的程式確會執行惡意行為。

分析重點：

- 惡意程式會在對外網路連結過程中，並將敏感性資料混入訊息中傳出。
- 惡意程式會在對外網路連結過程中，將含有敏感性資料的檔案向外傳輸。
- 惡意程式會在操作應用程式的過程中下載其它的 apk 檔案。

SMS Content 的部份，從樣本觀察中發現部份惡意程式會在傳送 SMS 訊息時，將該系統的敏感性資料混入 SMS 訊息中傳出。也有一些惡意程式雖然不進行傳送敏感性資料的行為，但是會以一些規律性的行為寄送付費的 SMS 簡訊，

本研究再將以上的行為進行歸納，若有發生以下行為視同異常：

- 發送付費簡訊
  - 短時間內對不同號碼寄送兩封以上簡訊的行為。
  - 對同一個號碼發送簡訊兩次以上的行為。
- 發送的簡訊中會含有系統的敏感性資料。

4. 實驗

4.1 系統建置

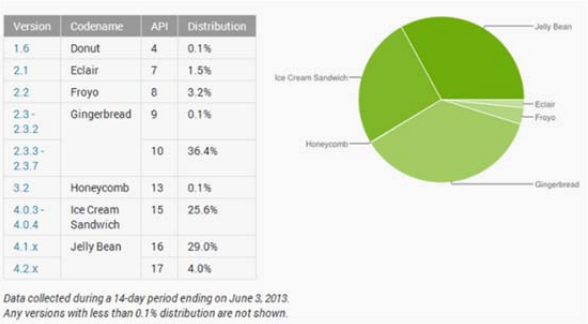


圖 8 Android 平台版本分布

Android 以版本號來說共有四個版本，分別以 1、2、3 與 4 為開頭，部份版本帶有同樣的代號名稱。以平台來區分的話，android 的第 1 版與第 2 版是用於智慧型裝置，第 3 版則是用於平版裝置。而後 Google 為了將方便開發團隊開發，將兩類平台整合為第四版。如圖 8 所示，2013 年 1 月的統計顯示 android 裝置的版本以 Gingerbread(36.5%)、Ice Cream Sandwich(25.6%)以及 Jelly Bean(33%)此三個版本使用率較高，其中又以 GingerBread 所佔的比例最高。由於硬體裝置的限制，很多使用者並無法更新到新版本的 Android 裝置。此外 android 第 2 版與第 3 版的差異主要在於改進開發者平台與使用者介面

上的改進，因此本系統 android 模擬器將以 GingerBread 的版本來進行建置。

4.2 樣本

本研究在惡意樣本方面總共收集到 10 個家族共 135 個樣本，10 個家族的名稱與行為如表 2 所示：

表 2 惡意樣本家族列表

名稱	行為
AnserverBot	在 Android 裝置開啟後門竊取資料傳送到遠端服務器。
BaseBridge	竊取資料傳送到遠端服務器。
BeanBot	受 C&C 服務器控制寄送 SMS 訊息。
Bgserv	獲取使用者手機資訊傳送至特定網址。
DroidKungFu	收集大量訊息記錄在檔案中並傳送至遠端服務器。
GoldDream	竊取資料傳送到遠端服務器
HippoSMS	寄送付費簡訊並攔截簡訊訊息。
Pjapps	在 Android 裝置開啟後門竊取資料傳送到遠端服務器。
RogueLemon	竊取資料傳送到遠端服務器
plankton	受 C&C 服務器控制能夠下載、安裝程式、寄送 SMS 簡訊等。

本研究在良性樣本的取得方面，由於使用者可以取得 apk 檔案的地方不僅止於官方 Google play 市場，也可於其它第三方市場處下載。原本 Google play 市場採用的是使用者回報機制，也就是當使用者發現應用程式為惡意程式時，可以回報並檢舉該應用程式。不過，單憑如此的回饋機制還是不能阻止快速成長的 Android 惡意軟體，因此 2012 年 2 月 Google 在保留原本的回報機制時，另外推出代號為 Bouncer 的安全服務[5]，該服務會在應用程式被遞交至 Google Play 時對應用程式進行分析，其範圍是針對已知的惡意軟體、間諜軟體與木馬程式。

為了盡量避免下載的樣本是遭受污染、惡意的 ，本研究選擇 Google Play 市場上的應用程式做為良性樣本來源，在 Google Play 的市場上應用程式有被分門別類，如表 3 所示。本研究在在各類別中各下載數個應用程式，並只選擇被其它使用者評價為四星等以上的熱門應用程式(最高為五星等)，作為本研究的良性樣本來源。

表 3 良性應用程式類別

交通運輸	新聞與雜誌
個人化	旅遊與地方資訊
健康塑身	漫畫
動態桌布	生活品味
商業	生產應用
圖書與參考資源	社交
天氣	程式庫與試用程式
娛樂	財經
媒體與影片	購物
小工具	通訊
工具	運動
攝影	醫療
教育	音樂與音效

4.3 評估

為評估本系統的在真實情況下的分類效能，我們與 Right Alert 及 Permission Friendly 兩個系統做效能評估分析。我們採用各 135 個惡意及 135 個良性應用程式作為系統測試的樣本，合計共 270 個樣本。

在惡意樣本的偵測率表現如表 4 所示，總計 135 個的惡意程式樣本，Right Alert 將 118 個樣本判別為高風險程式，其惡意判別率有約為 87%。Permission Friendly 將其中 120 個樣本判為高風險程式，其惡意判別率為 88%左右。本系統在 135 惡意樣本中成功視別出 123 個樣本，惡意判別率約為 91%。在惡意漏報率方面，Right Alert 誤判 17 個惡意軟體，約有 12%的惡意漏報率，Permission Friendly 誤判了 15 個惡意軟體，約有 11%的惡意漏報率。本系統則是誤判 12 個軟體，惡意漏報率約為 8%。

本研究在惡意程式偵測方面，約有 8.89%的樣本被誤判成良性軟體，重新手動檢視這些樣本後發現，以 BeanBot 家族為主產生的誤判率較高，8 個樣本中僅認出一個樣本，檢閱 BeanBot 的相關資料，他的行為有向遠方伺服器傳送行動裝置資料或是接收 C&C server 來發送惡意簡訊的行為。經過手動檢查樣本後，可以知道這些程式是偽裝成系統工具讓使用者可以進行應用程式掃描並進行刪除的動作，在操作過該應用程式之後，並沒有產生任何惡意或可疑的行為，有可能是因為 C&C Server 已停止運作，程式在沒有收到命令的情況下並不會執行任何的惡意行為，因此本系統造成了誤判。

在良性樣本的判別率表現如表 5 所示，Right Alert 在 135 個良性樣本中，將 73 良性樣本視別為高風險軟體，良性判別率僅 45%而惡意誤報率達到 54%，而 Permission Friendly 在 135 個良性樣本中，將 109 個樣本視為高風險軟體，良性判別率僅 19%惡意誤報率達到 81%。而本研究在 135 個良性樣本中，將約 10 個樣本視為惡意軟體良性判別率約有 92%惡意誤報率僅約為 7%左右。本系統在分辨良性與惡意程式上擁有較有效的能力。

其全部樣本偵測率如**錯誤! 找不到參照來**

源。6 所示，Right Alert 的分析其準確率為 66%，Permission Friendly 其準確率僅 54%，相較之下，本研究的準確率有 91%，而錯誤率僅約 9%。Right Alert 與 Permission Friendly 是透過權限為基礎來進行風險評估的，接觸到越多行動裝置系統資訊的權限或是與傳送資料有關的權限，這樣都視為是高風險的權限，因為應用程式在擁有這些權限的情況下，例如：讀取行動裝置訊息、網路存取、修改記憶卡等權限，可能造成安全風險較高，因而導致其風險分數偏高。但是在一般的應用程式上，這些權限可能也是程式運行所需要的基本權限，所以在良性樣本的判斷方面，會造成誤判率較高，無法有效做為區分。

本系統在良性程式偵測方面，重新檢視了 10 個被歸類為惡意程式的樣本，發現這些被歸類為惡意程式的應用程式，對外傳送了行動裝置的 IMEI 碼，但是在應用程式的規章中並沒有說明或記載外傳使用者的 IMEI 碼。這些 IMEI 碼在使用者不知情的情況下被廠商用來辨識行動裝置，也沒有透過任何的雜湊加密，這些風險軟體可能會在特定的情況下會造成使用者的資料外洩。

表 4 惡意樣本偵測率

名稱	惡意 (高風險)	良性	TPR	FNR
Right Alert	118	17	87.41%	12.59%
Permission Friendly	120	15	88.89%	11.11%
Proposed	123	12	91.11%	8.89%

表 5 良性樣本偵測率

名稱	惡意 (高風險)	良性	TNR	FPR
Right Alert	73	62	45.93%	54.07%
Permission Friendly	109	26	19.26%	81%
Proposed	10	125	92.59%	7.41%

註:TNR(True Negative Rate)、FPR(False Positive Rate)

表 6 全部樣本偵測率

名稱	惡意 (高風險)	良性	TPR	FNR
Right Alert	191	79	66%	34%
Permission Friendly	229	41	54%	46%
Proposed	133	137	91%	9%

註:TPR(True Positive Rate)、FNR(False Negative Rate)

5. 結論

本研究利用駭客們攻擊行動裝置的最大動機－竊取使用者的資料，透過追縱敏感性資料是否被傳出行動裝置的方式，以區分良性與惡性程式。從結果來說，不論是在區分惡意程式與良性判別方面都取得九成以上的正確率，與舊有的以權限為基礎等研究相比較，不僅能夠更加準確的偵測惡意程式，以往研究在良性樣本上面臨的高誤判率也能夠有效的降低。此外，相較以往動態分析需要報行並收集 10 分鐘以上的系統資訊才能夠進行分析，本系統在執行時間約 3 分鐘左右，就能夠分辨良性或是惡意程式。

在現行平台發展不建全，規章限制不完全的情況下，即使是一般的程式也能夠在不通知使用者的情況下，自由取得使用者行動裝置的資料(在適當的權限下)。此外，開發人員為了開發上的方便直接使用行動裝置機碼來識別使用者或是為了評估自身產品的效益而私底下收集使用者的資訊，在沒有經過適當保護的情況下(如：雜湊加密)，就可能會形成安全上的疑慮，而這些風險軟體也是行動裝置上另一個要解決的問題。 在建置環境方面，現行的 Android 模擬器版本相當多，各個應用程式所需要的套件並不大相同，即使是 Google 官方推出的模擬器也不一定能順利執行每個應用程式，這將使得建置模擬器上出現障礙無法使用同一規格的模擬器來進行測試，使得行為分析平台受到限制。

行動裝置出現的時間雖然不長，但是在近年來硬體科技進步下，行動裝置出現了極大的改變，所以也面臨像電個人電腦般一樣的網路安全問題。行動裝置除了面臨舊有傳統威脅外，也出現屬於該設備才有的網路安全問題。在面對舊有威脅上受限於行動裝置的限制，多數威脅並不能套用傳統的解決方法。同時，新的威脅不斷的出現，對於行動裝置更是一大考驗。在行動裝置上與惡意程式對抗的路還有很長的一段要走，除了各單位在分析與偵測方面的改進以外，也期許行動裝置能夠建立更建全的開發規章來規範開發者，在兩方共進的情況下才能避免更多的惡意程式誕生。

參考文獻

[1] IDC, “Android and iOS Combine for 91.1% of the Worldwide Smartphone OS Market in 4Q12 and 87.6% for the Year , According to IDC ", available at: http://www.idc.com/getdoc.jsp?containerId=prUS23946013, 2012.

[2] McAfee, “McAfee Threats Report:First Quarter 2012”, 2012.

[3] Statista, “Number of available applications in the Google Play Store”, available at: http://www.statista.com/, 2012.

[4] F-Security, “MobileThreatReport Q1 2013”, 2013.

[5] H.Lockheimer, “Android and Security”, available at: http://googlemobile.blogspot.tw/2012/02/android-and-security.html, 2012

應用蟻群最佳化與模糊分群演算法於資料隱私保護之研究

邵敏華 [1]　鄭仁豪 [1]
[1] 國立屏東科技大學資訊管理系
{ mhshao, m10056015 }@mail.npust.edu.tw

摘要

隨著個人隱私資料經常被使用於探勘技術中，如何合理的保護隱私資料，同時又能保證資料的可用性，成為目前資訊安全領域面臨的重大挑戰。匿名化是目前資料在公開發佈環境下實現隱私保護的主要技術之一，而 k-匿名(k-Anonymity)就是一種針對資料匿名化的隱私保護技術，能夠有效防止鏈結攻擊所造成的隱私揭露問題。從過去研究發現，許多方法處理上都是以減少資訊量的損失來建立 k-匿名，而使得資料品質遺失，因此為了確保處理後的資料仍具有分析研究的可用性，本研究提出了一個以蟻群最佳化為基礎於 k-匿名模型的方法，此方法以獲得良好資訊品質為目標，利用蟻群最佳化的穩健性和全域搜尋的優點，透過費洛蒙資訊的更新機制加速螞蟻在搜尋最佳解的執行過程，並結合模糊 C-means 分群法進行分群的改善，因此能有效減少偏離值的影響，達到降低資訊損失量，資訊品質與分群效率的提升，使得分群後的結果具有資料隱私保護能力，並兼顧了安全和資訊的效用。

關鍵詞：k-匿名、隱私保護、蟻群最佳化演算法、模糊 C-means 分群演算法、資料探勘、屬性。

1. 前言

隨著網際網路的蓬勃發展，資訊科技的各項技術與應用，使得企業的資料量不斷快速的累積增加，當企業面臨重要決策時，決策者要如何在這龐大的資料中取得有用資訊以幫助企業制定營運策略模式，這時資料的彙整與分析便相當重要[3]。但不可忽略的是，在這些資料當中可能隱含著企業交易客戶的基本資料，例如到購物中心選購日常生活用品或到醫院掛號看診，我們都會留下自身的基本資料，也因為網路的普及，資訊呈現高度透明化，這些隱密資料可能在相互傳遞的過程中存在著被有心人士竊取個資的可能風險，因此，對這些涉及個人隱私之基本資料採取預先防範的保護動作便成為相當重要的議題。

當資料在做特定用途時，必需經過隱私保護處理方能發佈，而 k-匿名(k-Anonymity)就是一個有效使用於保護個人資料不被他人識別(Identification)出來的技術[1][8][9]，主要是以分群演算法為基礎將資料依標準識別符號屬性(即可以識別個人身份的屬性欄位，例如年齡、性別、郵遞區號等)作為分群基準，將資料分為一群相似的群集後，再將每一相似群集分別進行泛化(Generalization)或抑制(Suppression)等處理方式將資料本身進行去識別化(De-identification)，為確保資料不被辨識則必需控制資料的揭露程度以滿足 k-匿名條件[1][7]，否則會破壞原先資料的完整性，因此，要做到資料的隱私保護與完整性，亦能提高在執行探勘上的效率，是當前研究所要追求的目標。

蟻群最佳化(Ant Colony Optimization，ACO)屬於萬用啟發式演算法的一種，隸屬於資料探勘技術，是藉由觀察自然界中螞蟻尋找食物的過程中，找尋出距離最短的路徑。從過去研究[1][7][8][9]中整理了近年來 k-匿名的各種方法，發現鮮少探討萬用啟發法則於 k-匿名上，為此本研究提出以 ACO 與 FCM 分群演算法結合於 k-匿名的方法，首先資料先經過 ACO 演算法執行群集運算，使用費洛蒙資訊作為資料在進行分群時機率計算之依據，依序作指派動作，然後在每一回合螞蟻找出現階段最佳解後，再將其作為 FCM 的初始群中心和初始分群數，藉由 FCM 的改善，以找尋出更佳的解，強化分群後的結果，使資訊品質能夠更好。一般當匿名 k 值越大，對資料隱私的保護效果會越好，被識別的機率等於 1/k，因此，個人資料就很難被辨識。

2. 文獻探討

2.1 k-匿名模型

k-匿名是由學者 Sweeney 於 2002 年所提出的一種隱私保護模型[8], [9]，其用途是保護資料隱私不被惡意攻擊者使用鏈結攻擊辨識以及有效解決標準識別符號(QI)揭露隱私問題的資料匿名化技術。

資料匿名化處理的原始資料，例如統計資料、醫療數據等，一般以資料表形式儲存，而且表中的每一筆記錄對應一個個人(包含多個屬性欄位)。這些屬性欄位可以分為三類，如下：

1. 唯一標識符號(Explicit Identifier)

可以唯一清楚標識單一個體的屬性，例如姓名、身份證字號、電話等；而為保護個人隱私資料安全，資料在發佈前會做加密或刪除的動作。

2. 標準識別符號(Quasi-Identifier，QI)

令表 T{P_1,…, P_n}為一個有限資料筆數(元素)的資料表，而屬性{P_1,…, P_n}為表 T 的有限屬性集合。假設這一資料表是一個有著 n 個屬性維度的資料表，且定義 N 為資料表中的資料總筆數。

給定一資料表 T{P_1,…, P_n}，而屬性的子集合{P_i,…, P_j}⊆{P_1,…, P_n}是表示{P_i,…, P_j}的所有元素屬性屬於{P_1,…, P_n}，且一筆資料的 t∈T，則 t{Pi,…, Pj}為{Pi,…, Pj}在 t 中的屬性值{Vi,…, Vj}；因此，T{P_i,…, P_j}可以表示表 T 在屬性{P_i,…, P_j}上的總集合。

3. 敏感屬性(Sensitive Attribute，SA)

指包含隱私資料的屬性，如圖 1(a)為一個原始客戶交易資料表，且每一筆記錄對應一個唯一的客戶姓名，其中{Name}為 Identifier，而{Race, Zip Code, Sex, Age}為 QI，{Goods}則為 SA。

(a) 未經匿名化之客戶交易資料表 T

	Identifier	Quasi-Identifier (QI)				
	Name	Race	Zip Code	Sex	Age	Goods
1	Mike	White	94130	Male	21	NB
2	Ivy	White	94138	Female	28	CD
3	Ben	Black	94140	Male	32	Book
4	Davy	Asian	94149	Male	39	Cup

(b) 匿名化後之客戶交易資料表 T* (k=2)

	Identifier	Quasi-Identifier (QI)				
	Name	Race	Zip Code	Sex	Age	Goods
1	Mike	White	9413*	Gender	[20, 30]	NB
2	Ivy	White	9413*	Gender	[20, 30]	CD
3	Ben	Person	9414*	Male	[30, 40]	Book
4	Davy	Person	9414*	Male	[30, 40]	Cup

圖 1 客戶交易資料表

接著，再以圖 1(a)舉例，假設在表 T 中的標準識別符號(QI)如果滿足 k-匿名條件時，表示在 QI 中的屬性集合的每一種組合必需在 T 表中至少出現 k 次。唯一標識符號(Identifier)指可以直接識別出個人真實身分的屬性(例如：姓名、電話、身分證字號)。標準識別符號(Quasi-Identifier，QI)指在公開資料表中，一種以上的欄位屬性在其他的公開資料表當中也有相同的屬性，而這些屬性是可以識別出個人的真實身份。圖 1(a)為未經過匿名化處理之客戶交易資料表，圖 1(b)為客戶交易資料表達 2-Anonymity 狀態(k=2)後的匿名之結果，匿名過後的資料表一般以 T*作表示之。

2.2 k-匿名之匿名技術

目前 k-匿名的研究主要集中在如何對原始資料表進行有效的匿名化，即實現匿名效果最好、資料可用性最高、且時間空間成本花費最小。資料匿名化一般採用兩種基本操作方式使得資料表滿足 k-匿名的條件，分別為泛化(Generalization)與抑制(Suppression)[8]，該技術不同於一般的扭曲、擾亂和隨機化等方法，它能夠保持發佈前後資料的真實性與一致性。

首先，泛化是對資料的屬性進行更廣義、抽象的描述，且不失原意。屬性的種類可以區分成類別型屬性與數值型屬性兩種，如圖 2(a)Race 為類別型屬性，可以(White→Person)進行泛化動作，而圖 2(b)Zip code 為數值型屬性，可以使用符號「*」進行泛化(94140→9414*→941**→*****)，因此，可以將 94140 與 9414*之間表示為 94140 $\leq_D$9414*，而為符合上述的泛化關係則必須滿足：(1) ∀ D_i, D_j, D_z ∈泛化域：$D_i \leq_D D_j$, $D_i \leq_D D_z \Rightarrow D_j \leq_D D_z \vee D_z \leq_D D_j$，(2)在所有的泛化域中，最高的泛化層級必定為單一節點。由此可知，泛化層級越高，資料匿名的程度越高，故可以明顯看出泛化是將底層的資料做模糊化，且泛化後的資料和原始的資料有相關性。

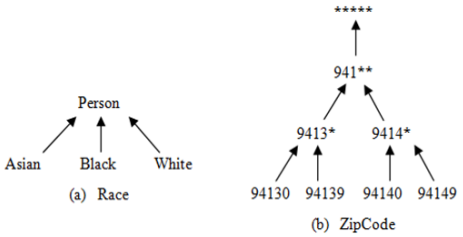


圖 2 屬性泛化層級示意圖

在 k-匿名化過程中，若某些記錄無法滿足 k-匿名條件時，一般採取抑制操作，係指在資料表或各類資料中，某些資料為了不被清楚辨識，採取的動作是將部份資料的相對應屬性利用其他符號作代替、隱藏或者刪除，亦即不發佈該屬性，以保持統計的特性，但由於抑制的轉換，隱藏的資料會有部份被破壞。

2.3 蟻群最佳化演算法

蟻群最佳化演算法(Ant Colony Optimization，ACO)是觀察真實世界的螞蟻覓食行為與特性將其轉換成數學模式，螞蟻在找尋食物的移動過程中會釋放出一種稱為"費洛蒙(Pheromone)"的化學物質，作為彼此溝通的工具[10][11][12][13]，因此其他的螞蟻便能間接得知食物位置，且可以此為依據來記錄行走的路徑，供後續抵達的螞蟻藉由殘留在路徑上的費洛蒙作為選擇移動路徑時的參考。

由於 ACO 是一個近似貪婪演算法的概念，亦

是一種找尋最佳解的方法，優點在不斷改善解字串(尋找周圍最佳解，然後往更佳的解作移動)，每次移動時都只選擇目前最佳的，直到無法改善為止。

1. 狀態轉換機率

在狀態轉換機率中，主要是利用開發(Exploitation)與探索(Exploration)兩種轉換機制來尋找路徑節點上要拜訪的下一個城市節點。

首先，開發指螞蟻依據目前最好的解來選擇下一個要走的城市，$u \in Jk(r)$表示 k 隻螞蟻在城市 i 所能選擇的城市 j (即已拜訪過的城市不能再重複拜訪)，如公式(1)；而 η 是一期望值，為 $1/d_{ij}$ 的倒數，q 則為一個介於 0~1 之間的隨機的參數設定值。

$$s=\begin{cases}\arg\max_{u\in Jk(r)}\{[\tau_{ij}(r,u)]\cdot[\eta_{ij}(r,u)]\}^{\beta} & ,\ if\ \ q\in q_0\\ S & ,\text{otherwise}\end{cases} \quad (1)$$

探索是指螞蟻會以隨機(Random)方式去挑選下一個要走的城市，可以增加解的廣度，如公式(2)；β 參數為控制城市之間關係程度之係數值。

$$S=P_k(r,s)=\begin{cases}\dfrac{[\tau_{ij}(r,s)]\cdot[\eta_{ij}(r,s)]^{\beta}}{\sum_{u\in Jk(r)}[\tau_{ij}(r,u)]\cdot[\eta_{ij}(r,u)]^{\beta}} & ,\ if\ \ s\in Jk(r)\\ 0 & ,otherwise\end{cases} \quad (2)$$

2. 費洛蒙更新

當螞蟻走過某一條路徑時會釋放費洛蒙在路徑上，而在路徑上的費洛的蒙濃度會隨著時間不斷更新揮發，其更新方式分為區域更新(Local Update)和全域更新(Global Update)兩種。區域更新指當每一隻螞蟻行經該路徑時會立即釋放費洛蒙作更新動作，即揮發與增加該路徑上的費洛蒙濃度。全域更新是指當全部螞蟻拜訪完所有城市後，每一隻螞蟻各自會產生一組解字串(Solution String)，將最佳的前幾組解依序作排序，更新最佳解路徑上的費洛蒙濃度矩陣，加速螞蟻在搜尋最佳解的執行過程。

2.4 模糊 C-means 分群法

模糊C-means分群法(Fuzzy C-means，FCM)是根據K-means分群演算法所衍生出來的模糊分群法，使用模糊邏輯(Fuzzy Logic)概念提升分群效果，由於具有"模糊"的特性，因此能利用隸屬函數(Membership function)使資料在不同情況下可以隸屬於不同的群集，不再絕對地屬於某一群集，而是以隸屬值(介於0~1)來表示資料隸屬於某一群集的程度[4]。在給定一個U上的一個模糊集A的定義為

對任何$u \in U$都指定了一個數$u_A(u) \in [0, 1]$與之對應，

因此$u_A(u)$稱為u對A的隸屬度，表示為$u_A: U \mid \rightarrow [0, 1]$且$u \mid \rightarrow u_A(u)$，這意味著此映射成為$A$的隸屬函數。從過去文獻知道，為分離出各資料所重疊的資訊，FCM是利用權重(Weight)方式給予模糊權重(Fuzzy weight)值，目的是希望能夠把偏離值的影響降到最低，以提高分群後的資料品質，因此FCM是有能力處理具重疊(Overlap)特性的資料[5]，這明顯會比傳統的資料分群法要來的合適且有效率。

計算目標函數值J_m，其計算如公式(3)。

$$J_m=\sum_{i=1}^{c}J_i=\sum_{i=1}^{c}\left(\sum_{j=1}^{n}u_{ij}^{m}\left\|X_j-C_i\right\|^2\right) \quad (3)$$

在執行FCM演算法時，需先設定初始參數，在各參數給定後，接著才開始計算初始群集中心，如公式(4)。

$$C_i=\frac{\sum_{j=1}^{n}u_{ij}^{m}X_j}{\sum_{j=1}^{n}u_{ij}^{m}} \quad (4)$$

一般在計算目標函數值時，J_m值越小表示每一群集內的資料相似度越高，分群結果就越好；待J_m值計算好(數值最小)後，接著就可以計算每一筆資料與各群集之間的隸屬度，最後做FCM的模糊矩陣的更新動作，如公式(5)。

$$u_{ji}=\frac{1}{\sum_{k=1}^{c}\left(\frac{\left\|X_j-C_i\right\|}{\left\|X_j-C_k\right\|}\right)^{\frac{2}{m-1}}} \quad (5)$$

FCM的收斂條件是當$|J_m^{(t+1)}-J_m^{(t)}|<\varepsilon$符合終止條件時就停止，否則繼續執行計算，直至符合終止條件為止。

3. 研究方法

本研究根據研究問題，以 ACO 與 FCM 作結合來建構出本研究之演算法流程，也因為是用於 k-匿名，因此將其命名為 KFACO 分群演算法(k-Anonymity of Fuzzy C-means and Ant Colony Optimization)。我們依據螞蟻在資料點與群組的選擇、目標函數的計算，以及費洛蒙更新來執行資料的分群，利用 ACO 全域搜尋的分群處理特性，將大量資料劃分成數個群集，在 ACO 階段結束後，接著再藉由 FCM 進行分群結果的改善，提高在經過匿名化後的資料分群準確性，最後，透過費洛蒙資訊的更新機制，加速螞蟻在搜尋最佳解的執行過程，使匿名化後的資料擁有更好的資訊品質，降低資訊量損失。圖 3 為本研究之研究流程架構。

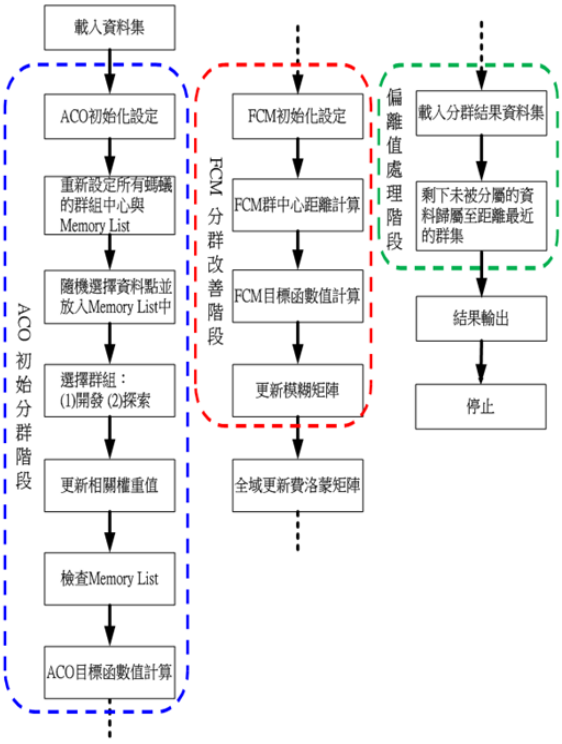


圖 3 研究流程架構

本演算法共分為三個階段，主要是以 ACO 為基礎，輔以 FCM 作結果的改善。

階段 1：ACO 初始分群階段

執行 ACO 全域搜尋作分群處理，結合 k-匿名隱私保護方法，使大量的資料不受偏離值影響，每一群集內的資料異質性最低，資訊量的損失降至最低，以求解出穩定的分群品質。

階段 2：FCM 分群改善階段

以 FCM 區域搜尋作階段 1 分群結果的強化，使用模糊權重於各群集中的資料，重新做計算，以改善資料的分群品質。

階段 3：偏離值處理階段

最後，於階段 3 處理剩下未被分群完整的偏離值(即雜訊)；最後做結果的輸出。

3.1 KFACO 分群演算法

本研究提出的KFACO分群演算法主要是利用 ACO 在全域搜尋上的優點，輔以 FCM 區域搜尋特性，來找出最佳分群數目及群集中心，使得求解出來的資訊品質能夠更好，也由於採用 FCM 中的模糊規則與權重進行推理，因此在穩健性與有效性上較好；KFACO 演算法的執行步驟如下：

步驟 1：測試資料集載入

將資料集依照 Identifier、QI、SA 三種屬性類別作劃分。將 Identifier 做刪除以保護原始資料，然後再篩選出 QI 做資料點轉換，轉換成 x 和 y 軸的數值型資料點，以便佈署於二維空間中。

步驟 2：ACO 初始參數設定

將費洛蒙濃度矩陣進行初始化，設定人工螞蟻數、菁英螞蟻數、疊代次數設為 0、門檻值 q_0 大小。

步驟 3：ACO 迴圈初始化

重新設定所有螞蟻的群中心與記憶表單(Memory List)。

步驟 4：資料點選擇

開始建構解(Solution)的次迴圈，在每個次迴圈執行時，每一隻螞蟻會以隨機的方式選擇下一個資料點，將已經選過的資料點置入螞蟻的記憶表單(已選過的資料點不能重複選取)中。

步驟 5：群組選擇

當一隻螞蟻所搭載的資料點 i 選擇群組時，有開發與探索兩種方式。選擇的方式是產生一隨機值 q(介於 0~1)，並與初始設定門檻值 q_0 作比較，如果 q 小於 q_0，則挑選現階段最佳的群組做配對；如果 q 大於 q_0，則依據 $P_k(r,s)$計算出機率值進行群組選擇。在群組選擇完畢之後，更新資料點 x_i 與第 j 群之間的關係權重值 W_{ij}。如果資料點 x_i 屬於第 j 群時，則 W_{ij} 設為 1；如果資料點 i 不屬於第 j 群的話，W_{ij} 則設為 0；相關公式如公式(6)及(7)所示。

$$W_{ij} = \begin{cases} 1, & \text{if data } i \text{ is clustered into cluster } j \\ 0, & \text{otherwise} \end{cases}$$

$$\text{Minimize } J(W, C) = \sum_{i=1}^{m} J_i = \sum_{j=1}^{g} w_{ij} \left\| x_i - c_j \right\| \quad (6)$$

$$\text{where} \left\| X_i - C_j \right\| = \sqrt{\sum_{v=1}^{n} (x_{iv}, c_{jv})^2} \quad (7)$$

其中 g 為預設分群數、m 為資料點總數、n 為資料維度數目、X 是資料矩陣、C 則是群中心矩陣、W 代表權重矩陣、x_{iv} 為資料點 i 的第 v 個屬性值、c_{jv} 係指在第 j 群中的所有資料點的第 v 個平均屬性值。

步驟 6：檢查記憶表單

每一隻搭載資料點的螞蟻的記憶表單是否已填滿，若沒有則返回到步驟 3 重新執行，反之則繼續往下執行。

步驟 7：計算 ACO 目標函數值

所有螞蟻已經建構出完整解，且每一隻螞蟻會搭載一組解字串(Solution string)，而計算出來的目標函數值 J 可用來判斷哪一隻螞蟻的解字串是較佳的，依照大小作遞增(由小到大)排序，而第一個解為本次迴圈的最佳解，然後再將產生的最佳解當作 FCM 的初始輸入，用來做為分群結果的改善。

步驟 8：FCM 初始參數設定

承接 ACO 的次迴圈最佳解和目標函數值。設定權重係數 m 和終止條件 ε、模糊矩陣 U，疊代次數設為 1。

步驟 9：計算 FCM 的群中心和目標函數值

為了求得最佳的目標函數值 J_m，我們針對各輸入的參數進行微分計算，當 J_m 小於我們設定的容忍誤差時，停止疊代計算，否則返回步驟 7 重新執行。

步驟 10：更新模糊矩陣 U

待資料點與群集之間的群中心之隸屬程度計算出來後，立即更新模糊矩陣 U。此時如果

$|J_m^{(t+1)} - J_m^{(t)}| < \varepsilon$ 則停止計算，否則返回步驟 9 重新執行。

步驟 11：費洛蒙矩陣的更新

我們採取費洛蒙"全域更新"方式，如公式(8)。在 ACO 搭配 FCM 找到分群最佳解後，判斷如果找到的解比原先 ACO 的解要來的更好的話，就依照新的解作為費洛蒙更新之依據，否則就依照原來的解作費洛蒙更新動作。其中 t 表示時間(即迴圈次數)係數、ρ 為費洛蒙遺留下來的係數、$(1-\rho)$為費洛蒙揮發係數。

$$\tau_{ij}(t+1) = (1-\rho)\tau_{ij}(t) + \Delta\tau_{ij} \quad i = 1,\ldots,m \; ; \; j = 1,\ldots,g \tag{8}$$

$$\Delta\tau_{ij} = \begin{cases} \frac{M}{d_{ij}} & (v_i, v_j) \in path_{best}(t) \\ 0 & else \end{cases}$$

步驟 12：是否已達到最大迴圈次數

在更新完費洛蒙濃度矩陣後，檢查是否已達 ACO 最大迴圈次數，如未達到，則返回步驟 2 讓所有螞蟻重新執行出發，找尋下一個迴圈的解。如果已達最大迴圈次數，則停止該演算法，輸出目前的結果，此時所輸出的解就是本演算法所能找到最佳解的資料分群結果。

步驟 13：偏離值處理

在經過分群處理過後，我們將得到的分群結果中未被指派的偏離值依照距離平方公式計算歸屬至距離最近的群集之中，最後才是我們所要的分群結果，然後才做輸出動作。

3.2 資訊損失量之量測

學者 Byun 於 2007 年提出一種用來度量資料在匿名化過程中，資料所損失的量值的計算方法[6]，如公式(9)。

$$D(G_k) = \sum_{i=1}^{m} \frac{Max_i(G_k) - Min_i(G_k)}{Max_i(T) - Min_i(T)} + \sum_{j=1}^{q} \frac{H(T_{c_j}(G_k))}{H(T_{c_j})} \tag{9}$$

在本研究中我們加入了權重的概念以作為計算各個資料點對每一群集的資訊損失量為基礎，如公式(10)。

$$D(G_k) = \sum_{i=1}^{m} \left(\frac{Max_i(G_k) - Min_i(G_k)}{Max_i(T) - Min_i(T)} \right) * W_{m_i} + \sum_{j=1}^{q} \left(\frac{H(T_{c_j}(G_k))}{H(T_{c_j})} \right) * W_{q_j} \tag{10}$$

在 $WG(G_k)$的 $Max_i(G_k)$、$Min_i(G_k)$、$Max_i(T)$、$Min_i(T)$、$H(T)$ 等因子跟原本 $D(G_k)$ 的因子一樣不變時，Wm_i 跟 Wq_i 表示使用者對該欄位所給予的權重值，而整個資料表的總體資訊損失量的計算如公式(11)。

$$IL(T) = \sum_{k=1}^{g} IL(G_k) \tag{11}$$

	Zip Code	Age	Gender
G_1	12713	21	Male
G_1	12451	23	Female
G_1	12411	34	Female
G_2	12736	39	Male
G_2	12713	30	Female
G_2	12799	20	Male

圖 4 資訊損失量計算之範例資料表

舉例來說，圖 4 的欄位給予的權重值分別為 *ZipCode*=3、*Age*=2、*Gender*=1，如果圖 4 當中的前三筆資料為資料集 G_1，而後三筆資料為資料集 G_2，則資料集 G_1 的資訊損失量計算結果為：$IL(G_1)=3*(\frac{34-21}{39-20}*2+\frac{2}{2}*3+\frac{1}{1}*1)=16.105$，而資料集 G_2 的資訊損失量計算結果則為：$IL(G_2)=3*(\frac{39-20}{39-20}*2+\frac{1}{2}*3+\frac{1}{1}*1)=13.5$。因此，我們在經由上述計算，可以得到整個圖 4 資料集的總體資訊損失量為 $IL(T)$= 16.105 + 13.5 = 29.605，而資料集 G_2 的資訊損失量要比資料集 G_1 的資訊損失量來的較小。因此，本研究的目標函數值為求得每一個群集的權重資訊損失量最小化，也就是 *Min*(*Function*)，即 *Function*=$L(G_k)$。

3.3 偏離值的處理

在經過階段 1 與階段 2 分群計算過後，各個資料點都已經被歸屬至某個群集之中，假如所有群集的大小皆已經滿足 k 筆資料，則將剩餘資料，也就是偏離值(Outlier)依照距離平方公式計算，將其計算結果指派至最接近的群集之中，這樣可以不必受群集大小的限制，便可以得到一個完整的群組集合，且所包含在內的任一群集皆已經滿足 k-匿名的條件限制，並且具有良好的資料分群品質。

4. 實驗設計

4.1 開發工具與實驗平台

本研究在開發工具上以 Microsoft Visual Studio 2010 for C#作編寫，以 Intel Core(TM) i5-2500 CPU@3.30GHz 之中央處理器與 4GB 之記憶體為實驗平台，作業系統為 Windows 7。

4.2 測試資料

本研究採用國際通用資料庫，資料來源為 UCI repository of machine learning databases 網站上[2]所下載的 Adult dataset，是一般用來評估 k-匿名結果的公開資料集，在刪除遺漏值不採計部分，總共剩有 30,162 筆資料做為本實驗測試之用；相關資訊如圖 5 所示。

Data Set Characteristics：	*Multivariate*	Number of Instances：	*48842*
Attribute Characteristics：	*Categorical, Integer*	Number of Attributes：	*14*
Associated Tasks：	*Classification*	Area：	*Social*

圖 5 Adult dataset

4.3 資料預處理

將實驗的 Adult dataset 載入，依照使用者自訂方式對其做資料前置處理，我們將屬性欄位劃分為 QI、Identifier、SA 三種屬性類別，如圖 6 所示。

資料行名稱	資料類型	允許 Null
aid	int	☑
age	int	☑
education	int	☑
workclass	nvarchar(50)	☑
maritalstatu	nvarchar(50)	☑
occuption	nvarchar(50)	☑
race	nvarchar(50)	☑
gender	nvarchar(50)	☑
nativecountry	nvarchar(50)	☑
salary	nvarchar(50)	☑
x	nvarchar(50)	☑
y	nvarchar(50)	☑

圖 6 Adult dataset 欄位設定

在執行 k-匿名資料保護之前，我們必須先觀察資料集中的每一個屬性欄位，以了解存於資料集的屬性是數值型(Continuous)屬性資料還是類別型(Categorical)屬性資料，而圖 7 為我們將 Adult dataset 載入 SQL Server 後，資料經過維度轉換處理後，已經從真實資料轉換成 x 軸和 y 軸的數值型資料點型態，並且佈署於二維的空間之中，方便做分析。

	aid	age	education	workclass	maritalstatu	occuption	race	gender	nativecountry	salary	x	y
1	25848	25	10	Private	Separated	Adm-clerical	White	Female	United-States	<=50K	-0.041941	-0.040405
2	25851	35	10	Private	Married-civ-spouse	Handlers-cleaners	White	Male	United-States	<=50K	0.020246	0.20513
3	25865	32	10				White	Male	United-States	<=50K	0.094149	0.15186
4	25879	20	10				White	Female	United-States	<=50K	0.012343	-0.0026182
5	25880	27	10				Black	Male	United-States	<=50K	-0.054915	-0.034662
6	25883	34	10				Black	Male	United-States	>50K	-0.02132	0.17828
7	25885	24	10				White	Male	United-States	>50K	-0.0035234	-0.01026
8	25887	20	10				White	Female	United-States	<=50K	0.0084819	-0.0012812
9	25888	51	10				White	Male	United-States	<=50K	0.033219	0.032732
10	25892	19	10				Black	Male	United-States	<=50K	0.024896	0.0019971

圖 7 資料維度轉換

4.4 實驗分析

本研究主要是以 k-匿名隱私保護為主，在實驗驗證部份將會採用現有 k-匿名的隱私保護資料分群演算法作為本研究的實驗對照組。在比較的項目上主要以資訊損失量總和及分群品質為主，如下：

1. 總體資訊損失量

在本實驗階段因為對照組和本研究的方法在資訊損失量的計算公式不一定相同，在比較時會針對實驗對照組的資訊損失量計算方式，與本研究的方法之分群結果下去計算，方便進行比較；而本研究的資訊損失量計算方式也亦會用於對照組的分群結果下去做計算並進行比較。

2. 資訊品質

依照資料分群在各階段的處理方式的不同，將執行的 k-匿名分群結果進行比較，針對群集之間的變異程度做比較，以便做分群品質的評估。

5. 結論

本研究基於以資料的隱私保護為前提下，為了維持資料在做探勘時的可用性，故設計了以螞蟻覓食時的特性為基礎，讓資料集當中的資料欄位的屬性資料能夠依據 k-匿名理論進行資料分群的動作，同時還要符合隱私保護的基本要求。

在現階段我們將先以小樣本模擬演算法之執行過程，未來在實驗的驗證部分，將針對 KFACO 演算法所建構出的資料分群結果來計算資訊損失量、執行時間與不同參數下之執行結果。而因為對照組和本研究的方法在資訊損失量的計算公式不一定相同，所以在比較時會將對照組的資訊損失量計算方式針對本研究的方法之分群結果下去計算，進行比較；而本研究的資訊損失量計算方式也亦會用於對照組的分群結果下去做計算並進行比較。在資訊品質方面會依據系統執行 k-匿名所分群出來之分群結果好壞與對照組做相互的比較。

總體而言，本研究由於結合具有全域性和穩健性優點之 ACO 演算法與具有優良分群品質及能夠處理具重疊性資料的 FCM 分群法兩者，在分群結果上將能夠達到改善資料解品質的效果，使得分群效率進而提升，降低資訊損失量，在提升高資訊效用的同時亦能夠達到保護個體隱私權益之目的。

參考文獻

[1] A. Friedman, R. Wolff and A. Schuster, "Providing k-Anonymity in Data Mining," in the VLDB Journal, Israel, 2007, pp. 789-804.

[2] C. Blake and C. Merz. Uci Repository of Machine Learning Databases. 1998.

[3] C. Legany, S. Juhasz and A. Babos, "Cluster Validity Measurement Techniques," the 6th International Symposium of Hungarian Researchers on Computational Intelligence, 2006, pp. 388-393.

[4] J. C. Bezdek, "Pattern Recognition with Fuzzy Objective Function Algorithms," Plenum, 1981.

[5] J. C. Dunn, "A Fuzzy Relative of the ISODATA Process and Its Use in Detecting Compact Well-Separated Clusters," Journal of Cybernetics, 1973, pp. 32-57.

[6] J. W. Byun, A. Kamra, E. Bertino and N. Li, "Efficient K-Anonymization Using Clustering

Techniques," in Internal Conference on Tabase Systems for Advanced Applications, USA, 2007.
[7] K. LeFevre, D. J. DeWitt and R. Ramakrishnan, "Mondrian Multidimensional K-Anonymity," in Proceedings of the 22nd IEEE International Conference on Data Engineering, USA, 2006.
[8] L. Sweeney, "Achieving K-Anonymity Privacy Protection using Generalization and Suppression," International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, USA, 2002.
[9] L. Sweeney, "K-Anonymity: A Model for Protecting Privacy," International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, USA, 2002, pp. 571-588.
[10] M. Dorigo, V. Maniezzo and A. Colorni, "Ant System: An Autocatalytic Optimizing Process," Technical Report No.91-016, Italy, 1991.
[11] M. Dorigo and L. M. Gambardella, "Ant colony system: a cooperative learning approach to the traveling salesman problem," IEEE Transactions on Evolutionary Computation, 1997, pp. 53-66.
[12] O. A. Mohamed Jafar and R. Sivakumar, "Ant-based Clustering Algorithms: A Brief Survey," International Journal of Computer Theory and Engineering, 2010, pp. 1793-8201.
[13] P. S. Shelokar, V. K. Jayaraman and B. D. Kulkarni, "An ant colony approach for clustering," Analytica Chimica Acta, India, 2003, pp. 187-195.

以合理輸入值驗證為基礎之預存程序組合型 SQL 指令植入式攻擊防禦

陳威霖　　田筱榮
中原大學資訊工程系
W.L.Chen@cycu.org.tw　tyan@ice.cycu.edu.tw

摘要

SQL 指令植入式攻擊(SQL Injection Attack)可能導致與網路服務相連的資料庫系統遭受破壞或是資料庫內的資料遭到竊取。過去的研究多以防禦 SQL 指令植入式攻擊為目的，然而對於以預存程序(Stored Procedure)為對象的攻擊較缺乏防禦做法，在本研究中我們將防禦範圍擴展到能處理發生於預存程序內的組合型 SQL 指令植入式攻擊。在靜態分析階段，除了分析網頁原始碼之外，並針對資料庫內的預存程序內容做分析，找出使用者輸入參數與程序內 SQL 指令之間的關係，在動態分析階段，使用者進行參數輸入時能夠檢查參數代入預存程序內與 SQL 指令結合後是否產生 SQL 指令植入式攻擊，將其阻擋並拒絕請求。藉由我們的防禦機制，使用者和網頁程式設計師可以不需知道防禦程式如何運作狀態下即可達到防禦效果；系統管理者只需將防禦程式掛載於網頁伺服器端即可達到防禦功能。

關鍵詞：網頁應用程式安全、SQL 指令植入式攻擊、輸入驗證、預存程序

Abstract

SQL injection attacks may lead to data theft, content destruction, even database crash. Many defense mechanisms have been proposed to resolve explicit SQL injection attacks, where the attacks take advantage of the web application programs. However, defense against SQL injection attacks aiming at stored procedures provided by supporting database system have not been successfully addressed. In this study, we extend the input legitimacy validation method to SQL injection attack on stored procedures. Besides the web application program, the statics analysis is also performed on the stored procedures provided by database system to obtain knowledges on the relationships between user input parameters and the stored procedures. During on-line dynamic analysis phase, input parameters are verified according to the previously derived knowledges. If a potential SQL injection attack is detected, the user request will be rejected before forwarding to the web application programs. The proposed enhancement to the original method provides a more comprehensive defense on SQL injection attacks. Our method is transparent to users and web application program designers. It provides effective defense with no need to rewrite application programs.

Keywords：Web application security, SQL injection attacks, input validation, Stored Procedure

1. 簡介

在科技不斷進步的時代，網際網路成為人們生活中不可或缺的一環，對於網站技術而言，大部分都是使用動態網頁，例如：PHP(Hypertext Preprocessor)、JSP(JavaServer Pages)、ASP(Active Server Pages)，搭配資料庫系統來運作，伴隨著網路安全威脅事件日漸增加的趨勢，假如這些網站沒有受到相當程度的防護，往往會成為駭客們覬覦的對象，例如：SQL 指令植入式攻擊，造成系統檔案損毀或是個人資料外洩。

根據 OWASP Top Ten Project[3]提到 2010 年至 2013 年十大安全弱點中 Injection 排名高居第一，SQL 指令植入式攻擊包含在 Injection 之中，利用 SQL 語法的特性去組合輸入的字串，與網頁程式中的 SQL 指令組合出含有惡意的請求，造成網頁伺服器和資料庫系統遭受破壞或是給予預期之外回應，導致資訊安全受到嚴重的威脅。

因為 SQL 語法能夠允許多種不同指令層層組合，所以 SQL 指令植入式攻擊種類也非常多樣化，從輸入驗證(Input Validation)的角度來探討 SQL 指令植入式攻擊方式，可以分類為恆值邏輯(Tautologies)、註解化(Commentization)、嵌入查詢(Embedded queries)、預存程序(Stored procedures)四大類型。

SQL 指令植入式攻擊通常是程式設計師的疏失或是經驗不足所造成的漏洞，如果要修補程式漏洞，需要重新檢視程式，從中找出有問題的程式碼，但此種方法需大費周章且不切實際，所以將重點擺放於網頁應用程式開發完成上線運作狀態，使用者送出請求後網頁伺服器接收參數時針對使用者輸入的合理性驗證，我們主要目的是設計一個不需更動網頁應用程式原始碼的防禦機制，而且延續[1][2]採用輸入驗證(Input Validation)的方式來防禦 SQL 指令植入式攻擊，驗證方式並非單純的對參數做特徵過濾，而是在離線狀態時對網頁原始碼和資料庫內容做分析，接著上線運作階段在網頁伺服器接收請求時利用離線狀態分析所得之資訊來檢查使用者輸入的請求參數是否構成 SQL 指令植入式攻擊，因此具有容許非典型輸入值的可能。除了延續[1][2]的作法，我們將防禦範圍擴展到能夠處理發

生於預存程序內的組合型 SQL 指令植入式攻擊，針對此攻擊將提出修正版的合理輸入值驗證機制。

接下來第二節會介紹 SQL 指令植入式攻擊防禦的相關研究與成果；第三節會說明我們的分析規劃與系統架構；第四節為實作，將會展示我們的系統如何防禦 SQL 指令植入式攻擊，並討論改良後的結果；第五節則是結論和未來工作。

2. 相關研究

SQL 指令植入式攻擊的防禦階段分類，根據（圖 1），應用程式開發完成上線運作狀態，此狀態又可分為四個階段來探討，使用者送出請求階段是屬於瀏覽器端防禦，後面三個皆屬於網頁伺服器接收請求階段、應用程序執行階段、送出 SQL 請求存取資料庫階段，皆屬於伺服器端的防禦。

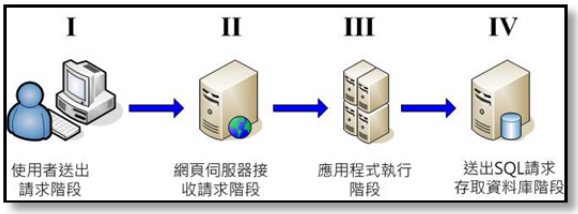


圖 1. SQL 指令植入式攻擊之防禦階段分類

至目前為止，針對 SQL 指令植入式攻擊已有許多方法能夠偵測與防禦，防禦類型通常可分為靜態、動態、動靜態混合式防禦，也因為於方法不同，所以能夠防禦的攻擊種類與特色各有差異，如(表 1)。

表 1. SQL 指令植入式攻擊相關研究比較表

	Taut.	Com.	Embedded	Stored proc.	不需要更動程式碼	上線運作階段
Input Legitimacy Validation[1][2]	○	○	○	X	○	II
ModSecurity[4]	○	○	○	○	○	II
SQL Guard[10]	○	○	○	X	○	III
SQL Check[11]	○	○	○	X	○	III
WASP[12]	○	○	○	○	X	III
SQL-IDS[13]	○	○	○	○	○	IV

Taut.：恒值邏輯　Com.：註解化
Embedded：嵌入查詢　Stored proc.：預存程序

輸入合理性驗證 (Input Legitimacy Validation)[1][2] 系統架構分成靜態分析與動態分析兩部分，靜態分析是掃瞄出網頁程式內含有 SQL 語法部分，並產生「參數元素過濾檔」，提供給動態分析來判定網頁伺服器接收到的參數有無符合 SQL 指令植入式攻擊

ModSecurity[4]是屬於網路應用程式防火牆，利用正規表示法(Regular expression)編譯規則集，使用規則制定特徵進行 SQL 指令植入式攻擊過濾。

Buehrer、Weide 和 Sivilotti 提出 SQL Guard 的方法[10]，其做法是在程式執行時會產生語法樹，將程式碼裡的 SQL 指令和語法樹做比對。

Wassermann 和 Su 提出 SQL Check 的方法[11]，其做法是事先產生定義好語法樹，在程式碼裡將 SQL 指令和事先產生定義好的語法樹做比對。

Halfond、Orso 和 Manolios 提出 WASP 的方法[12]，其做法是在網頁程式碼轉換成 bytecode 時，將疑似有弱點的參數加入檢測用的字串作為標記，並立即過濾檢查，但此做法會更動程式碼，有可能會影響原本程式執行的目的和結果。

Kemalis 和 Tzouramanis 提出 SQL-IDS 的方法[13]，其做法是使用特徵比對方法，佈署在應用程式送出 SQL 請求至資料庫之間，使用規則過濾 SQL 指令植入式攻擊，其判斷的準確度會依據特徵制定嚴謹度有所不同。

3. 分析規劃與系統架構

3.1 分析規劃

我們主要目的是設計一個不需更動網頁應用程式原始碼的 SQL 指令植入式攻擊防禦系統，並以[1][2]提出的方法為基礎，將輸入合理性驗證檢查延伸至預存程序的輸入參數大到防止預存程序內的組合型 SQL 指令植入式攻擊的目標。

在前人的研究中所提出的防禦機制是將系統架構分成靜態分析和動態分析兩部分，靜態分析是在系統處於離線狀態時事先對網頁程式碼做掃描檢查的動作，找出程式碼內含有 SQL 語法部份，針對 SQL 語法的內容結構產生「參數元素過濾檔」，並在動態分析時利用靜態分析產生的「參數元素過濾檔」來判定伺服器接收自使用者傳來的請求字串是否含有 SQL 指令植入式攻擊。

但此方法無法有效偵測預存程序內的組合型 SQL 指令植入式攻擊，因為使用預存程序在網頁程式碼中是找不到任何 SQL 語句，只能在網頁上找到預存程序的呼叫指令，僅知道欲呼叫之程序名稱以及傳入的參數內容，而不知道程序內 SQL 語句結構，將無法判斷程序傳入之參數所對應的 SQL 欄位名稱是如何組合而成的。如果只單純判斷傳入的參數，將可能會導致嚴重的誤判或漏判情形發生，所以在我們的系統架構上，靜態分析步驟會特別針對資料庫裡的預存程序內容做分析，找出程序內的 SQL 語句搭配傳入的參數做結合，產生一份資訊提供給動態分析步驟做為參考，判斷預存程序內的 SQL 語句是否有構成 SQL 指令植入式攻擊。

3.2 系統架構

這是完整的預存程序系統分析架構(圖 2)，結合了靜態分析與動態分析，接下來將會分別詳細介紹靜態分析以及動態分析的組織架構和運作流程。

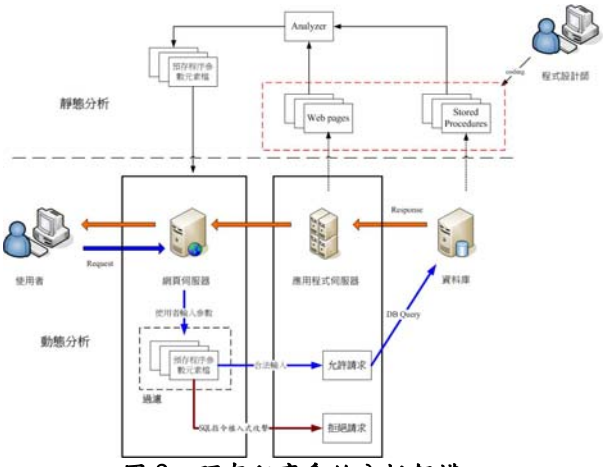


圖 2. 預存程序系統分析架構

3.2.1 靜態分析

靜態分析的架構如(圖 3)，這是使用者對伺服器送出請求，配合網頁應用程式的執行，向資料庫送出 SQL 請求，得到相對應的結果回傳至使用者。在進行一系列的步驟之前，我們會先在離線狀態時做出分析動作。首先我們會針對網頁上掃瞄出有呼叫預存程序的指令，接著在資料庫將預存程序的程式碼匯出成為可分析的檔案，搭配在網頁上欲呼叫的程序名稱和參數進行分析，最後組成一個預存程序參數元素檔，此檔案中所記錄的資訊是為了在動態分析時能夠辨別使用者輸入請求參數的性質，可以判斷使用者輸入的參數型態、長度是否符合，並分辨出單一型參數或是組合型參數。

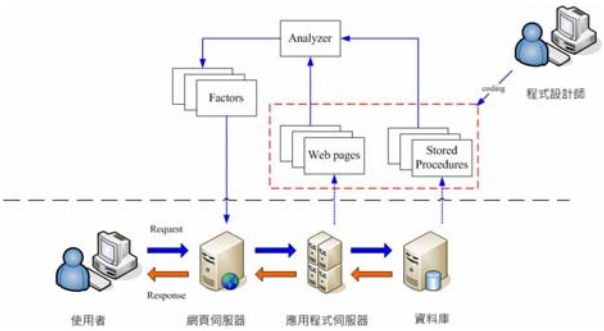


圖 3. 靜態分析架構

接下來以(圖 4)來說明靜態分析的流程和步驟。

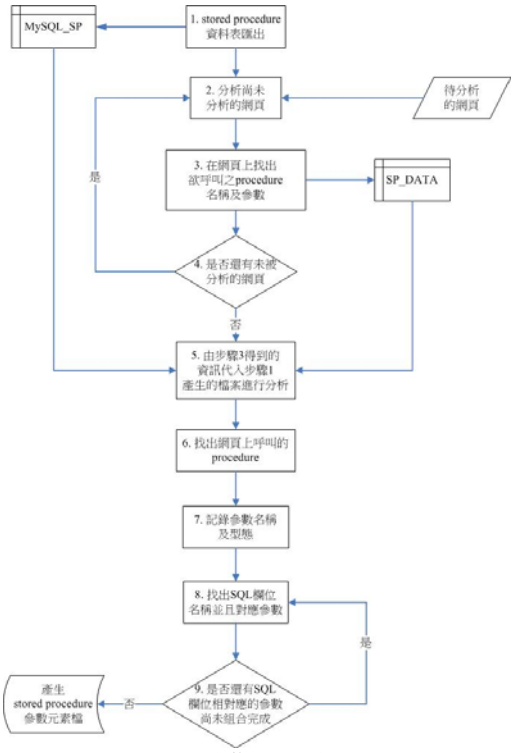


圖 4. 靜態分析流程圖

1. 將預存程序從資料庫匯出，如(圖 5)。

```
DELIMITER //
CREATE DEFINER=`root`@`localhost` PROCEDURE
`sp_test`(IN uname VARCHAR(50), IN pin1
VARCHAR(50), IN pin2 VARCHAR(50), IN pin3
VARCHAR(50))
BEGIN
SET @sql=CONCAT('select * from school where
id =\'', uname, '\' and pwd =\'', pin1, pin2, pin3, '\'
# select student info');
PREPARE stmt FROM @sql;
EXECUTE stmt;
END //
DELIMITER ;
```

圖 5. 預存程序匯出資料表

2. 開始掃瞄網頁原始碼是否有出現預存程序呼叫的指令。
3. 在網頁程式碼中找出欲呼叫之程序名稱及參數並記錄下來，如(圖 6)。

```
sp_test(id, pwd1, pwd2, pwd3)

sp_test1(uname, password)

sp_test2(id)
```

圖 6. 網頁原始碼呼叫預存程序指令

4. 重覆步驟 2、3，直到所有網頁分析完成。
5. 由步驟 3 的資訊代入步驟 1 的檔案進行分析。
6. 找出呼叫的程序名稱進行分析。
7. 記錄程序的參數名稱、型態、長度。
8. 找出 SQL 欄位名稱並且找出相對應的參數。
9. 如果是組合型參數，將其組合完成並且對應給 SQL 欄位名稱。

以上步驟都完成後，將產生一份預存程序參數元素檔如(圖 7)。

```
#sp_test
$uname, VARCHAR, 50
$pin1, VARCHAR, 50
$pin2, VARCHAR, 50
$pin3, VARCHAR, 50
@id, uname
@pwd, pin1, pin2, pin3
```

圖 7. 預存程序參數元素檔

3.2.2 動態分析參數過濾

此階段為上線運作狀態，如(圖 8)，在網頁伺服器端接收使用者輸入的參數，並且參照靜態分析階段產生的預存程序參數元素檔來過濾使用者輸入之參數，防止使用者輸入的參數代入預存程序內與 SQL 語句結合後可能造成 SQL 指令植入式攻擊的問題發生。

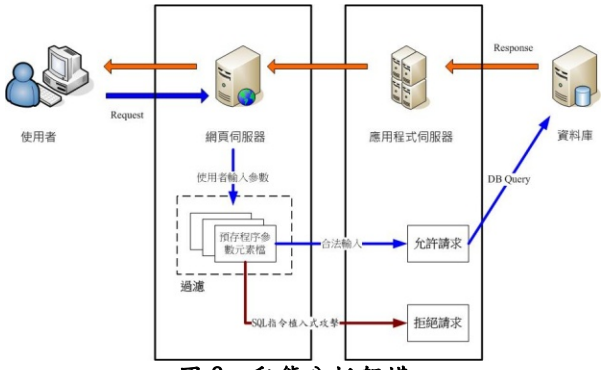


圖 8. 動態分析架構

動態分析的參數過濾流程如(圖 9)，首先取得使用者輸入參數，接著依照靜態分析階段產生的預存程序參數元素檔針對組合型參數做參數結合動作，然後進行參數型態檢查、字串檢查，確認參數代入預存程序內是否形成 SQL 指令植入式攻擊。

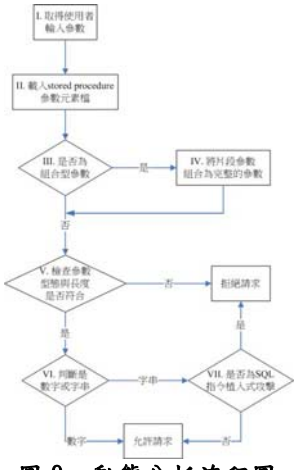


圖 9. 動態分析流程圖

I. 取得使用者在網頁上輸入的參數。

II. 載入靜態分析時產生的預存程序參數元素檔做為判斷之依據。

III. 根據預存程序參數元素檔內容判斷使用者輸入的參數是否為組合型參數。

IV. 如果是組合型參數，如(圖 10)，將片段參數組合為完整參數。

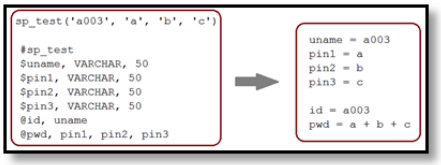


圖 10. 預存程序組合型參數

V. 檢查參數的型態以及長度是否有符合預存程序參數元素檔內記錄之標準，如果不符合便拒絕使用者輸入的請求。

VI. 判斷參數是字串還是數字，因為字串可能含有 SQL 指令植入式攻擊，必須進一步檢查，如果是數字則直接允許請求。

VII. 如果參數是字串的話則進入字串檢查流程，如(圖 11)，判斷出參數字串中含有 SQL 指令植入式攻擊特徵，將拒絕請求，若無 SQL 指令植入式攻擊特徵，將允許請求。

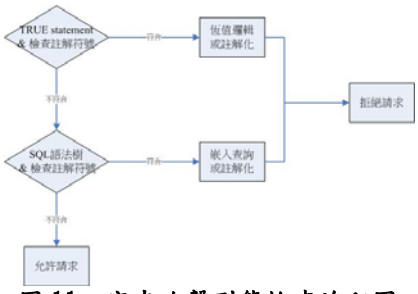


圖 11. 字串攻擊型態檢查流程圖

(1) 判斷字串中是否包含運算子和註解符號：

SELECT student FROM test.school WHERE id='a001' AND pwd='' **OR 1=1 --**;

若運算子存在且運算式為恆等式，例如：1=1、0<1，且運算式前有出現邏輯運算子，例如：AND、OR，則判定使用者輸入的參數為恆值邏輯的 SQL 指令植入式攻擊。

若 SQL 語句中有出現註解符號，例如：--、#，將判定使用者輸入的參數為註解化的 SQL 指令植入式攻擊。

(2) 檢查 SQL 語法中是否有嵌入第二段 SQL 語句：

SELECT student FROM test.school WHERE id='' **UNION SELECT math FROM test.score WHERE id='a001' --** ' AND pwd='111';

我們使用 SQL 語法樹來輔助判斷，如(圖 12)，藉由語法樹架構來分析每一段字串，判別是否含有嵌入查詢的 SQL 指令植入式攻擊。

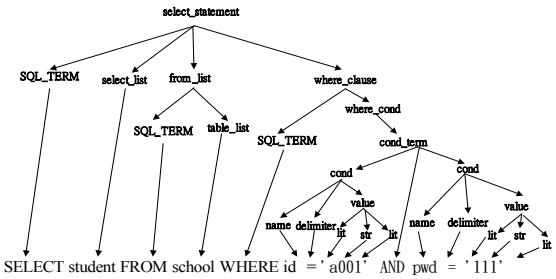


圖 12. SQL 語法樹

4. 實作與討論

為了驗證我們的方法能夠抵擋在預存程序內發生的 SQL 指令植入式攻擊。在 4.2 節我們將會示範展示實作的系統如何防禦 SQL 指令植入式攻擊。

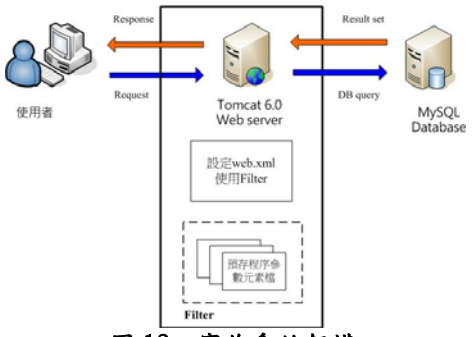


圖 13. 實作系統架構

4.1 實作環境

本實驗所使用的網頁伺服器為 Tomcat6.0，網頁應用程式使用 JSP 做編輯，資料庫伺服器則是使用 MySQL Server 5.1，並安裝於相容的作業系統(Windows 7 64-bit)。另外我們在 Tomcat 中的 web.xml 設定所有 JSP 及 servlet，全部套用 web.xml 中所制定的<filter>。

4.2 實作與防禦

我們實作的登入系統之中，SQL 語句是寫在預存程序內部，並非在網頁原始碼中，在網頁原始碼只看的到程序的呼叫指令以及傳入程序的參數，如(圖 14)，是正常輸入帳號密碼登入系統所得到的資訊，密碼部份是利用 3 組參數所組合起來的完整字串對應給程序內的 SQL 欄位。

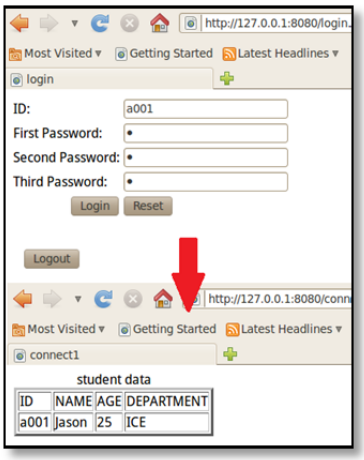


圖 14. 實作範例(正常登入)

接著我們將含有 SQL 指令植入式攻擊的惡意字串(a' OR 1=1#)拆散，分別寫在密碼部份的 3 組參數做為請求，如(圖 15)，即可成功登入系統，且將資料庫內所以資料全部顯示出來。



圖 15. 實作範例(SQL 指令植入式攻擊)

若在網頁伺服器 Tomcat 中的 web.xml 掛載 Filter，啟動防禦系統，將會在靜態分析時蒐集資訊產生一份「SP_FACTOR.txt」預存程序參數元素檔，如(圖 16)，並且在使用者輸入參數送出請求後，依照「SP_FACTOR.txt」的內容分析使用者輸入參數，假如判斷內容含有 SQL 指令植入式攻擊，將其阻擋拒絕請求，並將網頁導向錯誤訊息畫面，如(圖 17)。

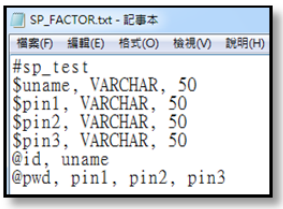


圖 16. sp_test 的參數元素檔內容

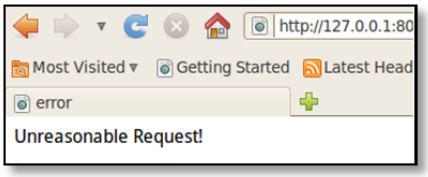


圖 17. 實作範例(成功防堵 SQL 指令植入式攻擊)

4.3 討論

實作中我們發現，在靜態分析時對預存程序的傳遞參數以及內部的 SQL 語句徹底分析，例如：判斷對應給 SQL 欄位的參數是單一型還是組合型，若是組合型參數，再判斷參數的排列順序為何。有了充足的資訊，在動態分析時即可有效阻擋預存程序內部發生的 SQL 指令植入式攻擊。另外我們延續[1][2]的特點，不需要更動網頁應用程式原始碼，只需在網頁伺服器 Tomcat 的 web.xml 中設定好需要掛載的防禦系統(Filter)，即可達到防禦效果。

5. 結論與未來工作

SQL 指令植入式攻擊是一項已經存在許久的攻擊手法與威脅，但此問題始終一直發生，而且攻擊排名統計居高不下。防禦方面，在應用程式開發階段，除了本身加強程式撰寫的能力，減少程式漏洞產生以外，在應用程式上線運作時，網頁伺服器端加上一道防禦系統以防堵 SQL 指令植入式攻擊也是一個完善的解決方法。

我們延續[1][2]的研究特點，在離線狀態時先做靜態分析，針對資料庫內的預存程序內容產生一份預存程序參數元素檔提供給動態分析時參考，在動態分析時，網頁伺服器接收參數，並根據靜態分析產生的預存程序參數元素檔進行分析，檢查參數代入程序內與 SQL 語句結合後是否會產生 SQL 指令植入式攻擊。我們的防禦機制與[1][2]同樣不限制網頁應用程式撰寫語言，以及網頁伺服器選擇，但目前實作的防禦系統僅能在 Tomcat 網頁伺服器上執行，以及使用 JSP 撰寫的網頁應用程式做檢查。

未來我們將針對不同的網頁應用程式上做偵測防禦，例如：PHP、ASP，在不同的網頁伺服器上掛載我們的防禦系統，例如：Apache、IIS。另外，希望能在靜態分析掃瞄預存程序內容時，加入檢查會受程序流程影響而改變的 SQL 指令，例如：條件式(if、else)、迴圈(while、for)…等，並且在動態分析時依據影響程序流程的條件式做檢查，正確找出要執行的 SQL 指令。

參考文獻

[1]. 吳靜茹，「以合理輸入值驗證為基礎之 SQL 指令植入式攻擊防禦」，中原大學研究所，碩士論文，中華民國九十八年七月。

[2]. 李安娜，「以合理輸入值驗證為基礎之組合型 SQL 指令植入式攻擊防禦」，中原大學研究所，碩士論文，中華民國一○○年七月。

[3]. OWASP Top Ten Project https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[4]. ModSecurity Open Source Web Application Firewall http://www.modsecurity.org/

[5]. Wu X.R. and Chan P.P.K, "SQL injection attacks detection in adversarial environments by k-centers", *IEEE Machine Learning and Cybernetics (ICMLC), 2012 International Conference on (Volume:1), Page406 – 410, 15-17 July 2012*

[6]. Sruthy M., Manesh T., and Varghese P., "SQLStor: Blockage of stored procedure SQL injection attack using dynamic query structure validation." *Intelligent Systems Design and Applications (ISDA), 2012 12th International Conference on*. IEEE, 2012, *Page 240 – 245, 27-29 Nov. 2012*

[7]. Moosa A., "Artificial Neural Network based Web Application Firewall for SQL Injection", *World Academy of Science, Engineering & Technology; Vol. 64, p12, Apr 2010.*

[8]. Ezumalai R., Aghila G., "Combinatorial Approach for Preventing SQL Injection Attacks", *Advance Computing Conference, 2009. IACC 2009. IEEE International, 6-7 March 2009, India*

[9]. Khochare N., Chalurkar S. and Meshram B.B., "Web Application Vulnerabilities Detection Techniques Survey", *IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.6, June 2013*

[10]. Buehrer G.T., Weide B.W., and Sivilotti P.A., "Using parse tree validation to prevent SQL injection attacks." , *International Workshop on Software Engineering and Middleware (SEM) at Joint FSE and ESEC*, pages 106–113, Sept. 2005.

[11]. Wassermann G. and Su Z., "The Essence of Command Injection Attacks in Web Applications", *33rd Annual ACM SIGPLAN - SIGACT Symposium on Principles of Programming Languages*, pages 372-382, Jan. 2006.

[12]. Halfond W., Orso A. and Manolios P., "WASP: Protecting Web applications using positive tainting and syntax-aware evaluation." *Software Engineering, IEEE Transactions on 34.1 (2008): 65-81.*

[13]. Kemalis K. and Tzouramanis T., "SQL-IDS: a specification-based approach for SQL-injection detection." *2008 ACM symposium on Applied computing, pages 2153-2158, 2008.TSE, 34(1):65, 2008*

使用靜態分析與機器學習以偵測 Android 惡意程式

蘇民揚* 張文銓
銘傳大學資訊工程學系
*minysu@mail.mcu.edu.tw irons7654321@gmail.com

摘要

相對於個人電腦上已有的安全防護，智慧型手機是新興的平台，其安全防護措施比電腦薄弱。Android 智慧手機目前的使用者對於行動通訊資訊安全的意識薄弱，往往沒看清楚軟體的要求權限，就跳出視窗按確定，以至於手機被植入病毒都不知道，而在 Android Market 中，也有很多惡意軟體會偽裝成遊戲或者圖片被使用者下載，然後再進行如惡意消費、手機資源消耗、協助犯罪，或者竊取資料等等，所以本篇研究將著重在防範惡意程式被安裝在 Android 智慧型手機上。研究內容為透過 Android 應用程式的許可權(permission)與程式碼函式來分析是否為惡意程式，並利用基於機器學習的加權分析來提高精確度。

關鍵詞：Android、智慧型手機、安全、許可權、機器學習。

1. 前言

這幾年來智慧型手機等行動設備的發展相當迅速，並結合了 Wi-Fi 和 3G 無線網路的技術使得手機的用途大大的提升，但在使用者享受手機所帶來的便利之餘，網路所帶來的威脅也漸漸影響到日漸強大的智慧型手機。

智慧型手機是一種類似個人電腦，具有獨立的作業系統，並且可以通過自行安裝或官方更新各種軟體程式，像是許多工具與遊戲等等。通過這些程式可以不斷的對智慧型手機進行功能擴充，而且也可以通過行動網路(wifi、3G 等)來進行網路行為，這一類型的手機就統稱為智慧型手機。智慧型手機的作業系統有相當多種，常見的作業系統為: Nokia 的塞班(Symbian)、微軟作業系統(Windows phone)，蘋果作業系統(iOS)、Linux 相關作業系統(含 Android, WebOS 等)、黑莓作業系統(BlackBerry OS)。

現今智慧型手機的主流，非 Google 的 Android 和 Apple 的 IOS 莫屬，其中 Android 手機最大特色在於其作業系統屬於開放原始碼，讓各個公司都能自行衍生、創作，且每位開發者所撰寫的程式都能發佈到 Market 供人下載，讓使用者能安裝各種不同的軟體客製化屬於自己的手機。相對其他智慧型手機系統，Android 系統具高度自由，在 linux 或 windows 主機上都可以進行開發，且在實體手機上執行也無須額外花費，只有在打算將完成的程式上架時，才需要購買開發者帳號。Android 開發者帳號只要 25 美金，帳號期限為無限期，間接導致免費軟體較多，其軟體豐富性深受使用者的喜愛，目前為市場占有率最高的作業系統，而且銷售量也不斷的增加。

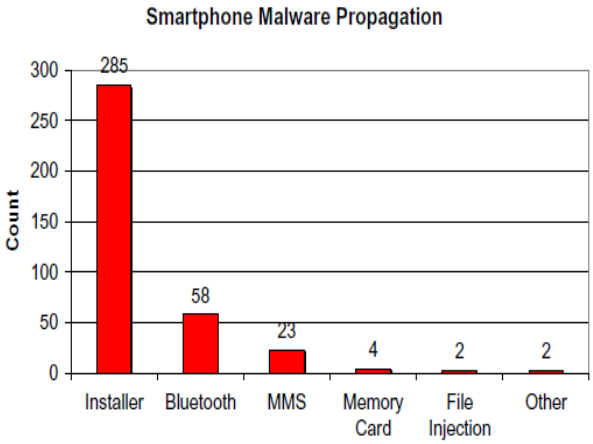


圖 1：智慧型手機惡意程式傳播途徑[1]

本研究的主要目的是要防範惡意程式被安裝在 Android 智慧型手機上，如圖 1 顯示了惡意軟體傳播方式，由此可知，大部分惡意軟體都是使用者在不知道的情況下安裝的。Android 系統的安裝檔為 APK(全名為 Android Package)，任何程式都需要封裝成副檔名為 .apk 的檔案，在經過使用者允許後安裝在手機上，因此即使下載到惡意程式檔案，只要不被安裝到手機上，該惡意程式就不會造成威脅。本篇研究根據許可權(permission)組合來分析使用者欲安裝的程式是否為惡意程式，並利用基於機器學習的分析來提高精確度。這將使得使用者可以在第一時間阻止惡意程式下載與安裝。

2. 相關研究

Android 由於開放原始碼的緣故，惡意程式的數量逐年快速增加，因此吸引許多專家學者從事這方面的研究，像是 W. Enck 等人[2]提出了一個基於核心的 Android 惡意程式行為分析檢查。該系統收集 Linux 層和應用程式的日誌並進行分析，其日誌內有系統紀錄與目標應用程式的事件。這是一種輕量級的偵測惡意程式機制，可以在安裝 Android 應用程式時比對惡意程式特徵。然而他們的研究有個重大的問題就是惡意程式有辦法避免在應用程式日誌上留下紀錄，因此僅能透過 Linux 層日記來協

助判斷。

A. P. Felt 等人[3]認為，Android 許可權限系統的目的是通知使用者安裝應用程式的風險，因此 Android 使用者是否注意且理解各種許可權限是相當重要的，但作者根據 308 位 Android 使用者進行了兩次調查，發現只有 17%的使用者注意到安裝過程中的權限，而只有 3%的使用者能正確回答出三種權限的功能。因此作者指出目前的 Android 應該提高使用者對許可權限的關注和理解，以確保安全。

M. Nauman 等人[4]指出，雖然 Android 有許可權限機制這個安全系統，但是當使用者想要安裝 Android 應用程式，就必須允許所有請求的許可權限，且沒有辦法對特定情況進行權限限制。因此作者提出的 Apex 框架允許使用者有選擇性地授予許可權限，因此可以更加嚴謹與安全的使用許可權限。

M. Zhao 等人[5]的研究使用 SVM 算法建構一個惡意程式檢測框架:AntiMalDroid，其基於特徵碼分析並可以檢測到惡意程式和它們的變種，還可以動態且有效地運行和擴展惡意程式特徵庫。A. Apvrille 和 T. Strazzere[6]提出一個靜態分析方法，採用 39 種不同的標誌，例如 Java API 調用、嵌入可執行文件的存在、代碼大小與網址等等。每個標誌都被分配一個不同的權重，基於統計計算哪些是 Android 惡意程式撰寫者最常使用在他們的程式碼中。

A. Shabtai, Y. Fledel, and Y. Elovici 三人[7]的研究運用機器學習（ML）技術，從 Android 的應用程式文件萃取資訊。例如從 Android 的 Java 字節碼(即特徵萃取，dex 文件）和其他文件類型像是 XML 文件等等。該文中重點擺在 Android 應用類型的其中兩種類型：工具和遊戲，實驗結果成功分類遊戲和工具。這種機器學習方法也可運用於檢測 Android 惡意程式。

3. 研究方法

3.1 Permission 許可權介紹

許可權(也被稱為許可權限、權限)是一種 Android 手機上的安全系統，Android 為避免手機功能遭濫用，透過設置許可權，可以讓使用者有效的知道且管理手機資源。若程式需用到某功能，開發者就要在程式中宣告許可權。目前最新版本中，Android 總共有 130 個許可權，圖 2 中顯示部分許可權。

收集程式許可權限的方法:1. 透過手機自帶的檢驗機制(圖 3)來取得程式的許可種類；2.透過萃取工具來取得程式的許可種類。透過萃取工具的這個方法，是使用一個萃取工具 apktool[8]進行提取 AndroidManifest.xml 檔案(圖 4)裡面的許可權。本篇研究主要是透過此工具取得資料集中所有應用程式的許可權類型。

Category	Android Permissions
Contacts	WRITE_SYNC_SETTINGS, WRITE_CONTACTS, READ_CONTACTS, MANAGE_ACCOUNTS, GET_ACCOUNTS, ACCOUNT_MANAGER
SMS-MMS messages	WRITE_SYNC_SETTINGS, WRITE_SMS, VIBRATE, SET_ORIENTATION, SEND_SMS, RECEIVE_SMS, RECEIVE_MMS, READ_SMS, FLASHLIGHT, BROADCAST_SMS
Call Log	VIBRATE, PROCESS_OUTGOING_CALLS, FLASHLIGHT, CALL_PHONE, CALL_PRIVILEGED
Audio & Video	WRITE_EXTERNAL_STORAGE, SET_ORIENTATION, RECORD_AUDIO, MODIFY_AUDIO_SETTINGS, GLOBAL_SEARCH, FLASHLIGHT, BLUETOOTH, BLUETOOTH_ADMIN, CAMERA
Tasks & Calendar	WRITE_CALENDAR, REORDER_TASKS, READ_CALENDAR, GLOBAL_SEARCH, GET_TASKS, BLUETOOTH_ADMIN
Browser History	WRITE_SYNC_SETTINGS, WRITE_HISTORY_BOOKMARKS, READ_HISTORY_BOOKMARKS
Images	WRITE_EXTERNAL_STORAGE, SET_WALLPAPER_HINTS, SET_WALLPAPER, SET_ORIENTATION, READ_FRAME_BUFFER, GLOBAL_SEARCH, FLASHLIGHT, BLUETOOTH, BLUE-TOOTH_ADMIN, CAMERA

圖 2: 部分 permissions 類型

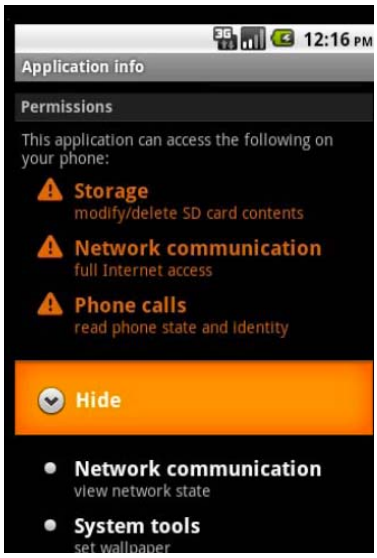


圖 3: 安裝程式時的 permissions 請求

```
<?xml version="1.0" encoding="utf-8"?>
<manifest ...
  xmlns:android="http://schemas.android.com/apk/res/android">
    <uses-sdk android:minSdkVersion="8" android:targetSdkVersion="14" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.BROADCAST_STICKY" />
    <application android:label=...>
        ...
    </application>
</manifest>
```

圖 4： AndroidManifest.xml 檔案

3.2 資料集

本研究資料集總共收集 534 個 Android 應用程

式，其中又分成訓練集與測試集。訓練集中正常程式共 201 個，惡意程式共 60 個，合計 261 個應用程式；測試集中正常程式共 213 個，惡意程式共 60 個，合計 273 個應用程式。表 1 為資料集正常程式的數量與分類，表 2 為資料集惡意程式個數。

正常程式來源為 Google Play[9]中熱門推薦的前幾頁，這些被熱門推薦且排在最前面幾頁的應用程式，絕大部分都是使用者下載數多與評分高，因此本研究將其視為正常程式；而惡意程式的來源是來自 contagio mobile dump[10]這個網站，他們收集的這些惡意程式都有附上防毒公司或防毒網站的檢測報告，因此可以確信其為惡意程式。

將各應用程式取出的許可權限進行統計，若有使用該許可權限，就設為 1；沒有便設為 0，如此就可以建立出相鄰矩陣(adjacency matrix)用來記錄每個應用程式與每個許可權限的對應關係。

3.3 分析方法

對於惡意程式而言，有些 permission 是重要且常常需要的，因此有必要找出這些惡意程式常用的 permissions。例如:INTERNET(將偷取的資料傳送給攻擊者)，或是 SMS_SEND(進行發送大量簡訊的破壞行為)。

本文中將透過機器學習分類的多種演算法來進行偵測惡意程式正確率的比較。

表 1: 資料集正常程式

	訓練集正式程式	測試集正常程式	數量
休閒	18	22	40
益智	20	26	46
工具	24	23	47
社交	24	26	50
通訊	24	24	48
多媒體	23	23	46
程式庫	23	22	45
街機與動作遊戲	20	22	42
生產應用	25	25	50
總數	201	213	414

表 2: 資料集惡意程式

	訓練集惡意程式	測試集惡意程式	總數
數量	60	60	120

機器學習是設計和分析能使電腦可以自動「學習」的演算法，並可通過經驗自動改進的演算法。也就是說，機器學習演算法從數據中自動分析獲得規律，並利用規律對未知數據進行預測。

機器學習演算法通常分為三種不同類型：監督式學習、無監督式學習、半監督式學習。監督式演算法，訓練數據集必須要有正確答案（例如：某一個應用程式是否為惡意程式）。無監督式學習演算法試圖將數據依相似性進行群聚，因此數據不需要正確答案。最後，半監督式學習演算法混合使用具有正確答案和沒有正確答案的數據，相對於無監督學習提高了準確度。因為本研究的資料集皆有標示是否為惡意程式，因此用監督式機器學習進行分析。以下介紹本研究使用的幾種演算法:

1. 貝氏網路為一有向量的非循環圖形，由節點(Nodes)與連結線(Edges)所組成，其中每個節點都有一組狀態機(Condition Probability Tables)。

2. 單純貝氏分類(Naïve Bayes)也稱為樸素貝氏分類或簡單貝氏分類，主要是根據貝氏定理(Bayesian Theorem)來預測分類的結果，是一種簡單且實用的分類方法。

3. 類神經網路使用大量簡單的人工神經元來模仿生物神經網路的能力，由很多非線性的運算單元(我們叫神經元 Neuron)和位於這些運算單元間的眾多連結所組成，這些運算單元通常是以平行且分散的方式在作運算，因此可以同時處理大量的資料，而這樣的設計就可以被用來處理各種需要大量資料運算的應用上。在 weka 工具中，MultilayerPerceptron 就是一種類神經網路，本研究使用它來進行分類。

4. 支持向量機(SVM)對於一群在空間中的資料，希望能夠在該空間之中找出一個超平面(Hyperplan)，並且希望此超平面(Hyperplan)可以將這些資料切成兩群(如:群組 A、群組 B)。屬於群組 A 的資料均位於 Hyper-plan 的同側，而群組 B 的資料均位於 Hyper-plan 的另一側，如此就將不同類別的資料完美的分開。超平面與不同類別的距離愈大愈好。在 weka 工具中 SMO 就是一種支持向量機，本研究使用它來進行分類。

5. k-最鄰近法(k Nearest Neighbor, k-NN)，KNN 是屬於案例學習(Instance -based learning)中的一種方法，KNN 將每個案例(instance)表示為 n 維空間上的一個點。假設空間中存在若干已分類好的樣本案例(sampling instances)，面對一個未知類別的案例『x』時，KNN 演算法會找出樣本案例中與『x』最接近的 k 個案例，其中多數者之類別即判斷為『x』之類別。本研究使用的 IBK 是一種 KNN 的演算法，並設定 k=1, 2, 3 進行分類。

6. 決策樹是一種語意樹(Semantic Tree)，與資料結構中的樹狀結構相仿，皆擁有根(Root)、節點(Node)以及樹葉(Leaf)等結構。而每一節點都有一個

分類的測試條件，就如「IF-THEN」的控制結構，利用測試結果來決定資料將分類於此節點的哪一棵子樹(Branch)，並繼續作為分類的條件和最後的決策。本研究使用的 J48 就是一種決策樹，並且使用 C4.5 演算法[11]。

除了許可權可以當作特徵外，本研究還將進行 android 應用程式檔案反編譯，透過反編譯可得到 smali 檔案。反編譯的過程是 Android 應用程式專案在開發完成後，將編譯打包成 APK，而其中 Java code 在編譯後，變成 classes.dex 檔案。對 classes.dex 進行反編譯後，可得到 smali 檔案。Smali 檔案的特色是可以很清楚看到函式是怎麼被呼叫使用的，包含此函式是哪個類別的或此函式所需傳入的參數等等，因此利用 smali code 來進行提取函式是非常適合的。因此函式也是一種有效的特徵，可與 permission 一起當作特徵增加惡意程式判斷正確率。本研究將利用此 smali 檔案進行函式特徵提取。

4. 實驗結果

表 3 為經由機器學習分類，得到的各演算法實驗結果(AVGTPR, AVGFPR, Accuracy)，而圖 5 是將表 3 繪製成長條圖，可以看出 AVG TPR 是 IBK(KNN, k=3)最高，其值為 0.919，J48(決策樹)最低，其值為 0.853；而 Accuracy 則是 IBK(KNN, k=3)最高，其值為 0.919；J48(決策樹)最低，其值為 0.845。一般而言大家較注重 Accuracy 而不是 AVGTPR。

本節方法相當有效，精確度基本上都有 0.84 以上，下一節實驗為加入新的特徵(將程式碼函式當作特徵)，以許可權和函示特徵一起進行機器學習分析。

表 3：機器學習分類結果

分類演算法	AVG TP Rate	AVG FP Rate	Accuracy
BayesNet	0.857	0.16	0.879
NaiveBayes	0.879	0.166	0.889
MultilayerPerceptron(類神經網路)	0.861	0.327	0.854
SMO(支持向量機)	0.872	0.299	0.867
IBK(KNN, k=1)	0.908	0.229	0.906
IBK(KNN, k=2)	0.912	0.24	0.91
IBK(KNN, k=3)	0.919	0.238	0.919
J48(決策樹)	0.853	0.365	0.845

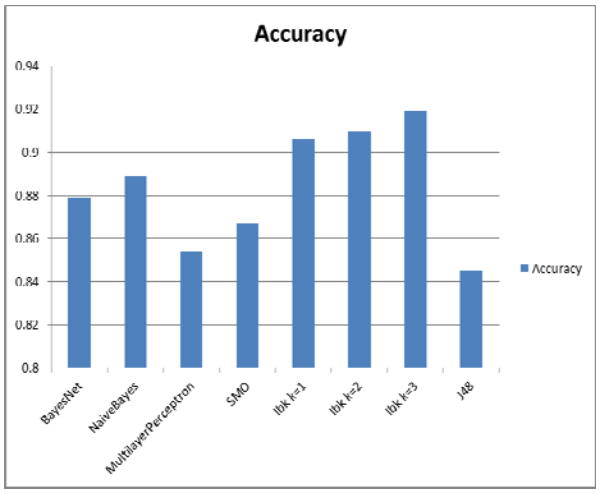


圖 5：偵測惡意程式精確度比較圖

圖 6 為許可權加函式特徵法實驗結果，此結果為使用函式與許可權當作特徵，再利用數種機器學習演算法進行分析得出。為了與圖 5 的精確度做區隔，在此我們將得到的精確度稱為 Accuracy-method。由圖可知 SMO 演算法可得到最好精確度。

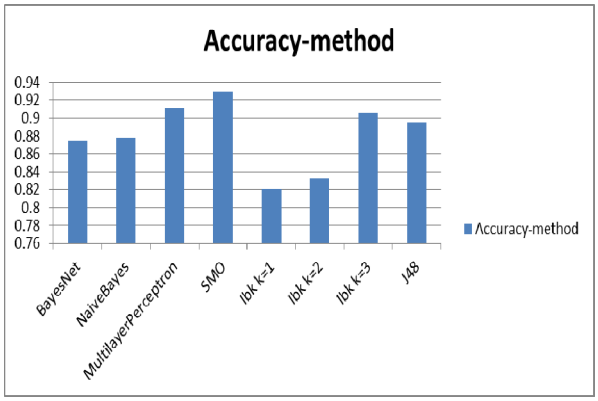


圖 6：透過機器學習分析函式與許可權當特徵的實驗結果

5. 結論與未來目標

通過本文中的方法，可以知道機器學習具有高正確率是較好的選擇，而且也確實得知許可權與函式都可以用來進行特徵分析。然而本研究還有可提升精確度的空間。在本研究中的機器學習是使用 weka 工具，其分類演算法都是使用內建的加權方法，並無法使用自己的，因此之後將自行撰寫可套用加權方法的分類演算法，便可把更好的加權方法配合機器學習來進行分類，相信可以再提升惡意程式偵測正確率。而另一種改良方向為透過應用程式類型個別進行許可權分析，分析出每個程式類型使用許可權的趨勢與差異，如此也可以提升正確率。目前由於用於分析的惡意程式檔案數不夠，因此分類後每個類中的檔案數過少，導致無法進行有效分析，期望將來能有機構或網站收集許多惡意程式，如此分類研究才能完成。

誌謝

感謝行政院國科會專題研究計畫之補助(101-2622-E-130-001-CC3, 101-2221-E-130-016, and 102-2221-E-130-006)，使本論文得以順利完成。

6. 參考文獻

[1] A.-D. Schmidt, H.-G. Schmidt, L. Batyuk, J. H. Clausen, S. A. Camtepe, S. Albayrak, and C. Yildizli, "Smartphone malware evolution revisited: Android next target?," in *2009 4th International Conference on Malicious and Unwanted Software, MALWARE 2009, October 13, 2009 - October 14, 2009*, Montreal, QC, Canada, 2009, pp. 1-7.

[2] W. Enck, M. Ongtang, and P. McDaniel, "On lightweight mobile phone application certification," in *16th ACM Conference on Computer and Communications Security, CCS'09, November 9, 2009 - November 13, 2009*, Chicago, IL, United states, 2009, pp. 235-245.

[3] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *8th Symposium on Usable Privacy and Security, SOUPS 2012, July 11, 2012 - July 13, 2012*, Washington, DC, United states, 2012, p. CyLab; National Science Foundation; Microsoft; Nielsen; RIM.

[4] M. Nauman, S. Khan, and X. Zhang, "Apex: Extending Android permission model and enforcement with user-defined runtime constraints," in *5th ACM Symposium on Information, Computer and Communication Security, ASIACCS 2010, April 13, 2010 - April 16, 2010*, Beijing, China, 2010, pp. 328-332.

[5] M. Zhao, F. Ge, T. Zhang, and Z. Yuan, "AntiMalDroid: An efficient SVM-based malware detection framework for android," in *2nd International Conference on Information Computing and Applications, ICICA 2011, October 28, 2011 - October 31, 2011*, Qinhuangdao, China, 2011, pp. 158-166.

[6] A. Apvrille and T. Strazzere, "Reducing the window of opportunity for Android malware Gotta catch 'em all," *Journal in Computer Virology*, vol. 8, pp. 61-71, 2012.

[7] A. Shabtai, Y. Fledel, and Y. Elovici, "Automated static code analysis for classifying android applications using machine learning," in *2010 International Conference on Computational Intelligence and Security, CIS 2010, December 11, 2010 - December 14, 2010*, Nanning, China, 2010, pp. 329-333.

[8] *apk-tool*. Available: http://code.google.com/p/android-apktool

[9] *Google Play*. Available: https://play.google.com/store

[10] *contagio mobile dump*. Available: http://contagiominidump.blogspot.com/

[11] J. Quinlan, *C4.5 programs for machine learning*: Morgan Kaufmann Publishers, 1993.

Agent-Based Social Network Search Mechanism
以代理人機制為基礎的社群網路資料搜尋之研究

李佳菁　　賴宥呈　　陳明僑
國立臺東大學資訊工程系
maius531@yahoo.com.tw, keith54105@yahoo.com.tw , joechen@nttu.edu.tw

摘要

社群網路服務幾乎是民眾日常生活裡無可或缺的服務，社群網路服務提供線上的人際關係網，隨著社群網站裡的人際關係越來越龐大，所獲得的資訊也越來越多，使用者被大量的資訊淹沒，結果真正重要的資訊卻不容易取得，因此，本論文提出代理人機制負責收集我們在社群網站上相關的互動資料，考慮網路社群裡發佈的status、photo、blog，以及其他人回應的方式和頻率，我們建立社群網路的關係密切程度函數，再使用線性規劃的方式得出關係密切程度的最大值，當使用者進行資料搜尋時，代入關係密切程度的數值進行資料搜尋的重要因素，最後再經由視覺化時間軸的方式呈現，提供使用者精確的搜尋結果、以及易於瀏覽的呈現方式。

關鍵詞：關係密切程度、時間軸、社群網站、代理人

Abstract

Social Network Service (SNS) plays an increasing role in people's lives. Social Network Service enables Internet users to interact with family, friends, or colleagues, to share their personal information, and to build a social relationship. With the rapid growth of network users, the quantity of data also increased tremendously, the search of this increasing amount of contents become more complicated and difficult. Therefore, this paper proposes an Agent-Based search mechanism to collect status, photo, and blog interactive content, response time and frequency. The mechanism uses linear programming approach to maximize the relationship function as the correlation of search results. Finally, the paper provides a timeline visualization methodology to show efficiently and effectively the result for users.

Keywords: Social Networks, Multi-Agent System, Search Mechanism, Relationship Function

1. 前言

社群網路服務(Social Network Service, SNS)對於大多數的民眾而言，幾乎是每日生活裡無可或缺的存在，透過網路在虛擬的社群裡和家人、朋友以及同事們，彼此分享個人的想法、感受，藉由這種分享和互動的過程，建立新世代的社群關係。近年來提供社群網路服務最著名的就是 Facebook，Facebook 之所以大受歡迎，在於它創新的想法，讓使用者以新的方式將彼此聯繫在一起，它藉由使用者自我描述的 profile，建立彼此之間的關聯，再進而建立個人的社群網路，由於這些關聯是取決於不同的因素，可能是朋友的關係，也可能是具有相同的嗜好、或是喜歡同一個偶像，甚至是相同政治信仰的陌生人。

隨著社群網路使用者快速增加，隨之而來所產生的資料量也跟著急遽增加，要處理如此龐大的資料量，就變得相當複雜與困難。因此，在一個以使用者為導向的社群網路，使用者應該不需盲目的摸索或查詢，就可以讓使用者快速而精確的找到所需的訊息，這需要一個有效的運作機制，才能夠在社群網路龐大的資料裡，萃取出使用者真正需要的資訊。

同時，社群網路的持續成長，其組成結構也越來越複雜，每位使用者之間原本所存在一個或多個特定的相互依存的關聯(例如：朋友、親戚、共同嗜好、信仰、知識等等)，也會因應社群網路的成長而更加複雜，於是產生更多間接、隱藏且容易被忽略的資訊與關係，因此，思考如何設計一個能夠有效發現這些隱含資訊與關係的機制是有其必要性的。

本論文的目的有二：一是設計適合社群網路的搜尋機制(Search Mechanism)，讓使用者可以快速、有效且準確地搜尋明確所需的資訊；二是以時間軸的方式將前項搜尋結果以視覺化的方式呈現。

2. 文獻探討

2.1 社群網路服務

社群網路服務（Social Network Service, SNS）主要是提供一群擁有相同興趣與活動的使用者可以在網路上建立的線上社群。這類服務是透過網際網路、提供使用者各種聯繫、交流的互動網路，例如即時訊息、即時通、電子郵件等，他們通常通過朋友、親戚或是同事將人際網路展延出去。

大多數的社群網路會提供多種方式讓使用者

彼此互動，例如：訊息分享、心情分享、聊天、影音或檔案分享、部落格、討論群組等，社群網路為資訊的交流與分享提供了新的途徑。對於現代的網路使用者而言，使用社群網路服務幾乎成為每天的生活必需項目之一。目前在世界上有許多提供社群網路服務的網站，知名的包括 Facebook、MySpace、Orkut、Twitter、Flickr 等等。

早期的社群網路服務大多數是提供使用者透過聊天室進行交流，隨著 Blog 等新的網路社交工具的出現，使用者可以透過網站建立個人首頁來分享喜愛的資訊。2002 年至 2004 年間，世界上三大最受歡迎的社群網路服務類網站是 Friendster、MySpace、Bebo。在 2005 年之際 MySpace 成為了世上最大的社群網路服務網站。甚至傳聞當時其頁面存取量超越了著名的搜尋引擎--Google。2006 年，Facebook 提供 API 允許第三方使用、開發相關的應用程式，使得 Facebook 隨後一躍成為全球使用者量增長最快的網站。

社群服務網站的發展驗證了「六度分隔理論」（Six Degrees of Separation）[1]，即「在人際關聯脈絡方面，你必然可以透過不超出六位中間人，間接與世上任意一個人產生聯繫」。個體的社交圈會不斷地擴大和重疊，並在最終形成大的社群網路。在此類透過對「朋友的朋友是朋友」原則的實作，而得到發展的線上社群網路中，Friendster 是一個典型的代表。透過社群網路服務，我們與朋友保持直接的聯繫，建立起大的人際關係，以 Facebook 為例，它提供的尋找使用者的工具，幫助使用者尋到失去聯絡的朋友們。另外，在社群網站裡的使用者，通常有很多志趣相同並互相熟悉的使用者群組，相對於網路上的其他廣告而言，商家若在社群網站裡針對特定使用者群組打廣告更有效果。

2.2 多代理人系統

多代理人系統是一個快速成長的研究領域，也是成長最快速的 IT 產業之一。代理人(software agent, agent)本身是一組程式，主要的目的是希望可以代替使用者運作，產生自主性。多代理人系統(Multi-Agent System, MAS)是一個分散式系統，由一組彼此互動的代理人所組成。由於代理人的自主性，所以多代理人系統並不受限在一個特定的系統裡，只要是支援代理人的系統都可以執行。

代理人是具有溝通(communication)與合作(collaboration/cooperation)的機制。國際間有許多訂定代理人技術標準的單位或組織，例如：FIPA (Foundation for Intelligent Physical Agents)[2]與 OMG (Object Management Group) [3]。

一般代理人所具備的特質如下：

1. Adaptivity：具備學習能力並能隨經驗增長。
2. Autonomy：具有主動性，朝達成目標的方向下有自主能力採取啟發性的行為。
3. Collaborative behavior：具備可以與其他代理人合作並一起達成目標的能力與行為。
4. Inferential capability：具備推論的能力。
5. Knowledge-level communication ability：在與其他代理人溝通時，具備使用人性化語言與溝通方式的能力。
6. Mobility：具備機動引導之能力，可以從一個 host 移至另一個。
7. Personality：具備個性化之特質。
8. Reactivity：具備選擇性感測與反應的能力。
9. Temporal continuity：具備保持身分扮演一致性的特質並能夠長時間的維持。

代理人具有能力可自主地完成特定的任務，然而，當代理人面對一些複雜的問題時，例如處理分散式資料或是與分散式控制的系統互動時，就需採用多代理人系統(Multi-Agent System, MAS)。其中每個代理人都具備不同的特性功能，在完成某一個共同目標的過程中扮演不同的角色。多代理人系統是透過非緊密式連結(weakly coupled)所形成的網狀系統，在不同環節裡包含很多不同的個別解決方案(problem solver)，而這些 problem solver 結合後的解決問題的能力，遠大於個體的 solver。因此，多代理人系統包含多種自動化 component 組合而成，其具備下列的特性：

1. 每個代理人不具備完整可以獨力解決問題的能力
2. 採用分散式的控制系統
3. 代理人之間共用與分享同一個資料庫
4. 採用不同步的計算方式

基於以上的探討，多代理人系統特質裡的 adaptivity, autonomy, personality 等，使得多代理人系統非常適合處理社群網路的相關問題，例如：

1. 多代理人系統的 adaptivity 特性，使得代理人可以依據使用者的興趣而改變，採取以目標為導向的行動，並且提供使用者更合適且個人化的資訊服務。
2. 多代理人系統的 autonomy 特性，使得代理人可以獨立地搜尋資訊，不用使用者的直接介入，如此就可以完成主動式的資訊服務，節省使用者的時間跟精力。
3. 多代理人系統的 Personality 以及彼此間溝通的特性，使得具有相同興趣與嗜好的代理人可以相互溝通，並提供使用者更多更好的資訊。
4. 多代理人系統的學習能力，使得代理人可以透過互動與使用者學習，以至於能感知使用者興趣的改變，進而調整 interest model, 這也是個人化資訊服務的以實現的重要關鍵[4]。

2.3 社群搜尋機制

隨著社群網路資料量的日益增加，要處理龐大的資料會變得相對複雜與困難。雖然每個人每天都會透過社群網站得到所需的資料，然而關於如何改善搜尋以及搜尋品質的問題，尤其是如何即時地提

供使用者有效率及有用的資訊，是一個需要持續努力的議題。重要的關鍵並不是搜尋不到資料，而是搜尋引擎可能無法快速提供使用者真正想要或是有興趣的資料，因此，以目前而言，社群網路的搜尋，仍是一件很費時費力的工作。

搜尋引擎的缺點包括：一個 query 可能會傳回大量的回覆結果，以及缺乏個人化(Personalization)，也就是通常對於相同的一個 query，針對不同的使用者應該會依據不同的使用者特質，會有因人而異的結果[5](如圖 1)。上述的第一個缺點可以透過使用者對搜尋引擎重新輸入合適的 query 而得到改善，這需要使用者某種程度的直覺與經驗。另外，對於缺乏個人化這部份，就是實質地針對不同的個人提供不同的 query 結果，而不僅僅只是針對關鍵字進行回應而已。



圖 1 個人化網頁

有許多 meta-search 引擎提供了主要的個人化服務。例如： Query Server, Profusion, Infogrid, Mamma, Ixquick 等，讓使用者可以自行定義要使用的搜尋引擎[6]。Excalibur 專案[7]提出一個個人化的 meta-search 引擎，可以隱含的擷取使用者的喜好並且使用 Naïve Bayesian 分類器做 ranking 與相似度量測(resemblance measure)。Radovanovic 等人[8]提出一個稱之為 CatS 的 meta-search 引擎，利用文字分類技術(text classification)改善搜尋結果，使用經由 dmoz Open Directory topic 階層所推演出的 topic 樹顯示出來，供使用者瀏覽。在 Captain Nemo 專案[9]提出一個具有個人化階層式 search space 的全功能(full-functional)的 meta-search 引擎，可以根據個人化擷取模式與呈現風格去擷取與顯示搜尋結果。WebNaut 專案[10]提出一個以多代理人為基礎的 meta-search 引擎，其包含一組互連的代理人以及一個 meta-genetic 演算法，藉以學習使用者的嗜好與個人化搜尋結果。Kanteev 等人[11]提出一個多代理人的文字瞭解系統(text understanding system)，使用語意瞭解內容並且產生語意描述(semantic descriptor)，並且運用儲存於本體(ontology)內的問題領域知識。

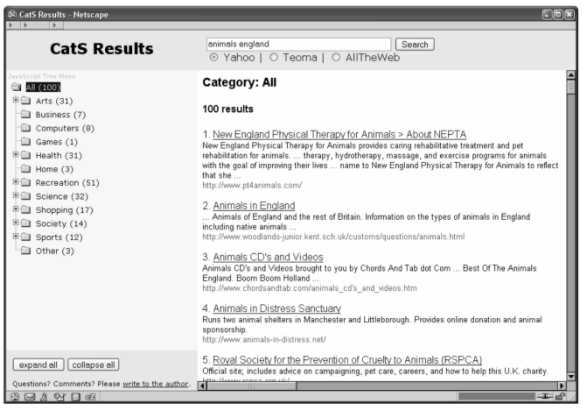


圖 2 Cats Meta-Search 引擎[8]

除此之外，推薦系統(recommender system)也可被視為有效存取有用資訊的重要工具之一。它們可分成 content-based, collaborative filter 以及 hybrid system 三大類，以下大略說明之：

1. Content-based system：藉由分析之前所瀏覽的網頁所得到的資訊，以及使用經由瀏覽相似內容的網頁，產生推薦內容。
2. Collaborative filtering system：經由計算不同使用者的相似度，將相似度相近的使用者所存取過的內容提供給供使用者。
3. Hybrid system：適當的結合以上兩種方法。

Wei 等人[12]提出一個 market-based 推薦系統。它提供一個可以代表使用者的多代理人系統，讓推薦內容可以顯示在 slidebar 上。其他參與的代理人也會按順序的顯示在 slidebar 上，而 agent-initiator 會選擇的內容提供給使用者。提供的選項如果被使用者接受，就會得到獎賞。此代理人系統藉由採取多重階層的推薦方法做出最好的推薦內容。Yu 等人[13]提出一個多代理人的推薦系統，他們提出一個 MARS 知識管理轉送系統負責配置代理人給使用者，代理人藉由互動產生使用者所提出問題的答案。這個系統使用預先定義好的本體(ontology)，由各代理人一起分享，如此就可以很輕易的分享知識，共同解決問題。

Degemmis 等人[14]提出了一個結合 collaborative filtering 與學習使用者 profile 技術的推薦系統，此外，這個系統也結合了 collaborative 與 content-based 策略，藉由使用者的知識可以呈現在 profile 內，以及 collaborative filtering 演算法減少推薦產生的時間。Chau 等人[15]提出一個 collaborative 多代理人網頁探勘系統—Collaborative Spiders，藉由不同型態的代理人依據排程各司其職的擷取網頁內容、執行 post-retrieval 分析、與使用者互動、分享使用者搜尋的資訊、執行 profile 配對以及實施擷取與分析工作。

Zhu 等人[16]提出一個利用使用者行為模式去預測相關網頁的推薦系統—WebICLite，並將瀏覽網頁概念化為搜尋一個特定定義好的資訊需求(need)，而將這些需求識別為使用者瀏覽的網頁與作用在其他的動作(action)，並且參考與比較一些識別

information-need-revealing 樣式的特定演算法，並依序使用這些演算法用於推論使用者所使用的搜尋引擎的資訊需求。Macedo 等人[17]提出一個應用推薦系統除了支援使用者網頁瀏覽，也幫助推薦其他尋求推薦的使用者。而這個系統也允許使用者基於隱私權的考量，隱藏該使用者所搜尋的網頁一段時間。

3. 研究方法

本論文的目標是經由建構於社群網路的多代理人系統為基礎，進行收集與處理各使用者相關的資訊與喜好，設計一套適合社群網路的搜尋機制(Search Mechanism)，便於使用者可以快速、有效且準確地搜尋明確所需的資訊，進而開發一套發現機制(Discovery Mechanism)強化與發現出隱含不易發現的資訊。

多代理人系統所具備的 adaptivity, autonomy, social, personality 等特質，非常適合處理社群網路的相關問題。因此我們提出一個如圖 3 所示的多代理人系統架構，其中包含了 3 種型態的代理人：圖形使用者介面代理人(Graphic User Interface Agent, GA)、使用者代理人(User Agent, UA)、以及社群代理人(Social Agent, SA)。

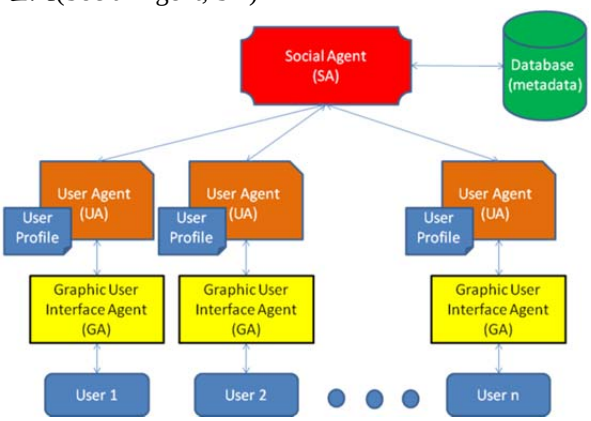


圖 3 多代理人系統架構

每位使用者都有一個 UA 與它所伴隨的 GA。在多代理人系統中，UA 就是設計為代表使用者。GA 的功能就是提供使用者與其 UA 之間的介面。GA 會提供一個圖形化介面，讓使用者透過系統所提供的功能與其他使用者溝通，並且使用圖形化介面顯示相關的資訊與個人化的訊息給使用者。而 SA 的角色就是提供社群網路服務所需的所有支援與協助，不像其他兩種型態的代理人(每一個使用者都會被分配一個 GA 與 UA)，SA 不屬於特定的人，對整個系統而言，它是一個管理者(manager)的角色，SA 統籌處理所有關於儲存、管理現存所有的使用者群組、協調所有系統中 UA 之間交換的訊息等。

社群網站的使用者原本就基於相同的興趣、共同的喜好、或是某些密切的關係，而在網路上群聚在一起的使用者，因此，本論文基於二個主要的基礎：物以類聚、共同的話題，建置本論文的系統架構圖如圖 4 所示，主要內容包括：

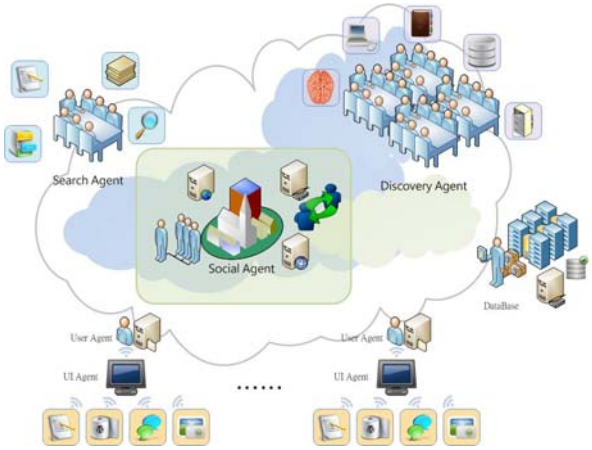


圖 4 系統架構圖

3.1 代理人服務機制之關係搜尋法

多代理人系統(Multi-Agent System, MAS)具備適合應用於社群網路的重要特質，由代理人學習得知使用者與其他使用者之間的友好關係狀態，並依彼此的關係不斷演進而因應需要進行調整，代理人之間也會藉由合作與溝通完成任務。社群網路多代理人機制所開發建置的 UI Agent、User Agent 與 Social Agent，藉由代理人間相互的通訊與合作，收集各使用者相關的資訊與互動的密切程度，也藉由回饋機制，學習、改變與調整相關的個人化資料模型。

以社群網站最多人使用的 facebook 為例，facebook 的使用者可以透過 facebook 的設定，將某些關係指定為『家人』、『摯友』、『點頭之交』、『大專院校』、『高中』或者任職的公司，代理人以原有 facebook 的分類為基礎，再將使用者與不同使用者、不同關係之間的互動狀態隨時記錄下來，藉此分析並得知與我們互動最為密切的朋友或是群組。

假設以向量 r 來表示 facebook 裡設定的朋友關係(摯友、特定名單、家人關係、未分類名單…等)的係數，另外，向量 x_{ij} 其中的 i 代表發佈的近況、相片、部落格，其中的 j 表示對 i 按讚、訊息回應、同時按讚與訊息回應的次數，以 s_k 表示針對發佈的近況按讚、訊息回應、同時按讚與訊息回應的係數，以 p_k 表示針對發佈的相片按讚、訊息回應、同時按讚與訊息回應的係數，以 b_k 表示針對發佈的部落格按讚、訊息回應、同時按讚與訊息回應的係數，我們得到使用者的關係密切程度函數可以表示如下：

$$S = s_1x_{11} + s_2x_{12} + s_3x_{13}$$
$$P = p_1x_{21} + p_2x_{22} + p_3x_{23}$$
$$B = b_1x_{31} + b_2x_{32} + b_3x_{33}$$
$$R = rS + rP + rB$$

我們再透過線性規劃的方式來找出它的最大值，如下：

Maximize $R = rS + rP + rB$

Subject to

$$s_1x_{11} + s_2x_{12} + s_3x_{13} = S$$
$$p_1x_{21} + p_2x_{22} + p_3x_{23} = P$$
$$b_1x_{31} + b_2x_{32} + b_3x_{33} = B$$
$$x_{i1}, x_{i2}, x_{i3} \geq 0$$
$$s_1, s_2, s_3 \geq 0$$
$$p_1, p_2, p_3 \geq 0$$
$$b_1, b_2, b_3 \geq 0$$
$$r_1, r_2, \ldots\ r_n \geq 0$$
$$S \geq 0, P \geq 0, B \geq 0$$

由關係密切程度函數所得出的數值越大的，表示關係程度越密切，數值越小的表示關係程度越疏遠，因此，當使用者搜尋資料時，將以此為主要排序依據，由關係程度最密切的方向開始，依序往關係程度較疏的方向進行尋找，所搜尋到的資料內容也是關係比較密切的內容或資料來源。

3.2 時間軸之視覺化顯示

facebook 目前並未提供針對內容進行搜尋的功能，而且，以 facebook 現有的資訊呈現方式來看，主要分為『人氣動態』、『最新動態』二種，由於社群網站的型態，其資料更新的頻率非常快速，因此，facebook 預設是以『人氣動態』的方式呈現，將目前比較多人在回應的內容顯示在比較上方，主要目的在於吸引社群使用者的目光焦點，但是當使用者要尋找某些資料時，就只能使用捲軸往下拖曳，以眼球搜尋的方式自行尋找資料。

本論文除了搜尋使用者所發表的訊息內容，提供使用者可以隨時搜尋過往的資訊，另外一個主要目標在於提供使用者快速、有效且準確的搜尋機制，使用者不需要盲目的摸索與探詢、重複嘗試著不同的關鍵字，就能夠快速且準確地找到所需的資訊。因此我們發展適合社群網路之搜尋機制，藉由前述建立的使用者間的關係狀態，同時，在不同的時間點，社群裡討論的話題或是觀注的焦點會不斷的變換，但是以較為微觀的角度來看，在某些時間的區間，社群裡所談論的話題應偏向某些特定的主題，因此，我們基於前項的關係密切程度下，導入時間群聚的概念，觀察與使用者密切關係的群組裡，在某些時間區間裡較多的討論主題，藉以提高或命中使用者在搜尋時所期望出現的搜尋結果。因此，最容易且最有效的方式即以視覺化呈現再結合時間軸的方式，使用者可以在時間軸的呈現結果裡，一目瞭然搜尋結果的密集程度，越密集的就表示越有可能就是使用者要的搜尋結果。

4. 系統實作

4.1 關係密切程度函數

依據關係密切程度方式，可以將使用者彼此互動的狀況，帶入以下公式計算而得到其值：

Maximize $R = r_iS + r_iP + r_iB$

Subject to

$$0.1x_{11} + 0.6x_{12} + 1.0x_{13} = S$$
$$0.1x_{21} + 0.6x_{22} + 1.0x_{23} = P$$
$$0.1x_{31} + 0.6x_{32} + 1.0x_{33} = B$$

以下說明各係數的狀況及代表的權重：

r_j的係數表示如下：

r_1=1.0，摯友

r_2=0.8，特定名單

r_3=0.5，家人關係

r_4=0.2，未分類名單

s_1, p_1, b_1=0.1，按讚的權重

s_2, p_2, b_2=0.6，以訊息回應的權重

s_3, p_3, b_3=1.0，同時按讚及訊息回應的權重

最後計算出來的數值越大表示彼此互動的關係越密切，數值越小表示彼此之間互動的關係越少，透過關係密切程度函數所得到的值，做為系統搜尋資料時的主要依據。

4.2 時間軸之視覺化顯示

當網頁內容超過一頁時，大多會以縱向的方式呈現，不過，對於時間軸的概念而言，我們會比較習慣以橫向的方式，以 XY 二維平面來看，X 軸是時間，X 軸的左方是比較過去的時間，右方則是比較新的時間，因此，我們將前項搜尋的結果以橫向時間軸的方式呈現。

此部份的技術，我們將使用以 BSD license 釋出的 SIMILE Timeline Project，使用 JavaScript 方式，將資料以橫向時間軸方式呈現，同時，還可以具有大小二種不同的時間刻度，使用者可以直接滑動大小不同刻度的時間軸，如圖 5 所示，進行搜尋結果的瀏覽。

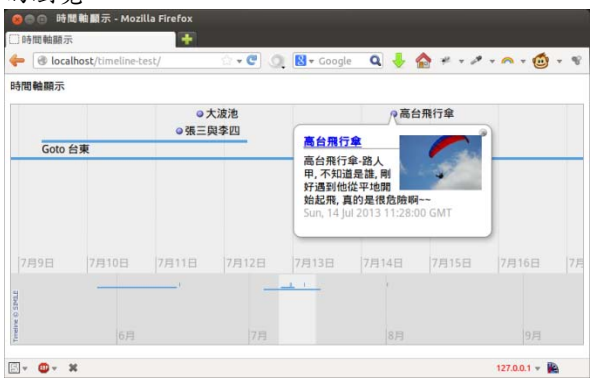


圖 5 搜尋結果以時間軸之視覺化方式呈現

5. 結論

社群網站的使用者快速增加，隨之而來所產生的資料量也跟著急遽增加，在一個以使用者為導向的資料搜尋，將變成非常困難的任務，本論文透過

代理人機制，定期收集使用者在網路社群裡互動的狀態，例如個人 status 的更新、發佈新的照片，以及其它好友的回應狀況，將狀態與內容儲存於本論文所建置的資料庫，將前述的彼此互動的狀態，透過關係密切程度函數經由線性規劃方法，計算出社群網站裡使用者之間的最大關係密切程度，當使用者透過本論文所建置的系統進行資料搜尋時，系統將得到的關係密切程度導入搜尋資料的動作，因此，藉以確保搜尋的結果將與使用者具有較密切的關係。最後，系統以視覺化時間軸的方式將結果呈現，提供使用者一目瞭然的搜尋結果。

本論文所提出的系統，可以提供使用者在社群網路龐大的資料進行搜尋時，萃取出與使用者密切相關的資訊。

致謝

本論文由國家科學委員會補助部分研究經費，計畫編號 NSC100-2221-E-143-001、NSC101-2221-E-143-003 及 NSC102-2218-E-143-001。

參考文獻

[1] X. Ke, “A Social Networking Services System Based on the “Six Degrees of Separation” Theory and Damping Factors,” Proceedings of Second International Conference on Future Networks (ICFN ‘10), pp.438-441, 2010.

[2] FIPA, http://www.fipa.org

[3] OMG, http://www.omg.org

[4] J. Chen, “Research on Individualized Information Retrieval System Based on Multi-Agent,” Shanghai Jiao Tong University, Master’s Thesis, December 1, 2006.

[5] M. Gori and I. Witten, “The Bubble of Web Visibility,” Communications of the ACM, vol. 48, no. 3, March 2005.

[6] S. Souldator, T. Dalamagas and T. Sellis, “Sailing the Web with Captain Nemo: A Personalized Meta-Search Engine,” Proceedings of the ICML 2005 Workshop: Learning in Web Search (LWS ‘05), Bonn, Germany, Aug, 2005.

[7] L. Yuen, M. Chang, Y. K. Lai and C. K. Poon, “Excalibur: A Personalized Meta-Search Engine,” Proceedings of 28th Annual International Computer Software and Applications Conference (COMPSAC ‘04), vol. 2, pp.49-50, 2004.

[8] M. Radovanovic and M. Ivanovic, “Cats: A Classification-Powered Meta-Search Engine,” Advances in Web Intelligence and Data Mining, Springer-Verlag, vol. 23, pp.191-200, 2006.

[9] S. Souldatos, T. Dalamagas and T. Sellis, “Captain Nemo: A Meta-Search Engine with Personalized Hierarchical Search Space,” Informatics, vol. 30, pp.173-182, 2006.

[10] N. Zacharis and T. Panayiotopoulos, “SpiderServer: The Meta-Search Engine of WebNaut,” Proceedings of the 2nd Hellenic Conference on Artificial Intelligence, pp.475-86, 2002.

[11] M. Kanteev, I. Minakov, G. Rzevski, P. Skovelev and S. Volman, “Multi-Agent Meta-Search Engine Based on Domain Ontology,” Springer, vol. 4476, pp. 269-274, July 2007.

[12] Y. Z. Wei, L. Moreau and N. R. Jennings, “Recommender System: A Market-Based Design,” Proceedings of the second International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS ‘2003), pp.600-607, New York, NY, USA, 2003.

[13] B. Yu and M. P. Singh, “An Agent-Based Approach to Knowledge Management,” Proceedings of the eleventh International Conference on Information and Knowledge Management, pp.642-644, New York, NY, USA, 2002.

[14] M. Degemmis, P. Lops, G. Semeraro, M. F. Costabile, O. Licchelli and S. Guida, “A Hybrid Collaborative Recommender System Based on User Profiles,” Proceedings of ICEIS, pp.162-169, 2004.

[15] M. Chau, D. Zeng, H. Chen, M. Huang and D. Hendriawan, “Design and Evaluation of A Multi-Agent Collaborative Web Mining System,” Decision. Support System, vol. 35, no. 1, pp.167-183, 2003.

[16] T. Zhu, R. Greiner, G. Haubl, B. Price and K. Jewell, “Behavior-Based Recommender Systems for Web Content,” Proceedings of the 10th International Conference on Intelligent User Interfaces, New York, NY, USA, 2005.

[17] A. A. Macedo, K. N. Truong, J. Antonio and M. Pimentel, “Automatically Sharing Web Experiences through A Hyperdocument Recommender System,” Proceedings of the fourteenth ACM Conference on Hypertext and Hypermedia, pp.48-56, New York, NY, USA, 2003.

[18] Wikipedia, “Linear programming”, http://en.wikipedia.org/wiki/Linear_programming

[19] Simile Widgets, http://www.simile-widgets.org/timeline/

LOM: 領隊導向多人連線遊戲自動匹配演算法

宋管翊 江振瑞
國立中央大學 資訊工程學系
jrjiang@csie.ncu.edu.tw

摘要

在多人連線遊戲(Multiplayer Online Games)中，自動匹配(matchmaking)的定義為將多位玩者(player)匹配在一起共同進行遊戲的程序。目前自動匹配的準則可以分為兩大類: Connection Based 與 Skill Based。前者將一群彼此網路互相連線速度較快的玩者匹配在一起;而後者則將一群彼此技能評分(Skill Rating)接近的玩者匹配在一起。本論文首先提出一項稱為 Association Based 的玩者匹配準則。在此準則下，關聯度(Association)較高的玩者被匹配在一起進行遊戲。並提出一個新的自動匹配演算法 LOM (Leader Oriented Matchmaking)來匹配系統中的玩者。LOM 使用到了 Minimum Cost Maximum Flow 演算法的概念，以最佳化的方式來匹配玩者。我們針對 LOM 與基本的貪婪式(greedy)玩者匹配演算法及隨機(randomized)玩者匹配演算法進行模擬與分析，以評估其效能。我們發現雖然 LOM 執行時間較長，但可產生最佳的平均玩者關聯度。

關鍵詞：多人連線遊戲、自動匹配、最小成本最大流量演算法、技能評分。

Abstract

In multiplayer online games (MOGs), matchmaking is a process that arranges players for online game sessions. Currently, there are two types of matchmaking criteria: connection-based and skill-based. In the connection-based criterion, players with higher mutual network connection speed are arranged together. In the skill-based criterion, players with close skill ratings are arranged together. In this paper, we propose a new criterion, association-based criterion, by which players with high association are arranged together. According to the proposed criterion, we also propose a new matchmaking algorithm, called LOM (Leader Oriented Matchmaking), using the concept of the minimum-cost maximum-flow algorithm to arrange players in an optimized way. We perform simulations and analyses for LOM, and compare it with two basic algorithms, the greedy and the randomized matchmaking algorithms. Although LOM has the longest execution time, it produces the best average association.

Keywords: Multiplayer online games, matchmaking, minimum cost maximum flow algorithm, skill rating.

1. 前言

多人連線遊戲(Multiplayer Online Games)是讓多位玩者透過網際網路(Internet)、區域網路(LAN)或是隨意網路(Ad-Hoc)連線在一起共同遊玩的一種遊戲模式。遊玩的平台可以是個人電腦(Personal Computer)、手持行動裝置(Handheld Device)或是遊戲主機(Video Game Console)。

自動匹配(Matchmaking)在多人連線遊戲的定義上，是將多位玩者(players)匹配在一起共同玩遊戲的一個過程。其興起和電視遊樂器開始支援網路連線功能有著密不可分的關係，與傳統 PC game 從伺服器瀏覽器中點選自己想進入的伺服器相比，直接點選一顆按鈕即能找到其他玩者的自動匹配明顯花費較少的力氣進行遊玩，也因此適用在電視遊樂器中較不方便的視窗瀏覽操作上。故自動匹配有取代伺服器瀏覽器的趨勢。現在已經有許多 PC game 也開始支援自動匹配的功能，並且也有許多學術研究開始探討自動匹配議題[1][3][6][7][8]。

自動匹配依照其匹配玩者的準則可以分為兩大類: Connection Based 與 Skill Based。前者將一群連線速度相近的玩者們匹配在一起遊玩，故其匹配玩者的準則為玩者彼此間互相連線的速度。後者付予每位玩者一個用來代表該玩者實力強弱的數值，稱為技能評分(Skill Rating)[2][5][9]。在匹配玩者時，自動匹配將技能評分相近的玩者匹配在一起比賽，故其匹配玩者的準則為玩者彼此間技能評分的差異。

本論文提出一個新的玩者匹配準則，並依此準則提出一項新的自動匹配演算法來匹配系統中所有的玩者。新提出的玩者匹配準則稱為 Association Based。在此準則下，關聯度(Association)較高的玩者被匹配在一起進行遊戲，而關聯度值得大小則代表兩位玩者間的關聯程度高低。新提出的自動匹配演算法稱為 LOM (Leader Oriented Matchmaking)，利用最小成本為大流量(Minimum Cost Maximum Flow)演算法[4]的概念，以最佳化的方式，將關聯度最高的玩者匹配在一起。值得一提的是，Connection Based、Skill Based 與 Association Based 準則，皆可套用於此演算法中去匹配玩者，並皆可依各自的需求得到最佳的輸出結果。套用在 Association Based 準則，它可以幫系統中的每一位玩者匹配出最佳的團隊出來。套用在 Connection Based 準則，它可以最佳化系統中每一位玩者的網路連線速度。套用在 Skill Based 準則，它可以讓系

統中同場遊戲玩者間的技能評分差距最小。

本論文其他部份的內容安排如下: 我們在第二節中介紹相關的研究，第三節中描述問題的定義並在的第四節中提出解決的方法。第五節則是呈現相關方法的模擬結果，而第六節則總結全篇論文。

2. 相關研究

我們在本節中回顧一下過去有關於多人連線遊戲之 Matchmaking 的相關研究。

在 2009 年，Microsoft Research 的 Sharad Agarwal 與 Jacob R. Lorch 於 SIGCOMM '09 發表了一篇論文[1]，它的主題集中在 Connection based 的匹配玩者準則。提出了一個名為 Htrae 的系統，它為一基於地理位置資訊的網路延遲預測系統(Geographical Based Network Latency Pre-diction System)，用來為預估玩者間的網路延遲大小。

在 2011 年，Justin Manweiler, Sharad Agarwaly, Ming Zhangy, Romit Roy Choudhury 和 Paramvir Bahly 於 MobiSys11 發表了 Switchboard 系統 [3]，它提出了一個適用於手持行動裝置的 Matchmaking 系統架構。並做了許多實驗探討了不同基地台間之手持行動裝置在進行 P2P 遊戲時的網路延遲大小。

在 2012 年，Olivier Delalleau, Emile Contal, Eric Thibodeau-Laufer, Raul Chandias Ferrari, Yoshua Bengio 與 Frank Zhang 針對 Skill based 匹配玩者準則加以改進[3]，對於網路連線速度方面他是假設所有玩者都可以連線到延遲大小對他而言較低的伺服器，故此論文不考慮玩者的網路連線速度，只考慮玩者間實力差距的平衡。

3. 問題定義

假設系統中有 n 個玩者，分成若干隊，每一隊人數皆為 i 人，$1 < i \le \lceil n/2 \rceil$。我們先選出 k 位玩者當隊長，並令隊長(Leader)所成的集合為$\mathcal{L}$，$\mathcal{L} = \{\ell_1, \ell_2, \ell_3, \dots, \ell_k\}$。再取系統中的隊伍數為 k 個，並令隊伍所成之集合為 G，$G=\{g_1, g_2, g_3, \dots, g_k\}$，其中 $k=\lceil n/i \rceil$。剩下的$n-k$位玩者稱為隊員(Member)，令隊員所成的集合為$\mathcal{M}$，$\mathcal{M} = \{m_1, m_2, m_3, \dots, m_{n-k}\}$，每位隊長各需在其中選出 i-1 位玩者來當自己的隊員。這也代表會有 n mode i 位屬於$\mathcal{M}$集合的玩者被排除在外，不屬於任一隊。在此定義隊員和隊長間存在一個權重值，代表他們倆間關聯度之高低、稱為 Association Factor，簡稱$AF_{\ell_\alpha m_\alpha}$，值愈低代表關聯度愈高。而在 Skill Based 準則中，此權重值代表他們倆間技能評分之差值、在 Connection Based 準則中，它代表他們倆間網路連線延遲大小，由於本論文提出此演算法之最主要目的是去解如何以 Association Based 準則來匹配玩者之議題，故接下來我們統一使用$AF_{\ell_\alpha m_\alpha}$來稱呼此權重值，$\forall \ell_\alpha \in \mathcal{L}$，$\forall m_\alpha \in \mathcal{M}$。假設目前系統中存在一個隊伍$g_A \in G$，此隊有 1 個隊長$\ell_A \in \mathcal{L}$及 j 個隊員$\{m_{A1}, m_{A2}, m_{A3}, \dots, m_{Aj}\} \subseteq \mathcal{M}$，則我們在此定義 g_A 隊的綜合權重值為AF_{g_A}，其中$AF_{g_A}=\sum_{k=1}^{j} AF_{\ell_A m_k}$。此問題定義之圖解如圖 1 所示。為了能讓系統中的每位隊長都找到最適合他的隊員，我們的目標為：1.$\forall g_\alpha \in G, |g_\alpha|=i$。2.最小化$\sum_{g_\alpha \in \mathcal{T}} AF_{g_\alpha} / k*(i-1)$，$\forall k$=系統中的隊伍數，i=每一隊需要的人數，之所以要除 k*(i-1)是為了去突顯 Minimum Cost Maximum Flow 定義中 minimum cost “per” flow 的概念。

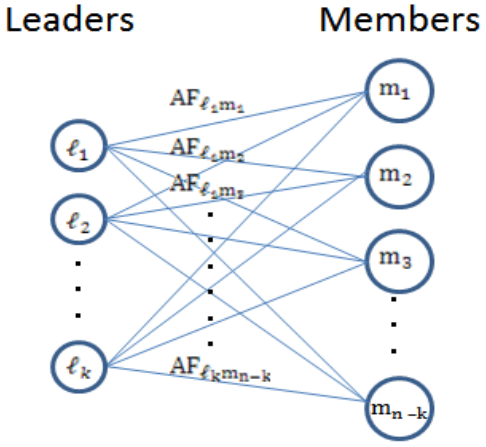


圖 1 問題定義示意

4. 提出方法

我們將上段導出的模型轉換成適合套用 Minimum Cost Maximum Flow 演算法的型式。首先新增兩個虛擬結點 S 和 T，並將 S 與$\mathcal{L}$集合中所有結點相連，T 與$\mathcal{M}$集合中所有結點相連。再來付予圖中的點α一個權重值 d(α)，並重新定義邊上的權重為二維向量$(CP_{\alpha\beta}, AF_{\alpha\beta})$。我們可以將$CP_{\alpha\beta}$看成邊$\overrightarrow{\alpha\beta}$上的容量、$AF_{\alpha\beta}$看成流過邊$\overrightarrow{\alpha\beta}$的成本，$\forall \alpha, \beta \in S \cup \mathcal{L} \cup \mathcal{M} \cup T$。其中$CP_{S\ell}$=i-1，$AF_{S\ell}$=0，$CP_{\ell m}$=1。$CP_{mT}$=1，$AF_{mT}=0$。在演算法的輸出結果中若$\ell$和 m 之間有流量，則代表隊長$\ell$和隊員 m 被匹配到同一隊伍中，若沒有，則代表他們不在同一隊，$\forall \ell \in \mathcal{L}$，$\forall m \in \mathcal{M}$。如圖 2 所示，我們稱此圖為$\mathcal{N}$。

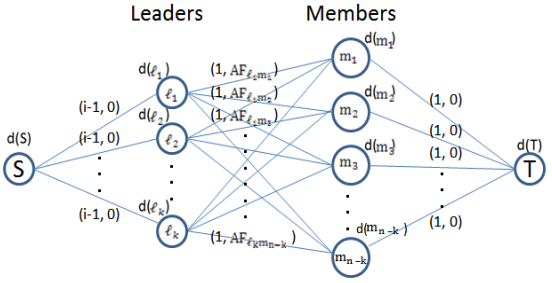


圖 2 $\mathcal{N}$的圖解

有了$\mathcal{N}$之後，我們可以將它視為 Minimum Cost Maximum Flow 問題。此問題有各種不同的演算法可以解。在本論文中，我們採用 Algorithm Design : Foundations, Analysis and Internet Examples[4]一書中 Chapter 8.4 提出之 Successive Shortest Path Algorithm。詳細流程如下：

Algorithm : MinCostFlow

***Input*:** Weighted flow network $\mathcal{N}$

***Output*:** A maximum flow with maximum cost f_{ST} for $\mathcal{N}$

```
1: Initialize flows of all edges to 0
2: Initialize weights of all vertex to 0
3: Repeat
4:   Compute the weighted residual network Rf
5:    for each edge uv ∈Rf do
6:      AF_uv ← AF_uv+ d(u) - d(v)
7:    end for
8:    Run Dijkstra's algorithm on Rf using the
weights AF'_uv
9:    for each vertex α ∈ N do
10:     d(α)←Distance ofαfrom S in Rf
11:   end for
12:   if d(t) < +∞ then
13:     Δ← ∞
14:     for each edge αβ ∈ π do
15:       if Δ_f(αβ) <Δ then
16:         Δ← Δ_f(αβ)
17:       end if
18:     end for
19:     for each edge αβ ∈ π do
20:       if αβis a forward edge then
21:         f_αβ ← f_αβ+Δ
22:       else if αβ is a backward edge
23:         f_αβ ← f_αβ-Δ
24:       end if
25:     end for
26:   else
27:     stop← true
28:   end if
29: until stop
```

在解釋該演算法如何運作前，我們先說明何謂剩餘網路(Residual Network)。首先定義何謂剩餘容量(Residual Capacity)。假設$\mathcal{N}$為一網路圖，$\forall\overrightarrow{\alpha\beta}\in\mathcal{N}$，則我們定義$\overrightarrow{\alpha\beta}$之剩餘容量$\Delta_f(\overrightarrow{\alpha\beta})=CP_{\alpha\beta}-f_{\alpha\beta}$，$\overrightarrow{\beta\alpha}$之剩餘容量$\Delta_f(\overrightarrow{\beta\alpha})=f_{\alpha\beta}$，其中$CP_{\alpha\beta}$為邊$\overrightarrow{\alpha\beta}$的容量，$f_{\alpha\beta}$為邊$\overrightarrow{\alpha\beta}$的網路流量。假設現在有一空圖 Rf，若$\exists\overrightarrow{\alpha\beta}\in\mathcal{N}$使得$\Delta_f(\overrightarrow{\alpha\beta})\neq0$，且$\overrightarrow{\alpha\beta}\notin Rf$，則我們在圖 Rf 中加上邊$\overrightarrow{\alpha\beta}$與邊$\overrightarrow{\beta\alpha}$，並將其權重值設為$\Delta_f(\overrightarrow{\alpha\beta})$與$\Delta_f(\overrightarrow{\beta\alpha})$，直到$\mathcal{N}$中所有剩餘容量不為 0 的邊都存在於 Rf 為止。最後的 Rf 即為$\mathcal{N}$之剩餘網路，它顯示了$\mathcal{N}$中每條邊可用的流量剩多少。

Successive Shortest Path Algorithm 大致的作法為，在每一回合中，從剩餘圖中找出一條從 S 到 T，邊上權重值總和最小的路徑，並延著它送出一條最大並且可容納於此邊之容量的網路流。再來更新剩餘網路上的資訊，更新的方法為，假設邊$\overrightarrow{\alpha\beta}$有一條網路流流過，$\forall\overrightarrow{\alpha\beta}\subseteq\mathcal{N}$，$\overrightarrow{\alpha\beta}$之成本為$AF_{\alpha\beta}$、容量為$CP_{\alpha\beta}$，則我們在剩餘網路中將$CP_{\beta\alpha}$加一、$CP_{\alpha\beta}$減一，並將$AF_{\beta\alpha}$設為負$AF_{\alpha\beta}$。在每一回合中重複作相同的事，直到無法從剩餘網路中找到任何可以從 S 通到 T 的路徑為止。而根據在剩餘網路中尋找最短路徑的找法，此演算法可分為兩種版本，運算時間複雜度 $O(|f_{ST}|m\log n)$的 Dijkstra 版本與運算時間複雜度 $O(|f_{ST}|mn)$的 Bellman-Ford 版本，其中$|f_{ST}|$=網路流量數，m=邊數，n=點數。Bellman-Ford 版本可以處理權重值為負的邊，而 Dijkstra 版本沒辦法。但是我們可以去調整邊上的權重值使之為正。調整方法為，先為剩餘圖上每一點α賦予一權重值 d(α)，它代表在剩餘圖中從 S 到α節點需經過的邊數，並在每一回合演算法去更新剩餘圖中的資訊時，將每邊的成本AF_{uv}調整為AF'_{uv}，其中$AF'_{uv}=AF_{uv}+d(u)-d(v)$，這樣就能保證每邊的成本為正。由於時間複雜度較低之關係，我們選用 Dijkstra 版本並去調整邊上的權重值使之為正。

5. 模擬

在本章中，我們以 Association Based 準則為例，讓我們的自動匹配演算法 LOM (Leader-Oriented Matchmaking)，去和其它自動匹配演算法進行比較。比較的方式為執行結果的好壞與執行時間之快慢。比較的對象分別為 M2L Greedy、L2M Greedy 和 Random。M2L Greedy 即為第一章提到的 Greedy 法，每一位隊員會去輪流檢查每一位隊長，並選出關聯度最佳的與之相連。L2M 為 M2L 的變形，作法為每一位隊長輪流去檢查每一位隊員，再選出關聯度最佳的與之相連。Random 法，假設系統中有 k 個隊長，每一隊需要 i 人。我們隨機選出 k*(i-1)位隊員，並將之切成 k 個區間，每個區間的玩者匹配給屬於各自區間的隊長。至於在 Association Factor 的定義方面，在一般情況中，系統為了求出此值，通常會先去取出每個玩者的個人資料(Profile)與記錄檔(Log)，並依此計算出玩者間的差異性。由於較小的差異性代通常表著較接近的關係，故我們在此定義 Association Factor 值愈小代表關聯度愈佳。

我們使用 C++來實作自動匹配演算法的模擬程式，並選定每一隊人數為 10 人，系統中等待遊玩的玩者數量設從 100 人到 500 人。每一次固定選前 k(同上一章所描述的 k)名玩者當隊長，剩下沒被選中的玩者當隊員。再來在所有隊長和隊員間隨機產生介於 1 到 100 間的關聯度。再來讓本論文提出的演算法 LOM 與其它三種演算法分別下去執行，比較輸出結果。在圖 3 中，橫軸的部份代表系統中

玩者的數量，縱軸的部份代表系統每位玩者的平均關聯度大小。

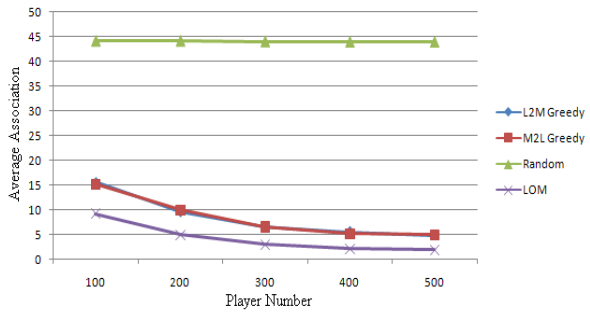


圖 3 各種自動匹配演算法輸出結果比較，其中橫軸的部份代表系統中玩者的數量，縱軸的部份代表系統每位玩者的平均關聯度大小

由圖 3 可以看出當使用 L2M Greedy、M2L Greedy 與 LOM 來匹配玩者時，它們的曲線有開口朝上，緩慢下滑的趨勢。原因在於，當系統中的玩者數量增多時，隊長與隊員之間的邊數隨之增多，進而代表權重值(關聯度)特別高和特別低的邊，其出現次數變多。又由於這三種演算法會專門去挑選權重值特別低的邊。導致系統中玩者愈多時，被挑中之低權重值的邊也愈多，造成整體系統的權重值之平均下降。

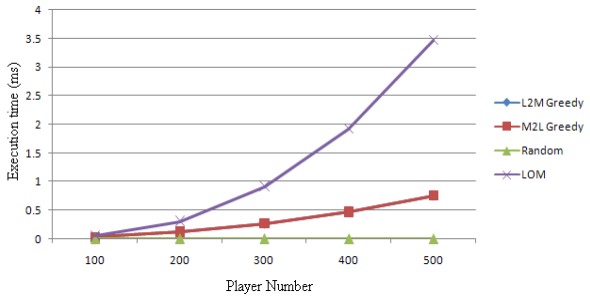


圖 4 各演算法的執行時間模擬結果

圖 4 為各演算法的執行時間模擬結果，橫軸為系統中玩者數量，縱軸為執行時間，單位為毫秒(millisecond, MS)。執行本模擬之電腦的規格為：AMD Phenom(tm) 9650 Processor 2.41 GHZ、2.00 GB Memory、Windows XP32 bits。雖然在執行時間之快慢的比較上，本論文提出的自動匹配演算法是需要較多時間的，但是因為採用多項式執行時間複雜度(polynomial time complexity)的 Minimum Cost Maximum Flow 演算法的概念解決問題，因此執行時間仍然在可以接受的範圍內，而且隨著電腦硬體性能快速的提升，以及近幾年非常熱門的雲端運算技術，相信此問題可以在這些因素的幫助下被克服。

6. 結論

目前自動匹配有兩大匹配玩者的準則，Connection Based 與 Skill Based 準則，前者將一群網路互相連線速度快的玩者匹配在一起進行遊戲，後者將一群彼此技能評分接近的玩者匹配在一起進行遊戲。但是這兩種準則都是以找出適合當自己對手的玩者為目標，而忽略了在多人連線遊戲中玩者的另一種互動模式，合作。故本論文額外提出了一種新的匹配玩者準則，稱為 Association Based。在此準則下，一群彼此關聯度的玩者被匹配在一起進行遊戲，可以大大的增加玩者間團隊合作的樂趣。

為了去解如何以 Association Based 準則來匹配玩者之議題，本論文提出了一個自動匹配演算法，稱為 LOM (Leader Oriented Matchmaking)。它使用到了 Minimum Cost Maximum Flow 演算法，以最佳化的方式去匹配系統中的玩者。值得一提的是目前現存的兩大匹配玩者準則，Connection Based 與 Skill Based，亦可套用於 LOM 中去匹配玩者，並皆可依各自的需求得到最佳的輸出結果。套用在 Association Based 準則，它可以幫系統中的每一位玩者匹配出最佳的團隊出來。套用在 Connection Based 準則，它可以最佳化系統中每一位玩者的網路連線速度。套用在 Skill Based 準則，它可以讓系統中同場遊戲玩者間的技能評分差距最小。故本論文提出的自動匹配演算法可以針對不同的匹配玩者準則，做到最佳的輸出結果。進而最佳化系統中每一位玩者在進行多人連線遊戲時的體驗。

在模擬中，我們以 Association Based 準則為例，讓我們的自動匹配演算法 LOM，去和其它自動匹配演算法進行比較。比較的方式為執行結果的好壞與執行時間之快慢，在執行結果好壞的比較中，我們驗證了 LOM 的執行結果優於其它演算法。雖然在執行時間之快慢的比較上，LOM 是最慢的，但是隨者電腦硬體性能快速的提升，以及近幾年非常熱門的雲端運算技術，相信此問題可以在這些因素的幫助下被克服。

未來，我們希望能探討在 Association Based 匹配玩者的準則下，應該如何更精確的利用玩者的個人資料(Profile)與記錄檔(Log)上的資料，來計算隊長和隊員間的關聯度。以求能更真實的反映出他們之間的團隊默契。

參考文獻

[1] S. Agarwal, and J. R. Lorch, “Matchmaking for online games and other latency-sensitive P2P systems,” in Proc. of ACM SIGCOMM Conference on Data Communication, pp. 315-326, 2009.

[2] R. Coulom, “Whole-history rating: A Bayesian rating system for players of time-varying strength, “ in Proc. of the 6th International Conference on Computers and Games (CG ’08), pp. 113–124, 2008.

[3] O. Delalleau, E. Contal, E. Thibodeau-Laufer, R. C. Ferrari, Y. Bengio, and F. Zhang, “Beyond skill rating: advanced matchmaking in ghost recon online,” IEEE Trans. on Computational Intelligence and AI in Games, Vol. 4, Issue. 3, pp. 167-177, Sep. 2012.

[4] M. T. Goodrich and R. Tamassia, Algorithm Design: Foundations, Analysis, and Internet Examples, Baker & Taylor Books, 2001.

[5] R. Herbrich, T. Minka, and T. Graepel, “TrueSkill: a bayesian skill rating system,” Advances in Neural Information Processing Systems, pp. 569–576, 2006.

[6] J. Jimenez-Rodriguez, G. Jimenez-Diaz, and B. Diaz-Agudo, “Matchmaking and case-based recommendations,” in Proc. of Workshop on Case-Based Reasoning for Computer Games, the 19th Int. Conf. on Case Based Reasoning, pp. 53–62, 2011.

[7] J. Manweiler, S. Agarwaly, M. Zhangy, R. R. Choudhury, and P. Bahlym, “Switchboard: a matchmaking system for multiplayer mobile games,” in Proc. of the 9th International Conference on Mobile Systems, Applications, and Services (MobiSys '11), pp. 71-84, 2011.

[8] J. Riegelsberger, S. Counts, S. Farnham, and B. C. Philips, “Personality matters: incorporating detailed user attributes and preferences into the matchmaking process,” in Proc. of the 40th Annu. Hawaii Int. Conf. on System Sciences, pp. 87-87, 2007.

[9] R. C. Weng, and C.-J. Lin, “A Bayesian approximation method for online ranking,” Journal of Machine Learning Research, pp. 267–300, 2011.

行動虛擬社群科技壓力之研究

洪為璽　　蘇永松
國立中正大學 資訊管理學系
fhung@mis.ccu.edu.tw
song299558@gmail.com

摘要

隨著科技的進步，網際網路與無線通訊快速的帶起行動科技的發展，而由於無線網路以及通訊的發達，使得智慧型手機變成近幾年來最受矚目的科技之一。而使用者最常使用的行動服務是社交網路，尤其是 Facebook。但也伴隨而來許多負面的使用體驗，例如:手機焦慮、科技依賴等等所形成的科技壓力。

本研究欲探討在目前行動化環境下使用者透過智慧型裝置來使用虛擬社群是否會發生下列問題：(1)當使用者過度依賴智慧型手機使用行動虛擬社群，是否會增加使用者的「無所不在科技壓力」?(2)哪些因素影響使用者過度依賴於行動虛擬社群?根據上述研究問題本研究針對「認知易用性」、「娛樂性」、「專注性」及「知覺控制」等因子，探討是否會影響使用者使用行動虛擬社群(Facebook)造成「科技依賴」，進一步降低或者是提升「無所不在的科技壓力」。

並且以有使用行動虛擬社群(Facebook)之使用者為研究對象，共回收了 1013 份問卷，並以 SPSS 20 及 AMOS 20 做為資料分析工具，並建立結構方程模型，檢定研究架構中各構面的路徑關係。研究結果發現「認知易用性」、「娛樂性」、「專注性」及「知覺控制」皆會影響「科技依賴」，「科技依賴」會正向影響無所不在科技壓力的產生。

關鍵詞：行動虛擬社群、Facebook、科技依賴、無所不在科技壓力、結構方程模式。

Abstract

With the advances in technology, the use of the Internet and wireless communications leads to the prevalence of mobile technology, and due to wireless networks and communications infrastructure, the smartphone has become one of the high-used technologies in recent years. Among the mobile services, the most frequently used is social networks, especially Facebook. However, such use also brings a lot of negative impacts, such as: mobile anxiety, technology dependence, technostress, and so on.

This study aims to answer the following questions when the users use smart devices in the virtual community at mobilize environment (1) When the user over-rely on the smartphone for mobile virtual community will increase the user's " Ubiquitous Technostress "? (2) Which factors will affect the user's behavior of over-relying on the Mobile Virtual Community? According to the research questions, this study focuses on "Perceived Ease of Use", "Playfulness", "Concentration" and "Perceived Control" and investigate will affect the user to the use of mobile virtual communities (Facebook) and cause "technology dependent" to further reduce or enhance the " Ubiquitous Technostress."

In this study, a total of 1013 questionnaires were collected, and using SPSS 20 and AMOS 20 as data analysis tools, and the structural equation model technique was utilized to verify the path relationships in the proposed research framework. The results found that "Playfulness" and "Concentration" will positively affect "Perceived Ease of Use"; "Playfulness", "Concentration" and "Perceived Control" will all positively affect "Technology Dependent"; "Technology Dependent" will positively affect the "Ubiquitous Technostress".

Keywords: Mobile Virtual Community、Facebook、Technology Dependent、Ubiquitous Technostress、SEM.

1. 前言

近年來行動科技的快速發展以及基礎設施的成熟，人人手上幾乎都有一支手機，人們對手機功能的需求也從早期僅能撥打電話、簡訊功能、簡單的遊戲功能，演化到現在，不僅手機具有透過 Wifi、3G 上網的功能也具有智慧型作業平台，幫助處理工作、娛樂、資訊上，儼然成為可以隨身攜帶的資料庫，讓人們越來越需要它。

使用社群網站已成為全球使用者所從事的行動上網活動中成長最快速的一個，這也是手機使用者與他人交流常用的方式，因而成為促使人們行動上網的驅動力。但也隨著社群網路使用的時間越來越久，可能造成社群網路沉迷，讓使用者覺得必須無時無刻要去關注社群上的最新動態，以免自己跟不上別人的話題，無形中造成使用上的壓力，這樣就與社群網站本身的立意大相逕庭，隨著行動設備的普及化，甚至有一個新的名詞「低頭族」，指的是因為太過於依賴行動科技而無時無刻拿著智慧型裝置滑來滑去的族群，所以行動化加上社群網站帶來的壓力可能只會增加，不會減少。

因應上述目前行動化環境下使用者透過智慧型裝置使用虛擬社群所造成的負面影響，本研究欲探討下列問題：(1)當使用者過度依賴智慧型手機使用行動虛擬社群，是否會增加使用者的「無所不在

科技壓力」?(2)哪些因素影響使用者過度依賴於行動虛擬社群?根據上述問題本研究提出「認知易用性」、「娛樂性」、「專注性」及「知覺控制」等因子，探討是否會影響使用者使用行動虛擬社群(Facebook)造成「科技依賴」，進一步降低或者是提升「無所不在的科技壓力」。

2. 文獻探討

2.1 虛擬社群

虛擬社群(virtual community)又稱為線上社群(online community)、網路社群(network community)、或是電子社群(electronic community)。虛擬社群的起源可追溯到 1976 年實行的電子資訊交換系統，此系統著重電腦化會議系統，使人們能行使群體智慧的能力。而在 1970 年代末期，個人電腦透過數據機連接網路，讓許多人一同參與虛擬討論，這種電子佈告欄系統屬早期虛擬社群的形式[1]。

而「虛擬社群」此名詞，最早是由[2]所提出，Rheingold 認為虛擬社群是「社會集合體，發生於有夠多的人在網路上進行長久的公開討論，並付出充分的情感，在網路空間所形成的人際關係網路。」其後有不同的學者也對虛擬社群給予定義。[3]則認為線上社群最基本的定義就是「一群使用電腦中介傳播而溝通的使用者，彼此間有相同的興趣或目標，並分享資源。」，[4]定義虛擬社群是「在數位環境中的中介社會空間，使群體能透過持續的溝通過程，而形成與維持。」，[5]認為人們在網路上為了獲取資訊或提供資訊而聚集，通常就稱為虛擬社群，並將虛擬社群定義為「一群有著共同興趣或工作的人們，以有組織的方式，在網路上透過共同擁有的電子空間和機制持續規律的溝通」。

2.2 Facebook

Facebook 是一個社群服務網站，於 2004 年上線，根據 Facebook 統計至 2012 年 10 月截止已有 10 億用戶使用 Facebook，其中每月約有 6 億次使用紀錄是透過行動裝置使用，由於 Facebook 是目前使用人口最多的社群平台，因此對於社群網站最具有代表性，故本研究針對 Facebook 為研究主題。

Facebook 成立之後的短短幾年之內，就快速成為全世界最受歡迎的虛擬社群網站，尤其是大學生，在校園中學生的使用率高達 90%以上[6]。

2.3 行動虛擬社群

自從智慧型手機流行之後，社群網站也趁勢在不同手機平台推出 APP，也因為「行動」這個特性，讓社群行為中最受到歡迎的功能，包括照片分享、旅遊資訊（含位置服務）、即時線上傳訊、影片 streaming 上傳下載等功能變得能隨處使用，行動服務業者也搭乘這波行動虛擬社群風潮，提供整合具雙向溝通功能的多元服務，藉以吸納更多用戶加入，並依此獲取更多行動服務商機。所以本研究將「行動虛擬社群」定義為：利用行動化的特性，透過行動裝置使用的虛擬社群。

雖然行動社群被視為虛擬社群的延伸，然而這兩個平台它們之間還是有一些差異存在，[7]對於行動虛擬社群和虛擬社群提出了幾點差異：(1)行動社群可以透過行動設備來進行(2) 透過行動網路的運用，行動社群可以提供新的溝通服務(3) 行動社群和虛擬社群相比，有不同的使用模式。[8]則認為行動設備具有四項特性，分別是位置察覺性 (Location awareness)、無所不在性 (Ubiquity)、可辨識性 (Identification)以及立即性 (Immediacy)。行動社群便是運用這些特性，使其本身的運用價值大幅提升。

2.4 科技依賴

[9]提出網路成癮(Internet addiction)有以下心理依賴特性：(1)耐受性(Tolerance) ：指的是隨著網路使用經驗的增加，當事者必須透過更多的網路內容或更長時間來滿 足使用網路的程度。(2)戒斷(Withdrawal) ：指的是如果當事人被迫離開電腦，容易出現負面的情緒反應，例如：情緒低落、生氣、 空虛感等，或是注意力不集中、心神不寧、坐立不安等反應。(3)復發(Recurrence)：使用者在戒除該成癮行為後，仍不斷的復發及故態復萌，再重複過去的成癮行為模式。

而使用行動虛擬社群，是使用智慧型載具透過網路連上虛擬社群網頁或是虛擬社群應用程式，若是過度使用也可能會發生依賴甚至成癮的症狀。

2.5 使用者意圖理論

使用者意圖理論觀點認為，使用者使用系統是一種行為表現，而影響行為最重要的因素是意圖(動機)，因此，使用者意圖理論學派認為不論系統如何，如果使用者不使用就是一個失敗的資訊系統，而使用者的意圖會影響資訊系統的成功失敗。所以必須瞭解哪些因素會影響使用者的使用意圖，才能改善系統，進而提升使用資訊系統的頻率。

本研究根據使用者意圖理論為基礎，提出認知易用性、娛樂性、專注和知覺控制可能影響使用者使用行動虛擬社群之屬性與特徵作為變數。

2.6 無所不在科技壓力

科技壓力（Technostress）最早由[10] 提出，其定義為：是一種近代在健康管理上的適應疾病，主要因為沒能力處理新電腦科技而產生。[11]更進一步定義科技壓力為：任何因為科技直接或間接而產生在態度、思想、行為或心理的負面影響。現代人日常生活中充斥著資訊科技，資訊科技也日新月異的進步，導致使用者們一直適應新科技所帶來的效用，而引起負面反應，這些科技所帶來的負面因素就是所謂的科技壓力(Technostress)。

根據[12]發展並驗證科技壓力的衡量量表，此量表定義出五個組成科技壓力之因素，描述使用電腦科技可能產生科技壓力的情況。包括：

(1)科技超載(Techno-overload)：通訊科技(ICTs)促使員工工作加快。(2)科技侵犯(Techno-invasion)：充斥各處的通訊科技侵犯個人生活。(3)科技複雜性(Techno-complexity)：新科技的複雜性使得員工感到無法勝任。(4)科技不安性(Techno-insecurity)：由於科技迅速改變，使得員工感到在工作上有所威脅，深怕被科技取代。(5)科技不確定性(Techno-uncertainty)：通訊科技軟體及硬體的持續改變、更新及錯誤修正，造成員工壓力。

根據[13]認為網路以及無線行動裝置（例如行動手機、PDA）所具有持續連線以及無所不在的特性，使得個人在使用這些行動裝置時等於暴露在一個被隨時監控和隨叫隨到（On Call）的環境底下，讓個人感受到科技過度的侵犯。而在工作之中，因為行動科技導致得員工必須處理來自四面八方的任務需求，工作時間也隨著行動科技帶入員工在工作以外的私人時間，如此都會影響到員工的生產力。[14]認為近年來因為通訊技術的發展，帶給我們越來越便捷的生活，徹底改變了我們的日常生活和工作型態，讓我們可以在任何地點任何時候接收到來自四面八方的訊息。然而行動科技的快速發展，也造成我們處於一個行動科技無所不在的環境底下，因此導致一些負面情緒的產生。[15]在研究中首先提出了「無所不在科技壓力」(Ubiquitous Techno-Stress）的概念。[15]推論以往人們感受到科技壓力的因素已經有所改變，以往因為不熟悉科技所產生的壓力，已經轉為因為長時間曝露在科技的環境底下所造成，形成所謂的「無所不在科技壓力」。

3. 研究方法

3.1 研究架構

本研究根據先前第二章文獻探討將過去研究整理出的四個前置因素：認知易用性、娛樂性、專注和知覺控制來探討對行動虛擬社群的使用是否產生科技依賴，最後進一部探討科技依賴是否會降低或是提高使用者使用行動虛擬社群所造成的無所不在科技壓力。

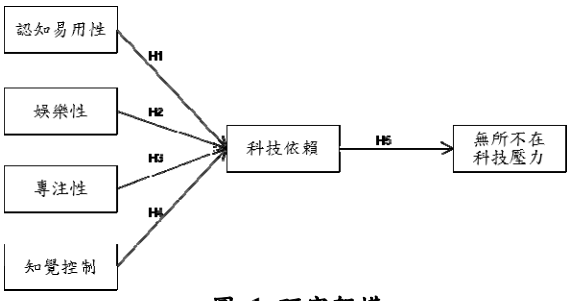


圖 1 研究架構

表 1 操作型定義

構面	衡量變數與定義
無所不在科技壓力	使用者因長期使用具有高度可及性、行動性與具有無所不在特性之行動虛擬社群，以致於處在一個高度連結的環境下，進而所產生之無形壓力
專注性	使用者全心全力投入在使用行動虛擬社群
認知易用性	使用者認為使用行動虛擬社群是容易的
娛樂性	使用者使用行動虛擬社群中感到愉快的狀態
知覺控制	使用者認為自己能完全掌控行動虛擬社群的操作
科技依賴	過度依賴行動科技設備連結行動虛擬社群而造成在手機上的過度使用和成癮的情形

3.2 研究假說推導與建立

使用者意圖對科技依賴的影響

這部分以使用者意圖為基礎探討是否會造成使用者對使用行動虛擬社群產生科技依賴，推導出下列假說:

先前的文獻研究指出，易用性對於個人意圖是較強烈的決定因子[16]。[17]研究發現當消費者認知到學習使用新科技的「認知易用性」越高時，對該新科技的態度也會越佳。本研究認為行動虛擬社群如果具有易用性，能讓使用者更容易去熟悉使用行動科技，可能會有進一步的依賴情況發生。

H1：認知易用性會增加行動虛擬社群使用者科技依賴的效果

根據[18]指出，網路成癮的影響因素包括有娛樂性(Playfulness)等許多因素，尤其又以娛樂性影響最大，當使用者感覺到愉快時會增加使用上的信心，最後增加網路探索的行為。

H2：娛樂性會增加行動虛擬社群使用者科技依賴的效果

根據[19]的研究指出個體會花費許多時間在網路遊戲中，會因為過度的投入於網路遊戲之中，而影響個人的生活，一旦被要求停止網路遊戲行為會感覺到挫折，個體也會出現強迫性使用網路遊戲的情況。當使用者越專注越投入於使用行動虛擬社群時，越會造成行動虛擬社群的依賴。

H3：專注會增加行動虛擬社群使用者科技依賴的效果

根據[20]人機互動的研究中指出，人們沉迷於線上遊戲而享受其中，最主要的原因是玩家對於線上遊戲有強大的控制感，將會沉迷於其中，表現出

更積極的行為，以致於依賴的產生。
當人們操作電腦介面時須要有控制感，才會令人進入享受其中的感覺，有高度的網站瀏覽知覺控制，就會越想使用而造成依賴。當使用者自覺具有使用某項資訊科技資源時，其對於該使用行為的知覺控制性會增加，因而使得個體會傾向於使用該科技[21]。

H4：知覺控制會增加行動虛擬社群使用者科技依賴的效果

科技依賴對無所不在科技壓力的影響

網路和電腦相關技術已成為日常生活工作中不可或缺的一部分[22]。越來越多人使用科技產品去改善生活，換句話說人們也越來越依賴科技產品。

根據[23]指出一個人如果具有較高的科技依賴，可能面對的麻煩包含科技過載、科技複雜性、不確定性等與科技壓力相關的特性而且智慧型手機也是最近最熱門的科技產品之一。

H5：科技依賴會增加使用者使用行動虛擬社群所造成的無所不在科技壓力。

根據[23]指出一個人如果具有較高的科技依賴，可能面對的麻煩包含科技過載、科技複雜性、不確定性等與科技壓力相關的特性。

4. 資料分析與討論

本研究的主要對象為使用行動虛擬社群的使用者(使用智慧型手機、平板等行動裝置使用Facebook)，而問卷的發放方式主要採取線上問卷的方式進行，問卷資訊張貼於國內各大網站與論壇，此外為了提高問卷的回收率，本研究提供抽獎活動來提升填答意願。問卷回收期間為民國 102 年 5 月 22 日至 6 月 05 日，回收的問卷總計 1013 份，在刪除不符合資格（例如：填答從未使用行動虛擬社群、反向題答錯）、重複作答（例如：整份問卷勾選同一答案）以及離群值，共計刪除 80 份問卷，最後實際有效樣本為 933 份。並使用 SPSS 20.0 與 AMOS 21.0 統計套裝軟體來做為問卷資料的分析工具。

表 2 性別、學歷及年齡基本資料分析

資料項目	類別	次數	百分比
性別	男	511	54.7%
	女	422	45.3%
學歷	國中以下	5	0.5%
	高中	31	3.3%
	大學	605	64.8%
	研究所以上	291	31.3%
年齡	20 歲以下	80	8.6
	21~30 歲	707	75.8%
	31~40 歲	133	14.3%
	41~50 歲	11	1.2%
	51 歲以上	2	0.2%

表 3 職業及年資基本資料分析

資料項目	類別	次數	百分比
職業	學生	520	55.7%
	軍公教人員	68	6.2%
	服務業	127	13.6%
	工商業	182	19.5%
	其他	36	5.0%
年資	150,000 以上	2	0.2%
	100,001-150,000 元	8	0.9%
	80,001-100,000 元	6	0.6%
	65,001-80,000 元	8	0.9%
	50,001-65,000 元	47	5.0%
	35,001-50,000 元	109	11.7%
	20,001-35,000 元	197	21.1%
	20,000 元以下	556	59.6%

4.1 信度分析

信度(Reliability)是用來測量結果的一致性(Consistency)和穩定性(Stability)，也是用來衡量工具的可靠程度，信度高代表的是變異程度較低。一個具有信度的測量工具，必須在不同的條件下都能夠獲得穩定的測量結果。而信度測量方式主要有四種：有測法(Retest method)、複本法(Alternative-form method)、折半法(Splithalves method)和內部一致性法(Internal consistency method)。本研究將採取 Cronbach’s α值來測量問卷的內部一致性，α愈高表示衡量工具的可信度愈高，而[24]則建議 Cronbach’s α值應高於 0.7，若 低於 0.35 應給予拒絕，本研究將採取此原則對後續樣本做信度檢驗分析。

表 4 刪除後 Cronbach’s α 及組合信度

構面	Cronbach’s α	組合信度
認知易用性	0.843	0.8961
娛樂性	0.860	0.8991
專注性	0.863	0.9069
知覺控制性	0.862	0.8965

科技依賴	0.832	0.8831
無所不在科技壓力	0.839	0.8844

4.2 效度分析

收斂效度

收斂效度以觀察變項對潛在變數的因素負荷量為指標，而[25]建議平均變異抽取量(Average Variance Extracted, AVE)需大於 0.5，平均變異抽取量是計算各觀察變項對其潛在變數的平均變異解釋力，平均變異抽取量越高的話，證明該潛在變數有越高的收斂效度及區別效度。區別效度的判斷依據為每一構面的平均變異抽取量之平方根要大於其他構面間的相關係數，如此就證明有一定程度的區別效度[26]，分析結果顯示，平均變異抽取量均大於 0.5 且各構面之平均變異抽取量之平方根皆大於其他構面之相關係數，表示本研究量表具有一定程度的收斂效度及區別效度。

建構效度

轉軸後的成分矩陣，本研究採用最大變異數法(Varimax)，其以共同因素為主，目的是使變項在同一個共同因素的因素負荷量的變異極大化，以便於探討個別的共同因素較能代表哪些變項。為方便觀看，將小於 0.5 的值加以隱藏，結果顯示題項皆沒有交叉因素負荷量，沒有共同方法偏誤的問題，因此無需刪除任何題項，表示本研究具有良好的建構效度。

4.3 模型配適度評估

本研究的整體模式配適度如下所示，卡方值自由度為 2.606，符合需小於 3 之標準；GFI 值為 0.918，符合需大於 0.8 之標準；RMR 值為 0.088，不符合需小於 0.05 之標準；RMSEA 值為 0.042，符合需小於 0.08 之標準；AGFI 值為 0.918，符合需大於 0.8 之標準；NFI 值為 0.902，符合需大於 0.9 之標準，NNFI 值為 0.919，符合需大於 0.9 之標準；CFI 值為 0.948，符合需大於 0.9 之標準；RFI 值為 0.909，符合需大於 0.9 之標準；IFI 值為 0.948，符合需大於 0.9 之標準；PNFI 值為 0.886，符合需大於 0.5 之標準；PCFI 值為 0.814，符合需大於 0.5 之標準；PGFI 為 0.840，符合需大於 0.5 之標準。從以上結果來看，大部分配適度指標皆符合標準，表示整體模式的適合度良好。

4.4 假說驗證

本研究建構一個模型研究科技依賴對無所不在科技壓力的影響，提出「認知易用性」、「娛樂性」、「專注性」、「知覺控制」、「科技依賴」與「無所不在科技壓力」之模型路徑圖。

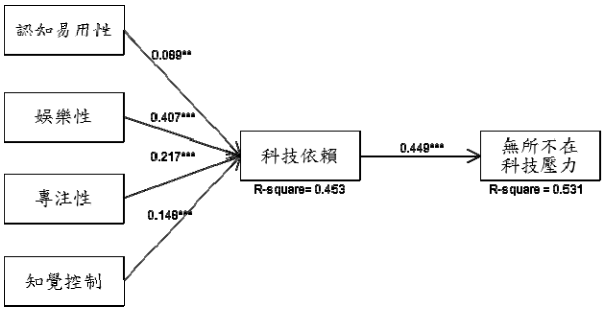


圖 2 模型路徑圖

表 5 假說判定

編號	是否成立	T 值	路徑係數
H1	是	2.564	0.089**
H2	是	9.599	0.407***
H3	是	6.108	0.217***
H4	是	4.242	0.148***
H5	是	9.882	0.449***

從本研究的實證結果中可以發現「認知易用性」、「娛樂性」、「專注性」及「知覺控制」皆會對「科技依賴」有顯著的正向影響，「科技依賴」對提升「無所不在科技壓力」有顯著的正向影響。

5. 結論

5.1 研究結論

本研究利用問卷調查後進行實證，分析出許多結果，在此根據本研究之研究問題提出以下各問題的結論與看法。

本研究發現「認知易用性」、「娛樂性」、「專注性」及「知覺控制」皆會對「科技依賴」產生正向影響，也就是說以上因素都會造成使用者過度依賴於使用行動虛擬社群，造成成癮的現象，並且研究結果也證實「科技依賴」的產生會增加使用者感受到的「無所不在科技壓力」，表示當使用者離不開使用行動虛擬社群也會讓使用者感受到生活不斷被行動虛擬社群打擾，但卻又離不開它。

本研究結果也發現「娛樂性」及「專注性」這兩個因子是影響使用者產生科技依賴的兩個最強因子，而本研究蒐得樣本使用者年齡大多集中在 21 到 30 歲的學生族群，這個族群本身就是最容易沉迷於科技使用的族群，而娛樂性一直以來都是被視為接納科技的關鍵因素，專注性可以代表使用者涉入行動虛擬社群的程度，行動虛擬社群讓使用者越感到有趣或涉入越深，就會讓使用者花費更多時間在使用行動虛擬社群而產生成癮，若要避免成癮，使用者應避免因為行動虛擬社群娛樂價值高就不

斷的使用，打亂生活作息。

5.2 研究貢獻

以往文獻探討虛擬社群的使用較多是以在電腦上使用為主，而考慮到近年智慧型手機的普及以及行動虛擬社群的流行，所以本研究結果發現在使用行動虛擬社群的情境下，「認知易用性」、「娛樂性」、「專注性」及「知覺控制」皆會對「科技依賴」有顯著影響。

5.3 限制與未來研究

本研究抽樣對象為網路發放問卷的方式蒐集而來，對象大多以 Facebook 以及 PTT 實業坊裡面的幾個版，包括 Q_ary、draw、Android、IOS 等，其中 Facebook 的對象大多為朋友以及朋友的朋友，而 PTT 實業坊的對象則大多為大學生以及研究生，但是根據調查目前使用行動虛擬社群的使用者大多分布在 21 歲到 30 歲跟學生族群，跟本研究蒐得樣本結果符合，但若是將來能多蒐得其他年齡層的使用者來與蒐得樣本結果做比較，將會更完善。

目前行動虛擬社群平台不只有 Facebook 而已，Plurk、Myspace、Twitter 以及 Line 等等，雖然這些社群平台用戶人數已 Facebook 占大多數，但其它社群用戶數量也不容小覷，若以這份研究推論到其他社群平台，與其他社群平台做比較，了解本研究結果是否一樣適用於其他平台。

參考文獻

[1] Balasubramanian, S., & Mahajan, V. (2001). The Economic Leverage of the Virtual Community. International Journal of Electronic Commerce, 5(3), 103-138.

[2] Rheingold, H. (1993). The Virtual Community: Homesteading on the Electronic Frontier . Cambridge: Mass. MIT Press.

[3] Preece, J. (2002). Supporting Community and Building Social Capital. Communications of the ACM, 45(4), 37-39.

[4] Bagozzi, R.P., & Dholakia, U.M. (2002). Intentional Social Action in Virtual Communities. Journal of Interactive Marketing, 16(2), 2-21.

[5] Ridings, C.M., Gefen, D., & Arinze, B. (2002). Some Antecedents and Effects of Trust in Virtual Communities. The Journal of Strategic Information Systems, 11(3), 271-295.

[6] Ellison, N.B., Steinfield, C., & Lampe, C. (2007). The Benefits of Facebook "Friends:" Social Capital and College Students' Sse of Online Social Network Sites. Journal of Computer‐ Mediated Communication, 12(4), 1143-1168.

[7] Fremuth, N., Tasch, A., & Fränkle, M. (2003). Mobile Communities–New Csikszentmihalyi, M. (1975). Beyond Boredom and Anxiety: The Experience of Play in Work and Games. San Francisco: Jossey‐ Bass.

[8] Prykop, C., & Heitmann, M. (2006). Designing Mobile Brand Communities: Concept and Empirical Illustration. Journal of Organizational Computing and Electronic Commerce, 16(4), 301-323.

[9] Griffiths, MD. (1998). Internet addiction: Does it really exist? In J. Gackenbach (Ed.), Psychology and the internet: Intrapersonal, interpersonal and transpersonal implications. New York: Academic Press.

[10] Brod, C. (1984). Managing technostress: optimizing the use of computer technology. Personnel Journal, 61(10), 753-757.

[11] Weil, M. M., & Rosen, L. D. (1997). Technostress: Coping with Technology @ work @ home @ play. New York: Wiley.

[12] Tarafdar, M., Tu, Q., Ragu-Nathan, B.S., & Ragu-Nathan, TS. (2007). The Impact of Technostress on Role Stress and Productivity. Journal of Management Information Systems, 24(1), 301-328.

[13] Clark, K., & Kalin, S. (1996). Technostressed Out? How to Cope in the Digital Age. Library Journal, 121(13), 30-32.

[14] Hoffman, D.L., Novak, T.P., & Venkatesh, A. (2004). Has the Internet Become Indispensable? Communications of the ACM, 47(7), 37-42.

[15] Hung, W.H., Chang, L.M., & Lin, C.H. (2011). Managing the Risk of Overusing Mobile Phones in the Working Environment: A Study of Ubiquitous Technostress. Paper presented at the Proc 15th Pacific Asia Conference on Information Systems, Brisbane.

[16] Venkatesh, V., & Morris, M.G. (2000). Why Don't Men Ever Stop to Ask for Directions? Gender, Social Influence, and Their Role in Technology Acceptance and Usage Behavior. MIS Quarterly, 24(1), 115-140.

[17] Davis, F.D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13(3), 319-340.

[18] Chou, T. J., & Ting, C. C., 2003, "The role of flow experience in cyber-game addiction", CyberPsychology & Behavior, 6, 663-675.

[19] Suler,J.(2004). The online disinhibition effect. CyberPsychology and Behavior,7, 321-326.

[20] Mathwick, C., & Rigdon, E. (2004). Play, Flow, and the Online Search Experience. Journal of Consumer Research, 31(2), 324-332.

[21] Taylor, S., & Todd, P.A. (1995). Understanding Information Technology Usage: A Test of Competing Models. Information Systems Research, 6(2), 144-176.

[22] Shin, D.H., & Shin, Y.J. (2011). Why do People Play Social Network Games? Computers in Human Behavior, 27(2), 852-861.

[23] Shu, Q., Tu, Q., & Wang, K. (2011). The Impact of Computer Self-Efficacy and Technology Dependence on Computer-Related Technostress: A Social Cognitive Theory Perspective. International Journal of Human-Computer Interaction, 27(10), 923-939.

[24] Hair, J. F., Anderson, R. E., Tatham, R. L. and William, C. (1998). Multivariate data analysis (5 ed.). Upper Saddle River, NJ: Prentice Hall.

[25] Fornell, C., & Larcker, D.F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research, 18(2), 39-50.

[26] Gefen, D., Straub, D. W. and Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice. Communications of the Association for Information Systems, 4(7), 1-70.

智慧型手機即時通訊軟體使用行為之調查研究

蔡瑋哲
靜宜大學資訊傳播工程學系
g9973006@pu.edu.tw

蔡英德
靜宜大學資訊傳播工程學系
yttsai@pu.edu.tw

摘要

隨著資訊科技的發展，智慧型手機越來越普及，行動通訊網際網路速度漸漸提升，在傳統個人電腦上的即時通訊軟體已無法滿足使用者，即時接收傳遞訊息的需求。無所不在的方式讓手機即時通訊軟體扮演著新興通訊重要角色。在未來手機通訊軟體也將演變為社群交友工具。

本論文主要探討智慧型手機即時通訊軟體使用意向與實際之行為，透過整合性科技接受模式(UTAUT)為研究架構，針對 LINE、Skype、WhatsApp、WeChat 使用者進行問卷調查，回收有效樣本 533 份。調查使用者目前對於手機即時通訊軟體的使用意向、接受度與使用情況。結果顯示：手機通訊軟體之促成環境皆未影響使用行為。本論文也探討各軟體的績效期望、努力期望與社會影響對其行為意向及使用行為的影響關係。

關鍵詞：整合性科技接受模式、智慧型手機、即時通訊軟體。

Abstract

With the development of information technology, the smart phones get more and more common and the speed of mobile telecommunication Internet gets higher. The Instant Messenger software on traditional Personal Computer can't satisfy the users in the need of receiving instant messages. And the Instant Messenger software on phones play the important roles in new communication. In the future, mobile Instant Messenger software will evolve as communities dating tool.

The research uses Unified Theory of Acceptance and Use of Technology (UTAUT) as the research framework to study the users of smart phones. And the effective samples are 533 copies. The research adopts questionnaires collected from the users on their intention, acceptance, and state. The result showed that: The Facilitating Conditions of mobile Instant Messenger software are not affect Use Behavioral. This thesis also explored various software Performance Expectations, Effort Expectancy, Social Iinfluence and Behavioral Intention to use its influence behavior relationship.

Keywords: Unified Theory of Acceptance and Use of Technology, Smart Phone, Instant Messenger.

1. 緒論

隨著資訊科技的發展，手機行動網路的普及，智慧型手機的興盛與蓬勃發展，全球使用手機上網人口快速增加，智慧型手機已徹底影響我們的日常生活。除了透過網路帶給使用者前所未有的便利性，也深深的影響人們傳遞訊息的模式。

根據國家通訊傳播委員會（NCC）資料顯示，2012 年第 3 季我國行動電話門號數達 2,936 萬戶，其中可行動上網的門號有 1,948 萬個，其中有開通行動數據服務達 66.3%，表示越來越多人使用手機行動上網。而相較於電子郵件，手機即時通訊軟體，如 LINE、Skype、WhatsApp、WeChat 等，不須嚴謹的格式，且更快速、更即時、更容易形成社群群組溝通，因此吸引越來越多用戶使用。

本研究從使用者角度，探討使用智慧型手機通訊軟體的關鍵因素。並透過「整合性科技接受模式(Unified Theory of Acceptance and Use of Technology, UTAUT)」為理論基礎，探討智慧型手機即時通訊軟體使用意向與實際行為。本研究目的有三：一、探討使用者使用智慧型手機通訊軟體間的差異；二、了解不同智慧型手機通訊軟體之特徵，與使用行為的成因。三、希望可藉由了解使用者的關鍵因素後，進而提供未來軟體供應商建置設計之參考。

2. 文獻探討

2.1 即時通訊

「即時通訊軟體」即是“透過網路，讓您與您的同事、朋友、親人之間即時溝通，而為了通訊方便，可建立自己的親朋好友名單。當名單上的連絡人上線時，您可以立即得知。您們可以交談、傳送立即訊息、照片或檔案、撥打電話，或是透過網路攝影機看見彼此。再加上一些有趣的表情符號讓您更能生動的傳達您的情緒。即使親愛的朋友或家人遠在他鄉，也可以保持密切聯繫”[20]。

早期即時通訊(IM)只以文字為主的溝通方式，已經無法滿足網友需求，業者也藉著手機的發展，與網際網路速度的提升，針對智慧型手機開發手機專用的通訊軟體。

APP01 網站對 10 萬名使用智慧型手機的會員進行調查，調查結果指出近 67%的用戶使用「LINE」，而較早推出的「WhatsApp」則有 17%使用者使用，其他通訊軟體如「M+Messenger、WeChat、Cubie Messenger、FreePP 免費電話」等手機通訊軟體雖

有不錯的口碑與下載量，但仍非手機用戶的首選選擇[2]。以下將介紹使用者較常使用之手機通訊軟體。

LINE 是由 NHN Japan Corp.開發的一智慧型手機應用程式，使用者可以透過網際網路跨國界、跨電訊網路營運商，與其他使用者進行免費語音通話、圖片傳遞或訊息傳遞。LINE 最初是針對女性用戶設計，供用戶傳遞情感的軟體，女性用戶大多以圖片代替文字，表示難以表達之圖片符號。所以貼圖功能也是 LINE 的最大賣點，除了饅頭人（Moon）、熊大（Brown）、兔兔（Cony）和詹姆士（James），使用者還能購買多款知名卡通的系列貼圖，在傳訊時刻增添更多歡樂色彩。

Skype 是一群由愛沙尼亞的軟體開發人員於 2003 年開發，支援語音通訊的即時通訊軟體，採用點對點技術與其他用戶連接。除了具備即時通訊(IM)所需的功能，如視訊聊天、多人語音會議、多人聊天、資料傳輸、文字聊天等功能。Skype 可以進行免費語音通話，也可跨電信跨網路撥打國內、國際電話，無論室內電話、行動電話，皆可直接撥打、簡訊傳送等功能。

WhatsApp 是由美國科技公司 WhatsApp Inc.所開發，WhatsApp 類似於傳統電腦上的 MSN 、Yahoo! Messenger，皆透過網路傳送訊息，差別在於，WhatsApp 可直接註冊手機號碼成為帳號，並與電話簿裡的同時也安裝 WhatsApp 的好友進行通訊。身為元老級的手機通訊軟體，WhatsApp 的使用介面簡單俐落，適合男性與商務目的、作為純粹的簡訊工具；所以關於貼圖及表情符號方面，也是在目前所有通訊軟體中最簡單的。與 LINE 不同之處，WhatsApp 為須付費軟體。

微信 WeChat 是由大陸的騰訊網所創的通訊軟體，雖然在 2011 年才推出，但只花了 433 天就讓用戶數達到 1 億，目前，微信用戶已經超過 3 億，是中國手機上網人數的一半。WeChat 的功能在所有通訊軟體中堪稱最齊全，除了 WhatsApp 的基本功能，還具有視訊通話服務，同時也提供即時錄音傳遞，相較於其他手寫輸入更為簡單，貼圖方面則類似傳統電腦中的 MSN，允許用戶自製貼圖。更特別的是 WeChat 能提供隨機交友，能與在周遭幾百公尺甚至幾十公里內的陌生人聊天，或是不受距離限制跟你同時間搖晃手機的陌生人聊天。

2.2 整合性科技接受模型

隨著資訊科技的發展，在眾多理論中選擇模型與構面，或選擇一個優勢的模型時，常會忽視其他模式的貢獻，並常令研究者面臨選擇科技接受模型之困難，因此，需要對過去研究使用者接受模式加以回顧與整合，Venkatesh 等人[11]發展出一整合性科技接受模型(Unified Theory of Acceptance and Use of Technology, UTAUT)，以幫助在資訊科技領域中未來之研究。

整合性科技接受模型[11]對使用行為的解釋能力高達 70%，比先前的各種模型更具解釋力，使用者接受模式基本概念圖如圖 1，當使用者在面對新的資訊科技時，個人的反應會影響使用資訊科技意願，而是否實際使用會受到行為意向的影響，其架構圖如圖 1：

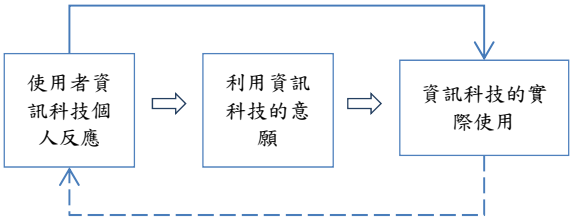


圖 1　使用者接受模式基礎概念圖

資料來源：[11]

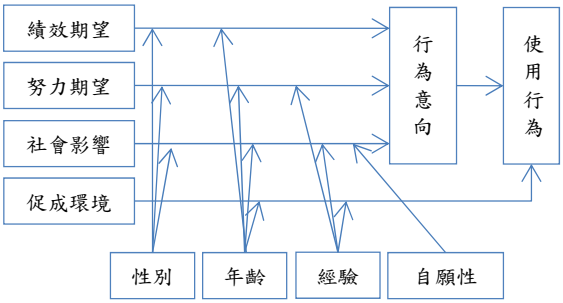


圖 2　整合性科技接受模型

資料來源：[11]

Venkatesh 等人[11]在整合性科技接受模型(UTAUT)，將經驗證過的八個理論、三十二個構面，進行比較性的實證研究，最後整合成四個構面，分別為：績效期望(Performance Expectancy, PE)、努力期望(Effort Expectancy, EE)、社會影響(Social Influence, SI)、促成環境(Facilitating Conditions, FC)；其中績效期望(Performance Expectancy, PE)、努力期望(Effort Expectancy, EE)與社會影響(Social Influence, SI)，3 個構面為使用者的行為意向因素而促成環境(Facilitating Conditions, FC)與行為意向(Behavioral Intention, BI)是直接對使用者產生實際使用的影響。四個構面又受四個控制變數影響，分別為：性別(Gender)、年齡(Age)、經驗(Experience)、自願性(Voluntariness of Use)。以下將以 Venkatesh 等人[11]之整合型科技接受模型的四個主構面，四個控制變數含意分別敘述：

一、績效期望(Performance Expectancy, PE)

績效期望是指「使用者認為使用新系統、新科技將會幫助他獲得工作績效程度，並影響其接受使用度，而有較高的行為意象(BI)」，其中包含五個子構面：

(1)認知有用性：源自 TAM[4]/C-TAM-TPB[8]。

(2)外在動機：源自 MM[5]。

(3)工作相關：源自 MPCU[9]。

(4)相對優勢：源自 IDT[7]。

(5)對成果的預期：源自 SCT[3]。

「績效期望」是指使用系統後可獲得顯著的獎勵回饋。在該研究中發現，單獨考慮性別此變數時，男性比女性顯著，若以年齡與性別同時考慮，則積極追求績效的年輕男性較為顯著。

二、努力期望(Effort Expectancy, EE)

努力期望是指「使用者認為使用系統的容易程度」其中包含三個子構面：

(1)認知易用性：源自 TAM[4]/C-TAM-TPB[8]。

(2)系統複雜度：源自 MPCU[9]。

(3)操作簡單性：源自 IDT[7]。

Venkatesh 等人[11]在該研究發現，「努力期望」會因性別、年齡不同有所差異，尤其以女性且年長者影響較為顯著，但隨著使用經驗的增加而減少。

三、社會影響(Social Influence, SI)

社會影響是指「個人對於新科技的接受與使用，會受到他人影響」，屬於外來的影響，其中可分為三個子構面：

(1)主觀規範：源自 TPB[1]/C-TAM-TPB[8]。

(2)社會因素：源自 MPCU[9]。

(3)公眾形象：源自 IDT[7]。

「社會影響」會受到性別、年齡、經驗與自願性等變數影響，社會影響會因為使用者的使用經驗的增長而降低。

四、促成環境(Facilitating Conditions, FC)

促成環境是指「個人相信現有組織與技術結構都會支持資訊系統的使用」又可分為三個子構面：

(1)認知行為控制：源自 TPB[1]/C-TAM-TPB[8]。

(2)促進條件：源自 MPCU[9]。

(3)相容性：源自 IDT[7]。

「促成環境」會因為年齡與經驗的不同而有差異。

五、控制變數(Moderators)

在整合性科技接受度模型中，除了績效期望、努力期望、社會影響、促成環境四個主構面，還有四項控制變數，分別為：性別、年齡、經驗、自願性。

過去的研究，在性別方面指出不同的構面對行為意圖(BI)的影響與性別有關。如，在績效期望(PE)行為意圖(BI)的影響方面，由於女性比男性在乎他人的看法因此，女性比男性要來的顯著，另一方面，社會影響(SI)也因相同的因素呈現顯著的情況[4]。

Venkatesh 等人 [11]認為整合性科技接受模式目的在於提供管理者的一種使用工具。可供組織再導入新科技前的一種衡量評估方式，並能夠提供預測與解釋使用者接受資訊科技的行為，以供管理者進行修正與評估。本研究利用整合性科技接受模式的四個構面，來探討手機的使用者對於接受與使用即時通訊軟體的動機，並結合其四個外在控制變數來探討使用者個人接受與使用手機即時通訊軟體的模式；依據以上關於整合性科技接受模式，整理於表 1 表示之。

表 1 整合性科技接受模式定義與理論來源

主構面	子構面	理論來源
績效期望	認知有用性	TAM/ TAM2/ C-TAM-TPB
	外在動機	MM
	工作相關	MPCU
	相對優勢	IDT
	對成果的預期	SCT
努力期望	認知易用性	TAM/TAM2
	系統複雜度	MPCU
	操作簡單性	IDT
社會影響	主觀規範	TRA/TAM2 /TPB/DPTB/ C-TAM-TPB
	社會因素	MPCU
	公眾形象	IDT
促成環境	認知行為控制	TPB/DTPB/ C-TAM-TPB
	促進條件	MPCU
	相容性	IDT

資料來源: 研究者整理自 Venkatesh 等人 [11]

3. 研究方法

3.1 研究架構

本研究以整合性科技接受模型(UTAUT)為基礎，經由上述的文獻探討，並衡量本研究之目的，針對智慧型手機即時通訊軟體使用進行研究。研究主架構如圖 3。

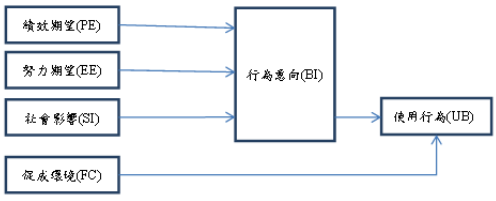


圖 3 研究架構

3.2 研究流程

本研究之研究流程首先從研究動機，開始做一系列的資料蒐集與整理，整理後研讀並確認研究目的與問題後，針對研究問題之相關文獻做一深度探討。在相關文獻回顧與探討後，再由研究架構中設計問卷。

於問卷設計完成後，先行前測，再依前測結果調整問卷，再施行後測。於問卷回收後，進行資料

的分析與歸納，完成後產生結論與建議。

3.3 研究工具

本研究以網路問卷調查方式進行資料的蒐集以驗證本研究之架構模型。量表設計參酌， [12、13、15、16、17、18、19、21]等人之相關研究。問項基礎，主要以 [11]的整合性科技接受模式(UTAUT)，為達有效程度，將配合研究主題修改部分用詞。

根據本研究之研究架構，將問卷分為三部分：第一部分為個人基本資料、第二部分為使用者經歷、第三部分為智慧型手機通訊軟體實際使用經驗。

4. 資料分析

4.1 敘述性統計

本研究根據研究所需，統計曾經使用過之智慧型手機通訊軟體總共 533 人。如表 2。

表 2 實際使用情況

	LINE	Skype	WhatsApp	WeChat
曾經使用人數	490	348	180	135
百分比	91.9%	65.3%	33.8%	25.3%

N=533

由資料分析結果可知曾經使用過百分比最高為 LINE 的 91.9%，最低為 WeChat 的 25.3%。

4.2 LINE 族群路徑分析

透過迴歸分析，可得相關參數，茲整理如表 3。

表 3 LINE 之迴歸分析摘要表

自變項	顯著考驗 *t* 值	標準化迴歸係數(Bata)	依變項
績效期望(PE)	8.898	.349***	行為意向(BI)
努力期望(EE)	9.120	.330***	
促成環境(FC)	5.266	.210***	
促成環境(FC)	1.948	.088	使用行為(UB)
行為意向(BI)	5.293	.233***	使用行為(UB)
績效期望(PE)	3.084	.168**	使用行為(UB)
努力期望(EE)	-.240	-.012	
社會影響(SI)	1.851	.103	

N=490，***p<.001；**p<.01；*p<.05

透過表 3 可得，績效期望對使用行為之路徑係數 β 值為.168**(P<.01)，績效期望透過行為意向在影響使用行為之路徑係數為.081(.349*.233=.081 余民寧[8])，故績效期望與使用行為間之行為意向無中介效果，亦即績效期望直接影響使用行為。努力期望對使用行為之路徑係數 β 值為-.012，努力期望透過行為意向在影響使用行為之路徑係數為.076(.330*.233=.076)，故努力期望須透過行為意向間接影響使用行為。社會影響對使用行為之路徑係數 β 值為.103，社會影響透過行為意向再影響使用行為之路徑係數為.048(.210*.233=.048)，故社會期望須透過行為意向間接影響使用行為。

綜合上述，將模型重製如圖 4。

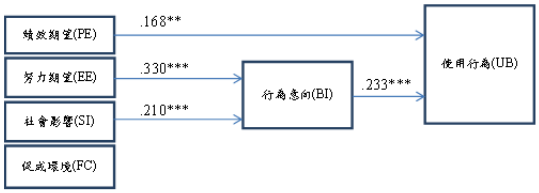


圖 4 LINE 族群之路徑分析

由資料分析觀察，在不考慮控制變數下：

當使用者認為，使用 LINE 有助於通訊相關活動、加強人際關係、與朋友關係更良好，就會增加使用 LINE 頻率，績效期望則直接影響使用行為。無中介效果；當使用者會因為 LINE 操作簡易、使用上不需花太多時間，將會持續使用 LINE，進而增加使用頻率。達中介效果；當使用者的親朋好友推薦或鼓勵使用 LINE，使用者將會持續使用 LINE，使用者進而增加使用 LINE 的頻率。達中介效果；在 LINE 使用者中促成環境對使用行為未達顯著影響效果。

4.3 Skype 族群路徑分析

透過迴歸分析，可得相關參數，茲整理如表 4。

表 4 Skype 之迴歸分析摘要表

自變項	顯著考驗 t 值	標準化迴歸係數(Bata)	依變項
績效期望(PE)	5.515	.278***	行為意向(BI)
努力期望(EE)	6.079	.280***	
社會影響(SI)	5.389	.269***	
促成環境(FC)	-.445	-.024	使用行為(UB)
行為意向(BI)	.705	.038	使用行為(UB)
績效期望(PE)	-.116	-.008	使用行為(UB)
努力期望(EE)	.085	.005	
社會影響(SI)	.948	.063	

N=348，***p<.001；**p<.01；*p<.05

透過表 4 可得，績效期望對使用行為之路徑係

數β值為-.008，績效期望透過行為意向在影響使用行為之路徑係數為.010(.278*.038=.010)，故績效期望須透過行為意向間接影響使用行為。努力期望對使用行為之路徑係數β值為.005，努力期望透過行為意向在影響使用行為之路徑係數為.010(.280*.038=.010)，故努力期望須透過行為意向間接影響使用行為。社會影響對使用行為之路徑係數β值為.063，社會影響透過行為意向再影響使用行為之路徑係數為.010(.269*.038=.010)，故社會期望須透過行為意向間接影響使用行為。

綜合上述，將模型重製如圖 5。

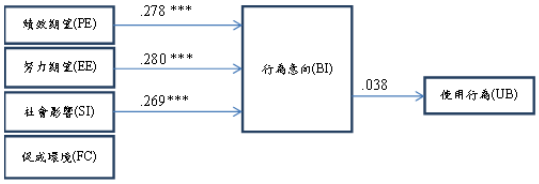


圖 5 Skype 族群之路徑分析

由資料分析觀察，在不考慮控制變數下：

當使用者認為，使用 Skype 有助於通訊相關活動、加強人際關係、與朋友關係更良好，將會持續使用 Skype，進而增加使用頻率。達中介效果；當使用者會因為 Skype 操作簡易、使用上不需花太多時間，將會持續使用 Skype，進而增加使用頻率。達中介效果；當使用者的親朋好友推薦或鼓勵使用 Skype，使用者將會持續使用 Skype，使用者進而增加使用 Skype 的頻率。達中介效果；在 Skype 使用者中促成環境對使用行為未達顯著影響效果。

4.4 WhatsApp 族群路徑分析

透過迴歸分析，可得相關參數，茲整理如表 5。

表 5 WhatsApp 之迴歸分析摘要表

自變項	顯著考驗 t 值	標準化迴歸係數(Bata)	依變項
績效期望(PE)	5.627	.404***	行為意向(BI)
努力期望(EE)	1.894	.116	
社會影響(SI)	4.517	.318***	
促成環境(FC)	1.963	.146	使用行為(UB)
行為意向(BI)	2.954	.217**	使用行為(UB)
績效期望(PE)	-.481	-.048	使用行為(UB)
努力期望(EE)	1.417	.122	
社會影響(SI)	2.214	.218	

N=180，***p<.001；**p<.01；*p<.05

透過表 5 可得，績效期望對使用行為之路徑係數β值為-.048，績效期望透過行為意向在影響使用行為之路徑係數為.087(.404*.217=.087)，故績效期望須透過行為意向間接影響使用行為。努力期望對使用行為之路徑係數β值為.122，努力期望透過行為意向在影響使用行為之路徑係數為.025(.116*.217=.025)，故努力期望與使用行為之間之行為意向無中介效果，亦即努力期望直接影響使用行為。社會影響對使用行為之路徑係數β值為.218*(P<.05)，社會影響透過行為意向在影響使用行為之路徑係數為.069(.318*.217=.069)，故社會影響與使用行為間之行為意向無中介效果，亦即社會影響直接影響使用行為。

綜合上述，將模型重製如圖 6。

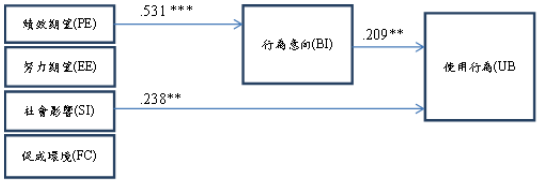


圖 6 WhatsApp 族群之路徑分析

由資料分析觀察，在不考慮控制變數下：

當使用者認為，使用 WhatsApp 有助於通訊相關活動、加強人際關係、與朋友關係更良好，將會持續使用 WhatsApp，進而增加使用頻率。達中介效果；在 WhatsApp 使用者中努力期望對行為意向與使用行為皆未達顯著影響效果；當使用者的親朋好友推薦或鼓勵使用手機通訊軟體，會增加使用者使用手機通訊軟體頻率。無中介效果；在 WhatsApp 使用者中促成環境對使用行為未達顯著影響效果。

4.5 WeChat 族群路徑分析

透過迴歸分析，可得相關參數，茲整理如表 6。

表 6 WeChat 之迴歸分析摘要表

自變項	顯著考驗 t 值	標準化迴歸係數(Bata)	依變項
績效期望(PE)	6.136	.531***	行為意向(BI)
努力期望(EE)	.294	.021	
社會影響(SI)	3.038	.238***	
促成環境(FC)	.737	.064	使用行為(UB)
行為意向(BI)	2.478	.209*	使用行為(UB)
績效期望	.927	.109	使用行為

(PE)			(UB)
努力期望(EE)	.620	.061	
社會影響(SI)	1.808	.193	

N=135，***p<.001；**p<.01；*p<.05

透過表 6 可得，績效期望對使用行為之路徑係數β值為.109，績效期望透過行為意向在影響使用行為之路徑係數為.110(.531*.209=.110)，故績效期望須透過行為意向間接影響使用行為。努力期望對使用行為之路徑係數β值為.061，努力期望透過行為意向再影響使用行為之路徑係數為.004(.021*.209=.004)，故努力期望與使用行為間之行為意向無中介效果，亦即努力期望直接影響使用行為。社會影響對使用行為之路徑係數β值為.193，社會影響透過行為意向再影響使用行為之路徑係數為.049(.238*.209=.049)，故社會期望須透過行為意向間接影響使用行為。

綜合上述，將模型重製如圖 7。

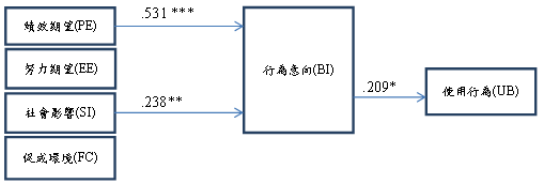


圖 7 WeChat 族群之路徑分析

由資料分析觀察，在不考慮控制變數下：

當使用者認為，使用 WeChat 有助於通訊相關活動、加強人際關係、與朋友關係更良好，將會持續使用 WeChat，進而增加使用頻率。達中介效果；在 WeChat 使用者中努力期望對行為意向與使用行為皆未達顯著影響效果；當使用者的親朋好友推薦或鼓勵使用 WeChat，使用者將會持續使用 WeChat，使用者進而增加使用 WeChat 的頻率。達中介效果；在 WeChat 使用者中促成環境對使用行為未達顯著影響效果。

5. 結論與建議

本研究目的在於探討智慧型手機通訊軟體使用意向與實際使用行為。研究發現四個手機通訊軟體，在使用者沒有任何使用經驗，或沒有人指導情況下使用者皆會使用這四個手機通訊軟體；

由資料分析結果可知曾經使用過 LINE 達 91.9%為最多，其次為 Skype 的 65.3%，WhatsApp 的 33.8%，而 WeChat 僅 25.3%為最低，其原因透過分析得知 LINE 使用者認為使用軟體可加強人際關係、對通訊相關活動有幫助、操作簡易、容易上手，且使用者普遍認為使用 LINE 的經驗是愉快的。同時也發現 LINE 操作比其他軟體更容易；相較之下，WeChat 使用者較少，原因是使用者認為軟體操作不盡理想、功能太過複雜，另一原因可能是 WeChat 提供隨機交友，未能過濾陌生人，進而減少使用者使用意願。使用者對 Skype 持續使用未達顯著，未來使用意願也較弱；WhatsApp 帶給使用的便利性較弱，使用意願相對較低。

參考文獻

[1] Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckman (Eds.), Action-control: From cognition to behavior (pp. 11- 39). Heidelberg, Germany: Springer.

[2] APP01(2012)。熱門通訊APP大調查。http://www.app01.com.tw/。

[3] Bandura, A., (1986), “Social Foundations of thought and Action: A Social Cognitive theory”, Prentice Hall, Englewood Cliffs,NJ.

[4] Davis, F. D., (1989), “Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology”, MIS Quarterly, 13, pp. 319-340, September.

[5] Davis, F.D., Bagozzi, R.P., Warshaw, P.R., (1992). Extrinsic and intrinsic motivation to use computers in the workplace. Journal of Applied Social Psychology 22, 1111–1132.

[6] Fishbein, M., and Ajzen, i. (1975), “Belief, Attitude, Intention and Behavior: An Introduction of Theory and Research”, Addison-Wesley, Reading, MA.

[7] Rogers, E. M. (1983). Diffusion of innovation (3rd ed). New York: The Free Press.

[8] Taylor, S. and Todd, P. A. (1995), “Understanding information technology usage: a test of competing models”, Information Systems Research, 6:2, pp.144-176.

[9] Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal computing: Toward a conceptual model of utilization. MIS Quarterly, 15(1), 124-143.

[10] Venkatesh, V. & M.G. Morris. (2000). Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behavior. MIS Quarterly, 24(1), 115-139.

[11] Venkatesh, Viswanath, Morris, Michael G., Davis, Gordon B., & Davis, Fred D. (2003). USER ACCEPTANCE OF INFORMATION TECHNOLOGY: TOWARD A UNIFIED VIEW. MIS Quarterly, 27(3).

[12] 王占魁（2009）。智慧型手機網路使用意願及相關因素探討，樹德科技大學資訊管理學系碩士論文。

[13] 王政欽（2007）。網際網路使用者對網路電話接受度之研究。國立中山大學，企業管理學系碩士論文.

[14] 余民寧(2006)。潛在變項模式：SIMPLIS 的應用。臺北市：高等教育。

[15] 林秀芬、趙時樑與王誠煦（2011）。即時通訊軟體使用意願影響因素之研究-以海運承攬業為例。 Electronic Commerce Studies, 9(1), 35-60.

[16] 邱美如(2011)。研發人員使用專利分析軟體之關鍵影響因素－以工研院為例。屏東科技大學科技管理研究所碩士論文。

[17] 張月美（2008）。消費者採用網路銀行之相關因素探討。國立東華大學企業管理學系碩士論文。

[18] 張宗榮(2012)。以整合性科技接受模式及沉浸理論探討 App 之使用行為模式 - 以行動社群 App 為例。國立臺中教育大學數位內容科技學系碩士論文。

[19] 莊庭安(2012)。大學生使用行動網路服務之探討： 整合性科技接受模型觀點。高雄師範大學人力與知識管理研究所碩士論文。

[20] 蔡燕平(2004)。組織採用即時通訊軟體與組織溝通之研究。銘傳傳播學資訊管理所碩士論文。

[21] 謝松豪（2008）。網站可用性對旅遊網站使用者接受度之影響。義守大學資訊管理學系碩士班碩士論文。

以 Facebook 為基礎之社群服務系統

王民翰　　張焜翔　　江清泉
銘傳大學資訊傳播工程學系
ccchiang@mail.mcu.edu.tw

摘要

近年來高速網路以及網路社群快速興起，社群網站的使用已經變成了人與人之間交換資訊的重要管道之一，改變了以往使用者使用網路的習慣，使得人們更喜歡、更仰賴社群網路的需求。各種網頁技術的推出例如 PHP5、CSS3、jQuery、Ajax 等技術，皆強化了使用者透過瀏覽器使用社群的感受及線上服務的即時性。其中，更以 Facebook 崛起速度為之最，使用 Facebook 已經變成了大部分人每天的習慣，因為如此，Facebook 的使用人數非常多，高使用率以及可觀的使用人數，背後隱藏的資源是無可限量的。本研究提出一套以 Facebook 網站為基礎的服務系統，系統會以網頁呈現提供服務，使用者僅需藉由可上網的設備，如智慧型手機、平板、筆記型電腦、個人主機等開啟瀏覽器連上系統即可使用。任何在系統上所操作的動作產生的資訊、資料都會儲存在資料庫，系統建立了網路機器人，藉著網路機器人以及社群網站提供的 API[10]，能強化其社群網站的功能並減少操作需要大量且頻繁的動作來達到減少使用者重複性的操作。

關鍵詞：社群運算，網頁爬網，網路機器人。

Abstract

Internet has being connecting the computers around the world and network services provide a platform for transferring information. Web applications become the most popular network services. Social web sites such as Facebook have been growing rapidly and dominate the web services over the last few years, thus developing the social network. It will be very useful to explore the power of social web sites including members and interacted data. Network robot programs are designed to automatically browse the web sites as human beings. In this paper we develop an automatic social service by using API and crawl programming skills. The robot programs are designed to be able to automatically login the Facebook and then perform the work by exploring the social members and exchanged information, and thus achieve the goal of social computing. The major services are message announcing, Q&A, and Searching. Message announcing service uses robot programs to post important message on the Facebook to deliver the information to users. Q&A service applies robot programs to spread the questions to online users of the social network and instantly get the answers back from members. Searching service runs robot programs to extract and filter information from Facebook. Mobile apps and web pages are developed in this project to provide users with friendly and feasible interfaces to access the in social services. The power and benefit of social services are present in this research to accomplish the goal of the social computing.

Keywords: Social computing, Web crawling, robot program.

1. 前言

在目前電腦的時代因有了高速網路與瀏覽器的結合應用，使得人們更喜歡、更仰賴網路的需求。起初眾多網路服務提供者以各式各樣的網頁服務資源，供大眾瀏覽使用；一開始技術尚未成熟互動性也欠佳，所能呈現的資料樣式也受侷限。漸漸的許多瀏覽器的推出(如 IE、Chrome、Firefox)以及網頁技術的提升(如 PHP5、CSS3、jQuery、Ajax)，在這些技術下所繁衍出的相關應用，種類甚多，如網路硬碟(Dropbox、Google Drive)、網路相簿(無名小站、Flickr)、視訊影音(YouTube)、購物(Yahoo 購物、拍賣)、社群網站(Facebook、Twitter)、線上掃毒(F-Secure Online Virus Scanner)等；而也因網路上有許多人在使用社群資源，在線上供眾人相互分享，衍生出多樣化的資源。

根據 comScore Media Metrix 報告，台灣 2013 年 4 月不重複使用網友人數為 1,187 萬位，平均每位使用者當月份上網 1,411 分鐘或 23.5 小時、瀏覽 2,416 個網頁，其中網域主排名第三名為 Facebook，共有 927.4 萬位使用者，為 78.1%到達率，平均每位使用者在此花費 379 分鐘、瀏覽 544 個網頁，每位使用者花費時間為全台最長[11]。

社群網站種類繁多，其中以社交類的 Facebook 為全台使用之冠，因而藉此簡化其功能並強化，加入許多設定，減少部分操作的頻繁動作，來達到減少使用者重複操作。

2. 相關技術與研究

本章節說明與本研究相關的文獻跟建置整合服務系統所使用到的技術以及相關功能探討。

2.1 社群網站種類介紹

由於社群網站種類及服務甚多，因此我們先將對目前網路上所存在的社群網站系統做個簡單的分類，以下我們將其大致上分為五類：檔案類型、

論壇類型、文章類型、影音類型、複合式類型。

檔案類型：檔案類型的社群網站會提供使用者免費空間，可以讓檔案上傳、下載以及分享，而通常這類型的網站的收入都以打廣告為主。目前知名的 Dropbox[12]，它透過雲端儲存實現網際網路上的檔案同步，使用者可以儲存並共享檔案和資料夾，免費的 Dropbox 戶口只有 2GB 容量。

論壇類型：論壇型的社群網站主要是以討論特定主題為重點，其分類方式根據不同的討論性質而進行分門別類而著名的社群網站，PTT[13]論壇是以主題看板來分類，由網友在每個分類看板內，自發性的發表主圖文章與其他人分享。

文章類型：文章類型的社群又可以稱為部落格、網誌，它是一種由個人管理、不定期張貼新的文章、圖片、影片的網頁或線上日記，用來抒發情感或分享資訊，部落格上的文章通常根據張貼時間以倒序方式由新到舊排列，一個典型的部落格結合了文字、影像、其他部落格或網站的超連結、及其它與主題相關的媒體。能夠讓讀者以互動的方式留下意見，是許多部落格的重要要素。

影音類型：隨著影音網站 YouTube[14] 在網路上的盛行，帶起一種另類的影音社群，YouTube 是設立在美國的一個影片分享網站，讓使用者上載、觀看及分享影片或短片，它創辦原意是為了方便朋友之間分享錄影片段，後來逐漸成為網友的回憶儲存庫和作品發佈場所。

複合式類型複合式類型在近幾年推出，使得傳統社交模式在短時間逐漸的改變，如 Facebook[15]、Twitter[16]、Plurk[17]等，就是綜合以上五種類型的社群網站，因整合的服務多元化，且大部分所提供的服務都是免費的，這讓許多使用者紛紛投向複合式類型社群網站的懷抱，也因為如此，複合式類型的社群網站。

2.2 Facebook API

Facebook 官方提供給開發者使用的套件，透過 API 能間接得到使用者的一些基本資訊，並且能加以使用。Facebook API 可以應用在多種的環境下，包括網站(Web)、行動應用程式(Mobile Apps)。根據不同的平台也提供了不同的 SDK[18]給開發者使用。透過這些 API 能更快速運用使用者資料，配合這些資料，來達到快速整合之服務。

2.3 網路機器人相關文獻探討(爬網技術)

現 Matthew Hurst 等兩位學者[3]指出，利用社交媒體內容的應用程式必須為是有效的有權訪問此資料的最小發佈採集的延遲時間，而有效的部落格爬網方式應滿足以下要求：低延遲、高可擴充性、較高的資料品質和適當的網路禮貌。

Guo Guohong 等兩位學者[4]提出架構基於 Web 的視頻信息採集的網絡爬蟲，也被稱為“網路蜘蛛”，網路蜘蛛(Web spider)也叫網路機器人，指的是「自動瀏覽網路」的程式。這樣的電腦程式是為了自動從網路擷取特定的資料，或為了組織網路上的資料，所設計的『自動瀏覽網路』的程式。

綜合所探討的相關文獻，社群的應用及型態相當的多元化，主要還是以用戶與用戶之間的互動和線上提供服務的多元性較具吸引人，而整合多元化的社群服務、資源以及技術將是本研究的重點，因此將上述之文獻做為參考。

利用網路機器人，能整合 Facebook 的基本功能，並強化原有設計，還能自己增加原先 Facebook 沒有的功能，來達到整合服務之目的。

3. 系統設計

本章節將詳細介紹本系統架構系統建置方法與整體實驗環境及利用 PHP 程式語言建構出系統核心和系統的網頁介面撰寫，最後說明網路機器人的內部運作。

3.1 系統架構

本系統架構如圖 1 所示，以下將針對圖 1 的部分進行詳細的介紹。

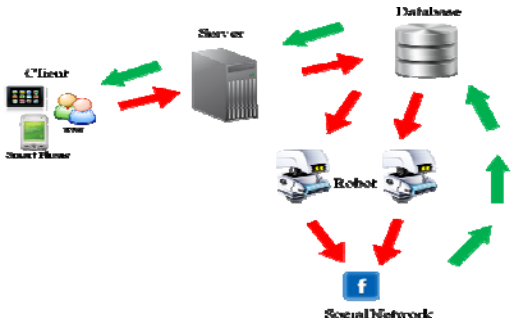


圖 1 系統架構示意圖

1. User：使用者介面，是使用者接觸系統的第一個通道。透過智慧型手機、平板電腦、網頁等連結到系統。使用者能透過使用者介面清楚了解系統提供的功能以及服務，是系統以及使用者相互連結的平台。
2. Database：資料庫，以儲存資料為主。由於系統需要運用到大量的資料存取的動作，於是資料庫的運用變成了系統架構的一個重點，使用者會透過使用者介面存取資料庫的資料，網頁伺服器的資料也會透過資料庫呈現，是系統架構重要的一個環節。
3. Server：網站伺服器，是使用者透過使用者介面直接連結的一個平台，能透過智慧型手機或者網頁直接連結。伺服器主要提供使用者系統功能的操作以及改變，伺服器會透過資料庫存取資料並呈現給使用者。網站伺服器也是我們管理系統的工具，一方面提供功能給使用者使用，一方面也方便我們更改系統上的設定以及所有資料流向。
4. Robot：網路機器人程式以 PHP 來撰寫，是系統工作的核心。主要功能是收取資料並分析後傳送至社群網站。由網站伺服器收到訊息後，並依照分

類分別向資料庫存取資料，除了收集及固定資料外也會進行散佈來源的動作，還能讓使用者的好友能透過使用者使用系統並連結到網站伺服器，進一步提高網站的使用率。

5. Social Network：泛指各大社群網站或者提供資源的網站，也是系統索取資料以及散佈資料的地方，系統能透過網站伺服器以及機器人的雙向配合連結至許多資源的社群網站，並利用社群網站上的功能以及資料，使系統更有效率，這邊以 Facebook 作為代表。

3.2 系統流程

此節詳細說明系統的運作流程，如圖 3，介紹各流程的內容與目的。

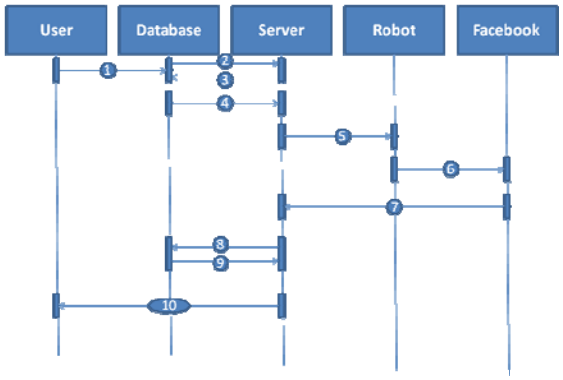


圖 2 系統流程圖

（一） 由使用者介面輸入資料傳至資料庫，並記錄使用者資訊（如圖 2 流程 1）。

（二） 資料庫將資訊送往網站伺服器，並提供資料給網站伺服器（如圖 2 流程 2）。

（三） 確定是否為第一次進入系統，並開放認證，並將認證資料存回資料庫（如圖 2 流程 3）。

（四） 確認無誤的資料將會傳回網站伺服器，並依照認證的資料顯示在網站伺服器中（如圖 2 流程 4）。

（五） 使用者透過網站伺服器將資料紀錄至資料庫，並由網站伺服器發送指令給機器人（如圖 2 流程 5）。

（六） 機器人接收到指令後會依照指令去執行工作，並將並將工作內容傳送至社群網站（如圖 2 流程 6）。

（七） 機器人直行指令過程中，也會附上基本資訊回傳給伺服器，讓使用者可以得知目前狀態以及運作狀態（如圖 2 流程 7）。

（八） 使用者看見指令執行成功後，會先將第一手資料存入資料庫，再由伺服器做存取，並顯示給使用者（如圖 2 流程 8、流程 9、流程 10）。

3.3 系統功能簡介

系統功能涵蓋的範圍廣泛，除了可以使用一般提供給使用者使用的功能外，還能控制以及操作系統，如圖 3，可以清楚得知網頁所規劃的功能以及項目：

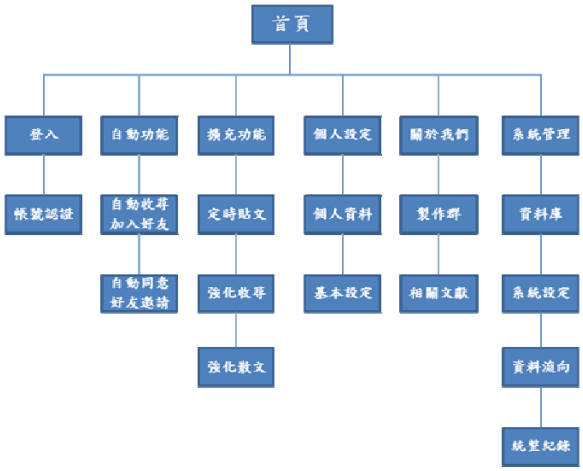


圖 3 系統功能圖

主要功能如下：

1. 首頁：以登入為第一步驟，登入後取得 Facebook 認證後即可使用系統功能。

2. 自動功能：自動功能這邊提供兩種服務，第一種是自動收尋好友並加入，這功能會收尋建議好友並自動加入，系統會設定時間自動加好友；另一種是同意好友邀請，只要有人加好友，就自動同意。

3. 擴充功能：擴充功能提供三種服務，包含定時貼文、強化收尋以及強化散文，定時貼文顧名思義就是依照使用者設定的時間貼文，強化收尋的功能，是用在 Facebook 的收尋功能，系統背後會有好幾個網路機器人控制某些帳號，而且會自動同意並加好友，運用此過程來達到廣大的人脈，並將收尋功能串在人脈上面，利用廣大人脈來收尋；而最後的強化散文，也是利用系統背後的機器人，將使用者張貼的文章透過系統機器人背後的好友去散佈資訊，好友越多，散播的資訊就越廣，越能達到散佈資訊的效能。

4. 個人設定：一些基本的資料顯示以及帳號權限的設定。

5. 關於我們：一些關於研究的基本資料以及相關文獻。

6. 系統管理：管理者登入使用，可以管理機器人，並設定系統相關設定。

3.4 伺服器與網路機器人的建置

本節最主要是介紹伺服器與網路機器人的建置方法。

3.4.1 伺服器建置

系統是以網頁方式呈現，因此需要架設網頁伺服器提供所有的服務運作。網頁伺服器主要扮演角色是位於使用者與機器人之間的橋樑，它負責將使用者所操作的指令傳達給機器人，並記錄使用者操作資訊。網頁伺服器主要以 Linux Fedora10 系統建置，網頁功能使用 Apache HTTP Server，Apache HTTP Server（簡稱 Apache）是 Apache 軟體基金會

的一個開放原始碼的網頁伺服器，可以在大多數電腦作業系統中執行，由於其跨平台和安全性被廣泛使用，是最流行的 Web 伺服器端軟體之一。它快速、可靠並且可通過簡單的 API 擴充。

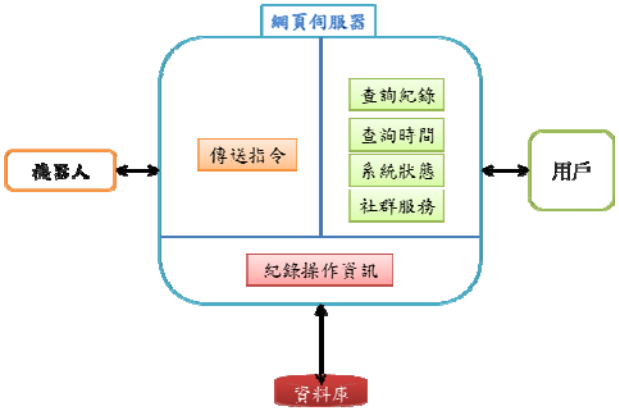


圖 4　SERVER 端內部結構

如圖 4 ，網頁系統與網路機器人位於 Server 端也是本系統最重要的部分，它負責使用者與機器人之間的溝通以及任務的分配，Server 端內部網頁系統由 PHP 程式語言建置，同時也包含了 PostgreSQL 資料庫儲存資料，將使用者每次操作的動作及資訊存至資料庫，可供日後查詢使用。

3.4.2 建立網路機器人



圖 5　瀏覽器 vs 網路機器人上網動作

如圖 5 ，一般上網模式以瀏覽器來說，由於瀏覽器所提供的功能相當豐富，且許多上網的細部動作也以自動化，所以使用者只須操作滑鼠點擊超連結即可達到上網的動作。網路機器人是由人為建構的程式語言，內部的程式撰寫，須由設計者是先建立腳本，讓網路機器人可以依續執行。當機器人腳本建立後，只需等待接收由伺服器傳送的指令，將結果回傳即可。

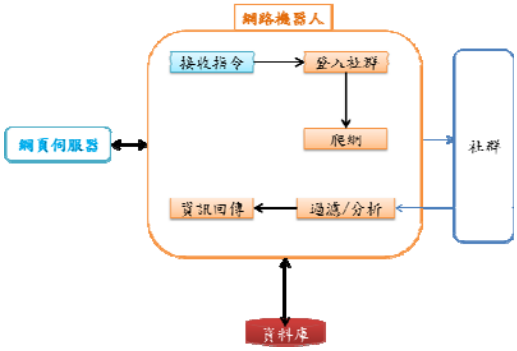


圖 6　網路機器人流程圖

如圖 6 ，為了能夠把目標網站的內容截取回來並呈現給用戶端，因此使用 PHP 程式語言加上 cURL[19]函式庫設計核心服務如下圖 7 ，網路機器人需要完成接收到從 Server 端傳送的 PHP 指令，會依照指令類型的不同驅使網路機器人達成不同的功能，如自動加好友、自動訊息發布如下圖 8、強化搜索；網路機器人開始執行後，會先登入社群網站系統，確認登入後進行網頁內容的抓取，過濾網頁內的標籤語言會以 PHP 正規劃表示法過濾文字，會以指令型態的不同選取服務，分析資訊與使用者所詢問的是否相同，最後將資訊回傳，呈現在用戶端的頁面，在每次執行後會紀錄每一筆資訊如使用者相關資訊、時間、操作內容…等，將這些資訊都寫進資料庫。

```
1.  Setp 1 建立瀏覽器表頭資訊
2.  $agent = "Mozilla/5.0 (Windows NT 5.1; rv:5.0).....
3.  $headers[] = "Host: www.facebook.com";
4.  $headers[] = "Accept: image/gif, image/x-bitmap.....
5.
6.  Setp 2 建立Cookie儲存資訊
7.  $cookiefile=getcwd()."/cookies.txt";

8.  Setp 3 建立封包傳送格式
9.  $ch = curl_init();
10.     curl_setopt($ch, CURLOPT_COOKIEJAR, $cookiefile);
11.     curl_setopt($ch, CURLOPT_COOKIE, $cookie);
12.     curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);
13.     curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, 0);
14.     curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);

15.     curl_setopt($ch, CURLOPT_HTTPHEADER, $headers);
16.     curl_setopt($ch, CURLOPT_USERAGENT, $agent);
```

圖 7　Curl 連線資訊



圖 8　網路機器人發文步驟圖

4. 研究成果與實驗分析

本系統是以網站 API 搭配網路機器人為主要工作核心，操作系統則以網頁方式呈現，使用者或系統管理員將透過不同的等級身分登入，由系統依據該身分給予應有的操作權限，系統會統一將使用者尚未登入的狀態通通當成匿名使用者，僅有查詢紀錄、觀看系統狀態而法操作使用任何的功能。

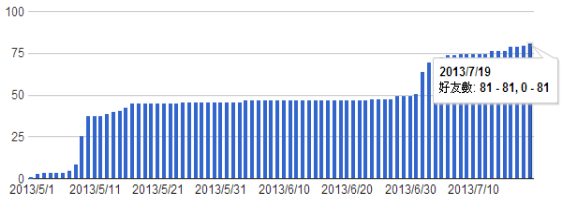
社群技術的服務整合能夠更為完整以達到有效的利用，使功能更為簡潔、快速，主要是統一交付給網路機器人處理，網路機器人是以 PHP 語言撰寫的，將使用者的操作模式以程式的型態逐一編寫成機器人的內部功能，透過 Web Server 給予不同指令來驅動網路機器人，令機器人能夠連結社群網站來達成任務，且依照不同的功能撰寫設計網路機器人。

4.1 強化散文功能落點分布

本系統有提供使用者強化散文的功能，這功能最主要還是比照網路機器人的功能而去做判定，目前規劃出能散佈的點有「使用者塗鴉牆、機器人塗鴉牆、機器人好友塗鴉牆、機器人好友訊息、粉絲專頁」等，網路機器人好友的數量也會牽涉到散出去文章的數量，因此，機器人好友數量越多，能散佈的點也就越多。以使用者的角度而言，對每個好友去發送同樣的訊息會耗盡很多的時間，但是透過強化散文的功能，能讓網路機器人透過你的資訊來幫你傳遞訊息，不僅節省時間，還能讓所有朋友都知道此訊息，藉此達到簡化、省時的作用。

4.2 網路機器人好友資料

如圖 9 ，分別是系統的網路機器人自動加好友的資料狀態，Facebook 針對每個帳號都有給一組類似身分證的 ID 碼，Facebook 的每項指令都是透過這 ID 碼來進行動作，透過網路機器人爬網技術，分別從網頁上截取到推薦好友的 ID 碼，並透過 ID 碼進行快速加入好友來達到增加網路機器人的好友數量，這動作一方面可以藉由系統本身的機器人確認此功能是否正常進行，另一方面系統的機器人也能藉藉機加好友量，好友數量越多，強化收尋以及強化散文的部分就會越強。



(a)　機器人



(b)　機器人

圖 9　器人好友數 (a)機器人、(b)機器人

4.3 平台分布(統計使用者登入之平台資訊)

每一個使用者使用的平台、瀏覽器皆不相同，因此當每個使用者開啟系統頁面時，系統將會透過 PHP 內建函數紀錄使用者的使用平台資訊。圖 10 使用者平台分布，會在網頁系統上呈現出各個使用者常用的平台統計圖，可以方便觀察出，目前受到大家所喜愛及常用的瀏覽器及平台。該圖顯示出目前為 Google Chrome 最為受到歡迎。

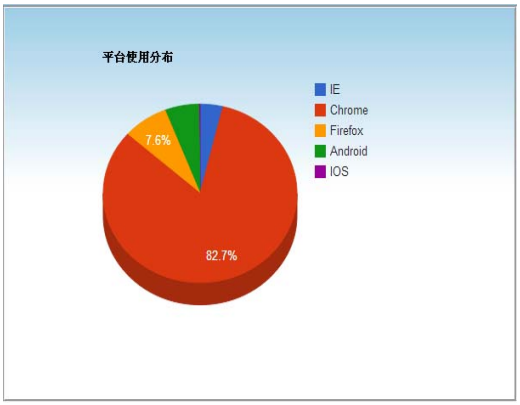


圖 10　使用者平台分布

4.4 系統限制

使用此系統因結合社群網站，需在使用者完全同意提供個人資訊、同意系統社群帳號與使用者加好友及操作內容的蒐集。因此如有任何一樣不同意提供，即無法完整分析及提供服務；系統需配合提供服務的社群結合，因此系統設計與使用者在使用服務的同時，須符合各社群的使用規範，否則容易造成系統操作上的錯誤及影響其他同時在線的使用者。

現行的社群網站，因網站本身有許多的限制存在，如好友邀請，系統會偵測使用者是否惡意的、頻繁的邀請陌生人為好友，進行阻擋及過濾。這對網路機器人相當不利，因此必須針對社群系統的機制去排解可能被阻擋的問題。

社群種類繁多，系統能整合的數量也有限，且每一個網站使用的技術也不大相同，因此在短時間無法一一克服所有技術，僅能呈現出較陽春的社群服務。

4.5 社群網站(Facebook)限制

為了能順利使社群網站上的功能更簡便，除了使用網站提供的 API，接著就是使用網路機器人的概念去實行簡化的步驟，但，在執行的過程中，難免會受到社群網站(Facebook)的限制。例如:「自動加好友」這項功能，這項功能看似便利，後面卻隱藏著網站對其步驟的限制，過度或快速的加好友反而會導致網站偵測異常使用並封鎖其帳號的使用，為了防止封鎖帳號的事情發生，這過程中投入了大量的時間以及人力去測試網站的每個環節，來使被封鎖的機率降到最低，雖然能降低機率不過卻還是存在著風險，因此如何將此風險降到趨近於零，並能達到簡化使用以及強化功能的目的，將是本研究最大的挑戰。

5. 結論

本論文提出一個以網路機器人技術為基礎之社群服務系統，透過本系統提供的系統網頁，即可快速、簡單的將想散佈訊息散佈至社群網站，使用者操作時不需安裝任何軟體，只需使用可上網的裝置如個人 PC、筆記型電腦、智慧型裝置、行動裝置等設備皆可使用。

藉由 HTTPS 的安全性連線，以確保使用者的資訊不易被竊取，透過系統提供的社群整合服務功能，不需頻繁操作，系統內建之機器人將會代勞。為了讓系統方便管理，本系統也提供後端管理介面，方便管理人員能快速維護系統，也可觀察各項服務的流量及機器人狀態。

上網人口不斷增加，線上社群服務也越來越多且多樣化，結合部分人的力量就有不可小看的強大能力，未來系統將可以繼續結合其他社群網站服務以增強系統的可用性，讓這份特別的能力擴及全世界。

參考文獻

[1] Cristian Gadea, Bogdan Solomon, Bogdan Ionescu, Dan Ionescu,“A Collaborative Cloud-Based Multimedia Sharing Platform for Social Networking Environments”, Computer Communications and Net-works (ICCCN), 2011 Proceedings of 20th International Conference, Year: 2011, Page(s): 1- 6

[2] Weider D. Yu, Hongbin Yuan,“An Approach to Explore Mobile Software Engineering Advances in Cloud Computing Environment”, Computer Software and Applications Conference Workshops (COMPSACW), 2011 IEEE 35th Annual, Year: 2011, Page(s): 292 - 297

[3] Matthew Hurst, Alexey Maykov, “Social Streams Blog Crawler”, Data Engineering, 2009. ICDE '09. IEEE 25th International Conference, Year: 2009 , Page(s): 1615-1618

[4] Guo Guohong, Wei Wei, “Video Semantic Information Architecture Based on Web Crawlers”, Internet Technology and Applications (iTAP), 2011 International Conference on Year: 2011, Page(s): 1-4.

[5] osuke Jimbo, Masaki Kohana, Shusuke Okamoto, “A Twitter Service for School Event”, ICNC '11 Proceedings of the 2011 Second International Conference on Networking and Computing Pages 266-270

[6] 陳孟瑋、張創詠，「社群網路的應用-具有可信度的即時訊息蒐集平台」，逢甲大學資訊工程系，專題研究報告，May 2011

[7] Manoj Parameswaran, Andrew B. Whinston”SOCIAL COMPUTING: AN OVERVIEW”, 2007, Santa Clara University, The University of Texas, Austin

[8] 陳宜樫、葉榮椿、游捷閔、吳柏襄（2011）。「影響社群網站黏著度之因果關係模式建構：期望確認理論的觀點」，TANET 2011 台灣學術網路研討會論文集。宜蘭大學。

[9] 黃夙賢、洪子堯、賴正文（2011）。「適用於 Yahoo!奇摩知識+中文問答系統之兩層式分析法」，明新科技大學資訊管理系。

[10] Facebook Developer，「API」，http://developers.facebook.com/

[11] ARO/MMX 公佈 2013 年 4 月 Media Metrix 網路流量報告，http://www.insightxplorer.com/news/news_05_22_13.html

[12] Dropbox ， ttps://www.dropbox.com/

[13] PTT，http://www.ptt.cc/index.html

[14] YouTube ，ttps://www.youtube.com/

[15] Facebook，http://www.facebook.com/

[16] Twitter ，https://twitter.com/

[17] Plurk，http://www.plurk.com/t/Taiwan

[18] SDK，http://developer.android.com/sdk/index.html

[19] cURL http://php.net/manual/en/book.curl.php

網路社群之社會支持：以大學生 Facebook 使用者為例

鍾才元　楊政穎　陳明終　劉晏廷
臺北市立大學
tchung@utaipei.edu.tw

摘要

本研究以大學生 Facebook（FB）使用者為對象，探討網路社群之社會支持與使用者性別、年級、及 FB 功能使用頻率之關聯性。資料以紙本問卷及線上問卷二種方式進行收集，共取得有效樣本 578 人；研究工具為 FB 使用調查表與 FB 社會支持量表。主要發現如下：一、大學生自 FB 社群獲得之情緒面社會支持顯著低於訊息或評價面之社會支持；二、男性與女性在訊息、評價、與情緒面之社會支持並無顯著差異；三、較低年級的大學生比大四或延畢生得到較多的情緒面社會支持；四、除遊戲功能外，FB 之熱門功能（如相簿、塗鴉牆、聊天室等）使用頻率高者所獲得之訊息與評價面社會支持亦顯著高於偶爾或從未使用者。研究者針對這些發現在大學之學生輔導與諮商工作方面的意義進行討論，並對未來研究方向提出若干建議。

關鍵詞：社交網站、社會支持、網路社群、網際網路、臉書。

Abstract

The present study investigates the relationship between Facebook (FB) users' social support received from web community and their gender, age, and use of FB functions. A sample of 578 college students participated in the survey, in which they filled out a checklist of FB use and a rating scale of FB social support. Results indicated that college students received significantly less emotional support than informational and evaluative aspects of support, and that male and female students did not differ in the extent of the three aspects of social support. Furthermore, senior students reported receiving significantly less emotional aspect of FB social support than did freshmen, sophomores, and junior students. Finally, students who always or frequently used FB functions (Photo, The Wall, Like, Group, Chat, Note, and Events) reported receiving significantly more social support than did those who occasionally or rarely used these functions. The implications of these findings for counseling with college students are discussed, as well as suggestions for future research.

Keywords: Facebook, Internet, Social Network, Social Support, Web Community.

1.前言

網際網路的世界裡，社交網站（Facebook、Friendster、LinkedIn、MySpace、Yahoo 交友等）的人氣一直高居不下，反映的是當代人透過網際網路尋求與維繫人際關係，並藉此滿足其人際需求的現象。社交網站中，以 Mark Zuckerberg 所成立的 Facebook（以下簡稱 FB）最負盛名，全球活躍用戶數已超過 1,110,000,000 人[1]。FB 在台灣也是註冊人數最多的社交網站，估計有 1320 萬使用者，位居亞洲第七；若以人口比例來看，則以 56.7%奪下亞洲第一名[2]。FB 用戶可以邀請他人成為自己的好友，也會被他人邀請為好友，每一個使用者都是 FB 世界中一個或多個社交網絡的一個成員。FB 的眾多特色之一為，用戶的好友幾乎都是個人所認識且自願加入的。

「社會支持」（social support）是實體社群極為重要的互動機制，意指個人得自於社群中其他成員的精神、知識、或物質上的援助或支持。由於擁有社會支持，個人在面對壓力與困難時，不致於感到孤立或無助；社群成員彼此的支持，也間接地強化社群的向心力，使社群得以持續存在。

網路世界的社群同樣地具備上述的特性與機制。個人加入社交網站（如 FB），即如同加入更多的社交網絡，也拓展獲取社會支持的來源。以 FB 為例，它的許多功能（如相簿、塗鴉牆、按讚等）都可視為協助使用者獲取社會支持的設計。然以往探討 FB 與人際關係的研究中，主要著重於 FB 在人際互動應用方面的滿意度或接受度、社會資本、或隱私權等，對 FB 社群可提供給其使用者之社會支持則著墨不多，實有待更多的實證研究。有鑑於此，本研究以大學生 FB 使用者為對象，探討網路社群之社會支持與使用者背景變項及 FB 功能使用頻率之關聯性。

2.文獻探討

2.1 網路社群的本質與功能

社群（social community）是指特定區域內共享設施、互相交流、彼此認同的一群人。在今日，由於電腦與網路科技的進步，網際網路（Internet）提供了一種不同於以往的聚集方式，人與人之間可以在網際網路互通訊息，進而彼此認識與交往。社交網站乃因此應運而生且蓬勃發展，其使用者自然而然在網路世界中形成各類型的社群。網路社群即延伸自實體社群的一個專有名詞，意指在網際網路上

有足夠的人數持續參與的社會聚集體[3]。Rheingold 認為，網路社群是一種新型的社會組織，並有四種特質：表達的自由、缺乏集中的控制、多對多的傳播、與自願的參與行為[3]。

網路社群與實體社群相同，對其所屬成員具有許多功能。以 FB 為例，會員可以和老同學或舊朋友聯繫、可以結交新朋友、可以更進一步深化與維持友誼、以及可以擴充人脈與社會資源等。其中一個極為重要的功能，也是維繫網路社群能否持續存在的重要機制是，成員之間的互相支持與協助（如交換訊息、分享資源與經驗、彼此鼓勵等）。

2.2 社會支持的內涵

社會支持（social support）是指個人得自於他人的精神、知識、或物質上的援助或支持。社會支持是社群的一個非常重要的特性，成員之間的精神或物質支持使個別成員不致感到孤立或無助，有能力面對壓力，有信心與方法解決困難。社群成員間的支持，也間接地強化社群的向心力。易言之，一個社群的成員是否彼此提供社會支持，是該社群可否繼續存在與維持的重要機制。

House [4]將社會支持區分為：一、情緒支持：表達尊重、愛、信任、關愛、聆聽等；二、評價支持：表達肯定、正向回饋、鼓勵等；三、訊息支持：提供忠告、建議、指導等；四、工具支持：提供金錢或物質的協助以及行動的介入。Cohen 與 Wills [5]又將社會支持的內涵加入二個向度：自尊支持（esteem support）與夥伴關係（social companionship）。前者指在人際交往過程中讓他人感受到尊重和接納；後者則指與他人共享休閒和娛樂，使其獲得親密需求的滿足。

以往研究顯示，社會支持有性別與年齡的差異。在性別方面，女性較男性更常扮演關懷照顧者的角色，也較男性更能表達情感。對於人際關係的敏感度也促使女性成為社會支持的主要提供者，在個人認知面上也比較感知到情感類的社會支持[6][7]。國內研究結果與以上描述相似[8]。在年齡方面，國外研究指出青少年隨著年齡的增長，感受家庭支持的程度有明顯下降的情形[9]。國內有關高中或大學生的研究亦有相似的發現，即較低年級的學生比高年級學生獲得較多的社會支持[10][11][12]。

2.3 網路社群之社會支持

網路社群（web community）雖非實體社群，但對參與者而言，其實是真實存在的社群，因為每一成員，不管認識與否，都是活生生、能思想、會回應、有情緒、有感情的生命體。既然網路社群具有實體社群的許多特徵，必然可以提供其成員各種的社會支持，如訊息支持、評價或自尊支持、情緒支持、或工具支持等。Walther [13]甚至指出網路社群的社會支持，相較於現實的社會支持，有更多的優勢，如化名、即時性、與非同步性等。使用者把個人的喜怒哀樂或困惑疑難發佈到社交網站上後，或多或少都會得到「好友」的回應，達到分享經驗、減輕壓力、或解決問題之目的。易言之，社交網站不僅拓廣成員的社交網絡，也增加成員獲取社會支持的來源與時間。以 FB 為例，它的許多功能（如動態、相簿、塗鴉牆、按讚、訊息、聊天室、遊戲等）更儼然是協助其用戶獲取社會支持的設計。舉例而言，FB 用戶和好友們在線上聊天或一起玩遊戲，即可得到有人陪伴、一起打發無聊時間的效果。因此，較頻繁於使用這些功能的 FB 會員，也會得到更多的社會支持；反過來說，想要從網路社群得到社會支持的使用者，會比較熱衷於使用這些功能。以下就 FB 使用者較常獲得的社會支持加以說明：

一、訊息支持： FB 使用者可將個人的近況、困難或疑惑公告於塗鴉牆與聊天室，透過 FB 的自動更新與即時通知，或以訊息（即信件）讓好友們知悉，在短時間內即可得到好友們所提供的意見或相關資訊，也就是所謂的訊息支持。

二、評價或自尊支持：FB 使用者上傳新的動態訊息或相片後，很快地便會得到好友們的「讚」，這只是使用者從 FB 社群得到評價支持的其中一個方式而已。好友們也可將表達接納或尊重的文字留在對方的塗鴉牆上或直接以訊息寄給對方等。藉由這些方式，FB 使用者得到尊重與接納，並被視一個有價值的個體。尤有甚者，有些 FB 使用者在網路社群獲得比實體社群（如班級或學校等）還要多的社會支持。

三、情緒支持：FB 使用者將自己的心情發布在塗鴉牆或網誌上，或以訊息方式讓所選擇的好友或社群知道後，好友們通常會表達樂意分享或感同身受的回應。由於網際網路的無遠弗屆，即使遠在千里的好友們，也都可以彼此分享喜怒哀樂，不致於有孤單無人傾訴的窘境。

總而言之，對網路社群而言，提供與獲取社會支持是很重要的功能與機制。然而，由於以往在這方面的研究並不多，我們對網路社群的社會支持也就了解甚少。基於 FB 乃最受歡迎的社交服務網站，且大學生為 FB 之主要使用族群，因此本研究選擇以大學生為對象，探討 FB 使用者在網路社群所獲取的社會支持。研究問題有三：一、網路社群的社會支持是否有性別差異？二、網路社群的社會支持是否存在著年級的差異？三、各項 FB 功能使用頻率不同者所得到的社會支持是否有所差異？

3.研究方法

3.1 受試者

本研究以二種管道取得樣本。紙本問卷調查部份係以北區與中區五所大學之大學部學生為抽樣對象，共發出 380 份問卷，回收 274 份，有效問卷 270 份。線上問卷部分是將紙本問卷以線上問卷設

計軟體（MySurvey）加以編輯後，於 BBS 及 FB 張貼問卷網址，徵求自願者協助填答，條件為必須是大學在學生，且每台電腦 IP 位址只限作答一次。研究者另請朋友及網友們幫忙轉貼問卷網址給他們的朋友們，而他們的朋友可再繼續轉貼問卷網址給其他人填寫。以此方法共回收 319 份，有效問卷 309 份。本研究有效問卷共 578 份。

樣本中，女性（N = 332）的比例比男性（N = 246）多 14.8%。年級方面，大一人數最多（N = 210），其次為大二（N = 124）、大三（N = 124）、與大四（N = 99），另有延畢生 21 人。大多數學生使用 FB 已逾二年以上（74.2%），每天平均使用時間為 1~4 小時（66.4%），朋友數 100 人以上（88.4%），可推論為屬於 FB 愛用者且參與至少一個以上的 FB 社群。

3.2 研究工具

本研究之研究工具為 FB 使用調查表與 FB 社會支持量表。受試者於 FB 使用調查表上填答個人基本資料（性別、年齡、公私立、學校類型、科系、就讀年級）與 FB 使用情形（已使用時間、每天平均使用時間、朋友列表人數、熱門功能使用頻率）。

FB 社會支持量表係根據本研究之目的並參考相關理論與測量工具而編製之工具，分訊息支持、評價支持、情緒支持三個分量表，合計 23 題。訊息支持分量表測量受試者得到 FB 社群之建議與指導的程度（如「在 FB 上有人能幫我解決學業問題」）；評價支持分量表測量受試者得到 FB 社群之正向回饋、肯定、或接納的程度（如「當我把好的表現在 FB 與他人分享時，有人會留言稱讚我」）；情緒支持分量表則測量受試者之情緒得到 FB 社群回應或接納的程度（如「在 FB 有人對我的情緒反應表示關心」）。量表題目隨機排列，每一題目之後為 Likert-Type 五點量尺，由受試者圈選一個數字，以表達其實際感受（1 代表「非常不同意」；5 代表「非常同意」）。計算分量表分數時，係以各分量表內可保證內部一致性信度值至最佳水準之六個題目為依據。訊息、評價、與情緒支持分量表之 Cronbach α 係數值依序為 .90、.86、與 .74；全量表之 α 係數為 .92。

4.研究結果

4.1 性別、年級與 FB 社會支持

以下依序呈現與研究問題相關之分析結果。表 1 為大學生樣本在 FB 社群所得到社會支持的數據。本研究以 2（性別）x 3（分量表）之重複量數變異數分析進行檢定，以了解 FB 社會支持是否因性別或測量向度而有差異。結果顯示，性別效應與交互作用效應未達顯著水準，唯分量表效應達顯著水準，F（2, 1152）= 219.54，p < .001。事後比較顯示，FB 社群之訊息支持（M = 22.55, SD = 4.22）與評價支持（M = 22.56, SD = 4.28）皆顯著高於情緒支持（M = 18.53, SD = 6.17），但二者彼此間並無顯著差異。簡言之，男性與女性大學生在所感知的訊息、評價、或情緒面社會支持並無顯著差異，且大學生整體而言所感知的情緒面社會支持顯著低於訊息或評價面社會支持。

表 1 大學生自 FB 社群所得之社會支持

性別	訊息支持	評價支持	情緒支持
男生（N=246）	22.45 (4.05)	22.19 (4.24)	18.42 (6.06)
女生（N=332）	22.62 (4.35)	22.84 (4.3)	18.61 (6.25)

註：表格內數值為平均數與標準差（括號內）。

表 2 為各年級學生的 FB 社會支持。為檢定各年級間之差異是否達顯著水準，本研究以 2（性別）x 5（年級）變異數分析（ANOVA）逐一針對三個分量表分數進行檢定。此分析結果顯示，以訊息支持為依變項時，性別效應與交互作用效應未達顯著水準，唯年級效應達顯著水準，F（4, 568）= 3.10，p < .05。經事後比較發現，大三比大一的學生得到較多的訊息性支持（見表 2）。依變項為評價支持時，性別效應、年級效應、以及性別與年級之交互作用效應均未達顯著水準。依變項為情緒支持時，性別效應與交互作用效應亦未達顯著水準，唯年級效應達顯著水準，F（4, 568）= 6.54，p < .001。經事後比較發現，大一、大二、與大三學生的情緒性支持顯著高於四年級與延畢生。

表 2 各年級大學生自 FB 社群所得之社會支持

年級	訊息支持	評價支持	情緒支持
大一 (N=210)	21.93[a] (4.61)	22.96 (4.58)	19.33[a] (5.7)
大二 (N=124)	23.00 (3.69)	22.94 (3.79)	19.02[a] (5.84)
大三 (N=124)	23.46[b] (4.26)	22.58 (4.56)	19.12[a] (6.45)
大四 (N=99)	22.48 (3.79)	21.51 (3.93)	16.54[b] (6.62)
延修生(N=21)	21.19 (3.89)	21.57 (3.25)	14.05[b] (5.51)

註：表格內數值為平均數與標準差（括號內）。平均數上標字母不同者，代表彼此有顯著差異（p < .05）。

4.2 FB 功能使用頻率與社會支持

為了解各 FB 功能（相簿、塗鴉牆、按讚、社團、聊天室、網誌、活動、及遊戲）之使用頻率與社會支持之間的關聯性，本研究分別就每一功能，

以訊息、評價、與情緒支持為依變量，進行 2（性別）x 4（使用頻率）ANOVA。如某一頻率等級（如「從未使用」）人數過少時，則併入相鄰之頻率等級，進行 2（性別）x 3（使用頻率）ANOVA。這些分析結果極為相似，亦即僅使用頻率效應達顯著水準，而性別效應與交互作用效應則未達顯著水準，以下就使用頻率效應部分之事後比較（Scheffe 法）結果說明如下：

4.2.1 相簿與塗鴉牆功能

由表 4 可看出相簿功能使用頻率不同者之社會支持。訊息支持部分，幾乎每次使用此功能者與經常使用者無顯著差異，但二者均顯著高於偶爾使用者與從未使用者；偶爾使用者與從未使用者則無顯著差異。評價支持部分，幾乎每次使用者顯著高於經常使用者，經常使用者顯著高於偶爾使用者，且偶爾使用者亦顯著高於從未使用者。情緒性支持部分，幾乎每次使用者顯著高於從未使用者。

表 4 相簿與塗鴉牆使用頻率不同者之社會支持

使用頻率	訊息支持	評價支持	情緒支持
	相簿功能		
從未使用 (N=28)	19.96[a] (4.83)	19.64[a] (5.14)	16.11[a] (5.53)
偶爾使用 (N=342)	21.88[a] (4.25)	21.98[b] (4.16)	18.14 (5.95)
經常使用 (N=176)	23.90[b] (3.57)	23.72[c] (3.98)	19.24 (6.25)
幾乎每次使用 (N=32)	24.50[b] (3.89)	25.03[d] (3.67)	20.91[b] (7.39)
F (3, 570)	15.62***	14.00***	3.29*
	塗鴉牆功能		
從未使用 (N=32)	19.22[a] (5.88)	18.78[a] (6.29)	15.38[a] (7.12)
偶爾使用 (N=254)	21.87[b] (4.13)	21.80[b] (3.86)	17.96[ab] (5.69)
經常使用 (N=212)	23.05[c] (3.72)	23.17[c] (3.95)	18.97[b] (6.14)
幾乎每次使用 (N=80)	24.69[d] (3.69)	24.91[d] (3.84)	20.43[c] (6.66)
F (3, 570)	16.99***	19.67***	5.96**

註：表格內數值為平均數與標準差（括號內）。平均數上標字母不同者，代表彼此有顯著差異（$p < .05$）。
* $p < .05$. ** $p < .01$. *** $p < .001$.

在「塗鴉牆」功能部分，幾乎每次使用者所獲得之訊息支持與評價支持顯著高於經常使用者，經常使用者又顯著高於偶爾使用者，且偶爾使用者亦顯著高於從未使用者（如表 4）。情緒支持方面，幾乎每次使用者顯著高於從未使用者與偶爾使用者；經常使用者亦顯著高於從未使用者。

4.2.2 按讚、社團、與聊天室功能

在 FB 按讚功能的部份（詳見表 5），幾乎每次使用者所得自網路社群之訊息、評價、與情緒性社會支持均顯著高於經常使用者；經常使用者所得之訊息、評價、與情緒性社會支持亦均顯著高於偶爾／從未使用者。

表 5 按讚、社團、與聊天室功能使用頻率不同者之社會支持

使用頻率	訊息支持	評價支持	情緒支持
	按讚功能		
從未(N=5)／偶爾使用(N=102)	20.93[a] (4.83)	20.07[a] (4.78)	15.38[a] (7.12)
經常使用 (N=223)	22.13[b] (3.77)	22.23[b] (3.80)	18.97[b] (6.14)
幾乎每次使用 (N=248)	23.62[c] (4.04)	23.94[c] (3.92)	20.43[c] (6.66)
F (2, 572)	18.58***	31.86***	10.16***
	社團功能		
從未(N=7)／偶爾使用(N=191)	21.57[a] (4.41)	22.13[a] (4.57)	18.55 (6.01)
經常使用 (N=263)	22.57[b] (3.89)	22.37[a] (3.95)	18.22 (6.07)
幾乎每次使用 (N=117)	24.16[c] (4.14)	23.72[b] (4.33)	19.19 (6.62)
F (2, 572)	14.43***	5.40**	0.81
	聊天室功能		
從未(N=10)／偶爾使用(N=162)	21.21[a] (4.74)	21.78[a] (4.73)	18.03 (5.91)
經常使用 (N=241)	22.20[b] (3.72)	22.21[a] (3.74)	18.36 (5.84)
幾乎每次使用 (N=165)	24.45[c] (3.65)	23.89[b] (4.25)	19.29 (6.82)
F (2, 572)	27.37***	9.80***	1.69

註：表格內數值為平均數與標準差（括號內）。平均數上標字母不同者，代表彼此有顯著差異（$p < .05$）。
** $p < .01$. *** $p < .001$.

在 FB「社團」功能部分（表 5），幾乎每次使用者獲得之訊息支持顯著高於經常使用者，且經常使用者亦顯著高於偶爾／從未使用者。在評價支持方面，幾乎每次使用者顯著高於經常使用者與偶爾／從未使用者；後二者則無顯著差異。在情緒支持

方面，使用頻率不同者之間沒有顯著差異。

在 FB「聊天室」功能部分（表 5），幾乎每次使用此功能者之訊息支持顯著高於經常使用者；經常使用者亦顯著高於偶爾／從未使用者。在評價支持方面，幾乎每次使用者顯著高於經常使用者，亦顯著高於偶爾／從未使用者；後二者則無顯著差異。在情緒支持方面，使用頻率不同者之間沒有顯著差異。

4.2.3 網誌與活動功能

在 FB「網誌」功能部分（表 6），幾乎每次／經常使用此功能者得到之訊息支持顯著高於偶爾使用者與從未使用者，後二者則無顯著差異。在評價支持方面，幾乎每次／經常使用者與偶爾使用者沒有顯著差異，但均顯著高於從未使用者。在情緒支持方面，使用頻率效應雖達顯著水準，但使用頻率不同者之間並無顯著差異。

表 6 網誌與活動功能使用頻率不同者之社會支持

使用頻率	訊息支持	評價支持	情緒支持
	網誌功能		
從未使用 (N=301)	21.97[a] (4.31)	21.97[a] (4.46)	18.03 (6.06)
偶爾使用 (N=228)	22.86[a] (4.03)	23.05[b] (3.97)	18.88 (6.23)
幾乎每次(N=38) ／經常使用(N=11)	24.61[b] (3.81)	23.92[b] (4.04)	20.00 (6.30)
F (2, 572)	9.74***	9.02***	3.15*
	活動功能		
從未使用 (N=132)	20.89[a] (5.03)	21.18[a] (4.85)	16.87[a] (6.15)
偶爾使用 (N=368)	22.68[b] (3.74)	22.81[b] (3.91)	18.85[b] (5.98)
幾乎每次(N=69) ／經常使用(N=9)	24.72[c] (3.76)	23.74[b] (4.44)	19.81[b] (6.56)
F (2, 572)	20.99***	10.12***	6.49**

註：表格內數值為平均數與標準差（括號內）。平均數上標字母不同者，代表彼此有顯著差異（$p < .05$）。
* $p < .05$. ** $p < .01$. *** $p < .001$.

在 FB「活動」功能部分（表 6），幾乎每次／經常使用此功能者所得到之訊息支持顯著高於偶爾使用者，偶爾使用者顯著高於從未使用者。在評價支持與情緒性支持方面，幾乎每次／經常使用者與偶爾使用者沒有顯著差異，但二者均顯著高於從未使用者。

4.2.4 遊戲功能

表 7 為「遊戲」功能使用頻率不同者之社會支持，無論是訊息、評價、或情緒性社會支持，皆未因使用頻率不同而有顯著差異。

表 7 遊戲功能使用頻率不同者之社會支持

使用頻率	訊息支持	評價支持	情緒支持
從未使用 (N=96)	22.54 (3.64)	22.10 (4.52)	17.43 (6.53)
偶爾使用 (N=332)	22.45 (4.24)	22.67 (4.24)	19.04 (5.92)
經常使用 (N=82)	23.20 (3.16)	22.62 (3.84)	17.91 (6.20)
幾乎每次使用 (N=68)	22.26 (5.76)	22.62 (4.69)	18.34 (6.60)
F (3, 570)	0.92	0.61	2.02

註：表格內數值為平均數與標準差（括號內）。

5. 討論與建議

本研究的若干發現有其重要性，有進一步加以討論的必要性。首先，本研究發現，FB 使用者所感知的情緒面社會支持顯著低於訊息或評價面之社會支持。研究者認為，此差異實肇因於線上人際互動的特性。網路的優勢在於無遠弗屆且迅速的訊息交換，有利於訊息性或評價性的社會支持，原因是此二向度的社會支持以簡短的文字即可正確、充分地表達，且不易被誤解。相反地，以文字表達情緒支持則有其力有未逮之情況。在面對面的人際互動情境下，情緒面社會支持通常藉由表情、眼神、聲音及語調、與肢體動作（如擁抱）等方式表達，但這些方式卻無法在線上人際互動中充分地表現。此外，或許 FB 使用者也很清楚地了解線上人際互動的特性，對於提供或獲得情緒面社會支持的期待比較低，因而較為不積極於給予彼此情緒面之社會支持。

由上述研究結果看來，一個極有趣的問題便是 FB 是否可藉由增加某些功能而讓其用戶更能夠回應與表達對好友的情緒支持呢？ FB 的「按讚」功能是很受歡迎的功能，因為此設計可讓使用者對好友的訊息或狀態表達喜歡、認同與讚賞。然而從本研究的結果看來，FB 在情緒面的社會支持相對低於其所提供的訊息或評價面的支持。因此，或許 FB 的系統開發人員可以朝加強此部分努力，增加可讓使用者表達或接受種種情緒的貼心設計（如內崁的可表達情緒支持的表情符號或簡短文字範本等），讓使用者在無法面對面溝通的線上人際互動中，仍然能夠貼切地傳達彼此的情緒性支持。對其使用者而言，FB 不應只是想法、相片、旅遊心得、或好康美食經驗的分享而已，它應該也可以是提供與獲取社會支持的重要來源。

其次，本研究之發現與以往現實社會支持之研

究結果有相似與相異之處。相似之處為，FB 社群亦傾向於給予年紀較小者相對較多的情緒支持。由此看來，隨著年齡增加而社會支持相對減少的現象，並不會因社群是屬於現實社會或網路世界而有不同。本研究有別於以往之處在於，男性與女性在社會支持方面的差異並未複製於網路社群。以往的研究顯示，女性較能表達情感、有較高之人際關係敏感度、常扮演關懷照顧者角色、也較常成為社會支持的提供者[8][9]。然本研究與另一探討 MSN 線上社會支持類型之研究相似[14]，並未發現性別差異。研究者認為，其原因應與前述線上社群人際互動特性有密切關聯，亦即不利於情緒面社會支持之表達。女性在現實生活人際互動之強項在於情緒敏感度與表達性，然此優勢卻無法在線上人際互動情境下充分地表現，間接地弭平二性間原有的差異。

本研究之另一重要發現為，社交網站會員獲取線上社會支持之程度高低，亦與其使用該網站互動功能的頻率有極大之關聯。以本研究之 FB 使用者為例，除遊戲之外的熱門功能（相簿、塗鴉牆、按讚、及聊天室等），使用頻率不同者所獲得的訊息或評價面社會支持亦有顯著的差異。整體而言，愈頻於使用這些功能者，也得到較多的社會支持。從另一個角度觀之，想獲得更多線上社會支持的使用者，也會更勤於（或樂於）使用可滿足此種需求的互動功能。在本研究中，遊戲功能雖然沒有相同的效果，但我們卻不可據此推論遊戲功能與社會支持毫無關聯，原因在於本研究並未探討「陪伴」（social companion）向度的社會支持。或許，線上遊戲所提供的正是此向度的社會支持。

本研究之發現，對大學之學生輔導與諮商工作有若干重要的意義。其一是學校或輔導人員應重視 FB 所提供之訊息面社會支持的效率性與普及性。目前的大學生幾乎人手一支智慧型手機，鮮有不是 FB 的使用者。FB 不僅是大學生聯繫友誼與認識新朋友的地方，也是他(她)們獲取各種訊息的主要管道；大學生從 FB 獲得訊息的量與速度甚至勝過於從學校正式管道而來的訊息。因此，學生輔導（或健康促進）中心建立專屬的 FB 帳戶，隨時提供學生應知的有關學習、生活、或升學與就業等方面的訊息，應該會是一種比較積極且與時俱進的輔導方式。其二是學校輔導人員應重視 FB 所能提供之評價面社會支持。對大學生而言，線上人際關係自有其不可取代的重要性，對某些人而言，甚至可彌補現實人際關係的不足。FB 社群無形中已成為新世代年輕人獲得肯定、提升自我概念的重要社會組織。有鑑於此，大學輔導教師對 FB 不可陌生，最好自己也是 FB 用戶，並且邀請學生加入為 FB 朋友。果能如此，輔導老師即可在 FB 上隨時提供導生所需要的訊息面的或評價面的社會支持、大幅度地縮短與學生的距離、且有效地提升輔導成效。

有關 FB 社群社會支持方面的研究，未來仍有許多極具潛力與重要性之方向。第一、由於本研究未探討 FB 社群之屬性（如專業或聯誼、工作職場或學生組織），未來研究者可探討社群屬性與社會支持面向之關聯性。舉例而言，LinkedIn 也是另一以專業領域為訴求之社交網站，研究者可探討 LinkedIn 社群是否在訊息或評價面之社會支持又更勝於情緒面之社會支持。第二、本研究僅從接受者的角度探討網路社群之社會支持，未來研究者則可從提供者的觀點切入，探討提供線上社會支持的影響或相關因素（如性別、人格特質、好友類別等）。第三、未來研究者亦可探討網路社群社會支持的實質影響。訊息支持是否有效協助學業問題的解決？評價支持是否可提升自我概念或自尊？情緒面社會支持是否可有效降低焦慮？以上問題之後續研究將有助於我們對網路社群社會支持的完整了解。

參考文獻

[1] Wikipedia, “Facebook,” 2013, retrieved from http://en.wikipedia.org/wiki/Facebook.

[2] 數位時代, “日網路公司 Facebook 亞洲用戶數調查”, 取自 http://www.bnext.com.tw/focus/view/cid/103/id/27267

[3] H. Rheingold, “The Virtual Community: Homesteading on the Electronic Frontier,” Cambridge, Mass: MIT Press, 2000.

[4] J. S. House, Work Stress and Social Support, Philippines: Addison-Wesley Publishing Company, 1981.

[5] S. Cohen, and T. A. Will, “Stress, social support, and the buffering hypothesis,” Psychol. Bulletin, 98(2), 310-357, 1985.

[6] V.J. Derlega, A. Barbee, and B. A. Winstead, “Friendship, gender, and social support: Laboratory studies of supportive interactions,” in The communication of social support: Messages, interactions, relationships, and community, T. Albrecht, I. Sarason, and B.R. Burleson, eds. London: Sage Publication, 1994, pp. 136-151.

[7] S. E. Hobfoll, and J. P. Stokes, “The process and mechanics of social support,” in Handbook of personal relationships: Theory, research and interventions, S. Duck, ed. New York: John Wiley & Sons, 1988.

[8] 李金治, “國立臺灣師範大學四年級學生生活壓力、因應方式、社會支持與其身心健康之相關研究”, 國立臺灣師範大學碩士論文, 2003.

[9] M. Helsen, W. Vollebergh, and W. Meeus, “Social support from parents and friends and emotional problems in adolescence,” J. of Youth and Adoles., 29 (3), 319-335, 2000.

[10] 屈寧英, “高中生生活壓力、社會支持、行為模式與幸福感相關性之研究－以臺北市立某女子高級中學為例”, 國立臺灣師範大學碩士論文, 2004.

[11] 徐珮瑜, “影響大學生親密關係分手調適因素之研究－以北部地區為例”, 國立臺灣師範大學碩士論文, 2005.

[12] 賴美蒨, “大學生背景變項、人際親密、社會支持與幸福感之差異研究”, 臺北市立教育大學碩士論文, 2009.

[13] J. B. Walther, “Computer-mediated communication: Impersonal, interpersonal, and hyperpersonal interaction,” Communication Research, 23, 3-43, 1996.

[14] 陳蓉萱, “線上社會支持類型初探—以即時通訊軟體 MSN 為例”, 中華傳播學會 2005 年學刊.

人格特質、Facebook 使用動機對人際關係之衝擊研究 —以台灣地區大學生為例

劉勇伸　張青桃
國立雲林科技大學資訊管理所
g9923751@yuntech.edu.tw
changct@yuntech.edu.tw

摘要

本論文目的在探討人格特質及 Facebook 使用動機對於人際關係的影響。本研究之進行乃透過五大人格特質問卷、Facebook 使用動機問卷及人際關係問卷為測量工具，並對台灣地區的大學生 Facebook 使用者進行調查，並用統計方法分析資料，並且歸納解析研究成果。藉此提出一套人格特質影響 Facebook 使用動機及人際關係的理論模式，希望透過此模式在探討 Facebook 的使用方面可以更加完整。

關鍵詞：人格特質, Facebook 使用動機, 人際關係

1. 緒論

網際網路應用的相關發展，讓各式各樣的網站在短短數年不斷興起，近年來的以社群網站的最為熱門。社群網路是將實體社會中的社區、團體概念延伸到網路上，網友可以依據各項宗旨在社群網站中成立不同的團體，並藉此進行聯絡與溝通。而它最大的意義在於與其他人產生互動、情感維繫以及得到更多資訊的需要，並提供一個虛擬空間，讓關心相同主題的使用者群聚在一起並且分享資訊。目前以 2004 年推出的 Facebook 獨佔目前社群網站的龍頭。Facebook 最初在美國成立的目的是以服務大學生為主要業務，希望讓大學生創造及維持社交關係。近年來，Facebook 也在台灣成了許多使用者交集的社群平台，改變了大家的網路使用習慣，這使得 Facebook 不再是一個建立人際關係的平台，更是深深影響人際關係模式的重要媒介。

面對今日蓬勃發展的 Facebook，他成功吸引到大量的使用者，但令人好奇的是在財團法人台灣網路資訊中心 2012 年 3 月份研究調查公布的「台灣寬頻網路使用調查」裡發現，有 1/4 的台灣使用民眾已經感受到因網路社群服務影響而減少本身日常生活的人際互動[1]。Orr, Sisic, Arsenault, Simmering, & Orr (2009)在探討人格特質的如何影響 Facebook 使用的研究裡發現，人格特質的差異會影響 Facebook 使用者對 Facebook 的使用動機，但只描述幾種動機的可能性，並沒有針對人格特質的不同有更完整的討論。而面對今日蓬勃發展的 Facebook，它除了成功吸引到大量的使用者使用外，其功能與特性更是引發使用者去使用 Facebook 的動機，並藉此創造了一個社會關係網絡的社交平台，提供不同人格特質的使用者能在其中順利發展人際關係。

2. 文獻探討

2.1 人格特質

目前最被廣為接受的是 Costa & McCrae (1992) 所提出的五大類人格特質構面：神經質(Neuroticism)、外向性(Extraversion)、開放性(Openness to experience)、親和性(Agreeableness)、嚴謹性(Conscientiousness)[2]。一般認為只要用以上五個基本人格特質就足以描述一個人的人格，經由許多研究的證實，五大人格特質已經被公認為近代心理學中最主要的性格結構。五大人格特質面向分述如下：. ：

一、 神經質(Neuroticism)：指能激起一個人的負面情感之刺激所須要的數目及強度，當一個人所能接受的刺激越少，則其神經質越高，換句話說，只需少許的刺激，一個人的負面情感就能被激起，這種人則被認為神經質特質較高之。

二、 外向性(Extraversion) ：指一個人對於與他人之間關係感到舒適的程度，若一個人和其他人關係之舒適程度越高，則表示這個人越外向。

三、 開放性(Openness to experience)： 包括活躍的想像力、審美感、對內心感受的專注性，對種類的偏好，以及對知識的好奇心。若一個人興趣越多樣化，但相對深度比較淺，則其開放特質越高。

四、 親和性(Agreeableness)：指一個人對於他人所定下之規範的遵從。親和型的特徵是有禮貌、令人信賴同時也容易信任別人、待人友善、容易相處、樂意合作、有明顯的同情心。

五、 嚴謹性(Conscientiousness)：指一種按照良心支配自己的行動的人格特質。它包括自律、細心、徹底性、條理性、審慎，以及成就需要等元素。

2.1 人際關係

大學階段是一個人一生中非常重要的階段，很多的價值觀都是在這個時期建立的，而在此時建立良好的人際關係，乃是青少年時期的重要發展之一，

大學生在學校中人際關係的好壞，對學生的生活及身心都有極大的影響[3]。整體來說，潘菲(1992)在【論青少年的人際關係】中，提出最重要的人際關係包括四種：(一)同儕關係、(二)異性關係、(三)親子關係、(四)師生關係，分述如下：

一、 同儕關係：大學生隨著年齡的增加，對友誼需求水準的提高，標準變得相當複雜，會嚴格區分朋友和一般夥伴。

二、 異性關係：親密關係是青少年、青年發展的重要助力，如果沒有親密關係將會阻礙未來人際關係的開發與維持。

三、 親子關係：青少年、青年階段同儕的影響力大增，父母的影響力相對的減低，但基於金錢、教育、生涯規劃等方面之需要，仍會與父母維持某種程度的親密關係，而較不願意在個人問題上與父母交談，反而喜歡找同儕提供意見。

四、 師生關係：青少年、青年不再把教師看作父母的化身，教師的權力也不再如此的大，只要是學生合法的權益，皆受到合理的保障。

2.3Facebook 使用動機

陳憶菁(2012)以列出代表性的關鍵字清單的方式，針對清單中的關鍵字進行探索性因素分析（Exploratory Factor Analysis，EFA），提出影響網友使用 Facebook 的因素主要有以下五個構面[4]：

一、 關係性：包含「維繫親情」、「維繫愛情」。

二、 社交性：包含了「分享近況」、「分享資訊」、「分享心情」、「尋找失聯的朋友」、「分享照片與影片」。

三、 資訊性：包含「方便分享資訊」、「快速分享資訊」、「方便獲得資訊」。

四、 遊戲性：包含「遊戲多樣」、「遊戲好玩」。

五、 娛樂性：包含「抒壓解悶」、「消磨時間」。

2.4 人格特質與、社群網站使用及人際關係之相關研究

2.4.1 社群網站使用及人際關係相關研究

Lindgren(1953)指出一個人能否被其所處的團體吸引，會影響其人格的發展與社會適應[5]。石文宜(2005)指出人格特質為親和性、嚴謹性、外向性及開放性的個體，比較容易與人建立良好的關係[6]。陳嬿竹(2002)亦對學生進行人格特質與人際關係的研究，發現親和性、嚴謹性較高者，與父母之間關係較佳；外向性、親和性較高者，與朋友之間關係較佳；人格特質對與網友之間的關係影響比較薄弱[7]。王汝潔、張斐媄、楊依姍、楊宜蓁(2013)指出親和性高者人際關係也越好[8]；Asendorpf & Wilpers (1998)也表示，外向性的人，喜歡建立朋友網絡，朋友及同儕關係數目較多；人格特質傾向於親和性的與同儕的衝突較少[9]。Wilkinson & Walford (2001)指出外向性的人在互動中感受到親近的感覺，人格特質傾向神經質的人在互動的親近感呈現負相關[10]。

2.4.2 社群網站使用及人際關係相關研究

林淳蔭(2010) 指出使用社群網站使用動機高的青少年，大多都是與家人關係和諧、又是有知心好友的，而且個性較為開朗，亦是喜愛與他人互動的人，因此人際關係互動越親密[11]。蔣孟軒 (2012)也指出社群網站的參與度與網路人際關係具有顯著關係，參與度越高，實際人際關係也越好[12]。李柔萱、林玉容、韓彥卉(2012)在 Facebook 對人際關係的影響的研究中也發現使用 Facebook 後會讓我們更容易認識新朋友。使用的時間越久，其在增加信任、聊天廣度、分享心情方面的人際互動面會比較強烈，且使用 Facebook 可以增進朋友和朋友間的情誼，甚至是可以比日常生活交新朋友來的容易[13]。

2.4.3 人格特質及社群網站使用相關研究

Amichai-Hamburger & Vinitzky (2010) 在人格特質和 Facebook 使用行為的研究中，發現人格特質和 Facebook 的使用有高度的關聯。外向性者擁有比較多的朋友和社團。神經質者在個人檔案有較多的個人資料且喜歡用私人簡訊跟朋友聯繫。隨和型者喜歡在 Facebook 放較多照片。開放性者會使用較多的 Facebook 功能。嚴謹性高者有較多朋友，但 Facebook 上的照片較少[14]。Ross et al. (2009) 調查人格特質對 Facebook 使用的影響，發現不同的人格特質會影響他們使用不同的 Facebook 功能。外向性的人喜歡加入較多的社團，而神經質的人喜歡用塗鴨牆，神經質較低者則喜歡張貼照片，開放性的人喜歡在 Facebook 社交[15]。Correa et al. (2010) 也指出人格特質跟社群網站使用的關係，他們發現外向性跟開放性者喜歡用社群網站[16]。Ebeling-White et al. (2007) 也發現神經質喜歡在線上聊天和交朋友[17]。

3.研究方法

3.1 研究架構

參考前章相關文獻探討結果，故建立本研究架構如下圖 3.1：

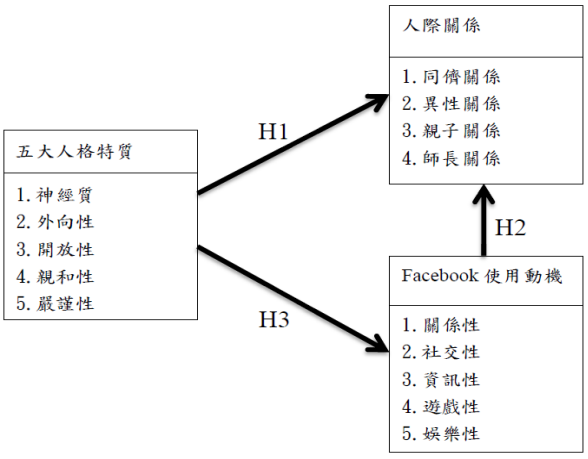


圖 1 研究模型

3.2 研究假設

石文宜(2005)表示人格特質為親和性、嚴謹性、外向性及開放性的個體，比較容易與人建立良好的關係[6]。劉立仁(2012)也指出人格特質之開放性、嚴謹性、和善性者，與其人際關係呈顯著正相關[18]。Wilkinson & Walford (2001)也指出外向性的人在互動過程中容易感受到親近的感覺，人格特質傾向神經質的人在與人的互動中的不易感受到親近感[10]。故本研究提出下列假設：

H1：人格特質對人際關係有影響性：

H1-1：神經質人格特質對人際關係上有負向影響
H1-2：外向性人格特質對人際關係上有正向影響
H1-3：開放性人格特質對人際關係上有正向影響
H1-4：親和性人格特質對人際關係上有正向影響
H1-5：嚴謹性人格特質對人際關係上有正向影響

蔣孟軒(2012)指出參與社群網站可以克服焦慮感，可以得到滿足及歸屬感，參與動機也越強，因此對人際關係能有所突破[12]。由此本研究提出下列假設：

H2：Facebook 使用動機對人際關係有影響：

H2-1：Facebook 的關係性動機對人際關係上有正向影響關係
H2-2：Facebook 的社交性動機對人際關係上有正向影響關係
H2-3：Facebook 的資訊性動機對人際關係上有正向影響關係
H2-4：Facebook 的遊戲性動機對人際關係上有正向影響關係
H2-5：Facebook 的娛樂性動機對人際關係上有正向影響

Correa et al. (2010) 發現外向性跟開放性人格特質的人喜歡用社群網站，但神經質者不喜歡用社群網站，因此本研究提出下列假設[16]：

H3：人格特質對其 Facebook 使用動機有影響性：

H3-1：神經質人格特質對 Facebook 關係性動機上有正向影響
H3-2：外向性人格特質對 Facebook 關係性動機上有正向影響
H3-3：開放性人格特質對 Facebook 關係性動機上有正向影響
H3-4：親和性人格特質對 Facebook 關係性動機上有正向影響
H3-5：嚴謹性人格特質對 Facebook 關係性動機上有正向影響

H3-6：神經質人格特質對 Facebook 社交性動機上有正向影響
H3-7：外向性人格特質對 Facebook 社交性動機上有正向影響
H3-8：開放性人格特質對 Facebook 社交性動機上有正向影響
H3-9：親和性人格特質對 Facebook 社交性動機上有正向影響
H3-10：嚴謹性人格特質對 Facebook 社交性動機上有正向影響

H3-11：神經質人格特質對 Facebook 資訊性動機上有正向影響
H3-12：外向性人格特質對 Facebook 資訊性動機上有正向影響
H3-13：開放性人格特質對 Facebook 資訊性動機上有正向影響
H3-14：親和性人格特質對 Facebook 資訊性動機上有正向影響
H3-15：嚴謹性人格特質對 Facebook 資訊性動機上有正向影響

H3-16：神經質人格特質對 Facebook 遊戲性動機上有正向影響
H3-17：外向性人格特質對 Facebook 遊戲性動機上有正向影響
H3-18：開放性人格特質對 Facebook 遊戲性動機上有正向影響
H3-19：親和性人格特質對 Facebook 遊戲性動機上有正向影響
H3-20：嚴謹性人格特質對 Facebook 遊戲性動機上有正向影響

H3-21：神經質人格特質對 Facebook 娛樂性動機上有正向影響
H3-22：外放性人格特質對 Facebook 娛樂性動機上有正向影響
H3-23：開放性人格特質對 Facebook 娛樂性動機上有正向影響
H3-24：親和性人格特質對 Facebook 娛樂性動機上有正向影響
H3-25：嚴謹性人格特質對 Facebook 娛樂性動機上有正向影響

3.3 研究對象及樣本蒐集

本研究主要研究對象為台灣地區曾經使用過 Facebook 網站之大學生，並利用『mySurvey』(http://www.mysurvey.tw/)製作網路問卷，透過網路傳播媒介將網站連結張貼傳遞，方便受測者自行連結填寫。

3.4 樣本資料處裡

透過電子郵件，網路線上填答的方式對大專院校學生發放問卷，總計回收問卷 584 份，剔除 38 份重複樣本及 1 份填答不完全的無效問卷後，有效問卷為 545 份。以 SPSS18.0 進行資料分析，藉由分析實證資料進行研究假設之驗證，本研究採用(一)敘述性統計、(二)信度分析(Cronbach's α)、(三)皮爾遜相關分析、(四)多元迴歸分析等資料分析方法。

4.研究結果

4.1 研究結果

研究假設	實證結果
H1-1：神經質人格特質對人際關係上有負向影響	不支持
H1-2：親和性人格特質對人際關係上有正向影響	支持
H1-3：外向性人格特質對人際關係上有正向影響	支持
H1-4：開放性人格特質對人際關係上有正向影響	支持
H1-5：嚴謹性人格特質對人際關係上有正向影響	支持
H2-1：Facebook 的關係性動機對人際關係上有正向影響	支持
H2-2：Facebook 的社交性動機對人際關係上有正向影響	支持
H2-3：Facebook 的資訊性動機對人際關係上有正向影響	支持
H2-4：Facebook 的遊戲性動機對人際關係上有正向影響	支持
H2-5：Facebook 的娛樂性動機對人際關係上有正向影響	支持
H3-1：神經質人格特質對 Facebook 關係性動機上有正向影響	不支持
H3-2：親和性人格特質對 Facebook 關係性動機上有正向影響	支持
H3-3：外向性人格特質對 Facebook 關係性動機上有正向影響	支持
H3-4：開放性人格特質對 Facebook 關係性動機上有正向影響	支持
H3-5：謹慎性人格特質對 Facebook 關係性動機上有正向影響	支持
H3-6：神經質人格特質對 Facebook 社交性動機上有正向影響	不支持
H3-7：親和性人格特質對 Facebook 社交性動機上有正向影響	支持
H3-8：外向性人格特質對 Facebook 社交性動機上有正向影響	支持
H3-9：開放性人格特質對 Facebook 社交性動機上有正向影響	支持
H3-10：謹慎性人格特質對 Facebook 社交性動機上有正向影響	支持
H3-11：神經質人格特質對 Facebook 資訊性動機上有正向影響	不支持
H3-12：親和性人格特質對 Facebook 資訊性動機上有正向影響	支持
H3-13：外向性人格特質對 Facebook 資訊性動機上有正向影響	支持
H3-14：開放性人格特質對 Facebook 資訊性動機上有正向影響	支持
H3-15：謹慎性人格特質對 Facebook 資訊性動機上有正向影響	支持
H3-16：神經質人格特質對 Facebook 遊戲性動機上有正向影響	不支持
H3-17：親和性人格特質對 Facebook 遊戲性動機上有正向影響	支持
H3-18：外向性人格特質對 Facebook 遊戲性動機上有正向影響	支持
H3-19：開放性人格特質對 Facebook 遊戲性動機上有正向影響	支持
H3-20：謹慎性人格特質對 Facebook 遊戲性動機上有正向影響	支持
H3-21：神經質人格特質對 Facebook 娛樂性動機上有正向影響	不支持
H3-22：親和性人格特質對 Facebook 娛樂性動機上有正向影響	支持
H3-23：外向性人格特質對 Facebook 娛樂性動機上有正向影響	支持
H3-24：開放性人格特質對 Facebook 娛樂性動機上有正向影響	支持
H3-25：謹慎性人格特質對 Facebook 娛樂性動機上有正向影響	支持

4.1 人格特質與人際關係

本研究不支持 H1-1：神經質人格特質對人際關係無負向影響。顯示具神經質人格特質不影響大學生的人際關係。本研究支持 H1-2：親和性人格特質對人際關係上有正向影響。顯示親和性的人格特質對大學生人際關係的維持和建立上有顯著影響。本研究支持 H1-3：外向性人格特質對人際關係上有正向影響。顯示親和性的人格特質對大學生人際關係的維持和建立上有顯著影響。本研究支持 H1-4：開放性人格特質對人際關係上有正向影響。顯示開放性的人格特質對大學生人際關係的維持和建立上有顯著影響。本研究支持 H1-5：嚴謹性人格特質對人際關係上有正向影響。顯示嚴謹性的人格特質對大學生人際關係的維持和建立上有顯著影響。

4.2 Facebook 使用動機與人際關係

本研究支持 H2-1：Facebook 的關係性動機對人際關係上有正向影響。顯示 Facebook 的關係性動機對大學生人際關係的維持和建立上有顯著影響。本研究支持 H2-2：Facebook 的社交性動機對人際關係上有正向影響。顯示 Facebook 的社交性機對大學生人際關係的維持和建立上有顯著影響。本研究支持 H2-3：Facebook 的資訊性動機對人際關係上有正向影響。顯示 Facebook 的資訊性機對大學生人際關係的維持和建立上有顯著影響。本研究支持 H2-4：Facebook 的遊戲性動機對人際關係上有正向影響。顯示 Facebook 的遊戲性機對大學生人際關係的維持和建立上有顯著影響。本研究支持 H2-4：Facebook 的娛樂性動機對人際關係上有正向影響。顯示 Facebook 的娛樂性機對大學生人際關係的維持和建立上有顯著影響。

4.3 人格特質與 Facebook 使用動機

一、人格特質對 Facebook 關係性動機

本研究不支持 H3-1：神經質人格特質對 Facebook 關係性動機上沒有正向影響。顯示神經質人格特質在對大學生使用 Facebook 的關係性動機上沒有影響關係。本研究支持 H3-2：外向性人格特質對 Facebook 關係性動機上有正向影響。顯示外向性人格特質在對大學生使用 Facebook 的關係性動機上有影響關係。本研究支持 H3-3：開放性人格特質對 Facebook 關係性動機上有正向影響。顯示開放性人格特質在對大學生使用 Facebook 的關係性動機上有影響關係。本研究支持 H3-4：親和性人格特質對 Facebook 關係性動機上有正向影響。顯示親和性人格特質在對大學生使用 Facebook 的關係性動機上有影響關係。本研究支持 H3-5：嚴謹性人格特質對 Facebook 關係性動機上有正向影響。顯示嚴謹性人格特質在對大學生使用 Facebook 的關係性動機上有影響關係。

二、人格特質對 Facebook 社交性動機

本研究不支持 H3-6：神經質人格特質對 Facebook 社交性動機上沒有正向影響。顯示神經質人格特質在對大學生使用 Facebook 的社交性動機上沒有影響關係。本研究支持 H3-7：外向性人格特質對 Facebook 社交性動機上有正向影響。顯示外向性人格特質在對大學生使用 Facebook 的社交性動機上有影響關係。本研究支持 H3-8：開放性人格特質對 Facebook 社交性動機上有正向影響。顯示開放性人格特質在對大學生使用 Facebook 的社交性動機上有影響關係。本研究支持 H3-9：親和性人格特質對 Facebook 社交性動機上有正向影響。顯示親和性人格特質在對大學生使用 Facebook 的社交性動機上有影響關係。本研究支持 H3-9：嚴謹性人格特質對 Facebook 社交性動機上有正向影響。顯示嚴謹性人格特質在對大學生使用 Facebook 的社交性動機上有影響關係。

三、人格特質對 Facebook 資訊性動機

本研究不支持 H3-11：神經質人格特質對 Facebook 資訊性動機上沒有正向影響。顯示神經質人格特質在對大學生使用 Facebook 的資訊性動機上沒有影響關係。本研究支持 H3-12：外向性人格特質對 Facebook 資訊性動機上有正向影響。顯示外向性人格特質在對大學生使用 Facebook 的資訊性動機上有影響關係。本研究支持 H3-13：開放性人格特質對 Facebook 資訊性動機上有正向影響。顯示開放性人格特質在對大學生使用 Facebook 的資訊性動機上有影響關係。本研究支持 H3-14：親和性人格特質對 Facebook 資訊性動機上有正向影響。顯

示親和性人格特質在對大學生使用 Facebook 的資訊性動機上有影響關係。本研究支持 H3-15：嚴謹性人格特質對Facebook 資訊性動機上有正向影響。顯示嚴謹性人格特質在對大學生使用 Facebook 的資訊性動機上有影響關係。

四、人格特質對 Facebook 遊戲性動機

本研究不支持 H3-16：神經質人格特質對 Facebook 遊戲性動機上沒有正向影響。顯示神經質人格特質在對大學生使用 Facebook 的遊戲性動機上沒有影響關係。本研究支持 H3-17：外向性人格特質對 Facebook 遊戲性動機上有正向影響。顯示外向性人格特質在對大學生使用 Facebook 的遊戲性動機上有影響關係。本研究支持 H3-18：開放性人格特質對 Facebook 遊戲性動機上有正向影響。顯示開放性人格特質在對大學生使用 Facebook 的遊戲性動機上有影響關係。本研究支持 H3-19：親和性人格特質對 Facebook 遊戲性動機上有正向影響。顯示親和性人格特質在對大學生使用 Facebook 的遊戲性動機上有影響關係。本研究支持 H3-20：嚴謹性人格特質對Facebook 遊戲性動機上有正向影響。顯示親和性人格特質在對大學生使用 Facebook 的遊戲性動機上有影響關係。

五、人格特質對 Facebook 娛樂性動機

本研究不支持 H3-21：神經質人格特質對 Facebook 娛樂性動機上沒有正向影響。顯示神經質人格特質在對大學生使用 Facebook 的娛樂性動機上沒有影響關係。本研究支持 H3-22：外向性人格特質對 Facebook 娛樂性動機上有正向影響。顯示外向性人格特質在對大學生使用 Facebook 的娛樂性動機上有影響關係。本研究支持 H3-23：開放性人格特質對 Facebook 娛樂性動機上有正向影響。顯示開放性人格特質在對大學生使用 Facebook 的娛樂性動機上有影響關係。本研究支持 H3-24：親和性人格特質對 Facebook 娛樂性動機上有正向影響。顯示親和性人格特質在對大學生使用 Facebook 的娛樂性動機上有影響關係。本研究支持 H3-25：嚴謹性人格特質對Facebook 娛樂性動機上有正向影響。顯示嚴謹性人格特質在對大學生使用 Facebook 的娛樂性動機上有影響關係。

5 結論與研究建議

5.1 結論

一、五大人格特質變項與人際關係變項之關係

根據研究結果發現神經質人格特質對人際關係無影響關係，而外向性、開放性、親和性、嚴謹性人格特質對人際關係則有顯著的影響關係。由此可知，具神經質人格特質的大學生，其特質並不影響他們在人際關係上的維持建立；而具有外向性、開放性、親和性、嚴謹性等人格特質的大學生，其人格特質在對人際關係的建立和維持有一定的正面影響力。

二、Facebook 使用動機變項對人際關係變項之關係

研究顯示，Facebook 的關係性動機、社交性動機、資訊性動機、遊戲性動機、娛樂性動機對人際關係均具有顯著的影響關係。此結果與以往社群網站及人際關係相關研究結果相同，顯示 Facebook 的使用動機對大學生在人際關係的建立和維持上有正面影響力。

三、五大人格特質變項與 Facebook 使用動機變項之關係

研究顯示，神經質人格特質對 Facebook 關係性動機、社交性動機、資訊性動機、遊戲性動機、娛樂性動機均無顯著影響關係，而外向性、開放性、親和性、嚴謹性人格特質在對 Facebook 關係性動機、社交性動機、資訊性動機、遊戲性動機、娛樂性動機方面，則均有顯著影響關係；結果與以往對於人格特質對社群網站的研究中神經質人格特質喜歡在線上聊天和交朋友、使用塗鴨牆、用即時訊息與朋友聯繫、且個人檔案有較多的個人資料的結果研究不同。因為並不是所有神經質人格特質的大學生都擁有豐富的社會資本和社會網路連結，因此也對自我認同程度的也不盡相同，陳憶菁(2012)指出 Facebook 會讓使用者覺得缺乏隱私、耗時、易受打擾、缺乏真實感。這些負面因素也會使神經質人格特質的人更缺乏安全感，越降使用 Facebook 的動機。

5.2 研究建議

一、研究對象

不同的族群屬性具有不同的特性。本研究針對大專院校學生樣本來做研究，樣本僅代表大專院校學生之調查結果。後續的研究可以擴大研究的群體樣本，對整體做更客觀的探討。

二、量表的使用

本研究所使用的五大人格特質量表、人際關係量表、Facebook 使用動機量表，均採用先前研究者所自編及改編之衡量量表，屬於比較主觀的衡量方式，若能同時運用自評及他評的方式，包含本人、指導人員及專家的評估，或許能夠有更客觀周延的分析結果。

三、地區的選擇

本研究探討地區為台灣地區，因此無法判斷是否在不同文化習俗的地區間也會有所差異。

四、社群網站的選擇

社群網站在不同地區的受歡迎及流行的程度都不盡相同。雖然 Facebook 算是目前最流行通用的社群網站，但在某些網路較封閉的地區就幾乎是被禁止的使用的，因此並無法單用 Facebook 來衡量其他地區的情況。

[1] 財團法人台灣網路資訊中心(2012 年 7 月 9 日)。台灣寬頻網路使用調查。取自 http://www.twnic.net.tw/download/200307/20120709c.pdf。

[2] Costa, P. T., Jr. & McCrae, R. R. (1992). NEO-PIR: Prpfessional Manual,FL:Psychological Assessment Resources.

[3] 潘菲(1992)，論青少年的人際關係，共同學科期刊，2，pp.109-120。

[4] 陳憶菁(2012)。社交網絡服務網站的使用者動機與負面評論之研究－以 Facebook 為例(碩士論文)。國立彰化師範大學企業管理學系，彰化市。

[5] Lindgren, H. C., (1953), “Psychology of personal and social adjustment”, New York:American Book Company.

[6] 石文宜(2005)。國中生人格特質、師生互動關係與偏差行為之關係(碩士論文)。國立政治大學教育研究所碩士論文，台北市。

[7] 陳嫿竹(2002)。網路與真實人際關係、人格特質及幸福感之相關研究(碩士論文)。屏東師範學院教育與輔導研究所，屏東市。

[8] 王汝潔、張斐媄、楊依姍、楊宜蓁(2013)。以社群網站為例探討人格特質、社群網路使用態度、人際關係對社群意識與社群忠誠度之影響。正修科技大學企業管理系，高雄市。

[9] Asendorpf, J. B., & Wilpers, S. (1998). Personality effects on social.

[10] Wilkinson, R.B.& Walford, W.A. (2001). Attachment and personality in the psychological health of adolescents. Personality and Individual Differences, 31, pp.473-484.

[11] 林淳蔭(2010)。高中生社群網站使用行為與現實人際互動、學習風格之相關研究-以台北縣市為例(未出版之碩士論文)。淡江大學，新北市。

[12] 蔣孟軒(2012)。社群網站對人際關係影響之調查研究(碩士論文)。中華大學科技管理學系碩士論文，新竹市。

[13] 李柔萱、林玉容、韓彥卉(2012)。探討 Facebook 對中學生人際關係之影響。海青高級工商職業學校，高雄市。

[14] Amichai-Hamburger, Y., & Vinitzky, G. (2010), Social network use and personality, Computers in Human Behavior, 26. pp.1289-1295.

[15] Ross, C., Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G., & Orr, R. R. (2009). "Personality and motivations associated with Facebook use." Computers in Human Behavior, 25(2): pp.578-586.

[16] Correa, A.W. Hinsley & H.G. de Zúñiga(2010). Who interacts on the Web? The intersectionof users’ personality and social media use. Computers in Human Behavior 26 , pp.247–253.

[17] Ebeling-Witte, M.L. Frank and D. Lester(2007). Shyness, Internet use, and personality. CyberPsychology and Behavior, 10,pp.713–716.

[18] 劉立仁(2012)。實習生人格特質與工作滿意度之研究-以人際關係為中介變數(碩士論文)。國立中正大學，嘉義縣。

運用社群網路技術之主題式資訊整合服務：以校園社團資訊應用為例

詹孟穎、吳嘉峰、方慕堯、馬尚彬
國立台灣海洋大學資訊工程學系
himeng0130@gmail.com, ktpt1412@hotmail.com.tw, ricky920404@hotmail.com, albert@ntou.edu.tw

摘要

隨著近年來社群網路服務(Social Networking Service)的快速興起，帶給人們許多便利，社群網路儼然成為新一代的主流媒體之一。然而，雖然社群網路分享之資訊量豐富且即時，但社群網路服務之資訊雜亂，使用者不易地瀏覽與搜尋特定主題之資訊。因此，本論文以校園社團資訊分享服務為案例，說明如何基於社群網路資訊達成主題式的資訊分享與加值服務應用。本研究提出之 Clubook 行動應用系統不僅可享有社群網路服務的好處，如資訊分享與取得容易、散佈快速等，亦可以彌補單純運用社群網路分享資訊的缺點，如無法主題式地閱讀與瀏覽資訊、無法便利地搜尋、沒有與其他服務(如行事曆與地圖)整合等問題，讓使用者可以透過 Clubook 系統得到即時有效的校園社團活動資訊，且可容易地調用相關之加值服務。

關鍵詞：社群網路、加值服務、資訊整合、社團資訊

1.緒論

社群網路[1]服務(Social Networking Service)在近年來發展迅速，根據英國在 2010 年的研究指出社群媒體(Social Media)網站的流量已經超越了搜尋引擎的流量，使用者透過社群網路服務吸收各類資訊已成常態[2]，且社群網路服務之涵蓋率已經擴及到全世界 80%以上的線上人口[3]，且根據 APP 分析平台 Flurry [4]之統計數據指出，使用者在使用 App 的時間已經比瀏覽網頁的時間還要長，而在使用 App 的時間中有 30%是花在社群網站上，可見 App 將取代傳統網站，社群網路服務也日漸重要[5]。目前知名的社群網站有 Facebook、Twitter、LinkedIn 等，都擁有上億的活躍用戶[3]，顯示在數位化時代的趨勢下，社群網路已經成為主要的溝通工具[6]。社群網路是將實體社會中團體、社區的概念延伸到虛擬的網路上，讓人們可以在社群網站上依據不同的需求成立不同的團體，藉此達到與他人產生互動、情感維繫[7]以及得到更多資訊[8]的需求。然而，雖然社群網路上有各式各樣的豐富且大量資訊，但是其資訊雜亂、不易主題式的去歸納、瀏覽與搜尋資訊，往往使得人們也得花費相當的時間去篩選自己所需的資訊，再由使用者自行將這些片段的資訊拼湊起來，在使用上極為不便。

延續上述觀點，本研究認為若能在 App 的開發架構中適度地將社群網路服務之概念與日常所需的資訊系統做結合，並加以歸納分類，讓使用者可以主題式的獲取其相關資訊[9]，不僅利於宣傳資訊，亦可大幅提昇應用系統之使用便利性，且可享有社群網路服務既有的優點[10][11]。緣此，本論文將介紹本團隊開發之校園社團資訊整合應用系統: Clubook，並藉由此來探討如何在行動應用程式(Mobile App)中有效的以社群網路服務技術為基礎，結合其他的 Web API，以提供一個主題式的整合服務平台。Clubook 不僅僅提供一個社團的資訊系統不可或缺的基本功能，如查詢社團資訊(包括創社時間、社團成立宗旨等等)、查詢社團活動資訊等，亦結合最被廣為使用的社群網站：Facebook [12]，以透過社群網路功能提昇系統之使用性。此外，如前所述，Clubook 更融合日常所需的資訊服務，加入

了地理資訊(Google Map)查詢、行事曆登記、以及活動提醒等功能，使其與社團各項搜尋做結合，如可以搜尋特定區段內所有社團或關注社團的活動資訊、搜尋各項活動資訊後跟行事曆功能搭配進而達到活動提醒效果、透過社群網站的人際關係突顯使用者較有興趣的資訊等，讓使用者可以透過此系統得到即時有效的便捷資訊，滿足使用者之需求。

本論文接下來之章節安排如下，第二章詳述本研究所提出之研究方法與架構，第三章說明Clubook之實作結果，第四章提出結論。

2.研究方法與架構

在此章節本研究將詳述本系統之研究方法，分為系統操作概念與系統架構來進行說明。

2.1 系統操作概念

目前大多數相關的服務或系統，其功能都是片段的，但使用者的需求往往無法靠著單一功能來滿足。就校園社團資訊服務而言，使用者所需的功能包含(1)瞭解關注的社團近期舉辦哪些活動、(2)能清楚知道社團活動舉辦的所在地、(3)能有方便的介面邀請朋友去參加活動、(4)在活動將至時能適時的提醒等，其牽涉的資訊與服務相當煩雜，在目前的環境下，使用者必須完成先搜尋其有興趣的社團(搜尋個別的社團網站或社群網站的社團專頁)、搜尋其社團的活動內容(網站內搜尋或直接瀏覽社團專業)、邀請志同道合的人一同參加(透過e-mail或社群網路服務之邀請功能)、搜尋活動地點之地圖(透過Google Map搜尋地點)、再設置活動提醒(透過行事曆之提醒服務)，使用者必須自行分開處理這些問題，且由於缺乏主題式的整合式服務，其操作過程可能非常繁瑣且費時，不僅對於使用者不易使用，對於校園社團管理者而言社團活動也不易推廣。

因此，本系統將校園社團資訊透過結合社群網路服務(Social Networking Service)[6]以及其他的Web API進行主題式的服務整合，讓使用者得以在一個應用平台上輕鬆瀏覽其喜好的社團資訊，並提供完整的搜尋系統供其查看所有活動詳細內容、查看有哪些朋友[13]也在關注此項活動、將關注活動設定為行事曆提醒，並可讓使用者搜尋在某個特定區域上有哪些活動即將舉辦或曾經舉辦，且能指引使用者如何抵達活動所在地，達成適地性服務(Location-Based Services, LBS) [14]之目標。除此之外，本系統亦允許社團的管理者可以透過此系統建立活動，並分享至Facebook平台，邀請朋友一起參加社團活動、一起按讚和分享活動的資訊與評論。本研究以社群網路的概念與技術將這些功能整合成一個應用平台的服務，透過結合現今最熱門的社群平台，使用者可以直接享用平常在社群網站的功能，並以更多元的方式滿足使用者的需求[9]。

使用者預設以Facebook帳號登入Clubook系統，登入後會顯示其為一般使用者或是社團管理者，使用者可以搜尋查閱各社團的詳細資訊，在各個社團活動裡可以查閱到有哪些使用者已關注此項活動，系統會特別標註關注者中哪些是使用者的朋友[9]，而點選關注者後可以進入此使用者之個人Facebook首頁與其進行互動。若為社團管理者，則可以利用此系統發佈社團活動，活動將可同時分享至Facebook上。此外，透過此系統亦可以在各項社團活動中直接看到Facebook平台上對此項活動的所有評論資訊、按讚(Like)數、按讚的使用者等。換言之，本系統保留Facebook在社交圈中資訊流通的便利性，但透過本系統對於社團資訊系統化的組織與呈現，讓使用者不但可便利地取得社團活動與調用相關服務，亦可以Facebook提升資訊的能見度，且能有效運用Facebook上廣泛被使用的按讚與評論功能。

綜上所述，運用社群網路資訊與技術達成主題式的資訊分享與加值應用為本系統設計的重點，本系統依據使用者平常對社團活動關注的行為模式進行模組設計，並搭配常用的Web API來達到加值應用的效果。以一般使用者的觀點，Clubook中社團活動之生命週期如圖1所示，首先使用者透過Clubook可透過瀏覽熱門社團清單或所有社團列表

去挑選有興趣的社團，且可對興趣之社團進行關注之設定。在關注的社團中，使用者可挑選有興趣的活動瀏覽其資訊，並可關注個別活動；同時，使用者可邀請朋友共同關注此活動(Clubook 透過 Facebook API 達成)或設置活動提醒(Clubook 透過 Android 的行事曆 API 達成)。到了活動舉辦時間，Clubook 會主動提醒使用者，使用者可透過路線指引(Clubook 透過 Google Map API 達成)前往活動現場參與活動。而在活動進行過程中或活動結束後，使用者可針對此社團活動發表感想或評論(Clubook 透過 Facebook API 達成)，亦可發佈此活動的照片或影片。

以在關注活動後將活動設定於行事曆中達到提醒的功能以及可以明確的知道其活動地點方位並該如何前往等；在使用者認證模組裡，本研究結合 Facebook 的登入系統，以 Facebook 帳號作為此系統的登入條件；在行事曆提醒模組裡，本研究搭配了 Android 的行事曆 API，方便使用者可以隨時查閱行事曆，而不用額外執行程式；在 Facebook 功能模組裡，本研究使用了其社群主要的五大功能，包含:評論活動、邀請朋友、取得關注朋友、分享活動以及查看活動按讚數，讓使用者可以充分的利用 Facebook 的社群功能；在社團活動發佈模組裡，本研究搭配了 Facebook 功能模組及 Google map 的功能，在發佈活動時，管理者可以藉由 Google map 功能得知活動地點是否便於前往，提供管理者辦活動的參考，此外，活動發佈的資訊不僅僅存入後端之活動資訊資料庫，同時也分享於 Facebook 平台，藉此，可以有效地透過社群網路來宣傳社團活動資訊。

圖 1 社團活動關注週期圖

2.2 系統軟體架構

在系統之架構設計上(如圖 2 所示)，本系統將模組主要分為社團活動搜尋模組、社團活動擷取模組、使用者認證模組、行事曆提醒模組和 Facebook 功能模組、社團活動發佈模組等模組。在社團活動搜尋模組裡，本研究將所有活動依據活動的主題、日期以及活動關注人數做主題式的歸納，其中活動關注人數更結合了 Facebook 功能模組，讓使用者可以看到所有在 Facebook 的朋友所關注的活動，亦可邀請好友關注此活動，甚至也可以搜尋特定區段內的所有社團或關注社團的活動，進而滿足使用者蒐尋資訊的需求；在社團活動擷取模組裡，本研究除了顯示其活動的詳細資訊外，更結合了 Facebook 功能模組、行事曆提醒模組及 Google Map 的功能，讓使用者可以在本系統中也可以取得此活動在 Facebook 平台中所發表的文章資訊並進行評論、可

圖 2 系統架構圖

3.實作成果

根據上述之操作概念與系統架構，本研究團隊已開發完成此行動應用程式：Clubook，並已將其發佈至 App 平台上[1]。在實作成果上，本系統依據各種統計數據進行主題式的校園社團推薦(如圖 3)，包含熱門社團與熱門活動，並提供更詳盡的排名解說(如圖 4)供使用者參考。若使用者已有透過 Facebook 登入，則在"你可能有興趣"的功能中，Clubook 會根據此使用者其朋友的社團關注紀錄，推薦較多朋友有興趣的社團給使用者；若未登入，則直接隨機推薦社團給使用者。在"我的社團"功能中，則結合了社群平台 Facebook 的登入功能，會先要求使用者進行登入再進行關注的設定，登入後在首頁的部分會出現使用者名稱，若為社團管理者則會多一項"發佈活動"的功能(如圖 5)，而在"我的社團"裡也可以進行管理關注社團和行事曆管理的功能(如圖 6)。



圖 3 社團推薦種類

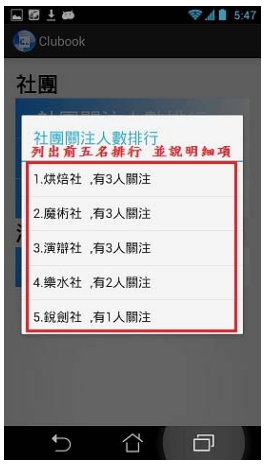


圖 4 社團關注排名

Clubook 的"管理關注社團"功能中，本研究提供一般的社團排序、依好友關注數排列、依所有人關注數排列(如圖 7)，讓使用者依照其喜好模式來進行排序挑選，確定後即會顯示在"我的社團"頁的列表上(如圖 6)。在列表中會顯示使用者所選的社團名稱，使用者點選後即會顯示出其各類活動及關注人數，若點選關注人數，則會顯示出此活動的關注者，並將使用者的朋友以藍色背景排列顯示在前(如圖 8)，而點選後便可連到該朋友 Facebook 的個人首頁。



圖 5 首頁登入後情況



圖 6 "我的社團"登入



圖 7 管理社團排序



圖 8 關注清單

在社團活動列表中，若使用者點選活動則會顯示其詳細的活動資訊(如圖 9)，並於下方設置一個"關注"鈕，若按下關注，系統會記錄此系統已關注，且會詢問是否將此活動設訂為需提醒。如果選擇需提醒，則會進入行事曆之提醒功能(如圖 10)，讓使用者自行設定其所需之提醒模式。在此活動資訊中也搭配了 Google Map 系統和 Facebook 平台，若點選活動地點(如台北市台北車站)，則會跳出地圖供使用者參考其方位(如圖 11)，若點選查看 Facebook 貼文，則會顯示其活動在 Facebook 上貼文，使用者可以直接在上面與好友執行按讚、分享活動、評論

[1] Clubook App 可透過 Hami 商城進行下載(網址為: http://apps.emome.net/plaza/softIntro.jsp?id=0300011081)

活動資訊等功能(如圖 12)，這些動作會即時同步到 Facebook 上。除此之外，在社團活動列表中，若使用者長按社團名稱則會顯示該社團的詳細資訊。



圖 9 活動詳情資訊



圖 10 設置行事曆提醒



圖 11 活動地點



圖 12 活動貼文

在關注活動後，使用者可以按"查閱行事曆"功能，即會顯示內建行事曆，裡面除了關注的活動也包含日常的活動資訊(如圖 13)，假如使用者只想單純查看他曾經關注哪些活動，就可以按"查看我的活動列表"便會進入關注活動的所有清單(如圖 14)。

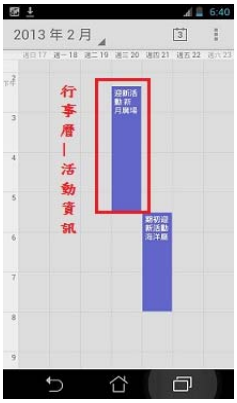


圖 13 行事曆清單



圖 14 個人活動清單

除了上述功能之外，本研究也特別為社團管理者設計"發佈活動"的服務，除了一般的選單發佈功能外(如圖 15)，也整合了 Facebook 平台和 Google Map 的功能，如果活動地點是在校外的話，就會切換至 Google Map 搜尋頁，讓管理者輸入地址並回傳(如圖 16)，在確認發佈後，則會將此活動資訊上傳並分享至 Facebook 平台(如圖 17)，讓管理者不需額外登入社群網路發佈活動，而可以直接藉由此系統達成活動資訊宣傳之功效(如圖 18)。此功能可讓使用者不管透過 Clubook App 或 Facebook 都可看到此社團資訊，雙管齊下將活動資訊宣傳發揮到最大效益。



圖 15 活動發佈表



圖 16 選擇地點地圖



圖 17 發佈至 Facebook



圖 18 Facebook 活動資訊

4.結論

本團隊所開發之 Clubook App 不僅提供一般社團服務應有的基礎功能，亦透過社群網路資訊達成主題式的資訊分享與加值服務應用。本系統藉由分析使用者的社團活動關注之生命週期，設計出符

合使用者需求的系統，並加上有系統的搜尋、Google Map地圖、行事曆提醒以及社群網路的概念與技術，不只便於使用者進行任何社團活動的搜尋，更打破傳統網路宣傳的方式，讓社團管理者可以更輕鬆地宣傳、管理社團活動。此外，本系統亦提供一個透過社群網路服務技術達成主題式的資訊分享與加值應用之參考範例。根據本系統之服務整合模式，可在社群網路架構上加上主題式的資訊分析和應用，可有效提升社群網路資訊之價值，達成一加一大於二的效果。

本研究未來希望能夠以 Clubook 為基礎，建構隨插即用(Plug and Play)的服務元件管理功能，日後若有任何新的服務需整合至既有平台上，應可透過變更設定的方式直接將新功能嵌入既有的平台中，以達成提升系統可擴充性(extensibility)之目標。

5.參考文獻

[1] D. M. Boyd and N. B. Ellison, “Social Network Sites: Definition, History, and Scholarship,” October 2007. Available: http://www.postgradolinguistica.ucv.cl/dev/documentos/90,889,Social_network_boyd_2007.pdf

[2] M. Dascalu, C. Delcea and L. Dascalu,“A Survey on Innovative Knowledge Creation Methods in Enterprise Environments,” The 34th ARA Congress Scientific Research – Security – Sustainaible Development Connections, Bucharest, Romania, pp. 220-224, May 2010.

[3] 數位策略編輯室, “你必須要知道社群網路的十件事(上) ,” December 22 2011, Available: http://www.socialnetwork.tw

[4] C. Newark-French , “Mobile App Usage Further Dominates Web ,Spurred by Facebook,” Jan 09 2012. Available: http://blog.flurry.com/bid/80241/mobile-app-usage-further-dominates-web-spurred-by-facebook

[5] K. Purcell, L. Rainie, T. Rosenstiel and A. Mitchell, “How mobile devices are changing community information environments,” Mar 14, 2011. Available: http://www.pewinternet.com/~/media/Files/Reports/2011/PIP-Local%20mobile%20survey.pdf

[6] 數位策略編輯室, “你必須要知道社群網路的十件事(下) ,” January 03 2012, Available: http://www.socialnetwork.tw

[7] H. Y. Tseng and P. T. Yeh , “Web community analysis structure: The case of Facebook,” 2010. Available: http://www.tais.org.tw/2010/pdf/1/4.pdf

[8] N Park, K. F. Kee and S. Valenzuela, M.A, “Being Immersed in Social Networking Environment: Facebook Groups, Uses and Gratifications, and Social Outcomes,” Number 6, 2009. Available: https://www1.chapman.edu/~kee/PDF/P04.pdf

[9] L. LICĂ, “Mobile and Social: Ten Best Practices for Designing Mobile Applications,” 2010. Available:http://revistaie.ase.ro/content/55/1005%20-%20Liviu%20Lica.pdf

[10] D. Cosmato , “Advantages and Disadvantages of Social Network,” Available: http ://socialnetworking.lovetoknow.com/ Advantages_and_Disadvantages_of_Social_Networking

[11] S. Valenzuela, N. Park and K. F. Kee , “Is There Social Capital in a Social NetworkSite ? Facebook Use and College Students’ Life Satisfaction, Trust, and Participation,” July 2009.

[12] Kevin Lewisa, Jason Kaufmana, Marco Gonzaleza, Andreas Wimmerb and Nicholas Christakisa , “Tastes, ties, and time: A new social network dataset using Facebook.com,” October 2008 . Available: http://www.sciencedirect.com/science/article/pii/S0378873308000385

[13] Ellison, N. B., Steinfield, C. and Lampe, C. **, “** The benefits of Facebook "friends:" Social capital and college students' use of online social network sites**,”** Journal of Computer-Mediated Communication, 12(4), 2007,Available: http://jcmc.indiana.edu/vol12/issue4/ellison.html

[14] N. Belloni, L.E. Holmquist and J. Tholander, “See you on the subway: exploring mobile social software,” Proceedings of the 27th international conference extended abstracts on Human factors in computing systems table of contents, Boston, MA, USA, pp. 4543-4548, 2009.

腦波儀研究在各領域之應用

陳昆顯　何淑君
高師大資訊教育所
flyonluck0102@gmail.com
sch@nknu.edu.tw

摘要

近年來腦波儀(EEG)應用在各學術領域及現實生活中的相關研究越見顯學，因此本研究之目的乃希望能將腦波研究進行分門別類的整理，並提供欲投入腦波儀研究者之參考及研究方向。本研究先按照「腦波發生位置」、「BCI 相關」，以及「常見腦波」來進行文獻收集，並依據 SJR 的排名，盡量保留評價最高等級（Q1）的文獻，再進行資料分析。研究發現文獻中依據腦波分析方式，可分類出三大類：「直接觀察型」、「線性分析型」以及「非線性分析型」;另外，若根據「應用領域」則可分類出四大領域：「醫學」、「商學」、「心理學」以及「腦機介面」。研究顯示腦波在腦部四大葉產生的狀況都有所不同，且較少應用在商業以及藝術方面。加上研究方向也比較傾向於研究腦波的成因，而少有利用腦波改善實際生活的研究，且腦波結合科技的應用雖是潮流但研究數量也仍有偏少。因此，在結論建議方面，未來腦波研究可以試著朝向商業以及藝術領域發展。此外，也可利用刺激誘發腦波的技術來引起各種基本能力需求的腦電波，以改善生活，如睡眠、專注。當然，結合科技應用的 BCI，一直是重要且值得延續的課題。

關鍵詞：腦電圖、腦波儀、事件相關電位、腦機介面、文獻回顧法。

1. 前言

自從漢斯柏格（Berger, Hans）於 1929 年發表了腦波圖，腦波研究開始它的輝煌時期。在這麼多種研究中，卻沒有專門的文獻研究針對現在已有的腦波研究進行統整並加以分門別類，在開發出不同於以往的創新研究方面也無相關發展。綜合以上所述，可見腦波研究是現今研究的重大議題，而針對其研究發展出一套完整的分類架構，並開發出不同以往新的研究方向，確有其必要性。

本研究的目的主要有二:

一、針對 EEG 的文獻提供一個分類架構並進行分析及意義說明，以了解各學術領域目前運用腦波圖的成效。

二、提供未來欲投入腦波相關研究者之參考，以及研究方向。

2. 文獻探討

2.1 腦波圖(Electroencephalogram, EEG)

腦波儀的種類多樣，根據連結方式可分為 32 頻道腦波儀、64 頻道腦波儀、128 頻道腦波儀以及不需要連接線的無線腦波儀等。然而無論種類為何，其最終目的都是為了要進行腦波測量以及分析。腦波研究開端於 19 世紀末，當時德國生理學家漢斯柏格（Berger, Hans）觀察到電鰻身上發出電波，讓他猜測人類身上也會有相同的現象；1929 年，柏格首次在人類的頭蓋骨上記錄相同的電波活動，這是人類史上第一次發表腦波記錄，命名為「腦波圖」（electroencephalogram:EEG），他不僅發現了腦波圖，也描述了各種腦波。他還描述了形態各異的腦波圖，如癲癇、創傷和各種病理腫瘤。腦波圖是記錄大腦頭皮上的電流活動，方法為在頭皮上放置電極，記錄或在特殊情況皮質的神經生理測量，所導致的痕跡稱之，而某兩點電位差隨時間的變化圖，通常以微伏（百萬分之一伏特）為單位。

2.2 事件相關電位(Event-Related Potential, ERP)

被所欲探討的刺激(或稱為事件)所引發的正負電壓可以稱為「峰」、「波」或是「成分」，而這些峰值出現的時機只跟某特定事件相關，則此電位就被稱為事件相關電位（Event-Related Potential:ERP）。也有人將其翻譯成為刺激誘發電位，一般的腦波圖記錄不到，需將腦波圖經由平均（average）萃取才能得到[1]。其命名方式多樣，如根據其峰值與相應事件的時間（又稱為事件「潛伏期」）關係取名，如 P100、N100、P300、N400、P600 等。也可根據其峰值的序列性，簡言之即刺激誘發的顯著成分順序，如第一個出現就稱為 P1、N1，第三個出現就稱為 P3、N3 等。除此之外，也有特地為了凸顯其本身的特殊性或是具體研究對象關係的命名法，例如根據其物理屬性，會在 P300 後出現的所有正成分都被稱為晚期正成分（Late Positive Component:LPC），或是在選擇性注意事件中觀察到的，被非注意刺激所誘發的腦電負成分則稱為失匹配負波（MisMatch Negativity:MMN）。又如 N2pc 是根據其特色而命名，其中 N2 表示第二負偏轉，通常為 200ms，”pc”是指後部對側（posterior-contralateral）等等。而由眼睛注視所誘

發的電位，稱為視覺誘發電位;由聽覺所引發的電位，稱為聽覺誘發電位;又由姿勢體態所誘發的電位，稱為體態誘發電位。

2.3 腦機介面 (Brain-Computer Interface, BCI)：

腦機介面 BCI，也有人稱直接神經介面，或人機介面 MMI(mind-machine interface)，是一種大腦與機器直接通信的途徑。首次期刊提出是在 1973 年[2]。一開始主要在恢復聽覺、視覺以及觸覺的應用[3]，陸續在其他領域嶄露頭角。腦機介面有許多種，有直接將電極植入視覺皮層以改善視力的侵入式 BCI，或將設備植入顱骨內，而不在灰質外腦的部分侵入式，以及不需侵入人體的非侵入式。其中腦波圖是非侵入式中最普遍拿來應用在 BCI，因其具有良好的時間解析度、易用性、便攜性和相對低廉的價格等優點。其方法主要是利用生物訊號放大器透過腦波感應器取得使用者的腦波圖案，並經由小波分析特徵化轉譯成特別的指令，與實體環境溝通。

3. 資料分析

本研究方法主要採用非介入性文獻回顧研究中的次級資料分析法來進行研究。而本研究文獻收集主要按四步驟依序進行。第一步：在 SDOL 資料庫中，以腦波圖的英文縮寫「EEG」為關鍵字搜尋所得文獻為母群體。第二步：再從這些母群體中，以英文關鍵字：腦波發生位置—「Frontal Lobe」、「Occipital Lobe」、「Temporal Lobe」、「Parietal Lobe」、常見腦波—「α」、「β」、「θ」、「δ」或腦機介面—「BCI」等篩選出文獻。第三步：從第二步中所得的資料，再依據「可判斷發表起源」或「應用不同領域」去篩選出相關文獻。第四步：最後再依據 SJR，把排名最低，評價較差的期刊論文排除，因受限於篇幅，本文僅從評價最高的 Q1 級別中的期刊先選出 31 篇相關文獻，另為了增加文獻的多樣化，也在 Q2、Q3 中分別挑選了 8 篇以及 3 篇研究方向差異較大的文獻進行統整比較。也因此文獻收集的第四步驟是相當必要且重要的，因為藉由 SJR 的評比，可知本研究大多數的文獻均屬於 Q1 級別，由這些評價高且令人信服的文獻中所獲得的結論，會是較具代表性的。今依據關鍵字「腦波發生位置」、「腦機介面」、「常見腦波」將所收集的文獻資料區分為三大類，結果分析描述如下：

3.1 腦部四大葉，額葉（Frontal Lobe）、頂葉(Parietal Lobe)、枕葉(Occipital Lobe)以及顳葉(Temporal Lobe)腦波相關研究：

腦部四大葉各司其職，其中額葉主要跟推理、計畫、某些語言與運動（運動皮質）、情緒以及問題解決有關。可以利用左右額葉不對稱的特性來當做一種診斷工具，以探討當顧客看到廣告時，會對產品出現什麼真實反應[4]。有研究分析顯示，高愉快會造成左額葉腦波電位顯著提高[5]。另右額葉明顯跟焦慮有關，如看到可怕的面孔影像，右額葉活躍的程度變大[6]，知足常樂的心情與第二形式的同理心也與左額葉有關[7]。枕葉與視覺有關，著名的 Alpha(α)波也是由此起源[8]，當遇到熟悉面孔時，枕葉部分會引起較多的正600f [9]。顳葉與知覺、聽覺刺激辨識、以及記憶(hippocampus)有關。研究顯示老年人在額葉，顳、頂葉及皮層下大腦地區會比年輕人減少更多的神經反應[10]。此外，熟悉的面孔（不論說謊與否）比陌生的面孔在中間和右側頂葉和顳葉區域會引起較少顯著的N400f [9]。最後是頂葉，其與觸覺，壓力，溫度以及疼痛有關。研究顯示，在決策中會顯示的P300(P3b)，主要就是由頂葉起源。也有研究顯示，將神經科學應用在廣告行銷去測量腦電波時，在額葉、顳葉跟枕葉的部位，會有明顯增大，研究結果顯示影響購買餅乾的因素中，餅乾的口味是比餅乾的形狀來得重要[11]。

表 1. 腦部四大葉研究彙整

主題	功能	腦波相關研究貢獻	篇數
額葉	推理、計畫、某些語言與運動(運動皮質)、情緒以及問題解決有關。	1.根據左右額葉不對稱可用來探討顧客看廣告時，對產品的真實反應。 2. 判斷愉快與不愉快。	[4]~[7]，[11]共 5 篇。
枕葉	與視覺有關。	1.Alpha(α)起源。 2.遇到熟悉面孔時，枕葉部分會引起較多的正 600f。	[8][9]，共 2 篇。
顳葉	與知覺、聽覺刺激辨識、以及記憶有關。	老年人比年輕人有較少神經反應。	[10]，共 1 篇。
頂葉	與觸覺，壓力，溫度以及疼痛有關。	1.熟悉面孔引起較少N400f。 2.p300 起源。	[9]，共 1 篇。

3.2 BCI 相關研究：

傳統上有關 BCI 的研究多應用在醫療上，多半在輔助一些肢體殘障的患者。如有研究顯示 BCI 輔助在「通訊和控制」，「電機替代」，「娛樂」，「運動恢復」四方面，可真正幫助並影響到肢體殘障人士[12]。BCI 也被應用在基於穩態視覺誘發電位（Steady State Visual Evoked Potential：SSVEP）的腦驅動機器人或輪椅 [13]。BCI 可利用腦波操作神經義肢，如使用 P300 以及 N2PC 來操作機器手臂[14]，也可幫助耳聾殘疾人士，或配合侵入式 BCI，

以幫助人來視物。不過近年來有越來越多的人開始將 BCI 應用在非醫療的領域上，試著將 BCI 在真實世界中做更有效的應用，如從虛擬鍵盤選擇字母[15]。藉由 P300 進行控制的拼寫設備也有廣泛的研究和開發[16][20][17][18][19]，建立一個藉由 P300 操作的網頁瀏覽器[14][21][22]或互相結合設計出基於 P300 去操作的網頁，同時也框架出一個使用 P300 去執行的拼寫系統 [23]。應用在虛擬環境中，可進行導航[24]、操作虛擬 3D 直升機[25]或利用聽覺誘發電位擔任在虛擬實境中存在的評估指標[26]，利用自發以及誘發腦電波玩遊戲[27]。

為了增進 BCI 的效能，混合 BCI(hybrid BCIs：hBCIs)的系統架構也被提出。如使用事件相關非同步（Event-Related Desynchronization：ERD）和 SSVEPs 操作系統[28]。又如運動想像（motor imagery：MI），這是一個在精神層面中給予一個模擬的動作，讓人以主體感覺去操作，藉此與 SSVEPs 結合，去探討一些離線研究[29]。也因為 BCI 結合腦波有這麼多的發展應用，開始有部分研究探討在使用 BCI 時，腦波圖的變化。又或者有研究發現，因為使用 BCI 需要訓練，如果操作者情緒波動過大，將導致 BCI 無法讀取真正意圖的腦波型態，因而造成操作困難或甚至會有某些危險發生。因此採用共享控制在機器人跟輪椅的技術也隨之而生[30][15][31]。而利用玩遊戲來改善腦功能的嚴肅遊戲，也是研究的重心所在[32]。而既然腦波圖可以識別人類的心理狀態，如疲勞、注意力、認知過程等，因此，有部分 BCI 基於 P300 腦波去設計在人疲憊時，由機器自行掌握控制權，將人送到床上休息等功能。

表 2. BCI 研究彙整

BCI		
主題	研究貢獻	文獻篇數
醫學	1. 神經假肢。 2. 神經遙控機器人跟輪椅。	[12]~[14]，共 3 篇。
網際網路	1. 腦波網頁瀏覽器的製作。 2. 虛擬鍵盤與腦波拼寫系統。 3. 虛擬實境中的導航、操作與評估指標。 4. 玩遊戲。	[15]～[27]，共 13 篇
混合系統	1. RED 結合 SSVEPS。 2. MI 結合 SSVEPS。	[28][29]，共 2 篇。
共享控制	為了避免情緒波動影響腦波操作，於是由機器負責主導操作。	[15][30][31]，共 3 篇。
嚴肅遊戲	結合 BCI 可改善腦功能的遊戲。	[32]，共 1 篇。

3.3 常用腦波：α、β、θ、δ相關研究

3.3.1 Alpha(α)

Alpha(α)波首先是由Karbowski K. Hans Berger於1931年首先提出，神經震盪的頻率範圍為8-14赫茲，主要是由枕葉起源[8]。根據腦波儀與臨床生理學會國際聯盟(International Federation of Societies for Electroencephalography and Clinical Neurophysiology)的定義：Alpha(α)波主要和放鬆的心理狀態連結。因此此波以往都幾乎是有相關於睡眠的研究[33]。有研究顯示，腦波圖可以藉由上α波進行有意義的問題解決，是研究洞察力的判斷標準[34]。有相關研究顯示，心情愉快會跟此波呈現正相關，即越愉快則此波越活躍[5]。在虛擬實境中，觀賞單牆掛式大螢幕的3D虛擬實境，會伴隨著頂葉α波段的增加，即觀察3D影像比觀察2D影像會有較多的α波段產生[35]。此外，現今也有許多研究藉此波與放鬆心理的連結來進行生物反饋訓練活動，如最常用的日冥想，可幫助人克服恐懼，或使過動兒安靜下來，也可利用此波來進行謊言探測器。也有研究專門將Alpha(α)的功能進行整理彙整，以便使人們更輕易去了解其應用[36]。

3.3.2 Beta(β)

根據腦波儀與臨床生理學會國際聯盟，此波頻率為 12Hz 以上，但一般很少高於 50Hz。清醒及警覺時尤其明顯，也是邏輯思考、計算、推理時需要的波，屬於「意識層面」的波。在頂葉部及額葉會較明顯，電位約 20μV。研究顯示，β波的振幅可用來當做警覺性的間接測量指標，當振幅越高，代表警覺性越高[37]。而藉由此波測量數值，代入公式也可作為疲勞檢測的指標[38]。

3.3.3 Theta(θ)

根據腦波儀與臨床生理學會國際聯盟，此波頻率介於 4-8Hz，主要在兒童的頂葉及顳葉會出現，在深睡作夢、深度冥想時特別明顯，屬於「潛意識層面」的波，許多的腦疾病患者，可以找到θ波。一開始此波的發現是歸功於研究海馬（hippocampus）的重要課題[39]，大多研究來自老鼠、貓跟兔子等「海馬 theta 波」，此 theta 波最流行的理論在於與短期記憶鏈結的機制。但因海馬太深層，無法在人體進行植入性研究，此時另一種「人類皮層 thata 波」也隨之被發現探討。研究發現，人類皮層 thata 波其實跟海馬無太大相關。有研究顯示，資優兒童比正常同齡人有顯著較大的δ和θ活動[40]。此波也被用來判別聲音、顏色以及形狀的依據[41]。在廣告行銷方面，發現如果去觀察愉快或不愉快的廣告會分別在左或右半球，增加θ和α活性的不對稱 [5]。θ和 γ 之間的協同效應被認為

是跟認知有關，尤其在聽覺言語幻覺[42]。也有實驗在虛擬實境中研究發現，女性有較高的θ基線，而女性導航性能和θ波的增加成正相關，相對於男性導航性能下降時，θ波卻是增加的。這些結果可能表明女性擁有高於男性的一個強大的感覺整合能力，於是推測皮質θ活動中出現了性別差異[26]。

3.3.4 Delta(δ)

根據腦波儀與臨床生理學會國際聯盟定義，此波頻率介於0.5~4Hz的腦波頻段，在一歲大嬰兒睡眠時，以及有嚴重器官性疾病的患者身上尤其明顯，主要出現在兒童的枕葉部，及成人的額葉部。資優兒童比正常同齡人有顯著較大的δ增量[40]。

今將各常用波相關研究彙整如表3。

表 3. α、β、θ、δ研究彙整

波	特徵	研究貢獻	篇數
α	1. 8-14 Hz。 2.枕葉起源。 3.「意識」與「潛意識」層面。 4.想像力來源	1.放鬆時明顯。 2.日冥想，克服恐懼，安撫過動兒，進行測謊。 3.可用來分辨 3D 與 2D。	[5]、[8]、[34]~[36]，共 5 篇。
β	1.50>β>12(Hz)。 2.意識層面。 3.清醒、警覺時高。 4.在頂葉與額葉會較明顯。	1.當振幅高時，警戒性高，可當做警戒性的測量標準。 2.代入公式，可當做疲勞指標評估。	[37]、[38]，共 2 篇。
θ	1.4~8Hz。 2.頂葉與顳葉出現。 3.潛意識層面。 4.創造力與靈感來源。 5.分為海馬θ跟皮質θ。	1.智力高者顯著。 2.與短期記憶有關 3.可判斷顏色、聲音及形狀。 4.有性別差異。 5.愉快廣告可增加。 6.與認知過程有關。	[5]、[39]~[42]，共 5 篇。
δ	1.4>δ>0.5Hz。 2.無意識層面。	1.在一歲大嬰兒睡眠時，以及有嚴重器官疾病者明顯。資優兒童較多。 2.資優兒童較多。	[40]，共1篇。

4. 研究發現

研究分析顯示，雖然腦波文獻範圍分布既細且廣，但仍可將其依據「腦波圖分析方式」分為三類：

(1) 直接觀察型:一般腦部示波圖，如 Alpha(α)、Beta(β)、Theta(θ)及 Delta(δ)等直接從示波器上直接描繪而成的腦波圖。

(2) 線性分析型：如頻譜圖以及時頻圖，在固定的某頻率內，可找出規律性的 ERP，如 N400、P300、P600 等即為此類。

(3) 非線性分析型：包含利用非線性分析函式來分析腦波圖，或是觀察無固定波段跟特別突出的峰值，但卻可在觀察腦波波型找出規律變化的分析方式。

且又可根據腦波實際「應用領域」相關，將其區分 4 類：

(1) 醫學：本研究收集醫學相關文獻 14.28%(6 篇)。包括醫學診斷、醫學治療，以及醫學輔具。其中醫學治療又包括物理治療跟化學治療，而醫學輔具將結合腦波，所以將其歸類在腦機介面。

(2) 心理學:本研究收集心理學相關文獻 26.19%(11 篇)。主要研究喜怒哀樂等情緒，以及利用腦波改善教育方法的教育心理學，或是測謊的犯罪心理學，甚至進行人際溝通等社會互動的社會心理學方面，均屬此類。

(3) 商學：本研究收集商學相關文獻 4.76%(2 篇)。其主要應用在神經行銷學，可了解顧客看到廣告對產品的真實反應。或是了解顧客對產品真實感興趣的部份，如品牌、價位以及成分等因素。部分可應用於決策方面，藉此用來預測顧客決定。

(4) 腦機介面:本研究收集腦機界面相關文獻 54.77% (23 篇)。主要可分為醫學輔助、網際網路、混合系統以及共享控制四類。

5. 結論

腦波的研究多采多姿，所包含的範圍也既細且廣，而本研究希冀能為未來有意研究腦波者，提供參考以及研究方向。故將本研究所得結論歸納及未來發展建議如下：

(1) 在研究領域方面：由本研究所收集的文獻發現，近代腦波的應用研究相當多樣，但大部分的應用主要都在醫學以及心理學方面。在藝術方面以及商業應用方面，卻無太多相關的文獻，因此若未來能多往這兩方面發展，相信會有更大的貢獻。

(2) 在腦波儀硬體設備方面：腦波儀的類型發展快速，目前已有 32 頻道腦波儀、64 頻道腦波儀、128 頻道腦波儀以及不需要連接線的無線腦波儀。但仍容易受到周遭電磁波的影響，而腦波的讀取正確與否，將影響到後續分析及歸納的重要性，所以如何改善機器讀取腦波訊號的能力，相信在腦科學相關的工業設計上，扮演著重要角色。

(3) 在腦波分析軟體方面：實驗設計的系統架構，腦波分析的方式，建立能更精確分析結果的程

式，也是一研究課題。而結合著名的 data mining（資料探勘），以及專家系統（Expert system），相信在收集分析腦波資訊，應有更大的成就。

(4) 在生活應用方面：腦波雖結合科技，但容易受到周遭環境影響，因此如何讓腦波遙控科技可以凌駕於 wisee 以及體感科技之上，相信也會是科學家未來努力的目標以及方向。

(5) 在腦機介面方面：腦波的應用在腦機介面，可以進行如間腦視物，以及腦波搖控機器，解決通訊問題，技術方面已開始見臻成熟，但昂貴的儀器以及部分機體過大，目前幾乎都以 P300 來進行遙控，因此如何改善機體價格、體積以及找尋更容易刺激操作的腦波，是未來持續努力的重點所在。

(6) 在腦波段歸類分析方面：現今文獻大多以振幅、頻率、波型來進行腦波圖分析。在震盪方面的研究較少。且大多文獻都還是以目前著名的α、β、δ、θ波為研究題材，而這些幾乎都是 20 世紀前即發現且大量應用的波段，即便現今有文獻開始開發其在不同領域上的應用，但基本上都是換湯不換藥，差別性不大，其嶄新的意義性也不多。因此把目標放在找尋大腦其他特定的波段與各領域結合研究，是未來重要的課題。處理一些並未落入特定波段，但可用其他的非線性分析所測得的某些波段範圍，也都可以當做未來研究的課題。因此找尋新興波段以利研究發展其在不同領域上的應用，相信也是指引未來腦波研究的導航目標之一。

6. 參考文獻

[1] T.W. Picton, S. Bentin, P. Berg, E. Donchin, S.A. Hillyard, R. Johnson, JR., G.A. Miller, W. Ritter, D.S. Ruchkin, M.D. Rugg, and M.J. Taylor, "Guidelines for using human event-related potentials to study cognition: Recording standards and publication criteria ," Psychophysiology, vol. 37, pp127–152, 2000.

[2] J.J.Vidal, "Toward direct brain-computer communication," Annual review of biophysics and bioengineering, vol. 2, pp157–80, 1973.

[3] Simon P. Levine, Jane E. Huggins, Spencer L. BeMent, Ramesh K. Kushwaha, Lori A. Schuh, Mitchell M. Rohde, Erasmo A. Passaro, Donald A. Ross, Kost V. Elisevich, and Brien J. Smith, "A direct brain interface based on event-related potentials," IEEE transactions on rehabilitation engineering : a publication of the IEEE Engineering in Medicine and Biology Society, vol. 8, no. 2, pp.180–5, 2000.

[4] R. Ohme, D. Reykowska, D. Wiener, and A. Choromanska, "Application of frontal EEG asymmetry to advertising research," Journal of Economic Psychology, vol.31, no. 5, pp.785-793, 2010.

[5] G. Vecchiato, J. Toppi, L. Astolfi, F. D. V.Fallani, F. Cincotti, D. Mattia, F. Bez, and F. Babiloni, "Spectral EEG frontal asymmetries correlate with the experienced pleasantness of TV commercial advertisements," Med Biol Eng Comput, vol. 49, no. 5, pp.579-583, 2011.

[6] J. Avram, F. R. Baltes, M. Miclea, and A. C. Miu, "Frontal EEG activation asymmetry reflects cognitive biases in anxiety: evidence from an emotional face Stroop task," Appl Psychophysiol Biofeedback, vol. 35, no. 4, pp.285-292, 2010.

[7] Sharee N. Light, James A. Coan, Carolyn Zahn-Waxler, Corrina Frye, H. Hill Goldsmith, and Richard J. Davidson, "Empathy Is Associated With Dynamic Change in Prefrontal Brain Electrical Activity During Positive Emotion in Children," Child Development, vol. 80, no. 4, pp.1210 – 1231, 2009.

[8] S. Palva and J.M. Palva, "New vistas for a-frequency band oscillations."Trends Neurosci, 2007.

[9] D. Sun, C. C. H. Chan, T.M.C.Lee, "Identification and Classification of Facial Familiarity in Directed Lying: An ERP Study," PLoS One, vol. 7, no. 2, e31250, 2012.

[10] G. Juckel, S. Karch, W. Kawohl, V. Kirsch, L. Jager, G. Leicht, J. Lutz, A. Stammel, O. Pogarell,M. Ertl, M. Reiser, U. Hegerl, H.J. Möller, C. Mulert, "Age effects on the P300 potential and the corresponding fMRI BOLD-signal, " NeuroImage, vol. 60, pp.2027–2034, 2012.

[11] R.N. Khushaba, C. Wise, S. Kodagoda, J. Louviere, B. E. Kahn, C. Townsend, "Consumer neuroscience: Assessing the brain response to marketing stimuli using electroencephalogram (EEG) and eye tracking," Expert Systems with Applications, vol. 40, pp.3803–3812, 2013.

[12] J. d. R. Millan, R. Rupp, G. R. Muller-Putz, R. Murray-Smith, C. Giugliemma, M. Tangermann, C. Vidaurre, F. Cincotti, A. Kubler, R. Leeb, C. Neuper, K.R. Muller, and D. Mattia, "Combining brain–computer interfaces and assistive technologies: state-of-the-art and challenges," Frontiers in Neuroscience, Neuroprosthetic, vol. 4 , pp.161, 2010.

[13] P. F. Diez, S.M. Torres Muller, V. A. Mut, E. Laciar, E. Avila, T. F. Bastos-Filho, and M. Sarcinelli-Filho, "Commanding a robotic wheelchair with a high-frequency steady-state visual evoked potential based brain–computer interface," Medical Engineering & Physics, vol. 35, pp.1155– 1164, 2013.

[14] J.L. Sirvent Blasco, E. Ianez, A. Ubeda, and J.M. Azorin, "Visual evoked potential-based brain–machine interface applications to assist disabled people," Expert Systems with Applications, vol. 39, pp.7908–7918, 2012.

[15] J. Williamson, R. Murray-Smith, B. Blankertz, M. Krauledat, and K.-R. Muller, "Designing for uncertain, asymmetric control: interaction design for brain–computer interfaces," Int. J. Hum. Comput. Stud., vol. 67, pp.827–841, 2009.

[16] S. Silvoni, C. Volpato, M. Cavinato, M. Marchetti, K. Priftis, A. Merico, P. Tonin, K. Koutsikos, F. Beverina, and F. Piccione, "P300-based brain–computer interface communication: evaluation and follow-up in amyotrophic lateral sclerosis," Front. Neurosci, vol. 60, no. 3, 2012.

[17] H. Cecotti, "Spelling with non-invasive Brain–Computer Interfaces – Current and future trends," Journal of Physiology – Paris, 105:106–114, 2011.

[18] I. Kathner, C. A. Ruf, E. Pasqualotto, C. Braun, N. Birbaumer, and S. Halder, "A portable auditory P300 brain–computer interface with directional cues," Clinical Neurophysiology, vol 124, pp327–338, 2013.

[19] William Speier , Itzhak Fried, Nader Pouratian, "Improved P300 speller performance using electrocorticography," Clinical Neurophysiology, vol 124, pp1321–1328, 2013.

[20] Bernardo Dal Seno,Matteo Matteucci,and LucaMainardi, "Online Detection of P300 and Error Potentials in a BCI Speller,"Computational Intelligence and Neuroscience. Vol. 2010, Article ID 307254, 5 pages, 2010.

[21] E.M. Mugler, C. A. Ruf, S. Halder, M. Bensch, and A. Kubler, "Design and Implementation of a P300-Based Brain-Computer Interface for Controlling an Internet Browser," IEEE TRANSACTIONS ON NEURAL SYSTEMS AND REHABILITATION ENGINEERING, vol. 18, pp.599-609, 2010.

[22] Mugler, E., Bensch, M., Halder, S., Rosenstiel, W., Bogdan, M., Birbaumer, N., and Kübler, A. " Control of an internet browser using the P300 event-related potential. "Int. J. Bioelectromagn, vol. 10, pp.56–63, 2008.

[23] L. Mayaud, S. Filipe, L. Petegnief, O. Rochecouste, and M. Congedo, "RobustBrain-computer Interface for virtual Keyboard (RoBIK): Project results.," IRBM, vol. 34, pp.131–138, 2013.

[24] R. Ron-Angevin and A. Diaz-Estrella, " Brain–computer interface: Changes in performance using virtual reality techniques.," Neuroscience Letters, vol. 449, pp.123–127, 2009.

[25] A. J. Doud, J. P. Lucas, M. T. Pisansky, and B. He, "Continuous Three-Dimensional Control of a Virtual Helicopter Using a Motor Imagery Based Brain-Computer Interface," PLoS ONE, 6:10, 2010.

[26] S. E. Kober and C. Neuper, "Sex differences in human EEG theta oscillations during spatial navigation in virtual reality," International Journal of Psychophysiology, vol. 79, pp.347–355, 2011.

[27] A. Finke, A. Lenhardt, and H. Ritter, "The MindGame: a P300-based brain–computer interface game," Neural Netw., vol. 22, pp.1329–1333, 2009.

[28] Brendan Z. Allison, Clemens Brunner, Christof Altstatter, Isabella C. Wagner, Sebastian Grissmann, and Christa Neuper, "A hybrid ERD/SSVEP BCI for continuous simultaneous two dimensional cursor control," Journal of Neuroscience Methods, vol. 209, pp.299– 307, 2012.

[29] C. Brunner, B. Z. Allison, D. J. Krusienski, V. Kaiser, G. R. Muller-Putz, C. Neuper, and G. Pfurtscheller, "Improved signal processing approaches in an offline simulation of a hybrid brain–computer interface," J. Neurosci. Methods, vol. 188, pp.165–173, 2010.

[30] F. Galan, M. Nuttin, E. Lew, P. W. Ferrez, G. Vanacker, J. Philips, and J. d. R. Millan, " A brain-actuated wheelchair: asynchronous and non-invasive brain–computer interfaces for continuous control of robots," Clin. Neurophysiol, vol. 119, pp.2159–2169, 2008.

[31] S. J. Luck and S.A. Hillyar, "Electrophysiological correlates of feature analysis during visual search," Psychophysiology, vol. 31, pp.291-308, 1994.

[32] Yunsick Sung, Kyungeun Cho, and Kyhyun Um, " A Development Architecture for Serious Games Using BCI (Brain Computer Interface) Sensors," Sensors, vol. 12, no. 11, pp.15671-15688, 2012.

[33] L. A. Finelli, H. Baumann, A. A. Borbealy and P. AChermann, "Dual Electroenceplalogram markers of human sleep homeostasis: Correlation between Theta activity in waking and slow-wave activity in sleep," Neuroscience, vol. 101, no. 3, pp. 523-529, 2000.

[34] Simone Sandkuhler and Joydeep Bhattacharya, "Deconstructing Insight: EEG Correlates of Insightful Problem Solving," PLoS ONE, Issue 1, 2008.

[35] S. E. Kober, J. Kurzmann, and C. Neuper, "Cortical correlate of spatial presence in 2D and 3D interactive virtual reality:An EEG study," International Journal of Psychophysiology, vol. 83, pp.365–374, 2012.

[36] Olga Bazanova, "Comments for Current Interpretation EEG Alpha Activity: A Review and Analysis," Journal of Behavioral and Brain Science, vol. 2, pp.239-248, 2012.

[37] Laurent Poupard, Richard Sartene, Jean-Christophe Wallet, "Scaling behavior in β-wave amplitude modulation and its relationship to alertness ," Biological Cybernetics, vol. 85, pp. 19-26, 2001.

[38] Budi Thomas, Sara Lala, Peter Fischerb, Evangelos Bekiarisc, "Using EEG spectral components to assess algorithms for detecting fatigue," Expert Systems with Applications, vol. 36, pp.2352-2359, March 2009.

[39] JD Green and A. Arduini, "Hippocampal activity in arousal," J Neurophysiol, vol. 17, no. 6, pp.533–57, 1954.

[40] T. Liu, J. Shi, D. Zhao, and J. Yang, "The event related low frequency activity of highly and average intelligent children," High Ability Studies , vol 19, no 2, pp131-139, 2008.

[41] M.C.M. Bastiaansen, R. Oostenveld, O. Jensen, and P. Hagoort, "I see what you mean: theta power increases are involved in the retrieval of lexical semantic information," Brain Lang, vol. 106, no. 1, pp.15-28, 2008.

[42] Elias Koutsoukos, Elias Angelopoulos, Antonis Maillis, George N. Papadimitriou, Costas Stefanis, "Indication of increased phase coupling between theta and gamma EEG rhythms associated with the experience of auditory verbal hallucinations," Neuroscience Letters, vol. 534, pp.242–245, 2013.

DNA 序列浮水印技術之強化設計

林琨祐　陳建銘　林韓禹　白敦文*
國立臺灣海洋大學資訊工程學系
*twp@mail.ntou.edu.tw

摘要

次世代定序儀大幅度降低定序實驗的難度與花費，隨著資料的大量產出，如何在共享研究資料的同時，保護原研發單位定序的研究成果乃是一個重要的課題。因此本研究提出一套基於比較基因體學的理論基礎且強調具有生物意義的去氧核醣核酸序列浮水印演算法，透過與模式物種基因組序列的比對，系統得以避免將數位浮水印嵌入在具有生物意義的區域上。程式並透過加密演算法、分段嵌入與反方向嵌入等技巧提升浮水應整體的強健性。實驗結果顯示本方法可以透過個人電腦有效率地完成染色體基因序列長度的浮水印加密，而且經過加密之序列具有高度的強健性及容錯能力。本數位浮水印加密技術可以提供生物學家在分享所定序之序列同時提供額外的安全保障。

關鍵詞：DNA 浮水印、Playfair Cipher、資訊安全。

Abstract

With advance development of NGS technologies, challenges and expenses of sequencing experiments are greatly reduced. In the big biological data world, one of the most important issues is how to share sequencing results with preventing the risk of plagiarism. In this research, we proposed a DNA watermarking technique by emphasizing the subject of biological significance. After comparing the target sequence with suitable genome sequences from model species, our proposed system reduced the ratio of embedding watermarks within the biological regulatory elements. The proposed method also applied several techniques including Playfair encryption, segmentation insertion, and dual-direction insertion for increasing the robustness. Experimental results have shown that our proposed methods could be efficiently applied on sequence size at a chromosome-level only by a general personal computer equipment, and the high robustness and fault tolerant ability against random-mutation attacks were also demonstrated by practical applications. The proposed digital DNA watermarking technique provides biologists an extra secure protection layer when sharing their own biological sequence data in public domain.

Keywords: DNA Watermark, Playfair Cipher, information security.

1. 前言

次世代定序儀為生物序列定序技術帶來革命性的進步，使得序列資料目前正以爆炸性的速度累積。隨著序列資料量的成長，其資料所有權的議題也日益重要。除了具有高度商業價值及專利保護的各種基因改造作物(Genetically Modified Organism, GMO)，多樣性的生物序列也因為學術單位的研究成果發表及論文出版而開始有了所有權的爭議及顧慮。原本就預計公開的序列資料，也可能因為序列遭事先的不當使用，而使得原定序者無法得到任何應有的功勞。然而序列本身並不具備原創性，縱使序列遭到剽竊使用也難以申訴。這樣的隱憂，嚴重削弱序列擁有者將所定序的序列資料上傳至公開資料庫或與他人共享資源的動機。縱使各種優秀的演算法可以用於加密序列以達到完整的保護防竊，但是這些加密過的序列可能嚴重破壞原先生物序列的特性，卻也無法再被任何生物資訊工具進行註解分析或施行具有應用價值的實驗驗證，無法發揮巨量序列資料的所有附加價值，甚為可惜。

避免數位資料被剽竊的方法之一，即是為資料加上不可見的浮水印，並透過解密程序來進行資料使用歷程的追蹤及認證。所謂的浮水印，是指透過某些方式隱含特定資訊在原始資料，乍看之下難以察覺，卻可以透過某些特定方法還原回其隱藏資訊的處理方式。相對於常見的加密方式為將原始資料完全隱藏起來的事前預防，浮水印技術則更加適合在內容無法或不願隱藏的狀態下，卻不願被剽竊盜用的事後追蹤[1]。去氧核醣核酸(DNA)浮水印，是一種將資訊隱含在 DNA 序列中，透過特殊的方式編碼並修改部分的核甘酸，藉此追蹤序列的不當使用等資訊。其序列隱含的資訊則可能包含擁有者、作者、定序時間或其他資訊編碼等可以用來驗證原始序列的所有權。DNA 浮水印常被應用於基因改造作物或是人工合成的序列中[2]。其中一個有名的例子，則是由 J. Craig Venter Institute 在 2010 所發表的人工合成基因組細菌，即在四段浮水印 DNA 中，紀錄數十位參與計畫者的姓名、三句名言、甚至包含了一個簡單的網頁。由於 DNA 序列本身的文字字串性質，因此傳統上使用空間域與頻域互相轉換的浮水印技術並不適用於此。目前已發表的浮水印技術如 DNA-Crypt，則是以透過類似傳統影像資料浮水印儲存於最低重要位元(Least

Significant Bit, LSB)的特性，將其資料隱藏在編碼區的第三碼，藉由其蛋白質編碼的同義置換，來放置其隱含資訊[3]。針對透過該種編碼方式將隱含資訊置放於啟動子區域(promoter region)並進行細菌的活體實驗，結果發現加入浮水印在編碼區[4]或是在啟動子區域[5]皆不影響基因功能的正常表現。隨著生物恐怖攻擊事件危機的發生，此類技術更被建議用在具感染特性病原體的相關研究之中[6]。

隨著我國將生技產業視為行政院重點發展產業，產官學界均開始採購次世代定序儀器並投入相關定序研究的今日，可以預見各單位對序列的保全需求將日益加重。因此，本論文的目的即在於提供一套具生物意義的 DNA 序列浮水印演算法，在使用者進行定序實驗後所產出之 DNA 序列中加入隱藏浮水印資訊的同時，並保持不破壞該序列原本可能具有之基因區域、基因調控因子或是生物標記等具有生物意義重要資訊，期能不影響使用者後續進一步的分析與研究。這樣的技術應用可以做為日後序列的原始擁有權認證，杜絕蓄意剽竊他人研究成果的情形。更可以進一步鼓勵產官學界對定序資料成果進行資源共享，提升我國在生技方面的產業競爭力與學術研發能量。

2. 方法與實作

2.1 系統流程圖

本論文提出的方法可分為嵌入浮水印以及擷取浮水印兩個系統模組。在嵌入浮水印的技術，使用者需要定義要加入的浮水印訊息與一個用於加密浮水印訊息的密鑰。在嵌入浮水印的演算法部分又可細分為三個模組：首先，為了保存加入浮水印序列後原始序列具有的生物意義區域，系統針對原始的明文序列進行可能具有生物功能區域的搜尋並標記，再將可能具有功能片段以外的區域定義為容許嵌入人工浮水印序列的區域。其次，為了使隱藏的資訊加入序列中，這些資訊的內容必須以 DNA 的方式包裝。同時，為了使浮水印的內文保持隱密性，以避免被輕易背去除或竄改，系統透過改良的 Playfair 演算法，對浮水印訊息進行加密，令攻擊者在不知道密鑰的情況下，無法得知正確的浮水印內容。最後，則依照上述兩個模組的輸出，由第三個鑲嵌模組進行資訊的嵌入動作，以產生具有浮水印資訊同時又可以盡量保有原生物功能的加密程序。詳細的嵌入浮水印系統流程圖在圖 1 中呈現。

在擷取浮水印資訊的系統模組，其基本原理是加入浮水印程序的反向操作，唯一不同的是先前定義的生物功能區域可以沿用加密過程中所產生的結果，因此不需要重新進行序列搜尋。透過輸入具備生物意義區域的位置清單、使用者所設定的密鑰以及具有加密的浮水印序列，系統將會自動找出原先嵌入訊息的位置，並透過 Playfair 的解密，將原始的浮水印訊息還原，並可同時復原原始未加密的序列。詳細擷取出浮水印的系統流程圖則在圖 2 呈現。

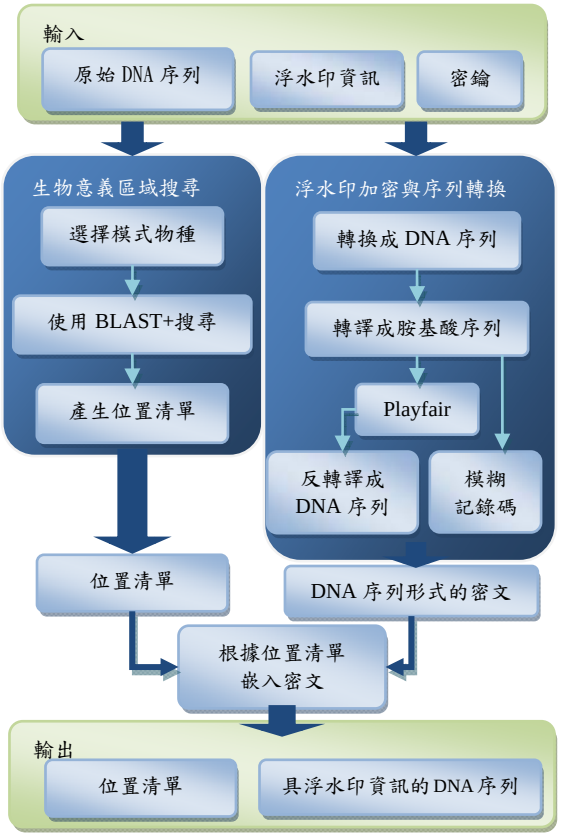


圖 1：嵌入浮水印系統流程圖。

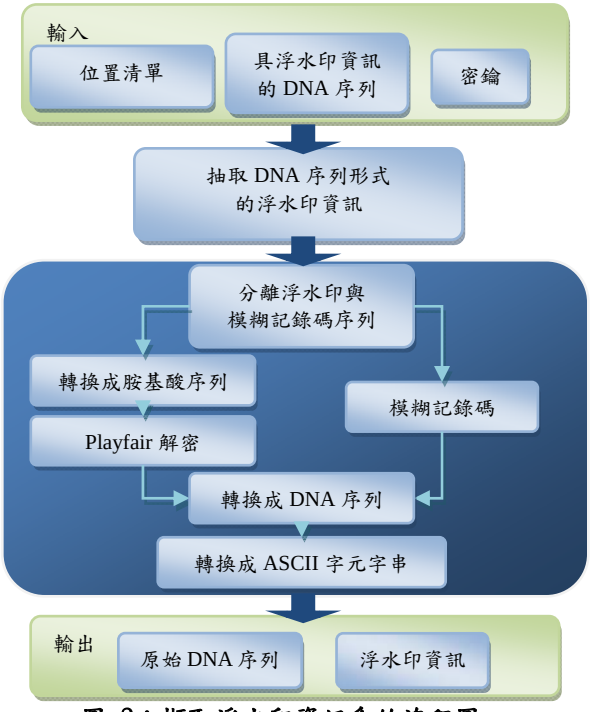


圖 2：擷取浮水印資訊系統流程圖。

2.2 生物意義區域搜尋

為了使加入浮水印的序列依然保留原先可能具備生物意義的區域，使該加密序列依然可以用於比較基因體學、轉錄因子調控分析、親緣演化分析等生物應用，本系統所提出方法的第一步，即是標示可能具有潛在生物意義之調控區域，並將這些區域在浮水印序列的鑲嵌步驟時進行排除。然而，使用者的原始序列可能來自尚未被研究過的新興物種，如何在不具備有任何標註資訊的序列上找出具有生物功能的區域將是第一個挑戰。過去的研究指出，透過跨物種比較生物序列共同保留的部分，可以有效地偵測序列中的調控因子，這也正是比較基因體學的核心概念[7]。因此，本系統將針對使用者輸入的序列，對已知完整序列的模式物種進行相似子序列的比對搜尋，並將所搜尋到的相似子序列標註為可能具有生物意義的區域。在模式物種基因體序列資料的收錄，本研究使用歐洲分子生物實驗室(Ensembl)資料庫中第 72 版的 DNA 序列，該資料庫包含 61 個不同的模式物種，使用者可以依照目標定序物種與已知模式物種的親緣演化關係進行模式物種的選擇。在選定模式物種後，系統使用 BLAST(Basic Local Alignment Search Tool)演算法，進行相似序列區域的比對搜尋。在實作方面，本研究使用由美國國家生物資訊中心 NCBI 所發表的 BLAST+工具組中的 blastn 工具，對模式物種與輸入序列的 DNA 序列進行搜尋[8]。經序列比對搜尋，系統將從 BLAST+的輸出取得一份與模式物種具備相似區域的位置清單，這份位置清單將提供後續浮水印鑲嵌的座標依據。

2.3 浮水印加密與序列轉換

由於 DNA 序列的性質，浮水印資訊需經過一連串的轉換與加密才能嵌入到 DNA 序列。本論文將使用由 Mona Sabry 在 2010 年所發表的基於 Playfair 加密演算法的 DNA 序列訊息轉換方式進行實作[9]。以下先針對該演算法進行精簡的描述。DNA 序列是由 A、T、C、G 四種不同鹼基所構成的字串，可以知道該類字串資料的儲存，每一個鹼基至少需使用兩個位元的資料進行儲存。該演算法首先將浮水印訊息的每個字元根據其 ASCII 編碼，轉換成對應的位元流(bitstream)，再將該位元流中以每兩個位元為基本單位進行取出，並根據表 1 轉換成 DNA 的序列。由表 1 知道前兩個位元的不同組合可以直接代表 A、T、C、G 四種不同鹼基的組合，而其中模糊（Ambiguity）記錄則是為了提供胺基酸序列轉譯回 DNA 序列時、面對一對多情形提供精準反轉譯的依據，模糊記錄詳細的使用時機將在下一節說明。

表 1、位元與模糊記錄碼轉 DNA 表。

第一位元	第二位元	模糊記錄	DNA
0	0	0	A
0	1	1	C
1	0	2	G
1	1	3	T

表 2、修改過具唯一對應特性的 Codon Table。

Codon	模糊記錄			
	0	1	2	3
A	GCT	GCC	GCA	GCG
R	CGT	CGC	CGA	CGG
N	AAT	AAC		
D	GAT	GAC		
C	TGT	TGC		
Q	CAA	CAG		
E	GAA	GAG		
G	GGT	GGC	GGA	GGG
H	CAT	CAC		
I	ATT	ATC	ATA	
B	TAA	TGA	TAG	
U	AGA	AGG		
Z	TAC			
L	CTT	CTC	CTA	CTG
K	AAA	AAG		
M	ATG			
F	TTT	TTC		
P	CCT	CCC	CCA	CCG
S	TCT	TCC	TCA	TCG
T	ACT	ACC	ACA	ACG
W	TGG			
Y	TAT			
V	GTT	GTC	GTA	GTG
O	TTA	TTG		
X	AGT	AGC		

為了使浮水印序列的內容保持隱密性，以避免被惡意使用者可以直接偵測、甚至進一步的竄改所有權資訊，因此對序列使用隱藏式的加密技術是一項必要的步驟。基於生物序列的特性，演算法使用 Playfair 加密演算法作為核心。Playfair 是一種對稱式加密法，其金鑰為 25 個英文字母所構成一個 5*5 的置換矩陣，該矩陣通常可透過任意使用者指定的片語所產生。在加密過程中，將預計要加密的訊息以兩個字元為一組的方式，根據此置換矩陣進行替換。該加密方式除了具有高效率特性外，由於人體內的蛋白質約由 20 餘種不同的胺基酸所組成，因此該加密技術亦十分適合以胺基酸為主的蛋白質序列使用。在該演算法中，所有欲加密的 DNA 序列將會先轉譯成對應的蛋白質序列，並透過 Playfair 加密後，再轉換回原始對應的 DNA 序列。在標準的生物轉譯過程中，DNA 轉譯成蛋白質胺基酸會由三個 DNA 核苷酸轉換為一個胺基酸的規則進行，而不同的核苷酸組合有可能會轉譯到同一種蛋白質胺基酸，因此在進行蛋白質反轉譯過程會發生一對多的模糊(Ambiguity)轉換的問題。為了克服此一問題，演算法透過記錄轉譯蛋白質時所對應的形式

編號進行克服。但是，在自然的脊椎動物蛋白質轉譯表中，可能有多達六個不同 DNA 核苷酸的組合可以轉譯到同一個胺基酸，為了節省浮水印所需要的序列空間，演算法使用一個經過人工修改的特殊編碼表來進行轉譯與反轉譯的唯一對應機制，使其每一個胺基酸對應機制的可能性皆不超過四種組合，如此即可以透過單一一個 DNA 字元進行儲存。表 1 記錄模糊對應編號的轉換位元標示，表 2 則為修改過的編碼表。

2.4 浮水印序列的鑲嵌

在經過前面所述兩個子模組運算之後，進行浮水印加密的最後一步即為加密浮水印序列與原始序列的鑲嵌組合。透過生物意義區域的比對搜尋結果，程式自動避開可能具有生物功能或影響生物功能的區域進行嵌入作業。透過排除由 BLAST 所確認與模式物種高度相似的序列區域，我們可以得到許多分散在序列中與模式物種無法匹配的區段，這些區段被定義為可寫入浮水印資訊的區域。在統計所有可寫入區段的座標位置之後，系統可依寫入區域註解資訊及區域數量平均分為前後兩個部分，如果可寫入區域的總數為奇數，則依照其座標忽略最中間可寫入區段。再針對目標序列的前後兩部份依相反方向及相對應的可寫入區段，進行相同加密內容但方向相反的浮水印密文嵌入動作，如此的設計可以提升加密資訊在目標序列的均勻分布特性並加強序列浮水印的強健性與隱密性。

為了避免惡意使用者透過剪切攻擊，亦即捨棄某一段連續序列的方式來刪除浮水印資訊，本系統對欲加入的浮水印密文進行分段嵌入[10]。首先程式依照序列前半部可寫入區域的正向區段進行統計分析，將浮水印密文序列依照長度平均切割，切割數量選擇與前半部分可寫入區域的數量相同，唯為了避免雜訊攻擊，每一段嵌入的浮水印密文片段不得少於 3 個鹼基，若是無法達到此一標準則減少分段的數量，並放棄部分可寫入區域進行嵌入的過程。當切割完畢後，系統在每一個可寫入區域的起始位置進行密文嵌入。最後針對序列後半部的可寫入區域，以反方向的順序重複進行一遍浮水印密文片段的嵌入，以完成序列加密的所有步驟。最後，系統記錄在嵌入過程所有隱藏在原始序列的座標資訊並輸出至序列擁有者，以提供未來解密或確認之用。

2.5 浮水印序列的擷取與解密

若要針對已加入浮水印的密文序列進行浮水印的擷取與解密，並進一步還原最原始的生物序列，則使用者需要同時輸入密文序列、加密程式所產生嵌入位置清單、以及加密時所設定的密鑰。其解密流程基本上就是加密流程的反向操作，唯解密過程並不需要再透過 BLAST 工具進行生物意義區域搜尋，因此速度可以更有效率。在輸入嵌入位置清單後，系統自動將加密過的密文擷取，並合成一段完整的密文 DNA 序列，此時的序列即為原始不含任何浮水印資訊的明文序列。從密文 DNA 序列中，程式將自動分離反轉譯所需要的模糊序列與用來加密的胺基酸序列編碼；此時，使用者所指定的密鑰可以產生與加密相同的矩陣，並可以透過反向運算進行 Playfair 解密。經 Playfair 解密後，所得到的胺基酸序列可以依照模糊資訊進行 DNA 序列的反轉譯，最後再轉回 ASCII 序列，即可以得到原始的浮水印資訊。最後，上述所有步驟需要針對正向與反向可寫入區域的解碼，同時在不同方向進行兩次解密動作，如此即可得到兩組同步解出的浮水印資訊。

3. 結果與討論

3.1 浮水印序列加密範例展示

表 3、浮水印訊息內容、序列轉換及 DNA 密文展示。

	內容	長度
密鑰	Hello World	10
浮水印資訊	Kyl Good Day 2013-08-1323:00:00	30
DNA 序列	CAGTCTGCCGTACACTCG TTCGTTCGCAAGAACACA CGACCTGCATAGATAAAT ACATATAGTCATAAATGA AGTCATACATATAGAAAT AGATATATGGATAAATAA ATGGATAAATAA	120
密文 DNA 序列	TCTCACTAGATCAGTGTT ACAATTGGTCAGAATAAC TTTCCCTCAATGGATGAA TATAAGTGTGTTTGCAAA TCTGTACAAGAACTTATC TAAAACAGAACTTATCTG TACACATAAGAAGTTATA CAGGTATGTATCTAAAAA GGTATGTATCTAAAAA	160

為了驗證本論文所提出方法的可行性，我們透過 Java 語言進行觀念驗證，該加解密系統是使用單機程式的設計開發。為示範本研究將明文的密鑰與浮水印資訊轉換成 DNA 序列的過程，表 3 顯示一個簡單的密鑰與浮水印資訊，透過前面所述之 Playfair 演算法進行加密的運算。在本範例中，使用的密鑰字串為“Hello World”，而使用的浮水印資訊為“Kyl Good Day 2013-08-1323:00:00”，長度為 30 個字元。表格的第三行為直接透過 ASCII 轉換的 DNA 序列。因為 ASCII 字元是由 8 個位元進行一個字元的表示，而 DNA 每一個鹼基僅有兩個位元的資訊含量，因此從 ASCII 字串轉換成 DNA 序列的話，其長度可預期會成長 4 倍，亦即本範例 30 個字元的浮水印資訊需 120 個 DNA 鹼基字元。表格的第四行為經過 Playfair 加密後的 DNA 序列。經過 Playfair 的方式加密後，因為每 3 個 DNA 就會額

外儲存一個模糊位元的數字，加上 Playfair 演算法中所可能產生的額外空間消耗，因此序列會比單純轉換為 ASCII 字串要來的更長。以本範例來說，密文與明文的長度比率約為 5.3 倍。其實際倍率可能因序列與密鑰內容不同而有所浮動，但是可預見差距不會有過大的情形。

3.2 實際生物序列浮水印應用測試

除了上述所展現演算法細節的範例外，本論文為了展現所提出的方法可以實際應用在真正的生物序列上，實際使用常被生物學家作為研究樣板的模式物種序列進行測試。在本項測試中，我們分別使用稻田魚(Oryzias latipes)與金娃娃(Tetraodon nigrovirdis)的第一條染色體序列，作為輸入的明文序列。此範例是選擇以斑馬魚(Danio rerio)做為比對生物意義區域的模式物種。所有上述的序列皆從 Ensembl FTP 第 72 版下載。

針對這兩條明文序列，我們先與斑馬魚的全基因組序列進行比對，先定義所有可寫入區域的座標資訊。在確認所有可寫入區域後，分別使用兩個長短不同的浮水印訊息進行加解密測試，訊息內容分別是(1) “Tun-Wen Pai” 及(2) “Tun-Wen Pai Department of Computer Science and Engineering National Taiwan Ocean University”。密鑰則為 Hello World。表 4 為詳細測試所需的執行時間與加密序列長度等結果。其中時間的單位一律為秒。本研究所使用的設備為一般個人電腦，詳細的規格：Intel i7-920 中央處理器、6G DDR3 記憶體、 7200 轉 SATA2 硬碟機、及 Eclipse 開發環境進行範例測試。測試結果顯示主要的時間瓶頸仍在於 BLAST 比對過程，但是整體執行時間已證明本方法僅依靠個人電腦等級的硬體，即能夠有效率套用於實際的生物基因組規模序列中。此外，對執行時間的主要影響因素主要是取決於生物序列的總長度，浮水印序列的長度對執行時間僅有小部分的影響。

表 4、實際生物序列長度、可加密區塊數量、及加解密所需電腦計算時間。

		稻田魚	金娃娃
	序列總長度 (bps)	39973033	22983436
	BLAST 所需時間	728.443s	56.170s
	可寫入區域個數	2846	1195
密文 1	**浮水印嵌入長度**	60	60
	浮水印嵌入時間	4.995s	1.421s
	浮水印解密時間	9.609s	5.647s
密文 2	**浮水印嵌入長度**	516	516
	浮水印嵌入時間	4.937s	5.026s
	浮水印解密時間	10.374s	6.146s

3.3 強健性測試

為證明本方法所加入之數位浮水印具備高強度及抗雜訊的特性，本研究更針對前節所述之兩條序列進行強健性測試。在強健性測試中，我們使用前節所使用之序列、浮水印資訊、及相同的密鑰。但是在進行解密前，我們將加密過的序列，以千分之一的機率進行隨機 DNA 字元替換，再測試由前後兩端是否還可以解出浮水印資訊，若是任何一個字元與原來的浮水印資訊不同即為失敗。圖 3 為四組資料的強健性測試結果。從結果可以發現當浮水印序列越長時，由於嵌入序列的長度等比例增加的關係，較容易受到雜訊攻擊的影響。但是即使是在長度達 516 個字元的浮水印序列下，在稻田魚的序列亦保有 90%的召回率，在金娃娃魚的序列亦有 93%的召回率。針對短浮水印資訊的測試狀況下，都可以達到 100%的召回率。從測試結果可以觀察到經由其中一端所提供正確召回的比率極高，證實由本論文所提出之兩端反向進行嵌入加密訊息的方式確實可以有效的提升整體強健性。

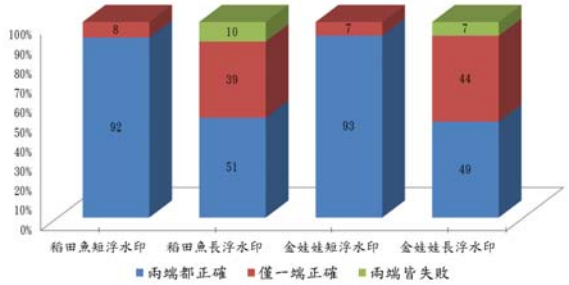


圖 3：強健性測試結果。使用兩組測試序列及兩組不同長度的浮水印訊息內容進行加密測試，對已經加入浮水印的序列中分別隨機插入原長度 1/1000 的隨機突變雜訊。將含有隨機雜訊序列進行解密還原後，以短浮水印訊息加密的序列可以完全被解密及辨識，但嵌入長浮水印訊息及含隨機雜訊的序列則分別有 10%及 7%的辨識失敗率。

4. 結論

本研究提出一個針對 DNA 序列加入浮水印資訊的強化技術。除了應用前人所提出以 DNA 與胺基酸作為基礎的 Playfair Cipher 加密法外，本研究更透過比較基因體學的方式，辨識目標序列與模式物種序列相似區域，進行嵌入浮水印資訊的排除區端參考，便免可能具備生物意義的區域受到浮水印的破壞。此外，本研究更進一步的改良前人的浮水印嵌入技術，透過頭尾兩端反向進行平均分散式密碼嵌入的設計，提升整體加密與解密的強健性及容錯力。透過實驗結果顯示本方法不僅可以在有限的運算資源下以合理的時間套用至全基因組等級的序列，其強健性及容錯能力測試更顯示出該方法可以有效的抵抗隨機突變或是區域整段刪除的攻擊。此方法將可以作為生物學家未來在開放共享自

己研究所產生序列時，可以提供額外的保障，更有機會進一步成為生技產業中用以保護智慧財產的有效依據，以保障相關學術與產業應用的發展。

誌謝

本論文承蒙國立台灣海洋大學海洋中心與行政院國家科學委員會之計畫經費贊助，計畫編號為 NSC 102-2321-B-019 -001，僅此誌謝。

參考文獻

[1] M. Stamp, *Information Security: Principles and Practic*: wiley, 2006.

[2] D. Heider, *et al.*, "Watermarking sexually reproducing diploid organisms," *Bioinformatics*, vol. 24, pp. 1961-2, 2008.

[3] D. Heider and A. Barnekow, "DNA-based watermarks using the DNA-Crypt algorithm," *BMC Bioinformatics*, vol. 8, p. 176, 2007.

[4] D. Heider and A. Barnekow, "DNA watermarks: a proof of concept," *BMC Mol Biol*, vol. 9, p. 40, 2008.

[5] D. Heider, *et al.*, "DNA watermarks in non-coding regulatory sequences," *BMC Res Notes*, vol. 2, p. 125, 2009.

[6] D. C. Jupiter, *et al.*, "DNA watermarking of infectious agents: progress and prospects," *PLoS Pathog*, vol. 6, p. e1000950, 2010.

[7] E. H. Margulies and E. Birney, "Approaches to comparative sequence analysis: towards a functional view of vertebrate genomes," *Nat Rev Genet*, vol. 9, pp. 303-13, Apr 2008.

[8] C. Camacho, *et al.*, "BLAST+: architecture and applications," *BMC Bioinformatics*, vol. 10, p. 421, 2009.

[9] M. Sabry, "A DNA and Amino Acids-Based Implementation of Playfair Cipher," *International Journal of Computer Science and Information Security*, vol. 8, pp. 129-136, 2010.

[10] A. K. Ahmed Atito, S. Z. Rida, "DNA-Based Data Encryption and Hiding Using Playfair and Insertion Techniques," *Journal of Communications and Computer Engineering* vol. 2, pp. 44-49, 2012.

細胞自動機與 RFID 之基因密碼辨識與管理資訊系統 -以 miRNA 為例

林守羿 [1]　蔡孟勳 [1,2]　吳協昌 [1]
[1] 國立中興大學資訊管理研究所
[2] 國立中興大學基因體暨生物資訊學研究所
xup6zeo@gmail.com

摘要

近年來，隨著人們對生物多樣性的重視，世界各地為保存生物的多樣性開始收集各種生物的基因序列，隨著序列的收集增加，許多科學家開始思考著如何資訊化或運用這些基因序列，2003 年，加拿大的學者 Paul Hebert 提出了利用基因序列來當作物種辨識的條碼(DNA barcode)，基因條碼(DNA barcode)提供了一種新的辨識物種方法，相較於過去傳統分類的耗時耗力，基因條碼能更快速的辨識物種，本研究使用 miRNA 序列來做處理基因條碼，經由細胞自動機方法來轉換序列，並將序列轉換成圖像，轉換出的 miRNA 圖像除了可直接藉由肉眼觀察序列間的相同相異部分外，本研究還觀察出調控相同卵巢癌基因的 miRNA 序列有其共通性，未來可將收集這些相關的序列圖形建立資料庫，結合 RFID 與後端的 miRNA 資料庫，形成一基於 RFID 的 miRNA 條碼辨識系統，用在自動的條碼辨識上。

關鍵詞：細胞自動機、基因條碼、miRNA、RFID

1. 緒論

由於人類對基因的解碼，人類開始探討基因的功能及結構，加上世界的上的物種繁多，為了保存生物的多樣性，各國皆開始收集及建立物種的基因序列資料。2003 年，加拿大學者 Paul Hebert 提出了 DNA barcode 的概念[1]，利用 DNA 序列當作物種的辨識條件，將基因序列作為物種分類，以及辨識身分不明或物種之用。然而目前基因條碼的運用範圍，都只是特定種類及固定範圍的小區域分析，而且大部分都是藉由人力來處理資料及分類，一旦需要辨識的物種變多，基因資料量變大，手工分類及檢測將會是緩慢及沒效率的。因此，我們提出一個基於無線射頻辨識(Radio Frequency Identification，RFID)的基因條碼系統，除了能系統化建置基因條碼外，還能快速辨識圖形化基因條碼，不僅能提升辨識及管理基因條碼的效率，且藉由管理化系統資料庫的建立，未來若要將資料運用在分類及比對上，將會更加便利且迅速。

2. 研究方法與架構

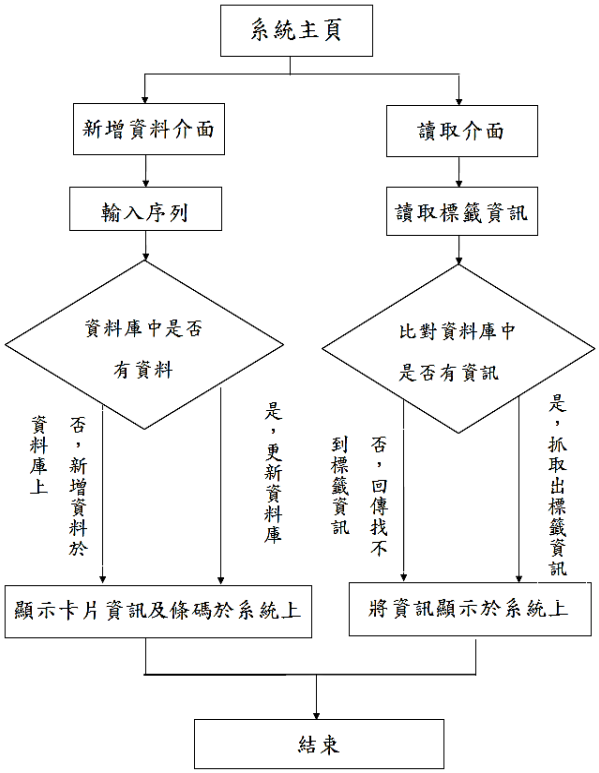


圖 1 系統流程圖

本系統主要分成兩大部分，第一部分是針對 miRNA 的圖像條碼化，將輸入的 miRNA 序列轉換成可處理的資料序列並轉換成圖形，以及把圖形存入到後端資料庫之後並管理。第二部分是系統如何與 RFID 作讀取和寫入的部分，以及和後端的資料庫作比對並將結果輸出至系統畫面上。

2.1 新增資料介面

在新增資料介面中，主要的步驟分成三個，第一步驟是針對 MiRNA 作序列轉換將序列成可以處理的資料序列。第二步驟是對等待處理的資料序列轉換成圖形。第三步則是對於轉換成而的圖形存入 RFID 卡片，並將圖形及相關的序列資訊也存入後端資料庫中，以便之後辨識卡片之用。

2.1.1 輸入序列

目前所常用的基因條碼，主要都是由 DNA 序列或者是蛋白質序列來使用，但是 DNA 序列及蛋白質序列都相當的長(用 DNA 序列來實作的基因條碼約為 650 個字母的長度)，如此大的資料量對於存入 RFID 標籤是一個很大的問題，而且大量的資料也是不利於快速辨識，因此我們選用了長度較短，約為 20 個字母左右的 miRNA 來實作系統。

本研究使用調控影響卵巢癌基因的微核糖核酸(miRNA)來作為輸入序列，除了觀察相同的序列是否會轉換成相同圖形讓肉眼易於觀察外，另外希望能找出圖形化序列是否可以看出原始序列無法看出的共通及相似性，表 1 為影響卵巢癌基因名稱以及調控這些基因的 MiRNA 名稱。

表 1 影響卵巢癌的基因與其調控的 miRNA

影響卵巢癌的基因	miRNA
SMAD2	hsa-miR-142-5p [2] hsa-miR-105 [3]
CCND3	hsa-miR-15a [4] hsa-miR-424 [2] hsa-miR-16 [4,5] hsa-miR-195 [2]
PAPPA	hsa-miR-142-5p [2] hsa-let-7d [3,6,7] hsa-miR-15a [4] hsa-miR-200a [3,5,8,9,10]
MTMR2	hsa-miR-101 [3] hsa-miR-9 [3,11,12]
MAOA	hsa-miR-495 [7]
HELZ	hsa-miR-29a [2,5] hsa-miR-15a [4]
RARHOGAP	hsa-miR-495 [7] hsa-miR-429 [9,10] hsa-miR-15a [4] hsa-miR-424 [2]
PTPN9	hsa-miR-126 [3]
NAP1L1	hsa-miR-495 [7] hsa-let-7d [3,6,7] hsa-miR-657 [2] hsa-let-7c [3,13] hsa-let-7g [13] hsa-miR-9 [3,11,12]
ID2	hsa-miR-381 [2]

2.1.2 序列轉換

在 miRNA 序列輸入後，需要先把它轉換為二進位序列。由於 RNA 序列是由腺嘌呤(A)、鳥嘌呤(G)、胞嘧啶(C)和尿嘧啶(U)所組成[14]，每個基因也都代表著不同意義，為了讓這些基因轉換後還能保有原本意義，並且將來也能藉由系統將資料從二進位序列轉換回來，我們根據表 2，將它們各賦予一個 3 位數的二進位值，如此一來 miRNA 序列將會轉換成一組有意義的二進位序列。

表 2 微型糖核酸編碼表

miRNA	Binary Notation	miRNA	Binary Notation
A	000	U	010
G	100	C	110

2.1.3 細胞自動機生成圖像

當 miRNA 轉換成二進位序列後，之後便是將序列轉換成圖像，本研究所採用的是利用細胞自動機來對序列作轉換，將其轉換成一維的條碼圖像。細胞自動機最初是由 John von Neumann 於 1960 年代提出[15]，細胞自動機是一種離散的動態系統，每一個細胞會根據周圍細胞狀態，更改自己的狀況。細胞自動機可以說是一堆單細胞的集合，而每個細胞在每個時間點只會有一種狀況。

細胞自動機目前主要之應用主要為一維與二維，本研究中使用的是一維細胞自動機[16]來做轉換。

一維細胞自動機是由一組根據時間改變狀態的變數S_i^t組成，i 從 0 開始到 N-1，N 為變數的個數，可以將每一個變數放在一個格子中，這樣的組成就稱為一個細胞；每一個細胞有各自個狀態，在一維細胞自動機中只有將狀態區分為 0 與 1，將 0 與 1 轉換成黑(0)與白(1)。在細胞自動機中，S_0代表一開始的起始狀態，F 表示為細胞自動機之規則，每個細胞會被自己與指定範圍內的鄰居狀態影響，改變下一個時間點之自身狀態。h代表指定的鄰居個數，S_{t+1}^i 為下個時間點的狀態，最後可表示為 $S_{t+1}^i = \mathrm{F}(S_t^{i-h} \ldots S_i^t \ldots S_t^{i+h})$。在本研究中，鄰居個數 h 設為 1，即表示會影響自身下個時間點狀態的細胞為：自己左邊的細胞（鄰居 1）、自己、自己右邊的細胞（鄰居 2）(圖 2)。由於含自己共三個細胞，因此每個細胞會被影響的狀態組合為，每個細胞又都有兩種狀態(0 和 1)，所以總共會有種組合，而每一種組合就是一條細胞自動機之規則。而在本研究中其序列轉換圖形步驟可轉化成下列式子：

$$D_{(i,j)} = F\left[D_{(i-1,j-1)}, D_{(i-1,j)}, D_{(i-1,j+1)}\right]$$
$$If\ 1 \le j < S-1; 1 \le i < S-1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$
$$D_{(i,0)} = F\left[D_{(i-1,s-1)}, D_{(i-1,0)}, D_{(i-1,1)}\right]$$
$$If\ j = 0; 1 \le i < n \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$
$$D_{(i,s-1)} = F\left[D_{(i-1,s-2)}, D_{(i-1,s-1)}, D_{(i-1,0)}\right]$$
$$If\ j = S-1; 1 \le i < n \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

其中，$D_{(i,j)}$表示轉換後該細胞自動機序列陣列之某一(i,j)位置之 0 或 1 之狀態值；i 為選定行數；S 代表該二進位序列之長度；F 為該序列重排演算之規則函數。

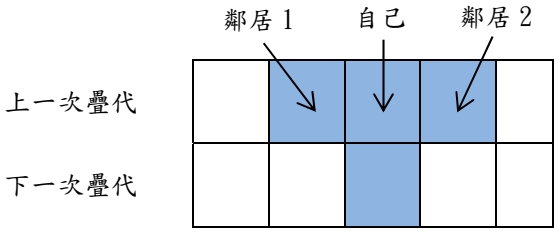


圖 2 疊代示意圖

2.1.4 存入 RFID 標籤與資料庫

將 MiRNA 轉換成圖形之後，系統將會把圖形存入 RFID 標籤及後端資料庫之中，本研究中所存入的 RFID 標籤為 MIFARE 卡，除了存入卡片之外，我們也需將資料寫入資料庫中，本研究所使用的資料庫為微軟的 SQL server 2008 ，因為 SQL server 2008 能與 Microsoft Visual Studio 的專案做快速整合與連結，而且介面淺顯易懂。在本研究實作的資料庫中主要包含幾個欄位，卡片序號(TagID)、miRNA 名稱(NAME)、原始 miRNA 條碼(barcode)、經細胞自動機轉換後的序列圖像(barcodeimage)，並將具有唯一性卡片序號設為 Primary Key。

2.2 RFID 標籤讀取與辨識界面

在處理序列的圖形轉換及 RFID 標籤和資料庫的寫入後，另一個部分便是有關 RFID 標籤讀取的部分，以及如何對後端資料資庫做比對。接下來將會介紹如何實作 RFID 標籤存取以及後端資料庫的比對部分。

在 RFID 標籤抓取資料出來之後，需要辨識 RFID 標籤的內容以及將 RFID 標籤的內容與後端資料庫做比對，來觀察 RFID 標籤資料是否與後端資料庫一致，若是抓出的 RFID 標籤辨識碼與抓出的圖像矩陣與後端資料庫 RFID 標籤辨識碼一致，則顯示出 RFID 標籤的卡號、miRNA 名稱、原始條碼和圖像條碼。整個卡片辨識流程如下：

1. 系統會抓取電腦上所有的外接裝置，找尋 RFID 裝置。

2. 搜尋到裝置後便可選擇與 RFID 裝置連線。

3. 連線後可選擇開始執行程式。

4. 系統會每隔一段就偵測讀卡機上 RFID 標籤內容。

5. 若是讀取到 RFID 標籤則將 RFID 標籤資料抓取出來並與後端資料庫做比對，若是 比對發現資料庫有此資料則將相關資訊呈現在系統介面上，反之，則回傳找不到結果。

6. 按下停止鍵結束搜尋。

3. 實驗結果與討論

3.1 開發環境

本系統使用VB語言撰寫，並使用Visual Studio 2008做為開發工具。另外，為方便處理圖形轉換，本系統後端使用Matlab負責處理條碼圖形的部分，並用SQL server 2008來建立後端資料庫。

3.2 新增修改資料

當進入新增修改資料頁面後，會進入卡片輸入介面。在卡片輸入界面中，一開始需要選擇與電腦連接的 RFID 裝置來啟動連線，當選擇完 RFID 讀取器後便需輸入卡號、miRNA 名稱以及 miRNA 的原始序列條碼，之後選取寫入便可將條碼及資訊寫入資料庫和 RFID 標籤之中。

在卡片的寫入過程中，由於本研究中是將miRNA序列的矩陣圖像存入卡片之中，程式會呼叫Matlab將所需要寫入的序列轉換成圖像，但是在序列轉換成圖像前需先進行二進位序列轉換(圖3)。在轉換成圖像矩陣後，Matlab會將其結果回傳給系統做後續的寫入卡片與資料庫部分。

```
case {'A', 'a'}
    seqBinVec(seqBinVecCount-1) = 0;
    seqBinVec(seqBinVecCount) = 0;
    seqBinVec(seqBinVecCount+1) = 0;
case {'U', 'u'}
    seqBinVec(seqBinVecCount-1) = 0;
    seqBinVec(seqBinVecCount) = 1;
    seqBinVec(seqBinVecCount+1) = 0;
case {'G', 'g'}
    seqBinVec(seqBinVecCount-1) = 1;
    seqBinVec(seqBinVecCount) = 0;
    seqBinVec(seqBinVecCount+1) = 0;
case {'C', 'c'}
    seqBinVec(seqBinVecCount-1) = 1;
    seqBinVec(seqBinVecCount) = 1;
    seqBinVec(seqBinVecCount+1) = 0;
```

圖 3 序列轉換成 2 進位條碼 程式碼片段

當系統接收細胞自動機轉換圖像後，系統會根據RFID標籤的識別碼去搜尋資料庫中是否有RFID的識別碼存在，若是RFID標籤已經存在於資料庫中，系統將會更新資料庫的資料，並更新卡片的資料。資料庫之中沒有讀取到的RFID標籤識別碼資訊，則會將此卡片資訊新增到資料庫之中。

當系統更新完資料庫之後，之後便將圖像寫入RFID標籤之中，當整個程序都完成之後系統會把轉

換出的條碼顯示在系統界面上，表示系統對資料庫及RFID卡片標籤更新完成。

3.3 RFID 標籤辨識

在RFID標籤辨識部分，程式會一直偵測RFID讀取器是否有讀取到卡片，如果有讀取到RFID標籤，會將RFID標籤資訊抓取出來與後端資料庫進行比對，如果後端資料庫有其資料，會將其相關資訊(RFID標籤、miRNA名稱、原始條碼)以及圖形條碼顯示在系統界面上(圖6)，若是後端資料庫找無RFID標籤資訊，則會在系統上顯示找無此miRNA條碼的資訊(圖7)。

3.4 細胞自動機圖形條碼之探討

當序列從字串轉換為二進位數字後，就可以開始將數字序列轉換為圖形，根據指定的細胞自動機之規則進行疊代。所謂細胞自動機的規則由於細胞本身改變後狀態會受到自身改變前狀態(細胞的狀態只有 0 或 1)及改變前左右鄰居的影響，所以三個為一組共有 000、001、010、011、100、101、110、111 這八種狀態，而每一種狀態在改變後都只有 0 或 1 兩種狀態 所以共有 28=256 種組合，意即有 256 種規則，而根據規則不同，轉換後得到的圖形也會不相同。底下的圖為根據 hsa-let-7g-3p 這組 miRNA 序列並搭配不同的規則所轉換得到之圖形。



圖 4 序列 HSA-LET-7G-3P 經規則 2 轉換之圖形



圖 5 序列 HSA-LET-7G-3P 經規則 35 轉換之圖形



圖 6 序列 HSA-LET-7G-3P 經規則 187 轉換之圖形



圖 7 序列 HSA-LET-7G-3P 經規則 230 轉換之圖形

圖 8 序列 HSA-LET-7G-3P 經規則 255 轉換之圖形

由圖 4~圖 8 可知，雖然疊代的規則有 256 種，但是並非各種疊代方式都能有效的表現出各序列的差異，舉例來說，越是後面的規則，由於規則轉換後值為 1 的部分將會越來越多，所以整體的圖像將會偏白，較無法藉由圖像看出序列的差異，反之，越前面的規則在轉換後值為 0 的部分會越來越多，整體圖像會偏黑，也較無法看出圖像間的差異，所以在規則的選擇上需要多加測試。在本研究中經由測試選出了規則 187 來當作鑑別物種的規則，接下來將會使用 187 結果出來的圖形作接續的探討。



圖 9 序列 hsa-miR-142-5p 經規則 187 轉換之圖形



圖 10 序列 hsa-miR-105-3P 經規則 187 轉換之圖形



圖 11 序列 hsa-miR-105-5p 經規則 187 轉換之圖形

hsa-miR-142-5p	cauaaaguagaaagcacuacu
hsa-miR-105-3P	acggauguuugagcaugugcua
hsa-miR-105-5P	ucaaaugcucagacuccuguggu

圖 12 hsa-miR-142-5p、hsa-miR-105-3P、hsa-miR-105-5P 之原始序列

如圖 9、10、11 所示、hsa-miR-142-5p 和 hsa-miR-105是藉由miR2Disease資料庫查詢調控有關卵巢癌基因SMAD2的miRNA基因，由圖可知，這三個調控同樣SMAD2的基因在圖像上在圖像最右下角都有一個點，藉由圖像上可發現到這些圖像的共同點，但是若是由圖12中卻無法看出這三條序列的相同或相異之處。



圖13 序列hsa-miR-15a-3p經規則187轉換之圖形



圖14 序列hsa-miR-15a-5p經規則187轉換之圖形



圖15 序列hsa-miR-429經規則187轉換之圖形

hsa-miR-15a-3p	caggccauauugugcugccuca
hsa-miR-15a-5p	uagcagcacauaaugguuugug
hsa-miR-429	uaauacugucugguaaaaccgu

圖16　hsa-miR-15a-3p、hsa-miR-15a-5p、has-miR-429原始序列

圖13~15是有關調控基因RARHOGAP的相關miRNA序列圖形，而RARHOGAP是被發現影響卵巢癌的基因之一，由圖像中可知，所有的圖像右下角都有點的存在，而從圖16的所有原始序列中，只能觀察各自序列部分的異同之處，但對於全部序列找出異同點則沒有辦法，相較於用序列判斷，用圖像觀察反而能觀察出相似之處。



圖17 序列hsa-miR-15a-3p經規則187轉換之圖形



圖18 序列hsa-miR-15a-5p經規則187轉換之圖形



圖19 序列hsa-miR-142-5p經規則187轉換之圖形

hsa-miR-15a-3p	caggccauauugugcugccuca
hsa-miR-15a-5p	uagcagcacauaaugguuugug
hsa-miR-142-5p	cauaaaguagaaagcacuacu

圖20 hsa-miR-15a-3p、 hsa-miR-15a-5p、hsa-miR-142-5p之原始序列

圖17~19是有關調控基因PAPPA的部分相關miRNA序列圖形，而PAPPA也是有關影響卵巢癌發生率的基因之一，由圖像中可知，所有的圖像右下角如同之前調控卵巢癌相關基因的miRNA一樣，右下角的都有一個點的存在。從圖20之原始序列中，並無法輕易的用肉眼觀察出序列的差異，但是藉由圖像的轉換後，反而能從圖像看出其相同之處。

綜合上述三組有關調控影響卵巢癌基因的圖像可知，原始相同的序列在轉換後會成為相同的圖形，而從結果上來看，我們可以直觀的從肉眼看出序列的相同部分，除此之外，在本研究中所使用的例子，包含影響SMAD2基因的miRNA：hsa-miR-142-5p、hsa-miR-105-3P、hsa-miR-105-5P；影響RARHOGAP基因的miRNA：hsa-miR-495、hsa-miR-429、hsa-miR-15a-5p、hsa-miR-15a-3p、hsa-miR-424-5p、hsa-miR-424-3p：影響PAPPA基因的miRNA：hsa-miR-142-5p、hsa-let-7d-5p、hsa-let-7d-3p、hsa-miR-15a-5p、hsa-miR-15a-3p、hsa-miR-200a-5p、hsa-miR-200a-3p。上述這些調控影響卵巢癌基因的miRNA序列在原始序列中無法看出的共通性，但是藉由細胞自動機轉換成圖像之後，其圖像發現了相同之處，而且不只是調控相同基因的圖像間有相同之處，這些相關於調控卵巢癌基因的miRNA都出現了相同之處，或許這些相同的序列片段對於調控卵巢癌基因可能有相同的影響，將來可藉由生物實驗去測試這些出現共同圖像的片段是否功能上也有其關聯之處，將可做為miRNA在調控基因上功能之參考。

4. 未來展望

本研究未來希望能夠改進一些目前系統的缺陷、及增加實用性及範圍性。第一、希望能更加改進讀寫的速率，由於目前系統在生成圖像方面是藉由 MATLAB 來執行、而且在資料庫的寫入上耗費的時間也比想像的長，希望將來能改進寫入資料的時間以及改進圖像生成的時間，將 Matlab 的方法轉成 package 給系統直接執行，不需呼叫 Matlab 來執行，相信能更減少執行的時間。第二，本文所實作的 RFID 系統所使用讀取器讀取範圍並不大(<10CM)，若未來希望增加系統的泛用與實用性，則需要將讀取器改成遠距離的讀取器，藉此提升系統的實用性。第三、本文研究所轉換的圖像主要是希望能用肉眼觀察其結果，一旦資料量越來越多，肉眼辨識也是需要耗費相當大的時間，因此希望未來希望能再新增比對系統部分，因為目前序列比對是生物序列主要的運用之一，探究物種間不同的結構、功能，找出重要的序列結構，所以希望未來能讓使用者除了對序列做辨識之外，也能藉由系統直接對不同序列直接做比對。

致謝

本人誠摯感謝審稿者提出的寶貴建議與意見，改善了本文的內容與品質。本文與台中榮民總醫院與國立中興大學合作研究計畫(榮興計畫)，計畫編號 TCVGH-NCHU 1027619，以及行政院國家科學委員會，計畫編號 NSC 102-2622-E-005-011-CC3 共同合作。

參考文獻

[1] Hebert, P. D. N., A. Cywinska, et al. (2003). "Biological identifications through DNA barcodes." Proceedings of the Royal Society of London. Series B: Biological Sciences 270(1512): 313-321.

[2] Dahiya, N., C. A. Sherman-Baust, et al. (2008). "MiRNA expression and identification of putative miRNA targets in ovarian cancer." PLoS One **3**(6): e2436.

[3] Iorio, M. V., R. Visone, et al. (2007). "MiRNA signatures in human ovarian cancer." Cancer Res **67**(18): 8699-8707.

[4] Bhattacharya, R., M. Nicoloso, et al. (2009). "MiR-15a and MiR-16 control Bmi-1 expression in ovarian cancer." Cancer Res **69**(23): 9090-9095.

[5] Nam, E. J., H. Yoon, et al. (2008). "MiRNA Expression Profiles in Serous Ovarian Carcinoma." Clinical Cancer Research **14**(9): 2690-2695.

[6] Park, S. M., S. Shell, et al. (2007). "Let-7 prevents early cancer progression by suppressing expression of the embryonic gene HMGA2." Cell Cycle **6**(21): 2585-2590.

[7] Zhang, L., S. Volinia, et al. (2008). "Genomic and epigenetic alterations deregulate miRNA expression in human epithelial ovarian cancer." Proc Natl Acad Sci U S A **105**(19): 7004-7009.

[8] Bendoraite, A., E. C. Knouf, et al. (2010). "Regulation of miR-200 family miRNAs and ZEB transcription factors in ovarian cancer: evidence supporting a mesothelial-to-epithelial transition." Gynecol Oncol **116**(1): 117-125.

[9] Yang, H., W. Kong, et al. (2008). "MiRNA expression profiling in human ovarian cancer: miR-214 induces cell survival and cisplatin resistance by targeting PTEN." Cancer Res **68**(2): 425-433.

[10] Hu, X., D. M. Macdonald, et al. (2009). "A miR-200 miRNA cluster as prognostic marker in advanced ovarian cancer." Gynecol Oncol **114**(3): 457-464.

[11] Guo, L. M., Y. Pu, et al. (2009). "MiRNA-9 inhibits ovarian cancer cell growth through regulation of NF-kappaB1." FEBS J **276**(19): 5537-5546.

[12] Laios, A., S. O'Toole, et al. (2008). "Potential role of miR-9 and miR-223 in recurrent ovarian cancer." Mol Cancer **7**: 35.

[13] Shell, S., S. M. Park, et al. (2007). "Let-7 expression defines two differentiation stages of cancer." Proc Natl Acad Sci U S A **104**(27): 11400-11405.

[14] Quaresma, Alexandre J.; Nickerson, Jeffrey A. (2013). "Regulation of mRNA export by the PI3 kinase/AKT signal transduction pathway", *Mol Biol Cell* **8** (8): 1208–21.

[15] Von Neumann, J. and A. W. Burks (1966). "Theory of self-reproducing automata." Urbana, University of Illinois Press.

[16] S Wolfram (1983)."Statistical mechanics of cellular automata" Reviews of modern physics(55): 601-644.

利用高通量定序資料預測老鼠微核醣核酸轉錄起始位置

方浩宇 [1] 許郁彬 [1] 朱虹瑄 [1] 謝立青 [1,2,*]
[1] 國立中興大學基因體暨生物資訊研究所 [2] 國立中興大學生物科技發展中心
*liching@nchu.edu.tw

摘要

微核醣核酸 (microRNA; miRNA) 是一種非編碼小片段核醣核酸 (non-coding small RNA)，它的主要功能為抑制訊息核醣核酸 (messenger RNA; mRNA) 的轉錄進而影響蛋白質表現與否。確認微核醣核酸的轉錄起始位 (transcription start sites; TSSs) 對於研究微核醣核酸上游調控網路相當重要。目前已經有少數分析人類微核醣核酸轉錄起始位的研究正在進行，在本研究我們則專注在老鼠微核醣核酸轉錄起始位位置的預測，因為預測老鼠微核醣核酸轉錄起始位對於微核醣核酸上游調控網路演化的研究將有很大的助益。我們整合了 Cap Analysis of Gene Expression (CAGE) 與 Transcription Start Sites Sequencing (TSS Seq) 這些利用高通量定序得到與基因起始位置相關的研究資料，並利用支援向量學習機 (Support Vector Machine; SVM) 方法有系統地預測老鼠微核醣核酸轉錄起始位。最後我們利用支援向量學習機找到可能含有轉錄起始位的區域，並利用表現序列標籤 (Expression Sequence Tag; ESTs) 與序列保守性 (Sequence Conservation) 作為判斷轉錄起始位的依據。

關鍵詞：微核醣核酸；轉錄起始位；老鼠；高通量定序；支援向量學習機

Abstract

MicroRNAs (miRNAs) are non-coding small RNAs that inhibit protein coding gene expression by hybridizing with messenger RNAs (mRNAs). MiRNAs are involved in a lot of diverse biological processes and various diseases. To identify miRNA transcription start sites (TSSs) is important for studying the upstream regulatory networks of miRNAs. Up to now the studies regarding miRNA TSS identification are all focus on human miRNAs. We are interested in other species and our aim in this study is to identify mouse miRNA TSSs and the result would contribute to understanding the evolution of upstream regulatory networks of miRNAs.

In this study, we integrated two types of high-throughput sequencing data, i.e. transcription start sites sequencing (TSSseq) and Cap Analysis of Gene Expression (CAGE), as the evidence of miRNA TSSs. A machine-learning-based Support Vector Machine (SVM) was developed to identify mouse miRNA TSSs. In addition, we also incorporated the ESTs (expression sequence tag) and sequence conservation information to provide evidence for mouse miRNA TSSs.

Keywords: miRNA; transcription start sites; mouse; Support Vector Machine

1. 介紹

微核醣核酸 (microRNA; miRNA) 為一段大約 22-nt (nucleotide) 單位大小的核甘酸序列，微核醣核酸會藉由結合在訊息核醣核酸 (messenger RNA; mRNA) 的 3’端未轉譯區 (3’ - untranslated regions; 3’UTR) 來抑制訊息核醣核酸的表現或使訊息核醣核酸降解，進而使得蛋白質無法被合成。而這種調控基因表現的功能，在生理上可能與細胞代謝、細胞凋亡以及其他生物功能息息相關，同時其功能也牽涉到癌症的病程發展 [1-3]，因此有關於微核醣核酸的研究非常重要。

微核醣核酸的合成是一個複雜的過程，當一段表現微核醣核酸的基因序列藉由核糖核酸聚合酶 II開始進行轉錄，其轉錄後的核糖核酸序列上會有部分區域形成髮夾狀的結構，此時這段核糖核酸序列稱為初始微核糖核酸 (primary-miRNA; pri-miRNA)。之後這一段序列上的髮夾結構會被酵素 Drosha 切下生成前驅微核糖核酸 (precursor-miRNA; pre-miRNA)，再經由酵素 Dicer 將前導微核糖核酸上的環狀結構切掉，形成一個雙股微核醣核酸 (miRNA-miRNA* duplex)，而其中的一段便是參與基因調控的成熟微核醣核酸 (mature-miRNA)。成熟微核醣核酸會與一些蛋白質形成核糖核酸誘導沉默複合體 (RNA-induced silencing complex; RISC) 的蛋白質複合體，核糖核酸誘導沉默複合體與蛋白質編碼基因 (protein coding gene) 上的微核醣核酸標靶位置 (miRNA target) 結合後會使被結合的訊息微核醣核酸被降解或是無法進行轉譯。這種獨特的功能使微核醣核酸在基因調控網路上扮演著重要角色，進而影響到各種生物的生理與代謝功能。

近年對於微核醣核酸的研究也著重於微核醣核酸標靶，例如 TarBase, miRecords, miR2Disease 和 miRTarBase 都有許多關於微核醣核酸標靶位置的預測或實驗資料 [4-7]。而研究微核醣核酸的上游例如微核醣核酸的轉錄起始位置相對來說卻很少。

微核醣核酸轉錄起始位置的預測是相當困難的，miR-34a 是一個已知的微核醣核酸，老鼠微核醣核

酸 miR-34a 髮夾結構所在與轉錄起始位置有一段距離 (~2 萬 nts)，微核醣核酸與轉錄起始位置的距離可能很遠，這就是預測微核醣核酸轉錄起始位置困難的原因[8]。

由於科技發展與計算機科學的進步，傳統的定序方法隨著機械學、生物資訊、電腦資料庫和儀器發展，起了革命性的變化。次世代定序 (next-generation sequencing) 技術，又稱為高通量定序 (high-throughput sequencing) 技術的誕生對生物基因體學有著重大的影響；高通量定序大幅度地降低定序的成本；隨著新平台的發展，目前一次可定序多達超過數十億個鹼基。高通量定序的方法對於泛基因體 (genome-wide) 核醣核酸相關的分析和非編碼核醣核酸 (noncoding RNA) 的發現等研究有很大的幫助。次世代定序可以同時定序大量的序列資料，藉由對定序後的小片段序列進行比對、組合，次世代定序對於基因體的研究有很大的幫助 [9, 10]。

高通量定序在近年的發展中，有許多衍生而出的應用，像是可以知道蛋白質與序列關係的 ChIP-seq 法，以及可以建立轉錄體資訊的 RNA-seq 法 [11]等等。由於轉錄起始位置的資訊位於訊息核糖核酸的 5 等端，所以本研究所使用的資料需要帶有訊息核醣核酸 5’端的資訊；TSSseq (transcription start sites sequencing) 和 CAGE (cap analysis of gene expression) 也是高通量定序延伸出來的定序應用，而這兩種資料皆帶有靠近基因 5 序端的資訊。

目前已經有一些對於微核醣核酸上游調控區域的相關研究；由於微核醣核酸基因起始表現與蛋白質編碼基因相同需要有核糖核酸聚合酶 II (RNA polymerase II) 的結合，所以有些要尋找微核醣核酸轉錄起始位置 (transcription start sites; TSSs) 之研究會使用核糖核酸聚合酶 II 結合 ChIP-seq (Chromatin immunoprecipitation sequencing) [12]方法的實驗資料，來為微核醣核酸轉錄體 5’端建立模型，藉此判斷微核醣核酸轉錄起始位 [13, 14]。除了核糖核酸聚合酶 II 的 ChIP-seq 資料，現在也有一些高通量定序是專注於研究基因轉錄起始位，諸如 TSSseq, CAGE [15]和組蛋白修飾作用 (histone modification) [16]等研究，這些特徵都與基因轉錄起始區域有關；曾有研究利用上述的特徵為基因的轉錄起始位置建立模型，並依此為依據來預測人類微核醣核酸的轉錄起始位得到很好的結果[17]。

本研究利用上述類似方法針對老鼠的微核醣核酸作轉錄起始位置的預測，希望藉由研究人類以外的物種來觀察微核醣核酸的上游調控網路與物種演化的關係。

2. 研究方法

2.1 資料收集

本研究從 DBTSS [18]中收集老鼠有關 TSSseq 的研究資料，從 FANTOM4 [19, 20]中收集有關老鼠 CAGE 的研究資料，這兩組資料中有多種細胞株，TSSseq 有 4 種細胞株 (3T3,10Thalf, ATDC5, embryo)；CAGE 中則有 14 種細胞株 (cerebellum, Embryo, lung, liver, macrophage, blood , heart, prostate, muscle, heart, visual cortex, somatosensory, preadipocyte, brain)，採用多種的細胞株能夠找到更多樣化的基因表現。

DBTSS 中的資料庫也含有老鼠的蛋白質編碼基因起始位置，由於蛋白質編碼基因與擁有自己的轉錄起始位的微核醣核酸有著類似的轉錄起始位特性，故將這些蛋白質編碼基因起始位置用以建構 TSSseq 和 CAGE 資料在機械語言學習法之中的模型，該模型將作為預測基因起始位置的判定標準。為了確認蛋白質編碼基因起始位置是否會與基因序列重疊，我們從 Ensembl Genome Browser [21]收集老鼠的蛋白質編碼基因序列位置，若預測的位置與蛋白質編碼基因重疊則不予以採用。另外收集來自於 UCSC [22]之序列保守性 [23]和表現序列標籤 [24]的相關資料，這些資料將被用於微核醣核酸轉錄起始位置預測的可信度判斷。

miRBase 是一個收錄許多物種前導微核醣核酸或成熟微核醣核酸資訊的資料庫網站 [25]，本研究從 miRBase 中收集關於老鼠的微核醣核酸資料，在之後的研究中將預測這些微核醣核酸的轉錄起始位置。微核醣核酸依其在序列的位置有兩種分類，若微核醣核酸的位置在一個有蛋白質編碼基因序列內，稱為基因內 (intragenic) 微核醣核酸，通常這類微核醣核酸會與其宿主基因 (host gene)擁有共同的轉錄起始位置；反之微核醣核酸若位於沒有表現蛋白質的基因序列上則稱為基因間 (intergenic) 微核醣核酸，此類微核醣核酸擁有自己的轉錄起始位，而我們的主要預測目標為基因間微核醣核酸。從 mirBase 的資料庫下載的有關老鼠的微核醣核酸，經由篩選將基因內微核醣核酸的資料去除，剩下來的微核醣核酸為沒有與基因重疊的基因間微核醣核酸，總共有 1047 個微核糖核酸資料，從中篩選出有 178 個基因間微核醣核酸。

本研究採用老鼠 GRCm38 (mm10) 的基因圖譜版本，從 DBTSS 和 CAGE 收集的關於 TSSseq 與 CAGE 相關資料，其基因圖譜版本皆為 GRCm37。為了使基因圖譜版本一致，我們利用來自於 UCSC 的 liftover 軟體，將 GRCm37 轉換為 GRCm38。本實驗的 TSSseq 和 CAGE 的研究資料皆經由 liftover 轉換為 GRCm38 基因圖譜版本。

2.2 模型建立

從 DBTSS 的資料庫中下載獨立蛋白質編碼基因的轉錄起始位置，將每個轉錄起始位置取前後 1100 bp，共有 2200 的範圍內以分別 200 bp 為單位分隔出 11 格的框架，分別計算每個區塊中 TSSseq 標籤和 CAGE 標籤的密度。目前有 11415 個蛋白

質編碼基因轉錄起始位置的資料將其作為正向資訊，如圖 1 所示；另外再以每個蛋白質編碼基因轉錄起始位置的前後 10000 bp 的位置，分別計算其前後 1100 bp 位置中 2200 bp 的範圍內每隔 200 bp 區塊中 TSSseq 標籤和 CAGE 標籤的密度，這部分的資料作為負向資訊。將正向資訊和負向資訊作為支援向量學習機的訓練資料，去產生一個支援向量學習機模型，此支援向量學習機模型將用於尋找轉錄起始位置。本研究利用一套共享的向量學習機程式 LibSVM [26]來訓練與建立模型。

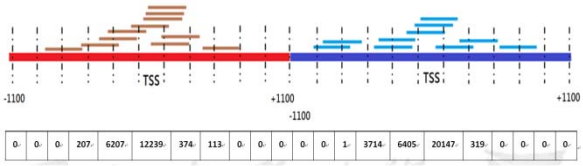


圖 3. 正向支援向量學習機模型

2.3 預測轉錄起始位置

利用從 miRBase 中得到的 178 個老鼠前驅微核醣核酸位置資訊，有研究指出 2 個微核醣核酸若距離在 50000 bp 範圍內則可能共用一個轉錄起始位 [27]，所以我們取微核醣核酸上游 50000 bp 的範圍內，從微核醣核酸的位置，每隔 100 bp 的位置，取前後各 1100 bp 的範圍內以分別 200bp 為單位分隔出 11 格的區塊，分別計算每個區塊中 TSSseq 標籤和 CAGE 標籤的密度。利用建立的支援向量學習機模型去掃描上述資料尋找符合正向資訊的位置，藉此幫助我們找出可能含有轉錄起始位置的區域。整體資料分析流程請見圖 2。

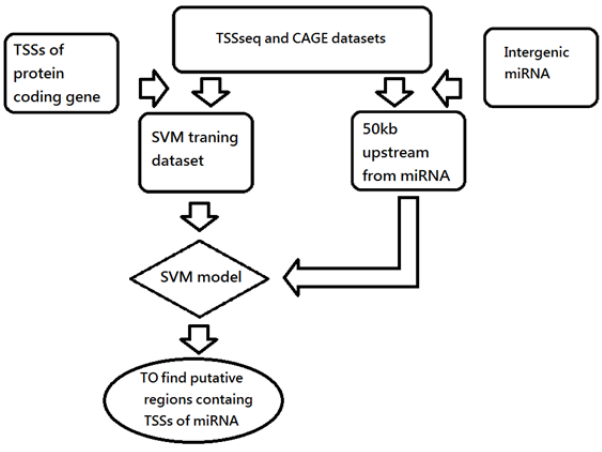


圖 2. 資料分析流程圖

同時為了提高準確性，參考相關的研究論文 [17]，還需要符合以下條件: (1) 被支援向量學習機判斷為正向。(2) 被判斷為正向區域且不能與蛋白質編碼基因序列重疊。(3) 表現序列標籤和基因保留性的特徵。(4) 距離微核醣核酸的上游位置愈近愈好。

3. 結果

3.1 TSSseq 和 CAGE 與轉錄起始位置

一般我們知道核糖核酸聚合酶 II 可以用來判斷 mRNA 轉錄的起始位置，因為核糖核酸聚合酶 II 與基因序列結合的位置與轉錄起始位置極為接近。所以同理也可以運用於微核醣核酸 轉錄起始位的預測，而除此之外，TSSseq 和 CAGE 的提供的實驗數據也可以為我們用來研究微核醣核酸的轉錄起始位，TSSseq 和 CAGE 的實驗包含有一個轉錄體的 5'端資訊，這些 5'端的資訊也是最接近轉錄起始位的所在，為了驗證此法的可行性，可以從一般的蛋白質編碼基因驗證。將總共 11415 個從 DBTSS 中收集到的蛋白質編碼基因的轉錄起始位置，分別計算 TSSseq 標籤和 CAGE 標籤在蛋白質編碼基因轉錄起始位置附近的平均表現量，從轉錄起始位置開始到其前後 1100 位置，以 200 單位為框架，如圖 3 所示，從已知蛋白質編碼基因的轉錄起始位區域都可以觀察到 TSSseq 標籤和 CAGE 標籤的表現量集中的訊號，故利用 TSSseq 標籤和 CAGE 標籤的實驗資料也可以應用於微核醣核酸 轉錄起始位置預測，這些研究資料也將用於支援向量學習機中訓練模型的資料。

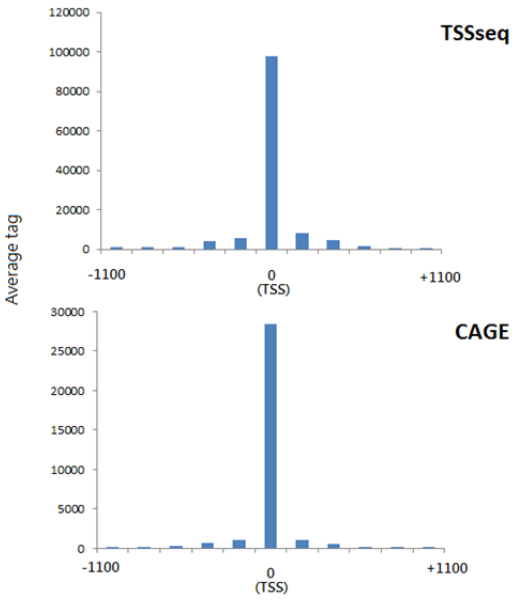


圖 1. TSSseq 標籤和 CAGE 標籤在蛋白質編碼基因轉錄起始位附近的平均的表現量

3.2 利用支援向量學習機有系統地預測微核醣核酸轉錄起始位

支援向量學習機是一種用於分類的機器學習，主要是嘗試在空間中，尋找一個超平面 (Hyperplane) 能將不同類別的資料完美的分開，同時此超平面能與不同的類別的資料距離愈大愈好。為了找到 TSSseq 與 CAGE 於微核醣核酸的上游有高表現的區域，我們需要訓練的資料也必須具有類似的資訊，DBTSS 的資料庫中有許多老鼠的表現蛋白質基因的轉錄起始位資料，而 TSSseq 和 CAGE 的實驗資料在這些老鼠表現蛋白質基因的轉錄起始位置上，大部分都呈現高的表現，所以從 DBTSS 裏篩選出獨立的已知蛋白質編碼基因的轉錄起始位置，特別選用獨立的轉錄起始位，是因為獨立的已知蛋白質編碼基因轉錄起始位由於沒有相近的轉錄起始位置，所以 TSSseg 和 CAGE 的才會統一在轉錄起始位置有大量表現，可以由圖 4 老

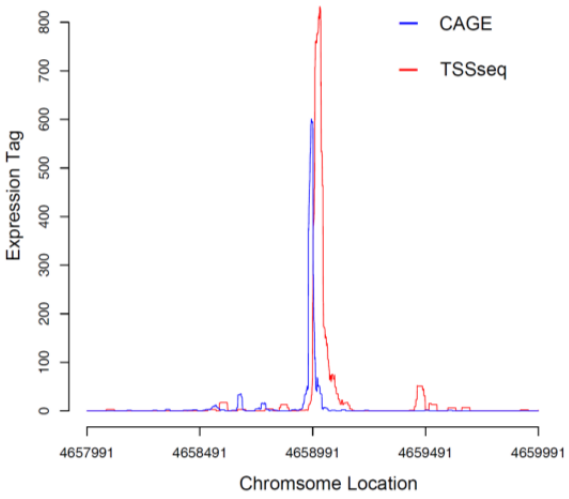


圖 4. 獨立轉錄起始位蛋白質編碼基因 (NM_172894)

鼠 NM_172894 基因的例子看出。而圖 5 可以看出含有叢集 (cluster) 轉錄起始位置的蛋白質編碼基因 NM_172894 會因其轉錄起始位相距太近使得 CAGE 和 TSSseq 的表現不會只集中在轉錄起始位的位置。而共有 11415 組的資料從 DBTSS 中篩選出配合 TSSseq 和 CAGE 的表現作為支援向量學習機訓練的資料。在支援向量學習機的預測下，老鼠的 178 個微核醣核酸可以在其中 138 個微核醣核酸找到被判斷為具有轉錄起始位之正向資訊的區域。

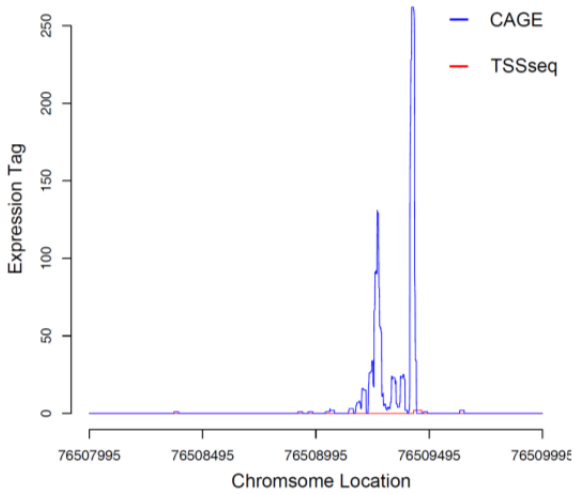


圖 5. 叢集轉錄起始位蛋白質編碼基因 (NM_198894)

3.3 微核醣核酸轉錄起始位預測結果

將 11935 個獨立的蛋白質編碼基因轉錄起始位取前後 1100 位置，分別 200bp 為單位計算每個區塊中 TSSseq 和 CAGE 表現的密度，以此做為支援向量學習機訓練模型的資料，再來從 mirBase 收集 178 個老鼠基因間微核醣核酸，以每個基因間微核醣核酸序列起始位置到上游 50000 的範圍內，每隔 100 單位取前後各 1100 的範圍內以分別 200bp 為單位延伸出 11 格的區塊，分別計算每個區塊中 TSSseq 標籤和 CAGE 標籤的密度。將這些基因間微核醣核酸上游中若有被判斷為正向資訊的區域，這些區域為可能有轉錄起始位的區域，選出這些區域中具有 TSSseq 和 CAGE 高表現的位置，做為可能的轉錄起始位，除了 TSSseq 和 CAGE 的高表現外，表現序列標籤和序列保守性這兩種特徵可以判斷序列在基因中是否表現以及演化的重要性，故用作判斷轉錄起始位的依據，UCSC 網站有老鼠相關的表現序列標籤和序列保守性資料，利用這兩種特徵來看是否與具有 TSSseq 和 CAGE 高表現位置可能的轉錄起始位重疊，同時這些序列不能與蛋白質編碼基因序列重疊。若以上條件符合，則此位置很有可能為轉錄起始位。分析結果從 178 個基因間微核醣核酸中找到了 138 個符合分析區域不與蛋白質重疊的微核醣核酸，再利用支援向量學習機方法結合以上的特徵分析找到 79 個基因間微核醣核酸的轉錄起始位置（請見補充資料）。

3.4 預測準確度

有關於實驗的準確度，可以從敏感性 (sensitive)、特異性 (specific)、準確性 (accuracy)、精確性 (precision) 4 種參數判斷，將用來製作支援

向量學習機模型的資料放入支援向量學習機模型進行預測 (表 1) 。

表 1. 預測準確度

Sensitive	Specific	Accuracy	Precision
98.7%	92.5%	94.4%	84.7%

4. 討論

4.1 預測方法的優勢

微核醣核酸調控蛋白質基因,使得它在生物學上扮演重要的調控角色。但想了解整個微核醣核酸調控網路，就需要了解上游調控微核醣核酸的轉錄因子 (transcription factors),所以一個好的預測微核醣核酸轉錄起始位置方法用於定義啟動子區域(promoter region)是很重要的。本篇藉由兩種與轉錄起始位置有關的高通量定序的實驗,來預測 mirBase 中的基因間微核醣核酸轉錄起始位置，實際上此方法在人類微核醣核酸轉錄起始位置上已有成功研究的範例[17]。而此方法用於老鼠上，經由之前的分析，也可以觀察到 TSSseq 和 CAGE 的實驗資料在轉錄起始位置的表現雷同，故此預測方法在老鼠上也是可行的。但本實驗中沒有用到組蛋白修飾作用的相關實驗資料，原因在於現在的網路資料庫並沒有現成的有關於老鼠組蛋白修飾作用 Chip-seq 序列定位的資料，相較之下缺乏一個特徵可能會影響到微核醣核酸轉錄起始位置的預測。

4.2 預測的困難及改善

微核醣核酸與轉錄起始位置的距離通常很遠，可以由本實驗的結果統計微核醣核酸與轉錄起始的位置，在 50kb 的範圍內都可以找到轉錄的起始位置，但這種特性增加了微核醣核酸轉錄起始位置預測的困難，結果中有部分的微核醣核酸沒有找到轉錄起始位置，表示這些微核醣核酸的轉錄起始位無法被本實驗的特徵所辨認，其原因可能為特徵不足，使得部分微核醣核酸沒有訊號而被辨認，另外也有可能部分微核醣核酸只能利用核醣核酸聚合酶 II 所辨認，再來是這些起位置超出了 50kb 之外。

為了能找出未辨認微核醣核酸轉錄起始位置，方法的進一步改善是必須的，可以加入組蛋白修飾作用 特徵來為微核醣核酸做預測，或是加入 RNA-seq 的資料，藉由與完整的基因轉錄體互相比對找出微核醣核酸的起始位置。

4.3 老鼠與人類微核糖核酸轉錄起始位的比對

我們將老鼠跟人類的微核醣核酸基因轉錄起始位做比對，其中老鼠微核醣核酸的轉錄起始位置在預測時只選出為帶有表現序列標籤或序列保守性的結果，在算出轉錄起始位置與微核醣核酸的距離。再以相同的預測方法用在人類微核醣核酸上（數據沒有呈現），不過人類在預測上不一定具有表現序列標籤或序列保守性的驗證，比對後可以得到表 3 與表 4 的結果，其中表 4 為距離相近且共用轉錄起始位置的叢集微核醣核酸，這些資料可以觀察到除了一組微核醣核酸叢集外（mir-106a, mir-20b, mir-363 與 mir-92a-2），大部分的人類微核醣核酸與其轉錄起始位置的距離是大於老鼠的，這表示在演化的過程中，人類微核醣核酸與其轉錄起始位置之間多出了許多序列，而這些多出的序列是否有意義或帶有功能且有利於人類是個有趣的問題。

表 2. 微核醣核酸與轉錄起始位置的距離

miRNA	Species	Distance between TSS and miRNA
mir-451a	human	36318
	mouse	35253
mir-193a	human	10294
	mouse	7328
mir-150	human	46188
	mouse	17934
mir-192	human	44646
	mouse	28601
mir-298	human	21384
	mouse	16705
mir-296	human	22023
	mouse	16932
mir-30b	human	32103
	mouse	25668
mir-30d	human	27765
	mouse	21780

表 3. 微核醣核酸叢集與轉錄起始位置的距離

miRNA cluster	Species	Distance between TSS and miRNA cluster
mir-450, mir-542	human	8412
	mouse	7703
mir-221, mir-222	human	20845
	mouse	20262
mir-106a, mir-20b, mir-363, mir-92a-2	human	3613
	mouse	30193

從 Ensembl 的資料統計關於蛋白質編碼基因的編碼區序列與內含子的平均總長，從表 5 看出人

類的編碼區序列 (Coding Domain Sequence; CDS) 與老鼠的編碼區序列的平均總長度極為接近，而內含子的平均總長度變化卻很大。而其中可能的原因是編碼區序列中的外顯子是蛋白質編碼基因中轉譯蛋白質的中心區域，只要外顯子減短或增長都會對生物造成不可預期的影響，所以演化上外顯子的序列大部分保留下來，長度也幾乎不變。而在微核糖核酸的部份，由於微核糖核酸基因也具有內含子，所以微核醣核酸與其轉錄起始位置演化上的距離的變化很有可能主要是受到內含子長度變化的影響。但由於微核糖核酸基因是非編碼基因，它的轉錄主要來自微核糖核酸的結構性，所以演化中其非結構性限制部分之外顯子序列長度的改變很有可能不會影響微核糖核酸的功能，這也可能造成人類微核糖核酸與老鼠微核糖核酸與轉錄起始位置之間的距離改變。

表 4. 老鼠與人類每個蛋白質編碼基因外顯子與內含子平均總長

Species	Average CDS size	Average combined intron size
mouse	1369.50	39011.00
human	1229.37	47038.29

誌謝

本論文承蒙國家科學委員會之計畫經費贊助，計畫編號為 NSC 100-2621-B-005-001，僅此誌謝。

參考文獻

[1] I. Alvarez-Garcia, E.A. Miska, "MicroRNA functions in animal development and human disease", Development, vol. 132. 2005, pp. 4653-4662.

[2] N. Bushati, S.M. Cohen, "microRNA functions", Annual review of cell and developmental biology, vol. 23. 2007, pp. 175-205.

[3] G.A. Calin, C.M. Croce, "MicroRNA signatures in human cancers", Nature reviews. Cancer, vol. 6. 2006, pp. 857-866.

[4] S.D. Hsu, F.M. Lin, W.Y. Wu, C. Liang, W.C. Huang, et al., "miRTarBase: a database curates experimentally validated microRNA-target interactions", Nucleic acids research, vol. 39. 2011, pp. D163-169.

[5] Q. Jiang, Y. Wang, Y. Hao, L. Juan, M. Teng, et al., "miR2Disease: a manually curated database for microRNA deregulation in human disease", Nucleic acids research, vol. 37. 2009, pp. D98-104.

[6] G.L. Papadopoulos, M. Reczko, V.A. Simossis, P. Sethupathy, A.G. Hatzigeorgiou, "The database of experimentally supported targets: a functional update of TarBase", Nucleic acids research, vol. 37. 2009, pp. D155-158.

[7] F. Xiao, Z. Zuo, G. Cai, S. Kang, X. Gao, et al., "miRecords: an integrated resource for microRNA-target interactions", Nucleic acids research, vol. 37. 2009, pp. D105-110.

[8] V. Tarasov, P. Jung, B. Verdoodt, D. Lodygin, A. Epanchintse, et al., "Differential Regulation of microRNAs by p53 Revealed by Massively Parallel Sequencing", Cell Cycle, vol. 6:13,. 2007, pp. 1586-1593.

[9] E.R. Mardis, "Next-generation DNA sequencing methods", Annual review of genomics and human genetics, vol. 9. 2008, pp. 387-402.

[10] E.R. Mardis, "The impact of next-generation sequencing technology on genetics", Trends in genetics : TIG, vol. 24. 2008, pp. 133-141.

[11] A. Mortazavi, B.A. Williams, K. McCue, L. Schaeffer, B. Wold, "Mapping and quantifying mammalian transcriptomes by RNA-Seq", Nature methods, vol. 5. 2008, pp. 621-628.

[12] L.J. Zhu, C. Gazin, N.D. Lawson, H. Pages, S.M. Lin, et al., "ChIPpeakAnno: a Bioconductor package to annotate ChIP-seq and ChIP-chip data", BMC bioinformatics, vol. 11. 2010, pp. 237.

[13] D.L. Corcoran, K.V. Pandit, B. Gordon, A. Bhattacharjee, N. Kaminski, et al., "Features of mammalian microRNA promoters emerge from polymerase II chromatin immunoprecipitation data", PloS one, vol. 4. 2009, pp. e5279.

[14] Y.W. Guohua Wang, Changyu Shen, Yi-wen Huang, Kun Huang, Tim H. M., K.P.N. Huang, Lang Li, Yunlong Liu, "RNA Polymerase II Binding Patterns Reveal Genomic Regions Involved in MicroRNA Gene Regulation", PloS one, vol. 2010, pp.

[15] T. Shiraki, S. Kondo, S. Katayama, K. Waki, T. Kasukawa, et al., "Cap analysis gene expression for high-throughput analysis of transcriptional starting point and identification of promoter usage", Proceedings of the National Academy of Sciences of the United States of America, vol. 100. 2003, pp. 15776-15781.

[16] S. Dambacher, M. Hahn, G. Schotta, "Epigenetic regulation of development by histone lysine methylation", Heredity, vol. 105. 2010, pp. 24-37.

[17] C.H. Chien, Y.M. Sun, W.C. Chang, P.Y. Chiang-Hsieh, T.Y. Lee, et al., "Identifying transcriptional start sites of human microRNAs based on high-throughput sequencing data", Nucleic acids research, vol. 39. 2011, pp. 9345-9356.

[18] R. Yamashita, H. Wakaguri, S. Sugano, Y. Suzuki, K. Nakai, "DBTSS provides a tissue specific dynamic view of Transcription Start Sites", Nucleic acids research, vol. 38. 2010, pp. D98-104.

[19] H. Kawaji, J. Severin, M. Lizio, A.R. Forrest, E. van Nimwegen, et al., "Update of the FANTOM web resource: from mammalian transcriptional landscape to its dynamic regulation", Nucleic acids research, vol. 39. 2011, pp. D856-860.

[20] H. Kawaji, J. Severin, M. Lizio, A. Waterhouse, S. Katayama, et al., "The FANTOM web resource: from mammalian transcriptional landscape to its dynamic regulation", Genome biology, vol. 10. 2009, pp. R40.

[21] P. Flicek, M.R. Amode, D. Barrell, K. Beal, S. Brent, et al., "Ensembl 2012", Nucleic acids research, vol. 40. 2012, pp. D84-90.

[22] L.R. Meyer, A.S. Zweig, A.S. Hinrichs, D. Karolchik, R.M. Kuhn, et al., "The UCSC Genome Browser database: extensions and updates 2013", Nucleic acids research, vol. 41. 2013, pp. D64-69.

[23] T. Doerks, R.R. Copley, J. Schultz, C.P. Ponting, P. Bork, "Systematic identification of novel protein domain families associated with nuclear functions", Genome research, vol. 12. 2002, pp. 47-56.

[24] S.H. Nagaraj, R.B. Gasser, S. Ranganathan, "A hitchhiker's guide to expressed sequence tag (EST) analysis", Briefings in bioinformatics, vol. 8. 2007, pp. 6-21.

[25] A. Kozomara, S. Griffiths-Jones, "miRBase: integrating microRNA annotation and deep-sequencing data", Nucleic acids research, vol. 39. 2011, pp. D152-157.

[26] C.C. Chang, C.J. Lin, "LIBSVM: A Library for Support Vector Machines", Acm T Intel Syst Tec, vol. 2. 2011, pp.

[27] S. Baskerville, D.P. Bartel, "Microarray profiling of microRNAs reveals frequent coexpression with neighboring miRNAs and host genes", Rna, vol. 11. 2005, pp. 241-247.

鈣離子通道基因剔除小鼠微陣列資料分析

林守羿[1]　蔡孟勳[1,2]　何宜霖[1]
[1]國立中興大學資訊管理研究所
[2]國立中興大學基因體暨生物資訊學研究所
xup6zeo@gmail.com

摘要

大腦內的各個腦區分別執掌不同的功能，其中的海馬負責空間記憶及短期記憶形成長期記憶。Cav3.2 T型鈣離子通道的開啟會觸發許多細胞內生物化學的反應，例如肌肉收縮、基因表達、神經傳導物質的釋放等。近期文獻指出，α1H T型鈣離子通道在海馬中有高度表現，並造成依賴海馬相關的學習障礙缺陷。本研究中利用微陣列基因晶片，取得α1H T型鈣離子通道剔除小鼠在接受痕跡恐懼實驗前後的左右側海馬內之基因表達數據，進行成對樣本T檢定分析（Paired-Samples T-Test），確認小鼠於訓練前後左右兩側海馬內基因表現量具有顯著差異；再利用線性迴歸分析（Linear Regression Analysis）篩選出表現量顯著改變之標靶基因。接著，利用階層式分析（Hierarchical Clustering）找出尚未在醫學中被證實生物功能的NA(non-available)基因所屬分群，並透過基因資料庫比對標靶基因是否與海馬功能有所關聯，進而探討標靶基因對學習記憶之影響。研究結果顯示，α1H T型鈣離子通道剔除小鼠的右側海馬在接受訓練後基因表現量改變不大；記憶訓練則使左側海馬內基因表現量回復到α1H T型鈣離子通道未被剔除之野生型小鼠相似之水準，本論文之研究成果將為基礎醫學研究者未來針對這些標靶基因進行功能探討之可行方向。

關鍵詞：鈣離子通道、微陣列晶片、學習與記憶、成對樣本T檢定、線性迴歸、關聯階層式分群

1. 緒論

海馬是大腦形成長期記憶的區塊，和情境學習與空間記憶有所關連。已有研究證實α1H-T型鈣離子通道確實在依賴海馬學習試驗上扮演一個重要角色[1]。目前已知α1H T 型鈣離子通道相關疾病，如自閉症(Autism)、兒童癲癇症候群(Childhood absence epilepsy)，便是因為鈣離子通道的結構和功能異常所導致的。又當記憶不再重複使用，或是在腦部受到損傷、罹患疾病如阿茲海默症、過度壓抑痛苦經驗下，記憶學習能力也就慢慢喪失。本研究動機便是希望可以發現在鈣離子通道受損的狀況下，是否導致其他基因表現量顯著改變，並且是否在接受學習訓練後可以改善其基因表現程度。本研究中運用小鼠腦中Cav3.2 T型鈣離子通道基因剔除小鼠之海馬微陣列基因晶片數據進行分析，比較左右兩側海馬內之基因在恐懼制約前後的表達量是否有差異，並且探討差異表達之基因群中與學習記憶相關者，其表達程度與Cav3.2T型鈣離子通道剔除間的關聯性。

2. 研究方法與架構

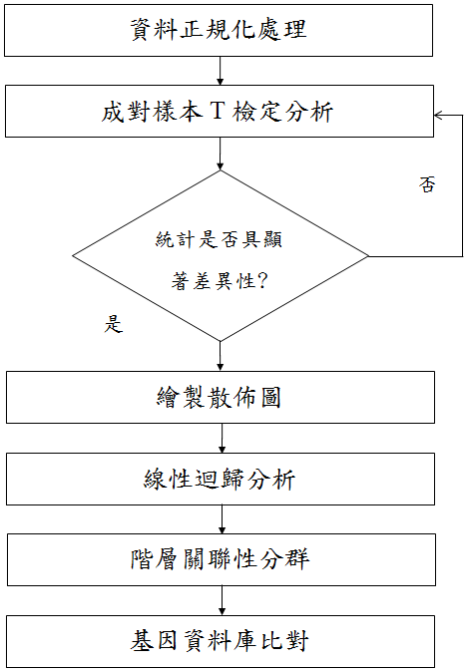


圖 1　系統流程圖

本研究先將微陣列基因晶片數據進行正規化處理。再利用成對樣本T檢定，分析Cav3.2基因剔除小鼠在訓練前後的基因表現量是否具有顯著差異。若無顯著差異，則調整P-Value 並重新進行統計分析；若有顯著差異，則透過散佈圖來觀察樣本間呈現的相關模型。接著，利用直線迴歸分析篩選離群值作為本研究之可能標靶基因。因數據中有尚未被醫學證實生物功能之NA(non-available)基因，故利用階層式分析分群，生物醫學可依結果進一步

推論是否同一分群內具有相近之生物功能。最後，將標靶基因透過基因資料庫比對，期望可以找出在剔除Cav3.2 T型鈣離子通道後對學習記憶有所影響之基因，以達成研究目的。

2.1 資料正規化

本研究所使用的資料是以cDNA微陣列所記錄的39,200筆基因表現資料，將一些空值、雜訊等可能會影響結果的數據刪除除後，左腦剩下39,194 筆數據；右腦剩下39,187筆數據。本研究中分為剔除鈣離子通道之未受訓練組的左腦、未受訓練組的右腦、受訓練組的左腦、受訓練組的右腦各2組，共8組的資料去做分析(表1)。

表 1 老鼠鈣離子表型實驗樣本表

NO	Sample	Name	Gpr	備註
1	KONLHIP080907	ut_L1	H09-1060806055	未受訓練組_左腦
2	KONLHIP080907	ut_L2	H10-1060806054	未受訓練組_左腦
3	KOTLHIP080907	t_L1	H13-1060807337	受訓練組_左腦
4	KOTLHIP080907	t_L2	H14-1060807338	受訓練組_左腦
5	KONRHIP080907	ut_R1	H11-1060807213	未受訓練組_右腦
6	KONRHIP080907	ut_R2	H12-1060807214	未受訓練組_右腦
7	KOTRHIP080907	t_R1	H15-1060807358	受訓練組_右腦
8	KOTRHIP080907	t_R2	H16-1060807359	受訓練組_右腦

利用公式來調整基因表現量顯著程度，正規化公式如下：

$$\log_2\left\{\left(\frac{X-min}{(max-min)}\right)*(max-min)\right\}$$

公式中X為基因表現量；max為母群體中最大值；min為母群體中最小值。經過正規化後數據便介於0至19之間。

2.2 成對樣本T檢定（Paired-Sample t-test）

自成對母體中抽取元素，同一元素前後兩個觀察值所構成的樣本稱為成對樣本（paired samples）[2]。若兩群體的資料是成對出現，也就是資料間具有相依性，如未訓練和訓練後的數據，則必須應用成對樣本T檢定。此類T檢定同樣是檢定兩群體特性的期望值是否相等之一種常用的統計方法。

本研究中，設定一個標準的P-value值來做為標靶基因的篩選。P-value值越小期信賴水準度越高（如P-value小於0.05，信賴水準為95%；若P-value小於0.01，信賴水準為99%）。在研究中設定虛無假設H_0為基因於受訓練前後無顯著差異、對立假設H_1為基因於受訓練前後有顯著差異。若計算出的P-value值大於前述的標準值，則表示接受虛無假設，代表訓練前後基因表現量無顯著差異；反之則拒絕虛無假設H_0，表示訓練前後基因表現量具顯著差異。

2.3 散佈圖分析（Scatter Plot）

分別在散佈圖之橫軸(X)與縱軸(Y)上標示未受訓練的基因表現量與受訓練的基因表現量。每一筆資料對應圖中的一個點，可顯示在同一個體上度量的兩個變數之間的關聯、方向、強度。直線關聯是普遍的散佈型態，當點的分佈接近直線，則表示兩變數間關聯強度高，反之若點的分佈較廣，則表示兩變數間關聯強度低，而偏離整體的點，稱之為離群值（outlier）。利用相關係數（γ）可以觀察兩變數之間直線關聯的方向和強度，其值介於-1 到+1之間。當γ值靠近0，代表關聯性強度低；若γ值向-1 或+1接近時，表示關聯性強度逐漸增強，並且點的分佈接近於一直線。

2.4 迴歸分析（Regression Analysis）

迴歸分析[3]（Regression Analysis）是由Francis Galton所發現。迴歸分析是建立因變數Y（或稱依變數，dependent variables）與自變數X（independent variables）之間關係的模型。可以了解自變數與依變數關係、影響方向與程度，並利用自變數與估計的方程式對依變數做預測。因微陣列基因晶片中取得的資料過於龐大，故本研究中利用迴歸分析中的簡單直線迴歸（Simple Linear Regression）作為篩選標靶基因的工具。將每個基因的殘差值遞增排序後，從中挑出基因表現量具顯著差異的觀察值做為標靶基因。

2.5 階層關聯性分群（Hierarchical Clustering）

階層式分群法（hierarchical clustering）[4]透過一種階層架構的方式，將資料層層反覆地進行分裂或聚合，最後產生樹狀結構。常見的方式有兩種：如果採用聚合的方式，階層式分群法可由樹狀結構的底部開始，將資料或群聚逐次合併；如果採用分裂的方式，則由樹狀結構的頂端開始，將群聚逐次分裂。在本研究中，輸入的變數為左腦受訓練前與受訓練後基因表現量之平均，群數凝聚過程是以歐基里德直線距離平方測量區間，當個體間有最小歐式距離平方時，將分為同一群聚。

3. 研究結果

3.1 成對樣本 T 檢定結果

本研究中，在成對樣本T檢定中設定P-value 值來做為標靶基因的篩選，假設檢定中，虛無假設H_0

為基因於受訓練前後無顯著差異；對立假設H_1為基因於受訓練前後有顯著差異。表2為左海馬未訓練與訓練之成對樣本T檢定結果。基因個數為39,194個，在P-Value小於等於0.05(信心水準95%)的成對樣本T 檢定之下，小鼠在接受訓練前與訓練後的數據相關性為0.959，並且達到0.000顯著性。故，拒絕虛無假設H_0，表示左海馬內基因群在訓練前後具有顯著差異。表3為右海馬於訓練前後之成對樣本T檢定結果。基因個數為39,187個，P-Value 小於等於0.05(信心水準95%)的成對樣本T檢定之下，小鼠在接受訓練前與訓練後的數據相關性為0.977，並且達到0.000顯著性。故，拒絕虛無假設H_0，表示左海馬內基因群在訓練前後具有顯著差異。

表 2 左海馬未訓練與訓練之成對樣本T檢定結果

基因個數		訓練前後之相關性	顯著性	
39194		.959	.000	
平均數	標準差	平均數的標準誤	差異的 95%信賴區間	
			下界	上界
-0.440293	0.837874	0.004232	-0.44859	-0.432
t	自由度	顯著性(雙尾)		
-104.033	39193	0		

表 3 右海馬未訓練與訓練之成對樣本T檢定結果

基因個數		訓練前後之相關性	顯著性	
39187		.977	.000	
平均數	標準差	平均數的標準誤	差異的 95%信賴區間	
			下界	上界
0.338054	0.678214	0.003426	0.331339	0.34477
t	自由度	顯著性(雙尾)		
98.67135	39186	0		

3.2 散佈圖分析結果

將成對樣本T檢定運算後的結果輸入散佈圖中，X軸為未受訓練之控制組的基因表現平均值(ut_average)，Y軸為受訓練之實驗組的基因表現平均值(t_average)。圖1為小鼠左側海馬中基因表現散佈圖（P-Value<=0.01，信心水準99%以上），R平方達到0.832。圖2為小鼠左側海馬中基因表現散佈圖（P Value<=0.05，信心水準95%以上），R平方達到0.865。從圖1和圖2中可以了解未訓練與受訓練兩變數之間關聯性強度，由於兩者相關系數平方均接近+1，表示關聯性強度強，並且點的分佈接近於一直線。圖3為小鼠右側海馬中基因表現散佈圖（P-Value<=0.01，信心水準99%以上），R平方達到0.323。圖4為小鼠右側海馬中基因表現散佈圖（P-Value<=0.05，信心水準95%以上），R平方達到0.807。代表兩變數間關聯性低；但信心水準95%時，相關係數平方達到0.807，表示兩變數關聯性增強。

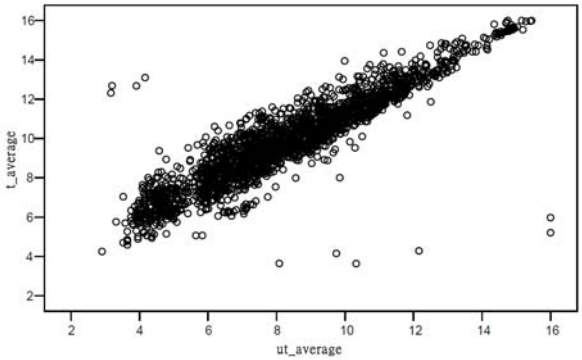


圖 1 小鼠左側海馬中基因表現散佈圖（P<=0.01）

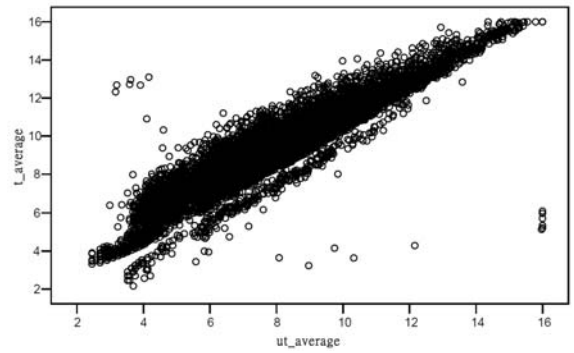


圖 2 小鼠左側海馬中基因表現散佈圖（P<=0.05）

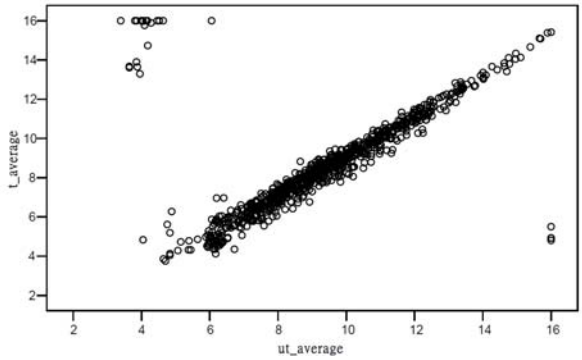


圖 3 小鼠右側海馬中基因表現散佈圖（P<=0.01）

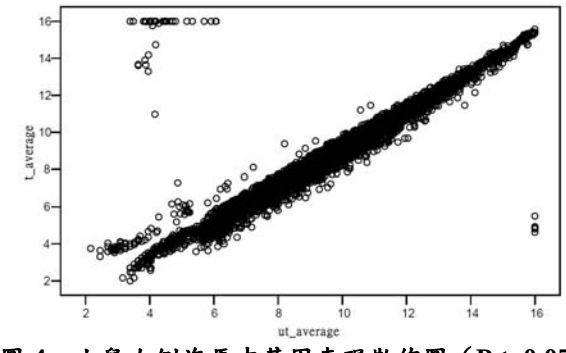


圖 4 小鼠右側海馬中基因表現散佈圖（P<=0.05）

3.3 迴歸分析結果

迴歸分析的使用是希望可以降低大量數據的

維度，本研究以P-Value<=0.001（信賴水準99.9%）、P-Value<=0.005（信賴水準99.5%）、P-Value<=0.01（信賴水準99%）、P-Value<=0.05（信賴水準95%）為基準進行基因篩選。圖5為左海馬線性迴歸分析後結果。當P-Value<=0.001（信賴水準99.9%）時，篩選出4筆基因；當P-Value<=0.005（信賴水準99.5%）時，篩選出8筆基因；當P-Value<=0.01（信賴水準99%）時，篩選出17 筆基因；當P-Value<=0.05（信賴水準95%）時，篩選出36筆基因。圖6為右海馬線性迴歸分析後結果。當P-Value<=0.001（信賴水準99.9%）時，未篩選出任何基因；當P-Value<=0.005（信賴水準99.5%）時，篩選出19筆基因；當P-Value<=0.01（信賴水準99%）時，篩選出38 筆基因；當P-Value<=0.05（信賴水準95%）時，篩選出59筆基因。左側海馬中被篩選出來的基因與尚未被醫學驗證的NA（nonavailable）基因，將作為往後研究的標靶基因。而右側海馬內除了篩選出作為監控實驗流程的控制探針（如Ambion Control、MEEBO Tiling Control），未有其他基因數據。在此推論出Cav3.2基因剔除小鼠，即使接受訓練也無法改善右海馬內基因水準，但在左海馬內發現可能影響學習與記憶的標靶基因。

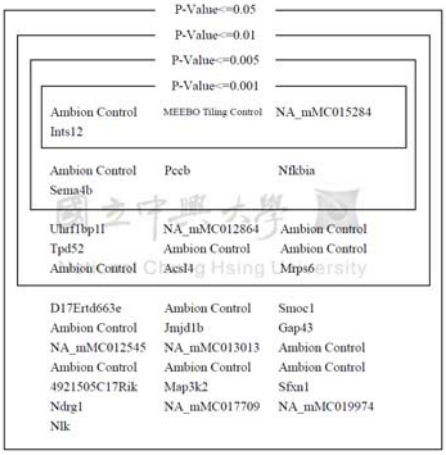


圖 5 左海馬線性迴歸分析後結果

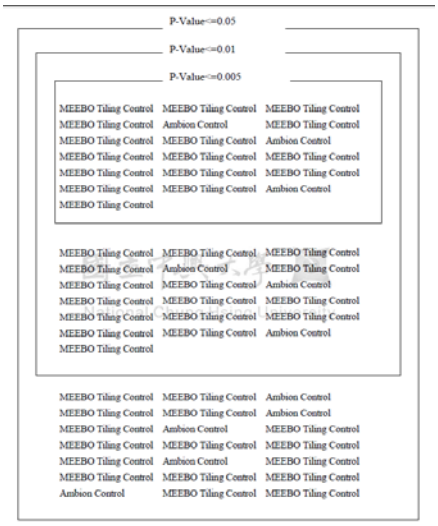


圖 6 右海馬線性迴歸分析後結果

3.4 階層關聯性分群結果

針對左海馬，在迴歸分析P-Value<=0.05時篩選出來的36筆標靶基因進行聚合式關聯性分析。先將標靶基因在未受訓練時的基因表現量進行群數凝聚過程，產生了圖7的分群結果。以歐式距離平方來看，當距離等於3時，可以分為三個群組；當距離等於5時，可以分為三個群組；當距離等於10時，可分為兩個群組。

將標靶基因在受訓練後的基因表現量進行群數凝聚過程，產生了圖8的分群結果。以歐式距離平方來看，當距離等於3時，可以分為四個群組；當距離等5時，可以分為三個群組；當距離等於10時，可分為兩個群組。從結果來看，小鼠剔除大腦鈣離子通道後，接受相關訓練會導致基因間的調控產生了變化，過訓練前後分群會有所不同。生物醫學也可以針對這樣的分群結果，找出同一分群基因的生物功能關聯性，並推論到分群中尚未被證實的NA基因。

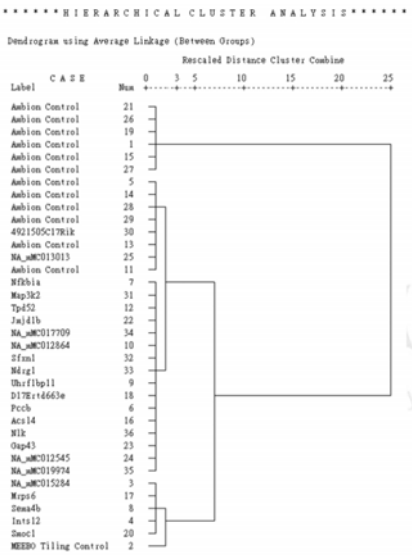


圖 7 左海馬未受訓練時，標靶基因分群結果

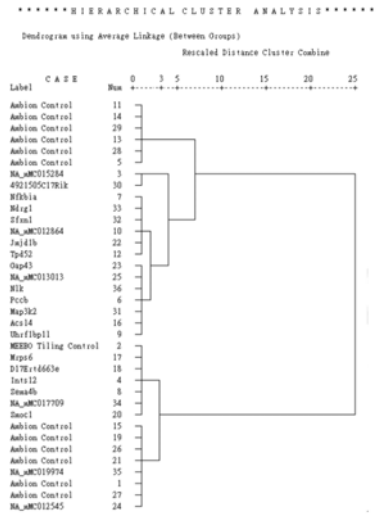


圖 8 左海馬受訓練後，標靶基因分群結果

4. 研究結果分析

首先我們觀察標靶基因在Cav3.2基因剔除前後和訓練前後之基因表現量。以基因Gap43(Growth Associated Protein 43)為例，表4中表示野生型小鼠組(WT)在受訓練前後基因Gap43 的表現量平均約2500左右；而基因剔除小鼠組(KO)中明顯發現基因表達下降，但經過訓練後可以改善原本不正常的狀況，並且接近野生型小鼠組受訓練後之基因表達程度。

表 4 Gap43(Growth Associated Protein 43)的基因表現量比較表

Name	Raw Intensity			
	WT_ut1	WT_ut2	WT_t1	WT_t2
Gap43 (Growth Associated Protein 43)	2813	3075	2712	2116
	KO_ut1	KO_ut2	KO_u1	KO_u2
	123	80	2189	1742

在實驗結果中，我們發現右側海馬內並無法篩選出標靶基因，故針對左側海馬中標靶基因之散佈位置做進一步的分析。圖9為P_Value<=0.05 時的基因表現量散佈情形，每個點代表不同的基因，顏色較深的點則為標靶基因。圖中被圈選出來的區塊A，代表的均是做為監控實驗流程的控制探針(Ambion Control)；再以相關係數平方0.865 來切割散佈圖，從左上與右下兩部分來看，表5為右下部分的標靶基因列表；表6為左上部分的標靶基因列表。

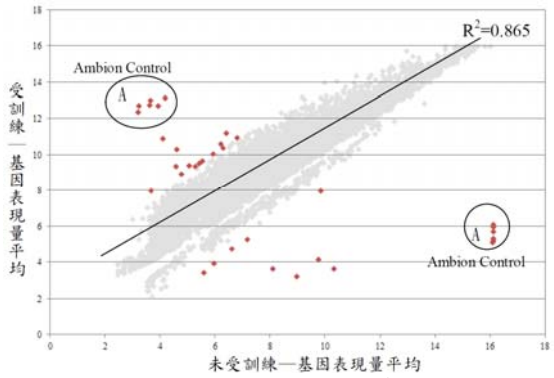


圖 9 加強標示左側海馬內之標靶基因散佈位置，P-Value<=0.05

表 5 散佈圖中，位於右下角的標靶基因

NA_mMC015284	Mrps6	NA_mMC012545
Ints12	D17Ertd663e	NA_mMC017709
Sema4b	Smoc1	NA_mMC019974

表 6 散佈圖中，位於左上角的標靶基因

Pccb	Acsl4	Map3k2
Nfkbia	Jmjd1b	Sfxn1
Uhrf1bp1l	Gap43	Ndrg1
NA_mMC012864	NA_mMC013013	Nlk
Tpd52	4921505C17Rik	

針對挑選出來的標靶基因，進行文獻探討與基因資料庫的相關研究。透過基因資料庫等文獻資料，我們發現Nfkbia (NF-kappa-B hibitor alpha)、Acsl4 (Acyl-CoA synthetase 4) 、 Mrps6 (Mitochondrial ribosomal protein subunit 6) 、Smoc1 (SPARC related modular calcium binding 1) 、 Gap43 (Growth Associated Protein 43) 、 Ndrgl (N-myc downstream-regulated gene 1)、Nlk (Nemo-like kinase) 等7個基因均與大腦有關。以下分別概述各個基因具有的生物性功能。

NF-kB (NF-kappa-B nhibitor alpha) 是轉錄因子的一種（ transcription factor），調節許多基因表現並在細胞過程如增殖、凋亡和發展等扮演關鍵角色。NF-kB 的活性影響神經退化性疾病，如阿茲海默症[5]、帕金森氏症、亨廷頓氏病[6][7]，在認知缺陷中驗證NF-kB 信號是缺損的[8]。Acsl4 (Acyl-CoA synthetase 4)在腦中的arachidonate 代謝與神經細胞分化扮演重要角色[9]。Mrps6 (Mitochondrial ribosomal protein subunit 6)為可能導致智力低下如唐氏症的候選基因[10]。Smoc1 (SPARC related modular calcium binding 1)在人類基因重組表現中是種具有鈣依賴特性的醣蛋白(glycoprotein)[11]。在早期發育階段，海馬錐體神經元中的Ndrg1 (N-myc downstream-regulated gene 1) 可能與未成熟大腦的代謝變化有關[12]。NLK（Nemo-like kinase）是多功能性蛋白，參與神經細胞生長與存活且可能會增強突觸關於記憶與學習的機制[13]，又與腦傷後神經細胞凋亡有關[14]。

生長相關蛋白GAP-43（Growth-associated protein 43）在神經發育過程中或是神經受損後的修復過程中，對於神經纖維的生長以及調節神經可塑性、突觸重整（reorganization）[15]、刺激軸突末梢的生長[16]等均扮演的重要的角色。有研究表示，當細胞內鈣離子濃度增加或神經細胞活化進而活化protein kinase C （PKC）時， PKC會將GAP-43 Ser41 的位置磷酸化，進而使其於神經細胞體的囊泡轉位至生長中神經纖維的細胞膜內面，促使軸突延伸[17]。

綜合以上統計結果分析，我們發現標靶基因中有尚有未被醫學發表的NA(non-available)基因，對於其功能仍缺乏相關文獻驗證，也無法了解真正的生物功能和基因間調控方式。但在階層式分析下，依照分群結果可以推論同一組的基因應該會具有相似的生物功能，這部分仍須仰賴醫學上的驗證。

剔除Cav3.2基因會導致細胞間無法順調節生長與增殖，也影響相關神經細胞及海馬的表現，進而影響海馬的記憶與學習運作。小鼠左側海馬在剔除Cav3.2基因後，發現有些基因如Gap43產生表現量低落或者驟增的數據；在接受痕跡恐懼實驗後，基因表現程度卻接近野生型小鼠(WT)接受訓練後的基因表現水平。這代表，即使剔除Cav3.2基因會導致基因的不正常表現，但只要經過適當的訓練，就可以讓基因表現量幾乎恢復到正常水平。在就基因

剔除鼠(KO)之右側海馬內基因來討論，在訓練前後所篩選出來的標靶基因，均為監控實驗流程的控制探針，表示右側在剔除Cav3.2基因後，小鼠的訓練與否並無法修正海馬內其他基因的表現量程度，也就是右側海馬的記憶與學習能力不會因為剔除Cav3.2基因而有所差異。

最後，針對標靶基因Gap-43來看，目前尚未有研究明確指出Gap-43基因表現量低落會對記憶產生影響，但相關研究提出小鼠在基因Gap-43高表現量時記憶力有所增強，並且基因Gap-43在海馬區域中扮演了助記憶的雙向調節處理的舉足輕重角色[18]。故推論大腦剔除Cav3.2基因後，會影響海馬無法順利進行細胞功能，小鼠在接受訓練後，基因Gap43與鈣調蛋白激酶II 進行調控維持了生物活動平衡，修正了海馬的記憶與學習的功能。本資訊分析系統之推論仍待更多生物醫學加以驗證，並做更深入之探討。

5. 未來展望

生物功能是在神經系統、細胞、基因之間的環環相扣，進行相互抑制與促進 等機制下正常運作。若生物體內的控制機制出現失衡，也會因此導致疾病的產生，如α1H T型鈣離子通道缺損導致的兒童癲癇症候群(Childhood absence epilepsy)，便是在教育環境中會遇到的類型。但在研究結果中我們發現只要有適當的訓練方式，仍可讓學習者改善與提升學習與記憶能力，甚至接近一般常模。

本研究中運用統計分析與基因資料庫分析等方法，統整出以下結論。(1)、基因剔除鼠之左側海馬只要經過適當訓練，便可以改善基因表現水準，而右側海馬則不會因為接受訓練與否而有所改變。(2)、尚未被醫學發表的NA基因，可能與同一分群基因有相似的生物功能。(3)、篩選出與海馬之記憶功能相關的標靶基因。這些研究結果仍須仰賴醫學上的驗證與深入探討。

致謝

本人誠摯感謝審稿者提出的寶貴建議與意見，改善了本文的內容與品質。本文與台中榮民總醫院與國立中興大學合作研究計畫(榮興計畫)，計畫編號 TCVGH-NCHU 1027619，以及行政院國家科學委員會，計畫編號 NSC 102-2622-E-005-011-CC3 共同合作。

參考文獻

[1] 沈哲緯、劉怡均博士(2007),“Hippocampal-dependent learning of mice deficient in α1H T-type calcium channel”, 慈濟大學人類遺傳學研究所.

[2] 林惠玲、陳正倉，基礎統計學觀念與應用，雙葉書廊(2004) 382 頁

[3] Armstrong, J. Scott (2012). "Illusions in Regression Analysis". *International Journal of Forecasting (forthcoming)* 28 (3): 689.

[4] Arvind K. Virmani, Jeffrey A. Tsou, Kimberly D. Siegmund, et al. “Hierarchical Clustering of Lung Cancer Cell Lines Using DNA Methylation Markers”, Cancer Epidemiology, Biomarkers & Prevention 2002; 11:291–297.

[5] Kaltschmidt B., Uherek M., Volk B., Baeuerle P.A., Kaltschmidt C., “Transcription factor NF-kappaB is activated in primary neurons by amyloid beta peptides and in neurons surrounding early plaques from patients with Alzheimer disease.” Proc. Natl. Acad. Sci. USA. 1997;94:2642–2647.

[6] Hunot S., Brugg B., Ricard D., Michel P.P., et al. “Nuclear translocation of NF-kappaB is increased in dopaminergic neurons of patients with parkinson disease.” Proc. Natl. Acad. Sci. USA. 1997;94:7531–7536.

[7] Khoshnan A., Ko J., Watkin E.E., Paige L.A., Reinhart P.H., Patterson P.H., “Activation of the IkappaB kinase complex and nuclear factor-kappaB contributes to mutant huntingtin neurotoxicity.” J. Neurosci.2004;24:7999–8008.

[8] Orianne Philippe, Marlène Rio, Astrid Carioux, et al. ”Combination of Linkage Mapping and Microarray-Expression Analysis Identifies NF-κB Signaling Defect as a Cause of Autosomal-Recessive Mental Retardation”, Am J Hum Genet. 2009 December 11; 85(6): 903–908.

[9] Yong-Yeon Cho, “A novel role of brain-type ACS4 isotype in neuronal differentiation”, Biochemical and Biophysical Research Communications Volume 419, Issue 3, 16 March 2012, Pages 505–510.

[10] Marc Sultan, Ilaria Piccini, Daniela Balzereit, Ralf Herwig,1 Nidhi G Saran, et al. ”Gene expression variation in Down's syndrome mice allows prioritization of candidate genes”, Genome Biol. 2007; 8(5): R91.Published online 2007 May 25.

[11] Vannahme C, Smyth N, Miosge N, Gösling S, Frie C, Paulsson M, Maurer P, Hartmann U, ”Characterization of SMOC-1, a novel modular calcium-binding protein in basement membranes.”, J Biol Chem. 2002 Oct 11;277(41):37977-86. Epub 2002 Jul 18.

[12] Wakisaka Y, Furuta A, Masuda K, Morikawa W, Kuwano M, Iwaki T., ”Cellular Distribution of NDRG1 Protein in the Rat Kidney and Brain During Normal Postnatal Development”, J Histochem Cytochem. 2003 Nov;51(11):1515-25.

[13] Luo Y, Long JM, Lu C, Chan SL, Spangler EL, Mascarucci P, Raz A, Longo DL, Mattson MP, Ingram DK, Weng NP., ”A link between maze learning and hippocampal expression of neuroleukin and its receptor gp78.”, J Neurochem. 2002 Jan;80(2):354-61.

[14] Li Z, Cui G, Wang J, Yu Z, Zhao L, Lv Z., ”Nemo-like kinase (NLK) involves in neuronal apoptosis after traumatic brain injury.”, Cell Mol Neurobiol. 2012 Apr;32(3):381-9. doi: 10.1007/s10571-011-9766-2. Epub 2011 Nov 30.

[15] Min-Ching, Hsu(2003), “Regulatory Mechanisms of Growth-Associated Protein 43 (GAP-43) Expression and Phosphorylation in Developing Neurons”, Taipei Medical University Graduate Institute of Medical Sciences.

[16] A.J.G.D. Holtmaat et al., ”Directed expression of the growth-associated protein B- 50/GAP-43 to olfactory neurons in transgenic mice results in changes in axon morphology and extraglomerular fiber growth”, J. Neurosci., 15 (1995), pp. 7953– 7965.

[17] Yu-Ting, Hsu(2006), “Protein-Protein Interaction of GAP-43 and Gephyrin in Developing Cortical Neurons”, Taipei Medical University Graduate Institute of Medical Sciences.

[18] Jerome L. Rekart, Karina Meiri, Aryeh Routtenberg, “Hippocampal-dependent memory is impaired in heterozygous GAP-43 knockout mice”, Hippocampus Volume 15, Issue 1, pages 1–7, 2005.

挑選具有非線性關聯性之基因選取機制：以演化式計算模式搭配多目標決策作法

唐瑋君　　蔡毓舜　　鍾翊方
國立陽明大學生物醫學資訊所
g30123003@ym.edu.tw　g39528010@ym.edu.tw　ifchung@ym.edu.tw

摘要

近年來微陣列基因晶片因為能夠檢測基因的表現資料，使其可用於觀察不同組織之間的基因表現狀況或因基因表現改變造成的疾病等而被廣泛使用[1][2]，但因為人類有三萬多個基因，基因之間組合的情況會非常多，因此，從大量的資料中找尋有用的基因用於診斷系統的建立目前是一個大家感興趣的研究議題。由於基因數目很多，如何找出可用的基因組有多種作法，而一般的基因挑選機制通常選出的基因是基因與類別之間關係強烈且希望挑出來的基因數量是較少的，雖然選出的基因有具有線性關係與非線性關係，不過大多數都針對基具有線性關係的基因作探究，因為非線性交互作用的基因間的關係並無固定的規則，在探究基因的生物意義時，往往有較大的挑戰；我們希望能夠將演化式計算模式中結合多目標問題的方法運用在基因挑選機制上面，透過原有的 mRMR 基因挑選機制的多目標定義作延伸，將基因之間不同的問題演變成不同的目標去找出具有非線性關聯性的基因，因此，我們提出以演化式計算模型搭配多目標決策作法(Feature Selection: Evolutionary Computing with Multiobjective Strategy，簡稱 FS-ECMOS)來針對微陣列基因晶片做非線性關聯性之基因的挑選，除了考慮基因對於類別的區分能力之外，我們還考慮基因之間的非線性關聯性以及所選用的基因數目，希望藉由演化式計算的概念，搜尋所有的解空間中符合多目標條件的基因，使我們能夠保留較多具有非線性關聯性的基因，幫助我們更加了解這些具有非線性關係的基因之間的生物意義。

關鍵詞：相互資訊值、特徵選取、微陣列基因晶片、多目標決策作法、基因選取。.

1. 前言

微陣列基因晶片(Microarray)近幾年被廣泛用來檢測基因的表現狀況，常用與觀察生物體內不同組織的基因表現狀況或者相同組織之間因基因表現的改變造成的疾病等。由於微陣列基因晶片的資料提供豐富的基因表現資料，使得這些資料量都非常龐大，因此，在大量的基因表現資料當中，挑選適當數量的基因用於建立模型或者當作診斷的生物標記是個很重要的一個議題。

微陣列基因晶片資料的基因挑選方式，可以概分為三種[3]：(1) Filter：此種方法主要先獨立執行基因的篩選，基於挑選機制(統計檢定、皮爾森相關係數或其他做法等為常用於挑選基因的方法)提供的評估數據，利用排序方式，選出排名前面的基因當作較佳且具有類別區分能力的，最後將這些基因丟入分類器，因為此種方法只有使用到評分機制，與分類器的選用並無關聯，優點是不需要考慮太多的時間複雜度，可以使得計算簡單快速，不過因為這種方法只有對基因跟類別之間的關係作考慮，並無考慮到基因與基因之間的關聯性，所以這是缺點的一部分。(2) Wrapper：這種方法會使用機器學習的技巧，根據學習演算法的效能指標評估學習結果，將能夠提高效能指標數值的基因納入考慮，藉此達到提高效能選取基因的方法，此種方法的優點有考慮到基因與基因之間的關聯性與分類器造成的影響，缺點是因為利用機器學習的方法考量後再使用分類器作評估，花較多的時間。(3) Embedded：此作法會透過用分類器中嵌入的參數來考慮挑選出來的基因是否能夠提高選取基因的效能，Embedded 作法與 Wrapper 作法類似，差別在於兩種作法之間的挑選基準不一樣。

一般基因挑選作法會希望找尋基因與類別之間關係強烈並且希望將挑選的基因數量減少，我們希望將這些不同問題變成不同的目標，與多目標問題作法進行結合。演化式計算法為 wrapper 方法其中之一，此作法在做基因特徵選取方法時，只有解決單目標的問題，並無考慮到多目標問題的結合，我們透過文件探勘，發現在演化式計算模式中結合多目標問題較有名的方法有 NSGA-II [4]與 MOEA/D [5][6]，而在基因挑選機制上，因 mRMR 作法[7]有定義多目標問題的機制，我們希望透過此作法的多目標定義進行延伸，因此我們主要針對 NSGA-II、MOEA/D 兩種方法與基因挑選機制(mRMR)作探究。

我們發現這些方法一般都是以基因之間具有高線性關係的做保留，而且並沒有強調挑選出來的基因是否全都是具有線性關係的基因，因此我們設定不同的機制探討基因與基因之間是否具有非線性關係，除了希望能夠使用我們的多目標決策作法，透過演化式計算模式針對基因做演化，從微陣列基因晶片資料中找出多組基因解，使這些基因對於類

別有很高的相關性、基因與基因之間也具有非線性(Non-linear interaction relationship)的關係之外，也希望挑出來的基因皆是非線性關係基因的組合，最後讓我們可以針對這些非線性關聯性的基因去做分析，了解非線性關聯性的基因對於分類的能力。

2. 基因挑選機制

在運用基因演算法在做基因挑選機制時，用來探究基因與類別之間的關係與基因之間的關係的方法有兩種：(1) 皮爾森相關係數(Pearson's correlation coefficient) (2) 相互資訊值(Mutual information)；一般皮爾森相關係數方法主要是測量兩連續變數間關係的強弱(計算線性關係情況)，針對有特殊圖形的非線性關係基因是算不出來的，因此我採用相互資訊值(Mutual information)方法來做基因之間的關聯性運算。相互資訊值是利用熵(Entropy)與機率理論(Probability)來測量兩變數之間關聯性的一個方法。

相互資訊值作法：

$$E(X) = -\sum_{i=1}^{n} P(X_i) log_2 P(X_i) \quad (1)$$

首先會先分別計算兩個變數的各自的熵，計算方法如方程式(1)，運用機率概念做運算。

$$H(X,Y) = -\sum_{i=1}^{n}\sum_{j=1}^{n} P(X_i,Y_j) log_2 [P(X_i,Y_j)] \quad (2)$$

再計算兩變數聯合在一起後的關聯情況，將兩變數合併在一起計算聯合熵(Joint entropy) H(X,Y)。

$$I(X;Y) = H(X) + H(Y) - H(X,Y) \quad (3)$$

最後透過將兩個變數各自的熵相加後相減聯合熵來得到我們想知道的兩變數之間的相互資訊值 I(X；Y)。

在基因選取的方法中，使用相互資訊值作為搭配比較有名的有“minimum redundancy maximum relevance”(簡稱 mRMR) [7]，此方法訂定兩個目標，目的希望能夠找出基因與類別之間關聯性高的(稱為 Relevance，簡稱 Rel)及基因與基因之間關聯性低的情況(稱為 Redundancy，簡稱 Red)。

目標一：基因與類別之間的關聯性

$$Rel_I = \frac{1}{|S|}\sum_{g\in S} I(c,g) \quad (4)$$

為了了解一組基因與類別之間的關聯性(c 為類別，S 為一組基因)，目標一計算基因與類別之間的相互資訊值，並採用平均方法來看一組基因與類別之間的關聯性，希望關聯性越大越好。

目標二：基因與基因之間關聯性

$$Red_I = \frac{1}{|S|^2}\sum_{g_i,g_j\in S} I(g_i,g_j) \quad (5)$$

由於有些基因與基因之間關係呈現高度關聯性，而我們其實只要使用其中一個基因來做代表用於分類也會得到相近的預測效果，不需用整個基因組合的基因作考量，因此目標二的目的是希望基因與基因之間關聯性越小越好，除了避免只使用部分基因當作代表外，也能避免彼此造成影響，所以在目標二中對於基因與基因之間關聯性的測量，同樣是使用相互資訊值作法來測量基因與基因之間的關係(g_i, g_j 皆為一組基因，兩組基因不相同)，不過會希望基因與基因間關聯性越小越好。

由於 mRMR 基因選取作法想找出高的 relevance 且低的 redundancy 基因，所以 mRMR 基因選取的策略為 Mutual information difference(簡稱 MID)，此方法採用前進選擇法(Forward selection)的作法做基因選取：

$$max\ (Rel_I - Red_I) \quad (6)$$

首先會先挑基因與類別之間關聯大的基因進來，接著第二個要挑的基因，會去看是什麼樣的基因進來，會使得整個組合的 Rel_I 很大，Red_I 很小，運用 MID 方法找出能使值最大的基因，當作第二個被選入的基因，第三個被選進來的基因會先考慮第三個加進來後對於原本 Rel_I 與 Red_I 的影響。

雖然 mRMR 是解決兩目標的問題，但此種作法若將解最大化或最小化，最終其實只會得到一個解，在解多重目標的作法中，是不可能找到一個解可以同時最佳化這些目標，反而是找尋那些解可以同時考慮各種目標，並在目標之間求得合理的情況(這些合理情況的解稱為 Pareto set，如圖 1 所示)。

由於我設定的基因挑選作法需同時考慮多重目標，而 mRMR 作法雖有使用到相互資訊值作為基因挑選機制，不過並沒有實際應用在解多目標問題，且此作法也無提到挑選出的基因有多少數量是與類別具有高度相關性，因此 mRMR 方法並不適用在解多目標的問題。後來，我們發現有演化式演算法(Evolutionary algorithm)可以用來解決多目標問題與求取 Pareto set。

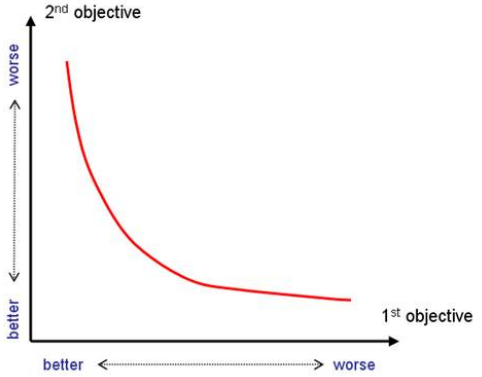


圖 1：Pareto Set 示意圖

3. 多目標演化式演算法

演化式演算法是以達爾文物競天擇的概念發展出來的全域搜尋演算法且被用於解決不同的最佳化問題，此作法的運作機制首先會透過隨機的方式產生初始解，透過適應函數(Fitness function)給予各個解適應各種不同目標的適應值(Fitness score)用以評估解的好壞，並透過突變(Mutation)及交配(Cross-over)來產生新的解，最後用適者生存不適者淘汰的機制來演化，最終目的是希望漸漸找到一個全域最佳解來解決最佳化問題。

演化式演算法用來解多目標問題的方法中較有名兩種方法為 Non-dominated Sorting Genetic Algorithm (簡稱 NSGA-II) [4]與 Multiobjective Evolutionary Algorithm Based on Decomposition (簡稱 MOEA/D) [5][6]。

NSGA-II 方法主要利用隨機產生出來的群體去計算出各自的適應值，根據這些適應值，把這些結果點在空間中，針對非支配解情況(Non-dominated)去作排序，由圖 2 來做說明，圖中同一顏色的解中，我們並無法說明哪個解可以支配誰，根據不同的目標定義，各自有各自好的部分，因此我們同一顏色都當作同等重要，而根據這樣畫出來的結果，我們最終可以得到多組的 pareto set。

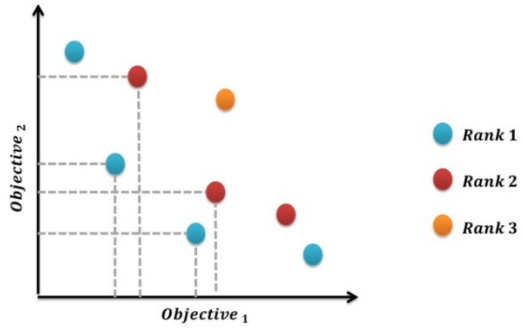


圖 2：NSGA-II 示意圖

MOEA/D 方法也是利用隨機產生出來的群體去進行演化，將隨機群體的資料分成 n 等分，並給予每一等分一個權重值(Weight)，透過權重與鄰居關係的概念把 n 等分的資料化成 n 個單一子目標去進行求解；此作法計算每個解之間的距離，找出每個解的鄰居，如圖 3(a)所示，我們會找尋每一個解附近的鄰居。接著我們會透過適應函數給予這些解適應各種不同目標的適應值，讓每個解與周圍鄰近的鄰居能利用權重和適應值相乘的結果作比較，將好的解取代不好的解並變成下一代繼續演化下去，圖 3(b)為給予隨機群體中每個子目標權重值的示意圖，此範例設定兩個目標讓解進行演化並給予 n 個子目標權重值(不同目標之權重值相加總合為 1)，因此每個子目標有各自目標的權重值與適應值。而每次在進行演化時，還會給予一個參考點(Reference point)用來與目前空間中的解做比較，希望最後解能夠像 pareto graph 一樣往最佳化目標的方向前進，圖 3(c)為參考點的設定方式，圖中的解有各自符合不同目標的適應值，從圖中的 A 點來看，此解在目標一有最佳狀況，B 點在目標二有最佳狀況，因此我們會取 A 點與 B 點各自的適應值做組合，組成此代演化的參考點，供所有解與此參考點做比較並演化。當做完所有演化世代(Iteration)後，最後一代的解就是每個子目標的最佳化解，如圖 3(d)所示，由於此範例最小化兩個目標，因此解的走向會往左下角移動；藍色的點為一開始隨機選取的初始解，紅色點則為經過設定目標演化過後產生的符合每個子目標的最佳化解。所以 MOEA/D 的作法，我們可以想像成是 NSGA-II 方法中最終解集合裡的那一組解(如圖 2 中藍色點)。

由於微陣列晶片資料上面擁有數萬個基因的資訊，當同時將這些資料使用演化式演算法進行演化時，會因為搜尋偌大的解空間且有多種的解的情況組合，使得執行時間非常可怕，而 MOEA/D 是把多維度的資料化簡成單一子目標問題針對解空間作搜尋求解，所以此方法需要較少的執行時間且能夠找到較佳的解，因此我們改寫 MOEA/D 的流程，使其能夠適用於基因選取作法。

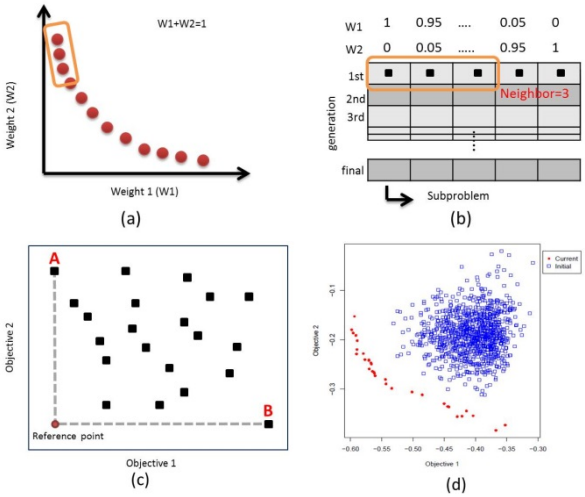


圖 3：MOEA/D 作法示意圖

4. 基因選取機制(FS-ECMOS)

為了將 MOEA/D 作法應用在基因選取機制上面，我們提出以演化式計算模型搭配多目標決策作法(Feature Selection: Evolutionary Computing with Multiobjective Strategy，簡稱 FS-ECMOS)，將每個解定義為與資料中基因數相同長度的二元染色體，以二元染色體編碼的方式來進行演化，當染色體的值為 1 時，代表我們所要挑選的基因，反之，若染色體的值為 0 時，代表我們不挑選的基因。

由於我們目標是希望從微陣列基因晶片資料中找出一組基因，這些基因對於類別有很高的相關性之外，基因與基因之間也具有非線性的關聯性，所以我們訂定以下三個目標：

目標一：一個基因與類別之間的關聯性

$$Rel(g,c) = \left\{\frac{I(g,c)}{H(g)+H(c)}\right\} \times 2 \; ; \; 0 \le Relevance \le 1 \quad (7)$$

對於第一個目標：一個基因與類別之間的關聯性(簡稱 Relevance)，我們採用基因與類別之間的相互資訊值來表示，由於需將資料化成離散的方式做運算，所以當資料型態為連續型資料，我們會先將資料數值轉換至 0 至 1 區間後，再區分為 10 等分的區間，計算每個區間中包含有多少個樣本後再轉換為機率值，估算基因與類別各自的熵(H(g)與 H(c))，並藉此計算基因與類別之間的相互資訊值 I(g, c)，最後用此相互資訊值用以代表基因與類別之間的關聯性(Rel(g, c))。

目標二：一對基因之間非線性的關聯性

$$\mathrm{Dep}(g_i, g_j) = \left\{1 - abs\left(Cor(g_i, g_j)\right)\right\} \times \left\{\frac{I(g_i, g_j)}{H(g_i)+H(g_j)}\right\} \times 2 ; 0 \le Dependency \le 1 \quad (8)$$

針對基因之間的關聯性(簡稱 Dependency)，根據相互資訊值的定義，若兩個基因之間有很大的相互資訊值，那麼就表示兩基因之間具有高度關聯性，同理，若兩個基因之間具有強烈的線性關係，那也表示兩基因之間具有很大的相互資訊值與存在著一定的關係，這樣的一組基因對我們來說是比較不具有參考價值的，因為性質相同的基因，其實只需要拿其中一方的當作代表就好，若同時接拿來參考，有時候造成的結果並不一定比較好，反而會覺得這些基因多餘了，此目標與 mRMR 目標二極大的不同點的地方在於我們是希望找出具有非線性關聯性的基因，因此 dependency 越大越好，而 mRMR 目標二是希望找出基因與基因之間關聯性低的情況，因此 redundancy 越小越好。

因為我們的目標特別著重在於那些具有特殊圖形且擁有非線性關係的基因，且希望找出全都是擁有非線性關係的基因，因此在我們目標二的公式 8 中，我們先針對這 g_i 與 g_j 這兩個不同的基因去算彼此之間的關聯性，而為了保留非線性關聯性的基因，我們設定{1- abs (Cor (g_i, g_j))}用以刪除具有高線性關係的基因，利用此公式用以判別基因之間關係是否具有非線性關聯性。

由於 MOEA/D 挑選的每個解都是一組基因，所以在目標一與目標二的部分，我們參考 mRMR 作法的目標一，使用相互資訊值的平均值來代表一組基因的 relevance 與 dependency，為了使 relevance 與 redundancy 的值能夠比較每組解，我們使用正規化將值控制在 0~1 的區間。

目標三：設定所選用基因的數目

$$no.of.gene = \left\{\frac{1}{[1+(k-n)^2]}\right\}^{exp(-q)} \quad (9)$$

k: targeted number of feature
n: number of feature
q: tunable parameter

針對第三個目標：設定所選用特徵的數目，允許特徵選擇一定數量範圍內的特徵，以控制每個解挑選出的特徵數目，在公式 9，利用我們想取得的基因數目 k 與實際挑選出的基因數目 n 彼此之間差異數量的平方根數與權重參數(q)來控制分數，用以當作評估的條件，讓我們挑出適當數量的特徵數目。

關於 q 值的設定，我們採用 exponential 策略(圖 4)，此策略可以有效控制選用基因的數目在一定範圍之內，假設我們想將選到的基因數目大約控制在比較小的範圍內，那麼我們可以將 q 值設定的比較小，這樣透過目標三算出來的分數，會使不同基因數目的控制分數彼此之間差異很大，使得不在我們想選的範圍之內的基因數目就比較不會被我們挑選到，反之，若我們將 q 值設定的很大，那根據基因數目算出來的控制分數彼此之間差異不大，會使得比較難將選用的基因數量控制在一定範圍之內。

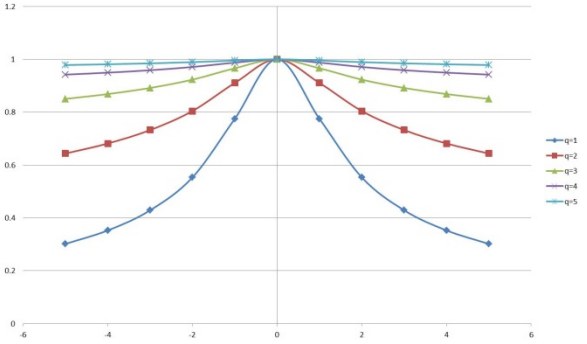


圖 4：權重(q)設定策略

圖 5 為整個搭配多目標作法的基因選取流程圖，由於此方法是只是改變 MOEA/D 的流程使其適用於基因選取，但還是如同一般演化式計算的方法，還需指定族群數目、演化世代、突變機率、交配機率值等。

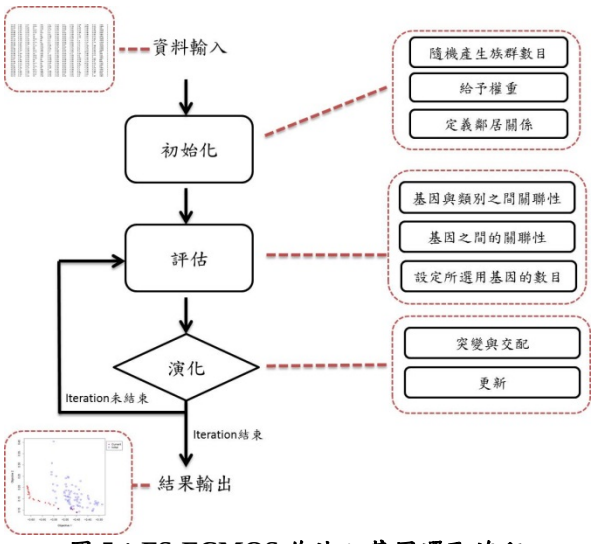


圖 5：FS-ECMOS 作法之基因選取流程

步驟一：初始化

首先會根據設定的族群數目，在解空間中隨機產生族群，接著會將這些隨機產生的族群轉成可以適用在解最佳化的問題，並給予各個族群權重，在 MOEA/D 作法中，此作法能夠比 NSGA-II 執行更快速的原因是因為 MOEA/D 透過鄰居關係的方式，將多目標問題轉化成單一子目標問題去做，所以我們利用歐幾里得距離(Euclidean distance)的方法，去找出與每一個子問題相近的鄰居，進而彼此比較。

步驟二：評估

在此步驟，我們會知道哪些基因是已經被選取到的，因此我們會將這些被選取到的基因去根據我們設定的目標，利用相互資訊值作法去計算 relevance 與 dependency，由於我們希望找到基因與類別之間具有高度相關性與基因之間具有非線性關係的基因，為了最後在圖形呈現上符合我們的視角，我們皆最小化這兩個目標的值，使其畫出來的圖類似 pareto graph，此外，透過設定的第三個目標讓基因只能選擇一定範圍內數量的基因。

步驟三：演化

我們會先從每個子問題與其鄰居中隨機挑選兩個解當作親代(parent)，根據交配機率來設定與解長度相同的二元染色體後隨機選取，若選取到的位置等於 1，那麼親帶會依據這個被選取到的位置，讓彼此同一邊的染色體作交配；而在突變的步驟，首先我們會根據步驟二產生的 relevance 值去針對基因排序，利用與做交配方式一樣的作法，隨機選取一個位置，若此二元染色體的位置的值為 1，那麼便對此位置做突變，同時也在另外沒被選到的位置上作突變，會這樣做的目的是希望能讓解往結果好的方向演化。

當我們做完突變與交配的步驟之後，我們會得到兩條新的子代染色體，這兩條子代染色體會與親代的染色體與鄰居做比較(利用權重和適應值相乘的結果)，將結果比較好的解留下來，繼續做演化。

步驟二與步驟三會重複做直到設定的演化世代結束，演化結束我們得到的族群中有很多個解，每個解都是一個子問題最好的解。

5. 結果

我們使用小圓藍細胞腫瘤(Small round blue cell tumors，簡稱 SRBCT)資料來套用我們的演化式計算模型搭配多目標決策作法 (Feature Selection: Evolutionary Computing with Multiobjective Strategy，簡稱 FS-ECMOS)，SRBCT 資料擁有 2308 個基因，63 個樣本與 4 種不同亞型的腫瘤(EWS、BL、NB 與 RMS)。

在 FS-ECMOS 做法中，我們指定族群數目為 1000、演化世代為 50、突變機率為 0.7、交配機率為 0.9，q 值為 1，並將基因數目控制在 2~5 的範圍內以利觀察探究，為了使挑出來的基因組合性更多，此實驗重複進行 30 次，此外我們透過最近鄰居分類法(Nearest neighbor classification，簡稱 NNC)結合交叉比對(Leave-one-out cross validation，簡稱 LOOCV)策略，針對挑選出來的基因組合去計算對於 SRBCT 資料分類的準確性(Accuracy)。

我們特別針對基因之間、基因與類別之間的資料去計算相互資訊值與皮爾森相關係數。計算之後，發現兩種相互資訊值的分布情況皆大部分落於 0.1~0.3 區間之間，而基因間的皮爾森相關係數分布情況大部分落在-0.3~0.3 區間之間。因此我們認為，在計算基因之間、基因與類別之間的關聯性時，只要相互資訊值大於 0.3，我們就認為彼此之間關聯性很高。基因之間的線性關係值為-0.3~0.3 之間時，則表示基因間線性關係不強烈。

表 1 為透過 FS-ECMOS 作法做基因挑選的部分結果，表中除了列舉該基因組合為哪些基因組合而成的之外，我們還將此組基因拆成成對的方式，針對成對的基因計算基因與類別之間的相互資訊值、基因與基因之間的相互資訊值、基因之間的線性關係以及對於 SRBCT 資料分類的準確性。

Solutions	Gene pair	F1vs. Classes	F2 vs. Classes	b/w Fs	Cor	Group Acc.
1389 1434	1389:1434	0.4682	0.3812	0.3029	0.046	0.8254
1389	1389:1434	0.4682	0.3812	0.3029	0.046	
1434	1389:2159	0.4682	0.2931	0.355	-0.0598	0.8889
2159	1434:2159	0.3812	0.2931	0.2841	-0.1393	
	552:867	0.299	0.3818	0.2984	-0.0034	
552	552:1389	0.299	0.4682	0.2919	-0.2864	
867	552:2159	0.299	0.2931	0.3241	-0.416	0.9524
1389	867:1389	0.3818	0.4682	0.2964	-0.332	
2159	867:2159	0.3818	0.2931	0.3062	0.2094	
	1389:2159	0.4682	0.2931	0.355	-0.0598	

表 1：FS-ECMOS 作法之部分結果

從表 1 的結果中，我們可以列舉幾個有趣的觀察現象：(1)從欄位 3 與欄位 4 來看，基因組合中個別基因與類別之間的相互資訊值很高；(2)欄位 5 的基因組合中的基因與基因之間的相互資訊值很高；(3)從欄位 6 中可以觀察到此結果符合我們目標二的設定，將基因之間高線性關係的組合拿掉，保留基因與基因之間線性關係低的(以平均模式做觀察)；(4)各組基因對於 SRBCT 資料做分類的準確率很高；在這幾個有趣的觀察現象中我們可以得知 FS-ECMOS 作法挑出來的基因組合有符合我們基因選取機制所設定的目標，挑出個別基因與類別之間相互資訊值高、基因與基因之間具有非線性關聯性的基因，且將基因數目控制在 2~5 的範圍之間。

為了瞭解各組基因對於 SRBCT 資料的分類效果，我們使用 Multidimensional Scaling (簡稱 MDS plot)將資料降成兩個維度的情況來對基因做檢視，圖 6 為各組基因中的其中一組(表 1 中的第三組，基因組合為基因 552、基因 867、基因 1389 與基因 2159)，從圖中可以觀察到藉由我們的 FS-ECMOS 作法篩選出來的基因組合可以使不同類別之間有好的區

隔力。

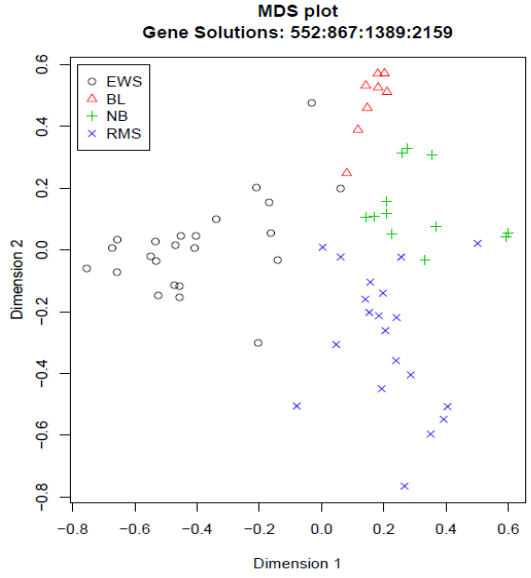


圖 6：FS-ECMOS 作法中 4 個基因組合的 MDS plot

6. 討論與結論

我們除了使用 SRBCT 資料套用我們的 FS-ECMOS 作法之外，還使用了 mRMR 方法中的前進選擇法(Forward selection)策略來做基因選取，表 2 為以 mRMR 作法做出的部分結果，我們選擇透過前進選擇法選出的前四名的基因，將這前四名的基因分別組合，分別以前 2 名基因、前 3 名基因、前 4 名基因的組合情況將各組基因拆成成對的模式，針對這些成對基因計算基因與類別之間的相互資訊值、基因與基因之間的相互資訊值、基因之間的線性關係及使用 NNC 結合 LOOCV 策略計算此組基因對於資料分類的準確性，再運用此結果與我們的 FS-ECMOS 作法做比較。

從表 2 中我們可以觀察到幾個有趣的現象：(1) 欄位 3 與欄位 4 的基因組合中個別基因與類別之間的相互資訊值很高；(2) 欄位 5 的基因組合中的基因與基因之間的相互資訊值很低；在這幾個觀察現象中，我們也可以得知，mRMR 作法挑選的結果符合基因與類別之間關聯性高的及基因與基因之間關聯性低的情況。

Solutions	Gene pair	F1vs. Classes	F2 vs. Classes	b/w Fs	Cor	Group Acc.
1389	1389:846	0.4682	0.363	0.161	-0.2392	0.8413
846						
1389	1389:846	0.4682	0.363	0.161	-0.2392	
846	1389:255	0.4682	0.3346	0.1562	-0.3376	0.8889
255	846:255	0.363	0.3346	0.1172	-0.2606	
	1389:846	0.4682	0.363	0.161	-0.2392	
1389	1389:255	0.4682	0.3346	0.1562	-0.3376	
846	1389:1955	0.4682	0.4036	0.256	-0.3455	0.9048
255	846:255	0.363	0.3346	0.1172	-0.2606	
1955	846:1955	0.363	0.4036	0.1898	-0.0797	
	255:1955	0.3346	0.4036	0.134	-0.1944	

表 2：mRMR 作法之部分結果

根據不同方法觀察到的有趣現象，可以得知 FS-ECMOS 作法除了對於 SRBCT 資料做分類的準確率很高之外，也能讓我們找出基因與基因之間線性關係低的解組合；從我們的 FS-ECMOS 作法與 mRMR 作法來比較，由於我們所設定的目標一(方程式 8)與 mRMR 設定的目標一(方程式 4)類似，，因此我們從表 1 與表 2 中觀察到的現象，均有基因組合中個別基因與類別之間的相互資訊值很高的情況，不過在目標二的地方，由於 mRMR 設定要找尋基因與基因之間關聯性低的情況，所以較沒辦法保留基因與基因之間相互資訊值高的基因組合，因為會被 mRMR 基因選取策略 MID 篩選，而我們的作法則是希望找出具有非線性關係的基因，且保留基因與基因之間相互資訊值高的基因組合，從此目標的結果上我們能夠得知我們方法與 mRMR 作法的差異，此外，從表 1 的欄位 6 也能觀察出我們挑出的解組合的線性關係低(以平均模式作觀察)，符合我們希望找出非線性關聯性基因的目標，而在 mRMR 中作法則無對基因之間的線性關係作探究。

mRMR 的前進選擇法策略最後只能挑出一組基因，而使用我們演化式計算模式的多目標決策作法，因為此作法是搜尋所有的解空間，找出同時符合多個目標的解組合，所以在分類效果上因我們的方法找尋較好的結果，因此在分類效果上會比 mRMR mRMR 作法來得好。

不過，針對我們的方法，我們的解組合目前是使用平均狀況來對線性關係作評估，所以有些基因對的線性關係或許還是會比較高，所以我們希望未來我們能夠再針對我們的目標做一些調整，將那些基因對線性關係高的解組合作篩選，使得挑出的結果能夠更符合我們的目的且能夠再針對基因與基因之間關係為非線性的圖形做更深入的探討。

參考文獻

[1] Isabelle Guyon, Andr'e Elisseeff. (2003) "An Introduction to variable and Feature Selection." Journal of Machine Learning Research, vol. 3, pp. 1157-1182.

[2] Huan Liu, Hiroshi Motoda. (1998) Feature Selection for knowledge Discovery Data Mining. Kluwer Academic Publishers, Norwell, MA.

[3] Yvan Saeys, Inaki Inza and Pedro Larranaga. (2007) "A review of feature selection techniques in bioinformatics." Bioinformatics, vol. 23 pp. 2507-2519.

[4] Kalyanmoy Deb, Associate Member, IEEE, Amrit Pratap, Sameer Agarwal, and T. Meyarivan. (2002) "A Fast and Elitist Multiobjective Genetic Algorithm: NSGA-II." IEEE Transactions on Evolutionary Computation, vol. 6, pp. 182-197.

[5] Qingfu Zhang, Senior Member, IEEE, and Hui Li. (2007) "MOEA/D: A Multiobjective Evolutionary Algorithm Based on Decomposition." IEEE Transactions on Evolutionary Computation, Vol. 11, pp. 712-731.

[6] Hui Li and Qingfu Zhang, Senior Member, IEEE. (2009) "Multiobjective Optimization Problems With Complicated Pareto Sets, MOEA/D and NSGA-II." IEEE Transactions on Evolutionary Computation, Vol. 13, pp. 284-302.

[7] Chris Ding, and Hanchuan Peng. (2003) "Minimum Redundancy Feature Selection for Microarray Gene Expression Data." IEEE, pp. 523-528.

演化式計算輔助整合特徵模型預測蛋白質瓜胺酸化位置

陳啟瑋　　洪慧芝　　朱彥煒
國立中興大學基因體暨生物資訊學研究所
ywchu@nchu.edu.tw

摘要

蛋白質瓜胺酸化(Citrullination) 藉由胜肽精胺酸脫亞胺酶(Peptidylarginine Deiminase，PAD) 將受質蛋白上的精胺酸轉變成不帶電的瓜胺酸，瓜胺酸化與類風濕性關節炎、多發性硬化症和阿茲海默症等疾病有關。由於受限於目前的資料量，現今尚未有針對瓜胺酸化的相關工具提供使用。因此，本研究發展一套針對資料量不足情況下，使用機器學習建構預測模型之實驗方法，並用於發展蛋白質瓜胺酸化位置預測工具。從 8 種特徵；文獻收錄之催化規則、序列相似度、演化保留訊息、胺基酸理化和生化特性、二級結構、蛋白質不穩定結構及結構表面可接觸性，透過資料與編碼後產生解決出不同解決問題能力的預測模型，進而透過整合方式獲得進一步提升的預測能力。而在機器學習的過程中，要如何調整適當的學習權重以獲得較佳的預測模型，本研究以基因演算法並支持向量機作為適性函數，挑選出適合之特徵權重最為訓練。其過程中並與前人文獻中之胜肽精胺酸脫亞胺酶催化規則有所呼應，最終生物意義並打破以往挑選最佳預測模型方式，以模型學習過程及特徵重要性做為評估方式。最終模型準確可達 Sn：0.79、Sp：0.98、Acc：0.89 及 MCC：0.79。

關鍵詞：瓜胺酸化、胜肽精胺酸去亞胺酶、支持向量機、基因演算法、特徵選擇。

1. 前言

胜肽精胺酸脫亞胺酶 (Peptidylarginine Deiminase，PAD) 屬於蛋白質轉譯後修飾酵素之一，當 PADs 與鈣離結合使催化中心結構改變，進而得以和受質結合，將蛋白質上帶正電的精胺酸(Arginine) 轉變成不帶電的瓜胺酸(Citrulline)，其過程稱為瓜胺酸化(Citrullination 或 Deimination)[1-4]。

PADs 有五種異構型(Isoforms)， PAD1-4 及 PAD6，並具有組織分布特異性，各自分布在特定的組織細胞中[5-8]。PAD1 位於皮膚表皮；PAD2 可見於各類器官，包括腦、骨骼肌、子宮、胰腺、涎腺、垂體腺、汗腺、脾、巨噬細胞和骨髓等。PAD3 表現於毛髮之毛囊細胞；PAD4 主要表現在淋巴細胞、內皮細胞、單核細胞和巨噬細胞，而 PAD6 主要表現在胚胎幹細胞與卵母細胞。其瓜胺酸化反應將受質蛋白質上，帶正電荷的精胺酸轉變成中性不帶電的瓜胺酸，可能造成蛋白質的構型改變，進而失去蛋白質原有之功能。蛋白質瓜胺酸化所牽涉的生理過程包括：上皮終端分化(Epithelial Terminal Differentiation)、神經生長、胚胎發育、基因表現之調節 (Gene Expression Regulation) 及細胞凋亡 (Apoptosis)。而病理表現則目前已知與類風濕性關節炎、多發性硬化症和阿茲海默症 (Alzheimer' s Disease) 等疾病有關[3, 5, 9-11]，其中 PAD4 是唯一具有細胞核定位訊號(Nuclear Localization Signal)，可使蛋白經由膜孔到細胞核中，主要表現於淋巴細胞、內皮細胞、單核細胞和巨噬細胞，此外，近幾年的文獻指出，PAD4 調節真核細胞中的基因的轉錄，並與 p53 在 DNA 修復都有密切的關係[12]。

然而，對於胜肽精胺酸脫亞胺酶，其受質之序列特定性以及蛋白質專一性，目前並不清楚，且其受質參與細胞內的調控路徑目前尚未全然釐清。若要進一步探究蛋白質瓜胺酸化所造成的結果，在生物上之意義或與疾病之相關性，尚須鑑定蛋白質瓜胺酸化，進而了解其生物作用與功能途徑[13]。因此有研究利用蛋白質陣列試圖尋找胜肽精胺酸脫亞胺酶之受質[14]。但人類蛋白質數量龐大且生物實驗費時費力，若能藉由資訊的計算提供最有可能之瓜胺酸化受質蛋白，可能將幫助實驗減少所需花費的金錢與時間。

但目前也無相關工具輔助實驗設計，為此，本研究主要在於建構瓜胺酸化預測工具，可望幫助生物學家尋找可能做為 PAD 受質之蛋白質，提供輔助實驗設計方向的建議資料，進一步做更深入的分析與討論。瓜胺酸化屬於蛋白質轉譯後修飾中的一種，而有收錄蛋白質轉譯後修飾相關資料的 Swiss-Prot 或 HPRD (Human Protein Reference Database) 等資料庫中，較多資料的為磷酸化、乙烯化、甲基化等，也因為這些數量較為豐富的後修飾非常適合利用數學、統計等領域並配合電腦的計算建構預測模型，許多這類後修飾的預測工具如雨後春筍般的被開發出來，對於資料量甚少的後修飾較為無人問津。而瓜胺酸化也同那些資料過於少量的後修飾一樣，有其生物上的重要性卻礙於目前現有資料而遲遲無法以生物資訊發展輔助工具，但這些資料量較不豐富的後修飾中存在著共同的因子，乃推測的資料多過實驗所證實之數量。然而，推測資料雖少部分可能是藉由實驗資料所做出的推測，其中包含著錯誤待實驗驗證之資料，但對於預測模型的好壞其必須包含容錯性，才具有將目前

資料以外的未知資料做出正確的預測。

基於此論點，本研究進而嘗試克服以資料量少無法建構預測模型之問題，並用以解決瓜胺酸化預測模型之建構，設計一套對於資料量不足的情況下所用之發展預測模型之方法，將所有的推測資料及實驗資料做為訓練集測試資料集，以 8 種特徵編碼產生不同性質之預測模型，進而將不同特徵編碼之模型所預測之結果利用整合方式建構第二層預測模型。並以基因演算法尋找其 8 種特徵其各自的重要性權重，進一步提升預測準確度其準確度達 0.80。

2. 材料與方法

2.1 蛋白質瓜胺酸化資料集

首先，必須先建立一個資料正確的瓜胺酸化資料集。處理的資料來源便是 UniProt 資料庫，UniProt 是現今最廣泛被利用的線上蛋白質資料庫之一，其 Protein knowledgebase (UniProtKB) 中包含兩個部分，分別為人工註解的 Swiss-Prot 與自動註解的 TrEMBL 資料集，而 Swiss-Prot 收錄的註解與文獻等資訊由專業的生物學家所提供，其準確性無庸置疑，因此本研究從中擷取與瓜胺酸化有關的蛋白質資料，共 84 個蛋白質 141 個瓜胺酸化位置，而 84 個蛋白中包含了 64 個組織蛋白(Histone)、10 個 MBP 蛋白(Myelin Basic Protein)、8 個 CXL(C-X-C Motif Chemokine) 和 2 個其他種類蛋白質。除了 UniProt 資料庫之外，並從 HIstome 人類組織蛋白轉譯後修飾資料庫中，獲得額外的組織蛋白瓜胺酸化位置共 6 筆。

使用一個完整、正確且資料量大的資料集，有利於使用機器學習方法做預測，然而，從 UniProt 中獲得了 141 個瓜胺酸位置，其中推測的位置有 109 筆，實際實驗之位置則有 32 筆，面臨到資料量過少，可能不足以反映瓜胺酸化問題之學習樣本。而推測之樣本數為實驗資料的 3 倍多，因此，本研究嘗試以推測之資料做為學習樣本，希望以此建構的預測模型，能預測出實驗之瓜胺酸位置。剔除推測與實驗衝突之瓜胺酸位置後，93 個推測之瓜胺酸位置資料集命為 S93 做為訓練預測模行之用，而從 UniProtKB 及 HIstome 收集實驗之 38 個瓜胺酸位置命為 S38 做測試之用。

在資料的處理上，將蛋白質上有註解精胺酸 (Arginine) 發生瓜胺酸化之蛋白質挑出做為 Positive data 瓜胺酸化位置，而蛋白質序列上其餘沒註解的精胺酸視為 Negative data 非瓜胺酸化位置。S38 的 Negative data 為 376 筆，S93 的 Negative data 為 768 筆。然而，以機器學習建構預測模型的過程中， Negative data 的使用將會影響模型的好壞，Positive 與 Negative 若數量差距過大往往造成學習產生偏頗的現象，因此本研究以 Positive 與 Negative 數量 1 比 1 的比例隨機挑選 Negative。

2.2 胜肽精胺酸去亞胺酶催化規則

使用機器學習方法建構預測模型需要一個完整、正確且資料量大的資料集，才可能做出較為準確的預測，而瓜胺酸化目前在蛋白質後修飾資料庫中，收錄的筆數甚少。因此，本研究從前人研究所發表的文獻中，收集可能之瓜胺酸化催化特性規則，希望以此規則輔助可能尚未足以代表瓜胺酸化問題空間的資料集，進行預測模型的建構。

由 Tarcsa *et al.*[15]與 György *et al.*[5]獲得 PADs 可能對於蛋白質一級結構和二級結構上的催化規則。 從 Kyouhei *et al.*[4]獲得 PAD4 偏好受質組織蛋白(Histone) 上精胺酸位於 N 端或 C 端。此外，於 Stensland *et al.*[16]獲得組織蛋白與聚角蛋白微絲蛋白(Filaggrin) 之瓜氨酸化位置周圍胺基酸組成可能偏好特性。

為了測試收集之規則，是否與目前已知的瓜胺酸化資料有所衝突，進一步以規則比對 S93 及 S38 資料集內的瓜胺酸與非瓜胺酸化位置，其中二級結構以 PSIPRED 預測工具取得結構資訊。

2.3 特徵模型

本研究主要使用機器學習做為預測方法，首先必須將資料抽象化，從中提取出做為學習之特徵，若所選擇之特徵較符合問題空間，可能獲得較佳之預測結果。因此，特徵的好壞影響預測其準確度。若要使電腦能夠自動對資料提取出特徵，作為分類之用所牽涉之技術較為複雜。為此，本研究以 PADs 受質喜好特性規則(Rule)、胺基酸向量化(Binary)、演化保留訊息(PSSM)、胺基酸理化和生化特性(AAIndex)、二級結構(Secondary Structure)、蛋白質結構穩定性(Disorder) 及蛋白質結構可接觸性與二級結構(Surface Accessibility and Secondary Structure) 做為特徵，分別依照不同特徵以 LIBSVM 實現支持向量機建構預測模型，進而評估與探討其資料在不同編碼下之特性。

2.3.1 規則編碼

藉由文獻收集之 PADs 受質可能喜好規則，包含一級結構 5 條規則、二級結構 4 條規則及精胺酸周圍四個位置喜好與非喜好之胺基酸 8 條規則，共 17 條規則，依照其規則與序列及結構匹配度編碼為：匹配 1、不匹配 0。其中精胺酸接近 N 端或 C 端評估方式為：該精胺酸位置除以蛋白質序列總長，若該值小於等於 0.3 或大於等於 0.7 將被視為接近 N 或 C 端，其編碼為 1，反之則為 0。一條序列片段將測試 17 個規則，並編碼為長度 17bit 的特徵值。但其規則參考之精胺酸周圍資訊甚少，一級結構僅一個胺基酸，或上下游 2 個胺基酸，二級結構僅考慮精胺酸結構，可能使機器學習過程中遺漏掉重要的訊息，因此，也進一步測試其他使用精胺酸周圍訊息之編碼。

2.3.2 胺基酸向量編碼

機器學習常將一筆資料以向量的方式表示，故將 20 種胺基酸包含 Gap，以 20 個維度之向量做編碼，該胺基酸所占之維度設為 1，例如：A 為[1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0] 、 Y 為[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1]，所有編碼為表 3.5 所示。因此，一個胺基酸以 20 個維度之向量所表示，共有序列片段胺的基酸數量乘上 20 個維度之向量，以胺基酸序列相似性做為機器學習之特徵。

2.3.3 演化保留訊息編碼

此方法利用蛋白質演化訊息作為特徵，蛋白質具有功能的區域其演化過程中較不易產生突變，得以將功能性保留下來，在特定的胺基酸片段下，瓜胺酸化之精胺酸周圍之評分矩陣，通常具有胺基酸保留性的特性，因此可能適合用來做為分類之特徵。本研究利用 PSI-BLAST 將蛋白序列對 NCBI nr (Nonredundant) protein dataset v2010_07_23 做比對，以指令 “blastpgp -d nr -i Preotein.txt -j 3 -h 0.001 -o Preotein.out -Q Preotein.pss”獲得每個胺基酸在該位置之演化保留分數，其輸出之結果如圖 2.7，因此，一個胺基酸有 20 個突變機率分數，編碼方式共有序列片段的胺基酸數量乘上 20 個維度之向量。

2.3.4 胺基酸理化與生化特性編碼

AAindex (Amino Acid Index Database) 收錄五百種以上藉由實驗所定義的胺基酸理化和生化特性，而要在眾多的特性中選擇適合用以解決問題的胺基酸特性較為不易。而有研究 William *et al.*將其胺基酸性質依照相似性簡化其繁多的特性，而 Mathura *et al.*從文獻中整理並歸納 5 種特性。William 簡化成 Polarity、Secondary structure、Molecular size or volume、Codon diversity 及 Electrostatic charge 5 種，Mathura *et al.* 歸納為 5 種特性；Hydrophobicity、Side chain length、α-helix propensity 、 Number of codons 及 β-strand propensity，每個胺基酸擁有一個數值來代表其理化及生化特性，例如 Side chain length 較短的 Glycine 值越大，Side chain length 較長的胺基酸其值越小。進一步將兩篇研究將眾多的胺基酸特性化中簡為 5 種特性的結果，藉由皮爾森相關係數計算其兩組簡化結果之間的相似性，如表 1。僅只有 Hydrophobicity 與 Polarity 有 0.7 以上較高的相似度，因此將兩篇研究所歸納之胺基酸特性結果視為兩種特徵做編碼之用，一個胺基酸將有 5 個值所表示，共有序列片段的胺基酸數量乘上 5 個維度之向量。

2.3.5 二級結構編碼

從文獻中發現，PADs 的受質喜好與結構有相關，因此若以蛋白質結構做學習之特徵可能有助於預測，但並非所有蛋白質被解結構，而較大的蛋白質其結晶結構也並非完全，導致以資訊方法解決問題將有所限制，為此，本研究以二級結構預測工具 PSIPRED 獲得蛋白質序列其可能的結構資訊。PSIPRED 提供三種二級結構的預測分別為 Helix、Strand 及 Coil，以及對該位置所做的預測信心分數(Confidence Score)，。進而將 Helix 編碼為 100、Strand 編碼為 010、Coil 編碼為 001 及 Gap 編碼為 000，包含預測信心分數一個胺基酸以 4 個值表示，共有序列片段的胺基酸數量乘上 4 個維度之向量。

表 1 Mathura 和 William 兩編碼相關係數

	hydrophobicity	side chain length	α-helix propensity	number of codons	β-strand propensity
Polarity	0.80	-0.55	0.13	-0.13	0.03
Secondary structure	0.39	0.60	0.66	-0.08	-0.13
Molecular size or volume	-0.34	-0.15	0.13	-0.11	-0.03
Codon diversity	0.17	0.49	-0.56	-0.57	-0.09
Electrostatic charge	-0.11	-0.13	0.14	-0.19	-0.24

2.3.6 蛋白質結構穩定性編碼

根據 Kyouhei *et al.*及 György *et al.*均認為不穩定結構 (Disorder) 對於 PADs 存在重要性，因此也加入該結構做為學習之特徵，可能將有助於預測。為此，本研究以不穩定結構預測工具 DISOPRED 獲得蛋白質序列其可能的結構資訊。DISOPRED 提供兩種結構的預測，分別為穩定 (Ordered) 與不穩定 (Disorder)，以及該位置不穩定可能性分數 (Disorder Probability)，若該值大於門檻值將預測為不穩定。進而將一個胺基酸以 2 個值表示，穩定編碼為 0、不穩定編碼為 1 及可能性分數，共有序列片段的胺基酸數量乘上 2 個維度之向量。

2.3.7 蛋白質結構可接觸性與二級結構編碼

胺基酸胜肽透過折疊使蛋白質產生有功能的構型，其中胺基酸位於蛋白質內或蛋白質外對於研究蛋白質之間的交互作用以及三級結構有非常大的重要性。而酵素與受質結合進行催化與結構表面可接觸性可能也具有影響，因此，從 NetSurfP ver. 1.1 獲得蛋白質結構表面可接觸性預測資訊，其提供資訊。其預測結果提供二級結構可能性分數、Relative Surface Accessibility、Absolute Surface Accessibility 以及胺基酸可能為 Buried 或 Exposed 共 7 個資訊，進而將一個胺基酸編碼為 Buried；10、Exposed；01、Gap；00 及 5~10 欄位之值，共有序列片段的胺基酸數量乘上 8 個維度之向量表示。

2.4 第二層預測模型

本研究以 PADs 受質喜好特性規則(Rule)、胺基酸向量化(Binary)、演化保留訊息(PSSM)、胺基

酸理化和生化特性(AAIndex)、二級結構(Secondary Structure)、蛋白質結構穩定性(Disorder) 及蛋白質結構可接觸性與二級結構(Surface Accessibility and Secondary Structure) 做為特徵，分別依照不同特徵建構預測模型。然而使用不同特徵所建構之預測模型，具有其不同的預測之特性及效能，為整合不同特性之預測模型，進而將 8 個特徵之預測結果透過支持向量機建構第二層預測模型，以進一步提升預測準確度。

2.5 演化式計算搜尋特徵模型權重

使用不同特徵所建構出的預測模型，其具有解決不同問題之能力，再加上使用之訓練資料與其中負向資料的差異，使得不同編碼與訓練資料產生更為複雜且較難選擇適合解決問題之模型。且並非所有特徵都適合用來解決瓜胺酸化預測的問題，因此勢必將調整 8 種特徵模型其權重，以改善第二層預測模型之學習效果。

為解決該問題，本研究利用基因演算法(Genetic Algorithm) 尋找每個特徵之重要性權重分數。其基因演算法參數設置為：Crossover rate 0.7、Mutationrate rate 0.05、Population 200、Chromosome length 40、Generations 20。

自然界中的染色體隱含著遺傳等訊息，而在人工的基因演算法染色體隱藏著解決問題的答案，因此以 40 個 0 與 1 組成 40Bit 2 進制長度的染色體，8 個 Bit 表示 1 個權重，再透過轉換成 10 進制除以 8Bit 最大值 31 做為權重值。該權重乘上特徵模型 1 預測之信心分數，做為特徵模型選擇所需建構模型之輸入，其模型以測試資料之準確度 (MCC) 做為該染色體之適應分數 (Fitness Value)，準確度越高表示適應分數越大，使得在演化過程中得以被保留並可能成為最終獲得之解答。

2.6 預測模型效能評估

當預測結果為瓜胺酸化位置且實際亦為瓜胺酸化則為 True Positive (TP)，若預測結果為瓜胺酸化位置但實際為非瓜胺酸化為 False Positive (FP)，而預測結果為非瓜胺酸化位置但實際卻為瓜胺酸化則為 False Negative (FN)，預測結果為非瓜胺酸化位置且實際亦非瓜安酸化為 True Negative (TN)。將利用下列公式評估預測系統的準確性。Matthews Correlation Coefficient (MCC) 顯示 Positive 和 Negative 的相關度，其值最大為 1 表預測完全正確，最小為-1 表示預測完全與正確結果相反 ，其公式如下：

$$MCC = \frac{(TP \times TN) - (FN \times FP)}{\sqrt{(TP+FN)\times(TN+FP)\times(TP+FP)\times(TN+FN)}} \quad \text{(Eq. 4)}$$

Accuracy (Acc)，顯示整體預測結果的預測正確率，其公式如下：

$$Acc = \frac{TP+TN}{TP+FP+TN+FN} \quad \text{(Eq. 5)}$$

Specificity (Sp)，顯示預測結果對於非瓜胺酸化位置的辨識能力，其公式如下：

$$Sp = \frac{TN}{TN+FP} \quad \text{(Eq. 6)}$$

Sensitivity(Sn)，顯示預測結果對於瓜胺酸化位置的辨識能力，其公式如下：

$$Sn = \frac{TP}{TP+FN} \quad \text{(Eq. 7)}$$

3. 結果與討論

3.1 特徵模型預測準確度

將 8 種特徵編碼分別建構 8 個預測模型，以及將 8 種特徵混合建構一個預測模型，共 9 種方式建構預測模型，以三組交叉驗證方式評估準確度，其結果如表 2。並以 S38 測試其預測準確度，結果如表 3。由表 2 顯示，透過交叉驗證評估發現所有特徵模型，其預測準確度略顯較高。其原因在於透過推測資料整理之訓練集資料間較為相似，而本研究嘗試以推測之資料做為學習樣本，希望以此建構的預測模型，能預測出實驗之瓜胺酸位置。因此由實驗資料整理之測試集，其準確度優劣才是本研究著重的焦點。

然而，不同特徵編碼其可解決之問題也不盡相同，從表 3 測試結果可發現蛋白質不穩定結構(Disorder) 與蛋白質結構可接觸性與二級結構(NetSurfP) 對於大部分瓜胺酸化位置有較高的預測準確度，這呼應了胜肽精胺酸脫亞胺酶在選擇受質催化規則中的特性。而其餘特徵編碼可能善於預測非瓜胺酸化位置。在使用所有 8 種豐富且能解決不同問題空間的特徵編碼模型中(All)，未能獲得較好的預測準確度，正是因為其中存在著干擾學習及不必要之特徵，在以往的研究中，將會以此預測模型進行特徵選擇，使模型預測準確度提高，但在此瓜胺酸化的預測中，資料數量尚未達使用特徵選擇的條件，斷然以特徵選擇提升準確度可能將造成過度擬合(Overfitting)，使得模型的容錯性降低進而無法預測目前尚未確定的瓜胺酸化位置。因此，進而以整合 8 個特徵模型之預測結果，建構第二層預測模型(Meta)。然而，其準確度不及使用所有編碼(All)，其原因可能在於整合的過程中，機器學習對於 8 個特徵模型其重要性尚未掌握，因此勢必將 8 種特徵模型其學習權重再做修正。

表 2 訓練集三組交叉驗證之預測準確度

Training S93	Sn	Sp	Acc	MCC
AAIndex 2005	0.92	0.98	0.95	0.91
AAIndex 2001	0.98	0.98	0.98	0.96
Binary	0.98	1.00	0.99	0.98
DISOPRED	0.92	0.86	0.89	0.79
NetSurfP	0.98	0.95	0.96	0.93
PSIPRED	0.91	0.94	0.93	0.85

PSSM	0.97	0.93	0.95	0.90
Rule	0.87	0.86	0.87	0.74
All	0.99	0.97	0.98	0.96

3.2 演化式搜尋特徵模型權重之預測準確度

不同特徵模型其擅長預測資料不盡相同，反映出訓練資料與特徵編碼產生之差異性。使用 8 種不同特徵建構 8 個預測模型，以其預測結果之信心分數做為建構第二層模型之輸入，準確度 Sn 達 0.71、Sp 0.97、Acc 0.85 及 MCC 0.72。透過基因演算法調整其特徵模型適合之學習權重後，準確度 Sn 為 0.79，相較於未調整前權重提升 0.08。而 MCC 也從 0.72 提升至 0.79，上升 0.07。且使用基因演算法調整權重所建構之第二層預測模型，準確度均高於單一特徵模型準確度(MCC)。

表 3 測試集預測準確度

Test S38	Sn	Sp	Acc	MCC
AAIndex 2005	0.68	0.94	0.82	0.65
AAIndex 2001	0.63	0.95	0.80	0.62
Binary	0.71	0.98	0.85	0.72
DISOPRED	0.82	0.71	0.76	0.53
NetSurfP	0.92	0.86	0.89	0.78
PSIPRED	0.74	0.88	0.81	0.63
PSSM	0.66	0.90	0.79	0.59
Rule	0.68	0.94	0.82	0.66
All	0.79	0.95	0.87	0.76
Meta	0.71	0.97	0.85	0.72
GA	0.79	0.98	0.89	0.79

為探討基因演算法找出之權重結果並分析，圖 1 為基因演算法尋找之準確度可達 0.79 的 78 條最佳權重組，及尚未調整前之權重。在未調整前(Meta)使用之權重為 AAIndex 2005：9.71、AAIndex 2001：12.3、Binary：17.32、DISOPRED：1.49、NetSurfP：9.09、PSIPRED：4.03、PSSM：5.24、Rule：1.65，以 Binary 序列相似性視為較重要之特徵，其次為胺基酸理化及生化特性。而藉由基因演算法尋找學習權重，平均 78 條後的權重為 AAIndex 2005：0、AAIndex 2001：0、Binary：0.39、DISOPRED：0.35、NetSurfP：0.69、PSIPRED：0.56、PSSM：0.50、Rule：0.49，以蛋白質結構可接觸性與二級結構較為重要，其次為演化保留性及規則。而在未調整前支持向量機認為有較高重要性之 AAIndex 在基因演算法之下被認為是完全無重要之特徵，這可能是由於 AAIndex 包含許多不同的胺基酸特性，在尚未從其中特性做挑選的前提下，混和多種特性可能因此導致對於解決瓜胺酸化問題便的較無幫助。而基因演算法將其權重調整為零可提升準確度，這也驗證移除會干擾學習之特徵可獲得較好的準確度。

由圖 1 分析 78 條最佳權重組合，有 0.92 預測瓜胺酸化準確度最高的 NetSurfP (藍色)，以及 0.98 最佳非瓜胺酸化預測準確度的 Binary (綠色)，以尋找權重的過程中可以發現，當 Binary (綠色)有較高權重值時 NetSurfP (藍色)權重較低，而 NetSurfP (藍色)權重較高時，則 Binary (綠色)權重較低，還無法使兩者做緊密的結合，這可能是由於這兩種編碼受限於目前訓練資料貧乏之缺陷所導致，或僅演化 20 世代尚未找尋到最佳學習權重。而在第 28 染色體之權重組以 Rule 及 DISOPRED 最高，這也說明文獻中之規則也可扮演機器學習上重要的學習項目。



圖 1 最佳權重組

4. 結論

PADs 與許多疾病有關，如類風濕性關節炎，多發性硬化症，牛皮癬，阿茲罕默症，也關係到細胞抗癌機制作用的過程，但其詳細的調控機制仍未非常明朗。而現今尚未有瓜胺酸化相關的生物資訊工具可供使用，因此，本研究主要在於建構瓜胺酸化預測工具，進而有辦法對未知是否會受該酵素作用的蛋白質序列作預測，幫助生物化學與分子生物研究者在設計蛋白質與研究。

本研究以機器學習方法透過不同特徵編碼與訓練資料產生出不同的解決問題空間之能力，透過整合其 8 種結果建構第二層預測模型，並利用基因演算法調整適當的學習權重，其過程中也驗證學習特徵與文獻規則具有相呼應。最終提升預測準確度並使準確度優於單一特徵模型，模型準確達 Sn：0.79、Sp：0.98、Acc：0.89 及 MCC：0.79。

誌謝

本論文承蒙行政院國家科學委員會之計畫經費贊助，計畫編號為 NSC 101-2221-E-005-085 與 NSC 102-2221-E-005-081，僅此誌謝。

5. 參考文獻

[1] J. E. Jones, C. P. Causey, B. Knuckley, J. L. Slack-Noyes, and P. R. Thompson, “Protein arginine deiminase 4 (PAD4): Current understanding and future therapeutic potential,” Current opinion in drug discovery & development, vol. 12, p. 616, 2009.

[2] Z. Ke, Y. Zhou, P. Hu, S. Wang, D. Xie, and Y. Zhang, “Active Site Cysteine Is Protonated in the PAD4 Michaelis Complex: Evidence from Born− Oppenheimer Ab Initio QM/MM Molecular Dynamics Simulations,” The Journal of Physical Chemistry B, vol. 113, pp. 12750-12758, 2009.

[3] T. A. Cafaro, S. Santo, L. A. Robles, N. Crim, J. A. Urrets-Zavalia, and H. M. Serra, “Peptidylarginine deiminase type 2 is over expressed in the glaucomatous

optic nerve," Molecular vision, vol. 16, p. 1654, 2010.
[4] K. Arita, T. Shimizu, H. Hashimoto, Y. Hidaka, M. Yamada, and M. Sato, "Structural basis for histone N-terminal recognition by human peptidylarginine deiminase 4," Proceedings of the National Academy of Sciences, vol. 103, pp. 5291-5296, 2006.
[5] B. György, E. Tóth, E. Tarcsa, A. Falus, and E. I. Buzás, "Citrullination: a posttranslational modification in health and disease," The international journal of biochemistry & cell biology, vol. 38, pp. 1662-1677, 2006.
[6] C. Foulquier, M. Sebbag, C. Clavel, S. Chapuy- Regaud, R. Al Badine, M. C. Méchin, et al., "Peptidyl arginine deiminase type 2 (PAD- 2) and PAD- 4 but not PAD-1, PAD- 3, and PAD- 6 are expressed in rheumatoid arthritis synovium in close association with tissue inflammation," Arthritis & Rheumatism, vol. 56, pp. 3541-3553, 2007.
[7] E. R. Vossenaar, A. J. Zendman, W. J. van Venrooij, and G. J. Pruijn, "PAD, a growing family of citrullinating enzymes: genes, features and involvement in disease," Bioessays, vol. 25, pp. 1106-1118, 2003.
[8] C. Anzilotti, F. Pratesi, C. Tommasi, and P. Migliorini, "Peptidylarginine deiminase 4 and citrullination in health and disease," Autoimmunity reviews, vol. 9, pp. 158-160, 2010.
[9] M. Moscarello, L. Pritzker, F. Mastronardi, and D. Wood, "Peptidylarginine deiminase: a candidate factor in demyelinating disease," Journal of neurochemistry, vol. 81, pp. 335-343, 2002.
[10] Z. Baka, P. Barta, G. Losonczy, T. Krenács, J. Pápay, E. Szarka, et al., "Specific expression of PAD4 and citrullinated proteins in lung cancer is not associated with anti-CCP antibody production," International immunology, vol. 23, pp. 405-414, 2011.
[11] Z. Baka, B. György, P. Géher, E. I. Buzás, A. Falus, and G. Nagy, "Citrullination under physiological and pathological conditions," Joint Bone Spine, vol. 79, pp. 431-436, 2012.
[12] C. Tanikawa, K. Ueda, H. Nakagawa, N. Yoshida, Y. Nakamura, and K. Matsuda, "Regulation of protein Citrullination through p53/PADI4 network in DNA damage response," Cancer research, vol. 69, pp. 8761-8769, 2009.
[13] S. K. Bhattacharya, "Retinal deimination in aging and disease," IUBMB life, vol. 61, pp. 504-509, 2009.
[14] Q. Guo, M. T. Bedford, and W. Fast, "Discovery of peptidylarginine deiminase-4 substrates by protein array: antagonistic citrullination and methylation of human ribosomal protein S2," Molecular bioSystems, vol. 7, pp. 2286-2295, 2011.
[15] E. Tarcsa, L. N. Marekov, G. Mei, G. Melino, S.-C. Lee, and P. M. Steinert, "Protein unfolding by peptidylarginine deiminase Substrate specificity and structural relationships of the natural substrates trichohyalin and filaggrin," Journal of Biological Chemistry, vol. 271, pp. 30709-30716, 1996.
[16] M. E. Stensland, S. Pollmann, Ø. Molberg, L. M. Sollid, and B. Fleckenstein, "Primary sequence, together with other factors, influence peptide deimination by peptidylarginine deiminase-4," Biological chemistry, vol. 390, pp. 99-107, 2009.

使用機器學習與特徵選擇預測明膠酶的受質切位

張浩禎　　朱彥煒
基因體暨生物資訊學研究所
ywchu@nchu.edu.tw

摘要

明膠酶(gelatinase)有 gelatinase A (MMP-2) 和 gelatinase B (MMP-9)兩型，具有裂解細胞外基質的活性。近來研究指出基質金屬蛋白酶家族在生理和病理機制上，有多種調控，如免疫反應、腫瘤發展和幹細胞分化等。MMP-2、MMP-9 會引發腫瘤轉移，其抑制藥物也進入臨床試驗，成功抑制腫瘤轉移但病人的存活率卻沒有提升，前人探究其原因為基質金屬蛋白酶家族同源性高，結構相似，使得抑制藥物專一性不高；以及對 MMP-2、MMP-9 受質的調控路徑尚未全面了解，以致產生副作用。因此，若能準確預測 gelatinase 之作用受質與位置，有益於其生理和病理作用機制之探討。本預測架構為整合二進制、物理化學屬性、蛋白質不穩定區段和溶劑可接觸性與二級結構等不同類別的資訊、加上我們首先採用的群間差異特徵，配合支持向量機的使用，建立第一層預測模型；接著將其輸出的預測機率做為第二層系統之特徵，同時比較多種機器學習方法來建構第二層的預測系統，MMP-2 及 MMP-9 受質的預測效能分別之馬修斯相關係數為 89.4%和 64.4%。並進一步利用物理化學屬性之特徵選擇，對 MMP-2 與 MMP-9 在活性中心的屬性進行分析，以提供藥物設計時參考。此預測系統建立完成後，有助於發現 MMP-2 與 MMP-9 新的可能受質，以推估其未發現的調控路徑。

關鍵詞：Gelatinase、MMP-2、MMP-9、支持向量機、最近鄰居法、群間差異。

1. 前言

蛋白質轉譯後修飾調控各種細胞代謝過程。常見的轉譯後修飾為可逆性。而蛋白水解為蛋白酶水解胺基酸與胺基酸之間連結的胜肽鍵；為不可逆性，因此在各種蛋白質體中，都有廣泛且重要的影響[1]。在人類基因體中，蛋白酶之基因約佔 2%，且其中約有 5-10% 已作為藥物標靶[2，3]。要了解特定蛋白酶在生物體內的功能與訊息調控路徑，需要辨別其受質，也就是裂解體研究；並利用受質切位的特異性作為藥物設計之參考。但蛋白質體的複雜動態性高，不同的組織、細胞、以及所處的發育或疾病時期，都有獨特的蛋白質組成和不同的轉譯後修飾情形，使得同一蛋白酶在每種蛋白質體中有不同的裂解體[1，4]。

基質金屬蛋白酶(matrix metalloproteinase)可降解細胞外基質與腫瘤發生有高相關性[5]。在二十年前就開始研究抑制藥物，並進入人類的臨床試驗。但試驗結果卻是失敗的，雖然可抑制腫瘤轉移但病人的生存率卻沒有上升，且引發肌肉疼痛或關節疾病等副作用。而後科學家探討其原因大約有兩點：一、MMPs 為 23 個結構相似且含鋅原子的胜肽內切酶，藥物無法專一性抑制特定 MMP，導致非目標 MMP 也被抑制，影響其他正常生理功能。二、近來研究指出除了細胞外基質，MMPs 更作用在細胞激素、細胞膜上受器和生長因子等，影響細胞生長、分化、移動等多樣的細胞機制。且由於任何一種 MMP 都未全面了解其受質所參與的調控路徑，無法全盤考量對其抑制後的影響範圍[6-8]。在 MMPs 之中，MMP-2 與 MM-9 受到較高的矚目。因為他們在多種的惡性腫瘤裡有高度表現，為癌症生物標記。MMP-2 和 MMP-9 因其結構和受質又稱明膠酶(gelatinase)，與其他 MMPs 結構不同在於催化區上有三個纖維鏈結蛋白域。MMP-2 與 MM-9 結構極為相似，差別在於催化區與血紅素結合蛋白樣結構域之連結區段長短，而他們的受質有部分重疊，也各自催化不同受質，影響不同訊息路徑[9]。另外，相較於其他有特定胺基酸切位的蛋白酶，如 caspase 都切除在 aspartate 後的肽鍵[10]；MMP-9 與 MMP-2 無固定的切位胺基酸，且切位周邊的氨基酸特異性也不盡相同[11]，因此較困難預測其切位與受質。要瞭解 MMP-2 與 MM-9 的受質裂解體，可透過質譜分析，但不同時期且各種細胞之蛋白質體不盡相同，如利用實驗進行全面的受質辨認需花費長時間和高額金錢。因此，in silico 進行 MMP-2 和 MMP-9 受質切點預測可以進行大規模的受質裂解體的註解。在生物實驗設計上，可以減少且提供準確性高的候選者。

目前有多種蛋白酶受質切位的預測系統，其所使用的方法可分兩種[12]， 一、分數計算：GPS-CCD 利用 BLOSUM 62 進行胺基酸轉換，透過自行設計之演算法以預測 Calpain 受質切位。CaSPredictor 利用 BLOSUM 62 進行轉換並加入 PEST-like sequence 計算分數[13]。PoPS 讓使用者定義受質特異性的物理化學分數與權重來計算分數[14]。SitePrediction 利用每個位子的每種胺基酸發生的頻率和氨基酸替換矩陣計算分數以預測受質切位[15]。PoPS 和 SitePrediction 均可進行目前已發現的所有蛋白酶的受質切點預測，且提供二級結構

預測等額外資訊。二、機器學習： Pripper 使用 binary 編碼，分別利用支持向量機、隨機森林、J48 預測 caspase 受質切位[16]。另外一樣預測 caspase 受質切位的系統 Cascleave 除了 binary 編碼，更加入結構資訊和 Bi-profile Bayesian signature 編碼，以支持向量回歸來建立預測系統[17]。PCSS 讓使用者自行輸入訓練數據集並利用序列與結構等資訊編碼，利以支持向量機建立預測系統。也因為是使用者自行輸入訓練數據集，故可預測各種蛋白酶之受質[18]。

為了更精確地預測其受質切點以作為癌症標靶藥物設計之影響範圍參考，本研究建立 MMP-2 與 MMP-9 受質預測系統。此預測系統為兩層式，第一層建立利用二進制(binary)、物理化學屬性(physical-chemical property)、結構資訊、以及本實驗最新使用可以值展現數據庫中切位點(positive site)和非切位點(negative site)之胺基酸數量差異倍數(fold change)等特徵，並配合支持向量機建構四種特徵之模組。在第二層時，彙整每種特徵模組的預測信心指數並比較多種機器學習方法以建立模組。且第一層的每種特徵模組都測試七組不同的非切位點集，以得到適合且最能展現特徵編碼的特性之非切位點集。因此，整個預測系統可以學習更多的非切位點資訊。並針對其作為癌症標靶藥物失敗的原因，進一步利用物理化學屬性之特徵選擇，利用 MMP-2 與 MMP-9 在活性中心的屬性作為特徵，加上呈現資料庫中切點與非切點胺基酸組成差異倍數的資訊，提升預測系統準確度。

2. 材料與方法

2.1 資料收集

下載 MEROPS 9。5 版(西元 2011 年 7 月 1 日)[19]，篩選出人類的 MMP-2 與 MMP-9 受質，去除重複，並經過 Cd-hit 去除 70%相似的蛋白質，以整理出不冗餘的資料[20]。MMP-2 進行實驗的資料有 1269 筆受質切位在 630 個蛋白質中。MMP-9 的資料相對於 MMP-2 數量少，其受質切位數量為 269 筆，共在 42 個蛋白質中。沒有被註解為 MMP-2 與 MMP-9 作用的其他位點，均作為 negative site。因為 MMP-2 與 MMP-9 無特定胺基酸切位，使得 negative site 非常大量，分別為 330457 和 30558 筆。Training set 的好壞決定預測結果的準確度高地。因此本實驗隨機 7 次選出與 positive set 數量 1：1 的 negative sets(N1~N7)，各別與 positive set 形成 training set，共有 7 個 training set 並做不同編碼方式訓練，期望找到每一種編碼最好預測效能的 positive set 與 negative set 組合。其後，建立第二層預測時，將隨機挑選除了 N1~N7 以外的 negative set(N8)做為第二層之 training set。

2.2 建構預測系統

本研究利用機器學習方法建立預測系統，首先必須將蛋白質序列的資料型態轉換成機器學習所能讀取的特徵。本研究選用 binary、physical-chemical property、結構資訊、fold change 等特徵進行編碼，並利用 SVM 建構第一層的四種特徵模組，再將各種特徵模組預測結果的機率信心值彙整，經過第二層機器學習，以提升其準確率。第二層的預測模組將測試 5 種機器學習方法分別有 LibSVM、Naïve Bayes、Random Forest、IBK[21]以測試出準確度最高的方法，以建立兩層的預測系統。每種機器學習都以 10 倍交叉驗證進行預測效能計算。

2.3 第一層的特徵模組

第一層的特徵模組分別有二進制(binary)、物理化學屬性(physical-chemical property)、結構資訊、差異倍數(fold change)等四個。序列片段長(window size)的表示，被切的肽鍵往 N 端的第一個氨基酸為 P1，往 C 端的第一個胺基酸為 P1’。最長取到第二十個胺基酸 P20，P19，P18…P1P1’…P18’P19’P20’。

1. Binary：將測試 P20 到 P20’各種長度組合的胺基酸片段以向量的方式表示，故將 20 種胺基酸包含 Gap，以 21 個維度之向量做編碼，該胺基酸所占之維度設為 1。例如：
   Alanine(A) 000000000000000000001、
   Cysteine(C) 000000000000000000010。

2. Fold change：將 MMP-2 與 MMP-9 的 training set 中 positive site 和 negative site 的 P20-P20’片段輸入 Icelogo 軟體中[22]，依據下列公式，計算出每種胺基酸在每個位子上所出現的頻率並相除得到 fold Change 值。以顯示 positive site 和 negative site 每個胺基酸出現頻率的倍數差，以顯示不同 dataset 中 positive 與 negative 資料的差異性質。如利用 P+N1 建立模組，在進行 10-fold cross-validation 時，positive set 將分為 10 份，分別與總和 N2~N7 的 negative set 計算出 Fold Change 替換表。

$$Frequency+ = \frac{AA1}{all\ AA}\ \text{in positive set} \quad \text{(Eq. 1)}$$

$$Frequency- = \frac{AA1}{all\ AA}\ \text{in negative set} \quad \text{(Eq. 2)}$$

$$Fold\ chang = \frac{Frequency+}{Frequency-} \quad \text{(Eq. 3)}$$

3. 結構資訊： 將 dataset 中的蛋白質分送到 DISOPRED[23]和 NetSurfP[24]輸出的預測結果，取 P20-P20’片段進行編碼。編碼的資訊含有 DISOPRED 預測每個位子為 disorder 的機率和 NetSurfP 預測每個位子的 Relative Surface Accessibility、Absolute Surface Accessibility、Z-fit score、Probability for Alpha-Helix、Probability for Beta-strand、Probability for Coil。

4. Physical-chemical property：從 AAindex[25]資料庫下載胺基酸的物理化學性質，最初下載有 544 筆資料，去除空值與去除資料之間皮爾森相關係數大於 0.8 後，剩下 371 筆資料。加上由 Venkatarajan, M.S. 等人在 2001 年發表之論文，其將 237 個胺基酸物理化學性質，整合成 5 個向量之特徵[26]。而 gap 的數值為 20 個胺基酸的屬性數值之平均。因此，使用的物理化學特徵共有 376 個。取 P20-P20' 之切點與非切點片段用 376 筆物理化學性質編碼後，每一個位子將與 positive (+1) 和 negative(-1)進行皮爾森相關係數檢定，當相關係數|R|值大於 0.05 到 0.3 以及 P 值小於 0.001 時，此位子之相對特徵將被選出，其餘剔除。因此，非每一個位子都會進行編碼，且有進行編碼的位子的特徵數也不相同。

2.4 第二層整合模組

每種編碼的最好預測效能之 training set 來建立預測模組。重新隨機選取不包含第一層之 7 組 negative set 且與 positive site 數量 1:1 的 negative site 形成 negative set 8 (N8)：送給由四種特徵用 SVM 建立的第一層特徵模組。SVM 其輸出的預測結果有 positive site 和 negative site 的機率，此機率作為第二層之特徵。第二層分別 B、PCP、DS 特徵模組預測結果以及彙整 B、PCP、DS、FG 特徵模組預測結果作為特徵輸入給機器學習建立預測系統。將測試 5 種機器學習方法： LibSVM、Multilayer Perceptron、Naïve Bayes、Random Forest、IBK，找出最好的第二層預測方法。

2.5 數據集相似度分析

Positive set 和 7 個 negative ste(N1~N7)將分別利用 BLOSUM62 分數矩陣比對兩個胺基酸的相似度。將每一個位子的每一個胺基酸與相同位子的其他胺基酸的比對分數平均。舉例：共有 100 筆資料，第一個位子的第一個胺基酸將與其他 99 個胺基酸利用 BLOSUM62 矩陣轉換分數並加總後平均，即為第一個位子的相似度分數。將有 P20~P20'的平均分數。

2.6 模組預測能力評估

當預測結果為切點且實際亦為切點則為 True Positive(TP)，若預測結果為切點但實際卻非切點為 False Positive(FP)，而預測結果為非切點但實際卻為切點則為 False Negative(FN)，預測結果為非切點且實際亦非切點為 True Negative(TN)。將利用下列公式評估預測系統的準確性。Matthews Correlation Coefficient(MCC)顯示 Positive 和 Negative 的相關度，其值最大為 1 表預測完全正確，最小為-1 表示預測完全與正確結果相反 ，其公式如下：

$$MCC = \frac{(TP \times TN) - (FN \times FP)}{\sqrt{(TP+FN)\times(TN+FP)\times(TP+FP)\times(TN+FN)}} \quad \text{(Eq. 4)}$$

Accuracy(Acc)，顯示整體預測結果的預測正確率，其公式如下：

$$Acc = \frac{TP+TN}{TP+FP+TN+FN} \quad \text{(Eq. 5)}$$

Specificity(Sp)，顯示預測結果對於非切點的辨識能力，其公式如下：

$$Sp = \frac{TN}{TN+FP} \quad \text{(Eq. 6)}$$

Sensitivity(Sn)，顯示預測結果對於切點的辨識能力，其公式如下：

$$Sn = \frac{TP}{TP+FN} \quad \text{(Eq. 7)}$$

3. 結果

3.1 第一層預測效能

Binary model (B)-Binary 編碼呈現蛋白質的一級序列訊息。由序列片段由切位往 N 端和 C 端各 20 個胺基酸進行準確度測試。MMP-2 與 MMP-9 當片段從 P3 開始時，MCC 都有明顯上升。而 MMP-2 的片段長度從 N 端 P3 到 P15 以其 C 端 P3'到 P20 都有 MCC 都有 0.5 以上，其 MCC 最好的收斂約在 P3 到 P13'之間。MMP-9 的片段長度從 N 端 P3 到 P15 以其 C 端 P2'到 P20'有 MCC 都有 0.4 以上，其 MCC 最好的收斂約在 P3 到 P9'之間 (圖 1)。收斂區域，呈現了 MMP-2 與 MMP-9 切位附近的氨基酸特異性之決定長度。MMP-2 每組 training set 的 Sn 都有 0.9 以上，Sp 都在 0.85 以上，ACC 接近 0.9。而預測效果最好的 training set 為第 7 組(P4-P5')，其 MCC 為 0.808。MMP-2 最好與最差的 MCC 相距 0.034(表 1)。而 MMP-9 每組的 Sn 都有 0.7 以上，Sp 都在 0.75 以上，ACC 約為 0.75。預測效果最好的 training set 為第 7 組(P3-P5')，其 MCC 為 0.570。MMP-9 最好與最差的 MCC 相距 0.108 (表 2)。

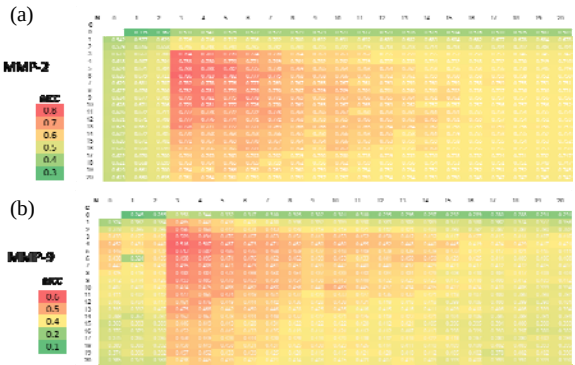


圖 1 MCC of vary window size by binary coding。 X,Y 軸分別表示往 N 端和 C 端延伸的氨基酸長度。(a) Heat map of MMP-2。(b) Heat map of MMP-9。

表 1
MMP-2 的第一層特徵模組內之 training sets 最高與最低 MCC 差異。

MMP-2 first layer models	Highest	Lowest	Difference
Binary	0.808 (7)	0.774 (2)	0.034
Fold change	0.796 (3)	0.687 (2)	0.109
Structure	0.649(7)	0.609 (2)	0.04
Physical-chemical property (|R| > 0.05)	0.814 (1)	0.778 (6)	0.036

表 2
MMP-9 的第一層特徵模組內之 training sets 最高與最低 MCC 差異。

MMP-9 first layer models	Highest	Lowest	Difference
Binary	0.570 (7)	0.462 (5)	0.108
Fold change	0.386 (2)	0.305 (4)	0.081
Structure	0.400 (2)	0.309 (1)	0.091
Physical-chemical property (|R| > 0.2)	0.613 (7)	0.446 (5)	0.167

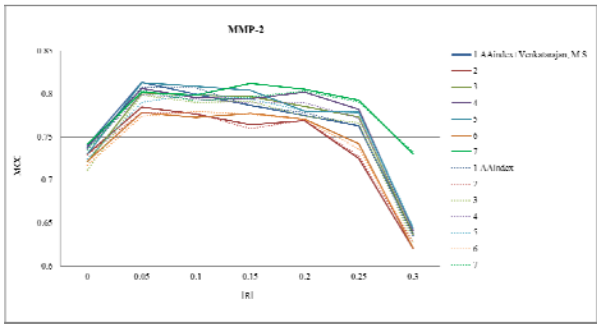
Fold change model (FG)- MMP-2 與 MMP-9 以 icelogo 輸出的 fold change 值進行 P20-P20'共 40 個胺基酸編碼，以展現每個位子的 positive 與 negative 的每一種胺基酸比例差異倍數值。MMP-2 每組的 Sn、Sp 都在 0.83 以上，ACC 在 0.85 左右，預測效果最好的 training set 為第 3 組，其 MCC 為 0.796。MMP-2 在 fold change 編碼上最好與最差的 MCC 相距 0.109(表 1)。MMP-9 每組的 Sn 約為 0.6，Sp 差距較大，ACC 約為 0.65。預測效果最好的 training set 為第 2 組，其 MCC 為 0.386。最好與最差的 MCC 相距 0.081(表 2)。

Structure model (S)-利用結構預測系統輸出的結果作為特徵，MMP-2 每組的 Sn、Sp 都接近 0.8 以上，ACC 約 0.8。預測效果最好的 training set 為第 7 組，其 MCC 為 0.649。MMP-2 最好與最差的 MCC 相距 0.04(表 1)。MMP-9 每組的 Sn、Sp 都在 0.65 以上，ACC 約在 0.65。預測效果最好的 training set 為第 2 組，其 MCC 為 0.4。MMP-9 最好與最差的 MCC 相距 0.091(表 2)。

Physical-chemical property model (PCP)- MMP-2 與 MMP-9 的物理化學屬性編碼，先以 P20-P20'片段以相關係數檢定進行特徵選擇，最後呈現不連續性片段的編碼，以凸顯特定位子的重要性。經過相關係數 0 到 0.3 的門檻選擇，不同門檻編碼的位子和使用的特徵不盡相同。MMP-2 的資料在|R|>0.05 時，所選擇出的特徵建構的模組之 MCC 約 0.8。隨著|R|上升，MCC 逐漸下降到約 0.6(圖 2(a))。MMP-2 的第 1 組且當|R|>0.05 時，有最高 MCC 為 0.814。在同樣的|R| > 0.05 下，最差的 MCC 為第 6 組的 0.778，最好與最差的 MCC 相距 0.036(表 1)。MMP-**9** 在 physical-chemical property 編碼，以不同相關係數篩選特徵，其隨著|R|上升，每組的 MCC 趨勢不盡相同(圖 2(b))。MMP-9 之第 7 組 training set 隨著|R|上升到 0.2 時，有最好的 MCC 為 0.613。在同樣的|R| > 0.2 下，最差的 MCC 為第 5 組的 0.446，最好與最差的 MCC 相距 0.167(表 2)。

加入 Venkatarajan, M.S. 等人在 2001 年發表之五維胺基酸特性，確實可以提升準確度。隨著相關係數上升，被選擇出來的特徵數下降，在 AAindex 佔大量特徵下，五維胺基酸特性約佔整體特徵的 1%。探討 physical-chemical property 編碼中最好的模組，MMP-2 在|R|>0.1 時，五維特徵可使 MCC 上升 0.01(圖 2(a))。MMP-9 在|R|>0.1 到 0.2，五維特徵都有使 MCC 上升。尤其在 R=0.2 時，上升了 0.04(圖 2(b))。

(a)



(b)

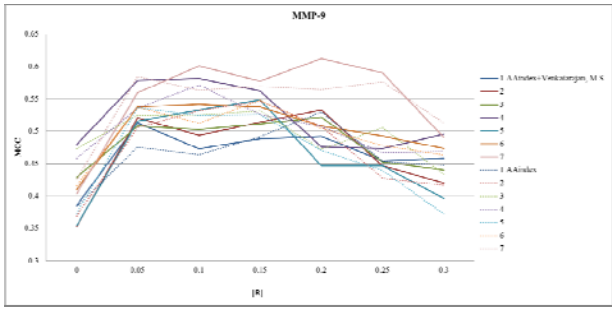


圖 2 Physical-chemical property models 相關係數之特徵選擇後 MCC 趨勢。實線為 AAindex 加上五維特徵。虛線為只有 AAindex 之特徵。(a)MMP-2 之 7 個模組，Y 軸從 MCC 為 0.6 開始。(b) MMP-9 之 7 個模組， Y 軸從 MCC 為 0.3 開始。

3.2 第二層預測效能

整合每種特徵最好的預測效果組別，MMP-2 之 binary 特徵預測效能最好是第 7 組，fold change 為第 3 組， structure 為第 7 組，physical-chemical property 為第 1 組(表 1)。MMP-9 之 binary 特徵預測效能最好是第 7 組，fold change 為第 2 組，structure 為第 2 組，physical-chemical property 為第 7 組(表 2)。第 2 層的建立首先比較彙整 3 個特徵模組(B、PCP、S)以及加入數據庫的差異倍數資訊的 4 個(B、

PCP、S、FG)特徵模組的預測效果並測試 4 種機器學習方法: LibSVM、Naïve Bayes、Random Forest、IBK。MMP-2 第二層的預測結果 3 或 4 個特徵模組，MCC 都在 0.8 以上，最好的為彙整 4 個特徵模組並利用 LibSVM 建構的預測系統，其 MCC 為 0.894。測試有無 FG 模組的輸出預測機率的特徵，可以發現加入 FG 模組的預測準確度 MCC 平均可以提升 5.52%(表 3)。MMP-9 第二層的預測效能結果，最好的 MCC 為彙整 4 個特徵模組並利用 IBK (K=23) 機器學習法建構的預測系統，其 MCC 為 0.644。加入 FG 模組的預測機率，預測準確度 MCC 平均可以提升 10.62%(表 4)。最後的完整預測系統架構，是由第一層每種不同特徵之最好 MCC 之模組，和彙整四個特徵模組的第二層最好 MCC 之機器學習方法所建成。

表 3 MMP-2 第二層利用不同機器學習比較有無 FG 模組的 MCC

MMP-2 second layer	Naïve Bayes	Random Forest	IBK	LibSVM
3 models	0.82	0.821	0.829	0.834
4 models	0.847	0.888	0.893	0.894
Increase	2.7%	6.7%	6.4%	6%

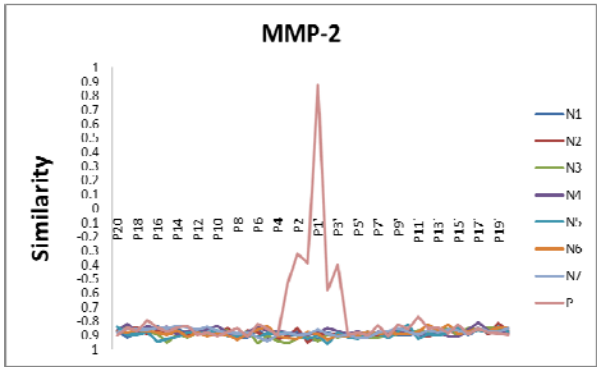
表 4 MMP-9 第二層利用不同機器學習比較有無 FG 模組的 MCC

MMP-9 second layer	Naïve Bayes	Random Forest	IBK	LibSVM
3 models	0.522	0.447	0.503	0.512
4 models	0.602	0.6	0.644	0.625
Increase	8%	15.3%	14.1%	11.3%

4. 討論

MMP-2 在四種編碼中，最高與最低的 MCC 相差約在 0.03 左右，與 MMP-9 的編碼相差有 0.1 之多。探究其原因為 MMP-2 與 MMP-9 資料相差五倍。有 1269 positive sites 的 MMP-2 在每種編碼上都有比 MMP-9 的 MCC 高出 0.2 以上，因為 MMP-2 資料量多較易得到好的 negative site 建構預測系統。MMP-9 資料量少，在隨機選取時相較於 MMP-2 較易選到集中性質的 negative site 導致預測效能偏頗，影響預測系統的正確度。至於，每種編碼的最高與最低 MCC 的組別都不盡相同，是因為隨機選取的 negative site 的組成不同，對於各編碼的屬性有不同的影響。以 BLOSUM62 計算 positive 與 negative sites 胺基酸相似率，可以看出每組 negative set 相對於 positive 的趨勢線都不盡相同(圖 3)。各個 negative set 與 positive set 相似度的差異，導致預測系統訓練時的不同，因此準確度會依 negative set 變化。有趣的是，MMP-2 在 P4 到 P4'片段(圖 6(a))以及 MMP-9 在 P13、P3、P1-P3'、P12'、P15'、P18'等位置(圖 6(b))，positive 與 negative sites 胺基酸相似曲線明顯不同。這些位置剛好對應到 physical-chemical property 編碼經過相關係數特徵選擇後留下的有編碼位置。表示使用相關係數作為特徵選擇，不僅 MCC 會上升且也符合序列相似度的關係。

(a)



(b)

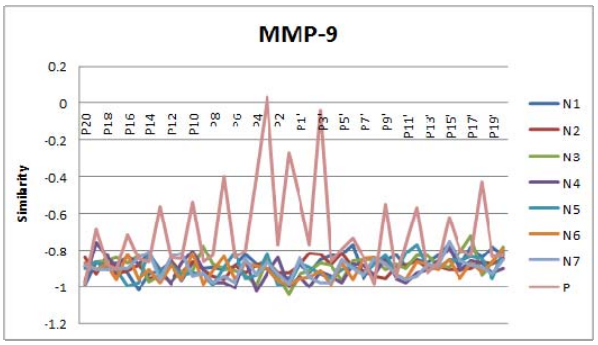


圖 3 切點與非切點之胺基酸序列的相似比率。 P 為切點資料庫。N1 為第一組之非切點資料庫，以此類推。(a)為 MMP-2 的資料庫相似度趨勢圖。(b)為 MMP-9 的資料庫相似度趨勢圖。

本實驗流程設計，讓機器學習更多樣的 negative set，讓每種編碼擁有最適合的 training set。並以第二層彙整不同意義之編碼使之帶有更多 negative 的訊息。 以解決 negative site 過於龐大之問題。可作為之後相關研究之預測系統架構之參考。本實驗最先使用 Icelogo 所提供的 fold change 數值，以顯示 training set 裡 positive 和 negative 的倍數差異。這個特徵在第二層彙整時，佔很大的重要性，他可以顯著地幫助預測較能的提升。此編碼亦可解決 negative data 過多的問題，如能選擇出適當的非切點群以代表全部的非切點資料，即可得到良好的 fold change 值，以展現全面性的差異。

相較於現有的預測系統，本系統更加友善且準確。本系統為現在唯一預測 MMP-2 與 MMP-9 受質切點的專職預測系統。系統的輸入，將設計可以一次輸入大量蛋白質序列，以實現 proteome 的預測功用。MMP-2 與 MMP-9 和腫瘤轉移有密切關係。為全面了解其受質所參與的調控路徑，本研究分別建立 MMP-2 與 MMP-9 受質切位的預測系統，以預測新的可能受質，之後將推估其他調控路徑，作為在製作抑制子時的全盤考慮與規劃，以避免副作用。

誌謝

本論文承蒙行政院國家科學委員會之計畫經費贊助，計畫編號為 NSC 101-2221-E-005-085 與 NSC 102-2221-E-005-081，僅此誌謝。

參考文獻

[1] Doucet A, Butler GS, 1. Doucet A, Butler GS, Rodríguez D, Prudova A, Overall CM: Metadegradomics. Molecular & Cellular Proteomics 2008, 7(10):1925-1951.

[2] Puente XS, Sánchez LM, Overall CM, López-Otín C: Human and mouse proteases: a comparative genomic approach. Nature Reviews Genetics 2003, 4(7):544-558.

[3] Overall CM, Blobel CP: In search of partners: linking extracellular proteases to substrates. Nature Reviews Molecular Cell Biology 2007, 8(3):245-257.

[4] López-Otín C, Overall CM: Protease degradomics: a new challenge for proteomics. Nature Reviews Molecular Cell Biology 2002, 3(7):509-519.

[5] Kessenbrock K, Plaks V, Werb Z: Matrix metalloproteinases: regulators of the tumor microenvironment. Cell 2010, 141(1):52-67.

[6] Coussens LM, Fingleton B, Matrisian LM: Matrix metalloproteinase inhibitors and cancer—trials and tribulations. Science 2002, 295(5564):2387-2392.

[7] Turk B: Targeting proteases: successes, failures and future prospects. Nature reviews Drug discovery 2006, 5(9):785-799.

[8] Drag M, Salvesen GS: Emerging principles in protease-based drug discovery. Nature reviews Drug discovery 2010, 9(9):690-701.

[9] Bauvois B: New facets of matrix metalloproteinases MMP-2 and MMP-9 as cell surface transducers: Outside-in signaling and relationship to tumor progression. Biochimica et Biophysica Acta (BBA)-Reviews on Cancer 2011.

[10] Timmer JC, Zhu W, Pop C, Regan T, Snipas SJ, Eroshkin AM, Riedl SJ, Salvesen GS: Structural and kinetic determinants of protease substrates. Nature structural & molecular biology 2009, 16(10):1101-1108.

[11] Prudova A, Auf Dem Keller U, Butler GS, Overall CM: Multiplex N-terminome analysis of MMP-2 and MMP-9 substrate degradomes by iTRAQ-TAILS quantitative proteomics. Molecular & Cellular Proteomics 2010, 9(5):894-911.

[12] SONG J, TAN H, BOYD SE, SHEN H, MAHMOOD K, WEBB GI, AKUTSU T, WHISSTOCK JC, PIKE RN: Bioinformatic approaches for predicting substrates of proteases. Journal of bioinformatics and computational biology 2011, 9(1):149.

[13] Liu Z, Cao J, Gao X, Ma Q, Ren J, Xue Y: GPS-CCD: a novel computational program for the prediction of calpain cleavage sites. PLoS One 2011, 6(4):e19001.

[14] Boyd SE, de la Banda MG, Pike RN, Whisstock JC, Rudy GB: PoPS: a computational tool for modeling and predicting protease specificity. In: 2004. IEEE: 372-381.

[15] Verspurten J, Gevaert K, Declercq W, Vandenabeele P: SitePredicting the cleavage of proteinase substrates. Trends in biochemical sciences 2009, 34(7):319-323.

[16] Piippo M, Lietzén N, Nevalainen OS, Salmi J, Nyman TA: Pripper: prediction of caspase cleavage sites from whole proteomes. BMC Bioinformatics 2010, 11(1):320.

[17] Song J, Tan H, Shen H, Mahmood K, Boyd SE, Webb GI, Akutsu T, Whisstock JC: Cascleave: towards more accurate prediction of caspase substrate cleavage sites. Bioinformatics 2010, 26(6):752-760.

[18] Barkan DT, Hostetter DR, Mahrus S, Pieper U, Wells JA, Craik CS, Sali A: Prediction of protease substrates using sequence and structure features. Bioinformatics 2010, 26(14):1714-1722.

[19] Rawlings ND, Barrett AJ, Bateman A: MEROPS: the database of proteolytic enzymes, their substrates and inhibitors. Nucleic acids research 2012, 40(D1):D343-D350.

[20] Li W, Godzik A: Cd-hit: a fast program for clustering and comparing large sets of protein or nucleotide sequences. Bioinformatics 2006, 22(13):1658-1659.

[21] Witten IH, Frank E: Data Mining: Practical Machine Learing Tools and and Techniques. 2005.

[22] Colaert N, Helsens K, Martens L, Vandekerckhove J, Gevaert K: Improved visualization of protein consensus sequences by iceLogo. Nature methods 2009, 6(11):786-787.

[23] Ward J, Sodhi J, McGuffin L, Buxton B, Jones D: Prediction and functional analysis of native disorder in proteins from the three kingdoms of life. Journal of molecular biology 2004, 337(3):635-645.

[24] Bent P, Thomas P, Pernille A, Morten N, Claus L: A generic method for assignment of reliability scores applied to solvent accessibility predictions. BMC Structural Biology 2009, 9.

[25] Kawashima S, Pokarowski P, Pokarowska M, Kolinski A, Katayama T, Kanehisa M: AAindex: amino acid index database, progress report 2008. Nucleic acids research 2008, 36(suppl 1):D202-D205.

[26] Venkatarajan MS, Braun W: New quantitative descriptors of amino acids based on multidimensional scaling of a large number of physical–chemical properties. Journal of Molecular Modeling 2001, 7(12):445-453.

標準化病人自動化動作分析訓練系統

林志豪　吳建勳　林雨慶　陳治華
亞洲大學 資訊多媒體應用學系
chlin@asia.edu.tw　99011016@live.asia.edu.tw
skyrex2011@gmail.com　popcochohqoq@hotmail.com

摘要

一位良醫必須做到深刻的了解病人的需求。醫生必須聽進病人目前病症概述，以及根據病人背景瞭解該名病患的病因。近年各大醫學院，紛紛導入「標準化病人」課程。從這門課程中獲得實務上經驗以及迅速判斷該名標準化病人目前急需要的資源、治療。本研究主要運用 Kinect 體感裝置來偵測標準化病人在表演中表演動作是否一致。運用此裝置記錄下標準化病人腳本中所有關節動作，進一步分析前幾次標準化病人參與該劇本時表演情況。每次練習都會記錄下來，如此一來達到每次表演都能夠一致目標。當正式表演時，不會因為練習不足、沒人指導造成標準化病人在表演上錯誤或腳本誤解。此系統讓標準化病人在表演時擁有充分的練習，避免錯誤動作導致無法符合本次表演主題。

關鍵詞：標準化病人、肢體語言、Kinect 體感裝置、一致性

Abstract

A good doctor must do a deep understanding of the needs of patients. Doctor must listen carefully to the patient's current condition overview, according to the working and living habits of the patient to understand the background of patient likely causes, but not all of doctors are experienced and accurate judgments. In recent years, the major of Medicine have to import "standardized patients" courses. Practical experience obtained from this course, and quickly determines the standardized patients are urgently needed resources to treatment. In this study, the main use of the Kinect somatosensory device to detect the standardized patient in performing the action is consistent performances. Use of standardized patient script This device records all joint action performances circumstances, further analysis of previous standardized patients to participate in the screenplay. Each practice will be recorded this way to achieve the goal of each performance consistently. When the formal performance, not because of lack of practice, no guidance caused in performances on standardized patient error or script misunderstanding. This system has standardized patients performing practice to avoid malfunction cannot be in line with the theme of the show.

Keywords: standardized patients, Kinect sensor, body language, consistency

1. 前言

近年來，醫療糾紛、醫療爭議等詞彙在社會新聞中層出不窮，引起了許多社會人士、政府高層與學術界人士的撻伐與高度關注。醫療糾紛以下有幾種因素：一、過失、二、醫病關係問題、三、損害、四、時序相鄰之間接因素(proximate cause)。而醫療爭議與糾紛之形成，大多與醫病關係之問題有著密切的相關[4]。外，從許多不良的醫療事件中研究發現，造成醫療錯誤的幾項因素中，雖以個人因素為主要原因佔 37.8%，如技術不佳、判斷錯誤或未能取得足夠資訊；但仍有 15.6%是源自於人與人之間的溝通不良[2]。

醫學院利用 1975 年由蘇格蘭 Dundee 大學的 Dr. Harden 提出。客觀結構式臨床技能測驗（Objective Structured Clinical Examination, OSCE）來改善醫療品質；政府並於二零一二年納入國家考試。標準化病人在國外已行之有年。而在整個 OSCE 中本研究將重點放在於標準化病人身上，因為它是一個能讓醫生瞭解他真正痛苦的根源，假若表達不完整也會導致醫學生的誤判。或是可以訓練醫學生；當遭遇到無法自行完整表達時該如何詢問該病患的方式。標準化病人在本研究中主要針對標準化病人自身練習時；練習的情況以及練習完畢給予標準化病人適當的評估。

本研究是要建置一套標準化系統，並使用 Kinect 體感裝置來記錄標準化病人所有動作，結合視窗程式設計與資料庫，來達到方便使用並且快速記錄。並且將標準化病人與自己之前的表演動作來進行分析比對。當標準化病人根據不同的劇本完成該劇本表演動作時，本系統會將該動作的骨架資訊進行分析，再與之前動作的分析結果進行比對，並給予該表演動作一致性之評分。

本研究之系統比對主要針對標準化病人與自己比較而非其他標準化病人。評分產生後可以讓標準化病人、考官瞭解需要加強的部分，此評分結果可讓標準化病人與考官進行討論，推估問題如何發生，進而從中得到改善，更能因此將正確的醫療知識導入標準化病人本身，而達到彌補醫學知識錯誤以及不足之目的。

2. 文獻探討

2.1 客觀結構式臨床測驗-標準化病人

近年大家對於醫生的經驗及醫生互動變得相當重視。各大醫學院、醫學中心正在推動客觀結構式臨床測驗（OSCE）[14]。促使醫療品質及醫生溝通能夠大幅提升。

OSCE（Objective Structured Clinical Examination，客觀的臨床能力試驗）是以客觀的方式評估臨床能力的試驗方式的一種。包含醫療面談及身體檢查的“技能”與“態度”的評估，特別是要維持其客觀性（objective）是很困難的，所以在以前被認為無法實行。這裡所謂“高客觀性”的評估指的是：不論是誰都能以相同的基準接受評估，答案正確與否的判斷並不會受到評分者的個人主觀所影響。[6]OSCE 主要三大重要人物，考官、考生、標準化病人。然而在 OSCE 中對於標準化病人（Standardized Patient）需求是相當大量。對於該如何訓練標準化病人卻沒有特定的系統培育，各國、各醫學院也不同。不過主要都是針對標準化病人，是否正確表演出腳本內容，以及標準化病人的演出品質是否正確一致性。而在此將台灣所採用的標準化病人訓練工作流程歸納如圖 1。



圖 1：標準化病人的訓練工作流程表

標準化病人，在 OSCE 扮演著很重要的角色，會因為他的演出將學生帶入虛擬環境中，而標準化病人的表達就相當重要。標準化病人必須給予反饋這樣才能達到提升醫療品質以及良好的溝通[19]。

標準化病人從開始面試，訓練[11]，正式考試，考試結束，皆運用監測設備，紀錄每位標準化病人在「客觀結構式臨床測驗（OSCE）」[10]從頭到尾都必須掌握每一位標準化病人表演技巧、隨時由訓練者或導演監看。訓練演出過程是否太過誇大以及與腳本是否相符。在同一劇本中；標準化病人的演出是必須盡可能達到一致性，不可差異性太大也包含談話內容，為了瞭解標準化病人表演是否有一致性，錄影監測在訓練標準化病人時擁有相當重要地位，錄影監測也是輔助訓練者跟導演方便反覆觀看標準化病人的動作，再加以利用加拿大麥克馬斯特大學（McMaster University）標準化病人演出評量表現，對標準化病人評量是否合格。

2.2 肢體語言

肢體語言（Body Language）是人和人除了用語言溝通外，相當重要的一種溝通技巧。利用肢體語言讓彼此瞭解雙方所要表達的意思。所以肢體語言在人們在表達時是不可或缺的一種方式，也可以加強所要表達的內容，並強調其內容的重要性。肢體語言代表著很多種含意，各國也有不同的解讀方式，有時肢體語言也可以當作一種編碼，作為其他種用途、例如：人的行為活動[12]、人體的識別[17]等等。

肢體語言最常被運用在教學、演講。教學中有良好的肢體語言[15]，可以讓學生對課程內容感到興趣並且加深學生對上課內容的印象。藉此提升學生上課內容吸收，讓學生能夠快樂的學習。在考試時、可以利用回想到的上課情節幫助學生，不會因為緊張或者是壓力過大導致無法順利作答。反而記得上課老師在此部分時是利用甚麼肢體語言。學生可以輕鬆做答，讓學習不再都是枯燥的書本。

本論文中卻是讓學生或是考官明顯明白標準化病人目前所要傳達的意思，以及有可能的判斷依據。所以正確的肢體語言可以傳達正確的訊息，當然如果錯誤或是不當的肢體語言則是帶給錯誤的判斷及資訊。肢體語言在傳達訊息上相當重要不可以做出錯誤的訊息。所以標準化平常的練習相當重要考官或指導者可以給予標準化病人建議；或改善其表演方式。直接命中該劇本想要傳達的理念。

2.3 Kinect 體感裝置

Kinect 體感裝置[8]的運作技術，可以一次擷取三種資訊，分別是一般 Webcam 的彩色影像、紅外線具深度和骨架資料、最後是輸入聲音的訊號。深度資訊取得的技術主要來自於紅外線的發射器與紅外線攝影機的接收，由此來知道與物體的距離。微軟使用的 3D 偵測技術來自於與一家以色列公司 Prime Sense 的合作。Prime Sense 提供了動作感測技術以及感測晶片 PS1080，並使用 Light Coding 技術。在 Light Coding 技術的關鍵技術是 Laser Speckle 雷射光散斑，當雷射在不同的材質表面上或是穿透具有透明度的物體時，會形成隨機的反射斑點，而這些斑點就稱之為散斑，並由紅外線攝影機來紀錄下每個散斑，由此原始資料透過晶片計算成具有 3D 深度的圖像資料。骨架的追蹤是由深度資訊轉換成的 3D 圖像，進而轉換到骨架追蹤系統。該系統最多可以同時偵測到 6 個人出現在測量空間中，另外可同時分辨出 2 個人的動作，而針對每個人的生物特徵可紀錄下 20 組骨架數據資料。[1]

Kinect 也運用在醫學上也有相當不錯的成效，本研究利用 Kinect 骨架與彩色影像所產生數據產生

輸出[18]。骨架資訊含有人體 20 個關節點如圖 2。可詳細記錄在遊戲中時所有的運動情況。彩色影像就與一般攝影機相同大約一秒鐘 30FPS。運用 Kinect 此兩項便可輕鬆紀錄標準化病人所有動作、影像存取在電腦中。

2.4 影像動作分析

影像動作分析利用攝影機或是電腦視訊演記錄下，人、地、時間、物。在攝影機開啟時便開始記錄下所有過程，一分一秒都不放過，並將所有過程記錄在電腦中或是指定的空間中。接來來在進行分析，將在這過程中所產生的數據、影像一一做比對或是相關演算法，來完成主要目的。影像動作分析主要相關應用：體育、防盜、醫學等。

棒球，拍攝時採用運動攝影（sports photography）[9]可以清楚看到投手所有動作，從準備姿勢、握球、投出、一連串動作皆在高速相機拍攝下來。然而眾多體育賽事都不乏利用影像動作來分析該動作畫面判斷出界、或利用慢動作呈現影像，來追蹤球員與球的動向[16]。以及利用影像分析賽車以及滑雪的路程軌跡是否相似來找尋最佳的路線。播報時增加觀眾的可看性，並給予觀眾最新賽事資訊。除此之外在訓練時也須要藉助影像的幫忙以集資料數據化[7]，提升運動員的本身技巧及能力，才能使得賽事更加好看。促使運動員的準確動、靈巧性等全方面的提升。

在生活中監視錄影成為保障自身安全重要的一環，有效判讀出影片中的人物也是相當重要。每當事件發生時必須先了解疑犯何時進來？或是最近有相似體型、穿著等藉由錄影設備來判定。有時發生事件的人可能是大樓住戶，利用後端資料庫可有效判定是否為大樓住戶。如果可以在畫面中可以顯示他是哪一位住戶，或是計算出疑犯的大約身高[13]皆可有要幫助警察破案。但在這其中如果能有清晰臉部容貌是最好不過，在運用臉部判斷技術即使光線較為薄弱也可幫助判讀出叫好的影像。防盜並不只有監視錄影技術，其中也有包含了許多指紋比對、聲波比對、虹膜比對。接是需要將指紋、聲波、虹膜等運用影像、深度圖檔，記錄下來才能達成比對。

本研究因為 Kinect 體感裝置有相當多醫學上應用如：慈濟醫學資訊系開發「Kinect 居家復健系統」，署立豐原醫院復健科黃建華物理治療師針對中風、脊髓損傷患者進行居家復健推廣，確認患者是否認真進行復健，以及動作是否正確。因此可知 Kinect 體感裝置是目前最熱門的研究工具。本研究利用 Kinect 體感裝置從人體動向，將其動向數據化並且建立後端資料庫，在其研究其動向數據。

3. 研究方法

3.1 系統架構

標準化病人自我練習系統主要目的，在於標準化病人可自行在家進行動作的自我練習，且將練習過程經由系統分析而給予評分。本系統主要結構分別為登入系統模組、標準化病人資料庫、校正模組、比對模組與評分模組等 5 個部分，如圖 7。標準化病人在家自我練習時，可通過登入方式讓系統能夠確認當下使用者為誰，確保個人練習紀錄不會與其他使用者的紀錄混雜到一起。本系統將拍攝標準化病人在練習時的動作，並記錄骨架資訊於資料庫當中，然後將此骨架資訊經由校正與比對計算得出該動作的一致性評分，讓標準化病人可以透過此評分結果，進行動作上的修正，達到動作一致性之目的。

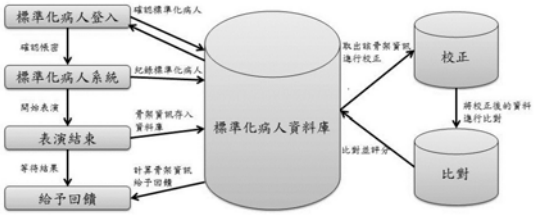


圖 2：系統架構圖

3.2 校正模組

本研究發現，Kinect 體感裝置攝影機在拍攝與記錄骨架資訊時，鏡頭成像是以圓錐體的放射方式投影在螢幕上，所以當標準化病人在進行自我練習時，因不同的位置而導致最後計算的結果有所偏差，為了避免這種誤差的發生，本校正模組將拍攝與記錄到的骨架資訊，全部統一投影在離 Kinect 體感裝置攝影機 3 公尺平面上，透過校正測試實驗的結果導出校正公式為 $((Z_\alpha - Z_i) \div 0.11) \times 5$，$Z_\alpha$，相關的參數與數據，在 4.2 節校正測試中，有詳細的說明，為距離 Kinect 體感裝置 3 公尺處的 Z 軸座標值，由此校正達到降低誤差率的可能性，下圖 3 為校正示意圖。

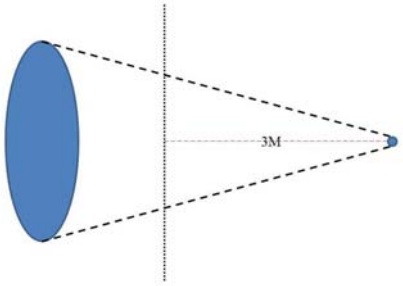


圖 3：校正示意圖

3.3 比對模組

本研究演算法是將人體上 20 個關節點；頭、左肩膀、右肩膀、中間肩膀、左手肘、右手肘、左手腕、右手腕、左手掌、右手掌、脊椎、左髖關節、右髖關節、中間髖關節、左膝蓋、右膝蓋、左腳踝、右腳踝、左腳掌、右腳掌，如圖 9 所示，其中的頭與中間髖關節這 2 個關節點作為基準點，並將其餘 18 個關節點與基準點分別做歐基里斯距離計算，計算公式如下所示。每個項目的 k 值可以根據實際的需要，例如劇本動作的注重程度給予適當的調整。

$$\sum_{i=1}^{19} k_i \sqrt{(X_i - X_n)^2 + (Y_i - Y_n)^2 + (Z_i - Z_n)^2}$$

3.4 評分模組

計算完所有距離後，並將所有距離相加取平均數，此平均數再與前次動作所計算的距離平均數做相減並取絕對值，此數值為該動作的一致性評分。數值越趨近於零，代表一致性程度越高，反之數值越高代表，代表此次動作與前次動作越不一致。評分公式如下所示。

$$\sum_{i=1}^{18} k_i \sqrt{(X_i - X_n)^2 + (Y_i - Y_n)^2 + (Z_i - Z_n)^2} + ((Z_\alpha - Z_i) + 0.11) \times 5$$

3.5 骨架資訊儲存

本研究利用 kinect 體感裝置產生骨架資訊，接著使用 Microsoft Visual Studio 2010 C# 連結 Microsoft .SQL Server 2008 將數據連結進入資料庫中。

首先利用 kinect 體感裝置產生骨架資訊，開啟 Microsoft Visual Studio 2010 C# Windows Form 將程式加入三個 kinect 重要的參考分別為 1.Microsoft.Research.Kinect ；2.Microsoft.Research.Kinect.Nui ；3.Coding4Fun.Kinect.WinForm。

kinect 體感裝置，啟動流程圖如，圖 4 所示。

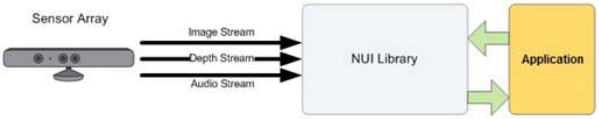


圖 4：啟動流程

Kinect 的 NUI 程式庫提供應用程式取得 Kinect 感應器傳送至主機的三種資訊串流[26]：1.彩色影像串流；2.深度影像串流；3.聲音串流。圖 5、就是完整的 Kinect for Windows SDK 架構圖。

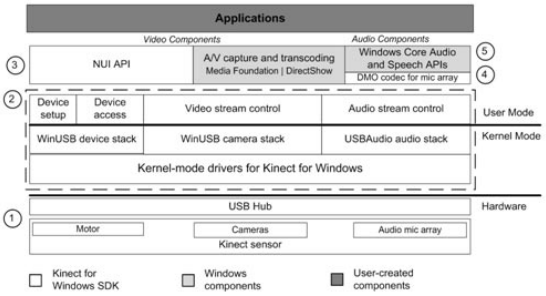


圖 5：Kinect for Windows SDK 架構圖

NUI API 初始化，Kinect API 接收感應器資訊，透過 Runtime 物件，因 Kinect 應用程式的第一步就是建立一個 Runtime 物件來接收感應器的資料，然後呼叫 Initialize 方法進行初始化，在應用程式結束時要呼叫 Uninitialize 方法，關閉 Kinect 設備。利用以上觀念將其方法與套入 Microsoft Visual Studio 2010 C# Windows Form 中。順利將骨架資訊顯示出來時會如下圖 6 所示。



圖 6：骨架數據

4. 系統實作與實驗結果

4.1 標準化病人系統介面操作

系統介面分為主介面，新標準化病人加入介面，標準化病人練習介面等三部分。主介面為標準化病人登入畫面如，圖 7。本介面主要為標準化病人登入，必須登入使用者帳號、密碼，才有辦法登入本系統。



圖 7：標準化病人登入畫面

標準化病人若是第一次使用本系統會要求標準化病人註冊新使用者。而新使用者介面如，圖 8。新使用者介面中，標準化病人必須設定專屬的帳號，密碼。標準化病人也必須填入標準化病人個人資料，如介面中所項目姓名，性別，出生年月日(西元)，最高教育程度，抽菸，血型，酗酒，通訊地址，過往疾病。以上標準化病人需填入資料。而過往疾病可在未來找尋標準化病人時是重要的依據。上述資料都是在未來找尋符合劇本的標準化病人是相當重要。可利用上述條件來找尋，並可在眾多資料中來尋找相關的標準化病人。

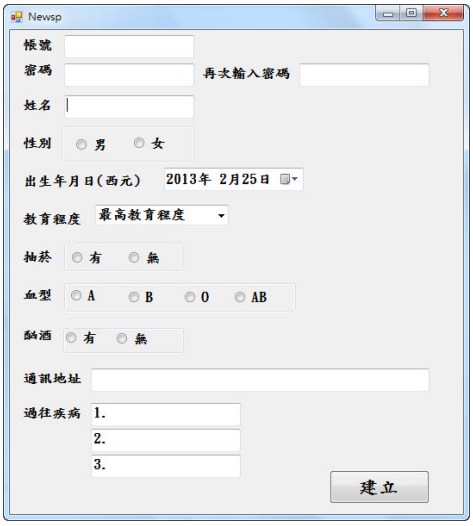


圖 8：新使用者介面如

標準化病人若以有此系統帳號、密碼，可以在主畫面中點選登入進入動作介面。登入後可以看到動作介面，如，圖 9。在此介面可以清楚看到目前動作介面中選項，在此介面時可點選動作說明來瞭解目前此動作需要達到哪些，圖 9 中動作說明主要說明該動作必須達成哪些動作，以及該注意哪些肢體動作，以便標準化病人準確完成動作。觀看完所有動作說明後，可以選擇想要執行的動作，輸入想要的項目後，滑鼠點擊開始後便可開始進行表演，如圖 10。標準化病人表演完成後可以點擊結束按鈕。表示已完成表演，表演過程中所有骨架數據會進入電腦資料庫中，本研究的運算評分系統將迅速計算出標準化病人，自身在此劇本以往表演的結果比較，並給予標準化病人評分、回饋。讓標準化病人瞭解未來可以改善哪些動作。



圖 9：動作介面

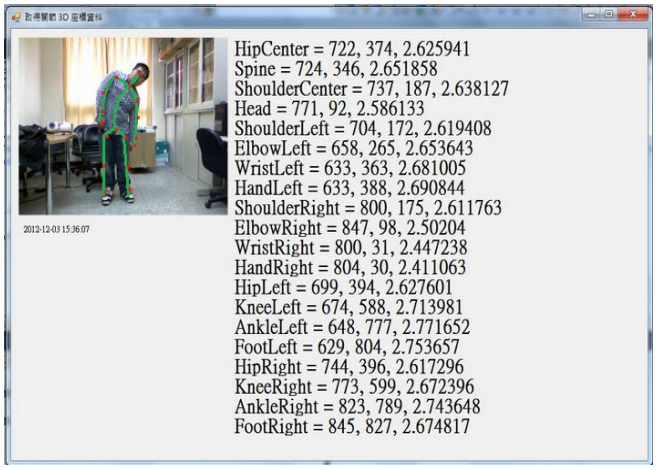


圖 10：表演畫面

4.2 校正測試

Kinect 裝置攝影機會因為拍攝與記錄的距離不同，而造成比對上的誤差，因此本研究針對此進行校正測試，測試內容為受測者離 Kinect 體感裝置攝影機 2.6 公尺處進行拍攝與記錄，且以每 0.2 公尺向後移動且拍攝與記錄，直至 3.4 公尺處為止，在動作上皆保持為站立不動的姿勢進行測試，且分別測試筆數總計約為 5 萬筆數據，進而確保分析之精準。透過此校正測試得知，2 個關節點間的距離會受到拍攝與記錄的距離遠近而產生些許誤差，且受測者離 Kinect 體感裝置攝影機越近，則 2 關節點間距離顯示越大，反之受測者離 Kinect 體感裝置攝影機越遠，距離顯示越小。

本研究將校正測試結果中內左肩與左手肘、左手肘與左手腕、右肩與右手肘、右手肘與右手腕、

左髖關節與左膝蓋、左膝蓋與左腳踝、右髖關節與右膝蓋、右膝蓋與右腳踝等部位，因各部位配對屬於同一根骨頭上，並不會受到動作的扭曲變化而改變其兩點間距離的特性，而進行各部位配對距離結果和受測者與Kinect體感裝置間的距離進行分析計算，最後經由分析結果得知，受測者在拍攝動作時，每向前移動 0.1 公尺其最後計算的距離向量將減少 5 個單位向量，反之退後移動 0.1 公尺則該加上 5 個單位向量。以下圖 11 為各部位根據不同距離所計算出兩點間的距離結果。

	A	B	C	D	E	F
1		2.6M距離	2.8M距離	3M距離	3.2M距離	3.4M距離
2	左肩肘	133.9559	123.8429	114.7470	103.9966	95.6685
3	左肩腕	245.7441	228.9230	208.8843	195.4490	179.6038
4	左肘腕	114.0695	107.0406	96.7993	92.9075	85.9744
5	右肩肘	143.9515	129.9075	119.7110	112.4144	110.4070
6	右肩腕	260.5595	238.2933	216.4106	206.1526	192.5972
7	右肘腕	117.6221	109.2394	97.7174	95.1307	87.9977
8	左寬膝	255.1441	233.3235	215.1483	194.5407	178.0232
9	左寬踝	428.0837	391.0397	363.4162	332.8374	307.3080
10	左膝踝	173.4045	158.2295	148.8091	138.9201	129.8142
11	右寬膝	266.4209	237.9848	221.5645	197.7797	178.2491
12	右寬踝	452.2776	408.2317	373.5238	340.6430	309.8955
13	右膝踝	185.9610	170.4473	152.5232	143.0817	131.6984
14						

圖 11：校正數據

本研究在校正測試當中，將所有距離、動作關節點的 Z 軸數值和受測者與 Kinect 體感裝置間的距離進行分析，經結果得知，當受測者在拍攝動作時，每向前移動 0.1 公尺則關節點座標中 Z 軸數值會減少 0.11 單位，反之向後移動 0.1 公尺則 Z 軸數值會增加 0.11 單位。本研究將 5 萬多筆數據進行 Z 軸數值距離分析。Z 軸座標測試結果如下表 1 所示。

表 1 Z 軸座標測試表

	2.6M	2.8M	3M	3.2M	3.4M
Z 軸	2.06672	2.287991	2.508959	2.735692	2.956184

本研究透過所有校正結果得知，當受測者在拍攝動作時，會因為受測者與 Kinect 體感裝置間的距離，而改變座標中 Z 軸數值和最後計算出兩點間的距離，因此本研究根據此特性，推導出校正公式為((Z_α-Z_i)÷0.11)x5，Z_α 為距離 Kinect 體感裝置 3 公尺處的 Z 軸座標值，Z_i 為比對的關節點 Z 軸座標值。

4.3 比對結果

本研究設計五項不同動作進行測試，動作項目分別為；雙手平舉、雙手高舉、右手平舉且左手高舉、左右側彎以及雙手高舉且左右側彎，而每項動作依偏差程度分別做 4 次的紀錄與拍攝，以達到最後結果之差異性。本研究設計動作 1 為標準動作，動作 2 為與動作 1 相近，動作 3 為與動作 1 極為偏差，動作 4 則是採取站立不動的姿勢。以下為本研究的測試截圖。


圖 12 雙手平舉動作 1


圖 13 雙手平舉動作 2


圖 14 雙手平舉動作 3


圖 15 雙手平舉動作 4


圖 16 雙手高舉動作 1


圖 17 雙手高舉動作 2


圖 18 雙手高舉動作 3


圖 19 雙手高舉動作 4


圖 20 右手平舉且左手高舉動作 1


圖 21 右手平舉且左手高舉動作 2


圖 22 右手平舉且左手高舉動作 3


圖 23 右手平舉且左手高舉動作 4



圖 24 左右側彎動作 1



圖 25 左右側彎動作 2



圖 26 左右側彎動作 3



圖 27 左右側彎動作 4



圖 28 雙手高舉且左右側彎動作 1



圖 29 雙手高舉且左右側彎動作 2



圖 30 雙手高舉且左右側彎動作 3



圖 31 雙手高舉且左右側彎動作 4

表 2 比對結果

	動作 1 與動作 2	動作 1 與動作 3	動作 1 與動作 4
雙手平舉	4.824065	11.814766	17.714450
雙手高舉	10.205737	16.174658	31.699402
右手平舉且左手高舉	9.484020	16.346170	24.586551
左右側彎	6.966788	12.134571	10.010377
雙手高舉且左右側彎	18.259377	27.731562	53.355019

本研究測試主要比對內容主要將動作 1 設定為標準動作，其餘動作分別向動作 1 進行比對。經由比對結果發現，雙手平舉、雙手高舉、右手平舉且左手高舉以及雙手高舉等 4 個項目比對結果，達到本研究所要求之目的，及一致性程度為動作 4<動作 3<動作 2，但唯有左右側彎項目比對結果不如預期，其一致性程度為動作 3<動作 4<動作 2，因此本研究針對此項目進行評估，最後發現因本研究比對演算法主要針對各關節點與基準點間之距離而加以計算，而左右側彎項目動作中，本身各關節點座標變異不大，而動作 3 因刻意造成偏差，所以造成關節點座標有所差異，而導致此狀況發生。

5. 結論與未來展望

本研究研發一套標準化病人系統結合 Kinect 體感裝置來幫助標準化病人紀錄自身所有表演實況，並且能夠評比該名標準化病人自身表演情況，也能提供給考官來給予標準病人建議，並且即時給予標準化病人回饋。在本研究建置標準化病人資料庫，考量到挑選標準化病人人選，可以快速找尋到合適的標準化病人，給予適當的幫助。然而本研究最終目的在於精準擷取骨架資訊進入資料庫中，而本系統則會從資料庫中擷取該動作與前次動作相關的骨架資訊，進行校正與比對程序，最後給予標準化病人動作的一致性評分。。

未來本研究會持續關注標準化病人資料庫內容，將標準化病人運算評分系統加入，能夠提升準確目前只是初步的評分系統還達不到本研究的要求，未來會減少骨架資訊過於龐大問題藉此提升此系統的執行效率。減少數據量並且配合演算法希望能夠達到本研究目標準確計算，以及精確的給予標準化病人回饋。並且與標準化病人中心遠端連結，讓考官可以藉由網路關心標準化病人最新練習情況，並且給予最迅速、正確的醫學資訊。讓本研究系統能夠更加的完善，已達成隨時監看等目的，並且運用本系統到其他相關運動或是醫學影像處理。

致謝

本文為亞洲大學研發處補助之專案研究計畫，對於其在研究過程的協助，謹此致謝。亞洲大學研究計畫編號 101-Asia-33。本文的刊登承蒙審稿委員的指正與包容，作者銘感於心。

參考文獻

[1] 王森，Kinect 體感程式設計入門，碁峰，台北市，2012

[2] 石崇良，”醫療團隊合作與病人安全”，澄清醫護管理雜誌，4（1），4-9，2008。

[3] 李石增，標準化病人訓練養成指引，台灣愛思唯爾 P.82-85，2011，一月。

[4] 李明濱，”醫病溝通教育與評估Ⅱ”，行政院國家科學委員會專題研究計畫（計畫編號：NSC91-2516-S-002-004），未出版，2003。

[5] 李廣均，”初探網路醫療的發展和限制-以醫療資訊網站為例”， the Journal of Health Science April 2001;3:200-214.

[6] 高雄標準病人訓練中心，網址：http://osce.dlearn.kmu.edu.tw/osce.htm
[7] 黃榮松、許逸雯，”手球攻擊射門打點電腦分析系統發展與運用”，2003。
[8] 維基百科．Kinect．網址：http://zh.wikipedia.org/zh-hant/Project_Natal。
[9] 劉碧華、陳俊合，”運動攝影之棒球投手投球動作決定性瞬間表現之質性研究”，2009。
[10] 歐良修、王兆寧、周宏學，”客觀性結構式臨床技能測驗（OSCE）手冊”，桃園：庚醫院標準化病人中心，2009。
[11] 蔡詩力、楊志偉、葉啟娟等，”標準化病人的招募與訓練，台大醫院的經驗”，醫學教育，11，174-181，2007。
[12] Gkalelis, Nikolaos ; Tefas, Anastasios ; Pitas, Ioannis ” Human identification from human movements”Image Processing (ICIP), 7-10 Nov. 2009
[13] Hae-Min Moon ; Sung Bum Pan; ” A New Human Identification Method for Intelligent Video Surveillance System” Computer Communications and Networks (ICCCN), 2010 Proceedings of 19th International Conference on Issue Date : 2-5 Aug. 2010
[14] Harden RM, Stevenson M, Downie WW, Wilson GM.: “Assessment of clinical competence using objective structured clinical examination.” British Medical Journal, pp. 447-451, 1975.
[15] Jia, Lianzhi ; Wang, Runlan ” The Application Skills of Body Language in Teaching”Artificial Intelligence and Education (ICAIE), 29-30 Oct. 2010
[16] Kopf, S. , Guthier, B. , Farin, D. , Jungong Han , ” Analysis and retargeting of ball sports video” , (WACV), 2011 IEEE Workshop on5-7 Jan. 2011
[17] Oh, Chi-min ; Islam, Zahidul Zahidul ; Lee, Chil-Woo Woo ” Pictorial Structures-based Upper Body Tracking and Gesture Recognition”Frontiers of Computer Vision (FCV), 2011
[18] Solaro, John,” The Kinect Digital Out-of-Box Experience”, Computer, June 2011, Volume: 44, Issue: 6,Page(s): 97- 99
[19] Turan S.a*, Üner S.b, Elçin M.a “The Impact of Standardized Patients’ Feedback on the Students’ Motivational Levels “Procedia - Social and Behavioral Sciences, Volume 1, Issue 1, 2009, Pages 9-11

個人健康紀錄的醫學建議知識庫系統

林志豪　張家維　林俊成　鄭稚翰
亞洲大學 資訊多媒體應用學系
chlin@asia.edu.tw　99011047@live.asia.edu.tw
smart0133@hotmail.com　alex198791@hotmail.com

摘要

隨著網際網路的發達，線上健康教學的應用也日益廣泛，許多不同領域的線上問答系統也陸續開發推出，而社會大眾的詢問行為也從書上慢慢轉移至網路上。隨著國民知識水平的提升，現代人們對於醫療品質也逐漸重視。因此，自我健康保健管理的重視度也日漸升高，因而越來越多人投入開發個人健康紀錄的相關系統。本研究利用個人健康記錄系統，建構出以健康保健知識為資料來源；透過知識自動匯入系統，讓系統資料更龐大，利用本體論去除網頁雜訊與個人健康記錄進行適當的知識搜尋與回覆，目的在於達到適合的知識建議。預期此研究架構的設計，在研究上，能夠幫助自然語言的相關研究；在生活上，能夠讓使用者對於自身的健康照護及醫療計畫更加的重視與投入。

關鍵詞：個人健康記錄、問答系統、本體論、維基百科

Abstract

As development and popularization of Internet, application of the on-line health education is more widely use. In different domains are developing several on-line QA System, hence via Internet become people's querying step. Along with the enhancement of national knowledge level, the quality of medical care gradually turns importance to human. Therefore, according to, the importance of Self-health care management has risen; more and more people intend to develop relative system of the Personal Health Record (PHR). Because language is the most naturally used to people's intercommunication, it's a complicated engineering that let computers to understand the language. Therefore, main factors in QA system's accuracy not only the Natural Language Processing (NLP), but also the response efficiency.

We collate Wikipedia system to build a healthcare knowledge base; employs auto importing system to enlarge the medical knowledge resource and do search and reply the fitness knowledge for user via the knowledge ontology and PHR system at the final. The purpose lies in fitness knowledge suggestions and reply prompt. In this research, expect this study can be the improve the knowledge of the QA System , expect can allow users attach importance to the personal health record themselves and be more participate in the personal medical plan.

Keywords: Personal Health Record (PHR), QA System, Ontology, Natural Language Processing (NLP)

1. 前言

由於網際網路近年來的快速發展，許多的病患都會透過網際網路去搜尋他們想要的資訊做為參考。但是病患從網路上搜尋到的資訊，並不一定能符合病患的情況。因此，本研究提出一線上醫療建議系統以提供一個以病患個人健康紀錄做輔助的醫療建議的管道。本系統預先建構出系統詞庫以及醫療建議知識庫，並且利用 TOVE 評價法將醫療建議知識庫建構出知識本體，讓病患以輸入自然問句的方式向系統發問，並經過系統的斷詞與語意分析模組進行問句斷詞及語意分析後，結合本實驗團隊研發的 PHR 系統進行，建議知識的搜尋，並提供病患適當的醫療建議，以達到線上即時的醫療建議回覆。建構出以健康保健知識為資料來源；透過知識自動匯入系統，讓系統知識更加龐大，並且利用本體論的法則去除網頁雜訊與個人健康記錄進行適當的知識搜尋與回覆，目的在於達到適性化的知識建議。期望能夠讓使用者對於自身的健康照護及醫療計畫更加的重視與投入。

2. 文獻探討

2.1 電子健康記錄

電子健康紀錄是個人終其一生的健康狀態及醫療照護之電子化資訊[1]，目的在於能提供醫療人員或病患即時且能共享的資訊。美國病歷發展協會(MRI)將傳統紙本病歷到最後的電子健康紀錄間的發展過程，分成了五個階段：

(1)Automated Medical Record：
自動化病歷階段，主要是將傳統紙本病歷逐漸以電腦表單取代。

(2)Computerized Medical Record：
電腦化病歷階段，將病歷資料以電子媒體檔案方式表示，達成無紙化系統。

(3)Provider-based Electronic Medical Record：
以醫療提供者為主的電子病歷階段，亦可稱電子

化病歷(EMR)階段，醫師看診不再仰賴紙本，所需資料皆已建成資料庫。

(4)Electronic Patient Record：

電子病患紀錄階段，此階段強調跨出個別醫院的藩籬，以病人為中心，具跨區域性，全球性的病歷資訊架構。

(5)Electronic Health Record：

電子健康紀錄，為電子病歷發展的最後階段，打破傳統病歷概念，紀錄及整合個人從出生到死亡的疾病和行為，可提供病患參與查詢管理或提供學術研究使用。

而國內目前的狀況，根據 2002 年衛生署的調查，大多屬於第三階段，發展緩慢的原因有二，一為國內法律上的限制，病歷被限定要用紙本的方式保存；二為建置電子健康紀錄系統花費金額龐大，許多中小醫院無力負擔[2][3]。所以期許電子簽章法能在未來立法並通過，而相關系統也能在各界的努力下，開發出低成本且適合本土條件的系統。

2.2 ICD-9

國際疾病分類(International Classification of Diseases, ICD)由世界衛生組織(World health Organization, WHO) 所發展出來的疾病診斷分類標準，為一個提供編號，以對疾病與許多徵兆、症狀、異常、不適、社會環境與外傷等所做的分類。任何健康狀況皆分配到專屬的分類及代碼，而 ICD 分類原則是由於疾病的統計分類具周延性、排斥性及有限性，即分類項數必需有限；且彼此之間不相重疊，並能涵蓋所有可能的病況(國家衛生研究院，1999)，而且這些分類項目的選擇必需是可促進疾病的統計與研究(行政院衛生署，2002)。目前 WHO 最新已經出到 ICD-10 版本，但是由於該版本編碼系統龐大且複雜性高，因此全球目前還是以 ICD-9 編碼系統為較通用之版本(范碧玉，2005)。ICD-9 的疾病編碼是由單純的數字構成，最長含 5 字的編號；至於其手術處置分類碼至多為 4 字的編號(行政院衛生署，2008)，「9 版」編碼模式為數字型態，不同於「10 版」的編碼模式為英文及數字構成，但是皆區分為主類目碼以及次類目碼，是依其各疾病病因及部位來使用作分類，在台灣 ICD-9 也是醫學界目前所使用之疾病編碼形式。在歐洲早期對疾病編碼予以分類，開始是用於疾病率和死亡率的統計，之後逐漸變成針對疾病的國際標準的診斷分類及健康管理目標，包含有人口健康狀況分析及疾病普及和影響的監控[4]。

2.3 問答系統

近年來有越來越多不同領域的問答系統(Question & Answering system, QA)被研發出來，並且在網路上提供使用者進行查詢。而很多自然語言處理相關的期刊及研討會徵稿都特別有規劃出一個領域題目，提供學者發表關於問答系統的應用及創新想法的管道。例如：國際計算語言學會議(International Conference onComputational Linguistics, Coling)、計算語言學期刊(Computational Linguistics, CL)、計算語言學會年度會議(Annual Meeting of Association for Computational Linguistics, ACL)。由此可以看出，問答系統已經是個越來越受重視的一個研究方向[5][6]。

目前問答系統的主要發展有兩大方向，一個方向是根據 TREC 競賽，使用 TREC 競賽所提供的文件作為回覆測詴的來源，並且遵循問答系統的要求與規範[7]；另一方向利用網際網路上大量的資料作為答案回覆的來源。以下小節中將分別對 TREC 和 WEB 問答研究之發展介紹[8]。

2.3.1 TREC QA

TREC 於 1999 年的第八屆大會中，首次舉辦問答系統的競賽（Question Answering track），其主要鼓勵更多的文字資訊處理領域的學者，能參與自然語言問答的研究，將過去資訊擷取系統以文件回應為主的方式，進階到以更精簡的答案做為系統的回應資訊。TREC QA 競賽的目的在於建立一個開放領域問答系統（Open Domain Question Answering System）[9]，亦即所開發之系統必須要能處理不同學科領域之知識詢問，因此需要更龐大且涵蓋領域的後端知識庫或文件庫，作為答案萃取之來源。

2.3.2 WEB QA

雖然 TREC 所提供的 Answer Corpus 文件數量已經相當的龐大，但是相對網際網路上持續劇增的文件資源，TREC 文件數量等集顯然的無法相比，而能回答的問題種類亦受限於其後端的文件集之新聞主題，而使系統的限制性也相較為多，因此有越來越多研究者，將相關問答處理技術轉移至網路上的資源作為運用，目前已有許多運用網路資源作為答案來源之自然語言問答系統開放線上使用，這些系統有些只針對某特定學術領域而設計的，但也有開發不少類似 TREC 的開放領域問答系統。

2.3.3 QA 系統處理過

不同的問答系統所採用的 Answer Corpus 或處理方法雖然需多不同，但是在大部分的問答系統中，處理過程通常都包含了有下列幾個步驟[10]：

(1)問句分析(Question Analysis)：

自然語言問句輸入到問答系統時，需要針對問句中語意資訊作分析，除此 之外，一般會對問句類型或答案類型作判斷，主要目的在於了解問句的意思。

(2)查詢建構(Query Formulation)：

根據問句中的重要字詞建構查詢，並以此查詢從大量的文件中擷取出可能含有答案的相關文件[11]。關於字詞重要性的決定以及如何擴充查詢

以提高文件擷取之精確度，在資訊擷取(Information Retrieval) 領域中有許多相關研究。

(3)文件擷取(Document Retrieval)：

為加快文件的擷取速度，後端龐大的文件集必預先做一些前處理，包括對文件作主題分類以及建立索引表(Index table)等，以提昇問答系統之整體處理速度。

(4)答案擷取(Answer Extraction)：

答案擷取所觸及的技術層面包含了自然語言處理(Natural Language Processing)及資訊萃取(Information Extraction)等，作用在於處理文件中句子之語句結構分析，以利進行答案之萃取。最後擷取出的所有候選答案還需要依其正確性作排序(Answer Ranking)。

2.4 語意網路

語意網路(Semantic Network) 在 1998 年，由全球資訊網的創始者 Tim Berners-Lee 所提倡，語意網路是一種可以處理網路上文件的語意的技術，能將 Html 等等人類可以理解的資料，賦予讓電腦可以理解的詮釋資料(Metadata)，使得軟體代理人程式能夠進行解析，進而代替人類做出各式各樣的處理[12]。在過去，網頁之間只能以超鏈結(Hyperlink)來表現資源之間的關連，而語意網路則可表達出資源與資源之間知識性的關連。語意網路是由網際網路標準組織(W3C)持續地訂定相關標準，目前已完成 RDF(Resource Description Framework)層、RDF Schema 層與知識本體(Ontology)層的標準定義，而在知識本體層之上的層次則是尚未開始標準化。對於網路服務的語意描述也就是基於這三個架構層。

2.4.1 RDF

RDF 稱之為資源描述框架(Resource Description Framework, RDF)[15]。在人工智慧的領域裡，知識表達法(Knowledge Representations)可大略分為四大類，數理邏輯(Predicate Calculus)、法則式專家系統(Rule-Based Expert System)、框架(Frames)及語意網(Semantic Network)。而 W3C 所採用的資源描述框架將框架與語意網的特色混合了。在這裡，知識是以物件(Object)、屬性(Attribute)與值(Value)的三元架構來表達，並可使用有序對、有向圖及 XML 三種方式來呈現。有序對及有向圖為觀念的闡述，且可以程式實作的只有 XML。網際網路標準組織提出了 RDF 標準，將資源之間的關聯表達出來，並希望利用此共通的標準，能夠讓不同系統的資料在網路環境中能夠互通。RDF 是一個可以攜帶多種不同的元資料(Metadata)並透過網路交換與傳送的工具。RDF 為資源這種資料模型提供了一種簡單的語義。基本上，RDF 是以述語(Predicate)、主詞(Subject)與受詞(Object) 三個述句(Statement)構成的，其中述語代表屬性(Property)，主詞代表資源(Resource)，受詞可為資源或文字(Literal)。例如：現在有一台筆記型電腦(Laptop)作為受詞，其擁有者是 Lin，若我們以有向圖來表現，其中橢圓代表主詞及受詞，箭號代表述語，則其表現如圖 1 RDF 基本模式示意圖：

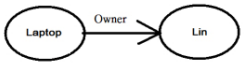


圖 1：RDF 基本模式示意圖

由上圖說明 RDF 的基本資料模式包含了三種物件型態：資源(Resource)、特性(Property)與敘述式(Statement)，並且利用這三種物件型態來描述事物。

2.4.2 RDF Schema

RDF 並沒有特別針對資源所擁有的屬性描述，以及針對這些屬性與其他資源的關係提供詳細的定義。RDF Schema 則是用來表示資源的屬性定義與資源之間的定義，也可表示資源的類別以及類別之間的定義與限制條件[13]。除了定義語彙本身的定義，像是人名或年齡等，連人名是屬於文字，年齡是屬於數字等等的範疇分類也都加以定義。

2.4.3 Ontology

在人類的世界中，透過彼此的溝通協調合作來完成困難的任務是愈來愈重要，相同的，在電腦的世界中，愈來愈多的電腦透過 Internet 互相連結，他們彼此之間都有可能需要作某種程式的溝通。然而在電腦之間作有效的溝通之前必須先達到語法(syntax)及語義(semantic)的協定[14]。舉例來說，電腦網路是由好幾層的 Layer 所構成，每一層的 Layer 都是一個語法及語義的集合。這些協定的集合通常被稱為 protocols 或是 standards。例如 TCP/IP(Transmission Control Protocol/Internet Protocol) 就是 transport layer 中的一個實例。目前，有愈來愈多的應用程式及愈來愈多的協定，而不同的應用程式要相互溝通就必須要交換彼此的協定(mapping)，這讓彼此之間的溝通變得愈來愈麻煩，尤其特別是在語義上的問題[15]。當我們指語義上的協同是指對相互溝通的部份在這個領域有一個一般性的了解。在真實的生活中，人們之間可以互相溝通是因為我們對於所說的內容已經有一個共通了解的詞彙。而這共通了解的詞彙實際上就是一個字典。每一個字所代表的意義在字典中都有詳細的說明。在電腦中的應用系統想要互相溝通

時，它們也需要字典來解釋在訊息中每個字或是欄位的真正意義。電腦所使用的字典與人類所使用的不同，因為人類的語言是非正規化的(informal)而電腦語言是正規化的(formal) [16]，所以電腦的字典必須以正規化的方式來呈現，而這個正規化的字典就是 ontology[17]。

2.4.4 TOVE 評價法

TOVE 評價法是由多倫多大學提出的多倫多虛擬企業本體 (TOronto Virtual Enterprise Ontology)。TOVE 本體使用一階邏輯進行描述，其中包括企業設計本體、工程本體、計劃本體和服務本體[18]。由於 TOVE 評價法採用一階邏輯進行描述，因此很容易結合其它的人工智慧系統或本體表示語言使用。它也是現階段較為嚴僅的本體建置方法，所以本研究使用 TOVE 評價法為基礎，做為建立醫療建議知識本體的建構方法。

2.5 自然語言處理

自然語言處理技術(Natural Language Processing,NLP)能夠幫助句子結構及字詞之間關係的分析。語意分析，有分為深度分析(Full Parsing)與淺度分析(Shallow Parsing)。深度分析是指將語句中可能的主詞(Subject)、述詞(Predicate)及受詞(Object)等資訊分析出來，而淺度分析僅能標記出字詞詞性為動詞、名詞或是形容詞等，對於句子架構的分析沒有深度分析所能提供的資訊來的詳細，也因為分析的資訊較少，所以淺度分析是快過深度分析的。因此，分析的速度及時間與資訊的細膩程度是分析過程中必須要取捨的因素[19]。在本論文中，利用在問句分析以及答案擷取時，對句子作詞性標記(Postging)的處理，以分析句子的詞性結構，協助確認問句的詢問目標(Question Target)，以及判定答案於文中出現的位置。此外，經過詞性標記後的問句，藉由詞性的資訊配合字組組成規則，斷出句中的名詞片語，形容詞片語及副詞片語等字組，可以用來提供在建立擷取文件用之查詢時所需相關字詞資訊。

2.5.1 Autotag

中央研究院詞庫小組 CKIP 在 1994 年完成的中文自動斷詞系統，運用該小組完成的大規模中文平衡語料庫為斷詞依據。語料庫總計有五百萬目詞。在中文平衡語料庫中的文章，都是已經經過斷詞的，並且語料都有標上詞性標記，提供了一個具有統一標準的資源[20]。

2.5.2 知網

知網(How-Net)：利用漢語和英語雙語的詞語所代表的概念來描述物件，用以表達概念的屬性之間的關係以及概念與概念之間的詞語知識庫[21]。知網在對詞句進行定義時，會標示出詞語的類別屬性，並訂出其附加的屬性，以表示其本質屬性。知網共收錄了六萬個漢語詞語，271 個語法結構模式，11000 句的實例，句法分布模式和句法結構模式各五十餘個，而目前尚在擴充中。

2.5.3 同義詞詞林

同義詞詞林是由大陸學者梅家駒、竺一鳴、高蘊琦等人共同編寫而成。主要是為了解決一般人在寫作及翻譯時詞窮的問題。同義詞詞林總共收錄了近七萬的辭彙，全部按照詞義做編排。除了以詞義為分類原則，也兼顧了詞類。詞語分為大，中，小類三級，共分 12 個大類，94 個中類，1428 個小類，小類下再依同義的原則畫分詞群，分成 3925 個詞群，是一部具有以詞義做查詢的工具書。同義辭辭林中，並沒有收錄專有名詞，除非此專有名詞有同義的現象[22]。

3. 系統架構

本研究可分為問答系統以及使用者介面。在使用者介面，主要負責執行使用者登入、輸入問句以及建議回覆的動作。在問答系統方面，利用問答系統裡的自然語言處理模組以達到了解使用者的問句，並針對問句，同時從 PHR 資料庫抓取使用者的資料以及從醫療知識庫內搜尋相對應的知識並進行建議的回覆。本研究預先建構出醫學知識建議庫，讓使用者以輸入自然問句的方式發問，並經過系統分析及知識搜尋後，提供線上即時的醫學建議。圖 2 為系統架構圖。本研究依照登入使用者的不同，能針對使用者的個人健康紀錄回覆適當的醫療建議，因此，同樣的問題在不同使用者提問時，得到的答案不一定會一樣。

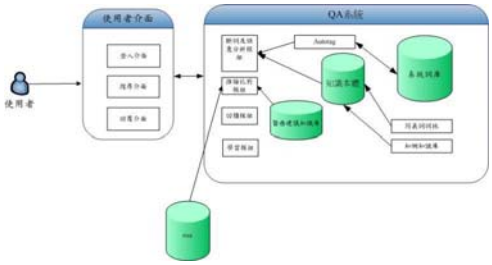


圖 2：系統架構圖

3.1 使用者提問及回覆流程

本研究針對使用者的個人健康紀錄作知識搜尋以及建議回覆。因此，使用者欲使用本系統時，必須先進行登入的手續。當使用者輸入自然式問句進行發問時，問句首先會透過系統的斷詞及語意分析模組內的 Autotag 斷詞系統進行斷詞。接著利用同義詞詞林及知網知識庫針對專業知識領域製作出知識本體，利用來針對斷詞後的語料進行語意的分析，以了解其中的含意。最後進入推論比對模組，把剛分析完的語料與系統的醫療建議知識庫及 PHR 資料庫的個人健康紀錄做知識的搜尋及比對，最後將醫療建議回覆給使用者。圖 3 為使用者提問及回覆流程。

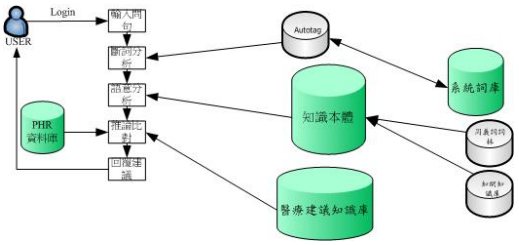


圖 3：使用者提問及回覆流程圖

3.2 斷詞及語意分析模組

本模組內含有系統詞庫，在接收到自然問句後，先利用 Autotag 及系統詞庫對輸入的自然問句做斷詞動作，接者將斷詞後的語料搭配上同義詞詞林及系統詞庫做同義詞判斷，並且使用 TOVE 評價法建立知識本體，以利進行斷詞後的語料分析，以及進行後續的推論比對。

3.2.1 系統詞庫

在斷詞及語意分析模組中，會將自然問句在斷詞模組做斷詞處理之後的語料，使用同義詞詞林及系統詞庫做同義詞的判斷，以及透過知網知識庫做語料分析的處理，用來提供後續的推論比對動作。
在本研究中，內建一個系統詞庫提供斷詞及語意分析模組使用。在系統詞庫中包含有疑問詞詞庫、斷詞規則庫以及醫療同義詞詞庫。當模組進行斷詞步驟時，使用 Autotag 搭配系統詞庫的斷詞規則庫及疑問詞詞庫做斷詞動作，斷詞後會產生出語料，即可使用同義詞詞林與系統詞庫內的醫療同義詞詞庫做同義詞的判斷。

3.2.1.1 斷詞規則庫

在句子裡面，含有「字」、「詞」兩種元素。字為一個一個的符號，而詞則是由一個或多個字組成有意義的單位。也就是說，詞是有意義的語言單位，是構成句子文法的基本單位。因此，若要了解整個句子中的涵意，須先將句子中的詞做出判斷及斷詞。本模組使用最長向後批配法做斷詞的動作，當使用者輸入自然問句時，從句子的第一個字，依照向後最長匹配原則，針對系統詞庫內的詞進行搜尋；若找到詞，則以此詞彙斷詞處，向斷詞處後方以最長匹配原則進行搜尋，直到整個匹配結束。例如:「亞洲大學」為一詞意完整的詞彙，而不是單指「亞洲」等涵意。

3.2.1.2 疑問詞詞庫

疑問詞的出現，通常是針對動作、使用者、原因等發生疑問，例如:「什麼人、什麼時候，為什麼要…」等。疑問詞的種類依照內容可分為九大類[5]，有人名疑問詞、動作疑問詞、工具疑問詞、量詞疑問詞、地點疑問詞、原因疑問詞、反詰疑問詞。
在本研究中，並沒有用到這麼多種疑問詞，因此列出下表 1，將本研究中所需要用到的分類列出。

表 1：疑問詞分類表

動作疑問詞(Action interrogative)	動作疑問詞	做什麼、做了哪些事.....
工具疑問詞(Instrument interrogative)	工具疑問詞	使用什麼.....
量詞疑問詞(Time interrogative)	數量疑問詞	多少、幾.....
地點疑問詞(Interrogative)	目的地疑問詞	到哪裡
原因疑問詞(Reason interrogative)	原因疑問詞	為何、為什麼.....
反詰疑問詞	不能單獨使用	嗎

3.2.1.3 醫療同義詞詞庫

在中文斷詞的技術上有個難題，就是一詞多意與多詞一義兩種。同義詞詞庫就是為了處理多詞一義的狀況而建立的。其資料庫因為醫療知識範圍廣大，所以須由人工手動建立同義詞詞庫，搭配 MIMS 做藥物名詞轉換、UMLS 做醫學詞彙轉換，ICD-9 疾病碼做疾病的分類，進而達到同義詞的轉換。

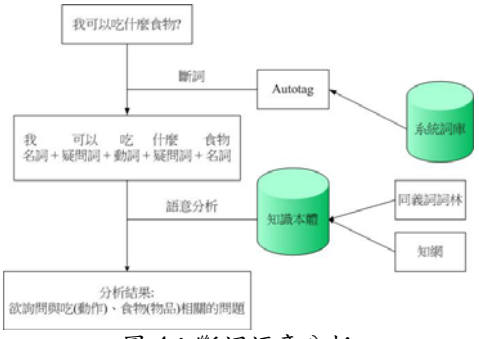


圖 4：斷詞語意分析

3.3 推論比對模組

在本模組中，將使用醫療建議知識本體針對斷詞後的語料詞性以及句法做分析，接著將使用者的問句與知識庫以及 PHR 資料做推論比對及搜尋，進而做出適合使用者的建議回覆。

3.3.1 醫療建議知識庫

本研究的醫療建議知識庫內建一般使用者提問頻率較高的「醫病六問」，並分別針對不同的健康狀況，做出適合的醫療知識建議。為了使不同使用者的身體狀況與醫療知識對應，本系統也內建各項檢驗值資料，使推論比對模組在做知識比對搜尋時能找到比較適當的建議。

3.4 PHR

在本研究中，個人健康紀錄取自於實驗團隊製作的 PHR 系統。這系統將分散各醫療單位的電子病歷整合，並利用本體論建置個人病歷本體以整合病歷資訊。本研究與 PHR 系統做搭配，從中擷取出病患的個人健康紀錄，將 ICD-9 代碼、各項檢驗數值，進而與本系統推論比對模組配合，搜尋出適當的建議並回覆給使用者。

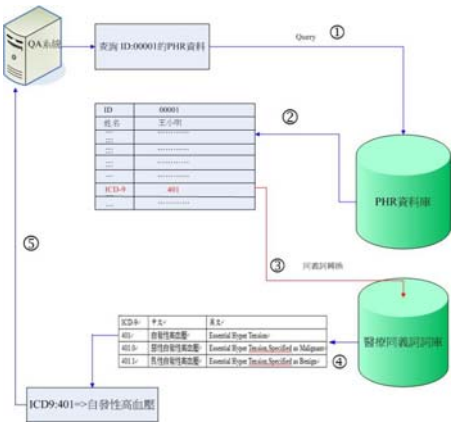


圖 5：PHR 資料擷取過程圖

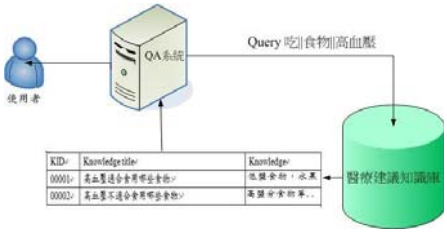


圖 6：建議知識回覆圖

3.5 醫學建議知識庫匯入模組

本研究將根據國際疾病分類代碼(ICD-9)上的病名稱，使用網路相關知識庫 Wikipedia、醫學百科網站等，經由分析比對之後，將格式、內容轉換至符合本系統之知識本體格是，自動匯入到健康保健知識本體內。

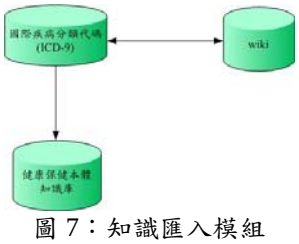


圖 7：知識匯入模組

4. 系統實作

本研究的運作主要就是提供符合個人狀況的醫療建議，所以不管是管理者或是一般使用者都必須先做登入動作，系統才能夠進行系統的使用，兩者不同的是一般使用者的權限只限於詢問建議，而管理者可以做其他的管理動作。

當一般使用者登入本系統使用詢問功能時，可以輸入自然問句以詢問相關的醫療建議，圖 8 為問答頁面。



圖 8：詢問畫面

當送出問句後，系統會進行斷詞及語意分析並且將結果與會員的 PHR 資料做比對，搜尋出適合的結果列表呈現於網頁上，提供使用者選擇瀏覽，如圖 9



圖 9：知識回覆

4.1 系統評估

系統的測試實驗，主要是為了突顯出系統的適性化醫療知識建議。因此，本實驗分別請 5 種不同健康狀況的使用者，提出 2 個有關「食」(飲食)或「行」(動作)的問題，並將所獲得的結果記錄下來，以利實驗數據的統計及分析。

以下整理出本系統的實驗環境。系統的知識量共計有 100 筆，能處理的問題領域有「食」、「行」兩種；測試問題共計有 50 筆，包含「食」領域問題 36 筆及「行」領域問題 14 筆；在使用者的方面，共計有 25 位測試者，包含 5 種患有高血壓或糖尿病的不同病況的病患各五位，並分別提出兩個有關「食」或「行」領域的問題，病患病況敘述於下並整理如表 2：

Wang：患有高血壓，在半年內有就醫紀錄。

Chen：患有糖尿病，在半年內有就醫紀錄。
Lin：同時患有高血壓及糖尿病，在半年內有就醫紀錄。
Cheng：同時患有高血壓及糖尿病，在半年內有就醫紀錄。(其中一項疾病就醫紀錄已超過半年)。
Tsai：同時患有高血壓及糖尿病，在半年內無相關就醫紀錄。

表 2：使用者健康狀況表

	Wang	Chen	Lin	Cheng	Tsai
健康狀況	高血壓	糖尿病	高+糖	高+糖 (其一超出半年)	高+糖 (皆超過半年)

本實驗使用上述的測試環境進行效能的測試，目的除了突顯出系統的自然問句處理能力及適性化醫療知識建議外，還特別針對同義詞模組的使用與否進行數據分析，目的在於了解系統使用同義詞模組與否的的效能差異，得到結果如下圖 10、圖 11、表 3、表 4。

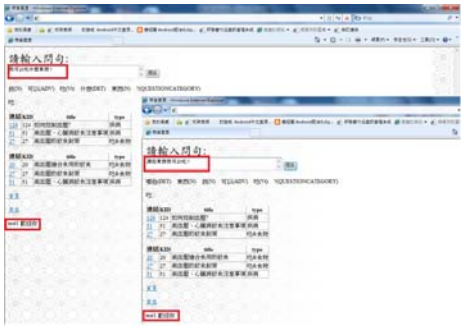


圖 10：相同使用者用不同問句尋問同問題



圖 11：不同使用者詢問相同問題

表 3：系統效能分析表(召回率)

Recall rate	高血壓	糖尿病	兩個病	一個病過期	兩病都過期
食(飲食)	0.55556	0.66667	0.76562	1	n/a
食(飲食)(同義)	0.83333	0.66667	0.875	1	n/a
行(動作)	0.25	0.16666	0.20	0.25	n/a

表 4：系統效能分析表(精確率)

Precision rate	高血壓	糖尿病	兩個病	一個病過期	兩病都過期
食(飲食)	1	1	1	1	n/a
食(飲食)(同義)	1	1	1	1	n/a
行(動作)	1	1	1	1	n/a

由上述實驗中，可以從數據得到一些結論，以下分成效率分析的結論及分析：
結論：

1. 使用同義詞模組後，召回率與精確率確實有所提升，代表著本模組在系統中確實發揮作用。
2. 於行方面的數據均偏低。
3. 所搜尋到的知識擁有高精確率，不會任意出現不相關的知識。

分析：
無法滿足使用者的原因，主要有以下幾項：

1. 系統內建語意分析樣板不足，以至於無法判斷詢問意圖。
2. 系統同義詞詞庫尚不足，以至於無法完全達到提升效率。
3. 系統知識庫內知識量不足，以至於無法提供建議。
4. 無法判斷錯別字。
5. 管理者新增知識時，沒有完整將資訊輸入造成無法搜尋到。
6. 只支援使用自然語言問句發問，不支援關鍵字搜尋。

5. 系統實作

為了讓使用者能夠以人性化及自然的方式做詢問的動作，以及使系統能做出準確的語意判斷，因此選擇採用了自然語言處理的方式設計語意樣板以供語意分析使用，目的在於讓使用者能夠輕鬆且自然的利用本系統詢問建議，並利用個人健康記錄的資料搜尋出適合使用者身體狀況的醫療健康知識建議。
本研究可以讓使用者可以不必從網路上那堆繁雜無經整理的資訊中尋找及整理知識，並且省去專程至醫療院所詢問醫師的時間及空間，使個人在自身的醫療計畫參與度上更佳提升，且更有效的運用醫療資源；在學術上，本研究架構使用自然語言處理技術並搭配個人健康記錄，提供了回覆適性化的想法及利用語意樣板的分析方式，本研究最大期許是希望能帶給問答系統一種新的思維及研究方向。

致謝

本文為亞洲大學研發處補助之專案研究計畫，對於其在研究過程的協助，謹此致謝。亞洲大學研究計畫編號 101-Asia-33。本文的刊登承蒙審稿委員的指正與包容，作者銘感於心。

參考文獻

[1] 李宜昌，病歷電子化國內之現況及發展趨勢，第七期資管人電子書。

[2] 陳秀雯，電子病歷資訊共享效益分析之研究，私立中原大學工業工程學系碩士論文。
[3] 行政院衛生署，“醫療資訊標準推動計畫”。http://www.doh.gov.tw/
[4] 楊叔卿，“電腦網路推展至中小學：一個超媒體網路師生培訓的研究初探”，第七屆國際電腦輔助教學研討會論文集，1998，476-483 頁。
[5] 歐陽彥隆，“電信服務業務 FAQ 查詢系統之研製”，碩士論文，交通大學資訊科學學系，2000/6。
[6] 2013 數位內容與多媒體應用研討會 ISBN 978-986-85814-3-2 383[6] 王亭雅，“網頁搜尋引擎問答”，碩士論文，中正大學資訊科學碩士班，2003/7。
[7] 莊宗南、龔榮源、陳俊龍，“以資料探勘技術建立病患就醫導引：以胃腸科病患為例”，台灣醫學資訊學會醫療資訊雜誌，第十五卷，第一期，2006/3，17-34 頁。
[8] 李雯婷、郭光明、李兆殷、蔡家安，“個人健康紀錄入口網站雛型系統開發：以冠狀動脈心血管疾病照護為例”，第六屆亞太 HL7 健康資訊交換標準研討會論文集，2007/6，199-211 頁。
[9] 郭子鼎，“應用本體論於國中社會科線上問答系統”，碩士論文，亞洲大學資訊科學與應用學系碩士班，2008/7。
[10] 歐陽渭城，圖解人工智慧入門，1992。
[11] 江柏勳，“基於自然語言處理文件技術之網路文件問答系統”，碩士論文，成功大學資訊工程學系碩士班，2005/7。
[12] Tim Berners-Lee., Weaving the Web: Origins and Future of the World Wide Web, Texere Publishing, US.1999.
[13] W3C, RDF Vocabulary Description Language 1.0: RDF Schema, 10 February2004,http://www.w3.org/TR/rdf-schema/.
[14] 王聖榮，“以比對法處理似中文式查詢句之設計”，碩士論文，淡江大學管理科學研究所，1988/7。
[15] 中央研究院中文詞知識庫小組 CKIP，“研究院語料庫的內容及說明”，技術報告，1995/02。
[16] 林俊成，“基於個人健康記錄之線上健康保健知識建議系統”，碩士論文，亞洲大學資訊科學與應用學系，2010/6。
[17] 臺灣醫療改革基金會，六大看病必問重點，2008 健康筆記，http://www.thrf.org.tw，2008。
[18] Michael Gruninger and Mark S Fox, “TOVE Methodology for the Design and Evaluation of Ontologies”, Department of Industrial Engineering University of Toronto, Toronto, Canada, M S A, 1995.
[19] Mike Uschold, Michael Gruninger. The Knowledge Engineering Review, 1996.
[20] 中央研究院中文詞知識庫小組 CKIP，“研究院語料庫的內容及說明”，技術報告，1995/02。
[21] 董振東，”How-net Document”，http://www.keenage.com/html/c_index.html，1999。
[22] 梅家駒、竺一鳴、高蘊琦、殷鴻翔，同義詞詞林，上海辭書出版社，1996 年。

人類蛋白質在細胞內位置的預測

徐筱姍[1]　游景盛[1,2]
[1]逢甲大學生醫資訊暨生醫工程工程學程
[2]逢甲大學資訊工程學系
yucs@fcu.edu.tw

摘要

細胞內蛋白質的功能與其所在子細胞位置的關係十分密切，蛋白質在細胞內若要正常運作必須要在正確的子細胞位置才能發揮其功能。因此，如果想要進一步了解未知功能的蛋白質，可以藉由確認蛋白質在細胞內的位置間接獲得重要線索。藉由預測蛋白質在細胞內的位置所使用的特徵，許多研究工作如人類發展藥物篩檢、疫苗設計與基因的註解具有醫藥發展的潛在應用。在這篇研究裡，我們利用 *n*-胜肽組成份特性以支持向量機器(Support Vector Machine, SVM)的演算法進行改進預測人類蛋白質在細胞內位置的準確性。我們將每條蛋白質的序列使用不同的特徵藉由支持向量機器分類器來進行第一階預測，再將其多樣性的結果由支持向量機器分類器進行第二階整合預測。在本研究使用的Hera資料集中，分屬於細胞內的九個位置的2233人類蛋白質序列，經十次交叉驗證可達整體預測準確性 71%，與前人的研究比較，同在 74%資料集涵蓋率的條件下，我們的方法可由 78%提升至 80%。另外前人研究中剩下的 26%無法預測的資料我們也可以達到 45%預測準確率。很明顯的我們的方法可以明確的提升預測準確性，我們預期這樣的技術將有助於未來對人類基因體學與蛋白質體學的相關研究。

關鍵詞：*n*-胜肽組成份、支持向量機器、子細胞位置。

Abstract

The biological function of a protein in a cell is often closely correlated with its subcellular localization. Hence, the information about where a protein localized often offers important clues toward knowing the function of an uncharacterized sequence. The protein subcellular localization can be used as an important feature to screen for drug candidates, vaccine design, and gene products annotation. Here, we applied the support vector machine algorithm to a benchmark dataset of human protein sequence based on multiple *n*-peptide composition properties. The first cascade in our approach is that we classify the protein sequence by different feature then use Support Vector Machine (SVM) algorithm to predict subcellular localization. In second cascade, we integrate the predicted results from the first step as the features to obtain the final prediction by SVM, too. We use the benchmark Hera dataset, which including 2233 human proteins separately in 9 subcellular localizations inside of cell. Our method improves an overall classification accuracy of 80% as estimated by using a 10-fold cross-validation test with coverage of 74% in previous work. For the rest 26% sequences, our method achieves an overall classification the accuracy of 45%. This research should provide an important tool in human genomics and proteomics studies.

Keywords: *n*-peptide composition、Support Vector Machine (SVM)、subcellular localization

1. 前言

生物學家長久以來對蛋白質如何運送和細胞生理調控的關係有著濃厚的興趣，在儲存大量蛋白質子細胞位置資訊的資料庫中，複雜的蛋白質網路關係難以令生物學家整理出一系統全貌。因為蛋白質的功能與蛋白質在細胞內位置有著非常密切的關係，藉由了解蛋白質在細胞內的位置仍有助於進一步了解蛋白質的相關功能。

近年來預測蛋白質子細胞位置的相關研究，生物資訊學者藉由各式不同的蛋白質序列特性以及演算法策略發展工具，如最近鄰算法(Nearest Neighbor approach) [1]、支持向量機器 [2, 3]、貝氏網路方法(Bayesian Network approach) [4]等機器學習的自動化分類的方法應用在預測蛋白質在細胞內位置的相關研究。其中，尋找有助於機械學習以進行分類的生物意義特徵十分重要。除了已知分泌蛋白與細胞核內的蛋白質先驅物(precursors)具有訊號序列能夠引導蛋白質進入正確的子細胞位置，細胞內許多蛋白質缺乏顯而易見的序列特徵。因此許多方法選擇以 N 端的序列區固定長度計算胺基酸的組成份 [5-7] 、合併使用序列的胺基酸組成份 [8, 9] 、計算雙胜肽(dipeptides)與間隔(gapped)雙胜肽的胺基酸的組成份[10]等特徵做為發展預測蛋白質在細胞內的位置的根據。

由許多文獻已知預測不同物種的蛋白質子細胞位置的研究多具有很高的準確性。如 CELLO[2]預測格蘭氏陰性菌(Gram negative bacteria)準確度 88.9%； TargetP[1]預測植物蛋白質準確度 85.3%。而預測人類蛋白質的子細胞位置，PSLT[4]預測準確度可達 78%，但其中將近 30%的蛋白質無法進行預

測，我們希望應用支持向量機器自動化分類且從序列擷取特徵的方法進行預測，希望提升預測人類蛋白質在細胞內的位置的準確度。

在本研究中，我們計算序列中存在的 *n*-胜肽組成份之特徵並使用兩階段的支持向量機器(SVM)演算法預測人類蛋白質在細胞內的位置，除希望能提升人類蛋白質預測的準確性，同時釐清蛋白質的組成份上在不同細胞內的位置、在有不同的條件如學習資料集與預測對象的序列同源性在不同子細胞位置的意義與影響，以期應用於更多物種和更細緻的生物系統知識深入分析。

2. 材料方法

PSLT 方法在人類蛋白質在細胞內的位置的預測，單一位置預測最好的結果準確率雖高達 78%但資料庫的涵蓋率僅有 74%，因為其方法所使用的資料集僅有 74%可在 InterProt 資料庫[11]查得相對應的資訊。在本研究中我們使用相同的人類 Hera 資料集(www.mcb.mcgill.ca/~hera/PSLT)（如表 1）。

表 1. 人類 Hera 資料集。

子細胞位置(*l*)	數量
Cytosol	357
ER	340
Secreted	294
Golgi	96
Lysosome	91
Mitochondria	222
Nucleus	584
Peroxisome	44
Plasma membrane	205

我們使用 LIBSVM[12]預測人類蛋白質在細胞內的位置。首先第一階段以序列上胺基酸的組成份當作特徵，運用這些特徵訓練和測試，找出最適合的參數建立分類器。第二階段將第一階段的數個分類器預測結果為輸入值以確定預測蛋白質在細胞內的位置。我們並以十次交叉驗證(10-fold cross-validation test)程序評估預測的準確性。

我們將 n-peptide 特徵下述五類，分別是 20 種胺基酸組成份（C_n）、間隔胜肽組成份(D_g)（如圖一）、將序列等分 k 段並分別計算各段胺基酸的組成份(X_k)(如圖二)、將 20 種胺基酸依物理性質分類(如表二)後再計算分段胺基酸組成份(A_nX_k)（如圖三）、局部序列胺基酸組成份(N_iC)（如圖四）。

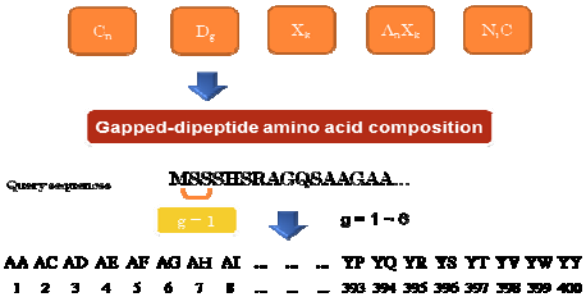


圖 1. 間隔雙胜肽組成份計算。

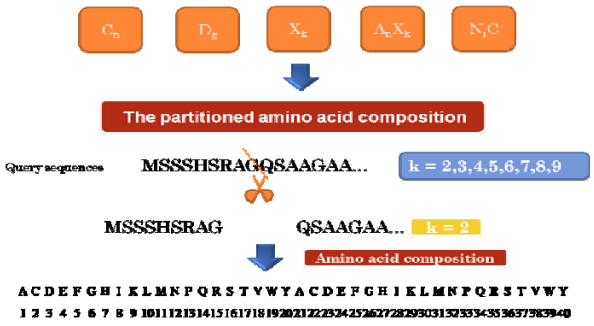


圖 2. 序列等分 k 段胺基酸組成份計算。

表 2. 胺基酸物理化學特性分類表。

分類代碼	分類依據形成	胺基酸依據類別
E	Acidic 酸性	DE
	Basic 鹼性	HKR
	Aromatic 芳香基團	FWY
	Amide 醯胺團	NQ
	Small hydroxyl 微羥基	ST
	Sulfur-containing 含硫氨基酸	CM
	Aliphatic 1 不飽和脂肪酸	AGP
	Aliphatic 2 飽和脂肪酸	ILV
F	Acidic 酸性	DE
	Basic 鹼性	HKR
	Polar 極性	CGNQSTY
	Nonpolar 非極性	AFILMPVW
P	Lowpolarity 低極性	LIFWCMVY
	Neutralpolarity 中極性	PATGS
	Highpolarity 高極性	HQRKNED
S	Acidic 酸性	DE
	Basic 鹼性	HKR
	Aromatic 芳香基團	FWY
	Amide 醯胺	NQ
	Small hydroxyl 微羥基	ST
	Sulfur-containing 含硫氨基酸	CM
	Aliphatic 脂肪酸	AGPILV
V	Small 小	GASCTPD
	Medium 中	NVEQIL
	Large 大	MHKFRYW
Z	Lowpolarizability 低極化	GASDT
	Mediumpolarizability 中極化	CPNVEQIL
	Highpolarizability 高極化	KMHFRYW
H	Polar 極性	RKEDQN
	Neutral 中性	GASTPHY
	Hydrophobic 疏水性	CVLIMFW

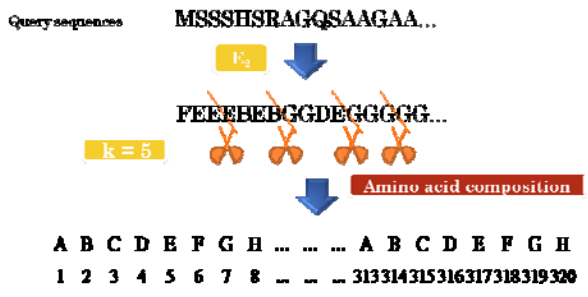


圖 3. 序列等分 k 段之胺基酸物化特性組成份。

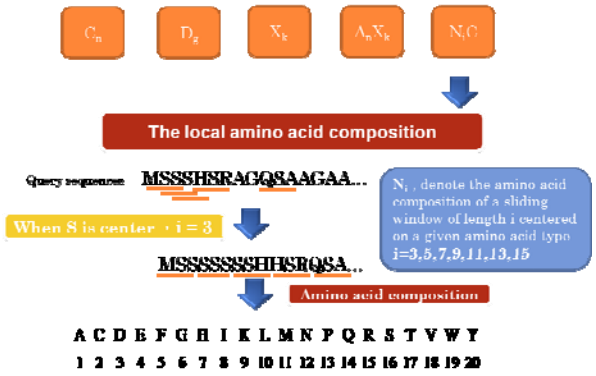


圖 4. 局部序列胺基酸組成份計算。

3. 預測表現評估

在本論文中，我們使用準確率進行預測的表現評估，並將結果和 PSLT 結果列於表 3:

P_ℓ 表示每個位置預測的準確率，ℓ 是細胞內的位置，L_ℓ 在 ℓ 的位置預測正確的蛋白質的數量， L_ℓ 在 ℓ 位置蛋白質的數量，如公式(1)。

$$P_\ell = L_\ell / N \times 100 \ \% \qquad (1)$$

P 表示整體的預測準確率，將每個位置的準確度累加除以九個位置，如公式(2)。

$$P = \sum_\ell P_\ell / \ell \times 100 \ \% \qquad (2)$$

4. 結果與討論

在本論文結果和 PSLT 結果列於表 3:

我們根據支持向量機器預測所得九個子細胞位置預測的機率值最大者視為其預測信賴值進行排序，前 74%視為 74%涵蓋率與 PSLT 進行比較，其中預測準確率達 80%，整體提升了 2%，九個位置分別：Cytosol（69%）、ER（76%）、Secreted（90%）、Golgi（29%）、Lysosome（67%）、Mitochondria（83%）、Nuclear（92%）、Peroxisome（14%）、Plasma membrane（80%）。超過半數的子細胞位置預測準確率皆有提升，Cytosol 提升 4%、ER 提升 7%、Secreted 提升 1%、Lysosome 提升 7%、Mitochondria 提升 6%。

表 3. 根據 Hera 人類蛋白質資料集，比較本論文預測蛋白質子細胞位置的預測結果與 PSLT 方法。

子細胞位置 (l)	PSLT Coverage = 74%	Our method Coverage = 74%	Our method Coverage = 26%
Cytosol	65(83)	69(93)	42(77)
ER	69(82)	76(86)	53(76)
Secreted	89(93)	90(93)	43(51)
Golgi	60(64)	29(54)	32(55)
Lysosome	60(71)	67(72)	23(55)
Mitochondria	67(71)	83(87)	43(63)
Nuclear	93(97)	92(96)	60(80)
Peroxisome	43(64)	14(36)	6(20)
Plasma Membrane	89(91)	80(86)	40(62)
Accuracy	78(86)	80(89)	45(68)

註:表格內的數值為本論文預測最高分結果的準確率，括弧內為前兩高分結果的準確率評估結果。

我們將資料集另外 26%的預測結果視為 PSLT 方法無法進行預測之資料集部份，平均準確性達 45%，九個子細胞位置預測的結果：Cytosol（42%）、ER（53%）、Secreted（43%）、Golgi（32%）、Lysosome（23%）、Mitochondria（43%）、Nuclear（60%）、Peroxisome（6%）、Plasma membrane（40%）。

本論文整體預測準確性可達 71%，同樣在九個子細胞位置中，預測第一高分為預測結果的平均準確性各別為：Cytosol（60%）、ER（70%）、Secreted（81%）、Golgi（30%）、Lysosome（52%）、Mitochondria（74%）、Nuclear（85%）、Peroxisome（11%）、Plasma membrane（70%）。另外若以前兩高分者為預測結果計算正確的準確性結果中，當涵蓋率 74%時最高準確率為 86%，預測九個位置的結果：cytosol（83%）、ER（82%）、Secreted（93%）、Golgi（64%）、Lysosome（71%）、Mitochondria（71%）、Nuclear（97%）、Peroxisome（64%）、Plasma membrane（91%）。

與前人預測方法比較下，當資料集的預測涵蓋率為 74%時，我們的方法的準確率可提升 2%。而對於 26%資料在原方法無法預測的情況下，依然可預測且準確性可到 45%，應可視為有用的輔助資料。

本論文使用序列比對軟體 ALIGN[13]針對個別蛋白質序列取得與對應的學習資料中可獲得的最大同源序列相似度值，並與所預測的子細胞位置計算所得機率值分析預測的結果，探討不同子細胞位置的預測信賴度與學習資料的關係。

如圖 5 中藍色的長條圖表示不同預測機率值區間的預測準確率，如預測的機率值介於 0.9~1 之區間的所有蛋白質序列，其預測準確率為 92.4%，機率值介於 0.8~0.9 之區間預測準確率為 91.3%，機率值介於 0.7~0.8 之區間預測準確率為 79.4%，機率值介於 0.6~0.7 之區間預測準確率為 65.5%，機率值介於 0.5~0.6 之區間預測準確率為 52.6%，機率值介於 0.4~0.5 之區間預測準確率為 48.4%，機

率值介於 0.3~0.4 之區間預測準確率為 44%，機率值介於 0.2~0.3 之區間預測準確率為 32.2%，預測的機率值介於 0.1~0.2 之區間並無序列。隨著預測機率值越低，預測準確性也越低。

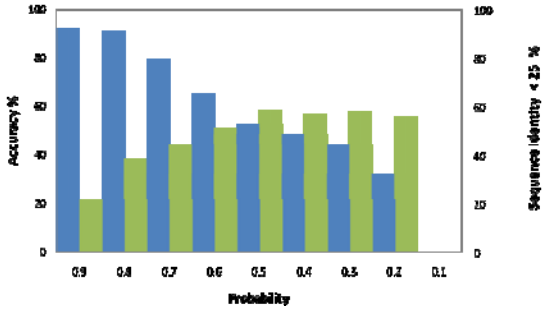


圖 5. 預測準確性與序列相似度的關係圖。X 軸為機械學習預測九個位置的機率值區間。藍色的長條圖表示該區間的預測準確率，綠色長條圖表示在區間中序列相似度小於 25%的序列在區間裡所有的序列的比例。

我們同時針對資料集中序列與序列間同源的屬性討論是否可能影響預測蛋白質在細胞內的位置的結果。根據序列比對軟體 ALIGN 計算序列與序列之間的相似度，從中選出序列相似度最高的序列做為序列與序列間同源性的依據。若序列相似度小於 25%，視為兩序列間無同源關係，我們計算在區間中序列相似度小於 25%的序列在區間裡所有的序列的比例，如圖 5 綠色的長條圖所示。當機率值在 0.5 左右會有交點，表示同源序列在同區間的資料中占 50%時，預測準確率達 66%，機率值在 0.6 時，當同源序列在同區間的資料中占 60%時，預測準確率達 50%以上。當資料集中同源序列比例越高，預測的準確性也越高，整體來看同源序列比例約占 40%，但機率值小於 0.5 時，預測準確率則急遽下降，當機率值大於 0.5、同源序列比例占 50%以上，預測的準確率可達到 60%以上的準確性。

另一方面，我們根據不同子細胞位置詳細探討預測準確性與序列相似度的關係。由圖 6，大部分支持向量機器預測的機率值越高，同源的序列數量也越多。在 ER 子細胞位置發現即使同源序列很少但預測的準確性還是可以維持在 50%以上，在 Nuclear 同源序列很多預測準確性很高。從趨勢線的交叉口的大小，Secreted 子細胞位置即使同源序列很多，沒辦法可以有很高的準確性，這個現象可能是因為這個位置的蛋白質性質呈多樣性，在 Peroxisome 子細胞位置發現現象完全相反。我們發現在不同的位置即使有同樣的條件下，會有不同的預測結果。

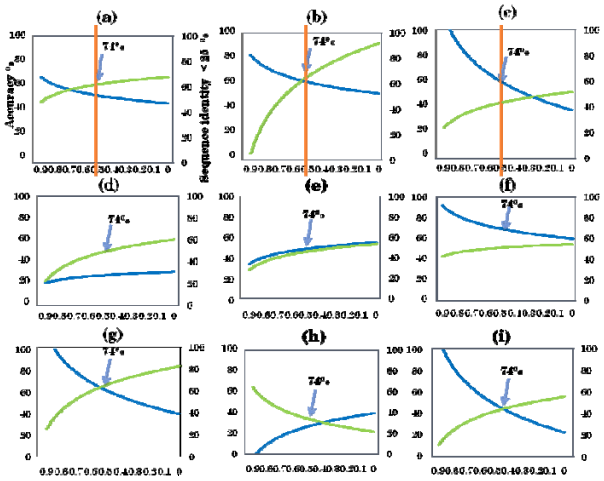


圖 6. 說明預測準確性與序列相似度的關係。(a)Cytosol 、(b)ER 、(c)Secreted 、(d)Golgi 、(e)Lysosome 、(f)Mitochondria 、(g)Nuclear 、(h)Peroxisome、(i)Plasmamembrane。藍色線代表預測準確性趨勢線，綠色線代表序列相似度小於 25%的序列在區間裡所有的序列的比例的趨勢線。

參考文獻

[1] O. Emanuelsson, H. Nielsen, S. Brunak, and G. von Heijne, "Predicting subcellular localization of proteins based on their N-terminal amino acid sequence," *J Mol Biol*, vol. 300, pp. 1005-16, Jul 21 2000.

[2] C. S. Yu, Y. C. Chen, C. H. Lu, and J. K. Hwang, "Prediction of protein subcellular localization," *Proteins*, vol. 64, pp. 643–51, Aug 15 2006.

[3] C. S. Yu, C. J. Lin, and J. K. Hwang, "Predicting subcellular localization of proteins for Gram-negative bacteria by support vector machines based on n-peptide compositions," *Protein Sci*, vol. 13, pp. 1402–6, May 2004.

[4] M. S. Scott, D. Y. Thomas, and M. T. Hallett, "Predicting subcellular localization via protein motif co-occurrence," *Genome Res*, vol. 14, pp. 1957-66, Oct 2004.

[5] O. Emanuelsson, H. Nielsen, and G. von Heijne, "ChloroP, a neural network-based method for predicting chloroplast transit peptides and their cleavage sites," *Protein Sci*, vol. 8, pp. 978-84, May 1999.

[6] H. Nielsen, J. Engelbrecht, S. Brunak, and G. von Heijne, "Identification of prokaryotic and eukaryotic signal peptides and prediction of their cleavage sites," *Protein Eng*, vol. 10, pp. 1-6, Jan 1997.

[7] M. Reczko and A. Hatzigerrorgiou, "Prediction of the subcellular localization of eukaryotic proteins using sequence signals and composition," *Proteomics*, vol. 4, pp. 1591-6, Jun 2004.

[8] A. Hoglund, P. Donnes, T. Blum, H. W. Adolph, and O. Kohlbacher, "MultiLoc: prediction of protein subcellular localization using N-terminal targeting sequences, sequence motifs and amino acid composition," *Bioinformatics*, vol. 22, pp. 1158-65, May 15 2006.

[9] K. Nakai and M. Kanehisa, "A knowledge base for predicting protein localization sites in eukaryotic cells," *Genomics*, vol. 14, pp. 897-911, Dec 1992.

[10] K. J. Park and M. Kanehisa, "Prediction of protein subcellular locations by support vector machines using compositions of amino acids and amino acid pairs," *Bioinformatics*, vol. 19, pp. 1656-63, Sep 1 2003.

[11] R. Apweiler, T. K. Attwood, A. Bairoch, A. Bateman, E. Birney, M. Biswas, P. Bucher, L. Cerutti, F. Corpet, M. D.

Croning, R. Durbin, L. Falquet, W. Fleischmann, J. Gouzy, H. Hermjakob, N. Hulo, I. Jonassen, D. Kahn, A. Kanapin, Y. Karavidopoulou, R. Lopez, B. Marx, N. J. Mulder, T. M. Oinn, M. Pagni, F. Servant, C. J. Sigrist, and E. M. Zdobnov, "The InterPro database, an integrated documentation resource for protein families, domains and functional sites," *Nucleic Acids Res*, vol. 29, pp. 37–40, 2001.

[12] C. C. Chang and C. J. Lin, "LIBSVM: a library for support vector machines.," 2001, p. Software available from http://www.csie.ntu.edu.tw/~cjlin/libsvm/.

[13] E. W. Myers and W. Miller, "Optimal alignments in linear space," *Comput Appl Biosci*, vol. 4, pp. 11-7, Mar 1988.

數位匯流技術應用於到院前緊急救護服務平台

顧皓翔　林鴻逸　黃思淵
華夏技術學院 資訊工程系
kuhh@cc.hwh.edu.tw

摘要

本論文將數位匯流應用至到院前緊急救護情境(First-Aid Services)，提供救護車與醫院之通訊服務匯流，藉由匯流技術強化過去因通訊載具或傳輸內容差異所形成之溝通障礙。到院前緊急救護一直為醫療體制中最重要的一環，透過救護車至事故或災禍現場救助受傷或不適之民眾，但往往隨車之醫療照護人員僅利用簡單之通訊器材將病患情況回報至醫院，再由醫院調派急診室醫生待命診療病患，無法第一時間進行病患診療救護之相關協助。有鑑於此，本論文利用數位匯流技術建置一具有開放性與通透性之開放式緊急救護服務平台(An Integrity and Transparency-based Open First-aid Service Platform, IT-OFA)，透過到院前緊急救護人員之手持式設備，結合開放式到院前緊急救護服務系統與具通透性之無接縫醫療照護服務平台，建立起延伸之醫療環境，並透過整合設備概況網路服務(Device Profile for Web Services, DPWS)、行動閘道器(Open Mobile Gateway)、開放式服務閘道平台(Open Services Gateway initiative, OSGi)、會話發起協議(Session Initiation Protocol, SIP)與 Web2.0 等標準與協定並串連病患資訊，使得醫生能在醫院電腦前面獲得事故現場受傷人員之生理訊號與病患資料，進而提供相關醫療行為與服務建議給位於事故現場之醫護人員。

關鍵字：數位匯流、到院前緊急救護服務、設備概況網路服務、開放式服務閘道平台、網頁技術。

Abstract

First-Aid Services have been an important part of the health care system. However, a few multimedia contents of patients are opportunely gotten by medical staffs and delivered to the hospital. Hence, this study designs and proposes an Integrity and Transparency-based Open First-aid Service Platform, which is called IT-OFA. IT-OFA is composed of mobile gateways in ambulances and a digital convergence server in the hospital. Medical staffs can interact with IT-OFA using various appliances and retrieve physiological and monitoring data via web interface. Delivered contents of digital convergence are based on Device Profile for Web Services (DPWS), Open Mobile Gateway、Open Services Gateway initiative (OSGi), Session Initiation Protocol (SIP) and Web 2.0 techniques. Medical staffs can easily get patients' information among ambulances and hospitals.

Keywords： digital convergence, first-aid service, Device Profile for Web Services, Open Services Gateway initiative, Web 2.0 Techniques.

1. 前言

近年來，醫療資訊網路與照護技術趨於成熟，各類的醫療資訊服務平台也逐漸開發出來輔助醫護人員進行全方位之醫療照護，現今之醫療照護服務平台已逐漸利用生理訊號感測器(EKG)收集病患之生理資訊，以輔助醫護人員進行病患情況之掌握[1]。但針對到院前緊急救護服務，救護車至事故或災禍現場救助受傷或不適之民眾，往往隨車之醫療照護人員僅將病患載上救護車後，就只利用簡單之通訊器材將病患情況回報至醫院，再由醫院調派急診室之醫生待命診療病患，無法第一時間進行病患之診療救護。但隨著數位匯流的興起，以前多設備之資料互相傳遞、設備運算之限制瓶頸已逐漸被打破。在現今科技發展下所產生之數位匯流現象，整合了語音通信、數據傳輸、與視訊服務之多合一服務，逐漸的成為市場上的新秀。因此，本論文將透過數位匯流整合將到院前緊急救護(First-Aid Services)建構較為完整資訊服務及救護車與醫院之醫療服務匯流，藉由網路及數位化內容打破過去因載具或傳輸內容差異所形成之障礙。若需打造一個到院前緊急救護平台應考慮到以下三個議題：

(1) 整合性(Integrity)。傳統醫療資訊系統都是針對不同問題所設計，因此相容性甚差，甚至資料無法互相傳遞，所以透過網頁服務平台(Web-based Service Platform)之延伸標記語言(Extensible Markup Language, XML)、簡單物件存取協定(Simple Object Access Protocol, SOAP)與網頁服務描述語言(Web Services Description Language, WSDL)並整合 Health Level Seven (HL7)與 Digital Imaging and Communications in Medicine (DICOM) 等協定，將相關之醫療資訊服務相互整合。

(2) 通透性(Transparency)。傳統醫療照護服務均為護士實際量測病患生理資訊，再寫到紙本報表上，然後再輸入電腦備存，除生理資訊不即時外亦常有人工誤植之問題。這類照護並非即時，醫生無法即時獲得病患相關資訊，因此透過各類感測器直接將病患生理資訊即時存入系

統，再透過數位匯流資料傳遞技術，將資料發送給相關醫療照護人員，所有病患資訊可以正確無誤傳遞至醫護人員。

(3) 多媒體擴增性(Media Scalability)。多媒體種類越來越多，若需展示不同的媒體需不同介面模式，可透過 Web2.0 技術，大量整合不同多媒體與匯流情境，並有效展示於系統畫面上，提供完整多媒體資訊。

有鑑於此，本論文提出一具有開放性與通透性之開放式緊急救護服務平台(An Integrity and Transparency-based Open First-aid Service Platform, IT-OFA)，透過到院前緊急救護人員之手持式設備，結合開放式到院前緊急救護服務系統與具通透性之無接縫醫療照護服務平台，建立起延伸之醫療環境，透過整合設備概況網路服務(DPWS)、行動閘道器(Open Mobile Gateway)、開放式服務閘道平台(OSGi)與 Web2.0 等標準與協定並串連病患資訊，使得醫生能在醫院電腦前面獲得事故現場受傷人員之生理訊號與病患資料，進而提供相關醫療行為與服務建議給位於事故現場之醫護人員。此外，透過手持式設備，能預先通知醫院病患資料並準備急診室病房或開刀房，達到無接縫(Seamless)之醫療照護服務。

在本論文的第 2 節將相關研究做一整理與說明；第 3 節將對所提出之具有開放性與通透性之開放式緊急救護服務平台其架構與設計做一論述；第 4 節將展示相關實作畫面；並於第 5 節做一結論。

2. 文獻回顧與探討

醫療照護資訊系統之生理訊號感測網路技術已經慢慢成熟，但較少學者討論與研發到院前緊急救護服務平台與醫療照護平台之接軌。近年來，各式各樣不同的生理訊號感測裝置，包括將感測器做成飾品形狀、嵌入至衣物內或做成耳機式簡易佩戴，降低病患對感測器的排斥性，並可獲得病患最即時之生理資訊。P.T. Chung 等學者規劃與設計出一或然性關聯資料庫(Probabilistic Relational Database, PBD)並與網頁技術整合應用於醫療資訊系統上[2]。此 PBD 雖然可透過或然率推算未知狀況，有助於病患病情的推估與診斷，但若可整合平時生理狀態資料之蒐集，更可擁有更多推估之參考資訊。J. Fayn 等學者利用 EPI-MEDICS，整合 Ambient Intelligent 與 12 種感測訊號之感測器，形成一個心臟病學之個人健康社群[3]。雖然形成此社群，但若可加入資料主動推播機制，會對資訊傳遞更有效率。H. Li 等學者使用一部 PDA 收集身體感測網路(Body Sensor Network)訊號，並利用心跳速率驅動網路 MAC 傳輸，節省電力增加系統生命周期[4]。此機制雖然可延伸生命周期，若可將此生理訊號延伸應用，此系統會更臻完善。S. Park 將生理訊號感測器放置衣服內，病患只要穿著此保護衣，監護人員即可獲得此病患之生理訊號[5]。T. Taleb 等學者設計與規劃一 Pervasive Environment for AffeCtive Healthcare (PEACH)系統架構，規劃與整合生理感測器與定位服務[6]。PEACH 除可監控病患資訊外，還具備緊急服務功能，但均為偵測數值型態資料，若可整合大量多媒體資料，系統亦會更臻完善。Y. Zhang 與 H. Xiao 學者提出一整合式遠端監護系統，將有線與無線感測器之資料收集於主機中，監護人員即可於遠端查看病患生理訊號資訊[7]。此篇論文中雖以整合有線與無線生理訊號感測器，若可增加主動通報機制給監護人員，如此系統會更臻完善。

傳統醫療的醫療資訊蒐集分享服務平台均是針對特定醫院或特定問題進行規劃與設計，通常只考慮到隱私與安全性，因此大多缺乏互通性、整合性、移動性等功效，僅具資料收集與分享之功能較為欠缺一個有效的即時互動平台來傳遞所蒐集來之資訊，再者除需整合各式不同感測器外，還需提供緊急狀態警訊通知服務，輔助監護人員照護病患，並將到院前緊急救護之功能有效發揮，使救護車到達災禍現場時即可讓位於醫院之醫護人員能有效掌握病患資訊。

3. 系統架構

本論文透過數位匯流將完整之資訊服務及救護車與醫院之醫療服務匯流，建置一具有開放性與通透性之開放式緊急救護服務平台(An Integrity and Transparency-based Open First-aid Service Platform, IT-OFA)，整合救護車端與醫院端之開放平台，其架構圖如圖 1 所示。透過到院前緊急救護人員之手持式設備，建立起延伸之醫療環境，使得醫生能在醫院電腦前面獲得事故現場受傷人員之生理訊號與病患資料，進而提供相關醫療行為與服務建議給位於事故現場之醫護人員。IT-OFA 其主要包含開放式到院前緊急救護服務系統與具通透性之無接縫醫療照護服務平台兩部分，其相關述說如下。

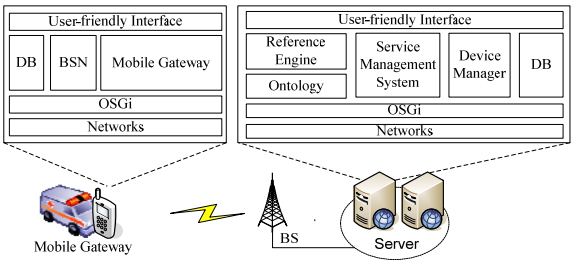


圖 1：IT-OFA 平台架構

2.1 開放式到院前緊急救護服務系統

於建構開放式到院前緊急救護服務系統，其主要透過載具匯流之概念整合(1) Google Android 手機載具匯流服務平台、 (2) 開放式服務平台(Open Service Platform)、 (3) 行動閘道器(Open Mobile Gateway)、(4) 跨異質網路(Over Heterogeneous Networks)、(5) 跨網服務(Cross-LAN Service) 、(6)

生理訊號感測網路等相關技術，以下將簡介主要之設計內容。

(1) 開放式Google Android 手機載具匯流服務平台

Android 為開放手持裝置聯盟(Open Handset Alliance)所規劃與發佈的開放手機作業系統平台，並提供相當完整的函式庫，由應用程式到 Linux 系統核心分為：(a) Application Framework、(b) Android Runtime、(c) Libraries、與(d) Linux Kernel[8]。其架構近似 Java 的運作環境，以虛擬機器(Virtual Machine)達成跨平台的運作架構稱為 Dalvik。於開示放服務平台建構數位匯流服務，數位匯流服務包含網路匯流(Network Convergence)、載具匯流(Device Convergence)、服務匯流 (Service Convergence)。其中，載具匯流意指在終端設備中，使用者能夠使用各種設備經網路在任何時間、地點自由獲得所需要之資訊，使得病患資料在任何載具與情境間能夠流暢、無縫接軌。

(2) 行動閘道器與開放式服務平台

開放式到院前緊急救護服務系統與具通透性之無接縫醫療照護服務平台之匯流模式，透過建置開放式服務閘道平台(Open Services Gateway initiative, OSGi)至 Android 平台上形成行動式閘道器，即可透過 DPWS 將資料有效傳遞至醫院端。使用者所使用之行動式閘道器(Mobile Gateway)透過開放式服務平台之通訊介面與設備控制平台(Device Control Platform)進行通訊，並建立起聯結，使得位於遠端之使用者即可對不同的設備進行操控。其中所使用之訊息均採用標準之 DPWS SOAP 訊息，並觸動所設定好之 WSDL 服務模式。於論文所設計之設備控制平台包括設備註冊單元(Device Register Unit)、設備查詢單元(Device Query Unit)與設備訂閱單元(Device Subscribe Unit)三部分，如圖 2 所示。

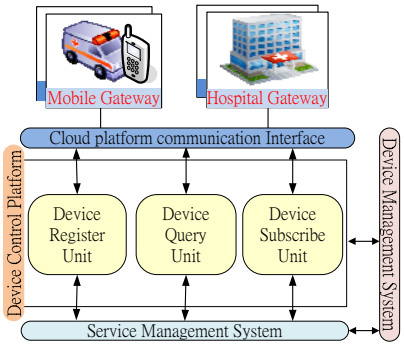


圖 2：設備控制平台架構圖

a. 設備註冊單元(Device Register Unit)：設備註冊單元主要用以管理所有設備。當一個新的醫療感測設備透過設備管理系統(Device Management System)註冊且提供設備服務清單，並轉送設備訊息至特定網路之醫療感測設備。

b. 設備查詢單元(Device Query Unit)：設備查詢單元主要用以控制設備與不同子網域(Sub-network)間之通訊。當網路接到要求描述與展示訊息時，設備查詢單元即會查詢是否有此醫療感測設備位於本網路中且發出回應訊息。

c. 設備訂閱單元(Device Subscribe Unit)：設備訂閱單元主要用以訂閱更新之設備資訊或相關事件。當一個新醫療感測設備註冊至設備註冊單元時，設備訂閱單元即會送出訂閱訊息至訂閱服務。服務管理系統將會得到設備最新之服務資訊，進而透過部落格介面提供給使用者。

2.2 具通透性之無接縫醫療照護服務平台

具通透性之無接縫醫療照護服務平台主要整合(1) 開放式服務閘道平台(Open Services Gateway initiative, OSGi)、(2) 整合設備概況網路服務(Device Profile for Web Services, DPWS)、(3) 案例式推論(Case-based Reasoning, CBR)、(4) 網頁技術(Web 2.0 Techniques)，並規劃與建立(1) 行動設備管理平台與(2) 服務平台部分，以下將介紹主要的設計內容。

(1) 行動設備管理平台

若要建立具備即時監控功能之行動式使用者端情境，需考量不同之閘道器設計，包括行動閘道器(Mobile Gateway)與設備閘道器(Appliance Gateway)以橋接(Bridge)本地端(Local)與遠端(Remote)醫護設備之通訊。因行動閘道器具備電力與計算能力限制之問題，故於本論文中將於行動閘道器中設計行動設備管理平台(Mobile Device Manager Platform)用以處理有效資訊傳遞與通透性問題。行動設備管理平台包括訊息管理單元(Message Management Unit)、遠端設備管理器(Remote Device Manager)與本地端設備管理器(Local Device Manager)。

a. 訊息管理單元(Message Management Unit)：訊息管理單元主要用以控制 DPWS 協定與 SOAP 訊息，主要包括以下三個功能。(a) 監控所發送之 SOAP 訊息以及接收由開放式醫護服務伺服器與開放式服務平台所傳遞之訊息。(b) 翻譯從設備來的 SOAP 訊息與轉遞此訊息至行動設備管理平台。(c) 編譯與轉遞從行動設備管理平台發送出之 SOAP 控制訊息。

b. 遠端設備管理器(Remote Device Manager)：遠端設備管理器主要用以管理遠端之醫療感測設備。圖 3 為遠端設備管理器之架構圖，主要元件為資料庫與遠端設備通訊介面(Remote Device Communication Interface)。資料庫儲存遠端設備資訊，而遠端設備通訊介面提供開放式服務平台(Open Service Platform)通訊介面。遠端設備管理器首先透過訊息管理單元會接收位於遠端設備之起始與歡迎訊息(Initial and Hello Message)，再將相關訊息存於資料庫

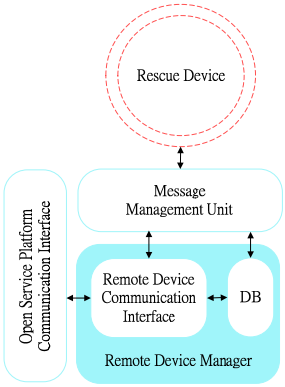


圖 3：遠端設備管理器架構圖

中，並協助建立通訊。

c. 本地端設備管理器(Local Device Manager)：本地端設備管理器負責管理本地端設備與傳送訊息至遠端設備，圖 4 為本地端設備管理器之架構圖。本地端設備管理器主要之工作為透過本地設備通訊介面(Local Device Communication Interface)將本地端設備資訊轉遞。此外，本地端設備將會把設備控制訊息轉遞至醫療感測設備。

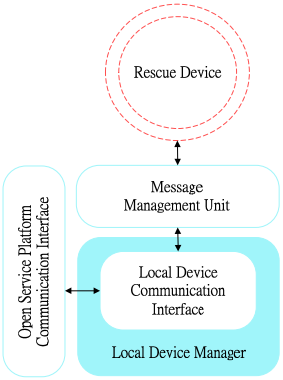


圖 4：本地端設備管理器架構圖

(2) 推論模組

傳統之救護工作只能透過人到現場評估，往往一樣的事件但因專業醫護人員之經驗與處理方式不同，易造成不同之結果。有鑑於此，透過建立本體論與案例式推論機制，建立起建議之流程並配合開放式服務平台進行控制各項醫療感測設備，使得相關之醫療服務能具整體性，其中本體論(Ontology)主要用以敘述與說明該領域下之概念與知識，藉以表達該知識領域下存在的事件與彼此間的關係。可以將 Ontology 分為概念(Concept)、關係(Relation)以及實例(Instance)等元素之組合。圖 5 所示即為：(a) 概念(Concept)：以多個底層物件所建構之範圍，即由各種不同領域相關概念所組成之集合，透過此集合能讓系統了解到定義概念(Concept)所代表的意思。(b) 關係(Relation)：為 Ontology 所描述之領域知識中各個概念與其實例之間的關聯性。(c) 實例(Instance)：用以描述表達與關係(Relation)之關聯性描述將此領域知識中各個概念

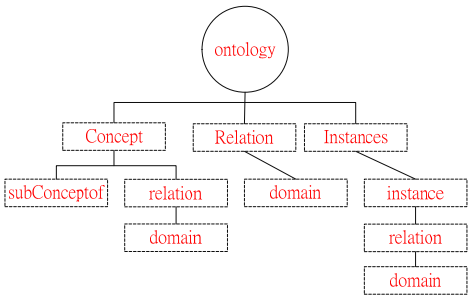


圖 5：本體論概念圖

與實體連接。圖 6 表示的是一個到院前緊急救護之 Ontology 架構，這裡利用屬性來描述其所屬之 Concept 下的某些特徵與特性，因此在其它 Concept 與 Instance 中也都會有各自的屬性來表達該 Concept 的結構與性質。

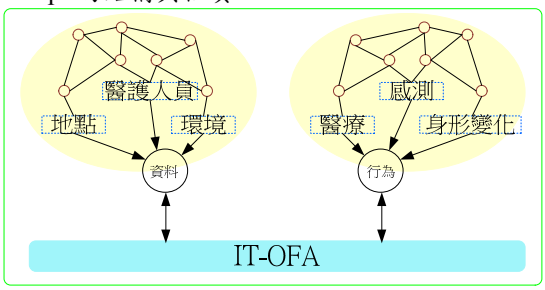


圖 6：First-Aid 情境下之本體論建置模式

(3) 案例式推論(Case-based Reasoning, CBR)

位於網際網路後端之主動式資料庫，彙集相關之觸發因子(Triggers)、改良傳統資料庫成為一個主動式資料庫(Active Database)，在所設計之主動式資料庫中採用 E-C-A(Event-Condition-Action)模型處理資料，讓所有的資訊不再被動查詢，主動式資料庫將依感測網路與三軸加速規感測器所感測之情況主動通知使用者，不需讓使用者自己下查詢語法(Query Language)，進而影響資料通報時間，因此主動式資料庫 E-C-A 模式之設計如圖 7 所示。

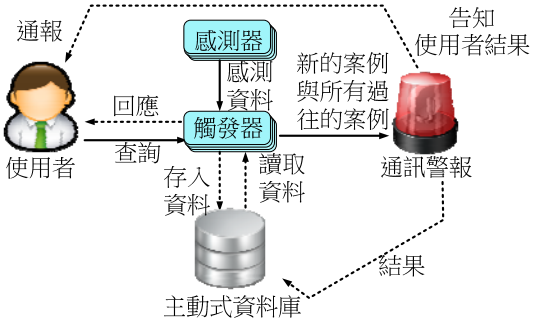


圖 7：主動式資料庫與觸發因子選定與推論

首先感測器感測資料輸入主動式資料庫，然後觸發器判別，判斷是否有危險因子(Factors)存在於所輸入的資料中。當有危險因子時會將此訊息主動傳遞給使用者，不需等待。在此計劃觸發因子為心跳、脈搏、血壓與體溫。

案例式推理主要的功能是將新的案例與過往所遇到案例進行比對，由過去舊案例的結論推估到現

在所遇到問題並產生建議的結果[9]。案例式推理的運作流程如圖 7 所示。CBR 主要的四個步驟為取出過往案例(Retrieve)、重覆使用(Reuse)、修改(Revise)與保留(Retain)四個部份。於本論文案例式推理為利用歐基里德距離(Euclidean Distance)公式，並配合平均相對誤差(MMRE)與平均絕對誤差(MARE)進行誤差值之計算。其相關公式如公式(1)所示：

$$ED_i = \sqrt{(\alpha_i - \alpha)^2 + (\beta_i - \beta)^2 + (\gamma_i - \gamma)^2 + \cdots} \quad \forall i \in case_{\{1..i\}} \tag{1}$$

ED_i：對於第 i 個案例所產生的歐基里德距離。

$Case_i$：第 i 個案例。

α,β,γ：新案例之特徵值。

$\alpha_i,\beta_i,\gamma_i$：新案例之特徵值。

所運算出來最小 ED_i 值為所遇到新問題與此舊案例之最相似評估值，進而可以推斷兩個案例所發生的結果可能相似。但新舊案例並非全然相同，在評估時會產一誤差值，因此需使用平均相對誤差(MMRE)進行研判誤差值是否過高，此外並偵測出偏離的方向，如公式(2)所示：

$$MMRE = \left(\sum_{i=1}^{n} \frac{A_i - E_i}{E_i}\right) \times \left(\frac{1}{TC}\right) \tag{2}$$

A_i：評估案例的實際值。

E_i：過往案例的實際值。

TC：過往案例的總數量。

由於 MMRE 有正負偏差，誤差範圍很大或會被抵消，因此測量誤差值的公式可採用平均絕對誤差(MARE)方式，希望透由 MARE 來偵測出預測偏離值。如公式(3)所示：

$$MARE = \left(\sum_{i=1}^{n} \frac{|A_i - E_i|}{E_i}\right) \times \left(\frac{1}{TC}\right) \tag{3}$$

計算出預估值之後配合誤差值運算結果，使得推論研判更為精準。

(4) 會話發起協議(Session Initiation Protocol, SIP)

SIP是一個基於TCP/IP協定上層運作之信令協議，SIP協議主要是用來描述如何建立網際網路電話呼叫、視訊會議、及其他的多媒體連結，在SIP環境中的元件主要分為兩種，分別為SIP客戶端User Agent Client(UAC)以及SIP伺服器端User Agent Server(UAS)，在SIP中凡是送出Request就稱之為SIP Client而伺服器端則是負責回應客戶端所發出的Request進而發出Response的元件，SIP只負責控制信號而不負責傳輸資料，資料的傳輸是由會話描述協議(Session Description Protocol, SDP)負責描述，SDP可視為SIP的一部份，SIP若是沒有SDP則不能單獨運作，資料的傳輸可由SIP配合RTP、TCP、UDP等通訊協定來完成，本論文結合OSGi將IP CAM建置在行動式閘道器上，透過行動式閘道器將IP CAM所攝錄之即時畫面利用SIP上傳至IT-OFA進行備份並可即時於數位電視上進行監控[10]，如圖 8 所示。

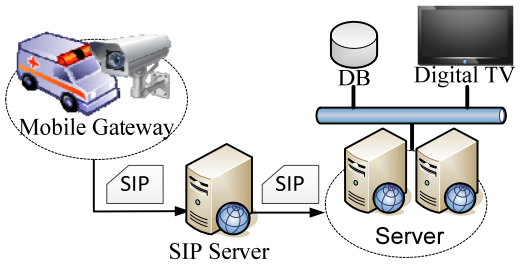


圖 8：即時監控架構圖

(5) 網頁技術(Web 2.0 Techniques)。

RSS 監控技術匯流：當所訂閱之部落格或病患資訊更新時，則將所訂閱之資訊利用 RSS 技術傳遞給使用者，主要研究議題包括 RSS 訂閱服務、部落格(BLOG)與 XML 標籤轉換器(XML Transformer)三部份，其架構如圖 9 所示。

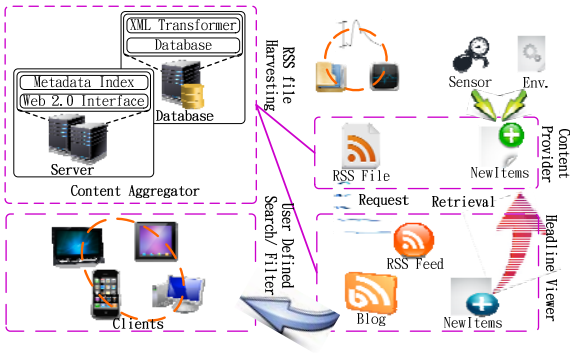


圖 9：RSS 技術架構圖

在此規劃為三部份，包括內容供應者(Content Provider)、內文集結器(Content Aggregator)與瀏覽者(Headline Viewer)。(a) 內容供應者：提供不同的感測器所擷取之資料，並將此資料利用 XML 之 TAG 轉換成 RSS 格式，以利發佈。(b) 內容集結器：主要是收集不同來源的 RSS 檔案，依照不同的 RSS 性質來分類且客製化成不同的形式。依照訂閱者的需求來提供過濾或是搜尋不同的 RSS 檔案，並存於資料庫中以便發佈。(c) 照護者：透過 RSS 技術可以依照護者的 RSS 內容集結器取得想要的 RSS 檔案並且顯示在不同的設備上，再透過組裝技術(Mashup)成為所需之資訊，如此使用者只要連上具開放性與通透性之開放式緊急救護服務平台就可以享受到完整的資訊不需再選取。

4. 系統實作

本章節將展示具有開放性與通透性之開放式緊急救護服務平台(An Integrity and Transparency-based Open First-aid Service Platform,

IT-OFA)相關之實作畫面，其系統畫面如圖 10 所示。



圖 10：IT-OFA 平台畫面

此外於救護車監控畫面透過 SIP 協議來進行即時畫面之傳輸，除了將其儲存至 IT-OFA 上資料庫外更可透過數位電視來進行即時監控以便保障病患之權利。本論文之數位電視使用 Eclipse Google TV Add-on(API Level 13)進行模擬用以接收即時監控畫面，即時監控畫面則以病床監控畫面進行實現，其監控畫面如圖 11 所示。

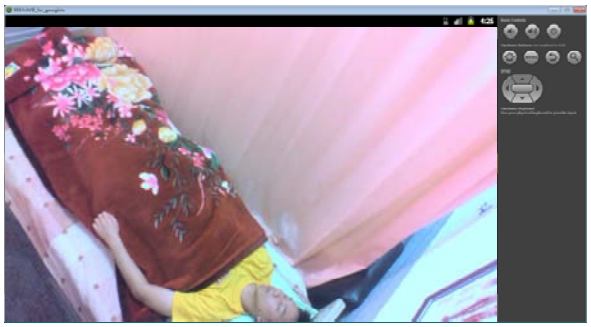


圖 11：救護車即時監控模擬畫面

5. 結論

本論文利用數位匯流技術建置一具有開放性與通透性之開放式緊急救護服務平台(An Integrity and Transparency-based Open First-aid Service Platform, IT-OFA)，透過到院前緊急救護人員之手持式設備，結合開放式到院前緊急救護服務系統與具通透性之無接縫醫療照護服務平台，建立起延伸之醫療環境，實現(1) 無線與行動通訊網路 (Wireless and Mobile Network Communications)情境。利用無線行動通訊環境進行即時(Realtime)雙向資訊之傳遞，病患之生理訊號會透過感測器進行收集，再由救護車傳遞至醫院中。主要技術包括整合 3G 行動通訊服務、藍牙(Bluetooth)與 Zigbee 等相關通訊服務。(2) Web2.0 部落格技術之規劃與制定。規劃與實現匯流式 Web 介面，透過 XML、SOAP 與 WSDL 等網頁技術、並提供一個友善的介面給使用者，在此將整合設備概況網路服務(DPWS)、開放式服務閘道平台與推論機制服務。 (3) 行動化閘道器(Mobile Gateway)。透過 android 開放式服務平台技術，將於手持式設備上與醫院環境中建置開放式 OSGi 閘道器，以使控制信號(Signal)、訊息(Message)與資料(Data)能相互流通。

於未來研究方向將朝向(1) 對於推論機制模組化與適性化整合並可於感測資料海中探勘相關之資料建立反饋機制(Feedback mechanism)並獲得與調適(Adaptive)所需之服務。(2) 將加速本體論推論機制，並整合多項感測因子進行推論，輔以更正確與更迅速達到有效推論機制之建立。(3) 匯整更多不同的輔助媒體與情境，增強多媒體輔具的整合。

6. 致謝

本研究承蒙國科會研究計畫予於補助，(計畫編號：NSC 101-2221-E-146-005 與 102-2815-C-146-004-E)，得以順利完成此研究，在此獻上最誠摯的謝意。

參考文獻

[1] H.H. Ku and C.M. Huang, “Web2OHS: A Web 2.0-based Omni-bearing Homecare System,” IEEE Transactions on Information Technology in Biomedicine, Vol. 14, No. 2, pp.224-233, 2010.

[2] P.T. Chung, F. Afzal and H.H. Hsiao, “A Software System Development for Probabilistic Relational Database Applications for Biomedical Informatics,” Proceedings of International Conference on Advanced Information Networking and Applications Workshops, pp. 1002-1007, 2009.

[3] J. Fayn, P. Rubel, “Toward a Personal Health Society in Cardiology,” IEEE Transactions on Information Technology in Biomedicine, Vol. 14, No. 2, pp. 401-409, 2010.

[4] H. Li and J. Tan “Heartbeat-Driven Medium-Access Control for Body Sensor Networks,” IEEE Transactions on Information Technology in Biomedicine, Vol. 14, No. 1, pp. 44-51, 2010.

[5] S. Park and S. Jayaraman, “Smart Textile-Based Wearable Biomedical Systems: A Transition Plan for Research to Reality,” IEEE Transactions on Information Technology in Biomedicine, Vol. 14, No. 1, pp. 86-92, 2010.

[6] T. Taleb, D. Bottazzi, N. Nasser, “A Novel Middleware Solution to Improve Ubiquitous Healthcare Systems Aided by Affective Information,” IEEE Transactions on Information Technology in Biomedicine, Vol .14, No. 2, pp.335-349, 2010.

[7] Y. Zhang and H. Xiao, “Bluetooth-Based Sensor Networks for Remotely Monitoring the Physiological Signals of a Patient,” IEEE Transactions on Information Technology in Biomedicine, Vol. 13, No. 6, pp. 1040-1048, 2009.

[8] Google, Android, http://code.google.com/intl/zh-CN/android/what-is-android.html

[9] A. Amodt and E. Plaza, “Case-Based Reasoning: Foundational Issues, Methodological Variations, and System Approaches,” AI Communications, Vol. 7, No. 1, pp39-59, 1991.

[10] S. Spinsante and E. Gambi, “ Remote health monitoring by OSGi technology and digital TV integration”, IEEE Transactions on Consumer Electronics IEEE Transactions on, Vol. 58, pp.1434-1441, 2012.

A Multimedia Sharing Scheme on IMS-based Digital Convergence Platform

Jian-Wei Li
Department of Information and Communication Engineering, Chaoyang University of Technology
Taichung, R.O.C
lijw@cyut.edu.tw

Yen-Lun Chiu
Department of Information and Communication Engineering, Chaoyang University of Technology
Taichung, R.O.C
s10030610@cyut.edu.tw

Yi-Chun Chang*
Department of Computer Science and Information Engineering, Hungkuang University
Taichung, R.O.C
changyc@sunrise.hk.edu.tw

ABSTRACT

In this era with network environment omnipresent, a person accesses network services anytime through the mobile network and a personal device but probably fails in sharing video streaming among all surrounding friends via his/her own mobile device with a finite-sized screen. In this paper, we studied and designed a multimedia sharing scheme by which a sharer allows synchronous video streaming to be accessed by other users through their own mobile devices as is the sharer. Preferably, the sharing service constructed on the IP Multimedia Subsystem (IMS) in this study can be available for more users via different access networks in the future.

Keyword: multimedia sharing; IMS; video streaming; synchronous video streaming.

I. INTRODUCTION

People who live in a technology-advanced environment have more channels to catch information or to enjoy multimedia services, for example, data query, e-mail and multimedia service access which is realized by Quad-Play technology through mobile networks (e.g., Wi-Fi and 3/3.5G) and personal devices (e.g., Android Phone and iPhone) in recent years. With existing telecommunication networks, broadcast TVs and Internet integrated, the Quad-Play technology provides convenient mobile application services to users who can use a single platform to access multiple services including data, audio, video and mobile communications [1] in addition to traditional desktop computers and wired networks.

Although convenient, the mobile network service such as multimedia streaming enjoyed by one user through a personal handheld device outdoors may not be shared by surrounding friends simultaneously due to a finite-sized screen on a handheld mobile device.

Against this background, we designed the multimedia sharing scheme through which the authority to enjoy multimedia streaming possessed by one user originally is shared by surrounding friends according to control of SIP (Session Initiation Protocol). In this regard, these people depending on the mobile network and personal mobile devices utilize the same multimedia streaming broadcasted synchronously as does the original owner who still owns exclusive session control over multimedia contents. Similar to a conference call in which all invitees or participants communicate with each other through a host control server, the multimedia sharing still has its feature different from the conference call, for example, the multimedia sharing is based on REFER that allows receivers to make conversations with the multimedia source and synchronously receive but not control multimedia from the source.

In this study, the multimedia sharing service is constructed on the IP Multimedia Subsystem (IMS) network which is not only the core architecture of the Next Generation Network (NGN) formulated by 3GPP and 3GPP2 [2][3] but also one platform accessed by users who intend to use top-level application services through different network technologies (e.g., 3G, LTE and Wi-Fi). IMS supports multimedia application services such as Push to Talk over Cellular (PoC), Voice over IP (VoIP) [4] and Internet Protocol Television (IPTV) [5]. Based on SIP to control and manage the multimedia session, IMS is able to find appropriate application services after processing a user's service requests .

The other sections in this paper are introduced as follows: section 2, background of IMS network system/architecture and introduction of the similar multimedia sharing technology; section 3, the system architecture of multimedia sharing technology used in our research; section 4, introduction of environment and methods to use multimedia sharing and the process to transmit message on the IMS network(s); section 5, conclusion.

II. BACKGROUND KNOWLEDGE

As one platform on which the services such as multimedia sharing are constructed, the whole IMS network needs to be introduced and understood, for instance, its basic architecture and operation of relevant components. Another topic to be investigated herein is session mobility [6] related to multimedia sharing in SIP.

A. *IMS Network*

The IMS Network, i.e., IP Multimedia Subsystem Network, which is the control layer of the Next Generation Network (NGN) and formulated by 3GPP and 3GPP2 [2][3], is used to access different network technologies such as Wi-Fi, LTE, 3G/3.5G and wired network and depends on SIP as the communications protocol to control SIP signals by the Call Session Control Function (CSCF). The brief network architecture of IMS is shown in Fig. 1.

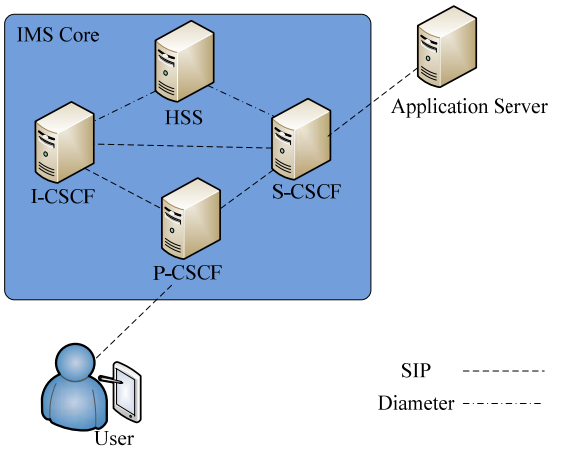


Figure 1. Brief network architecture of IMS

1) P-CSCF (Proxy-CSCF): As the first IMS network server faced by one user, P-CSCF forwards a user's messages into IMS, SIP messages to I-CSCF for further processing, and any SIP signal response to a user.

2) I-CSCF (Interrogating-CSCF): I-CSCF is a query server which relies on a user's SIP requests or information brought by P-CSCF to find an appropriate S-CSCF for relevant services and saves the information in HSS for other queries later.

3) S-CSCF (Serving-CSCF): S-CSCF is a service server which is particularly used in processing a user's service requests and depends on the requests to find a corresponding application server.

4) HSS (Home Subscriber Server): HSS in IMS is particularly used in storing users' data such as e-mail, phone number and user's authority to access services.

5) Application Server (AS): As a top-layer application server such as multimedia streaming and monitoring system, AS depends on S-CSCF to give a user services.

B. *Session Mobility*

The session mobility means current sessions transferred from one communications device to the other one by SIP with no session service interrupted and utilizes a mechanism known as Call Transfer classified into two methods, REFER and 3PCC (Third Party Call Control), which are formulated by RFC 3515[7] and RFC 3725[8].

As shown in Fig. 2, 3PCC is used to construct a session between a third party controller who is responsible for media negotiation and two or more other participants. Controller initiates a session and controls the session between two users including Customer Service (CS) and User Phone: Controller sends "INVITE" with no SDP inside to CS; CS responds "200 OK" with supported session types included; Controller sends "INVITE" including CS information to User Phone; User Phone responds its own "200 OK" with supported session types included to "INVITE"; Controller provides information for supported session types to CS; all participants own equivalent information; the conversation is completed [9].

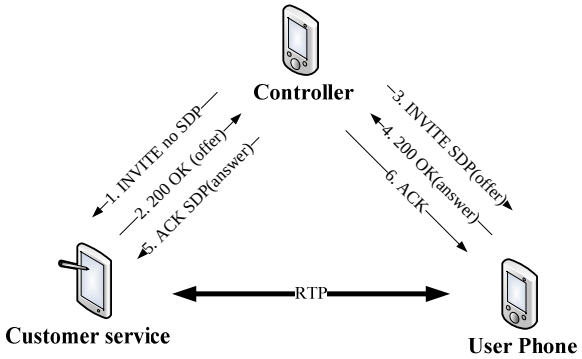


Figure 2. Schematic diagram of a 3PCC process [9]

As shown in Fig. 3, REFER that is one technique of inviting a new user or one device to join a session through an original user defines the header "Refer-To" recording the third party's SIP URI by which the original user can invite the third party to construct a session after receiving "REFER".

In Fig. 3, Alice, who has a session with Bob and intends transferring the session to Carol, sends Bob "REFER" with Carol's URI included; Bob gives Carol "INVITE" and Alice "Accepted" by which Alice recognizes "REFER" is received by Bob; Bob receives "200 OK" from Carol, who agrees the session, and sends Alice "NOTIFY"; Alice identifies the session between Bob and Carol and completes the session with Bob [9].

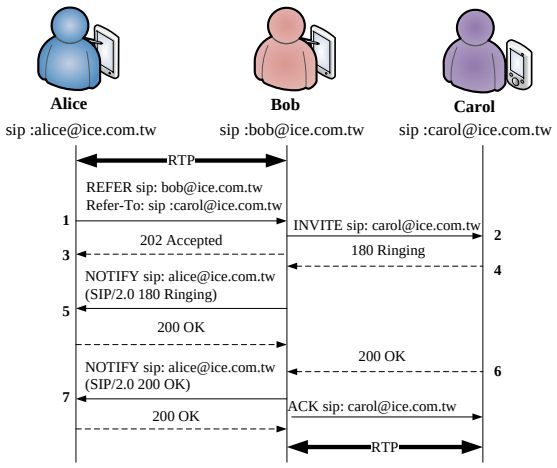


Figure 3. Steps to transmit REFER signals [9]

Based on 3PCC and REFER, session mobility contributes to a session transferred to an appropriate device by one user at a different environment, for example, a video session via the 3G network and a user's mobile device switched to via a home computer and the network by session mobility for endless service. In addition to session mobility, session split is another service introduced in [6][10]. For instance, the multimedia streaming video or audio program broadcasted via a mobile device and the 3G network outdoors is also played on an Internet Protocol TV or stereo at home with streaming split to a distinct device according to prevailing environment and equipment.

In the case of users' and their friends' personal mobile devices rather than alternative devices, multimedia sharing is effective in multimedia streaming shared among the surrounding friends' mobile devices and synchronously watched by device owners through the mobile network. In this regard, the method based on REFER for multimedia sharing is particularly introduced in section 4.

III. System Architecture

In this study, multimedia sharing is constructed on an IMS platform with system architecture as shown in Fig. 4. The IMS platform can be separated into three parts, IMS Core, IMS Client, and IMS Application Server (IMS AS). IMS Clients includes users and their mobile devices or are classified into sharers and receivers: a sharer (User1 in Fig. 4) shares multimedia streaming with receivers (User2 and User3 in Fig. 4) who access no multimedia service in the beginning. IMS AS includes servers such as Multimedia Agent (MA) and Presence Server (PS): MA provides users multimedia sources, e.g., multimedia streaming server, webcam, etc.; PS presents information of on-line friends, who are recognized by a sharer, and contributes to multimedia sharing services on the IMS network.

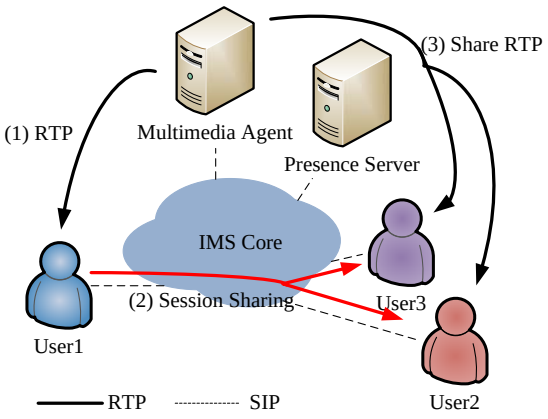


Figure 4. IMS-based multimedia sharing architecture

As shown in Fig. 4, RTP (Real-time Transport Protocol) streaming between a sharer and MA has existed before a session is shared by a sharer. Then, the sharer identifies any on-line receiver via PS and makes multimedia sharing available to the receiver who prefers the sharer's streaming services.

IV. Method of Mutimeida Sharing

A. Context of Application Service

Alice and her friends Bob and Carol go to a party outside. Suddenly, Alice who has been staying gossiping with her friends wants to check her home and links a household webcam via her handheld device to find something interesting about her family members. Alice intends to share it with both guys but the image on her handheld device is too small to be watched by three persons simultaneously. Considering no device with a bigger display there, Alice shares her own multimedia streaming at Bob's and Carol's handheld devices and makes an interesting thing at home clearly displayed on their personal devices.

In this context, Alice's role is the sharer, Bob & Carol are receivers accepting multimedia sharing, and the household webcam is MA which is accessed and controlled by someone with the authority, for example, premium channel or private web camera installed in a house or office and accessed by others who are authorized by the sharer. In this regard, these devices or services cannot be controlled by an authorized receiver watching videos but by the service sharer who possesses control rights.

B. Designs of Signal Transmission in a Process of Multimedia Sharing Service

In this study, the multimedia sharing service is constructed on the IMS network(s). Against this background, Alice, who has interacted with MA to get multimedia streaming before sharing, utilizes REFER to request a connection built between a receiver, Bob or Carol who needs multimedia streaming, and MA. Fig. 5 illustrates the first design for Alice, Bob and Carol on the same IMS network.

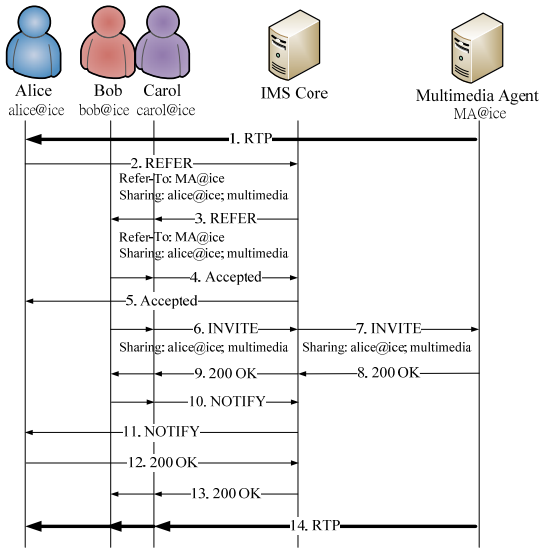


Figure 5. Steps for signal transmission of multimedia sharing (a sharer and receivers on the same IMS network)

The detailed steps for signal transmission of multimedia sharing in Fig. 5 are shown as follows:

Step 1: Alice interacts with MA to get multimedia streaming before multimedia sharing.

Step 2: Alice sends “REFER” to Bob and Carol recognized as on-line users by Alice through the Presence Server before sharing multimedia streaming.

Steps 3-5: Bob and Carol respond “Accepted” to Alice through the IMS network after receiving “REFER”.

Steps 6-7: The “INVITE” along with the header “Sharing” from Bob’s and Carol’s personal mobile devices is sent to MA through the IMS network.

Steps 8-9: MA sends “200 OK” after receiving “INVITE”.

Steps 10-11: Bob and Carol send “NOTIFY” to Alice via the IMS network after receiving a response from MA.

Steps 12-13: Alice who has received “NOTIFY” recognizes multimedia sharing and sends “200 OK” to Bob and Carol for the same multimedia streaming shared by the sharer and receivers.

V. Efficiency Analysis and Comparison

In contrast to a traditional conference call which depends on a host server to control and transmit conversations or multimedia videos among participants who invite other users to join the conference anytime, the multimedia sharing features a sharer who manages other conference members (i.e., receivers) and administers multimedia. In the case of fixed users on the same network who have mobile devices and try to enjoy authority-based multimedia streaming, the users can access multimedia provided by a sharer after accepting the sharer’s sharing on the basis of multimedia sharing scheme; however, a sharer in a conference call has to post the source location of multimedia streaming and provide authority information such as username and password to fixed receivers who incline to access multimedia but spend more time to take them.

VI. Conclusion

The advantage of this study is a sharer, who tries to share authority-based multimedia streaming with surrounding users or friends holding personal mobile devices only, is able to reach his/her goal by way of multimedia sharing, for example, the users or friends watch synchronous video streaming on their own mobile devices. Moreover, users can access services via different wireless network technologies (e.g., Wi-Fi, 3G and LTE) in the IMS network environment.

VII. Acknowledgment

The research is supported by the National Science Council of the Republic of China under the grant Number NSC 102-2221-E-324-012 and NSC102-2221-E-241-015

Reference

[1] J. Ulm, B. Weeks, “Next Play Evolution: Beyond Triple Play & Quad Play,” IEEE International Symposium on Consumer Electronics (ISCE) , pp. 1-6, 20-23 June 2007.

[2] IP Multimedia Subsystem (IMS) Handbook. Syed A. Ahson, Mohammad Ilyas: CRC Press.

[3] Converging NGN Wireline and Mobile 3G Networks with IMS: Converging NGN and 3G Mobile. Rebecca Copeland: CRC Press.

[4] Y. He, J. Veerkamp, A. Bilgic, “Analyzing the Internal Processing of IMS-based and traditional VoIP systems, ” Telecommunications: The Infrastructure for the 21st Century (WTC) , pp. 1-6, 13-14 Sept. 2010.

[5] E. Mikoczy, S. Schumann, P. Podhradsky, T. Koski, M. Heinikangas, “Hybrid IPTV Services with IMS: Integration of IMS Based IPTV with Broadcast and Unicast Mobile TV Services Using DVB-H,” International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST) , pp. 76-81, 14-16 Sept. 2011.

[6] M. Rawashdeh, A. Karmouch, “Seamless Video Handoff in Session Mobility over the IMS Network,” IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks & Workshops (WoWMoM) , pp. 1-6, 15-19 June 2009.

[7] R. Sparks, “The Session Initiation Protocol (SIP) Refer Method,” RFC 3515, IETF, April 2003.

[8] J. Rosenberg, J. Peterson, H. Schulzrinne, G. Camarillo, “Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP) ,” RFC 3725, IETF, April 2004.

[9] M. Chen, C. Peng & R. Hwang, “SSIP: Split a SIP Session over Multiple Devices,” Computer Standards and Interfaces, vol. 29, no. 5, pp. 531-545, Jan. 2007.

[10] K. Geunhyung, Y. Gunil, “Streaming Session Mobility across Multiple Devices in Mobile IPTV Environments,” Proceedings of the 4th International Conference on Ubiquitous Information Technologies & Applications (ICUT) ,pp. 1-6, 20-22 Dec. 2009.

急診即時查詢與導航服務系統之研發

曹祐誠[1] 李昭賢[1] 陳昭文[2] 王冠傑[2]
[1]國立臺北科技大學電子工程系
[2]高雄醫學大學附設中和紀念醫院
chlee@ntut.edu.tw (Correspondence)

摘要

近年來智慧型手機之普及，帶動各式各樣的APP 不斷推陳出新，其中整合全球定位系統(GPS)與地理資訊系統(GIS)之適地性服務(LBS)儼然成為民眾生活不可缺少的重要網路應用服務之一，隨處可見民眾透過智慧型手機，搭配 Google Map 線上地圖服務，使用導航功能尋找並指引前往目的地。本論文將應用適地性服務於急診醫療之服務品質改善，透過整合提供急診服務之醫療單位，提供即時的急診服務壅塞狀態，如：急診等待人數、病床容量、救護人員數量…等，為方便使用者快速判別各急診情形，本次設計之 APP 將會將複雜之急診服務品質參數轉換成容易識別之燈號，並依照使用者目前所處之地理位置，動態顯示周圍提供急診服務的醫療院所即時狀態給需要就醫之民眾，一方面可避免民眾出外不熟悉地區造成延誤就醫、另一方面可避免就醫等待過久之痛苦與焦慮。

關鍵詞：急診、適地性服務、範圍查詢、地圖導航、路徑規劃。

Abstract

With the widespread of smart phones, various APPs are developed to provide all kinds of network services. Location-based service (LBS) integrating Global Positioning System (GPS) and Geographic Information Service (GIS) gradually becomes one of the essential Internet services for modern life. More and more people utilize their smart phones to access Google Map service and then navigate themselves to the destination. This paper applies LBS into emergency medical service for quality improvement. We cooperate with several hospitals to deliver real-time congestion status of emergency medical unit, e.g., the patient number in the waiting room, occupancy rate, the number of doctors and nurses, etc. In order to let patients realize the congestion status easily, the APP proposed in this paper converts complex metrics about the emergency departments into simple signals, i.e., red, yellow and green. Then, our APP would show these signals on the map. Patients can access the congestion signals based on their locations. At the same time, patients can be navigated to the neighboring and available emergency department and avoid waiting for a long time.

Keywords: Emergency Medicine, Location-based Service (LBS), Range Query, Map Navigation, Route Planning

1. 前言

人生無常，誰也不知道下一秒自己或者周遭會發生什麼意外，新聞中經常出現車禍災害、肇事逃逸、工安意外…等報導，若未能把握急救的黃金時刻而導致傷重更為嚴重，甚至喪失寶貴的性命將造成二次傷害，故緊急醫療救護攸關人命，不能賭任何運氣，緊急病患運送流程必須以最迅速或最適當作為責任醫院運送的條件篩選，在運送途中，由緊急醫療技術員(Emergent Medical Technician，EMT)進行初步急救，延長寶貴的黃金救護時刻。

除了上述緊急情況外，在現實生活經驗中，民眾亦經常發生就醫不便之情況，舉例來說：中國農曆年假時間或一般非門診時段，若民眾臨時發生病痛，僅剩各醫院急診處可提供民眾就醫，一般民眾會直覺前往鄰近之醫院，但可能會發生(1)身處不熟悉之地理環境，故不清楚臨近之醫院所在，或(2)到達鄰近醫院卻發生人滿為患，需等待多時才可接受治療之窘境。

依據臺北市政府消防局統計資料顯示，臺北市救護量逐年攀升，轄區內 78 部救護車，13 年來、已出勤超過137萬次，也就是平均每2名台北市民，就有一人曾撥打119叫救護車；而去年使用救護車、超過 10 次以上者，就有 149 位。因此，緊急醫療救護資源更顯珍貴，濫用救護車除直接影響真正需要的民眾外，更可能危及廣大市民之生命安全，並有違社會資源公平共享之精神，長久下來勢必降低緊急醫療服務之效率及品質，臺北市政府衛生局呼籲若非屬緊急狀況，例如拿藥、換藥或門診就醫等需求，應優先利用其他交通工具就醫，避免造成救護車濫用之情形，使民眾獲得最妥適的服務，也讓緊急醫療救護資源得以發揮最大之效用。

倘若有一套緊急醫療服務之即時查詢與應變服務系統，可避免並改善民眾就醫可能遭遇之延誤或不便。本論文提案整合緊急醫療單位，將各醫療院所的即時急診服務狀態，如：急診等待人數、病床容量、救護人員數量…等轉換成急診壅塞指標，並透過適地性服務將急診服務狀態提供給需要就醫之民眾或第一線負責緊急救護之人員使用與參考，本論文中將結合適地性服務(LBS)中用來篩選

臨近興趣點(Point of Interests，PoI)，其中，範圍查詢(Range Query，RQ)與 k Nearest Neighboring (k-NN)演算法可從眾多醫療院所中依據就醫民眾的地理位置過濾出最合適的候選責任醫院[1]-[4]，依照提案情境，若使用者是一般民眾且屬於未危及生命安全之就醫需求，則一般民眾可透過此 APP 獲得最即時的急診服務狀態，選擇最適合的醫院就診。

根據以上動機與目標，本論文之綱要如下：第 2 節回顧相關文獻與發展現況；第 3 節介紹研究方法與步驟；第 4 節說明系統實作細節；最後，第 5 節為結論與未來展望。

2. 文獻探討與回顧

適地性服務(LBS)可透過 GPS 訊號取得經、緯度或透過無線網路基地台(包含：Wi-Fi 或 3G/3.5G/4G 電信網路)取得大致地理位置座標，然後搭配可輸入、儲存、查詢與分析地理空間資訊的 GIS 系統，提供使用者地理資訊相關的加值服務[5]-[7]。根據使用者目前所在地理位置進行特殊資料讀取行為，讓適地性服務(LBS)孕育出不同領域、多樣性的應用，包含：(1)尋找某一人或物的地理位置，如：找距離最近之郵局或加油站；(2)引導前往某處的路徑，如：導航(Navigate)使用者前往最近之電影院；(3)追蹤人或物的地理位置，如：貨運包裹目前運送狀態、車輛移動路徑；(4)行動商務(Commerce)與廣告(Advertising)，如：當使用者進入商場範圍，可自動接收商場特價商品資訊；(5)個人氣候預報，如：當外出旅行自動取得當地的旅遊氣候資訊…等，過去已有研究設計並實現上述服務，並完成相關系統[8]-[10]。

使用者透過送出適地性查詢(Location-based Query)以取得適地性服務，適地性查詢可分成(1)空間查詢(Spatial Query)與(2)時間查詢(Temporal Query)，其中時間查詢可再分成(1)連續查詢(Continuous Query)和(2)非連續查詢(Non-continuous Query)，依據過去研究顯示，常見的空間查詢有(1) 範圍查詢(Range Query，RQ)：在指定的區域內尋找是否有指定物件的存在，範圍查詢(RQ)依照其指定的物件是靜止不動或可移動，又可以分成 Static RQ 與 Moving/Mobile RQ 兩種；(2) Nearest Neighbor (NN)：根據指定地理座標，尋找距離最近的指定物件，假設欲尋找的物件數量為 k，則 k-NN 代表根據指定地理座標，尋找前 k 個距離最近的指定物件[11]。

過去研究為了提升查詢與檢索(Indexing)效能，常透過建立 R-tree 作為檢索之資料結構，因此，有研究針對 Continuous k-NN Query 提出以 ISR-tree 替代 R-tree，ISR-tree 的特點是利用 Grid 結構取代 Tree 結構，因此可避免不必要之父節點(Parent Node)查詢，而直接前往鄰近節點(Neighbor Node)查詢[12]；有研究則針對 Moving/Mobile RQ 提出以 Grid R*-tree 作為檢索之資料結構，配合提出之 Query Update 演算法可有效減少比對時間消耗，以及避免不必要的更新[13]；另一方面，有研究則同時考慮 k-NN Query 與 RQ，利用 Estimated Valid Region (EVR)找出查詢的有效空間與時間區域，針對不同查詢產生不同檢索結構，以 EVR-tree 負責 k-NN Query、Grid Index 負責 RQ [14]。

3. 研究方法與步驟

本論文將選擇 Android 作業系統作為本次開發平台，設計一套可整合緊急醫療單位，將各醫療院所的即時急診服務狀態以急診壅塞指標呈現至 Google Maps 之上，提供給需要就醫之民眾或第一線負責緊急救護之人員快速且直覺化之急診資訊傳遞，此外，使用 RQ 演算法自動將眾多醫療院所依據就醫民眾的地理位置過濾出最合適的候選責任醫院，期望大幅提升病患的運送效率，進而提升病患的生存率。本論文研究方法及步驟分述如下：

Step 1：了解並制定急診壅塞指標

由於急診服務狀態會隨時間而不斷改變，舉凡當班人數、就診人數、檢傷級別、呼吸器使用人數、急診佔床率、各別候診或待床時間、每單位時間醫師看診人數、留置病患人數、醫師病患比例…等現場狀態，皆可反映或呈現集錦運作的順暢性，故研究的第一步必須先了解前述各項參數的精確計算與影響性，並參考相關文獻參考，導入各種急診壅塞評估模型，計算出最佳之急診壅塞指標，最後以直覺化方式呈現，在本論文中預計將採用類似交通號誌：紅、黃、綠三種不同顏色燈號作為急診服務

表 1 急診壅塞指標計算與參數

急診工作負荷指數(EDWIN)	
EDWIN = $\sum n_i t_i / N_a (B_t - P_{board})$	
急診壅塞指數(NEDOCS)	
NEDOCS = $(P_{bed}/B_t)*85.8*(P_{admin}/B_h)*600 + W_{time}*5.64 + A_{time}*0.93 + R_n*13.4 - 20$	
急診佔床比率(Occupancy Level)	
OL = $100 * (P_{bed}/B_t)$	
急診工作分數(Work Score)	
WS = $3.23*(P_{wait}/B_t) + 0.097*(\sum n_i t_i / N_n) + 10.92*(P_{board}/B_t)$	
n_i：已檢傷尚未看診人數	t_i：反向檢傷級別
N_a：急診醫師數	B_t：急診總病床數
P_{board}：已看診病人數	P_{admin}：住院病人數
P_{bed}：急診目前總病人數	B_h：醫院總病床數
W_{time}：最後病患配床時間	R_n：呼吸器數
A_{time}：掛號後留置最久時間	N_n：護理人員數

P_{wait}：等待看診病人數

狀態之呈現方式。本系統預設之急診狀態收集與回報機制以半小時為單位，換言之，加入此緊急醫療即時查詢與應變服務的醫院，每半小時回報其急診服務相關參數至本服務平台的伺服器，讓使用者可透過 APP 查詢即時的急診壅塞狀態。表 1 顯示本論文使用之急診壅塞指標。

Step 2：實作以 Range Query 為基礎之緊急醫療即時查詢與應變服務系統 APP

本次設計之 APP 執行後會自動定位，以使用者目前位置為中心，如圖 1 所示，將方圓半徑 X 公里內的所有醫院標示出來，並連線至本服務之伺服器，使用 RQ 演算法取得周圍醫療院所之急診壅塞指標，其結果如圖 2 所示。



圖 1 所有醫院與 RQ 檢索範圍示意圖

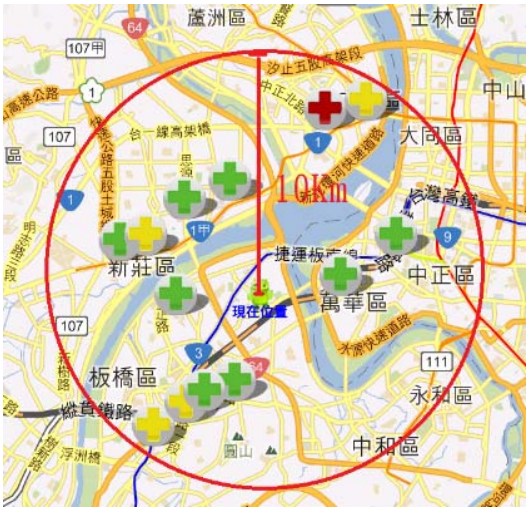


圖 2 RQ 演算法篩選結果示意圖

為了提升資料傳輸與篩選的效率，本論文自訂一套兩階段 RQ 演算法。首先，第一階段先透過 GPS 定位出使用者所在地，再利用 Google Map API 經緯度與地址之間的轉換，接著分析轉出來的地址取出地區關鍵字，例如：台北市、新北市...等，以完成第一階段之區域性篩選；第二階段以使用者目前位置為中心，將方圓半徑 X 公里內的所有醫院標示於地圖之上，並連線至本服務之伺服器取得周圍醫療院所之急診壅塞指標。

Step 3：依照救護責任範圍制定區域查詢(RQ)範圍

依照救護車調派分級，第一級屬緊急情況、有生命危險，救護車應於 9 分鐘內抵達；第二級屬嚴重但無生命危險，救護車應於 12 分鐘內抵達，因此，本 APP 設計的第二階段之區域查詢(RQ)範圍是參考一般平面道路的速限是 60 公里/小時，參考表 2，若要在 12 分鐘內到達，12 分鐘內救護車能移動的直線距離為 12 公里；若考慮救護車執勤平均時速大約為 80 公里/小時，則在 12 分鐘內可以移動的直線距離為 16 公里；若是碰上第一級傷患須在 9 分鐘內抵達，以一般速限 60 公里/小時換算，9 分鐘內救護車能移動的直線距離 9 公里；另一方面，若考慮 80 公里/小時，則 9 分鐘內救護車能移動的直線距離 12 公里。綜合以上，救護車在各級平均移動移動距離為 12.1 公里。由於路況的變化屬於未知數，路況不好，則會耽誤抵達事發現場的時間；若路況好，則可能提早抵達事發現場。故本次 APP 將以 10 公里作為區域查詢(RQ)的半徑。

表 2 救護車調派各級時速換算

時速 / 級數	一般 (60 km/hr)	值勤 (80 km/hr)
第一級	60*(9/60) = 9	80*(9/60) = 12
第二級	60*(12/60)=12	80*(12/60)=16

Step 4：系統效能校正與比較分析

雖然本論文不會直接危及生命安全，但涉及到緊急病患運送，仍必須確認其定位系統與候選責任醫院之建議是否精確，故實作出來的緊急醫療即時查詢與應變服務系統仍須進行實地測試，比對傳統由緊急救護人員決定之醫院與系統建議之間的差異，如果能達到一致的結果，未來可依循本論文建置模式，技轉至衛生署或各區域緊急救護體系系統，以達成全方面之緊急病患運送服務。

4. 系統實作與成果展示

本次實作之 APP 包含下列功能：(1)定位功能：假設想要重新知道使用者身在何處，只須點擊設定好的按鈕，即可立即更新 GPS 定位服務，本 APP 會將使用者位置標註於地圖之上。(2)下載資料功能：

由於即時查詢所需急診壅塞資訊必須要向伺服器下載即時更新。(3)地址搜尋功能：普羅大眾對於經、緯度並不熟悉，故本 APP 將提供地址搜尋功能，可接受中、英或其它可辨識之多種語言。(4)點擊查看資訊功能：本 APP 特別針對效率設計的功能，讓使用者短時間內能獲得所需之急診壅塞資訊。(5)清單功能：以二階段區域查詢(RQ)篩選出目前所在位置方圓 X 公里內的所有醫療院所，並以清單方式呈列給使用者，使用者亦可點即清單內項目，並直接啟動導航功能。(6)導航功能：使用者可自行輸入起始位置和終點位置，預設起始位置為透過 GPS 所感測之現在位置。(7)地圖文字開關功能：為了保持畫面的簡潔，預設只標示圖片，不顯示醫院文字；使用者可依個人喜好，自行透過文字開關來顯示/關閉文字。圖 3 為本系統的架構圖，各醫療單位將轉成紅綠燈號誌的壅塞指數，利用 PHP 上傳至資料庫伺服器，資料庫伺服器負責接收醫療單位上傳的資料，也負責接收使用者發送的需求，並提供使用者下載急診壅塞資訊，APP 使用者藉由操作 APP 可獲得所需之急診壅塞資訊，並進一步的執行導航。



圖 3 系統架構圖

圖 4 為本系統的流程圖，使用者開啟 APP 與定位服務後，本 APP 首先會進行相關的地圖設定，之後於背景自動將現在定位的位置透過 URL 發送至伺服器要求第一階段的區域性篩選，APP 將篩選結果下載至記憶體內，再進行第二階段的資料篩選，然後顯示給使用者參考，使用者能夠依據所在地理位置進行急診壅塞狀態查詢，並且進一步的點選地圖上的任何醫院標誌，進行導航服務。



圖 4 系統流程圖

圖 5 為本次實作之 APP 主要畫面，為了讓使用者短時間內能獲得最詳細的資訊，使用者可直接點選畫面中的任一家醫院燈號，即可顯示指定醫院詳細資訊(如圖 6 所示)，則可選擇立即撥打電話(如圖 7 所示)或導航至目標醫院(如圖 8 所示)。



圖 5 急診壅塞狀態顯示畫面

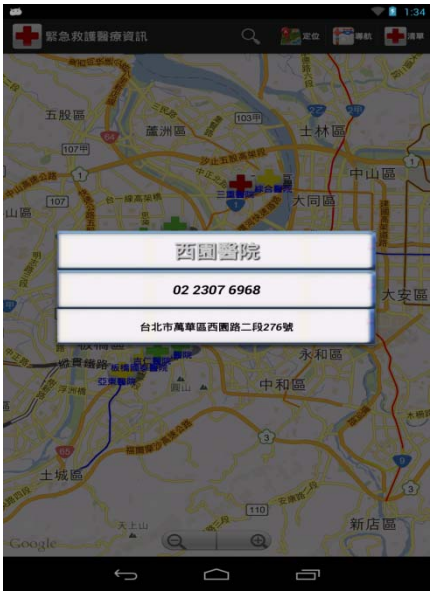


圖 6 醫院資訊顯示畫面

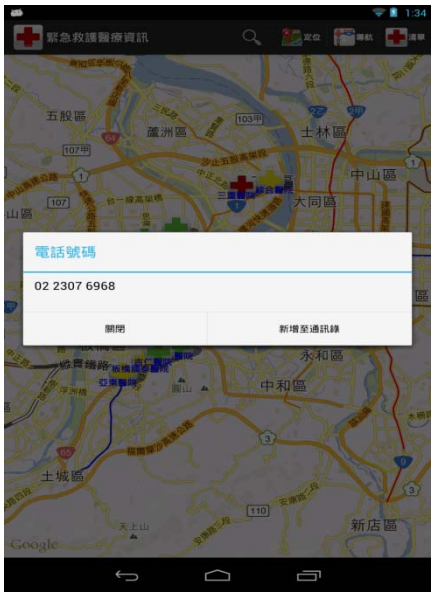


圖 7 撥打電話畫面

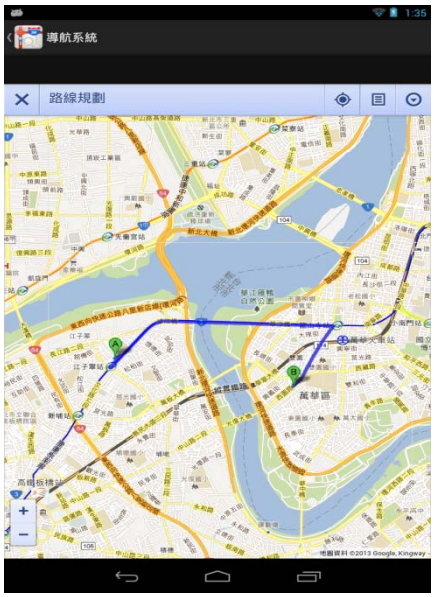


圖 8 路徑規劃畫面

5. 結論與未來展望

本論文實作一套急診即時查詢與導航服務之Android APP，合作之醫療單位會將最新的急診室壅塞情況透過網際網路回報，本系統會依照回報資訊計算壅塞指標，並決定出紅、黃、綠三色的壅塞燈號，讓使用者可即時獲得急診室最新的壅塞情況，並依自行狀況評估以及地理位置，透過本 APP 的醫院導航功能，協助使用者就醫選擇的參考依據，以期降低濫用緊急醫療資源的浪費。未來計畫開發緊急醫療人員所使用之 APP，將整合救護車上的醫療器材所量測到的傷患生理數據，例如：血壓、心跳指數、昏迷指數、負壓指數..等等，透過藍芽傳送到緊急醫療人員的終端設備，更進一步透過網際網路將這些生理數據即時傳送到資料庫端進行比對，更進一步篩選出最適合的醫院，同時，讓目標醫院可提前了解救護車內急救情況。

致謝

本論文由國家科學委員會個人型計畫計畫(計畫編號：NSC 102-2221-E-027-105-)補助。

參考文獻

[1] 曾國傑,"運用 kNN 文字探勘分析智慧型終端 App 群集之研究", 國立政治大學／資訊管理研究所／碩士論文, 2011.

[2] 何宗翰, "針對具不確定性的移動物體去處理連續 k 個最近鄰居天際線之查詢", 國立成功大學／資訊工程學所／碩士論文, 2011.

[3] 何凱云, "無線廣播環境下 k 個最近鄰居搜尋方法的探討", 國立台北科技大學／自動化科技研究所／碩士論文, 2007.

[4] 游雨蘋,"以策略行銷架構探討 LBS 技術之使用者意圖—以行動裝置為例", 國立彰化師範大學／企業管理學系國際企業經營管理／碩士論文, 2011.

[5] A. Dey, J. Hightower, E. de Lara, and N. Davies, "Location-Based Services", IEEE Pervasive Computing, Vol. 9, No. 1, pp. 11-12, Jan. 2010.

[6] S. Ilarri, A. lllarramendi, E. Mena, and A. Sheth, "Semantics in Location-Based Services", IEEE Internet Computing, Vol. 15, No. 6, pp. 10-14, Nov. 2011

[7] R. Barnes, J. Winterbottom, and M. Dawson, "Internet geolocation and location-based services", IEEE Communications Magazine, Vol. 49, No. 4, pp. 102-108, Apr. 2011.

[8] T. Zhu, Y. Zhang, F. Wang, and W. Lv, "A location-based push service architecture with clustering method", Proceedings of the 6th International Conference on Networked Computing and Advanced Information Management (NCM), pp. 107-112, Aug. 2010, Seoul, Korea.

[9] N. Fernando, D. Dias, and S. Wijesekara, "A framework to develop location based services applications using OGC map services", Proceedings of the 5th International Conference on Information and Automation for Sustainability (ICIAFs), pp. 521-526, Dec. 2010, Colombo, Sri Lanka

[10] W.-S. Lai and C.-C. Shih, "A mobile hot-spot navigator for instant POI finding in an unfamiliar area", Proceedings of the 17th International Conference on Geoinformatics, pp. 1-5, Aug. 2009, Fairfax, USA.

[11] K. Tabassum, M. Hijab, and A. Damodaram, "Location Dependent Query Processing – Issues, Challenges and Applications", Proceedings of the 2nd International Conference on Computer and Network Technology (ICCNT), pp. 239-243, Apr. 2010, Washington, DC, USA.

[12] Y. Park, D. Seo, J. Lim, J. Lee, M. Kim, W. Bao, C. T. Ryu, and J. Yoo, "A New Spatial Index Structure for Efficient Query Processing in Location Based Services", Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, pp. 434-441, Jun. 2010, California, USA.

[13] T. Zhu, C. Wang, W. Lv, and J. Huang, "Continuous range monitoring of moving objects in road networks", Proceedings of the 10th International Conference on Intelligent Systems Design and Applications (ISDA), pp. 1412-1417, Nov. 2010, Cairo, Egypt.

[14] J. Huang and C. Huang, "A Proxy-Based Approach to Continuous Location-Based Spatial Queries in Mobile Environments", IEEE Transactions on Knowledge and Data Engineering, doi: 10.1109/TKDE.2011.203, Sep. 2011.

行動視訊播放與管理系統

葉耀明　　鄭皓中
國立臺灣師範大學資訊工程所
ymyeh@csie.ntnu.edu.tw　rock3300178@hotmail.com

摘要

本研究主要以 HTML5、JSP、XML、eXist、NFC 等技術實現行動視訊播放與管理系統。利用 OpenCV 來分析影片內容，找出關鍵畫面並做為影片的分段點，自動為整部影片分割成多個片段，系統依照影片類別，要求使用者輸入和此類別相關的片段資料並以 XML 的格式儲存相關資訊，並以原生 XML 資料庫 eXist 儲存 XML 文件，並且利用 XQuery 查詢語言查詢資料庫中影片及片段內容，讓使用者能夠快速地找到想要瀏覽的影片內容，例如運動影片的精彩畫面或是英語教學影片中的特定授課內容、角色對話，增加使用者瀏覽影片的效率。我們使用 HTML5、CSS、JavaScript 設計出影片的瀏覽頁面，在不需要額外安裝任何的附加元件情況下就能夠正常的播放影片內容，能夠提供使用者無論是行動裝置或是個人電腦都有一個良好的瀏覽環境。另外本系統透過與 NFC 技術結合，感應不同的場所以及不同功能的 tag，產生出更多樣化的用途。

(關鍵詞: HTML5、XML、eXist、JSP、智慧型手機、NFC)

Abstract

This research uses the technologies including HTML5, JSP, XML, eXist, and NFC to implement a mobile video playback and management system. Our work uses OpenCV to analyze the video content and identify the key frame to index the cutting point of the video so that it can provide the automatic clipping function for the video to be viewed according to the indexed point. Our system can store the uploaded video according to the provided classification and use the XML format as the basic unit of the eXist Database System. XQuery can be used to provide the query function for the users to navigate the required video. We use HTML5, CSS, and Javascript to design the mobile webpages for the video, which can playback video without extra plugin module. In addition, our system also include the NFC tag for the purpose of video searching which can provide an new interface and experiences for users.

Keywords: HTML5, XML, eXist, JSP, smart phone, NFC

1. 簡介

近年來隨著資訊科技快速的發展，使得網路和電腦提供了人們各式各樣方便、快速的功能，使得現在大多數人們的日常生活已經和電腦、手機等 3C 產品息息相關，電腦在人們的各個領域，例如工作、學習、休閒...等已經成為不可或缺的工具，網路分享資訊很方便，大多數使用者的頻寬也很足夠，線上教學成為了各方面資訊學習非常熱門的方式，在網路上找的到許多的教學影片，例如語言學習、電腦相關學習、甚至是部份補習班也有線上觀看教學影片的服務。由於多媒體技術的蓬勃發展以及網路儲存空間日漸增加，因此線上分享影音資訊已經變得非常容易，網路上就有許多影音分享的平台提供人們進行瀏覽、分享，根據 Alexa 的排名，全球最大的影音分享平台 YouTube 已經成為全球第三大網站，僅次於 Google 和 Facebook[2]，代表瀏覽、分享影音資訊已經成為大多數人們使用網路的一部分了。

最近幾年智慧型手機也是發展非常快速的一項 3C 產品，到這兩年已經是幾乎人手一隻，功能也越來越強大，結合了傳統手機和個人電腦的功能，因此也能夠隨時隨地的連結網際網路從事各種活動，例如瀏覽網頁、玩遊戲、收發郵件...等等，當然也可以連結到影音分享平台進行瀏覽、分享。HTML5 是 HTML(HyperText Markup Language，超文件標示語言)的最新版本，其中有一項最重要的新增語法<video>，可以讓 HTML5 格式的網頁在不增加任何附加元件的情況下播放影片，這對於目前市面上有不只一種熱門作業系統的智慧型手機來說，HTML5 是非常適合用來做為影音分享平台的網頁撰寫格式。

由於目前影音分享技術的蓬勃發展，任何人在網路上瀏覽影片都變得非常方便，但是這只限於完整影片的搜尋，在影音分享平台或是線上教學的單位，到處可見數十分鐘長的影片，如果只想觀看影片的特定片段，或是從中間某個場景開始瀏覽，就要花上不少時間在尋找正確的時間點上，尤其是教學影片，時間通常都有蠻長的時間，但是學生可能一次不想看完全部，或者是只想觀看某個部份的教學時，會顯得比較不方便，如果可以分析整部影片，找出影片內的各個主題，為影片分段，並且擷取關鍵畫面作為縮圖，最後為片段建立詳細的描述，就可以輕鬆的為整部教學影片分割成多個適當的章節，學生只需要根據關鍵字搜尋，就可以快速的瀏覽教學影片的內容，減少尋找欲觀看內容的時間，大大的增加學生學習以及一般使用者觀看影片的效率。

2. 研究架構與方法

2.1 系統架構

如圖 1，本系統主要由兩個部分組成，第一個是由許多個 JSP 網頁所組合成的整個系統的入口，使用者可以在此進行使用者登入、影片上傳、影片查詢、片段查詢、影片清單以及影片管理的動作。使用者在上傳影片之後，系統會將上傳時輸入的相關資訊集合成一個 XML 檔案，此 XML 檔案的內容是利用 Dublin Core 的格式來對影片內容做描述。之後系統會自動將影片依照影片長度切割成數個片段，每個片段都會產生一個 XML 檔案，檔案中會有數個標籤來描述片段的內容，依照影片的分類，會有不同的標籤來描述不同種類的影片，所有的 XML 檔案都會儲存在 XML 原生資料庫:eXist [3]中，使用者可以利用系統中影片查詢和片段查詢的功能快速的找到想要觀看的影片或片段。查詢完畢後會將結果傳送至 HTML5 的頁面做影片的瀏覽，在瀏覽頁面中，使用者可以對片段資訊做新增、修改、刪除的動作，來增加影片的查詢效率和準確度。

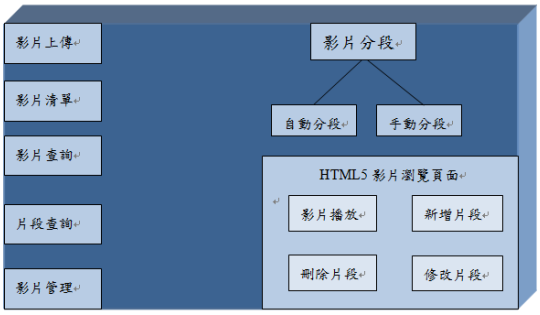


圖 1

■ **影片上傳相關功能**

本系統使用 jspSmartUpload API 完成影片上傳之工作。上傳過程中，使用者選擇欲上傳影片路徑、輸入影片相關資訊後，系統會將使用者輸入的影片相關資訊，製作成一份利用 Dublin Core[4]格式描述影片內容的 XML 檔案。所用到的 Dublin Core 資源描述元素有影片上傳者、影片的主題類別、影片的相關描述、影片的上傳日期、資源所屬的類別、影片的格式、影片的唯一識別、影片中使用的語言、影片的來源，表 1 為影片描述檔案範例、表 2 為每個 XML 元素所對應的 Dublin Core 資源描述元素。

影片描述檔案

```
<?xml version="1.0"?>
<rdf:RDF
xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
xmlns:dc="http://purl.org/dc/elements/1.1/">
<rdf:Description
rdf:about="http://www.w3school.com.cn">
<dc:title>basketball</dc:title>
<dc:identifier>b77e5d14-cabb-4641-8ec4-5bda85e72d19
</dc:identifier>
<dc:creator>me</dc:creator>
<dc:language>en</dc:language>
<dc:date>2013/06/13</dc:date>
<dc:source>NBA</dc:source>
<dc:rights>NBA</dc:rights>
<dc:format>mp4</dc:format>
<dc:type>video</dc:type>
<dc:subject>高畫質專區.體育.籃球</dc:subject>
<dc:description>basketball</dc:description>
</rdf:Description>
</rdf:RDF>
```

表 1

元素名稱	定義
Title	影片名稱
Creator	影片上傳者
Subject	影片的主題類別
Description	影片的相關描述
Date	影片的上傳日期
Type	資源所屬的類別
Format	影片的格式
Identifier	影片的唯一識別(UUID)
Language	影片中使用的語言
Source	影片的來源
Rights	影片的版權

表 2

■ **影片管理相關功能**

因為隨著時間的增加本系統中的影片資源會越來越多，因此利用網路本體語言(OWL)技術為系統資料庫做管理的工作，將每部影片依類別分類，對於影片資源的管理來說更加的方便和整齊。由於每份 XML 影片描述檔，都是獨立無相關性的，本系統為了提供完整且方便的查詢功能，利用 OWL

技術，並將所有影片依照所屬的類別，分類管理，如圖 2 所示。

本系統使用 Protégé API[5] 來建立 RDF/OWL 格式的 XML 檔案。Protégé 為一個免費、公開程式碼的本體語言編輯工具，其提供了一套完整的 OWL API，供開發人員使用。

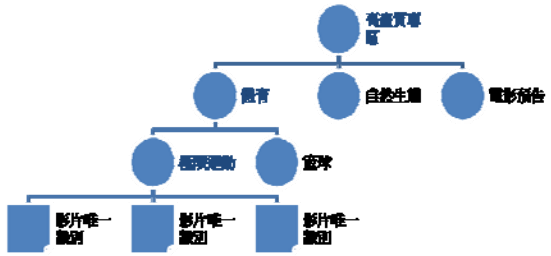


圖 2

■ **影片查詢相關功能**

查詢功能為影片資料庫中相當重要的功能，系統依使用者輸入的查詢關鍵字，在資料庫中找出符合的影片資源。本系統中主要提供使用者三種查詢:(1)依影片類別(2)依影片名稱(3)依影片相關描述。

● Query RDF/OWL format file

如圖 4，當使用者選取影片類別後，系統會利用 Protégé OWL API，依照影片類別尋找所有符合的影片。系統將 RDF/OWL 文件載入後，搜尋檔案之樹狀結構。由較大的分類往下搜尋至樹狀結構的最底層，將影片 ID 送至 HTML5 影片瀏覽頁面呈現。

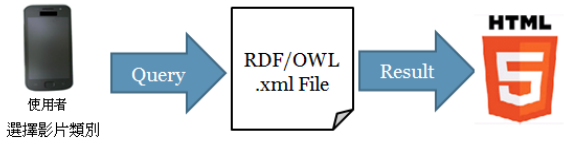


圖 2

● Query eXist Database

如圖 5，當使用者依影片名稱或影片相關描述來做查詢動作時，系統會利用 XQuery[6]查詢語言，在儲存影片相關資訊的 XML 檔案的 eXist 資料庫中尋找該影片，並將查詢結果傳送至 HTML5 影片瀏覽頁面進行瀏覽。

eXist 資料庫支援 XQuery 查詢語言，XQuery 是由 W3C 的 XML Query 工作小組所開發和定義的語言，為專門查詢 XML 檔案的查詢語言。XQuery 語言是一種路徑運算式(Path Expressions)、FLWOR 運算式(類似 SQL 語法)、條件運算式和 XQuery 函數所集合而成的。本研究統合 eXist 提供的 API 與 XQuery 查詢語言，輸入影片關鍵字，即會回傳所有查詢結果，大幅提高資料庫的搜尋效率。

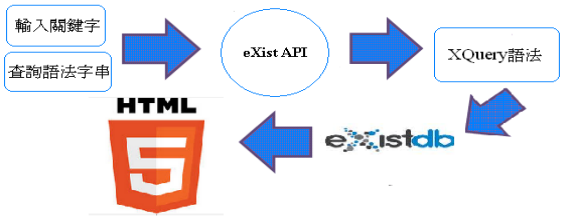


圖 3

■ **影片分段相關功能**

當使用者上傳影片之後，系統會利用自動分段的功能將影片依照長度切割成數個片段，長度越長，就會切割越多片段，切割完畢之後，使用者需要前往瀏覽系統中利用片段修改的功能，將切割出來的片段依照影片種類的不同編輯一些相關的資訊，讓其他使用者能夠更快速的找到這些片段，假如自動分段的結果使用者並不滿意，也可以在瀏覽系統中手動進行片段的新增或刪除。自動分段的功能是利用 OpenCV[7](Open Source Computer Vision)函式庫對影片進行處理，判斷出場景轉換的時間點，對影片進行切割的動作。

OpenCV 是一個由 Intel 公司所開發出來的 C/C++語言的 Open Source 圖形演算法的函式庫。包含了 300 多個 C 語言函數的跨平台的中高層 API，可以製做圖片、視訊、矩陣運算、統計、圖論...等等的 C/C++語言程式設計，不依賴其他外部的函式庫，其中大部份的函數用來解決以下領域中的問題，例如人臉辨識、動作分析、物體追蹤、傅立葉轉換和圖像分割等，主要應用在靜態圖片(BMP、JPG、TIF、PNG)和動態 Webcam 的影像處理。

● 影片自動分段

影片上傳之後，系統會自動找出影片中場景轉換的地方，並且設為一個分段點，產生一個片段。優點在於不需要自己花時間為影片分段，系統會自動完成。缺點就是準確度可能會比不上使用者手動的分段，所以使用者有可能要做一些細微的修改，並且片段產生後，XML 檔案中的相關資訊還是需要使用者自己來完成，自動分段流程如下所示：

1. 將影片切割成許多畫面
2. 擷取相鄰畫面
3. 將畫面灰階化
4. 比對相同位置像素
5. 統計差異度大的像素個數
6. 依照影片長度選出數個分段點，切割成片段

● 影片手動分段

使用者在 HTML5 影片瀏覽頁面中可以為影片新增片段，只要輸入片段的起始和結束時間，以及依照影片類別的不同，輸入片段相關的描述和資訊，系統就會產生片段和存有相關描述和資訊的 XML 檔案。優點在於可以很清楚的找到影片中各個主題或者是最精彩的部分，缺點在於使用者必須完整的瀏覽過影片一次，才能切割出所有的片段，

如果影片時間比較長，所花費的時間或精力就會比較大。

2.2 HTML5 影片瀏覽系統

在一個影音分享平台中，最重要的就是在於提供使用者一個良好的影片瀏覽環境。本系統使用 HTML5 網頁技術來設計整個影片瀏覽系統，近年來智慧型手機和平板電腦這些行動裝置的普及率越來越高，功能也越來越強，扣除掉一些較吃硬體效能的功能(例如玩畫面較精緻的遊戲)，這些行動裝置已經可以做到大部分一般人使用電腦時所做的事情。因為目前主流行動裝置上預設的瀏覽器都能夠支援 HTML5，並且 iOS 和 Android 這兩大行動裝置作業系統也宣布未來不會再支援 Flash，因此本研究選擇使用 HTML5 配合 JavaScript 以及 CSS 來設計整個影片瀏覽系統。

如圖 6 所示，影片瀏覽頁面主要分成數個功能及區塊：影片瀏覽視窗、搜尋結果區塊、影片資訊區塊以及新增至清單、新增片段和片段播放三個功能。系統使用流程如下：

1. 在 JSP 頁面搜尋到的結果傳到影片瀏覽頁面後，使用者可以在搜尋結果區塊點擊想要觀賞的影片截圖，點選之後，上方的影片瀏覽視窗就會將影片載入，使用者就可以點擊播放鍵播放影片，另外下方的影片資訊區塊也會顯示出該影片的相關資訊。
2. 使用者如果想要將影片記錄下來供日後瀏覽，點擊新增至清單的按鈕，系統就會將影片加入到目前所登入的帳號下的影片清單，之後只要在 JSP 頁面使用影片清單的功能，就會看到所記錄的全部影片。
3. 使用者可以在此頁面進行片段的新增，只要點擊新增片段的按鈕，頁面會跳出多個輸入欄位，依照影片類別的不同，每個輸入欄位要輸入的資訊也會不同，使用者輸入完畢之後，系統會將所輸入的片段資訊存成 XML 檔案，並存入 eXist 資料庫中。
4. 如果想要瀏覽或修改目前播放影片的所有片段，可以透過點擊片段播放的按鈕，頁面便會跳至片段播放頁面，如圖 7 所示，即可進行片段的瀏覽或修改。



圖 6

片段瀏覽頁面格式和影片瀏覽頁面非常相似，主要分成數個功能及區塊：片段瀏覽視窗、搜尋結果區塊、片段資訊區塊以及播放片段、修改片段、刪除片段和回主畫面四個功能。系統使用流程如下：

1. 在 JSP 頁面進行關鍵字的搜尋或在影片瀏覽頁面使用片段播放功能，頁面都會跳至片段瀏覽頁面，使用者可以在搜尋結果區塊點擊想要觀賞的片段截圖，點選之後，上方的片段瀏覽視窗就會將影片載入，使用者只要點擊播放片段按鈕就可以進行片段的瀏覽，另外下方的影片資訊區塊也會顯示出該片段的相關資訊。
2. 使用者如果認為片段的相關資訊和片段內容有出入需要修改，只要點擊修改片段的按鈕，頁面會跳出和新增片段時相同的數個輸入欄位，使用者只需要輸入正確的片段資訊並點擊送出按鈕，系統便會將修改過的片段相關資訊，傳至 JSP 修改頁面，然後在 eXist 資料庫中找到此片段相關資訊之 XML 檔案，並且進行修改。
3. 使用者可以在此頁面進行片段的刪除，只要點擊刪除片段的按鈕，頁面會將片段名稱傳至 JSP 刪除頁面，然後在 eXist 資料庫中找到此片段相關資訊之 XML 檔案，並且進行刪除，如此就可以將使用者認為比較多餘或者不重要的片段刪除。
4. 下方有一個回主畫面的按鈕，使用者點擊之後頁面便會跳至目前播放片段的影片瀏覽頁面，進行完整影片的瀏覽。



圖 7

3. 系統實作

本研究結合 XML、RDF/OWL、eXist、HTML5、NFC 等多項技術實做行動視訊播放與管理系統，並利用。本章針對系統內部規劃做詳細說明，首先以「新舊系統比較圖」[1]，如圖 8，呈現本研究新增加的功能以及相關說明。

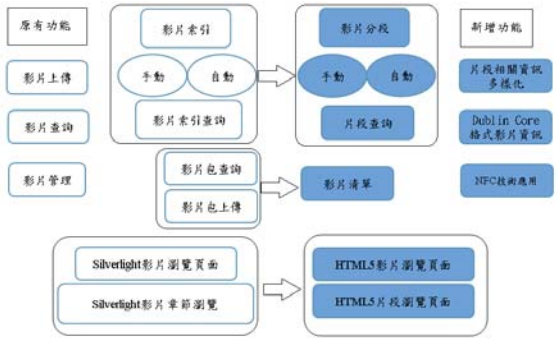


圖 8

■ 片段資訊多樣化

使用者在對影片新增片段時，無論是手動或是自動新增片段，系統都會要求使用者輸入片段的相關資訊，此時依照原影片的類別，會有不同種類的相關資訊來讓使用者輸入，藉此來讓這些片段的相關資訊能夠更清楚的對片段進行描述。

■ Dublin Core 格式影片資訊

每部上傳至影片資料庫的影片都會有一個 XML 檔案來儲存影片相關資訊，影片資源的描述格式是利用 Dublin Core 資源描述格式來對影片進行描述，Dublin Core 總共有 15 種元素可以對資源進行描述，在本研究中會用到其中 11 種，如表 2 所示，透過這 11 種元素就可以對使用者所上傳的影片進行非常詳細的描述。

■ NFC 技術應用

本系統利用與 NFC 的結合，展現出更多樣化的用途，例如在不同地方感應該處的 tag，例如體育館、運動場的 tag，會呈現所有和運動相關的影片，或者是在英語教學的教室、場所的 tag，則是會呈現所有英語教學的影片，可以讓使用者瀏覽和所在位置相關的影片。另外透過感應不同的 tag，可以針對不同的 Dublin Core 元素進行影片查詢，讓使用者可以有更多的搜尋方式可以使用。最後則是在像博物館、展覽館之類的場所，感應在各個展覽物品、區域的 tag，就能夠播放該物品、區域的介紹、導覽影片，對於使用者在參觀上有一定的幫助。

4. 系統使用分析

圖 9 為本系統的使用案例圖，系統總共有 7 大功能，分別為:影片上傳、新增片段、影片查詢、片段查詢、影片清單、影片瀏覽、影片管理。其中使用者可以使用的功能為前六項，而系統管理者除了前六項外，還可以使用影片管理的功能，各功能的說明如下:

1. 影片瀏覽:使用者可在此功能下觀看查詢結果的所有影片內容。
2. 影片上傳:使用者可以將想要分享的影片上傳至影片資料庫中，提供其他使用者或自己觀賞，也可以對自己所上傳的影片作新增片段等等的處理。
3. 新增片段:使用者可以在瀏覽頁面中手動新增影片片段，依照影片類別的不同，輸入不同的片段資訊，接著將這些資訊利用 JDOM 的 API 建立一個 XML 檔案，並上傳至資料庫。
4. 影片查詢:使用者可選擇依照影片類別、影片名稱、影片描述進行查詢，透過 XQuery 語法查詢資料庫中的 XML 檔案，將符合條件的影片結果列於 HTML5 瀏覽頁面中。
5. 片段查詢:使用者輸入關鍵字在資料庫中依照片段描述搜尋所有影片片段，接著將所有結果列於 HTML5 瀏覽頁面中。
6. 影片清單:使用者可藉由此功能建立自己帳號中的影片清單，可以將想要收藏的影片加入清單中，之後便可以在系統首頁中點選影片清單的功能，在 HTML5 瀏覽頁面中便會列出所有此帳號收藏的影片，讓使用者點選播放。
7. 影片管理:管理者才可使用的系統功能，可針對影片類別做新增或是刪除的動作。

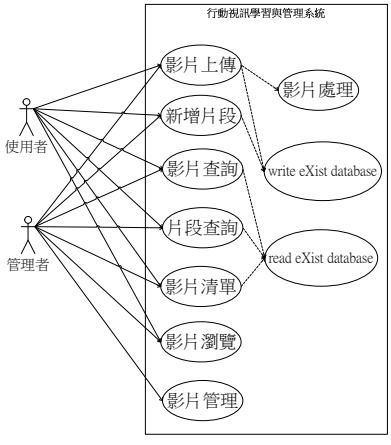


圖 9

5. 結論與未來發展

5.1 結論

在現今的網路環境中有著非常豐富的資源，人們在網路上可以找到幾乎是你想找到的任何東西，近年來由於影音分享平台的蓬勃發展，在網路上能夠找到的影片資源也是越來越多。本系統提供一個良好的影音分享平台，透過功能豐富的使用者介面，使用者可以上傳影片與他人分享，而使用者也可透過搜尋的功能來瀏覽資料庫中的影片資源。但是由於影片長度較長以及影片資源過於豐富等等原因，使用者可能會不容易找到想要瀏覽的影片內容，因此本系統提供了自動分段和手動分段的功能，將影片切割，並且依照影片類別輸入不同的片段相關描述，提供使用者進行搜尋，讓使用者能夠更輕鬆的找到想要瀏覽的內容，例如影片中的精彩畫面和重點場景或是教學影片中的特定主題。並且搭配影片字幕、影片清單的功能，影片字幕可以為影片增加文字，例如英語影片的翻譯、運動相關影片的解說、教學影片的輔助等等，影片清單的功能則是可以將想要收藏的影片集合起來，類似書籤的功能，以便於日後想要重新瀏覽該影片。綜合以上各項功能，利用本系統可以提升影片的瀏覽效率以及學生瀏覽教學影片時的學習效率。並且結合 NFC 的功能，可以在特定的場所中讀取 NFC tag，獲得相關的影片資源，為本系統展現出更多樣化的用途。

5.2 未來發展

■ 增加與 NFC 技術結合之應用

目前本系統中與 NFC 技術結合的功能大部分是屬於搜尋方面的功能，但是還有許多 NFC 技術的特色沒有利用在本系統中，未來可新增更多除了搜尋相關功能的應用，能夠為本系統在使用上能夠更多用途、多樣化。

■ 直播頻道

HLS（HTTP Live Streaming）是一個由 Apple 公司提出的基於 HTTP 的直播技術，HTML5 的多媒體相關元素能夠利用此技術進行影片直播的功能，目前大部分是應用在 Apple 公司的相關產品及系統中，未來預計會成為 HTML5 多媒體相關應用中線上直播的主要技術。

6. 參考文獻

[1].栢慶瑞 語言學習之影音索引技術研究. 國立臺灣師範大學資訊工程研究所碩士論文.(2011)
[2].Alexa Top 500 Global Sites
http://www.alexa.com/topsites
[3].eXist-db Open Source Native XML Database.
http://exist.sourceforge.net/
[4].DCMI Home: Dublin Core® Metadata Initiative (DCMI)
http://dublincore.org/
[5].The Protégé Ontology Editor and Knowledge Acquisition System
http://protege.stanford.edu/
[6]. W3C Recommendation (2007, Jan). XQuery 1.0: An XML Query Language. Retrieved from
http://www.w3.org/TR/xquery/
[7]. OpenCV | OpenCV http://opencv.org/

從現行著作權法制談封鎖外國網站政策的可能性

陳秉訓
國立臺北科技大學智慧財產權研究所
cstr@ntut.edu.tw

摘要

2013 年 5 月 21 日智慧財產局宣布推動封鎖境外重大侵權網站之政策。在輿論反彈後，6 月 3 日又宣布停止推動封網政策。但其宣告事實上仍有繼續推動封網政策之意涵。本文透過著作權法的分析而認為智慧局可按照現行法執行封網政策。為降低此可能性，本文建議應修改著作權法第 90 條之 4 第 3 項的「通用辨識或保護技術措施」，並加入二個基本要件：(1) 指監控內容物的合法性之技術措施；(2) 指監控內容物之設備、器材、零件、技術或其他科技方法。

關鍵詞：著作權，ISP 業者，封網，智慧財產局。

Abstract

On May 21, 2013, the Intellectual Property Office (“IPO”) announced that it will launch a website-blocking policy against outside-border websites that severely infringe copyright. After a huge protest from the public, the IPO announced on June 3 that it will stop the policy. But, the announcement in fact implied the IPO’s intent to continue the website-blocking policy. This paper is intended to show that under the current Copyright Act, the IPO can execute the website-blocking policy. To reduce the possibility of executing the policy, this paper urges an amendment of Article 90-4, Paragraph 3. The definition of “general technical measure of identification or protection” should be added with two elements: (1) technical measure monitoring the legitimacy of a content material; (2) equipments, tools, parts, technology, or other technical measure, for monitoring a content material.

Keywords: Copyright, ISP, website-blocking, Intellectual Property Office.

1. 前言

2013 年 5 月 21 日經濟部智慧財產局（以下稱「智慧局」）以新聞稿（以下稱「521 新聞稿」）提出四點主張：(1)「境外重大侵權網站戕害文化產業，建置快速處置措施有其必要」；(2)「智慧局再推打擊網路侵權新措施，封鎖境外重大侵權網站」；(3)「封鎖境外重大侵權網站，國際間已有相關立法」；(4)「兼顧各方權益，智慧局審慎規劃評估」[1]。

此政策引發過大反彈[2]，進而導致智慧局於 6 月 3 日再以新聞稿宣布停止推動封網政策[3]。不過，智慧局的態度並非完全停止。其一方面說「**有關智慧局研議封鎖重大境外侵害著作權網站，由權利人提出申請，並由著作權專責機構認定後主動送請法院審核之規定，因各界反映恐有擴張行政權致侵害言論自由及資訊接觸自由之虞，智慧局為避免各界疑慮，對於原先規劃由行政機關先行認定之方向，將不再推動**」[4]。另方面又說「**至於如何有效保護智慧財產權人之權利，將與司法機關深入探討研議**」[4]。亦即，智慧局仍要執行封網政策，但不同的是其所採管制方式由行政行為轉變為司法行為。

智慧局封網政策的關鍵決策時點是今年 3 月 18 日時其召集「權利人團體、ISP 業者及學者專家」以舉辦「『打擊境外重大侵權網站』意見交流會」[5]。根據智慧局的記錄，「**權利人團體均強調訴求快速、便捷之程序執行封鎖，以避免損害擴大，對象則僅限封鎖『重大』境外侵權網站，一般網站縱有少數侵權資料並非封鎖之對象；至於封鎖技術方面，權利人團體同意採取執行成本較低之 DNS 封鎖或 IP 位址封鎖，ISP 業者亦表示在採 DNS 封鎖或 IP 位址封鎖技術之情形下，技術上配合執行可能性較大**」[5]。此顯示智慧局已找到封網的技術，並且該技術是網路服務提供者（Internet service provider，ISP）—即 ISP 業者—可配合執行的手段。

如果智慧局已有可執行的封網手段，並且以封網來達成所謂保護文化產業的目的仍是其不完全放棄的政策，那麼在現有的智慧財產權法制下，智慧局是否能達成其目的？這是本文想回答的問題。

本文認為按照現行的著作權法制，智慧局的確可以要求 ISP 業者封鎖設在外國的網站。以下，本文首先分析 ISP 業者為何因為著作權法而必須接受智慧局封網的命令。其次，本文討論智慧局會依據何種法規或理由來要求 ISP 業者封鎖特定的外國網站。最後，筆者提出著作權法的修法建議，以期望能革除智慧局封網政策的可能性。

2. 著作權法與 ISP 業者的侵權責任

2.1 ISP 業者的定義

根據著作權法第 3 條，ISP 業者有四類：

(1)「連線服務提供者」，指「透過所控制或營運之系統或網路，以有線或無線方式，

提供資訊傳輸、發送、接收，或於前開過程中之中介及短暫儲存之服務者」。

（2）「快速存取服務提供者」，指「應使用者之要求傳輸資訊後，透過所控制或營運之系統或網路，將該資訊為中介及暫時儲存，以供其後要求傳輸該資訊之使用者加速進入該資訊之服務者」。

（3）「資訊儲存服務提供者」，指「透過所控制或營運之系統或網路，應使用者之要求提供資訊儲存之服務者」。

（4）「搜尋服務提供者」，指「提供使用者有關網路資訊之索引、參考或連結之搜尋或連結之服務者」。

因為網路使用者主要透過「連線服務提供者」（例如，HiNet）和「搜尋服務提供者」（例如，Google）來連接外國網站，智慧局的封網命令對象應會以這二類 ISP 業者為主，才有阻止網路使用者接觸外國網站之效果。

2.2 ISP 業者的侵權風險

在智慧局封網政策中，其對象為「**『重大』境外侵權網站，一般網站縱有少數侵權資料並非封鎖之對象**」[5]，亦即，「**提供少量或部分未經授權著作的網站，不會在封鎖之列**」[6]。所謂「『重大』境外侵權網站」是其「**網站內容幾乎全為惡意侵權，且多屬視頻網站或其商業模式鼓勵網友侵權之網路空間**」[7]。

使用者如果由外國網站下載或接收侵權內容物，則可視為著作權法下的侵權人。ISP 業者在外國網站和使用者之間所處的角色如同幫助侵權行為人完成侵權行為。ISP 業者基本上會被視為「共同侵權人」而與使用者負擔相同的責任。為讓網路世界的運作與著作權的維護間取得合理的平衡，著作權法有所謂 IPS 業者的民事免責事由，以降低 ISP 業者無意或過失的著作權侵害風險[9]。

2.3 ISP 業者的民事免責事由

ISP 業者的民事免責事由是指 ISP 業者如果執行特定措施則可免除民事侵權責任。ISP 業者必須有所謂的「通知/取下」機制[8]。根據著作權法第 90 條之 4 第 1 項，ISP 業者必須採取四個措施：

（1）「以契約、電子傳輸、自動偵測系統或其他方式，告知使用者其著作權或製版權保護措施，並確實履行該保護措施」。

（2）「以契約、電子傳輸、自動偵測系統或其他方式，告知使用者若有三次涉有侵權情事，應終止全部或部分服務」。

（3）「公告接收通知文件之聯繫窗口資訊」。

（4）「執行第三項之通用辨識或保護技術措施」。

針對「連線服務提供者」，除了這四個措施，第 90 條之 4 第 2 項要求其「於接獲著作權人或製版權人就其使用者所為涉有侵權行為之通知後，將該通知以電子郵件轉送該使用者」。如此，則「連線服務提供者」才履行第（1）項措施。亦即，「連線服務提供者」必須代轉權利人的警告給有侵權疑慮的使用者。

在履行第 90 條之 4 第 1 項的四個措施後，著作權法分別於第 90 條之 5 和第 90 條之 8 規定某種條件，以免除「連線服務提供者」和「搜尋服務提供者」與使用者分攤侵權責任。

根據第 90 條之 5，「連線服務提供者」之免責條件為：（1）「所傳輸資訊，係由使用者所發動或請求」；（2）「資訊傳輸、發送、連結或儲存，係經由自動化技術予以執行，且連線服務提供者未就傳輸之資訊為任何篩選或修改」。

根據第 90 條之 8，「搜尋服務提供者」之免責條件為：（1）「對所搜尋或連結之資訊涉有侵權不知情」；（2）「未直接自使用者之侵權行為獲有財產上利益」；（3）經著作權人或製版權人通知其使用者涉有侵權行為後，立即移除或使他人無法進入該涉有侵權之內容或相關資訊」。

或許技術上而言，「連線服務提供者」和「搜尋服務提供者」可達成著作權法第 90 條之 5 和第 90 條之 8 所規定之免責條件。但對於第 90 條之 4 第 1 項所指「通用辨識或保護技術措施」，不是 ISP 業者可自由選擇，而是要由智慧局所核可。透過此，智慧局就可要求 ISP 業者封鎖外國網站。

3. 智慧局可能採取的手段

3.1 使用者從外國網站下載或接收未授權內容物之行為

「使用者從外國網站下載或接收未授權內容物之行為」涉及未授權內容物的傳輸和重製。因為傳輸至國內而且最終的重製（從網站下載內容物到使用者的儲存器）發生在國內，這類使用行為是可能構成著作權侵害。

對權利人而言，其行使權利會遇到的困境是無法知道使用者透過網路的使用而下載了什麼侵權內容物。不過，著作權法第 84 條給予權利人對有侵權之虞的狀況主張防止該狀況發生之權利。因此，只要權利人證明可透過 ISP 業者連結到外國網站並下載未授權之內容物，則其可能證明若 ISP 業者不限制該外國網站的連結，則非法下載的侵權行為將有可能發生。因此，ISP 業者將受到權利人的民事責任追究。

3.2 通用辨識或保護技術措施

因為使用者連結外國網站的網路行為仍會讓 ISP 業者負擔民事責任之風險，ISP 業者必然要配合智慧局執行封網政策，以求民事責任之免除。

雖然現行著作權法未直接賦予智慧局封網處

分的權利，但其可透過第 90 條之 4 的執行來達成封網政策。

根據第 90 條之 4 第 3 項，所謂「通用辨識或保護技術措施」之執行是指「著作權人或製版權人已提供為保護著作權或製版權之通用辨識或保護技術措施，經主管機關核可者」。智慧局曾解釋，「辨識或保護技術措施」是指「**用以辨識（identify）或保護（protect）著作權或製版權之相關措施，如過濾網路侵權資訊、監測網路流量之技術等，均屬之**」[10]。其中的「過濾網路侵權資訊」可能包括「外國侵權網路網址名單」。「資訊」可包含文字，即網址。「重大侵權網站」的「網址」是可被視為一種「網路侵權資訊」。

因此，智慧局可把「外國侵權網路網址名單」視為「通用辨識或保護技術措施」，並要求 ISP 業者執行封網政策，以符合民事免責事由之規範。

4. 著作權法修法的建議

如果要避免單純的「網址名單」被視為第 90 條之 4 第 3 項的「通用辨識或保護技術措施」，該條的修法是必要的，以限制智慧局的行政權力。什麼樣的「技術措施」才是適當的措施，其不只是「技術問題」，而仍應考慮技術背後所執行的手段是否有法律依據。

4.1 「網址」不等於侵權行為

在網路使用的情境下，如果只考慮使用者的下載問題，所涉及的著作財產權為重製權[11]。根據著作權法第 22 條第 1 項，「著作人除本法另有規定外，專有重製其著作之權利」。根據第 3 條，「重製」之定義為「以印刷、複印、錄音、錄影、攝影、筆錄或其他方法直接、間接、永久或暫時之重複製作」。

關於網址的封網技術，智慧局的原意為「IP 位址（Internet Protocol address）或 DNS（Domain Name System）封鎖」[1]。「IP 位址」是由號碼所組合數字序列，以做為網路位置的標定，例如「172.31.255.255」[12]。「DNS」即網域名稱，例如「www.ntut.edu.tw」，而「網頁地址」為網頁內容在 DNS 下的確切位置，例如「http://www.libertytimes.com.tw/index.htm」[13]。二者基本上都是文字或數字的組合。二者都和侵權內容物無關，亦即非為未經授權的重製物。因此，「網址」本身並非侵權行為，其不應做為「通用辨識或保護技術措施」的管制對象。

至於「網址」所儲存的內容物，該內容物變成侵權物的時點是該資訊傳輸並重製於國內時。在該內容物傳輸至國內時，其才屬於侵權物，也才成為「通用辨識或保護技術措施」所監視的對象。

因此，「通用辨識或保護技術措施」的要件之一應為「**指監控內容物的合法性之技術措施**」。「內容物」指影片檔或影音檔，或聲音檔。「監控」為動詞，檢視電子檔案的合法性。「監控內容物的合法性」整體來看即限制「技術」執行的對象是「內容物」而非「來源」。此使得智慧局不能將「外國侵權網路網址名單」視為一種「通用辨識或保護技術措施」，因為「網址名單」是「來源」而非「內容物」本身。

4.2 以「技術」為中心

除了監視標的之外，為了排除「文字或數字的組合」就可當成「技術措施」，「通用辨識或保護技術措施」的要件應更貼近「技術」特性。

本文認為可參照著作權法第 3 條對「防盜拷措施」之定義，其「指著作權人所採取有效禁止或限制他人擅自進入或利用著作之設備、器材、零件、技術或其他科技方法」。據此，「通用辨識或保護技術措施」的要件之一應為「**指監控內容物之設備、器材、零件、技術或其他科技方法**」。透過「科技方法」的強調，「技術措施」的意涵可排除「文字或數字」的單純內容。

5. 結論

2013 年 5 至 6 月智慧局從主張封鎖所謂國外重大侵權網站到遽然停止此政策。此風暴為台灣的資訊接觸自由蒙上陰影。雖智慧局宣布停止推動封網政策，但從其新聞稿文義中，本文認為智慧局仍有封鎖外國侵權網站的企圖。

本文試圖證明按照現行著作權法，智慧局的確有機會執行其封網政策。為了免於與使用者共同負擔著作權侵害之責，ISP 業者必須執行第 90 條之 4 第 1 項所定之四項措施，包括採用智慧局所核可的「通用辨識或保護技術措施」。「辨識或保護技術措施」是指「用以辨識（identify）或保護（protect）著作權或製版權之相關措施，如過濾網路侵權資訊、監測網路流量之技術等，均屬之」。本文認為「過濾網路侵權資訊」可包括「外國侵權網路網址名單」。因此，智慧局有可能「外國侵權網路網址名單」視為「通用辨識或保護技術措施」，而命令 ISP 業者執行封網政策。

對此疑慮，本文建議應修改著作權法限制智慧局的權力。第 90 條之 4 第 3 項的「通用辨識或保護技術措施」應給予二個基本要件：(1) 指監控內容物的合法性之技術措施；(2) 指監控內容物之設備、器材、零件、技術或其他科技方法。如此，排除「網紙名單」做為一種技術措施，並限定技術措施就是「科技方法」。

參考文獻

[1] 經濟部智慧財產局（智慧局），新聞稿（2013 年 5 月 21 日）「境外侵權網站無法管？智慧局研擬對策」，取自

http://www.tipo.gov.tw/ct.asp?xItem=425645&ctNode=7123&mp=1，到訪日：2013 年 8 月 18 日。

[2] 蒼弘慈（2013 年 6 月 4 日），「封鎖境外侵權網站 喊卡」，中時電子報，取自 http://news.chinatimes.com/focus/501013588/112013060400072.html，到訪日：2013 年 8 月 18 日。

[3] 林信男（2013 年 6 月 3 日），「政策轉彎！ 智慧局：不推動行政權封網」，ETtoday 東森新聞雲，取自 http://www.ettoday.net/news/20130603/217386.htm，到訪日：2013 年 8 月 18 日。

[4] 智慧局，新聞稿（2013 年 6 月 3 日）「智慧局參考各界反映，調整推動封鎖境外侵權網站之處理方向」，取自 http://www.tipo.gov.tw/ct.asp?xItem=454976&ctNode=7123&mp=1，到訪日：2013 年 8 月 18 日（以下稱「603 新聞稿」）。

[5] 智慧局，「貫徹保護智慧財產權行動計畫」102 年 1 至 3 月各機關列管追蹤表，頁 25-26，下載於 http://www.tipo.gov.tw/ct.asp?xItem=426263&ctNode=6880&mp=1。

[6] 智慧局，新聞稿（2013 年 5 月 24 日）「針對解決『封鎖境外重大侵權網站』問題，智慧局特此說明」，取自 http://www.tipo.gov.tw/ct.asp?xItem=426267&ctNode=7127&mp=1，到訪日：2013 年 8 月 18 日（以下稱「524 新聞稿」）。

[7] 陳沛佑（2013 年 5 月 28 日），「不理反彈 智財局：『節制』封鎖侵權網站」，新頭殼 newtalk，取自 http://newtalk.tw/news/2013/05/28/36854.html，到訪日：2013 年 8 月 18 日。

[8] 林利芝，影音網站著作權侵害與過濾機制衍生爭議之研究，東吳法律學報，第 23 卷第 4 期，2012 年 4 月，頁 89-124。

[9] 羅明通，著作權法論（II），台英商務法律，台北，7 版，2009 年 9 月，頁 480-494。

[10] 智慧局，「新修正著作權法第 90 條之 4 第 3 項之「通用辨識或保護技術措施」所指為何？網路服務提供者（ISP）應如何執行？」，http://www.tipo.gov.tw/ct.asp?xItem=207034&ctNode=7193&mp=1，到訪日：2013 年 8 月 18 日。

[11] 顏上詠，從 Kuro 與 ezPeer 司法爭訟個案來看網路音樂產業之管理法制分析，月旦法學雜誌，第 163 期，2008 年 12 月，頁 138-172。

[12] 財團法人網路資訊中心，「IP 位址」，取自 http://dns-learning.twnic.net.tw/internet/intro7.html，到訪日：2013 年 8 月 19 日。

[13] 台灣師範大學資訊中心，「網域名稱」，取自 http://www.itc.ntnu.edu.tw/service1630.php，到訪日：2013 年 8 月 19 日。

整合異質性資料來源成為行動網站的方法

周椽家[1] 翁瑞元[2] 王祥安[3] 黃翰隆[3]
[1]元智大學資訊管理學系 [2]元智大學資訊工程學系 [3]中央研究院數位文化中心
[1]s991646@mail.yzu.edu.tw, [2]s993330@mail.yzu.edu.tw,
[3]{sawang, hlhuang44}@iis.sinica.edu.tw

摘要

開發者在建置行動應用網站時，對於多種異質性資料的來源，可能沒有一個統一格式或來源，需依照各種資料來源逐一撰寫資料的抓取程式，可能會造成繁複的程式開發工作。因此，本研究提出結合 Solr 軟體及 Kurogo 軟體將異質性的資料整合並成為行動網站的方法。透過 Solr 軟體整合異質性的資料，並運用本研究開發的對應欄位設定軟體，橋接 Solr 軟體與 Kurogo 軟體的資料處理流程，且可以快速的產生將資料轉換成行動網頁的功能，Kurogo 軟體再透過此功能取得 Solr 軟體整合後的資料，將資料轉換成適合不同解析度的行動裝置呈現樣式。此方法可以降低對於不同行動裝置需要開發不同的行動網頁之複雜度，並快速的將整合異質性資料的網站轉換成行動網站。

關鍵詞：行動網站、異質性資料整合、行動中介軟體、響應式網頁

1 前言

隨著多樣化數位化設備及軟體的發展，會產生許多不同格式的資料，若要整合這些資料，要將不同格式的資料轉換成統一的格式，需要撰寫程式來轉換資料，所以資料整合是不易的工作。根據 Google 提出的多螢幕時代來臨，資訊會根據不同行動裝置螢幕的大小被呈現[1]。但是，將資料在不同的行動裝置上呈現適合的樣式是需要經過繁瑣的處理。因此，將不同資料來源整合，並提供一個統一的架構來提供資訊於各行動裝置，來解決上述的困難是本研究的目的。

使用適合的方式建置行動網站(Mobile Web)，並透過此網站將組織想傳遞給使用者的資訊呈現於行動裝置是目前的趨勢。根據 Mary Meeker 在 D11 會議中提到，直至 2012 年底，全球有超過 24 億的網路使用者，行動上網用戶更從 11 億增加至 15 億人相較 2011 年增加 30% [2]。由此可知，行動上網用戶的提升，促使透過行動裝置瀏覽網頁的人數攀升，因此透過行動網站傳遞資訊給使用者已是目前的趨勢。

針對於多螢幕時代，Ethan Marcotte 提出了響應式網頁設計(Response Web Design)的概念[3]，此設計方式，主要針對不同的行動裝置修改 CSS/Javascript 語法等，給予使用者介面優化的體驗，讓使用者可以降低點擊次數來取得所需資訊，而不需要在解析度較小的螢幕上，以放大或縮小的方式來瀏覽網頁內容。

為了解決前面所提到的問題，因此我們提出了一個方法，此方法整合兩套開放原始碼軟體(open source software)，解決異質性資料來源整合檢索並以較佳的方式呈現於不同的行動裝置，讓行動網站建置更為簡單，因此，本研究透過 Solr 軟體將異質性資料整合，再透過自行開發的對應欄位設定軟體連結 Kurogo 行動中介軟體與 Solr 軟體，有效的整合資料並降低程式開發者對於不同解析度的行動裝置建置複雜度，可降低建置行動網站的成本。

2 相關文獻探討

2.1 行動網站建置的方法

若要建置一個行動網站，以網頁語言開發一套跨平台行動裝置瀏覽的網站主要是以瀏覽器支援的語言來編寫的應用，可以採用以下幾種不同的方式來建置行動網站：(1)Web 軟體框架(Web application framwork)，(2)行動中介軟體(mobile middleware)，(3)網路服務轉成行動網站。

2.1.1 Web 軟體框架

Web 軟體框架是一種電腦軟體框架，主要用來支援動態網站及網路服務的開發[4]。可以同時相容於多種行動裝置平台，使得原本一定要用原生應用程式(native APP)開發框架才能做出的使用者體驗，多能利用 HTML5 和 CSS3 的技術來完成，為了提供服務給不同的行動裝置，強調使用 HTML5 來完成跨平台行動網站開發的框架(Frameworks)陸續出現，例如：jQuery Mobile、Sencha Touch、SproutCore[5]，其中 jQuery Mobile 是較普遍使用的架構。

jQuery Mobile 為以 jQuery 為基礎來開發針對相容各行動裝置所開發出來的一套架構，jQuery Mobile 很容易開發，但也有不足之處，最大的問題在於設計方式要符合 jQuery Mobile 所定好的 HTML 程式及 CSS 規範，各種瀏覽器在不同的手機

平台上表現也不相同，雖然目前 jQuery Mobile 提供很好的使用者介面，可透過自動針對螢幕大小與解析度做出縮放與重新編排，但若 jQuery Mobile 要實行響應式網頁設計也需要透過 CSS 針對不同大小的裝置平台去花費大量的時間做客製化樣式的呈現。若需要從資料庫抓取資料，開發者對於異質性資料的處理也只能靠程式去一步步抓取，這樣的製作方式對於行動應用網站的開發者無法有效地將資料整合於跨平台的應用服務網站。

2.1.2 行動中介軟體

中介軟體(middleware)是提供系統軟體和應用軟體之間連接的軟體如圖 1，以便於軟體各元件之間的溝通，特別是應用軟體對於系統軟體的個別應用，在現代資訊科技應用框架如 Web 服務、面向服務(service-oriented)的環境中應用比較廣泛。

行動中介軟體[6]，是介於企業組織後端的系統軟體與應用軟體，透過無線網路和 client 端的行動裝置相連結，透過組織內區域網路和伺服器的溝通，將所需資訊透過無線網路傳送到行動裝置呈現。

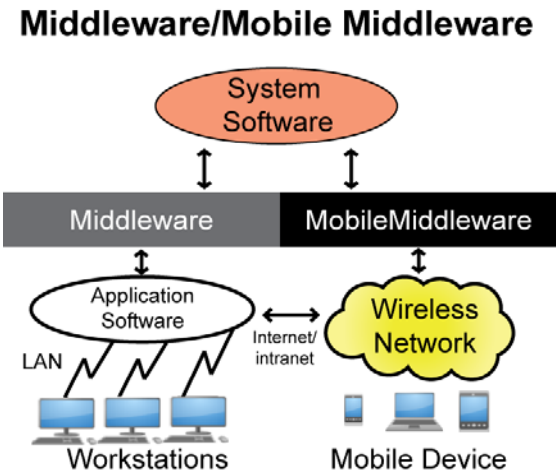


圖 1 中介軟體與行動中介軟體架構圖[7]

2.1.3 網路服務轉成行動網站

網路上提供許多服務，將呈現給個人電腦呈現的網站內容，透過各網路服務自行分析並產出適合行動裝至呈現的網站內容，例如：GinWiz、Mobify、ConvertWebsite。這些網站共同的優點是皆可以快速的針對於解析度較小的裝置優化，轉換成使用者方便閱讀的行動網站，不需要撰寫複雜程式的方式來轉換行動網頁。但其限制是只能讀取原始網站的內容頁面，其他格式的資料內容則無法讀取，而且，它們讀取原始網站時，可能會造成解析不完全正確。

2.2 Solr 全文檢索軟體

Solr 是一套開放原始碼軟體(open source software)的全文檢索軟體[8]，它可以從文件檔案或者資料庫中萃取出訊息。開發者可以透過編寫設定檔進行資料庫整合或處理格式不同的文件(例如：Word、XML）成為一份 Solr 索引檔。索引檔是為了提高檢索速度而發展出來的檔案結構，其中包含了多份文件，一份文件中有多個自行定義的欄位，一個欄位裡包含許多詞組(terms)，詞組由成對的字串所組成。Solr 具有表徵狀態轉移(REST)的軟體設計風格，可以接受多種請求方法，例如：使用 GET 方法取得資料，而資料回應的格式也可以讓開發者自行決定(如：XML、JSON、CSV)，只要透過 HTTP 協定的程式都可以跟 Solr 軟體進行溝通。

由於 Solr 整合異質性資料來源、提供全文檢索以及擁有 REST 的特性，解決了檔案格式不一致、難以取得檔案資料和程式不相容的問題，因此，本研究採用 Solr 來實作此研究方法。

2.3 Kurogo 行動中介軟體

隨著行動裝置的普及而誕生 Kurogo 軟體[9]，它是一個以 PHP 語言所編寫而成的行動中介軟體，可以將不同的資料格式，從後端資料層與前端瀏覽器連結，呈現最適合的樣式給不同解析度的行動裝置，成為一個適合大型組織開發行動網站的方法。

Kurogo 的架構，如圖 2 [9]。模組(Module)為邏

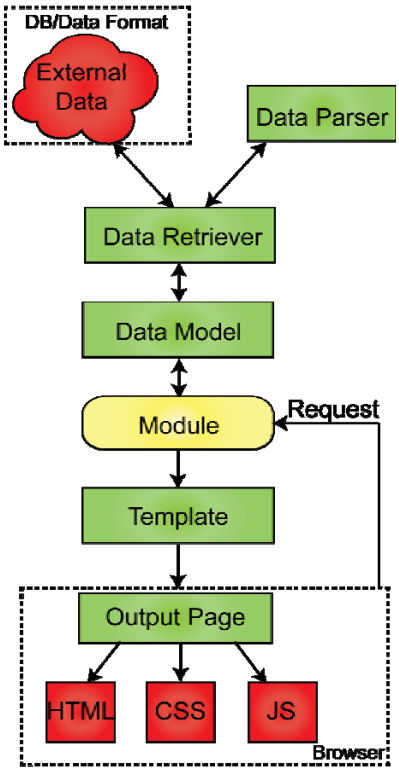


圖 2 Kurogo 架構圖

輯運算的核心，其主要功能為接受使用者的請求(UserRequest)、處理資料來源、將資料送至樣板(Template)。當客戶端的請求送到各模組中，模組會透過 Kurogo 資料設定檔來處理預先定義的資訊，例如：透過 Kurogo 資料設定檔的資訊到外部資料庫或不同資料檔案(DB/DataFormat)進行查詢，讓資料抓取程式(Data Retriever)及資料解析程式(Data Parser)解析後送回模組，經模組處理後，將結果傳至樣板引擎(Template)，Kurogo 採用 Smarty 樣板引擎，讓開發者可以將商業邏輯與呈現邏輯分開，降低程式設計師與樣板設計人員的耦合度，也可以在此樣板中嵌入 HTML、CSS 和有限制的 Javascript(JS)，讓網頁版面的調整控制性及擴充性更佳。

Kurogo 具有四種特色：(1)裝置偵測會根據裝置的硬體類型、作業系統、瀏覽器來決定呈現的網頁形式，網頁形式主要是運用 CSS、Javascript 來選定，平台使用特定的作業系統作為判斷基礎，瀏覽器使用何種瀏覽器來觀看此網站。(2)自訂資料來源，可以設定不同的資料來源、自行建置模組，甚至可以在輸出端依照需求，修改樣板的呈現方式。(3)管理者可透過介面來編輯該行動網站的設定及各模組的資訊設定，如：模組中各頁面的顯示名稱、權限控制等。(4)開發者下載 Kurogo 軟體後，其檔案內包含原生範例模組，其模組可以符合大多數組織行動網站所需要呈現給使用者的功能，只需透過模組的資料來源設定，即可以達到行動網站的建置。由於 Kurogo 上述四項優點，本研究採用 Kurogo 軟體來實作此研究方法。

3 系統架構

本系統採用的架構是 Client-Server 的軟體架構，在 Server 端，使用 Solr 軟體、Kurogo 軟體及我們所開發的對應欄位設定軟體(DataField Config Program)，其整體架構如圖 3。(1)Solr 軟體負責資料整合的處理，透過 Solr 設定檔，將異質性資料來源(Data Source)整合統一，它可以將資料庫、XML、CSV 等資料格式的來源，整合至 Solr 軟體。(2)對應欄位設定軟體，其主要功能為溝通 Solr 軟體及 Kurogo 軟體。因為 Kurogo 軟體需要去設定資料來源或向資料來源撰寫資料抓取程式，此過程需要透過會撰寫程式的使用者才能做到，因此，我們開發一個對應欄位設定軟體，它會去自動取得 Solr 資料的綱要(schema)，讓使用者設定呈現於行動網站的內容，Kurogo 再依使用者的設定將 Solr 的資料取回，轉換成行動網頁。(3)Kurogo 軟體主要功能為將 Solr 軟體的資料來源根據網站使用者的裝置環境來轉換成行動網頁，然後傳送到 client 端的瀏覽器(Web Browser)。Kurogo 抓取資料時，可以透過 REST 方式來向 Solr 抓取資料，並可以利用緩存(Cache)的機制來降低伺服器的負擔。

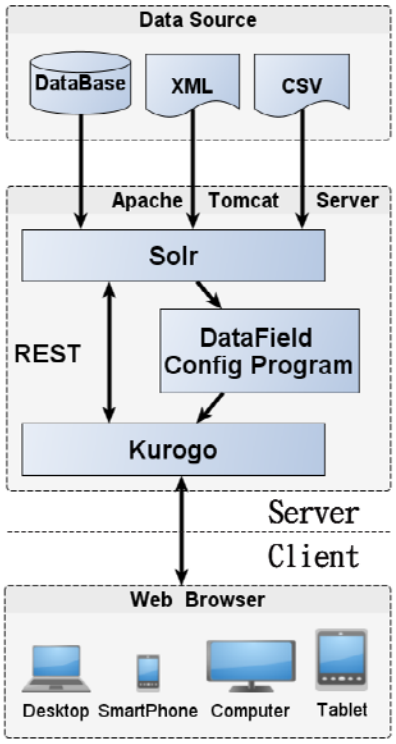


圖 3 軟體架構圖

4 實作過程與結果

本研究針對整合異質性資料成為行動網站提出一套實作的方法。以「中央研究院數位典藏資源網」為例[10]，如圖 4 所示，它是透過 Solr 軟體來整合異質性資料來源，整合的資料庫與網站超過 150 個，並透過 Kurogo 軟體來製作它的行動網站。整個實作的過程可以分為二個部分，第一部分編寫 Solr 綱要及設定檔，目的是將異質性資料來源匯入 Solr 軟體、第二部分使用對應欄位設定軟體來設定 Kurogo 軟體要向 Solr 軟體抓取的資料，以做為呈現行動網站的內容。

第一部分，為了將異質性資料來源整合成 Solr 索引檔，首先使用者需設定 XML 格式的 Solr 綱要、資料設定檔、系統設定檔，分別說明如下：

- Solr 綱要：主要定義在 Solr 中的欄位名稱(field name)、屬性以及類型。
- 資料設定檔(data config)：此檔案的作用是設定資料來源的位置，從各異質性資料來源的欄位(column)對應到 Solr 的欄位(name)中。
- 系統設定檔(config)：設定收到請求所要進行的處理，設置觸發監聽器(listener)的事件，以及 Solr 所需使用的函式庫。

Solr 軟體讀取上述三個設定檔後，可以從異質性資料來源萃取出使用者所需要的資料，建立 Solr 索引檔。



圖 4 中研院數位典藏資源網的專題文章頁面

第二部分，本研究所開發的對應欄位設定軟體可以簡單的透過設定來新增 Kurogo 模組及設定異質性的資料來源。由於 Kurogo 軟體可以自行新增模組，但使用者新增模組時，需在固定的檔案路徑下自行新增有限制的模組資料夾及檔案名稱，常會造成使用者的不便。使用者對於 Solr 軟體資料也需要自行撰寫程式去抓取所要的資料，因此，對應欄位設定軟體主要提供新增原生範例模組及 Solr 串接 Kurogo 的模組兩個重要的功能，分別說明如下：

第一個功能為快速的新增原生範例模組，它提供多數組織行動網站所需要呈現給使用者的功能，例如：(1)最新消息模組，採用 RSS 標準輸出格式的資料做為資料來源，主要提供組織網站之最新消息。(2)地圖模組，以 Google Map 匯出 KML 檔案格式的方式來標示位置，主要提供組織的所在位置，並且顯示在行動網頁上等，若使用者想要快速的開發一個網站，並使用相同的原生模組功能，需透過資料夾的複製，才能實現原生模組的功能。因為檔案名稱的不同進而要改寫模組內的程式，而無法透過簡易地操作來新增模組，因此，我們開發僅需透過設定即可快速新增原生範例模組的功能，使用者只須抽換原生範例模組的資料來源，就可輕易產生具有與原生範例模組功能或版面相同，但資料來源不同的模組。

第二個功能為設定異質性資料的來源，透過新增 Solr 串接 Kurogo 的模組設定 Kurogo 軟體要向 Solr 軟體抓取的資料，僅需透過簡單設定 Solr 主機及資料來源資訊，即可以自動取得 Solr 資料的綱要，將綱要內所要呈現的資料，透過 Kurogo 軟體呈現於行動裝置上。此功能設定如下：使用者需提供整合於 Solr 軟體下資料來源的 Solr 主機 IP 位置、Solr 名稱以及 Solr 核心資料的名稱，當按下連結按鈕時會自動去連結 Solr 資料存放主機位置。

設定完成 Solr 軟體資料來源的連結後，由於 Kurogo 軟體提供在同一台伺服器下可以建立多個行動網站，因此，需要選擇新增的模組位於哪個行動網站(site)中，如圖 5。在此展示網站名稱 mysite，顯示模組名稱(Module Name)為專題文章，模組功能

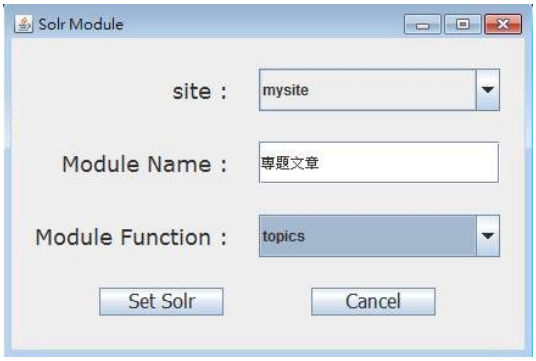


圖 5 模組命名及功能選擇

(Module Fuction)為 topics 的模組。其主要功能為將不同類型的文章分類，方便行動裝置使用者閱讀文章。按下設定 Solr 按鈕(Set Solr)後，需要進階設定此模組需要新增對應 Solr 軟體及 Kurogo 軟體的資料欄位並呈現於行動網頁的資訊。例如：在專題文章模組中，使用者需設定兩軟體的資料對應欄位方式，讓 Kurogo 軟體知道要向 Solr 軟體抓取對應欄位的資料，如圖 6 所示。

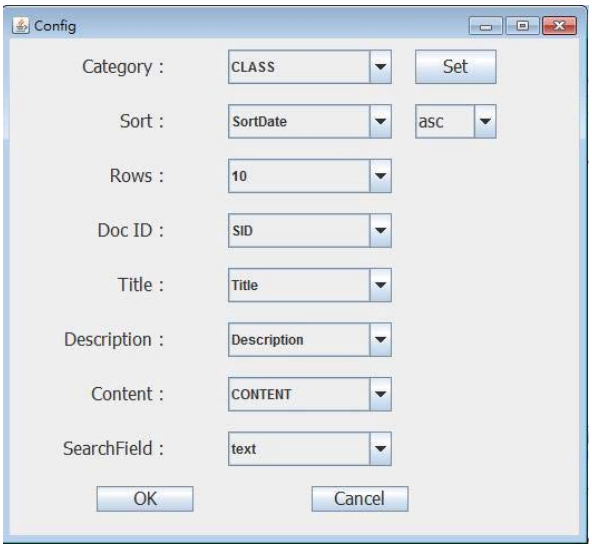


圖 6 專題文章對應欄位設定

分類的詳細設定，左方為呈現在行動網頁上分類所要顯示的名稱(Display Name)，右方為 Solr 軟體分類的網要欄位值(Solr Value)，設定的目的為向 Solr 軟體抓取資料傳至 Kurogo 軟體來取得文章的分類。下方的按鈕功提供新增、刪除及增加包含所有上方分類的全部文章(All Category)，如圖 7 所示。



圖 7 專題文章分類詳細設定

當完成前兩個功能設定後，即可以將「中央研究院數位典藏資源網」內的專題文章內容，包含歷史文物、人文社會、植物生態、海洋生態、技術新知、文學創新，為使用者在圖 7 中所填入的顯示名稱，透過本研究的方法實做出行動網站，並呈現於行動裝置，如圖 8 所示。



圖 8 中研院數位典藏資源網的專題文章行動頁面

對應欄位設定軟體可以快速的新增原生範例模組及透過我們新增的 Solr 串接 Kurogo 軟體模組。我們提供簡單的設定於 Kurogo 軟體上呈現整合異質性資料於 Solr 軟體資料的對應欄位方法，可以不需另外撰寫程式碼呈現於 Kurogo 行動網站上的資訊。如果不透過此方式，可能需要自行撰寫和異質性資料格式或資料庫溝通的資料抓取和解析程式，且需將資料整理成統一格式，並自行撰寫呈現於各行動裝置網站的偵測程式，困難度及複雜度會相對提高。

針對使用者透過對應欄位設定軟體設定完成的資訊，我們進一步開發透過 Kurogo 軟體的管理者介面，將使用者所設定的資訊做成介面化的呈現，如圖 9。透過 Solr 軟體資料的修改，管理者可



圖 9 專題文章於 Kurogo 中的管理者介面

以直接透過此介面對呈現內容做些微的調整，不需要自行修改 Kurogo 資料設定檔或再次透過對應欄位設定軟體來修改專題文章模組中 Solr 資料來源的主機位置、分類方式、透過 REST 方式向 Solr 溝通的主要搜尋欄位、文章排序方式、每頁回傳筆數、需要與 Solr 軟體溝通並回傳呈現於 Kurogo 軟體的資料欄位。使用此介面，可以讓網站管理者在日後維護及 Kurogo 軟體對於 Solr 軟體資料的修改呈現於行動網站的內容更為方便。

5 結論

本研究提供一套方法讓開發者使用 Solr 軟體整合異質性資料，並透過行動中介軟體 Kurogo 來製作成行動網站。經由 Solr 軟體處理異質性資料來源，開發者不需撰寫程式，只需撰寫 XML 格式的綱要及設定檔，讓龐大的異質性資料整合變為簡單。透過我們開發的對應欄位設定軟體定義 Solr 欄位與 Kurogo 欄位，將 Solr 整合後的資料透過 Kurogo 軟體呈現至行動網站，Kurogo 軟體會依據硬體類型、作業系統、瀏覽器來偵測不同解析度的行動裝置，自動調適成使用者方便閱讀的網頁形式，達到響應式網頁設計的概念。

在未來的研究方面，可擴充本軟體的功能，讓使用者透過 HTML5 與 CSS3 樣式的調整來改變主題顏色、按鈕樣式。使用者也可以透過檔案上傳行動網頁的 logo 或圖片，讓開發者可以有更大的彈性來做樣板及樣式的修改，例如：客製化各行動裝置行動網頁的頁首(header)、頁尾(footer)等。

致謝

本研究計畫由臺灣數位成果永續維運計畫－數位成果推廣應用計畫（I）資助，計畫編號：NSC 102-3113-P-001-003。

參考文獻

[1] The new multi-screen world study, http://www.google.com/think/research-studies/the-new-multi-screen-world-study.html.

[2] M. Meeker and L. Wu, “Internet trends,” D11_Conference, pp.30–37, 2013.

[3] App vs the Web, http://mattgemmell.com/2011/07/22/apps-vs-the-web/.

[4] M. Lu and W. Yeung, “A framework for effective commercial Web application development,” Internet Research: Electronic Networking Applications and Policy, vol. 8 iss: 2, pp.166–173, 1998.

[5] A. Charland and B. Leroux, “Mobile application development: web vs. native,” Communications of the ACM, vol. 54 iss: 5, pp.49–53, May 2011.

[6] F. Adelstein, S. K. S. Gupta, G. Richard, and L. Schwiebert, Fundamentals of mobile and pervasive computing, 1st ed., McGraw-Hill Professional, 2004, pp.113–125.

[7] T. Kanoc, “Mobile middleware: the next frontier in enterprise application integration，” White paper, Nettech Systems Inc., April 1999.

[8] D. Smiley and E. Pugh, Solr 1.4 enterprise search server, Packt, August 2009.

[9] Kurogo, http://kurogo.org/home/.

[10] 中央研究院數位典藏資源網, http://digiarch.sinica.edu.tw/.

網路與手機雙重成癮者之人格特質分析

鍾才元　陳明終　賴阿福　楊政穎　林慧婷
臺北市立大學
tchung@utaipei.edu.tw

摘要

本研究旨在分析網路成癮者與手機成癮者在人格特質方面的異同。樣本為 1,011 位大學生，其中男性 445 人、女性 566 人；大一至大四人數依序為 391、272、211、及 137 人。調查問卷內含網路與手機使用調查表、網路及手機成癮量表、與 Mini Markers 人格量表。參與者依據其網路成癮及手機成癮之程度分為四組：網路成癮者(*N*=111)、手機成癮者(*N*=189)、網路及手機雙重成癮者(*N*=72)、以及正常使用者(*N*=639)。本研究以正交對比(orthogonal contrasts)分析此四組在五大人格特質(外向性、親和性、正直自律性、情緒穩定性、與經驗開放性)方面之異同。本研究所發現之主要差異為：一、網路成癮者之外向性、情緒穩定性、與經驗開放性皆顯著低於手機成癮者。二、雙重成癮者之外向性顯著高於網路成癮者。三、雙重成癮者之親和性與正直自律性顯著低於手機成癮者。四、網路成癮者之外向性、正直自律性、情緒穩定性、與經驗開放性顯著低於正常使用者。五、手機成癮者之情緒穩定低於正常使用者。六、雙重成癮者之親和性、正直自律性、與情緒穩定性顯著低於正常使用者。根據以上發現，研究者就網路成癮與手機成癮之主要人格影響因素提出相關討論，並對未來研究方向提出若干建議。

關鍵詞：人格特質、手機成癮、手機使用行為、網路成癮、網路使用行為。

Abstract

The present study investigated the personality traits of users addicted to Internet, mobile phone, or both. A total of 1,011 college students (445 males and 566 females) participated in the survey, in which they filled out a checklist of Internet and mobile phone use, a rating scale of Internet and mobile phone addiction and a Mini-Marker personality test. Based on the measures of Internet addiction and mobile phone addiction, participants were classified into four groups: Internet addicts (IA), mobile phone addicts (MPA), dual addicts (DA), and normal users (NU). Orthogonal contrasts among the four groups were performed on big-five personality traits. The major findings were: 1. IA had significantly higher scores on extraversion, emotional stability, and openness than did MPA; 2. DA had significantly lower extraversion scores than did IA; 3. DA's agreeableness and conscientiousness were significantly lower than those of MPA; 4. IA scored significantly lower on extraversion, conscientiousness, emotional stability, and openness than did NU; 5. MPA had significantly lower emotional stability than did NU; 6. DA had significantly lower agreeableness, conscientiousness, and emotional stability than did NU. Based on these findings, a proposition is presented regarding the major personality trait(s) associated with Internet addiction and mobile phone addiction, followed by suggestions for future research.

Keywords: Internet Addiction, Mobile phone Addiction, Personality Traits.

1. 前言

隨著網際網路(以下簡稱網路)在頻寬與速度的提升、以及電腦及各種行動載具(如 Tablet、Smart Phone)的高滲透率，我們對網路與行動電話(mobile phone；以下簡稱手機)的仰賴程度也與日俱增，嚴重者甚至有網路成癮(Internet addiction)或手機成癮(mobile phone addiction)的問題。目前，網路成癮與手機成癮還不是正式的醫療診斷病症，但卻是引起許多學者重視的心理健康問題。

網路成癮或網路異常使用(Internet pathological use)方面的研究顯示，成癮者或異常使用與一般正常使用者之間有若干心理特徵或人格特質上差異[1]。同樣地，手機成癮或手機依賴(mobile phone dependence)的研究也發現，某些心理或人格特質變項可有效預測手機異常使用行為[2]。然而，由於網路成癮與手機成癮引起學者們重視的時間有前後之差別，鮮少有研究者同時探討網路成癮與手機成癮，所以我們無法根據以往的研究結果，論斷此二類成癮者在人格特質上的差異。再者，大多數網路使用者也都擁有手機，網路成癮者有可能同時就是手機成癮者。這些雙重成癮者的人格特質也很值得加以探討。

國外已有學者開始將網路成癮和手機成癮問題合併一起探討與研究[3][4]，惟國內目前尚未見同時探討網路成癮與手機成癮的研究。有鑒於此，本研究透過同時對網路成癮與手機成癮的測量，區分出網路成癮者、手機成癮者、雙重成癮者與正常使用者，然後對比分析此四群組在五大人格特質方面之異同，以求有助於更完整地了解現今網路成癮與手機成癮的現象。

2. 文獻探討

2.1 網路成癮

Kimberly S. Young 於 1996 年的美國心理學會年度大會指出，網路成癮與「病態性賭博」(pathological gambling)非常接近，是「一種未涉及麻醉品之衝動控制失調症」(an impulse-control disorder which does not involve an intoxicant)[5]。網路成癮比較正式的說法是：「由重複地對於網路的使用所導致的一種慢性或週期性的著迷狀態，並帶來難以抗拒的再度使用之欲望，同時並會產生想要增加使用時間的張力與耐受性、克制、退癮等現象，對於上網所帶來的快感會一直有心理與生理上的依賴」[6]。

目前，網路成癮尚未被正式列入《心理疾病診斷與統計手冊第五版》(The Diagnostic and Statistical Manual of Mental Disorders-V; DSM-V)，然多位學者認為，網路成癮會導致個人在日常生活、學習、工作、健康、人際關係、或理財等方面的混亂現象[1][7][8]，因此，網路成癮已經廣泛地引起美國、中國大陸、英國、臺灣、韓國與許多地區的學者之重視和研究[9]。研究者測量網路成癮時，通常透過檢核表或量表，由受試者以自我陳述之方式進行。檢核表或量表上常見的行為描述句均與上網行為或所衍生的問題有關，如「我需要花更多時間上網才能得到滿足」、「我會害怕萬一沒有網路後生活將是非常空虛與無趣」、「我曾試過想花較少的時間在網路上但卻無法做到」、以及「我只要有一段時間沒有上網，就會覺得心裡不舒服」等[5] [10]。

網路之所以容易讓許多使用者沉迷其中，網路科技與網路環境的特性是一個極重要的關鍵。這方面的特性包含網路頻寬與速度之提升、介面友善性、互動性、資訊豐富性與易取性等[1]。此外，網路的虛擬性、即時性、匿名性等特色，也被認為是想要逃避現實生活壓力或挫敗感的使用者可輕易地滿足其生理或心理需求與宣洩壓力的管道及方式[7]。值得一提的是，網路成癮者通常較頻於使用可雙向溝通或互動的應用程式與功能，前者如聊天室、新聞群組等，後者如各種角色扮演或多人線上遊戲等[1][5] [8] [11]。

網路成癮是否與使用者的心理因素或人格特質有關，一直是許多研究者關注的焦點。就目前已知的研究發現看來，網路成癮者與一般正常使用者在某些心理特徵或人格特質上是有明顯差異的。網路成癮者似乎有較高之寂寞感[12]；較高之憂鬱傾向[13]；較低自尊 [12]；有較高自主性、偏愛獨自活動、社交生活較為限縮、情緒感受與反應較為強烈、與較不順從社會規範[14]；以及有較高之焦慮感受與焦慮依戀傾向[15]。因此，一些學者認為，網路提供這些使用者一種既安全、又可與他人保持距離的互動機會，並同時滿足他（她）們的社交需求與成就感[14]。

2.2 手機成癮

隨著手機的高滲透率，其使用者的年齡範圍也就愈來愈廣，而且無論是上班族、學生、家庭主婦或退休族，人人都是手機一族。手機已經成為生活不可或缺的工具，甚至許多使用者已經有手機成癮或稱手機依賴(mobile phone dependence)的嚴重情況。手機成癮是繼電腦成癮、電腦遊戲成癮、及網路成癮等科技成癮(technological addictions)問題之後，獲得許多研究者重視的問題。目前多數學者均沿用病態性賭博或網路成癮之定義，來定義手機成癮，只是在用詞上聚焦於手機使用而已[16][17]。手機成癮之測量亦與上述網路成癮之測量方式大體相同。在檢核表或量表上常見的陳述句有「我因使用手機以致睡眠不足」、「我發現使用手機的時間比原先預期的多」、及「我的朋友和家人抱怨我的手機使用行為」等[16] 。手機成癮目前也尚未被列入 DSM-V，但已被認為和賭癮與網路成癮類似，屬於一種尋求立即滿足而不知節制之行為成癮現象，且會對個人工作表現、課業學習、或個人理財等產生不利之影響。

手機成癮被廣泛研究的時間雖落後於網路成癮，然此方面的研究也陸續顯示，手機使用者的心理與人格特質與其手機成癮的程度有關。一項研究指出外向性人格特質與低自尊感可有效預測手機異常使用行為[16]；另有研究發現，手機成癮問題與急性情(urgency)及堅毅力(perseverance)[2]、寂寞感[17]、衝動性(impulsiveness) [2][18]、情緒智力(emotional intelligence)[4] 、與自我監控能力(self-monitoring) 及他人認可動機 (approval motivation) [19]等心理或人格變項有顯著的相關。

2.3 小結

由以上研究文獻回顧可知，網路成癮者或手機成癮者都各有不同於一般使用者的某些心理特徵或人格特質。然而，以往之研究仍存有二個限制。首先，由於這二項科技產品問世的年代不同，當時的研究者僅能單方面地探討網路成癮或手機成癮，並未直接比較這二類成癮者在人格特質上的差異。由以往之研究結果看來，網路成癮者往往較為內向或寂寞；他們喜歡沉浸於一個人的世界，不善於也不熱衷於社交活動。相反的，手機使用者卻往往比較外向，喜歡隨時和朋友保持聯繫與互通訊息，也比較在意他人的看法。然而，以上描述僅屬間接臆測，其有效性仍有待實證研究之驗證。

再者，目前許多網路使用者也都是手機使用者。此情形在智慧型手機(smart phone)問世以後更為明顯。目前各廠牌的智慧型手機的重量愈來愈輕，觸控螢幕卻愈來愈大、且解析度愈來愈好，不僅可以通話、收發簡訊、播放音樂、玩遊戲、記事，

還可以照相、錄影、上網與視訊通話等。在第三代(3G)無線通訊技術引進後，只要能接受到訊號的地方，就可以用手機上網，其上網的便利性遠遠勝過於筆記型電腦，無怪乎近年來以手機上網的比例迅速地增加。也因為如此，網路成癮與手機成癮的界限已經不若以往涇渭分明，許多網路成癮者很可能也同時是手機成癮者。換句話說，有不少使用者有網路及手機雙重成癮(dual addiction)的情形。事實上，已有少數學者將網路和手機之過度使用問題一起研究[3] [4]。一份針對西班牙大學生所進行的研究報告指出，6.2%的學生屬網路成癮者，10.4%的學生屬手機成癮者，而 3.86%的學生同時有網路及手機成癮的問題[3]。很可惜的是，這些僅有的研究並未進一步探討網路與手機雙重成癮者(以下簡稱雙重成癮者)的人格特質。簡言之，網路與手機雙重成癮現象已逐漸普遍，而雙重成癮者有哪些不尋常的人格特質以及他(她)們在人格特質上是否與網路成癮者或手機成癮者有明顯的差異，是一個亟待解答的實證問題。

2.4 研究目的與問題

以往之研究者鮮少同時探討網路成癮與手機成癮現象，所以對此二類成癮者在心理特徵或人格特質的異同並無實證上的直接線索。此外，手機上網功能大幅提升後，網路成癮與手機成癮的界線漸趨於模糊，且衍生網路與手機雙重成癮的現象，然尚未見此方面之實證研究。有鑒於此，本研究藉由同時測量網路成癮與手機成癮，區分出網路成癮者、手機成癮者、雙重成癮者、與正常使用者，然後比較此四個族群在人格特質方面的異同。研究問題有四：(1)網路成癮者與手機成癮者的人格特質差異為何？(2)雙重成癮者與網路成癮者之人格特質差異為何？(3)雙重成癮者與手機成癮者之人格特質差異為何？(4)以上三種成癮者與正常使用者之人格特質差異為何？本研究希望藉由上述問題之探討，可對網路成癮與手機成癮有整合性的認識。

3. 研究方法

3.1 受試者

本研究以二種管道取得樣本。網路問卷調查是將問卷網址發表於臺大批踢踢實業坊(telnet:// ptt.cc)及優仕網(http://www.youthwant.com.tw/)的問卷看版中，徵求條件限定為大學在學生，以此方法共收集 215 份有效問卷。紙本問卷調查係以隨機方式抽取北區與中區五所大學，然後以叢集抽樣方式，由願意協助本研究之授課教師或助教在教室直接將問卷發給上課學生填答。實際發出的問卷為 1,048 份，扣除無效問卷後，實得有效問卷 1,011 份。由於網路問卷的有效份數相對較少、且無法百分百確定填答者均為大學生，因此本研究僅以紙本問卷樣本進行分析。

樣本中，男性(N = 445)少於女性(N = 566)；年級方面以大一人數最多(N = 391)，其次為大二(N = 272)、大三(N = 211)、與大四以上學生(N = 137)。接受調查的學生中，已使用網路五至十年者 585 人(57.9%)，超過十年者 365 人(36.1%)；使用手機已三至五年者為 249 人(24.6%)、五至十年者為 532 人(52.6%)、十年以上者為 99 人(9.8%)，可見大多數學生對於網路與手機既不陌生、也不外行。

3.2 研究工具

本研究所使用工具為「大學生網路與手機使用現況調查問卷」，內含三個部分：

一、網路與手機使用調查表：此調查表包含個人基本資料(性別、就讀年級、隸屬學院、經濟來源、住宿情況)、網路使用經驗與情形(每日平均上網時數、每週平均上網時數、最常上網地點、與上網最常從事的活動)、及手機使用經驗與情形(擁有手機數、持有手機之價位、持有手機之功能、最常使用之功能、與每天平均通話分鐘數)。

二、網路與手機成癮量表：此量表係特為本研究編製之工具，分成網路成癮與手機成癮二個分量表，各20題。網路成癮分量表之題目為Young所編製[20]，本研究採用蘇文進之中文翻譯[21]。手機成癮分量表係將廖婉沂參考Young之網路成癮量表所編寫之19個題目[22]稍加修改並新增1題後編排而成，以求與網路成癮分量表在題數上相同、且可以有一致的成癮程度之界定標準。此量表每一題目之後為五個選項(很少如此、偶爾如此、經常如此、常常如此、總是如此)，由受試者依據近三個月內實際使用網路或手機的情況勾選。分量表分數為加總20題後之分數，最低為20分，最高可為100分；分數愈高，表示網路或手機成癮之可能性愈高。本研究信度分析結果顯示，二個分量表之Cronbach's α 係數值為 .89(網路成癮)與 .93(手機成癮)。本研究依據受試者之網路與手機成癮分數分成三個等級：正常至輕度(≦49)、中度(50～79)、與重度(≧80)。

三、Mini-Markers 人格量表：此工具為測量五大人格特質之精簡型量表，由 Saucier 所編製[23]，且經研究證實為具有良好效度[24]。此量表的五個分量表分別為外向性(Extraversion)、親和性(Agreeableness)、正直自律性(Conscientiousness)、神經質／情緒穩定性(Neuroticism)、與經驗開放性(Openness to experience)；每一個分量表各有 8 題，合計 40 題。本研究將此量表之題目翻譯為中文後，再施測於受試者。受試者根據題目與個人感受的符合程度，勾選合適選項(非常不同意、不同意、稍微同意、同意、非常同意)。各分量表之分數愈高，表示具有該向度人格特質的程度愈高。本研究之信度分析結果顯示，此人格量表之 α 係數值分別為 .81(外向性)、 .70(親和性)、.84 (正直自律性)、.79 (情緒穩定性)、與 .81 (經驗開放性)。

4. 研究結果

4.1 網路成癮者、手機成癮者、與雙重成癮者之比例

本研究首先分析網路成癮與手機成癮之相關，其結果顯示二者屬低度正相關(r = .29，p < .001)，據此可推估約僅有 9%的參與者之網路成癮分數與手機成癮分數有同時高或低之情形。由於網路成癮程度屬重度者為 5 人，手機成癮程度屬重度者為 7 人，均相對較少，所以本研究將網路或手機成癮程度為中度與重度者合併。表 1 為網路成癮程度與手機成癮程度之交叉分析結果。

表 1 網路成癮與手機成癮程度之交叉分析

網路成癮 [1]	手機成癮 [1]			卡方檢定量 ($d.f.$ = 1)
	正常	中重度	合計	
正常	639	189	828	21.35***
中重度	111	72	183	
合計	750	261	1,011	

註：表格內數值為人數

[1] 正常：成癮量表分數低於或等於 49；中重度：大於或等於 50。

*** p < .001.

針對表 1 進行卡方檢定後之結果顯示，網路成癮程度與手機成癮程度彼此有關聯性存在(χ^2 = 21.35，p < .001)，然其關聯強度極低(Somer' d = .14，t = 4.14，p < .001)。因此，依據此交叉分析結果，本研究將受試者分成四組：

一、網路成癮者(N = 111)：即網路成癮程度屬中重度、而手機成癮程度屬輕度或正常。

二、手機成癮者(N = 189)：即手機成癮程度屬中重度、而網路成癮程度屬輕度或正常。

三、雙重成癮者(N = 72)：即網路成癮程度與手機成癮程度均屬中重度。

四、正常使用者(N = 639)：即網路成癮程度與手機成癮程度均屬輕度或正常。

4.2 網路成癮者、手機成癮者、雙重成癮者之人格特質分析

上述四組使用者在人格測驗五個分量表上之平均數詳如表 2。為分析此四組之人格特質，本研究先以受試者之人格測驗分數為依變項，進行單因子多變量變異數分析(one-way multivariate analysis of variance; MANOVA)。MANOVA 之結果顯示，此四組使用者在五大人格特質方面確有差異存在(Phillai's Trace statistic = .09，F = 6.19，p < .001)。

表 2 網路成癮與手機成癮者之人格量表分數

分量表	網路與手機成癮組別			
	網路成癮者 (N = 111)	手機成癮者 (N = 189)	雙重成癮者 (N = 72)	正常使用者 (N = 639)
外向性	24.12 (5.50)	26.83 (4.17)	26.85 (4.37)	26.38 (5.00)
親和性	28.89 (3.95)	29.40 (3.61)	28.11 (4.66)	29.64 (3.87)
正直自律性	26.16 (5.45)	26.87 (3.85)	25.33 (4.74)	27.61 (4.71)
情緒穩定性	24.91 (4.79)	26.04 (3.98)	25.29 (4.78)	27.60 (4.51)
經驗開放性	24.45 (4.56)	25.65 (4.32)	25.36 (5.22)	26.08 (4.68)

註：表格內數值為平均數與標準差(括號內)。

為進一步了解此四組使用者在五大人格特質之異同，本研究逐一以各分量表分數為依變項，進行單因子變異數分析之正交對比分析(orthogonal contrasts)。表 3 為就每一人格特質分數所進行之六個正交對比與其對比係數，其中之對比 1 即網路成癮者與手機成癮者之比較，對比 2 則為網路成癮者與雙重成癮者之比較，…以此類推。

表 3 正交對比係數表

對比	網路成癮與手機成癮組別			
	網路成癮者	手機成癮者	雙重成癮者	正常使用者
1	1	-1	0	0
2	1	0	-1	0
3	0	1	-1	0
4	1	0	0	-1
5	0	1	0	-1
6	0	0	1	-1

依據正交對比分析之結果，各組之間在人格特質上之差異，依序彙整呈現如下：

4.2.1 網路成癮者 vs. 手機成癮者

對比 1 的其中一組之網路成癮程度屬中度或重度、但在手機使用方面屬正常使用者，而另一組之手機成癮程度達中度或重度、但在網路使用方面屬正常使用者。對比結果顯示，二組差異達顯著水準之特質為外向性(t = -4.48，p < .001)、情緒穩定性(t = -2.12，p < .05)、與經驗開放性(t = -2.16，p < .05)。由表 2 可知，網路成癮者之外向性、情緒穩定性、與經驗開放性皆顯著低於手機成癮者。

4.2.2 網路成癮者 vs. 雙重成癮者

對比 2 的二組之網路成癮程度均屬中度或重

度，但其中一組(雙重成癮者) 之手機成癮程度也達中度或重度。分析結果顯示，二組在外向性之差異達顯著水準(t = -3.72，p < .001)，在其他四個特質之差異則均未達顯著水準。由表 2 可看出，雙重成癮者之外向性顯著高於網路成癮者。

4.2.3 手機成癮者 vs. 雙重成癮者

對比 3 的二組之手機成癮程度均達中度或重度，但其中一組之網路成癮程度也達中度或重度。二組對比結果顯示，僅親和性(t = 2.40，p < .05)與正直自律性(t = 2.46，p < .05)之差異達顯著水準，其他三種特質之差異則否。由表 2 可知，手機成癮者之親和性與正直自律性顯著高於雙重成癮者。

4.2.4 網路成癮者 vs. 正常使用者

對比 4 的二組均為手機正常使用者，然其中一組的網路成癮程度屬中度或重度。對比分析結果顯示，二組除在親和性之差異未達顯著水準外，在其他四個特質之差異均達顯著水準，依序為外向性(t = -4.05，p < .001)、正直自律性(t = -2.64，p < .005)、情緒穩定性(t = -5.86，p < .001)、以及經驗開放性(t = -3.40，p < .001)。由表 2 之平均數可知，網路成癮者之外向性、正直自律性、情緒穩定性、與經驗開放性之平均值均顯著低於正常使用者。

4.2.5 手機成癮者 vs. 正常使用者

對比 5 的二組都是網路正常使用者，然其中一組之手機成癮程度屬於中度或重度。對比分析結果顯示，二組在正直自律性(t = -2.22，p < .05)與情緒穩定性(t = -4.22，p < .001)之差異達顯著水準，在其他三個特質之差異則否。由表 2 可知，手機成癮者之正直自律性與情緒穩定性低於正常使用者。

4.2.6 雙重成癮者 vs. 正常使用者

對比6的其中一組在網路與手機成癮二方面均屬中重度，而另一組則為網路與手機正常使用者。二組對比結果顯示，差異達顯著水準有三種人格特質，分別是親和性(t = -3.17，p < .005)、正直自律性(t = -3.95，p < .001)、與情緒穩定性(t = -4.16，p < .001)。由表 2 可知，雙重成癮者之親和性、正直自律性、與情緒穩定性皆顯著低於正常使用者。

5. 討論與建議

本研究之重要性在於同時測量網路成癮與手機成癮，然後藉由正交對比分析，同時比較網路成癮者、手機成癮者、雙重成癮者與正常使用者在人格特質方面之異同。此外，正由於此四組之對比分析，讓我們對網路成癮或手機成癮的主要人格影響因素有更清晰的認識。此二論點進一步闡述如下：

首先，本研究發現，在五大人格特質上，網路成癮者與手機成癮者確有明顯之差異，其差異即在於外向性、情緒穩定性、與經驗開放性三個向度，且手機成癮者在這三個向度上均高於網路成癮者。由於本研究係直接對比此二類成癮者，因此所發現的人格特質差異應比間接的推測更具有效性。因為手機基本上是以社交互動為主要訴求的科技產品，所以手機成癮者之外向性與經驗開放高於網路成癮者是很合理的發現。一般而言，具外向性人格特質者通常也較為重視人際關係。因此，我們可推論手機成癮者也較網路成癮者更為重視人際互動過程，相對地也需要有較高的情緒穩定性。

其次，本研究也發現網路及手機雙重成癮者是另一獨特的成癮族群，至少在本研究所探討的人格特質方面如此。雙重成癮者不僅與正常使用者不同，也不同於單純的網路或手機成癮者。由三者之間的對比分析結果看來，雙重成癮者的親和性、正直自律性、與情緒穩定性顯著低於正常使用者；他(她)們的親和性與正直自律性也顯著低於手機成癮者。相反地，雙重成癮者的外向性卻顯著高於單純的網路成癮者。

藉由雙重成癮者與網路或手機單方面成癮者的對比，亦可對網路成癮或手機成癮的主要人格影響因素有更清晰的認識。具體言之，雙重成癮者與手機成癮在人格特質上差異(親和性與正直自律性)可解釋為影響網路成癮之主要人格因素，因為二者都在手機成癮方面達中高之程度，但前者在網路成癮程度也達中高級，而後者則否。至於手機成癮之主要人格影響，則可由雙重成癮者與網路成癮在人格特質上差異(外向性)加以推論而知，因為二者都是網路成癮程度達中高度的使用者，但前者在手機成癮方面也達中高程度，而後者則否。總而言之，人格特質中的親和性與正直自律性明顯較低者，容易有網路成癮的傾向，而外向性顯著較高者則比較是手機成癮的高危險群。

最後，本研究尚有若干不足之處，仍待其他研究者進一步加以探討。首先，本研究發現已有部分的網路與手機使用者有雙重成癮的現象，而目前最流行的智慧型手機是一種將通話與上網結合的科技產品，其使用者成為網路成癮、手機成癮、或雙重成癮者的比例是否也因而大幅度增加，的確很值得未來研究者加以直接探討。其次，本研究並未探討成癮類型與人格特質間的關係。依據使用的內容，網路或手機成癮尚可分線上性成癮(如瀏覽色情網站)、線上人際關係成癮、與強迫行為(遊戲、賭博、購物)等[25]。網路或手機成癮者未必都有這些成癮問題，而不同成癮類型的人格影響因素也可能有別。舉例而言，網路或手機遊戲成癮者的人格特質就應該會與迷戀於線上人際關係的使用者有明顯的差異。再者，網路與手機的某些功能或特殊應用與成癮問題有較強的關聯性[8][10]，但有些人熱衷於經營線上社群，有些人卻沉迷於多人線上遊戲；即使是同樣的應用程式，有些使用者有成癮現

象，有些人則無。以目前最膾炙人口的 Facebook(或稱臉書)為例，有些會員隨時惦念著好友們是否回應或更新動態消息，有些會員則獨鍾於網誌或內建的遊戲。換言之，應用程式類型與人格特質可能會有交互作用的現象，亦即具有某些人格特質的使用者會特別容易沉溺於特定之應用或功能。後續研究者如能就上述假定進行實際驗證，應有助於更完整地了解現今網路成癮和手機成癮的成因。

本研究者也建議未來的研究者應針對年幼學生的網路或手機成癮問題加以深入探討並謀求因應之道。大學生固然是最容易有網路或手機成癮問題的學生族群，但由於網路與手機的超高滲透率，目前小學生擁有手機(甚至是智慧型手機)的比例亦以令人驚駭的速度大幅提升，因此網路成癮、手機成癮、或雙重成癮的問題勢必向下延伸至高中(含)以下教育階段的學生，尤其是在週末或寒暑假等學生自主時間更多、更長的時期。所以，對年輕學生族群的網路或手機成癮之盛行率與相關影響因素的研究，實屬當務之急。然而，由於兒童與青少年的人格特質仍在形塑當中，影響他(她)們沉迷於網路或手機的影響因素，恐怕必須從人格特質以外的因素(如家長之監控能力、同儕影響)著手。從另一個角度來看，政府與學校在資訊教育領域比較重視的是隱私權的保護、網路詐騙的防治、與智慧財產權等，對所謂的「資訊科技成癮」卻著墨不多。資訊科技成癮問題與上述其他問題其實是密不可分的。愈容易成癮的使用者，也愈容易有侵害智慧財產權、罔顧他人隱私、網路詐騙他人或被詐騙的機會。政府與各級學校實在有必要重視與探討這方面成癮問題的成因、所造成的影響、以及其防治之道。

參考文獻

[1] C. Chou, L. Condron, and J. C. Belland, “A review of the research on Internet addiction,” Educ. Psychol. Review, 17(4), 363-388, 2005.

[2] J. Billieux, M. Van der Linden, and L. Rochat, “The role of impulsivity in actual and problematic use of the mobile phone,” Applied Cog. Psych., 22(9), 1195-1210, 2008.

[3] C. Jenaro, N. Flores, M. Gomez-vela, F. Gonzalez-gil, and C. Caballo, “Problematic internet and cell-phone use: psychological, behavioral, and health correlates,” Addiction Research and Theory, 15(3), 309-320, 2007.

[4] M. Beranuy, U. Oberst, X. Carbonell, and A. Chamarro, “Problematic internet and mobile phone use and clinical symptoms in college students: the role of emotional intelligence,” Comput. Human Behav., 25, 1182-1187, 2009.

[5] K. S. Young, “Internet addiction: The emergence of a new clinical disorder,” Cyberpsychol. Behav., 1(3), 237-244, 1998.

[6] 周倩，“我國學生電腦網路沈迷現象之整合研究-子計畫二：網路沉迷現象的心理病理之教育傳播觀點研究”，行政院國家科學委員會專題研究計畫，1999。

[7] K. S. Young, “Internet addiction: A new clinical phenomenon and its consequences,” Am. Behav. scientist, 48(4), 402-415, 2004.

[8] A. Kapahi, C. S. Ling, S. Ramadass, and N. Abdullah, “Internet addiction in malaysia causes and effects,” iBusiness, 5, 72-76, 2013.

[9] X. Carbonell, E. Guardiola, M. Beranuy, and A. Belles, “A bibliometric analysis of the scientific literature on lnternet, video games, and cell phone addiction,” J. of the Med. Libr. Assoc, 97(2), 102-107, 2009.

[10] 陳淑惠、翁儷禎、蘇逸人、吳和懋與楊品鳳，“中文網路成癮量表之編製與心理計量特性研究”，中華心理學刊，45(3)，279－294，2003。

[11] C. Chou, and M. C. Hsiao, “Internet addiction, usage, gratifications, and pleasure experience–The Taiwan college students’ case,” Comput Educ., 35(1), 65-80, 2000.

[12] J. Morahan-Martin and P. Schumacher, “Incidence and correlates of pathological Internet use among college students,” Comput. Human Behav., 16, 13-29, 2000.

[13] K. S. Young and C. R. Rodgers, “The relationship between depression and Internet addiction,” Cyberpsychol. Behav.,1, 25-28, 1998.

[14] K. S. Young, and C. R. Rodgers, “Internet addiction: personality traits associated with its development,” 1998, retrieved from http://www.netaddiction.com/articles/personality_correlates.pdf

[15] 林以正、王澄華、吳佳燁，“網路人際互動特質與依戀型態對網路成癮的影響”，中華心理學刊，47(3)，289－309，2005。

[16] A. Bianchi and G. J. Phillips, “Psychological predictors of problem mobile phone use,” Cyberpsychol. Behav., 8, 39-51, 2005.

[17] W. K. Park, “Mobile phone addiction,” in Mobile Communications, London: Springer, 2005, pp. 253-272.

[18] H. Y. Koo and H. S. Park, “Factors influencing cell phone addiction in adolescents,” J. of Korean Acad. Child Health Nursing, 16(1), 56-65, 2010.

[19] M. Takao, S. Takahashi, and M. Kitamura, “Addictive personality and problematic mobile phone use,” Cyberpsychol. Behav., 12(5), 501-507, 2009.

[20] K. S. Young, Caught in the net: How to recognize the signs of internet addiction--and a winning strategy for recovery, NY: John Wiley & Sons, 1998.

[21] 蘇文進，“青少年網路使用與寂寞感相關因素研究－以雲林縣高中職學生為例”，2006，取自臺灣碩博士論文系統(094CCU05396003)。

[22] 廖婉沂，“青少年手機使用與成癮因素之探討，2008，取自臺灣碩博士論文系統(096NCYU5576075)。

[23] G. Saucier, “Mini-Markers: A brief version of Goldberg’s unipolar big-five Markers,” J. of Personality Assessment, 60(3), 506-516, 1994.

[24] J. K. Palmer and J. M. Loveland, “Further investigation of the psychometric properties of Saucier's big five ‘mini-markers’: evidence for criterion and construct validity,” Individual Differences Research, 2(3), 231-238, 2004.

[25] 王智弘，“網路成癮的成因分析與輔導策略”，輔導季刊，44(1)，1－12，2008。

偏遠地區國中學生資訊素養之變遷-以嘉義縣某國中為例

游淑惠　　尤國任　　王偉達
南華大學 資訊管理系
p87221438@yahoo.com.tw、graham@mail.nhu.edu.tw、b2267513@gmail.com

摘要

本研究旨在瞭解國中學生資訊素養能力現況及相關因素，以嘉義縣中埔國中學生七、八年級學生為研究對象，採用調查法進行分析，並就分析的結果與 94 年許永諒針對中埔國中七、八年級學生研究結果做一比較。

根據調查結果分析，本研究之結論如下：嘉義縣中埔國中七、八年級學生資訊素養能力有不錯的水準。其資訊素養能力會隨著性別、家中有無個人電腦、家中電腦可否連上網路、家中是否有書刊雜誌、每週使用電腦的時間、家中是否有人可請教電腦問題、父母親是否支持學習電腦而有所差異。再針對本研究與 94 年的研究比較發現：不同的個人背景變項、學習經驗背景變項、學習環境背景變項之資訊素養均有顯著差異。根據研究結論，本研究並提出相關建議供學校教育行政機關及教師授課參考。

關鍵詞：國民中學、電腦素養、資訊素養。

1. 緒論

知識經濟社會的來臨，資訊科技的快速發展以及網際網路的普及，數位化資訊得以用迅速且便利的方式傳播至世界各地，網際網路已成為人類有史以來最大的知識體，其所伴隨而來的資訊使用能力成為各界矚目的議題。善用資訊來創造優勢，成為未來人才面對新時代挑戰的致勝關鍵。本研究宗旨在探討偏鄉地區國中學生資訊素養之現況，並以嘉義縣中埔國中七、八年級學生為例。

1.1 研究背景與動機

教育部為配合行政院縮減數位落差政策，101 年起執行「偏鄉數位關懷推動計畫」:第一期(94~96 年）為「縮減數位落差」，第二期（97~100 年）為「創造數位機會」，第三期（101~104 年）為「深耕數位關懷」，積極協助偏遠地區民眾、弱勢學童資訊應用與數位服務。教育部於 2005 年起設置了 168 個數位機會中心（Digital Opportunity Center；簡稱 DOC）(教育部,2009)，讓鄉村的居民可以學習資訊化應用，DOC 成為一個提供數位資訊學習的場所。發展偏鄉地區文化與地方特色產業，還需讓數位化應用帶入到鄉鎮中、小學，即早給予縮減數位落差觀念，將地方文化及產業特色結合教學內容，以符合當地數位化發展做有效推廣。歐盟資通訊政策認為，透過更強力的公共政策方案才能克服因地理及社會造成的數位落差問題[1]。

因以上原因引起研究者對嘉義縣資訊素養研究的興趣，且教育部在嘉義縣所設置的 10 個偏鄉數位機會中心中(中埔鄉、番路鄉、義竹鄉、竹崎鄉、大埔鄉、梅山鄉、六腳鄉、東石鄉、鹿草鄉、阿里山鄉) [2][3]，研究者發現許永諒於 94 年曾針對嘉義縣中埔國中學生資訊素養做過研究探討[4]，故本研究希望藉此更加深入探討國民中學學生之資訊素養現況及變遷，了解國中學生是否有足夠的資訊素養利用資訊及資訊科技，以解決問題，自主學習、終身學習此亦為本研究主要之動機。

1.2 研究目的

本研究旨在探討國民中學學生之資訊素養概況，分析來自不同家庭背景之國民中學學生之資訊素養差異情形，探討其造成的相關因素及究竟有那些方式可以提昇其資訊素養。

茲將本研究之目的條列如下：

一、了解國民中學學生資訊素養之現況。
二、探討於不同個人背景變項國中學生與其資訊素養的關係。
三、探討於不同學習經驗變項學生與其資訊素養的關係。
四、探討於不同學習環境背景變項國中學生與其資訊素養的關係。
五、探討不同年度學生於不同個人背景因素國中學生與其資訊素養的關係。
六、探討於不同年度國中學生與其資訊素養的關係。

2. 文獻探討

2.1 素養

所謂的素養是用來描述「人和外界能做合理溝通」的一種狀況。素養（literacy）一詞，原本指的是人人都需要的讀、說、聽、寫等能力，例如語文素養等。學者李隆盛(1996)認為構成素養的要件和特性是「基本」和「必要」。意即對於某一領域的素養而言，除了要認識和了解外，更要能運用該領

域的知識和技能[5]。

2.2 資訊素養

資訊素養這個名詞最早是由當時的美國圖書館與資訊科學學會主席 Paul Zurkowski 於 1974 年提出，主要是指個人具有找出、評估、與利用各種不同來源資訊的能力。美國圖書館學會將資訊素養定義為四種能力，即能「確認、評估、尋找、使用」各種資訊的能力。對資訊素養的解釋為，資訊素養是在資訊時代中一種生存的技能。一位具有資訊素養的人，不管他所選擇的資訊是來自於網路、書籍、報章雜誌、政府機關、影片，或是任何其它的來源，他都知道如何去發現、評量和有效地使用它們，他有解決一個特殊問題或是做出一個決定的能力。[6]

綜合以上文獻探討，研究者將「資訊素養」定義為：

一、在有需求或問題時能夠迅速搜尋所需資訊之來源。
二、能有效率地由資訊來源處獲取資訊。
三、能夠判斷並解讀所取得之資訊正確性，
四、能分析並瞭解所獲得資訊的價值與用途。
五、能有效率地組織綜合有用資訊。
六、能利用所整合的資訊解決相關問題，並轉化成為個人的能力、技術與態度。

2.3 數位落差

「數位落差(Digital Divide)」這個名詞在 1990 中期開始在美國出現，而被廣泛的討論，並且在柯林頓政府宣佈要開始努力減少數位落差起，成為大家重視的議題。

經濟合作發展組織(Organization for Economic Co-operation and Development, OECD, 2001)對於數位落差下了一個定義，即「不同社會階層之個人、家庭及區域，在接觸資訊通信科技與使用網際網路從事各項活動的機會差距」。

3. 研究方法

3.1 研究架構

綜合本研究之研究動機、研究目的及相關文獻，探討影響嘉義中埔國中學生資訊素養的因素及資訊素養現況分析。本研究有 10 個自變項分述如下；而依變項即為本研究之資訊素養。

一、本研究之個人背景自變項
（一）、學生背景因素：
1 .性別： 分為(1) 男(2) 女
2 .年級： 分為(1)七年級(2)八年級
（二）、學習經驗背景因素
1 .是否參加校外電腦課程
2 .是否玩過電腦遊戲
3 .每週使用電腦的時間
（三）、學習環境因素
1 .家中有無個人電腦
2 .家中電腦可否連上網路
3 .家中是否有電腦書刊雜誌
4 .父母親是否支持學習電腦
5 .家中是否有人可請教電腦網路問題
二、本研究之依變項：
即指本研究之資訊素養，包括
（一）、發現問題的能力
（二）、尋求資訊的能力
（三）、檢索資訊的能力
（四）、使用資訊的能力
（五）、綜合組織資訊能力
（六）、評估分享資訊能力

3.2 研究假設

本研究提出研究假設，茲分列如下：

H1：不同「性別」之中埔國中學生資訊素養呈現顯著差異。
H2：不同「年級」之中埔國中學生資訊素養呈現顯著差異。
H3：是否參加過校外電腦課程之中埔國中學生資訊素養呈現顯著差異。
H4：是否玩過電腦遊戲之中埔國中學生資訊素養呈現顯著差異。
H5：每週使用電腦的時間之中埔國中學生資訊素養呈現顯著差異。
H6：家中是否有電腦設備之中埔國中學生資訊素養呈現顯著差異。
H7：家中電腦是否有連上網路之中埔國中學生資訊素養呈現顯著差異。
H8：家中是否有相關電腦書刊雜誌之中埔國中學生資訊素養呈現顯著差異。
H9：父母是否支持學習電腦之中埔國中學生資訊素養呈現顯著差異。
H10：家中是否有人可以請教電腦網路問題之中埔國中學生資訊素養呈現顯著差異。
H11：94 年度與 101 年度之中埔國中學生於個人背景其資訊素養呈現顯著差異。
H12：94 年度與 101 年度之中埔國中學生於學習經驗背景其資訊素養呈現顯著差異。
H13：94 年度與 101 年度之中埔國中學生於學習環境其資訊素養呈現顯著差異。

3.3 研究對象

本研究採取問卷的方式針對偏鄉地區進行探討，以嘉義縣中埔鄉為其研究區域，研究者親至嘉義縣中埔國中施行問卷，其研究對象為嘉義縣中埔

國中之七、八年級普通班學生，為了與 94 年許永諒所做之研究做一比較，故不包含三年級及特教班學生。並將其問卷與 94 年許永諒所做之問卷結果做為對照比較[4]。

3.4 研究工具

本研究所採用之問卷主要是許永諒(2005)研究者據大六技能(Big Six Skills)所編製之「國民中學學生資訊素養之研究— 以嘉義縣中埔國中為例」問卷[4]。正式問卷信度檢定，如表 1，所以此測驗亦具有良好信度。

表 1 資訊素養各構面之 Cronbach’s α值

構面	Cronbach’s α
發現問題的能力	0.806
尋求資訊的能力	0.746
檢索資訊的能力	0.718
使用資訊的能力	0.723
綜合資訊的能力	0.813
評估分享的能力	0.821
整體能力	0.898

而其問卷內容分為二部份。
(一)第一部份：「國民中學學生基本資料」
(二)第二部份「國民中學學生資訊素養能力量表」分為六個向度，共三十題。

本研究問卷第二部份作答方式採用李克特（Likert）四點量表，由受試者依其個人認知，針對本問卷之各題項，擇一填答。計分方式為「完全同意」得四分、「部份同意」得三分、「部份不同意」得二分、「完全不同意」得一分。

3.5 資料處理與分析

本研究採用問卷調查法，實際施測並蒐集資料，以探討受測者資訊素養之現況，並透過 SPSS for Windows12.0 版統計套裝軟體的程式比較受測者個人背景變項與其資訊素養的差異[7]，並與 2005 許永諒之研究結果做對照比較。

根據嘉義縣中埔國民中學 101 學年度學生人數概況表，七、八年級的普通班學生總計有 487 人。本研究的正式問卷施測採用全面普測，並與教務主任連繫，研究者親至各班級進行問卷之分發、解釋、施測、回收。總計分發的正式問卷有 487 份，共回收 470 份，回收率達 97%，可用的有效問卷有 421 份，有效可用率有 90%。

4. 分析與討論

表 2 不同性別之中埔國中學生資訊素養 t 檢定摘要表

	性別	年度	平均數	個數	標準差	T 值	P 值
發現問題	女	94	2.97	244	0.5913	-1.899	0.058
		101	3.07	203	0.5062		
	男	94	2.85	254	0.6057	-2.532	0.012
		101	2.99	218	0.5909		
尋求資訊	女	94	2.82	244	0.6859	-11.57	<0.001
		101	3.48	203	0.4783		
	男	94	2.77	254	0.5932	-11.73	<0.001
		101	3.4	218	0.5684		
檢索資訊	女	94	2.92	244	0.6673	-10.67	<0.001
		101	3.5	203	0.4307		
	男	94	2.89	254	0.5642	-10.08	<0.001
		101	3.4	218	0.5281		
使用資訊	女	94	3.03	244	0.62	-2.771	0.006
		101	3.18	203	0.503		
	男	94	2.94	254	0.64	-1.027	0.305
		101	3	218	0.6245		
綜合資訊	女	94	2.96	244	0.59	-4.64	<0.001
		101	3.22	203	0.5896		
	男	94	2.84	254	0.65	-4.547	<0.001
		101	3.11	218	0.6351		
評估分享	女	94	2.3	244	0.33	-9.25	<0.001
		101	2.77	203	0.7066		
	男	94	2.11	254	0.43	-10.47	<0.001
		101	2.71	218	0.7871		
整體能力	女	94	2.86	244	0.53	-7.262	<0.001
		101	3.2	203	0.444		
	男	94	2.76	254	0.53	-7.071	<0.001
		101	3.1	218	0.5098		

表 3 不同年級之中埔國中學生資訊素養 t 檢定摘要表

	年級	年度	平均數	個數	標準差	T 值	P 值
發現問題	七年級	94	2.84	255	0.5906	-3.22	0.001
		101	3.02	209	0.6093		
	八年級	94	2.98	243	0.6051	-1.15	0.251
		101	3.04	212	0.4913		
尋求資訊	七年級	94	2.76	255	0.6624	-11.09	<0.001
		101	3.41	209	0.5834		
	八年級	94	2.83	243	0.6154	-12.37	<0.001
		101	3.47	212	0.4653		
檢索資訊	七年級	94	2.92	255	0.6025	-9.216	<0.001
		101	3.41	209	0.5272		
	八年級	94	2.89	243	0.6314	-11.41	<0.001
		101	3.48	212	0.4396		
使用資訊	七年級	94	2.96	255	0.64	-2.597	0.01
		101	3.11	209	0.5925		
	八年級	94	3.01	243	0.62	-0.899	0.369
		101	3.06	212	0.5577		
綜合資訊	七年級	94	2.86	255	0.64	-4.315	<0.001
		101	3.12	209	0.6527		
	八年級	94	2.94	243	0.6	-4.701	<0.001
		101	3.2	212	0.5749		
評估分享	七年級	94	2.12	255	0.41	-11.11	<0.001
		101	2.74	209	0.7676		
	八年級	94	2.29	243	0.35	-8.34	<0.001
		101	2.73	212	0.7322		
整體能力	七年級	94	2.78	255	0.53	-7.264	<0.001
		101	3.14	209	0.5325		
	八年級	94	2.85	243	0.53	-6.812	<0.001
		101	3.16	212	0.4257		

表 4 94 年度和 101 年度之學生資訊素養 t 檢定摘要表

	年度	個數	平均數	標準差	T 值	P 值
發現問題	94	498	2.91	0.5986	-3.099	0.002
	101	421	3.03	0.5525		
尋求資訊	94	498	2.79	0.6386	-16.6	<0.001
	101	421	3.44	0.5275		
檢索資訊	94	498	2.90	0.6147	-14.8	<0.001
	101	421	3.45	0.4857		
使用資訊	94	498	2.98	0.6302	-2.494	0.013
	101	421	3.08	0.5753		
綜合資訊	94	498	2.90	0.6206	-6.427	<0.001
	101	421	3.16	0.6152		
評估分享	94	498	2.20	0.3810	-14.05	<0.001
	101	421	2.74	0.7491		
整體能力	94	498	2.81	0.5300	-10.12	<0.001
	101	421	3.15	0.4813		

5. 結論與建議

5.1 結論

根據問卷調查的分析結果，歸納本研究結論如下：

壹、 嘉義縣中埔國民中學學生的整體及各向度資訊素養現況尚可。

就整體而言，嘉義縣中埔國中學生資訊素養能

力，平均數 3.15，在李克特 4 點量表上居中等以上的程度，顯示現階段嘉義縣中埔國中學生資訊素養能力有一定的水準。

在「發現問題能力」、「尋求資訊能力」、「檢索資訊能力」、「使用資訊能力」、「綜合組織資訊能力」、「評估分享資訊能力」六個向度中，以「檢索資訊能力」向度所得平均數最高(M=3.45)，其次是「尋求資訊能力」(M=3.44)，「綜合組織資訊能力」(M=3.16)，「使用資訊能力」(M=3.08)，「發現問題能力」(M=3.03)，「評估分享資訊能力」(M=2.74)為最低。

貳、不同背景變項的嘉義縣中埔國中學生資訊素養有不同的差異情形

根據本研究結果，嘉義縣中埔國中學生資訊素養會隨著個人背景不同而有所差異。分述如下：

一、不同個人背景變項學生的資訊素養是否有顯著差異

(一)性別：不同性別的嘉義縣中埔國中學生資訊素養有顯著差異，且學生的整體資訊素養女性高於男性。

(二)年級：不同年級的嘉義縣中埔國中學生其資訊素養沒有顯著差異。

二、不同學習經驗背景變項學生的資訊素養是否有顯著差異

(一)有無參加校外電腦課程：有無參加校外電腦課程之嘉義縣中埔國中 學生資訊素養沒有顯著差異。

(二)是否玩過電腦遊戲：是否玩過電腦遊戲之嘉義縣中埔國中學生其資訊素養沒有顯著差異。

(三)每週使用電腦的時間：每週使用電腦的時間不同的嘉義縣中埔國中學生資訊素養未有顯著差異。

三、不同個人學習環境背景變項學生的資訊素養是否有顯著差異

(一)家中是否有個人電腦設備：家中是否有個人電腦設備之嘉義縣中埔國中學生資訊素養具有顯著差異，且家中有個人電腦設備學生之整體資訊素養高於家中沒有個人電腦設備的學生。

(二)家中電腦可否連上網路：家中電腦可否連上網路的嘉義縣中埔國中學生資訊素養具有顯著差異，且家中電腦可連上網路學生之整體資訊素養高於家中電腦不可連上網路的學生。

(三)家中有無電腦書刊雜誌：家中有無電腦書刊雜誌的嘉義縣中埔國中學生資訊素養具有顯著差異。且家中有電腦書刊雜誌學生之整體資訊素養高於家中無電腦書刊雜誌的學生。

(四)父母是否支持學習電腦網路：父母是否支持學習電腦網路的嘉義縣中埔國中學生資訊素養具有顯著差異，且父母支持學習電腦網路學生之整體資訊素養高於父母不支持學習電腦網路的學生。

(五)家中是否有人可請教電腦網路問題：家中是否有人可請教電腦網路問題的嘉義縣中埔國中學生資訊素養具有顯著差異，且家中有人可請教電腦網路問題學生之整體資訊素養高於家中沒有人可請教電腦網路問題的學生。

參、94 年和 101 年嘉義縣中埔國中學生資訊素養有不同的差異情形

根據本研究結果，94 年度嘉義縣中埔國中學生和 101 年度的學生其資訊素養有所差異。分述如下：

一、94 年和 101 年不同個人背景變項學生的資訊素養是否有顯著差異

（一）性別：94 年和 101 年不同性別的嘉義縣中埔國中學生資訊素養有顯著差異，且學生的整體資訊素養 101 年度的學生高於 94 年度的學生。

（二）年級：94 年和 101 年不同年級的嘉義縣中埔國中學生其資訊素養有顯著差異，且學生的整體資訊素養 101 年度的學生高於 94 年度的學生。

二、94 年和 101 年不同學習經驗背景變項學生的資訊素養是否有顯著差異

（一）有無參加校外電腦課程：有無參加校外電腦課程之 94 年和 101 年嘉義縣中埔國中學生資訊素養有顯著差異。且學生的整體資訊素養 101 年度的學生高於 94 年度的學生。

（二）是否玩過電腦遊戲：有玩過電腦遊戲之 94 年和 101 年嘉義縣中埔國中學生其資訊素養有顯著差異。而沒有玩過電腦遊戲之 94 年和 101 年嘉義縣中埔國中學生其資訊素養沒有顯著差異。

（三）每週使用電腦的時間：每週使用電腦的時間不同之 94 年和 101 年嘉義縣中埔國中學生資訊素養有顯著差異。且學生的整體資訊素養 101 年度的學生高於 94 年度的學生。

三、不同個人學習環境背景變項學生的資訊素養是否有顯著差異

（一）家中是否有個人電腦設備：家中是否有個人電腦設備之 94 年和 101 年嘉義縣中埔國中學生資訊素養具有顯著差異，且學生的整體資訊素養 101 年度的學生高於 94 年度的學生。

（二）家中電腦可否連上網路：家中電腦可否連上網路之 94 年和 101 年嘉義縣中埔國中學生資訊素養具有顯著差異，且學生的整體資訊素養 101 年度的學生高於 94 年度的學生。

（三）家中有無電腦書刊雜誌：家中有無電腦書刊雜誌之 94 年和 101 嘉義縣中埔國中學生資訊素養具有顯著差異。且學生的整體資訊素養 101 年度的學生高於 94 年度的學生。

（四）父母是否支持學習電腦網路：父母是否支持學習電腦網路之 94 年和 101 嘉義縣中埔國中學生資訊素養具有顯著差異，且學生的整體資訊素養 101 年度的學生高於 94 年度的學生。

（五）家中是否有人可請教電腦網路問題：家中是否有人可請教電腦網路問題之 94 年和 101 嘉義縣中埔國中學生資訊素養具有顯著差異，且學生的整

體資訊素養 101 年度的學生高於 94 年度的學生。

5.2 研究限制

一、 本研究以嘉義縣立國民中學之七、八年級的普通班學生為主要研究對象，概化範圍僅限為以農業為主之鄉鎮地區的國中學生。
二、本研究因欲與 94 年度許永諒之研究做一比較，故採用其問卷且未加以修改。

5.3 建議

根據本研究結論，分別針對學術上及實務上提出以下幾項建議，以便於提供教育主管機關、學校教師、及學生家長作為提昇資訊素養的參考。
壹、學術上
一、擴大研究地區
本研究取樣地區僅限於嘉義縣中埔鄉，若未來研究能擴及至臺灣其它鄉鎮，甚至台北、高雄等都會地區，將可更廣泛瞭解目前全臺灣國中學生資訊素養能力之現況及變遷。
二、增加研究對象
本研究只限於嘉義縣中埔國中七、八年級學生進行調查，未來研究對象可擴及國小、國中其他年級、高中及大學或其他職業。
三、採取不同研究方法
因本研究採取問卷調查法之資訊素養能力測驗，受測學生容易受到當時的環境或個人心態等因素，影響其研究結果之客觀性，故未來研究可針對其研究對象採取觀察或實際訪談等質性研究方法，做更進一步之探討。
四、研究工具使用
本研究所採用之問卷為 94 年研究者許永諒所編製，但因資訊科技日新月異，變化速度太快，因此本研究之工具也應參考當時的情況，才能編製出更適合有效的調查問卷。
貳、實務上
一、教育主管機關
本研究學生在評估分享資訊能力平均數最低，建議教育部可每年編列預算，使學校可擴充及維護其資訊相關網路軟硬體設備，並且多加設置 DOC 相關設施，營造一個數位學習的環境，讓學生可以多加練習使用網路，如此一來學生更容易獲取資訊及知識，並提升學生的資訊能力。
二、學校及學校教師
學校是學生獲取資訊與知識相當重要的場所之一，故學校的學習環境及學校教師的資訊素養相當的重要，學校可增設其電腦網路及圖書館資訊，讓教師將資訊素養能力融入各科教學課程中，提升學生之資訊素養能力，讓每個學生可以學習各科知識之外也能加強資訊素養能力。此外，學校應鼓勵教師多參加資訊素養相關之研習或進修，以便於提升教師的資訊能力，進一步教導及培育學生資訊素養的能力。
三、學生家長
建議學生家長能充實家中資訊相關設備，多關心學生使用電腦情形，並有限度的讓學生使用資訊設備和網際網路，並且提昇自身的資訊素養能力。若教育單位或社區有開設民眾資訊教育課程，可與學生一同踴躍參加，將有助於增進學生及家長自身的資訊素養能力。

6. 參考文獻

[1]行政院研考會，101 年個人家戶數位落差調查報告，2012。網址：http://www.rdec.gov.tw/public/Attachment/312113493071.pdf
[2]教育部，資訊教育白皮書，臺北市：教育部，1998。
[3]教育部，偏鄉數位機會推動計畫，臺北市：教育部，2008。
[4]許永諒，國民中學學生資訊素養之研究-以嘉義縣中埔國中為例，南華大學資訊管理研究所論文，2005。
[5]李隆盛，談資訊素養教育，社教雙月刊，1996，頁 73，23-24。
[6]American Library Association Presidential Committee on Information Literacy, January 1989. http://www.infolit.org/docoents/89Report.htm
[7]吳明隆，SPSS 統計應用實務。松崗電腦圖書公司，2000。
[8]中央教育科學研究所，國際教育百科全書，教育科學出版社，1992。
[9]王秋絨、張稚鳳，成人資訊素養研究，資訊素養與終身學習社會國際研討會會議論文集，1999，頁 201-234。
[10]何榮桂、籃玉如，落實教室電腦教師應具備之資訊素養。資訊與教育雜誌，2000，頁 85,5-21。
[11]吳美美，資訊素養的意義。圖書與資訊學刊，1997。
[12]李清泉，高職學生的電腦態度調查分析。國立高雄師範大學資訊教育研究所論文，2003。
[13]李德竹，資訊素養的意義、內涵與演變。圖書與資訊學刊，2000，頁 35，1-25。
[14]李德竹，由圖書館資訊服務規劃我國圖書館資訊素養之培方針與評量指標，國科會專題計畫，1997。
[15]沈中偉，國小資訊教育的省思與理念。資訊與教育雜誌，1999，71，頁 52-57。
[16]沈美如，公共圖書館讀者資訊素養之研究—以台南市公共圖書館為例。國立中興大學圖書資訊學研究所論文，2002。
[17]卓俊良，國民小學教師九年一貫課程教學資訊素養之研究。屏東師範學院國民教育研究所碩士論文，2002。

利用網路學習平台實施補救教學之可行性研究
－以偏遠國小為例

沈保信[1]　　陳昌盛[2]
[1]新竹縣花園國小
[2]國立交通大學資訊技術服務中心
hs5640@nc.hcc.edu.tw ; cschen@mail.nctu.edu.tw

摘要

十二年國教政策即將上路，針對學習低成就學生的補救教學是一個相當重要且受到關注的議題。眾所周知，在現今M型社會底下，仍存在著相當大的城鄉差距與數位落差。本文旨在探討利用網路學習平台在新竹縣一所偏遠小學進行六年級數學科分數單元學習低成就學生的補救教學之成效。在本研究中，我們安排兩組（班）的學生參與，並比較二者之學習成效。針對甲班（實驗組，共三名學生），我們採用網路式的補救教學；另外，針對乙班（對照組，共九名學生），則採用傳統式的補救教學。其次，為了驗證網路式補救教學的有效性，針對甲班，我們還進行了問卷調查，以進一步了解學生對於網路式補救教學的態度和看法。本研究主要的結果與發現如下：一、大致而言，網路式補救教學有一定的成效。二、學生對於網路平台式補救教學大多抱持正面的態度和看法。三、網路學習平台個別化及適性化的特性，有助於補救教學。

關鍵詞：十二年國教、補救教學、城鄉差距、網路學習平台。

Abstract

The remedial teaching for underachievers is one of the most important issues of the coming twelve-year basic education policy. This paper aimed to explore the use of an online e-learning platform to conduct the remedial teaching of the mathematical discipline (on the topic of the decimal fraction unit) for underachievers in sixth-grade classes of an elementary school of Hsinchu county. For comparison, we had two groups (i.e., two classes) of students participating in this study. On the one hand, we applied the remedial teaching on Class A (i.e., the experiment group, having three students); on the other hand, we applied the traditional approach on Class B (i.e., the control group, having nine students). Moreover, to validate the effectiveness of the online remedial instruction methods applied, we had also conducted a questionnaire in Class A to further study the students' attitudes and perceptions about the online approaches. The major results and findings of this study are as follows: First, according to expertise, online remedial e-learning systems are effective in promoting remedial education teaching. Second, according to our limited survey results, most students expressed the very idea that the online remedial teaching approach was more interesting than the traditional instruction one.

Keywords: twelve-year basic education policy, remedial teaching for underachievers, urban-rural gap, online e-learning

1. 前言

十二年國教即將上路，在目前的教育氛圍中，補救教學是一個相當重要且受到關注的議題。然而，在現今 M 型社會底下，仍存在著相當大的貧富差距、城鄉差距與數位落差。例如，研究者目前所任教的學校，就是屬於這類貧窮、位於偏鄉，且數位機會落後的學校。

本文旨在探討利用網路學習平台在一所偏遠小學進行六年級數學科分數單元補救教學之成效。如圖1所示，為了便於比較，我們安排兩組（班）的學生參與此一研究。甲班，總共有三名學生；而乙班，共有九名學生。針對甲班（即實驗組），我們採用網路式的補救教學方式；另一面，針對乙班（即對照組），則採用傳統式的補救教學方式；以比較二者之成效。此外，為了驗證網路式補救教學的有效性，針對甲班，我們還進行了問卷調查，以進一步了解學生對於網路式補救教學的態度和看法。

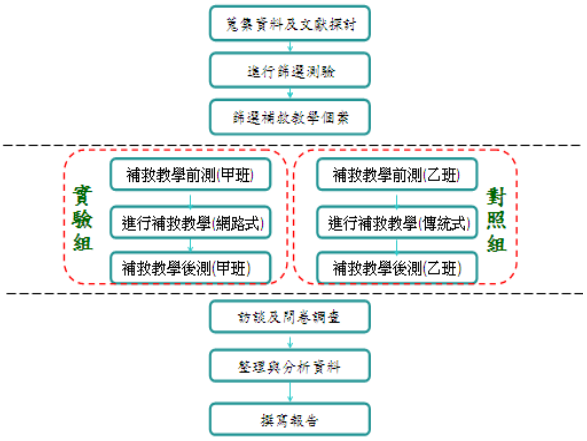


圖1 研究流程圖

本研究主要的結果與發現如下：一、大致而言，網路式補救教學有一定的成效。二、學生對於網路平台補救教學大多抱持正向的態度和看法。三、網路學習平台個別化及適性化的特性，有助於補救教學。根據以上的研究結果，我們建議數學科教學者應重視補救教學，特別是個別化與適性化的問題，並且能夠嘗試採用網路平台來進行補救教學。

本論文後續章節內容如下：第二節提到研究動機及文獻探討；第三節，進一步闡述本論文的研究方法；第四節說明本研究的實驗結果與分析。最後，第五節則提出本研究的結論與對未來教學者的建議。

2. 研究動機及文獻探討

2.1 研究動機

補救教學的對象為學習低成就的學生。所謂「學習低成就學生」，一般學者將其定義為：智力正常，但實際的學業表現卻明顯低於其能力水準者。然而根據「國中、小補救教學實施方案」作業要點所指學習低成就學生，係指參加補救教學篩選測驗，結果未達60分者。

自102年起，教育部整合「攜手計畫」及「教育優先區」為《國民小學及國民中學補救教學實施方案》單一計畫，目的在扶助每一位學習成就落後的學生，不因身分而有差別。因此，教育部要求全國各國中、小學生（單一學科成績在該班級後百分之三十五者）必須參加補救教學篩選測驗（包括國語、英語、數學三科），以作為是否要接受補救教學之依據，研究者服務的學校亦不例外。然而，施測的結果，單就數學科而言，六年級學生竟然全數未通過；換句話說，所有的六年級學生均需接受補救教學，此一結果令人驚訝，也引起研究者的注意。究竟是何原因造成學生數學成就如此低落？再者，如欲進行補救教學，究竟採取何種方式會比較有效，這些都是研究者亟欲探討的問題，亦是本研究的重點。

2.2 城鄉差距 – 從 PISA 談起 [1][2]

PISA (the Program for International Student Assessment) 國際學生能力評量計劃，係OECD (經濟合作暨發展組織)自 1997 年起所籌劃的一項跨國性評量計畫，每三年舉行一次大規模測驗，內容涵蓋閱讀，數學和科學三個領域，由所有OECD 會員國與其他非會員國的夥伴國家（地區）共同合作來完成。評量試題包括選擇題、封閉式問答題（類似填充題）、開放式問答題等題型，目的在考驗學生批判和推估能力。

PISA 2009 顯示東亞國家（經濟體）學生數學素養表現優異，數學素養前五名依序為上海、新加坡、香港、韓國與臺灣。數學量尺以 PISA 2003 的調查為基準，臺灣在 PISA 2006 平均為 549 分，與芬蘭、香港、韓國等三個國家並列世界第一。2009 參與國家數量由 57 增加至 65，臺灣的平均得分為 543，相較 2006 退步 6 分，排名第五。與第四名韓國的差異未達統計顯著。然而從表 1 可知，在兩次 PISA 數學表現優秀的前十名國家中，臺灣學生的個別差異都是最大的（標準差分別是 103、105）。

學生的數學表現分為六個精熟水準，根據這些水準，可以具體描述學生數學的表現概況。表 2 是臺灣與參照國家在數學素養不同水準學生人數比例分配對照（含 2006 臺灣資料）。在數學部分，臺灣的高分群表現（水準 5 以上）學生佔 28.5%，上海佔 50.4%、新加坡 35.6%、香港 30.7%。然而在數學低分群（水準 1 及未達水準 1)比較當中，臺灣人數的比例則是最高的[2]。

表 1 PISA 2006 與 PISA 2009 數學素養排名（前 10 名）

名次	2006 年			2009 年		
	國家	平均數	(標準差)	國家	平均數	(標準差)
1	台灣	549	(103)	上海	600	(103)
2	芬蘭	548	(81)	新加坡	562	(104)
3	香港	547	(93)	香港	555	(95)
4	韓國	547	(93)	韓國	546	(89)
5	荷蘭	531	(89)	台灣	543	(105)
6	瑞士	530	(97)	芬蘭	541	(82)
7	加拿大	527	(86)	列支敦斯登	536	(88)
8	列支敦斯登	525	(84)	瑞士	534	(99)
9	澳門	525	(93)	日本	529	(94)
10	日本	523	(91)	加拿大	527	(88)

表 2 臺灣與相關國家在各項數學素養水準的學生比例分配

國家	數學素養水準						
	未達 1 (低於 357.8)	1 (357.8~ 420.1)	2 (420.1~ 482.4)	3 (482.4~ 544.7)	4 (544.7~ 607)	5 (607~ 669.3)	6 (高於 669.3)
臺灣	4.2	8.6	15.5	20.9	22.2	17.2	11.3
臺灣 2006	3.6	8.3	14.3	19.4	22.4	20.1	11.8
上海	1.4	3.4	8.7	15.2	20.8	23.8	26.6
韓國	1.9	6.2	15.6	24.4	26.3	17.7	7.8
芬蘭	1.7	6.1	15.6	27.1	27.8	16.7	4.9
香港	2.6	6.2	13.2	21.9	25.4	19.9	10.8
新加坡	3.0	6.8	13.1	18.7	22.8	20.0	15.6
日本	4.0	8.5	17.4	25.7	23.5	14.7	6.2
澳門	2.8	8.2	19.6	27.8	24.5	12.8	4.3
OECD 平均	8.0	14.0	22.0	24.3	18.9	9.6	3.1

2006 年台灣 PISA 數學成績高居世界冠軍，然而城鄉差距卻是 OECD 國家的 2.6 倍；2009 年台灣數學成績排名第五，城鄉差距更高達 OECD 國家的 5 倍。城鄉差距有擴大的趨勢，此一現象值得關注[3]。

2.3 補救教學

以教學歷程來說，最常見的就是 Glaser(1962) 所提出的基本教學模式，補救教學可以說是一種「評量—教學—再評量」的教學模式，但強調的是循環的歷程。常見的補救教學方式有以下幾種[4]：一、資源教室；二、學習站；三、學習實驗室；四、套裝學習材料；五、電腦輔助教學。

本研究擬採用的是電腦輔助教學的方式，並與

傳統教學模式做比較。隨著資訊科技的進步，個人電腦已逐漸普及和大眾化，不僅許多家庭擁有電腦，各級學校也都設有電腦教室，電腦已成為教學的主要媒體之一。不僅提高個別化教學的可能性，也為補救教學的實施提供了另一種可行的管道。運用教學科技的學習活動，適合少數個別化教學及較差的學生；因為教學科技的運用能營造積極主動的學習態度，增進低成就學生的成功經驗。

另一方面，國外學者Slavin [5]；McLaughlin & Vacha [6] 指出，補救教學的策略有以下幾種：一、直接教學法（the direct instruction）；二、精熟教學(the mastery teaching)；三、個別化教學(the individualized instruction)；四、合作式學習(the cooperative learning)。本研究採取的是個別化教學的策略。所謂個別化教學(individualized instruction)與個別教學不同；它是一種教學的策略，其目的在打破僵化的班級教學，達到創新教學設計，靈活教學活動，適應個別差異的效果[7]。

2.4 網路學習模式與網路學習平台

網路學習模式，大致可分為：同步式、非同步及混合式網路學習模式等三類[8]：(1) 同步式網路學習模式：是一種老師和學生在相同時間、不同地方進行教學的網路學習模式;(2) 非同步網路學習模式：是一種允許老師和學生在不同時間、不同地方進行教學的網路學習模式;(3) 混合式網路學習模式：是老師視教學需要，實際結合同步與非同步的一種網路學習模式。

其次，網路學習平台，大致可分為學習管理系統、學習內容管理系統、串流影音系統和同步教學系統等四種類型[9]。本研究所指的網路學習平台是指以Moodle所架設的「數學科補救教學網路學習平台」，透過有效管理之網路平台，具體協助教師之教學，使教師能利用此平台進行網路教學活動，藉以達到教學之目的。平台上除提供教師放置數位教材之外，還提供課程資訊、教材管理、線上測驗、作業繳交、成績統計、互動討論等功能。

3. 研究方法

3.1 研究設計與流程

本研究為瞭解本校六年級學生對網路學習平台的感受及其與補救教學之間的關係，採用準實驗研究法進行研究。實施步驟簡述如下:

步驟1：蒐集國內外有關網路學習及補救教學相關之文獻，進行閱讀與統整，作為本研究之理論基礎。

步驟2：選取國小數學科分數相關教材單元作為補救教學的內容，編製成適合本研究之研究工具，進行補救教學實證研究。

步驟3：按照前測 → 補救教學 → 後測之順序進行實驗，先後進行前測、「分數的乘法」補救教學及後測；本研究分兩組進行，甲班（實驗組）採網路平台學習方式，乙班（對照組）則採傳統補救教學方式，以了解不同方式之成效，實驗設計如表3所示。

步驟4：後測之後，針對甲班（實驗組）學生，再施以問卷調查，以了解學生對網路學習平台的感受。

步驟5：最後，根據兩組受試者的前後測結果進行統計分析，以瞭解網路平台學習與傳統教學在補救教學的成效上是否有差異

表3 補救教學實施方式（採準實驗研究法）

主題	組別	對象	教學方式	前測	後測
分數的乘法	網路組（實驗組）	甲班	Moodle平台教學	O1	O3
	傳統組（對照組）	乙班	課堂教學	O2	O4
備註	O1、O2為前測分數；O3、O4為後測分數。				

兩組學生進行前測後，傳統組的學生由該班老師在班級進行補救教學，並作學習單的練習，針對同學錯誤的題目和相關的概念做講解。利用一週（五天，不含週末），每天30分鐘的時間做練習和討論。最後再進行後測，並記錄各個學生前、後測的答對題數。

網路組的學生則一樣利用一週（五天，不含週末），每天30分鐘，利用中午午休，到電腦教室進行網路平台補救教學。補救教學計畫如表4所示。

表4 補救教學實施計畫表

星期 / 組別	一	二	三	四	五
網路組（實驗組）	前測卷＋影片 1＋學習單 1	影片 2＋學習單 2	影片 3＋學習單 3	影片 4＋學習單 4	影片 5＋學習單5＋後測卷
傳統組（對照組）	前測卷＋學習單 1	學習單 2	學習單 3	學習單 4	學習單5＋後測卷
備註	傳統組的學習單，請任課教師做簡單的檢討；網路組則不做檢討，僅做網路影片教學。				

3.2 研究對象

本研究之對象為本校六年級兩個班，在數學科補教教學篩選測驗中未達 60 分的學生，其中甲班全班 3 位學生，3 位學生未通過；乙班全班有 9 位學生，9 位學生均未通過。換句話說，兩個班級的全部學生均需參加補救教學；因此，參與本研究的學生一共有 12 位。

3.3 研究工具

本研究使用的工具包括Moodle網路學習平台、YouTube教學影片、前測卷、後測卷、學習單，以及問卷等，分別說明如下：

一、 Moodle網路學習平台



圖2 Moodle補救教學課程選單
http://163.19.57.131/moodle/

二、 YouTube教學影片



圖 3 分數的乘法教學影片

三、 前測卷、後測卷

為了解學生的起點行為，以及接受補救教學後的成效，分別製作前測卷與後測卷。以「分數的乘法」為內容，分別進行傳統課堂式以及網路平台式的補救教學，以作為對照和比較。製作的原則係從題庫中挑選合適的題目，根據單元內容，平均分配題目，題目的難易度屬中間偏易。後測卷和前測卷屬相同的題型，僅作數字和題號的改變。避免前後測因難易度差異太大而影響到測驗的信度與效度。

四、 學習單

在每一次的補救教學活動結束後，都會發一張學習單，一方面驗證是否學會，一方面作為練習之用。這些學習單是教育部委託專家依據「數學學習領域補救教學基本學習內容」編製而成的，每一張包含一個概念，除了問題情境與解題引導外，也提供題目供學生練習，希望透過一個概念銜接一個概念的學習方式，澄清學生的迷思概念，補強學生的基本能力。這些學習單就放置在教育部「國民小學及國民中學補救教學資源平台」[10]，免費供老師下載使用，是很方便、很好用的補救教學教材。

五、 問卷

補救教學結束後，讓網路組學生填寫「國小數學第十冊-分數的乘法補救教學活動後感受與滿意度調查問卷」，藉以了解學生對於網路學習平台的態度以及接受程度，以作為研究分析與未來教學之參考。

4. 研究結果與分析

4.1 網路式與傳統式補救教學之比較

為了解網路平台式補救教學與傳統課堂式補救教學的差異性。於是採用準實驗研究法，分兩組（班）同時進行，甲班學生採用網路平台式補救教學，乙班學生則採用傳統課堂式補救教學，分別由該班導師擔任教學者。首先，先分別進行前測，其次，由兩班導師分別進行為期一週（五天）之補救教學，教材單元為「分數的乘法」，內容分為：「分數乘以整數」、「整數乘以真分數」、「真分數乘以真分數」、「帶分數和假分數的乘法」、「分數的分配律」等五個小單元，每天分別進行三十分鐘之網路平台學習及傳統課堂教學，課程結束後，再分別進行後測，得到的前、後測結果如表5、表6所示：

表5 網路平台補救教學前、後測成績摘要表（N=3）

	S1（小梅）	S2（小麗）	S3（小恩）	平均
前測	25	25	15	21.7
後測	40	35	15	30.0

表6 傳統課堂補救教學前、後測成績摘要表（N=9）

	S4	S5	S6	S7	S8	S9	S10	S11	S12	平均
前測	25	80	35	50	95	45	25	20	70	49.4
後測	75	90	25	90	95	80	40	85	60	71.1

為了解補救教學後兩組學生在「分數的乘法」單元成績上的差異，本段將分別針對網路組與傳統組學生「分數的乘法」前、後測成績進行成對樣本t檢定，藉以分析兩組學生在補救教學前後，在「分數的乘法」單元的成績表現上是否有顯著差異。

表7 網路組與傳統組補救教學前後測分數成對樣本t檢定對照表

組別	人數	前測 a		後測 a		t 值	P 值
		平均數	標準差	平均數	標準差		
網路組（甲班）	3	21.67	5.774	30.00	13.229	1.890	.199
傳統組（乙班）	9	49.44	26.745	71.11	24.467	2.404	.043*

*p<.05

網路組學生人數為3人，在「分數的乘法」測驗前測平均分數為 21.67分，標準差為5.774分；後測平均分數為 30.00分，標準差為13.229分。後測的平均分數比前測提高了8.33分，前後測成績的成對樣本 t 檢定的結果，p = .199 ＞ .05，表示網

路組前、後測分數未達顯著差異；傳統組學生9人，在「分數的乘法」測驗前測平均分數49.44分，標準差為26.745分；後測平均分數71.11分，標準差為24.467分。後測的平均分數比前測提高了21.667分，前、後測成績的成對樣本 t 檢定的結果，p = .043＜.05，表示傳統組前後測分數達顯著差異。

根據前面的統計分析，雖然我們得到的結果是網路組前、後測分數未達顯著差異，而傳統組前、後測分數則有達到顯著差異。但我們若以兩組學生的前、後測進步率來做比較的話，會發現兩組學生的成績均有明顯的進步，而且相差並不多（網路組進步率38%，傳統組進步率44%），如下表8所示。

表8 兩組學生補救教學前後測進步分數對照表

	人數	前測 平均分數	後測 平均分數	進步 平均分數	進步率
網路組（甲班）	3	21.67	30.00	8.33	38%
傳統組（乙班）	9	49.44	71.11	21.67	44%

4.2 學生問卷調查回饋分析

經過補救教學之後，研究者給予網路組學生填寫「國小數學第十冊-分數的乘法補救教學活動後感受與滿意度調查問卷」，每一個問題有五個選項，分別是：（1）非常同意（2）大致同意 （3）有些同意 （4）大致不同意 （5）非常不同意，藉以了解網路組學生對於網路平台式補救教學的感受以及滿意程度。透過問卷調查，可以進一步了解學生對於網路式補救教學的態度和看法，以作為未來研究與教學之參考。

表9 網路式補救教學感受量表統計結果

問題1)	我覺得「分數的乘法」課程難易度適中。
人數	（1）1（2）2（3）0（4）0（5）0
百分比	（1）33%（2）67%（3）0%（4）0%（5）0%
問題2)	我覺得網路教學方式比較能夠引起我的興趣。
人數	（1）2（2）1（3）0（4）0（5）0
百分比	（1）67%（2）33%（3）0%（4）0%（5）0%
問題3)	我覺得網路教學方式，我比較沒有壓力。
人數	（1）1（2）2（3）0（4）0（5）0
百分比	（1）33%（2）67%（3）0%（4）0%（5）0%
問題4)	我覺得網路教學方式，我比較聽得懂。
人數	（1）2（2）0（3）1（4）0（5）0
百分比	（1）67%（2）0%（3）33%（4）0%（5）0%
問題5)	進行網路補救教學時，我會覺得心煩。
人數	（1）1（2）0（3）2（4）0（5）0
百分比	（1）33%（2）0%（3）67%（4）0%（5）0%
問題6)	我覺得網路影片教學的速度適中。
人數	（1）1（2）0（3）0（4）2（5）0
百分比	（1）33%（2）0%（3）0%（4）67%（5）0%
問題7)	我覺得網路教學的補救教學比較適合我。
人數	（1）1（2）2（3）0（4）0（5）0
百分比	（1）33%（2）67%（3）0%（4）0%（5）0%
問題8)	經過網路補救教學，我進步比較多。
人數	（1）0（2）3（3）0（4）0（5）0
百分比	（1）0%（2）100%（3）0%（4）0%（5）0%

表9顯示，甲班學生經過「網路式」補救教學後，覺得「分數的乘法」課程的難易度大致適中（67%）、非常同意網路教學方式能夠引起學生的興趣（67%）、覺得網路教學方式大致上沒有壓力（67%）、非常同意網路教學方式比較聽得懂（67%）、網路教學方式會覺得有些心煩（67%）、覺得網路教學的速度不夠適中（67%）、覺得網路教學方式大致（67%）和非常（33%）適合、大致同意經過網路補救教學後進步較多（100%）。

綜而言之，甲班學生在經過「網路式」補救教學之後，接受程度頗高。尤其是非常同意這樣的方式能夠引起他們的興趣、也比較聽得懂；也大致同意這樣的方式比較適合他們、同時進步較多。

4.3 個案學生答題分析

經過補救教學實驗之後發現，學生S1的進步幅度頗大，令人驚喜； S2也有進步，但是S3則完全沒有進步，如下表10所示。此一結果，引發研究者的好奇，想進一步探究其原因。

表10 甲班補救教學前後測個人進步分數摘要表

	前測	後測	進步分數	進步率
S1（小梅）	25	40	15	60%
S2（小麗）	25	35	10	40%
S3（小恩）	15	15	0	0%

由於前測卷與後測卷題型相同，僅作數字和題號的改變；因此，研究者想從試題分析的角度對甲班學生作個案的分析，探討其中可能的原因。於是研究者根據題型，整理出兩位個案學生的前、後測答題情形對照表，如下表11、12所示。

表11 甲班學生S1前、後測答題對照表

小單元名稱	前測題號	S1（小梅）	後測題號	S1（小梅）
分數乘以整數	6	X	5	X
	7	X	17	X
	14	○	12	X
	18	○	3	X
	20	X	1	○
整數乘以真分數	2	○	14	○
	17	X	16	X
真分數乘以真分數	4	X	7	○
	10	X	8	○
	16	X	2	○
	19	X	4	○
帶分數和假分數的乘法	3	X	18	X
	8	X	10	X
	11	X	11	X
	12	○	19	X
	13	X	20	X
	15	X	15	○
分數的分配律	5	X	6	X
	9	○	9	X
綜合題	1	X	13	○
合計答對題數		5		8

※上表中○表示答對，X表示答錯

表12 甲班學生S3前、後測答題對照表

小單元名稱	前測題號	S3（小恩）	後測題號	S3（小恩）
分數乘以整數	6	×	5	×
	7	○	17	×
	14	×	12	×
	18	×	3	○
	20	×	1	×
整數乘以真分數	2	×	14	○
	17	×	16	×
真分數乘以真分數	4	×	7	×
	10	×	8	×
	16	×	2	○
	19	○	4	×
帶分數和假分數的乘法	3	×	18	×
	8	×	10	×
	11	×	11	×
	12	×	19	×
	13	×	20	×
	15	○	15	×
分數的分配律	5	×	6	×
	9	×	9	×
綜合題	1	×	13	×
合計答對題數		3		3

※上表中○表示答對，X表示答錯

S1小梅的部分，根據表11，我們發現，在「真分數乘以真分數」小單元中，前測時，小梅四題全部答錯；到後測時，卻四題全部答對。由此可知，就「真分數乘以真分數」部分而言，小梅的答對率是100%，可說完全學會；換句話說，這一部分的網路平台補救教學是有成效的，這也可以說是小梅後測進步最多的原因所在。至於，其他小單元部分，答對的題目都是零星的，甚至有的題目前測答對，後測卻答錯，前測與後測之答題結果，幾乎沒有相關；可能是學生似懂非懂，也可能是完全沒有學會。

S3小恩的部分，根據表12，我們發現一個有趣的現象：前、後測各20題，小恩各只答對3題，小恩所有前測答對的題目，到了後測全部答錯；而後測答對的題目，前測時則又全部答錯。此一結果顯示，小恩答對的題目似乎全憑猜測，並非真的了解；也顯示補救教學在小恩的身上並無成效。

綜合以上的分析，我們可以診斷出個案學生，那些單元已經學會，那些單元還沒有學會。已經學會的單元則不必再做補救教學，至於還沒有學會的單元，則可以安排學生再接受網路平台補救教學，重複練習，不受時空及次數的限制，這是傳統教學做不到的地方。

5. 結論與建議

5.1 結論

根據前面的研究結果與分析，我們提出以下三點結論：

一、大致而言，網路平台式補救教學仍有一定的成效。雖然根據實驗及統計分析的結果，網路式補救教學的成效沒有比傳統式補救教學來得顯著。但根據表8，若以進步率來做比較，網路平台式補救教學仍有一定的成效。

二、學生對於網路平台式補救教學抱持正面的態度和看法。根據表9，學生認為：（一）網路教學的方式比較能夠引起他們學習的興趣；（二）網路教學的方式，他們比較聽得懂；（三）網路式的補救教學方式比較適合他們。

三、網路學習平台具有個別化及適性化的特性，有助於補救教學。根據表11、12的答題分析，我們能夠找出學生的盲點；只要針對尚未學會的部分，進行補救教學，不需要重複已經學會的部分，也不需要進行「大鍋飯」式的補救教學。

5.2 建議

根據前面的結論，本研究提出幾點建議，供數學科教學者作參考，希望能夠對日後的數學科補救教學有所助益。

一、 重視補救教學：根據研究的結果，整體而言，接受補救教學的學生，不論是傳統組或網路組，成績皆有所提升；可見只要實施補救教學，學生都有進步的可能。因此，建議數學科教學者，千萬不要放棄學習低成就的學生。

二、 重視個別化與適性化：接受補救教學的學生，雖然整體而言，成績有所提升，但是個別來說，卻也有原地踏步，甚至不進反退的情形。可見，沒有一體適用的方法；雖然是「補救有益」，但也要講求方法。針對數學科低成就的學生，必須了解其學習盲點以及迷思概念，才能夠「對症下藥」，給予個別化的教學以及適性化的輔導。

三、 重視數位學習：雖然本研究的結果顯示，「網路式」補救教學不如「傳統式」補救教學來得有成效；但根據學生問卷的回饋可以發現，學生對於網路平台式教學的接受度很高。姑且不論其成效，光從引發學生的學習動機，提高學生的學習興趣而言，網路式學習還是有其長處。我們不否認，傳統式補救教學有其一定的效果；但若能結合網路式學習，相信會有加乘的效果。

參考文獻

[1] 台灣 PISA 國家研究中心（民 102）。關於 PISA。取自 http://pisa.nutn.edu.tw/pisa_tw.htm

[2] 台灣 PISA 國家研究中心（民 102）。台灣 PISA 2009 精簡報告。取自 http://pisa.nutn.edu.tw/download_tw.htm

[3] 許添明（民 102）。影響我國偏遠與非偏遠地區國中學生學業成就之教育資源研究。行政院國家科學委員會專題研究成果報告（編號：尚未公開），未出版。

[4] 張新仁、邱上真、李素慧(民 89)。國中英語科學習困難學生之補救教學成效研究。教育學刊，16 期，163-191。

[5] Slavin, R. E. (1989). Student at–risk for school failure. In R. E. Slavin, N. L. Karweit, & N. E. Madden (Eds), Effective programs for students at-risk (p.3-19). Boston: Allyn & Bacon.

[6] McLaughlin T. F., & Vacha, E. F. (1992). The at-risk student: A proposal for action. Journal of instructional psychology, 19, 66-68.

[7] 吳清山（民 86）。初等教育。台北市：五南。

[8] 資策會教育訓練處講師群（民 92）。數位學習最佳指引。台北市：財團法人資訊工業策進會教育訓練處。

[9] 黃國禎、蘇俊銘、陳年興（民 101）。數位學習導論與實務。新北市：博碩文化。

[10] 教育部國民中小學補救教學資源平台 http://asap.moe.gov.tw/

語意網在偏鄉遠距課輔教材分享上的應用

溫敏淦　　樂美邑　　陳博智
國立聯合大學 資訊管理學系
brianyuehmi@gmail.com

摘要

都市化的全球趨勢，讓城鄉差距越來越明顯，除了早已眾所周知的經濟環境落差外，人類社會賴以拉近知識及社經地位差距的教育環境，也在少子化浪潮下，城鄉有了更大的機會差異。都市學生在享有學校相對完善的教學資源時，偏鄉卻因不具經濟規模、教師高流動性及缺乏正式合格教師下，在學習上產生立足點的不平等；另外因青壯人口往都市移生，造成偏鄉隔代教養情況普遍存在，對學童學習的督促與協助往往心有餘力不足，再加上課後補習輔導及補救學習機會闕如，讓偏鄉在學習起點上失去了許多的機會。這樣的現象不但形成偏鄉個別學童弱勢世襲複製的悲劇，也讓一些本該受學校教育保護的孩子，因學習障礙產生對學校的排斥而產生價值觀偏差、最終讓社會為此付出難以估算的代價。

社會落差的改善，除了政府政策制定推動的力量外，社會關懷的民間力量也是極重要的一環，而針對偏鄉中學以下的課業輔導，為了克服空間距離的限制，使用遠距一對一線上課輔是一個極為可行的方案。現代公民使用資訊及網路的能力已是基本的要求，政府為了弭平數位落差(digital divide)，早已投入大量的經費建置偏鄉的硬體設備，此時結合大學生豐沛人力及多元知能的特質，不但可以讓教育落差改善，大學生對偏鄉學童的關懷，容易形成學習典範的效益，同時提供偏鄉學童文化刺激的機會，同時大學生也有機會更瞭解社會不同族群的思維面向，促進社會的包容理解與和諧。

在推動偏鄉遠距課輔5年的觀察中發現，大學生對於偏鄉伸出援手雖然有極大的意願，但因需持續長期投入時間及心力，大學生對己身時間支配未臻成熟，加上對教學能力也無充分信心足以勝任，往往造成偏鄉遠距課輔的不穩定性，讓關懷的美意大打折扣。本文即探討以資訊工具協助從事課輔服務的大學生，以互助分工方式，分享課輔教材，讓大學生備課壓力降到最低，也容易形成課輔教學經驗的傳承分享，讓大學生有做好事的心，也有把事做好的能力。本研究旨在探討資訊科技在偏鄉課輔的協助與應用，針對國中小學數位學習教材的資源擷取，設計了一個以九年一貫課綱為基礎的語意詞彙表本體論(RDFS/OWL)，做為開發一個有效率的數位學習資源擷取系統根據。

關鍵詞：數位學習、資源擷取、語意網。

1. 動機與目的

學習是人類不斷進步發展的原動力，在這個多元的社會中，學習更是以各式各樣的方式進行著，只要能因勢利導、運用良好的資源，以有效的方式進行學習，就能有好的效用。數位學習便是在網路數位化的社會中因應出現的一種學習，具有許多面向及定義。以現在對網路使用的普及，所有的學習活動很難不使用到與數位學習相關的技術及概念[1]。教育部於95 年開始試辦推動「偏鄉地區中小學網路課業輔導服務計畫」，運用遠距教學的方式，由大學生在網路上輔導偏遠地區的國中小學學生，以提升偏遠地區學生的學習成效。

為了要改善數位落差，社會關懷的力量促使許多大學生積極參與遠距課業輔導。聯合大學參與了教育部偏鄉遠距課輔計畫，由大學生陪伴偏鄉學童進行一對一遠距數位學習。由於課輔教師是大學生，要帶領學童學習，充分備課是必要的要求，但大學生忙於課業或其他活動，相對能準備的時間較不充分，尤其是長達整個學期的課輔歷程，要能夠持之以恆的每週完整準備教材來教學也是極不容易達成的要求。為了協助課輔的順利進行，也為了減輕非專業師資的大學課輔學伴，我們設計了一個能夠快速的搜尋並且分享教材的平台，讓上課用的課本、課輔老師自製教材等，能有效容易的分享及擷取。這樣不僅能夠讓課輔老師快速取得教材資源，還能夠讓課輔老師自製的教材、經驗能夠傳承下去。

在搜尋擷取資源的過程中，人們大都利用搜尋引擎或直接到相關特定網站下載資源，然而多數情形下不清楚可以利用資源的所在，加上有時又不容易清楚以關鍵字表示需求，因此往往找不到所需的資料。在這個經驗中，若這些散佈分散的資源如果有明確清楚註解描述，就可以更有效率地協助需求者擷取運用。

雖然搜尋引擎的能力十分強大，但許多人也發現關鍵字的搜尋結果常常與使用者的搜尋意圖不相符合，因此有些搜尋服務開始提供分類搜尋。分類搜尋雖然讓搜尋結果某種程度的提升符合使用者需求，但仍有相當努力空間。因此本文運用語意網的技術，將大量的文件借

由適當的後設資料標註，並以資源描述架構(Resource Description Framework, RDF)[2]的資料形式做為擷取資源的依據。這不但可以對現有的大量文件資料加以補充註釋或是評論推薦，也能讓擷取資源的課輔老師及學童獲得更高的方便性。

2. 研究方法

2001 年 Tim-Berners Lee 提出語意網的概念(Tim-Berners Lee, 2001)[3][4]，目的在於建構一個更容易讓機器可以處理的資料網(Web of Data)。藉由語意網的技術，大量的文件可以藉由適當的後設資料標註，並以 RDF(Resource Description Framework)的資料形式提供網路擷取者搜尋，以更精確的搜尋到所需的文件資料。利用語意加註，數位資源可以具有能夠讓機器直接存取的語意資料，就可以提供明確的語意搜尋指引或提供更多的線索進行資料發掘。

為了提供課輔大學生一個方便取得教學資源的工具，我們的想法是讓網路上有關國中小學的數位學習資源都能有一個明確的語意描述，然後以語意查詢(Sparql Query)，對這些描述資料作查詢，以獲得符合需求的結果。Sparql Query 是一種用於 RDF 上的查詢語言，類似我們熟悉的 SQL Query。而資源描述架構(RDF Schema,RDFS)則提供了知識的基本要素來描述本體。

系統中首先定義一套 RDFS(RDF Schema)詞彙表，並在詞彙表中定義學習資源的屬性，如：標題、科目、主題、能力指標、資源類型、作者、出版社、上傳者、日期等。其中科目是指國文、英文、數學等，主題則是如：數與量、幾何、代數、機率等概念。在主題下面我們依據九年一貫課綱設計了能力指標。此外為了利用使用者資料以及資源使用情況的紀錄，我們也定義了使用者、存取紀錄、書籤等詞彙，這個詞彙定義表我們是以 RDFS 來完成。由於是以九年一貫課程的能力指標為對象，因此命名為 K9LR(K9 Learning Resource)。接著，我們利用定義的 K9LR，對目標資源擷取出 RDF 資料。目標資源包括了網路上可存取的資源(以一個 URL 形式表示)以及我們課輔進行中所上傳的檔案資料。

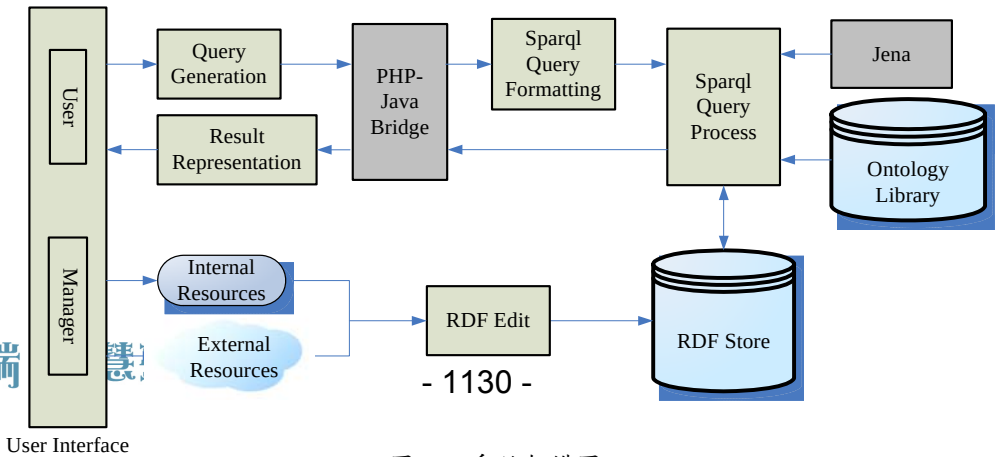
而在上傳及搜尋資源的部分，我們的系統架構如圖 1，可依照年級、領域、資料類型進行資源的搜尋、並在搜尋到資料後再找尋出相關的教材資源並顯示於頁面中，方便使用者做搜尋。新增教材資源的功能，可以讓使用者上傳相關教材的檔案、網站、影片、動畫等。在教材資源的提供者新增 URL 時，必須填寫對教材資源相關的描述，以讓其他使用者更容易找到所提供的教材資源。

教材搜尋者透過輸入介面輸入想要搜尋教材資源的方式後，系統將收到使用者送出的訊息，系統啟動 Query Generation 以得知使用者所選的分類項目，經由 PHP-Java Bridge 傳送相關參數到後端的 Sparql Query Formatting 模組轉換。再由 Sparql Query Process 處理 Sparql Query。由於 K9LR 使用了 OWL 本體論，因此這個 Sparql Query 是含有 RDFS/OWL 推論的查詢。最後由 Result Representation 將後端傳回的相關資料，依照使用者的權限，篩選其權限可觀看的內容，再以表格及圖形的形式呈現給使用者。

在 K9LR 的本體論設計上，我們以國中小學的數位學習資源為例，以語意網概念及技術，提出一個方法論並建置一個查尋系統。

RDF 是語意網的基礎，其內涵就是在作資源的描述，然而如何讓這些資源的描述具有明確的語意，就需要一個明確定義的詞彙表，或稱之為 RDF Schema。因此我們的第一個工作就是要建立適合描述國中小學習資源的詞彙表 K9LR(K9 Learning Resources)，然後讓網路上的國中小學習資源都能有一份 K9LR 描述。在 K9LR 的定義中，我們也需加入一些本體論的設計，以便在進行查詢時，能有較為高階的查尋功能。K9LR 本體論示意如圖 2。

在設計 K9LR 本體論時，主要使用史丹佛大學研發的 Protégé 4.1 Ontology 編輯器，利用這個工具，我們將能檢查本體論的邏輯並協助我們完成標準 OWL 檔案。接著我們需設計幾個網頁工具，用來對遠距課輔計畫的學習資源庫，以及依課輔老師的擷取經驗所獲得的線上國中小數位學習資源，以自動/半自動方式產生 K9LR 描述(RDF triples)，並且匯入到所建置的 RDF store 中。圖二中，我們設計出來的本體論架構是以資源為中心，並且建立出每個節點間的描述，例如：資源以及資源類型的描述為"資源有資源類型"。而節點間的描述主要



有三種關係，分別是：本研究所定義的 dlp(用於描述本體論語意資訊)、以及由 Mikael Nilsson 等人所定義的 DublinCore(dc)[5]，和 Dan Brickley, Libby Miller 所定義的 friend of a friend(foaf)[6]。K9LR 共設計了 12 個 Classes 如表一，Properties 則共有 28 個，其中 14 個為 object properties 如表二，14 個為 data properties 如表三。

表一 Classes of K9LR

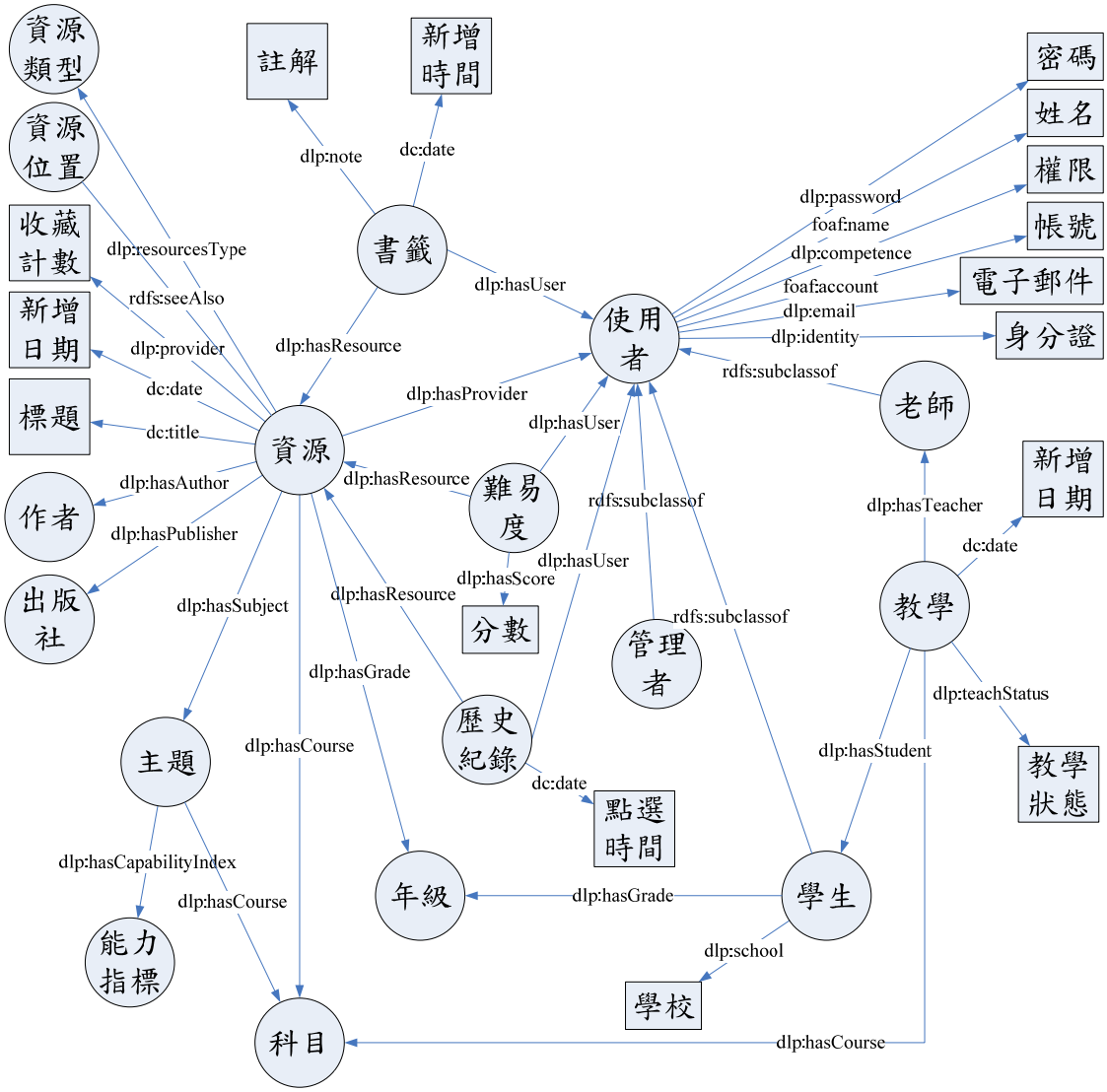
Class	Description
難易度(Diffcoult)	同類型教材的難易度。
藏經閣(BookMark)	建立標籤。
能力指標(CapabilityIndex)	所有的能力指標。
科目(Course)	課程，國、英、數。
歷史紀錄(HistoryRecord)	記錄歷史的資料。
作者(Creater)	作者。
出版社(Publisher)	出版社。
資源(Resource)	因為需對所上傳的教材附加詳細的語意。
資源類型(ResourceType)	資源型態，包括文件、圖片、影片、聲音、網頁。
主題(Subject)	主題，包括幾何、代數、聽、說、讀、寫等。
教學(Teach)	記錄教學狀態。
使用者(user)	所有的使用者，包括管理者、學生、老師。

表二 Object Properties of K9LR

Object Properties	Description	Domains	Ranges
BT	為更廣泛	Subject	Course
NT	是 BT 的反義詞，更狹隘	Subject	CapabilityIndex
hasCapabilityIndex	能力指標	Resource	Course
hasCourse	對應課程	Resource	Creator
hasCreator	作者	Resource	Grade
hasGrade	年級	User	Resource
hasPost	主要是用於能力指標的前後(教材的深淺)關係。	User	Resource
hasPrevious	為 hasPost 的反義詞	Resource	User
hasPublisher	出版社	Resource	Publisher
hasResourceType	資源型態	Resource	ResourceType
hasResource	對應資源	BookMark HistoryRecord Diffcoult	Resource
hasStudent	學生	Teach	Student
hasSubject	主題	Resource	Subject
hasTeacher	老師	Teach	Teacher

表三 Data Properties of K9LR

Object Properties	Description	Domains	Ranges
score	分數：主要是在教材的難易度做評分	Difficult	string
title	教材的標題	Resource	string
account	使用者的帳號	User	string
address	使用者的地址	User	string
competence	使用者的權限	User	string
date	日期	Resource BookMark	string date
email	使用者的 Email	User	string
education	學生的教育程度	Student	string
grade	使用者的年級	Student Resource	string int
name	使用者的名字	User	string
password	使用者的密碼	User	string
subject	主題	Resource	string
telephone	使用者的電話	User Publisher	string
note	書籤的註解	BookMark	string



圖二、K9LR 本體論示意圖

3. 實做成果

我們設計的目標是為了分享資源、減輕課輔老師的備課負擔以及提升使用者學習的效率，而我們為了方便尋找教材，設計的平台包括了上傳、下載、分享等功能。我們依照年級、科目、資料類別等方式搜尋教材。並且為了讓課輔老師和學童建立關係進而追蹤學童上課進度，系統也建立了一個上課清單的頁面，方便老師了解學生學習的狀況如圖 3。圖右方的藏經閣可以收藏課輔教師需要的教材，以便再次使用；圖左方的教學資源，可以讓使用者快速依照年級、科目、資料類別，以點選分類的方式搜尋所需要的教材，授課清單的部分，可以讓課輔老師跟學童建立關係，進而追蹤學童上課進度，圖左方的教學資源上傳可以上傳教材並且分享、增加平台的學習資源；圖左下方是進路圖，它分為三個部分，中間最大的圈圈，是學童目前的學習進度，根據箭頭的指向，可以知道左方是他學習過的上一個課綱進度，右方是學童需要學習的下一個課綱，讓課輔老師能知道學童的學習狀況及進度。

本系統提供三種搜尋教材資的方法。第一種搜尋方式是以輸入的詞彙為基礎，加上下拉式選單的輔助功能讓使用者能更快速的找到正確的關鍵字，方便取得所需的資源，示意如圖 4。

第二種搜尋方式是藉由點選年級、科目、資料類別的方式分類檢索，示意如圖 5。使用者能直覺的找到所需要的學習資源，達到學習的目的，在點選完之後可以看到學習資源列表，示意如圖 6。

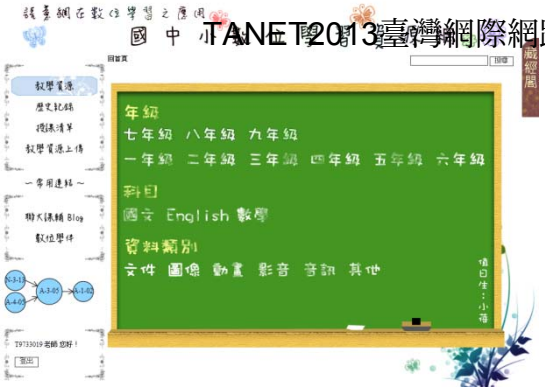


圖 3、系統瀏覽畫面

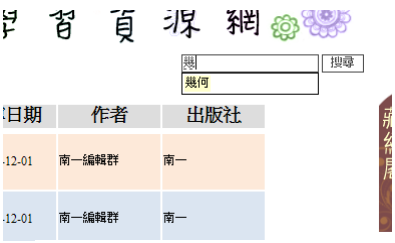


圖 4、相關詞彙搜尋



圖 5、分類檢索式搜尋



圖 6、資源列表瀏覽畫面

第三種搜尋方式是依據九年一貫課綱的相關性，設計了一個進路圖式的搜尋方式。進路圖是為了讓使用者可以依照目前所學習到的進度，可以搜尋上一個課綱或是下一個課綱的相關學習資源，來進行複習或是預習的相關操作，藉此達到學習的目的，示意如圖 7 的左下角。

另外上傳功能能夠讓課輔老師把自己撰寫或取得的資源分享出來，且為了讓其他課輔老師及學童能夠迅速的就學習進度找到此資源並加以利用，因此我們加入九年一貫能力指標的選項並建立能力指標的前後關係，示意如圖 8。在填入屬性後，可以方便學童以及課輔老師搜尋。

藉由上傳所取得的學習資源資料，提供了一個可以讓使用者能方便的了解到此資源的相關訊息，並能進行收藏、下載、尋找簡單一點、更多一點或是更難一點的相關操作。在管理學習資源上，系統也建置了一個讓課輔老師對教材進行難易度評分的功能，對同一指標內的教材作區分，示意如圖 9。

學生在學習時，總會想要搜尋適合自己的學習資源，搜尋這種資源時，搜尋的流程或記錄方式總是很麻煩，因應這樣的情況，在頁面設計時，加入了收藏功能，收藏之後，在下次使用者登入，只要在頁面右方的藏經閣，就能很方便的找到之前收藏的資源並學習，在使用者作收藏時，我們後台也會進行資源收藏的統計，當使用者在搜尋某個資源時，我們便能根據收藏時所進行的統計數據，推薦給使用者。

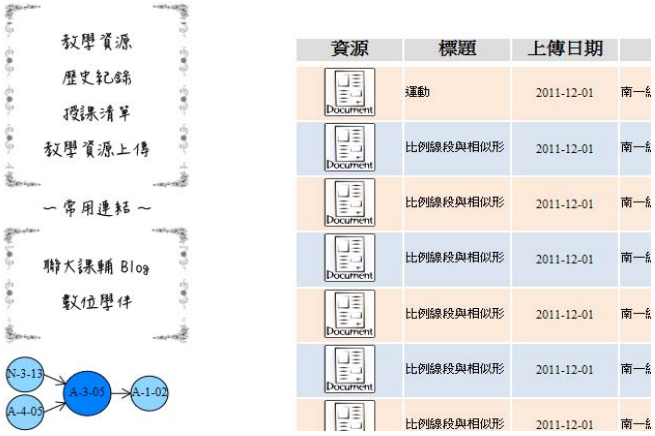


圖 7、進路圖瀏覽畫面



圖 8、上傳資源瀏覽畫面

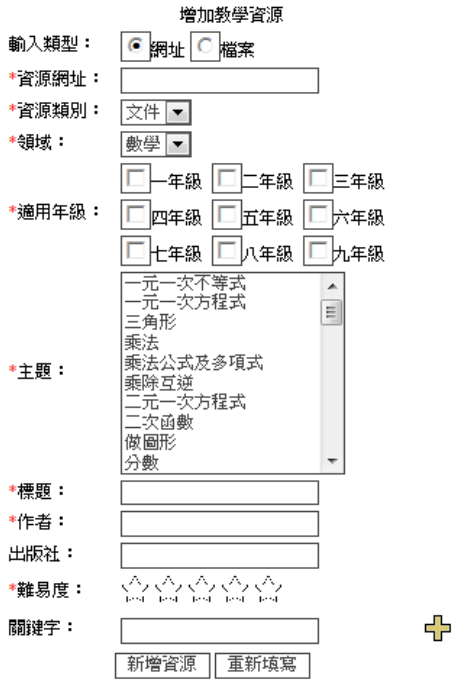


圖 9、上傳資源瀏覽畫面

4. 結論與討論

由於全球資訊網的普及，讓資源分享以及網路的服務及應用更為方便，而我們也了解到城鄉的學習差距很嚴重，雖然教育部已經推行偏鄉課輔的計畫，也有許多的志工參與這樣的活動，讓城鄉差距能夠稍微得到改善，但是要有更好的學習環境以及資源，才能夠做更大的改變，因此建立了這樣的學習平台，設計一個資源管理以及擷取的系統，希望能夠將這些技術用在偏鄉關懷活動中。

我們設計一個以九年一貫課綱為基礎的本體論— K9LR，定義了一些學習資源描述的語意詞彙，並以此詞彙開發我們的 RDF 擷取工具，用來對上傳的資源以及可取得的網路資源擷取出 RDF 資料。這些資料以 Jena 的 RDF Store 儲存。另外，我們藉助了一個本體論編輯工具 Protégé編輯並將 K9LR 以 OWL 的格式匯入到 Jena 的模型中。

利用 Jena 的 SPARQL 引擎及 RDFS/OWL 推論引擎，我們設計開發資源查詢核心，這個核心能夠利用 Ontology library 提供的領域知識，對使用者的需求提供有推論的查詢。為了發揮推論查詢的優點，我們在介面設計上，盡量提供提示引導的環境，讓使用者可以更能發掘所需的資源。

雖然完成這個資源擷取系統雛型建置，但系統仍有許多改善的空間。首先，目前僅對在系統中上傳的資源產生 RDF 資料，我們希望對網路上的其他資源也能有類似的語意描述，如此就能更進一步擴大系統的可使用性。因此，若能在未來設計自動化的 RDF 資訊擷取(information extraction)工具，就能讓我們的系統更充分的發揮效用。其次，在可使用的提示擷取介面的設計上，高度視覺化的設計將幫助系統取得更符合使用者意圖的資訊來產生語意查詢語句，並依此進行語意查詢，因此我們的設計視覺化應該再做更好的設計。

整體而言，我們應用了語意網的連結資料及本體論的推論，在一個我們建置的學習資源典藏系統中，以視覺化、提示性的介面讓使用者能夠更方便的擷取學習資源。

參考文獻

[1]陳年興、楊錦潭，民 95，「數位學習理論與實務」，博碩文化。

[2] O. Lassila, R.R. Swick (Eds.), Resource description framework (RDF) model and syntaxspecification, W3C Recommendation, 22 February 1999,

http://www.w3.org/TR/REC-rdf-syntax

[3]Tim Berners-Lee.Hendler, James; Lassila, Ora(17 May 2001). "The Semantic Web".Scientific American.

[4] Tim Berners-Lee. Linked Data - Design Issues, 2006.http://www.w3.org/DesignIssues/LinkedData.html.

[5] Mikael Nilsson, Andy Powell, Pete Johnston, Ambjörn Naeve , 14 January 2008

http://dublincore.org/documents/dc-rdf/

[6] Dan Brickley, Libby Miller , 9 August 2010

http://xmlns.com/foaf/spec/

家庭傳播型態與父母介入對於兒少網路隱私關注與態度影響之研究

黃琬翎
國立中正大學電訊傳播所碩士班二年級
adela541@gmail.com

摘要

本研究旨在探討父母介入與國小中高年級生保護網路隱私權態度之影響，以及不同變項間的差異情形，並探討彼此間的關係。為達到研究目的，本研究採用問卷調查法來進行，以彰化縣彰化市某國小的四～六年級生為研究對象，有效樣本共計241份，根據問卷填答結果來進行資料處理。

本研究同時以「父母介入」與「家庭傳播型態」中的「社會取向」與「概念取向」所形成的家庭傳播型態，來討論不同家庭傳播型態下，父母介入學童對於隱私權關注程度的關係。結果發現，父母越多時間規則制訂，學童在週間上網的頻率越低。此外，以社會取向為主的家庭傳播型態，比起以概念取向為主的家庭傳播形態，父母會有較多的時間規則制定以及內容規則制訂，且學童對隱私權關注的程度也較高。其中，女生較男生多受到父母介入的影響；且越高年級的學童也受到父母較多的介入。

本研究亦發現女生較男生更認為學校應積極教導保護隱私權的觀念。而在以社會取向所形成的家庭傳播型態中的學童，更認為學校應積極教導保護隱私權的觀念；當父母在內容規則制訂的介入越多時，學童更認為學校應積極教導保護隱私權的觀念。

關鍵詞：父母介入、家庭傳播型態、隱私權。

Abstract

The study presents the effect of parental influence on teens' attitude toward privacy protection. The data show that teens high in socio-oriented family communication tend to engage in high level of privacy concern, which, in turn, affects their level of privacy concern; moreover, teens tend to have more family rules. This study also finds that parental mediation and teens' concern level explain their attitude toward privacy protection measures. I hope the findings of this study provide not only an overview of current relationship between FCP and teens' privacy protection attitude but also new insights for future research directions regarding this vital issue.

Keywords: parental mediation, FCP, privacy.

1. 前言

1.1 研究背景與動機

現今這群新世代生長在一個網路蓬勃發達的數位時代，這些網路世界原住民接觸網路的年齡大幅提前，且頻率逐漸增加。根據兒盟「2012年兒少網路行為調查報告」發現有高達八成三的孩子平常會上網，尤其是週休放假期間，高達七成一的孩子週末兩天都會上網，甚至有一成的孩子上網時間超過6個小時。然而上網的時間越長，就越容易陷入網路的危機當中。該調查報告中將兒少在網路上容易遇見的危機分為四類，分別是：沈迷、資訊不分級、隱私不設定、交友不設限。其中「隱私不設定」這部分，當Facebook的應用程式向孩子索取個資時，近六成選擇同意；此外，八成四的孩子會讓朋友的朋友在個人的塗鴉牆上按讚，一點都不在意私密留言或個人資訊會被陌生人看光（兒盟，2012年兒少網路行為調查報告）。

此外，根據白絲帶工作站的「青少兒網路安全素養調查報告」（2005）研究結果顯示，近四成的學童不知道或不懂個人資料安全保護，也有近四成的學童表示家長不會監督孩子網路使用行為，同時，有二成五的學童不知道或不懂個人密碼資料的保護（歐陽誾，2004）。此外，該調查報告也發現與父母相處的情形會影響學童的網路安全素養，與父母討論兩性關係的情況越好，對網路安全素養程度越高。為了避免讓青少兒陷入網路危機的泥淖，必須及早讓他們學習網路、媒體識讀知識與技能，為他們打下良善的基礎，讓青少兒有足夠的識讀能力來面對危機四伏網路世界。

1.2 研究目的

本研究希望解答的問題是，家庭傳播型態與父母介入是否會影響兒少對隱私關注程度與保護網路隱私權之態度？以及其關聯性何在？進行研究同時需要考慮性別、年級、網路使用頻率，因為這些變項也可能會影響兒少對隱私權關注程度與保護隱私權的態度。因此本研究將這三個變項作為控制變項，以探討性別、年級、網路使用頻率等變項，與家庭傳播型態、父母規則制訂介入對兒少在隱私關注程度及保護隱私態度，是否存有互動的關係。

2. 文獻探討

2.1 消費者社會化與家庭傳播型態

Ward在1974年提出「消費者社會化」理論，認為消費者的社會化是人們獲得技巧、知識以及態度的過程，它可以幫助消費者在購買過程中發揮既定的功能（周文琪，2002：165）。國外學者如Moore與Moschis（1981）強調父母在塑造與發展兒少的消費規範、價值和動機等方面扮演著重要角色。尤其是消費行為隱藏著潛在風險，Koesten與Anderson等人認為兒少透過與父母直接或間接的互動來學習如何處理潛在知覺的風險，這些和父母的互動包括討論、規則制訂，以及強迫（Youn, 2008: 367）。Lenhart（2005）研究也指出兒少在網路上洩露個資容易遭遇不同風險，像是垃圾信件、身份盜用、或受到陌生人的騷擾。因此，父母影響是兒少社會化過程中非常重要的因素之一，藉由父母的影響可以提高兒少對隱私關注的程度，以及保護線上隱私的動機。

在本研究中，父母的影響將透過家庭傳播型態來檢驗消費議題。家庭作為一個重要社會化機構，其傳播型態會影響個人之人格，乃至於對許多事物的認知、態度及行為（王嵩音，1994：147）。McLeod和Chaffee將家庭傳播型態分成兩個面向：一種是社會取向（Socio-oriented），此種取向的家庭強調父母與子女之間的和諧關係，子女必須服從父母的權威，避免與他人衝突，因此社會取向的家庭模式中的父母會管制子女的消費行為，並和子女分享同一套消費觀。另一種是概念取向(Concept-oriented)，父母強調的是子女與觀念間的關係，子女被鼓勵勇於表達己見、獨立思考，且不避諱與他人爭論。在概念取向的家庭模式中，子女對於消費較有獨立思考的機會（Carlson, Grossbart, and Stuenkel, 1992）。

關於家庭傳播型態與線上隱私權議題之國外研究不多，僅有 Moscardelli 與 Divine（2007）研究發現兒少對隱私關注與概念取向家庭傳播型態有關，而非社會取向的家庭傳播型態。國內對此議題研究則甚少，因此本研究試圖檢驗家庭傳播型態與父母介入隱私權的相關性為何？以及如何影響子女對於隱私權關注的程度，與他們對保護隱私權之態度。

2.2 家庭傳播型態與父母規則制訂之介入

父母介入（Parental Mediation）係指父母針對子女的收視行為所做的管理（禁止與選擇）、注意與瞭解、親子共視、討論與評論等等。（蔡菁秤，2000：11）父母介入的方式可分為三種類型：規則制訂型（Rulemaking）、評價型（Discussion）、共視型（Coviewing）。規則制訂型介入的父母會控制子女在媒體使用的次數、時間，或內容。本研究將規則制訂型的父母介入運用在線上隱私權這方面，藉此驗證出父母介入隱私權的類型，並結合家庭傳播型態，研究在不同的社會取向與概念取向的家庭傳播型態中，會如何影響父母介入隱私權。

Fujioka 與 Austin（2002）提出在開放的概念取向家庭傳播類型，父母較會與子女共同收視媒體或進行討論。而社會取向的家庭傳播型態的父母則強調順從，會限制子女使用媒體的行為，例如父母偏好使用電視分級系統來為子女選擇電視節目。在高社會取向家庭傳播型態的家庭中，父母會限制其子女接觸像是媒體這類的外部影響，因為他們可能視這些外來的影響為對父母權威的威脅。因此，這些父母會透過規則制訂來保護他們的子女，使其免於受到有爭議的媒體訊息或商業的說服廣告（Moschis, 1985）。

藉由以上文獻耙梳，我們推測在社會取向為主的家庭中，父母較會限制子女們的網路使用，以及在網路上的個人資訊揭露。此外，在社會取向為主要傳播型態之家庭中長大的子女，家中會有較多的關於網路使用與資訊揭露的規則制訂，且家庭中的規則制訂可能會減少父母與子女之間因資訊揭露引起的紛爭。因此，本研究提出以下兩個假設：

H1：比起以概念取向為主的家庭傳播型態，以社會取向為主的家庭傳播型態之兒少，受到父母較多的時間規則制訂，像是網路的使用時間、長度。

H2：比起以概念取向為主的家庭傳播型態，以社會取向為主的家庭傳播型態之兒少，受到父母較多的內容規則制訂，像是上網的內容與個人資料揭露。

2.3 父母規則制訂介入與兒少隱私關注程度

如同前面文獻分析所述，制訂規則的父母介入可能被當成是一種工具，讓父母能持續掌控子女們使用網路的時間或內容以及資訊揭露。這類型的父母介入通常被認為能將家庭隱私風險降到最低，並且避免因為洩露家庭或個人資料給網路商家所引起的家庭糾紛（Youn, 2008）。Moscardelli 與 Divine（2007）發現，以社會取向為主的家庭傳播型態與兒少對隱私權的關注並無相關性，也就是說兒少對隱私權的關注，並不必然是透過家庭規則制訂而發展出來的。但這些結果對於規則制訂與增加兒少的隱私關注程度，並沒有呈現出強烈的相關性。在缺乏有力的文獻之下，本研究欲檢驗以下幾個研究問題：

RQ1：時間規則制訂與兒少關注隱私程度的關聯為何？

RQ2：內容規則制訂與兒少關注隱私程度的關聯為何？

另外，在相同在父母規則制訂介入與子女保護隱私權之態度的研究文獻甚少，故本研究亦提出下面的研究問題：

RQ3：時間規則制訂介入與兒少保護隱私權之態度的關聯為何？
RQ4：內容規則制訂介入與兒少保護隱私權之態度的關聯為何？

2.4 兒少隱私關注程度與保護隱私之態度

國外一些研究結果認為隱私關注程度與隱私保護行為之間有正向關係。LaRose 與 Rifon（2007,133）提出消費者對隱私議題的涉入度越高，則越傾向閱讀隱私聲明，以及越反抗提供個人資訊給網路商家。Sheehan 與 Hoy（1999）發現當隱私關注程度增加，消費者越傾向接受隱私保護行為。同時也發現兒少對線上隱私關注程度越高時，越會保護自己免於隱私權的風險。基於這些發現，本研究假定當兒少關心網路的隱私權問題，他們會渴望獲得保護隱私權之方法的協助。因此，本研究提出以下假設：

H3：兒少保護隱私權的態度與其認為學校應教導隱私權觀念之態度呈現正相關。

本研究之架構如下：

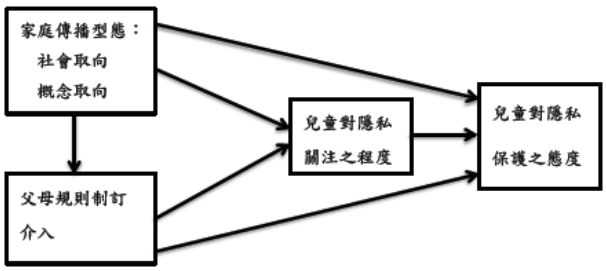


圖 1 本研究之架構

3. 研究方法

3.1 研究對象與抽樣方法

根據兒童與少年福利法規定未滿十八歲之兒童及少年皆屬於兒少法保障之對象，尤其是十二歲以下之兒童更需要受到保護。加上網路世代來臨，這一代的兒少幾乎都是網路世代的原住民，接觸網路的年齡大幅度提早，甚至上網已成為他們的生活習慣之一。觸網年齡提早，加上兒少年紀輕，因此他們更需要儘早學息網路、媒體識讀等相關知識、技能，才能保護自身，免於受網路風險之害。

故本研究將以國民小學的學生為主要研究對象。研究的母體為彰化縣國小四、五、六年級普通班學生。採問卷調查法進行本研究的調查，以茲建立地區性研究資料，並提供未來其他地區研究資料及相關研究的參考。

本研究抽樣方式採取隨機抽樣，抽取彰化縣中山國小為母體，在該所學校中四年級共 10 個班級，五年級共 11 個班級，六年級則有 12 個班級。接著隨機抽取四、五、六年級各三班，共 9 個班級為施測對象。總計發放問卷共 265 份，有效問卷共計 241 份，完成率為 90.9%，正式施策時間從 2013 年 5 月 24 日至 2013 年 5 月 30 日。

3.2 問卷設計

本研究問卷分為六個部分，第一部分控制變項，共四題。包括性別、年級（四年級、五年級、六年級）、星期一到星期五一天平均花多少時間在上網（無、30 分鐘以下、30 分鐘以上～1 小時以下、1 小時以上～1 個半小時以下、1 個半小時以上～2 小時以下、2 小時以上）、星期六到星期日一天平均花多少時間上網（無、30 分鐘以下、30 分鐘以上～1 小時以下、1 小時以上～1 個半小時以下、1 個半小時以上～2 小時以下、2 小時以上）。

第二部分為測量家庭傳播型態的變項，本研究測量「家庭傳播型態」主要採用的是 Moschis, Moore 與 Smith 等人（1984）所發展出的量表。此一量表包含兩個因素，一為社會取向家庭傳播，另一為概念取向家庭傳播，共 8 題。此量表採用李克特（Likert scale）四點量表計算，分為「從來沒有」、「很少」、「有時候」、「經常」此四個程度，「從來沒有」設定為 1 分，「很少」設定為 2 分，「有時候」設定為 3 分，「經常」設定為 4 分，回答方式是請受試者在四個選項中選擇一個答案。此一量表中的社會取向家庭傳播 Cronbach's α 達到 0.674 的信度標準，概念取向家庭傳播 Cronbach's α 達到 0.536 信度標準。量表效、信度測試如表 1：

表 1 家庭傳播型態影響與父母介入隱私權之因素分析

家庭傳播型態影響與父母介入隱私權之各題項	因素命名	
	社會取向	概念取向
爸媽會告訴我，我不能買哪些東西	.815	-.063
當我買了爸媽不喜歡的東西時，他們會念我	.702	.039
爸媽會想知道，我怎麼花我的零用錢	.591	.457
爸媽會告訴我什麼對我是最好的，我不應該反抗他們	.568	.040
爸媽會告訴我，我可以買哪些東西	.525	.299
爸媽讓我自己決定如何花我的零用錢。	.005	.731
爸媽讓我自己決定什麼東西應該買，什麼東西不應該買。	.229	.690
爸媽認為買我自己喜歡的東西很重要，就算別人不喜歡這些東西也沒關係。	-.003	.664
特徵值	2.576	1.338
解釋變異量	32.200%	16.726%
總解釋變異量	48.926%	
平均值	2.69	2.48
標準差	.72	.79
Cronbach' s α	.674	.536

註：表中各因素的數值為因素負荷量

第三部分為父母介入隱私權之測量，主要是測

量學童在父母介入網路隱私權這部分的感知。本研究選定 Seounmi Youn 所發展的量表，而其量表是參考 Austin 等人發展的父母介入廣告與媒體、以及青少年與隱私權量表進行修改而成，並且在用字遣詞上修正為適合本研究之量表。本研究只著重在父母介入中的「規則制訂」，再細分為「時間規則制訂」、「內容規則制訂」這兩個變項，共 6 題。受試者被要求回答父母是否會限制上網的時間、長度、內容、個人資料揭露等問題。此量表採用李克特四點量表計算，分為「從來沒有」、「很少」、「有時候」、「經常」此四個程度，「從來沒有」設定為 1 分，「很少」設定為 2 分，「有時候」設定為 3 分，「經常」設定為 4 分，回答方式是請受試者依據實際狀況，在四個選項中擇一回答。此一量表中的時間規則制訂 Cronbach's α 達到 0.81 的高信度標準，內容規則制訂 Cronbach's α 達到 0.78 的高信度標準。量表效、信度測試如表 2：

表 2 父母介入隱私權之因素分析與信度測試

父母介入隱私權之各題項	因素命名	
	內容規則制訂	時間規則制定
爸媽會限制我在網路上買東西。	.838	.148
爸媽會限制我跟網友見面。	.821	.034
爸媽會限制我在網路上提供個人資料。	.776	.285
爸媽會限制我可以上哪些網站	.516	.440
爸媽會限制我一天可以上網多久。	.154	.898
爸媽會限制我什麼時候可以上網。	.144	.878
特徵值	2.971	1.193
解釋變異量	49.520%	19.882%
總解釋變異量	69.402%	
平均值	2.90	3.00
標準差	1.02	.99
Cronbach' s α	.782	.809

註：表中各因素的數值為因素負荷量

第四部份是測量隱私權的關注程度。本研究參考 Seoumi Youn 發展的量表，該量表是根據 Milne 等人關於隱私權的研究，與消費者隱私相關研究文獻發展而成。受試者必須回答他們是否關心購物網站在網路上蒐集他們的個人資料等問題。此量表採用李克特（Likert scale）四點量表計算，分為「從來沒有」、「很少」、「有時候」、「經常」此四個程度，「從來沒有」設定為 1 分，「很少」設定為 2 分，「有時候」設定為 3 分，「經常」設定為 4 分，回答方式是請受試者依據實際狀況，在四個選項中擇一回答。此一量表中的 Cronbach's α 達到 0.54 的信度標準。量表效、信度測試如表 3：

表 3 隱私權關注程度之因素分析與信度測試

隱私權關注程度之各題項	隱私權關注程度
當我逛購物網站後，我擔心購物網站會蒐集和使用我的個人資料。	.838
我認為在網路上用信用卡買東西是很危險的。	.821
我關心購物網站如何在網路上蒐集和使用我的個人資料。	.776
特徵值	1.605
解釋變異量	53.501%
平均值	2.86
標準差	.74
Cronbach' s α	.542

註：表中各因素的數值為因素負荷量

4. 資料分析與解釋

4.1 研究樣本人口特徵描述

本研究有效樣本（N= 241）中，男生佔 55.6%，共 134 人；女生佔 44.4%，共 107 人。四年級生佔 33.2%，共 80 人；五年級生佔 34.4%，共 83 人；而六年級生佔 32.4%，共 78 人。在上網時間的部分，週一到週五有高達 39.4%的學童是不上網，其次 24.1%的上網時間是 30 分鐘以下；至於週末則有 27.4%的學童上網時間達 2 小時以上，此結果顯示國小學童上網的時間多為週末。

4.2 家庭傳播型態與父母規則制訂介入

本研究依據前述研究假設進行統計分析，一一加以驗證。

H1：比起以概念取向為主的家庭傳播形態，以社會取向為主的家庭傳播型態之兒少，受到父母較多的時間規則制訂，像是網路的使用時間、長度。

H2：比起以概念取向為主的家庭傳播形態，以社會取向為主的家庭傳播型態之兒少，受到父母較多的內容規則制訂，像是上網的內容與個人資料揭露。

在假設一和假設二的驗證方面，本研究採用階層迴歸之統計方法比較家庭傳播型態與父母介入的影響力。本驗證以二次階層迴歸分析「家庭傳播型態」中的「社會取向」與「概念取向」的影響，來討論不同家庭傳播型態下，父母規則制訂介入對於子女隱私權關注程度的關係。第一階層輸入人口學變項，包括性別、年級、週間與週末上網使間。第二階層則輸入家庭傳播型態的社會取向與概念取向。表5呈現階層迴歸之統計結果。

結果發現，在「時間規則制訂型」的父母介入方面，第一階層迴歸分析中，只有「週間使用網路頻率」的影響達顯著（β = -.256, p <0.01），而且影響為負向，即父母越多時間規則制訂，子女在週間上網的頻率越低。第二階層的迴歸分析中，週間使

用網路頻率（β = -.253, p <0.001）依舊是對時間規則制訂具有預測利。而控制了人口學變項後，兩種取向的家庭傳播型態之中僅有「社會取向」（β = 0.249, p <0.001）對於時間規則制訂的影響達顯著。也就是控制了人口學變項後，以社會取向為主的家庭傳播型態，比起以概念取向為主的家庭傳播形態，父母會有較多的時間規則制訂。整體看來，在第一階層中，只投入人口變項時，週間使用網路頻率能解釋的變異量為9.8%。第二階層再加上家庭傳播型態之社會取向的預測力，解釋變異量增為26%。此外，經過共線性檢測，所得之VIF皆小於2之標準，顯示沒有共線性之問題。

在「內容規則制訂」的父母介入方面，第一階層迴歸分析中，有「性別」（β = -.163, p <0.05）與「年級」（β = 0.150, p <0.05）的影響達顯著。其中「性別」的影響為負向，即女生較男生多受到父母介入的影響；而「年級」的影響為正向，表示越高年級的兒少，在內容規則制訂方面較多受到父母的介入。

第二階層的迴歸分析中，「性別」、「年級」不具預測力。此外，控制了人口學變項後，兩種取向的家庭傳播型態之中僅有「社會取向」（β = 0.347, p <0.001）成為顯著的預測變項，意即以社會取向為主的家庭傳播型態，比起以概念取向為主的家庭傳播形態，父母會有較多的內容規則制訂。整體看來，在第一階層中，只投入人口變項時，兩個人口變項能解釋的變異量為 6.2%。第二階層再加上家庭傳播型態的預測力，解釋變異量增為 25.8%。同樣經過共線性檢測，顯示沒有共線性之問題。

根據以上分析結果，在「社會取向」家庭傳播型態中之兒少，父母給予較多的時間規則制訂以及內容規則制訂。假設一、假設二獲得支持。

表 5 家庭傳播型態

	時間規則制訂	內容規則制訂
第一階層		
性別（男=1）	.025	-.163*
年級	.067	.150*
週間使用網路頻率	-.256**	-.059
週末使用網路頻率	-.103	-.059
R^2	.098	.062
第二階層（FCP）		
性別（男=1）	.052	-.119
年級	.042	.113
週間使用網路頻率	-.253***	-.057
週末使用網路頻率	-.076	-.022
概念取向	.023	.065
社會取向	.249***	.347***
R^2	.162	.196
全部可解釋變異量	.260	.258

說　　明：*：p <.05，：p <.01，***：p <.001。**

4.3 父母規則制訂介入與兒少隱私關注程度

RQ1:時間規則制訂與兒少關注隱私程度的關聯為何？
RQ2：內容規則制訂與兒少關注隱私程度的關聯為何？
RQ3：時間規則制訂介入與兒少保護隱私權之態度的關聯為何？
RQ4：內容規則制訂介入與兒少保護隱私權之態度的關聯為何？

在研究問題 1~4 的驗證方面，本研究採用階層迴歸之統計方法比較家庭傳播型態與父母介入對於兒少在隱私權關注程度與保護隱私權態度的影響力。本研究以三次階層迴歸進行分析。第一階層輸入人口學變項，包括性別、年級、週間與週末的網路使用頻率。第二階層輸入家庭傳播型態之概念取向與社會取向。第三層輸入父母介入之時間規則制訂與內容規則制訂。表 6 呈現階層迴歸之統計結果。

在「隱私權關注程度」方面，第一階層迴歸分析中，只有「年級」的影響達顯著（β = 0.239, p <0.001），而且影響為正向，即越高年級的兒少對於隱私權關注的程度越高。第二階層的迴歸分析中，「年級」依舊對隱私權關注程度具有預測力。而控制了人口學變項後，兩種家庭傳播型態之中僅有「社會取向」（β = 0.196, p <0.01）對於隱私權關注程度的影響達顯著。也就是控制了人口學變項後，在以社會取向所形成的家庭傳播型態中的兒少，對隱私權關注的程度也越高。第三層的迴歸分析中，「年級」依舊對隱私權關注程度具有預測力，但「社會取向」則不具預測力。在控制了人口學變項、家庭傳播型態後，兩種父母介入之規則制訂之中只有「時間規則制訂」（β = 0.146, p <0.05）成為顯著的預測變項，意即當父母在時間規則制訂的介入越多時，子女對隱私權關注的程度也會越高。整體看來，在第一階層中，只投入人口變項時，年級能解釋的變異量為6.9%。第二階層加上社會取向的預測力，解釋量增為19%。第三階層再加上時間規則制訂的預測力，總解釋變異量增加為34.8%。此外，經過共線性檢測，所得知VIF皆小於2之標準，顯示沒有共線性之問題。

在保護隱私權態度方面，本研究調查兒少認為學校應該更積極教導保護隱私權的觀念之態度。在第一階層迴歸分析中，只有「性別」的影響達顯著（β = -.173, p <0.05），而且影響為負向，表示女生較男生更認為學校應積極教導保護隱私權的觀念。第二階層的迴歸分析中，性別（β = -.156, p <0.05）依舊學校教育具有預測力。而控制了人口學變項後，家庭傳播型態當中僅有「社會取向」（β = 0.164, p <0.05）對學校教育的影響達顯著。也就是控制人口學變項後，在以社會取向為主的家庭傳播型態中之兒少，更認為學校應積極教導保護隱私權

的觀念。第三階層迴歸分析中，性別與社會取向不再具有預測力。而控制了人口學變項、家庭傳播型態後，「內容規則制訂」（$\beta = 0.233, p < 0.05$）對學校教育的影響達顯著，也就當父母在內容規則制訂的介入越多時，學童更認為學校應積極教導保護隱私權的觀念。整體來看，在第一階層只投入人口變項時，性別能解釋的變異量為 3.3%。第二階層加上社會取向的預測力，解釋變異量增為 9.3%。第三階層再加上內容規則制訂的預測力，總解釋變異量增加到 20%。此外，經過共線性檢測，所得知 VIF 皆小於 2 之標準，顯示沒有共線性之問題。

根據以上分析結果得知，受到越多時間規則制訂的兒少，對隱私關注程度越高。受到越多內容規則制訂的兒少，則對保護隱私權之態度越正向。

表 6 父母規則制訂介入對兒少保護隱私權態度

	隱私權關注程度	保護隱私權態度
第一階層		
性別（男=1）	-.086	-.173*
年級	.239***	-.038
週間使用網路頻率	-.051	.048
週末使用網路頻率	.032	-.031
R^2	.069	.033
第二階層		
性別（男=1）	-.054	-.156*
年級	.216**	-.054
週間使用網路頻率	-.051	.049
週末使用網路頻率	.051	-.013
概念取向	.077	.013
社會取向	.196**	.164*
R^2	.121	.060
第三階層		
性別（男=1）	-.048	-.129
年級	.197**	-.081
週間使用網路頻率	-.008	.067
週末使用網路頻率	.064	-.007
概念取向	.067	-.003
社會取向	.121	.078
時間規則制訂	.146*	.019
內容規則制訂	.112	.233*
R^2	.158	.107
全部可解釋變異量	.348	.200

說　　明：*：$p < .05$，：$p < .01$，***：$p < .001$。**

4.4 兒少隱私關注程度與保護隱私權之態度

H3：兒少關注隱私程度與其保護隱私權之態度呈現正相關。

在假設三的驗證方面，同樣採用階層迴歸之統計方法比較兒少對隱私關注程度與其保護隱私權之態度的影響力。本研究以四次階層迴歸分析兒少對隱私關注程度的影響。第一階層輸入人口學變項，包括性別、年級、週間與週末使用網路頻率。第二階層輸入家庭傳播型態之概念取向與社會取向。第三階層輸入父母介入之時間規則制訂與內容規則制訂。第四階層則輸入兒少對隱私關注程度。表 7 呈現階層迴歸之統計結果。由於表 7 中第一階層到第三階層的迴歸分析，結果皆與表 6 之結果相同，故此處不再贅述。

在學校教育方面，第四層迴歸分析中，內容規則制訂仍舊具有預測力。控制了人口學變項、家庭傳播型態、父母介入等變項後，「隱私關注程度」（$\beta = 0.175, p < 0.01$）對於學校教育的影響達顯著，且影響為正向。也就是對隱私關注程度越高的兒少，更認為學校應該多多教育關於隱私權保護之知識。整體看來，在第一階層只投入人口變項時，性別可解釋的變異量為 3.3%。第二階層加上社會取向，解釋變異量增加為 9.3%。第三階層加上內容規則制訂後，解釋變異量增為 20%。第四階層再加上隱私關注程度的預測力，總解釋變異量增加至 33.3%。此外，經過共線性檢測，所得之 VIF 皆小於 2 之標準，顯示沒有共線性之問題。

由以上分析結果得知，對隱私關注程度越高的兒少，對保護隱私權態度就越正向，也就是說對隱私關注程度越高，就越會保護隱私權。因此，假設三獲得支持。

表 7 兒少隱私關注程度與保護隱私權之態度

	保護隱私權態度
第一階層	
性別（男=1）	-.173*
年級	-.038
週間使用網路頻率	.048
週末使用網路頻率	-.031
R^2	.033
第二階層	
性別（男=1）	-.156*
年級	-.054
週間使用網路頻率	.049
週末使用網路頻率	-.013
概念取向	.013
社會取向	.164*
R^2	.060
第三階層	
性別（男=1）	-.129
年級	-.081
週間使用網路頻率	.067
週末使用網路頻率	-.007
概念取向	-.003
社會取向	.078
時間規則制訂	.019
內容規則制訂	.233**
R^2	.107
第四階層	
性別（男=1）	-.121
年級	-.116
週間使用網路頻率	.069
週末使用網路頻率	-.018
概念取向	-.014
社會取向	.057
時間規則制訂	-.007
內容規則制訂	.213**
隱私關注程度	.175**
R^2	.133
全部可解釋變異量	.333

說　　明：*：p <.05，：p <.01，***：p <.001。**

5. 結論與建議

自從傳播學者 McLeod 和 Chaffee 提出四種類型的家庭傳播型態之後，國外許多學者前仆後繼地投入相關主題的研究，已累積了大量的研究成果。早期學者們多將家庭傳播型態或父母介入運用在傳統媒體的研究上，像 Moore 和 Moschis（1978）曾發現家庭傳播型態會影響子女受廣告影響的程度（羅文輝、鍾蔚文，1988）。近年來則陸陸續續將家庭傳播型態運用在網路上，尤其是國內，甚少有將家庭傳播型態運用在網路隱私權上做研究。本研究證實國內家庭傳播型態與父母規則制訂介入，對於兒少的隱私關注程度與保護隱私之態度是有影響的。

本研究發現以社會取向家庭傳播型態為主的兒少，他們會受到父母較多的規則制訂之介入，包括時間規則制訂，父母會限制他們使用網路的時間及長度；也包含內容規則制訂，父母會限制他們不能上哪些網站。此結果呼應了 Fujioka 和 Autstin（2002）之研究發現：社會取向家庭傳播型態之父母較強調順從，會限制子女使用媒體的行為。

此外，本研究亦發現，父母規則制訂介入與兒少對隱私關注呈現相關性。Moscardelli 和 Divine（2007）的研究指出，社會取向家庭傳播型態對兒少的隱私關注並無相關性。然而，本研究將家庭傳播型態與父母規則制訂介入交互作用後，發現社會取向家庭傳播型態中的兒少，對隱私關注程度與隱私保護態度有正向相關，意即社會取向家庭傳播型態中的兒少，對隱私關注程度越高，也越傾向保護隱私權之態度。

另外，本研究結果顯示兒少對隱私關注之程度與其保護隱私之態度呈現正向相關，也就是對隱私關注程度越高的兒少，越傾向會保護其網路隱私權。此結果與 Sheehan 和 Hoy（1999）的研究相同，他們指出當兒少對線上隱私關注程度增加時，他們越會保護自己免於受到隱私權風險之危機。

根據兒盟的「2012 年兒少網路行為調查報告」，超過五成以上的孩子在使用 Facebook 時不懂保護自己的個人資料。白絲帶工作站在 2005 年的「青少兒網路安全素養調查報告」亦顯示，近四成的學童不知道或不懂個人資料安全保護。如何讓這些數據下降，尤其是當這群網路新世代的生活型態逐漸改變，娛樂、消費習慣大不同於以往，讓這群網路原住民的兒少們儘早學習保護網路隱私權之識讀能力是當前相當重要的課題。

除了父母應積極介入子女的網路使用狀況，給予正確的指導，使其提高對網路隱私權之關注與保護之態度。學校教育也應該同步加強對網路資訊、媒體識讀之能力與知識，教導兒少網路資訊的分級制度、網路內容的虛實、以及保護個人資料的重要性，避免其受到不必要的困擾與恐慌，也避免個人資料被濫用的風險，替兒少打造一個良善的網路環境，並且保障兒少能享有優質的網路環境之權利。

參考文獻

[1] 兒童福利聯盟（2012）。《2012 年兒少網路行為調查報告》。台北市：作者。

[2] 歐陽誾（2004）。〈網路世界不設防—淺談兒童及青少年網路安全的重要性〉，《國教之友》，58（3）：25-33。

[3] 周文琪（2002）。〈傳播接觸管道對消費者社會化的影響〉，《通識教育年刊》，4：163-179。

[4] 王嵩音（1994）。〈蘭嶼學童之家庭傳播型態與媒介使用〉，《新聞學研究》，48：147-151。
[5] 蔡菁秤（2000）。《兒童電視識讀能力與父母介入兒童收視行為》。臺中師範學院國民教育研究所碩士論文。
[6] 羅文輝、鐘蔚文（1988）。〈家庭傳播形態在兒童對電視廣告的認知、態度即行為上所扮演的角色〉，《新聞學研究》，40：111-139。
[7] 陳佳宜（2008）。《第三人效果與父母介入子女電視收視行為》。國立中正大學電訊傳播研究所碩士論文。
[8] 張威龍（1999）。〈青少年家庭溝通型態對物質主義和強迫性購買之影響研究〉，《管理評論》18（2）：87-117。
[9] 黃芳銘（2007）。〈在學青少年手機消費忠誠度—消費者社會化的觀點〉，《αβγ 量化研究學刊》，1：123-150。
[10] 黃葳威、林紀慧、呂傑華 （2006）。〈台灣學童網路分級認知與網路安全素養探討〉。
[11] 劉靜怡（2002）。〈網際網路時代的資訊使用與隱私權保護規範：個人、政府與市場的拔河〉，《資訊管理研究》，3：137-161。
[12] Ward, Scott. 1974. Consumer Socialization. Journal of Consumer Research, 1 (2): 1-14.
[13] Moore, Roy L. & George P. Moschis. 1981. The Role of Family Communication in Consumer Learning. Journal of Communication, 31 (4): 42-51.
[14] Seounmi Youn (2008). Parental Influence and Teens' Attitude toward Online Privacy Protection. The Journal of Consumer Affairs, 42(3), 362-388.
[15] Lenhart, Amanda. 2005. Protecting Teens Online. Pew Internet & American Life Project. Retrieved 23. June. 2013, from http://www.pewinternet.org/~/media//Files/Reports/2005/PIP_Filters_Report.pdf.pdf
[16] Carlson, Les, Sanford Grossbart, and J. Kathleen Stuenkel. 1992. The Role of Parental Socialization Types on Differential Family Communication Patterns Regarding Consumption. Journal of Consumer Psychology, 1 (1): 31-52
[17] Moscardelli, Deborah M. and Richard Divine. 2007. Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships with Privacy-Protecting Behaviors. Family and Consumer Sciences Research Journal, 35 (3): 232-252.
[18] Fujioka, Yuri and Erica Weintraub Austin. 2002. The Relationship of Family Communication Patterns to Parental Mediation Styles. Communication Research, 29 (6): 642-665.
[19] Moschis, George P. 1985. The Role of Family Communication in Consumer Socialization of Children and Adolescents. Journal of Consumer Research, 11 (March): 898-913.
[20] LaRose, Robert and Nora J. Rifon. 2007. Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. Journal of Consumer Affairs, 41 (1): 127-149.
[21] Sheehan, Kim B. and Mariea G. Hoy. 1999. Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns. Journal of Advertising, 28 (3): 37–51.
[22] Couts, Andrew (2012.02.23). Obama unveils consumer privacy bill of rights. Digital Trends. Retrieved June 23, 2013, from Digital Trends on the World Wide Web: http://www.digitaltrends.com/web/obama-unveils-consumer-privacy-bill-of-rights/
[23] Les Carison & Grossbart, S. 1988. Parental Style and Consumer Socialization of Children. Journal of Consumer Research, 15: 77-94

iTNUA 校園資訊入口及單一帳號登入整合之實作

林明灶　　劉仲凱
國立臺北藝術大學電子計算機中心
臺北市、臺灣
mtlin@tnua.edu.tw　chongkai@tnua.edu.tw

摘要

本文主要描述國立臺北藝術大學(Taipei National University of the Arts, TNUA)，在自主開發建置單一帳號簽入統整各校務行政資訊系統的過程架構及方法，以分享系統實務流程經驗，於建構整合校園行政系統資訊入口(Enterprise Information Portal, EIP)，及學校 e-mail 單一帳號登入(Single sign-on, SSO)，便利使用教務系統、學務系統、人事系統、電子郵件、資訊查詢…等各項校園資訊系統，提供實務開發經驗分享應用。開發流程重點於帳號管理設定、輕量級目錄存取協定(Lightweight Directory Access Protocol, LDAP)資料架構設計及建置、LDAP 應用程式介面 API、帳號開啟系統及帳號整合機制規劃。運用 OpenLDAP 原理延伸目錄服務管理大幅降低軟體建置成本，且資訊系統的程式開發語言皆有支援 LDAP API，迅速修改系統認證機制，達成單一登入之開發。

關鍵字: 單一帳號登入, 校園行政系統資訊入口, 輕量級目錄存取協定.

ABSTRACT

This paper is mainly introduction the self-development of the integration of Single sign-on (SSO) and Enterprise Information Portal (EIP) for academic administration information system of Taipei National University of the Arts (TNUA). The purposes are to share the practical systems experience regarding EIP and email SSO, improve convenience for using academic administration information systems including academic information system, student affairs system, human resource information system, email, information inquiry, etc. Besides, it could substantially reduce development cost by applying the Open Lightweight Directory Access Protocol (OpenLDAP) theory and the developing system language could also support LDAP Application interface to efficiently revise system recognition mechanism to reach the SSO development. The key processes for this whole design include account management, data design and construction for Lightweight Directory Access Protocol and LDAP, application program interface (API) for LDAP, account opening system, and account integration design.

Keywords: Single Sign-On, SSO、Enterprise Information Portal, EIP、Lightweight Directory Access Protocol, LDAP

1. 前言

大學校務系統的開發管理與經營控管，對於大學行政績效的提升，具有關鍵性的影響。數位化校園建設中行政系統資訊化，不同時期陸續開發完成教務資訊系統、學務資訊系統、人事資訊系統、總務資訊系統與招生試務系統及其它相關子系統等建置更新作業，以提昇教務處、人事室、學務處、推廣教育、總務...等行政效率與服務品質，及資料庫整合之即時及一致性作業，提供各項資訊自動化作業、管理報表及報部報表[1]。校務行政資訊系統均需要使用者鍵入帳號密碼進行認證，認證通過後，各系統針對登入的帳號進行授權，取得相對應的功能與權限。但開發過程中，各系統的帳號因無相互整合，使用者就需要針對每個系統去進行帳號的建立(如以身份證字號、email帳號、學生學號或個別帳號…等)，密碼的設定。系統增加，相對需記憶之帳號密碼亦增加。因此對使用者帳號密碼管理是困擾的。當人員資料異動時，需以非資訊化機制如書面或定時管理帳號資料。可能面臨的困難點，於各系統帳號的不同、資訊系統上線而無法全面修改帳號、開發程式語言不同及委外系統廠商的經驗與配合度。因此統整各應用系統的帳號，使用單一組帳號密碼登入如圖1於各應用系統是必需的。

企業入口網站(EIP)及單一帳號簽入之開發，以目前學校校園及企業界為例，多以廠商協助開發，在系統整合過程雖有標準化作業流程，與充足之經驗，但開發費用接近10萬美金以上之要求，及每年至少需10%以上之維護費用，且委託單位面臨程式無法自主及核心技術無法獲得，新系統開發之介接仍需依賴於廠商，廠商之資訊人員異動頻繁常造成技術銜接有代溝，時效管理都有所延遲。自主開發除了能節省開發費用，效能與功能符合業務單位需求，且能精進各系統開發人

員之技術能力，亦能熟稔系統之實質架構。需挑戰的是系統與EIP整合之協調溝通，及資訊安全之設計。

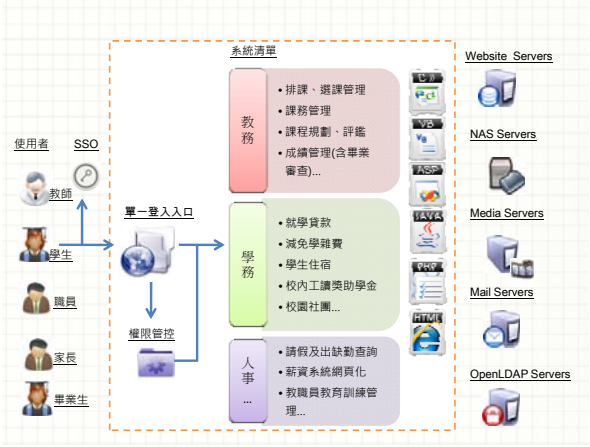


圖 1 校務系統單一簽入架構規劃圖

EIP 及 SSO 之發展已近十餘年，相關論文著重於單一學術主題討論，帳號管理關鍵技術在於使用輕量級目錄存取協定 LDAP，經研究廠商使用之 LDAP 技術，區分為 AD (Windows)、eDirectory(Novell) 、 Directory Server(IBM) 及 OpenLDAP，經由評估其優缺後選用 OpenLDAP，因為免授權費用與開放式源始碼(Open Source)及效能可以應付本校教職員生共約 3,000 人，與功能符合本校需求。目前多為開發廠商之核心技術而無法取得開發之報告，本論文在於本校全面性自行開發與研究 EIP 與 SSO，得就開發之成果得以呈現與揭露核心技術於論文，並廣為推廣學校與企業應用。

目前於各資訊系統的帳號大致可以區分為 Email、學生學號、身份證字號、個別帳號如表 1 所列，為達成單一簽入式登入帳號，因考量外籍人士無法取得身份證字號，規劃以 Email 帳號為統一的帳號。

2. SSO 帳戶資訊管理機制

綜合 SSO 業界整合技術分為 2 種及共同合併使用，其運作模式如下圖所示：

1. 使用者帳號資訊存放於目錄服務系統如 LDAP、AD (Active Directory)，目前業界廠商如 Direk Tech Inc.、Novell、IBM 大都以目錄服務系統來開發 SSO 相關產品。
2. 使用者帳號資訊存放於資料庫系統如 MSSQL、Oracle、MySQL，目前業界廠商如狀態網際網路大都以資料庫系統來開發 SSO 相關產品。

表 1 資訊系統與使用登入帳號分類表

登入帳號	資訊系統
Email 帳號	無線網路、webmail、數位學習、總務系統…
教職員身分證、學生學號	教務系統、學務系統、掛失系統、圖書館系統…
教職員身分證	出納系統、招生系統、人事系統…
個別帳號	官網、電子公文、數位典藏…

比較分析學校各資訊系統的屬性後，使用者帳號資訊存放於 LDAP 及 DB 共同合併使用，若系統無法以 LDAP 進行帳號認證時，則將採取使用帳號資訊存放於 DB，其中 DB 俱有之優點：DB 容易與各資訊系統進行資料交換與資料同步。帳號資訊存放於 DB 容易被各系統的開發語言所使用，資料的備份與備援機制健全。使用資料庫存放使用者資訊可自由快速的附加其他欄位屬性，無需重新啟動服務，擴充性與便利性較高，更新資料速度快，寫入資料的比例比讀取資料的比例還高，允許多個連線同時更新同一筆資料。使用帳號資訊存放於 DB 相對存放於 LDAP，俱有以下缺點：存取控制(Access Control List, ACL)較不安全，LDAP 的 ACL 較 DB 完整，DB 的存取技術難度雖相較 LDAP 簡單，LDAP 通訊協定是屬於 protocol，支援的異質平台較多，但 DB 通訊協定不屬於 protocol，所以支援的異質平台較少。所以本系統在資料安全性維護上，有規劃相對應的配套「資訊安全規劃」如後說明。

2.1 EIP SSO 流程說明

SSO 運作原理分為以下四個步驟如圖 2：

1. 使用者所有登入都連到 SSO Server 進行。
2. 未經登入無法存取 Web Application。
3. 登入之後，SSO Server 給予使用者憑証，證明已經通過身分認證。
4. 使用者取得憑證後，就可以存取 Web Application，並由 SSO Server 告知 Web Application 使用者的身分。

若資訊系統已有 LDAP 認證機制，不以上述 SSO 認證方式，Web service 直接認證 LDAP。

3. 系統開發流程

系統開發主要核心於帳號管理同步程式開發、OpenLDAP 資料架構設計及建置、修改資訊系統至 LDAP 認證關鍵程式、及資訊安全規劃。

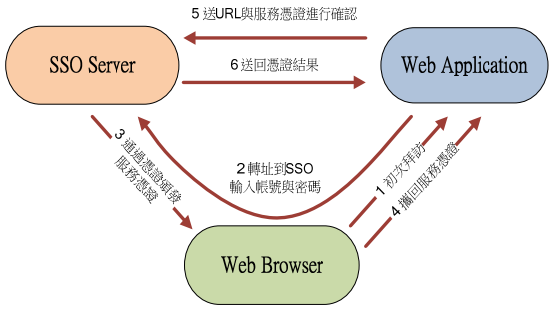


圖 2 SSO 運作原理

3.1 帳號管理同步程式開發

帳號管理平台引進了標準的 LDAP 服務，為一種目錄服務，可以使用 LDAP 來記錄各種人員資訊。由於 LDAP 是一種標準的通訊協定，不同的應用系統只要遵守此一共通的通訊協定，即可與 LDAP 服務進行溝通，取得其內的資料如帳號基本資料、權限資料等。 此一目錄服務已被各界廣泛運用於帳號管理，認證、授權等機制。由於它的標準性及普遍性，故採用其相關產品來作為我們帳號管理平台。經由評估測試，採用的是 OpenLDAP 軟體與資料同步軟體。

目前LDAP的資料架構在整合每一個資訊系統的不盡相同過程中，整合的方式分為:

1. 原系統帳號與LDAP帳號一致：資訊系統由於帳號與LDAP帳號一致，只有密碼可能不一樣，故整合的方式只需要將原認證的方式改由向LDAP伺服器進行認證即可如圖5，現在開發之程式語言都有內建與LDAP伺服器溝通的函示庫提供整合。即認證帳號與LDAP一致時，同步認證帳號 Attribute 到 LDAP Attribute。
2. 原系統帳號與LDAP帳號不一致：資訊系統由於原使用的帳號和LDAP帳號不一致，整合的方式就是原帳號資料中，屬性值是LDAP帳號基本資料中也同時具有的，通常為身份證號碼。修改原認證的機制改由LDAP帳號完成認證後，再透過額外的函示庫取得該帳號所對應的屬性資料，如前所述的身份證號碼，透過此屬性資料對應到原系統帳號。簡單說同步共同Attribute到 LDAP Attribute。

LDAP 相關名詞 DC (Domain Component)、CN (Common Name)、OU (Organizational Unit)。學校的使用者分為教師、職員、學生。教師、職員的基本資料來自於人事系統;學生的基本資料來自於教務系統，故此帳號管理同步程式(圖 3)每日至人事系統同步教師、職員的基本資料到 ou=member, ou=people, dc=tnua, dc=edu.tw 如圖 4; 帳號管理同步程式每日至教務系統同步學生的基本資料到 ou=member, ou=people, dc=tnua, dc=edu.tw 如圖 5。

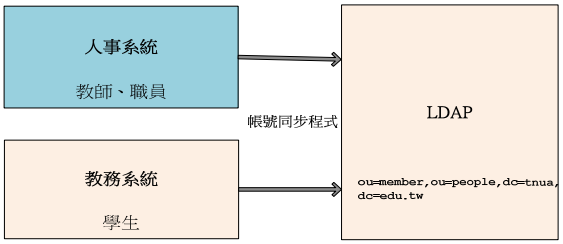


圖3 教務系統人事系統帳號同步管理

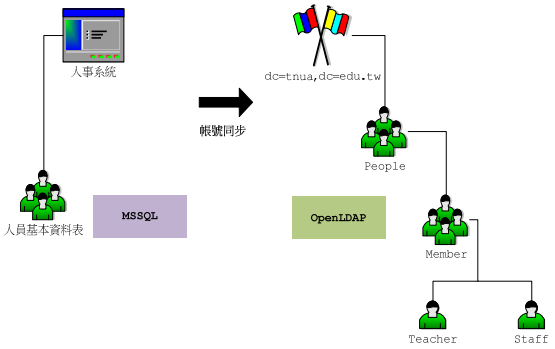


圖 4 人事系統教師職員帳號同步管理

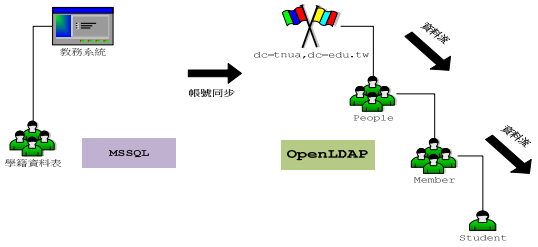


圖 5 教務系統學生帳號同步管理

3.2 OpenLDAP資料架構設計及建置

LDAP 模型以項目(entry)中 objectclass 之屬性的集合[2-6]。每一項目都有一組識別名稱(DN)，用來清楚對照項目。在 LDAP，項目以階層式結構方式排列，如圖 6 之階層圖，為本校之 LDAP 結構。代表學校的項目位在樹狀結構的頂端也就是(dc=tnua, dc=edu.tw)，學校底下有組織，分別為「系統使用群組(ou=service, dc=tnua, dc=edu.tw)」和「國立臺北藝術大學群組(ou=people, dc=tnua, dc=edu.tw)」，國立臺北藝術大學群組底下有「LDAP 管理者群組(ou=ldapmanager, ou=people, dc=tnua, dc=edu.tw)」和「教職員生群組(ou=member, ou=people, dc=tnua, dc=edu.tw)」，最後在樹狀最末端的項目一般是代表人員 (person)，每一個樹狀最末端的項目都有一個相對的識別名稱，它在樹狀結構分枝的其他同層物件中必須是唯一的。

例如：

cn=xxx@tnua.edu.tw,ou=member,ou=people,dc=tnua, dc=edu.tw

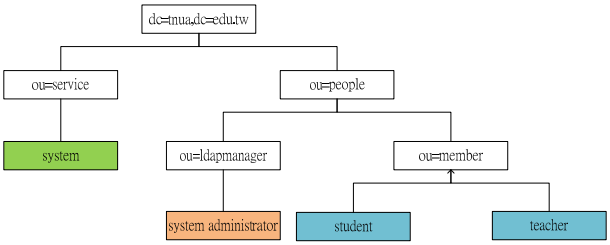


圖 6 LDAP 階層圖

目前在 LDAP「教職員生群組(ou=member, ou=people, dc=tnua, dc=edu.tw)」內存放教職員生的資料架構， 每個人員資料內有數個屬性，其中 LDAP 個人員資料屬性比較重要的如表 2 所列。

3.3 LDAP API程式撰寫

現有各資訊系統的使用者資訊，記錄在各資訊系統的資料庫裡，且各系統自行認證。為統一各資訊系統帳號與密碼，若資訊系統可以LDAP進行帳號進碼認證，則需修改原本的認證機制，改到LDAP進行認證如圖7。

表 2 LDAP 個人員資料屬性表

Attribute	Value	屬性說明
gidNumber	10000	群組識別碼
objectClass	inetOrgPerson	LDAP 物件
objectClass	posixAccount	LDAP 物件
objectClass	inetLocalMailRecipient	LDAP 物件
mail	xxx@tnua.edu.tw	電子郵件
uid	xxx@tnua.edu.tw	LDAP 帳號
uidNumber	2001	單位識別碼
cn	xxx@tnua.edu.tw	使用者帳號
homeDirectory	/home/xxx@tnua.edu.tw	Samba 私人目錄
hrstudent	1	是否在人事系統有帳號
idNumber	xxxxxxxx	身分證
givenName	xxx	姓名
mobile	xxxxxxxxxx	行動電話
birthday	1980xxxx	出生年月日
status	1	是否在職/學
sn	B0804	人事代碼/學號
title	tea	身分群組(教職員/學生)
cardNo	02xxxxxx	教職員證、學生證晶片序號
mailHost	mymail.tnua.edu.tw	Mail Server
userPassword	{CRYPT}FQIVLBeq	使用者密碼
	PEQgI	
postalAddress	xxx	通訊地址
postalCode	xxx	郵遞區號
ou	1201	單位代碼
description	E01	身分別

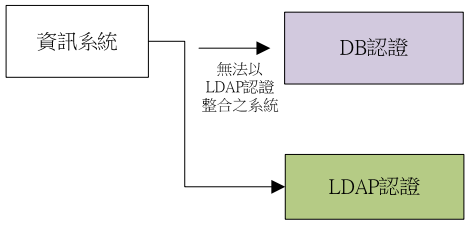


圖7 資訊系統改LDAP進行認證

LDAP認證關鍵程式，是以C#為例至LDAP認證。SSO Server關鍵程式碼[8]，SSO Server 是以 Microsoft Visual Studio 2010為開發工具，以 C# 為程式開發語言，以下為SSO Server產生XML的主要程式碼，XML如下圖所示。

```
1.  public string sessionStatusXML
2.      {
3.        get
4.  { //宣告XML物件
5.          XmlDocument xmldoc = new XmlDocument();
                XmlDeclaration node_dec =
      xmldoc.CreateXmlDeclaration("1.0", "utf-8", "yes");
6.          xmldoc.AppendChild(node_dec);
7.          SessionUser =
    xmldoc.CreateElement("SessionUser");
8.  //如果找不到GUID相對應的User
9.          if (id == 0)
10.         {
11.           user = xmldoc.CreateElement("member");
12.           user.InnerText = "null";
13.           SessionUser.AppendChild(user);
14.           xmldoc.AppendChild(SessionUser);
15.         }
16.         else
17.         {
18. //如果User已離職或離校
19.           if (disabled == true)
20.           {
21.             user = xmldoc.CreateElement("member");
22.             user.InnerText = "null";
23.             SessionUser.AppendChild(user);
24.             xmldoc.AppendChild(SessionUser);
25.           }
26.  //GUID對應到User且User身分是在職或在學
27.           else
28.           {
29.   //產出member屬性欄位
30.         user = xmldoc.CreateElement("member");
31.           user.InnerText = member.id;
32.           SessionUser.AppendChild(user);
33.     //產出其他欄位
34.           username[姓名]、 type [身分] 、
35.           staffId [人事代碼/學號] 、idNo [身分證] 、
36.           guid [User登入時的GUID] 、userIP [登入IP]、
37.           logDate [登入時間] 、disabled [帳號是否停用]、
38.           minutesDiff [有效時間] 、unit [User單位代碼]
```

```
39.                 }
40.             }
41.             //產出結果XML回傳給Client
42.             return xmldoc.OuterXml;
43.         }
44.     }
```

Client 端關鍵程式碼中，Client 依據 Web Application 本身撰寫的語言來 Parsing(解析) SSO Server 回傳的 XML 檔，進一步得知使用者的身分。以下是以 C#為例 Parsing(解析) SSO Server 回傳的 XML。

```
1.  protected void Page_Load(object sender, EventArgs e)
2.  {
3.   //取得User 登入EIP的GUID
4.   string guid= Request["guid"];
5.   //宣告XML物件
6.   XmlDocument doc = new XmlDocument();
7.   //指定到SSO Server取得XML檔
8.   doc.Load(
9.       //詢問SSO Server該GUID是哪一個User
10.
    "http://eip.tnua.edu.tw/Portal/CheckGUID?memberLog.guid="+guid
11.         );
            //Parsing XML member attribute欄位資料
12.  string mail =
    doc.SelectNodes("//member").Item(0).InnerText;
13.  //Parsing XML ip attribute欄位資料
14.  //接續Web Application本身的登入驗證模式
15. }
```

3.4 資訊安全規劃

如第 2 節說明，使用帳號資訊存放於 DB 相對存放於 LDAP，俱有存取控制較不安全缺點 ，所以本系統在維護資料安全性上有規劃，相對應的配套「資訊安全規劃」。設計有

1. 非法登入通知:一小時內超過 3 次登入失敗，即會透過 Email、簡訊。如圖 8 所示：



圖 8 非法登入通知

2. 不准許多重登入:同一時間只能准許同一個帳號進行登入 EIP 系統、如果多重登入最先登入的用戶，會被登出。如圖 9：

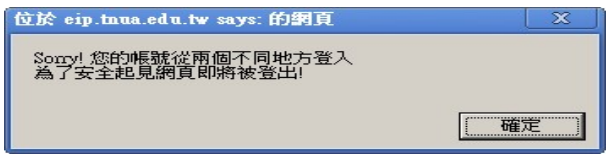


圖 9 多重登入通知

3. Access Control List (ACL):啟動 IP Tables 只准許合法的 IP 進行 GUID 的 Query。
4. 敏感資料加密:使用者密碼採用 Base64 進行加密。
5. LOG 記錄使用者登入留有 LOG 記錄；使用者 SSO 登入不同資訊系統留有 LOG 記錄。

4. 開發成果

校務行政資訊系統單一簽入，與帳號功能整合個人化入口網站開發之過程，EIP 資料來源的確認與人事資料較正，教師身分(專任教師、兼任教師)、職員身分(人事系統職員身分、教師兼一、二級主管)、學生身分；SSO 的安全登入機制、帳號密碼管理(密碼強度、密碼時效性、忘記密碼處理流程、修改密碼機制)、與新舊 LDAP 資料同步、原有系統使用 LDAP 認證轉移至 EIP LDAP、EIP 的版型架構、EIP 提供 Portlet 的服務、美術編輯及系統推廣教育訓練…等，是單一簽入與帳號功能整合所需規劃之開發細節，每一步驟確認才能完整整合校務行政資訊系統單一簽入。

校務行政資訊系統單一簽入，與帳號功能整合個人化入口網站(Portal)，於本校建立之校園資訊入口網(Information Portal of Taipei National University of the Arts, 簡稱 iTNUA)，iTNUA 單一簽入入口網自行開發建置(校園資訊入口網站 http://eip.tnua.edu.tw/)，於 2012 年 7 月開始進行開發研究，完成單一簽入入口網已建置完成，並自 2013 年 6 月開始上線啟用。

帳號密碼登入、密碼查詢及及 EIP 操作頁面如圖 10-圖 12，並將所有系統的訊息統一集中到入口網，用戶只須登入到入口網，便可存取內部被授權的各類資源，並設計於 EIP 頁面框架與顯示分割功能頁面(Portlet)[9]。目前已經成功整合的校務行政資訊系統如下:

1. 教務系統：含開課查詢、學籍、研究生學位考、成績查詢、畢業審查及離校系統…等。
2. 學務系統：學生獎懲、請假、兵役、獎學金、操行、宿舍管理系統…等。
3. 總務系統：薪俸查詢、停車證申請、場地租借、悠遊卡掛失系統…等。
4. 資訊相關系統：電子郵件信箱、電子報系統、簡訊發送系統、校園無線網路系統…等。
5. 人事相關系統：人事系統、差勤系統…等。
6. NAS、卡務系統、門禁系統 、圖書館自動化系統、教師自我評鑑系統、數位學習平台人事相關系統…等。



圖 10 系統登入首頁



圖 11 忘記密碼查詢



圖 12 EIP 操作頁面

5. 結論

iTNUA 單一簽入入口網自行開發建置，運用 OpenLDAP 原理延伸出的目錄服務管理可以大幅降低軟體建置成本，並將資源集中，各資訊系統的程式開發語言皆有支援 LDAP API，可快速的修改系統認證機制，進一步達到單一登入（Single sign-on）的運用。另達成主要目的與效益為:

1. 以 OpenLDAP 目錄服務為主要存取認證中心，來達成使用者單一簽入（SSO, Single Sign On）的目標。簡單的來說，使用者僅需一組帳號與密碼，即可進入已整合之各系統網站。
2. 不需要以不同的帳號密碼，重複登入各系統網站，解決教職員及學生記憶多組帳號及密碼的困擾，減少忘記密碼情況之發生。
3. 登入 iTNUA 單一簽入資訊入口網後，每位使用者輕易快速的開啟校內提供各系統網站之服務，獲得個人及各相關單位所發佈之資訊，有效提升學校所提供 e 化服務之使用率。

更重要的自主開發除了能節省開發費用，效能與功能符合業務單位需求，且能精進各系統開發人員之技術能力，亦能熟稔系統之實質架構。本論文在於本校全面性自行開發與研究 EIP 與 SSO，得就開發之成果得以呈現與揭露核心技術於論文，並廣為推廣學校與企業應用。

參考文獻

[1] 周盟淵, “校務行政系統帳號整合,” 國立師範大學電子計算機中心技術文件，2011年3月25日.
[2] 楊世帆、劉泳霖、方怡雯、蔡旭昇, “結合LDAP之校園電子郵件系統,” 第三屆離島資訊技術與應用研討會，pp. 372-377, 2003年6月.
[3] LDAP 入門, http://www.l-penguin.idv.tw/ article /ldap-1.htm, 查詢時間 2013年6月.
[4] Tom Jackiewicz, “Deploying OpenLDAP,” New York: Apress, 2004.
[5] 蔣大偉, “LDAP系統管理,” Taiwan Branch: O'Reilly, 2003.
[6] LDAP入門, http://www.l-penguin.idv.tw/article/ldap-1.htm, 2008.
[7] OpenLDAP Foundation, OpenLDAP Software 2.3 Administrator's Guide, http://www.openldap.org/ doc/admin23/index.html, 2008/2012.
[8] 廖文淵, “Single Sign-On(SSO)的優越融合－以IBM WebSphere Application Server V. 5和Lotus Notes/Domino 6為例,” 臺北: 資策會數位教育研究所, 2004/2012.
[9] Portals and Portlets: The Basic, http://editorial.mcpressonline.com/web/mcpdf.nsf/ wdocs/5232/$FILE/5232_EXP.pdf, 2006/2012.

選課系統問題分析及其解決方案

賴秀香　　蔡錫鈞
國立交通大學資訊技術服務中心
carollai@nctu.edu.tw, sctsai@cs.nctu.edu.tw

摘要

近年來國內大學對於相關經費是錙銖必較，不可能僅為了解決選課系統某幾天的高峰期，就花大筆經費添購設備。因此，無法透過增購及置換設備來改善選課系統緩慢及效能不足的問題。我們藉由虛擬技術的支援，採用低成本、不需額外經費的方式，解決選課系統的效能問題。

本文描述解決交通大學選課系統效能問題所實施的三個階段改善方案，從現況描述、問題分析至解決方案，相信這些經驗可提供給面臨類似問題的機構做為參考。

關鍵詞：選課、複寫、Nginx、負載平衡。

Abstract

In this article we show how to resolve the performance problem of online elective system without extra budget. We believe this will provide a very useful guideline to troubleshoot similar performance problems.

Keywords: online elective system, load balance.

1. 前言

許多大學的選課系統都有個一直存在的共同問題，就是每當選課期間，大批的學生同時湧入選課系統時，選課系統就會變得十分緩慢，緩慢到學生無法順利選課，嚴重時甚至會當機而無法使用。通常解決系統緩慢或系統效能不足，最先被提出的方案大都是增購或置換設備。在經費縮編、凡事錙銖必較的今日，花大筆經費添購設備，卻僅為了解決選課某幾天的高峰期?這樣的方案通常都不會被採納，而且其投資效益有限。而選課系統能否正常運作，直接關係著學生是否能選到課程，為確保學生選課的權益，如何維持選課系統於選課期間能順利運作，就成了各大學計算機中心的一個重大的課題。

對於一個每年只有幾個特定時段才會大量使用的系統進行測試及除錯原本就不是件簡單的事，因為使用量不大時，問題是不會出現的，況且該系統已歷經不同的開發者及管理者，問題的掌握更是具有挑戰性。

交通大學資訊技術服務中心對於這個問題進行了三個階段的改善方案來解決選課系統的問題。首先我們釐清瓶頸的來源，並發現連線的負載須先解決，透過模擬壓力測試，我們適度增加 Web 主機，以三台實體機搭配兩台虛擬主機將網路大量連線的瓶頸解決。之後我們發現資料庫是另一個瓶頸的來源，經過分析資料庫讀和寫的比例，我們發現寫資料到資料庫的比例是相對很低的，於是我們複製資料庫到多台虛擬機，以分散讀取資料庫的負擔，再使用一台虛擬機負責將選課資料寫入資料庫，並將資料同步，取得一致性。至此我們已將選課系統常見的瓶頸解除，即使在尖峰時段系統塞車的問題已不復見。然而在這過程中衍生了另一問題，使用者經過一段時間後會被系統登出，亦即 session 無法共用的問題，於是我們導入 Nginx 的技術將上述問題一併解決。總之，透過新興的網路及虛擬技術，我們以很經濟的方式，有效地解決了選課系統常見的效能及穩定問題。

本文的架構如下，在第二節我們介紹解決 Web Server 的負載問題。第三節介紹資料庫瓶頸問題的解決方式。第四節討論排除 session 共用的問題。第五節是本文的總結。

2. 第一階段：Web Server 負載問題

2.1 現況描述

造成選課系統緩慢的可能原因很多，首要先找出影響系統效能的瓶頸為何。我們採用一般的做法，針對選課系統進行壓力測試，以瞭解選課系統可能的效能瓶頸。壓力測試需在與目前運作系統相同的環境下進行，原本選課系統的主機架構是兩台 Web 主機及一台 Database 主機，而當時只有一台相同規格的 Web 實體機可利用，以當下的經費狀況也不容許添購主機，只有一台 Web 實體機的狀態下是無法以相同環境模擬下測試。選課系統原本的主機架構圖如圖 1 。



圖 1 選課系統原本主機架構圖

2.2 問題分析及解決方案

由於本校資訊技術服務中心已導入虛擬技術，在虛擬技術的支援下，複製多台與選課系統 Web Server 相同環境的虛擬主機進行壓力測試。壓力測試的過程由一台 Web Server 陸續增加 Web Server 的數量，並針對不同的同時上線人數來測試。圖 2 為壓力測試結果，結果反應增加 Web Server 數量能有效的降低平均回應間隔時間，並提高使用人數。依壓力測試結果顯示原本選課系統兩台 Web Server 無法應付尖峰時間大量的使用者，以至於 Web Server 反應間隔時間增加而傳回大量的 500 錯誤。根據壓力測試的結果，增加至四台 Web Server 雖足以應付選課系統尖峰時間的人數，但為了能再降低平均回應間隔時間，將選課系統增加至五台 Web Server。選課系統 Web 主機由原本兩台實體機，增加一台備援機，調整成三台實體機，再搭配兩台虛擬機，圖 3 為調整後的選課系統主機架構圖。

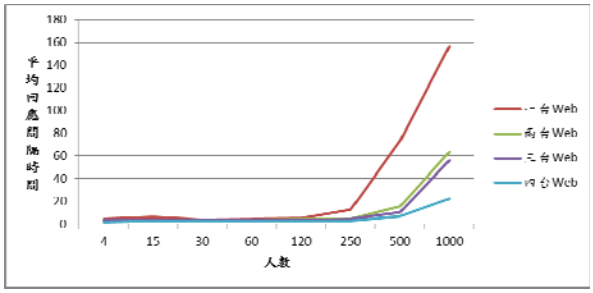


圖 2 壓力測試結果



圖 3 選課系統第一階段調整後主機架構圖

調整 Web Server 主機數量後，在選課尖峰時刻當機的次數明顯減少，系統瀏覽速度也有顯著的改善，學生也能順利選課。但是，在系統調整後，卻引發了另一個問題，課務組後端管理系統在選課尖峰時間會有無法使用的狀況。因此，需要再研擬下個階段的問題改善方案。

3. 第二階段：Database Server 負載問題

3.1 現況描述

課務組所使用的後端管理系統是由 Visual Basic 6.0 開發的 Application 系統，該後端管理系統是透過課務組桌機直接連至資料庫存取資料。為什麼後端管理系統會於選課尖峰時間無法使用?針對 Database Server 做觀察紀錄，以了解問題發生原因。

選課系統使用的 Database Server 是微軟的 MSSQL 2000 Server，選擇 MSSQL 本身提供的 SQL Profiler 工具，並搭配一些 MSSQL 監控程式，來確認後端管理系統無法使用的問題點。監控的數據顯示，後端管理系統在無法使用期間，Database Server 之 wait type 有大量 LATCH_* 、LCK_* 、PAGELATCH_*、PAGEIOLATCH_*、CXPACKET 等訊息。微軟亞太資料庫技術支持組官方博客網站中有提到：「Latch 是 SQL server 內部用來同步資源訪問的一個資料結構，和作業系統的 critical section 或 ReaderWriterLock 類似。Latch 保護了那些想保護的資源，使得訪問同步有序。比方說，當某個執行緒獲得某個資源的 Latch 的獨佔使用權的時候，別的執行緒如果也需要訪問這個 latch 則它必須等待[1]。Database Server 出現大量 Latch 相關的訊息，表示 Database Server 的資源已無法負荷 5 台 web server 及後端管理系統同時使用。

3.2 問題分析及解決方案

經由分析監控數據得知，選課 Database Server 有很大的比例都是在提供 Web Servers 的資料讀取，寫入的比例相對的很低。因此，我們採取的作法是將讀取及寫入資料分別使用不同 Database Server 的方式，以期能分散資料庫的負載量。讀取及寫入資料庫的方案，需要同時搭配「讀取資料庫」、「寫入資料庫」與「同步資料的機制」。「讀取資料庫」是利用原本在運行的選課系統 Web Server 虛擬主機再加裝 MSSQL 2005 Server，Web 與 資料庫同在一個主機上，這樣的架構不僅能節省建置 Database Server 的成本，還可以加速資料讀取速度；「寫入資料庫」則由原選課系統 Database Server 負責處理；「同步資料的機制」是使用 MSSQL 提供的交易式複寫機制。

圖 4 是選課系統「讀取」及「寫入」資料分別使用不同資料庫的架構圖，選課系統 Web Server

在讀取一般性資料時，是透過本機 Database Server(local DB)取得資料；寫入資料還是維持寫入選課系統 Database Server。然而遇到重要資料需要確認時，還是必須透過選課系統 Database Server 取得資料，避免因資料同步時差而產生其他問題。



圖 4 選課系統「讀取」及「寫入」資料分別使用不同資料庫的架構圖

MSSQL 的複寫機制中有三種角色，分別為「發行者」、「散發者」、「訂閱者」。圖 5 是 MSSQL 交易式複寫架構圖，「發行者」產生發行集，發行集可以是資料表、預存程序、檢視表...等。「散發者」會先利用「快照集代理程式」取得一份「發行者」所提供的發行集快照，之後只要發行集有任何交易紀錄，會再透過「紀錄讀取器代理程式」將交易紀錄傳送至「散發者」端。「散發者」確認與各「訂閱者」連線正常，會透過「散發代理程式」將發行集資料送至各「訂閱者」資料庫中。

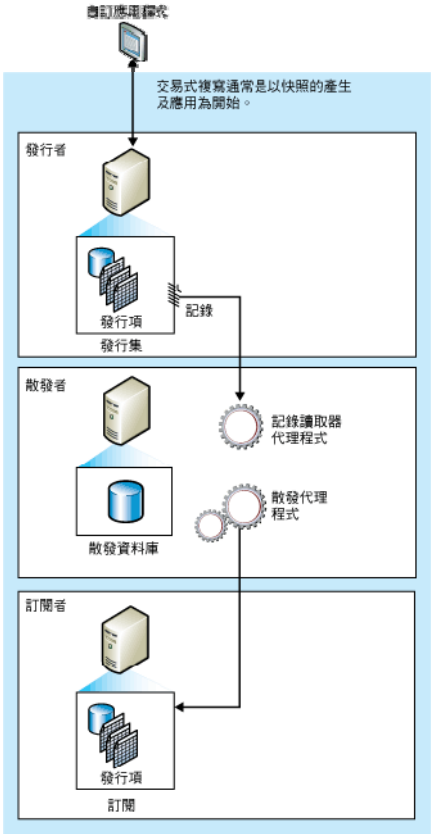


圖 5 MSSQL 交易式複寫架構圖[2]

「發行者」及「散發者」原可以同時由一個 Database Server 擔任，但「散發者」在記錄交易紀錄資料及散發資料給各「訂閱者」時會影響正式資料庫的運作，因此，如圖 6 所示，選課系統的資料複寫架構建立了三種角色的 Database Server 各司其職，將選課系統 Web Server「寫入」到選課系統 Database Server 的異動資料，複寫回 Web Server 的資料庫(local DB)中，以供「讀取」使用。

實行讀取及寫入資料庫的改善方案，不僅改善了後端管理系統於選課尖峰時間會無法使用的問題，也大幅改善 Web Server 在尖峰時間，瀏覽速度會降低的狀況，尖峰時間使用選課系統已與一般時間無異。

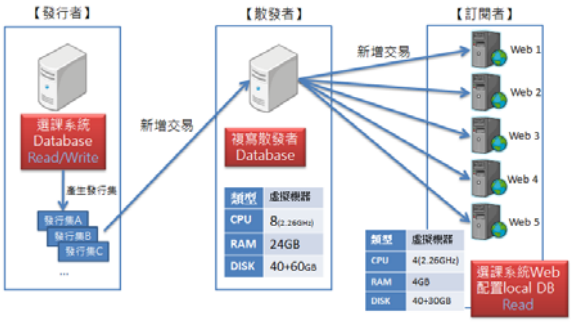


圖 6 選課系統資料複寫架構

4. 第三階段：Session 無法共用問題

4.1 現況描述

選課系統歷經兩階段改善方案後，已無使用者反應系統過慢問題，但卻陸續有使用者反應會有登入選課系統後隨即被登出的現象。經由交叉比對 IIS Log 與使用者登入資訊 Log，發現同一個帳號登入前後分別使用不同的 Web Server。當時，選課系統 Web Server 是用 DNS Round Robin 的方式隨機分配給使用者，只要網路中斷或者其他原因導致重新分配 Web Server 時，使用者會因為登入的 Session 不存在而被登出。一般解決此問題常使用的方式是將所有 Web Server 的 Session 共用就可以解決，但選課系統的開發語言是 ASP，ASP 的 Session 並不像 PHP 是以檔案形式儲存，而是存放在主機記憶體中，無法直接共用。除了共用 Session 外，還有另一種解決方式，讓同一個 IP 固定連相同的 Web Server 也能解決這個問題。Nginx 是兼有負載平衡的 Web Server，它的負載平衡機制只要設定成 ip_hash，就可以將同一個 C 網段的 IP 指向到相同的後端 Web Server。於是我們決定導入 Nginx 的負載平衡機制來解決 Session 的問題。

4.2 問題分析及解決方案

圖 7 是選課系統導入 Nginx 後的選課系統架構圖，選課系統 Web Server 被建構在 Intranet 中，使用者只能透過 Nginx 指向到選課系統 Web

Server，所有與 Web Server 的連線也都只能透過內部網路溝通，這樣的架構除了能解決 Session 無法共用問題，也能增加選課系統 Web Server 的安全性。

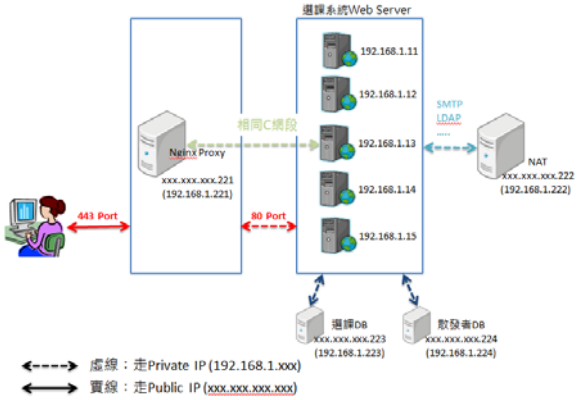


圖 7 選課系統導入 Nginx 架構圖

5. 結論

在科技日新月異的年代，系統為了因應快速變遷的環境，時時刻刻都可能面臨一些莫名、未知的問題。而且經常一個問題解決，卻又引發另一個問題的發生。解決問題除了憑藉系統負責人日積月累的經驗，再搭配他人研究發展的技術，慢慢的抽絲剝繭分析問題，找出可能的解決方案。找出快速又有效的解決問題方式，是所有系統負責人都希望的，交大在解決這個問題的過程中獲得許多寶貴的經驗，希望能提供給面臨類似問題的機構一個參考。

參考文獻

[1] 什麼是 PAGELATCH 和 PAGEIOLATCH, http://blogs.msdn.com/b/apgcdsd/archive/2011/11/29/pagelatch-pageiolatch.aspx, Retrieved July31, 2013.

[2] Transactional Replication, http://msdn.microsoft.com/zh-tw/library/ms151176.aspx, Retrieved July31, 2013.

應用 QR Code APP 在校園 E 化教室服務和管理之研究

陳明芳
國立臺灣師範大學資訊中心
mfchen@ntnu.edu.tw

摘要

由於智慧行動裝置的普及，APP 在行動商務、教育、和資訊管理系統的應用已幾乎是無所不在，加上 QR Code 高負載資料量、高安全性、高容錯性等強大的功能，一個 APP 結合 QR Code 掃瞄處理的資訊系統應用，將可達到資訊快速存取，資料即時處理和資訊自動化的目標。本研究以雛型系統設計方法，開發一個 QR Code APP 應用程式，使用行動裝置照相功能和 QR Code Scanner APP，快速讀取 E 化教室 QR Code 的資料和即時解碼，使用者可利用維修看板或手機簡訊來請求 E 化教室問題的支援，報修資料傳送到後端資料庫後，再結合 Web 網站維修電子看板的即時顯示和自動更新，維修人員可即時掌握 E 化教室的報修狀況並盡速加以處理，以快速回應的機制提升 E 化教室服務的品質，本雛型系統並配合 Web 後台管理系統更新 E 化教室維修進度，來加強 E 化教室的管理，唯有資料的快速存取和即時更新，才能達到提昇 E 化教室教學和教育品質的目標。

關鍵詞：智慧行動裝置、APP、QR Code、E 化教室、電子看板系統

Abstract

With the popularity of smart mobile devices, APPs are widely used among mobile commerce, education, and information management systems. Since the QR Code has great capabilities including high capacity of data, high security, and high error tolerance of the code, an APP combining QR Code scanner can achieve the goal of immediate information retrieval, real time data processing, and information automation. The approach of this study is by using a prototyping mechanism to develop a QR Code APP. This APP uses the camera on a smart device that associates with a QR Code scanner APP to read the E-Classroom QR Code data and decode it instantly. Users can either choose to post on the repair board or send a text message to report issues with the E-Classroom and to seek further assistance. Once the repairing information is stored into the database, a web-based electronic Kanban system can show the reported information of the E-Classroom in real time and update maintenance information automatically. Since the technical staff can watch the repairing status and deal with the problem as soon as possible, this quick-response mechanism can promote the service quality of the E-Classroom. This prototype is also associated with a web-based backend system to maintain the repairing progress of the E-Classroom to enhance the management. By allowing the E-Classroom repairing information to be retrievable and updated instantly, the teaching and educating quality of the E-Classroom can be greatly increased.

Keywords: Smart Mobile Device、APP、QR Code、E-Classroom、Electronic Kanban system

1. 研究背景和動機

由於電腦和電化教學設備的普及，在台灣各級學校建了許多 E 化教室，以提升老師教學的環境和品質。E 化教室建置完成初期，對老師教學確實有非常大的幫助，但隨著設備的老化，電腦和電化設備問題愈來愈多，如何讓 E 化教室持續運作下去，是學校經營 E 化教室的目標，對學校行政和管理人員更是一大考驗。

校園 E 化教室最重的特性有二個: 第一是每間教室一套電腦和電化設備，如投影機和音控系統等，主要是提供老師教學用。第二是 E 化教室分散在全校各教學大樓中，在教學支援上因距離問題，有一定的空間和時間上的限制。依據[1]和[2]的論文研究，電腦化的教室能夠成功的主要關鍵因素包括: 設備的維護和快速回應的支援。因此建立一套合理的維運管理機制，才能讓校園 E 化教室達到永續經營的目標。

本研究的動機在改善目前 E 化教室因距離問題造成問題報修費時，並利用當今行動裝置已無所不在的優勢，加上 QR Code 高負載資料量、高安全性、高容錯性等強大的功能[3][4]，開發一個行動裝置 APP 結合 QR Code 掃瞄處理的程式，以達到資訊快速存取，資料即時處理的自動化目標，並結合後端網站和資料庫，使用即時的維修電子看板，讓維修技術人員可以快速回應，充份利用現代資訊和電子科技，再造校務行政處理的流程[5]，以提升服務的品質及提高 E 化教室管理的效率，達到提昇 E 化教室教學和教育品質的目標。

2. 文獻探討

本研究的目的是利用目前普及的智慧行動裝

置，開發一個簡便的 APP 程式，結合 QR Code Scanner 程式，讀取事先設計好並貼在校區 E 化教室的 QR Code，做即時的問題回報和資料收集後之後續的維修和管理。因此我們主要討論的研究範圍包括: 智慧行動裝置、行動裝置 APP 應用程式、QR Code 的應用、和 Web 技術的應用。

2.1 智慧行動裝置

由於電子和資訊技術的一日千里，3C 產品愈來愈小，行動裝置因應而生，行動裝置顧名思義是攜帶方便的設備，最早被大家接受的產品是 PDA(Personal Digital Assisstant)，以個人資訊管理為主，如行事曆和行程管理、通訊錄、待辦事項、筆記本等功能[6]。

個人電腦的發展由桌上型、到筆電、到小筆電(Net PC)，其明顯的趨勢是體積愈來愈小，行動化的能力愈來愈好。當螢幕觸控技術誕生後，電腦的鍵盤和滑鼠不再是必需品，平板電腦產品也因此而更加成熟，對電腦使用族群來說，平板電腦便成為了另一個重要的隨身行動裝置。

行動通訊系統起源於 1980 年代，在不到 20 年的時間，從第一代到第三代，技術達到成熟，手機更是五花八門，在使用者的需求愈來愈多，手機和 PDA 功能結合的手機因應而生，這就是智慧型手機普及的原因，iPhone、Samsung Galaxy、HTC、Sony、Windows Phone、Blackberry…等產品早已無所不在地深入人類的生活之中[6][7]。

2.2 手機 APP 應用程式

APP 是 Application 的簡稱，在電腦的領域中，它是指一個應用程式，自從 Apple 2007 年 iPhone 上市後，建立了一個應用程式的發佈平台 APP Store，因此 APP 便成為了 Apple 手機或平板電腦上應用程式的代名詞。

Google 公司在 2007 推出以 Linux 為基礎的 Android 行動平台作業系統，這是一套開放原始碼的系統，免費提供給有興趣的軟體和行動裝置開發廠商，因此 HTC、Samsung、Sony 等大廠都採用 Android 系統，開發許多手機和平板電腦等行動裝置產品，因為此平台為開放架構，開發工具也都是免費的，因此自 2009 年 Google 推出 Android Market 應用程式商店後，各種 Android 應用程式如雨後春筍般地迅速長成，和 Apple 的 APP Store 形成兩大陣營互相抗衡，Google 更將 Android Market, Google Music 和 eBookstore 三個平台整合，於 2012 年 3 月推出 Google Play，因此現在 Android 行動裝置的應用程式平台已變成 Play 商店[6]。不管是 APP Store 或 Play 商店，上面所提供的都是行動裝置上的應用程式，或簡稱 APP，APP 這個名詞似乎再也不是 Apple 專屬專用的 Slogan 了。

2.3 QR Code 的應用

在目前市面上的商品，常見的條碼辨識大多數還是使用一維條碼為主，其簡短且掃瞄器讀取容易，結帳或盤點迅速，但其最大的缺點是資料容量小，污損就難以讀取。QR Code 解決了一維條碼的缺點，因此目前 QR Code 的應用系統，普遍應用到市場行銷[3]、行動商務和行動資訊系統[4][8]-[12]、GPS 應用[13]、教育教學[14][15]等各種不同領域。尤其 QR Code 的高容量和高容錯性，加上行動裝置的普及，對於其在不同領域資訊系統的創新和應用上，充滿了各種可能性。

2.4 Web 技術的應用

最近幾十年，Client-Server 架構的資訊系統已廣泛被使用，尤其是以 Web 技術為基礎的三層式資訊系統。由於 Android 開發平台亦支援 HTTP 協定[7][16][17]，因此本研究不管是 APP 程式，或是後台的管理系統，都運用了 Web 的三層式架構技術，解決了二層式主從架構系統中 Client 端程式佈署之困擾，並透過網際網路無遠弗屆的能力，達到資訊系統自動化的目標。

3. 系統開發環境

本系統開發環境主要分為兩部份，一是使用者端的行動裝置 APP 程式，二是維修電子看板和後台管理者端的 Web 管理程式，後端資料庫則使用 MySQL，說明如下:

3.1 行動裝置端

使用 eclipse 開發環境，加上 Android SDK 和 java 程式語言，設計一個行動裝置上的 APP 程式，可以在 Android 平台的手機和平板電腦上使用。主要使用的技術包括: Google ZXing Barcode Scanner、HTTP Protocol、HttpClient、Telephony SmsManager、JSON 格式資料傳遞等[7][16][17]。

3.2 維修電子看板和後台管理端

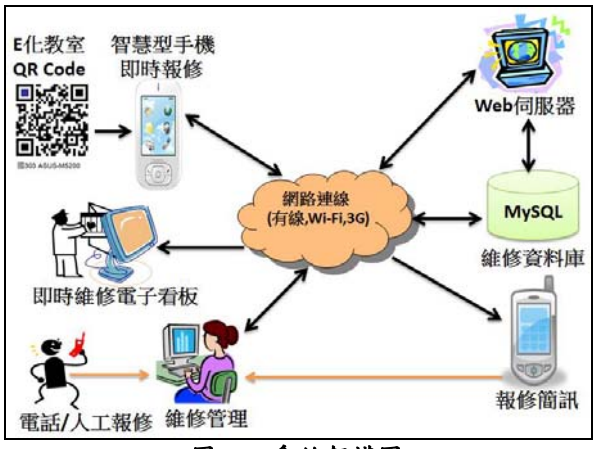
使用 CodeCharge 4.0 版快速開發環境和產生 PHP 程式語言，利用 Web 技術和 Web Server，設計即時顯示的維修電子看板和後端的管理平台，連結到 MySQL 資料庫做資料的有效管理。維修電子看板的設計主要在仿傚豐田式生產管理的即時化和自働化的精神[18]，並利用高速的網路讓資訊即時傳送並顯示到維修人員的螢幕看板上。

4. 系統架構和設計

4.1 系統架構

本系統功能面主要成三大部份: (1)行動裝置 APP: 使用者可利用 E 教室的 QR Code，透過 APP 和 QR Code 掃瞄程式，即時傳送到後端資料庫，或者用手機簡訊報修。(2)即時維修電子看板: 即時將

資料庫報修的資料，顯示到電子看板螢幕上，並使用網頁 Refresh 自動更新。(3)後台維修管理系統: 管理維修進度和人工或電話報修資料的建檔，使維修電子看板保持最新正確的資料，系統架構圖如圖一所示。



圖一: 系統架構圖

4.2 系統設計

本研究的主要目的在充份運用 QR Code 的 Quick Response 特性，以期快速回應和即時支援，達到提升服務品質的目的。因此在系統設計方面，主要的考量項目包括:

4.2.1 QR Code 設計

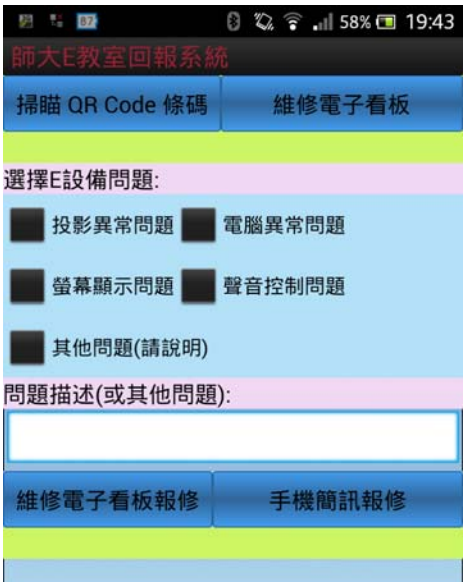
QR Code 的好處之一是可以儲存大量的資料，因此我們針對 E 教室維修和管理上的需求，將教室名稱、電腦型號和財產編號放到 QR Code 裡，如圖二，在條碼下方我們並加入可讀性的資訊，在報修和張貼管理上比較不容易混淆[19]。教室名稱代表大樓和地理位置，方便維修人員辨識迅速前往處理。財產編號則為預留資訊，對未來學校財產管理上應該有所幫助。



圖二: E 化教室 QR Code 設計樣本

4.2.2 行動裝置 APP 介面設計

人機介面的設計是 APP 程式是否實用的重要關鍵之一[20]，本系統的最高目標是快速回應，所以介面的設計愈簡單愈好，使用者在同一畫面即可操作完成，如圖三所示。



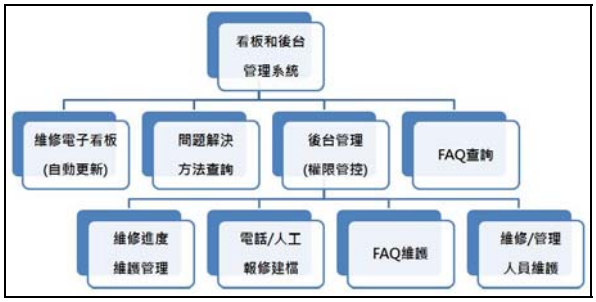
圖三: APP 介面設計

4.2.3 資料庫設計

資料庫的設計主要紀錄 E 化教室的 QR Code 資料、使用者報修問題、及維修進度和紀錄等，因此資料表包括: 問題和維修資料表、問題代碼表、維修進度代碼表、常問問題資料表、及維修和管理人員資料表。

4.2.4 電子看板和後台管理設計

為達到問題的快速處理，我們利用 Web 的技術，做一個即時的維修電子看板，並使用網頁 Refresh 的技巧，隨時更新報修的維修狀況和進度，報修案件有所異動時，電腦亦可發出警訊音響，告知維修人員，使用者也可使用 APP 即時查詢維修電子看板的維修進度。後台管理系統，則由管理人員維護處理進度，及建立電話或人工報修的案件，以便即時顯示到電子看板上。維修電子看板和後台管理系統的功能架構如圖四所示。



圖四: 電子看板和後台管理系統功能架構圖

5. 系統實作和測試

本系統主要分為兩部份: APP 程式和後台管理系統，另外還必需安裝一支 third-party 的 QR Code Scanner APP 程式，其實作和測試如后:

5.1 APP 的安裝

為充份運用 Google ZXing Barcode Scanner 的功能，本 APP 程式「師大 E 教室回報系統」參考了[17]的設計方法，呼叫第三方二維條碼掃瞄功能的 APP，讀取掃瞄結果作解碼再後續處理，本 APP 程式搭配使用的是 QuickMark APP，如圖五所示。



圖五：師大 E 教室回報系統和 QuickMark

5.2 APP 維修電子看板報修測試

「師大 E 教室回報系統」APP 主要在提供一個 E 化教室問題快速回報的管道，維修電子看板報修是利用 HttpClient 把資料傳到後端資料庫，並迅速顯示到即時維修電子看板上。使用者也可用 APP 維修電子看板功能，查看報修情況和目前的維修進度。測試畫面如圖六。



圖六：維修電子看板報修

5.3 APP 手機簡訊報修測試

第二種 E 化教室問題報修的方式，就是透過手機發送簡訊，因此行動裝置必需支援 Telephony 發送簡訊，一般平板電腦就無法傳送簡訊，另必需考慮通訊費用的問題，因此發送簡訊前 APP 會顯示警訊，讓使用者確認是否要使用此功能報修，如果手機月租方案是吃到飽的，使用者就不會有所顧慮了。測試畫面如圖七。



圖七：手機簡訊報修和接收

5.4 即時維修電子看板測試

要達到 Quick Response 的目標，除了使用行動裝置和 QR Code 迅速回報問題外，我們維修中心也必需立即看到回報的問題，即時維修電子看板就是這個目的。維修電子看板每 60 秒自動 Refresh 更新一次，當未完成的案件筆數增加時，則播放警訊音樂，通知維修人員立即前往處理。行動裝置端的測試畫面如圖八。



圖八：即時維修電子看板(手機瀏覽器)

5.5 後台管理系統測試

後台管理系統主要負責維修進度的即時更新，電話和人工報修的資料建檔，另外對 FAQ 的建檔，有助於使用者提昇自行解決問題的能力。使用者維護則是維修人員和管理人員的帳號建置和權限的設定，使系統的安全性更加完善。PC 端的測試畫面如圖九。



圖九：後台維護管理系統(PC 瀏覽器)

5.6 APP 在不同 Android 平台的測試

Android 為開放式平台，各大廠都各自推出許多不同款式的產品，但為彰顯各家公司產品的特色，難免做些客制化的修改，為確保 APP 程式在大部份廠牌上執行的可行性，我們做了一些不同平台的測試，如表一所示，結果 APP 都可正確執行。

表一：APP 在不同 Android 平台測試

行動裝置廠牌型號	O.S. 版本	QR Code 掃　瞄	使用電子看板報修	使　用簡訊報修
Sony Xperia SL	4.1.2	OK	OK	OK
HTC One V	4.0.3	OK	OK	OK
Samsung GT-S5660	2.3.3	OK	OK	OK
ASUS Eee Pad	4.0.3	OK	OK	N/A

6. 結論和未來工作

本研究設計一個行動裝置 APP，運用 QR Code 的優勢，配合即時維修電子看板和後台的管理系統，使 E 化教室的問題能夠快速回報，維修人員可以即時處理，以縮短維修服務時間，由系統實作和測試的結果，我們可以確定本研究之「快速回應」機制，確實可以在分散式的 E 化教室服務上，縮短維修支援時間，提高服務的品質，達到提昇 E 化教室教學品質的目標。

經過了系統的實作和測試，本研究在系統面的可行性已無庸置疑，但校務行政資訊系統的推行，最困難的部份在相關單位和使者的配合，以及主管的支持，才能使系統和行政工作順利推行，這是後續需要努力去建置和宣導的工作。

展望未來，由於 QR Code 的優點和行動裝置成本的降低，結合 QR Code 的行動商務和應用系統將會愈來愈普遍被接受和使用，例如餐點訂位和訂購服務[4][8][9]、設備管理和定位[11][13]、觀光導覽和訂票服務[12]、教育與教學應用[14][15]等。至於 QR Code 在校務行政上的應用，本研究在 QR Code 的設計上，放置了財產編號，希望未來在學校財產管理的運用上，可發揮其功效，例如開發財產管理和盤點的 APP，將可使這項繁瑣且需要「行動」到全校各單位的工作，利用 QR Code APP 的快速回應，以提高行政管理上之效率。另外在系統的擴充充性方面，由於 iPhone 和 iPad 的普及，未來若能增加 iOS 平台之 APP，將可擴大系統的實用性，以提昇系統的使用效率。

誌謝

感謝中心同事蔡俊男先生在 CodeCharge 和 PHP 程式部份的協助及碁峰資訊股份有限公司提供多本 Android 程式設計樣書，使得本系統得以順利開發完成。

參考文獻

[1] 吳文中，班級電腦教學之研究－以台北市班班有電腦為例，碩士論文，國立台北師範學院，2002 年 5 月。

[2] 陳明芳，校園 E 化教室維運和管理之研究-以臺師大林口校區為例，2013 資訊技術應用和管理研討會，2013 年 5 月。

[3] 張育綺，QR Code 解碼創意: 連結行銷活動手法大揭密，PC uSER 電腦人，2012 年 11 月。

[4] 謝德鑫、朱庭輝，二維條碼行動化點餐系統建置與應用，高苑學報‧第十六卷第一期，第 234~256 頁，2010 年 3 月。

[5] 呂郁婷、柯奕佑、林宣宏、詹博州、鄭中川、黃國賢，以資訊管理系統為基礎之組織內部設備報修流程再造，2012 資訊教育與科技應用研討會，第 C2-21~C2-26 頁，2012 年 3 月。

[6] 淡江大學資訊概論教學團隊，資訊概論，碁峰資訊股份有限公司，2012 年 8 月。

[7] 楊丰盛，Android 應用開發揭秘，佳魁資訊股份有限公司，2010 年 11 月。

[8] 黃國光、黃志文、蔡宏村、沈佳宜、許聖農、陳善濟，整合應用 QR Code 於訂位作業之 PDA 無線點餐系統，第八屆離島資訊技術與應用研討會論文集，第 531-538 頁，民國 98 年 5 月。

[9] 孫培真、劉育杰，餐飲訂購系統 APP 之設計發，2013 資訊技術應用與管理研討會，2013 年 5 月。

[10] M. Vazquez-Briseno, J. Nieto-Hipolito, E. Jimenez-Garcia, Using QR Codes to Improve Mobile Wellness Applications, International Journal of computer Science and Network Security, Vol.10, No. 12, Dec. 2010, pp.50-54.

[11] D. Suharta, D. Putra, W. Buana, QR Code Application for Water Meter Recorder Based on Windows Mobile Platform, International Journal of Computer Science Issues, Vol.10, Issue 2, No. 5, March 2013, pp.7-15.

[12] M. Zhang, D. Yao, Q. Zhou, The Application and Design of QR Code in Scenic Spot's eTicketing System – A Case Study of Shenzhen Happy Valley, International Journal of Science and Technology, Vol.2 No. 12, Dec. 2012, pp.817-822.

[13] 謝睿桓、林璟筠、傅珊蓉、陳朝傑、張林煌，即時定位及應用 QR code 搜尋商品資訊，國科會計畫編號：NSC99-2815-C-142-008-E，國立台中教育大學資訊科學學系，2011 年 1 月。

[14] N. Soman, U. Shelke,S.Patel, Automated Examination Using QR Code, International Journal of Engineering and Advanced Technology,Volume-2, Issue-3, Feb. 2013, pp.622-627.

[15] C. Law, S. So, QR Codes in Education, Journal of Educational Technology Development and Exchange, Vol. 3, No. 1, Oct. 2010, pp.85-100.

[16] 文淵閣工作室，Android 初學特訓班，碁峰資訊股份有限公司，2011 年 12 月。

[17] I. Darwin, Android Cookbook, O'Reilly Media, 2011.

[18] 周姚君譯，圖解豐田生產方式，經濟新潮社，2007 年 10 月。

[19] http://blog.qr4.nl/QR-Code-Text.aspx，2013 年 7 月瀏覽。

[20] Ian G. Clifton, Android User Interface Design: Turning Ideas and Sketches into Beautifully Designed Apps , Addison-Wesley, May 2013.

改良式準隨機亂數株落演算法之組裝平行測驗

胡芸菁[1]　張庭毅[2]　呂易鄙[3]　鄭培成[4]
[1]國立彰化師範大學 數位學習研究所
[2,3]國立彰化師範大學 工業教育與技術系
tychang@cc.ncue.edu.tw
[4]健行科技大學 資訊管理系
pccheng@uch.edu.tw

摘要

本研究採用 Chang 及 Shiu 提出的株落選擇演算法(CLONAL)進行改善，以株落選擇演算法為基礎，結合準隨機亂數(Quasi-Random Number Generator，QRNG)之平行測驗組裝方式，提出準隨機亂數株落演算法(QRNG CLONAL)，除了可以同時建立多份平行試卷、解決循序組裝的不平等問題及減少限制式外，準隨機亂數機制可以進一步降低與目標測驗的均方誤差。經一系列實驗結果指出 QRNG CLONAL 不論在增加題庫試題數量、平行測驗數或有限制組裝時間的情況下，皆有利於組裝各種條件的平行測驗且有效維持測驗設計與品質。

關鍵詞：株落選擇演算法、試題反應理論、準隨機亂數、選題策略、平行測驗。

Abstract

The simultaneously construct IRT-based parallel tests problem requires large numbers of variables and constraints, which leads to high computational complexities and now there is no polynomial time algorithm that exists for finding the optimal solution. Recently, Chang and Shiu proposed an adapted CLONAL algorithm to simultaneously construct IRT-based parallel tests. Their scheme is more efficient than its predecessors in terms of deviation and performance. In this paper, a Quasi-Random Number Generator is used for improving Chang and Shiu's scheme, called Q-CLONAL for short. The proposed Q-CLONAL not only avoids the inequality problem in the sequential construction, solves the drawback of larger numbers of variables, constraints in the simultaneous construction, but also has a better performance. Comparing with Chang and Shiu's CLONAL, under various situations (item bank size, the number of parallel tests, and the limit of execution time), the proposed Q-CLONAL is more suitable than Chang and Shiu's CLONAL in constructing IRT-based parallel tests..

Keywords: clonal selection algorithm, item response theory, parallel tests construction, quasi-random number generator, item selection.

1. 前言

測驗提供客觀的檢視、做出決定、評估受試者學習成果和能力，而測驗組合也因測驗目的與受試者的不同而有不同需求。近年來，電腦化適性測驗(Computerized Aptitude Tests，CAT)結合試題反應理論(Item Response Theory，IRT)被應用在各領域的大型測驗中，如托福、GRE 及 GMAT 等考試。在教育評量的相關研究中，「如何建構理想的測驗，以符合測驗設計者施測目的」，是過去許多學者探討的重要領域。隨著應用層面越來越廣，組裝高品質的 IRT 測驗變得越來越重要。

IRT 主要以個別試題的觀點，將受試者在某一試題上的表現情形與潛在特質透過一條連續性遞增的數學函數來表示，稱為試題特徵曲線(Item Characteristic Curve，ICC)。

組裝測驗(test construction)即是在某個教學及評量目標的引導之下，製作一組測量試題，以作為測量工具。組裝前，會先定義目標測驗，指在組裝測驗前訂定一份測驗規格作為組裝測驗目標，通常所考慮的準則包括內容、技巧、題型和作答時間，稱為多樣性限制條件，而組裝後所產生的測驗必須和目標測驗規格近乎相同。過去的研究中，組裝測驗的方法有：(1)隨機選取法(Random)、(2)標準法(Standard)、(3)中間難度法(Middle Difficulty)、(4)上下法(Up And Down)、(5)最大訊息法(Maximum Information)等[13]，其執行時間短但其誤差大。從大量題庫中組出符合測驗需求的多樣性限制條件，為組合最佳化問題(combinational optimization problem)，屬於 NP-hard 問題。為了在有限時間內求得次佳解，因此學者利用概念啟發式演算法(Meta Heuristic Algorithm)，例如類神經網路(Neural Network)[32]、蒙地卡羅演算法(Monte Carlo Algorithm)[4]、禁忌演算法(Tabu Search)[17]、免疫演算法(Immune Algorithm)[20]、粒子群最佳化演算法(Particle Swarm Optimization)[42]、蟻群演算法(Ant Algorithm)[21]、蜜蜂演算法(Bees Algorithm)[30]、基因演算法(Genetic Algorithm，GA)[11, 14, 16, 22, 25, 33]、株落選擇演算法(Clonal Selection Algorithm)[8]等方法分別應用在組裝測驗上，相較於傳統的組裝測驗方式，能在有限時間內，所組出之測驗與目標測驗有較小之誤差。

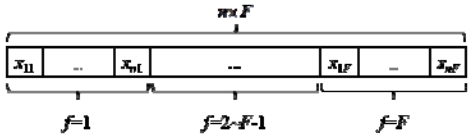
本研究利用準隨機亂數改善 Chang 及 Shiu[8]所提出的株落選擇演算法(CLONAL)同時組裝平行測驗方式。CLONAL 是經由 GA 演變後的方法，因為 GA 本質上不適合用來同時組裝多份測驗，因此是以循序組裝的方式，而 CLOANL 不但可以同時組裝 5 份試卷，且能降低與目標 TIF 的誤差值，根據 Chang 及 Shiu 實驗指出株落選擇演算法相較於基因演算法平均誤差少 8.28 倍。本篇進一步在 CLOANL 的初始化階段加入蒙地卡羅法中的準隨機亂數，稱為 QRNG CLONAL，更能增加平行搜尋機制與獨立發展的特性，且減少同時組裝平行測驗限制式過多的問題。本論文架構如下，第二節介紹平行測驗的起源、特性和步驟。第三節介紹本研究採用的株落選擇演算法、多目標組裝測驗的問題模型和改良型準隨機亂數株落演算法的詳細步驟。第四節將介紹實驗方法與實驗結果。最後一節則針對本文做討論與分析。

2. 相關研究

在實施測驗時，需要同時施測多份測驗的情況有：(1)週期性測驗、(2)給予不同受試者不同試卷以避免作弊、(3)包含前測和後測的二階段甚至多階段測驗、(4)多階段的適性測驗。目前大部分的平行測驗方法中，分為古典測驗理論(Classical Test Theory)與試題反應理論(Item Response Theory，IRT)。Armstrong 等人[2]使用古典測驗理論之試題指標，如鑑別度指標與難度指標，且結合 Network Flow 法再加上分數分佈指標(score distribution)、試題變異數(item variances)、試題與分數的相關(item-score correlations)等指標，提高了測驗平行的程度。由於 IRT 試題參數具有項目參數不變性、能力參數不變性與訊息函數功能，較優於古典試題理論，所以 IRT 試題參數逐漸成為主流。

平行測驗可分為循序組裝(sequential construction)與同時組裝(simultaneous construction)。Theunisse[36]使用數學規劃模型組裝 IRT 測驗時，採取隨機抽樣的組裝測驗方式，並且採用循序的方式進行，作法為組裝第一份測驗後，將題庫內用於組裝第一份測驗的試題排除，利用剩餘的試題組裝第二份測驗，用意是為了避免每份測驗試題重複。循序組裝測驗具備實作簡單與低運算量的優點，但組裝執行時間隨測驗多寡而增加，此外在組裝第一份試卷時，可能會將題庫內品質較好的試題先挑選出，導致優先組出的試卷品質最好，而後越來越差，這種情況稱為不平等問題(inequality problem)。若無法確保每張試卷品質一致，也無法測驗出受試者的學習情況，造成測驗間的偏差(bias)。

Armstrong 等人[2]的作法是在第一階段以循序的方式組裝多份平行測驗，第二階段將多份平行測驗的試題進行交換，以進一步降低整體誤差，但這樣的作法僅能稍微降低不平等現象所造成的誤差。延伸兩階段組裝測驗的概念，Adema[1]提出一個兩階段同時組裝測驗的方法。其作法是在第一階段組裝一份 題的試卷， 為試卷試題數，為平行測驗數。第二階段再使用 LP 演算法將第一階段的 題試卷分成 分相似的平行測驗，如圖一。其方法是用單一測驗模型去同時組裝平行測驗，因此不會有循序組裝的不平等問題，且不會有同時組裝變數與限制式過多的問題。雖然在第一階段能組裝出符合測驗規格的試卷，但在第二階段組裝測驗時不一定能確保平均測驗品質，因此仍有很大的改善空間。



圖一. Adema 的測驗編碼方式

過去只有少數研究能不需加入大量的變數和限制式且能解決不平等問題，但這些方法組裝的測驗不足以符合目標測驗規格或計算量太大，無法在短時間內同時產生多份低誤差的平行測驗[8]。由於測驗組裝是一種組合最佳化問題，試題組合會隨著試題數量增加而呈指數成長[38]。所以近年來朝向採用啟發式演算法，先前提到的啟發式演算法都是針對單一測驗組裝，也應用於平行測驗，像是模擬降溫法、Weighted Deviations model and Heuristic (WDH)法、基因演算法、株落演算法等。Stocking 等人[31]使用 WDH 法，作法分為兩階段，第一階段為組裝兩份測驗 a 和 b，針對題庫內每一題計算試題訊息量，選擇與題庫所有題目的平均試題訊息量距離最小者，交叉分配給測驗 a 和測驗 b；第二階段使兩份測驗的試題盡量相似，隨機從測驗 a 中選出一題，和測驗 b 中的所有試題訊息量差距最大者設為 x，再從剩餘試題中選出一題，和測驗 b 中所有試題訊息量差距最大者設為 y，如果 y<x，則交換兩題。相反地，將上述步驟測驗 b 取代為測驗 a，重複步驟直到沒有交換為止。此方法雖可有效的找出最好的組合，但其缺點是反覆執行，花費時間長。Wang 等人[41]將 Stocking 等人[31]的方式作進一步的改良，根據與目標訊息量的差距來選擇題目，選擇試卷中與備選試題差異最大的作交換。以上兩種方式皆基於遵循尋找目標和交換模式的啟發式算法，雖然可以有效的得到平行測驗，但可能造成無法收斂或無法找出最接近目標測驗的結果。Sun 等人[33]提出使用二進制基因演算法，世代數為 2000 的最佳情況下，均方差為 0.5321。在相同測驗規格下，和 Stocking 等人[31]與 Wang 等人[41]相比，改善率平均提升 95%。Hwang 等人[15]則提出實數型編碼的禁忌演算法來進行同時組裝平行測驗，其作法是在組裝時將多份測驗同時組裝在一起，再分成多份試卷，這樣可以避免試題重複的情形發生，也可以減少限制式，由於使用的是實數型，編碼長度較二進制短，因此可以降低不少執行時間。總結來說，同時測驗組裝雖然能有效的克服循序法的不平等問題[1, 6, 7, 15, 23]，但提高了問

題的複雜度導致增加平行測驗間的誤差。亦有學者朝向硬體發展，藉由電腦平行運算的技術組裝平行測驗，Songmuang 及 Ueno[30]應用蜜蜂演算法，使用多個處理器和多台電腦同時組裝測驗，以減少計算時間，但因設備成本太高，較不適合廣泛使用於組裝測驗系統上。

以往的組裝測驗研究幾乎都著重於相同目標測驗訊息量(Target Information Function，TIF)的平行測驗，根據 McDonald 的定義稱為 TSIF-Parallel tests，又稱弱平行測驗(weakly parallel tests)，有相同測驗特性的平行測驗則稱為 TCC-Parallel tests。當平行測驗同時符合 TSIF-Parallel tests 與 TCC-Parallel tests 就可提升平行測驗間相互比較的精確度。然而，除了 TIF 外，測驗特性也需完全相同，如測驗試題數、內容、題型和長度。由於符合兩種 TCC 和 TSIF 的平行測驗難度很高， Chang 及 Shiu[8]提出的株落選擇演算法於組裝平行測驗，藉由 CLONAL 的平行搜尋機制來解決限制式過多的問題，和 Sun[33]的 GA 相較之下，CLONAL 較 GA 的均方差平均改善了 8.71 倍。

Sun 等人[33]採用的 GA 和 Chang 及 Shiu[8]採用的 CLONAL 在組裝平行測驗中，其初始化步驟皆是使用一般虛擬亂數產生器(Pseudo Random Number Generator，PRNG)[29]作為試題編碼，PRNG 所產生的亂數會有叢聚的問題，產生隨機樣本不滿足均勻分布，造成題庫中的某些題目不會被選中的情形。本研究將採準隨機亂數(Quasi-Random Number Generator，QRNG) ，如圖三，可看出 QRNG 比 PRNG 分布較均勻。QRNG 又可稱為低差異數列(Low-Discrepancy Sequence，LDS)，是一種超均勻分布的隨機亂數，此種方法是給定一個規則產生數列，轉換後所得到的值大致上會落在(0, 1)的範圍內並且均勻分佈，所以可以快速的達到收斂，並可以節省大量的計算時間。近來有許多學者提出改進的方法[10, 12, 27, 35]，使得執行效率和準確率遠高於原始隨機亂數法。現代普遍常用的分為兩種，Halton sequences 和 Sobol sequences。

Maaranen 等人[24]在基因演算法的初始化步驟使用 QRNG，證實可以提升實驗結果的準確性，且可減少世代數。Reese[26]和 Kimura, Matsumura[19]進一步發現 QRNG 應用在 GA 解決非線性或多目標問題時可以提高搜尋效能。因此，本篇將 CLONAL 結合 QRNG 方法，CLONAL 可將分散在搜尋空間中的所有解，各自找出了所在區域中的局部最佳解[8]，再加上許多學者證實 QRNG 可提高搜尋效能，降低誤差，因此能有效提升組裝平行測驗的效果。

3. 株落選擇演算法

株落選擇演算法是 De Castro 及 Von Zuben[9]提出的啟發式演算法，此演算法是模擬生物免疫系統中的內容，並以生物學的觀點來模擬免疫行為，稱為人工免疫系統。此演算法是以其中的株落選擇概念衍生而成，有別於其他演算法，它利用族群相似程度的關係，增加族群的多樣性，以避免陷入局部最佳解的可能性，使得在求解空間的蒐尋過程中，能夠快速收斂且找到全域最佳解。

B 淋巴細胞是用來生產抗體(antibody)，當病毒、細菌、不同種的血液、移植的器官等出現時就是所謂的抗原(antigen)，B 淋巴細胞的抗體與抗原間的反應強度衡量稱為親和度(affinity)，親和度越高表示抗體越能有效對抗抗原，然後挑選出高親和力的抗體，B 淋巴細胞會迅速製造(增殖)一個或多個抗體，以擊退抗原，這些被增殖出的細胞就稱作克隆(clone)，再進行突變(mutation)，突變有利於增加親和度，此過程為株落選擇(clonal selection)，而這些高親和度的抗體將會越來越多，與抗原的親和力也會越來越高。

應用於測驗組裝的問題，每個抗體代表的是一份測驗，透過株落選擇的方式(增殖、突變)以滿足目標測驗的規格，目標測驗指的就是抗原，不斷重覆以上過程，直到產生最符合目標測驗規格(即親和力最高)的試卷為止。

主要步驟：

(1)產生初始族群(initialization)：以隨機的方式產生初始抗體族群(popu_size)，每一個抗體即代表一份測驗。

(2)計算親和力(calculate affinity)：計算抗體與抗原間的適合程度。在測驗組裝問題中，親和力代表組裝測驗與目標測驗之間的差距，差距越小表示親和力越高。

(3)增殖(proliferation)：選出較高親和力 n_{best} 個抗體來進行增殖，增殖出的抗體稱為克隆群體 C_{group}，而克隆群體內的抗體數量必須和原抗體的親和力成正比。

(4)突變(mutation)：將克隆群體進行突變，被突變的抗體由突變率決定，而突變率和親和力成反比，換句話說，親和力越低，突變率越高。

(5)重新選擇(re-selection)：重新計算克隆群體中所有抗體的親和力，然後選出 n_{best} 個親和力最高的抗體回族群取代原抗體。

(6)重組(meta-dynamic)：從族群中選出 $popu\_size - n_{best}$ 個親和力最低的抗體，隨機產生新的抗體做取代。

(7)循環(cycle)：反覆地執行步驟 2 到 6，直到完成指定的世代數。

株落演算法的搜尋機制是採用平行搜尋，族群中的每個解都是獨立發展，不會朝族群中最佳解的方向移動。到了搜尋後期所有解會分散在搜尋空間中，並各自找出所在區域中的局部最佳解。由於具備了獨立發展的特性且保有族群的多樣性，因此適合用於必須同時找出多個解的問題，非常符合平行測驗組裝的需求。

3.1 多目標組裝測驗的問題模型

本研究定義一個多目標測驗問題(Test Sheet

Composition Problem，TSC)，令題庫中有 N 個試題，分別為 $x_1, x_2, \cdots, x_N$，每題皆對應一種章節、技巧、題型，則可產生一份包含 C 個章節、S 種技巧和 Y 種題型的試卷，而 F 份試卷裡的所有題目皆不重覆。多目標平行組裝測驗的目的是建構出多份條件組合皆相同的試卷。以實數型表示模型問題，其定義如下：

Minimize $$\sum_{k=1}^{K}\sum_{i=1}^{n} I_{x_i}(\theta_k) \quad (1)$$

Subject to

$$\sum_{i=1}^{n} I_{x_i}(\theta_k) \geq D(\theta_k), \quad k=1,\ldots,K \quad (2)$$

$$\sum_{i=1}^{n} c_{x_i p} = C_p, \quad p=1,\ldots,P \quad (3)$$

$$\sum_{i=1}^{n} s_{x_i q} = S_q, \quad q=1,\ldots,Q \quad (4)$$

$$\sum_{i=1}^{n} y_{x_i r} = Y_r, \quad r=1,\ldots,R \quad (5)$$

$$\sum_{i=1}^{n} u_{x_i} \leq U \quad (6)$$

$$x_i \in [1, N], \quad i=1,\ldots,N \quad (7)$$

x_i	實數型變數，表示題庫裡的試題編號
n	目標測驗長度
$I_{x_i}(\theta_k)$	試題 x_i 在能力等級 k 時的試題訊息量
$D(\theta_k)$	等級 k 時的目標測驗訊息量
$c_{x_i p}$	二進制變數，若為 1，表示試題 x_i 屬於內容 p，反之則否
C_p	章節 p 的目標測驗題數
$s_{x_i q}$	二進制變數，若為 1，表示試題 x_i 屬於技巧 q，反之則否
S_q	解題技巧屬性 q 的目標測驗題數
$y_{x_i r}$	二進制變數，若為 1，表示試題 x_i 屬於題型 r，反之則否
Y_r	題型屬性 r 的目標測驗題數
u_{x_i}	表示試題 x_i 的字數
U	表示目標測驗字數

目標式(1)和限制式(2)表示在每個能力等級 k 試題訊息量的總和必須大於等於目標訊息量；限制式(3)、(4)及(5)分別代表試題在各章節 p、解題技巧 q 及題型 r 的題數必須符合目標題數；限制式(6)表示測驗字數總和必須小於目標字數上限；限制式(7)表示 x_i 為任意實數，即實數型編碼。下一節詳細介紹如何使用 QRNG 株落演算法來解決此組裝測驗模型。

3.2. QRNG 株落演算法

本文根據 Chang 及 Shiu[8]提出的 CLONAL，其初始族群步驟所使用的虛擬亂數產生器(PRNG)以準隨機亂數(QRNG)取而代之，PRNG 普遍用於一般電腦程式，其原理是利用序列或等式，產生 0 到 1 之間的資料組，但 PRNG 無法完全符合隨機變數的統計特性。針對上述問題，許多研究提出使用 quasi-random 改善均勻度不佳，與計算結果不準確和收斂速度慢的問題。因此，我們提出準隨機亂數(QRNG)改良 CLONAL，由於 quasi-random 產生的隨機數為均勻分佈，可以解決分佈不均的問題。

由於在產生初始族群、突變、重組三個階段有可能會導致試題重疊，解決方法是在演算法中加入排除機制，當試題被挑選到測驗時，則此試題會暫時列入排除試題區 *ban_list*，演算法挑選剩餘的試題，這個做法可以避免試題重覆，並且可同時組出多份測驗。以下將介紹 QRNG 株落演算法。

主要步驟：

(1) 產生初始族群：使用 QRNG[28]隨機產生 *popu_size* 個抗體(測驗)，每個抗體包括 n 個實數 x_i，而 $x_i \in [1, N]$，被選擇的試題暫時移到 *ban_list* 中，以避免試題被重覆挑選。

QRNG：

首先，選取 d 個隨機方向數，再以不同的本質多向式遞迴產生其他的方向數，其中 d 代表本質多項式的階數，利用方向數產生 QRNG 亂數，以下詳述 QRNG 產生過程：

(1.1)計算本質多項式：

令任意十進制奇數 B，將 B 轉換為二進制 $a_0, \ldots, a_d \in \{0,1\}$，形成本質多項式 P：

$$P = a_0 x^d + a_1 x^{d-1} + \ldots + a_{d-1} x^1 + a_d x^0 \quad (8)$$

(1.2) 求方向數：

方向數由等式(9)遞迴計算產生，其中⊕為 XOR 運算。為了方便計算，假設 $v_i = m_i/2^i$ 簡化為等式(10)。當 $i \leq d$ 時無法由等式產生 m_i，當 $i \leq d$ 時 需假設 $m_1, \cdots, m_d$ 為任意奇數並滿足 $0 < m_i < 2^i$。將 $m_1, \cdots, m_d$ 代入等式(15)，由 $v_i = m_i/2^i$ 推得方向數 v_i。

$$(v_i)_2 = \left(a_1 v_{i-1} \oplus a_2 v_{i-2} \oplus \ldots \oplus a_{d-1} v_{i-d+1} \oplus v_{i-d} \oplus [v_{i-d}/2^d]\right)_2, \ i > d \quad (9)$$

$$m_i = \begin{cases} 2k\text{-}1, \ k \in N, \ \text{for} \ \forall i \leq d, \ 0 < m_i < 2^i \\ 2a_1 m_{i-1} \oplus 2^2 a_2 m_{i-2} \oplus \ldots \oplus 2^{d-1} a_{d-1} m_{i-d+1} \oplus 2^d m_{i-d} \oplus m_{i-d}, \ \text{for} \ \forall i > d \end{cases} \quad (10)$$

(1.3)遞迴產生 QRNG 亂數：

根據等式(11)遞迴產生 $x(n)$ 數列，其中 $0 \leq n \leq 2^N - 1$，N 為任意正整數，n 以二進制表示時，由右至左搜尋第一個為 0 的位數為 k，由等式(14)得到 v 等式(11)遞迴產生 QRNG 亂數。

$$x(n) = \begin{cases} N, \ \text{for} \ n = 0 \\ x(n-1) \oplus v_k, \ \text{for} \ 1 \leq n \leq 2^N - 1 \end{cases} \quad (11)$$

(2)計算親和力：親和力是用來辨識抗體與抗原間的吻合度。本研究在親和力的計算上是使用測驗與目標測驗的誤差值為評估方式，等式(12)到等式(16)，根據問題模型來計算每份測驗的章節、技巧、題型、字數與目標測驗規格的誤差，等式(17)將所有

誤差乘上權重後全部相加即為親和力，權重為自訂的值，可依自認為重要性而作調整，而偏差值 E_I、E_C、E_Q、E_R、E_U 為 0 代表測驗完全符合目標測驗規格，表示親和力越高，越接近目標測驗。

$$\sum_{k=1}^{K}\left|\sum_{i=1}^{n} I_{x_i}(\theta_k) - D(\theta_k)\right| = E_I \qquad (12)$$

$$\sum_{p=1}^{P}\left|\sum_{i=1}^{n} c_{x_i p} - C_p\right| = E_C \qquad (13)$$

$$\sum_{q=1}^{Q}\left|\sum_{i=1}^{n} s_{x_i q} - S_q\right| = E_Q \qquad (14)$$

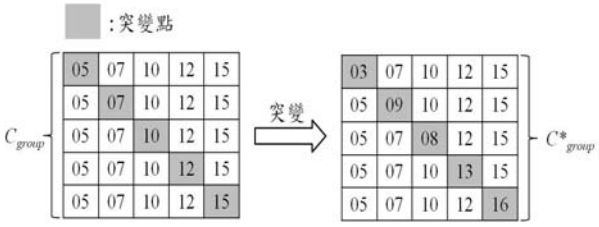
$$\sum_{r=1}^{R}\left|\sum_{i=1}^{n} y_{x_i r} - Y_r\right| = E_R \qquad (15)$$

$$\max\left(0, \sum_{i=1}^{n} u_{x_i} - U\right) = E_U \qquad (16)$$

$$affinity = W_I E_I + W_C E_C + W_Q E_Q + W_R E_R + W_U E_U \qquad (17)$$

(3)增殖：選擇親和力較高的 n_{best} 個抗體進行增殖，因為本文突變設計的關係，所以克隆數量設為 n，因此每個克隆群體 C_{group} 中有 n 個抗體，總共有 n_{best} 個抗體。

(4)單點突變：以 C_{group} 為單位進行單點突變，以圖二為例，假設一份測驗有 5 題試題，分別為 x_1, x_2, x_3, x_4, x_5 (題號 5、題號 7、題號 10、題號 12、題號 15)，因此克隆族群 C_{group} 為 5 個複製的抗體，第一個抗體突變 x_1 (題號 5)，x_1 從已經排除原本族群內試題的題庫中隨機選出一題(題號 3)作取代，突變後也將題號 3 這題納入 *ban_list*，第二個抗體突變 x_2(題號 7)，依此類推，突變後的 C_{group} 稱為 C^*_{group}。



圖二. 單點突變範例

(5)重新選擇：計算 C^*_{group} 內 n 個抗體和 C_{group} 原始抗體的親和力互相做比較，保留最佳親和力的抗體取代原始抗體，如果 C^*_{group} 內的抗體親和力比 C_{group} 原始抗體差，則保留原始抗體。

(6)重組：從族群中挑選出親和力最差的 *popu_size* - n_{best} 個抗體並用全新的隨機抗體取代，在產生隨機抗體時，同時也排除整個族群的試題再做隨機選擇。

(7)循環：重覆步驟(2)到步驟(6)，直到完成指定的世代數 *gen*。而其中挑選出前 F 個親和力較佳的抗體，即為 F 份平行測驗。

4. 實驗設計與結果

由於 Chang 及 Shiu[8]所提出的 CLONAL 較過去所有研究[33, 34, 41]有較佳的結果，因此本節針對和 Chang 及 Shiu 的 CLONAL 進行一系列實驗比較。本篇以 Chang 及 Shiu 的實驗設計題庫，題庫試題數量 16000 題，作為組裝測驗依據。題目參數鑑別度介於 0.8~3.0，困難度介於-3.0~3.0，猜測度介於 0.1~0.3，章節分為 1~10 章，技巧分為 1~6 種(計算、知識、記憶、推理、理解、應用)，題型分為 1~5 種(是非題、單選題、多選題、填充題、簡答題)，字數介於 20~50 字。

為了評估 QRNG CLONAL 是否能滿足測驗規格並且和 CLONAL 各作一百次的組裝，每次組裝的測驗目標都是隨機產生。本文考慮兩種組卷目標 TIF 波型，分別是單峰型和雙峰型。對單峰型 TIF，目標訊息量的隨機產生範圍為 4~5,6~8,18~21,6~8,4~5，分別對應到能力等級 。而對雙峰型 TIF，隨機產生範圍為 7~8,13~15,9~11,13~15,7~8，分別對應到能力等級 。章節、技巧、題型、測驗字數的目標題數也是隨機產生，而訊息量偏差值的精確率設為小數點後四位數，因此設 W_I=W_C=W_Q=W_R=W_U=10000。

在題庫為 16000 情況下，同時組裝 20 份評型測驗，CLONAL 和 QRNG CLONAL 執行一百次的平均實驗結果，誤差為和目標測驗間的差距，均方差代表的是平行測驗間的品質差距。表一顯示 QRNG CLONAL 改善率可達 45.3%與 33.6%。

表一. CLONAL 和 QRNG CLONAL 實驗結果(20 份)

	CLONAL		QRNG CLONAL	
題數	16000		16000	
TIF*	S	D	S	D
誤差	1.30	1.24	0.98	0.97
均方差	0.76	0.65	0.41	0.43
時間(分)	7.56	7.66	7.80	7.88
改善率**	-	-	45.3	33.6

*S=單峰 TIF，D=雙峰 TIF　**改善率=|QRNG CLONAL 均方差-CLONAL 均方差|/ CLONAL 均方差*100 (%)

5. 結論

先前的研究證明了啟發式演算法適合解決平行測驗問題[40]，本文提出了 QRNG 改良株落演算法，採用準隨機亂數將株落選擇演算法提升了平行測驗間的品質差異。並且從龐大的題庫中，將平行組裝測驗問題簡單化，解決了大量的選擇變數和多樣性限制條件所造成測驗品質下降的問題。實驗證明了和 Chang 及 Shiu 提出的 CLONAL 相較之下，QRNG CLONAL 的平行測驗的品質更好，且降低多份測驗間的差異，和目標規格也有更小的偏差。整體來說，使用 QRNG CLONAL 組裝測驗能解決循序組裝的不平等問題，有效降低問題複雜度，能在可接受的時間內組裝符合目標規格的測驗，當擴充題庫或平行試卷數，能保持測驗間的差異穩定度。

誌謝：非常感謝國科會計畫編號：

NSC101-2622-E-018-001-CC3

參考文獻

[1] J. J. Adema, “Implementations of the branch-and-bound method for test construction problems,” Methodika, 1992.

[2] R. D. Armstrong, D. H. Jones, and Z. Wang, “Automated parallel test construction using classical test theory,” Journal of educational and behavioral statistics, vol. 19, no. 1, pp. 73-90, 1994.

[3] F. B. Baker, A. S. Cohen, and B. R. Barmish, “Item characteristics of tests constructed by linear programming,” Applied Psychological Measurement, vol. 12, no. 2, pp. 189-199, 1988.

[4] D. I. Belov, and R. D. Armstrong, “Monte Carlo test assembly for item pool analysis and extension,” Applied Psychological Measurement, vol. 29, no. 4, pp. 239-261, 2005.

[5] E. Boekkooi-Timminga, “The construction of parallel tests from IRT-based item banks,” Journal of educational and behavioral statistics, vol. 15, no. 2, pp. 129-145, 1990.

[6] E. Boekkooi-Timminga, “Simultaneous test construction by zero-one programming,” Department of Education of the University of Twente, 1986.

[7] K. Breithaupt, A. Ariel, and B. P. Veldkamp, “Automated simultaneous assembly for multistage testing,” International Journal of Testing, vol. 5, no. 3, pp. 319-330, 2005.

[8] T. Y. Chang, and Y. F. Shiu, “Simultaneously construct IRT-based parallel tests based on an adapted CLONALG algorithm,” Applied Intelligence, vol. 36, no. 4, pp. 979-994, 2012.

[9] L. N. De Castro, and F. J. Von Zuben, “Learning and optimization using the clonal selection principle,” Evolutionary Computation, IEEE Transactions on, vol. 6, no. 3, pp. 239-251, 2002.

[10] H. Faure, “Discrépance de suites associéesa un systeme de numération (en dimension s),” Acta Arith, vol. 41, no. 4, pp. 337-351, 1982.

[11] M. Finkelman, W. Kim, and L. A. Roussos, “Automated test assembly for cognitive diagnosis models using a genetic algorithm,” Journal of educational measurement, vol. 46, no. 3, pp. 273-292, 2009.

[12] J. H. Halton, “On the efficiency of certain quasi-random sequences of points in evaluating multi-dimensional integrals,” Numerische Mathematik, vol. 2, no. 1, pp. 84-90, 1960.

[13] R. K. Hambleton, and H. Swaminathan, “Item response theory: Principles and applications,” Kluwer-Nijhoff Pub.(Boston and Hingham, MA, USA), 1985.

[14] J. H. Holland, “Adaptation in natural and artificial systems, University of Michigan press,” Ann Arbor, MI, vol. 1, no. 97, pp. 5, 1975.

[15] G.-J. Hwang, H.-C. Chu, P.-Y. Yin, and J.-Y. Lin, “An innovative parallel test sheet composition approach to meet multiple assessment criteria for national tests,” Computers & Education, vol. 51, no. 3, pp. 1058-1072, 2008.

[16] G. J. Hwang, B. M. T. Lin, H. H. Tseng, and T. L. Lin, “On the development of a computer-assisted testing system with genetic test sheet-generating approach,” Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, vol. 35, no. 4, pp. 590-594, 2005.

[17] G. J. Hwang, P. Y. Yin, and S. H. Yeh, “A tabu search approach to generating test sheets for multiple assessment criteria,” Education, IEEE Transactions on, vol. 49, no. 1, pp. 88-97, 2006.

[18] H. Jeng, and S. Shih, “A comparison of pairwise and group selections of items using simulated annealing in automated construction of parallel tests,” Psychological Testing, vol. 44, no. 2, pp. 195-210, 1997.

[19] S. Kimura, and K. Matsumura, “Genetic algorithms using low-discrepancy sequences,” Proceedings of the 2005 conference on Genetic and evolutionary computation, pp. 1341-1346, 2005.

[20] C. L. Lee, C. H. Huang, and C. J. Lin, “Test-sheet composition using immune algorithm for E-learning application,” New Trends in Applied Artificial Intelligence, pp. 823-833, 2007.

[21] W. L. Leite, I.-C. Huang, and G. A. Marcoulides, “Item selection for the development of short forms of scales using an ant colony optimization algorithm,” Multivariate Behavioral Research, vol. 43, no. 3, pp. 411-431, 2008.

[22] F. T. Lin, C. Y. Kao, and C. C. Hsu, “Applying the genetic approach to simulated annealing in solving some NP-hard problems,” Systems, Man and Cybernetics, IEEE Transactions on, vol. 23, no. 6, pp. 1752-1767, 1993.

[23] W. J. Linden, and J. J. Adema, “Simultaneous assembly of multiple test forms,” Journal of educational measurement, vol. 35, no. 3, pp. 185-198, 1998.

[24] H. Maaranen, K. Miettinen, and M. M. Mäkelä, “Quasi-random initial population for genetic algorithms,” Computers & Mathematics with Applications, vol. 47, no. 12, pp. 1885-1895, 2004.

[25] M. Melanie, “An introduction to genetic algorithms,” Cambridge, Massachusetts London, England, Fifth printing, vol. 3, 1999.

[26] A. Reese, “Random number generators in genetic algorithms for unconstrained and constrained optimization,” Nonlinear Analysis: Theory, Methods & Applications, vol. 71, no. 12, pp. 679-692, 2009.

[27] I. Sobol, “Multidimensional quadrature formulas and Haar functions,” Izdat" Nauka", Moscow, 1969.

[28] I. Soboĺ, “Quasi-monte carlo methods,” Progress in Nuclear Energy, vol. 24, no. 1, pp. 55-61, 1990.

[29] I. Sobol, and B. Shukhman, “Quasi-random points keep their distance,” Mathematics and Computers in Simulation, vol. 75, no. 3, pp. 80-86, 2007.

[30] P. Songmuang, and M. Ueno, “Bees algorithm for construction of multiple test forms in e-testing,” Learning Technologies, IEEE Transactions on, vol. 4, no. 3, pp. 209-221, 2011.

[31] M. L. Stocking, L. Swanson, and M. Pearlman, “Application of an automated item selection method to real data,” Applied Psychological Measurement, vol. 17, no. 2, pp. 167-176, 1993.

[32] K. Sun, and S. Chen, “A study of applying the artificial intelligent technique to select test items,” Psychological Testing, vol. 46, no. 1, pp. 75-88, 1999.

[33] K. T. Sun, Y. J. Chen, S. Y. Tsai, and C. F. Cheng, “Creating IRT-based parallel test forms using the genetic algorithm method,” Applied measurement in education, vol. 21, no. 2, pp. 141-161, 2008.

[34] L. Swanson, and M. L. Stocking, “A model and heuristic for solving very large item selection problems,” Applied Psychological Measurement, vol. 17, no. 2, pp. 151-166, 1993.

[35] S. Tezuka, “Polynomial arithmetic analogue of Halton sequences,” ACM Transactions on Modeling and Computer Simulation (TOMACS), vol. 3, no. 2, pp. 99-107, 1993.

[36] T. Theunissen, “Binary programming and test design,” Psychometrika, vol. 50, no. 4, pp. 411-420, 1985.

[37] W. J. Van der Linden, “Linear models for optimal test design,” Springer Science+ Business Media, 2005.

[38] W. J. Van der Linden, “Optimal assembly of psychological and educational tests,” Applied Psychological Measurement, vol. 22, no. 3, pp. 195-211, 1998.

[39] W. J. van ver Linden, and E. Boekkooi-Timminga, “A maximin model for IRT-based test design with practical constraints,” Psychometrika, vol. 54, no. 2, pp. 237-247, 1989.

[40] A. J. Verschoor, “Genetic algorithms for automated test assembly,” University of Twente, 2007.

[41] C. Wang, and T. Ackerman, “Two item selection algorithms for creating weakly parallel test forms using the IRT information functions,” Psychological Testing, vol. 44, no. 2, pp. 123-140, 1997.

[42] P. Y. Yin, K. C. Chang, G. J. Hwang, G. H. Hwang, and Y. Chan, “A particle swarm optimization approach to composing serial test sheets for multiple assessment criteria,” journal of educational technologyand society, vol. 9, no. 3, pp. 3, 2006.

校外租屋資訊微軟 APP

嚴本嘉* 陳鵬先**
台北海洋技術學院
*數遊系 **資通系
yen@mail.tcmt.edu.tw s818112@gmail.com

摘要

隨著智慧型手機的興起，改變人們的日常行為，以往電子商務只能透過電腦來完成，現在也可以透過智慧型手機的 APP 來達成。智慧型手機遊戲 APP 也大大影響線上遊戲的市場。隨著智慧型手機 APP 愈多愈好，本文就是以校園應用的 APP 為研究主題。以往學校對學生的服務只透過學校網頁，本計畫是將學校網頁上的租屋資訊以微軟芒果智慧型手機的 APP 呈現出來。用微軟公司 DreamSpark 校園計畫免費軟體，開發智慧型手機的 APP 結合谷哥地圖，顯示學校附近所有的租屋地點、房東姓名、電話號碼、租屋照片。當學生走到學校附近，可拿著智慧型手機，查詢附近租屋狀況，減少學生租屋的困難，同時也提供學校對學生進一步的照顧。

關鍵詞：校園 APP、租屋資訊、微軟芒果手機。

Abstract

As smart phones become universal, consumers therefore change daily behaviors accordingly. Furthermore, smartphones even replace some functions which could be conducted via computers. Particularly, online game markets are affected significantly. Previously, school could provide services through computer website. The plan is to display off campus rental information applying APP through Microsoft Mango smartphone. The APP provides location, owners, phone numbers and photos of off campus rental information with the use of Google map. The device enables students to search information anytime.

Keywords: Campus APP, off campus rental information, Microsoft phone.

1. 前言

每個學期開學的時候，遠地學生都會為尋找住宿地點而煩惱。學校宿舍有限，無法容納大量外地學生的需求，所以校外租屋資訊對學生來講幫助很大。一方面解決學生家長的困擾，一方面也減少導師的負擔。目前各大專院校 都有將校外租屋資訊，公布在學校網頁上，但對學生來講，服務還不夠周延。本文的目的就是將校外租屋資訊寫成 APP，供學生下載在智慧型手機上。當學生在學校附近找房子的時候，可以用智慧型手機上的谷歌地圖，查附近有無學生宿舍出租， 減少學生的困擾。

2. 用 Microsoft Visual Web Developer 2010 Express 建立資料庫

用台北海洋技術學院提供學生租賃資訊網頁檔案，再自行加上該租屋之經緯度座標，利用 Microsoft Visual Web Developer 2010 Express 程式設計成 Database1.mdf。 原本學生租賃資訊網頁，沒有含租賃房屋照片。在網路上尋找任一房屋照片代替。以便豐富添加資料庫的內容。如下表 1。

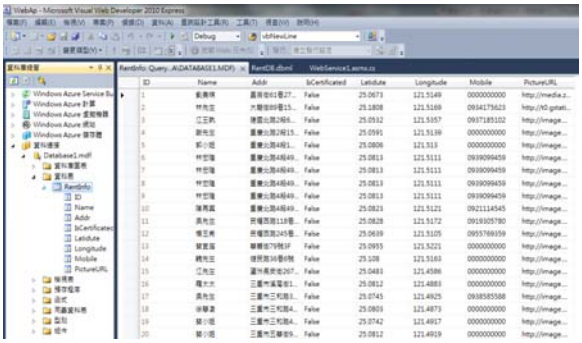


表 1 學生租賃資訊資料。

利用 WebService1.asmx 在 IE 上開啟 WebService1 網頁，點選 GetData 即可呈現原來在 Database1.mdf 上所有欄位資料。 同時供微軟手機程式 APP 使用原來在 Database1.mdf 上所有欄位資料， 如下表 2 學生租賃資訊資料庫。

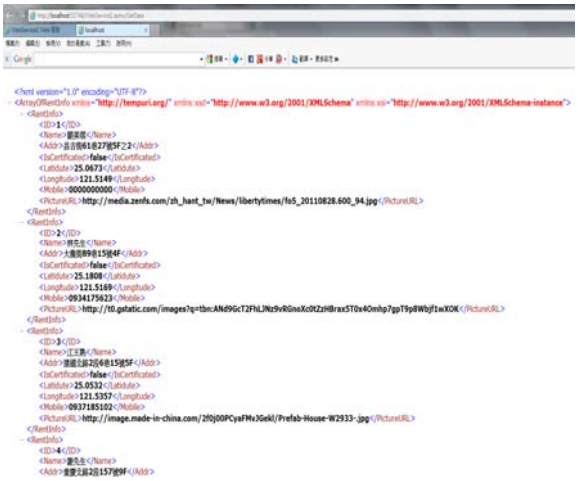


表 2 學生租賃資訊資料庫。

3.微軟芒果手機 APP 方塊磚的設計

使用 Microsoft Visual Studio 2010 Express for Windows Phone 程式去開發微軟芒果手機程式 APP。 在套件資料夾中，直接更新 ApplicationIcon.png 和 Background.png 的圖檔.利用本校的校徽做為方塊磚的圖案，凸顯本校附近的租屋資訊，如圖 1 和圖 2。



圖 1. 方塊磚　　圖 2. APP 市集

4. 微軟芒果手機 APP 首頁的設計

在首頁上先擺放地圖元件，再用滑桿開關 Slider switch 代替一般手機在 LCD 銀幕上，用手指滑動的功能。增加 2 個+，- 按鍵 有放大和縮小地圖的功能。增加顯示位置按鍵，可直接顯示淡水校區附近有租屋資訊標幟物的地圖，如圖 3。



圖 3. 租屋資訊 APP 首頁　圖 4. 顯示台北海院淡水校區的地理位置

當按下顯示位置按鍵，則地圖則直接跳到台北海院淡水校區的地理位置，同時顯示附近可供學生校外租屋的資訊，如圖 4。

部份重要程式設計功能如下：

```
//當按下顯示位置按鍵， 連結資料庫中所有住屋資料， 依經緯度，標記在地圖上。
        Private void button1_Click(object sender, RoutedEventArgs e)
{ if ((App.Current as App).RentInfomation != null)
{foreach (ServiceReference1.RentInfo item in (App.Current as App).RentInfomation)
{CreatePushPin(item);}}
map1.SetView(new System.Device.Location.GeoCoordinate(25.1844, 121.4387), 13); }
// 25.1844, 121.4387 為淡水校區經緯度座標， 13 是地圖縮放的參數。
// 當點選校外租訊的任一民房標記，即可跳到租屋資訊的畫面。
Private void
 CreatePushPin(ServiceReference1.RentInfo info)
{ int index= (App.Current as
 App).RentInfomation.IndexOf(info);
//建立圖層
MapLayer m_PushpinLayer = new MapLayer();
//建立標記
Pushpin pin = new Pushpin();
//當標記被點選時，要執行事件
pin.MouseLeftButtonDown += (ss, arg) =>{
NavigationService.Navigate( new Uri("/PageShowDetails.xaml?Item=" + index, UriKind.Relative));};
pin.Content = info.Name;
//在圖層上加入標記
m_PushpinLayer.AddChild(pin,
new GeoCoordinate() {
Latitude = info.Latidute.Value,
Longitude = info.Longitude.Value });
//把圖層加入地圖
map1.Children.Add(m_PushpinLayer); }
private void slider1_ValueChanged(object sender, RoutedPropertyChangedEventArgs<double> e){
if (slider1 != null)
this.map1.ZoomLevel = slider1.Value; }
private void button2_Click(object sender, RoutedEventArgs e) {
this.map1.ZoomLevel += 1;}
```

租屋資訊的畫面， 採用 page name 、3 個 TextBlock 和 Image 等元件去呈現 APP 所抓到租

屋資訊的資料，如圖 5 和圖 6。



圖 5. 設計租屋資訊畫面的顯示元件

圖 6. 顯示租屋資訊的畫面

```
protected override void
OnNavigatedTo(System.Windows.Navigation.NavigationEventArgs e) { base.OnNavigatedTo(e);
int i =
int.Parse( NavigationContext.QueryString["Item"].ToString());
this.PageTitle.Text = i.ToString();
//抓取詳細資料
ServiceReference1.RentInfo    item = (App.Current as App).RentInfomation[i];
PageTitle.Text = item.Name;
this.textBlock1.Text ="電話:"+ item.Mobile;
this.textBlock2.Text = "住址:" + item.Addr;
this.textBlock3.Text = "經緯度:" + item.Latidute + "," + item.Longitude;
BitmapImage bi = new BitmapImage(new Uri(item.PictureURL));
image1.Source = bi;}
```

如圖 7 和圖 8，當手指或滑鼠按到電話號碼時，即可顯示撥電話的功能！撥電話功能的程式如下所示：



圖 7. 當手指或滑鼠按到電話號碼時，即可顯示撥電話的功能。圖 8. 顯示電話直接通話的情形。

```
private void
textBlock1_MouseLeftButtonDown(object sender, MouseButtonEventArgs e) { string tel =
this.textBlock1.Text.Replace("電話:", "");
Microsoft.Phone.Tasks.PhoneCallTask pc=new Microsoft.Phone.Tasks.PhoneCallTask();
pc.DisplayName=PageTitle.Text;
pc.PhoneNumber=tel;
pc.Show();}
```

5. 用 Android 系統連上兩校區地址的 APP

原本計畫要用 Android 手機程式去寫智慧型手機程式淡水校區租賃資訊的 APP。但因用 Android 手機程式要去抓取用微軟 Microsoft Visual Web Developer 2010 Express 建立資料庫，但其呈現在 LocalHost 的 IP address， 用 Android 手機程式要去抓資料，卻無法連結 LocalHost 的 IP。畢竟 2 家公司系統還是有相容性的問題。所以我用定址的方式去呈現本校淡水校區和士林校區的位址 APP，如圖 9 和圖 10。



圖 9. Android 手機顯示淡水校區畫面

圖 10. Android 手機顯示士林校區畫面

。

6. 結論

由於微軟 DreamSpark 校園計畫免費提供用於學習的軟體和資源， 所以利用台北海洋技術學院提供淡水校區學生租賃資訊檔案，再自行加上該租屋之經緯度座標，利用 Microsoft Visual Web Developer 2010 Express 程式設計成 S M L 檔放在本地主機伺服器上，再利用 Microsoft Visual Studio 2010 Express for Windows Phone 程式再去抓取該租屋程式，呈現在模擬的微軟芒果手機銀幕上。因學校網頁上的租屋資訊，沒有附上租屋照片，所以用別的照片取代租屋照片。另外增加可直接撥通電話

接洽房東的功能，減輕新生校外租屋的困擾。

曾經利用宏達電手機去抓取 Microsoft Visual Web Developer 2010 Express 程式所做 Localhost 伺服器網頁程式，但顯示無法連結，可見 Microsoft Visual Web Developer 2010 Express、Microsoft Visual Studio 2010 Express for Windows Phone 兩程式均屬微軟系統，谷歌系統程式要去抓取軟系統程式有其困難。微軟有校園計畫，可讓師生免費使用開發軟體程式去完成微軟手機與伺服器資料庫的連結。尤其是微軟手機使用谷歌地圖非常簡單，只要在元件庫拉一個地圖元件，即可顯現谷歌地圖，而在谷歌手機上如要開發谷歌地圖卻需要繁雜步驟，首先要有谷歌郵件帳號登錄，配合每台電腦主機的網路卡帳號，才能得到谷歌地圖鑰匙。而且還限定只能在同一台電腦使用，如換至別台電腦就不行，而需重新申請。所以在教學上因每台電腦，均有不同學生使用，同學都要申請自己的谷歌密碼，而且會同時上網呼叫谷歌地圖，如果教室頻寬不夠，每次呼叫谷歌地圖，就等很久才能顯現谷歌地圖，將會造成教學上困難。本研究論文最主要的貢獻，在於成功用微軟公司 DreamSpark 校園計畫免費軟體，用行動通訊-智慧型手機結合谷歌地圖，成功地連結到網路上的租賃資訊資料庫。走到學校校區附近，用智慧型手機即可查閱附近學生宿舍租賃資訊。學校對學生資訊的服務，也可提昇到用智慧型手機 APP。每學期學生事務處都會要求導師訪視校外賃居生，依居家安全檢視圖表，記錄訪視結果。如果能將瓦斯熱水器是否放置於通風處所...等項目，也列入學生租賃資訊檔案，則 APP 的內容可更加豐富，增加學生和家長選擇租屋的參考。

7. 感謝

感謝陳鵬先、李東翰、江采薇三位同學參與這個智慧型手機程式研究，讓學生能夠學習到開發 APP 的經驗，也謝謝他們協助整理學校士林校區和淡水校區租屋資訊的資料庫，以及設計、撰寫 APP 程式和圖案。同時也謝謝微軟公司 DreamSpark 校園計畫免費軟體，和行政院勞委會職訓局補助大專院校辦理就業學程計畫，有機會和產業界專家溝通，才能順利完成本文。

參考文獻

[1] 董大偉著 Windows Phone 手機程式互動開發 書號 XP12057 松崗 2011
[2] 文淵閣工作室著 Android 初學特訓班 書號 CL0315 碁峯 2012
[3] Android 4.X APP 開發教戰手冊 黃彬華著 書號 EL0123 碁峯 2012
[4] 文淵閣工作室著 Dreamweaver CS6 我也會開發 APP 書號 CU0625 碁峯 2012
[5] 朱明中(小朱)著 Windows Azure Platform 應用程式開發教戰手札 第二版 書號 CL0367 碁峯 2013
[6] 朱明中(小朱)著 Windows Azure 教戰手札 第二版 書號 EL0106 碁峯 2010
[7] 陳會安著 ASP.NET 4.0 書號 F0476 旗標書局 2010
[8] 吳江華著 ASP.NET 4.0 書號 EL0108 碁峯書局 2010
[9] Build for Windows 8 and Windows Phone 8 Available at : https://dev.windowsphone.com/en-US
[10] Visual Studio 2012 Available at: http://www.microsoft.com/visualstudio/cht/products/visual-studio-express-for-web#product-express-web
[11] Windows Mobile 引路蜂地圖開發示例：本地查詢 Available at:http://www.2cto.com/kf/201207/140541.html
[12] 活用 HTML5 與 CSS3 的標準於行動網站開發上 Available at :http://www.youtube.com/watch?v=0V5nJLb-cEg
[13] Windows Azure 論壇 Available at : http://social.msdn.microsoft.com/forums/zh-tw/category/windowsazuretw
[14] MSDN Library Available at: http://msdn.microsoft.com/zh-tw/library/ms123401.aspx
[15] Tingxin Yan, David Chu, Deepak Ganesan, Aman Kansal, Jie Liu “ Fast app launching for mobile devices using predictive user context” 2012 Proceedings of the 10th international conference on Mobile systems, applications, and services Pages 113-126 ACM New York, NY, USA ©2012 table of contents ISBN: 978-1-4503-1301-8 doi>10.1145/2307636.2307648
[16] Jayaguru Panda, Shashank Sharma, C. V. Jawahar “Heritage app: annotating images on mobile phones” 12: Proceedings of the Eighth Indian Conference on Computer Vision, Graphics and Image Processing December 2012 Publisher: ACM Request Permissions
[17] Shing Tenqchen , Tai-Yu Chen , Dong-Ling Wu , Chi-Hwa Chen “Design of a rotary ring APP for Loving Sun-Moon Lake information capturer” ITS Telecommunications (ITST), 2012 12th International Conference on Digital Object Identifier: 10.1109/ITST.2012.6425167 Publication Year: 2012 , Page(s): 205 - 210 IEEE Conference Publications
[18] Jinsheng Lu , Qing Chen , Xijing Chen “App interface study on how to improve user experience Computer Science & Education (ICCSE)” , 2012 7th International Conference on Digital Object Identifier:10.1109/ICCSE.2012.6295176 Publication Year: 2012 , Page(s): 726 - 729 IEEE Conference Publications
[19] Nguyen, Thul “MapMyTrip app for android smart phone” ACM International Conference Proceeding Series, 2012, COM.Geo 2012 - International Conference on Computing for Geospatial Research and Applications; ISBN-13: 9781450311137; DOI: 10.1145/2345316.2345358; Conference: 3rd International Conference and Exhibition on Computing for Geospatial Research and Application, COM.Geo 2012, July 1, 2012 - July 3, 2012; Publisher: Association for Computing Machinery.

利用社群網路建構程式設計同儕學習與測驗環境

劉朝中　　林忠億
健行科技大學 資訊工程系
ccliu@csie.uch.edu.tw, jylin@ieee.org

摘要

程式語言的學習過程對一般人而言非常辛苦，師生間的隔閡與缺乏互動，加深了學習者的困難。程式設計在學習的過程中需要上機實作才有效果，但是在無人協助的情況下，學習過程中容易遇到瓶頸，導致程式語言的學習過程缺乏效率；同時，學習環境對學習者也有很大的影響，當學習者不在課堂上而是在其它場所進行自我練習時，發生問題將無法在短時間內得到想要的解答。

本論文建置一套系統(CodeBook)，利用社群網路的概念與導入同儕學習的機制，讓學習者除了可以向老師詢問外，同儕間能夠協助回答，加快尋求答案的時間；同時提供測驗環境使老師或是學習者能夠了解學習狀況，系統提供自動批改機制，有效率的即時回饋學生學習之成果，系統化的批改機制，能使老師迅速了解學習者的學習狀況，適度的對教學進度加以調整。

關鍵詞：程式設計學習、社群網路、同儕學習、線上評估系統。

1. 前言

對於理工學系的學生而言，程式設計的能力是非常重要的，但是在學習程式語言設計的過程中較為枯燥乏味，對於初學者而言，若沒有相當的興趣與耐心，初學者容易因為挫折而自暴自棄最後放棄學習；在初學者的學習過程中會遇到各式各樣的問題，若學習者無法在第一時間得到答案，久而久之學習者會漸漸的喪失興趣。近年來隨著電腦的快速發展，網際網路也越來越普及，使得社群網路，例如Facebook、Google +等等，越來越發達，人們已經慢慢習慣在社群網路這個虛擬世界中表達自己的意見與想法。因此這篇論文將利用Web 的特性創造一個可以在任何時間、任何地點都可以上線學習的系統，並且利用同儕之間的互相合作來達到互助學習的效果；同時，利用線上測驗的方式來協助學習者了解不足的部分，並且學習者與同儕之間可利用相互競爭來達到互相進步的目的。

2. 文獻探討

2.1 社群網路

社群網路(Social Networking)又稱作虛擬社群(Virtual Community)，通常是指有相同興趣或者是有相同目標的一群人所組成的團體。也可以說社群網路是一種透過網際網路拓樸來進行溝通、分享知識和策略的平台。

社群網路早期是以電子布告欄(Bulletin Board System , BBS)、電子郵件群組等方式來實現，然而隨著全球資訊網(World Wide Web , WWW) 的蓬勃發展，使得大多數網路社群平台改為採用 WWW 來做為平台。

學習社群是一群人透過網路溝通來分享知識、經驗與技術，擁有共同目的，增加集體成員的知識與能力；在學習社群中所營造的合作學習氣氛，透過各式各樣的溝通、互相的檢討、促進個人的自我反思，將可獲得知識技術的成長[1]。

2.2 同儕學習

同儕是指年齡近的人聚集在一起，彼此分享互相熟悉的價值、經驗與生活與風格，在學校中指的是同學。

在學校中除了老師與學生之間的互動之外，學生彼此之間互動更為頻繁，往往學生會因為害怕或害羞而不敢向老師提問，轉而請教能力較強的同學協助解決問題，根據研究指出，年紀相近的學習者相互學習能加強學習的效率[2]，也就是說能力較強的同學可擔任助教的角色，共同研究問題並得出解答。

同儕學習是指跳脫教師為中心，學習者彼此之間相互幫助，使同儕之間都能獲益的一種教學模式。

2.3 同儕師徒制(Peer Mentoring)

「同儕師徒制」是結合「同儕學習」與「師徒制」的概念，最主要是利用成年人或是能力較強的同儕幫助能力較弱的同儕，或是無經驗的學習者學習新知識與技能，在協助的過程中，屬於幫助人一方的同儕也可以在教導與互動的過程中，得到另一方面的成長，進而達到「教學相長」的目的。

在「同儕師徒制」中無論擔任師傅或徒弟的學生，都可以學到雙方的學科知識、如何成為一位適任的師傅以及有效的傾聽和溝通技巧[3]。

2.4 程式語言學習

學習程式設計最基本的方法就是上機實作[4]，上程式語言的老師理所當然會給學生許多的練習題與作業，希望學生能夠實際動手練習，造成有許多練習題與作業需要批改，若全部以人工的方式進行批改，不只效率非常差且容易出錯[5]。最為嚴重的問題是，學生需要等待較久的時間，才能從老師那邊得到答覆。

為了學好程式語言而進行大量的練習，部分學生會因為在反覆練習中遇到多次失敗，在失敗後失去原有的興趣與熱情，因此，找到影響學生學習動力的因素是非常重要的。有研究指出，影響程式設計學習的因子包含了個人態度和期望、具有挑戰性的目標與同儕間的壓力與競爭，同儕間的壓力與競爭證明對學生的學習是有影響力的[6]。

3. 研究架構

我們所提出的系統稱為 CodeBook，基於 Web 技術所開發，系統可進行線上編譯動作，免去事前繁雜的環境設定，在學習者討論過程中將不會因函式庫的不同而造成溝通上的困難；可協助同儕間的交流，同時可以利用測驗的方式幫助老師了解學生學習能力較弱的環節；這套系統主要由個人討論區與測驗平台兩部分所組成，如圖 1 所示。

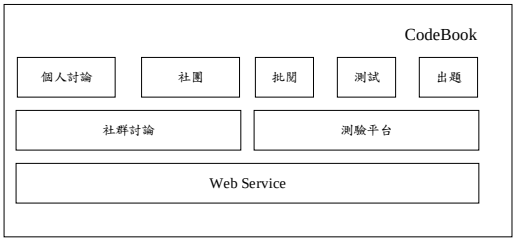


圖 1 系統架構

3.1 社群討論

在學習程式語言過程中難免會遇到阻礙，尤其是在發生在邏輯概念錯誤時，往往會找不出問題發生點，如果沒有外人指點，久而久之學習者多半會失去耐性，放棄學習；因此本系統想要提供一個平台，希望能有效率的尋求想要知道的答案。利用社群網路訊息快速傳播的特性，當使用者提出疑問時，這個問題能快速的散播開來，增加取得解決方案的機會。

當學習者有問題或新想法時，即可提出討論，討論可發布至個人討論或社團，其他人回覆後，將思考目前公認最好的答案，有沒有其他問題或是有更好想法，可提出回應討論，在良性互動的前提下最後就能取得比較好的

解決方案，如圖 2 所示。

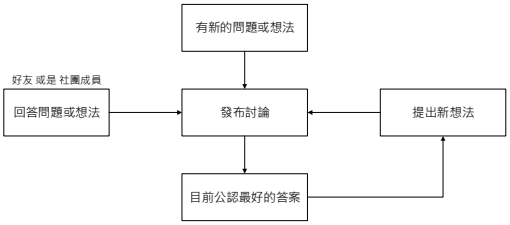


圖 2 提問流程

本系統仿效 facebook[引用 FB 網址]介面，設計出可供學習者線上相互討論的平台(圖 3)，本系統提供好友尋找的功能(圖 4)，例如現實中認識的朋友或同學，也可以直接邀請現實上不認識的人加入朋友圈。



圖 3 Codebook 介面

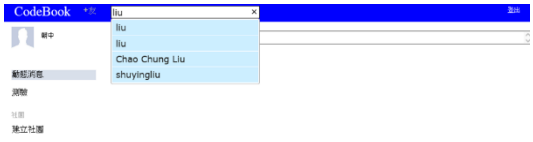


圖 4 好友搜尋

學習者不只是單方面的接收訊息，也可以提出自己對程式考試題目的解題想法或是概念，思路經過討論，學習者不單只是得到解答而已，更可以得到他人各種想法與概念，或許一些簡單的想法反而打破了自我認知，使自我達到突破性的成長，討論的過程畫面如圖 5 所示。



圖 5 程式討論

然而對於程式初學者而言，往往發生的錯誤都不屬於嚴重錯誤，例如:漏打分號、誤解了單引號與雙引號的意義、迴圈運算次數計算錯誤等。也因此我們的系統不只有將編譯執行的正確結果顯示出來，而是連同編譯錯誤與警告資訊都逐一顯示予使用者，該使用者在系統中所加入的好友皆可看到並幫助處理(圖 6)。

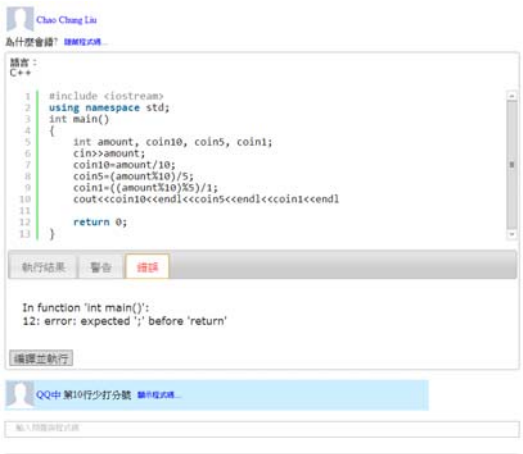


圖 6 錯誤詢問

提供社團機制，可提供一個小組或是程式設計特定主題的同好相互討論的環境，討論對象將不受限於自己的好友，可以更廣泛的接收新的概念與知識。

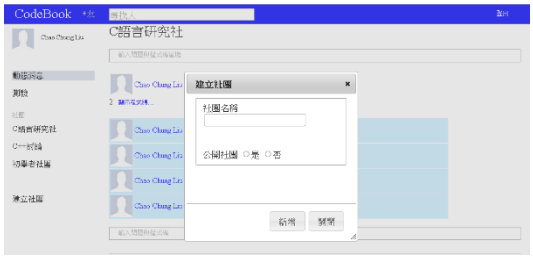


圖 7 社團機制

3.2 測驗平台

當學習者學習到一個階段，可以進行測驗來掌握自我學習狀況，從教學的角度來看，則是能協助老師了解到學習者所缺乏的部分或是觀念上的偏差；學習者也可進行小組競賽，利用同儕間的互相競爭達到互相進步的效果。

測驗系統利用網頁作答的方式，提供完整的測驗機制(圖 8)，以線上程式撰寫方式提供即時回饋，將不再受限於在特定區域測驗，教師也可利用此系統來進行考試，能夠快速的得知學生成績，免去批改的動作。

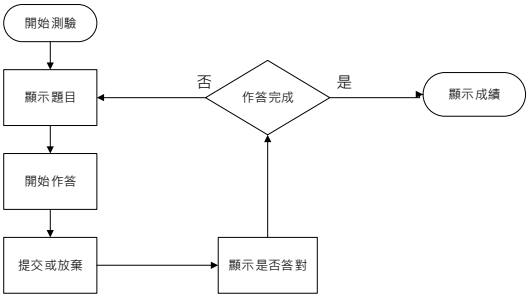


圖 8 測驗系統流程

測驗者在進行測驗時，撰寫完程式碼後自我測試都認為自己是正確的，但最後結果可能是錯誤的，這種現象大多是因為測驗者粗心大意，而不是觀念錯誤或是背景知識不足，因為在提交答案後已不能更改程式碼，若發生錯誤已無法補救，此類錯誤若經常發生，則測驗者將可能受挫而失去信心；因此，我們讓測驗者還未提交答案前即可進行測試，系統以該題測試資料來做為輸入資料，並以此來驗證程式的執行結果。

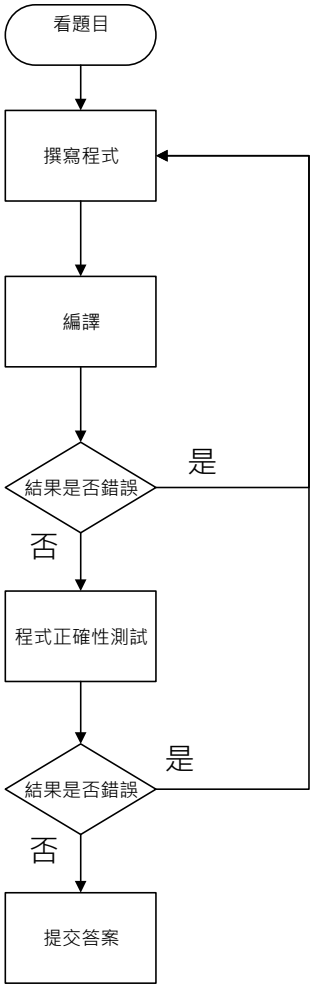


圖 11 測驗者作答流程

第四章 實驗結果

4.1 研究對象

本研究的研究對象為健行科技大學資訊工程系二年級學生，於必修課計算機程式設計實習中要求學生使用本系統，以問卷調查方式來取得學生回饋，回收有效問卷 111 份。

4-2 問卷設計

問卷內容如附錄所示，主要調查目的在於了解學生關於下列問題類別的意見

1. 學生對程式設計學習的態度

2. 學生對於同儕教學的態度
3. 系統的滿意度

4-3 結果分析

問卷分數由最高 5分 (非常同意) 到 最低 1 分(非常不同意)，其中一題複選題不在此列。我們將問卷計算分數後計算每一題的得分平均值，並呈現於圖 12。我們另外將問卷以每題為單位逐一顯示於圖 13。

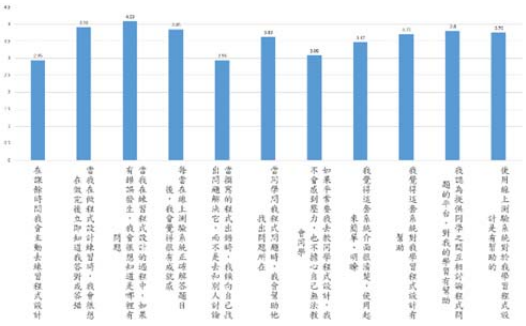


圖 12 問卷統計

由問卷結果顯示，在學習程式設計的過程中『當我在做程式設計練習時，我會很想在做完後立即知道我答對』以及『當我在練習程式設計的過程中，如果有錯誤發生，我會很想知道是哪裡有問題』分數較高，但是在出錯時會自己找答案的比例與其他項目相比來的要低，由這裡可以看出學生對自己的答案狀況感到在意，在發生錯誤時，多數學生傾向求助而非自己解決。

當無法自己找出問題時，由表 1 可知，大多數同學會尋求幫助的對象為其他學生，而不是老師，由圖 12，『當無法自己找出問題的時候，我會想問誰』得到平均 3.63 分可知，學生之間具有互助的意願，而且學生對自己回答他人問題是有信心的。我們認為，這樣的心態可以產生良性的互動，教學相長，對於觀念的修正與思考的邏輯都有幫助。

表 4.1 當無法自己找出問題的時候，我會想問誰

當無法自己找出問題的時候，我會想問誰				
其他人	學生	老師	學生、其他人	老師、學生、其他人
4	71	18	18	1
3.57%	63.39%	16.07%	16.07%	0.89%

結論

本論文提供一套可供同儕間互相交流的平台與及測驗系統，以現今普遍的社群網路概念來架構本系統，使同儕間能夠與好友相互討論，激發出新的想法，打破舊有的思維，同時結合線上編譯機制，快速的將想法進行實際測試，以實際行動驗證想法的可行性；本系統提供的社團機制，提供小組或者是程式設計同好專屬的討論空間，於社團中將不受限於自己的好友，也能夠與不認識的同好互相討論，達到知識的交流與突破。

本系統不只提供討論功能，同時也結合線上測驗機制，能在學習告一段落之後進行測驗，了解所學知識是否真正地被吸收，教導者也夠透過結果來確認被教導者的學習進度，為接下來的教學內容進行調整。

研究結果顯示同學對於此系統的操作介面表示過於單調，但是認為對程式設計學習是有所幫助；未來將持續增加程式設計語言類型，改進操作介面和功能設計。

參考文獻

[1] 王千倖，以「網路同儕教學」建構「網路學習社群」之行動研究，師大學報：科學教育類，第四十八卷第一期，119~142 頁，民國九十二年四月。

[2] Goodlad, S., Hirst, B., Peer tutoring. A guide to learning by teaching, Nichols Publishing, New York,

1989.

[3] Gartner, Audrey, Riessman, Frank, ” Peer-Tutoring: Toward a New Model”, ERIC Digest, 1993.

[4] Choy, M., Lam, S., Poon, C. K., Wang, F. L., Yu, Y. T., & Yuen, L.., “Design and implementation of an automated system for assessment of computer programming assignments.” , In Advances in Web Based Learning–ICWL 2007, Springer Berlin Heidelberg, pp. 584-596 , 2008.

[5] Kolb, David A., Experiential learning: Experience as the source of learning and development, NJ: Prentice-Hall, Englewood Cliffs, 1984.

[6] Kris MY , LEE, Victor , YU, Y. T. , “Learning motivation in e-learning facilitated computer programming courses”, Computers & Education, 55, 1, pp. 218-228, 2010.

誘導式結構發展彈性 ITI 建置校園 e 化雲端服務之研究 －以臺灣藝術大學為例

梅士杰
國立台灣藝術大學
frank@ntua.edu.tw

摘要

資訊管理及技術對藝術專業型大學組織管理而言，多處於配角的角色，或直接以資訊工具及技術層面來考量相關的議題，但外界環境在全球化、數位化和多元化的變遷潮流下，學校面對資訊科技諸多突破性發展時，幾乎都是循著原來的人力流程及組織結構的安排來設計資訊基礎建設。校園 e 化的過程都在組織既有流程與結構的角度中妥協，使資訊基礎建設所具備的彈性和適應性十分有限；因此，從符合資訊時代組織的角度與觀點來檢視校園 e 化的建設，是相當重要的研究議題。本研究以臺藝大教職員生資訊服務為對象，探討藝術專業型學校組織之資訊科技基礎建設(Information Technology Infrastructure ITI)角色扮演，透過誘導式結構模型(Heuristic Structure H.S.)釐清 ITI 發展的模糊地帶，從問題界定、歸納推論、情境定義到轉化策略，最終描繪出符合學校組織情境的資訊架構(Information Technology Architecture ITA)，並經由雲端概念及彈性的虛擬管理技術，發展符合校園學習、教學、研究、行政管理需求的 ITI 環境，以回應組織實況變遷及多元教學環境。

關鍵詞：資訊科技基礎建設、資訊科技架構、誘導式結構模型

Abstract

Information management and technology often plays a secondary role in the organizational management of art universities, or simply addresses management issues through the application of information tools and technology. The present study explores the role of ITIs in the organization of art universities with a focus on information services for faculty and students at National Taiwan University of Arts. This study attempts to shed some light on the development of ITIs through the Heuristic Structure model. From problem identification, inductive reasoning, definition of the situation, to transformational strategy, this study concludes with a framework for information technology architecture (ITA) suitable for educational institutions. Furthermore, by combining this framework with cloud computing concepts and flexible virtual management, an ITI environment is created that addresses learning, teaching, research, and administrative needs of schools and responds to actual changes in the organization and the conditions of a diversified teaching environment.

Keywords: ITI、 ITA、H.S.

1. 前言

本研究針對台灣藝術大學之資訊基礎規劃及建設，進行探討與研究。除探討臺藝大資訊基礎建設規劃外，還包括臺藝大資訊科技架構的設計，提供資訊基礎建設規劃時應考量之因素與程序，結合資源運用、綠色機房、雲端服務等功能，推導出臺藝大 ITI 設計原則，依此完成各項資訊建設實施方案。研究方法以「誘導式結構」理論作為操作工具，國內多應用於建築設計之概念建構及概念轉化為「空間結構」，即情境依空間組織邏輯之表達形式。組織 ITI 建構須以 ITA 為藍圖，而 ITA 本身也同樣為一邏輯結構型態，設計過程依歸於組織及使用者的需求來形成建構之概念，所不同於建築領域的是使用者使用之情境是透過 ITI 形成之虛擬空間。從進行論文思辯之問題、範圍、方向之界定與確認，並輔以文獻探討協助思考方向之資料收集，經由歸結(歸納)、推論(演繹)與所推導出之目標情境，轉化為本研究對象之「臺灣藝術大學 ITA 架構」的規劃設計概念。誘導式結構操作模型(如圖 1)共七階段：「問題界定、思考方向、重點提取、歸結、推論、目標情境、定義」。

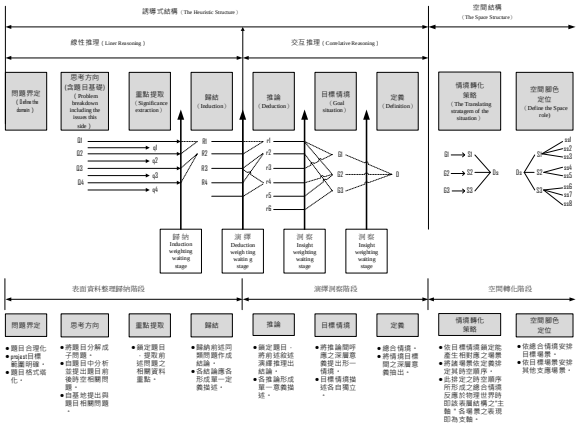


圖 1 誘導式結構模型與操作機制

2. 問題界定

本研究以臺藝大教職員生資訊服務為對象，發展具備彈性及適應性的 ITI，因組織資源匱乏情境中 ITI 發展困難，首先需設計規劃 ITA 架構，促成 IT 能力能夠塑型學校營運策略，反之學校營運策略也能塑型 IT 能力，以回應組織實況變遷及多元教學環境。依據文獻探討歸納包括：資源基礎議題、資訊科技基礎建設議題、資訊科技架構議題。形成問

題格式塔之介面如圖 2 所示，依此介面推導出臺藝大校園 e 化的 ITA 設計概念(目標情境)，終而導出定義(總體情境)，以為 ITA 表達形式之深層結構。

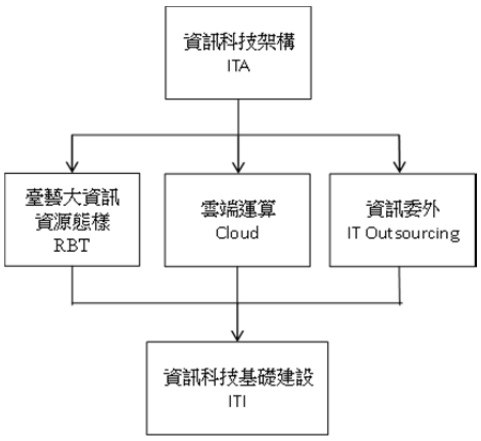


圖 2 問題格式塔

3. 思考方向

研究的目的在探討臺灣藝術大學 ITI 的需求和內涵，並建構一套具備彈性及適應性的 ITA，依此發展資訊服務系統。從文獻分析 ITI 是從資源基礎理論脈絡發展起，但大多文獻都以大型企業在完整組織架構下探討理論基礎，從資源匱乏情境探討之論述甚少，因此本研究文獻分析的相關領域主要有三大方面，第一為以企業資源基礎(Resource-Based Theory, RBT)的觀點出發，探討臺灣藝術大學資訊科技資源匱乏或不均之態樣，再進一步從 ITI 的彈性、適應性來探討 ITA 應如何策略性運用，包括新的科技雲端運算(Cloud)及資訊委外資源(IT Outsourcing)的整體規劃。最後，本研究並以誘導式結構模型理論(H.S.)，藉其操作模型歸納學校組織應如何建構 ITA，指引各項資訊系統提供適切服務與支援，並能配合學校永續經營所需持續發展調校 ITI 建設。以下將 ITI、ITA、RBT、Cloud、IT Outsourcing 這五個主要相關的研究領域及文獻，形成思考方向並鎖定問題界定之問題格式塔的五個議題：「資訊科技基礎建設議題」、「資訊科技架構議題」、「臺藝大資訊資源態樣議題」、「雲端運算議題」及「資訊委外議題」。其內容架構如表 1 所示。

表 1 思考方向之內容架構表

思考方向	子問題
資訊科技基礎建設議題(ITI)	資訊科技基礎建設的內涵
	資訊科技基礎建設的彈性
資訊科技架構議題(ITA)	資訊科技架構的內涵
臺藝大資訊資源態樣議題(RBT)	資源基礎
	臺藝大現況與未來
雲端運算的議題(Cloud)	虛擬化技術
	雲端運算與服務
公立學校資訊委外的議題(IT Outsourcing)	資訊委外的管理
	影響資訊委外專案績效的探討

4. 重點提取與歸結

本節由問題界定確立問題方向與範圍，並界定思考方向，收集國內外相關文獻，將前階依據子議題向度所搜尋之資料作出分類，經提取重點歸納同類資料交互建構獲得 23 項歸結描述。

4.1 資訊科技基礎建設議題

歸結一、 整合 ITI 必須有標準流程以降低作業複雜，而前端介面依使用者需求客制化、多元化

ITI 的角色是橫跨組織各單位共享的資訊科技服務，全球化市場強迫學校一方面要降低回應時間，另一方面又要以單一面向面對全球使用者，也就是說，同時要擁有集中化和非集中化二者的好處，同時 ITI 要能將資料集中統合於一致的標準下，結合流程降低作業的複雜，於前端資訊服務，依不同使用者需求進行客制化。

歸結二、 ITI 分成實體設施相關的科技服務、管理導向的人力服務兩個基礎建設

ITI 分成兩個概念，其一是科技基礎建設，提供實體設施的服務能力，其二是人力基礎建設，提供管理導向的服務能力，而前者為後者的基礎。

歸結三、 運用 IT 能力形成創新服務，網絡通路管理是必要條件

以學校組織而言，建立 ITI 通路能力是要組合不同通路，連結使用者或合作單位，而呈現出的是整合而一致的資料和作業，這一能力是啟動多項 e 化創意的必要條件。

歸結四、 資訊安全是共享資料的前提

資訊流通是以全校共享的資料為主，在安全與風險完善管理的前提下，提供使用者相互連結的通訊服務，進行全校共享的資料。

歸結五、 透過 ITA 進行 ITI 策略調準

ITA 與標準化是提供學校建立 ITI 的前導指引，ITA 呈現學校資訊能力及相關標準的服務，指示 IT 如何使用、如何整合，ITI 乃 ITA 的具體實現。

歸結六、 ITA 描繪出 ITI 應有得連結力和分享力，而 ITI 依此將應用系統與流程緊密結合

ITA 的設計規劃須清楚描繪出 ITI 應有的連結力和分享力，連結力是在思考網路要接到哪裡。連結力達成後可形成分享力有三個程度：資料分享，流程共享和創新服務。

歸結七、 經由整合化、模組化、IT 人員的彈性形成 ITI 的彈性

整合化、模組化、IT 人員的彈性，形成高彈性的 IT 基礎建設，有助於臺藝大透過：(1)對校務行政需求提供最好的回應力；(2)使易於進行最佳程度的 IT 創新；(3)對創新策略性業務應用系統，能降低開發的時間和成本；使學校創造價值有競爭優勢。

4.2 資訊科技架構議題

歸結八、 ITA 須整體描述學校 IT 的策略、作業、

科技能力

ITI和ITA實際上是同一件事的兩種表達形式，ITI是實體的、具象的；ITA是邏輯的、抽象的，ITA需能整體宏觀的描述學校的IT策略、作業能力、及科技能力。回顧IT建構的過程，因缺乏從組織的角度出發，做總體架構的規劃和設計，往往是組織內各部門提出不同的需求，就因應採用不同的硬體、軟體、系統平台和資料庫去滿足使用者需求，組織所得到的是一個個分散獨立自主的IT架構，這種自然形成的情況下，IT架構就會顯得雜亂無章，長期下來，IT反而成為組織經營發展的包袱。

歸結九、 ITA需反映出校務運作的整合與標準化

ITA圖是依據學校未來策略訂出的指導原則，並落實到如何運作，讓流程與資料密切聯繫。它的精神是要劃下校務如何運作的遠見，涵蓋「作業流程」和「資訊基礎建設」的邏輯結構，反映出校務運作所要求的「整合」和「標準化」，重點是清楚展示校務未來的運作方式。

歸結十、 臺藝大ITI策略定位為工廠型態，朝向轉型取得e化的策略價值

把「資訊科技」和「組織業務」相匹配，一直是資訊科技規劃的核心及關鍵的議題，學校思考本身在校務策略與資訊科技策略上的調準，有助於維持ITA的彈性。另外，學校也可以透過策略方格定位資訊科技策略，來建立有效轉型的動態能力，發展適性的ITA，善用新科技帶來的機會。

4.3 臺藝大資訊資源態樣議題

歸結十一、 資源互補成正向循環

臺藝大在101年度學校願景與發展特色之SWOT分析中，論出藝術大學環境中，組織人員多屬藝術人文專業人員，因缺乏經營管理資源，在組織與資訊科技整合的投入與運作上相對不足。因資源需要有整合能力將之運用而產生效能，能力必須靠資源的運用而展現出來，所以必須先運用資源培養教職員的核心能力，在資源內化為核心能力的過程中，為學校創造豐富的成果累積資源基礎。

歸結十二、 ITI應能完備資訊流通與精簡流程

ITI的功能可以無間隙地、自動地分享的資訊，以其為基礎，能使學校內部的資訊得以迅速流通，組織得以發展更先進的應用與活動，縮短作業流程的時間與跨部門的流程，提升資訊服務品質，形成策略性競爭優勢與機會

歸結十三、 資訊管理需形成共享性綜效

經由管理性的資訊科技，具有讓組織的知識與資源，更易被運用與更具共享性的功能，使組織內能夠跨越部門藩籬；換而言之，管理過程中管制規範的最終目標是形成共享性，所採取的限制動作也是為排除障礙，促使學校更迅速地回應師生的需求進而達到綜效。

歸結十四、 以學以致用提升成就感降低人力資源流失

由於所得與生產力之間有相關性存在，臺藝大因資訊人員薪資及教育訓練的預算普遍低於全國平均水準，所以可透過資訊科技應用提升業務效能，並形成個人自我表現與自我實現的成就感，降低人力資源流失。

歸結十五、 爭取計畫補助案能使資源高度被運用

政府歲出預算通常僅夠使資訊業務維持運作，不同於各大學基於未來發展方向積極爭取競爭性的經費，如大學卓越計畫之競爭性質，在申請過程中，由於審核嚴謹層層過濾，使得學校為了成功爭取資源，而激勵跨部門的單位能互相協調合作，經過卓越計畫辦公室的篩選，通過者已有完整的計畫目標、策略及方法，使爭取到的資源獲得高度運用。

4.4 雲端運算議題

歸結十六、 虛擬化可彈性運用資源降低營運成本

虛擬化技術對管理人員而言，可以將資訊硬體資源匯整成單一虛擬集區，降低管理複雜度及成本。實現在同一實體系統上運行多個作業系統，並允許系統資源在各個作業系統間按需求來進行資源分配。整體而言，虛擬化能打破伺服器隨新系統1：1成長的惡行循環，並可彈性運用資源，簡化管理負擔，降低營運成本。

歸結十七、 私有雲環境能有效駕馭現有基礎設備

雲模型的可用性有五個重要特徵，(1)依需求自助服務，(2)廣泛用任何網路裝置存取，(3)快速有彈性，(4)共享資源池，(5)被監控和量測的服務。私有雲環境能讓管理者有效駕馭現有基礎設備的現有功能，使之精整、架構標準化。

歸結十八、 校園IaaS動態調整雲端主機的服務

由學校建置硬體設備及可擴充的硬體架構，形成校園IaaS服務，提供電腦運算基礎設施，可以隨著運算尖峰或離峰時段，調整雲端主機的服務。師生只需要花費使用的成本就可以透過網路，使用雲端的各種作業系統及硬體資源來滿足其需求。

歸結十九、 校園PaaS服務節省工具軟體投資，及硬體的管理負擔

PaaS是用來開發與執行應用程式服務的雲端平台，使用者可依服務供應商所提供的API自行開發軟體及特定的作業系統及應用函式庫；校園PaaS服務為提供創作者軟體開發平台，如Adobe、AutoCad、3DMAX…等，使用者可節省工具軟體投資及硬體的管理負擔。

歸結二十、 校園SaaS服務進行作品的展示、遞送、媒合

SaaS以軟體應用程式為基礎，由服務提供者支援各種以服務為導向的應用，是一種軟體應用的提供模式，校園SaaS服務提供以網路服務形式，進行師生作品的展示、遞送、媒合，以符合文化創意產業市場需求。

4.5 公立學校資訊委外議題

歸結二十一、 臺藝大IT委外重點目標為強化資訊人資訊科技能力，及取得先進資訊科技

臺藝大資訊系統委外重點是在於彌補學校內

部因為成員對資訊科技處理能力的不足，並協助改善科技投資報酬率等目標，包括：增強資訊科技能力、強化資訊人員訓練、減輕運作成本、取得先進資訊科技。

歸結二十二、 學校官僚體系的文化缺乏競爭壓力驅使形成低集體效能

民營企業存在的目的是要賺取最大利潤，因此，民營企業一切以顧客導向，創新求變的滿足顧客需求。公務機構存在的目的，則是要服務人民，但大多數公務機構卻常有對顧客需求漠視的現象發生，主要是因為公務機構的經費並非直接向顧客收取來的。臺藝大屬典型官僚體系的組織文化，在缺乏競爭壓力驅使，組織中的成員越多往往易形成低集體效能的團隊，使專案參與人數與合作力量成反比。

歸結二十三、 親和性、激勵制度可改善官僚體系的文化

親和性有助於團隊成員發展共同的心智模式，並增加團隊內的社會互動，減少不必要的情感衝突與誤會；適切的激勵制度，則會影響專案成員對於專案認同的態度及績效。為有效解決目前大多數資訊委外專案所遇到實務上的問題，在高層需全力支持下，透過親和力在資訊委外專案中聚集業務內隱知識，同時將專案成員視為資產，並適時給予考評，予以激勵。

5. 推論

本節於前節歸結出23項臺藝大ITI設計要點描述後，將歸結之資料經演譯，得以解釋全部問題之概念，並建構臺藝大ITA之完整結構，形成一合乎邏輯過程之因果關係。

經過交互推理的過程中可以歸納出以下九個推論，從 ITI 實體設施相關的科技服務面向有五個推及 ITI 管理導向的人力服務面向有四個推論說明。

5.1 ITI 實體設施相關的科技服務

推論一、 應用系統前端介面需多元適性的客制化

綜合以下二項歸結得此推論：

歸結 1: 整合 ITI 必須有標準流程以降低作業複雜，而前端介面依使用者需求客制化、多元化。

歸結 9：ITA 反映出校務運作的整合與標準化。

推論二、 標準與規範須能達成系統之間的整合及相容度，維持資料的機密性、完整性、可用性。

綜合以下二項歸結得此推論：

歸結 4：資訊安全是共享的資料的前提。

歸結 7：經由整合化、模組化、IT 人員的彈性形成 ITI 的彈性。

推論三、 流程控管須提升資料的透通程度

綜合以下三項歸結得此推論：

歸結 12：ITI 應能完備資訊流通與精簡流程。

歸結 3：運用 IT 能力形成創新服務，網絡通路管理是必要條件。

歸結 6: ITA 描繪出 ITI 應有得連結力和分享力，而 ITI 依此將應用系統與流程緊密結合。

推論四、 資訊服務須由校務運作分析整體的 ITA 藍圖，以規劃 IT 的策略、作業和科技能力

綜合以下三項歸結得此推論：

歸結 2: ITI 分成實體設施相關的科技服務、管理導向的人力服務兩個基礎建設。

歸結 5：透過 ITA 進行 ITI 策略調準。

歸結 8：ITA 能整體描述 IT 的策略、作業、科技能力。

推論五、 綠色、集中、動態的 IDC 需支持整合、有彈性的雲端服務

綜合以下二項歸結得此推論：

歸結 16：虛擬化可彈性運用資源降低營運成本。

歸結 17：私有雲環境能有效駕馭現有基礎設備。

5.1.1 小結

當內部及外在環境變化時，ITI 實體設施相關對環境的調適能力、柔韌性、和回應能力是關鍵因素。富有彈性的動態 IDC 能滿足校務需求且不增加成本，更是取得長期競爭優勢不可或缺的基礎。本研究經由文獻歸結推論後，洞察出臺藝大在 ITI 實體設施相關的科技服務中，必須以動態 IDC 為核心，發展四個 MIS 技術發展主軸包括：應用系統、標準與規範、流程控管及資訊服務，因為如此才可將資源共享及再利用，如圖 3。

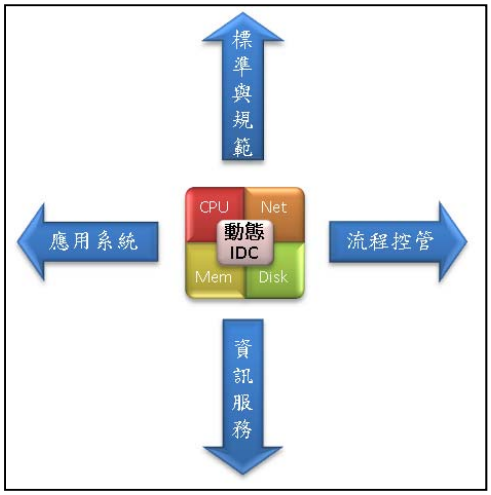


圖 3 實體設施相關的科技服務架構圖

5.2 ITI 管理導向的人力服務

推論六、 學習的取向是使 IT 人員能有效率的管理

綜合以下三項歸結得此推論：

歸結 11：資源互補成正向循環。

歸結 14：以學以致用提升成就感降低人力資源流失。

歸結 21：臺藝大 IT 委外重點目標為強化資訊人資訊科技能力，及取得先進資訊科技。

推論七、 管理的取向是使服務品質提升

綜合以下三項歸結得此推論：
歸結 18：校園 IaaS 動態調整雲端主機的服務。
歸結 19：校園 PaaS 服務節省工具軟體投資，及硬體的管理負擔。
歸結 23：親和性、激勵制度可改善官僚體系的文化。
推論八、 服務的取向是為支持產出優質智慧資產
綜合以下三項歸結得此推論：
歸結 13：資訊管理需形成共享性綜效。
歸結 15：爭取計畫補助案能使資源高度被運用。
歸結 22：學校官僚體系的文化缺乏競爭壓力驅使，形成低集體效能。
推論九、 智慧資產的取向是豐富學習能量
綜合以下二項歸結得此推論：
歸結 10：臺藝大 ITI 策略定位為工廠型態，朝向轉型取得 e 化的策略價值。
歸結 20：校園 SaaS 服務進行作品的展示、遞送、媒合。

5.2.1 小結

在 ITI 管理導向的人力服務中，從學習了解如何達成管理的綜效，由管理形成優質服務，組織成員享受便利的服務後，可產出智慧資產對學校做出貢獻，學校累積的智慧資產，再透過學習回饋給組織成員，亦可對未來文化創意產業形成加值分享的機制，為學校開闢新的經費資源。綜合前述推論結果洞察出從學習、管理、服務、智慧資產，學校可在 ITI 人力管理促成良性的循環。學校 ITI 發展過程中，需特別注意技術的發展，要配合 ITI 管理導向的人力服務四項目標，如圖 4。

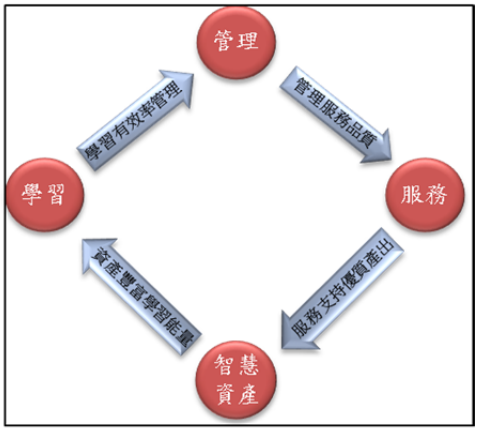


圖 4 ITI 管理導向的人力服務架構圖

5.3 臺藝大 ITI 科技服務與人力服務整體關係

從 ITI 實體設施相關的科技服務五個推論，及 ITI 管理導向的人力服務四個推論，經過交互推理的過程可以歸納出：臺藝大應以動態 IDC 為核心支撐應用系統、標準與規範、流程控管、資訊服務 4 個 MIS 主軸，由此 4 主軸資源的能量來完成學習有效管理、管理服務品質、服務支持優質產出、豐富智慧資產回饋學習資源 4 項目標，形成臺藝大 ITI 科技服務與人力服務整體關係圖，如圖 5。

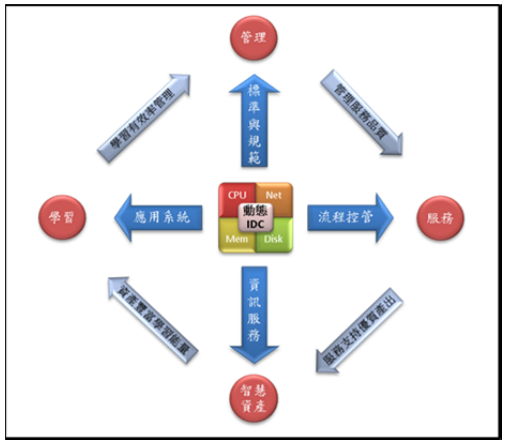


圖 5 臺藝大 ITI 科技服務與人力服務整體關係圖

6. 目標情境-臺藝大 ITA 設計

6.1 臺藝大 ITI 目標情境

依前述九個推論中相同之情境導出以下五個目標情境，其說明如下：
情境一、 整合校園資訊服務體系
綜合以下二項推論得此目標情境：
推論 1 應用系統前端介面需多元適性的客制化
推論 6 學習的取向是使 IT 人員能有效率的管理

由校園資訊入口網起，將資訊整合、資源共享、優化校園活動宣傳推廣，並需完備數位學習環境、數位內容資料庫，完善各種資訊環境提升管理作業的方便、有效性，最終能提供師生個人無時無地、使用任何載具，皆能順利獲得即時、正確的資訊服務。

情境二、 提升校務行政系統服務品質
綜合以下二項推論得此目標情境：
推論 2 標準與規範須能達成系統之間的整合及相容度，維持資料的機密性、完整性、可用性
推論 7 管理的取向是使服務品質提升

學生、教師、家長的服務由行政團隊提供，而行政人員要能提升提服務品質，則須依賴資訊系統效能，所以 IT 人員的管理作為應以服務為出發，促使委外合作團隊開發的資訊系統，更貼近業務服務需求。應成立專案小組以 CMMI 概念進行委外管理，將校務行政資訊系統整合、流程精簡專案，力求各利害關係者服務品質的提升。

情境三、 培養資訊素養提升競爭力
綜合以下二項推論得此目標情境：
推論 3 流程控管須提升資料的透通程度
推論 8 服務的取向是為支持產出優質智慧資產

教職員生獲得優質的服務後，在教與學的過程中，內化知識以充實個人素養，產出的智慧資產以充實學校智慧資產；從個人到組織內部的教學互動，提升溝通互動品質，包括資訊搜尋、保存、組織、管理、利用、分享的功能，也對資料及智慧資產進行資安權限控管，以法律智財權保護並加值運用。

情境四、 提供適用的個人數位工作環境

綜合以下二項推論得此目標情境：

推論 4 資訊服務須由校務運作分析整體的 ITA 藍圖，以規劃 IT 的策略、作業和科技能力

推論 9 智慧資產的取向是豐富學習能量

學校資訊科技的運用必須形成知識流的循環，並回饋組織與成員，資訊科技的架構最終也必須符合教職員生，個人數位工作環境的應用，要清楚明確的知道教職員生從事各項活動所需要的軟硬體，如提供專業套裝軟體、各單位網路磁碟空間、建立全校線上通訊錄、行事曆整合通訊環境、身分識別生命周期系統、線上簽核無紙化環境、學習歷程提供累積個人學習成果等。

情境五、 導入雲端、落實 ISMS 保證持續營運

綜合以下一項推論得此目標情境：

推論 5 綠色、集中、動態的 IDC 需支持整合、有彈性的雲端服務

校園 IDC 的環境有如資訊科技服務的心臟，應透過虛擬化技術建置私有雲後，可進行組織內、外部資訊資源的使用量測，依此進行資源調度形成雲端服務，俾確保 IDC 持續營運亦落實 ISMS 資安管理系統，降低非法使用干擾，可提升校內外網際網路速率與穩定，及完備 IDC 整體資安管理及機制。

6.2 臺藝大 ITA 設計

本研究依序探討了資訊科技基礎建設議題、資訊科技架構議題、臺藝大資訊資源態樣議題、雲端運算議題及資訊委外議題，並經過重點提取、歸結，形成九項推論，匯整出「臺藝大 ITI 科技服務與人力服務整體關係」，再結合 ITI 的五項情境目標包括：整合校園資訊服務體系，提升校務行政系統服務品質，培養資訊素養提升競爭力，提供適用的個人數位工作環境，導入雲端、落實 ISMS 保證持續營運。將臺藝大所期待的 IT 應用表達成一目了然的 ITA 架構圖，標示出資訊科技的高層次結構，提供學校決策者透過 ITA 圖和 IT 人員的協調討論，澄清了學校 IT 能力的選項，能夠掌握和監督資訊科技的應用，也劃下了組織如何運作的遠景，如圖 6 所示。

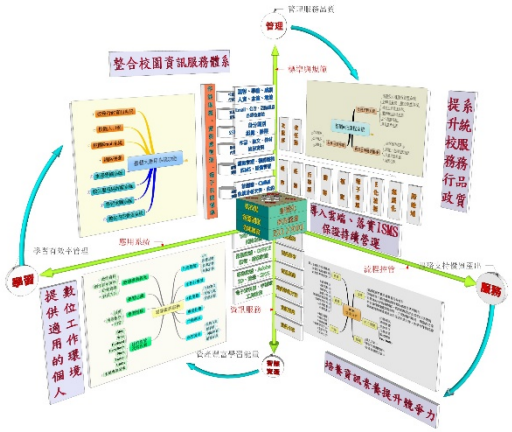


圖 6 臺藝大 ITA 架構圖

7. 情境轉化策略

從推論到目標情境擬定 ITA 的邏輯設計，最後從情境轉化策略，導出臺藝大 ITI 實體的、具象的措施。在此九個推論中，涵蓋了管理導向中的人力服務與實體設施，此相關的科技服務有兩個層面一起探討，其中是校務活動性質，也是資訊系統功能建構的虛擬空間，所形成的情境轉化策略與資訊系統角色定位，才是完整的規劃目標，如表 2。

表 2 目標情境之 ITI 轉化策略表

目標情境	ITI 建置方案
整合校園資訊服務體系	校務行政資料庫整合計畫
提升校務行政系統服務品質	導入校務流程系統計畫
培養資訊素養提升競爭力	導入 PIM 個人資訊管理計畫
提供適用的個人數位工作環境	導入藝術在雲端計畫
導入雲端、落實 ISMS 保證持續營運	動態 IDC 綠化節能虛擬管理計畫
	導入 ISO27001 認證計畫

8. 結論

在整個誘導式結構方法明確定義後，則透過情境轉化策略，將 ITA 角色定位出整個實質 ITI 結構，即為本研究第 6 節中之臺藝大 ITI 目標情境與 ITA 設計，並將概念的規劃轉化為實質資訊基礎建設的角色定位。在第 7 節中，推導出的要點轉化為目前臺藝大校園 e 化環境上之建置方案，最後給予整體規劃之設計建議。

一、 以資源互補形成正向循環，克服資訊資源匱乏或不均困境。

二、 善用虛擬技術的彈性，支撐 ITI 科技服務與人力服務，形成整體雲端服務。

三、 臺藝大 ITA 架構劃下 ITI 建設目標的遠見：「藝術植林在雲端、信捻巧思慧成塔」

四、 持續依據 ITA 規劃進行臺藝大校園 e 化實施方案內容設計。

參考文獻

[1] 陳貞夙，以資訊時代組織轉型觀點建構企業資訊基礎建設的理論模型，國立台灣大學資訊管理研究所博士論文，2001

[2] 蔡仁惠，誘導式結構理論在建築設計課程上之應用，城市與設計學報，都市設計學會，第二十二期，頁 199-238，1999

[3] 楊叔卿、張君豪，由校園資訊服務的觀點探討大學校院委外建置學習管理平台，2004 全球華人計算機教育應用大會，Hong Kong，2004

[4] Allen, B.R., and Boynton, A.C. “Information Architecture: In Search of Efficient Flexibility,” MIS Quarterly (15:4), pp.435-445, 1991.

[5] Barnes, F. R., “Putting a lock on Cloud-Based Information,” Information Management Journal, Vol. 44(4), pp. 26, 2010.

[6] Black, J. A. and Boay K. B., “Strategic resources: traits, configurations and sustainable competitive advantage,” Strategic Management Journal, Vol.15, Sum, pp.131-148, 1994.

[7] Claver, E., Gonzalez, R., Gasco, J. and Llopis, J., “Information Systems Outsourcing: Reasons, Reservations and Success Factors,” Logistics Information Management, Vol. 15, No. 4, pp. 294-308, 2002.

[8] Guri-Rosenblit, S. “Virtual universities: current model and future trends.” Higher Education in Europe, XXVI (4), pp.487-499, 2001.

非試不可（Facebook）--另類的幼兒園親師交流

童巧雯
台中市忠孝國小附設幼兒園
dearbellebn@hotmail.com

邱淑惠
台中教育大學幼兒教育學系
shuhui@ms3.ntcu.edu.tw

摘要

研究者以自己任教班級之家長及協同教師為研究對象。以個案研究的方式，自 2011 年 10 月至 2012 年 10 月使用 FB 進行親師溝通。透過訪談、網路互動及文件資料蒐集與分析，描述研究者如何應用 FB 進行親師交流、過程中遭遇哪些困境，以及因應困境的方式，並反思研究後獲得的收穫。
關鍵詞：幼兒園、facebook、親師交流。

Abstract

In this study, we described how parents responded to our tryouts of using FB to facilitate parent-teacher communication in a preschool classroom. Our case study started from October 2011 to October 2012, which lasted for one year. Problems encountered and strategies used to interact with parents were discussed.

Keywords: facebook, preschool, parent-teacher communication

1. 前言

1.1 研究背景與動機

幼兒園除了教學外，首重親師交流。幼兒教師與家長的溝通、互動及合作，會直接或間接地影響幼兒的學習方式。現今一般幼兒園進行親師交流的方式，大致上為面對面的溝通、書面往來、親子講座及活動、家長參與教學以及利用班級網頁提供家長資訊。但研究者本身使用班級網頁的經驗是，家長偏好由網站觀看小朋友們的活動照片，但對於留言版的使用、公佈的資訊內容往往視而不見，或是只有少數幾位家長點閱[1]，親師交流的成效有限。

有鑑於 facebook（簡稱 FB）的使用人口越來越多，教師與家長很容易連線至 FB，在 FB 呈現自己或觀看他人的動態活動以及與朋友互動。這讓研究者開始思考 FB 的獨特性是否也可以應用於親師交流。

在教育上應用 FB 的相關研究中，主要是針對學生和教師的使用情形進行調查[2.3.4]，或是應用於課程及學習方面與學生互動的研究[5.6.7.8.9]，抑或針對師生關係進行研究[10.11.12.13.14]。而過去應用網路進行親師交流的研究，大致上都是透過班級網頁[15.1]、部落格[16.17]、電子聯絡簿[18]及班級通訊電子報進行[19]。因此，幼兒教師若想應用 FB 進行親師交流，常缺乏相關研究可供參考。故研究者以自己的班級為個案，實際應用 FB 進行親師交流，期望透過本研究分享教師的應用經驗。

1.2 研究目的

基於上述的背景與動機，本研究欲達成的目的，分述如下：

（1） 瞭解幼教師可以如何應用 FB 進行親師交流。
（2） 探討幼教師應用 FB 進行親師交流的困境與因應策略。
（3） 反思研究者應用 FB 進行親師交流的收穫。

2. 文獻探討

2.1 網路新勢力--Facebook

科學家經常發明便利人與人溝通的方式，例如，貝爾發明電話，讓我們透過線路進行遠距離的溝通；而網際網路 (Internet) 的發明又是一大躍進[9]。網路盛行後，有眾多的網站可以提供資訊讓使用者瀏覽及查詢。但是單向性的操作模式不能滿足使用者與網頁互動的需求。隨著網路的進化，Web 2.0 的概念開始誕生，網站開始提供使用者更多不同於以往的互動方式。

O'Reilly 將 Web 2.0 定義為一個讓使用者彼此能進行故事分享和經驗傳遞的平台[20]。Web 2.0 的特性可歸納為下列五項：

（1） 共同創造網路資訊：資訊不再是網站經營者所給予，而是透過使用者不斷地進行創作與分享，讓網路資訊更為豐富。
（2） 網站更貼近使用者：許多網站提供免費程式讓使用者盡情地存取、使用及修改，讓網站或網頁更貼近使用者。
（3） 整合各式資訊：不同類型的資料，像是文字資料、照片、影音檔和留言，能透過連結整合，讓網站內容更加多元。
（4） 立即且迅速的互動模式：使用者透過傳遞訊息、雙向溝通，建立一個即時互動、回饋的平台，例如：FB、Plurk、Twitter 等。
（5） 多樣性的裝置：以往要使用網路只能透過電腦連上網際網路才能使用，現今除了電腦之外，透過 3G 行動網路的設置，行動裝置開始可以使用網路，像是 PDA 及手機都能使用網路，讓使用者更便捷地使用網路功能。

由上述可知，Web 2.0 確實改變了網路的運作模式，操作裝置也變得更加便利。Web2.0 讓使用者利用資訊的傳輸建立一個公開且互動的平台，也透過使用者的互動、共享，讓人的交流模式更為簡便、迅速。FB 更是 Web2.0 之代表性產物。

FB 於 2004 年 2 月 4 日由當時的哈佛大學學生 Mark Zuckerber 成立，原本只有哈佛校內學生可以加入，之後不斷擴展至其他長春藤名校，到目前為止已經有超過 7 億人口在 FB 註冊使用，台灣則有 1342 萬的人註冊（http://www.checkfacebook.com）。FB 的創辦人 Mark Zuckerberg 表示 Facebook 並不是要取代人們的實體社交生活，而是協助使用者藉由網路，跟自己現實生活中的朋友聯絡感情[21] 。它的使命是給人們權力去分享，使我們的世界變得更加開放、更有連結性[22]。

至 FB 誕生後，教育界亦嘗試應用 FB，相關的教育應用研究可分為三類：(一)了解教師或學生使用 FB 的現況；(二)分析在課程中應用 FB 進行教學的成效；(三)探討在 FB 裡的師生關係。有鑒於學前階段的親師關係甚為重要，故研究者亦希望透過 FB 進行幼兒園教師和家長的交流，希望透過此研究讓未來的親師交流更加有效。

2.2 親師交流

家庭和學校是幼兒成長及社會化最重要的兩個地方。家庭是幼兒發展的基礎，很多習慣和觀念都深受家長的教養觀所影響。在幼兒園中，透過親師交流能將教師的教育理念傳遞給家長，讓家長提供資源給予教師助力，在親師雙方互動下促進幼兒發展。對於幼兒教師來說，家長便是家庭的代表，教師如何和家長進行良好的互動，扮演其適切的角色，這是一個相當重要的課題。

每位家長都期望自己的孩子都能成龍成鳳，在目前的社會來說，因為家庭結構的改變及政策推動下，家長對於幼兒教師的期望，已經和以往大不相同了。現今的家長經常對幼兒的學習有過高的期望，對幼兒的行為及生活適應問題，則是將教育責任推給教師。因此常有家長和教師的教學理念不同，甚至意見相左的衝突產生。但若幼兒教師與家長有良好的雙向溝通，則能營造互助互信的關係。良好的互動是：教師能尊重每個家庭教養方式的不同，主動連繫家長說明幼兒在園內的狀況，而家長也能善意的回應。教師可定期提供家長育兒知識或是親職新知，幫助家長成長。除此之外，若是幼兒發生問題或困難時，教師和家長可以一同協商、溝通，討論如何處理為最佳方式。故親師關係的好壞深深地影響著幼兒的發展。

幼兒教師在親師交流中除了適切地扮演自己的角色之外，在幼兒園中也有不同的管道進行親師交流，像是透過口語溝通、書信往來、親職講座、家長參與、親子活動及網路資源等方式。透過多元的親師交流管道，讓家長和教師更了解幼兒的發展狀況，可讓幼兒獲得更適切的協助及教育。

隨著社會的進步及轉變，網路及電子產品不斷推陳出新，E 化的交流管道也不斷地開發、試用，透過網路及電子科技產品的快速性及便利性，能更完整地達到親師交流的效益。蔡瑞榮[23]認為幼教師可透過電話或電子郵件，針對孩子個別狀況，立即與家長進行溝通；張明輝[24]指出在學校網站設立留言版及討論區，可提供親師互動的機會，也可視情況透過電子郵件保持聯絡，促進親師交流效果；另外，Tobolka [25] 認為教師可藉網站可提供家長班級活動資訊。由此可知，應用網路進行親師交流，已經是目前可行的方式之一。

過去已有教師透過電子聯絡簿[18]、班級通訊電子報[19]、班級網站及部落格的方式，提供家長更多學校資訊[1.17]。研究發現藉由班級刊物、部落格及班級網頁，提供幼兒動態活動資訊，像是照片或影片，可讓家長更了解幼兒在學校中的狀況。透過留言版或討論區，可促進親師雙向溝通。雖然上述研究中，有些家長還是習慣傳統面對面的溝通方式，但是大多數的家長對應用網路進行親師交流持支持的態度。而 FB 除了擁有網路的功能外，也結合了我們生活的真實世界。在本文中，研究者期望透過實際嘗試應用 FB 進行親師交流，並以嚴謹的態度分析與反省使用經驗，作為其他教師之參考。

3. 研究設計

本研究採行動研究法，探討研究者如何應用 FB 功能選單進行親師交流、發生的困境及因應方式，並從中反思應用 FB 進行親師交流的收穫。

3.1 研究場域

本研究嘗試將現今最常用的網路媒介—FB 和親師交流的議題結合，實際應用 FB 中設立私密社團的功能，讓社團裡的成員不用擔心自己所發表的文字被別人看到，而侵犯自己的隱私權。此外，也可防止幼兒的資料在網路上直接公開，故透過這獨特的特性，讓家長可在社團內暢所欲言。研究者於 FB 成立的私密社團，僅供小鹿班家長使用，並命名為「小鹿斑比的秘密花園」（化名），故 FB 與「小鹿斑比的秘密花園」為本研究的主要研究場域之（見圖 1）。另外，FB 外之教師與家長的面對面與聯絡簿溝通等，因與研究主題相關，也納入此次研究資料的蒐集範圍。



圖 1　FB 秘密社團--小鹿斑比的秘密花園

3.2 研究參與者—小鹿斑比秘密花園的成員

研究參與者的成員為 2011 年小鹿班的家長，小鹿班為混齡班，這些幼兒依年齡分為中班生和大班生，中班生 3 人，大班生 27 人，共 30 人。在小鹿斑比的祕密花園社團中，共有 38 名成員，包括 21 個家庭裡的成員(有 9 名幼兒的家長沒有參與)、研究者、指導教授及協同教師加入社團。社團裡的 21 個家庭中，有 11 個家庭只有一位成員加入，有 8 個家庭為爸媽皆加入，另有 2 個家庭為三名以上成員加入，包括爸媽和其他的親戚。這 21 個家庭中，共有 30 名主要照顧者，大多數的職業為教師、商、家管和服務業，另外，還有以資訊及設計為職的家長。而主要照顧者的年齡層，大多數為 35-39 歲，其次為 30-34 歲，而 45 歲以上的也只有 1 人。此外，其他的成員也有奶奶是 55-60 歲，其他的親戚像是舅舅、阿姨、伯伯。綜合而言，社團成員大致上都屬於高社經地位及年輕的家長，而且對於操作電腦都是有經驗的。

4. 結果與討論

4.1 如何應用 FB 進行親師交流

研究者將自己角色設定為園丁，將研究歷程分為四期，分別為播種期、灌溉期、花開期與結果期，以下將說明這四期分別運用了哪些功能選單進行親師交流。

(1)　播種期

研究者透過「設立新帳號」、「搜尋好友並加入好友」及「成立祕密社團」這三個 FB 提供的功能。

（1.1） 設立親師溝通用新帳號

為了讓研究者的教學專業和私生活分開，讓與家長或與私人好友分享的資訊可以有所分別，研究者設立一個具專業形象的新帳號。因此，研究者可以依需要在不同的帳號中分享自己的生活或心情。設立親師溝通用帳號時，研究者會選擇使用，一張臉部清楚的相片作為大頭貼，並將所任職的學校及居住地加入說明，讓家長更清楚邀請的人為幼兒的教師。

（1.2） 搜尋好友並加入好友

在搜尋好友的當中，由於在搜尋處只輸入姓名，可能會產生很多相似的人名，搜尋過程中較為不易，故可利用電子郵件搜尋，讓搜尋過程較為簡單便利。加入好友之後，只需等待家長答覆好友回應，家長便為此 FB 帳號的好友。

（1.3） 成立秘密社團

在確認家長為好友的同時，研究者設立一個祕密社團，此類社團的特性是非成員無法從搜尋找到這些社團，或是查看有關社團的任何資訊，包括名稱或成員名單。社團名稱不會顯示在成員的動態時報中。若要加入私密社團，需要社團管理者將您新增到社團。設立秘密社團的目的不傷害社團成員或班級幼兒的隱私權。因此，研究者確定家長為好友間的關係後，再將家長加入社團中，此為本研究的第一階段播種期。在這段期間內共有 20 位家長，分別來自 17 個家庭的成員加入社團。

(2)　灌溉期

此階段共使用五項功能選單，分別為：「利用塗鴉牆說明各類訊息」、「透過網路文章給予親職知識」、「藉由打卡功能增進親子關係」、「透過私人訊息聯繫幼兒各類情況」以及「轉貼照片供家長欣賞」。以下分別說明之：

（2.1）利用塗鴉牆說明各類訊息

在幼兒園中，舉凡全園活動，或是班上活動都需要讓家長了解，故除了透過原本的聯絡單或口頭告知外，研究者也會在 FB 的塗鴉牆再次提醒，告知家長學校內近期發生的事項，像是戶外教學、學校運動會、教學需要協助事項，讓家長有多元管道得知學校訊息。

（2.2）透過網路文章給予親職知識

研究者於 FB 上尋找了一些跟教養有關的文章或是粉絲專頁分享給家長(例如，親子天下或是在 Yahoo 上看到新的新聞)，讓社團內的家長可以看見資訊內容，幫助家長成長。

（2.3）藉由打卡功能增進親子關係

在研究期間，研究者只要到適合親子出遊的郊外，都會透過「打卡」推薦給家長，讓家長知道每個季節可出遊的好去處，鼓勵家長多帶幼兒到戶外遊玩。

（2.4）透過私人訊息聯繫幼兒情況

在塗鴉牆上的資訊，所有社團成員都可看到，但顧及有些訊息涉及個人隱私，像是幼兒腸病毒事件、個人問題等，較不適合給所有家長看到，就在私人訊息與家長聯絡，讓家長放心溝通。

（2.5）轉貼照片供家長欣賞

家長們為幼兒拍攝照片的角度會有所差異，研究者因與家長為好友，所以可以看到有些家長很用心地幫幼兒們記錄幼兒生活的點點滴滴。但是班上的家長之間未必是好友，因此有些精彩紀錄其他家長未必能看見。故研究者經過家長同意後，藉由轉貼的方式，將照片或影片從個別家長的塗鴉牆上轉貼至社團內，讓每位家長甚至幼兒都能欣賞。轉貼前事先詢問當事者是否能進行轉貼，是獲得家長信任的重要工作。

灌溉期中家長幾乎沒有文字回應，甚至按讚的

人數也很少。因此，研究者試著嘗試使用 FB 中不同的功能選單，觀看成效，同時也以文字不斷地提醒家長可在社團內進行分享和回應，希望家長能給更多不同的回饋。但研究者能由按讚的人員資料了解有那些家長看過該篇訊息，不至於會像班級網頁上的訊息，貼文之後卻不曉得家長看到的有多少，這也是 FB 的功用之一。

(3) 花開期

在花開期階段研究者使用了六種FB的功能選單，分別為「轉貼社團成員照片及訊息」、「利用聊天室與家長進行交流」、「舉辦活動供家長了解活動狀況」、「上傳幼兒表演影片供家長欣賞」、「透過「打卡」讓家長了解戶外教學狀況」、「於塗鴉牆上尋求家長協助並感謝其支持」。以下分別說明之：

（3.1） 轉貼社團成員照片及訊息

在此時期，社團成員還是習慣於自己的塗鴉牆上發佈訊息及照片，而研究者透過轉貼的方式，讓家長可以得知更多與班上及幼兒相關的事項。這個階段與灌溉期的不同在於，除了照片之外，由於協同教師也習慣於自己的塗鴉牆發佈訊息，研究者無法改變其習慣，故經過協同教師的同意後，也以轉貼協同教師的分享，讓家長更了解協同教師的想法，例如，協同教師在他自己的塗鴉牆上寫著「小鹿班～ 你們真幸運...可以多當一天幼稚園小孩，也多一天當我和童老師的心肝寶貝^^"」（FB-20120619），這些資訊只有協同家長的好友看得到。但轉貼後，可讓每位社團成員都能看到這些溫柔的叮嚀。

（3.2） 利用聊天室與家長進行交談

聊天室是一個可以讓FB成員談天說地的虛擬場所，透過聊天室可以提出疑問、溝通彼此的想法，是一個培養情感的地方。研究者透過聊天室與家長進行對談，以了解幼兒在家狀況，更可提供家長教養建議，家長也可了解幼兒在校情形，讓幼兒發展更全面。

（3.3） 舉辦活動供家長了解活動狀況

「辦活動」是 FB 的功能之一，在活動頁面內可說明活動時間、地點，並簡介活動內容，透過邀請成員參與，成員可選擇參加、或許及拒絕三個選項，讓邀請人可以大致了解參與情況，以掌握參與人數。研究者是過後發現這個功能在社團內似乎成效不彰，因為只有六位家長點選是否參與，選擇跟老師口頭說明參加意願的人數較多，實際參與人數又是所有告知人數的四倍，故由此可發現，家長還是較習慣用口頭方式進行溝通。

（3.4） 上傳幼兒表演影片供家長欣賞

由於母親節活動時，並非家長休假日，且很多家長未必能請假蒞臨現場，故研究者製作影片上傳，讓未能到場的家長也能看到寶貝們的表演，避免有遺珠之憾；此外，在高峰活動「特別世界」舉辦的前一天，研究者也透過錄影的方式，誠摯地邀請家長參加，讓家長對於活動印象更為深刻，提升活動參加率。

（3.5） 透過「打卡」讓家長了解戶外教學狀況

在這個階段，打卡不只是讓家長了解當季遊玩的去處，更可以讓家長得知幼兒戶外教學狀況，讓家長更加放心。由於在下學期時，研究者曾帶全班幼兒搭乘公車至購物中心參觀，家長在事前曾詢問此次戶外教學相關事項，故透過「打卡」的方式，讓家長清楚知道當下狀況，以避免家長擔憂。

（3.6） 於塗鴉牆上尋求家長協助並感謝其支持

塗鴉牆上除了訊息的提供之外，研究者發現，其實尋找家長協助是一個很適合的地方，由於家長使用 FB 狀況愈來愈頻繁，所以，當研究者發出需求的貼文之後，家長會在留言處回應之外，也會直接到學校詢問相關事宜，讓班上運作更加流暢。除此之外，研究者也會透過 FB，感謝家長對於班上的支持及協助，激勵家長繼續支持班上活動。

花開期與灌溉期最大的不同在於，研究者於此階段大量地使用轉貼的功能，讓家長可以透過別人的照片或貼文更了解班上幼兒的狀況。此外，研究者也活用 FB 的功能選單，像是透過「打卡」功能讓家長了解幼兒戶外教學狀況；運用「辦活動」讓家長了解母親節相關活動；藉由錄影並將影片上傳至社團內，讓家長對幼兒母親節表演活動進行回饋，也讓未參與的家長能夠欣賞，讓家長清楚了解學校課程、幼兒學習及生活狀況，期望家長能多回應社團內的相關事項。在此階段，也能看到家長的回應已經比灌溉期較為頻繁，且按讚人數也變得較多，除此之外，家長也開始主動於社團內詢問相關事項，或製作影片、提供照片供大家欣賞。在在顯示，小鹿斑比社團已漸漸成為一個親師交流的場所。

(4) 結果期

在結果期這個階段，幼兒其實已經畢業了，但研究者仍利用 FB 了解幼兒畢業後的適應。此時期運用了三種 FB 的功能選單，分別為「在塗鴉牆詢問大家近況並抒發感謝之意」、「藉由提問題詢問家長參與活動意願」、「透過標籤期望家長回應留言」。

（4.1） 在塗鴉牆詢問大家近況並抒發感謝之意

畢業過後，研究者藉由貼文詢問大家的近況，透過成員間的回答，以維繫彼此間感情。除了詢問近況之外，也會在塗鴉牆上抒發自己的感謝，讓活動主辦者及參與的伙伴心情愉悅。

（4.2） 藉由提問題詢問家長參與活動意願

研究者藉由「提問題」的功能，詢問家長團聚意願，以及較願意參加的活動類型和較方便的時間，找到較適合社團成員的活動，讓幼兒有再重新相聚的活動。而研究者也可以透過這些活動，與家長及幼兒進行交流，了解幼兒小一的適應狀況。

（4.3） 透過標籤期望家長回應留言

標籤是 FB 的一項特別功能，只要被別人標籤了之後，當使用者打開 FB 時，就會被通知可前往被標籤的頁面之一。故研究者利用「標籤」的功能，期望家長回應研究者的問題，並可瀏覽該頁面的訊

息，以利社團成員內的交流。

結果期與前三期的不同，在於家長主動發言、主動辦活動、主動上傳照片。從幼兒小一編班出爐開始，到中秋烤肉活動，且小靜媽媽也協助銓銓媽媽（化名）設立帳號，並請研究者加入社團當中，不再是由研究者貼文，而是家長主動出擊。另外，研究者也利用一些問題，引導家長留言，並透過標籤的方式，引起家長注意，並回應該則貼文，發現留言的數量也比以往多更多。由此可知，小鹿斑比的祕密花園已成為一個親師交流的場所，也是延續社團成員間彼此情感的好所在。

綜合而言，在四個階段中，研究者運用了 FB 不同的功能選單及策略進行親師交流（見圖 2）。即使是相同的功能選單，應用的方式也有所差異。例如，在「灌溉期」時，是透過塗鴉牆發佈訊息讓家長了解學校班級事務，但在「花開期」時，藉由塗鴉牆提出課程和人員的需求，以利課程進行，最後在「結果期」時，透過塗鴉牆及「標註」功能，詢問畢業後近況，也在塗鴉牆上看到大家不同的問題及回應，除此之外，也運用塗鴉牆感謝各位家長的支持與協助，讓班級運作順利、親師生間繼續進行親密地聯繫。

另外，「打卡」在不同時期也發揮不同功能，例如，在「灌溉期」的打卡，主要是希望提供家長旅遊和美食資訊，鼓勵親子帶孩子出遊增加與孩子相聚的時光；而在「花開期」的打卡為配合戶外教學，讓家長能更了解幼兒的動態，減低家長的疑慮與擔心，也讓家長能和幼兒在家談論戶外教學的狀況。

在研究過程中，經由研究者不斷使用 FB 的功能選單及面對面對談的努力下，除了拉近親師間及家長間的距離，也提升家長參與社團內的對話，發現社團成員的主要照顧者漸漸從旁觀者轉變為主動參與者，讓社團漸漸成為親師交流的另一園地。

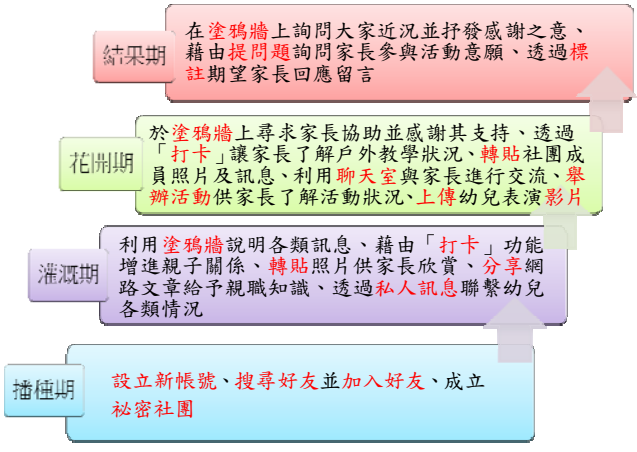


圖 2　各階段運用功能選單

4.2　幼兒教師應用 FB 進行親師交流的困境與因應策略

在研究過程中，共有三種情形較為難解決，分別為「家長因隱私權及不會加入 FB 而未加入社團」、「家長於社團內較少回應」最後為「與協同研究者發佈訊息上的意見相佐」，以下分別說明：

困境 1：因隱私權及不會使用 FB 而未加入社團

因應策略：研究者利用接送時間與家長進行溝通，得知其帳號並加入社團中。另外，對於不會使用 FB 而沒有加入社團的家長，則建議請其熟識的人幫忙設定帳號，並介紹大概的使用方式，家長便可開始使用 FB；此外，對擔憂隱私暴露的家長，則建議家長以幼兒名字設立一個新帳號，以便區隔自己的帳號，不互相干擾，又可以得知社團內的訊息。

困境 2：家長於社團內較少回應

因應策略：研究者發現由於家長之間信任感的不足，家長不太願意回應。家長間熟悉之後，家長漸漸開始在社團中回應，並主動留言及辦活動。除此之外，研究者也透過「腦力激盪」策略及「標籤」功能，讓家長能有更多參與回應的機會。

困境 3：與協同教師發佈訊息上的意見相佐

因應策略：協同教師不願意改變習慣在社團中貼文，還是執意貼文在自己的塗鴉牆上，讓自己的朋友(非家長)看到自己的心情。在無法改變對方的狀況下，研究者獲取同意後以轉貼的方式，分享至社團中，讓社團內的每位成員都看到協同教師在自己塗鴉牆上的分享，也能在社團內留下一份記錄。

4.3　應用 FB 進行親師交流的收穫

在研究過程中除了實際應用 FB 進行親師交流外，研究者發現 FB 可成為一個道新訊息發佈管道，讓家長更清楚學校狀況；其次為 FB 可補足班級網頁發言的功能，讓親師間都有發言權；FB 也讓親師溝通更無距離、更即時；透過 FB 分享幼兒在校表現，獲得家長好評，也能激勵研究者持續交流；透過 FB，家長能更了解研究者，且增進彼此間的關係；最後，FB 也讓研究者能追蹤幼兒幼小銜接的適應狀況，也讓親師生之間的情感可繼續延續下去。

5. 結論與建議

本研究依據研究目的與問題，分別從應用 FB 進行親師交流的歷程、困境及因應策略與研究者應用 FB 進行親師交流得到的收穫，歸納出三項研究結論：

（1）教師必須積極推動提高親師間之信任，才能使家長由旁觀者轉為主動參與者

（2）教師要善用社團、提問、標註與轉貼等功能以有效解決家長被動參與之困境

（3）應用 FB 後讓平時無法接送幼兒的家長能與教師直接溝通

5.1 建議

本研究欲探討幼兒教師如何應用 FB 進行親師交流，透過不同的資料蒐集方式記錄研究歷程，並提出以下建議供現場幼兒老師之參考。

(1) 增進親師信任關係，促進親師交流

由於本研究中社團成員間彼此不熟悉，故需長時間經營下，交流才會開花結果。故建議幼兒教師可以透過班親會及班級家庭旅遊，讓班級家長間產生更濃厚的凝聚力，並培養家長與教師間的信任感，促進親師交流。

(2) 增加自身資訊能力，應用 FB 得心應手

應用 FB 進行親師交流時，研究者發現除了需瞭解並會使用 FB 的功能選單，尚需經常性上傳照片及影片，故幼兒教師需要擁有製作影片及照片的能力。除此之外，幼兒教師也應保護幼兒的肖像權及家長隱私權。因此，建議政府教育單位應為現場幼兒教師辦理資訊教育相關研習，提供攝影技巧、製作影片及網路隱私等相關課程，以建立幼兒教師在職進修的管道。

參考文獻

[1] 楊清貴（2009）。**幼稚園教師使用班級網站進行親師溝通之個案研究**（未出版之碩士論文）。國立台北教育大學，台北市。

[2] Hew, K. F. (2011). Students' and teachers' use of facebook. *Computers in Human Behavior*, *27*, 662-676.

[3] Roblyer, M. D., McDaniel, M., Webb, M., Herman, J., & Witty, J. V. (2010). Findings on Facebook in higher education: A comparison of college faculty andstudent uses and perceptions of social networking sites. *Internet and Higher Education*, *13*, 134-140.

[4] 吳明鴻（2011）。**新北市一所國小高年級學童臉書使用情況之研究**（未出版之碩士論文）。臺北市立教育大學，台北市。

[5] 吳昭瑩（2012）。**Facebook 網路發表作品對五年級學童之英語字彙及閱讀理解成效研究**（未出版之碩士論文）。國立台北教育大學，台北市。

[6] Hayashi, P. (2011). A Learning Success Story Using Facebook. *SiSAL Journal*, *2*(4), 309-316.

[7] Kabilan, M. K., Ahmad, N., & Abidin M. J. Z. (2010). Facebook: An online environment for learning of English in institutions of higher education? Internet and Higher Education, *13*, 179-187.

[8] Haverback, H. R. (2009). Facebook: Uncharted territory in a reading education classroom. *Reading Today*, *27*(2), 34.

[9] 林濂芬（2011）。**合作與遊戲理論在化學課程臉書平台上的應用與研究**（未出版之碩士論文）。靜宜大學，台中市。

[10] 高旻(2009 年 11 月 25 日)。**西澳教師或被禁止用 Facebook 聯繫學生**。取自：http://www.epochtimes.com/b5/9/11/25/n2734058.htm

[11] Berhane, T., & Torey, H. (2011). Student-Teacher Interaction on Facebook: What Students Find Appropriate. *TechTrends*, *55*(3), 19-30.

[12] Decarie, C. (2010). Facebook: Challenges and Opportunities for Business Communications Students. *Business Communication Quarterly*, *74*(4), 449-452.

[13] Muñoz, C. L., & Towner, T. (2009). Opening Facebook: How to Use Facebook in the College Classroom. In I. Gibson et al. (Eds.), *Proceedings of Society for Information Technology & Teacher Education International Conference 2009*, 2623-2627.

[14] Mazer, J. P., Murphy, R. E., & Simonds, C. J. (2007). I'll See You On "Facebook": The Effects of Computer-Mediated Teacher Self-Disclosure on Student Motivation, Affective Learning, and Classroom Climate. *Communication Education*, *56* (1), 1-17.

[15] 東秋瑩（2012）。**幼教教師經營班級網站之信念探究-以新北市公立幼兒園為例**（未出版之碩士論文）。國立台北教育大學，台北市。

[16] 尤蕙茹（2010）。**幼稚園運用部落格進行親師溝通之參與式行動研究**（未出版之碩士論文）。朝陽科技大學，台中市。

[17] 孟憲蓓（2010）。**從部落格探討幼稚園親師溝通之研究**（未出版之碩士論文）。國立臺北教育大學，台北市。

[18] 陳蕙妃（2010）。**私立幼稚園使用電子聯絡簿現況之研究-以新竹縣市為例**（未出版之碩士論文）。朝陽科技大學，台中市。

[19] 郭素文（2004）。**運用班級通訊電子報促進親師溝通**（未出版之碩士論文）。國立台北師範學院，台北市。

[20] O'Reilly, T. (2006). *Web 2.0 principles and best practices*. O'Reilly Media.

[21] Lawrence（2011）。序。載於李芳齡（譯），**Facebook 臉書效應**（第 8 頁）。台北市：天下雜誌。

[22] Facebook（2012b）。**關於 Facebook**。取自：http://newsroom.fb.com/content/default.aspx?NewsAreaId=22

[23] 蔡瑞榮（2002）。疏暢溝通管親師線上三贏。**師說，163,** 5-6。

[24] 張明輝（2002）。 **企業管理理論在學校經營的應用及省思**。取自：http://web.ed.ntnu.edu.tw/~minfei/artical/artical(schooladmin)-20.htm

[25] Tobolka, D. (2006). Connecting Teachers and Parents through the Internet. *TechDirections*, *66* (5), 24-36.

多媒體影音部落格於幼兒教育親師生關係與互動提升之研究

梁佳蓁
臺中市南區國光國小
jen@kkes.tc.edu.tw

吳俊霖
國立中興大學資工系
jlwu@cs.nchu.edu.tw

摘要

多媒體影音部落格有助於幼兒教育親師生關係互動提升。透過多媒體影音部落格，教師能將孩子在學校的學習照片等多媒體影音資料，跨越時空之限制，讓家長在家即能線上觀看並透過班級部落格中相片的呈現或影音欣賞，了解孩子在幼兒園的學習與生活狀況，孩子在學校的學習情形也能藉此做一完整成長記錄。此外，就部落格的特性而言，部落格易於留言、回覆與發表想法的機制，讓班級部落格不僅成為教學的另一種輔助工具，也是促進多方對話、改善師生關係、維繫情誼的另一個空間與管道。就學校而言，部落格不僅能展現學校特色更能突破教室藩籬，讓「教」與「學」在最短的時間內發生。

本研究以臺中市南區國光國小附設幼兒園為例，探討多媒體影音部落格於幼兒教育親師生關係與互動提升之研究，本研究共發出問卷 58 份，回收之有效問卷 52 份，問卷回收率為 90%。在資料分析上，本研究分別使用了統計與類神經網路分群演算法來完成資料探勘，包含有(1)K-means 演算法；還有能將高維資料在保留其拓撲結構條件下降為二維空間的：(2)自我組織映射網路(Self-organizing map)與(3)可視化誘導自組織映射圖(Visualization- induced self-organizing map)。實驗結果顯示，三種方法探勘出共同的發現，家長使用網路經驗是其支持部落格的關鍵因素。有較豐富網路使用經驗的家長，越能藉由班級多媒體影音部落格與老師或其他家長產生互動，進而有效提升幼兒教育親師生關係。本研究顯示多媒體影音部落格於親、師、生的溝通、訊息傳達、學習輔導與親職教育等各種層面提升，皆具有顯著且正面之成效。

關鍵詞：幼兒教育，親師關係，資料探勘，K-Means，自我組織映射網路，可視化誘導自組織映射圖

1. 前言

幼兒教育階段是孩子離開家庭第一個接觸的社會團體。少子化的衝擊與社會結構的改變，為人父母的擔憂與期待也因孩子第一次進入學校這小型社會團體接踵而來。例如：團體規範、同儕生活、課程參與及與師長間的相處等，望子成龍、成鳳的期待，現代家長掌握住陪伴孩子成長的機會。

1990 年台灣學術網路（TANet）成立，開啟資訊網路教育蓬勃發展先機，利用資訊科技提升教育品質，不僅支援全國各級學校及研究機構之教學研究活動，並促進資源分享與合作交流等廣泛用途。邇來，教師資訊素養與能力的提昇，隨著網路文化的普及性、校園網路之建置完成，班級部落格改變傳統的班級經營型態成為教室的延伸。資訊科技不僅帶來教學的新契機，也正改寫傳統教學模式與學習經驗[1]。如今親師生可跨越時空，進行資訊交流、教學分享，形成處處皆教室、時時可溝通。家長亦可以透過班級部落格瞭解孩子在校生活點滴及各項學習，達到親師生三贏局面。

基於上述研究背景與動機，本研究之研究目的如下：

一、多媒體影音部落格進行親師生關係與互動提升的是否具有正面成效。

二、分析多媒體影音部落格協助親師互動的實施歷程中，所遭遇到的困難。

三、研究者在研究歷程中，對本研究的省思與專業成長。

2. 文獻探討

此節我們簡單回顧幼兒教育，親師關係與多媒體部落格的影響力。

2.1 幼兒教育（Preschool Education）

依據幼兒教育及照顧法，幼兒係指二歲以上至入國民小學前之幼兒。2012 年 1 月 1 日起幼托整合正式實施，幼稚園及托兒所改制為幼兒園。將原本兩者之主管權責分別隸屬教育及社政體系整合資源並改進現況。自此，2 歲至入國民小學前幼兒，由教育部負責監督管理，無論在收托機構名稱、主管機關及教保服務品質均齊一。

教育是奠定國家發展的基石，幼兒教育係國家存續發展的基礎教育，許多國家已將之列為義務教育。繼聯合國 1959 年訂定的「兒童權利宣言」之後，世界各國也陸續倡導兒童福利和教育均等觀點。例如，1965 年美國提倡的「啟蒙教育方案（The Head Start Program）」對幼兒教育提供大量補助經費；英國 1967 年頒訂「普勞登報告書（The Plowden Report）」擴充學前幼教；蘇聯 1968 年的幼教經費約占教育經費的 40%；日本 1971 年提出 4、5 歲的幼兒與低年級兒童在同一教育機構接受教育；台灣 1973 年公布「兒童福利法」[2]等。2010 年教育部推動「5 歲幼兒免學費教育計畫」，此外，對於弱勢家庭因貧窮而無法接受教育的幼兒，政府也提出相關政策與方案彌補，這些政策的修訂與推動，除普

及幼兒受教育機會，促進教育機會均等外並致力提升幼兒成就品質。由此可知，幼兒教育是一切教育之基石，普及幼兒教育、積極推展幼兒教育已成為國際上共同發展與關注的目標。

2.2 親師關係（Parent-Teacher Relationship）

新時代教育情境的親師關係，因社會變遷、教育改革、少子化浪潮，其教育模式、師生互動有著唯妙的變化。家庭本位(family-centered approach)的教育觀漸進融入了時代教育趨勢，幼兒教育必須要透過家庭才能滿足孩子的需求，也就是說老師如果想真正有效地滿足幼兒發展和學習上的各項需要，就必須與家長建立良性的互動與合作關係[3]。家長是教育的合夥人，父母和老師是船的左右兩個舵手，親師間良好的互動與溝通，不僅有助於幼兒在校的學習生活適應，也能協助孩子課業的學習和行為常規的養成。學齡前幼兒，其生活自理能力較弱，親師間需要配合的部分更多，雙方如果能建立良好的關係，彼此合作無間，對孩子的發展與學習才能產生正面的影響[4]。

根據 Bronfenbrenner 的生態系統理論，如圖 1 所示，家庭、父母與學校、老師都是影響幼兒發展的微系統(microsystem)，對幼兒的發展具有直接的影響力，當幼兒進到幼兒園學習這小型社會即是生態理論的中間系統[5]。家庭、幼兒園這兩股重要力量則是影響幼兒初期社會化的重要關鍵。美國國務卿希拉蕊也指出「培育一個小孩，需要一個村莊的力量」(It takes avillage to raise a child)。由此，良好的親師關係，不僅可以提昇幼兒學習成就、塑造正面且積極的行為與態度，更能幫助家長追求並掌握更多教育成長的資訊；對於學校而言，良好的親師關係有助於教師掌握更豐富的教學資源巧妙藉助親師間之資源整合為自己的教學加分、讓教學方案更形多元。綜上，突顯了親師雙方建立良好關係的必然性與必要性。

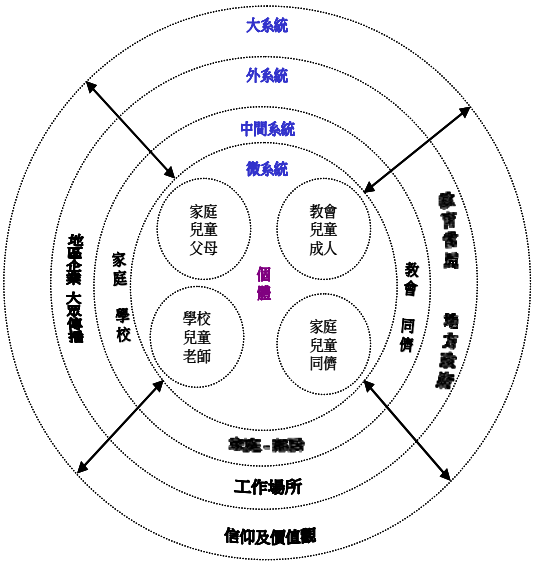


圖 1 Bronfenbrenner 的「生態系統圖」

2.3 多媒體部落格 (Multimedia Blog)

二十一世紀是高度資訊化時代，部落格的迅速竄起與 Web2.0 結合之後，更成為校園不可或缺的一員。知名的部落格搜尋引擎 Technorati 於 2009 年最新公布資料，全球部落格數量已超過一億三千三百萬。部落格之所以能引領風潮，主要歸因於便利性及互動性基於「書寫方便」、「社交互動」與「串聯傳佈」的特性 [6]。因部落格之操作容易，方便使用者可快速更新與維護，表達個人的經驗和想法，題材、版面、寫作風格均能依照時間順序及個人風格自由使用。此外，它更具備即時性、便利性與穿越時空互動之廣泛功能。Blood 曾在〈部落格: 一個歷史與觀點〉一文中提到，部落格具有共享性、個人敘事性的互動媒體與寬容性[7]。

就幼兒教育階段，學齡前幼兒其表達能力較薄弱對於學校訊息較無法完整傳遞，因此，教師主動促進親師關係更有其迫切性的需求。然親師溝通有許多管道，包括面對面談話、電話聯繫、聯絡簿、便條紙、通知單、親師座談會等等，方式雖多元，但仍有其優缺點。班級部落格可超越時空條件的限制，提供線上留言與回應的功能。在部落格介面中，有建置者的首頁、相簿、網誌、最新消息、留言、影音、相關連結..等等的內容，教師可以將想說的話、想做的事、課程紀錄之照片及錄影、參訪者的留言及回應等一一呈現在家長面前。幼兒教育的課程設計以幼兒為中心，並無固定的教材，資訊科技其實可以更靈活的用用融入幼兒園的主題教學中[8]。教師可以將幼童的上課情形、活動內容、課程內涵、幼兒行為表現，透過照片、影音以部落格為媒介傳遞訊息讓家長知道，建構教室以外的知識交流成為親師生交流。教師有效地規劃及運用部落格，無論是在班級經營、課程與教學或教師專業成長上，都有不容忽視的效果。是故，多媒體影音部落格與教育的結合是不可避免的趨勢。

3. 研究方法

本論文以資料探勘方法來挖掘出問卷調查的果，我們使用了三種方法，首先是基於統計的 K-means 分群演算法，接著我們使用非監督型(Unsupervised)類神經網路中的自我組織映射網路(SOM)與可視化誘導自組織映射圖(ViSOM)，這兩種網路能有效將高維度的資料，在保留其樣本之間的距離關係與拓撲結構下，降到二維平面，以利分群動作與檢視。

3.1 K-means 分群演算法

K-means 演算法基本上是以群聚的概念來對數據進行分類，從給定的數據集合中尋找同類的數據子集合，每一個子集合形成一個類別，使得同類別中的數據具有更高的相似性[9]，簡言之就是經過 K-means 演算法分群後的資料，每一群的資料具有高度相似性特徵。

假設我們有 N 筆資料欲分出 K 的類別，則

K-means 演算法的步驟如下：

(1)隨機指派初始群中心：在資料中隨機找出 K 筆資料作為初始的群中心。

(2)產生初始群集：計算資料集中每筆資料到各個隨機群中心的距離，比較該筆資料離哪一個群中心距離最近，則該筆資料會被指派到最近的群中心，依此產生初始群集。

(3)產生新的群集中心：

依據初始群集，我們可以計算該群集內資料的平均值，求得新的群集中心取代先前的初始群中心。

(4)進行分群動作：取得新的群中心後，藉由比較每一筆資料與新的群集中心之間的距離，然後根據最短歐式距離，重新分配每一個資料所屬的群集。

(5)反覆步驟 3、4，直到求出的 K 個類別群中心不再變動為止。

3.2 自我組織映射網路 (SOM)

SOM 是一種非監督式演算法，屬於類神經網路的一類。其概念來自人類大腦網路或生物網路在處理資訊時，處理相同資訊的神經元會聚集在一起的特性。此外，SOM 也是一種競爭式學習的網路，其架構圖如圖 2 所示，輸出層的每個神經元與輸入層的神經元皆有連結[10, 11]。

SOM 的最大用處是將高維的輸入資料映射至一維或二維的空間上，並且把有原本的拓樸關係與結構維持住，即用視覺化的低維度空間來表示原本高維度空間的資料，因為在低維度的空間上比較容易做觀察與分析。

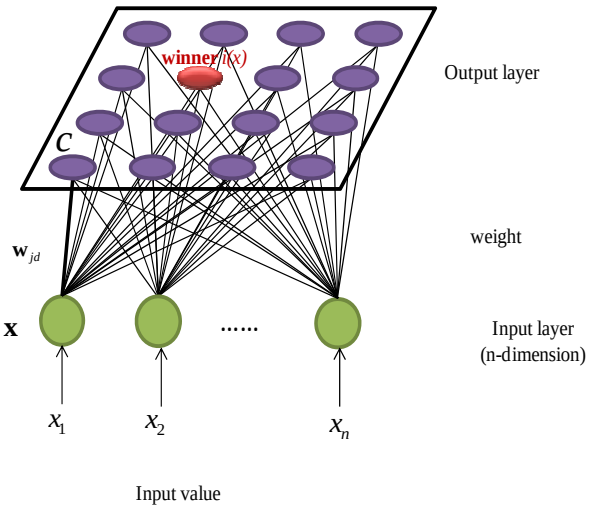


圖 2 自我組織映射網路架構圖

自我組織映射網路與一般競爭式學習的類神經網路不一樣。一般競爭式學習的類神經網路是採用贏者通吃(Winner take all)，而 SOM 除了贏家可以學習之外，它周圍的神經元也可以學習，更新其權重，如圖 3 所示。

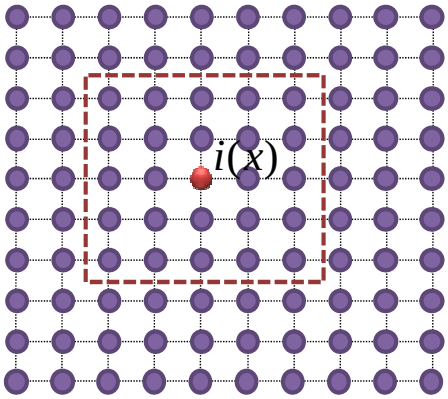


圖 3 贏者神經元與其周遭神經元才能更改其權重

自我組織映射網路演算法如下[10, 11]：

(1) 從輸入的資料集中挑選一個樣本(Pattern) x 到輸入層神經元。

(2)尋找與輸入樣本差距最小的神經元權重值，該神經元即為 Winner，如式(1)所示。

$$i(x) = \arg\min_j \|x - w_j\|, \ j = 1,...,n \qquad (1)$$

(3)更新 Winner 神經元及其鄰近神經元的權重，如式(2)所示。

$$w_j(t+1) = w(t) + \eta(t)\Lambda(i,j,t) \cdot \left([x(t) - w_i(t)] + [w_i(t) - w_j(t)] \frac{(D_{ij} - \Delta_{ij}\lambda)}{\Delta_{ij}\lambda} \right) \qquad (2)$$

其中 Δ_{ij} 代表神經元 j 與贏者神經元在原始資料空間的距離，$\eta(t)$ 是在時間 t 的學習速率。

(4) 隨著疊代次數的增多，學習速率 $\eta(t)$ 與贏者神經元的鄰居(Neighborhood)範圍會慢慢減小，進入收斂階段。

3.3 可視化誘導自組織映射圖 (ViSOM)

為了改進自我組織映射網路的可視性，有學者 Yin 提出了可視化誘導自組織映射圖[12]。相較為標準的自我組織映射網路，其更能在低維度的映射圖上，保留資料樣本間的拓樸結構與資料結構。

圖 4 所示為 ViSOM 神經元更新力(Updating force 的分解示意圖，參數 λ 控制了原始空間(Original space)的資料距離與投影後特徵空間映射圖(Feature map)的距離比值。較小的 λ 值，其特徵空間映射圖則提供較高的資料解析力。

ViSOM 演算法的學習方法與傳統的 SOM 相似，ViSOM 會在神經元的權重不再改變時才停止，如此一來，高維度的資料點便能在保留其相對位置結構的條件下，投影到二維平面。

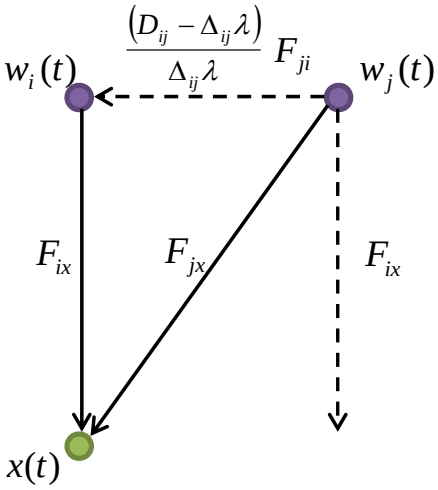


圖 4 ViSOM 神經元更新力(updating force)的分解示意圖

4. 實驗結果

本研究以臺中市南區國光國小附設幼兒園花鹿班 58 位家長為研究對象，探討教師使用班級部落格來進行師生互動之實施成效。幼兒園班級多媒體部落格的部分內容如圖 5 所示，透過部落格，教師能將孩子在學校的學習照片等多媒體影音資料，跨越時空之限制，讓家長在家即能線上觀看與瞭解。藉由部落格的留言與回覆機制，提供親師溝通的另一個管道。能將孩子一路上的學習情形與進步做一完整記錄。



(a)



(b)



(c)



(d)

圖 5 幼兒園班級多媒體部落格

問卷設計前 11 題為家長的背景與其使用網路的習慣，後面 20 題為關於班級多媒體部落格的使用情形與對親師關係的影響。本研究共發出問卷 58 份，回收之有效問卷 52 份，問卷回收率為 90%。

在資料分析部分，我們把每一張問券當成是一筆 31 維的資料，共有 52 筆資料，接著以三種不同的分群演算法來分析，而數量最多的那一群的群中心即為所探勘出來的代表資料。

在 K-means 部分，我們發現設定分群數 K=3 時的結果最好，疊代次數為 29 次，而最大群的樣本個數為 30。

在自我組織映射網路部分，我們設定輸出層的神經元個數為 10x10，使用所有 52 筆資料進行神經網路的訓練，其二維映射輸出結果如圖 6 所示，我們以右上角紅圈所示那一群為代表群。

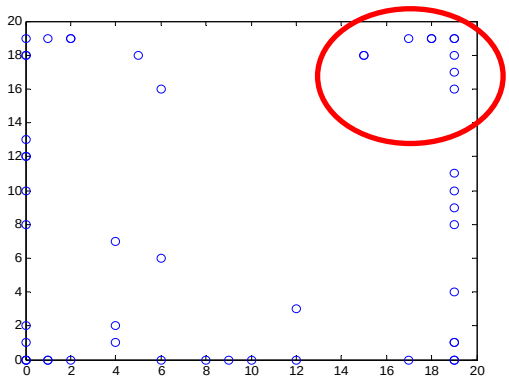


圖 6 自我組織映射網路的映射結果

最後在可視化誘導自組織映射圖方面，我們同樣設定輸出層的神經元個數為 10x10，也使用所有 52 筆資料進行神經網路的訓練，參數 λ 值設為 0.5，其映射結果如圖 7 所示，我們選定以右上角紅圈所示那一群為代表群。

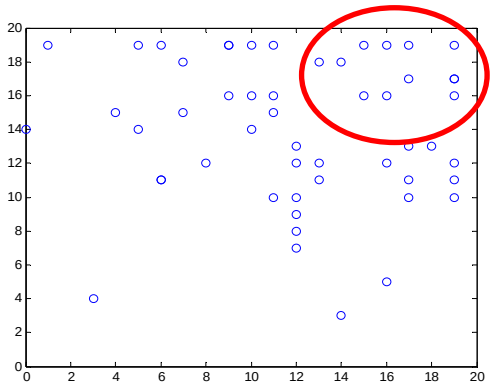


圖 7 可視化誘導自組織映射圖的映射結果

由以上的實驗結果發現，三個分群演算法挖掘得到近乎相同的規則：家長本身使用網路經驗是其是否支持部落格的關鍵因素，本身的網路使用經驗越豐富者，越常觀看幼兒園班級多媒體部落格且有所回應，也越能得到部落格所帶來的好處，包含能瞭解孩子在學校的生活與學習情形，與其他家長的交流，進而有效提升幼兒教育親師生關係等。實驗結果也顯示，多媒體影音部落格在親、師、生的溝通、訊息傳達、學習輔導與親職教育的提升，皆具有顯著之正面成效。我們也發現幼兒園使用網路經驗較為豐富的家長背景為女性，年齡介於 31 -40，專科學歷，經常上網地點是家庭，一星期瀏覽次數為 1~2 次，每次時間 30 分至 1 小時。其它發現，少部分家長較少瀏覽班級部落格，瀏覽時間不長，也沒有回應文章的習慣。其主要原因，家長不知道要寫什麼，加上智慧型手機上市，家長使用 iPAD 等平板或智慧型手機上網頻率提高了，但也因其讀取網頁的速度及打字較慢，基於保守習慣仍習慣上網瀏覽孩子的活動照片不習慣上網回應或留言。

5. 結論與建議

本研究以臺中市南區國光國小附設幼兒園為例，探討了多媒體影音部落格在幼兒教育中，親師生關係提升之研究，我們分別使用了統計與類神經網路分群演算法來完成資料探勘，包含有(1)K-means 演算法；(2)自我組織映射網路與(3)可視化誘導自組織映射圖。實驗結果顯示，三種方法探勘出共同的發現，家長使用網路經驗是其支持部落格的關鍵因素。本論文的研究發現包含有：

(1)實驗結果發現，利用多媒體影音部落格進行親師溝通之方式為家長所接受與認同，多媒體影音部落格確實能有效提升親師生關係與促進親師之對話與溝通。

(2)教師可在學期初先行瞭解家長使用電腦狀況及其資訊能力，包括家長使用部落格在操作技術及應用上的困擾。

(3)適時了解家長對多媒體影音部落格的期望與看法，並將部落格更新的訊息隨時以面對面溝通或聯絡簿的方式告知家長，邀請家長上網瀏覽。如此，更可隨時掌握家長上網情形與其保持密切互動。

(4)對於新移民家庭在語言文字上產生困擾等問題，可透過班級家長間的相互支援提供其協助。

(5)就教師專業發展而言，透過多媒體影音部落格教師能有效歸類整理各項學習活動，使多媒體影音部落格成為一個教學資料庫，透過教學互動更能增進教師專業成長。

(6)研究者認為班級多媒體影音部落格持續經營的動力主要來自於教師對教學工作的熱情與活力，而這熱情與活力之主要來源則是家長及同儕的認可與支持，例如：部落格的留言與回應及家長上網瀏覽的次數都是激勵教師是否繼續經營班級部落格的動力來源，有了這些催化劑，教師也就會積極並努力克服班級部落格在經營過程中所遇到的各種阻礙與難題。

參考文獻

[1] 戴翠華、張靜儀，資訊科技融入與社會建構應用於自然與生活科技教學之研究。教育資料與研究雙月刊，641，pp.110-118，2005。

[2] 吳榕椒、郭諭樺、廖又儀、王芳如、丁姿伶，幼兒教育概論。台北：華都文化，2008。

[3] G. S. Morrison, Early childhood education today (9th ed.). Upper Saddle River, NJ:Pearson Prentice Hall, 2004.

[4] S. Wilford, The role of families in your program. Scholastic Early Childhood Today, *19*(1), 18-19, 2004.

[5] U. Bronfenbrenner,.The Ecology of Human Development. Cambridge, MA: Harvard University Press, 1979.

[6] 李家菁，部落格可以幫教師什麼忙。師友，471，pp.19-22，2006。

[7] R. Blood, The Weblog Handbook: Practical Advice on Creating and Maintaining Your Blog. Cambridge, MA: Perseus Publishing, 2002.

[8] 邱淑惠，讓孩子製作電子書-探討幼稚園教師在提供鷹架時所面臨的困難。教學科技與媒體，85，pp. 53-66，2008。

[9] P. E. Hart, D. G. Stock and R. O. Duda, Pattern Classification, 2nd edition, Hoboken: NJ: Wiley, 2001.

[10] T. Kohonen, “The Self-Organizing Map,” in Proceedings of the IEEE, Vol.78, No.9, pp.1464-1480, Sep 1990.

[11] T. Kohonen., “The Self-Organizing Maps,” 3rd edition, Berlin, Springer, 2001.

[12] H. Yin, “ViSOM-a novel method for multivariate data projection and structure visualization,” IEEE Transactions on Neural Networks, Vol. 13, No. 1, pp. 237-243, January 2002.

亞洲大學協同合作辦公室建置經驗

潘信宏　陳家妍　陳柏凌　鍾仁宗　劉嘉政
亞洲大學資訊發展處
vincentpan@asia.edu.tw, shane@asia.edu.tw , chenbl@asia.edu.tw
jtchung@asia.edu.tw, jzliu@asia.edu.tw

摘要

綜觀國內各大專院校校內數位作業環境，多數院校的 IT 應用環境多以提供檔案分享及電子郵件作業為主，總體功能並未完備，兼之校內數位作業環境多由多個系統總合而成，而系統之間常各自獨立不整合，導致作業環境中人工及紙本作業比例居高不下；此外，部份院校工作生態使然，往往造成行政經驗與實務的累積皆集中於少數個人身上，一旦新血加入或職務異動，便須倚靠單位主管被動提醒工作及跟催進度。亞洲大學創校至今僅十三年時間，在國內堪稱年輕院校，但校方高層有感於校務自動化及 IT 應用環境的重要性，因此，於三年前便開始針對協同合作議題積極尋找並導入適當平台，本文即為亞洲大學導入 SharePoint 協同合作平台的規劃、建置，及應用之實務經驗分享，期望本文能提供國內各大專院校作為評估導入協同合作平台時的參考。

關鍵詞：辦公室自動化，協同作業，亞洲大學。

Abstract

As a general model for delivering Information Technology (IT) services, cloud computing has broad applicability for adopters with diverse needs. In Taiwan, cloud service for campus is a popular issue for now-a-day digital environments. However, most of colleges and universities provide only files sharing (FTP, Samba, etc.) and/or electronic mail (e-Mail) services. Some of these campus systems are combined by many isolated sub-systems. Moreover, the human operation and paper working rates are still high in those systems caused by poor integration. In some case, changes of human resources in aforementioned systems will seriously damage the system's day-by-day operations. Those systems are neither completed nor integrated cloud services. Asia University, our school, found in 1999, is a young school in Taiwan academic community. The university leadership believes that it is important to provide a complete IT environment, so three years ago, we started our survey and looking for a collaborative platform. This paper is a sharing of our experience in importing SharePoint collaboration platform. We wish this article could be a reference for other colleges and universities.

Keywords: Office Automation, Collaboration, Asia University.

1. 前言

近年來，企業在面臨經濟環境的快速轉變及全球企業的競爭下，為了強化企業體質投入多方面的努力，而「自動化」便是其中極為重要的一項重點。

「自動化」這個名詞最早出現在 1948 年[2]，起源與作業電腦化有直接關聯，加之政府方面也非常積極推動各類自動化，例如農業自動化、工業自動化、商業自動化，及生產自動化等等。1990 年代辦公室、電腦、通訊技術及消費者電子產品工具相互結合，帶動了「辦公室自動化」(Office Automation; OA)一波熱潮，亦被視為提升企業經營效率的一項措施。辦公室自動化包含了一些系統與科技，用以協助辦公室人員在商業環境中完成他們的業務。意即辦公室的人員與資訊等主要成員，透過辦公室應用軟體讓業務人員能夠更有效率的處理資訊。以辦公室自動化演進的過程來加以區分，概略可劃分為三階段：1. 作業設備之自動化；2. 作業流程之自動化；3. 辦公室管理之自動化。

辦公室自動化技術上的層面主要注重於儀器設備及相關程序上的使用。這些辦公室系統包含電腦、印表機、掃瞄器、影印機、傳真設備、電子郵件、語音信箱系統，及內部網路等現代化機器等設備。利用以上這些系統及技術，以支援大多數辦公室的活動，如資料處理、文書處理、簡報圖表、電子檔案，及個人試算等等。應用範圍亦包含電子郵遞、桌上排版文件處理、傳真、電子行事曆、音訊會議，及視訊會議等。也就是說，利用新的電腦科技、通訊網路、結合系統科學、人因工程等新的科技與知識，來協助各式辦公室的作業，以提高作業效率，提高作業品質，並降低作業成本。

辦公室自動化目標之一為無紙化作業環境，依維基百科對「辦公室自動化控制」之「主條目：無紙化」，界定為：「利用軟體程式技術及應用，將辦公室的文書資料或文書檔案，做有效率的管理，並結合傳真機、電話機、影印機、電腦等迅速地處理文書資料或文書檔案，以提供承辦人或決策主管參考。」[7]不僅要藉由辦公室作業流程合理化、推動自動化，以提昇辦公室內工作人員的效率，更重要的是透過辦公室自動化系統，在現有的人力之下提

供辦公人員更有用的業務資訊，以有效應用這些資訊處理正確的管理決策。經由通訊網路來共享辦公室設備、與公司內部與外部的成員或往來的客戶與廠商進行資訊溝通。

目前，多數大專院校的 IT 應用環境皆是以提供檔案分享及電子郵件作業為主，總體功能並不完備，再加上校內各系統之間經常各自獨立未進行整合，導致作業環境中人工及紙本作業比例居高不下。連帶地，部份院校工作生態使然，行政經驗與實務的累積往往都集中在少數個人身上，一旦有新進人員加入或職務異動，就必須倚靠主管被動提醒工作項目或跟催工作進度。

亞洲大學創校至今僅 13 年時間，在國內教育環境中尚屬年輕院校，但校方高層有感於校務自動化及 IT 應用環境的重要性，因此，於三年前便開始針對協同合作議題積極尋找並導入適當的平台，本文即為亞洲大學導入 SharePoint 協同合作平台的規劃、建置，及應用之實務經驗分享，期望本文能提供國內各大專院校作為評估即導入協同合作平台時的參考。

2. 文獻探討

以下針對辦公室自動化演進、協同合作平台以及整合通訊平台三者進行探討。

2.1 辦公室自動化的演進

辦公室自動化的演進過程，在過去的二、三十年間變化甚巨，在本節中將對其演進過程做一介紹，首先介紹傳統的辦公室簡單機器設備的應用，再來討論第一代的自動化-電腦的應用，最後，介紹第二代自動化-通訊網路的加入而邁向國際化，這些過程基本上可視為由點至線至面的自動化過程。

(1)傳統式的辦公室

又稱為第零代自動化辦公室，其主要的功能是將一些單純的業務由辦公室機器來處理，例如計算機、打字機、影印等。在本階段只能算是機器化，所提供之功能為針對某項業務的更快處理方式，並非全面性規劃下所產生的系統，所以嚴格說起來頂多是半自動化。

(2)第一代自動化--電腦化

隨著作業的需要，辦公室中資源共用的網路設備演變成以通訊為主的網路系統，且在辦公室自動化的過程扮演了非常重要的角色。早期的網路應用大多是在企業內部一小塊區域內的區域網路(Local Area Network, LAN)，頂多配合租用專線將不同的區域網路連結。自從九０年代初期，網際網路商用化了之後，低成本、跨平台、隨時隨地存取、開放式系統架構等特性，使得目前幾乎所有的企業將網際網路視為必備的辦公室工具之一。

(3)第二代自動化--國際化

國際化的辦公室自動化系統是藉著網路通訊技術的發展而產生的，其中包括了通訊技術、資料傳送、與網路架構系統的發展等[10]。在此之前的辦公室自動化只為一企業內部的封閉式自動化，就算一資訊系統的設立亦只為部門間資料的處理及轉換。在國際化的階段，辦公室自動化的目標放在與其他企業間資訊的傳遞。而使國際間的文件及訊息溝通就好像在企業內部一樣。

辦公室自動化系統 OAS（office automation system）即是運用電腦及通訊科技來協助辦公室作業，提升辦公室人員工作的品質、效率及生產力。所需的技術如文件管理技術：包括文書處理、桌上排版系統等。通訊技術：如區域網路、傳真機、整合語音資料交換系統。辦公室排程技術：個人、團體的會議、活動的排程工具，如電子日曆、關鍵路徑法 CPM 及計劃評核術 PERT 等。資料管理技術：資料庫軟體發展的辦公室資料管理軟體。群體軟體 groupware：協助團體提升討論、溝通、協調、決策、執行等活動的品質，有效率的達成共同目標等。

2.2 協同合作平台

協同合作平台可透過即時、群組分享的平台，提供群組成員共享資訊，簡化溝通時間、促進成員間的知識分享與腦力激盪，激發新的思維與解決方案，更快速、更有效地完成工作。協同合作平台，或稱群組軟體（Collaborative Software，或 GroupWare），係幫助群組使用者間相互通訊與協調活動的軟體，有助於組織辦公自動化系統整合，協同辦公軟體眾多，微軟的 SharePoint 2010（以下簡稱 SP2010）即為目前市場上的後起之秀。

SP2010 是繼 Windows SharePoint Service 3.0（WSS 3.0）之後，另外一個功能更加強大的網頁平台軟體[8]。透過 SP2010 可以快速的建置出支援 AJAX 技術的 Web 2.0 網頁，而在這個平台上可以允許管理者與使用者自行編修網站的內容，新的介面引進了 Office 的新版 Ribbon 功能表介面，讓 Web 的操作經驗和操作 Office 一樣容易、有效率，透過這個功能表介面，使用者可以如同在使用 Office 一樣的操控 SharePoint 網站。另外，在 SP2010 中也大量使用 AJAX 技術，許多的動作都可以在不需要切換網頁的狀況下，以對話方塊的方式來操作完成，例如新增、修改、刪除資料。

SP 2010 是新一代企業網站及協同合作平台，讓企業透過整合的豐富功能，提升企業效能。如圖 1 所示，目前的 SP2010 共包含『網站』、『社群』、『內容』、『搜尋』、『洞悉』及『綜合』六大功能[4]。



圖 1　Sharepoint2010 功能示意圖。

(1) 網站：

- Multi-tenancy（多租戶）：單一主機，服務不同客戶，適合做雲端架構的部署。
- Sandbox（沙箱式開發）：提供獨立的應用程式環境進行開發、測試和訓練，支援

大型企業的 IT 需求。

- Shared Service Applications（共享服務應用程式）
- Secure Store Service（安全儲存服務）：全新的服務，用最安全地方式來儲存帳號及密碼，達到 Single Sign On 的功能。
- Web Analytics（網站分析）：提供者更詳細的趨勢分析，提前規劃 Server 資源，有效增進 Server Forms 效能。

(2) 社群：

- 企業 Wikis：容易使用及管理的 Wikis 功能，集中整合企業的重要資訊。
- Tag（標簽）：Tag Clouds，Tag Profiles，Tag 及 Notes 工具，有效分類並組織資訊。
- Rating 評分：可以對 SharePoint 的網頁，清單，文件庫，文件給 1－5 顆星的評分，更容易找出有價值的資料。
- Organization Browser（組織瀏覽器）：以視覺化的方式瀏覽組織架構，更進一步了解同事，老闆在組織中的關係，事半功倍。

(3) 內容：

- Metadata（中繼資料）的建立與管理：還可以 Metadata-driven 的方式導覽內容。
- Shared Content Types：集中定義及管理 Content Types，讓它們可以跨 Server Farms 及

Site Collections，使用及管理都更方便。

- Document Sets：以單一物件的方式來管理關聯的內容，例如專案相關文件，可以一

次建立所有相關文件並一起設定屬性。

- Rich Media Management（多媒體管理）：針對多媒體內容的管理，如 Audio 及 Video。

(4) 搜尋：

- 自動分類：讓使用者更快找到想要的文件及資料。
- 排序：依照日期或標題排序。
- 預覽：可以預覽文件內容，更有效找到正確文件。
- Federation Search（聯邦搜尋）：可以結合其它搜尋引擎的結果，如 Yahoo，Bing 等。
- Advanced Content Processing（進階的內容處理）
- Business Intelligence Indexing Connector（商業智慧索引連結器）：可以全文檢索 BI 資料，如 Excel，Reporting Services。

(5) 洞悉（商業智慧）：

- KPI 企業計分卡
- 圖表 Web Parts
- Dashboards 數位儀表板
- Excel Services
- PowerPivot for SharePoint
- PerformancePoint Services
- Visio Services

(6) 綜合：

- InfoPath Form Services 表單服務：提供所見即所得的表單編輯功能。
- Access Services: 直接將 Access 資料庫發佈到 SharePoint，變成 Web 資料庫應用程式。
- Business Data Integration with the Office Client: 以使用者熟悉的工具，如 Outlook，Word 直接整合後端資料。
- Business Data Web Parts：用 Web Part 整合 LOB 系統建立商務應用程式。

而目前 SP2010 共分為下列四個版本[5]：

(1) SharePoint Server 2010 企業版客戶端存取許可功能：適用於期望擴充功能業務協作平台以便支援高階方案的組織。利用 SharePoint 的企業版功能充分與業務範圍之外的應用程式、Web 服務以及 Microsoft Office 客戶端應用程式進行相互協作；藉助豐富的視覺化資料、儀表板以及高階分析功能作出更加明智的決策；構建穩定的形式和以工作流為基礎的解決方案。

(2) SharePoint Server 2010 for Internet Sites（企業版）：適用於期望利用 SharePoint 的全部企業功能來建立面向客戶的公共網站以及專用外聯網的組織。此版本能夠提供 SharePoint Enterprise 的全部功能，不受任何技術限制。

(3) SharePoint Server 2010 標準版客戶端存取許可功能：適用於期望部署覆蓋各種內容的業務協作平台的組織。使用 SharePoint 的核心功能來管理內容和業務流程，尋找和分享訊息和

專業經驗，並簡化不同組織中人員的協作方式。

(4) SharePoint Server 2010 for Internet Sites（標準版）：適用於期望利用 SharePoint Server 2010 標準版功能來建立公共 Internet 網站以及基本外聯網的中小型組織。

2.3 整合通訊平台

由於企業內部的溝通與協同合作的重要性正不斷提升，傳統上企業組織都是利用電子郵件、電話、語音郵件、即時訊息、電話會議以及視訊會議等方式進行溝通。而因為每一種通訊溝通方式都各自採用不同的平台，以致企業用戶必須依聯絡對象或目的分別使用不同的基礎設備，在設備的更換或建置上還得再花一筆費用。此外，各類通訊平台的使用者識別架構、用戶端管理工具和資訊安全管理系統也都各不相同，可能會造成企業成本負擔加重，影響管理效率。而要使用不同的通訊平台，就必須分別輸入帳號與密碼，這對使用者而言相當不便，也將使生產力下滑。

針對上述面臨的這些問題，Microsoft Lync(以下簡稱 Lync) 提供了一個整合的通訊平台，功能包括使用者狀態資訊、即時訊息 (IM)、語音通話、Lync 會議 (視訊會議) 等等[6]。同時，Lync 可聯繫各處 Windows 8 和其他裝置的使用者，不論在公司內外的任何地點、場合，使用者都能以適當的通訊方式進行溝通。透過這個整合通訊平台，企業就能大幅簡化身分識別、工具與資訊安全等管理作業，可有效降低營運與管理成本。而企業進行 Lync 部署時，可依各種需求選擇要內部部署或利用雲端服務來部署；您也可以採取混合部署的方式，以最佳化的組態提高生產力與成本效率。

3. 協同合作平台之規劃及建置

目前，多數大學院校的 IT 應用環境是以公文系統和電子郵件為主，功能本就不夠完備，再加上系統之間各自獨立不整合，導致人工及紙本作業比例居高不下。連帶地，行政經驗與實務的累積往往都集中在個人身上，一旦有新進人員或職務異動，就必須靠主管去提醒工作、跟催進度。

再者，近年來各大學院校的人事都愈來愈精簡，尤其亞洲大學的人事精簡度幾乎位居全國院校之冠，換言之，一旦助理離職或異動，相關的行政實務就可能隨之流失，因此，想要傳承經驗就只能靠系統，必須重新打造以 IT 為中心的作業模式。

有鑑於上述問題及辦公室自動化及協同合作的重要性， 亞洲大學自 2009 年起即著手評估適合的協同合作平台，而預期此平台需具備檔案共享、權限控管、線上存取、可客製開發、建置成本低…等優點，期初目標除建置校內各行政及教學單位之共同平台、提高同仁間的行政工作效率外，亦期望能將個人本身所處理業務之相關檔案集中放置，將來若是離職，曾經手的相關資料亦能延續使用或是供其他單位搜尋利用。經多番比較後，選定當時發展已趨成熟的 SharePoint 平台，原因有三：(1)SharePoint 具備辦公室自動化需求的各項功能；(2)國內大專院校辦公軟體多數為微軟校園授權系列，Office 與 SharePoint 可作更密切的整合；(3)SharePoint 為微軟公司研發產品，國內外已有許多成功應用實例，可獲得較完整之技術諮詢服務。

現階段亞洲大學所用 SharePoint 為 2010 企業版，建置在由 Hyper-V 所管理的兩部虛擬主機上，一部為提供使用者及管理者使用的應用程式伺服器，另一則為資料庫伺服器，相關規格如表 1 所示。

表 1 亞洲大學 SharePoint 平台虛擬主機規格

	應用程式伺服器	資料庫伺服器
中央處理器	AMD 2.4GHz 4 cores	AMD 2.2GHz 4 cores
記憶體容量	8 GB	8GB
儲存空間容量	OS: 100GB Data:100GB	OS:100GB Data: 1,140GB

而權限控管上則與校內 Active Directory 機制(簡稱 AD)進行整合控管，整體協作平台架構如圖 2 所示。

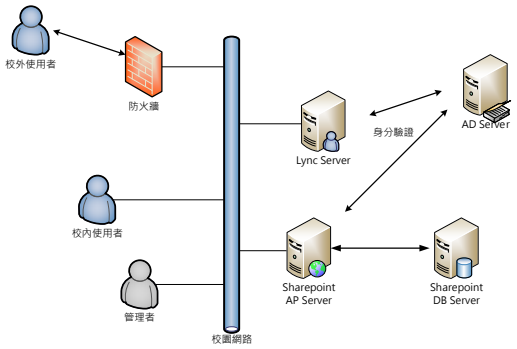


圖 2 亞洲大學協作平台架構圖

延續協同合作平台的建置，亞洲大學亦發現到整合通訊平台是推行辦公室自動化不可或缺的一環，在考量建置成本及使用便利性等種種因素，接著便導入了 Lync 作為校內教職員間的整合通訊平台。由於 Lync 亦是微軟相關產品，因此在帳號及權限控管上，亦能輕易的與校內 Active Directory 驗證機制進行整合，在很短時間內即將 Lync 建置起來提供校內同仁使用。

4. 實際應用經驗

亞洲大學於 100 學年度「教育部第二次大學評鑑」裡，為了支援評鑑準備工作和資料管理的需求，即選定 SharePoint 導入做為資料共享平台，跳脫傳統以檔案伺服器形式蒐集資料的作法。也正因如此應用的開端，而決定擴大 SharePoint 平台在校內的應用面，命名為「亞洲大學辦公室資訊彙整系統」(Office Information Communication and Collection; OiC)，圖 3 為 OiC 主畫面。現階段已可展現共同編輯、文件管理及訊息透通等多項協同工作效益。底下即針對亞洲大學的實際應用方式進行說明。



圖 3 OiC 主畫面

4.1 網站集合規劃

網站集合(Site Collection)及子網站(Sub Site)是 SharePoint 實際運用的一種組織結構，亞洲大學係以對應校內行政及教學兩大體系下的各一、二級單位方式，於 SharePoint 網站內建立相對應的子網站並維持一、二級單位的相應關係，以供各單位除能自行維護所屬的相關文件資料外，亦能經由樹狀結構進行權限的相關設定，減輕設定及管理上的負擔。圖 4 為 OiC 子網站架構。



圖 4OiC 子網站架構

4.2 權限設定方式

權限設定是 SharePoint 實際應用上頗為重要的一環，因其牽涉到各子網站內使用者的使用功能，亦影響了各單位文件資料的安全性，因此不可不慎。

亞洲大學行政及教學一、二級約有 50 單位左右，為減輕權限上的負擔及日後管理的彈性，在「辦公室資訊彙整系統」建立之初除上述子網站的階層式建構外，更搭配微軟 AD 目錄服務機制將校內教職員全數建立於目錄服務內，搭配 AD 的群組管理，直接將 AD 群組設定給子網站對應如擁有者或成員等角色。如此，當單位內人員異動時，即可透過調整 AD 上對應的群組，達到異動該使用者於「辦公室資訊彙整系統」內套用至對應的子網站與使用權限，讓權限管理方式更為簡便。圖 5 為 OiC 權限設定示意圖。

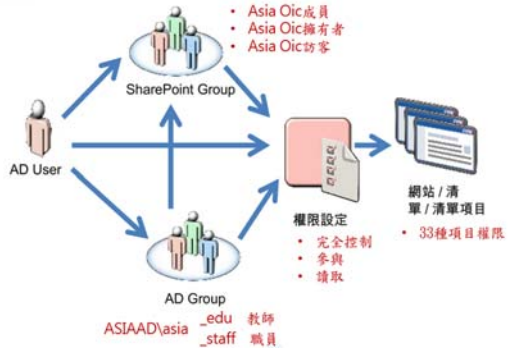


圖 5 OiC 權限設定示意圖

4.3 文件庫應用架構

SharePoint 文件庫是提供建立、儲存、更新，並與小組成員共同處理檔案的網站位置。每一種文件庫類型 (文件、圖片、表單和 Wiki 頁面) 都會顯示檔案清單及關於檔案的重要資訊，例如最後一位修改檔案的人員等。

OiC 針對每個單位的子網站規劃建立下列文件庫以供分類儲存不同屬性的檔案資料，圖 6 為 OiC 文件庫目錄結構：

(1) 共同編輯文件區：提供存放單位內目前進行中事務的相關文件檔案，若該文件需跨單位進行編輯，亦可在此設定適當權限供其他單位存取。

(2) 單位文件：提供單位存放過往已完成需歸檔之文件檔案。

(3) 單位法規：提供單位存放所屬相關法規之文件檔案。

(4) 會議記錄：提供單位存放過往已完成各式會議，需歸檔之會議記錄與相關文件檔案。



圖 6 OiC 文件庫目錄結構

4.5 校園通訊整合平台

在考量建置成本及使用便利性等因素下，亞洲大學於 OiC 建置後便接著導入了 Lync 作為校內教職員間的整合通訊平台。校內應用上，除了使用基本的傳送文字訊息功能外，Lync 亦提供了便利的檔案傳輸功能供同仁間即時傳輸資料、多人會議及電子白板功能供同仁間互相討論事項、而顯示桌面或程式功能則可提供資訊處同仁遠端進行系統檢查及維修，節省以往維修人員需四處奔走的時間，並更可快速地協助狀況排除。圖 7 為亞洲大學校內 Lync client 使用畫面。



圖 7 亞洲大學校內 Lync client 使用畫面

4.6 其他應用

OiC 於根網站內建置了「最新公告」及「全校行事曆」兩個功能網站，「最新公告」主要提供校內各單位針對校務相關事項進行公告。而「全校行事曆」則是顯示每學年內每月份既定安排的事項，事項係於每學年行事曆發布後即同步於 OiC 此功能如使用者透過 Outlook 軟體事先設定同步，當訊息發佈或變更時，教職員可即時得知，有助於訊息即時傳遞。圖 8 為 OiC 全校行事曆畫面。



圖 8 OiC 全校行事曆畫面

5. 結論及未來發展

辦公室自動化係根據辦公室三層功能：決策、管理、與操作的需求設計與開發，其演進過程由最早的機器化、電腦應用，再到現今通訊網路的加入，使得辦公室自動化邁入了無國界領域。在實施辦公室自動化時必須考慮到成本、共通性及制度化問題，除建置初期投資成本的考量外，評估與現行作業模式是否共通尤為重要，當作業制度逐漸形成，加上完善的教育訓練並配合維護計畫，方能使辦公室自動化邁向成功之路。

亞洲大學自導入 Sharepoint 協同合作平台及 Lync 校內即時通訊後，最大的好處是解決了以往單位同仁間分享公務檔案的不便，Lync 除了提供同仁便捷的溝通管道外，亦提供檔案傳輸、電子白板以及視訊會議等功能；Sharepoint 則是建構了校內分享檔案的統一平台，搭配合宜的權限控管機制，可在資訊分享中保有適當的存取安全，避免檔案不當使用。

未來，亞洲大學將以 Sharepoint 為基礎發展適合校內使用的電子表單及電子流程，進一步整合校園資訊環境。另外，微軟於 2012 年底推出的新版 Sharepoint 2013 本校亦已同步進行測試，Sharepoint 2013 除保有原 2010 架構外，，更強調企業社群智能累積及 Skydrive Pro 雲端儲存機制，已列為本校下階段導入目標，進一步實現協同合作的理想。

參考文獻

[1] 台灣微軟，亞洲大學以 SharePoint Server 2013 打造資訊匯整平台，http://www.microsoft.com/taiwan/casestudies/case/case_130318_asia.aspx

[2] 台灣大百科全書，辦公室自動化 http://taiwanpedia.culture.tw/web/fprint?ID=25398

[3] 台灣微軟, Sharepoint 2010, http://www.microsoft.com/taiwan/sharepoint2010/

[4] 台灣微軟, Sharepoint 2013, http://www.microsoft.com/taiwan/sharepoint2013/

[5] 維基百科，微軟 SharePoint 系統, http://zh.wikipedia.org/wiki/%E5%BE%AE%E8%BB%9FSharePoint%E7%B3%BB%E7%B5%B1

[6] 台灣微軟, Lync http://www.microsoft.com/taiwan/lync/lync2013.aspx

[7] 維基百科，自動控制, http://zh.wikipedia.org/zh-tw/%E8%87%AA%E5%8A%A8%E6%8E%A7%E5%88%B6#.E8.BE.A6.E5.85.AC.E5.AE.A4.E8.87.AA.E5.8B.95.E5.8C.96.E6.8E.A7.E5.88.B6.28Office_control_automation.29

[8] 台灣微軟, SharePoint 2010 雲端辦公室秘笈。

[9] 台灣微軟, Office 365 雲端辦公室快速體驗手冊。

[10] 辦公室自動化講義（樂斌編撰，僑務委員會中華函授學校出版）

學生學習成效分析－以國立臺北藝術大學為例

黃國倫　　張翠琳
國立臺北藝術大學
kulun@tnua.edu.tw　tlchang@academic.tnua.edu.tw

摘要

國立臺北藝術大學是以藝術、表演、人文研究、創作等領域為課程的學校。有別於一般大學，大學部的學生有八成以上是採取單獨招生方式入學。然而對於所錄取的學生，是否都能培養出符合預期的藝術人才，這也是學習成效分析的目的。基於這樣的想法，學校嘗試建置「學生學習成效資料庫」，並且匯整校內多個資訊系統的資料。藉由系統中招生階段、就學階段及畢業階段的分析功能，來評估三個不同時期學生的學習成效，進而建立「從學生入學到畢業」之全面性學習輔導機制。若從中找出影響學習成效的關鍵因素，將可導引學校檢討自身定位與方向，以發展出學校的教學特色。

關鍵詞：畢業流向、學習成效、學業表現。

1. 前言

國立臺北藝術大學（簡稱北藝大）是以藝術、表演、人文研究、創作等領域為課程的學校，並以培養專業藝術創作與研究人才為使命。北藝大擁有音樂、美術、戲劇、舞蹈、電影與新媒體、文化資源等六大學院，有別於一般大學，學生的入學管道有八成以上是採取單獨招生方式（以大學部為例）。近幾年配合教育部政策，也嘗試加入繁星推薦及個人申請的入學管道名額。

對於學校而言，最重要的特色是以傳統師徒相承的特殊教學方式，即使面對不同招生管道所錄取的學生，都能培養出符合預期的專業藝術人才，這也學校教育最主要的精神。為了達到這個目的，同時掌握學生在校學習的狀況，因而規劃建置「學生學習成效資料庫」，藉由匯整學生各項資料進行統計，並以質化及量化的分析方法，希望能評估學生的學習成效，以作為未來招生管道及教學方式的調整參考依據。

2. 文獻探討

2.1　臺灣高等教育整合資料庫

臺灣高等教育整合資料庫的建立目的在透過信實可靠資料之提供，提升高等教育相關校務、政策、學術研究水準，促進高等教育良善發展。其來源主要由「高等教育師生問卷調查」與「大專校院畢業生流向調查」兩項計畫的成果所結合而成，且都是由教育部高教司委託國立臺灣師範大學教育研究與評鑑中心辦理之調查計畫。

其中，「高等教育師生問卷調查」[1]，又包括「大一大三調查」與「大專教師調查」兩個項目，是藉由網路問卷為主，輔以紙本問卷的調查方式，而對高等教育大一、大三、二技一年級學生與大專教師進行長期的追蹤。以瞭解國內大專校院學生的在校經驗、課業修習狀況、生活作息、未來規劃、對學校與自己之看法、相關背景資料；以及全國專任大專教師在工作與生活情況、教學策略、方法及學生評鑑方式、對學生與學校的看法。這項調查計畫從學校的兩種身分：授教者與受教者，彼此對於學校教育的想法與意見。因此對學校而言，可以作為政策規劃與研究，以及進行自我評鑑、跨校比較、校務規劃與辦學改進之參考數據。

「大專校院畢業生流向調查」[2]在瞭解國內大專院校畢業生畢業後之流向，而蒐集國內大專院校畢業生求學與就業的相關經驗、表現與意見。它區分為應屆畢業生調查、畢業後一年追蹤調查及畢業後三年追蹤調查三項：應屆畢業生因為處於畢業前找工作的時期往往尚未確定未來的發展，因此所獲得的資訊也較不明確，在這階段主要在詢問目前狀況、就業情形、進修情形、求職意願、證照及求職意見等資訊；而畢業後一年，幾乎大多數的學生已經踏出學校的第一步，不論是進入職場獲得第一份工作或是繼續升學步入另一個學習階段，至少都有明確方向。因此這階段主要調查目前主要的計畫、就業情形、進修準備、證照或檢定證書、求學經驗的回顧、對學校的意見與看法；而畢業後三年對於就業或升學的畢業生是人生轉折的時期，因此這階段的調查是以目前狀況與初職經驗、就業情形、進修情形、求職意願、證照及求職意見、對自我及學校教育的評估為主。

臺灣高等教育整合資料庫迄今仍陸續公開各年度的調查分析報告與問卷內容，並開放線上分析系統[3]，讓全國大專校院可以查詢該校學生的調查結果，並提供統計方法更進一步進行分析。然而目前仍未開放原始資料予學校使用，故無法進一步結合學校的學習歷程平台或學習預警系統以達到最終的目標－個人生涯歷程檔案。但若是直接參考統計結果，仍可以讓學校了解學生畢業後的發展情形，以作為歷年差異分析與未來趨勢評估的依據。

2.2 104 升學就業地圖

104 人力銀行網站[4]是一個提供求職者及求才廠商媒合服務的資訊平台。除了針對不同身分的求職者以職務、地區及產業等條件查詢職缺；也提供就業輔導、市場調查及職場學習等多元化服務。其中，「升學就業地圖」就是利用曾經在該網站求職過的履歷資料，彙整十年內的畢業生其升學及經歷資料進行統計所建構的平台。在這平台中，可以從不同的分類群組，包括：學校、科系及學門查詢到各項升學、就業、薪資及專業技能的統計指標，每項指標都可以詳細看出畢業生升學或就業的分布情況及相對比例，如圖 1 所示。



圖 1 104 升學就業地圖

雖然薪資會因產業、個人工作績效、所具備的專業知識、工作複雜程度以及社會環境的綜合影響而有所不同，並不一定能適用於相同學校科系下的畢業生。而且目前網路上也存在不少相同性質的人力銀行網站，對求職者而言，並不一定選擇在 104 留下履歷資料，因此有效的樣本數也會影響統計結果的準確度。但不論如何，「升學就業地圖」的確提供了市場薪資行情及職涯發展方向的參考數據。

3. 系統設計

3.1 系統架構

學校的目的在提供學生各種教育的活動，學生在教育活動的過程是否真的獲得到應有知識，這也是學習成效分析的重點。如果把分析範圍套用在學生進入學校前所具備能力表現；以及之後進入學校後就學期間學業表現；至最後畢業離開學校升學或就業的表現，經由三個不同的時期分析更加能夠反應出學生在學校教育下的轉變，是否培養出符合社會及產業需求的人才。

為了讓「學生學習成效資料庫」能夠涵蓋入學前、就學期間及畢業後的分析範圍，其資料來源必須匯整學校內的資訊系統，包括：招生試務系統、學籍資料庫、教務系統、學務系統、校友資料庫及畢業流向調查系統，並依照這樣的架構設計出三個階段的系統功能，如下：

- 招生階段分析：利用學生在入學考試的各項成績，以及其他單位所舉辦的學術科能力測驗作為來源數據，以評估入學前的成效。
- 就學階段分析：學生進入學校後學習過程中經歷大大小小的測驗，最後在學業上所獲得的成績作為評估就學期間的成效。
- 畢業階段分析：當學生離開學校後，不論是升學的情形或是進入職場的工作及薪資，都可以用來評估畢業後的成效。

3.2 系統介面

「學生學習成效資料庫」的系統操作方式是採取瀏覽器為主，而介面設計是由三個部分組成：統計選項、統計圖表及統計資料。在操作流程上，使用者按照順序點選統計選項中的各種項目，共分為六個步驟，如下：

步驟一：請選擇指標項目（Y 軸）

步驟二：請選擇分組項目（X 軸）

步驟三：請選擇篩選條件

步驟四：請選擇排序方式

步驟五：請選擇圖表類型

步驟六：請選擇統計方法及數值

系統會依照統計選項過濾出符合條件的結果，並在統計圖表區域中呈現出圖表內容，而在統計資料區域中會顯示計算後的統計數值，如下圖所示。

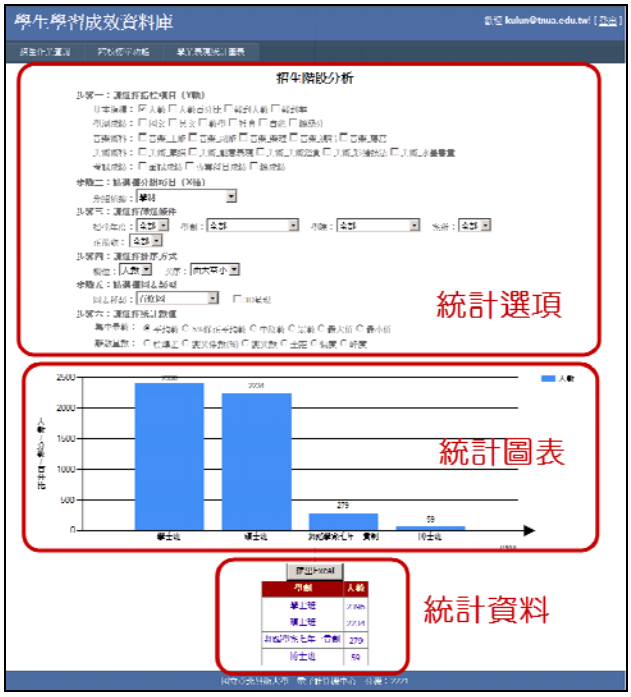


圖 2 系統介面

3.3 統計指標

目前系統所提供統計的指標項目，可分為兩種類別，一是量化指標項目，如表 1 所示。這是由數值型態所組成的欄位資料，因為是數值所以可以使用統計量數作為預估與測量的方法。目前系統提供兩種不同類別的統計量數：集中量數(Measures of Central Tendency) 與離散量數 (Measures of Dispersion)，如表 2 所示；另一類是質化指標項目，如表 3 所示，這是由非數值所組成的欄位資料，有別於量化指標，質化指標項目只能以次數分配及相對次數分配（百分比）作為統計方法。

表 1 量化指標項目

	量化指標項目
招生階段	學測成績：國、英、數、社、自、總級分 術科成績：音樂、美術 考試成績：面試成績、專業科目成績、總成績
就學階段	學業表現：學業成績、名次、學優獎 非學業表現：社團幹部、退學、休學
畢業階段	畢業流向：升學率

表 2 統計量數

	統計量數
集中量數	平均數、5%修正平均數、中位數、眾數、最大值及最小值
離散量數	標準差、變異係數、變異數、全距、偏度及峰度

表 3 質化指標項目

	質化指標項目
招生階段	招生年度、招生別、正備取、報到學校 畢業學校、居住地區、語言能力
就學階段	入學管道、學制、學院、系所 姓氏、人名、星座、性別、國籍、原住民、僑生、低收入
畢業階段	畢業年、畢業流向、工作性質、服務機構、職稱

4. 學習成效分析

「學生學習成效資料庫」提供三個階段的分析功能，涵蓋入學前、就學期間及畢業後的資料範圍。所以透過每個階段的分析將可以找出影響學習成效的關鍵因素。這些關鍵因素將作為學校未來招生管道及教學方式調整的參考依據。

4.1 招生階段分析

招生階段分析可以協助學校了解錄取學生的素質與能力，透過錄取生的統計，包括學生基本資料、正取生分佈、報到人數、畢業學校及可能就讀他校數據，將可導引學校檢討自身定位與方向，以發展出學校的招生方式。

因此以 101 學年度大學部錄取的正取生為統計範圍，計算出各學院錄取人數與報到情形，如圖 3 所示。

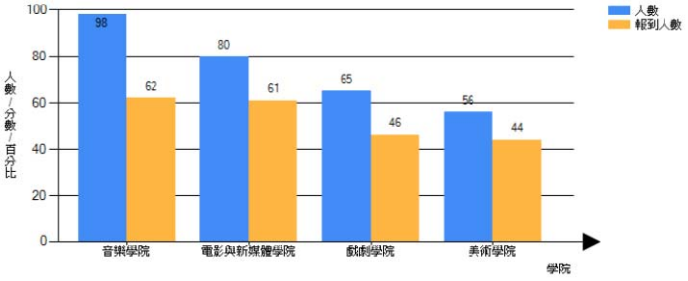


圖 3 錄取生報到統計

再進一步針對這些錄取生的畢業學校是否與報到比率有相關性，如此便能得知高中學生對於北藝大的喜好，如圖 4 所示。

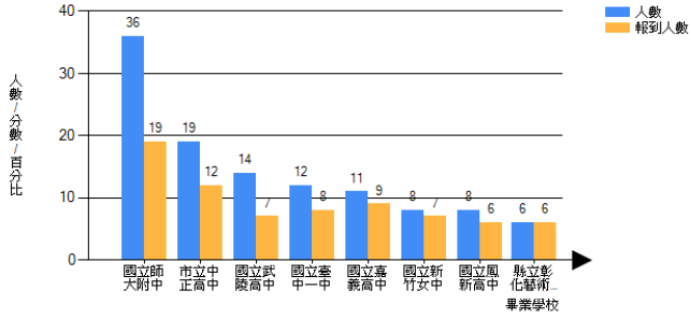


圖 4 錄取生畢業學校

從另一個角度分析，若針對放棄報到的錄取生去追蹤，統計他們最後就讀的學校，便能夠得知北藝大可能的競爭對手，如圖 5 所示。

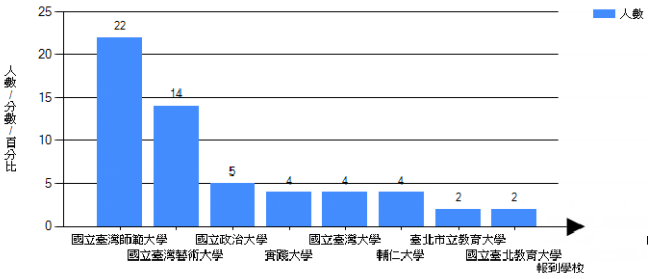


圖 5 錄取生放棄報到可能就讀學校

另外，也可以針對考試成績進行分析，以找出錄取生學測成績與面試成績的相關性，如圖 6 所示。

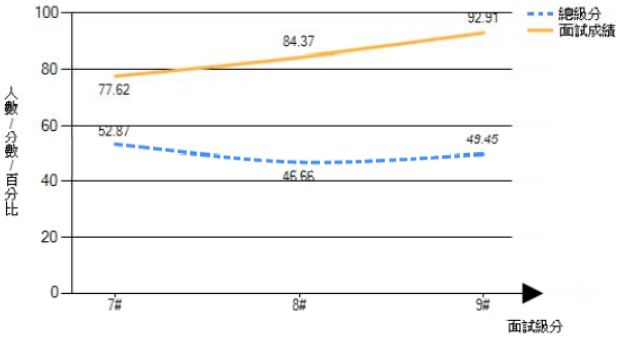


圖 6 學測成績與面試成績統計

4.2 就學階段分析

大一新生處於高中與大學之過渡時期，往往必須協助學生認識大學環境及建立自我，故透過就學階段分析，於一開始將學生學業成績進行分析，使其得以依其性向訂定生涯進路發展計畫，並建立新生輔導機制。

為了取得新生入學後的學業成績，因此以 100 學年度大學部的學生作為統計範圍，經過一年的就讀已經產出平均成績與名次，便可得知不同入學管道學生在學業上的表現。然而為了避免少數的學生影響統計的精準度，故選擇 5%修正平均數作為統計量數，即排除最好及最壞的各 5%學生，僅統計剩餘的 90%學生成績，如圖 7 所示。

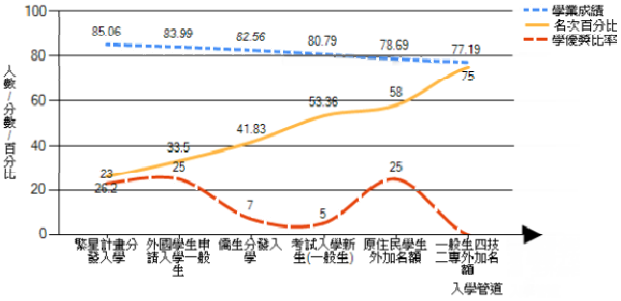


圖 7 學業成績 5%修正平均數統計

另一項可以作為參考的數據為休學退學的比率，如圖 8 所示。入學一年即辦理休學或退學，除非是重大的變故，否則代表著學習的過程發生了問題，這也是需要加以輔導的對象。

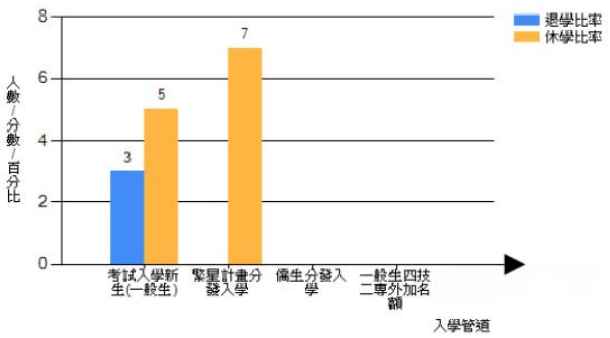


圖 8 休學、退學比率

一般而言，男女生在學業表現上會有顯著的差異，即使是藝術教育為主的學校仍然有相同的結果，如圖 9 所示。

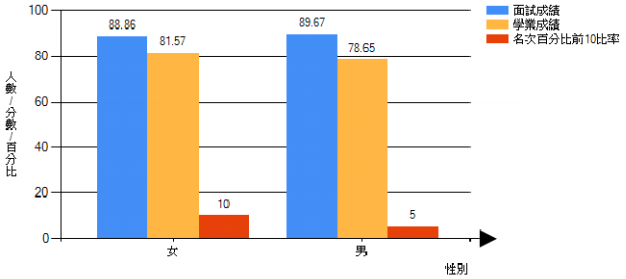


圖 9 男女生學業表現

學生在招生考試時的成績高低，是否代表進入學校後會有相同的表現，可以利用面試成績與學業成績進行相關性分析找出答案，如圖 10 所示。

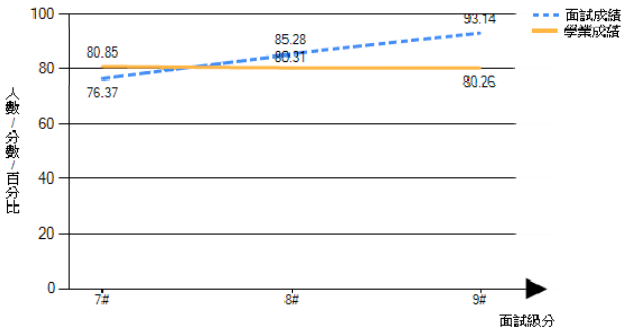


圖 10 學業成績與面試成績

4.3 畢業階段分析

畢業階段分析，最主要的重點在瞭解學生畢業後的流向，不論是升學或是就業的情形。透過這樣的分析，除了讓學生於課業中獲得基本專業知識外，同時為學生辦理性向分析，協助學生訂定學習計畫與職涯規劃，使學習內容逐步貼近生涯規劃藍圖。另一方面，讓學校教師瞭解社會人力需求趨勢，將有助於系所課程改革，調整學習的方向，以達到學以致用的目標。

因此設定以 97 學年度入學的大學生且順利於 100 學年度畢業的學生作為統計範圍，如圖 11 所示畢業流向的統計結果是以百分比方式呈現，其中有 46%的畢業生選擇繼續升學。

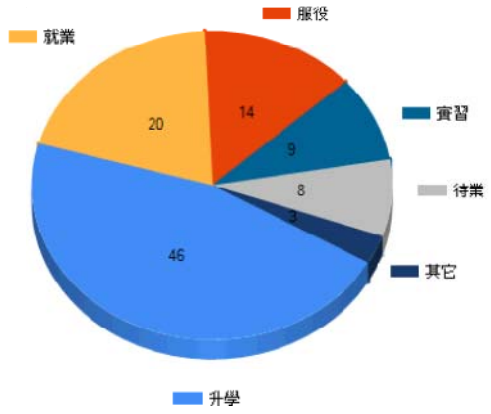


圖 11 畢業流向統計

若再更進一步針對升學狀況分析，各系所因為領域上的差異，所以也影響畢業生在升學的可能性，如圖 12 所示。

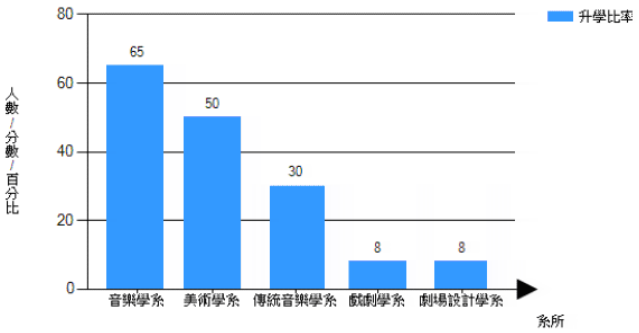


圖 12 系所升學比率

另外，仍有一部份的畢業生選擇進入職場，若排除掉兼職性的工作僅以專職工作為主進行統計，並以百分比方式呈現，即如圖 13 所示。大部份的畢業生在畢業後仍然從事藝術相關的工作。

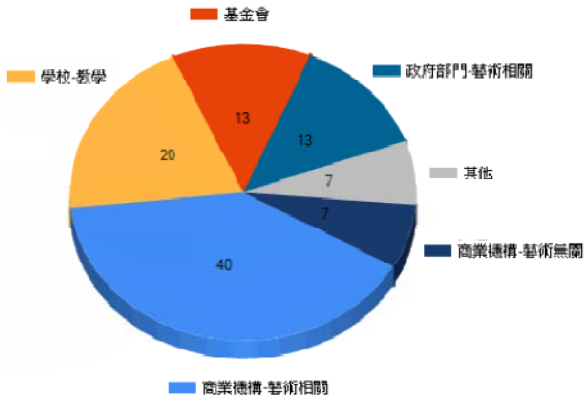


圖 13 就業工作性質

5. 結論

以往進行學生學習成效分析，僅以老師主觀所認定的表現為主，最多再利用學業成績作為評估的參考，這使得分析的過程缺乏客觀的資料，其結果更不準確。「學生學習成效資料庫」的建置目的在協助學校進行學習成效評估，除了提供線上資料分析平台，且系統所能統計的範圍並不僅於學業表現，而擴大從入學前及畢業後的表現皆能涵蓋。只要透過直覺式的勾選統計選項，就可以獲得各項統計數據。

當然系統的準確性仍取決於資料匯整的完整性及正確度，以及獲得到的統計數據如何加以解釋及分析，這才能真正評估出學生學習成效。如果從更長遠的目標來看，若能利用影響學習成效的關鍵因素，將可協助教師教學專業成長、提升學生學習風氣、改進課程結構及學習內容，並引導學校建立出「從學生入學到畢業」的全面性學習輔導機制。

5.1 未來工作

對於學生學習成效分析不應該只看單一指標或單一年度，而必須從長期且多面向的進行追蹤。由於「學生學習成效資料庫」是匯整學校內多個資訊系統的資料，因此，資料的處理與轉檔也是最花時間的工作。尤其未來每年必須於放榜後(匯入招生資料)、第一次教務會議後(匯入成績資料)及開學後(匯入畢業資料)定期匯整資料，才能維持資料的時效性與完整性。

除此之外，對於資料庫的分析及使用上也規劃下列三個發展方向：

- 擴大資料來源的範圍，提升分析的廣度(例如：畢業流向分析可以從薪資與產業別了解就業表現)及深度(例如：學業成績可以更細分為必修、選修及通識等成績)。
- 導入技術分析方法(例如：相關係數、變異數分析、迴歸分析)，建構出統計資料點、線、面之關係。
- 運用分析的結果，調整招生策略 (例如：招生管道、名額、考試方式、配分比例等)，甚至提供教務、學務、系所及校務評鑑作為參考依據。

參考文獻

[1] 臺灣高等教育師生問卷調查計畫，https://www.cher.ntnu.edu.tw/?cat=6
[2] 大專校院畢業生流向調查計畫，https://www.cher.ntnu.edu.tw/?cat=80
[3] 臺灣高等教育整合資料庫線上分析系統，https://das.cher.ntnu.edu.tw/index.php?site_=tiped
[4] 104 人力銀行，http://www.104.com.tw

網路電話系統在行動節費之應用

陳家祿　　楊世偉
國立暨南國際大學計算機與網路中心
{ gotop, eshin }@ncnu.edu.tw

摘要

隨著網際網路與無線通訊網路的蓬勃發展，VoIP 通信服務在這幾年正在不斷的發展，現今隨著各學校與台灣學術網路(以下簡稱「TANet」)之間頻寬的充足與穩定加上資訊網路發展均已完備，透過網際網路（Internet）的運用已漸漸普及並成為一種新的傳播媒介，VoIP (Voice over IP) 將語音及數據資料整合在單一 IP 網路架構上的技術，已為傳統通訊帶來革命性的改變。

教育部近年大力推廣網路電話系統，所以各縣市網下的國中小學幾乎都有建置網路電話，大專院校也有 48 所學校加入台灣學術網路語音交換平台，但是不少學校是網路電話與學校分機電話各為獨立的系統，有些是交換機透過 Gateway 與網路電話界接，市話可透過教育部的 ENUM 系統達到網路電話通話免費，但行動的部分則需透過電信業者的行動節費器，或透過電信 2 類業者下車達到節費效果，但都需要通話費用無法達網路電話通話免費的效果。

因此，在本文中，運用新一代網路技術的 IP-PBX，透過網路電話可提供多路由的特性，並結合行動電話業者 MVPN 通話免費的服務與部分行動業者網內互打免費的服務，來探討測試如何做到網路電話行動通訊免費之成效。

關鍵詞：VoIP、網路電話、Gateway、IP-PBX、MVPN

1. 前言

VoIP（Voice over Internet Portocol）技術自 1995 年開始萌芽，歷經 10 年來在國際通信市場上的研發及應用，目前在技術上可說是完全成熟。網路電話是指利用網路電話相關的硬體與軟體，將人說話的聲音取樣，並且將取樣後的信號壓縮及轉為數位語音封包後，透過 TCP/IP (Transmission Control Protocol/Internet Protocol)協定，利用網際網路傳送給對方，而受話端將所收到數位資料封包重組回成語音封包，並且解壓縮及轉換成語音信號，來進行雙方通話。透過既有的網路來做國際或長途的通話，在通話費上的成本遠低於傳統電路交換式電話(Public Switched Telephone Network，簡稱 PSTN)的通話費。

使用網路電話通訊是未來的趨勢，但許多學校的網路電話系統與交換機系統分屬不同的單位，造成許多學校在推廣網路電話上有些阻力，網路電話的優勢在於透過網路電話通話免費，由於行動通訊的發達學校對外聯絡方式，約有 50%以上都是撥打行動電話，不論是交換機系統或網路電話系統，透過電信業者撥打市話或行動都需要通話費用。

個人在學校是做電信業務原本只接觸傳統交換機，由於學校新接教育部區網中心的業務，所以個人又接下區網中心網路電話的業務，且學校傳統交換機老舊需汰換，因經費問題只能採取逐步汰換的方式，並採用新一代網路技術的 IP-PBX，個人因業務需求了解到各家電信業者的節費方案，想透過 IP-PBX 多路由的優點，思考如何透過各種的設備與電信業者的方案，達到撥打行動電話免費之研究。

2. 相關背景知識

在本章節中，我們將介紹幾個相關的通訊協定，以及各個相關的知識，建構起本論文所提出網路電話在行動節費上之應用。

2.1 IP-PBX

什麼是 IP-PBX，簡單來說是利用 IP 資料網路提供電話通信的完整電話系統。所有通信都以資料包的形式在網路中進行傳遞。

IP-PBX 能達到傳統 PBX 的功能，如具有呼叫轉接、代接、三方通話、群振、輪振、保留等功能，同時也集成傳統 PBX 難以提供的各種業務功能，如 IVR、音樂鈴聲、Voicemail 和錄音等功能。還能夠利用網路閘道器連接到傳統的 PSTN 線路上，進而能與傳統的 PSTN 互聯通訊。

2.2 MVPN(Mobile Virtual Private Network)

行動群組電話是專為企業量身設計的虛擬專用網路。可依企業客戶的不同需求，將企業成員的隨身行動電話號碼甚至是公司的總機號碼，在無需申裝任何額外電信設備下，透過智慧型網路聯結成一個迅速、高效能的群組式行動通信網路，無限延伸企業行動力。

以中華電信的行動群組為例，將中華電信行動電話設定為同一群組，此群組內成員間之通話或與群組外指定之中華電信行動電話及市內電話皆可以簡碼撥號並享有優惠費率，透過專案方式多家電

信業者都提供分機撥打群內行動費用零元。

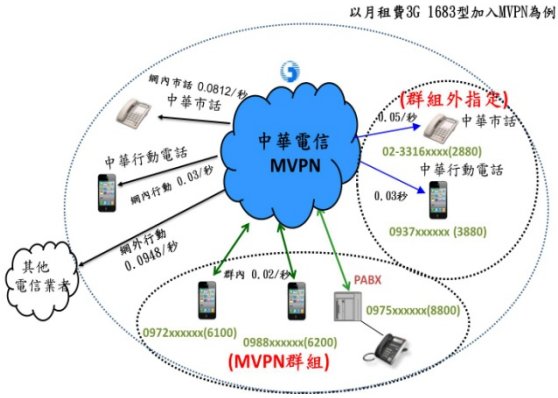


圖 1 中華電信 MVPN 群組圖

2.3 Session Initiation Protocol (SIP)

SIP 是近年來最流行的網路電話通訊協定，與先前同樣用來進行網路電話通訊的另一套網路電話通訊協定 H.323 相比，它擁有較大的彈性、容易實作、而且較適合應用在智慧型手機上。SIP 是一個信令通訊協定，在網路電話通訊中負責進行信令溝通的部分，它可以用來建立、修改、結束一通網路電話。以下用圖 **2** 來說明一通由 SIP 從建立到結束通話的流程圖。

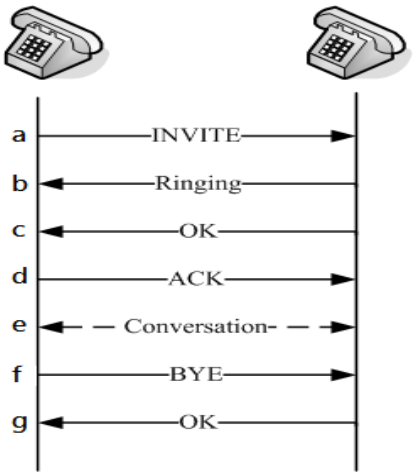


圖 2 SIP 網路電話通訊流程圖

如上圖：

a. 撥話端送出一個 INVITE 的訊息，邀請受話端進行網路電話通訊。
b. 受話端收到 INVITE 訊息時，話機開始響鈴，並且送出一個 Ringing 訊息給撥話端，表示該通電話正在進行處理中。
c. 受話端接起電話後，會送出一個 OK 訊息給撥話端，表示接受此通電話的邀請。
d. 撥話端在收到 OK 訊息後，送出一個 ACK 訊息，回應受話端的 OK 訊息。
e. 此時通話建立，兩端開始進行語音通訊。
f. 撥話端欲結束該通網路電話，送出一個 BYE 訊息。
g. 受話端收到 BYE 訊息後，回應 OK 訊息，此時通話結束。

在 SIP 的架構中，邏輯上有兩個重要的伺服器，一個是 Registrar(註冊伺服器)，一個是 Proxy Server(代理伺服器)。Registrar 的功能是提供使用者註冊上該伺服器。註冊封包之擷取圖如圖 3：使用者發出 Register 要求，如果該 Registrar 需要進行使用者認證才能註冊的話，則 Registrar 會送出一個 401 Unauthorized 訊息要求使用者進行認證。在認證成功後，Registrar 會送出一個 200 OK 訊息給使用者，表示註冊成功；Proxy Server 則是在使用者進行撥打電話的動作時，負責替兩端使用者轉送 SIP 訊息。圖 3 是透過 Proxy Server 撥打網路電話時，在撥話端上擷取到的 SIP 訊息封包，SIP 訊息的通訊流程可對照圖 **2**。在真實網路中，Registrar 跟 Proxy Server 通常都會被建置在同一台設備上。

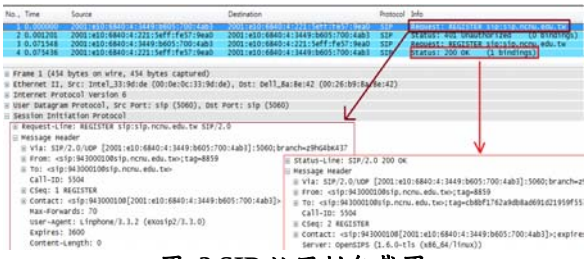


圖 3 SIP 註冊封包截圖

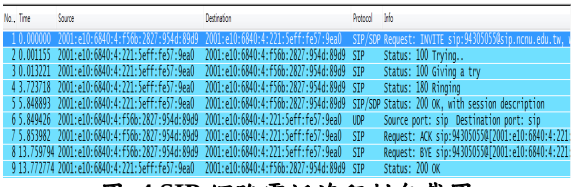


圖 4 SIP 網路電話流程封包截圖

在本論文所提出的網路電話系統中，Registrar 跟 Proxy Server 會建置在同一台設備上。

2.4 Session Description Protocol (SDP)

在上一節，我們提到了 SIP 是一個在網路電話通訊中只負責做信令溝通的通訊協定，所以它必須跟其他的通訊協定共同合作。而本節中所介紹的 SDP，會在建立一通網路電話時，被夾帶在 SIP INVITE 訊息中，用來告知兩端使用者，目前該通網路電話中媒體流(Streaming media)的相關設置信息，包含：語音封包的編碼方式、接收語音封包的位址及埠號(port number)等。SDP 結構圖如圖 4：

a. Protocol Version：代表 SDP 的版本
b. Originator and Session ID：該通網路電話的起始者以及該通網路電話的識別碼(Identification，簡稱 ID)
c. Session Name：該通網路電話的名稱
d. Session Time：通話持續時間
e. Media Name and Transport：語音型別、編碼方式以及語音傳輸的埠號
f. Connection Information：接收語音的位址

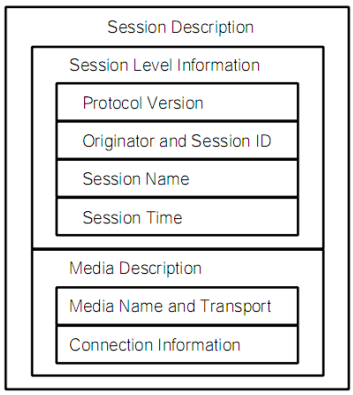


圖 5 SDP 結構圖

圖 6 則是當要開始進行網路電話通訊的時候，被夾帶在 SIP INVITE 訊息中的 SDP 封包截圖。由 c 欄位可以得知語音封包應該傳送至哪一個 IPv6 位址；由 m 欄位得知傳送的語音封包編碼方式以及應傳送的埠號。

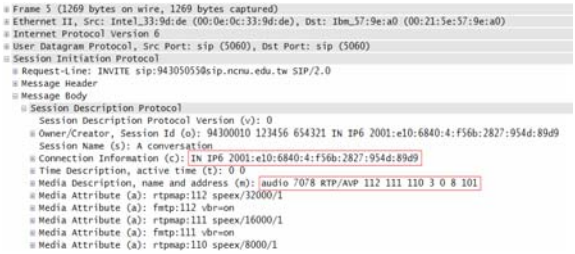


圖 6 SDP 封包截圖

2.5 Real-time Transport Protocol (RTP)

上兩節分別介紹了建立網路電話通訊的信令通訊協定，SIP；以及用來告知該通網路電話中媒體流相關設置信息的通訊協定，SDP。然而真正用來傳輸語音封包的通訊協定則是 RTP。圖 7 為 RTP Header(標頭)，在 RTP Header 中有一個 PT(Payload Type)欄位，代表的是在上一節中提到的語音封包編碼方式，該欄位共有 7 個位元(bit)，可用來表示最多 $2^7 = 128$ 種編碼方式。

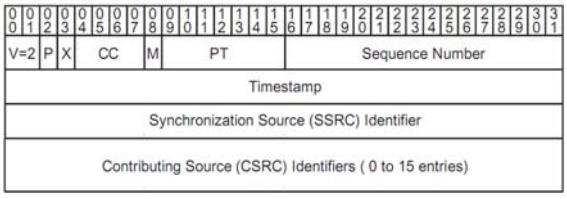


圖 7 RTP Header

表 1 為 PT 欄位所對應的編碼方式。圖 7 則為 SIP 建立通話後，在撥話端擷取到的 RTP 語音封包及其封包內所負載的編碼後語音資料(Payload)。

表 1 Payload Type(PT)與語音編碼方式對應表

Payload Type (PT)	編碼方式
0	PCMU
3	GSM
8	PCMA
18	G.729

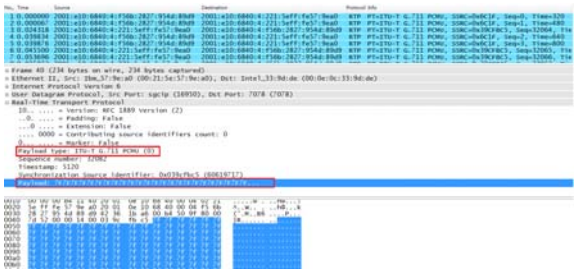


圖 8 RTP 語音封包及 Payload

2.6 網路電話閘道器（VoIP Gateway）

網路電話基本原理是通過語音壓縮演算法對語音資料進行壓縮編碼處理，然後把這些語音資料按 IP 等相關協議進行打包，經過 IP 網路把資料包傳輸到接收地，再把這些語音資料包串起來，經過解碼解壓處理後，恢復成原來的語音信號，從而達到由 IP 網路傳送語音的目的。

網路電話系統是把普通電話的類比信號轉換成電腦可聯入網際網路傳送的 IP 資料包，同時也將收到的 IP 資料包轉換成聲音的類比電信號。經過 VOIP 網路電話系統的轉換及壓縮處理，每個普通電話傳輸速率約佔用 8～11kbit/s 頻寬，因此在與普通電信網路同樣使用傳輸速率為 64kbit/s 的頻寬時，是原來的 5～8 倍。

網路電話系統具有路由管理功能，它把各電話區號映射為相應的閘道 IP 位址。這些資訊存放在一個資料庫中，有關處理軟體完成呼叫處理、數位語音、路由管理等功能。在用戶撥打網路電話時，網路電話閘道器根據電話區號資料庫，確定相對的 IP 位址，並將此 IP 位址加入 IP 資料包中，同時選擇最佳路由，以減少傳輸時間。

我們可以想成網路電話閘道器是一種連結傳統 PSTN 和 IP 網路的橋樑。將 PSTN 端之訊號數位化並壓縮再加以封包化(MG 部份)，加上 SG 的控制信令方式之調適與協調 SG 與 MG 功能之 MGC，便可把各類資料送至 IP 網路端。反之，接收端的網路電話閘道器把各個封包加以收集，解壓縮(MG 部份)，轉譯控制信令所指定的位址(MGC、SG)，然後以類比的形態送到 PSTN 網路。

網路電話閘道器在 PSTN 與 IP 網路間的位置如圖 9 所示，其組成之功能如下。

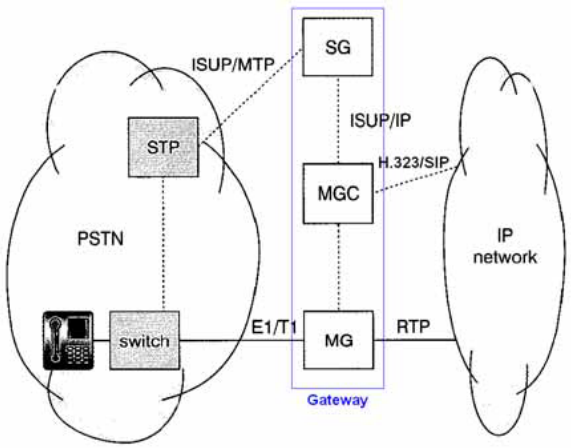


圖 9、Gateway 架構

功能說明:

MGC (Media Gateway Controller)：

位置在 MG、SG 和 GK 之間，其管理提供給眾多 MG 的可用網路資源和 IP 網路頻寬等。

SG (Signaling Gateway)：

提供了在 IP 網路與 PSTN 之間的信令轉譯功能。

MG (Media Gateway)：

提供了媒體對映或轉換的功能，主要是對於在 IP 網域和 PSTN 網域中的語音訊號做處理。

3. 行動優惠與設備介紹

本章節將介紹目前提供行動通訊服務的業者現況，以及各家行動電信業者的優惠，架構所需的設備。

3.1 行動電話業者現況

依據國家通訊委員會 102 年 6 月的資料，台灣目前提供行動電話服務的業者目前共有 5 家，分別是提供 2G 服務的有 3 家電信業者，3G 服務的則有 5 家電信業者，各行動電話業者的 2G 與 3G 門號的數量如表 2:

表 2 電信服務業者與門號數量

公司別	3G 用戶數（戶）	2G 用戶數（戶）	總用戶數（戶）
總計	23,528,474	5,241,343	28,769,817
中華電信股份有限公司	7,239,689	3,180,826	10,420,515
遠傳電信股份有限公司	5,997,428	1,000,779	6,998,207
威寶電信股份有限公司	1,735,262		1,735,262
台灣大哥大股份有限公司	6,046,422	1,059,738	7,106,160
亞太電信股份有限公司	2,509,673		2,509,673

3.2 門號可攜式服務 NP(Number Portability)

號碼可攜式服務 NP（Number Portability），就是用戶更換行動電話服務的提供業者，但可以不用更換行動電話號碼，用戶原本使用甲公司的行動門號服務，轉移到乙公司後，仍然保留原本使用的號碼，不需要重新申請一個號碼，以增加民眾的便利。

根據國家通訊委員會的資料如表 3 顯示，自從 2005 年開放門號攜碼服務，共有約 2 千萬次的行動門號進行攜碼服務，這代表我們不能依據行動電話的前幾碼來判斷，他是屬於哪家行動電信業者的門號，例如早期 0932 是中華電信 0935 是台灣大哥大 0982 是亞太電信，現在已不能依此作判斷，這影響到網路電話在做路由判斷時的設計。

表 3 電話號碼可攜服務生效統計

電話號碼可攜服務生效統計-2013 年 7 月			
	行動攜碼生效數	固網攜碼生效數	總生效數
2005 年總生效數	93,858	94	93,952
2006 年總生效數	511,358	516	511,874
2007 年 4 月份 2G-3G 資料搬遷	1,755,392		1,755,392
2007 年總生效數	2,080,264	1,093	2,081,357
2008 年總生效數	3,318,003	3,946	3,321,949
2009 年總生效數	3,220,594	8,109	3,228,703
2010 年總生效數	3,072,746	6,629	3,079,375
2011 年總生效數	3,068,243	5,102	3,073,345
2012 年總生效數	3,452,627	6,177	3,458,804
2013 年 1 月	294,022	420	294,442
2013 年 2 月	264,260	282	264,542
2013 年 3 月	266,646	326	266,972
2013 年 4 月	258,310	432	258,742
2013 年 5 月	278,489	481	278,970
2013 年 6 月	242,997	327	243,324
2013 年 7 月	306,198	281	306,479

3.3 行動電話網內免費

本次的研究主要是利用行動業者所提供的 MVPN 服務與簡碼撥號的特性，還有各家行動業者都有的撥打網內免費的方案，來規劃設計網路電話撥打方式及路由，所以需要了解各家行動業者所提供的優惠，以及達到撥打網內免費的最低門檻，再來規劃設計做法，表 4 是整理目前 5 大家電信業者所提供的服務與網內免費最低價錢。

表 4 電信業者提供服務與價錢

公司別	是否提供 MVPN 服務	是否提供網內免費服務	網內免費所需最低費用
中華電信股份有限公司	有	有	含上網 888
遠傳電信股份有限公司	有	有	含上網 1173
		7-mobile 使用遠傳線路用戶數約 70 萬網內互打免費	純語音 140
威寶電信股份有限公司	有	有	純語音 300
台灣大哥大股份有限公司	有	有	含上網 1100
亞太電信股份有限公司	有	有	純語音 333

3.4 行動電話節費器

行動電話節費器是一種採用 GSM 技術體制的無線固定語音接入設備，能在 GSM 蜂窩網覆蓋的範圍內，利用 GSM 網路系統快速地提供無線通信服務，能將 GSM 網路信號轉化為普通固定電話信號，適用於固定電話不易佈線地區，可直接代替固定電話，也能接入總機當成一路外線，。

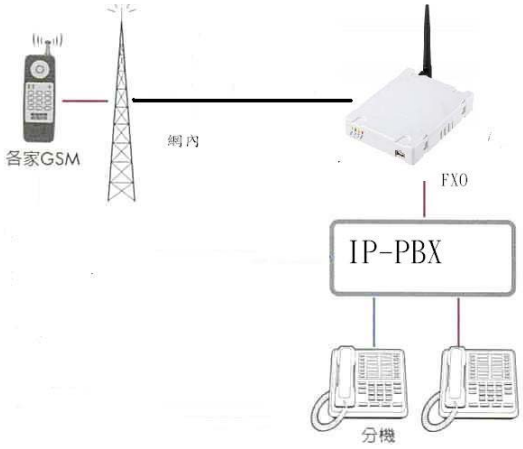


圖 10 行動節費器架構圖

4. 架構規劃設計

本章節將依據電信業者所提供不同的優惠方式，來設計不同的撥打行動電話免費的規劃，並規劃出如何達到行動通話免費之最大效益。

4.1 MVPN 群組免費之架構

利用 MVPN 群組免費是比較簡單的做法，利用 MVPN 群組簡碼撥號的方式路由規劃上也比較容易，圖 11 是 MVPN 群組架構圖。

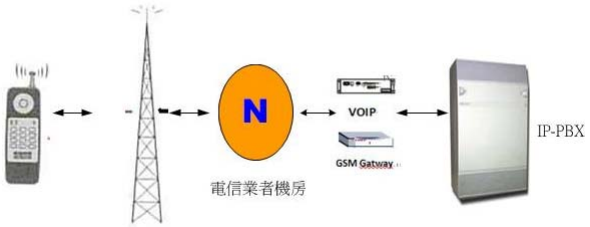


圖 11 MVPN 群組撥號架構

說明：

a. 電信業者行動電話 MVPN 服務是將一般外線透過 Gateway，將信號轉為 VOIP 信號回到電信業者機房，再經由行動基地台將訊號送至手機。
b. 利用行動電話 MVPN 群組簡碼撥號之功能，每支行動門號都會對應一組簡碼，例如行動電話號碼是 0920123456 對應簡碼 61234，在撥碼路由設計上，就可允許 6 開頭總長 5 碼的撥號經由行動節費出去。
c. 不同業者可規劃不同數字的簡碼開頭，例如中華電信簡碼開頭設 2 路由是 A，台灣大哥大簡碼開頭 3 路由是 B，這樣就可以做到行動通話免費。

4.2 經由行動節費器

各業者都有網內戶打免費的方案，使用不同業者的 sim 卡插上行動節費器上，透過撥打的號碼作路由辨識，這種做法是能夠達到最大免費通話之效果，缺點是因門號可攜的關係，作法上變的非常複雜，必須要將撥打的每支行動電話號碼區分是哪家業者，再建立資料庫做路由分辨，不同業者使用不同的行動節費器出去達到網內免費，再則受話方如果回撥電話則節費線路就會佔線，通話流程如圖 12。



圖 12 行動節費器架構

5. 結論

網路電話近年來已非常普遍，無論是台灣學術網路的語音交換平台，電信業者的國際節費電話與 070 的網路電話等等，這幾年校園網路電話在國中小學推廣上非常成功，透過 ENUM 系統也幫縣市政府節省了許多市話電話費用，許多老師反映是否能將行動電話也導入 ENUM 系統，撥打行動電話號碼轉成網路電話號碼達到通話免費，如果透過文中討

論撥行動免費的作法，透過撥打行動電話免費的做法撥接雙方都便利許多，教育部如能統合各校統一電信業者下車的路由，各校只要透過路由設定，不同業者經由不同路由下車，達到網路電話撥打行動通話免費最大之效益。

參考文獻

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, “SIP: Session Initiation Protocol,” IETF RFC 3261, June 2002.

[2] M. Handley, V. Jacobson, C. Perkins, “SDP: Session Description Protocol,” IETF RFC 4566, Jul. 2006.

[3] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications,” IETF RFC 3550, July 2003.

[4] David L. Mills, “Network Time Protocol (Version 3) Specification, Implementation and Analysis,” IETF RFC 1305, March 1992.

[5] Daniel Collins, “Carrier Grade Voice over IP 2nd Ed.” McGraw-Hill, September 2002.

[6] 陳炯良、施穎偉，「以『使用-擴散』觀點探討 VoIP 網路電話之擴散」，國立暨南國際大學資訊管理所碩士論文，2006 年。

[7] IEEE 802.3 Working Group, “IEEE Std 802.3af-2003-Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI),” July 2003.

[8] 李民慶、陳政良，「H.323 與 SIP 之 VoIP 閘道器架構探討」，亞東學報，2005 年

[9] 柯守全、趙啟時、劉安之，「VoIP 系統之建置與管理-以逢甲大學為例」，台灣網際網路研討會，2002 年.

[10] 中華電信網站，http://www.cht.com.tw/

[11] 國家通訊委員會，http://www.ncc.gov.tw/

下一代台灣電子發票系統與載具之評估與開發

賴源正[1]　黃淑容[2]　陳韋如[3]
國立臺灣科技大學資訊管理系
[1]laiyc@cs.ntust.edu.tw, {[2]M10109107, [3]M10109117}@mail.ntust.edu.tw

陳彥宏[4]
財團法人資訊工業策進會資安科技研究所
[4]pplong@gmail.com

馮壽元[5]　林榮輝[6]
財政部財政資訊中心
{[5]syfong, [6]N107711}@fia.gov.tw

摘要

台灣已於 2004 年開始採用電子發票，但如何在交易結束後讓消費者有效率地確認交易明細仍尚未有深入的探討和改進。因此本研究首先分析目前台灣電子發票系統的運作流程且進一步發掘出兩個議題，分別為(1)消費者無法立即檢視或查驗電子發票，以及(2)電子發票的整合效率低。為了解決這兩個議題，本研究探索目前現有的行動裝置與通訊技術以提出相對應的性能評估和解決方案。根據分析，不論是檢視電子發票的便利性或是電子發票的整合效率，配備 NFC 晶片的行動裝置都是最好的解決方案。本研究同時設計和實作基於 NFC 技術之電子發票系統以驗證此分析結果。此系統包含配備 NFC 的 POS 系統和行動裝置。該系統同時提供程式設計師與系統開發者一個測試平台來有效率地開發電子發票系統和相關應用程式，進而加速推廣台灣電子發票系統於各個領域的發展與應用。

關鍵詞：電子發票、NFC、POS。

1. 前言

發票是一個能增進政府稅務審計和公司財務管理的工具。因此台灣財政部於 1950 年推出『統一發票』紙本發票系統以提供政府稅務稽核的依據和商品服務交易行為的憑據[4]。近年來電子化交易的普及，使得採用紙本發行的統一發票無法讓政府或公司將交易憑據迅速整合進財務管理系統，進而耗費大量可避免的時間與金錢成本。因此台灣政府分別在 2004 年和 2009 年實行『電子發票系統』和『第二代電子發票系統』計畫來推行統一發票電子化。推動統一發票電子化的目的除了減少不必要的實體收據列印，也能提高交易憑據的整合性、加強交易認證的安全性和互通性，進一步促進電子商務的運作與發展[9]。根據 2007 年至 2011 年的統計，B2B 電子發票數量從一萬一千張增加至一千一百萬張，而 B2C 電子發票數量也由一千七百萬張增加至一億九千三百萬張[8]。

為了確保 B2C 交易的效率與便利性，B2C 電子發票不包含買家資訊。消費者必須透過可識別的載具(carrier)將電子發票與消費者建立綁定關係。亦即消費者首先透過台灣電子發票平台綁定載具與消費者之電子身分(如手機號碼或自然人憑證)，賣家即可透過載具綁定交易憑據與消費者[5]。載具可應用在任何可儲存資訊的卡片或設備上，例如會員卡、自然人憑證、信用卡、手機等。透過此機制與載具，當交易完成後，銷售點(POS, point of sale)系統先綁定載具與電子發票，再將完成綁定的電子發票傳送至台灣電子發票平台。隨後消費者可至電子發票平台檢索並管理該載具所綁定的電子發票與交易紀錄。然而，現存的載具面臨兩個問題。首先，消費者無法即時透過載具檢視交易的明細，仍須透過賣家將電子發票以副本方式列印於紙上。第二，銷售點所使用的技術，如一維條碼(Barcode)和 RFID(Radio Frequency Identification)，無法保護消費者隱私，且無法將電子發票整合進消費者的個人財務系統使得電子商務運作順暢[10]。這兩個問題不但讓消費者不願意使用電子發票，更阻礙電子發票的發展與推廣[6]。因此根據台灣電子發票系統的內部資訊，已發行之電子發票中只有 5%是真正落實電子發票的精神。

本研究提出一電子發票平台系統以解決上述兩個問題。發展此電子發票平台系統時，此研究首先分析目前所有可行通訊技術，包括 LTE[2]、Wi-Fi[11]、Bluetooth[1]、RFID 和 NFC（Near Field Communication)[3]，和各式行動性載具，如智慧型手機、平板電腦等的效能。開發本系統時，本研究同時考量與電子發票系統相關的各種因素，如連結

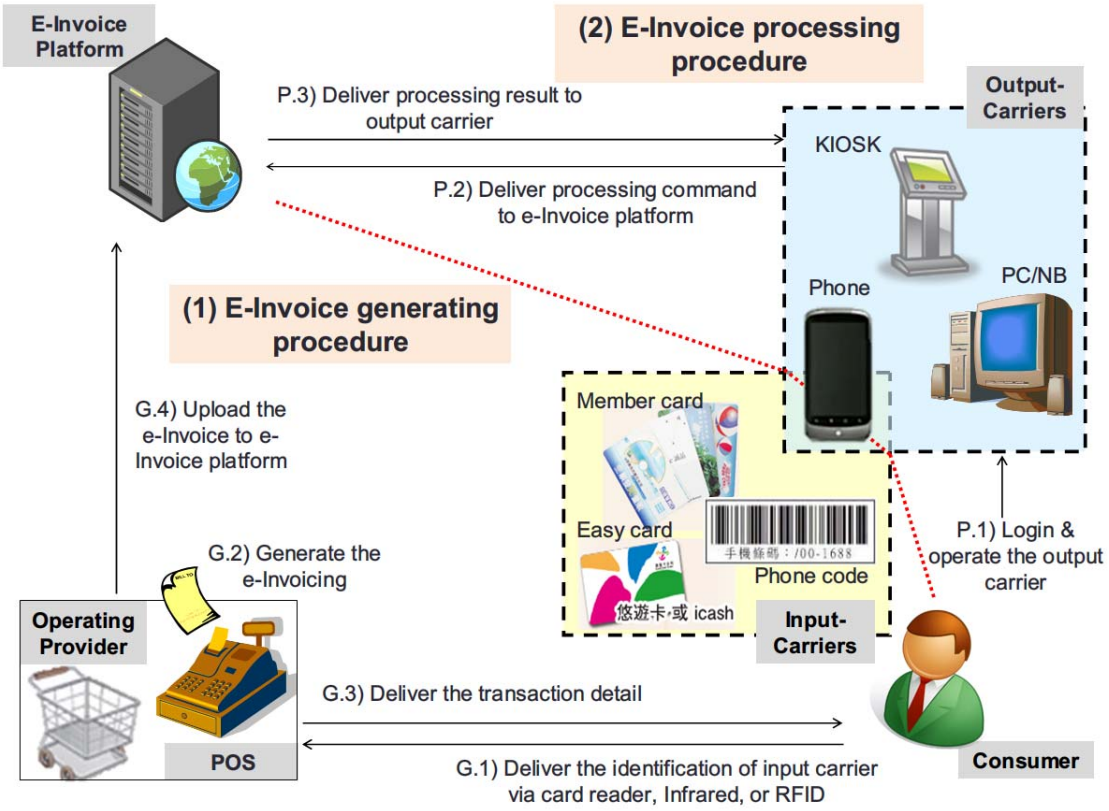


圖 1 本研究的電子發票之商業流程情境

時間、通訊成本、傳輸速率、隱私保護機制、基礎建設成本和顯示辨識率。根據分析，配備有 NFC 功能之智慧型手機為最適合做為電子發票的載具。故本研究所設計之電子發票平台系統是基於 NFC 技術，亦即由具備 NFC 功能的 POS 系統和智慧型手機所組成。此系統具有三個新特點：(1)所採用 NFC 技術除了有更好的通訊效能外，同時提供高擴展性與延伸性的系統架構以利於隱私保護機制和電子發票的應用與未來發展，(2)提供載具交易管理與購買模式分析功能有助於未來發展商業化知識管理，(3)提供 POS 端友善且精簡的 GUI 設計介面以呈現消費者購買行為，進而提昇並加強消費者和載具、KIOSK 之間的互動關係。透過以上三個特性，本研究所開發之 NFC 電子發票平台可提供消費者和各式電子商務應用軟體開發商一個測試平台來立即且有效地驗證所開發的相關電子發票軟體。

本文中的研究架構分做五章節：第二章回顧與電子發票相關的商業流程。第三章分析目前所有可應用於電子發票系統的載具和通訊技術之效率。第四章設計並展示基於 NFC 技術之電子發票系統以驗證第三章的分析。第五章為結論。

2. 電子發票商業流程之探討

關於電子發票之商業流程主要涉及電子發票平台、銷售點(POS)系統、輸入載具和輸出載具。電子發票平台隸屬於台灣財政部，用於儲存商業交易紀錄。POS 系統提供消費者付款換取商品或服務。輸入載具是一種透過可識別的物件，如會員卡、悠遊卡、手機電話號碼等，將電子發票歸屬於消費者。輸出載具則是能協助消費者處理電子發票的裝置，如智慧型手機、KIOSK、個人電腦等。

確定商業交易成功後，賣家電腦將製作電子發票，然後傳輸到台灣電子交易平台，以供查詢審核轉移等商業運用。如圖 1 所示，電子發票商業流程包含兩項程序，即電子發票產生程序和電子發票處理程序。敘述如下：

1) 電子發票產生程序

產生電子發票主要有四個步驟，如圖 1 中步驟(G1)到(G4)。亦即，消費者結帳付款後，POS 端將取得輸入載具的識別碼以製作電子發票。隨後 POS 端綁定電子發票與消費者的載具，並將交易明細紙本提供給消費者。需注意綁定後的電子發票稱為具識別性的電子發票。最後 POS 端上傳具識別性的電子發票至電子發票平台。

2) 電子發票處理程序

電子發票處理程序提供消費者處理查詢、審核、傳輸交易記錄等功能。然而消費者需要使用輸出載具，才能處理電子發票平台上的電子發票。圖 1 中顯示電子發票處理程序包含三個步驟，分別為

(P1)到(P3)。亦即消費者先透過輸出載具登入電子發票平台。接著輸出載具根據消費者所提供的輸入載具資訊在電子發票平台上處理電子發票。最後電子發票平台傳回處理結果給輸出載具。

然而，這些程序存在兩個問題。第一，POS 端和載具之間主要採用 RFID 或紅外線等較差傳輸速率的通訊技術。故無法提供完善的隱私保護和有效率地將電子發票整合進消費者的個人財務系統。第二，為了消費者立即檢視交易明細，交易明細仍需以紙本方式產生，進而無法達成電子發票無紙化的目標。

3. 載具與通訊技術之效率分析

因應第二章所描述目前台灣電子發票系統的兩個問題，本節探索並分析各種可行解決方案和效能。

3.1 載具與銷售點系統之間的通訊技術

目前 POS 端和載具之間主要採用的讀取機制為紅外線或 RFID 來交換製作電子發票所需資訊。由於這兩技術的低傳輸速度導致無法提高台灣電子發票系統效率，進而阻礙台灣電子發票系統的發展。因此，表 1 探討各種可行性通訊解決方案，包括 LTE、NFC、Bluetooth 4.0 和 Wi-Fi。考慮的因素有傳輸頻段、傳輸速率、傳輸距離、啟動時間、隱私保護機制，及通訊成本。

表 1 無線通訊技術之比較

	LTE	Bluetooth 4.0	Wi-Fi	NFC
Transmission Frequency Band	1.9GHz~2.1GHz	2.4 GHz 2.5 GHz	2.4 GHz	13.56 MHz
Data Transmission Rate	Upload 64 Kbps Download 2 Mbps	Approximately 1 Mbps	54 Mbps	424 Kbps
Transmission Distance Effectively	3000 M	Approximately 50 M	Approximately 100 M	0.2 M
Start-up Time	> 1 s	300 ms	500 ms	100 ms
Privacy Protection Mechanism	User-Defined	128-bit AES & User-Defined	User-Defined	Secure card IC
Communication Fee	High	Free	Free	Free

如表 1 所示，使用 LTE 會因載具和 POS 端間須透過基地台來傳遞資料而有較長的時間延遲。另一方面，由於 LTE 須使用授權使用頻段(license frequency band)，故在交換電子發票時需承擔額外的資料傳輸費用。Bluetooth 和 Wi-Fi 兩技術需要長時間的啟動程序以搜尋無線訊號頻率和配對。相對之下，NFC 除了不需要額外頻道掃描時間來配對 POS 系統與行動裝置，同時也提供高傳輸速率來支援交換電子發票時所需的隱私安全機制和財務整合功能。根據以上分析，NFC 是最合適且便利的電子發票系統通訊技術。

3.2 載具之效率分析

本節探索各種新輸入載具和輸出載具的方案以解決當前電子發票架構中消費者仍然需要索取紙本查看交易明細的不便性。

表 2 與表 3 為各式輸出與輸入載具之分析。輸入載具與 POS 系統溝通方式可歸類成兩種類別，分別是接觸式與非接觸式。接觸式意指卡片需要透過讀取器識別；而非接觸式則是可以利用紅外線或其他無線電訊號來讀取。

同表 2 所示，接觸式輸入載具，例如會員卡、Smart Pay、iCash 等需要額外的讀取器、平台和顯示器處理電子發票。這代表接觸式輸入載具無法立即提供任何硬體支援將電子發票資訊整合到消費者的財務應用程式。非接觸式輸入載具讓賣家的 POS 系統利用無線電訊號通訊取得消費者資訊以製作並傳送電子發票。例如 POS 端可利用 RFID 與悠遊卡交換資料、或是透過紅外線來讀取手機條碼。雖然消費者能將載具資料顯示於智慧型手機螢幕上，並直接使用智慧型手機的攝影機將電子發票匯入個人財務管理應用程式，但消費者仍須學習並使用各種繁雜耗時的手機操作方式來取得電子發票。對於需要即時性與便利性的小額付款交易更顯得其操作方式的不便與耗時。NFC ID 是指嵌入在智慧型手機中的 NFC 晶片，消費者僅需點選確認鍵即可透過 NFC 協定直接接收來自 POS 端的電子發票並立即檢視手機螢幕上顯示的交易明細。綜合以上結論，如表 3 所示，不論是提供檢視交易資訊或者是處理電子發票，輸入載具採取 NFC ID 是最具效率的方式。

表 2 各種輸入載具之分析

	Member card	Smart Pay	iCash	Easy card	Phone code	NFC ID
Carrier identification code	Member code	Smart Pay code	iCash code	Easy Card code	Phone code	NFC ID
Administration / Manager	Specific stores	Bank	UNI-PRESIDENT corp.	Easy Card corp.	Financial Data Center	Financial Data Center
Where to apply carrier	Specific stores	Specific stores	Specific stores	Specific stores	at e-invoice platform	at e-invoice platform
Contact / Contact-less	Contact	Contact	Contact	Contact-less with RFID	Contact-less with infrared	Contact-less with NFC
Processing platform	KIOSK	PC or KIOSK	PC or KIOSK	KIOSK	Mobile phone, PC, or KIOSK	Mobile phone, PC, or KIOSK

表 3 不同的輸入載具與輸出載具之組合效率分析

Input-carrier / Output-carrier	Member card			Smart Pay			iCash			Easy card			Phone code			NFC ID		
	R	I	C	R	I	C	R	I	C	R	I	C	R	I	C	R	I	C
KIOSK	O	X	F	O	X	F	O	X	F	O	X	F	O	O	F	O	O	F
PC	O	O	L	O	O	L	O	O	L	O	O	L	O	O	F	O	O	F
Phone	X	X	X	X	X	X	X	X	X	X	X	X	O	△	F	O	O	F

R: Immediate review I: Integration C: Cost
O: Highly support △ :Acceptable X: Not support
F: Free L: Low

4. 系統實作

本章設計並開發基於 NFC 通訊技術之電子發票系統以驗證第三章的分析結果。該系統具備以下特色來解決目前台灣電子發票系統的問題：(1)使用者在交易完成後可立即透過手機螢幕檢視或處理電子發票，(2)採用 NFC 通訊技術來交換電子發票以確保消費者的安全隱私並快速便利地將電子發票整合進消費者的財務系統。

此系統包含配備 NFC 晶片的 POS 系統和智慧型手機。其 POS 系統是於 Microsoft Visual Studio 2010 C#環境下開發，而行動裝置則以 Android 架構開發[7]。以下小節分別展示系統規劃、系統架構和使用者圖形介面。

4.1 系統功能與規劃

如圖 2 所示，本研究開發之電子發票系統是由兩個介面端所建構，分別是 POS 端和 APP 端。POS 端提供製作電子發票和推送已轉換成互換格式的電子發票給消費者的功能。要注意的是，此互換格式是基於台灣財政資料中心所制定出的 XML 格式。資料編碼使用採用 base 64 來確保系統可使用各種中文異體字來顯示交易明細。資料傳輸可採用主動和被動的兩種 NFC 傳輸資料模式，即

- 主動模式：交易完成後，消費者將智慧型手機放置在 POS 端的 NFC 讀取器上接收電子發票。優點為改善資料傳輸的效率。
- 被動模式：與主動模式相比，消費者先將智慧型手機放置於 POS 的 NFC 讀取器上待 POS 端推送電子發票。優點為確保傳輸過程的安全性。

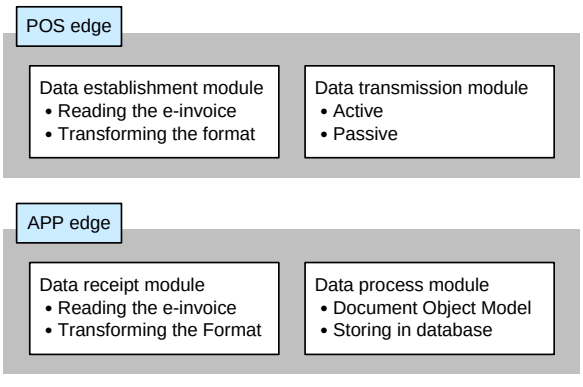


圖 2 系統功能

APP 端主要提供兩個功能：(1) 接收電子發票，與(2)檢視或處理電子發票。需注意，本系統使用 Document Object Model (DOM)的方式來接收或處理電子發票。這是因為在解析小型的 XML 文件時， DOM 能提供高於 Simple API for XML (SAX)的性能。

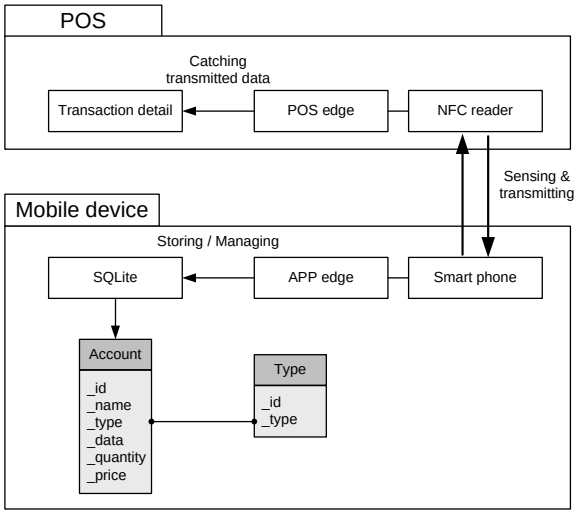


圖 3 系統架構圖

圖 3 為基於圖 2 所設計的系統架構圖，並包含 POS 和智慧型手機之間的運作流程。當中須注意，該架構的資料流需根據於行動裝置上的資料來設計，並遵循以下規則：

1. 「Account」及「Type」皆不可為空值的屬性。
2. 「Type」中的屬性「_type」須具唯一性。
3. 「Account」及「Type」皆採用屬性「_id」為主鍵。

4.2 使用者圖形介面

圖 4 和圖 5 分別為交易流程中 NFC 主動模式下，POS 端及智慧型手機的使用者圖形介面。其系統運作流程敘述如下：

1. 交易完成後，POS 端製作電子發票。
2. 消費者執行智慧型手機上的應用程式並點選應用程式中的「接收明細」按鈕以要求店家傳送電子發票。
3. 店家 POS 系統接收到消費者的要求後，傳送電子發票至消費者的智慧型手機。
4. 消費者確認收到電子發票並檢視交易明細訊息。
5. 通知電子發票傳送成功之畫面顯示於 POS 機的畫面上。

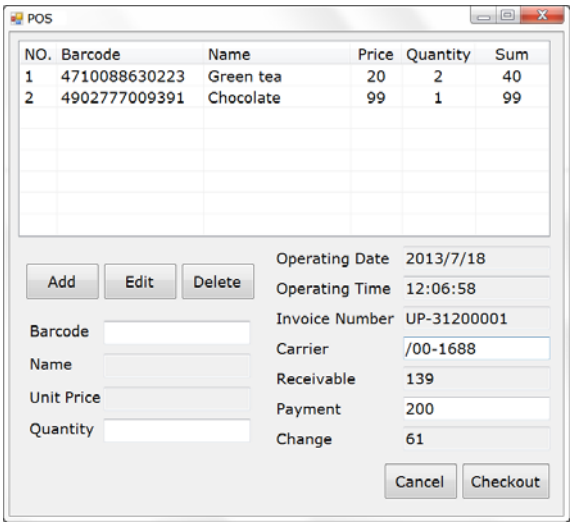


圖 4 POS 端 GUI



圖 5 APP 確認交易明細

5. 結論

本研究點出目前台灣電子發票系統的兩個問題：(1) 檢視電子發票的不便性和(2)交換電子發票資訊的通訊技術的低效率。為了解決這兩個問題，本研究探索與評估各式行動性載具和通信技術的解決方案和效能。根據分析，配備有 NFC 晶片的智慧型手機能提供最佳的檢視與交換電子發票效率。本研究更進一步設計並開發具有 NFC 功能的 POS 端和智慧型手機的電子發票系統平台來驗證其分析。該系統同時提供電子發票系統開發商一個測試平台。利用此系統可讓系統開發者迅速開發相關的 NFC 電子發票系統和應用程式並驗證其可行性與執行效率，進而推廣台灣電子發票系統於各個領域上的應用。

參考文獻

[1] Bluetooth Technology Special Interest Group. (2013, February). Specification Adopted Documents. Retrieved July 16, 2013, from https://www.bluetooth.org/en-us/specification/adopted-specifications

[2] Magdalena Nohrborg. (2013). LTE Overview [Online forum comment]. Retrieved July 16, 2013, from http://www.3gpp.org/Technologies/Keywords-Acronyms/LTE

[3] Near Field Communication. (2013). About Near Field Communication. Retrieved July 16, 2013, from http://www.nearfieldcommunication.org/about-nfc.html

[4] Regulations Governing the Use of Uniform Invoices. (2012, December 14). Law. Retrieved July 16, 2013, from

[5] Taiwan Ministry of Finance. (2013a). Use of Carrier. Retrieved July 16, 2013, from https://www.einvoice.nat.gov.tw/index!easyKnow?CSRT=16897659391144226479

[6] Taiwan Ministry of Finance. (2013b). E-Invoice Platform. Retrieved July 16, 2013, from https://www.einvoice.nat.gov.tw/

[7] Taiwan Ministry of Finance. (2013c). Electronic invoicing application API Specification Version 1.4. Retrieved July 16, 2013, from https://www.einvoice.nat.gov.tw/home/DownLoad?fileName=f1371195138997.pdf&CSRT=16897659391144226479

[8] Taiwan Ministry of Finance. (2013d, April 30). Integration of electronic invoice of the actual situation. Retrieved July 16, 2013, from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&ved=0CDkQFjAB&url=https%3A%2F%2Fwww.einvoice.nat.gov.tw%2Fhome%2FDownLoad%3Bjsessionid%3DflgSR5vJG2y1tkZshpGxbpxqTCgxBQKnnnj2PK79G1l62GvVfqyn!147166878%3FfileName%3Df1367301092297.pdf&ei=rMTkUeTNCcGIkwWDhIDoAQ&usg=AFQjCNHybP76_6rLjMJBnXYWXqbDwMTaUA&sig2=HD_IViUOyGXYpl1efNPsCA

[9] Taiwan Ministry of Finance. (2013e, July 15). Electronic invoice statistical information in the consumer channel. Retrieved July 16, 2013, from https://www.einvoice.nat.gov.tw/index!showDataStatistics?CSRT=16897659391144226479

[10] The RFID Network. (2011, October 24). What is Radio Frequency Identification? Retrieved July 16, 2013, from http://rfid.net/basics

[11] Wireless Networking in the Developing World, Third Edition. (2013, February). Retrieved July 16, 2013, from http://wndw.net/pdf/wndw3-en/wndw3-ebook.pdf

基於影像分析技術之自動化水位偵測警戒系統

曾建澔　羅世瑋　陳倫奇　吳志泓　林芳邦
國家高速網路與計算中心
{c00how00, c00swl00, casper, jhwu, fplin}@nchc.narl.org.tw

摘要

近年來全球受極端氣候變遷的影響下，災害規模不斷擴大、災害事件也急遽攀升，因此，防災議題便顯得受到重視。傳統監視系統（Surveillance System）已逐漸導入，以期可遠端掌控災情。雖然功能不斷地更新，但是隨著災害安全事件的日趨攀升，監視系統數量不斷增加，透過人工監看方式已經趕不上災情變化速度。另一方面，傳統監視系統，在面對惡劣環境下，經常因光影變化、雨水、霧氣等影響因素，造成影像模糊或是物件資訊損毀，使得後端防災應變延誤或是誤判之可能性。

本篇論文提出使用影像分析偵測技術，運用經濟部水利署所提供全台灣主要河川的影像監測資料進行自動化水域及水位即時偵測分析。影像分析技術主要利用區域成長法（Region Growing）與直線擬合法（Line Fitting）之應用，可以有效地克服惡劣環境所造成的影像光影變化之影響。因此，利用前端影像分析技術所得之偵測結果，分別導入防災資料計算模組，並基於經濟部水利署委託國家高速網路與計算中心所發展之水情監控平台，以達到自動化即時偵測通報之成效。

關鍵詞：監視系統、影像分析、區域成長、直線擬合、防災

Abstract

In recent years, the global under the influence of extreme climate change, disaster scale expands unceasingly, disaster events are rising sharply, and therefore, disaster prevention issues appear. Traditional monitoring system function while constantly update, but with the growing number of cameras and disaster safety events, surveillance system function has not apply the use by human beings. Traditional disaster monitoring devices, while operating in a harsh environment, often influence by changes of light, rain, fog, etc. As the result, the monitor images are often blurred or damaged, which increase the possibility of error judgment or delay of hazard mitigation process.

In this paper, we propose the detection technology for image analysis in hazard mitigations, the use of the ministry of economic affairs water conservancy office provided by Taiwan main rivers automated image monitoring data of water and water level real-time detection analysis. The image analysis technologies are mainly using two methods including: Region Growing and Line Fitting that can effectively overcome the bad environment caused by the image with the change of the light and shadow effects. Therefore, the detection results of the front-end image analysis technology, disaster prevention information calculation module, and the flood monitoring platform developed by National Center for High-performance Computing are used to achieve the automation of real time hazard detection and notification.

Keywords: Surveillance system, Image analysis, Region growing, Line fitting, Hazard mitigations

1. 前言

在 2009 年 8 月，莫拉克颱風為台灣各地帶來豪雨，尤其是中部山區阿里山氣象站測得之總雨量高達 2,748mm（連續 72 小時），並造成台灣各地受到巨大的災害[1]。然而，每年五月至十月正是台灣的梅雨季節，該期間因受到對流雲系之影響，常會引發短時間所造成的劇烈豪雨，導致部分河川或鄰近沿海的低窪地區河水氾濫，造成人民傷亡與財產損失。因此，如何在這些主要河川及具低窪災害潛勢區域導入各項前瞻技術之自動化監測系統、偵測通報系統及防災應變系統等，將傳統的人工水情監測作業進化成自動化即時監控平台，已成為近年來各界對於水情災害防治的重要發展課題之一。

經濟部水利署目前已在全台灣主要河川、水庫、抽水站及中下游的低窪地區等，建置高達 400 多個影像監測站，透過人力進行 24 小時輪班監視[2]。然而，對於監控人員在面對如此巨量之監測影像，無論是資料比對、災害通報等作業，將造成人力負擔或人為判讀之主觀性誤差。目前傳統對於水情監測預報作業，大多皆以大範圍區域的分析與預報為主，但是對於地方性河川的自動化即時水位偵測與警戒回報機制仍較為缺乏[3, 4]。倘若能進行地方性河川的水情監測系統，並透過監測資料的影像分析技術，導入防災資料計算模組，使得有效提升地方區域性之河川防災應變行動。

本論文使用經濟部水利署於高雄市田寮區崇德橋河段與楠梓區典寶溪河段的監視站影像資料作為驗證，主要選其中下游低窪地區作為測試案例，透過前端的監測資料進行影像分析與物件偵測技術，分別利用區域成長法（Region Growing）來進行河川水域之範圍偵測、直線擬合法（Line

Fitting）用於水位之高度偵測。利用該影像分析技術，可以有效地克服惡劣環境所造成的影像光影變化之影響，並精確地進行水位偵測之辨別。因此，藉由前端提出之影像分析與偵測技術，所得之水位辨別結果，導入後端防災資料計算模組，並透過國家高速網路與計算中心所發展出針對全國河川、水利設施及易淹水地區的水情影像監控系統平台作為災害警戒之決策[5, 6]，藉以提升自動化水位即時偵測通報之成效。

經由實例測試結果顯示，透過前端影像分析技術於水情監控平台，可以精確地偵測水位狀態，並有助於提升自動化預警系統之成效與降低監控人力之負擔。

2. 數位影像分析

自動化影像監測系統中，首要問題是環境光源的影響。在面對惡劣環境下，造成前端監測影像光影的劇烈變化，如果採用傳統的背景相減法（Background Subtraction），將無法有效地偵測前景水位之高度變化，導致後端監控系統誤判之可能性。為了進一步解決環境光源變化之監測影像，本論文將採用以下兩種影像分析處理技術，分別為區域成長法（Region Growing）來進行河川水域之範圍偵測、直線擬合法（Line Fitting）用於水位之高度偵測。

2.1 區域成長法

本節採用之區域成長法有兩個特點，第一為多點成長：可採用一個以上的起始點最為種子；第二為反向刪除種子：用以過濾背景中的自然物件如天空、白雲、建築等[7, 8]。因此，影像分割中的區域成長法可將監視影像中的水域物件分離出來，並以水域範圍作為自動監控程序的目標物件，加入可調控之預設虛擬水位警戒點，當水位擴大到警戒點時會自動計算出警戒程度值（以百分比%呈現），預設超過 80%則發出報告。水域偵測流程如圖 1 所示。

河川監控影像首先經過影像前處理器轉換為灰階影像，接著以影像分割技術，將水域物件分離出來，本文所使用的分割方法為區域成長法，其處理流程如下式(1)至(4)所示。

$$\bigcup_{i=1}^{n} R_i = R \tag{1}$$

where R_i is a connected region, i = 1,2,...n

$$R_i \cap R_j = \Phi, \quad \text{for all i and j, i} \neq \text{j} \tag{2}$$

$$P(R_i) = TRUE, \quad \text{for i} = 1,2,...\text{n} \tag{3}$$

$$P(R_i \cap R_j) = FALSE, \quad \text{for any adjacent region } R_i \text{ and } R_j \tag{4}$$

其中 R 為整張影像總和，R_i 為各個可能的分割區域，且各個分割區域不可與其他分割區域重疊如式(2)，當鄰近點滿足分割區預設條件則加入式(3)；反之則計算停止，如式(4)。區域成長計算流程如圖 2 所示。

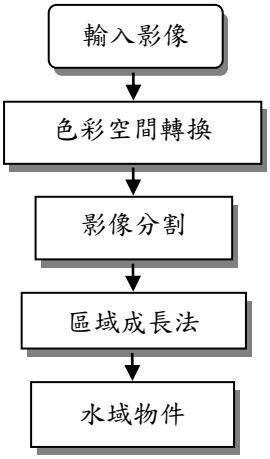


圖 1 水域物件分割之影像分析流程

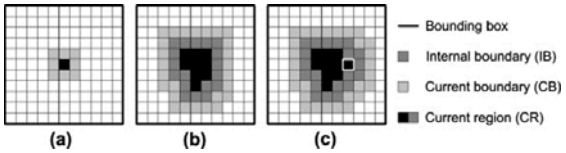


圖 2 種子起點的區域成長法[9]

圖 2 顯示 IB 為區域內部邊界，CB 為邊界，CR 為目前所成長之區域。圖 2 (a)利用設定一個或二個以上的種子作為區域成長的起始位置，與該種子相鄰之像素會依照預設條件進行擴張，直到相鄰的像素都無法滿足條件為止，最終的成長範圍即是所分割的區域。

設置種子點作為區域分割之起始點如圖 3 所示，分別設定了水域分割種子與背景分割種子，分別為紅色與藍色箭頭所指。綠色實線所框範圍為初步分割出來的水域物件。

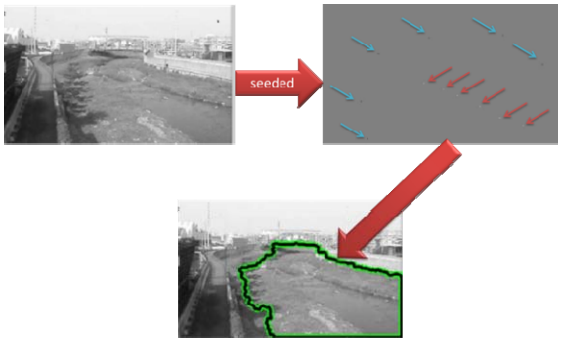


圖 3 典寶溪監測影像畫面為例，紅色箭頭所指為水位分割起點，藍色箭頭所指為背景分割起點

2.2 直線擬合法

本節使用直線擬合法主要應用於楠梓區典寶溪河段之測試案例，偵測流程分為以下四個步

驟：影像前處理、影像增強、ROI 擷取、偵測計算。圖 4 為本案例之水位偵測與方法流程。

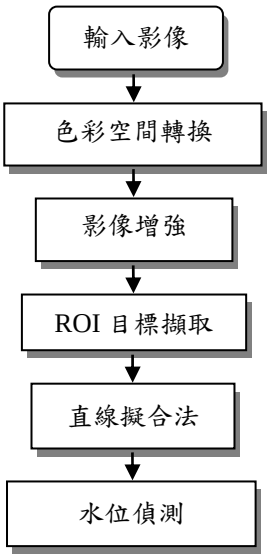


圖 4 水位高度偵測之影像分析流程

一、影像前處理

一般影像可表示為一個二維的數學連續函數關係 $I(x,y)$，其中變數 x 與 y 為空間座標（Region Growing），I 則是表示任意一對空間座標 (x,y) 的振幅，稱為影像資料在該點的亮度（intensity）或是灰階（gray-level）[10]。然而，為了提升影像計算之分析效率，茲將本影像測試案例由 RGB 色彩影像轉換為灰階影像，如圖 5 所示。一般而言，人類視覺對於綠色最為敏感，其次依序為紅色與藍色，故定義出 RGB 色彩影像轉灰階影像之計算公式，如式(5)所示：

$$\text{Grayscale value} = 0.299R + 0.587G + 0.114B \quad (5)$$

其中 R、G、B 分別為監測影像中紅色、綠色及藍色的像素深度值。



(a) 原始影像　　(b) 灰階影像

圖 5 色彩空間轉換

二、影像增強

由於影像監測站所架設之攝影裝置皆位於戶外，易受到自然雜訊、光源不穩定、陰影干擾等因素，而影響監測影像品質。因此，在進行影像處理時，常會利用濾波器過濾雜訊或是強化影像對比度，使得增強後之影像會比原始影像更適合進行物件分析。本研究將採用直方圖等化（Histogram Equalization）之時域影像增強方法，其目的乃是將灰階分佈集中於某微小區間的影像均勻展開，以增強影像之對比度（詳圖 6）。直方圖等化的轉換函數定義如下：

$$s_k = T(r_k) = \sum_{j=0}^{k} \frac{n_j}{n} = \sum_{j=0}^{k} p_r(r_j),\ \mathrm{k} = 0,1,2,...,255 \quad (6)$$

其中，r_k 是輸入影像灰階；s_k 為經直方圖等化後的輸出影像灰階；n_j 是第 j 種灰階的像素數目；n 是整張影像的像素數目；$p_r(r_j)$ 是影像灰階 r_j 的離散機率密度函數。

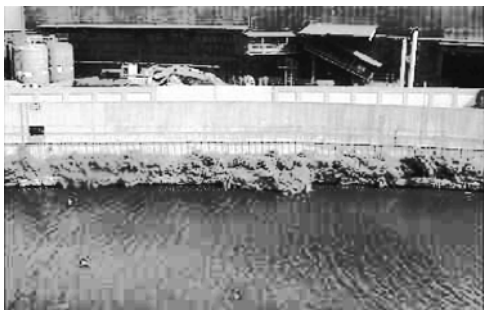


圖 6 直方圖等化影像

三、ROI 擷取

藉由上述影像增強，將測試影像中的河面或是主建物等相關特徵變得更為明顯，尤其是主建物圍牆與河面交界處之陰影，影像對比度提升不少。這些特徵對於擷取 ROI 區域之目標物件與物件分析過程（詳圖 7），將有助於提高物件偵測之精確度。

本測試案例之水位交界面，利用影像增強後，可以發現主建物圍牆與河面交界處會有明顯的陰影，因此，可以藉由設定一灰階門檻值，將 ROI 目標區域篩選出水位交界處之可能點。然而，被保留的像素位置將落在主建物圍牆與河面交界處附近。

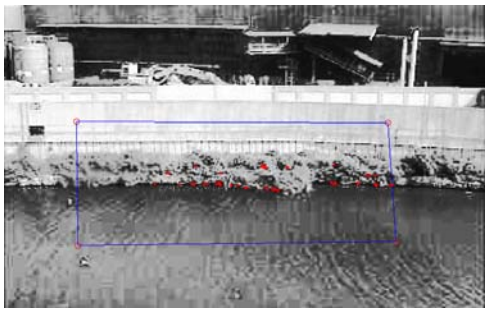
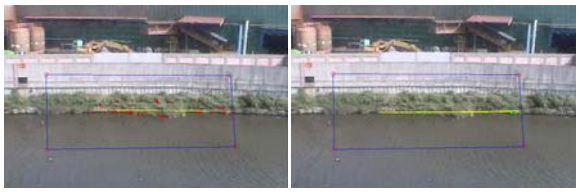


圖 7 ROI 目標區域擷取

四、水位偵測

本章節將應用直線擬合法做為水位偵測之決策。因此，利用 ROI 區域求得位於主建物圍牆與河面交界處之各點像素位置，透過直線擬合方程式[11, 12]，使得這些像素點位置到這條水位線的距離平方和為最小。然而，為了達到最佳水位線，本論文執行兩次直線擬合（詳圖 8），使得計

算結果更能趨近於實際水位高度。



(a) 一次直線擬合　　(b) 二次直線擬合

圖 8 應用直線擬合法於水位偵測結果

3. 實驗結果

本論文使用經濟部水利署於高雄市田寮區崇德橋與楠梓區典寶溪兩河段處的影像監視站，利用此中下游易淹水之低窪地區的實例影像資料作為前端影像分析技術的應用測試與驗證範例。然而，所選用之影像資料將挑選惡劣環境所造成監視畫面因光影變化、雨水、霧氣等影響因素，而易造成人為誤判之條件。以下測試案例將分別利用區域成長法（Region Growing）來進行河川水域之範圍偵測與直線擬合法（Line Fitting）用於水位高度之警戒偵測來做說明。

3.1 水域物件分割

本驗證案例使用 2010 年 9 月 19 日，凡那比颱風期間於田寮區崇德橋河段所拍攝的監測畫面。輸入畫面的整體時間為中午 12 點至下午五點，紀錄崇德橋下方水位逐漸升高之完整過程（如圖 9）。

圖 10 中經過使用者給予的 5 個成長起始點與 5 個刪除點分別以紅色與藍色箭頭指出。圖 11 展示了區域成長法對崇德橋水域的分割結果，分別取中午與下午兩個時間點進行測試，影像中的水域取出後以紅色輪廓表示。



圖 9 凡那比颱風期間，崇德橋下方河流隨時間淹漲之情形。（由上至下、由左至右依序排列）

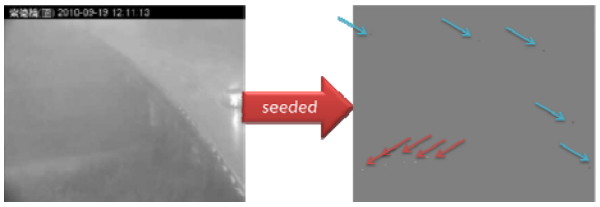
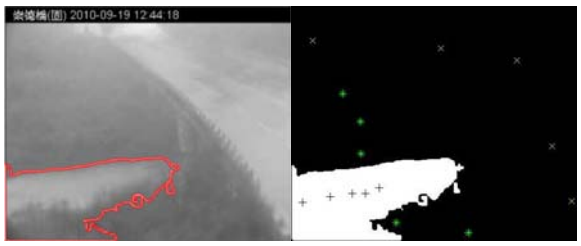
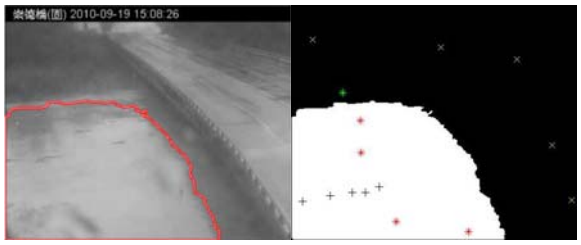


圖 10 區域成長之起始點與刪除點



(a) 中午時段監測畫面



(b) 下午時段監測畫面

圖 11 分別於中 12 點 44 分（上圖）與 15 點 08 分（下圖）所做的水域偵測結果。（十字標記為起始點，x 為刪除點，*為預設參考點）

測試結果顯示，本案例使用區域成長法可以針對不同場景做最佳化的種子點配置，強化水域分割的正確性。本方法同時增加了刪除背景的功能，減少以往背景容易被前景所過度成長的問題，並亦可有效去除水滴、水痕的雜訊，解決以往豪大雨造成畫面散滿水珠而發生錯誤分割之問題。

3.2 水位高度偵測

本驗證案例同為使用 2010 年 9 月 19 日，凡那比颱風期間於楠梓區典寶溪河段所拍攝的監測畫面，輸入畫面時間為下午 4 點左右。該日監測畫面因受颱風及豪雨影響，而造成影像嚴重受到雨水、霧氣干擾(如圖 12)，然而，經由影像前處理包括色彩空間轉換與影像增強，將物件資料的特徵強度提高，使得豪雨而造成河面漣起的波紋與主建物圍牆有明顯之對比。圖 13 則是透過灰階門檻值，將 ROI 目標區域篩選出水位交界處之可能分佈點。



圖 12 典寶溪河段暴漲之原始影像



圖 13 ROI 目標區域可能分佈點

將 ROI 目標區域篩選出可能的像素位置，運用直線擬合求得一條距離平方和為最小的直線。為了達到最佳水位線，本論文執行兩次直線擬合，使得計算結果更能趨近於實際水位高度(如圖 14)。圖 15 為二次直線擬合最小值之結果，標示出目前偵測的水位高度。結果顯示，利用二次直線擬合法可近似於實際水位之高度。



(a) 一次直線擬合　　(b) 二次直線擬合

圖 14 兩次直線擬合於水位偵測結果



圖 15 直線擬合於水位偵測結果

3.3 系統架構

目前現有的水情監測平台主要整合多重影像來源與多重串流技術與 GIS (Geographic information system)，水情監測平台上可快速的找出預觀測的監測站。本論文提出的影像分析技術導入於運行中的水情監控平台，其架構如圖 16 所示，影像伺服器擷取所有監測站影像後，將影像資料先備份於影像資料庫，水位偵測模組則不斷地撈取影像資料進行水位偵測，由於影像監測站數量龐大，且水位偵測須即時的產出水位辨識結果，故水位偵測模組採用高速平行計算技術實作，以快速即時地提供使用者端即時與方便的研判作業[13, 14]。

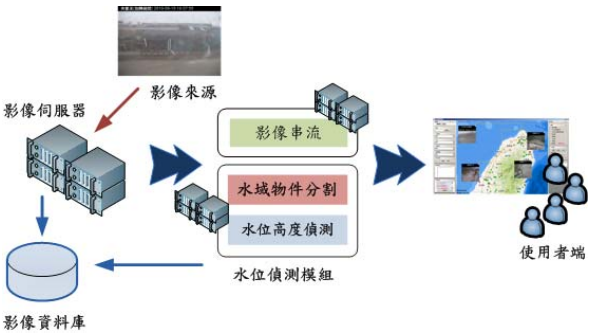


圖 16 基於水位偵測之水情監測平台架構

4. 結論與未來研究

針對傳統監控裝置，在面對惡劣環境下之影像處理技術，常常會因影像受到破壞或是光影變化等因素，而造成後端防災應變延誤或是誤判之可能性。為了有效處理惡劣環境所造成影像計算誤判之結果，因此，本篇論文提出使用影像分析偵測技術，運用經濟部水利署所提供全台灣主要河川的影像監測資料進行自動化水域及水位即時偵測分析。

實例測試結果顯示，藉由前端影像分析技術進行兩種河川環境之應用：區域成長法進行崇德橋河段水域之範圍偵測、直線擬合法進行典寶溪河段水位之高度偵測，可以有效地克服惡劣環境所造成的影像光影變化之影響。因此，利用前端影像分析技術所得之偵測結果，分別導入防災資料計算模組，並基於國家高速網路與計算中心所發展之水情監控平台，以達到自動化即時偵測通報之成效。

未來將持續加強影像計算之判斷法則，例如定義草木與水域之模糊邊界、太陽眩光與車燈等光線之散射等影響因素，將有助於影像計算的物件識別及目前正在開發的整合行動計算防災監控的決策應變。另一方面亦將整合高速計算相關技術，可透過影像分析於眾多監視影像中自動找出可能淹水之畫面，進而結合 GIS 自動找出可能淹水之地點，減少人工判讀，有助於防災應變之即時性。

參考文獻

[1] Y. F. Wang, ”Enhanced Actions for Water Disaster Warning System and Evacuation,” Southeast Asia International Program(SEAIP), 2009.

[2] 經濟部水利署防災應變格網作業平台，[Online]. Available: http://fmg.wra.gov.tw/.

[3] V. Bacu and D. Gorgan, “Resource Measurements for Water Detection Algorithm in MedioGrid Architecture,” 6th International Symposium on Parallel and Distributed Computing, Hagenberg, pp. 1–17, July 2007.

[4] E. Cheng, R. X. Zhang and F. Yuan, “Automatic Detection and Assessment System of Water Turbidity based on Image Processing,” Journal of Electrical Engineering, vol. 11, pp. 1506–1513, March 2013.

[5] 國家高速網路與計算心－防洪減災格網，[Online]. Available: http://www.floodgrid.nchc.org.tw/

[6] 經濟部水利署水情影像監控中心，[Online]. Available: http://hmerg.nchc.org.tw/sensornet/sensornet_center

[7] W. Cui, Z. Guan and Z. Zhang, “An Improved Region Growing Algorithm for Image Segmentation,” International Conference on Computer Science and Software Engineering, pp. 93–96, Dec. 2008.

[8] M. M. S. J. Preetha, L. P. Suresh and M. J. Bosco, “Image segmentation using seeded region growing,” International Conference on Computing Electronics and Electrical Technologies (ICCEET), Kumaracoil, pp. 576–583, March 2012.

[9] J. P. Monaco, J. E. Tomaszewski, M. D. Feldman, I. Hagemann, M. Moradi, P. Mousavi, A. Boag, C. Davidson, P. Abolmaesumi, A. Madabhushiemail, “High-throughput detection of prostate cancer in histological sections using probabilistic pairwise Markov models,” Medical Image Analysis, vol. 14, pp. 617–629, 2010.

[10] R. C. Gonzalez, and R. E. Woods, Digital Image Processing, 3rd ed. Prentice Hall, 2008.

[11] H. Qjidaa and L. Radouane, “Robust line fitting in a noisy image by the method of moments,” IEEE Trans. On Pattern Analysis and Machine Intelligence, vol. 21, pp. 1216–1223, 1999.

[12] R. Hanek and M. Beetz, “The Contracting Curve Density Algorithm: Fitting Parametric Curve Models to Images Using Local Self-adapting Separation Criteria,” International Journal of Computer Vision, pp. 1–38, 2004.

[13] 吳志泓，鍾德霖，常若愚，游輝宏，林芳邦，蔡惠峰“行動通訊於防救災作業之應用－以 J2ME 為開發平台,” TANET2007, 2007。

[14] 陳倫奇，吳志泓，林詠彬，林芳邦“行動計算於防災之應用,” TANET2012, 2012。

I Know You: 智慧型家庭網路影音傳送系統

黃宏宗[1] 林正倫[1] 阮明英[1] 胡誌麟[1] 蘇奕宇[2] 劉炳傳[2]
[1]國立中央大學通訊工程系
[2]台灣工業技術研究院
{101523047, 101523036, 101523601, clhu}@cc.ncu.edu.tw; {pioneersu, flashliu}@itri.org.tw

摘要

本論文在家庭網路的環境下，提出一套新穎的智慧型家庭網路影音傳送系統，提供使用者在家庭網路環境中不受居家空間限制的多媒體影音服務。此系統之設計整合 UPnP 網路內容分享平台、人臉辨識及人機互動介面設計等技術，並搭配家庭成員資料庫之建置，使得家庭成員在不同居家空間之間移動時，系統可以即時感知家庭成員所在位置的變換，提供個人化的影音傳送及播放服務。在實作與展示中，我們經由實機展示來具體呈現出這一套智慧型家庭網路影音傳送系統的功能，達成家庭網路環境下具隨意、隨地及隨選裝置特性之即時性與個人化的多媒體影音傳送服務。

關鍵詞：UPnP，人臉辨識，多媒體影音，家庭網路，數位家庭

1. 前言

隨著家庭寬頻網路的滲透率提升，各式新興網路多媒體裝置的推成出新，數位家庭的理念因應而生，也帶動網路多媒體裝置產品的迭代出新。在廣泛的數位家庭應用範疇中使用者最感興趣的主要是在家庭影音娛樂、家電自動化控制及居家安全監視。就最貼近消費市場的家庭影音娛樂而言，家庭成員希望可以在家中不同的空間，利用各式網路家電來和家人及朋友分享各種影音內容，也希望網路家電裝置能一改舊往只能被動的接收指令，可以主動地提供家庭成員有關家庭網路中最新分享的或是經常播放的影音媒體資訊。

本文提出的智慧型家庭網路影音傳送系統，採用符合國際數位家庭產業組織 Digital Living Network Alliance (DLNA)所規範的 Universal Plug and Play (UPnP)相容性技術[1]，在 UPnP 平台架構上發展 UPnP AV 多媒體影音內容分享服務，讓家庭網路環境下的網路裝置，可以發現彼此的存在、互相溝通及分享各自擁有的多媒體檔案。另一方面，對於家庭成員在居家環境中的移動和裝置使用習慣，此一智慧型系統支援多媒體內容同步播放及顯示服務，這服務的設計是在多媒體播放器裝置端結合人臉辨識技術，偵測靠近裝置的人臉影像畫面，辨識每一位家庭成員的身份。當使用者在居家空間內移動時，鄰近的多媒體播放器裝置可以發現某一使用者進入它的服務範圍，並立即在家庭網路中發佈這項消息，若家庭網路中有其他正在服務這位使用者的多媒體控制器，它將從網路中得知使用者位置的改變，隨即啟動同步轉置和播放功能，讓多媒體伺服器把正在播放的多媒體內容，改傳送到使用者當下所在位置附近的多媒體播放器端。

因此，本文所提出的智慧型家庭網路影音傳送系統的設計，可相容於 DLNA 和 UPnP 數位家庭產業標準，並在多媒體播放器裝置端結合人臉辨識技術，使得系統可辨識每位家庭成員，提供個人化的多媒體影音服務之目的。系統雛形的開發與實作部分，將是以消費市場既有的網路多媒體裝置為應用載具，實機展示出該系統的功能，讓使用者在家庭網路環境下體驗不同於以往的家庭網路多媒體影音服務，帶給使用者全新的使用者情境和體驗。

本論文的章節組織如下所述，第 2 章提出相關文獻與技術，第 3 章說明系統架構與功能，第 4 章描述系統雛型設計與實作，最後第 5 章總結本文的研究成果和展望。

2. 文獻探討

近年來許多高階嵌入式網路通訊裝置除了配備高級的資料處理器之外，更具備有相機模組及多媒體處理器的升級，因而有越來越多的影像辨識與 UPnP 的應用服務陸續提出，以下我們將分別對 UPnP、影像辨識和這兩項技術結合之應用作探討。

2.1 UPnP 之應用

[2]首先在家庭網路的環境下引薦入行動多媒體伺服器一角色，成功的透過 UPnP AV 模式，以簡易的網路遠端操控取代傳統的手動繁瑣操作，把行動裝置上的影音媒體轉置到網路電視上播放，展現出行動影音媒體分享的使用情境。[3]提出一套結合 UPnP 和 P2P 的家庭多媒體閘道器設計，讓支援 UPnP 的多媒體播放裝置可以直接執行來自外部網路的 P2P 檔案下載及串流服務，使得媒體來源不再侷限於家庭網路內部的媒體內容，延伸至網際網路上龐大的 P2P 多媒體內容來源。[4]則是在 UPnP 裝制架構上整合近場通訊技術(NFC)，提出一個新穎的手勢輔助的遠端操控方法。上述為本文作者先前

發表的部分研究成果，讀者可參閱[2]-[4]所屬的參考文獻，將可清楚 UPnP 技術與應用發展。

2.2 影像辨識之應用

影像辨識知識及技術應用相當廣泛，如車牌辨識、手勢辨識、人臉辨識等。如[5]所述，智慧型互動應用可分為兩類：人臉辨識在「智慧型環境」下的應用，以及人臉辨識在「智慧型裝置」上的應用。以上兩類是基於人的局部外貌之特徵，比對過去或事先已註冊的人臉圖資，辨識使用者的身份。然而由於影像辨識的運用相當仰賴裝置載具的資料計算能力，因此過去的應用範疇較少套用在消費性電子產品上，近年來許多高階消費型電子終端裝置，如行動通訊裝置、平板電腦及電視，其硬體規格大幅提升亦包含視訊模組，基於這類裝置的影像辨識技術與應用將很有發展性，因於人是這類裝置的主要操作者，人臉辨識技術的應用特別值得留意。

2.3 UPnP 結合影像辨識之應用

由於在網路家庭的環境下可能同時存在許多的媒體播放裝置，透過 UPnP 所發現的網路裝置名稱經常是製造商所給定的名稱，對消費者來說這類的命名方式並非直覺或主觀上可以輕易辨認出所屬的特定裝置，因此[6]提出一個較直覺的裝置操作方式，透過 UPnP 結合電腦視覺，讓使用者在行動裝置鏡頭所拍攝的畫面中做裝置的選擇，然後再對該裝置提供影音媒體分享。

由以上的討論中可以看出，儘管 UPnP 和人臉辨識兩者雖非全新提出的技術，但是至今尚未有具體整合兩技術並應用在數位家庭環境下的網路媒體服務，是以本文所擬之系統旨在整合兩大技術並設計新穎的多媒體影音轉送服務。

3. 系統架構與功能

以下將會詳細說明此系統的功能設計和運作方式，3.1 節描述系統架構及各子系統的功能設計，3.2 節將從系統面說明整體的運作流程。

3.1 系統架構

如圖 1 所繪，本系統的應用範圍為一個包含有網路多媒體媒體家電、個人電腦、網路儲存設備(通稱為多媒體網路裝置)的家庭網路環境。通常這種網路是由多媒體網路裝置透過固接網路或無線網路介面連接至路由器所形成的小型區域網路，多媒體網路裝置將可以從路由器取得 IP 位址，並利用這些裝置之間共同的 UPnP 通訊協定，以 IP 網路封包傳送與接收取得不同裝置的資訊、亦經由 UPnP 訊息來操控裝置的功能。另外，多媒體網路裝置可經由視訊模組的功能，擷取前方的影像交予後方軟件進

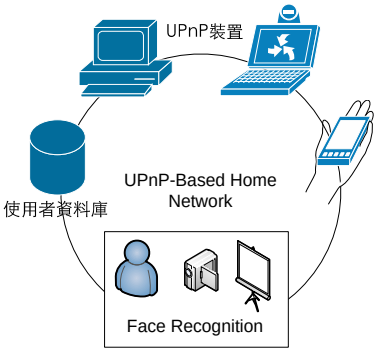


圖 1 系統環境示意圖

行影像辨識，辨識所得的資訊將可提供給區域網路中各個裝置使用。

如圖 2 所示，系統架構的組成包含四個子系統功能模組：影像辨識、控制端、媒體播放器、使用者資料庫。

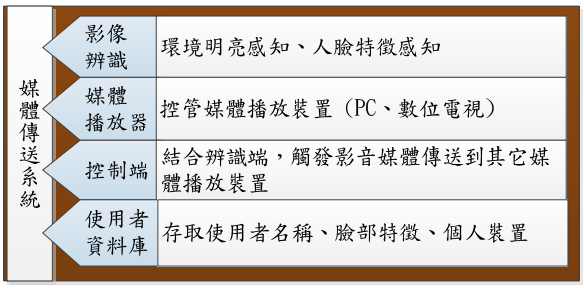


圖 2 系統組成之模組

3.1.1 影像辨識

影像辨識除了具備對人的感知能力外，也具備對環境明亮度的感知能力。在此模組採用 P.Viola 和 M.Jones 所提出的人臉偵測快速演算法[6]，這個演算法的運行包括三個步驟：第一為積分影像(Integral Image)，使用一個中間值代表一個影像，可以很迅速地計算矩形特徵，在 Viola 的系統中，每個矩形特徵值的計算，最多只需要從積分影像中取 9 個元素做加減運算，這就是其快速的原因。第二為弱分類器與 Adaboost 疊代演算法，透過從大量的弱分類器中選取最具有分類意義的來組合成強分類器，[7]使用矩形特徵作為分類的依據，共使用四種矩形特徵。第三步驟則是層級分類器，一個影像會有很多個子框架，層級分類器則由許多分類器組合而成，每一層都是由上述演算法訓練所得到的一個強分類器，配合閾值，使其排除了眾多子框架中非人臉的樣本。

[8][9]提出幾套著名的人臉辨識的方法，但考慮到嵌入式裝置有限的運算能力，以及家庭成員的組成人數不高，此處尚不需要使用過於複雜的方法，而是採用統計學中常被拿來做常態分佈比對的 Bhattacharyya 距離，即可符合辨識之所需，接著再搭配使用者資料庫後，此影像辨識模組能夠判斷其是否為家庭成員，若為已註冊的家庭成員，則針對該成員提供個人偏好的影音服務。

3.1.2 媒體播放器

媒體播放器是建構在本機端內部多媒體播放引擎之上的應用軟體和使用者界面，因此，媒體播放器可以蒐集本機裝置的資訊與媒體播放內容，系統的其他模組元件也將可已透過媒體播放器來間接操作多媒體播放裝置。

3.1.3 控制端

控制端可以藉由接收並解析家庭網路中由不同網路多媒體裝置所群播(Multicast)送出的封包，從中發現網路上存在兩種類型的 UPnP 裝置：第一為多媒體伺服器裝置(Media Server)以及多媒體播放裝置(Media Renderer)，當這些裝置離開時，控制端也可透過該裝置再次發出的群播封包得知其離開，並更新目前存在於網路中的裝置清單。

控制端能夠藉由 UPnP AV 服務，瀏覽各個多媒體伺服器本身儲存且願意分享出來的多媒體檔案目錄。對於 UPnP 多媒體播放裝置，控制端可以操控其播放狀態如：開始、暫停、停止以及播放進度。對於正在播放的多媒體內容，控制端可取得其檔案的 URI (Uniform Resource Identifier)，得知該檔案為哪一個多媒體伺服器所擁有以及所屬的媒體格式，除外，控制器也可以取得各個多媒體播放裝置可以支援的多媒體檔案類型及格式，經過比對檔案來源與接收端兩者之間的檔案處理與裝置播放能力是否相符，如此將可確保多媒體伺服器與多媒體播放器之間的相容性。

3.1.4 使用者資料庫

使用者資料庫紀錄家庭網路環境中使用者的註冊資訊。使用者第一次使用本系統時，須先拍攝照片並輸入使用者名稱以建立個人基本資料。完成後，可選擇在區域網路中常用的多媒體網路裝置和服務，以便本系統日後辨識出使用者時，可以立即提供使用者個人化的服務內容。

3.2 系統運作流程

關於本系統的運作方式，經歷一次完整的使用流程將包含：使用者註冊、進入偵測模式、後端資料相似度比對及提供個人化服務等階段；系統內部的運作則由影像辨識、控制端與使用者資料庫三個模組元件的互動來完成，圖 3 顯示其整體的運作。

影像辨識在此系統啟動後即隨之運作，藉由偵測裝置的鏡頭所拍攝到的即時影像，立刻透過快速演算法[6]篩選出人臉，與使用者資料庫內的人臉特徵去做相似度比對，之後會抓取該成員之姓名並顯示於偵測畫面中，表示系統核對成功之結果。使用者註冊時，亦會使用到此子系統，如同在偵測模式下一樣，當使用者按下擷取 ID 照後，鏡頭及人臉偵測相繼被啟動，當成功偵測出欲註冊成員之人臉特徵時，系統會切割出只有人臉特徵的資訊，此時該使用者可做確認來儲存其頭像資訊，以利與其他個人化設定做綁定。

控制端於本系統初始化時即開啟硬體的網路傳輸介面，接收區域網路封包，取得已加入的多媒體播放裝置。在使用者建立個人名稱和照片之後，控制端將區域網路中的裝置清單提供給使用者來選取慣用的裝置。之後，當影像辨識模組辨識出已註冊的使用者後，會將使用者名稱傳送至控制端，控制端向使用者資料庫以此名稱查詢相對應的裝置名稱，並且調用該裝置的影音服務，取得播放狀態和目前播放的內容。當控制端取得這些屬於特定使用者的資訊之後，將可以進一步控制對應的多媒體播放器，讓使用者可以決定是否接續播放方才在上一個裝置上尚未播放完的多媒體內容。

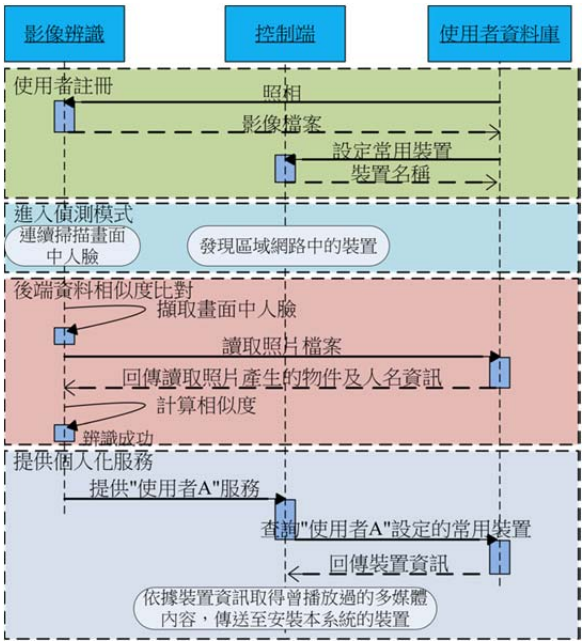


圖 3 元件互動

4. 系統雛型開發和展示

4.1 節說明系統開發平台與應用程式執行環境，4.2 節說明系統軟件的使用操作方式，4.3 節根據使用者情境的規劃，提出幾項實例以佐證之。

4.1 環境設備

此系統雛型的軟件研發採用 Java 及 C++程式語言，前者主要用於 UPnP 相關應用程式的開發，後者則是牽涉到 OpenCV 電腦視覺處理所需的軟體工作等。系統直接使用 Android 嵌入式行動終端裝置為，執行系統雛型所需的軟體程式和套件。以下兩小節敘述 UPnP 和影像辨識功能模組的實作方法。

4.1.1 UPnP on Android

此雛形的研發則利用 *Cling* Java/Android UPnP 程式函式庫及工具集，實作多項 UPnP 多媒體應用服務，例如：調用 AV Transport Service (AVT) 進行多媒體內容播放、瀏覽 Content Directory Service (CDS)的內容，以利於多媒體內容在區域網路中多媒體網路家電之間的傳送、轉置及播放。

4.1.2 OpenCV on Android

OpenCV (Open Source Computer Vision Library) 是一個跨平台的電腦視覺函式庫，原由一系列 C 函數和少量 C++函數構成，現今亦可用 Java 語言撰寫，並支援 Android 平台上軟體開發。OpenCV 可用於開發即時的圖像處理及計算機視覺等應用，它常被用於解決人機互動、物體辨別、圖像分割、人臉辨識、動作識別、運動跟蹤等圖像處理的問題。這部分的程式開發項目主要是在影像擷取、人臉偵測和辨識，以及圖像分割等，透過這些功能的串聯來實現系統感知使用者的出現和身份辨認等目標。

4.1.3 載具設備

圖 4 為系統雛型實作所使用的設備，標號 1 為一架網路電視，編號 2 是放置在網路電視上方，一架搭載 Android2.2 以上智慧型手機的影像偵測模組，編號 3 為家庭網路上各式的 UPnP 多媒體裝置，此處以筆記型電腦搭載 UPnP 軟體仿效之。



圖 4 系統雛型之環境設置

4.2 使用者操作流程

以下描述使用者在操作系統雛型的過程當中所執行的人機互動，如圖 5 所繪，這部分包含前端所產生的使用行為以及後端系統相對應的運作。

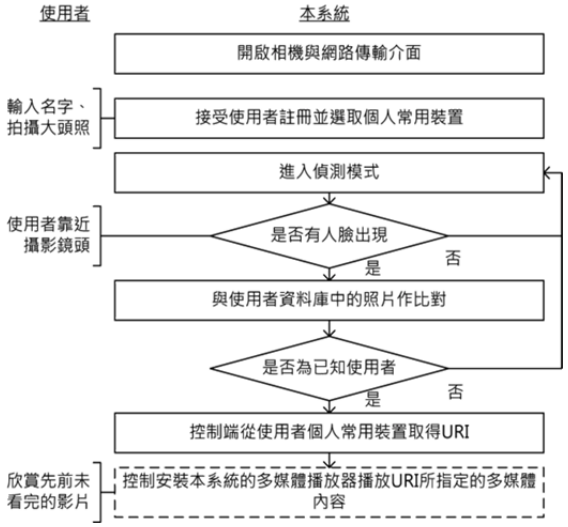


圖 5 操作流程

4.2.1 使用者註冊及常用裝置註冊

系統開啟影像攝影機，連續掃描在攝影機鏡頭前方的畫面，分析影像的特徵判斷是否有人臉出現，如果有則以一個綠色方框標示出被偵測到的人臉範圍。使用者僅需點選此方框即可將範圍內的人臉影像儲存為圖片於檔案系統中，並賦予此圖片檔案一個使用者自行定義的名稱。初步完成使用者資料的建立後，此系統尚須進一步分析該人臉資料在使用上的合適性，此時將會載入先前已經建立的人臉資料，比對人臉資料的差異性，如差異性大於系統預設的百分比值則會要求使用者更正人臉圖片。當成功建立人臉資料之後，可進一步附加上常用的多媒體裝置，系統將透過服務類型(UDA Service Type)過濾出具備多媒體播放能力的裝置，以列表方式顯示供使用者選取多媒體播放裝置。

4.2.2 人臉辨識驅動影音播放標的之轉換

在系統啟動時除了開啟攝影機鏡頭進行影像擷取之外，網路傳輸介面也會同時接受來自區域網路中的封包，以偵測其他裝置的存在，一旦辨識出已註冊使用者出現在攝影鏡頭前且從資料庫中取得該使用者名稱所對應的常用裝置，以常用裝置名稱比對目前存在區域網路與否，如果出現在區域網路中，則取得該裝置目前正在播放的多媒體檔案鏈結(URI)同時取得播放進度，設定系統指定的鄰近裝置上的多媒體播放器並準備播放的多媒體鏈結，完成後發送開始播放的指令。多媒體內容便透過人臉辨識的驅動，自動轉換播放標的從使用者常用的裝置到指定的鄰近裝置。

如圖 6 的實施例，以下說明人臉辨識和影音播放標的變換的操作細節。編號 1 為偵測模式的畫面，當系統啟動後，會直接來到此畫面，偵測畫面下方有三個選項，分別為 Members、UPnP 和 Switch：

Switch 選項是用來開關多媒體影音傳送功能，

為避免任一第三方裝置也同時偵測到該名成員時，相同的多媒體影音檔會重新被傳送，形成不斷重新播放的錯誤狀況。UPnP 選項讓使用者可以手動去選擇網路上多媒體播放裝置以及希望播放的影音媒體檔，這部分是依循 UPnP AV 模式，讀者可參閱[1][2]。Members 選項是切換到使用者註冊介面，如編號 2 畫面，使用者可點選下方圖鈕來新增成員，選擇後會進入編號 3 的個人化設定，輸入使用者名字及建立人臉圖片，最後進行個人裝置的選擇，如圖所示，使用者可以看到目前家庭網路環境下存在有一個媒體播放裝置 BRAVIA KDL-xxx，最後在使用者完成以上的個人化設定後，點選 OK 按鈕會回到編號 1 的偵測模式畫面，此時系統的使用者資料庫已經紀錄了上述的個人化設定。

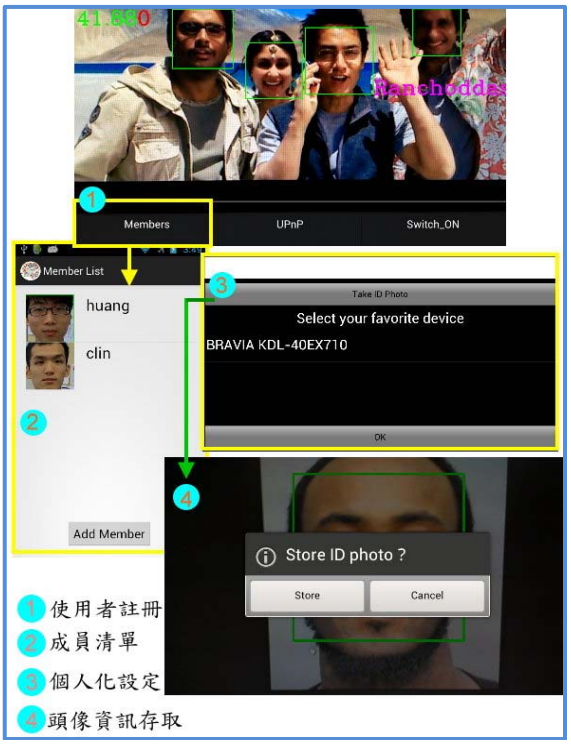


圖 6 使用者實機操作之實施例

4.3 實例展示

本系統研發成果的展示是以居家生活空間為應用實施的場景，如圖 7 所示，基本上一個居家生活空間可由許多不同的小型空間所組成，一般的居家設計上會有客廳(編號 1)、臥房(編號 2)，也許會有書房和飯廳(編號 3 和 4)。

展示的規劃上，假定偵測裝置是安裝在客廳的電視上方，其他空間也許會有家庭成員常用或喜愛的多媒體網路裝置，例如個人電腦、筆記型電腦和智慧型行動電話等。特別解釋的一點是，客廳是家庭成員感情交流的主要場地，因此在系統雛型的佈建及測試時，我們選擇把偵測裝置放在客廳裡。



圖 7 家庭空間組成示意圖

4.3.1 情境 1: 單人

一位家庭成員原先在臥房內使用電腦正在觀賞影片，不過他想換個更舒適更大的螢幕來欣賞，於是他走出房間來到客廳，當他坐在沙發上面對著電視，本系統會辨識出他的身份，並發現他常用的裝置即臥房內的電腦上有一部正播放的影片，系統將影片的播放轉送到客廳的電視以供觀賞。

4.3.2 情境 2: 多人且有一位家庭成員

某日家中來了許多親戚在客廳聚會，因為這些訪客先前尚未有過註冊，人臉辨識模組的判定之後，並不會執行任何動作。此時，有位家庭成員願意和大家分享方才在房間內觀看的影片，他只須走到客廳的電視前，系統成功完成人臉辨識，啟動多媒體影音傳送的動作，實際測試結果如圖 8。



圖 8 多人之中有一位家庭成員

4.3.3 情境 3: 多人且多位家庭成員

圖 9 展示同一個空間中有多個家庭成員的測試結果，畫面中兩人都已進行註冊，當其中一方較靠近偵測裝置時，此系統就會認定其為主操控者，此時螢幕上就會顯示該成員的名字。

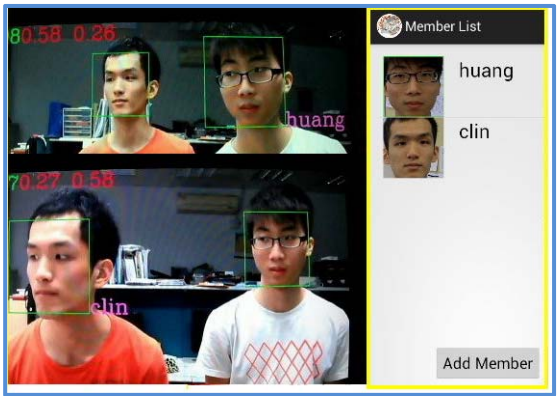


圖 9 主操作者選擇測試

4.4 系統封包分析

本系統實際運作時，利用 Wireshark 網路監測軟體取得裝置在區域網路中所發出網路封包資訊。圖 10 及 11 展示偵測裝置進入圖 3 的偵測模式時，以 4.2.2 章節所描述的運行方式，透過 HTTP 傳送訊息向使用者個人裝置取得多媒體內容資訊(圖 11a 處)，並轉送內容至指定的多媒體播放裝置，協助播放裝置向伺服器取得影片串流(圖 12b)。

表 1 各個裝置的 IP 位址

裝置	IP 位址
偵測裝置	192.168.1.116
使用者個人裝置	192.168.1.117
指定的多媒體播放裝置	192.168.1.106
多媒體伺服器	192.168.1.117

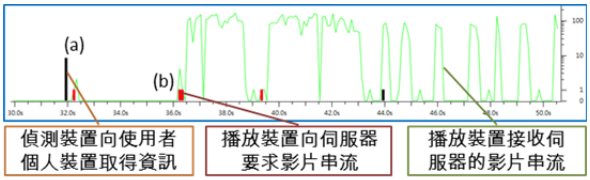
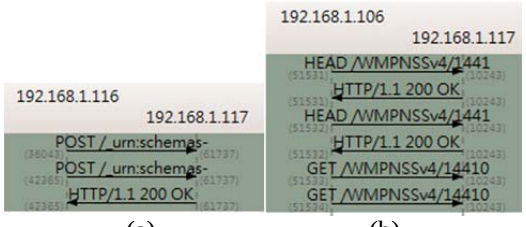


圖 10 系統運作過程之封包流量分析
(橫軸為時間(秒)，縱軸為封包數量)



(a) (b)

圖 11 (a)控制端與個人裝置間的 HTTP 訊息交換; (b) 指定的播放器向多媒體伺服器取得影片串流

5. 結論與展望

本論文提出在家庭網路環境下的智慧多媒體影音傳送系統之架構規劃、功能設計及雛型實作。本系統整合 UPnP 網路內容分享平台與人臉辨識兩大技術，搭配使用者資料庫，帶給使用者全新的人機互動方式，使得家庭影音分享不被居家空間的隔閡所限制。系統功能的特色在於一改傳統一個口令一個動作的手動操作模式，系統能夠自動根據家庭成員的身份，主動提動個人化的多媒體影音服務。至於系統雛型的實作，我們利用 Cling UPnP 與 OpenCV 等開放式軟體套件，完成一套可以建構在 Android 執行平台上的軟體模組並封裝為一組 Android 應用程式。最後，我們透過實機運行來真實呈現具即時性且個人化的智慧型家庭網路影音傳送服務。至於接下來的研發工作，我們將提升系統服務的個人化特色，讓使用者所屬的相關設定更為完備，並將加入客製化的多媒體內容服務，帶給使用者更多樣化的數位多媒體內容和應用。

致謝

本論文部分研究之進行，承台灣工業技術研究院之委研計畫 B5-10223-2H-1 經費支持。

參考文獻

[1] UPnP Forum, “UPnP AV Architecture:2 Version: 1.0”, Dec 2010.

[2] C.-L. Hu, W.-S. Liao, and Y.-J. Huang, “Mobile Media Content Sharing in UPnP-Based Home Network Environment”, *Information Science and Engineering Journal*, vol. 24, no. 6, pp.1753-1769, Jan 2008.

[3] C.-L. Hu, C.-L. Lin, P.-C. Lin, and Y.-Y. Su, “Gesture-Assisted Remote Control for Media Content Sharing and Distribution in Home Networks”, *Proc. of IEEE ISCE*, pp.87-88, Jun 2013.

[4] C.-L. Hu, B.-J. Hsieh , H.-C. Lin, and Y.-F. Hsu, “Integrated home gateway design for enabling P2P content sharing in UPnP-Based home networks”, *Proc. of IEEE ICCE*, pp. 229-230, Jan 2011.

[5] H. K. Ekenel, H. Gao, J. Stallkamp, M. Fischer, and R. Stiefelhagen, “Face recognition for smart interactions”, *Proc. of IEEE ICME*, pp. 1007-1010, July 2007.

[6] Petros Belimpasakis, and Rod Walsh, “A combined mixed reality and networked home approach to improving user interaction with consumer electronics”, *IEEE Transactions on Consumer Electronics*, vol. 57, no. 1, pp. 139-144, February 2011.

[7] P. Viola and M. Jones, “Robust Real-Time Face Detection,” International Journal on Computer Vision, vol. 57, no. 2, pp. 137-154, May 2004.

[8] P.N Belhumeur, J.P. Hespanha, and D.J. Kriegman,, "Eigenfaces vs. Fisherfaces: recognition using class specific linear projection," *IEEE Transactions, Pattern Analysis and Machine Intelligence*, 1997.

[9] M.A. Turk and A.P. Pentland, "Face recognition using eigenfaces," *Proc. of IEEE CVPR*, Jun 1991.

影像查詢技術應用於展場導覽系統設計之研究

黃國峰　施成憲　林善智　游耿能
國立臺中科技大學多媒體設計系
kfhwang@nutc.edu.tw galetter@livemail.tw rexl1008@gmail.com gny@nutc.edu.tw

摘要

隨著智慧型手機的普及，許多日常生活中與手機互動的方式亦受到改變，影像辨識科技的進步亦影響導覽行為的輔助模式。本研究應用影像查詢技術於展場導覽系統之設計，我們先針對研究目進行相關文獻的探討，而後分兩階段進行研究，第一階段以影像辨識技術建構一個應用於展覽時可使用之行動導覽系統，此導覽系統使用電腦視覺演算法 SIFT 來提取特徵值方式以辨識展覽目標。第二階段則將設計出之導覽系統，實際應用於一個書法展覽中，在現場用隨機方式邀請了 21 位觀眾使用此導覽系統以進行測試，初步結果顯示以影像辨識技術建構之導覽系統，有助於使用者實際的導覽體驗。
關鍵詞：行動導覽、SIFT、影像查詢。

Abstract

With the popularity of smart phones, interaction styles with the phone in our everyday are also subject to change. On the other hand, the advances of image recognition technology will also affect the patterns of mobile guiding behavior. In this study, image retrieval technology is employed in the design of an exhibition guiding system using mobile devices. We first explore and survey relevant literatures for this research. Then the study is conducted with two stages. In the first stage, we constructed a mobile guiding system by applying image recognition technique for guiding people during visiting exhibitions. We adopted the SIFT Computer Vision Algorithm and eigenvalues to extract image features in order to recognize targets in exhibitions. In the second stage, the prototype of the mobile guiding system is used to help viewers of a calligraphy exhibition. In this the scenario of practical application, 21 viewers are randomly chosen and invited to use this system for a preliminary user study, the results show convincing positive response in applying image recognition technology to build the mobile guiding system that helps users navigating experience.
Keywords: Mobile Guiding System, SIFT, Image Search

1. 前言

隨著智慧型手機與行動裝置的普及，行動導覽也漸漸成為導覽的使用設備。行動導覽不僅能為觀眾提供個人化的導覽解說，同時又能節省實體展覽資源與經費的耗費，行動導覽對展覽來說有利無害。國內常見的行動導覽，通常是語音、影片和互動 app 等導覽方式，而其中導覽查詢應用方面有一維條碼、二維條碼和網路定點呈現資料等。導覽查詢方式雖有多種選擇，但大多以定點給予查詢資料的概念為主，像是在展覽點貼上看板或媒體裝置，沒有更直覺式的查詢方式，若在資訊量多的展覽點上，使用者就必須去閱讀理解訊息，從中找出自己想找的東西，頓時就會耗費許多導覽時間。因此本研究嘗試建構使用這更直覺得查詢導覽系統。

影像處理已發展多年，其效率與實用性已普及在我們生活週遭，如相機中的環景功能、人臉辨識等。尤其是尺度不變特徵點演算法，其能達到抗旋轉、抗光影變化、抵抗遮蔽物等強大功能。然而既然電腦已能辨識影像，那麼將使用者想要找尋的影像交給電腦，再回傳需求的資料，就能輕易的達到使用者直覺選擇查詢項目的問題。為此想嘗試利用影像查詢輔助行動導覽的可行性成為本研究的動機。

2. 文獻探討

2.1. 導覽

本研究技術針對展場導覽，故查詢參考導覽方面研究，並對研究中需理解的參考資料做歸類，分別是導覽功能與行動導覽。

導覽的定義是「引導觀眾，藉由一種有意的安排，來實行引導活動， 經由導覽人員來進行， 以達到某種教育計畫性的目的」 [1]。有導覽的展覽比觀眾自由參觀更易於將作品的意義交給參觀者，這是一種輔助觀眾參觀的方式。導覽在本研究中的功能為：透過導覽系統引導觀眾，使其對展覽標的物有完整的認識，並從中得到資訊、教育、娛樂等作用。

無線技術的進步，推進了行動導覽開始普遍應用於展場中，最先是由 PDA 開始， 1993 年 Visible Interactive 公司開發了第一個互動影音導覽系統 iGo，並將其應用博物館導覽中，利用互動式多媒體，如文字、影、音等大大增加參訪者的個人經驗。後來陸續有許多大型導覽也開始嘗試行動導覽系統，除了行動導覽優越的互動性外，還兼具即時性，比如內容可提供行程表、餐廳資訊等。行動導

覽使得主辦者與參訪者距離大大縮短了，這意味著不僅是導覽，如研討會、都市導覽、觀光導覽等都能利用到行動導覽[2]。

2.2. SIFT 尺度不變特徵

尺度不變特徵之優勢，在於其能夠抵抗圖像的旋轉、縮放、變形、光影變化與抵抗遮蔽等效果，功能強大。而尺度不變特徵能做到這點是因為建構出能因應不同尺度的影像金字塔，並設計豐富訊息且特異性高的特徵點這兩個特性。本研究之影像查詢技術，就是應用尺度不變特徵點原理，找尋影像中特有的特徵以抵抗使用者上傳的各種不同影像變化。尺度不變特徵發展至今已有許多種演算法，如 SIFT、PCA-SIFT、GLOH、SURF 等，不同的演算法皆有自身的優勢與特點。而本研究實驗工具應用的演算法是 SIFT 演算法，SIFT 是各類尺度不變特徵演算法的始祖，雖然跟後進演算法相比慢了許多，卻依然是抵抗旋轉與尺度變換效果最好的，也是本研究使用他的理由。

SIFT(Scale-invariant feature transform)是一種電腦視覺演算法，由 David Lowe 於 1999 年所發表，並至 2004 年才給予總結，也立定了尺度不變特徵中圖像金字塔與多訊息特徵點的概念。主要流程大致可分為以下四類：

1. 建立尺度空間。
2. 找尋特徵點。
3. 賦予特徵點方向性。
4. 建立特徵敘述子。

SIFT 演算法內容豐富，因此依以上列各點，再分小節給予詳細的解釋。

2.2.1. 建立尺度空間：

建立尺度空間中又可分為三步驟，第一步，建立圖層金字塔(Pyramid layer)：

將原始圖依等比長寬縮小成各種尺寸，如 1/2、1/4、1/8 等，直至某個最小尺寸為止，影像堆疊起來如同金字塔般，故稱為圖層金字塔，如圖 1。

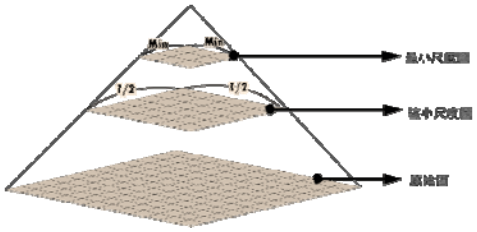


圖 1 圖層金字塔(Pyramid layer)

第二步，進階為高斯金字塔(Gaussian Pyramid)：

若將原始圖做為公式，則以 I(x,y) 已表示，而可變高斯模糊函式則以 G(x,y,nσ) 為表示(本研究 σ 表示為尺度大小)，把高斯模糊作為原圖的濾鏡產生的結果則可表示為 L(x,y,nσ) ，公式如圖 2。

$$L(x,y,n\sigma) = I(x,y) * G(x,y,n\sigma)$$

圖 2 高斯模糊公式

接著，這邊對每層不同尺度的圖形進行如上述所說的高斯模糊，不同的是，每張圖型會分別以不同變量過濾多次，通常執行至少 4 次，其變量是越來越大，如 σ、2σ、3σ...，以結果來看就是變得越來越模糊，高斯金字塔如圖 3。

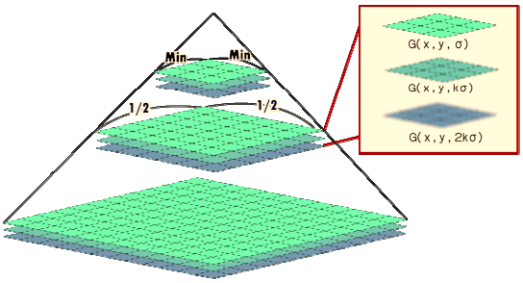


圖 3 高斯金字塔(Gaussian Pyramid)

第三步，得出高斯差異影像(Difference of Gaussian，DoG)：

DoG 這步驟是利用高斯金字塔產生的結果 L(x,y,nσ)，再兩兩相減產生差異圖形，如圖 4 所示，以利下一步驟找尋差異點。

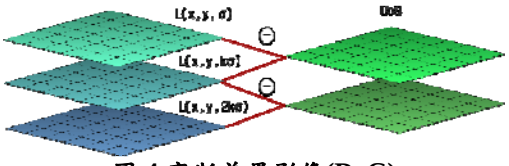


圖 4 高斯差異影像(DoG)

2.2.2. 找尋特徵點

SIFT 特徵點的找尋方式是用極大值檢定法，但他不只檢定單一 DoG 圖層，還包含圖像金字塔同一尺度中前後產生的 DoG 圖做比較，判斷每個像素在周圍鄰近 8 個點與上下兩 DoG 圖層各自的 9 個點，共 26 個點是否是最大或最小值，是則被標記為極值點，如圖 5。

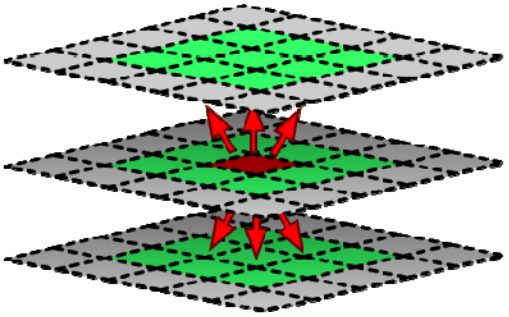


圖 5 極大值檢定法

獲得極值點後，為了得到更為精確的特徵，SIFT 又再次對每個極值點做 Hessian 角點過濾，Hessian 角點過濾特性是可獲得圖像明確的轉角，藉此可刪去在圖像邊緣的極值點，在此殘留下來的極值點可視為特徵點的中心。

2.2.3. 賦予特徵點方向性

找到特徵點後，會利用特徵點為中心，其半徑 3*1.5σ 內所有像數進行角度與強度的計算，在將其歸類為 8 個主方向累計強度，強度最高的方向視為主方向，如圖 6。

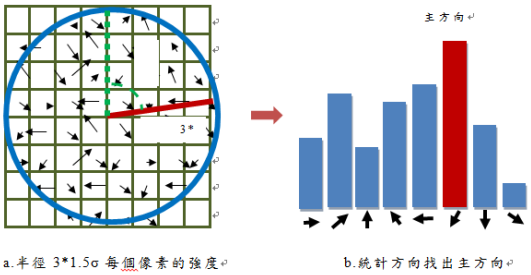


圖 6 SIFT 方向檢測

為了達成影像特徵的不變性，主方向確定後以特徵點為中心，將圖像旋轉 θ 角，再執行下一步的特徵資訊建立。

2.2.4. 建立特徵點敘述子

建立特徵敘述子第一步是以特徵點為中心，將四周分割為 4 乘 4 的區塊，再對每區塊計算 8 方位與其累積強度值，如圖 7，最後的結果每個特徵點能獲得 4*4*8= 128 個特徵值。

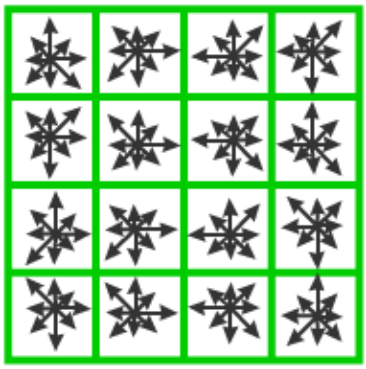


圖 7 SIFT 128 個特徵敘述子的生成

2.3. 尺度不變影像匹配應用

現今尺度不變演算以成熟，已利用於許多商務方面，如相機自動拼接的嘗試應用於衛星影像地圖的拼接研究[3]。利用其圖像辨識能力來解析交通號誌等[4]，以上足以證明尺度不變特徵發展潛力。

2.4. 介面互動設計

使用者介面定義為:整個系統除去影性數值運算、資料儲存、傳輸等所能見到聽到感受到的就是使用者介面[5]，往後推就能明白，使用者介面的設計關聯到設計者、系統與使用者間的關係。Norman 提出一概念模型[6]。敘述這 3 者的關係，如圖 8。

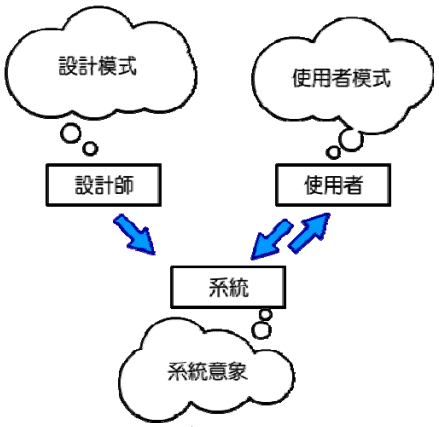


圖 8 設計者、系統與使用者關係圖

圖中表現出，設計師對於系統與使用者對於系統的認知是不同的，然而介面設計是設計師與使用者的對話，需要顧及互動性與操作過程，方能同理使用者的想法，減少使用者經驗上的挫折，如此做出有善於使用者的人機介面。

3. 系統設計

3.1. 系統設計方向

為了方便展方管理與編輯資料，為系統建立了給展方編輯用的後端系統，而後端系統又分兩個版本，分別是桌機與行動裝置版，後端行動裝置版系統是為了讓編輯者能快速取的與編修展場影像資料，而後端桌機版系統則是為了對於指展覽的詳細編修而設計，雙版本的設計除了各有優勢，還能同時一起使用，加速後端資料的編輯速度。後端系統完成後也為參訪者建立前端系統，前端系統相較於後端系統單純，僅有行動裝置板，而較特別的設計部分，是為了方便驗證與收集使用者反應，在前端系統尾端多設計了一套問卷系統，方便參訪者測試後直接填寫並傳回伺服器已統計，同時方便本研究做統計。

除了視覺介面上的前端系統與後端系統，視覺介面外的伺服器系統設計也是一大工程。伺服器系統本身負責與資料庫的溝通與回覆視覺介面的命令需求，同時解析影像特徵、影像匹配也是在這裡完成。查詢導覽系統簡易架構圖如圖 9。

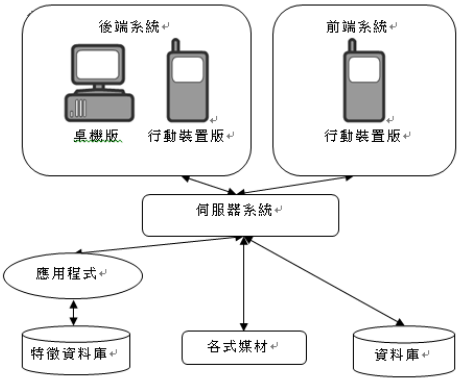


圖 9 查詢導覽系統簡易架構圖

3.2. 後端系統設計

後端編輯介面又分桌機板與行動裝置版，行動裝置版設計目的，是想利用行動裝置攜帶方便的特性，迅速把展場上的影像都收集歸類至資料庫內。為此目的，讓編輯者可在展覽會場直接拍照並做簡易的文字編輯，再上傳於伺服器中。相對於行動裝置版，桌機板的設計是為了詳細編修行動裝置版中建構的資料，也可快速的新增展覽項目、超連結與額外的多媒體檔案。行動裝置版與桌機板的設計，意味著資料建構能同時多人進行。

行動裝置版是讓編輯者能快速、簡易新增資料與配對測試的工具。因此依功能分類到編輯模式與使用者模式中，編輯模式主要讓編輯者拍照新增資料、瀏覽項目、更新與刪除等管理動作。使用者模式是在編輯者完成編輯後，可用在展場中使用此模式測試影像查詢結果。若無法查詢到照片，可能是照片拍照時搖晃造成模糊，抑或是亮度不足，造成解析度不足等問題，此時只要在編輯模式，重新拍照更新資料即可。編輯者能用以上方式，立即排除資料庫中有問題的圖像資料。介面架構圖如圖 10。

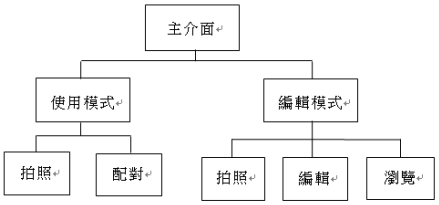


圖 10 行動裝置版介面架構圖

介面設計部分以簡單的漸層灰色調為主，如下圖 11 行動裝置版介面所示。

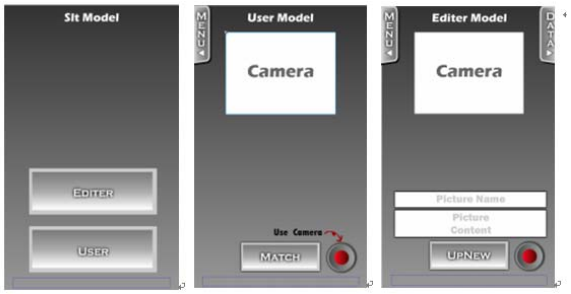


圖 11 行動裝置版主頁與各模式首頁

如上小節所說行動裝置版擁有使用者與編輯者兩模式，因此行動裝置版主頁，如圖 11a 簡單設計兩個按鈕 EDITER 與 USER 能連結進入這兩個模式。在各模式下，只要點擊左上角 MENU 按鈕，即可回到首頁，藉此切換模式。

使用者模式，如圖 11b，僅有此頁面，若要擷取照片可按下圖中紅色按鈕進入 Android 系統內建拍照模式進行拍照，之後照片會取代圖中 Camera 的部分。接著點擊 Match 便上傳照片至伺服器與資料庫中所有的照片配對，並將結果傳回圖中空白處。以上拍照與配對動作，可重複執行。

編輯者模式，如圖 11c，一進去是資料新增頁面，資料新增動作前得先完成拍攝，步驟如同使用者模式，點擊畫面中紅色按鈕即可進入 Android 內建拍攝模組，取得照片後便取代 Camera 圖像。接著在 PictureName 與 PicContent 兩文字輸入欄位輸入圖像名稱與簡易的內容，最後點擊 UpNew 按鈕即可將資料新增於資料庫中。圖像名稱欄位無資料，則以日期時間替代名稱，紀錄於資料庫裡。欲檢查資料庫中現有的資料內容，可點擊右上 Data 按鈕切換到資料頁面，如圖 12。



圖 12 編輯者介面-資料頁面

資料頁面列表中，是現有資料的 id 資訊、影像縮圖、名稱與刪除按鈕。欲刪除資料點擊刪除按鈕即可。點擊 id 資訊、影像縮圖、名稱皆會進入資料更新頁面。頁面中 All Clear 的按鈕，是刪除資料庫所有資料功能，是為了方便測試而設立的功能。資料列表底下的 PAGE 物件，是分頁顯示物件，能提醒使用者目前的頁數。而右上角 New 按鈕，功能是回資料新增頁面。

資料管理於行動裝置版中，會發現不提供影片、聲音資料與網路連結的管理，因為行動裝置版定義是快速新增影像資料，上傳影音媒體的步驟與輸入連結網址等相對於桌機處理麻煩許多，尤其是將媒體檔案上傳伺服器，會對網路成為笨重的負擔。況且需新增影音資料通常已準備好在桌機裡，沒必要由行動裝置中執行，因此詳細管理資料部分交給桌機版處理即可。

在資料更新頁面中如圖 13，會發現並無拍攝按鈕，此頁面資料更新僅提供更新圖像名稱與內容，同樣於 PictureName 與 PicContent 兩文字欄位輸入圖像名稱與內容，再點擊 UpData 按鈕即可更新資料庫資訊。位於此頁右上方的兩個按鈕 New 與 Data 分別連接回到資料新增頁面與資料頁面。



圖 13 編輯者介面資料更新頁面

桌機板的設計期望是快速與詳細的編輯資料，因此介面偏重功能導向，沒有分頁，僅分出項目列表與資料編輯欄位兩個區塊，能讓編輯者一目了然方便操作。起始頁面如下圖 14，此時右邊資料編輯欄位成灰色表示未選擇資料。

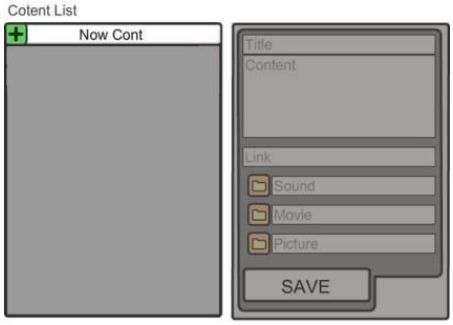


圖 14 桌機版起始介面(未有資料)

當按下 Now Cont 按鈕會增加一筆新的展覽項目，資料編輯欄位也跟著亮起，此時可編輯展覽項目，如標題、內容、連結與各項媒體檔案，如圖 15 所示。



圖 15 桌機版起始介面(新增資料)

其中資料夾符號表示為瀏覽檔案，會開啟瀏覽檔案視窗，方便使用者選擇媒體，編輯完成再按 SAVE 按鈕方可儲存入資料庫，此時會順便將存入的圖片做特徵值處理。而項目中 X 的按鈕表示刪除項目，此功能會清除所有內容、儲存在伺服器端的媒體檔案與特徵檔。

3.3. 前端系統介面

前端系統簡易架構如下圖 16，主要有 7 個頁面，系統實際操作時的主體是拍攝頁、資料展示頁與多選頁。

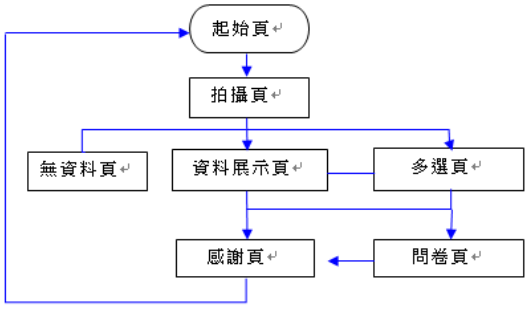


圖 16 前端介面架構圖

3.4. 伺服器設計

編輯者與使用者各自擁有分開的介面，各介面最後會將命令傳到到伺服器上傳或取得各式的資料與媒體，伺服器整體架構如圖 17 所示。來到伺服器的命令後續動作可分 A、B、C 三類，A 為透過網路動態語言與資料庫做溝通，此時取得資料與媒材檔案名稱或將資訊建於資料庫中，接著回傳結果於使用介面。B 為透過網路動態語言啟動應用程式，接著應用程式會執行特徵值資料庫相關的處理動作，可能是分析製作資料或比對特徵。C 部分是上傳媒材檔案或取得媒材的過程。

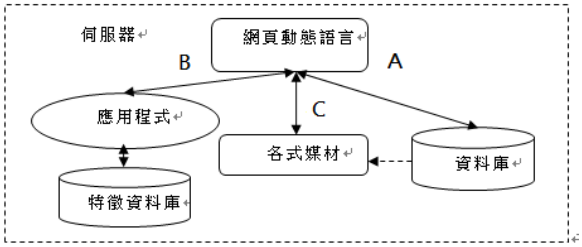


圖 17 伺服器簡易架構

這部分包含資料庫結構與命令流程設計，而命令流程是指使用者向伺服器回傳的命令項目，可分成四類，分別是：

a.上傳資料與特徵值處理
b.修改資料
c.刪除資料
d.匹配與查詢資料

4. 實驗結果與分析

系統完成後選擇 2013 中區書法聯展為實驗對象，展場狀況如圖 18，目的考驗系統對於平面展覽作品的抗旋轉、抗光影與抗角度的成效。在實驗中所使用的行動裝置載體為 Asus Transformer TF 101 平板電腦。



圖 18　2013 中區書法聯展，台中科技大學展次

2013 中區書法聯展是國立台中科技大學、國立中興大學與逢甲大學三校書法社聯展，作品繁多在三校中輪流展出，本次實驗是台中科技大學場次，辦於台中科技大學，中商大樓一樓川堂，展場示意圖如圖 19 所示。

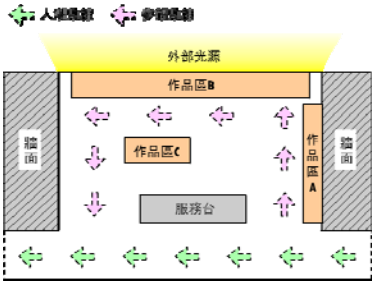


圖 19 展場示意圖

透過展場示意圖中，可了解展覽分 A、B、C 三個展區，A 展區靠於牆面上，B 展區則是靠於在窗戶上，C 展區則是平躺在桌面上的作品 ，展場示意如圖 19。

從以上可對展覽看出幾以下幾點：

a. B 區光線對外開放，各展區光源皆會受到天候影響，尤其 B 展區拍攝上逆光嚴重。

b. C 區展覽作品平躺於桌上，參觀者無法平面拍攝。

以第一點來說，雖然光線影響嚴重，但卻可以用來測試本系統查詢能力是否受光源影響。而對於第二點來說，原先資料庫中的對應影像是平面的，但到了現場，平躺角度關係讓作品拍攝後變形過份嚴重，如圖 20 所示。

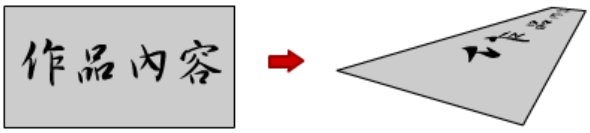


圖 20 拍攝變形示意圖

拍攝到的角度，無法每次都順利辨識，因此把其當成立體作品看待，對此作品在展覽中拍攝 4 個面，如圖 21 分別將不同的照片與特徵值和相同的做品敘述，分別紀錄於資料庫中，目的就是以使用者的角度建構以減少搜尋誤差。

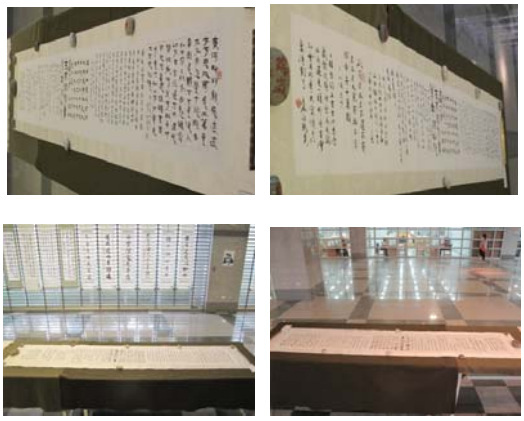


圖 21 作品區 C 重新拍攝的 4 個面

經過使用者操作後，訪問結果表示，有少數使用者認為本系統幫助不大，原因是輔助的媒體不夠多。而且其中有女性表示，長時間使用平板電腦對於女性使用者來說太過沉重，但使用者普遍認為此輔助導覽裝置是便利的。

5. 結論與未來展望

本研究以影像辨識技術建構一個應用於展覽的行動導覽系統，此導覽系統運用 SIFT 演算法來辨識使用者欲導覽之目標。目前系統所使用 SIFT 演算法對於比對資料仍有極限，資料庫中超過 50 筆資料，運作上會出現緩慢的情形，未來可嘗試 SURF 或 CCH SIFT 等其他方式來改善資料過多所產生的緩慢情形。

參考文獻

[1]余少卿，梁朝雲，莊育振 (2003)。行動數位導覽之博物館應用探討。圖書資訊學刊，卷期:1，頁 1-24。

[2]蕭顯勝，黃向偉，洪琬諦 (2007)。行動導覽系統於博物館學習之研究。高雄師大學。

[3]李慧，蘭啟忠，劉慶杰(2012)。基於 FAST 和 SURF 的遙感圖片自動配準方法。國土資源遙感，卷期:93:2，頁 28-33。

[4]胡錦城，李實英，李仁發(2012)。基於高穩定 SURF 特徵的交通標誌識別。計算機應用研究，卷期:29:8，頁 3179-3181。

[5]Lauesen, S. (2005),User interface design: A software engineering perspective. Addison Wesley

[6]Norman Donald A.(2007),設計&日常生活：如何選擇安全好用的日常生活用品，台北：遠流。

中醫症狀詞庫的研製

葉明憲
佛教慈濟綜合醫院
大林分院中醫科
yehlinlo@gmail.com

郭慧翔
國立中正大學
資訊工程學系
shawnshoo@hotmail.com

林迺衛
國立中正大學
資訊工程學系
naiwei@cs.ccu.edu.tw

摘要

中醫的診斷治療是以「辨證論治」的方式進行。中醫師會先根據望、聞、問、切四診收集病患的症狀及體徵資料，再根據收集到的症狀及體徵資料進行詳盡地分析，最後歸納出疾病的病因、病位、及病機，此即為「辨證」。中醫師最後根據辨證結果對病人進行適當的治療及用藥，此即為「論治」。我們希望研製一套中醫自動辨證系統，做為中醫的研究平台。然而中醫自動辨證系統的基礎在於中醫症狀標準化。

本研究建立一套中醫症狀詞庫系統，來解決中醫症狀標準化的問題。我們除了使用「症狀字詞比對」的方式進行症狀標準化，還使用「關鍵字詞比對」的方式進行症狀標準化。如果輸入的症狀已經經過標準化，並存在資料庫，系統可透過症狀字詞比對正確地查詢到其所對應的標準症狀。如果輸入的症狀尚未經過標準化，不在資料庫，系統會先將該症狀分割成一串已知的關鍵字詞，再透過關鍵字詞比對的方式，查詢這些關鍵字詞的語意。最後系統依據這些關鍵字詞的語意，查詢語意最接近的標準症狀。本研究顯示，運用語意資訊，可以明顯地提昇系統查詢標準症狀的正確率。

關鍵詞：中醫症狀詞庫、症狀標準化、語意

Abstract

The diagnosis and therapy of traditional Chinese medicine follows the approach of syndrome differentiation and treatment. For syndrome differentiation, the doctor first gathers the symptoms and signs of patients through the four examinations: inspection, listening and smelling, inquiry, and palpation. The doctor then performs a comprehensive analysis of the symptoms and signs to identify the cause, location, and mechanism of the illness. Finally, the doctor determines the treatment according to the identified syndrome. We planned to develop an automatic syndrome differentiation system as a research platform for traditional Chinese medicine. However, the foundation of an automatic syndrome differentiation system is the standardization of symptoms and signs.

This research develops a traditional Chinese medicine symptom thesaurus to solve the issue of the standardization of the symptoms and signs. In addition to string pattern matching of symptoms and signs, we also perform string pattern matching of keywords. If an inputted symptom or sign description has been standardized and is in the symptom thesaurus, the system will map this inputted symptom or sign description to its corresponding standardized symptom or sign. If an inputted symptom or sign description has not been standardized and is not in the symptom thesaurus, the system will first split the inputted symptom or sign description into a sequence of keywords. The system then performs string pattern matching of these keywords and enquires the semantics of these keywords. Finally, the system maps this inputted symptom or sign description to a standardized symptom or sign with the closest semantics. This research demonstrates that applying sematic information can significantly improve the correctness of the mapping to the standardized symptom or sign.

Keywords: traditional Chinese medicine symptom thesaurus, standardization of symptoms and signs, semantics

1. 前言

疾病在中醫被稱為「證」，所謂「證」就是由一定的「病因」作用於一定的「病位」，而發生一系列動態演變的過程[1]。

中醫先透由望、聞、問、切等四診，取得病患的身體症狀資訊，再透由分析這些症狀資訊來辨識疾病的病因及病位，這個過程稱為辨證。

我們長久以來一直希望研製一套中醫自動辨證系統，做為中醫研究的平台。然而，當我們開始著手研製中醫自動辨證系統時，首先遇到了中醫症狀尚未標準化的困難。

目前的古籍資料對於症狀的描述及其意義的解釋存在不一致的情形。我們若是想研製一套中醫自動辨證系統，假使症狀存在不一致性，電腦將會無法明確區分症狀的差異性，造成辨證的困難。因此，研製中醫自動辨證系統前，我們必須先完成症狀標準化。

有了統一的標準症狀後，中醫自動辨證系統就

能夠利用這些標準症狀的資訊，進行辯證，進而提供處方治療。

當我們著手要做症狀標準化時，遭遇到兩個主要的困難:症狀具有多詞一義及一詞多義的現象[2][3]。 症狀具有多詞一義的問題為，有多個不同的症狀描述，但是它們所表達的症狀意義卻是相同的。例如，症狀「大便不利」、「大便艱澀」、和「大便不通」都是表達大便有困難的涵義，我們希望可以將這三個症狀標準化成標準症狀「大便不暢」。症狀具有一詞多義的問題為，一個症狀描述卻包含多個症狀意義。原始症狀「二便不利」表達大便有困難以及小便有困難兩種涵義，我們希望可以將這個原始症狀標準化成標準症狀「大便不暢」及「小便不暢」。

我們做症狀標準化最主要的目標，就是想讓症狀描述可以達到一詞一義以及一義一詞，使得中醫自動辨症系統不會因為症狀多詞一義以及一詞多義的問題，而在進行辯證時遇到困難。

2. 研究目的

本篇論文的研究目的就是研製一個中醫症狀詞庫系統。此系統能夠對應任意的原始症狀到標準症狀，也能夠將標準症狀對應到所有同義的原始症狀。利用此系統，我們就能夠自動進行系統化的症狀標準化，減少人工進行標準化所花費的時間，也可避免相同症狀被重複標準化成不同標準症狀的錯誤，達到症狀一詞一義以及一義一詞的結果。

3. 相關研究

在林劉育的《中醫症狀標準化與初探》研究中[4]，林劉育以人工方式將《中醫證候學》中的原始症狀以人工的方式進行症狀的標準化，並且建立一套使用症狀字詞比對的中醫症狀詞庫系統。在此系統中，只要是已經經過標準化之原始症狀，都可以提供其所對應之標準症狀。但若是不在資料庫之原始症狀，則無法提供其所對應之標準症狀，也就無法自動進行症狀標準化。

在李宜泓的《以近似字詞比對方法輔助中醫症狀標準化》研究中[5]，根據林劉育的研究基礎，他所建立的中醫症狀詞庫系統，除了使用症狀字詞比對來做症狀標準化，還增加了使用近似字詞比對的方式來做症狀標準化。除了資料庫已標準化之原始症狀，可以提供其所對應之標準症狀，若是不在資料庫之原始症狀，他的系統還會透過近似字詞比對的方法，提供建議的標準症狀，但是他的系統是利用字詞的相似程度做搜尋，因此無法提供精確的標準症狀。

4. 研究貢獻

本研究建立了一套中醫症狀詞庫系統，用來解決中醫症狀標準化的問題。我們除了使用「症狀字詞比對」的方式進行症狀標準化，還增加了使用「關鍵字詞比對」的方式進行症狀標準化。如果原始症狀已經經過標準化，存在資料庫中，系統可透過症狀字詞比對正確地查詢到其所對應的標準症狀。如果原始症狀尚未經過標準化，不在資料庫中，系統會先將原始症狀分割成一串已知的關鍵字詞，再透過關鍵字詞比對的方式，查詢這些關鍵字詞的語意。最後系統依據這些關鍵字詞的語意，查詢語意最接近的標準症狀。本研究顯示，運用語意資訊，可以明顯地提昇系統查詢標準症狀的正確率。

5. 系統架構

本論文中所提出之系統功能分為五部分: 原始症狀對應表維護、關鍵字詞對應表維護、症狀知識本體維護、標準症狀對應表維護、以及原始症狀搜尋。

資料庫儲存五個資料表:原始症狀對應表、關鍵字詞對應表、症狀知識本體、標準症狀對應表、以及未標準化原始症狀集。系統架構圖如圖 1 所示。

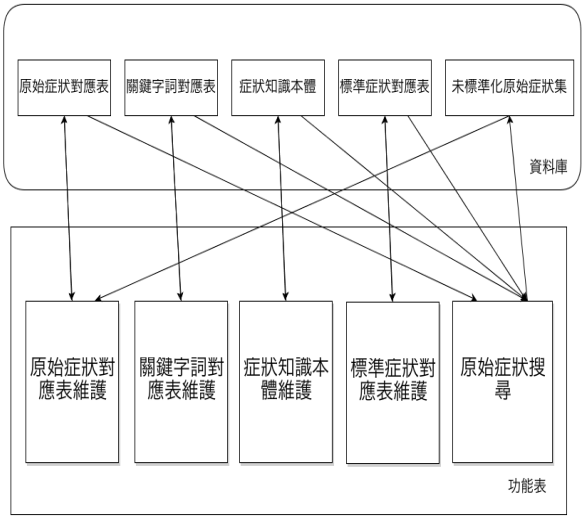


圖 1 系統架構圖

原始症狀搜尋使用原始症狀對應表作為搜尋依據，找出已標準化之原始症狀。若是在原始症狀對應表搜尋不到的症狀，會使用關鍵字詞對應表、症狀知識本體以及標準症狀對應表來做關鍵字詞搜尋，提供建議的標準症狀，這些症狀將會存到未標準化原始症狀集。系統管理者未來可以利用原始症狀對應表維護功能將未標準化原始症狀集中的症狀做標準化，並且新增到原始症狀對應表中。

原始症狀對應表記錄了原始症狀與標準症狀的對應關係。原始症狀對應表維護功能以新增、修改、刪除的方式來維護原始症狀對應表。

關鍵字詞對應表記錄了關鍵字詞與標準關鍵字詞的對應關係。關鍵字詞對應表維護功能以新增、修改、刪除的方式來維護關鍵字詞對應表。

症狀知識本體記錄了標準關鍵字詞之間的語

意關係。症狀知識本體維護功能以新增、修改、刪除的方式來維護症狀知識本體。

標準症狀對應表記錄了標準症狀與標準關鍵字詞(即階層式標準症狀)的對應關係。標準症狀對應表維護功能以新增、修改、刪除的方式來維護標準症狀對應表。

6. 系統實作

本系統的原始症狀搜尋功能主要分成兩部分:可搜尋到的原始症狀、以及未搜尋到的原始症狀,如**圖 2** 及**圖 3** 所示。



圖 2 系統介面圖



圖 3 原始症狀搜尋功能

- 可搜尋到的原始症狀

  我們使用完整字詞比對[6][7][8]方式搜尋資料庫內是否已存在此原始症狀,如果有,表示始症狀已經經過標準化。

- 未搜尋到的原始症狀

  如果原始症狀尚未經過標準化,不在資料庫中,系統會先將原始症狀分割成一串已知的關鍵字詞,再透過關鍵字詞比對的方式,查詢這些關鍵字詞的語意。最後系統依據這些關鍵字詞的語意,查詢語意最接近的標準症狀。

步驟如下:

I. 建立關鍵字詞對應表

我們在資料庫中建立了關鍵字詞對應表,如**表 1**,用來作為原始症狀斷詞的依據。關鍵字詞欄位為我們所整理出的症狀關鍵字詞,其中有包含許多同義字詞,而標準關鍵字詞欄位是把所有同義詞都統一對應到標準化的關鍵字詞。

表 1 關鍵字詞對應表一

原始關鍵字	標準關鍵字
大便	大便
不通	不暢
不利	不暢

II. 根據關鍵字詞對應表將原始症狀分割為關鍵字詞

我們需要在原始症狀中找出一些特定的關鍵字詞,作為搜尋的基準,因此我們必須對原始症狀先做斷詞,找出這些關鍵字詞。我們使用長詞優先法來對原始症狀進行斷詞。長詞優先法就是在進行斷詞時,使用資料庫中長度最長的原始關鍵字詞作比對[9]。

以原始症狀「大便不通」為例子,本系統將會斷出「大便」、「不通」。雖然在關鍵字詞對應表,如**表 2** 所示,中也有「大」、「便」這兩個關鍵字詞,但是因為「大便」的長度較長,因此成為斷詞的優先選擇。

我們會從原始症狀的第一個字開始對資料庫的原始關鍵字詞作比對,逐字往後做比對,直到找出最長的關鍵字詞,之後再從下一個字開始做比對,直到症狀的句尾為止。

表 2 關鍵字詞對應表二

原始關鍵字詞	標準關鍵字詞
大便	大便
不通	不暢
不利	不暢
大	大
便	大便

III. 對應原始關鍵字詞到標準關鍵字詞

在原始症狀做完斷詞後,我們再根據關鍵字詞對應表,把關鍵字詞作標準化。因為同義字即代表著相同的語意,所以我們只需用一個標準關鍵字詞就能代表這個語意,用來作為之

後搜尋的基準。

以關鍵字詞「大便」、「不通」為例，本系統會將其標準化成標準關鍵字詞「大便」、「不暢」。

IV. 根據標準關鍵字詞的語意建立症狀知識本體

因為知識本體[10]能夠表達出關鍵字詞之間的語意關係，我們希望能夠建立一個中醫症狀的知識本體，使得症狀可以用一些關鍵字詞互相的語意關係的方式來描述。

我們將關鍵字詞分為「症狀類別」、「症狀屬性」、與「症狀屬性值」三種不同詞類來定義。而這三種詞類之間具有包含的關係。「症狀類別」(例:小便、大便)包含了許多不同的「症狀屬性」(例:氣味、顏色)，有些相同，有些相異，而「症狀屬性」又包含了許多不同的「症狀屬性值」(例:臭、黃)。我們只要利用少許的關鍵字詞，就能透過它們所形成的語意關係，找出所有可能的標準症狀。只要這個症狀的知識本體越完整，我們系統所能找到的標準症狀將會越精確。如**圖 4**，為我們的症狀知識本體的一個例子。

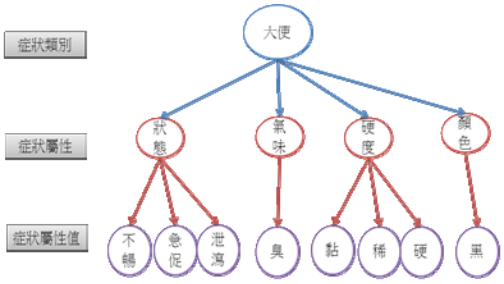


圖 4 症狀知識本體

V. 根據症狀知識本體搜尋標準關鍵字詞詞類

症狀知識本體建立完成後，我們就依據症狀知識本體裡的標準關鍵字詞定義，找出要搜尋的標準關鍵字詞的詞類。

以標準關鍵字詞「大便」、「不暢」為例，本系統將會找出它們對應的詞類定義「症狀類別」、「症狀屬性值」，如**圖 5**。

VI. 搜尋標準關鍵字詞路徑

在找出要搜尋的標準關鍵字詞的詞類後，我們可以在症狀知識本體中，依據標準關鍵字詞的詞類之間的關係，搜尋出可能的路徑，用路徑來建立階層式標準症狀。

以標準關鍵字詞「大便」、「不暢」為例，由於它們與「狀態」這個「症狀屬性」都存在語意關係，因而形成一條路徑，建立了一個階層式標準症狀「大便:狀態:不暢 」，如**圖 6** 所示。

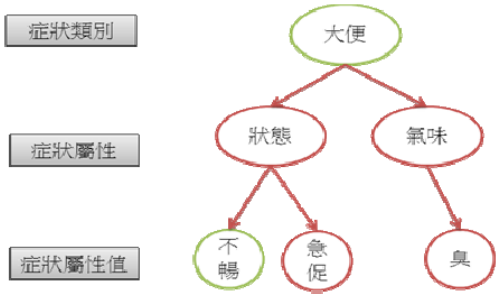


圖 5 關鍵字詞詞類對應

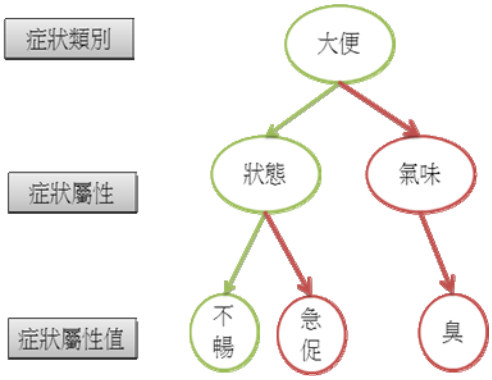


圖 6 關鍵字詞路徑

VII. 根據標準症狀對應表，對應階層式標準症狀到標準症狀

標準症狀對應表為標準症狀與階層式標準症狀的對應關係，因此我們利用此表，找出我們要搜尋的階層式標準症狀所對應的標準症狀，建議出此未標準化的原始症狀可能的標準症狀。

以階層式標準症狀「大便:狀態:不暢 」為例，它根據標準症狀對應表，如**表 3** 所示，找到符合之標準症狀「大便不暢 」，完成搜尋。

表 3 標準症狀對應表

標準症狀	階層式標準症狀
大便味臭	大便:氣味:臭
大便不暢	大便:狀態:不暢
大便挾血	大便:挾帶:血液
大便急促	大便:狀態:急促

以上步驟即為本系統將尚未經過標準化原始症狀「大便不通」，以關鍵字詞比對方式，提供建議的標準症狀「大便不暢 」的實作方法。

本系統的標準症狀對應表維護頁面如**圖 7** 所示，其功能分成三個部分，新增、修改、刪除資料庫的標準症狀以及階層式標準症狀。在此頁面上方按鈕為各個症狀類別按鈕，按下某一症狀類別按鈕後，會列出所有與此症狀類別相關的標準症狀以及對應之階層式標準症狀。因為目前資料庫中的標準症狀，並無法確定包含所有的標準症狀，所以使用者可以透過新增、修改、刪除功能，對標準症狀作維護。



圖 7 標準症狀對應表維護

本系統的關鍵字詞對應表維護頁面如**圖 8** 所示，其功能分成三個部分，新增、修改、刪除資料庫的關鍵字詞。在此頁面，會列出所有儲存在資料庫的關鍵字詞以及對應之標準關鍵字詞。因為目前資料庫中的關鍵字詞，無法包含所有可能的關鍵字詞，所以使用者可以透過此頁面進行關鍵字詞的變更。



圖 8 關鍵字詞對應表維護

本系統的症狀知識本體維護頁面如**圖 9** 所示，其功能分成三個部分，新增、修改、刪除資料庫的語意關係。在此頁面，會列出所有儲存在資料庫的語意關係。因為目前資料庫中的語意關係，沒有包含所有的語意關係，所以使用者可以透過此頁面進行語意關係的變更。



圖 9 症狀知識本體維護

7. 系統評估

我們先根據《中醫證候學》，在資料庫中建立了 1487 個已標準化的原始症狀。

《中醫症狀鑑別診斷學》[11]總共包含 500 個症狀，我們選用其中 190 個相關的症狀做測試。本系統可搜尋到的症狀共有 66 個，比例為 35%，而未搜尋到的症狀共有 124 個，比例為 65%。

在未搜尋到的 124 個症狀中，透過關鍵字詞搜尋，有 75 個症狀有提供建議標準症狀，比例為 60%，有 49 個症狀無提供建議標準症狀，比例為 40%。

在有提供建議標準症狀的 75 個症狀中，有 66 個症狀建議正確的標準症狀，比例為 88%，有 9 個症狀建議錯誤的標準症狀，比例為 12%。

因此，本系統以《中醫症狀鑑別診斷學》的 190 個相關症狀做測試，提供正確標準症狀 66 個，建議正確標準症狀 66 個，共 132 個，正確率為 69%。

我們在未使用關鍵字詞搜尋時，正確率為 35%，但是利用關鍵字詞語意資訊作搜尋，我們的正確率為 69%，有效地提升了原始症狀的搜尋能力。

8. 結論

本研究建立了一套中醫症狀詞庫系統，用來解決中醫症狀標準化的問題。我們除了使用「症狀字詞比對」的方式進行症狀標準化，還增加了使用「關鍵字詞比對」的方式進行症狀標準化。如果原始症狀已經過標準化，存在資料庫中，系統可透過症狀字詞比對正確地查詢到對應的標準症狀。如果原始症狀尚未經過標準化，不在資料庫中，系統會先將原始症狀拆成一串關鍵字詞，再透過關鍵字詞比對的方式，查詢這些關鍵字詞的語意。最後系統依據這些關鍵字詞的語意，查詢語意最接近的標準症狀。本研究顯示，運用語意資訊，可以明顯地提昇系統查詢標準症狀的正確率。

參考文獻

[1] 李洪成、李新平、李新曄：中醫證候學，中國醫藥科技出版社，大陸，2008。

[2] 柯廷諭：中醫症狀的結構化分析與標準化系統設計，碩士論文，國立中正大學資訊工程學系暨研究所，臺灣，2011。

[3] 李兵、劉國正、符永馳、裘儉、張偉娜：從中醫古籍數據庫建設看中醫古籍數字化，中國中醫藥信息雜誌，大陸，2009；16(3)：92-93。

[4] 林劉育：中醫症狀的標準化初探與應用，碩士論文，國立中正大學資訊工程學系暨研究所，臺灣，2011。

[5] 李宜泓：以近似字詞比對方法輔助中醫症狀標準化，碩士論文，國立中正大學資訊工程學系暨研究所，臺灣，2012。

[6] D. E. Knuth, J. H. Morris, V. R. Pratt, Fast pattern matching in strings. SIAM Journal on Computing, USA, 1977, 6(2): 323-350.

[7] R. S. Boyer, J. S. Moore, A fast string searching algorithm. Communications of ACM, USA, 1977, 20(10):762-772.

[8] R. Baeza-Yates, G. H. Gonnet, A new approach to text searching. Communications of ACM, USA, 1992, 35(10):74-82.

[9] K.-J. Chen, S.-H. Liu, Word identification for Mandarin Chinese sentences. Proceedings of the 14th COLING, USA, 1992, 101-107.

[10] J. F. Sowa, Semantic Networks, In Stuart C Shapiro. Encyclopedia of Artificial Intelligence, 1987.

[11] 姚乃禮、朱建貴、高榮林：中醫症狀鑒別診斷學，人民衛生出版社，大陸，2004。

中醫病因及臟腑辨證系統的研製

葉明憲
佛教慈濟綜合醫院
大林分院中醫科
yehlinlo@gmail.com

林育欣
國立中正大學
資訊工程學系
ninalin847@gmail.com

林迺衛
國立中正大學
資訊工程學系
naiwei@cs.ccu.edu.tw

摘要

辨證是中醫特有的臨床診斷形式。中醫的證型包含疾病的病因以及病位資訊，根據病患的症狀及體徵資訊來辨識疾病的病因及病位即是中醫的辨證。本論文根據《中醫證候學》的證型架構及審因定位的辨證方法，研製出一個中醫自動辨證系統。此系統包含病因辯證(辨識病因)及臟腑辨證(辨識病位)。本論文也利用《中醫證候學》的證候資訊(包含疾病的病因、病位、及病機資訊)來評估《中醫證候學》的證型架構及審因定位的辨證方法的一致性。評估結果顯示《中醫證候學》的證型架構及審因定位的辨證方法有相當高的一致性。

關鍵詞：證型、證候、中醫辨證、病因辯證、臟腑辨證

Abstract

Pattern identification in traditional Chinese medicine is a unique clinical diagnosis. Patterns in traditional Chinese medicine characterize the cause and location of the illness. Pattern identification identifies the cause and location of the illness according to the symptoms and signs of the patient. This thesis developed an automatic pattern identification system based on the pattern framework and the diagnostic method of cause differentiation and location determination in the book, Traditional Chinese Medicine Syndromes. This system includes cause identification (cause differentiation) and viscera and bowels identification (location determination). This thesis also utilized the syndrome (including the cause, location, and mechanism of the illness) information to evaluate the consistence of the pattern framework and the diagnostic method of cause differentiation and location determination in Traditional Chinese Medicine Syndromes. The evaluation results show that the pattern framework and the diagnostic method of cause differentiation and location determination in Traditional Chinese Medicine Syndromes reveal high consistence.

Keywords: pattern, syndrome, traditional Chinese medicine pattern identification, cause identification, viscera and bowels identification

1. 前言

《中醫證候學》[1]視疾病—稱為證—為一定的病因作用於一定的病位，而發生一系列動態的演變過程。中醫先透由望、聞、問、切等四診，取得病患的身體症狀資訊，再透由分析這些症狀資訊來辨識疾病的病因及病位，這個過程稱為辨證。《臨證指南醫案》[2]稱「若識證不明，開口動手便錯」，辨證是中醫的一大關鍵。

中醫歷史悠久，發展過程中融合了多項學科，內容十分廣博，光是辨證方法就包括八剛辨證、病因辨證、臟腑辨證、經絡辨證、六經辨證...等。而《中醫證候學》裡提出了審因定位的方法，即是審查症狀特徵後得知病因，並審定所犯之病位，就構成了證型的臨床診斷。而審因就是病因辨證，定位就是臟腑辨證。

《中醫證候學》將病因粗分為風、寒、熱、暑、濕、燥、火、氣、瘀、痰、飲、水、食、蟲、虛等 15 個證門。每一證門又再細分成若干證類，例如虛證門可分為氣虛、血虛、陰虛、陽虛等 4 個證類。15 個證門共分為 45 個證類。病位可分為心、肝、脾、肺、腎、胃、膽、腸等 8 類。每一證類可依病位分成若干證型。例如血虛證類可分為肝脾血虛、心脾血虛、心肝血虛、肝腎血虛等 4 個證型。45 個證類共分為 290 個證型。

然而在辨證之前中醫各家對相同症狀的描述卻有差異，再加上中文字的豐富多彩，對於症狀的描述更是複多樣，在某種程度上導致中醫症狀的不一致。於是本論文透過[4][5][6][7]取得標準症狀，依這些標準症狀進行病因及臟腑辨證系統的研製。

在《中醫證候學》裡每個證型包含大約 20 多個症狀，而許多相似的證型間僅有細微的差異。而讓電腦幫忙檢索並輔助判斷證型間的差異，就可提升判斷效率且降低錯誤率。於是研製了一個中醫病因及臟腑辨證系統(以下稱為本系統)，提供中醫研究的平台。本系統包含了病因辨證以及病位辨證。

2. 系統架構與設計

圖 1為本系統的架構圖，當逐一輸入病患的標準症狀時，會同時進行證門辨識、證類辨識及臟腑辨

證。輸入完病患的症狀，便可開始透由證門、證類及臟腑的排名順序，來推估病患可能的證型。

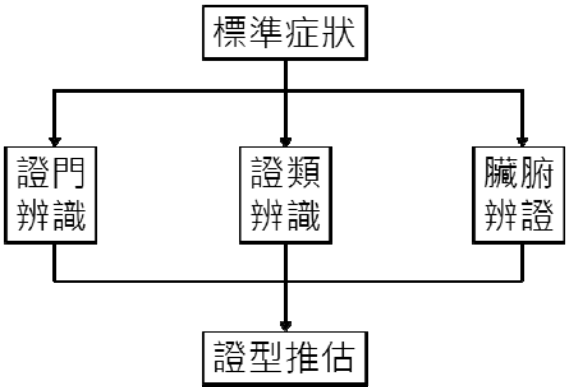


圖 1 系統架構

圖 2為本系統的介面設計，左欄可以輸入標準症狀，可以直接輸入，或用下拉式選單來選擇。輸入症狀後，中間欄位會呈現目前已經輸入的症標準狀。右邊三欄則會呈現目前證門、證類及臟腑的排序結果。

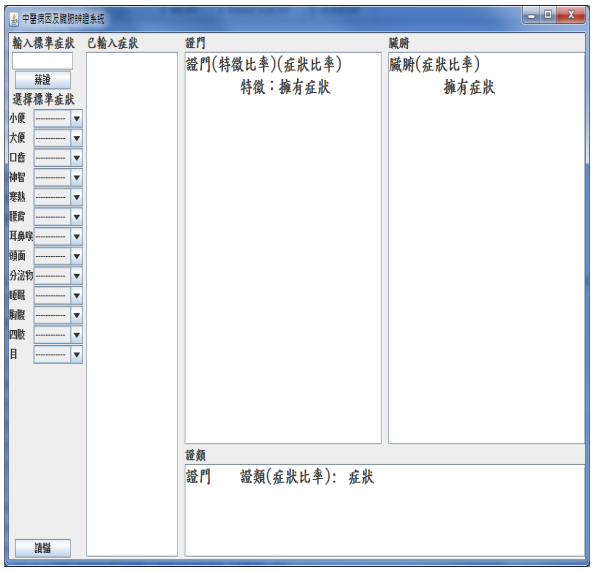


圖 2 系統介面

2.1 資料庫架構-標準症狀表

表 1是標準症狀中的小便類別，右邊欄位就是小便的標準症狀，將表 1轉化成 XML 檔儲存成標準症狀表如圖 3。標準症狀的屬性"size"為症狀類別的數量，也就是標準症狀有 13 個症狀類別。症狀類別的屬性"name"為症狀類別的名稱，"size"為該類別的症狀數量，標準症狀的第一個類別名稱為小便，此類別總共有 22 個症狀。

表 1 小便標準症狀列表

症狀類別	標準症狀				
小便	小便不暢	小便急促	小便不盡	小便失禁	小便疼痛
	小便灼熱	小便無力	小便挾血	小便挾精	小便挾砂
	小便挾膿	小便色清	小便色黃	小便色棕	小便色白
	小便色紅	小便味臭	小便次多	小便次少	小便量多
	小便量少	小便量不定	小便挾血	小便挾精	小便挾砂

```
<標準症狀 size="13">
  <症狀類別 name="小便" size="22">
    <症狀>小便不暢</症狀>
    ...
  </症狀類別>
  ...
</標準症狀>
```

圖 3 標準症狀表

2.2 資料庫架構-證門辨識表

每一證門都有 2~10 種特徵，每一特徵都有自己的原始症狀，而將原始症狀標準化後所得的標準症狀就是證門辨識的基礎。表 2是以虛證門為例的特徵、原始症狀及標準症狀，將表 2轉化成 XML 檔儲存成證門辨識表如圖 4。粗病因的屬性"size"為證門的數量，總共有 15 個證門。證門的屬性"name"為證門名稱，"property"為特徵名稱，"size"為每一特徵的症狀數量，虛證門的某一特徵為形氣衰減，此特徵總共有 7 個症狀。

表 2 虛證門的特徵、原始症狀及標準症狀表

虛證門		
特徵	原始症狀	標準症狀
少神	神衰萎糜，目瞑少神。	神疲、目瞑
形氣衰減	形體瘦弱或浮胖白嫩，倦怠乏力，氣怯少氣，或短氣似喘，身酸無力以動，懶言少語，聲輕微而短。	全身瘦弱、全身浮腫、四肢乏力、呼吸微弱、全身酸、寡言、聲弱
多汗	易汗，多汗或自汗不收，或夜間盜汗。	自汗、盜汗
喜按	脹痛時作，喜按，或頭痛，或脘、腹、腰痛。	喜按、頭痛、胃脘痛、小腹痛、腰痛

```
<粗病因 size="15">
  <證門 name="虛" property="形氣衰減"
      size="7">
    <症狀>全身瘦弱</症狀>
    ...
  </證門>
  ...
</粗病因>
```

圖 4 證門辨識表

2.3 資料庫架構-證類辨識表

每一證門分為若干證類，而每一證類都有自己的原始症狀，標準化後的標準症狀就是證類辨識的基礎，表 3為虛證門所有證類的原始症狀以及標準症狀。將表 3轉化成 XML 檔儲存成證類辨識表如圖 5。細病因的屬性"size"為證類的數量，總共有 45 個證類。證類的屬性"name"為證類名稱，"supername"為證類的父類別名稱，氣虛證類的父類別為虛證門，屬性"size"為每一證類的症狀數量，此證類總共有 11 個症狀。

表 3 氣虛證類的原始症狀及標準症狀

虛證門		
證類	原始症狀	標準症狀
氣虛	面淡黃或白，倦怠嗜臥，少氣乏力，自汗多汗，輕聲懶言，皮毛急薄毛落，食少便溏。	神疲、面色白、嗜睡、呼吸微弱、四肢乏力、自汗、寡言、聲弱、鬚髮脫落、食欲不振、大便泄瀉

```
<細病因 size="45">
  <證類 name="氣虛" supername="虛"
      size="11">
    <症狀>神疲</症狀>
    ...
  </證類>
  ...
</細病因>
```

圖 5 證類辨識表

2.4 資料庫架構-證類辨識表

《中醫證候學》裡並不是每一證門都包含所有臟腑，如表 4的虛證門僅擁有這六種臟腑的原始症狀。以心為例則出現在這些證門如表 5，而這些就是心的所有原始症狀，但是全部標準化後的標準症狀會太多，所以臟腑的標準症狀僅收錄重複次數多的標準症狀，如表 6為臟腑心的統計結果，括號內的數字代表此症狀出現的次數。

將表 6轉化成 XML 檔儲存成證類辨識表如圖 6。病位的屬性"size"為臟腑的數量，總共有 8 個臟腑。臟腑的屬性"name"為臟腑的名稱，屬性"size"為每一臟腑的標準症狀數量，臟腑心收錄了 9 個標準症狀。

表 4 虛證門的臟腑及其原始症狀

虛證門	
肺	短氣不續，聲低息短，面白多汗。
脾	倦怠少氣，少神懶言，面黃食少乏力，便溏，倦怠，嗜臥。
心	心悸怔忡，驚悸少寐。
胃	食少運遲，惡食，食後脹悶，早晨惡心吐涎，或嘈雜易飢。
肝	眩暈耳距，形寒內熱，夢擾紛紜，爪甲乾枯，筋脈攣急，麻木不仁。
腎	腰痛膝酸，小便頻數不禁，耳鳴耳聾，遺精滑泄，尾骶骨痛，足跟痛。

表 5 臟腑心的原始症狀及標準症狀

心	原始症狀	標準症狀
風	心悸怔忡，善忘易恐，善悲欲哭，或多笑，煩躁不安。	心悸、健忘、恐懼、悲傷、多笑、煩躁
燥	斑疹紅赤，神昏煩躁譫妄。	全身生斑、全身生疹、昏迷、煩躁、譫語
火	心煩不寐，躁擾不寧，入夜譫語，口舌生瘡，或多言喜笑，或語言顛倒，或昏迷不省。	煩躁、譫語、口瘡、多言、多笑、昏迷
氣	左胸痛，脅痛，煩滿短氣，心悸，臥起不安，或咯血瘀紫。	胸痛、脅痛、煩躁、呼吸微弱、心悸
痰	心煩不寐，神識如迷，甚則神昏譫語，或多言笑，或錯語妄言，或狂言舞蹈，或迷蒙昏厥。	煩躁、難眠、昏迷、譫語、多言、多笑
瘀	左胸痛引脅，或胸中攻刺痛，或咯吐瘀紫，或痛引肩臂。	胸痛、脅痛、吐血、肩痛、臂痛
虛	心悸怔忡，驚悸少寐。	心悸、難眠

表 6 臟腑心收錄的標準症狀

統計結果	心悸(3)、健忘、恐懼、悲傷、多笑(3)、煩躁(5)、全身生斑、全身生疹、昏迷(3)、譫語(3) 、口瘡、多言(2)、胸痛(2)、脅痛(2)、呼吸微弱、難眠(2)、吐血、肩痛、臂痛
標準症狀	心悸、多笑、煩躁、昏迷、譫語、多言、胸痛、脅痛、難眠

```
<病位 size="8">
  <臟腑 name="心" size="12">
    <症狀>心悸</症狀>
    ...
  </臟腑>
  ...
</病位>
```

圖 6 臟腑辨證表

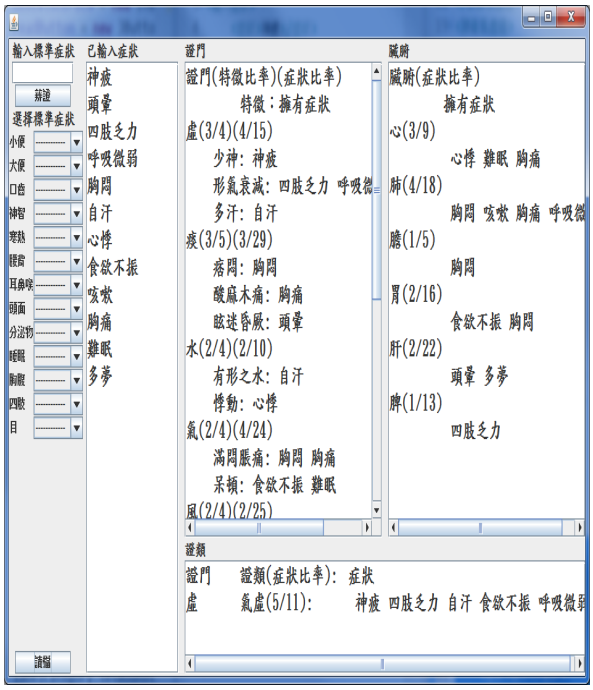


圖 8 心肺氣虛證

3. 系統實作

圖 7為程式流程圖，會先讀取所有資料庫，標準症狀表主要就是建立下拉式選單的選項，而證門辨識表、證類辨識表及臟腑辨識表則是後續辨證的判斷基礎。在讀取這三張表的同時，會給予其標準症狀相對應的證門、證門特徵、證類及臟腑的代碼，例如神疲這個標準症狀，此症狀屬於虛證門少神裡的某一症狀，在讀取的同時便會以陣列記錄成[神疲][14][76]，以方便後面記錄及統計。接著輸入標準症狀，每次輸入都會記錄及統計標準症狀次數，再將統計次數排序，最後呈現於視窗，當輸入完病患症狀後就可以推估證型了，圖 8為辯證範例，可以推估為心肺氣虛證。

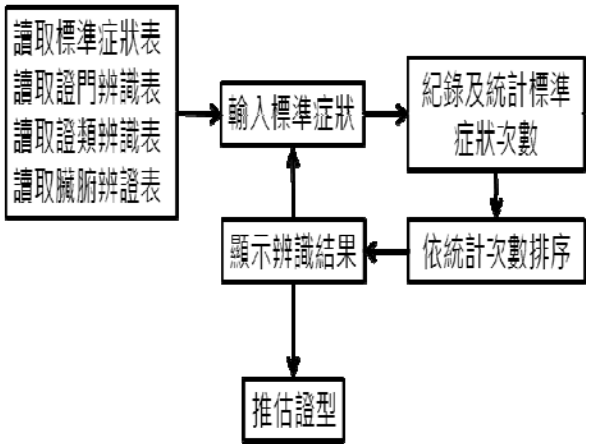


圖 7 程式流程圖

證門辨識的紀錄統計表包含了以下三個陣列：

1. [證門][特徵][症狀][1/0]：此陣列會記錄輸入的症狀，只要已經輸入的症狀有符合就會標記為 1。
2. [證門][特徵][1/0]：此陣列會記錄已經輸入的符合症狀屬於哪個特徵，只要有輸入一個特徵的症狀，此特徵就會被標記為 1。
3. [證門][特徵 n][症狀 n]：此陣列會統計目前輸入的符合特徵及症狀數量，之後會以此陣列作為排序的依據。

證類辨識的紀錄統計表包含了以下兩個陣列：

1. [證類][證門][症狀][1/0] ：此陣列會記錄輸入的症狀，只要已經輸入的症狀有符合就會標記為 1。
2. [證類][n] ：此陣列會統計目前輸入的符合症狀數量，之後會以此陣列作為排序的依據。

臟腑辨證的紀錄統計表包含了以下兩個陣列：

1. [臟腑][症狀][1/0] ：此陣列會記錄輸入的症狀只要已經輸入的症狀有符合就會標記為1。
2. [臟腑][n] ：此陣列會統計目前輸入的符合症狀數量，之後會以此陣列作為排序的依據。

記錄症狀的同時會讀取症狀相對應的證門及特徵、證類、臟腑代碼，就直接用代碼統計，而不用在記錄完之後再重新統計一次。而只要被標記為 1 的症狀及特徵，就不會被重複計算。統計之後，證門辨識會先依每一證門的特徵比率(符合特徵數量/總共特徵數量)排序，再依每一證門症狀比率(符合症狀數量/總共症狀數量)排序，而證類辨識及臟腑辨證皆是依症狀比率排序。

4. 系統評估

本系統以《中醫證候學》虛證門的 44 個證型做實測與評估。評估內容主要為每一證型的證門、證類及臟腑的排名，還有統計證門、證類及臟腑的辨識率。最後為這些統計結果下個結論。

4.1 證門辨識

表 7為證門辨識結果，僅列出氣虛證門 14 個證型以及血虛證門 4 個證型的辨識結果，證門欄位裡的數字代表此證型的證門排名為第幾名，例如肺脾氣虛證的虛證門在所有證門中排名為第一。若非第一名則會在名次後面列出排名在前的證門，例如胃腸氣虛證的虛證門排名為第三，第一名為食證門第二名為飲證門。但所屬證門不在排名上就會標記為"X"，例如肝肺氣虛證的虛證門未出現於排名。

表 7 證門辨識結果

證型	證門	證型	證門
肺脾氣虛證	1	脾胃氣虛證	1
肺衛氣虛證	1	胃腸氣虛證	3(食飲)
肺胃氣虛證	1	心脾氣虛證	1
心肺氣虛證	1	心肝氣虛證	1
肝肺氣虛證	X	肝脾氣虛證	1
肺腎氣虛證	1	脾腎氣虛證	1
肝脾血虛證	1	心肝血虛證	1
心脾血虛證	1	肝腎血虛證	1

表 8 證門辨識排名統計

證門	第一名	第二名	三名後
虛	41(93.1%)	0(93.1%)	3(100%)
氣	1(2.3%)	6(15.9%)	37(100%)
食	1(2.3%)	6(15.9%)	37(100%)
飲	1(2.3%)	4(11.4%)	39(100%)

表 8為表 7的統計結果包含其他證門的排名統計結果。欄位裡數字為此證門的排名數量，例如虛證門第一名的數量為 41 個，括號裡的比率是累加的比率，例如氣證門在前二名的比率為(1+6)/44×100%＝15.9%。

4.2 證類辨識

表 9為證類辨識結果，目前證類僅用虛證門的四個證類作為判斷基礎。證類欄位裡的數字代表此證型的證類排名為第幾名，例如肺脾氣虛證的氣虛證類在證類中排名為第一。若非第一名則會在名次後面列出排名在前的證類，例如肝肺氣虛證的氣虛證類排名為第三，第一名為陽虛證類第二名為血虛證類。所屬證類不在排名上就會標記為"X"。

表 10為表 9的統計結果。總數欄位的數字為44 個虛證門的證型中，此證類所占的個數。右邊欄位裡數字為此證類的排名數量，例如氣虛證類第一名的數量為 11 個。括號裡的比率為累加的比率，例如陽虛證類在前二名的比率為(6+6)/14×100%＝85.7%。比率欄位為四個證類的累加比率，例如所有證類在前二名的比率為(11+4+14+12)/44×100%＝93.2%。

表 9 證類辨識結果

證型	證類	證型	證類
肺脾氣虛證	1	脾胃氣虛證	1
肺衛氣虛證	1	胃腸氣虛證	1
肺胃氣虛證	1	心脾氣虛證	1
心肺氣虛證	1	心肝氣虛證	1
肝肺氣虛證	3(陽血)	肝脾氣虛證	1
肺腎氣虛證	1	脾腎氣虛證	1
肝脾血虛證	2	心肝血虛證	2
心脾血虛證	2	肝腎血虛證	2

表 10 證類辨識排名統計

總數	證類	第一名	第二名	三名後
12	氣虛	11(91.7%)	0	1(100%)
4	血虛	0	4(100%)	0
14	陰虛	8(57.1%)	6(100%)	0
14	陽虛	6(42.9%)	6(85.7%)	2(100%)
44	比率	56.8%	93.2%	100%

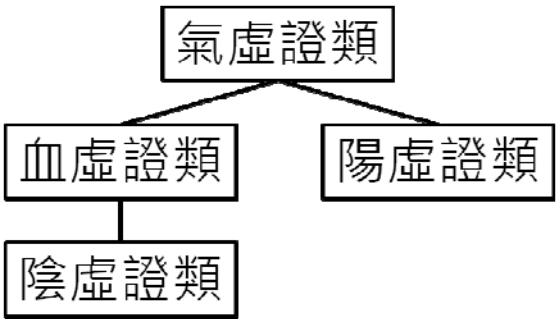


圖 9 虛證門四個證類關係圖

證類辨識的辨識率為 56.8%，本系統將虛證門的四個證類獨立來看，但《中醫證候學》裡有提到「氣統於血，氣能生血，故氣虛者易致血虛；血能裁氣，血虛者氣亦不足。尤以失血家，多氣隨血脫，是血虛亦能至於氣虛，故多氣血兩虛之證。」而四個證類亦有深淺關係如圖 9，若納入此關係則辨識率高達 93.2%。

4.3 臟腑辨證

表 11為臟腑辨證結果。臟腑欄位裡的數字代表此證型的臟腑排名為第幾名，例如肺脾氣虛證的

肺在臟腑排名為第一名，脾的排名為第二名。只要有其中一個不是第一名亦不是第二名則會在名次後面列出排名在前的證類，例如脾胃氣虛證的脾排名為第一名，胃的排名為第三名，那第二名為腸。所屬臟腑不在排名上就會標記為"X"，例如肝脾血虛證的脾未出現於排名。

表 11 臟腑辨證結果

證型	臟腑	證型	證類
肺脾氣虛證	1, 2	脾胃氣虛證	1, 3(腸)
肺衛氣虛證	X	胃腸氣虛證	4, 5(膽 肝脾)
肺胃氣虛證	1, 2	心脾氣虛證	2, 1
心肺氣虛證	1, 2	心肝氣虛證	1, 2
肝肺氣虛證	3, 2(脾)	肝脾氣虛證	2, 1
肺腎氣虛證	1, 2	脾腎氣虛證	2, 3(腸)
肝脾血虛證	2, X(心)	心肝血虛證	1, 2
心脾血虛證	1, 2	肝腎血虛證	1, 2

表 12 臟腑辨證排名統計

總數	臟腑	第一名	第二名	三名後
13	心	11(84.6%)	2(100%)	0
16	肝	3(18.8%)	11(87.5%)	2(100%)
17	脾	9(52.9%)	6(88.2%)	2(100%)
15	肺	7(46.7%)	6(86.7%)	2(100%)
13	腎	1(7.7%)	10(84.6%)	2(100%)
11	胃	3(27.3%)	2(45.5%)	6(100%)
2	腸	1(50%)	0	1(100%)
87	比率	40.2%	82.8%	100%

表 12為表 11的統計結果。總數欄位的數字為 44 個虛證門的證型中，此臟腑所占的個數，例如 44 個證型中包括心的證型有 13 個。右邊欄位裡數字為此臟腑的排名數量，例如心的第一名數量為 11 個。括號裡的比率為累加的比率，例如肝在前二名的比率為(3+11)/16x100%＝87.5%。比率欄位為八個臟腑的累加比率，例如所有臟腑在前二名的比率為(13+14+15+13+11+5+1)/87x100%＝82.8%。由於《中醫證候學》裡每一證型都由兩個臟腑組成，故臟腑辨證的辨識率為前二名的累加比率 82.8%。

由於目前的臟腑辨證表裡的標準症狀，是篩選重覆比率較高的症狀，所以可能忽略了某些判斷標準，才會導致臟腑辨證的辨識率不及證門和證類的辨識率。

5. 結論

本系統根據《中醫證候學》研製一個中醫病因及臟腑辨證系統。病因辨證又分為證門辨識及證類辨識，證門辨識的辨識率為 93.1%，而證類辨識的辨識率為 56.8%，但把證類間的關係性納入考量，那辨識率就會有 93.2%。臟腑辨證因每個證型都含有兩個臟腑，故直接納入前二名的辨識率為 82.8%。

雖然目前的辨識率都在可接受的範圍，但應該要想辦法提高辨識率。可以先往資料庫方面進行微調以達成更高的辨識率。病因辨證方面，每個證門、證類看似獨立其實之間都有相當的關係性，若是能將這層關係性納入本系統，想必能提高辨識率。而在臟腑辨證方面，辨識率不及證門辨識和證類辨識，可能跟臟腑辨證表有關，由於目前臟腑辨證表僅收錄重複性較高的標準症狀作為辨證基礎，或許將全部標準症狀納入後反而能提升辨識率。

本系統的資料來源是《中醫證候學》，評估的輸入資料亦是《中醫證候學》所提供。本系統因此驗證了《中醫證候學》的一致性，就評估結果來看《中醫證候學》的一致性是相當高的。

參考文獻

[1] 李洪成、李新平、李新曄：中醫證候學，中國醫藥科技出版社，大陸，2008.

[2] 葉桂：臨證指南醫案，清，1746.

[3] 李紹良、余明哲、陳國樹、詹寬仁：中醫診斷學，東大圖書股份有限公司，台北市，2008

[4] 林劉育：中醫症狀的標準化初探與應用，碩士論文，國立中正大學資訊工程學系，台灣， 2011.

[5] 科廷諭：中醫症狀的結構化分析與標準化系統設計，碩士論文，國立中正大學資訊工程學系，台灣， 2011.

[6] 李宜泓：以近似字詞比對方法輔助中醫症狀標準化，碩士論文，國立中正大學資訊工程學系，台灣， 2012

[7] 郭慧翔：中醫症狀詞庫的研製，碩士論文，國立中正大學資訊工程學系，台灣， 2013

環境災害管理資訊系統行動通訊軟體之建置

吳効遵　　羅榮華
佛光大學資訊應用學系
992762@mail.fgu.edu.tw
jhlo@mail.fgu.edu.tw

摘要

台灣是位於副熱帶季風區的海島型氣候國家以及位於歐亞大陸板塊與菲律賓板塊交接處，因此天然災害的發生頻率相當的頻繁。近年來全球的氣溫暖化與氣候異常，極端氣候發生除了頻率上升及強度增強外，一般災害的發生常會直接或間接的引響其他的災害，形成一種鏈結的關係，其造成的損害常常遠大於單一的災害。當天然災害發生時也有可能伴隨著發生停電等情況使得各地方的災情無法即時進行回覆通報，而無法控制災情蔓延等後果，造成社會及民眾與經濟的重大損失，有鑑於此本文為了便於各使用者能在緊急情況發生時，可避免受到各種不可抗拒之侷限下即時的進行通報各項災情資訊與各項支援的請求。因此開發 Android 版本的「環境災害管理資訊系統行動通訊軟體」(Emergency Management Information System Application 以下簡稱:EMIS APP)，讓使用者在災區可以進行快速且簡便的通報各項災害損失、上傳災區照片、請求支援等。此外由於災區常位於克難且無網路環境之中以及手機電池效能都將在本文之中進行討論。

關鍵詞：行動裝置開發(Mobile device develop)、網際網路服務(Web Service)、環境災害管理資訊系統(Emergency Management Information System)。

1. 前言

近年來的氣候變遷，不論是颱風、地震等天然災害的威力越來越強大，其破壞的程度也越來越高，有鑑於此，[1]民國 89 年我國制定「災害防救法」，以建立完整的災害防救體制，強化災害防救功能。其中為了減少災害所導致的環境污染，加速環境恢復，環保署依災害防救法第十四條規定，凡環境有發生災害之虞或已發生災害時，設置「行政院環境保護署災害防救緊急應變小組」以督導辦理災情通報、請求支援、環境清理、垃圾處理場廠區安全回報、消毒飲用水處理及水質抽驗等業務。基於災害通報處理時效所需、資源建立和管理的重要性、防災及決策支援資訊提供的便捷性等，開發「環境災害管理資訊系統」，供使用者利用線上方式進行環境災害的通報、查詢、管考等服務。因此考量到使用者至災區需先做紀錄再至個人電腦或筆記型電腦連至網站登入災情相關訊息，無法有效率的快速完成通報耗時且步驟繁瑣，因此開發此 EMIS APP 的目的為使用者至災區可以快速的完成回報、災區照片上傳、災區範圍回報與各項的人力、藥劑、車輛、補助款的請求，藉此達成有效率的回報通知，給予決策者立即可以了解目前災害的程度與狀況。因災區情況通常較為不便，所以規劃設計時希望以「精簡、整齊、單欄」為設計概念，畫面中不適合提供過多的資訊，否則容易顯得畫面擁擠且不易閱讀所以資訊的提供皆以精簡為主，在資訊的提供上除精簡外，皆以排列整齊以提高使用者對資料的閱讀性，由於目前智慧型手機具備觸控式螢幕因此使用者皆習慣以手指碰觸螢幕直接進行操作，因此在各項連結上皆以大圖示為主，以加強使用者的操作性。

2. 系統架構與開發流程

系統架構與開發流程共分為「系統架構」、「開發流程」、「網際網路服務」三區塊進行說明。

2.1 系統架構

EMIS APP 的系統架構主要分為三大部分，分別為「整備通報」、「災情通報」、「請求支援」三大區塊，以下將會說明三大區塊的功能與使用流程細節，系統架構如下圖 1 所示。

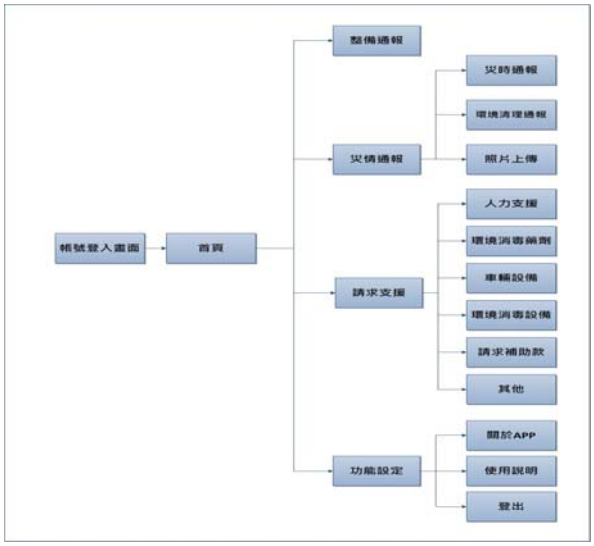


圖 1 系統架構

2.2 開發流程

2.2.1 災害前

當中央氣象局發佈海上颱風警報時，EMIS APP 會隨即取得由伺服器端建立啟動的災害名稱，當使用者登入之後進入首頁即會看到整備通報出現剛建立的災害名稱，便可開始進行災前的整備通報，進入「整備通報」頁面後可選擇要進行通報的災害名稱，並勾選人員以及設備是否皆已完成待命狀態，確認完畢後即可進行上傳通報動作。

2.2.2 災害中

當中央氣象局發佈陸上颱風警報時，使用者會於首頁畫面看到災情通報的災害已由無須通報變更為請通報，提醒使用者進行災害通報，當使用者進入「災害通報」畫面後，可選擇要進行通報的災害名稱並填寫災害面積與勾選是否有掩埋場或焚化廠損壞與預估廢棄物量，下方可填寫已完成的各項已完成處理的數量及已動用的人員，並於最後進行拍攝災區照片確認完畢後即可進行上傳通報動作。

2.2.3 災害中及災害結束

當中央氣象局已發佈陸上颱風或已解除時，進行災後環境整理及恢復時，使用者可進入「請求支援」頁面選擇需要的請求項目分別為「人力支援」、「環境消毒藥劑」、「車輛設備」、「環境消毒設備」、「請求補助款」、「其他」六項請求，進入各頁面後可選擇要通進行通報的災害名稱並填寫請求日期與請求所需資料，確認完畢後即可進行上傳通報動作。開發流程如下圖 2 所示。

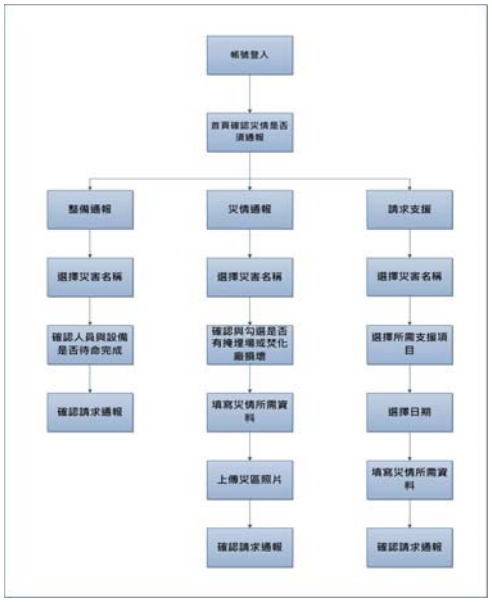


圖 2 系統架構

2.3 網際網路服務

EMIS APP 中各介面與伺服器網頁進行資料交換皆以 JSON 格式進行，其資料內容包含資料表名稱、欄位名稱、資料類型。各資料表編號、中英文名稱及用途如表 1 所示。

表 1 網際網路服務清單

編號	名稱(中文)	名稱(英文)	用途
W001	登入	wCheck_Login	登入驗證帳號與密碼
W002	災害名稱	wDisaster	判斷是否有災害
W003	整備通報	wPreparation	判斷是否有整備通報資料
W004	整備通報新增與修改	wPreparationSQL	整備通報新增或修改
W005	掩埋場與焚化廠	wTrash	所在縣市的焚化或掩埋廠
W006	災情通報檢驗	wAddDmaCheck	判斷是否有災情通報資料
W007	災情通報新增	wAddDmaInsert	災情通報新增
W008	災情通報修改	wAddDmaUpdate	災情通報修改

3. EMIS APP 成果展示

EMIS APP 成果展示共分為十一區塊，進行手機實際操作介面與說明。

3.1 登入帳號及密碼介面

當使用者首次登入 EMIS APP 時可利用原來在「環境災害管理資訊系統」中所申請的帳號與密碼登入 EMIS APP，為便於使用者之後能快速登入 EMIS APP 及當登入 EMIS APP 後會自動進入後台常駐程式，故本程式不會自行登出使用者帳號。因災區常發生較於不便且克難的地方，EMIS APP 為求進入災區後因應隨時會發生的無網路狀態，因此當氣象局發佈海上警報時伺服器端會隨即啟動該災害的名稱，使用者只要於 EMIS APP 於有網路狀態時取得過最新災害名稱後，即便進入災區處於無網路狀態仍可正常操作。登入介面如下圖 3 所示。



圖 3 登入帳號密碼介面



圖 4 首頁介面

3.2 首頁介面

當進入後使用者可看到已開啟的災害名稱，並分為「整備通報」、「災情及環境清理通報」、「請求支援」三大項目。首次進入颱風發佈海上颱風警報時「整備通報」會出現請通報及未通報兩種狀態提醒使用者是否完成災前通報佈署，而發佈陸上颱風警報時「災情及環境清理通報」會由無須通報更換為請通報及未通報兩種狀態，亦提醒使用者進行災害狀況通報，當颱風登陸中及解除時所申請的各項請求支援可於「請求支援通報」項目中觀看該筆災害的各項請求數量以確定是否足夠運用。整備通報及災情環境清理通報兩大項目於完成通報後送出時可至首頁觀看資料狀態，分別為上傳成功、通報完成、上傳失敗，當使用者按下確認通報後如資料傳送完畢會出現日期時間及綠燈通知使用者以上傳成功，但若災區發生無網路狀態時資料為傳送完畢則會出現通報完成的黃燈，系統將會自動每二十分鐘將傳送一次資料至伺服器，持續兩小時若時間內無法接收網路訊號則會放棄該筆資料並更改至上傳失敗的紅燈。設計時考慮到使用者長時間在外進行通報及可能同時出現多個颱風或災害的發生導致手機電力不足，故設計時以一天時間做測試，系統以二十分鐘發送一次傳送最為恰當。首頁介面如下圖 4 所示。

3.3 整備通報介面

中央氣象局發佈海上颱風警報時，可進入整備通報中選擇該災害名稱並勾選其已完成的佈署動作後便可進行通報，確定後會彈跳視窗告知使用者已送出資料，整備通報內容則所屬單位不同會有不同的勾選項目。整備通報介面如下圖 5 所示。



圖 5 整備通報介面

3.4 災情通報介面

中央氣象局發佈陸上颱風警報時，可進入災情通報中選擇災害名稱，並於災時通報中勾選有無掩埋場或焚化廠損壞，如勾選後會跳出新增掩埋場或焚化廠選項(圖 6 左下)，點選後即彈跳使用者該轄區內的掩埋場及焚化廠供使用者勾選(圖 6 左上)，並於環境清理通報中填寫目前已完成的作業及已動用的人員數量，最後並於上傳照片項目中可開啟相機功能及從相簿中選擇照片，並於畫面中進行預覽，確認通報內容後按下確認請求會彈跳視窗告知使用者已送出資料。災情通報介面如下圖 6 所示。



圖 6 災情通報介面

3.5 請求支援介面

進入請求支援畫面後共有六大項目「人力支援」、「環境消毒藥劑」、「車輛設備」、「環境消毒設備」、「請求補助款」、「其他」可供使用者選擇需要請求的支援。請求支援介面如下圖 7 所示。



圖 7 請求支援介面

3.6 人力支援介面

人力支援介面可選擇災害名稱，選擇完畢後點選需用日期圖片即跳出日期選擇視窗(圖 8 右上方)，下方則可填寫需請求的國軍及清潔隊人數與天數確認後。如有日期未選擇或國軍與清潔隊的人數與天數其一為空白則下方會提醒使用者未填選項目(圖 8 左上)，當日如已申請過此支援按下確認後則會提醒使用者當日已請求完畢是否要再次新增請求(圖 8 右下)。人力支援介面如下圖 8 所示。

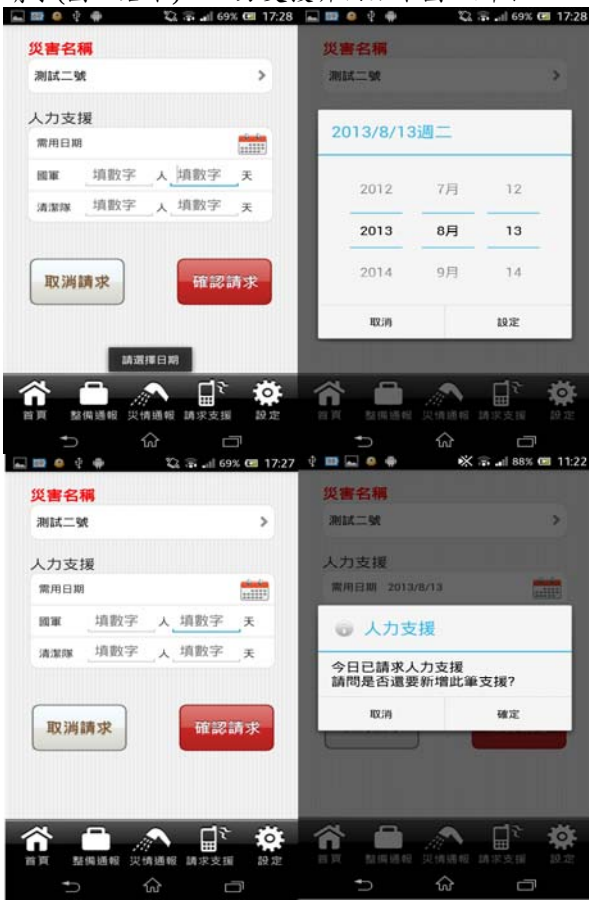


圖 8 人力支援介面

3.7 環境消毒藥劑介面

環境消毒藥劑介面可選擇災害名稱，選擇完畢後點選需用日期圖片即跳出日期選擇視窗，下方點選新增環境消毒藥劑則出現多選項視窗(圖 9 右方)，勾選後確定即新增已選擇項目供使用者填寫(圖 9 左方)。當日如已申請過此支援按下確認後則會提醒使用者當日已請求完畢是否要再次新增請求。環境消毒藥劑介面如下圖 9 所示。



圖 9 環境消毒藥劑介面

3.8 車輛設備介面

車輛設備介面可選擇災害名稱，選擇完畢後點選需用日期圖片即跳出日期選擇視窗，下方點選新增車輛設備則出現多選項視窗(圖 10 右方)，勾選後確定即新增已選擇項目供使用者填寫(圖 10 左方)。當日如已申請過此支援按下確認後則會提醒使用者當日已請求完畢是否要再次新增請求。車輛設備介面如下圖 10 所示。



圖 10 車輛設備介面

3.9 環境消毒設備介面

環境消毒設備介面可選擇災害名稱，選擇完畢後點選需用日期圖片即跳出日期選擇視窗，下方點選新增環境消毒設備則自動新增欄位，供使用者填寫(圖 11 右方)亦可刪除欄位。當日如已申請過此支援按下確認後則會提醒使用者當日已請求完畢是否要再次新增請求。環境消毒設備介面如下圖 11 所示。



圖 11 環境消毒設備介面

3.10 請求補助款介面

請求補助款介面可選擇災害名稱，選擇完畢後點選需用日期圖片即跳出日期選擇視窗，下方供使用者填寫請求補助款金額(圖 12)。當日如已申請過此支援按下確認後則會提醒使用者當日已請求完畢是否要再次新增請求。請求補助款介面如下圖 12 所示。



圖 12 請求補助款介面

3.11 其他請求介面

其他請求介面可選擇災害名稱，選擇完畢後點選需用日期圖片即跳出日期選擇視窗，下方點選新增其他則自動新增欄位，供使用者填寫(圖 13 右方)亦可刪除欄位。當日如已申請過此支援按下確認後則會提醒使用者當日已請求完畢是否要再次新增請求。其他請求介面如下圖 13 所示。



圖 13 其他請求介面

4. 結論與未來展望

4.1 結論

本研究利用智慧型手機的功能性、普及性與方便攜帶性的特色來做建置，對於一般傳統使用者進入災區後須以筆記型電腦、紙本記錄或以手機進行語音通報相對不方便，因此 EMIS APP 除加強使用者回報系統的效率提高外，並可直接上傳照片省去使用者須以相機照相後進行轉換格式的時間，同時也提供使用者進入災區時發生無網路狀態無法回報時，可以將資料於手機做暫存動作，並等待手機接收到網路訊號時即可自動將資料全數送出，以避免資料遺失等情況，對於使用者與決策者來說提供更多災前與災後來進行預防災害與了解災情狀況，加速災後修復的工作。

4.2 未來展望方向

本研究所建置的 EMIS APP 方向目標朝著快速、方便、精簡易懂的目標前進，但就功能面來說可以再結合擴增實境(Augmented Reality，AR)，因有時災區常發生全毀的狀況如地震、淹水，這時的災區有時無法分辨其原貌與位置，可以靠擴增時境及 Google maps 的定位與模擬恢復其原來的地形及建築方便使用者了解，此功能需建置相當龐大的資料庫系統，期望未來資料充足時如何把擴增實境功能加入 EMIS APP 裡提供使用者更方便、更快速的系統來保護我們的家園安全，是我們進一步研究的目標與方向。

5. 致謝

本研究承蒙國科會(計畫編號:NSC100-2221-E-431-002) 及佛光大學「行動式旅遊導覽平台建置」專題計畫經費贊助，方達科技股份有限公司提供「環境災害管理資訊系統」之究研所需相關資料，使本研究得以順利完成，謹此誌謝。

參考文獻

[1] “災害防救法暨相關規定”,行政院環境保護署網站,http://www.epa.gov.tw .

[2] 潘逸華,“消防勤務派遣輔助功能 Android App 開發一以臺東縣消防局為例”,國立臺東大學資訊管理學系碩士班碩士論文,民 101.

[3] 呂仁貴, “Android 行動旅遊系統-以高雄市風景區為例” 崑山科技大學資訊管理研究所碩士論文,民 101.

[4] 吳昌潭,“適性化校園資訊於 Android 平台上之實現”,國立高雄第一科技大學電腦與通訊工程研究所碩士論文,民 100.

[5] 佘志龍、陳昱勛、鄭名傑、陳小鳳,“Google Android SDK 開發範例大全第 3 版”,悅知文化, 2011.

[6] 孫宏明, “Android 4.X 手機/平板電腦程式設計入門、應用到精通(第二版--適用 Android 1.X~4.X)”, 碁峰, 2012.

基於 Wi-Fi 與 Bluetooth 混合式無線識別技術門禁控制系統之設計與實作

徐茂馨[a] 劉嘉惟[a] 高駿嘉[a] 廖子翔[a] 蘇暉凱[a*] 楊明達[b]
[a]國立虎尾科技大學 電機工程系
[b]工業技術研究院
[*]hksu@nfu.edu.tw

摘要

本文提出一個基於 Wi-Fi (Wireless-Fidelity) 與 Bluetooth 通訊技術之連線特性的裝置識別方法，以減少在使用 Wi-Fi 與 Bluetooth 通訊技術建立資料連線時所需的人為操作，且將此方法整合現階段具普遍性之 RFID (Radio Frequency Identification) 及 NFC (Near Field Communication) 識別技術，完成一套「基於 Wi-Fi 與 Bluetooth 混合式無線識別技術門禁控制系統」。本系統主要架構分為三個子系統：門禁控制器 (Door Controller，DC)、門禁控制閘道器 (Door Control Gateway，DCG) 及門禁控制中心 (Door Control Center，DCC)。門禁控制器依無線通訊技術的支援種類來區別，可分為高階門禁控制器 (High-End Door Controller，H-EDC) 及低階門禁控制器 (Low-End Door Controller，L-EDC) 兩種，其主要藉由多種無線通訊技術來識別使用者所持之識別媒體，並決策其入口的通行開放與否；門禁控制閘道器除了負責監控多個門禁控制器之外，更扮演著門禁控制中心與門禁控制器之間的橋樑。門禁控制器將其產生之識別記錄傳送至門禁控制閘道器，門禁控制閘道器會藉此將識別記錄顯示於 GUI (Graphic User Interface) 並傳送至門禁控制中心進行儲存；門禁控制中心與多個門禁控制閘道器連接來管理各個區域，並透過門禁控制閘道器來管控其底下之門禁控制器。此外，門禁控制中心提供系統管理者與一般使用者兩種角色之操作介面，除了能讓系統管理者進行管理之外，亦可讓一般使用者查詢個人資料與識別紀錄。在系統反應時間之效能測試部分，高階/低階門禁控制器之反應時間皆小於 31ms，故依系統實測及效能評估之結果來觀察，減少了以往在使用 Wi-Fi 與 Bluetooth 通訊技術時多餘的人為操作。
關鍵詞：門禁控制、無線身分識別技術、無線網路、藍芽、近場通訊、無線辨識。

Abstract

This master thesis proposed a device identification method based on the connection property of Wi-Fi and Bluetooth to reduce human operating. The method of device identification integrates with RFID and NFC technology, and implements a door control system with the hybrid wireless identification technology based on Wi-Fi and Bluetooth. This system is divided into three subsystems: Door Controller (DC), Door Control Gateway (DCG) and Door Control Center (DCC). DC is separated to two types according to the ability of the controller: High-End Door Controller (H-EDC) and Low-End Door Controller (L-EDC). Such controllers can identify user device with wireless technologies and control door lockers. In the proposed system, each area has a DCG, and each DCG connects to DC. Thus, DCG also is a bridge between DCC and DC. DCs will send identification records to DCG. The identification record can be shown and stored on the DCG. The DCC is to manage multiple DCGs. Moreover, DCC provides the functions of system management and door-access log for administrators and users. Additionally, the system performance was measured, and the identification time of H-E/L-EDC is less than 31ms. Therefore, according to the result of system performance, the human operating can be reduced when using the door control system with hybrid wireless identification technologies.
Keywords: Door Control, Wireless Identification Technology, Wireless Network, Bluetooth, Near Field Communication, Radio Frequency Identification.

1. 前言

在過去有關於身分識別方法的相關研究中，曾出現透過 Wi-Fi 與 Bluetooth 通訊技術來進行身分識別之研究[3-5]。在這兩種無線通訊技術的環境底下，使用者所持之識別媒體須事先建立與門禁控制器之間的連線後，該裝置才能與門禁控制器交換識別資料或控制指令來進行身分辨識。例如，在 Wi-Fi 通訊技術下，識別媒體須事先加入門禁控制器所在的無線區域網路內，並成功建立 TCP Socket 或者 UDP Socket 之連線後，才能與門禁控制器進行識別資料或控制指令的交換；而在 Bluetooth 通訊技術下，識別媒體與門禁控制器於連線前須進行掃描以及裝置配對，等待配對完成並建立連線後，才能進行識別資料或控制指令的交換。

由上述可得知在進行 Wi-Fi 及 Bluetooth 連線的前置作業下，將會花費較多作業時間以及繁瑣的前置設定。故若以反應時間及實用性層面來考量，皆會發現以下問題：1. 識別媒體須事先安裝該識別系統之應用程式；2. 識別媒體皆須針對門禁控

制器進行繫鎖的前置設定；3. 識別媒體與門禁控制器建立資料傳輸通道後，以交換資料方式來進行身分識別之行為，因此考慮其人為操作時間以及使用便利性的改進空間仍然很大。

本文為改善原先使用 Wi-Fi 與 Bluetooth 通訊技術進行身分識別時，會耗費太多時間在前置設定作業之人為操作上，故提出一個不同於過去使用 Wi-Fi 與 Bluetooth 通訊技術相關系統之識別方法，並以減少識別媒體之人為操作、不影響識別媒體之連線狀態及確保識別媒體之唯一性為目標，且整合現階段具普遍性之 RFID 及 NFC 技術，完成一套「基於 Wi-Fi 與 Bluetooth 混合式無線識別技術門禁控制系統」。

2. 相關知識背景

本文利用 Wi-Fi 與 Bluetooth 之連線特性提出混合式無線識別技術。在 Wi-Fi 識別部分，Wi-Fi 訊框之擷取方式是利用運行於 Monitor 模式之無線網路裝置來進行。由表 1 所示，參考 To DS 及 From DS 可得知當 STA 在傳收無線網路訊框時，路徑 1 以及路徑 2 之訊框以發送者 MAC Address 作為識別依據；路徑 3 之訊框則是以接收者 MAC Address 為識別依據；路徑 4 為 AP 之間交換的訊框，故不加以參考。綜合上述方法來作為混合式無線識別技術之 Wi-Fi 部分。如圖 1 所示，在混合式無線識別技術之 Bluetooth 部分，則是藉由 Master 裝置對 Slave 裝置發送 Inquiry 訊息後，Slave 裝置傳回具唯一性之 BD_ADDR，藉此來做為 Bluetooth 裝置識別之依據。本文除了提出上述之 Wi-Fi 裝置識別方法與 Bluetooth 裝置識別方法外，亦整合入了現階段最具普遍性之 RFID 識別方法及 NFC 識別方法，完成一套門禁控制系統。

表 1 Wi-Fi 訊框資料流向路徑表

Frame Type	Path	To DS	From DS	Addr1	Addr2	Addr3	Addr4
IBSS	1	0	0	DA	SA	BSSID	x
To AP	2	1	0	BSSID	SA	DA	x
From AP	3	0	1	DA	BSSID	SA	x
WDS	4	1	1	RA	TA	DA	SA

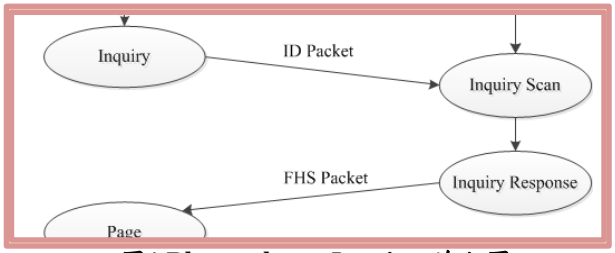


圖1 Bluetooth 之 Inquiry 流程圖

3. 系統架構

本文利用 Wi-Fi 之訊框特性及 Bluetooth 建立連線前之 Inquiry 作業所出現的連線特性，提出一個基於 Wi-Fi 與 Bluetooth 通訊技術之裝置識別方法，並將該方法整合目前具普遍性之 RFID 與 NFC 身分識別方式，完成一套「基於 Wi-Fi 與 Bluetooth 混合式無線識別技術門禁控制系統」。而該系統主要可分為四個部分來討論：

- 第一部分：介紹基於 Wi-Fi 與 Bluetooth 混合式無線識別技術門禁控制系統之系統架構及運作流程。
- 第二部分：介紹子系統-高階/低階門禁控制器之系統架構及運作流程。
- 第三部分：介紹子系統-門禁控制閘道器之系統架構及運作流程。
- 第四部分：介紹子系統-門禁控制中心之系統架構及運作流程。

本文所提出的「基於 Wi-Fi 與 Bluetooth 混合式無線識別技術門禁控制系統」之系統架構如圖 2 所示，主要可分為三個子系統：門禁控制中心、門禁控制閘道器以及門禁控制器。

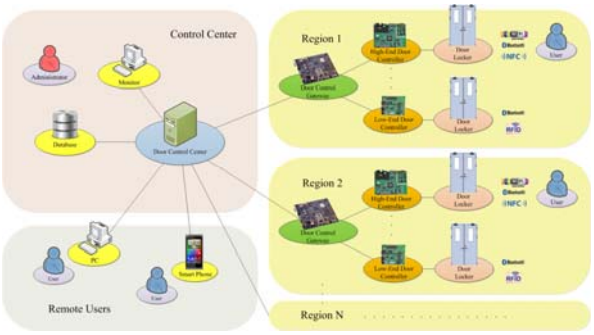


圖 2 門禁控制系統之系統架構

門禁控制中心擁有一個中央資料庫，負責儲存識別媒體之相關資料、門禁控制閘道器與門禁控制器相關設定以及使用者之識別記錄...等功能，並提供操作介面給予系統管理者進行識別媒體與系統裝置的資料編輯。另外，門禁控制中心亦提供一般使用者之操作介面，讓使用者可查詢個人相關資訊。而門禁控制中心為了達到多重區域控管之目的，將與多個門禁控制閘道器連接，使其可藉由門禁控制閘道器來進行多重區域控管；門禁控制閘道器除了扮演著區域管理者的角色以及監控多個門禁控制器之外，更扮演著門禁控制中心與門禁控制器之間的橋樑，使門禁控制器識別後所產生之識別記錄，能透過門禁控制閘道器傳送至門禁控制中心進行識別記錄之儲存；而高階/低階門禁控制器扮演著出入口的把關者，透過多種無線通訊技術來識別使用者所持識別媒體，負責開放通行與否的決策。

4. 系統設計與實作

本文所提出之基於 Wi-Fi 與 Bluetooth 混合式無線識別技術門禁控制系統可分為門禁控制器、門禁控制閘道器及門禁控制中心等三個子系統，各子系統皆負責不同之工作，在本章將討論各子系統軟硬體之相關設計。

4.1 高階門禁控制器設計

如圖 3 所示為高階門禁控制器硬體元件圖，高階門禁控制器採用 ADI Engineering Sidewinder 為系統開發平台，其核心為 IXP465。由於 Sidewinder 已提供 USB 2.0 通訊介面，因此 USB to GPIO 模組可直接透過 USB 連接至 Sidewinder；NFC 模組須將其 TTL 電位轉換為 RS232 電位後，再透過 USB to Serial 轉接線連接至 Sidewinder；Bluetooth Module 直接透過 USB to Serial 轉接線連接至 Sidewinder。而 Wi-Fi Module 則是透過 mini-PCI 連接至 Sidewinder。

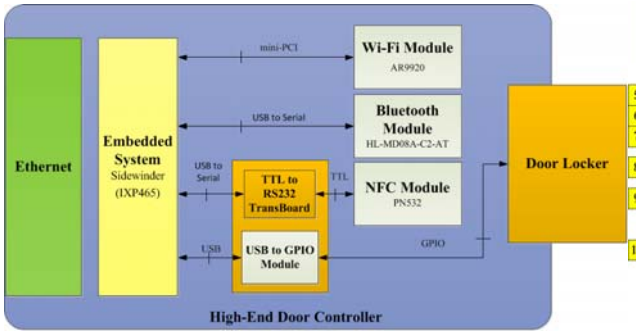


圖 3 高階門禁控制器硬體元件圖

4.2 低階門禁控制器設計

低階門禁控制器硬體元件如圖 4 所示，其採用 Microchip APP1632 為開發平台，並搭配 PIC32MX795F512L 之 MCU 為系統核心，另加裝 Ethernet 網路模組。無線通訊模組方面，Bluetooth 模組及 RFID 模組經由 RS232 電位轉換為 TTL 電位後連接至 PIC32MX795F512L 之 UART 接腳。另外，門鎖控制訊號由 PIC32MX795F512L 之 GPIO 直接輸出。

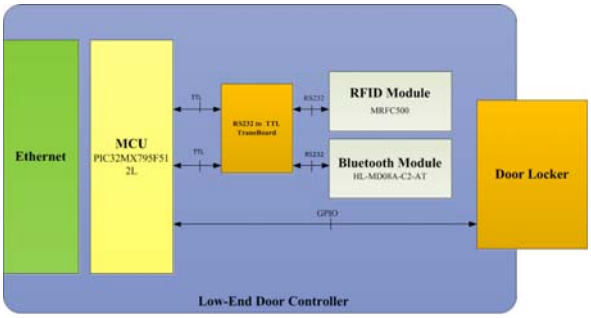


圖 4 低階門禁控制器硬體元件圖

4.3 門禁控制閘道器設計

門禁控制閘道器主要之功能在於蒐集其負責區域下所有高階/低階門禁控制器所傳來之識別記錄，以及提供使用者白名單給其所屬之門禁控制器，並利用圖形化介面使區域管理者進行監控。

當門禁控制閘道器啟動後會進入系統狀態頁面，而畫面上方共有四個分頁按鈕，分別為 Home、Log Message、Direct Control 以及 About 頁面。門禁控制閘道器啟動後會向門禁控制中心下載其所管理區域之相對地圖及使用者白名單…等相關資料。如圖 5 所示為門禁控制閘道器之系統狀態頁面，管理者可透過此畫面右半部了解該區域之結構以及其底下門禁控制器之裝設地點。而畫面之左半邊可分為上下兩欄，上欄在描述目前下拉式選單內所選擇之門口的相關訊息，如連線狀態、所屬規格及前次識別記錄等等；下欄為門禁控制閘道器之系統運作狀態，其可記錄各門禁控制器之連線與斷線以及識別記錄等。



圖 5 門禁控制閘道器之系統狀態頁面

4.4 門禁控制中心設計

為了讓使用者在存取門禁控制中心相關服務時，不會受到平台及作業系統的限制，因而採用 HTTP Server 來實現門禁控制中心。HTTP Server 選擇 Apache 作為伺服器以及 MySQL 作為資料庫。而門禁控制中心之使用者介面則是採用 HTML、PHP、CSS 及 JavaScript 等組合來呈現。

門禁控制中心主要在於儲存其底下之門禁控制閘道器與高階/低階門禁控制器相關資料，以及一般使用者與系統管理者的相關資訊。因此可將實體分為 4 類：門禁控制閘道器、門禁控制器、一般使用者以及系統管理者。

門禁控制中心主要在於儲存其底下之門禁控制閘道器與高階/低階門禁控制器相關資料，以及一般使用者與系統管理者的相關資訊。因此可將實體分為 4 類：門禁控制閘道器、門禁控制器、一般使用者以及系統管理者。

系統需儲存哪些使用者可以出入哪些門口，命名其為 Pass 實體型態；另外，系統需儲存使用者

在出入門口時所產生之識別記錄，命名其為 Log 實體型態，因此整理出上述幾個實體型態後，可以得到如圖 6 所示之門禁控制中心實體關聯圖 (Entity-Relationship Diagram，ERD)。

門禁控制中心之網站依使用角色可分為系統管理者及一般使用者，兩者皆為獨立個體，故門禁控制中心網頁管理介面之路徑也就跟著不同。系統管理者之角色可針對系統裝置或者是使用者裝置進行配置。在系統裝置方面，其主要針對目前資料庫內之門禁控制器及門禁控制閘道器等進行增刪與編輯；而在使用者裝置方面，主要針對使用者相關資料與識別媒體資料之修改，亦可對使用者進行增加或者刪減之動作。一般使用者之角色除了可瀏覽自身識別記錄及通行權限等相關資料，方便使用者取得所需資訊之外，亦可針對使用裝置之資料進行修改。

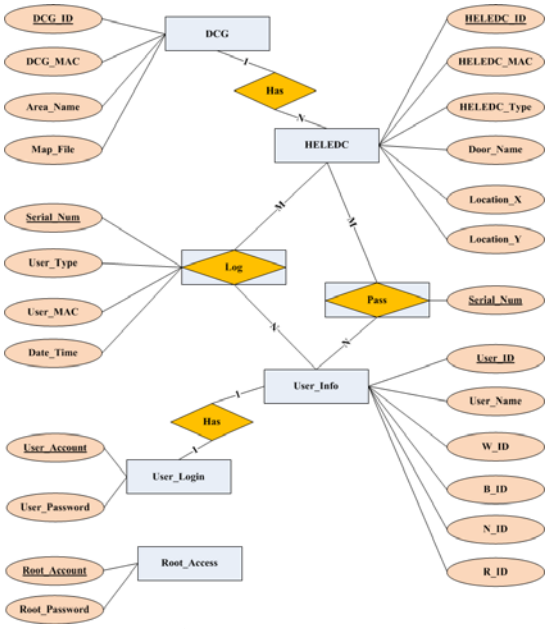


圖1 門禁控制中心之實體關聯圖

門禁控制中心除了提供網站給管理者及使用者使用外，在背景下提供了許多與門禁控制閘道器相關的功能模組，例如資料更新模組及資料上傳模組等。如圖 7 所示為系統管理者之網站架構圖。與一般使用者之使用的網站不同，門禁控制中心之系統管理者擁有一獨立存取之網站。

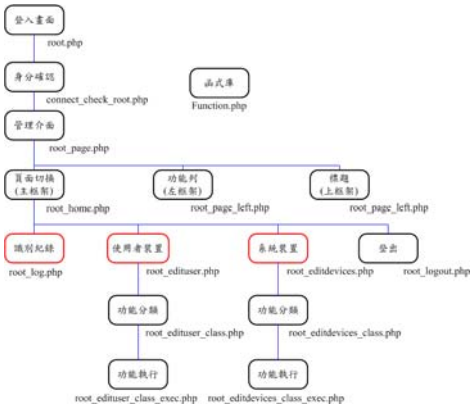


圖 7 系統管理者角色之網站架構圖

5 系統實測與效能評估

5.1 系統實測

在本節中，將套用情境來說明本文所提出之門禁控制系統整體之運作流程，其測試情境設定如下：新區域 Research and Development Department 將受本文所提出之制系統控管，其地圖檔為 research.png，且底下設有兩個出入口：West Door 及 East Door，分別安裝低階門禁控制器與高階門禁控制器；另外新增兩名使用者：EmnaLab 及 MaoSinSyu。

使用者即可利用其控制器所支援之識別技術來進行識別。如圖 8(a)所示，為使用者 MaoSinSyu 於低階門禁控制器前，利用智慧型手機之 Bluetooth 裝置來進行身分識別；如圖 8(b)所示，為使用者 MaoSinSyu 於高階門禁控制器前，利用智慧型手機之 Wi-Fi 裝置來進行身分識別。各控制器比對自身之使用者白名單後來決定是否解除門鎖，圖中各控制器皆已識別出使用者所持之識別媒體為可通行之裝置，並輸出門鎖控制訊號。



(a) 低階門禁控制器使用 Bluetooth 識別　(b) 高階門禁控制器使用 Wi-Fi 識別

圖 8 使用者於門禁控制器進行識別

5.2 效能評估

本文將系統安裝在一無 Wi-Fi 及 Bluetooth 等通訊干擾下之空間作為測試環境，並針對高階門禁控制器與低階門禁控制器進行系統反應時間與使用者白名單下載速度等效能測試。測試媒體採用智慧型手機與 RFID 卡。而資料平均次數為 20 次。

評估一套系統的好壞，其對於使用者行為之反應速度為重要考量之一。本文在測試環境中安排了高階門禁控制器與低階門禁控制器，針對使用者所進行之識別行為來進行系統反應速度測試。當使用者持識別媒體進入門禁控制器探測範圍 (本文設定其 RSSI 小於 -20dbm，約 1 公尺) 後，門禁控制器一接收到使用者識別媒體之訊框的瞬間為系統反應時間之起點，控制器經訊框分析、資料查詢比對到送出門鎖控制指令後，電控門鎖因控制指令而動作之瞬間為系統反應時間之終點。

如圖 9 所示，將系統反應時間測試數據轉換為直條圖後，可觀察出各門禁控制器之反應時間平均皆小於 31ms。另外，可發現使用 SQLite 之高階門禁控制器，系統反應時間比低階門禁控制器較為長，其原因在於高階門禁控制器進行識別時，需將讀取存放於 Flash Memory 之使用者白名單。而低階門禁控制器則是讀取存放於 RAM 之使用者白名單，故兩者速度才有如此的差異。本文將高階門禁控制器之 SQLite 取代為 RAM 後，重新進行系統反應速度測試，可發現高階門禁控制器從 RAM 讀取使用者白名單之速度明顯加快一倍以上。

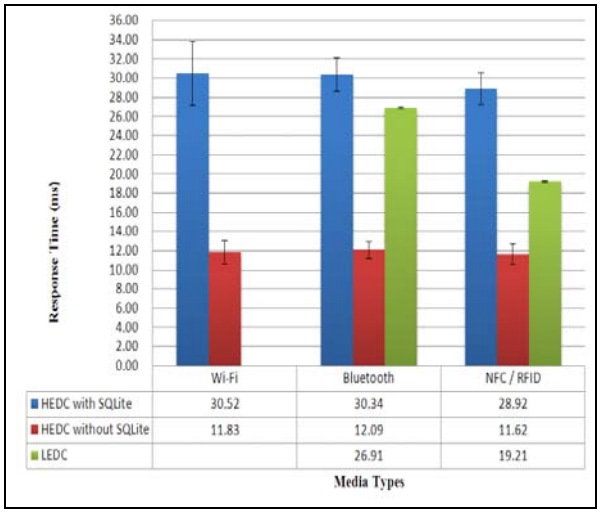


圖 9 系統反應時間比較圖

在門禁控制系統之效能測試上，本小節另外評估了高階/低階門禁控制器之使用者白名單下載速度，其對於各控制器之程式運作排程上為另一重要參考。門禁控制器另外須避免因使用者白名單尚在進行更新，卻發生控制器在擷取到裝置碼後而沒有資料可以進行比對的情況發生。因此本文在此小節將針對門禁控制器在進行使用者白名單下載時，其所花費之時間進行評估與測試。當高階/低階門禁控制器因定時更新或是門禁控制閘道器進行強制更新時，會以該時間點作為使用者白名單更新之時間起點。而在高階/低階門禁控制器更新使用者白名單並且儲存完成時，會以該時間點作為更新使用者白名單之時間終點。

如圖 10 所示，為高階/低階門禁控制器之使用者白名單下載速度測試圖，其測試下載的資料量分別為 10、20、50、80、100、200 及 500 筆使用者白名單，依控制器所支援的識別方式各進行 20 次清單下載測試，將其所測得之 20 個時間取平均值，並計算 95%信賴區間。可觀察到依照下載資料量的不同，各控制器所花費之時間亦會跟著有明顯差異。另外，依該圖可明顯發現高階門禁控制器之白名單下載時間皆比低階門禁控制器較為多，其原因一樣是在於高階門禁控制器是將使用者白名單存入其位於 Flash Memory 之資料庫內，以保持資料永久性。而低階門禁控制器則是將白名單暫存於 RAM，故兩者速度才有如此的差異。

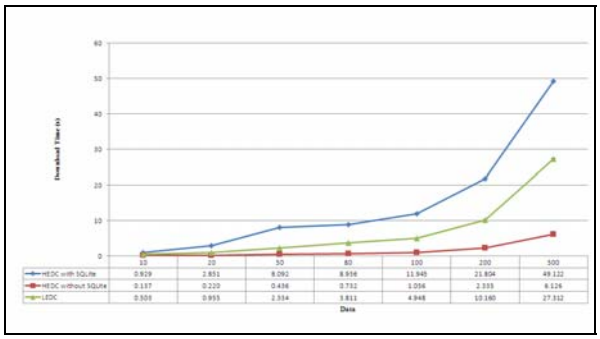


圖 10 門禁控制器白名單更新速度折線圖

6 結論與未來展望

本文利用 Wi-Fi 與 Bluetooth 通訊技術連線特性之裝置識別方法，並整合現階段具普遍性之 RFID 及 NFC 識別技術，完成一套「基於 Wi-Fi 與 Bluetooth 混合式無線識別技術門禁控制系統」。該系統之架構規劃了三個子系統：門禁控制器、門禁控制閘道器以及門禁控制中心，且各子系統皆負責不同之工作。門禁控制器依照無線通訊技術的支援種類來區別，可分為高階門禁控制器 (High-End Door Controller，H-EDC) 以及低階門禁控制器 (Low-End Door Controller，L-EDC) 兩種，其主要工作負責透過多種無線通訊技術來識別使用者所持之識別媒體，並負責開放通行與否的決策；門禁控制閘道器主要負責監控多個門禁控制器之外，亦扮演著門禁控制中心與門禁控制器之間的橋樑，使門禁控制器經識別動作後所產生之識別記錄，能透過門禁控制閘道器傳送至門禁控制中心進行識別記錄之儲存；門禁控制中心提供使用者之操作介面，讓使用者可查詢自身之相關資訊，且門禁控制中心為了達到多重區域控管之目的，其會與多個門禁控制閘道器連接，使其可利用門禁控制器來進行多區域之控管，讓各區域皆擁有門禁控制閘道器來進行區域管理。

本系統進行使用者白名單下載速度之效能評估後，可明顯發現高階門禁控制器白名單下載時間皆比低階門禁控制器較為多，而其原因在於高階門禁控制器是將白名單存入其資料庫之內，以保持資料永久性。而低階門禁控制器則是將白名單暫存於 RAM，因此兩者速度才有如此的差異。另外，系統反應時間之效能測試，屏除人為因素不考慮，可觀察到高階與低階門禁控制器之反應時間皆小於 31ms，屬於可接受範圍之內。因此，依照系統實測以及效能評估下來觀察，確實明顯地改善原先識別媒體在使用 Wi-Fi 與 Bluetooth 通訊技術與門禁控制器進行身分識別時的速度，去除了因網路相關前置設定所耗費的時間。本系統利用多種無線通訊技術作為身分之識別依據，未來可應用於人員進出管控或者服務業之暫時性身分識別依據，如人員進出管制、簽到退、電影票、遊樂園門票或其他暫時性服務之身分識別…等應用。

本系統藉由 Wi-Fi 與 Bluetooth 通訊技術的連線特性來使用智慧型手機進行身分識別，雖已達到不需識別媒體人工操作、不需安裝應用程式及確保裝置唯一性之目的，但由於所有識別媒體皆採無線技術，必然存在著遭到竊聽的可能性，故未來須加強安全性之部分。另外，在某裝置因斷電或其他外力因素而失去連線，為顧及系統之維護性，在未來將會加入 Error Code 機制，以利於維修人員進行系統修復。

參考文獻

[1] X. Li, G. Xu and L. Li, “RFID Based Smart Home Architecture for improving lives,” in Proc. 2008 2nd International Conference on Anti-counterfeiting, Security and Identification, 20-23 Aug. 2008, pp. 440-443.

[2] T. Mantoro and A. Milisic, "Smart card authentication for Internet applications using NFC enabled phone," in Proc. 2010 International Conference on Information and Communication Technology for the Muslim World (ICT4M), 13-14 Dec. 2010, pp. D13-D18.

[3] K. Y. Lian, S. J. Hsiao and W. T. Sung, “Home safety handwriting pattern recognition system,” in Proc. 2012 IEEE 11th International Conference on Cognitive Informatics & Cognitive Computing (ICCI*CC), 22-24 Aug. 2012, pp. 477-483.

[4] 籃嘉華，「無線網路技術應用於門禁系統之研究與實作」，國立中央大學資訊工程研究所，碩士論文，2004。

[5] J. Potts and S. Sukittanon, “Exploiting Bluetooth on Android mobile devices for home security application,” in Proc. 2012 Proceedings of IEEE Southeastcon, 15-18 March 2012, pp. 1-4.

[6] G. Dhivya C. Sethukkarasi and R. Pitchiah, “Wireless access control system based on IEEE 802.15.4,” in Proc. 2013 IEEE International Conference on Consumer Electronics (ICCE), Jan 2013, pp. 659-660.

[7] P. Wu, G. C. Wu, W. B. Xie, J. G. Lu and P. Li, “Remote Monitoring Intelligent System Based on Fingerprint Door Lock,” in Proc. 2010 International Conference on Intelligent Computation Technology and Automation (ICICTA), 11-12 May 2010, pp. 1012-1014.

[8] C. Z. Li and J. S. Lin, “Face recognition based on auto-switching magnetic door lock system using microcontroller,” in Proc. 2012 International Conference on System Engineering and Technology (ICSET), 11-12 Sept. 2012, pp. 1-6.

[9] “ Wireless Operating Modes”, http://wireless.kernel.org/en/users/Documentation/modes.

[10] W. S. Conner, J. Kruys, K. Kim and J. C. Zuniga, “IEEE 802.11s Tutorial Overview of the Amendment for Wireless Local Area Mesh Networking”, 13 Nov 2006.

[11] T. Thamrin, S. Sahib, “The Inquiry and Page Procedure in Bluetooth Connection,” Soft Computing and Pattern Recognition, 2009. SOCPAR '09. International Conference of, Dec. 2009, pp.218-222, 4-7.

[12] IEEE 802.11-2012, “IEEE Standard for Information Technology Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks Specific Requirements: - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, 29 March 2012.

[13] “Wi-Fi (Wireless Fidelity)”, http://www.wi-fi.org, 10 June 2013.

[14] IEEE 802.15.1-2005, “IEEE Standard for Information Technology Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)”, 14 June 2005.

[15] 繆嘉新，「NFC 技術演進與標準化」，中華電信研究所，2008。

[16] EPCglobal Inc., “EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz”, 10 June 2013.

[17] 劉穎昌，「RFID and NFC」，正隆 RFID 應用驗測中心，2008。

[18] ADI Engineering, Inc., “Sidewinder Board User’s Manual IXP465 Development Platform”, 17 July 2006.

[19] Wistron Neweb Corporation, “Approval Sheet for Model DNMA-92: An IEEE 802.11n a/b/g Mini-PCI module”, 13 Oct 2009.

[20] HotLife Electronic Technology Co.，「Bluetooth Serial Module HL-MD08A-C2 使用手冊」，2012。

[21] “ PN532 Board”, http://www.xfpga.com/html_products/PN532-breakout-board-24.html, 10 June 2013.

[22] USBIO Tech., “USB2ISP-2.0C Datasheet”, http://www.usb-i2c-spi.com, 10 June 2013.

[23] “ Airodump-ng”, http://www.aircrack-ng.org/doku.php?id=airodump-ng.

[24] Microchip Technology，「Microchip APP1632 使用說明書 (TW-UG-APP1632-E)」，http://www.microchip.com.tw，2010。

[25] Microchip Technology，「MCU4101T v2.0 Introduction PIC32 & MPLAB C32」，http://www.microchip.com.tw，2008。

[26] 鵬驥實業有限公司，http://pongee.diytrade.com.，2013。

[27] pandaboard.org, “OMAP4460 Pandaboard ES System Reference Manual”, http://pandaboard.org, 10 June 2013.

虛擬實境結合網頁體感用於家具擺設之研究

張晉豪　　徐豐明
臺中科技大學多媒體設計系
台中市、台灣
wite15@gmail.com　fms@nutc.edu.tw

摘要

近年虛擬實境技術已發展成熟以及Kinect的普及化帶動體感的應用，而在擴增實境方面，透過ARToolKit 等工具，需拿著標記物才能進行物件操作，並無直覺式操作概念，因此本研究基於直覺式操作構思，開發—體感虛擬擺設系統，藉由虛擬實境及體感技術用於網頁上，預先提供使用者模擬家具擺設情形。在網頁上運用 Kinect 偵測手勢之動作，操控系統中的虛擬家具物件同時呈現在真實的場景上，並且使用者能夠移動、旋轉、縮放、選擇物件材質等功能，當使用者依照喜好調整後，能將結果匯出。本系統目前已完成家具移動、旋轉、放大的雛型開發階段並可實際以直覺方式操作虛擬家具。

關鍵詞：Kinect，虛擬實境，直覺式互動，網頁體感，家具擺設

Abstract

Virtual Reality technology had been developed maturity and prevalence of Kinect brought up Somatosensory application in recent years. On Augment Reality, ARToolKit had to use a mark to project on specific object which means it doesn't contain an intuitive operation. Therefore, our approach based on an intuitive operation to develop a somatosensory furnishing system. It provides a prevision to users to simulate furnishing their house via combining Virtual Reality with Motion Sensing technology to reveal on a web page. On this web page users manipulate the virtual furnishings in an actually scene by Kinect gesture detection. We create some functionalities including movement, rotation, scaling object, or select the material of object in this system. After simulate furnishing, the results could export by user's hobbies. Our study is working on developing phase with functionalities as we mentioned and actual an intuitive operation for Virtual Reality.

Keywords：Kinect, Virtual Reality, Intuitive Interaction, Web page Interactive, Furnishing

1. 前言

近年來人們的生活水準逐漸提高，消費者漸漸地開始注重居家環境的生活品質，對於家中的家具擺設頗有想法，目前選購者能到家具店選購商品或者在網路上看到虛擬商品，並不清楚家具的款式擺放在家中是否美觀，得在家中套量尺寸後才能到家具店選購。現場選購家具時，因每位選購者對家具有所偏好及想法，會花許多時間考慮，考慮時間一久，選購者購買意願會降低，而這時得需要銷售人員在旁邊做推銷，提高選購者的購買意願，但銷售人員須費盡口舌才能說服消費者購買；消費者購買後覺得不滿意又得退貨，如無法退貨又得與店家有所爭執，因此許多消費者傷腦於選購家具，降低消費者的購滿意願也花費不少寶貴的時間。如果能好好規劃家具的擺設及樣式甚至在最短的時間內決定好家具的款式，這樣就能減少人力資源及搬運成本並提高購買者購買意願。

目前科技結合技術運用在家具擺設上有許多研究，為了使家具的擺設更方便，已經有研究者使用擴增實境中的ARToolKit標記物結合擺設家具[1]以及將ARToolKit運用於家具配置設計的研究[2]。經由以上的研究，利用虛擬擺設家具的實用性有明顯的提升，為了提供更方便的家具擺設，且不需要利用手持 ARToolKit 標記物來操控擺設家具，能運用直覺式手勢互動來操控家具擺設畫面，給予使用者直接的回饋並省略掉麻煩的標記物，才能提供擺設家具明顯的方便性。例如 IKEA 以虛擬環境選擇家具進行擺設，提供使用者利用 3D 或俯視圖來擺設正確家具位置，能迅速的設計出屬於自己的家。

本研究的目的是為了改善選購家具的困擾，可不必前往店家挑選家具而是在家中模擬擺設，並且在家中無需使用 ARToolKit 或任何的標記物(mark)擺設家具，而是利用直覺式互動，幫助使用者能迅速的選擇合適的家具。

為了解決以上的問題，而模擬一套擺設系統，此系統提供使用者在網頁上利用手勢來擺設家具，而家具款式只需店家建構模型放置伺服器上，提供給有 Kinect 的使用者利用手勢進行家具擺設，而無 Kinect 的使用者可從遠端觀看與討論家具擺設，希望此系統能提高使用者的購買家具的慾望。

此研究目標是為了解決以上的問題，並使用友善的介面及直覺式的互動手勢，能幫助使用者快速的選擇喜愛的家具，並解決不須利用 ARToolKit 標記物能更友善的幫助使用者減少麻煩的擺設標記物的動作，來提升虛擬家具擺設的實用性。

研究限制由於本研究重點在於用手勢來擺設家具，手勢的擺動方式過多，所以自行訂定簡易的操作手勢，且本研究不探討何種手勢為最理想。因畫面或場景的限制，以基本擺設場景為背景。

2.文獻探討

本研究探討虛擬實境的技術及應用，先介紹虛擬實境的由來及方法及 Kinect 擷取骨架方法，再介紹實際的應用。

2.1 虛擬實境介紹

虛擬實境（Virtual Reality，簡稱 VR）是利用電腦模擬產生出一個三度空間的虛擬世界，可以提供操作者許多感官在虛擬世界模擬。而提供操作者有互動效果，感受到在這虛擬世界有身歷其境的感覺，像是在真實世界中的感覺[3]。

虛擬實境是必須配合人的創作力所作成的技術，而虛擬實境包含三個主要的構成要素(3I)，Krueger 指出虛擬實境具有互動(interaction)、融入(immersion)和想像力(imagination)[4] [5]。此研究以這三點作為出發點。

2.2Kinect 簡介



圖 1 Kinect
(圖片來源：Kinect for Windows)

微軟從一開始推出 Kinect 就打著"你就是主角。"（All You Need is You.），只要能揮動手就可以啟動裝置，而 Kinect 會認出你的虛擬人物並偵測骨架，接著就能進行操作[6]。由此可知微軟要以使用者肢體取代控制器控制，Kinect 感應器能取得以下三種資訊，(1)彩色影像(2)3D 深度影像(3)聲音，如圖 1 [7]。此研究以前兩者為開發。

2.3 骨架追蹤

Kinect 最主要的功能為骨架的追蹤，骨架追蹤是實現自然互動的主要武器[8]，此系統可在感應器的範圍內主動追蹤六個人，包含最多兩位玩家的動作。而每個人可記錄到二十組細節，包含軀幹、四肢以及手指都是可追蹤的範圍，如圖 2。

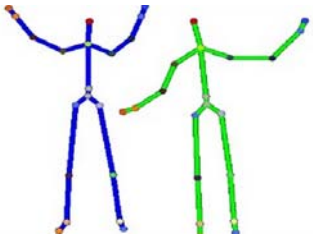


圖2 骨架追蹤(圖片來源：Kinect for Windows)

2.4 OpenNI

OpenNI(Open Natural Interation，稱為開放式自然操作)，它包含了語音、手勢、身體動作，也就是直覺性操作，不需要靠其他特殊裝置來操作。OpenNI 本身撰寫自然操作程式所需的 API，提供多語言(主要是 C/C++)、跨平台的 framework。使程式開發者使用視覺、聲音相關感應，對這些資料、分析的中介軟體時，可更方便，如圖 3 [9]。

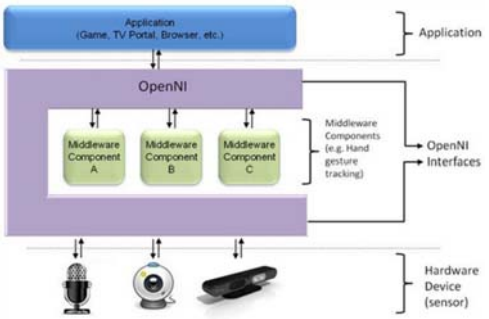


圖3 OpenNI 架構
(圖片來源：Kinect的軟體開發方案：OpenNI簡介)

2.5 家具模擬的應用

自虛擬實境發展以來，已經有某些公司用於家具，也因電腦處理速度提升，能更方便的利用 3D 模型快速的顯示出來[1]。而擴增實境以 ARToolKit 有研究者也在研究。以下分為虛擬實境與擴增實境來做應用。

IKEA 以虛擬實境來做擺設家具，像模擬家中的場景，可隨意拉動物件及方位；有四種模式可選擇，而圖 4 則選擇 3D 擺設，在左下角的類別可選擇想擺設的家具，中間部分可隨意搬動物體，因 3D 擺設會有死角而有俯視的角度提供使用者可放到正確位置，如圖 5。



圖4 IKEA 3D擺設

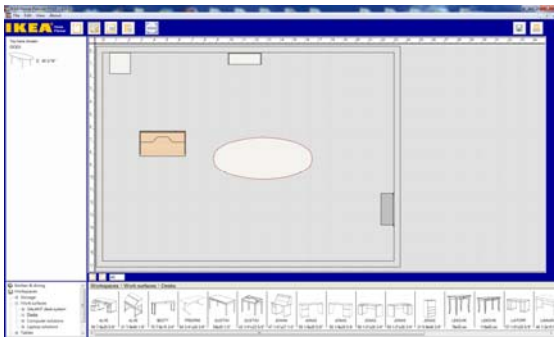


圖 5 IKEA 俯視圖

研究者以擴增實境中的 ARToolkit 來做家具擺設，當有動作時，手上拿著標記物如圖 6，共有兩個標記物做動作，當標記物移到何處，家具會跟著標記物移動，在螢幕的上方也有功能列能選擇不同家具做拖曳動作。利用網路攝影機所攝影到座標做定位，而網路攝影機有旋轉功能，由公式去運算得知移動方向，再做新的計算座標 [1]。



圖 6 家具擺設模擬介面
(圖片來源：顏子軒，基於擴增實境之家具模擬擺設系統)

另一個研究者以擴增實境中的 ARToolkit 的家具擺設，是攜帶設備到家中進行擺設，而放置標記物在地上由攜帶式螢幕中去觀看家具擺設的狀況 [2]，如圖 7。而畫面將透過展示機能看到虛擬家具的擺設狀況，如圖 8。



圖 7 標記物放置地上
(圖片來源：黃國豪，擴增實境應用於家具配置之可行性研究)



圖 8 透過展示看見的畫面
(圖片來源：黃國豪，擴增實境應用於家具配置之可行性研究)

3.研究方法

本系統主要提供使用者能與擺設傢俱的模擬功能有良好的互動性，利用 Kinect 進行手勢操作以提供最佳的人機互動，可選擇傢俱擺放到適合的位置，以提升模擬傢俱擺設功能的實用性，提供使用者能在遠端觀看或操作並互相討論，達到彼此共識。主要的研究技術與方法為以下五個小節說明。3.1 節說明系統模組，3.2 節說明系統功能流程，3.3 節說操作環境，3.4 節操作畫面與手勢互動，3.5 節說明使用流程。

3.1 系統模組

為了提供使用者有更方便的功能使用，則需考量到擺設方便性及網頁易用性，使整體效率能提高，也能提供使用者遠端觀看及討論，共同須連上伺服器，而分別敘述兩個模組(1)使用者擺設模組(2)使用者遠端連線模組，如圖 9。

3.1.1 使用者擺設模組

此模組提供使用者能更輕鬆的擺設家具，不須靠著標記物而是透過直覺式的互動手勢於擺設，能模擬真實擺設情況。

使用者透過瀏覽器連上伺服器(Server) ，並以 Zigfu 軟體進入到體感虛擬擺設系統，而有 Kinect 的使用者端(User)只要接上 Kinect 就能進入到系統介面。在系統介面裡，可以做家具選擇並利用擺設功能來改變家具。在這模組裡，能即時操控頁面並在線上與另一個使用者溝通，當雙方決定好時，能匯出擺設結果與紀錄擺設狀況，如圖 9。

3.1.2 使用者遠連線模組

此模組提供無 Kinect 的使用者能線上觀看，與另一位使用者做即時溝通，減少許多來回時間成本，利用網頁是為了方便性也是為了給使用者能即時開啟網頁即能觀看，不必安裝許多軟體。

使用者透過瀏覽器連上伺服器(Server)，並以 Zigfu 軟體進入到體感虛擬擺設系統。在介面裡，

利用溝通系統來互相討論，當決定好時，能匯出擺設結果與紀錄擺設狀況，如圖 9。

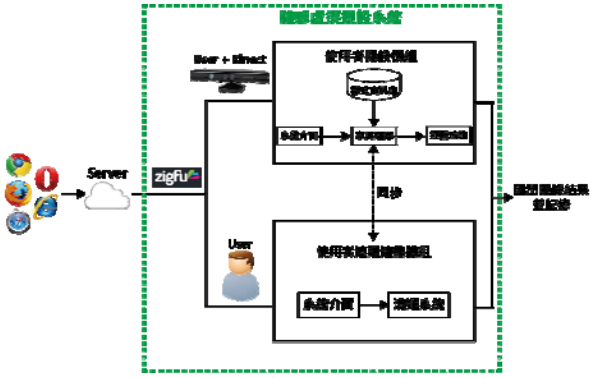


圖 9 系統架構圖

3.2 系統功能流程

本系統的系統功能架構，為進入家具樣式時，手部可開始控制物件。在擺放家具畫面時，可選擇家具款式，當選定好可進行變更。而變更家具則有四項功能，為刪除、材質、縮放、旋轉。點選刪除功能鈕後，再點家具會出現是否刪除，刪除後已完成刪除。點選材質功能鈕後，選擇家具的材質顏色，選定材質後會出現是否選擇，確定後為材質選定完成。點選縮放功能鈕後，兩手必須同時觸碰到家具，當觸碰到且雙手向外擴張時，家具會放大，而雙手內縮時，家具會縮小。點選旋轉功能鈕後，利用右手向螢幕的上、下、左、右方向進行旋轉，當旋轉完成後可確定方向。以上功能調整好後，如滿意則為設置成功，如不滿意可重新調整或選樣式，如圖 10 所示。

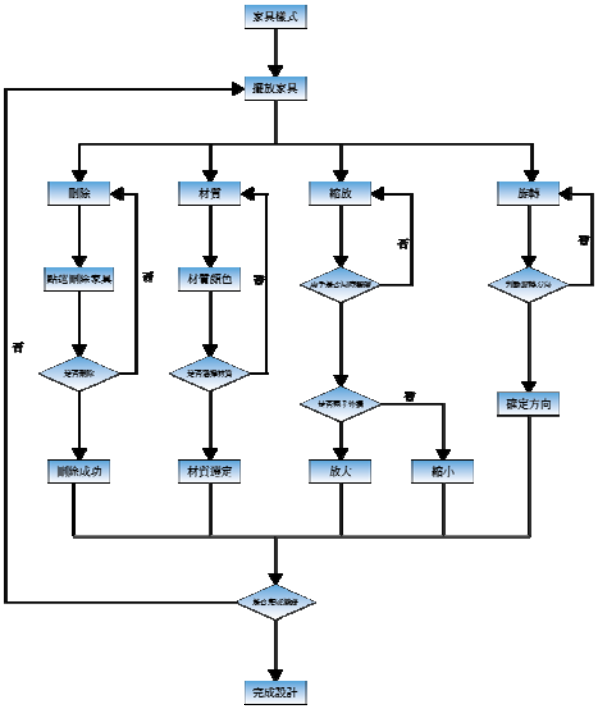


圖 10 系統功能流程圖

3.3 操作環境

本系統操作環境軟體為 Unity4.2，撰寫語言為 C#，以及利用 OpenNI1.5.4.0 及 Kinect for Windows SDK 1.7 作為輔，還利用 Zigfu (此為 Unity 與 Kinect 溝通的外掛軟體) 進行編寫此研究的工具，模型則取自 Unity 提供的 Asset Store 裡的免費提供模型。

本系統硬體為 Kinect 及兩台雙核心 2.33GHz 的電腦和須共同登入的 Server。

3.4 操作畫面與手勢互動

本系統進入家具擺設畫面且雙手揮動時，將會偵測到右手並螢幕上會出現手指的圖案出現在此研究把它稱為手套，即可做點選上排的按鈕。操作為如下圖 11。



圖 11 進入擺設畫面

當觸碰到家具按鈕時，手套上會附著著家具，可移到畫面下方任意擺置，只需停頓一到兩秒即可定位，當要再度移動時，再點家具按鈕則可繼續移動。操作為如下圖 12。



圖 12 移動家具畫面

當觸碰到旋轉按鈕時，手套會換成旋轉的手套，在此功能底下就能進行旋轉家具。而旋轉方向只需手套往上、往下、往左、往右，家具將會往四個不同方向旋轉。操作為如下圖 13。

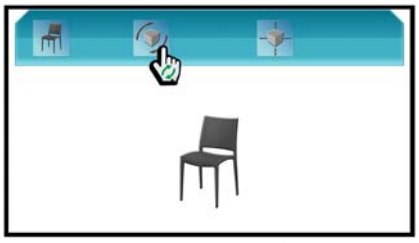


圖 13 旋轉家具畫面

當觸碰到放大縮小按鈕時，將再會偵測到左手並手套將會變左右兩手的手套，在此功能底下，可利用兩隻手觸碰到家具進行縮放。操作為如下圖14。

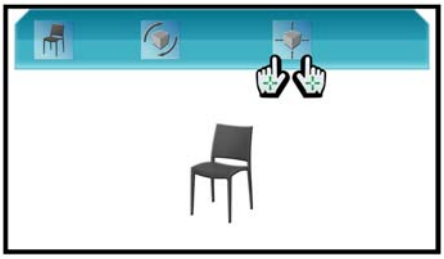


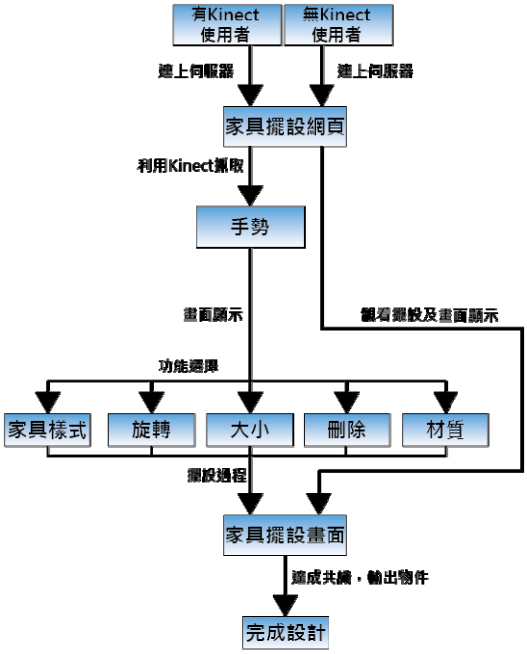
圖 14 縮放大小家具畫面

3.5 使用說明流程

本系統在系統模組裡分為有Kinect使用者與無Kinect使用者兩方面，他們連上伺服器為同一個網頁，只差在有無Kinect。

當連上家具擺設網頁，有Kinect的使用者需利用Kinect抓取手勢，而畫面會顯示家具擺設畫面，此時，能作功能選擇來擺設家具，再擺設過程中可進行溝通，如達成共識可輸出物件，完成設計。

無Kinect的使用者連上家具擺設網頁，此畫面與使用者是同樣畫面，在這畫面可進行共同討論，當達成共識時，也可輸出物件，完成家具設計，如圖15所示。



圖：15 操作流程圖

4.初步雛形開發成果

因研究上較於緩慢的關係，尚未將所有的功能作齊全，而先做個初步的系統，因此以下將會介紹及展示目前系統的操作，因可同步關係，所以分為操作者與觀看者來顯示成果。以下為說明使用者系統初步成果。

4.1 使用者初步系統

當登入家具擺設網頁時，會顯示功能列還有手套，剛開始進入畫面必須手上下擺動使Kinect利於抓取手的位置，當抓取到時，畫面的手套將會跟著操作者的手移動，如圖16。

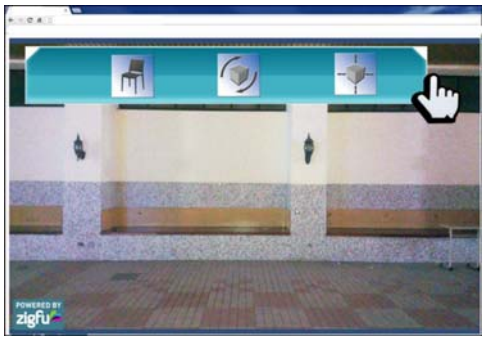


圖 16 進入擺設的頁面

操作者使用手套移動至家具按鈕(左邊第一個按鈕)，會有家具顯示並會黏著手套，此時可四處移動及擺放，如已經放置好，可再觸碰家具按鈕即可再移動，如圖17。觀看者則可從遠端看到家具移動狀態，如圖18。



圖 17 家具擺放位置(操作者)



圖 18 家具擺放位置(觀看者)

選好擺設定點時，可觸碰旋轉按鈕此為中間按鈕，此時手套會換成旋轉的手套，此模式底下，可往上、下、左、右揮動，往上是向上轉、往下是向下旋轉、往左是向左旋轉、往右是向右旋轉，即可變換家具的方向，如圖19。觀看者從遠端即可看到椅子旋轉的畫面，如圖20。

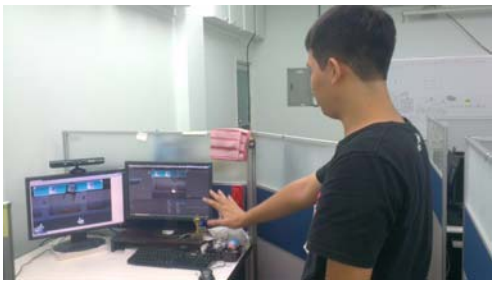


圖 19 旋轉家具(操作者)



圖 20 家具旋轉(觀看者)

選好家具並擺放好位置，可選擇放大按鈕此為最右邊的按鈕，觸碰到按鈕時，會出現兩只手套，此模式底下將利用左右兩手來控制，當手觸碰到家具，家具會跟著數值變大，如圖 21。觀看者從遠端即可看到家具被放大的畫面，如圖 22。



圖 21 家具放大(操作者)



圖 22 家具碰觸變大(觀看者)

5.結論與未來發展

本研究提出利用網頁體感來擺設家具的架構圖，並依照此架構完成一套體感虛擬擺設系統，此系統提供使用者能更直覺的利用手勢來隨意操作家具的位置，同時也能使用旋轉與縮放的功能改變家具的角度與大小，使家具能在不同地形做不同角度的轉變。在使用者遠端連線方面，只要連上擺設網頁，即可同步觀看擺設過程。目前體感虛擬擺設系統的功能已達到本研究的目的：

(1) 不必前往家具店選購家具，在家就能利用此系統選購，減少使用者選購家具的困擾。

(2) 此系統操作時，不需利用 ARToolkit 及任何標記物件來操控家具。

經由測試後，體感虛擬擺設系統能提供使用者更直覺地做互動家具擺設，因此本研究設定幾項目標，以下為達到的目標：

(1) 在本系統操作過程中利用直覺式的手勢與螢幕做互動，並操控家具做擺設。

(2) 使用本系統做擺設家具的過程中，使用到的功能能提高擺設家具的效率及方便性。

(3) 無 Kinect 的使用者，在本機端不必手動安裝任何套件即能從遠端連線進行同步觀看操作者做擺設過程。

(4) 有 Kinect 的使用者操控家具時，只需安裝 Kinect 的套件軟體且不必再開啟任何的程式，只需連上伺服器，即可進入家具擺設畫面。

此研究目前為雛型開發階段，希望在未來發展方面將會把功能做完整，希望能補足尚未完成的功能，以下為在未來能改進的方向有以下三點：(1)家具樣式豐富化。 (2)改進及增加刪除、材質的功能。 (3)雙向溝通及擺設結果匯出的功能。

文獻參考

[1] 顏子軒, 基於擴增實境之家具模擬擺設系統, 國立臺灣師範大學資訊工程研究所, 2011。

[2] 黃國豪, 擴增實境應用於家具配置設計之可行性研究, 國立成功大學工業設計研究所, 2004。

[3] 王泓斌, 互動超媒體設計應用於虛擬資訊空間之研究, 國立成功大學工業設計研究所, 2002。

[4] Myron K. Krueger, *Artificial Reality*, New York, Addison-Wesley Publishing Company, 1991.

[5] 洪彥伯, 以虛擬實境為基礎的前庭暈眩復健系統和復健成效分析與研究, 國立中央大學資訊工程學系, 2012。

[6] Kinect 台灣官方網站, 參閱日期 2013 年 7 月, http://www.xbox.com/zh-TW/Kinect 。

[7] Kinect for Windows 開發, 參閱日期 2013 年 7 月, http://msdn.microsoft.com/zh-tw/hh367958.aspx 。

[8] 劉超群, *Kinect體感程式探索－使用C#*, 松崗資產管理股份有限公司, p. 5-52, 2013。

[9] Kinect的軟體開發方案: OpenNI簡介, 參閱日期2013年7月 http://kheresy.wordpress.com/2011/01/19/openni_1st/ 。

基於 Wi-Fi 之家庭環境監控系統建置

陳響亮* 張書愷
國立成功大學製造資訊與系統研究所
* slchen@mail.ncku.edu.tw

摘要

隨著人們對生活品質與環境的要求越來越高，家庭環境空系統已經成為一熱門之研究議題。其中，臺灣的家庭擁有Wi-Fi無線AP的用戶數有上百萬戶，以推廣的角度來說，以Wi-Fi模組傳輸相較於Zigbee傳輸更具有推廣優勢。因此，本研究提出基於Wi-Fi之家庭環境監控系統，並設計各項感測器監控功能，包含溫度、濕度和氣體。當溫度感測器讀值超過門檻值時會啟動風扇，濕度溫度感測器讀值超過門檻值時則會開啟除濕機。另外，當檢測氣體(二氧化碳、一氧化碳、甲烷)分別超過門檻值時，會自動發送手機簡訊以警告使用者。本研究之成果主要包含遠端監控系統之建置與成果展示，供使用者隨時掌握家中環境狀況。

關鍵詞：Wi-Fi、家庭監控、簡訊派送、氣體檢測、濕度檢測。

Abstract

Recently academic research on home environmental monitoring system are usually designed based on Zigbee for its low power consumption and cost as the main way transmission. However Wi-Fi has been widely used in families in Taiwan, which has the advantage for design family monitoring systems. In this research, we proposed a monitoring system for family environment based on Wi-Fi and sensor technologies. A system prototype is proposed in this research with experiment results.

Keywords: Wi-Fi, SMS, family monitoring system, gas detection.

1. 研究動機與目的

臺灣的家庭擁有 Wi-Fi 無線 AP 的用戶數有上百萬戶，以推廣的角度來說，以 Wi-Fi 模組傳輸相較於 Zigbee 傳輸更具推廣優勢。本研究提出以 Wi-Fi 高速率傳輸，將感測器資料傳至電腦，透過遠端監控即時監測室內的溫、濕度及氣體的環境值。此外，利用 MPLAB IDE 程式開發工具，將程式寫入 MCU(Microcontroller Unit)，並設定溫、濕度及氣體門檻值。當超過門檻值時，開啟警報系統或是降溫、除濕等設施，最後，本研究利用手機簡訊的派送，當氣體濃度超過標準時便會發布簡訊通知管理者。本研究以 Wi-Fi 無線網路架構為基礎建構家庭環境監控系統，主要提出之幾項貢獻如下：

(1) 以資料庫、Wi-Fi 無線網路系統建構家庭環境監控中心。
(2) 以 Wi-Fi 無線網路為主之家庭溫度、濕度及氣體感測器佈建。
(3) 針對各項環境變化進行即時性調整室內環境值。
(4) 建構圖形使用者介面(Graphical User Interface，GUI)系統介面平台，監控家庭各項環境影響與自動化設施之啟閉功能。
(5) 建置於家庭監控之低成本嵌入式感測系統。
(6) 利用手機簡訊派送，氣體濃度超過標準時通知管理者。

2. 文獻探討

2.1 Zigbee 與 Wi-Fi 之特性比較

Zigbee 是一低速、短距離且採用 IEEE 802.15.4 通信協定的的無線網路協定，現今用途除了在軍事上，也能實現在居家照護、環境安全的用途，其傳輸距離約為數十公尺，傳輸速率為 10K 至 250Kbps。Peizhong Yi[1]等人提出 Zigbee 具有以下特性：

(1) 省電：透過電池即可支援 Zigbee 長達 6~24 個月左右的使用時間。
(2) 可靠度高：當有資料傳送需求時則立即傳送，並進行雙向確認，以此方式大幅提高系統資訊傳輸之可靠度。
(3) 高度擴充性：Zigbee 的網路最多包括有 64000 個網路節點。

Wi-Fi 是一個建立於 IEEE 802.11 標準的無線區域網路設備，也是屬於短距離無線通訊技術。Wi-Fi 速率最高可達 54Mbps，其傳輸距離最高可達半徑 100 公尺，而且 IEEE 802.11 的設備早已安裝在市面上的許多 3C 產品，如個人電腦、遊戲機、MP3 播放器、智慧型手機、印表機以及筆記型電腦…等，Wi-Fi 已經成為主流的標準配置，使用範圍主要在於資料大的網路傳輸，應用上包含移動視訊會議、公共無線上網等消費性電子的無線傳輸，Jin-Shyan Lee[2]等人提出 Wi-Fi 特性包含：

(1) 標準已成熟：早在 1997 年，IEEE 就陸續對 Wi-Fi 的使用頻寬、速率、物理層補充等相關技術做了明確的規範，至今日為止，相關規定及整合早已成熟。

(2) 大眾認知廣：現在 3C 產品幾乎都配有 Wi-Fi 裝置，iPhone 和 Android 等手機可以將自己當成小型路由器，讓周圍的裝置可以上網。
(3) 干擾少：Wi-Fi 使用的頻率是在 2.4GHz，不會受到藍芽、手機、微波爐等器具的干擾。

2.2 無線家庭監控相關研究

潘貞君等[3]在 2010 是「智慧居家生活」，主要是生活空間內外環境的感測，如溫度、溼度、照度等，以及空間內居住者的活動行為偵測，例如移動或靜止位置、看電視、聽音樂等，並推論適切服務的提供，增加人機互動的多樣性。

Sung-Nien Yu[4]等人提出利用藍牙(Bluetooth)結合 Wi-Fi 並整合感測模組，用來探查使用者的生命跡象以做到病人照護時的可靈活性、移動性以及可行性，讓心電圖等儀器可以帶著走。不過他仍然是用藍牙去做感測器的傳輸，用 Wi-Fi 去連接電腦以及遠端連線，如果他也使用 Wi-Fi 去做感測器的傳輸，在使用 Wi-Fi 的方面可以更全面性。

3.研究方法及步驟

3.1 家庭監控系統架構設計

本研究之智慧型家庭監控著重於家庭的溫、濕度以及氣體環境監控，透過風扇、除濕機以及簡訊警告來達成智慧型監控，本研究之系統之情境示意圖如圖 1。圖中上面為家庭監控中心系統，監控網路由 Wi-Fi 建置而成，感測節點佈置於房間各處，節點上連結各種感測器。佈建感測器於欲感測地點，並擷取其數據，藉由 Wi-Fi 模組將資料透過動態主機設定協定伺服（Dynamic Host Configuration Protocol Server， DHCP Server）傳輸至使用端建構出完整的家庭監控中心。

資料庫中心包含伺服器資料庫以及 PC 端，此平台負責存取監控等數據。家庭的監控中心包含使用者介面以及數據資料庫，使用者藉由電腦、平板電腦等平台，並透過設計之人機介面，操作各項自動化設備以及對各項環境因素進行監控。

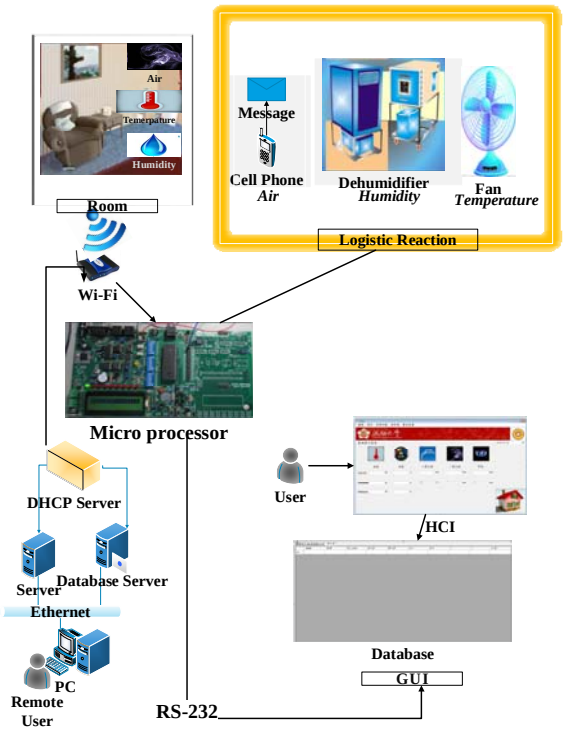


圖 1 情境架構示意圖

3.2 Wi-Fi 虛擬 IP 建置與實作

本研究的感測資料傳輸將透過 Wi-Fi 無線網路，而感測電路結合 Wi-Fi 模組後需要有一個 IP 位址才能經由無線 AP 上網傳輸資料。Wi-Fi 虛擬 IP 建置示意圖如圖 3-2。以基礎架構模式透過 DHCP Server 將無線範圍涵蓋到的 Wi-Fi 模組及行動化設備動態分配虛擬網際協議位址(Internet Protocol，IP)位址，使設備能加入網路並無線上網。這樣可以讓感測器連上網路並將感測資料上傳到資料庫。

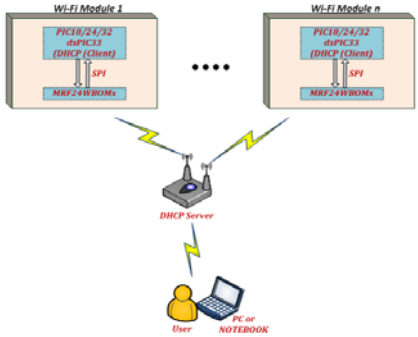


圖 2 Wi-Fi 虛擬 IP 建置圖

3.3 嵌入式系統架構

本研究將須進行資料傳輸的感測系統結合 Wi-Fi 無線網路，而 Wi-Fi 具有高傳輸特性、高傳輸距離與高普遍性不須多點跳躍傳輸資料，相當適合佈建於監控感測網路中。感測器將依環境需求佈建不同感測器，初步規劃以數字信號處理器(digital signal processor，DSP)為核心進行感測資料擷取及資料傳輸工作，電路架構圖如圖 3，中間為感測電

路與核心 DSP，左邊為各項感測器，上面為自動化設施之控制系統，右邊為資料庫及管理者介面。監控感測種類規劃為溫度、濕度、氣體(包含煙霧、一氧化碳及瓦斯)。

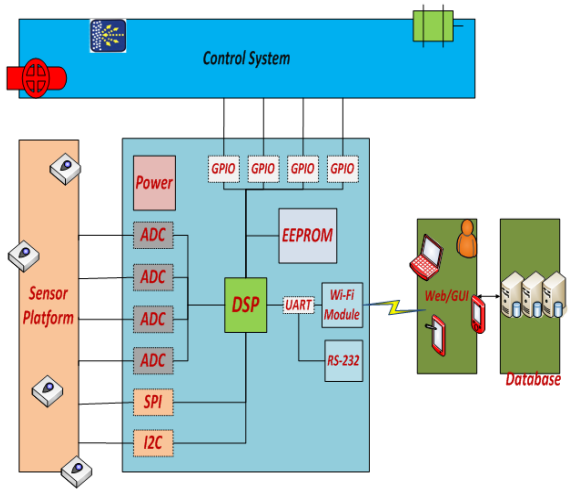


圖 3 感測電路架構圖

3.4 溫度感測器的監控

LM35 是由美國國家半導體公司(National Semiconductor)所生產的溫度感測器，感測的範圍是 0℃到 125℃，靈敏度為 0.25℃，0 度時輸出為 0V，每升高 1 度，輸出電壓增加 10mV。首先我們會設定一個區間值(T,default T=4)，讓溫度會維持在一個穩定的區間內，溫度的上限值(U)和下限值(L)可以手動調整的，其條件為 U-L≤T and U>L，當空調開啟之後，為了省電，所以加上把空調做關閉的動作，而當溫度低於下限值後空調會關閉改成送風，等到溫度又高過上限值後冷氣則再度開啟，溫度則會呈現區間震盪的情況。檢測流程如圖 4。

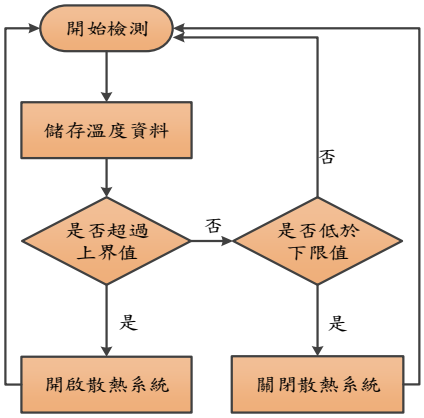


圖 4 溫度檢測流程

3.5 濕度感測器的監控

本研究選用 Arduino 公司所生產的 HR-31 型號之濕度感測器，其特色為感應濕度範圍寬廣，感測的溼度範圍為 20%到 80%，長期使用上的穩定度也較高，可以使用於倉儲、家庭、車內等室內環境的空氣品質的檢測，檢測流程圖如圖 5，首先會把當下溼度的數值儲存後去做判讀，當超過臨界值後便會開啟除濕的條件，當濕度低於下限值時，便會將除濕機關閉，並且將全部的資料儲存。

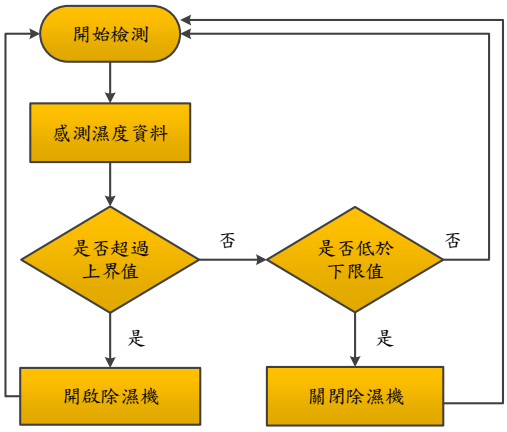


圖 5 濕度感測流程

3.6 一氧化碳、煙霧、以及瓦斯監控

本研究使用的一氧化碳感測器為 Arduino 公司所生產的 MQ-7 氣體傳感器而煙霧及瓦斯感測器是 Arduino 公司所生產的 MQ-2 氣體傳感器，檢測的靈感度為 10ppm 到 10000ppm 對於家庭氣體檢測的範圍是足夠的。檢測流程如圖 6，當濃度超過門檻值後就會發布簡訊直到判定不用發布警報才將其關閉。

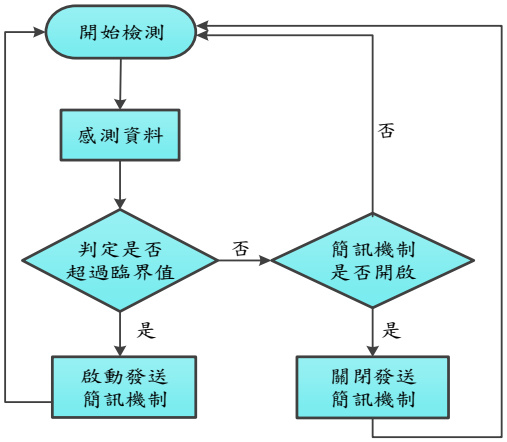


圖 6 氣體(一氧化碳、煙霧、瓦斯)感測流程

3.7 GUI 人機介面

本研究將以 Visual C#開發程式進行家庭監控系統介面設計，如圖 7，其介面可分為三項子項目，分別為：監控系統介面設定、監控系統以及各項感測器資訊之資料庫，其監控系統介面的設定參照 3.4 到 3.6 所討論的各項內容，而各項指標的安全值、

規範和使用者的設定則是 3.8 去做討論。



圖 7 GUI 人機介面

3.8 環境項目檢測指標之設定

一氧化碳的產生是由於燃料的不完全燃燒，另外瓦斯爐或熱水器滲漏，交通廢氣及室內人員抽菸也是室內一氧化碳的主要來源。因此本研究對一氧化碳的濃度極限值設定為 5ppm。

煙霧低濃度的環境下是無毒的，而根據行政院環保署的建議值，室內空氣的煙霧要在 700ppm 以下。因此本研究對煙霧的濃度極限值設定為 700ppm。

瓦斯可分為天然氣(CH4)和液化石油氣(C3H8)，一般瓦斯要達到爆炸的極限值只要佔室內空氣的 5%就有可能引發爆炸的。一般而言，我們對瓦斯的濃度的測定是以 0.1%(1000ppm)為極限值。[5]

由於每個人對於環境的溫、濕度的體感是不一樣的，因此可由使用者去決定他理想標準值。對於溫度的部分我們預設值參考行政院環保署對於室內溫度的建議值為攝氏二十五度，相對濕度為百分之五十五。詳細的溫度和濕度的上下限值以及預設值如表 1。

表 1 溫度和濕度的設定值

	溫度	濕度
上限值	28℃	70%
預設值	26℃	55%
下限值	18℃	40%

4.實驗結果

圖 8 是本研究的實驗完整架構圖，實驗的部分我們會分成三個實驗的區塊去做討論，分別為溫度(4.3 節)、濕度(4.4 節)以及氣體(4.5 節)。

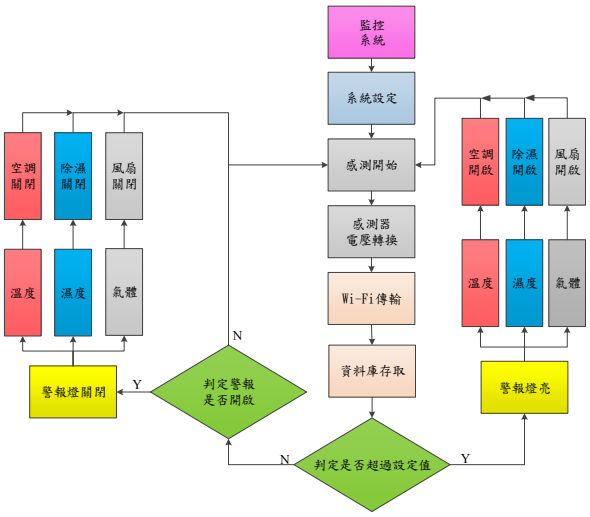


圖 8 系統架構圖

4.1 Wi-Fi 連接結果

圖 9 為 Wi-Fi 尚未連接完成的圖片，最左邊亮起了紅光代表連線尚未接通。此時我們使用 tera term 軟體把電腦當成終端機來連線，透過 COM port 來連接嵌入式系統的開發平台。



圖 9 Wi-Fi 尚未連結完成

打開 Tera Term 之後，選擇 Serial 的 Port 按 OK 後就可以執行連線；如果電腦本身沒有連到無線網路的情況下可以選擇輸入"Scan"去搜尋可以使用的無線網路，選定後後輸入"Join"並且加入欲連接的名稱就可以連上線。連線成功時 Wi-Fi 模組的圖片就會如同圖 10 一般。



圖 10 Wi-Fi 模組連線成功

4.2 資料庫建置

在按下圖 7 之中的「啟動」的按鈕之後，選擇「資料庫」裡的「建置資料庫」按鈕，就可以打開

以下的視窗，資料庫裡面的感測器的數據每 10 秒更新如圖 11。



圖 11 資料庫顯示介面

4.3 溫度感測模組與溫度感測結果

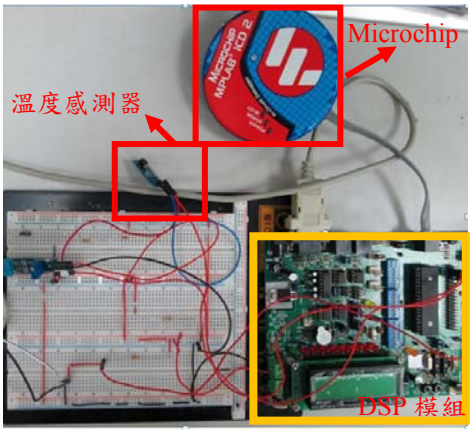


圖 12 溫度系統線路佈建圖

在實驗中，把上限值調成 24 度，而室溫則是維持在 26 度，風扇尚未啟動時如圖 13 所示，而當溫度超過設定值上限後就會啟動警示燈和風扇(如圖 14)。



圖 13 風扇和警示燈尚未啟動

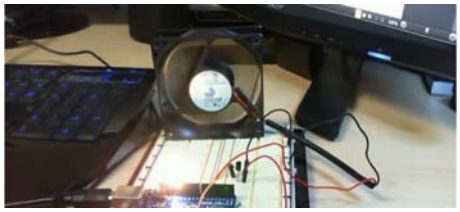


圖 14 風扇和警示燈已啟動

4.4 濕度感測結果



圖 15 濕的衛生紙沾在濕度感測器上

當我們改變濕度時，如圖 15，我們使用濕的衛生紙稍微沾一些在濕度感測器上，濕度會上升到 78%左右如圖 16，已經過了設定的門檻值 60%可以啟動除濕機如圖 17。

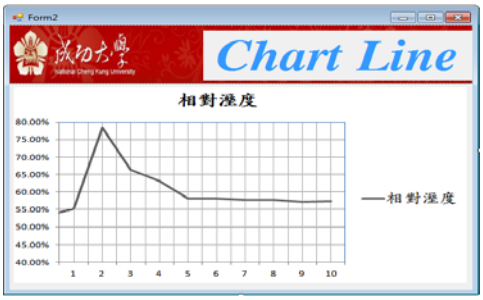


圖 16　相對濕度改變圖



圖 17 除濕機啟動亮起的燈號

4.5 氣體監控結果

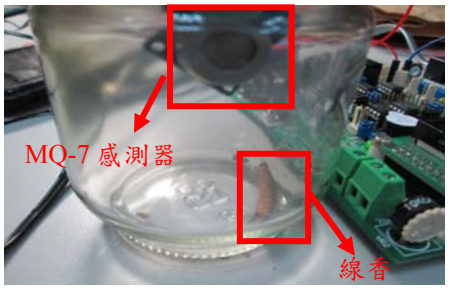


圖 18 充滿一氧化碳的環境圖

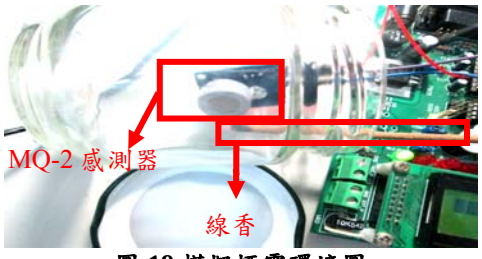


圖 19 模擬煙霧環境圖

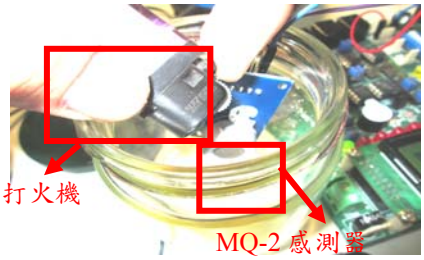


圖 20 模擬充滿瓦斯環境圖

本實驗製造一個充滿各種氣體的環境如圖 18 到圖 20，點燃線香後放在裡瓶子裡面讓它產生燃燒不完全的一氧化碳；點燃線香讓它產生煙霧；按著打火機使其產生瓦斯，系統將主動派送簡訊警告使用者，如圖 21。



圖 21 發送簡訊文字內容(以一氧化碳為例)

5.結論

臺灣的家庭擁有 Wi-Fi 無線 AP 的用戶數有上百萬戶，以 Wi-Fi 模組傳輸相較於 Zigbee 傳輸更具有推廣優勢。本研究提出之家庭監控系統，能夠有效的監測家庭的各項設定的環境指標。本研究實作之成果如下所述：

(1) 以資料庫、Wi-Fi 無線網路系統建構家庭環境監控中心。
(2) 以 Wi-Fi 無線網路為主之家庭溫度、濕度及氣體感測器佈建。
(3) 針對各項環境變化進行即時性調整室內環境值。
(4) 建構圖形使用者介面(Graphical User Interface，GUI)系統介面平台，監控家庭各項環境影響與自動化設施之啟閉功能。
(5) 建置於家庭監控之低成本嵌入式感測系統。
(6) 利用手機簡訊派送，氣體濃度超過標準時通知管理者。

表 2 整理出本篇論文的 Wi-Fi 導入本系統前後的差異。

表 2 Wi-Fi 導入此系統前後特性比較

項目	導入前	導入後
方便性	靠自己去做調整，方便性差。	透過電腦事前設定就好。
安全性	因為自己使用疏忽而產生安全上的疑慮。	
訊息即時性	無法在家裡以外的地方掌握家中的狀況。	可以透過遠端監控及資料庫了解家中狀況。
使用性	Wi-Fi 仍然維持一般上網的功能。	Wi-Fi 能夠將感測因子的資訊收集並且調整室內環境，Wi-Fi 的使用性更廣泛。

未來之研究目標以安全性為主要考量。例如：門禁管理功能。此外，也可以針對經濟型去作改良，例如節電管理。甚至可加入紓壓機、音響燈光等設備，依照使用者喜好調整的舒適程度。

致謝

感謝高科技設備前瞻技術發展計畫編號 302205501 與國科會編號 NSC 102-2221-E-006-107-之計畫，對本研究之經費提供與技術支援，使本研究得以順利進行，特此致上感謝之意。

參考文獻

[1] Pei-Zhong Yi, Student Member, IEEE, Abiodun Iwayemi, Student Member, IEEE, and Chi-Zhou, Senior Member, IEEE(2011), "Developing ZigBee Deployment Guideline Under WiFi Interference for Smart Grid Applications," IEEE Transactions on Smart Grid, VOL. 2, NO. 1, March 2011, pp 1-2.

[2] Jin-Shyan Lee, Yu-Wei Su, and Chung-Chou Shen (2007) , "A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," The 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON) Nov. 5-8, 2007 , Taipei, pp.1-5.

[3] 潘貞君、林志廷、吳文中、郭茂坤，"無線感測器網路平台及應用"，科學發展雜誌, 行政院國家科學委員會，447 期， pp.16~21，2010 年 3 月。

[4] Sung-Nien Yu and Jen-Chieh Cheng(2005), "A Wireless Physiological Signal Monitoring System with Integrated Bluetooth and Wi-Fi Technologies," Engineering in Medicine and Biology 27th Annual Conference, Shanghai, China, September 1-4, 2005, pp 2-3.

[5] Hanwei Eletronics co., LTD "MQ-2 Semiconductor Sensor for Combustible Gas," Retrieved June 9th,2013, from https://www.hwsensor.com.

綠色農場遠端自動化監控系統之研究

陳響亮* 陳廷宗 林昆輝
國立成功大學製造資訊與系統研究所
*slchen@mail.ncku.edu.tw

摘要

傳統農業往往僅是以人力勘查為主，無法立即得知農場環境周圍的狀況，為解決此問題，本研究提出綠色農場遠端自動化監控系統，以綠色能源太陽能，作為遠端自動化監控設備之供電來源。感測器的偵測的感測訊號經由 MCU(Micro-Controller Unit)作處理運算，經由高傳輸速率的無線 Wi-Fi 模組將所有的感測訊號無線化傳送至遠端使用者。農場遠端監控系統結合溫度、濕度以及土壤濕度感測器進行佈建，並利用 C#設計綠色農場遠端監控系統人機介面，供使用者進行農場遠端監控與操作。此外，本研究將搭配土壤溼度感測器設計灑水系統，當土壤濕度低於設定值時，微控制器將判斷是否開起灑水裝置。

本研究之主要目標為改善傳統農業所需監控人力之不足並且以 Wi-Fi 傳輸改善傳統農業遠端監控之訊息即時性低及提昇資料傳輸範圍。

關鍵詞：微控制器、Wi-Fi、灑水系統

Abstract

Traditional agriculture farm conditions are usually determined by farmers, which can't obtain the information of farms immediately. In this research, solar energy is used as a power supply, and MCU (Micro-Controller Unit) is used for sensor computing. High-transmission-speed Wi-Fi module is adapted for transmitting the sensor signals to remote monitoring system. Temperature sensor, moisture sensor and soil moisture sensor are used to build up the wireless sensor network for remote system of green farm, We use C# programming language to design the monitoring system interface for users. A sprinkler system is designed in this research with soil moisture sensor, and the soil moisture quantity will determine whether to start the sprinkler system or not.

The purpose of our research is to enhance and improve the transmission efficiency of information for farmers.

Keywords: Micro-controller, Wi-Fi, Sprinkler System

1. 前言

近年來，綠能環保意識抬頭，永續發展已是全球共識，農業的發展與環境的保護是各界關注的重點。另一方面，台灣自加入世貿組織(WTO)之後[1-2]，國內的農業發展已不能仰賴高關稅進口限制，價格支持等傳統保護措施，因此需調整農業生產結構，提升生產力與競爭力。面對各國對國內農業衝擊的影響，如何將自身的農業結構提升，結合現有的高科技，將台灣農業發展帶向全方面，並提升在國際間競爭力，將是未來農業界投入的重要課題。

隨著科技不斷的進步，農業發展也趨向由自動化生產代替人力勞工以及農業產品的改良，因此如何在自動化生產中實現遠端監控系統以節省人力成本，兼顧環境因素，將是農業遠端自動化監控所需致力發展的目標。

1.1 研究動機

在農場裡，農民無法隨時隨地進行場地勘查及土壤水分的變化，且農場內之灑水設施並須本人親臨現場操作，除了費時且無法即時性的調整。此外，由於在使用農業遠端監控系統上必須強調實用性，首要工作即是針對不同農場環境做為監控目標，建立相互應監控平台，並收集各種數據及建立資料庫作為農作物生長環境管理之依據，使農產品可獲得有效的管理。因為農場環境傳輸受到先天性的限制，使得無線感測網路技術成為一個適合應用於農業生產管理監控領域且實際應用價值之工具，相當獲得農業界重視，故本研究提出綠色農場遠端自動化監控系統。

1.2 研究目的

本研究針對以上問題提出以「綠色農場遠端自動化監控系統」，本研究之研究目的為下列 3 項：

(1) 以 Wi-Fi 無線網路為傳輸中心，建構農場遠端監控系統，達成符合大面積農場之傳輸範圍需求。

(2) 建構自動化灑水系統，針對土壤水分變化進行調整，取代傳統農業需以人力操作為主之控制方式。

(3) 建構遠端監控系統平台，監控農場各項周圍環境，使用者可於資料庫即時調閱歷史資料，取代傳統以人力勘查方式。

1.3 文獻回顧

蕭伯翰[3]使用可程式控制介面卡(PICNIC)做為驅動裝置，將多種感測器、IP 攝影機、無線基地台及遠端的個人電腦整合成無線多媒體感測網路

(WMSN)，並建構植物立體化萬苣栽培環境控制室之遠端監控系統，然而此系統未針對無線網路傳輸問題進行說明，無法得知遠端傳輸時，是否感測資訊能夠即時性的傳送到虛擬伺服器進行資料庫存取。

Park[4]等人提出使用 WSN 技術之遠端監控系統作為預測農作物上之露水是否凝結影響農作物之生長。Park 等人設計之遠端監控系統結合感測節點進行資料蒐集，並使用 Barenbrug formula 計算農作物上的露點作為感測器偵測露水之判讀以啟動設施。

2. 綠色農場遠端自動化監控系統

2.1 系統架構

圖 1 為本研究之系統建構圖，依此架構建立整個農場遠端監控系統。環境監控之感測資訊傳輸透過 Wi-Fi 模組(RN-131-EK Evaluation Board)將所有感測資訊透過SSID(無線基地台)傳送至遠端監控介面，使用者可於 GUI 介面平台之資料庫進行歷史訊息查閱。

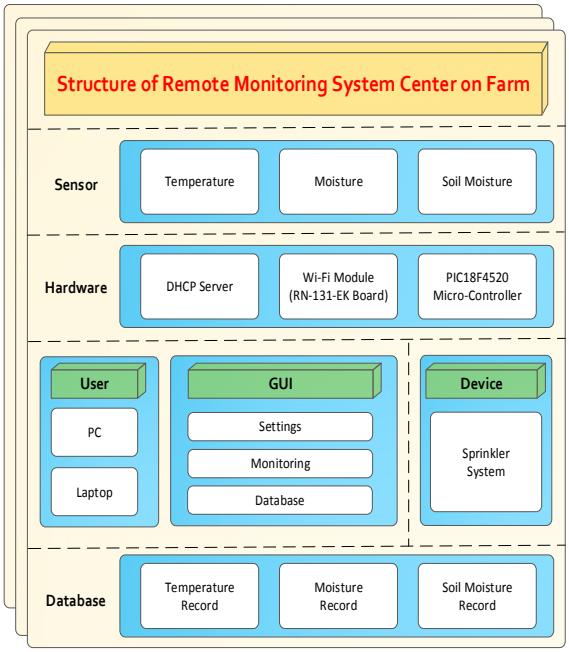


圖 1 本研究系統架構圖

圖中情境分為以下六大區塊，包含：(1)電源供應(2)感測器佈建(3)伺服端(4)自動化設施(5)遠端監控等五大部份，農場監控系統將以此情境逐步建立架構，並針對以上五大區塊進行說明。

(1)電源供應：

本研究以太陽能板及市電切換作為整個農場監控系統之電源供應來源。串接兩片太陽能板並搭配蓄電池充電以提供各項設施所需的 12V 電壓。由於太陽能轉換成電能的轉換效率有限，因此設計太陽能與市電切換電路，當蓄電池尚未充飽電壓時，繼電器打開轉由市電對於整個系統進行電源供應，以維持整個農場監控系統之運作。

(2)感測器佈建：

感測器佈建情境中，使用者將各項感測器佈置於農地，形成各個感測節點。感測器傳出的感測訊號傳送至微控制器（Micro-Controller）進行訊號處理，並透過 Wi-Fi 模組將資料傳送至伺服端。

(3)伺服端：

伺服端包含資料庫伺服器以及網頁伺服器，此平台將數據存取於資料庫伺服器，使用者可連線至網頁伺服器，從遠端調閱當時農作物的周圍環境狀況以及歷史資料。

(4)自動化設施：

自動化設施將依據土壤溼度感測器之數據，藉由微控制器(Micro-Controller)內之運算式判斷是否開啟或關閉灑水系統，達成自動化設施的運作。

(5)遠端監控：

使用者可使用本研究以 C#程式設計所開發之 GUI 人機介面以及資料庫，監看各項農場環境資料，其包含溫度、濕度以及土壤溼度等相關資訊，感測資料透過網路連線至伺服端進行即時的資料監控，並將各項資訊存入於資料庫，使用者可透過此系統進行農場周圍環境的歷史資料調閱。

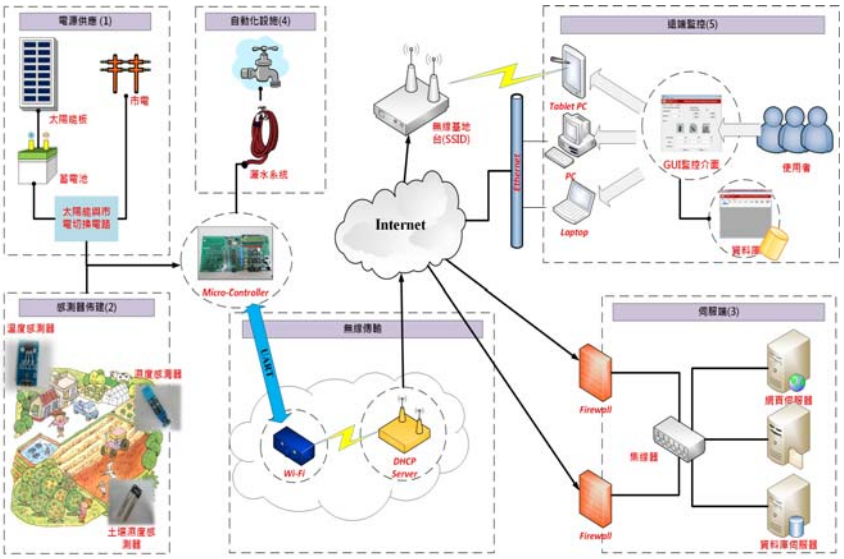


圖 2 本研究遠端監控系統情境圖

2.3 Wi-Fi 虛擬 IP 建置

本研究的感測資料將透過 Wi-Fi 無線網路傳輸。微處理機結合 Wi-Fi 模組後需要有一個 IP 位址才能經由無線 AP 上網傳輸資料。DHCP Server 會動態分配虛擬 IP 給 Wi-Fi 模組，使其能將資料傳送至伺服端。

農場監控系統，因需即時擷取溫度、濕度、土壤溼度等感測訊號後傳輸，因此用高傳輸速率及寬廣無線範圍的 Wi-Fi 網路，為使系統小型化及降低成本將使用嵌入式的 Wi-Fi 模組來進行數據傳輸。本研究以 RN-131-EK Evaluation Board 模組，進行評估及設計，模組支援 2.4 GHz IEEE Std. 802.11b 通訊協定，藉由無線 AP 上網，Data Rate 最高可至 2Mbps，網路涵蓋範圍最高 400 公尺，可用 Microchip 高階微控制器進行開發設計，降低網路建置成本，達成高速感測資料傳輸之目的。

感測器訊號由微控制器的 ADC 轉換成數位訊號之後，其感測資料藉由微控制器上的 UART 傳送至 Wi-Fi 模組，再由 Wi-Fi 傳送至遠端電腦進行傳輸，其示意圖如圖 3。

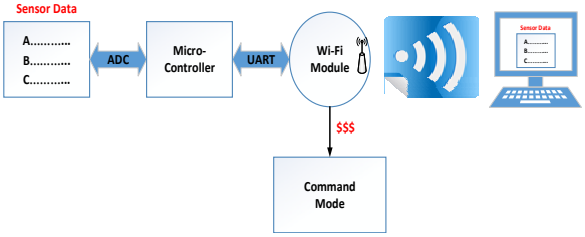


圖 3 Wi-Fi 模組與遠端連線示意圖

2.4 感測器系統建置與規劃

本研究之感測器建置規劃依序為溫度感測器、濕度感測器以及土壤溼度感測器，同時參考各項環境因子標準值、檢測方法及設置地點等進行感測器佈建。

初步規劃以 PIC18F4520 為核心進行感測資料擷取及資料傳輸，其資料處理程序以及 MCU 各項輸出入模組之腳位圖，如圖 4，以下將列出四項對各區塊進行說明：

(1)號區塊，微處理機中間部分為核心 PIC18F4520 單晶片，其操作速度可達 10MIPS，可快速進行感測訊號處理及相關運算與轉換。

(2)號區塊，各項感測器連結到 MCU 上的 ADC 模組，將類比電壓轉換為數位訊號。

(3)號區塊，灑水系統由 MCU 的 I/O 輸出入阜連結至控制電路，經由控制電路，使之開啟或關閉灑水系統。

(4)號區塊，Wi-Fi 傳輸模組藉由 Micro-Controller 將感測資料透過 Wi-Fi 模組傳送至伺服端。

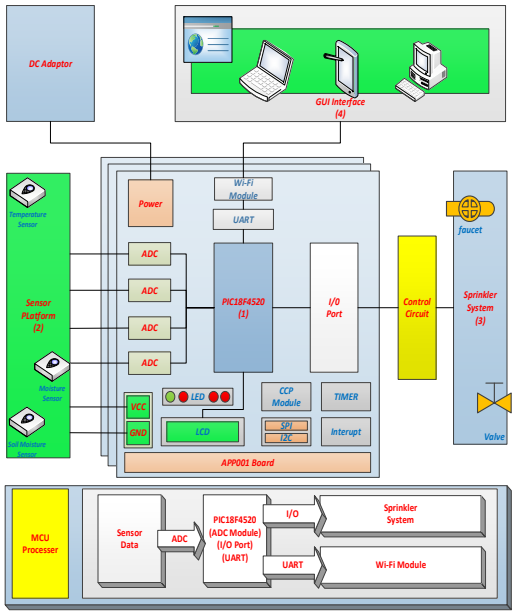


圖 4 微處理機與設備連結配置圖

2.4 節能迴路系統配置

圖 5 為整個節能迴路系統之架構，其灑水系統為負載端，串接蓄電池當系統後備電源，而蓄電池之充電來源為太陽能板，太陽能板模組充電電壓為 18V，電路保護串接逆流二極體防止電流逆流造成太陽能板損壞。因太陽能轉換電能效率有限，因此當蓄電池尚未有足夠電壓時，由市電提供負載端所需之能源。

綠色農場監控之電源來源除了市電之外，綠色能源的應用亦是研究的另一方向。本研究以太陽能發電結合蓄電池充電為主要備源架構。圖 6 為太陽能以及市電切換建構流程圖，而微控器需使用 9V 電壓，因此需搭配 DC 轉 DC，將蓄電池的電壓降壓，以提供微控制器的輸入來源。繼電器用來當作市電及太陽能的切換，當電路與插座連接時，繼電器 A 從原本 NC 跳至 NO，負載端的電力來源改由市電轉換，在繼電器的 NO 端加入一顆 LED 燈光，此顆 LED 可提醒使用者由太陽能切換為市電電源。

微控制器負責灑水系統，藉由 MCU(PIC18F4520)針對電磁閥的開關進行控制動作。

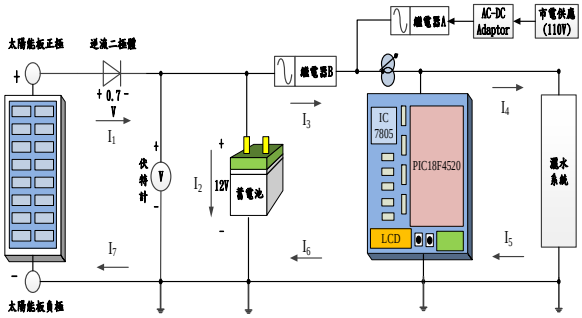


圖 5 監控系統節能迴路架構圖

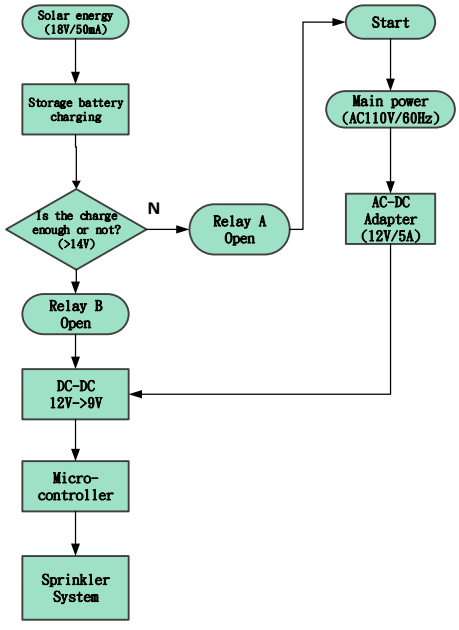


圖 6 太陽能及市電切換流程圖

3. 綠色農場遠端自動化監控系統

3.1 綠色農場

綠色農場的概念在於將現有的農場以及各項設施結合綠色能源(如：太陽能、風力、生物能源、海洋能…等)，達成響應環保及節約能源之目標。本研究之綠色農場之定義為以太陽能作為綠色能源，其太陽能取之不盡，用之不竭，可達成節能減碳效果。利用農場於戶外長時間日照之下，設置太陽能板於農場之中，以太陽能提供整個綠色農場遠端自動化監控迴路系統之電源供應來源。

3.2 感測器佈建與實作

此節將溫度、濕度及土壤濕度感測器進行佈建，如圖 7、圖 8 及圖 9。感測器之類比輸出腳位接於 APP001 開發板類比通道(AN0、AN1 及 AN2)，進行各項感測器之類比訊號傳輸，並使用 MPLAB IDE 建置 ADC 模組之 C 語言程式碼。A/D 轉換後之數位訊號須根據比較器選用之參考電壓進行轉換，以求得當時外界物理量。感測器工作電壓為 3.3V-5V，藉由 APP001 開發板之所內建的外部輸出電壓 5V，供應各項感測器所需的電壓。

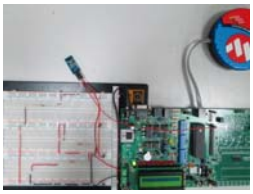


圖 7 temperature sensor



圖 8 濕度感測器佈建

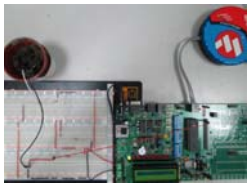


圖 9 濕度感測器佈建

3.3 灑水系統實作

本節將灑水系統進行實作，其迴路配置如圖 10，將微控制器連結至電磁閥進行水流的開關，而控制電路加裝繼電器以及 BJT 電晶體，將整個迴路進行連結。

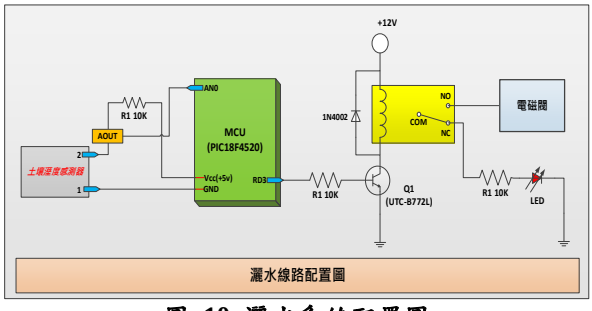


圖 10 灑水系統配置圖

3.4 Wi-Fi 無線感測網路實作

本節將針對 Wi-Fi 模組加入無線網路進行設定。利用 RN-131 EK Evaluation Board 的 USB 與電腦 COM Port 連結，當 Wi-Fi 完成加入網路時，將使用微控制器與 Wi-Fi 模組進行傳輸。感測器佈建將針對感測資料透過 Wi-Fi 模組傳送至遠端進行實作，如圖 12，其實作步驟如下：

(1) 首先，設定 Wi-Fi 為接收端，而微控制器為傳送端。

(2) 利用 Wi-Fi 模組的 UART Interface 上的 Pin 3 連結至 APP001 開發板上的 J6，進行單向之資料傳輸。

(3) 感測資料傳輸至 Wi-Fi 模組，藉由 Wi-Fi 模組傳送至伺服端，進而讓遠端使用者收到即時性的訊息。

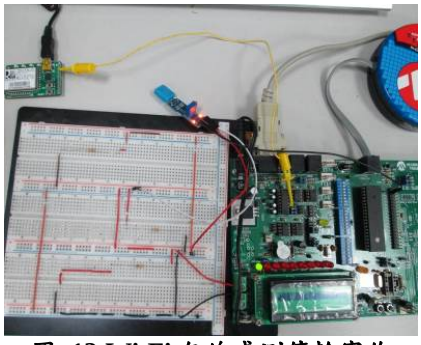


圖 12 Wi-Fi 無線感測傳輸實作

3.5 農場遠端監控系統人機介面

本研究設計監控系統使用者登入介面，如圖 13，使用者可藉由登入介面進入監控系統平台，並進行各項功能之操作。



圖 13 GUI 使用者登入介面

本研究所設計人機介面上之兩項子項目進行功能介紹，其依序如下：

(1)監控介面：如圖 14，此介面設計自動化設施之控制鍵、當時天氣狀況以及各項感測結果之動態顯示。感測器之動態顯示包含回傳之類比電壓和計算後之電阻值，以及各項感測數據轉換之後所得到的環境數據。介面另外設計自動化設施所需的控制鍵，使用者可根據環境狀況停止灑水系統，或藉由當感測值達到限制值時，即會開啟或關閉各項設施。當灑水系統為開啟狀態時，ovalshape 容器會顯示為綠色，反之為紅色，使用者可由此功能得知灑水系統是否已開啟或是關閉狀態。類比轉數位訊號之採樣時間選擇為 20Tad，其類比訊號轉換為每一個數位訊號位元所需時間為 32 μs。

(2)資料庫介面：圖 15 為監控介面所連結之資料庫，此資料庫採用 Microsoft Access 建立，結合 C#人機介面顯示各項感測器偵測的數據。資料庫主要欄位包含：使用者、日期、各項環境感測值及各項感測器輸入的類比電壓值。使用者可將所蒐集的數據儲存，並藉由日期調閱各項資訊以利得知當時周圍環境狀況。

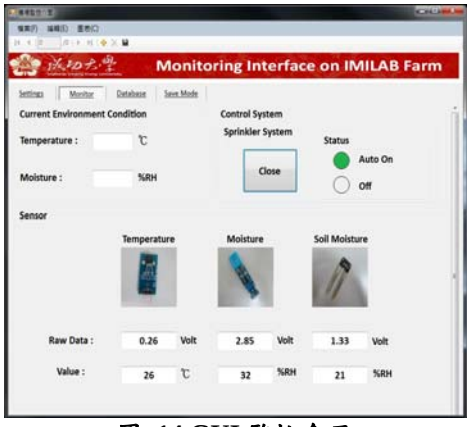


圖 14 GUI 監控介面

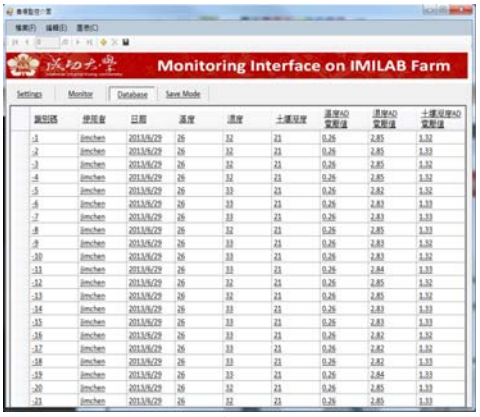


圖 15 GUI 資料庫紀錄功能

4. 綠色農場遠端自動化監控系統實作

4.1 自動化灑水系統實作

(1)首先，以農地進行綠色農場自動化系統佈建，如圖 16 與圖 17，利用土壤濕度感測器置入於土壤進行佈建，如圖 18 與圖 19，之後經過 MCU(PIC18F4520)的 ADC 模式進行運算處理，處理完的感測訊號，依據灑水系統程式碼，由微控制器判斷土壤濕度是否足夠進而開啟灑水裝置，當土壤濕度低於 30%RH 即會開啟。



圖 16 農場佈建(1)



圖 17 農場佈建(2)



圖 18 土壤溼度感測器佈建



圖 19 感測器與 MCU 連結

(2)太陽能板進行串接，如圖 20，提供蓄電池進行充電，如圖 21。灑水系統的控制電路藉由充電完成的蓄電池進行供電，如圖 6-8，而控制電路的繼電器與電磁閥的連結，並與微控制器進行連結，如圖 6-9、圖 6-10、圖 6-11 與圖 6-12 所示，整個灑水系統如圖 6-13、圖 6-14 與圖 6-15 所示。



圖 20 太陽能板串接



圖 21 蓄電池充電



圖 22 電磁閥



圖 23 控制電路



圖 24 控制電路與微控制器



圖 25 灑水系統

4.2 綠色農場遠端監控系統實作

首先，將溫、濕度感測器進行農場佈建，如圖 26 與圖 27，連接 Wi-Fi 模組(RN-131-EK Evaluation Board)並與電腦進行連接，如圖 28，進入 Command Mode 進行網路設定，將 Wi-Fi 加入於網路並進行感測訊號傳輸，微控制器與 Wi-Fi 模組使用 UART 模式進行傳輸，如圖 29，之後將各項感測數據藉由網路傳至遠端使用者的介面上進行農場遠端監控，並藉由伺服端進行數據資料庫之儲存，如圖 30 與圖 31。



圖 26 濕度感測器佈建於農場



圖 27 溫度感測器佈建於農場



圖 28 Wi-Fi 模組



圖 29 Wi-Fi 模組與 MCU 連結



圖 30 遠端連線

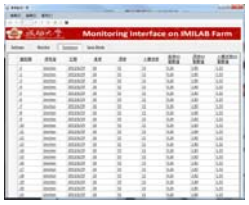


圖 31 資料庫顯示

5. 結論

本研究以溫度、濕度與土壤濕度感測訊號為主進行訊號擷取，採用LM35溫度感測元件，精度範圍±0.5℃。另外，在濕度訊號擷取方面，採用KSM006型之濕度感測器，其精度範圍±5%RH。在實驗設計上，我們同時監控各個感測器，其本研究使用之Wi-Fi模組皆可以維持資料傳輸的穩定性與即時性，大約可同時傳輸200平方公尺之農場土地面積。以下歸納出本研究之結論與貢獻：

(1) 以 Wi-Fi 無線傳輸應用於農業遠端監控系統，改善傳統農業以人力勘查方式，不須農民親自到現場，且較適合佈建於涵蓋大範圍之農場。

(2) 以 MCU 內之 ADC 模式結合 I/O 模式，可組成自動化系統。本研究之自動化灑水系統以此模式建立，當土壤溼度低於臨界值時，微控制器即可判斷是否開啟灑水系統，改善需人力啟動灑水系統，以達到即時性與便利性。

(3) 設計農場遠端監控系統人機介面，並搭配資料庫管理，將所有蒐集的環境感測資料及資訊存入於系統之中，使用者可即時性的調閱各項資料，提醒使用者農作物生長周圍的環境狀況。

6. 致謝

感謝高科技設備前瞻技術發展計畫 HTED 302205501 對本研究之經費提供與技術支援，由於賜福科技公司的支持，使本研究得以順利進行，特此致上感謝之意。

參考文獻

[1] ICT 在農業之應用, http://www.coa.gov.tw/view.php?catid=2445998, reference date: 2013/04/13.

[2] 行政院農業委員會, “農政與農情,” 農委會出版品, 第 242 期, Aug. 2011.

[3] 蕭伯翰, “植物立體化栽培控制環境之遠端監控,” 國立台灣大學生物產業機電工程學系碩士論文, 2009.

[4] Dae-Heon Park, Chul-Young Park, Sung-Eon Cho, Jang-Woo Park, “Greenhouse Environment Monitoring and Automatic Control System Based on Dew Condensation Prevention,” Embedded and Multimedia Computing (EMC), 2010 5th International Conference on IEEE, pp. 1-5, Aug. 2010.

[5] Hirafuji, M., Ninomiya, S., Kiura, T., Fukatsu, T., “Field Server Projects,” Applications and the Internet Workshops, 2007. SAINT Workshops 2007. International Symposium on IEEE, pp. 75, Jan. 2007.

[6] David Hest, “Farmstead Wi-Fi hotspots,” Farm Industry News, April. 2010.

[7] Dae-Heon Park, Chul-Young Park, Sung-Eon Cho, Jang-Woo Park, “Greenhouse Environment Monitoring and Automatic Control System Based on Dew Condensation Prevention,” Embedded and Multimedia Computing (EMC), 2010 5th International Conference on IEEE, pp. 1-5, Aug. 2010.

[8] Mahir Dursun and Semih Ozden, “A Wireless Application of drip irrigation automation supported by soil moisture,” Scientific Research and Essays, vol. 6, no. 7, pp. 1573-1582, April. 2011.

[9] Izzat Din Abdul Aziz, Mohd Hilmi Hasan, Mohd Jimmy Ismail, Mazlina Mehat and Nazleeni Samiha, “Remote Monitoring in Agricultural Greenhouse Using Wireless Sensor and Short Message Service(SMS),” International Journal of Engineering & Technology IJET–IJENS, vol. 9, no. 9, pp. 35-43, Oct. 2012.

[10] Swarup S. Mathurkar, D. S. Chaudhari, “A Review on Smart Sensors Based Monitoring System for Agriculture,” International Journal of Innovative Technology and Exploring Engineering(IJITEE), vol. 2, pp. 76-78, March. 2013.

[11] Clement Atzberger, “Advances in Remote Sensing of Agriculture: Context Description, Existing Operational Monitoring Systems and Major Information Needs,” Remote Sens., vol. 5, pp. 949-981, 2013.

Android 平台之旅遊規劃與事故偵測系統

吳思陳　　羅壽之
國立東華大學資訊工程學系
tim6578@ms8.hinet.net, sclo@mail.ndhu.edu.tw

摘要

隨著智慧型手機的普及化，各種手機應用程式油然而生，所帶來的便利及生活化已不容忽視。智慧型手機內建的感應器、GPS、相機、通訊等功能，可以有效地整合，運用於旅遊資訊平台。本論文提供一個旅遊應用程式，提供旅遊資訊查詢、行程規劃、路徑導航與意外事故偵測等功能。

關鍵詞：智慧型手機、行動應用、旅遊規劃、事故偵測。

Abstract

With the popularity of smart phones, a variety of mobile applications are raised, which brings non-negligible affects on convenience and life. The built-in functions of smart phones such as sensors, GPS, camera, and communications can be integrated into a tour information platform. In this paper, a mobile tour application is introduced by providing the query of tour information, the planning of a tour route, the guiding of a driving path, and the detection of a car accident.

Keywords: Smart Phones, Mobile Applications, Tour Planning, Accident Detection.

1. 前言

自從智慧型手機問世後，種類推陳出新、功能亦趨強大，已經改變用戶的通訊習慣。在眾多智慧型手機系統中，又以 Android 平台最受歡迎。目前智慧型手機除了在硬體效能不斷升級外，亦提供無線與行動網路通訊能力。為了提供更豐富的功能，整合不同特性的多軸感測器如加速度與方向等可設計出更人性化的行動應用程式。

本論文旨在整合智慧型手機的多樣功能，設計一個更符合使用者需求的旅遊資訊服務系統。除了提供即時與豐富的旅遊資訊查詢外，本系統提供自動行程規劃，依據使用者選取的造訪景點、出發時間與地點等資訊，規劃出各景點的遊玩順序。此外，本系統利用智慧型手機的感測器，運用於意外事故偵測。當事故發生時，系統會即時發送求救訊息於使用者的臉書上，描述位置資訊及可能事故原因，讓臉書上的朋友可以協助處理。

本論文架構如下：第二章說明系統功能架構，第三章介紹系統功能設計方式，第四章總結這篇論文，並說明未來展望。

2. 系統功能架構

本旅遊服務系統架設於 Android 智慧型手機上，主要提供三項功能如圖 1 所示，分別為旅遊資訊、行程規劃與導航（內含事故偵測）。於系統實做階段，旅遊內容主要以花蓮為主，並以花蓮縣觀光局提供的網頁[1]為參考內容。

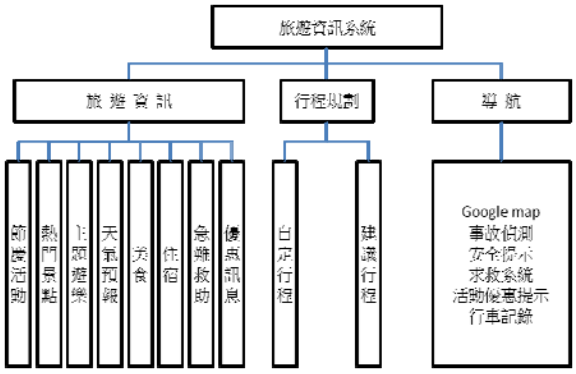


圖 1 系統功能架構

各功能說明如下：

（一）旅遊資訊

- 節慶活動：提供一年四季季節性的活動訊息。
- 天氣預報：即時顯示三個時段(當日白天、當晚至明晨、次日白天)的天氣、氣候、降雨機率、溫度等資訊。一週預報則顯示白天/晚上的氣候、溫度。
- 主題遊樂：提供特色遊樂資訊分別為樂活農業、溫泉泡湯、單車之旅、泛舟溯溪、戶外活動與生態之旅。
- 熱門景點：提供當地著名景點資訊，包含服務資訊、提供設備項目、景點照片、簡介等，並提供撥電話、導航、街景、網頁連結等功能。
- 美食：提供當地美食與小吃的資訊。
- 住宿：提供當地住宿資訊。
- 急難救助：提供當地警局、醫院、藥局等資訊。
- 優惠訊息：提供當地即時優惠訊息。

（二）行程規劃

- 建議行程：提供數種行程規劃，並提供該路線遊玩主題、路線簡介、路線順序等資訊。
- 自定行程：依使用者勾選的景點，並輸入起終點及出發時間，系統將自動規劃各景點的遊玩順序。使用者可以清楚的得到總遊玩時間、行車距離及行車時間等資訊。各景點顯示建議停留時間、到達及出發時間，使用者可微調停留時間。各景點間若有美食景點，使用者可以依喜好插入美食景點。

（三）導航

- 安全距離提示：利用手機內建 GPS 抓取車速，並依交通部建議之行車安全距離提醒駕使者。
- 優惠訊息提示：在進入導航時，系統預先載入優惠訊息，當附近有相關優惠訊息時進行提示。
- 行車記錄：本系統直接利用手機做為行車記記錄器，避免過多的電子設備架設在前面影響駕駛的行車安全。
- 事故偵測與求救：利用手機的加速度感應器觀察 G 力變化，判斷是否為撞擊固定物或是追撞等事故。另外利用方向感應器判斷車子是否翻覆或異常迴轉等事故。經由系統判定為事故時，由系統發出求救訊號。

3. 系統功能實做

3.1 旅遊資訊功能

旅遊資訊功能的焦點在提供使用者確實而有用的資訊，為達到此目的，此功能採用從網路擷取即時的資料，解析資料後分層顯示，方便使用者讀取。首先以 GradView 顯示旅遊資訊，在介面上較簡潔且可圖文顯示，較不會受到不同的手機尺吋影響導致版面與預期不同。使用者依據提供的功能選單點選，系統自動將相對應的網址載入，並將擷取的網頁存成字串格式，以便解析。解析的方式利用 xpath 擷取所需的文字、圖片路徑、及下一層連結路徑。最後利用 ListView 顯示出使用者所需的資訊。

旅遊資訊功能主畫面如圖 2 所示，其他部分子功能介紹如下：

圖 3 左畫面列出該年度季節性的活動、主題及活動地點，點選活動後，右畫面顯示活動的內容介紹。圖 4 左畫面列出主題遊樂清單，點選樂活農漁後，右畫面顯示內容的介紹。圖 5 以地區分類顯示熱門景點清單。圖 6 左畫面顯示景點相關資訊包含提供設施、簡介、服務等，右畫面的最下方提供其他功能鍵，包含導航、撥電話、街景與資訊。圖 7 顯示天氣相關的資訊，主要透過即時擷取中央氣象局的天氣資訊頁面。



圖 2 旅遊資訊功能主畫面



圖 3 節慶活動清單與介紹



圖 4 主題遊樂與介紹



圖 5 熱門景點清單



圖 6 景點查詢顯示畫面



圖 7 天氣查詢



圖 10 自訂行程顯示畫面

3.2 行程規劃功能

行程規劃是旅遊過程中重要議題，行程規劃的好壞，決定整個行程是否愉快。所以本功能實作時，預期要達到的目的:第一是提供熱門的路線給較無時間可以完整規劃路線的使用者作為參考;第二是列出熱門景點供使用者自行挑選，由系統規劃路線並計算遊玩時間和行車時間，使用者可自行微調路線及時間，分配遊玩和行車的時間比。

圖 8 左畫面顯示建議行程清單，右畫面提供路線介紹，包含路線名稱、建議遊玩項目、主題、簡介及行程路線等。圖 9 左畫面顯示自訂行程條件輸入，包括起點與終點，以及出發時間。按下預設按鈕系統自動設定起點與終點均為花蓮車站。右畫面顯示景點清單供使用者選擇。圖 10 左畫面顯示系統自動規劃的行程次序，使用者可利用介面的按鈕，調整停留時間和順序。上方顯示總行車時間、總行車距離、總遊玩時間、到達終點時間。右畫面顯示使用者可插入用餐地點，系統會自動檢查該時段仍為營業時間的附近餐廳列表。



圖 8 建議行程顯示畫面



圖 9 自訂行程輸入畫面

自訂行程的規劃方式，並非以最短路徑，算出最佳遊玩次序。這個問題等同旅行推銷員問題（TSP），是個 NP-Hard 的問題。本系統利用簡便又迅速的方式，賦予排序的一種固定規則，讓整個行程時間的安排合理，不至於發生最後回程到終點時都在趕路。

行程規劃分兩種狀態，處理步驟分述如下：

（一）起點與終點不同地

1. 判斷是否只有單一景點，若是則輸出起點→景點→終點的路線，否則下一步。
2. 判斷終點相對於起點在北邊或南邊，若終點在北邊則往南邊出發，若終點在南邊則往北出發。決定往北或往南後，檢視該方向是否有景點，若無則往反方向出發。先決定往終點的反方向遊玩的原因在於，如果往終點的方向先遊玩，再玩反方向，但最終還是要回終點，如此就會浪費時間在車程上。
3. 如果往北邊（南邊）出發，則判斷位於北邊（南邊）所有景點中最靠近南邊（北邊）的景點是在東方或西方。判斷完後往反方向依序造訪景點。此方法的用意在於，因為終點一定在反方向，把最接近該方向的點留到後面再玩，可以讓行程不至於發生中間有一段在趕路，讓行程中景點分部較平均。
4. 若終點方向有未造訪的景點，則先往終點所在地的另一個方向依序造訪景點。

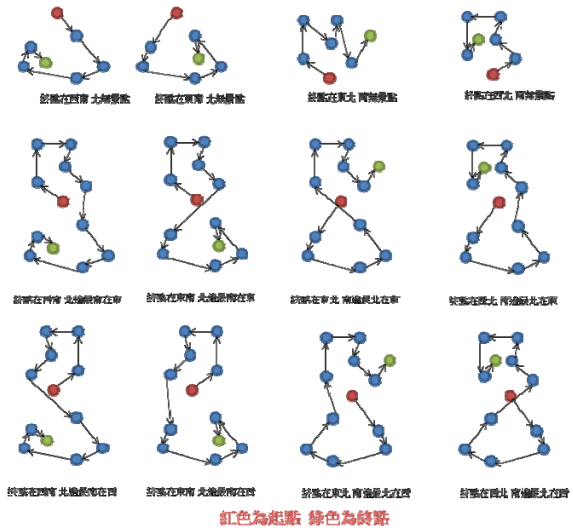


圖 11 起點與終點不同之路線規劃

依據以上步驟整個行程會有三種遊玩方式，分別為 8 字型、順時針與逆時針。圖 11 為各種情況的路線規劃結果。

（二）起點與終點同地

1. 判斷是否只有單一景點，若是則輸出起點→景點→終點的路線，否則下一步。
2. 判斷最靠近起點的景點相對於起點在北邊或南邊，若是在北邊則往北出發，若在南邊則往南出發。
3. 如果往北邊（南邊）出發，則判斷位於北邊（南邊）所有景點中最靠近南邊（北邊）的景點是在東方或西方。判斷完後往反方向依序造訪景點。
4. 判斷步驟 3 另一方向是否有未造訪的景點。如果有則判斷往北時最靠近南邊的景點是在東或西，往南時最靠近北邊的景點是在東或西，判斷完後往反方向玩。

依據以上步驟整個行程仍有三種遊玩方式，分別為 8 字型、順時針與逆時針。圖 12 為各種情況的路線規劃結果。

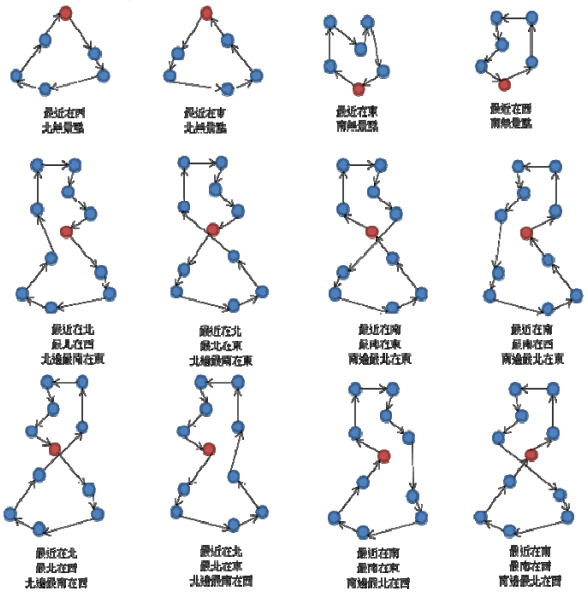


圖 12 起點與終點相同之路線規劃

3.3 導航功能

導航功能主要是使用 Google map 來達到導航的目的，並搭配手機內建 GPS 更新目前位置資訊，抓取即時車速推算出安全距離，提醒駕駛員保持安全距離。導航前必須先做手機的校正，校正介面如圖 13 左畫面，利用圖形模式讓使用者輕鬆校正。校正完成後，使用者輸入目的地，再利用 Google 提供的 Geocoder 服務，將地址轉成地標。右畫面顯示導航路線，上方提示安全距離及優惠訊息。

事故偵測的方法分為二種，第一種是利用加速度感應器偵測 G 力變化，由 G 力辨別是否發生撞擊；第二種是利用方向感應器偵測迴轉角度，由角度變化計算出角速度及曲率半徑，推算出臨界車速[2]，由目前車速判定是否發生事故。系統進入導航時，會儲存上述二種感應器的數值，利用此一連串的數值來辨別是否發生事故。



圖 13 起點與終點相同之路線規劃

偵測項目詳述如下

（一）正面撞擊固定物

依據報告[3]觀察之車輛正面撞擊固定物的 G 力變化，可以發現正面撞擊發生時，G 力會瞬間變大且持續時間約 0.15 秒，撞擊時 G 力瞬間極大值約 20g （$g = 9.81 m/s^2$）。本系統偵測到瞬間 G 力大於 15g，則判定為正面撞擊固定物。

（二）正面撞擊

根據車廠正常煞車測試，全力煞車之減加速度大概為 0.9g。當系統偵測到 0.9g 減加速度時，推算出持續以 0.9g 減速，車子將在 D_{brake} 公尺後停止，而車子實際停止的距離為 D_{rel} 公尺。令 W 為撞擊預測係數，當 $W = D_{brake} / D_{rel}$ 的值小於 0.8 時，則可能發生事故。系統進一步檢查這段煞車至車子停止出現的瞬間 G 值是否大於 1.2g，以確切判定為事故。以 1.2g 為臨界點的原因在於車子若處於上坡階段，加速度變化值最大為 1.2G[4]。

（三）翻覆

當車子發生傾角大於 60 度時，系統就會判定為翻覆。

（四）側滑

側滑的判定為過彎時，當時的車速若大於臨界車速(車輛轉彎時不會發生側滑或翻滾的最大車速)，則判定為事故。由方向感應器可以得到轉彎時的角度變化（$\triangle\theta$）與變化時間（$\triangle t$），利用公式 1 求得角度速度。由 GPS 取得目前的車速即切線速度（v），利用公式 2 求得曲率半徑（r）。再由公式 3 求得臨界車速（v_c），假定摩擦系數為 0.85（參考報告[5]）。

$$\omega = \Delta\theta / \Delta t \quad (1)$$

$$r = v / \omega \quad (2)$$

$$v_c = \sqrt{rg\mu} \quad (3)$$

送出求救流程如下：當發生事故時，系統用語音系統要求駕駛員回應，若 5 秒無回應，則系統自動發出求救。當發出求救時錄影將停止，避免電力

耗盡。訊息發佈分為簡訊及臉書。事故發生後，1 分鐘內十秒發一次訊息，超過一分鐘則 10 分鐘發一次訊息。

當事故發生時，系統採語音的方式接收使用者回覆，使用者僅須回覆 YES 或 NO 即可，如圖 14 所示。系統利用 Text to Speech 和語音識別等功能，完成與使用者互動的目的。當使用者回覆”YES”時，系統即發出求救訊息，圖 15 為在臉書上的訊息發佈。



圖 14 語音確認求救



圖 15 發佈臉書的求救頁面

4. 結論與未來展望

本論文利用智慧型手機開發旅遊服務系統，提供各種旅遊相關的服務，從資料查詢、行程規劃至意外事故的偵測。讓這套系統確實達到其實用性及普及化的效果。

目前的系統架構下，仍有很多可以改善的部份，以下就可以改善的部份做討論：

- 各功能資訊下載時間過長，依功能的不同載入部份需要圖片，大幅的影響其效能。未來將採取在系統啟動時，先將資訊載入資料庫，以提醒模式，建議使用者更新。
- 行程規劃目前仍以文字模式顯示，未來將加入地圖的行程預覽，讓使用者更清楚的知道各行程之相對位置。
- 事故偵測目前系統僅使用二種感應器，目前智慧型手機提供了接近感應器、溫度感應器、壓力感應器等。未來可以整合其他的感應器，提高事故偵測的準確度，並加入其他事故的偵測，如墜落。

誌謝

本研究計畫所需經費由國科會補助，計畫編號為 NSC 101-2221-E-259-027。

參考文獻

[1] “花蓮觀光資訊網”http://tour-hualien.hl.gov.tw/

[2] “南台科技大學-交通事故重建力學網站” http://faculty.stust.edu.tw/~ccchang/22222/formula/01.htm

[3] 馮德安 "車輛撞擊曲線之研究" 大葉大學 車輛工程研究所碩士論文。Jun. 2007.

[4] Vehicle-Used Automatic Alarming System Based on MEMS Accelerometer. *Chinese Journal of Sensors and Actuators*. Vol. 22. No. 6 Jun. 2009.

[5] 交通部運輸所安全組 “我國汽車煞車距離與行車速度關係之測試與研究” 交通部運輸研究所發行, 1995.

無鼠不在-Android 系統上的無線滑鼠

謝瑞宏　　張博誠　　李昱穎
東南科技大學資訊管理系
rhhsieh@mail.tnu.edu.tw　{ 49707153, 49707127 }@mail2u.tnu.edu.tw

摘要

本論文在 Android 手機上開發無線滑鼠的軟體及安裝於筆記型電腦的伺服器軟體，將 Android 手機當做無線滑鼠，並將此軟體命名為無鼠不在。本論文所開發的軟體可以依據場地的情形來決定使用 Bluetooth 或 Wifi 來跟筆記型電腦相連接，以方便使用者不用再攜帶另一支無線滑鼠就能操作。最後本論文以目前已出現的軟體：RemoteDroid、PRemoteDroid 與無鼠不在進行效能分析及成本效益評估，讓使用者可以選擇最方便有效的方式來進行操作。

關鍵詞：Android、Bluetooth、Wifi。

1. 前言

筆記型電腦在目前已是大多數人在外出時，不可或缺的重要工具，而能夠不受場地限制的無線滑鼠也是筆記型電腦的好夥伴，但每次要使用時卻還要額外攜帶，且當使用投影片報告時，筆記型電腦放置的位置有限，使用無線滑鼠的距離和方便性也有限，目前在市面上雖也有 Android 手機充當無線滑鼠的軟體，但在使用上還是有些限制存在。

因此本論文便搜尋這些類似程式，了解這些程式的優缺點並做出比較，最後開發出能把 Android 手機充當無線滑鼠的軟體及安裝於筆記型電腦的伺服器軟體，且因現在市面上類似的程式主要都是以英文介面為主，所以為了廣大的中文使用者在使用時，卻因為英文不熟悉而頭痛，因此將程式介面中文化為主要目的。並且在連線方式上也提供藍芽(Bluetooth)及無線網路(WiFi)兩種方法與筆記型電腦連線，就可以讓處在偏遠地區的人沒有 WiFi 時，也可以使用藍芽通訊來達成此軟體運作之目的。

2. 背景知識與相關研究

2.1 藍芽

藍芽(Bluetooth)是全球性無線連接的實際標準，使各種數位裝置擺脫了電纜的束縛。簡單來說就是一種電信、電腦的無線傳輸技術，其傳輸內容可以是資料、聲音。傳輸範圍最遠可達 10 公尺，並可同時設定加密保護且不受電磁波干擾。

藍芽具有許多優點，包括使用的 2.4 GHz (2.402~2.480 GHz)是全世界通用的免費 ISM (Industrial, Scientific and Medical) 頻段；藍芽需要的功率很低(1~100 mW)，適用於短距離（10~100 公尺）傳輸；藍芽使用跳頻(Frequency Hopping)技術以避免同頻帶之干擾；藍芽無紅外線傳輸受到須在視線範圍(Line of Sight, LOS)內連線之限制。

藍芽規範自 1998 年 0.7 版發布之後，其版本已歷經多次重大演進—由 2004 年 V2.0 EDR 將資料傳輸速率從 1Mbps 提高至 3Mbps；2007 年 V2.1 EDR 提高了設備安全性，增加 Secure Simple Paring(SSP)功能；2009 年 V3.0 High Speed 開始採用 Generic Alternative MAC/PHY 架構，讓應用系統能加快其速度；到 2010 年最新的 V4.0 Low Energy 版本。[1]

2.2 WiFi

本論文所會使用的連線方式有二，選擇使用 WiFi 是因為藍芽的傳輸範圍有限，而 WiFi 的網路範圍用一個典型的無線路由器使用 802.11b 或 802.11g 與天線可能有一個範圍是室內 32 公尺或室外 95 公尺。在 802.11n 可以超過這個範圍兩倍的距離。其範圍也隨頻率的波段調整。

WiFi 的設置至少需要一個 Access Point（AP）和一個或一個以上的客戶端（client）。AP 每 100ms 將 SSID（Service Set Identifier）經由信號台（beacons）封包廣播一次，信號台封包的傳輸速率是 1 Mbit/s，並且長度相當的短，所以這個廣播動作對網路效能的影響不大。因為 WiFi 規定的最低傳輸速率是 1 Mbit/s，所以確保所有的 WiFi 客戶端都能收到這個 SSID 廣播封包，客戶端可以藉此決定是否要和這一個 SSID 的 AP 連線。

WiFi 無線通訊也可以直接不需通過存取傳出從一台電腦到另一台。這就是所謂的 Ad-hoc 模式的 WiFi 傳輸。這種無線 Ad-hoc 網路模式已經獲得許多人的歡迎，例如掌上遊戲機、數位相機和其他消費電子設備。雖然拿藍芽與 WiFi 相比是不適當的，但因為 WiFi 是一個更加快速的協定，覆蓋範圍更大。雖然兩者使用相同的頻率範圍，但是 WiFi 需要當有網路時才可使用。藍芽可在不同的裝置之間建立無線連線，而 WiFi 則是個無線區域網路協定。當需要選擇兩者擇一來使用，可以依方便性來選擇。[2]

2.3 Android

本論文中所選擇使用的手機作業系統是Android，原因是因為Android是以Linux為基礎的開放原始碼作業系統，使用上自由性比較大。

由於Android在應用程式開發上，採取免費、開放的策略。開發者不僅可以免費地下載安裝Android SDK進行應用程式的開發。更重要地是，人們可以使用多數程式設計師所熟悉的Java程式語言進行應用程式的撰寫。因為這兩個特點，促使為數眾多的Java程式設計師蜂擁至Android應用程式的開發行列。

Google為了讓更多開發者參與Android應用程式的開發行列，因此，它開放給大眾免費下載安裝Android軟體開發工具包（Software Development Kit，SDK）。而且這個工具包可以安裝在Windows、Linux以及Mac等不同的作業系統環境當中。Android SDK除了提供了完整的Android API之外，更包括了Android應用程式除錯工具（Android Debug Bridge， ADB）以及Android手機模擬器（Android Emulator，此為在個人電腦上模擬Android手機的環境）。

除了Android SDK之外，其他配合它的軟體也是免費性質。這些軟體包括了Eclipse整合開發環境（Integrated Development Environment，IDE）以及Eclipse專用之Android開發工具外掛（ADT Plugin for Eclipse）。再加上原本就免費開放下載的Java開發工具包。開發者幾乎不用花費到一毛錢，便可以自己建構一個很完整且便利的Android應用程式開發環境，並專心構思與發展屬於自己的應用程式。[3]

2.4 測試RemoteDroid、PremoteDroid

本論文搜尋到目前已出現的軟體：RemoteDroid與PRemoteDroid，並實際使用來進行測試，以了解這2套軟體的優缺點，作為開發無鼠不在的依據。

RemoteDroid此軟體和目前本論文所要作的畫面有很大的不同。在畫面上面，它把左右鍵放在程式的下方，並在中間使用了小鍵盤的功能，顏色上也有很奇特的配色。在連線方面，它只有WiFi連線的方法，連線的速率也算流暢，但可能是流暢的關係，滑鼠游標比PremoteDroid還來的稍快一點，也有可能是PremoteDroid有靈敏度的調整。功能方面，它裡面的設計非常陽春，只有單純的左右鍵以及小鍵盤，並沒有額外的設定，小鍵盤也可能是外國語系，因此中文沒有辦法撰寫，只能在記事本上面撰寫英文。總體來說，此軟體是本論文目前第一個找到的軟體，陽春的設計可能是此種類首次製作的軟體，並沒有文獻可以辦法研究，這是它以後可以去做更新的方向。[4]

兩個軟體相較之下，PRemoteDroid軟體則具有多樣性，例如可開啟檔案總管讓在手機裡頭找資料更輕鬆、螢幕畫面擷取讓人不再搞不清楚游標在何處、安全（密碼）連線使得安全性更高資料也不容易洩密了。而在滑鼠的靈敏度方面，更是設計得可圈可點，完全不遜色於實體滑鼠。有鑑於測試後的成果，讓本論文在於中文輸出、支援介面中文化、以及產品個人化設定的部分有了加強的決心。[5]

RemoteDroid、PRemoteDroid測試列表如表一所示：

表一 測試RemoteDroid、PRemoteDroid表

軟體名稱：RemoteDroid	軟體名稱：PRemoteDroid
下載金額：Free（免費）	下載金額：Free（免費）
主要特點： 支援WiFi連線 支援滑鼠遊標和鍵盤功能 相容於Mac.Windows和Linux系統 版本支援1.6以上 解析度通用於Android系統	主要特點： 支援藍芽和WiFi連線 支援滑鼠遊標和鍵盤功能 檔案總管 螢幕擷取 安全（密碼）連線 版本支援2.0以上 解析度通用於Android系統
缺點： 沒有支援中文化介面 沒有支援藍芽連線功能	缺點： 沒有支援中文化介面

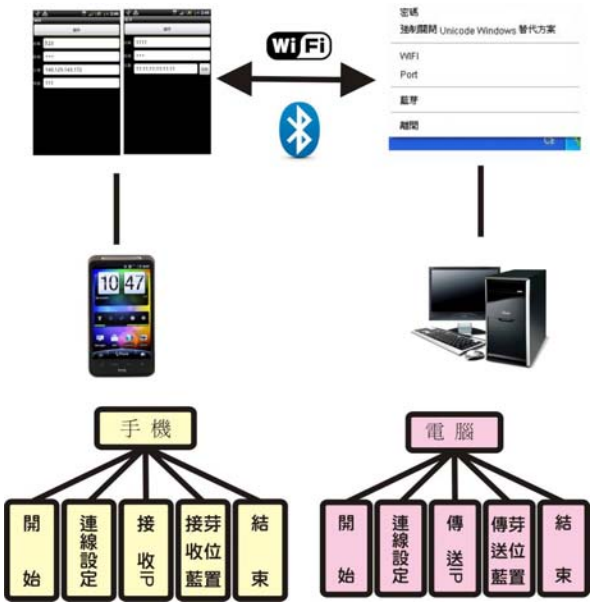
本論文研究的方向，著重在於PremoteDroid的外貌及功能設計，連線方面可以參考RemoteDroid的WiFi設定以及PremoteDroid的藍芽設定，並且新增個人化（背景更換）可供使用者選擇想要的畫面。

3. 設計原理及架構

3.1 系統架構

本論文針對使用者的需求及考量連線方式以及不受場地限制的便利性，將以連線方式「WiFi&藍芽」為系統架構的主要說明項目。

主要選單以上彈式選單來導引使用者操作，並且以中文說明以便降低使用者在瀏覽時所遇到的挫折感。並藉由圖文的排列方式，降低使用者在連線時所產生其他操作上的干擾。連線展示圖如圖一所示：



圖一 連線展示圖

3.2 開發環境與軟體設計

開發系統：Android 系統

開發工具：Eclipse 開發軟體

本論文的主介面架構重點在於中央的儲存，可把變更後的 Port 號和密碼存下來。程式重點如圖二所示：

```
private Preferences preferences;
private GodMouseServerApp application;
private TrayIcon trayIcon;

public GodMouseServerTrayIcon(GodMouseServerApp application) throws AWTException, IOExc
{
    this.application = application;

    this.preferences = this.application.getPreferences();

    this.initTrayIcon();
}

public void notifyConnection(GodMouseConnection connection)
{
    String message = "";

    if (connection instanceof GodMouseConnectionTcp)
    {
        GodMouseConnectionTcp connectionTcp = (GodMouseConnectionTcp) connection;
        message = connectionTcp.getInetAddress().getHostAddress() + ":" + connectionTcp
    }
    else if (connection instanceof GodMouseConnectionBluetooth)
    {
        message = "Bluetooth";
    }
```

圖二 主介面架構

本論文的 WiFi 連線架構包含預設 Port 號和 Socket 的語法。程式重點如圖三所示：

```
public final static int DEFAULT_PORT = 55050;

private Socket socket;

public GodMouseConnectionTcp(Socket socket) throws IOException
{
    super(socket.getInputStream(), socket.getOutputStream());

    this.socket = socket;
    this.socket.setPerformancePreferences(0, 2, 1);
    this.socket.setTcpNoDelay(true);
    this.socket.setReceiveBufferSize(1024 * 1024);
    this.socket.setSendBufferSize(1024 * 1024);
}

public static GodMouseConnectionTcp create(String host, int port) throws IOException
{
    Socket socket = new Socket();
    socket.connect(new InetSocketAddress(host, port), 1000);

    GodMouseConnectionTcp connection = new GodMouseConnectionTcp(socket);

    return connection;
}

public InetAddress getInetAddress()
```

圖三 WiFi 連線架構

本論文的藍芽連線架構包含 UUID 及密碼的設定。程式重點如圖四所示：

```
public static final String BLUETOOTH_UUID = "300ad0a7-0594-4d97-b9a3-eabe5f6af813";
public static final String DEFAULT_PASSWORD = "55050";

private DataInputStream dataInputStream;
private OutputStream outputStream;

public GodMouseConnection(InputStream inputStream, OutputStream outputStream)
{
    this.dataInputStream = new DataInputStream(inputStream);
    this.outputStream = outputStream;
}

public GodMouseAction receiveAction() throws IOException
{
    synchronized (this.dataInputStream)
    {
        GodMouseAction action = GodMouseAction.parse(this.dataInputStream);
        return action;
    }
}

public void sendAction(GodMouseAction action) throws IOException
{
    ByteArrayOutputStream baos = new ByteArrayOutputStream();
    action.toDataOutputStream(new DataOutputStream(baos));
```

圖四 藍芽連線架構

本論文的滑鼠移動架構是將手機的座標方位傳送至電腦上。程式重點如圖五所示：

```
import java.io.DataInputStream;

public class MouseMoveAction extends GodMouseAction
{
    public short moveX;
    public short moveY;

    public MouseMoveAction(short moveX, short moveY)
    {
        this.moveX = moveX;
        this.moveY = moveY;
    }

    public static MouseMoveAction parse(DataInputStream dis) throws IOException
    {
        short moveX = dis.readShort();
        short moveY = dis.readShort();

        return new MouseMoveAction(moveX, moveY);
    }

    public void toDataOutputStream(DataOutputStream dos) throws IOException
    {
        dos.writeByte(MOUSE_MOVE);
        dos.writeShort(this.moveX);
        dos.writeShort(this.moveY);
```

圖五 滑鼠移動架構

4. 成品展示及操作說明

此程式主要有六個頁面，分別是主畫面、Menu、連線（WiFi、藍芽）、幫助、小鍵盤及檔案總管，左右鍵及滾輪的按鈕，主要是模擬真實的滑鼠操作，主要按鍵有個人化、連線、小鍵盤、幫助、離開。Menu 請參考圖六所示：



圖六 Menu

其中的連接有 WiFi、藍芽介面可點選，選擇之後按新增，可以連至 WiFi 或藍芽的連線畫面，如圖七所示：



圖七 連線-WiFi、藍芽

以 WiFi 協定連線的介面，除了基本的名稱及密碼外，WiFi 所需要的主機 IP 以及 Port 號上都需要做設定才可連線，如圖八所示：



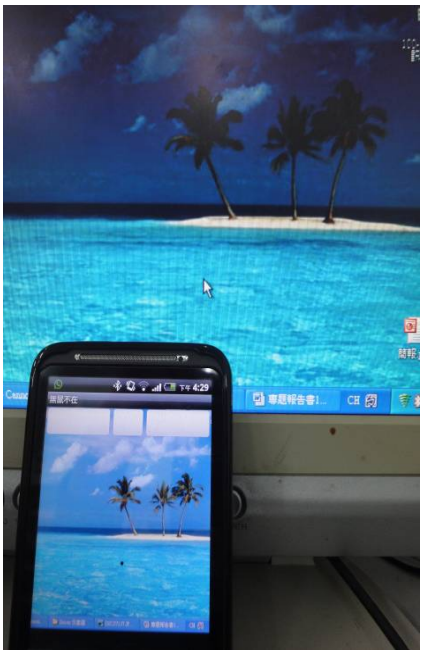
圖八 連線-WiFi

有關設定的部份可從 Menu 點選設定做選擇，功能包括有：靈敏度和進階控制可調滑鼠的速度及滑鼠的相關設定，反饋則可點選聲音及振動，勾選後可使手機在操作上發出聲音或振動，然而其他選項裡全螢幕可使畫面展開，另外鎖定畫面為固定滑鼠移動的位置，捕捉啟用則可擷取電腦螢幕上的畫面，並且顯示在手機背景上，進階捕捉內則是設定抓取的圖片格式以及中心點的設定，如圖九所示：



圖九 設定

擷取畫面的功能可以抓取到目前電腦桌面上的畫面，每操作一次便會自動更新，如圖十所示：



圖十 擷取桌面畫面

5. 成效評估

5.1 軟體成效及差異評估

本論文先以目前已出現的軟體：RemoteDroid、PRemoteDroid 與無鼠不在的功能做出比較，功能比較表請參考表二：

表二 相關應用軟體功能比較表

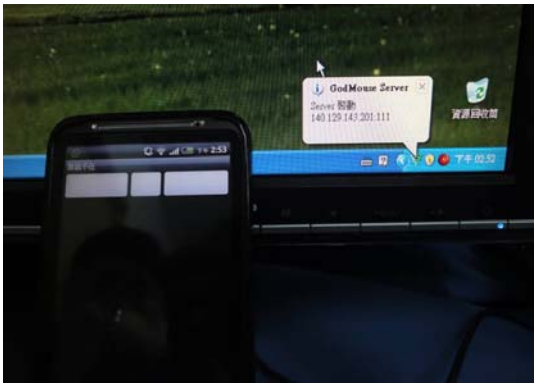
	無鼠不在	PRemoteDroid	RemoteDroid
使用藍芽傳輸	O	O	X
使用 WiFi 傳輸	O	O	O
無線鍵盤	O	O	O
無線滑鼠	O	O	O
介面中文化	O	X	X
解析度通用於 Android 系統	O	O	O
系統版本通用	2.2 以上	2.0 以上	1.6 以上

從上表可以發現本論文的軟體有以下優點

- 執行順暢，不受手機解析度不一的困擾。
- 可依據使用場合選擇 WiFi 或藍芽傳輸。
- 介面中文化，使用更簡單。
- 可切換滑鼠或鍵盤。

5.2 實際操作展示

圖十一為實際操作畫面，展現手機與電腦連線操作的畫面：



圖十一 連線操作

6. 結論

本論文所開發出來的的軟體可以讓目前擁有 Android 手機的使用者去使用手機來操作筆記型電腦，而且在操作的同時還可以擷取桌面上的畫面，可以用 WiFi 連線當作監視畫面，所以能知道這台電腦的畫面在做甚麼事。而在沒有 WiFi 服務的地區，也可使用筆記型電腦裡內建的藍芽去做連線，免除了其餘軟體只能使用 WiFi 連線的困境。

本論文的未來發展將考慮加入音控，避免太多複雜的輸入而造成使用者不便，以達到智慧生活科技的目的。

參考文獻

[1] 劉皓宇，一個以藍芽路由通訊協定所架構的 Ad Hoc 網路，國立中山大學碩士論文，2001 年。

[2] http://zh.wikipedia.org/wiki/WiFi，WiFi 維基百科

[3] http://zh.wikipedia.org/zh-tw/Android，Android 維基百科

[4] http://www.openfoundry.org/tw/foss-programs/8217--android RemoteDroid

[5] http://code.google.com/p/premotedroid/ Promotedroid

建立於 Android 系統之鑰匙自動辨識系統

王建仁　沈英謀　蔡哲民　鄭承淵
崑山科技大
電腦與通訊系、資訊管理系、資訊傳播系、電腦與通訊所
{ cjw, shenyin , tjm }@mail.ksu.edu.tw ;　jim122664@livemail.tw

摘要

生活中有許多地方都必須利用鎖來防止財物被他人竊取，所以一般人都會擁有一把以上的鑰匙來解開各種不同的鎖具。由於鑰匙在外型上都很相似，對於視力模糊、記憶力退化的年長者或是其他具有類似障礙的族群來說，可能難以分辨出鑰匙的種類。

本論文提出一套 Android Based 的鑰匙自動辨識系統，使用者只須使用智慧型手機的 Camera 拍攝欲辨識的鑰匙，系統就會自動從影像中切割出物件，與特徵資料庫進行比對，並將分析出來的鑰匙種類回傳給使用者。特徵資料庫主要分為「形狀」與「紋理」兩種特徵，為了防止使用者物件擺放的角度與位置的不同影響辨識結果，系統會先進行角度與大小正規化，再進行特徵擷取。形狀特徵是利用擷取物體的 Centroid-Contour Distance(CCD)來描述，紋理特徵則是先將影像透過 Sobel 進行邊緣偵測(Edge detection)，並將影像分成 N 個區域，再計算各個區域的邊緣數量，做為紋理區域分佈特徵。綜合以上兩種特徵值，再利用 K-nearest neighbor(KNN) 進行特徵比對。

本系統經過實際測試後，成功辨識率為 82.81%，未來將尋找測試對象，實際將此系統運用於使用者的日常生活，並持續探討如何優化使用者介面以及提高辨識率。

關鍵詞: 鑰匙辨識、智慧型手機、中高齡。

Abstract

Locks are widely used for preventing property stolen by others. Generally, most people would have lots of locks in various environments and results in possessing lots of keys. Since the appearances of the keys are similar, specifying the correct key is difficult for the people with blurred vision, memory loss or other obstacles.

This paper introduces an Android based automatic key recognition system based on image techniques. The system stores the features of all the keys owned by the user. The user only needs to use his/her smart phone to take the photo of the selected key. The system will automatically extract the features of the key and compare these extracted features with those in the database. The system will select the one in the database which is the most similar to the testing key as the recognition result. The features used in our system are shape and txture. In order to avoid the influence resulted in different position and angle of the key, after segmenting the key image from the background, the system would first rotate the key and align the key image on the y-axis of the test plane. Then the key image is scaled to a predefined size. The feature of the shape is the Centroid-contour-distance (CCD). The texture feature extraction is as follows: The key image is processed by Sobel edge-detection algorithm first, and then the divided into N regions and the edge points of each region is counted. These edge point counts serve as the texture distribution. The K-nearest neighbor (KNN) method is applied to perform the comparison task.

The recognition rate of the system reaches 82.81% during the field test. In the future, we will continue to explore ways to improve the recognition rate and optimize the user interface.

Keywords: Key Recognition, Smart Phone, Senior People

1. 前言

都市化人口集中後的結果，導致治安一直是現代人的顧慮。為了保護私人的財產與個人的人身安全，門戶管制已經成為必要的手段。平常最常見到的門戶管制方式就是利用鎖來管制進出的人員。由於鎖的成本較低、牢固且使用方便，所以被廣泛的運用在人們生活中，從家中大門、後門、汽機車、辦公室、甚至電腦、保險箱....到處都可以看到鎖的蹤跡，也因此幾乎每個人都會擁有一把以上的鑰匙。雖然鎖具可以使個人財物多一分保障，但對於視力模糊、記憶力退化的年長者或是其他具有類似障礙的族群來說，當擁有多把以上的鑰匙時，會經常無法分辨所持有的鑰匙與對應的鎖頭，而產生諸多不便。

近年來智慧型手機已越來越普及，雖然主要用戶還是以中低年齡層為主，但已經有越來越多業者開始針對高齡族群的使用者作研發設計，而且因為智慧型手機或平板電腦的螢幕比傳統手機還要寬大，市面上專為高齡族群設計的產品也越來越多，因此很多人都已將智慧型手機或平板電腦作為贈送長輩禮物的首選。也因為高齡族群的使用者越來

越多，許多軟體開發業者也開始投入開發適合高齡族群使用的手機應用程式，目前最常見的功能有拍照、攝影及健康管理[1]等，因此我們希望開發更多能夠融入高齡族群日常生活的應用程式。

目前已經有許多的平台逐漸開始運用影像辨識技術來辨識物件，但能夠真正用於日常生活中的卻不多，許多系統都只適用於特殊的研究單位，或者是必須仰賴特殊設備，讓一般民眾無法自行建立完整的辨識系統。過去我們曾經製作一套辨識平台[2]，透過辨識物件提供使用者一個互動式的學習環境。另外也製作過一套昆蟲影像辨識系統[3]，包含貝殼、甲蟲及蝴蝶等物種，使用者透過網頁上傳昆蟲的影像，即可辨識出相對應的昆蟲資訊。但這些影像辨識系統大多需要一個穩定的環境(辨識箱)，或是倚賴網路傳回雲端上的伺服器作運算，若使用者沒有適合的環境或是無線網路，便無法即時取得想要的資訊，因此本系統除了製作一套鑰匙辨識系統，最主要的目的，是希望能夠讓影像辨識流程可以直接在手機上獨立完成，以減少系統的使用限制。

本研究提出一套鑰匙辨識系統，用來幫助使用者辨識出鑰匙的用途。使用者只須使用智慧型手機的 Camera 拍攝欲辨識的鑰匙，系統就會自動擷取影像，然後利用由蔡哲民等人發展的影像自動切割技術[4]將 Camera 輸入之影像進行物件切割，再依據權重式主體判斷物件大小以及物件與畫面中心距離之比重取出標的物件。由於使用者物件擺放的角度與位置可能不完全相同，為了避免因這些狀況影響辨識率，系統會將擷取出的物件進行正規化，再進行特徵擷取。並且系統利用擷取物體的 Centroid-Contour Distance(CCD)[5]以及 Sobel 影像作為形狀與紋理特徵，以進行物件種類的比對。我們期望本系統能夠成為視覺與記憶退化者的居家幫手。

2. 研究方法

傳統的鑰匙辨識系統[6]擷取影像的設備為一內嵌 Webcam 的鑰匙辨識盒，因為辨識盒中 Webcam 為固定高度，並且附有固定光源，受控條件較多、環境也單純，因此能夠獲得極高的辨識率，但因為辨識盒體積過於龐大，且必須連接傳統電腦，仰賴電腦的硬體設備進行運算，因此在使用環境上有很大的限制。

目前應用於智慧型手機上的影像辨識系統，很多都是利用手機擷取影像後，透過網路將影像傳到雲端伺服器進行運算[7][8]，與特徵資料庫比對後，再將辨識結果回傳到手機。雖然雲端伺服器的運算能力較強，但使用上卻受限於手機必須連接網路，倘若使用者沒有網路可用或是網路品質不佳，將導致大量延遲甚至系統無法運作。而實際尚無線網路的普及率還不是 100%，且許多人礙於費率問題也無法隨時使用 3G 網路，因此實現一個利用手機本身取像與運算能力進行辨識的系統，是本研究希望完成的目標。

本系統的影像擷取設備為智慧型手機的後置鏡頭，並且將特徵資料庫儲存於手機端，由於一般家庭使用的鑰匙數量不多，因此透過智慧型手機本身即可完成整個影像辨識流程。

2.1 系統架構

圖 1 為系統運作流程圖，使用者利用本系統之拍照功能擷取影像後，由影像中擷取出欲辨識物件，先進行影像正規化，再將影像送入特徵擷取流程。若使用者選擇建立特徵資料庫，系統會將所擷取出之鑰匙特徵建立於資料庫中，若使用者選擇進行鑰匙辨識，系統會將擷取出的鑰匙特徵與資料庫中的數據進行比對，並判斷該物件種類或「非資料庫種類」。如果辨識物件不屬於資料庫內種類，則告知使用者重新放置其他物件，如果存在於資料庫，則輸出和檢索最相近的物件資訊給使用者。

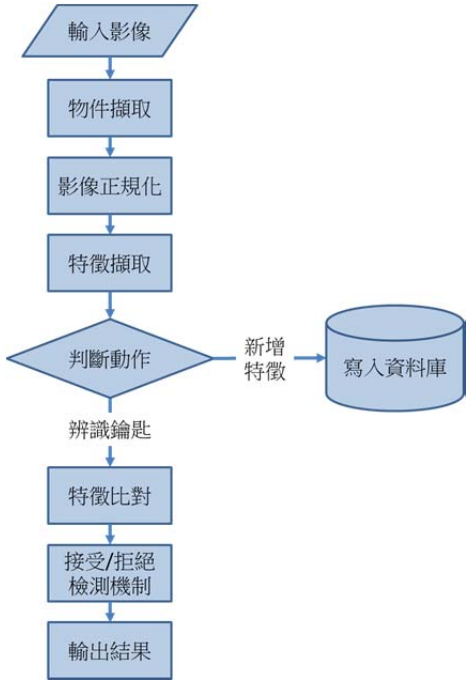


圖 1 系統運作流程圖

2.2 影像物件擷取

實際處理影像辨識之前，必須先將前景物件和背景影像分離，以避免受到背景物件的干擾。目前物件切割技術較常見的有背景相減(Background Subtraction) [9]、顏色分群(Color Clustering) [10]、分水嶺演算法(Watershed)[11]或是經由人工定義初始輪廓的方式擷取物件[12]。但是上述這些方式大都需要使用者介入，如標示初始輪廓、擷取背景、設定參數等，較不易於建置全自動化系統。

因此本系統採用由蔡哲民等人所發表的影像自動切割技術[4]進行擷取。首先將彩色影像轉為灰

階影像，利用 9x9 的均值濾波器(Mean Filter)去除多餘雜訊，再用 Sobel 邊緣偵測演算法，利用 3x3 遮罩分別對影像之水平軸與垂直軸進行掃描，取得二值化影像，再將此影像利用鏈碼(Chain Code)掃描取得物件的輪廓，最後依據權重式主體判斷物件大小以及物件與畫面中心距離之比重取出標的物件。

2.3 物件正規化

經由物件擷取程序取得之鑰匙影像，可能因拍攝時的角度不同或鑰匙擺放的位置不同，而導致擷取到的物件大小及角度不一致，這些差距將會影響物件特徵的擷取，所以為了讓所有物件可以在相同的條件下做比對，必須將所有影像調整至相同角度與大小。因此我們統一將鑰匙較窄的一端轉到上方，並且將物件影像較長的一邊正規化為 320 像素的長度，另一邊則等比例縮放，如圖 2 所示。



圖 2 (A)原始圖片、(B)物件擷取、(C)正規化

2.4 物件特徵擷取

本系統主要利用「形狀」與「紋理」做為描述影像的特徵。擷取形狀特徵時，是將整把鑰匙都列入特徵值計算，而擷取紋理特徵時，考量到鑰匙的握把大多為黑色，較無明顯的變化，因此只針對鑰匙前端金屬的部分擷取特徵。

2.4.1 形狀特徵

以往學者曾提出許多形狀特徵的演算法，本系統是採用 Centroid-Contour Distance(CCD) [5] 的方法來擷取形狀特徵。在取得完成正規化之影像後，計算其質心與物件輪廓之間的歐基里德距離，並以正 Y 軸為 0 度，依照順時鐘方向每 1 度取一次距離作為物件的 CCD 特徵，最後取出 360 個數值作為物件形狀的特徵。

2.4.2 紋理特徵

紋理特徵中較常見的有 Sobel 邊緣特徵[13]、哈爾小波轉換(Harr Wavelet Transformation) 以及統計矩(Moment)等方法，Sobel 邊緣特徵本身包含了許多非顏色的特徵資訊，非常適合應用在非顏色的影像辨識上；哈爾小波轉換是一種將空間域影像轉換成頻率域影像的演算法，但此種方法只能描述物件表面的複雜度，卻無法詳細描述物件紋理的分布；統計矩是使用強度直方圖的統計特性，通常用來分辨兩個影像之間的統計差異，雖然可以描述物件的顏色比例，但卻無法描述顏色的分佈位置，並且鑰匙表面較無明顯的顏色差異，因此本系統選擇利用 Sobel 邊緣特徵作為描述紋理特徵的方法。但由於此方法特徵數量較大，且在比較差異時可能因為些微的誤差導致辨識率降低，因此本系統將影像切割成 2 x 10 個相同大小的區塊，如圖 3 所示，並統計各區塊內邊緣的數量做為本研究的紋理區域分佈特徵，如此一來不僅可縮減資料量、增加比對速度，還可以有效降低正規化過程中的誤差所產生的影響。



圖 3 紋理特徵擷取過程

2.5 建立特徵資料庫

使用者進入系統時，若是選擇「建立特徵資料庫」(如圖 4)，系統完成特徵擷取後，就會自動寫入檔案並存入手機，每支鑰匙都必須建立兩次資料，包含垂直拍攝與水平拍攝，建立完成後，即可使用辨識功能。

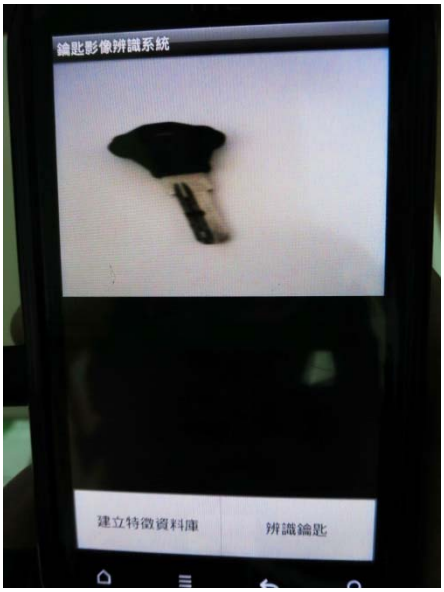


圖 4 選擇動作畫面

2.6 特徵比對演算法

使用者進入系統時，若是選擇「辨識鑰匙」，系統完成特徵擷取後，就會自動進行特徵比對，特徵比對演算法有很多種，常見的有 K 最近鄰居法(K-Nearest Neighbor)、投票法(vote)及類神經演算法(Neural Network Algorithm) 和 高 斯 演 算 法

(Gaussian-Based Algorithm)，由於一般家庭的鑰匙數量不會太多，對於類神經和高斯等演算法來說，在樣本數量較少的情況下，因缺少大量樣本的訓練，無法有良好的辨識率，但在樣本數較少的狀況下，能有良好辨識率的演算法並不多，K 最近鄰居法和投票法二種演算法就是比較具代表性的演算法。因為一般人所擁有的鑰匙通常不多，因此我們僅選用 K 最近鄰居法(K-nearest neighbor, KNN) [14]來進行特徵之比對演算。

K 最近鄰居法是採用向量空間模型的觀念來進行分類，其原理是同種類的樣本，彼此間的相似度會較高，所以可以藉著計算與已知種類樣本之間的相似度，來找尋找未知種類樣本可能歸於哪一種類中。K 最近鄰居法的執行步驟如下。

1. 依歐基里德距離(Euclidean distance, Ed)公式計算未知種類樣本與已知種類樣本之間的特徵值相似度。
2. 將其樣本特徵相似度大小排序，將其放入一相似集合中。
3. 從相似集合 NN 中取出前 K 名，依照多數種類決定，而得到該未知種類樣本的可能相似種類。

由於辨識的樣本種類並不多，所以我們僅採用 K=1，取最近似的一個樣本做為分類依據，並以最接近樣本之 Ed 值作為接受/拒絕檢測機制判斷的依據，辨識完成的結果如圖 5 所示。



圖 5 辨識結果畫面

2.7 接受/拒絕檢測機制

為了判斷使用者放置樣本是否為正確辨識樣本，所以本研究提出接受/拒絕檢測機制，利用 K 最近鄰居法去計算資料庫樣本之間的差異值 Euclidean distance (Ed)作為基礎，求出資料庫內的同一物種之間差距最大值 Max 和每一物種與其它不同種之間的差異最小值 Min。

關於門檻值的計算，本系統分別計算 Max 和 Min 之算術平均 Ari_{ave} (式 1)與幾何平均 Geo_{ave} (式 2)，作為該種鑰匙的門檻值。

$$Ari_{ave} = (Max_{Ed} + Min_{Ed})/2 \quad (1)$$

$$Geo_{ave} = \sqrt{Max_{Ed} * Min_{Ed}} \quad (2)$$

當特徵比對演算法找出資料庫內最接近使用者辨識樣本的物種後，接受/拒絕檢測機制便會將最接近物種之 Ed 值與門檻比較，當 Ed 值大於門檻則使用者辨識樣本為非辨識樣本，反之如果 Ed 值小於門檻則使用者辨識樣本為正確辨識樣本。經過測試我們最後選用非辨識樣本拒絕率較高的方法(2)。

3. 實驗結果與討論

本系統使用的實驗設備為 HTC Desire S，CPU 為 Qualcomm Snapdragon MSM8255 1GHz 單核心處理器、記憶體為 768MB 的智慧型手機，在 Android 系統下使用 JAVA 程式語言開發辨識系統。

我們總共進行了三項實驗，實驗內容為辨識 8 種不同的鑰匙，如圖 6 所示，並且分別旋轉八個方向進行測試，如圖 7 所示。我們分別利用形狀特徵與紋理特徵單獨進行辨識，最後再將兩種特徵以權種的方式混合進行辨識，以驗證同時利用兩種特徵進行辨識可以有效提升辨識率。

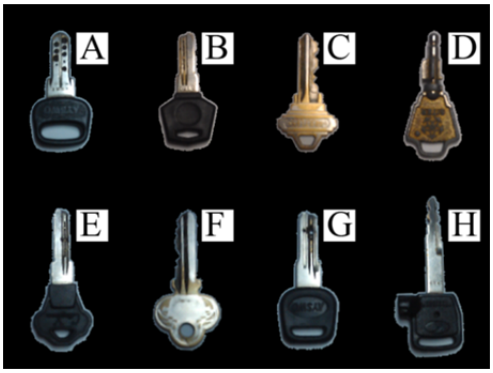


圖 6 鑰匙樣本

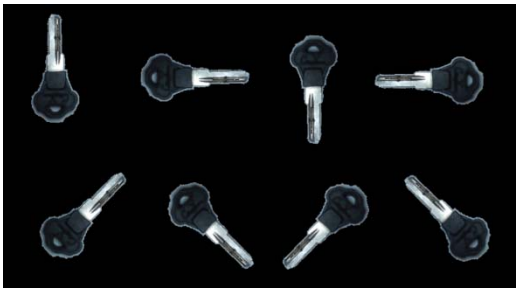


圖 7 拍攝鑰匙示意圖

表 1 辨識率測試結果

鑰匙樣本	形狀(%)	紋理(%)	形狀+紋理(%)
樣本 A	62.5	50	75
樣本 B	75	0	75
樣本 C	100	62.5	100

樣本 D	87.5	62.5	87.5
樣本 E	87.5	75	87.5
樣本 F	62.5	62.5	75
樣本 G	62.5	75	62.5
樣本 H	100	62.5	100
平均	79.7	56.25	82.81

實驗結果如表 1 所示，形狀特徵的平均辨識率為 79.7%，其中樣本 A、B、G 因其形體較接近，因此辨識率較低；紋理特徵的平均辨識率為 56.25%，因為鑰匙為金屬表面，拍攝影像時容易受到光線影響，因此也影響到 Sobel 的結果，但測試的過程中，部分因形體過於接近而導致形狀特徵無法正確辨識的鑰匙，卻因為紋理特徵的加權而辨識成功，因此雖然紋理特徵整體辨識率較低，但因紋理特徵能夠輔助形狀特徵達到提升辨識率的效果，因此證明同時利用形狀特徵與紋理特徵能有效提高辨識率。

4. 結論

過去的影像辨識系統大部分都偏向研究性質，或者是必須仰賴特殊設備才能使用，因為這些使用限制，而讓一般民眾無法享受到影像辨識系統所帶來的便利性。隨著智慧型行動裝置的發展，開發能夠融入民眾日常生活的應用程式已成為目前的趨勢，因此本論文提出一套基於 Android Based 的鑰匙自動辨識系統，讓民眾能夠利用自己的智慧型手機或是平板電腦，自行建立完整的影像辨識系統，讓家中的高齡族群或是記憶退化者，能夠藉由這套影像辨識系統，改善日常生活中的不便。

本系統目前已達到 82.81%的辨識率，未來將持續針對如何提高辨識率以及使用者操作方面進行改善。

參考文獻

[1] Newton Circus，2013 年 8 月 15 日取自 http://newton-circus.com/silverline/

[2] 蔡哲民、王建仁、吳明昆、蔡文吉。2007。基於影像識別技術之實物教學平台。臺灣網際網路研討會。

[3] 以顏色與梯度特徵為基礎的昆蟲影像辨識系統，2013 年 8 月 15 日取自 http://iden.vexp.idv.tw/iden1/

[4] 蔡哲民、蔡濟鴻、王建仁、沈英謀。2010。權重式之自動切割技術。優質家庭生活科技關鍵技術研討會(Uhome2010)。

[5] Wang, Z., Z. Chi, and D. Feng, 2003. Shape based leaf image retrieval. IEE Proceedings–Vision Image and Signal Processing, 150(1): 34 – 43.

[6] 蔡哲民、蔡濟鴻、王建仁、傅耀賢、沈英謀，2011，鑰匙自動辨識系統，優質家庭生活科技關鍵技術研討會(Uhome2011)。

[7] Google Goggles，2013 年 8 月 15 日取自 http://www.google.com/mobile/goggles/#text

[8] 台灣大學蝴蝶辨識系統，2013 年 8 月 15 日取自 http://www.flyingman.com.tw/portfolio/item/43-%E8%9D%B4%E8%9D%B6%E8%BE%A8%E8%AD%98

[9] Kehtarnavaz, N. and F. Rajkotwala. 1997. Real-Time vision-based detection of Waiting pedestrians. Real-Time Imaging 3: 433-440.

[10] Hong, A., G. Chen, J. Li, Z. Chi, and D. Zhang. 2004. A flower image retrieval method based on ROI feature. J. of Zhejiang Univ. Sci. 5: 764-772.

[11] Vincent, L. and P. Soille. 1991. Watersheds in digital spaces:an efficient algorithm based on immersion simulations, IEEE Trans. Pattern Analysis and Machine Intell. 13: 583-598.

[12] Kass, M., A. Witkin and D. Terzopoulos. 1987. Snakes-Active contour models. Inter. J. of Comp. Vis. 1: 321-331.

[13] T. Lindeberg,“Edge detection and ridge detection with automatic scale selection”, in Proc.of the IEEE Conf. on CVPR, pp. 465, June 1996.

[14] Iwerks, G.S., H. Samet and K. Smith. 2003. Continuous-nearest neighbor queries for continuously moving points with updates, VLDB 29 : 512-523.

以智慧型手機之定位功能結合微控裝置實現節能家電控制

程榮祥 [1*]　廖健智 [2]　林家鵬 [3]
崑山科技大學電腦與通訊系
[1]rscheng@mail.ksu.edu.tw, { [2]kenguerrilla, [3]n80813203 }@gmail.com

摘要

智慧型手機已經取代個人電腦，成為協助使用者處理生活瑣事，提供適地性服務的重要工具。由於現代人與智慧型手機幾乎形影不離，無線感應裝置也變得更加輕巧、無所不在，因此透過智慧型手機，居家連網的概念變得明確可行，但由於聯網家電的應用尚處於起步階段，除了極少數的聯網家電外，大部份的傳統家電仍然不具有網路連線功能，消費者因此無法感受到家電聯網帶來的好處。為解決此一問題，本篇論文在智慧型手機上開發具備網路連線功能並可進行遠端控制的智慧型家電管理系統。

關鍵詞：地理位置服務，智慧型家庭，智慧型手機

Abstract

Recently, smartphones have replaced personal comupters becoming an important tool which help users to manage daily things and provide location-based service (LBS). Owing to people nowadays can not live without smartphones, wireless sensors has become light-weighting and popular. Therefore, through smartphones, the concept of home networking is applicable now. However, because home networking appliances are on the starting phase, at present, in addition to few appliances, most traditional home appliances are unable to connect to network. Consumers thus have not felt the advantage of home networking appliances. To solve this issue, this paper developed a smart home appliance management system which can connect to network and allow users to conduct remote control on smartphones.

Keywords: LBS, Smarthome, Smartphone

1. 前言

隨著數位匯流的興起，多樣性與附加功能的通訊產品，讓產品在設計與定位上出現了跨產業整合的市場模式，同時也改變了人們的生活方式，廣播電視、資通訊產業的傳輸管道和服務範圍也日益多樣化，特別是在語音、視訊及數據三種服務的界限開始逐漸淡化，以整合服務為導向，人們也開始習慣透過網路、電視與電信等多元方式存取多媒體、遊戲、地圖、電子商務及雲端數據傳輸等應用，讓廣大的行動通信用戶能快速且隨時隨地獲取他們需要的資訊和服務[1]。

由於智慧手機可以提供適地性與個人化的行動加值服務，加上近年來智慧生活的概念逐漸受到重視，因此智慧型手機與終於消費電子產品的結合逐漸受到電信業者、內容提供廠商以及終端消費者的關注，並且成為消費性民生電子應用的重要研究議題，透過智慧型手機提供的個人化與適地性服務，居家聯網的概念變的逐漸可行，手機上不斷推陳出新的應用程式與各式各樣的APP也成為居家聯網應用的驅動引擎[2][3]。

雖然透過智慧型手機，居家連網的概念變得明確可行，同時也有愈來愈多的消費性電子產品也開始加入聯網家電的行列，但由於聯網家電的應用還在起步，除了極少數的聯網家電外，大部份的傳統家電仍然不具有網路連線功能；此外家庭設備的電腦自動化控制或是居家連網有時也需要配合建築物或是電器產品進行事先的規劃與設計，消費者因此無法感受到家電聯網帶來的好處。

為了提供使用者更好的智慧生活體驗，本篇論文品利用智慧型手機的GPS/藍牙/Wi-Fi功能提供省電控制的適地性服務，當使用者外出時，系統會逐步關閉沒有在使用的家電，當時用者返回時，則分級開啟可能會使用的電器用品，使用者也可以利用預先排程的方式調整電器產品的使用方式，因此控制系統會跟據使用者行為決定是否應該開啟或關閉家電，使得智慧生活與節能省電的目標更容易達成。

本篇論文的組織架構如下：第二節介紹相關Android與Arduino相關背景知識及應用，第三節介紹整體系統架構與功能模組設計，並說明整體系統的運作方式，第四節介紹系統操作介面與功能實測結果，第五節是結論。

2. 背景知識與相關應用

隨著智慧型手持式裝置性能的提升，允許使用者自行下載軟體做應用擴充，使其於近幾年在全球市場上迅速發展，配合上各家手機製造廠商

推出各具特色的客製化軟體與系統，現在智慧型手持裝置已普及於人們的生活當中，其功能已經可以完全取代 MP3、數位相機與 PDA，甚至能夠取代個人電腦處理特定的工作，讓使用者不管是瀏覽網頁或者收發電子郵件都不再需要透過特定的裝置便可完成工作。

作為目前市面上行動裝置主流的作業系統之一，Android 是一個以 Linux Kernel 為核心的開放式手持裝置作業系統，應用蹤跡遍佈智慧型手機、平板電腦、數位隨身聽等裝置平台，開放原始碼的授權方式使廠商與開發者不須負擔昂貴的授權費，降低開發時採購軟體的成本。Android 使用 Java 語言進行開發，但與一般 Java 程式不同的是，Android 使用是 Dalvik 虛擬機器(Dalvik virtual machine, Dalvik VM)，並非以往的 Java 虛擬機器(Java virtual machine, JVM)。此外 Android 擁有齊全的開發套件、模擬器、SDK 與官方開發文件，程式開發人員可以利用下載的方式免費取得，降低開發時的技術成本與時間。

Android 系統具有完整的硬體支援，如觸控螢幕、Wi-Fi、藍牙、NFC、GPS、陀螺儀、重力加速度感測器(G-Sensor)等，加上無線網路的技術蓬勃發展，並搭配上特定的 App 即可實現多元化的功能。因此智慧型手機除了可以上網瀏覽網頁或收 E-mail 外，也可以利用 GPS 定位結合 Google 地圖提供使用者地域性的服務，根據使用者的地理位置與個人化的設定提供比傳統網路服務更具智慧的使用者體驗情境服務，國際研究調查機構 Gartner 認為一個成功的 App 必須專門為行動環境量身打造，並預測 2012 年十大行動應用趨勢時，使用個人化的地理位置服務(LBS)的人數將達到 14 億以上，目前各大手機廠商皆提供豐富且完整的相關地圖資訊與定位服務[4]。

Arduino 是一個開源的微控制器板，其特色是開放源碼與公開的硬體電路設計圖，開發者可從網路下載免費開發軟體的 IDE，使用類似 C 語言的程式語言進行開發，特色在於簡單明瞭的程式架構，只要有基礎的程式、電子電路的概念即可輕鬆上手。基於開放的硬體，Arduino 的電路設計圖可從網路上下載，因此廠商與設計者可以根據電路設計圖設計出各類自製版本的 Arduino，如 Motoduino、Seeeduino 或 Roboduino。另外 Arduino 擁有許多符合特殊功能的擴充板，如感測器擴充板、麵包板擴充板、馬達擴充板與 Wi-Fi 擴充板，只需要將擴充板堆疊上去，再配合相關的函式庫即可使用，節省繪製電路圖與撰寫相關程式的時間。

目前已有利用網頁或手機 App 程式操控智慧家電系統，實現遠端智慧型家電控制，但系統的運作無法配合使用者的生活作息判斷使用者的地理位置進行條件式的智慧控制，因此無法有效的利用能源達到省電的效果。本篇論文利用手機 GPS 定位加上利用 Arduino 微控板與無線傳輸模組實現智慧家電控制，並將系統模組化，便於使用者安裝建置，降低使用者安裝與使用上的負擔。

3. 系統架構與功能模組設計

為了能夠即時控制電源狀態，本文建構一套 Android 手持式行動裝置為平台的 APP 系統，搭配無線網路環境下達指令給 Arduino 板控制電源插座的狀態，並使用資料庫紀錄系統狀態，用於整體系統的同步與資訊更新，避免系統各裝置狀態混亂而發生錯誤的情況。使用者可以自行設定專屬的情境模式，其中分別利用 GPS 定位資訊與時間定時作為判斷依據。GPS 情境判斷是利用使用者手持裝置的 GPS 與一個預先設定好的固定 GPS 位址，配合一定的公式運算藉此作距離判斷，當條件成立時微型伺服器便會依照使用者設定的情境設定作電源插座的狀態改變；定時控制則是使用者自行設定該情境模式啟動或關閉的時間，配合以上控制與判斷方式構成一個完整的系統。

3.1 系統架構

本文實作之系統架構由智慧型手機、微型伺服器、資料庫與 Arduino 微控板四個功能模組所組成。使用者可利用智慧型手機做相關設定或下達指令，微型伺服器則依據使用者的設定對 Arduino 微控板上的繼電器模組進行控制。目前可以使用的情境控制功能有兩種，一為定時控制，二為與定位控制，使用者可以使用上述兩方法設定電器的運作方式。

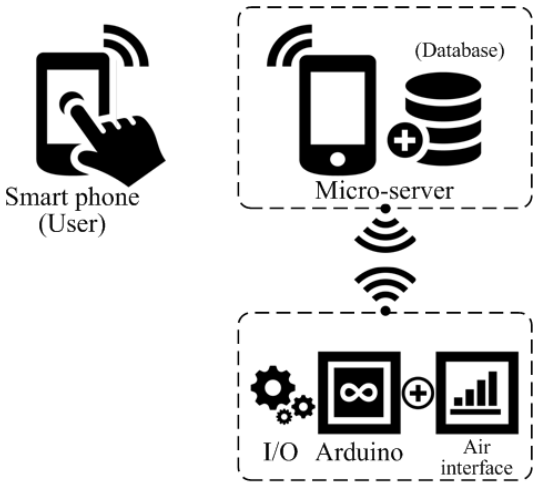


圖 1 系統架構

圖 1 中的微型伺服器是由智慧型手機與資料庫系統結合而成，其中資料庫可內建於智慧型手機或是設置於區域網路中；在這個系統中，資

料庫系統最主要的功能是紀錄系統狀態，提供資訊或推送參數給 Arduino 微控介面。當其接收到來自微型伺服器的指令時，Arduino 微控介面會解析指令內容，並送出指令改變腳位(Pin)狀態，進而觸發繼電器的運作而達到控制電器的目的，其電路示意圖如圖 2 所示：

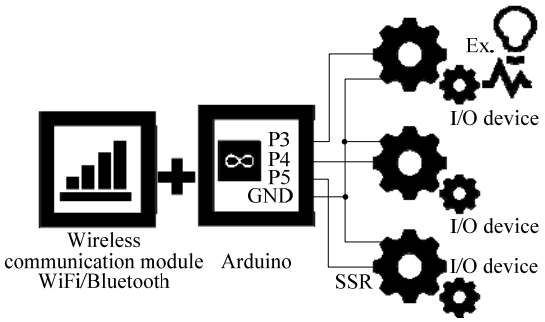


圖 2 Arduino 週邊簡易電路圖

3.2 定時控制功能

使用者開啟定時控制功能時，可以將時間作為情境設定條件，微型伺服器便會啟動定時功能，解析是否開啟電器裝置的控制條件。使用者可以進一步設定家電裝置的運作時間與運作方法，微型伺服器會依據設定的條件對 Arduino 控制介面的腳位進行定時控制；為了保持操作上的彈性，提供更佳的使用者體驗，使用者也可以利用網路對周邊裝置進行即時性的遠端遙控。定時控制的情境示意圖如圖 3 所示。

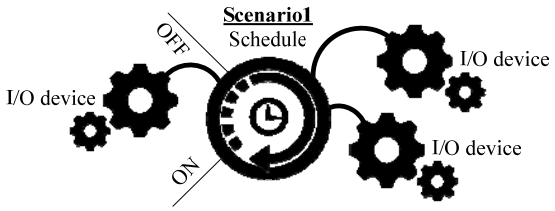


圖 3 情境 1：以排程的方法控制週邊電器的運作時間

3.3 定位控制功能

定位控制功能使用的是兩組 GPS 參數，微型伺服器配合特定的演算法計算出兩點距離後判斷是否改變 Arduino 腳位的狀態，使用定位控制功能時，微型伺服器會定時讀取使用者的智慧型手機所回傳之定位資訊，並以此資訊作為控制周邊 I/O 裝置之依據；這項功能主要是用在無法事先預知時間或是突發性、臨時發生的情境用，例如，使用者下班返回家中，或是臨時外出購物等，透過定位控制功能，使用者可設定外出即關閉客廳電燈或是在返家途中即開啟除濕機或空調設施等電器設備，使情境控制的功能更具備人性化。

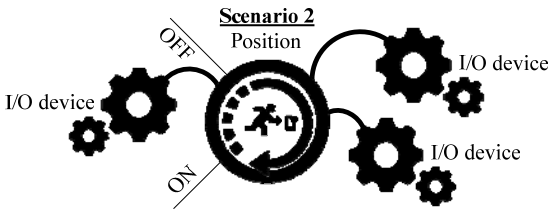


圖 4 情境 2：利用定位資訊作為開啟/關閉電器之依據

圖 4 為利用定位資訊作為開啟/關閉電器依據的情境示意圖；當使用定位情模式時，微型伺服器會將指定的固定位置(例如使用者的家)與使用者隨意移動的 GPS 定位資訊做計算與比較，並依據使用者的設定執行家電控制之動作，其資訊格式如表 1 所示：

表 1. GPS 資訊資料表欄位示意表

Position	經度	緯度
Fixed	XX.XX	XX.XX
Mobile	XX.XX	XX.XX

使用者可以設定啟動定位控制之距離範圍，其計算公式如下，其中 *Lat1* 表示起始點經緯度，*Lat2* 表示目的地經緯度，*a*、*b* 分別代表兩點之緯度差與經度差：

$$S = 2\arcsin\sqrt{\sin^2\frac{a}{2} + \cos(Lat1)\times\cos(Lat2)\times\sin^2\frac{b}{2}}\times 6378.137$$

3.4 微型伺服器的狀態更新與控制

為確保系統中各裝置的狀態一致，避免系統中的裝置狀態不一致而造成系統的混亂，使用者利用 APP 對系統下達命令與設定時，並不是直接對微型伺服器下達指令，而是先將設定參數推送至資料庫中，接著才由發微型伺服器將資料庫中的參數值取出解析後進行狀態更新，最後才將指令透過網路傳送到 Arduino 微控板對其 I/O 裝置進行控制。

如先前所述，使用者可以選擇使用定時功能或是定位功能透過微型伺服器對 Arduino 微控 I/O 裝置進行設定，微型伺服器會定期更新系統狀態，撈取資料庫的系統狀態及參數，解析後執行相對應的工作。Port 的狀態資訊如表 2 所示：

表 2. Port 狀態資料表欄位表(示意圖)

Device	Status	Watt	Port
Light1	ON	--	1

Light2	ON	--	2
Charger	OFF	--	3

4. 操作介面與功能實測

本章介紹系統操作介面與實測結果。由於微型伺服器和使用者的都是利用同一個 App 進行控制，因此第一次啟動時，App 會要求使用者進行行動運算裝置的模式設定，設定畫面如圖 5 所示：

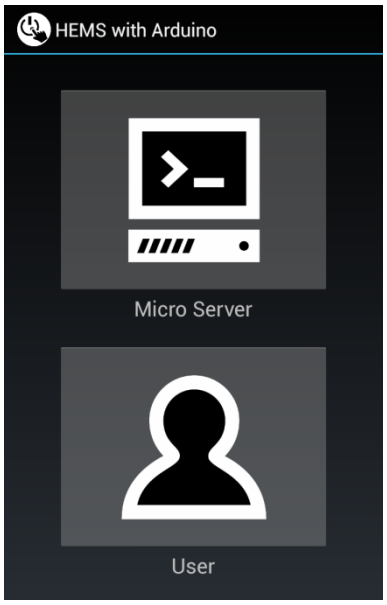


圖 5 裝置選擇頁面

若將行動運算裝置的運行模式設為「微型伺服器(Micro Server)」的話，App 就會常駐在系統中，進行控制周邊裝置、擷取資料與分析資料等工作；因此只有在將行動運算裝置作為微型伺服器使用時，才會選擇此一模式，一般情況下，App 的運行模式預設為「使用者(User)」模式。

4.1 使用者模式之設定

若將 App 的運行模式設為「User」，第一次使用時，App 會要求使用者指定一個固定經緯度(地點)，作為和微型伺服器之間計算定位距離的依據，在操作時，使用者可以直接在 Google Map 用手指直接點選自家或者公司位置，完成後點選返回功能鍵便可儲存指定的經緯度，完成定位設定，畫面如圖 6 所示：



圖 6 指定固定位置

如圖 7 所示，完成定位後，App 的畫面便會顯示裝置控制頁面，此頁面右上角有三個功能按鈕，分別為(1)新增裝置、(2)設定固定位置以及(3)情境管理設定。此時 App 會立即更新頁面上的資訊並顯示各電源的狀況、耗費瓦數與使用的插座編號，電源狀態以字體明暗表示，白色字體的欄位表示該裝置之狀態為開啟，灰色字體則為關閉，使用者可直接點擊畫面欄位對電源狀態進行控制。

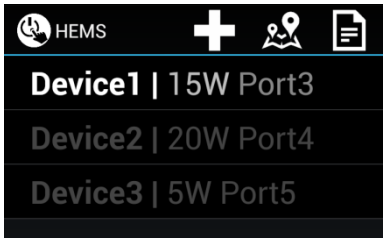


圖 7 裝置控制介面(含狀態)

如圖 8 所示，若使用者點選新增裝置，App 便會跳出編輯對話框，要求輸入新加入之裝置名稱、耗電量(瓦數)與電器連接點，使用者可以編輯該裝置標籤之相關資訊，以作為設定定時排程或定位功能時的參考依據：

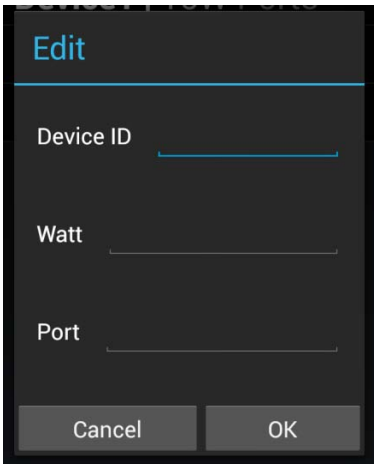


圖 8 新增裝置之畫面

如圖 7 所示，當使用者以"長按"的方式點選標籤欄位時，App 便會跳出一個可以編輯該欄位的對話視窗(請參見圖 9)，此時使用者可以選擇編輯或是刪除該欄位之相關資訊。

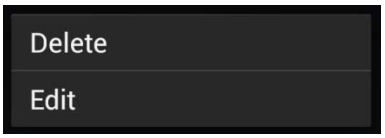


圖 9 編輯與刪除

情境設定頁面可提供使用者個人化的情境設定方式，其功能可分為定時設定與定位設定兩種；如圖 10 所示，使用者可以在操作介面中進行新增、編輯或刪除之設定，當設定之情境被啟動時，事件欄位會以比較顯眼的白色字體顯示，灰色則代表關閉狀態，使用者可點選右上角之按鈕進行使用情境之新增：

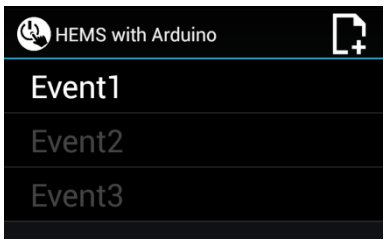


圖 10 情境管理欄位介面

如圖 11 所示，新增一個使用情境時後，使用者就可以對指定的周邊裝置進行設定，若使用者選用定時功能時，微型伺服器會依據參數之設定值，在指定的時間內對周邊裝置進行開關控制，並更新儲存在資料庫中的系統狀態；若未選擇啟動定時設定，則 App 預設會使用定位控制功能，同時微型伺服器會定期到資料庫中讀取使用者所在的隨意位置，並與指定的固定位置進行比較、分析與控制運算。

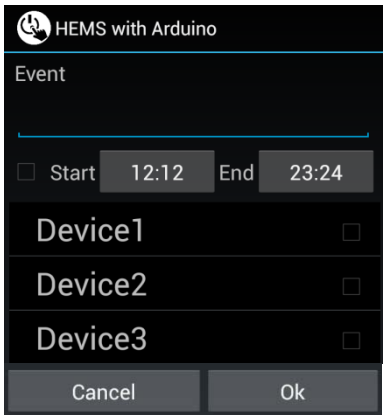


圖 11 情境模式編輯介面

4.2 微型伺服器模式之設定

若將手機的用途作為微型伺服器使用者時，在開始運作前，App 會要求輸入 Arduino 微控板的 IP 位址，以便對透過 Arduino 微控板對周邊 I/O 裝置下達控制指令，操作介面如圖 12 所示：

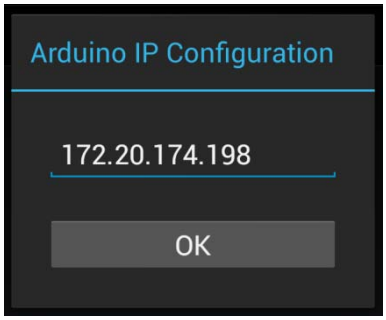


圖 12 微型伺服器 IP 位址之設定畫面

微型伺服器的主要工作是解析資料庫之各項參數資料，並作相對應的判斷與控制，再下達指令給 Arduino 微控板對周邊電路開關(例如固態繼電器)進行控制，由於微型伺服器最主要的功能為監控系統狀態並執行使用者設定之指令，因此微型伺服器的介面僅提供各裝置的運作狀態，而不提供操作與設定介面，微型伺服器各裝置狀態介面如圖 13 所示。

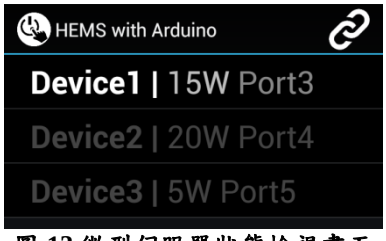


圖 13 微型伺服器狀態檢視畫面

圖 14 為實作之電源控制模組，其包含 Arduino 微控板、12V 電源供應器、繼電器模組板與一組埋入式插座，圖 15 為實作之 Arduino

微控模組，此模組包含 Arduino 微控介面以及一個 Wi-Fi 無線網路通訊介面；兩者串接後，微型伺服器便可透過此微控模組對週邊設備下達指令，當 Arduino 接收到指令時，透過改變腳位的電位狀態控制繼電器的運作，當繼電器為開路狀態時，便能控制電器的電源，達到電器設備控制之目的。

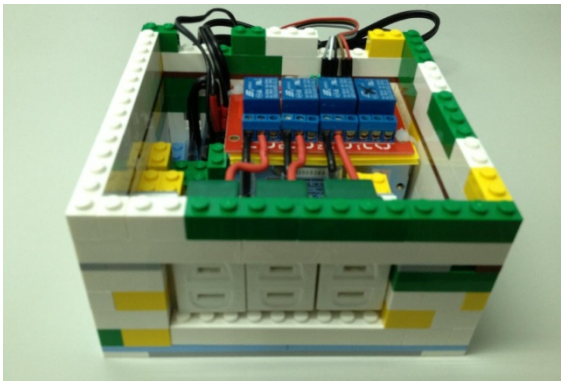


圖 14 電源控制模組

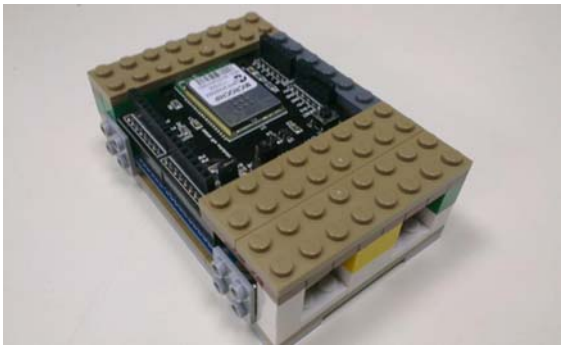


圖 15 Arduino 微控模組

5. 結論

以往的智慧家電控制目前的智慧手機都具有優異的運算能力，能夠完全替代 MP3、數位相機與 PDA，取代個人電腦執行大部分的事物，並支援 GPS、Wi-Fi、Bluetooth 等無線無通訊功能。因此本篇論文品利用手持式行動裝置作為家中的微型伺服器，使用智慧型手機將數據透過無線網路推送給微型伺服器，微型伺服器將訊息解析運算後依據使用者的設定對 Arduino 微控板下達指令，因此當使用者進入/離開系統當中設定的區域範圍或到達指定時段時，便會觸發情境模式透過繼電器控制插座電源的狀態，達到人性化的智慧型控制效果。

參考文獻

[1] 程榮祥, 洪偉峻, 林家鵬,在 Android 上以電話聯絡資料為基礎實作具備資訊分級功能的朋友定位器,2013 Conference on Information Technology and Applications in Outlying Islands (ITAOI'13), Quemoy, Taiwan, May 24-26, 2013.

[2] 徐椿樑, 許藤耀, 吳維彬, 鄭金林, 以嵌入式系統實現 3C 智慧家電, Conference on Information Technology and Applications in Outlying Islands (ITAOI'09), May 22-24, 2009.

[3] 石貴平, 李俊志, 洪可珈, 李竑豫, 陳功傑, 陳耀峰, 以物聯網促進生活便利性-以智慧型冰箱為例, Taiwan Academic Network Conference (TANET2012), Taoyuan, Taiwan, Oct. 23-25, 2012.

[4] Rung-Shiang Cheng, Chun-Yu Ke, Chung-Ying Tsai, and Chien-Jen Wang ,"A Mobile Homecare Application Combining with Alarm Clock and GPS Positioning Function", CCIS 223 (SUComS 2011), Springer, ISBN: 978-3-642-23948-9, Sep, 2011 (EI).

雲端同步通訊錄與防詐騙系統

廖子萱　李貞穆　劉名皓　盧聖軒　方文聘*
元培科技大學
*wpfang@mail.ypu.edu.tw

摘要

本文提出一種可以避免詐騙和提高撥號效率之整合型方法，利用智慧型手機與雲端儲存之特性，可以讓多人同步使用通訊錄、過濾非法來電與設計一件人性化快速撥分機號碼的方法，並且解決不同公司手機自動撥分機號碼符號不統一的問題，並示範所設計系統。
關鍵詞：智慧型手機、速撥、詐騙、雲端。

Abstract

This paper proposed a system to prevent cheat and reduce the time to dial telephone especially with ext. The contact list is store in cloud, users can update the latest version anytime if he connect to internet.
Keywords: smart phone, rapid dial, cheat, cloud.

1. 前言

隨著時代變遷，人類的通訊方式也不斷演變，早期電話皆為室內型且無內建通訊錄功能，為了便利性，人們通訊方式逐漸演變到手機時代，但手機通訊錄僅能記錄於SIM卡或手機裡，一旦手機或卡片損毀便失去通訊錄，因此演變至今的智慧型手機成為趨勢，智慧型手機可結合網路將通訊錄儲存於雲端。此外撥打市話時，如果為語音總機接聽，往往要聽一連串的語音說明分機號碼，且需另外按下分機號碼才有辦法接通到目的電話，所拖延時間皆為使用者付費，損失了寶貴的時間與金錢。

據內政部警政署[1]統計165反詐騙專線自93年4月26日成立至102年4月底止，共接獲民眾進線511萬餘通電話，數據顯示出龐大的詐騙電話數量，盡管有反詐騙電話可詢問，但接聽專員可能忙線造成無法接聽問題，新聞[2]就指出民眾撥打反詐騙電話專員未接聽問題。

綜合上述兩原因，本論文以元培科技大學為例提出應用程式具備一鍵撥打分機功能，簡化撥打分機等待時間與麻煩程度，同時具備判斷來電號碼是否為詐騙電話之功能，本論文其他部分包括第二段市面現有產品分析，第三段說明提出方法，第四段展示實驗結果，第五段討論與結論。

2. 市面現有產品分析

目前市面上通訊錄軟體資料分別為基本功能與較特別功能，本段分別討論之。

2.1 市面通訊錄基本功能

市面上通訊錄軟體其基本功能較主要的為以下以幾種舉例，便利通訊錄 APP [3]自動分組和自定義分組、各群組顯示圖標、通訊錄顏色、人名顏色更換，並可選擇聯繫人資料顯示完整度，例如、只顯示姓名、電話，或者要多顯示信箱、地址…等等，DW 聯繫人&撥號 APP(此為 App Store 常見應用程式)[4]批量傳送簡訊、最近通話、通過聯絡人姓氏尋找電話號碼、設定聯絡人來電鈴聲。

2.2 市面通訊錄特別功能

市面上通訊錄軟體其特別功能為以下舉例，DW 聯繫人&撥號 APP[4]語音搜索聯絡人任何屬性、來電防火牆（可自由的定義需要攔截的時間，星期）、撥號鍵盤的大小、背景、顏色和字體大小調整、智能刪除相同聯絡人判斷姓名與電話，同時工作在多選擇模式，來電防火牆（可自由的定義需要攔截的時間，星期），雲端通訊錄[5]將個人黑名單上傳至雲端與所有用戶共享。

3. 提出方法

本論文提出快速撥打分機號碼且能辨識詐騙電話的方法，主要分為系統架構、我的最愛、詐騙辨識三個流程，其中系統架構主要為資料更新後解析 XML 檔並更新至資料庫與透過資料庫以至動態產生分機表，我的最愛則可將常用的分機號碼存入以便快速使用，最後詐騙辨識則可幫助使用者在詐騙電話來電時自動掛斷以防止受騙。

3.1 XML 架構

透過 XML 的架構來製作資料檔以便快速有效率的進行分析並寫入資料庫，以下表 I 為 XML 範例，如圖 1 所示，透過階層的方式從根元素 RandDdiv 找到元素 Stuff，再從元素 Stuff 找到子元素 ID 和子元素 NUM 來取得值後存入資料庫中。

表 1 XML 範例[6]

```
<RandDdiv>
<Stuff>
      <ID>國際事務處</ID>
      <NUM>國際長/黃曉令 2401</NUM>
</Stuff>
<Stuff>
      <ID>教務處</ID>
      <NUM>教務長/駱詩富 2210</NUM>
</Stuff>
<Stuff>
      <ID>教務處</ID>
      <NUM>葉千翡 2211</NUM>
</Stuff>
<Stuff>
      <ID>教務處</ID>
      <NUM>傳真機 2209</NUM>
</Stuff>
</RandDdiv>
```

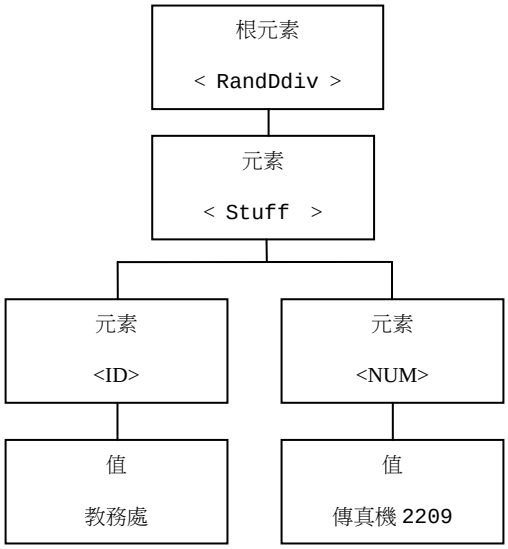


圖 1 XML 格式

3.2 搜尋樹設計

當二元樹的左子樹上所有節點的值均小於根節點以及右子樹上所有節點的值均大於根節點即為二元搜尋樹，它的時間複雜度最差為 O(n)、最佳為 O(logn) ，本文所使用的是十元樹來進行詐騙電話辨識，將詐騙電話切割成各個數字設為節點，時間複雜度為 O(logn)。

3.3 系統架構

系統架構如圖 2 所示，主要分為詐騙辨識、速撥以及我的最愛，詐騙辨識又分為撥號與來電辨識、速撥分為單位和連絡人，我的最愛又分為新增與刪除。

系統流程如圖 3 所示，當程式啟動時會先檢查是否連接網入，有連接的話則檢查分機與詐騙電話是否有更新，若有更新會將更新的資料寫入資料庫，最後透過資料庫來進行詐騙辨識、產生速撥表以及我的最愛。

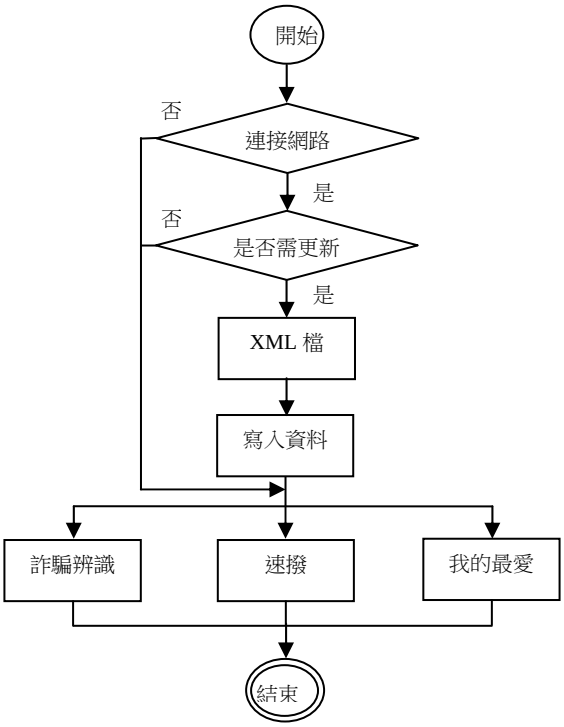


圖 3 系統流程圖

3.4 系統模組

模組分為我的最愛及詐騙辨識兩個，我的最愛模組如圖四所示，主要能進行新增與刪除連絡人。而詐騙辨識則如圖五所示，當有來電或者在撥打電話時會以電話號碼的各個數字透過十元樹來偵測是否為詐騙電話，如果是的話則將電話掛斷並由訊息框提出警示。圖六為假設將 0912345678、0932765430、0932765432、0932765434、0932765436、0932765438 等六個號碼設為詐騙電話所生成的十元樹。

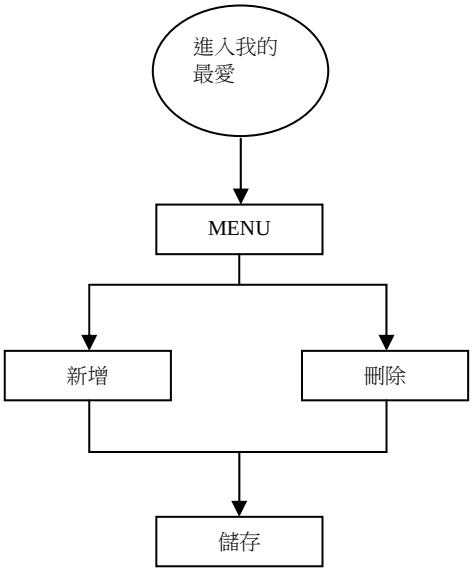


圖 4 我的最愛狀態圖

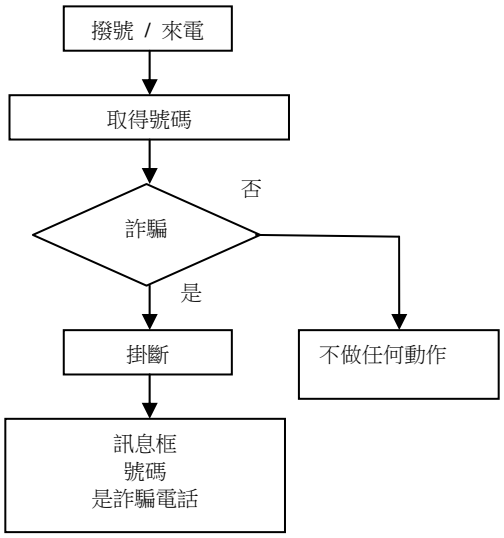


圖 5 詐騙辨識流程圖

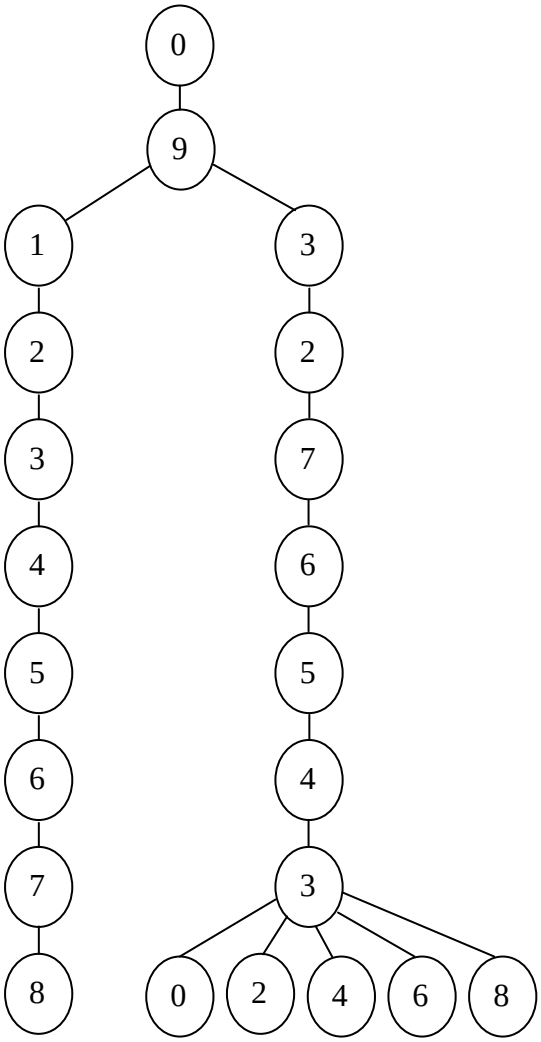


圖 6 詐騙電話轉十元樹

4. 實驗結果

實驗以元培科技大學為例，確定不必按下分機碼，直接選擇電話即可撥打分機，而詐騙電話經測試也能有效攔截，測試結果如圖七所示，(a)選擇元培科技大學各處室電話畫面 、(b)選擇各處室人員分機電話、 (c)功能表，選擇線上更新分機號碼與反詐騙資料、加入自己喜歡或者常用電話到我的最愛以利快速撥號、 (d)更新結果圖(已經是最新版本結果)、(e)我的最愛分機列表可進行新增與刪除、 (f)為詐騙電話來電提示。



(a)



(b)



(c)



(d)



(e) (f)

圖 7 實驗結果圖(a)分機類別圖 (b)人員分機表 (c)功能區 (d)更新結果圖(已經是最新版本結果) (e)我的最愛 (f)詐騙來電提示

5. 結論與討論

本論文提出一鍵撥打分機之方法，為市面上通訊錄軟體所沒有的，經實驗測試確定可以有效節省查詢分機號碼或者輸入分機時間，以元培科技大學總機為例，從聽完提示音所需的時間為 40 秒之後再輸入分機號碼到轉接完畢的平均時間為 50.6505 秒，但用一鍵撥打分機的話全程只需要 12 秒。

此外本論文提出防詐騙功能，詐騙電話資料來源為內政部警政署[1]所公布之資料，有別於[5]使用者黑名單功能，使用者上傳黑名單分享給其他使用者，有非詐騙集團卻被設成黑名單可能性，本論文所提出資料為官方正確資料具有公信力，不會有誤判可能性，最後本論文功能與目前市面最流行的 LINE 進行比較[7]-[8]，得到結果如表 III 所示，本文所提出三點通訊錄特色相較於 LINE 之特色皆優化或者較佳。

表 2 一般撥打分機時間表

第一次時間	50.584 秒
第二次時間	51.070 秒
第三次時間	51.375 秒
第四次時間	49.955 秒
第五次時間	50.124 秒
第六次時間	51.073 秒
第七次時間	50.824 秒
第八次時間	50.503 秒
第九次時間	50.329 秒
第十次時間	50.668 秒
平均時間	50.6505 秒

參考文獻

[1] http://www.165.gov.tw/work_stat.aspx, “內政部警政署反詐騙網”
[2] http://www.tvbs.com.tw/news/news_list.asp?no=blue20060118134957, “TVBS-N 新聞網”
[3] https://itunes.apple.com/cn/app/bian-li-tong-xun-lu-pro/id464538313?mt=8, “便利通訊錄APP”
[4] https://play.google.com/store/apps/details?id=com.dw.contacts.free, “DW 聯繫人&撥號APP”
[5] http://apk.91.com/Soft/Android/com.witmob.cloud_contacts-1.html, “雲端通訊錄APP”
[6] http://rritw.com/w3school/xml/xml_tree.html, “w3school”
[7] http://line.naver.jp/zh-hant/, “LINE官方網站”
[8] http://iapp.com.tw/2012/08/line-update-line-coin-and-my-favorites/, ”LINE最新功能介紹”
[9] 劉傳銘，資料結構與演算法：使用JAVA(第四版)，2007。
[10] 李信賢，常態模型轉折點之二元樹搜尋法，2004。
[11] 陳嬿如，二元樹之間的旋轉距離，2010。

基於智慧手機的室內 PDR 定位系統模組化快速開發平台

林恭煥　石佳雯　許雅婷　簡嘉瑩　廖峻鋒
逢甲大學資訊工程系
{m0103411, d9917112, d9971158, d9970555, cfliao}@fcu.edu.tw

摘要

航位推算 (Pedestrian Dead Reckoning, PDR) 是一 種不需額外基礎設施的定位技術,利用少數感測器, 在適當調校下即可達成不錯的精準度, 因此近年來有 許多以 PDR 技術為基礎的室內定位系統被提出。然 而,在實務上,建構精準的 PDR 定位系統過程相當 繁瑣,必須考量應用服務特色、使用環境及對象,不 斷嘗試各式演算法並調整參數。有鑒於此,本研究從 軟體工程的角度出發,提出一個基於智慧手機的室內 PDR 定位系統開發平台,將 PDR 室內定位系統中的 不同演算法與參數模組化,使研究人員可在開發過程 中藉由組裝、建構與測試各種演算法, 快速建構適用 於特定場合的定位機制。本論文同時也藉由一個實際 案例,說明如何透過此平台逐步改善定位系統的精準 度,經由案例討論,我們發現此一平台藉由彈性模組 組合及提供預設模組實作成品的方式,可有效降低研究人員於開發過程的負擔。

關鍵詞 室內定位系[1]統、手機定位、航位推算

1 前言

室內定位系統在智慧生活空間應用服務扮演不可 或缺的角色,在空間中,智慧生活空間應用服務需要得知使用者當前位置,才能給予最適當的服務。以居家健康照護為例,獨自生活的老人大都有行動不便的問題,當得知老人走到危險易滑倒區域時,會發 出輕柔語音提醒其留意步伐; 或是老人半夜如廁時, 貼心地延著路徑自動開啟照明設備等,都必須正確 得知使用者位置。因此,位置資訊在情境感知計算 (Context-Aware Computing) 領域被列為第一級重要 情境 (Primary Contexts) 資訊 [1]。

目前室外定位技術主要以 GPS 及 Wi-Fi 為主,此類系統準度約 10 公尺左右,在旅遊、尋找地標位置等大範圍服務有不錯的應用成效,不過此一精準度不足以滿足室內定位應用需求,例如在室內透過 GPS 定位 誤差往往過大,連使用者位於那個房間都難以正確判斷。一般住家及市區 Wi-Fi 基地台相當普及,因此也 有相當多研究是透過分析 Wi-Fi 訊號來定位,然而, 這種方法最大的問題是訊號源容易受到環境因素 (如 室內裝潢材質、溫濕度、風速風向) 的影響,當導致訊 號強度消減、不穩定、反射或折射時,精準度就大受 影響。此外,Wi-Fi 為主的室內定位需在附近有數個 Wi-Fi 基地台做為基礎設施,因此無法在特定場所使 用,例如對無線基地台有所限制的醫院或地點偏遠的 老人長照中心 [2]。最後,此類定位系統使用前必須進 行訊號觀測記錄動作 (site survey),此記錄的品質對 定位效果有重大影響。但一般未經訓練的使用者很難 做出良好的訊號觀測記錄 [3]。透過類似原理,其它也 有以無線感測網路的節點來進行室內定位 (如 Zigbee 等) 的機制 [4],這些設備除了建構額外基礎設施外, 無線感測設備還需要定期更換電池,這種維護工作非 常辛苦且耗費力。另外,也有利用紅外線陣列的定 位方法 [5],使用者於身上配戴紅外線發送器,與事先 安裝好的紅外線接收器一同運作。但其傳輸距離範圍 極短 (少於 5 公尺),且訊號極易受環境影響。

近年來,智慧手機已深入人們的生活,成為隨身攜 帶的配備,再加上電子技術的進展,各式感測器的 成本降低,大部份智慧手機均內建三軸加速計 (Ac- celerometer) 及方向感應器 (Orientation sensor),使 智慧手機成為理想的感測平台。因此,有許多研究人 員嘗試結合手機,在室內使用航位推算 (Pedestrian Dead Reckoning, PDR) 技術進行定位。首先,利用手 機上的三軸加速計及方向感應器計算出使用者的移動 距離與步數,再利用方向感測器得知使用者當前移動 的方向,再計算出移動的軌跡,並推算相對於出發點 的座標。

目前在學術上有關 PDR 定位系統的研究很多,這些系統雖然採用了不同的感測器及演算法,在 設計結構上卻都有十分類似之處 (如圖 1),我們將在 下一節詳細說明此一結構。相較於其它室內定位機制, PDR 最大的優勢在於不需事先佈署基礎設施,也不需 事先進行訊號觀測記錄工作,因此不易受環境影響, 定位品質穩定,且成本低廉 [6, 7]。然而,近年來也 有學者指出,大部份 PDR 定位機制研究為了學術貢 獻,往往將機制設計得過於複雜,使得實作困難,且 目前仍缺乏對此類定位機制實作挑戰的探討, 造成實 務上該類系統難以開發 [8]。在 PDR 定位系統開發期間,針對特定應用服務與特定環境嘗試不同演算法是 很常見的,但是開發過程中,若發現效果不好要更換 演算法,就必須重新改寫整個系統,因此在實務上開 發 PDR 定位系統所付出的成本經常居高不下。造成實務上該類系統難以開發 [8]。在 PDR 定位系統開發期間,針對特定應用服務與特定環境嘗試不同演算法是 很常見的,但是開發過程中,若發現效果不好要更換 演算法,就必須重新改寫整個系統,因此在實務上開 發 PDR 定位系統所付出的成本經常居高不下。

* 本論文接受教育部 102 年度資訊軟體人才培育推廣計畫與國科會研究計畫編號 102-2221-E-035-039 與 102-2627-E-002-001 經費補助。

針對此一觀察,本研究應用物件導向軟體設計技術,發展一套可使得研究人員快速開發低成本 PDR 室內定位機制的開發平台。此開發平台將 PDR 各資料處 理階段設計為具有相同輸出入介面的獨立模組,並提 供預先實作的各式常用演算法模組 (參考表 1),這些 模組可以在平台支援下,藉由 pipeline 或 workflow 般 的設計方式,以 Builder 設計樣式構成的簡單特定領 域語法 (Domain Specific Language, DSL) [9],自由組 合獨立模組來完成低成本的室內定位系統,使開發人 員可在定位機制設計階段,快速嘗試各種演算法模組 的組合,為其特定應用找到最好的搭配方式。

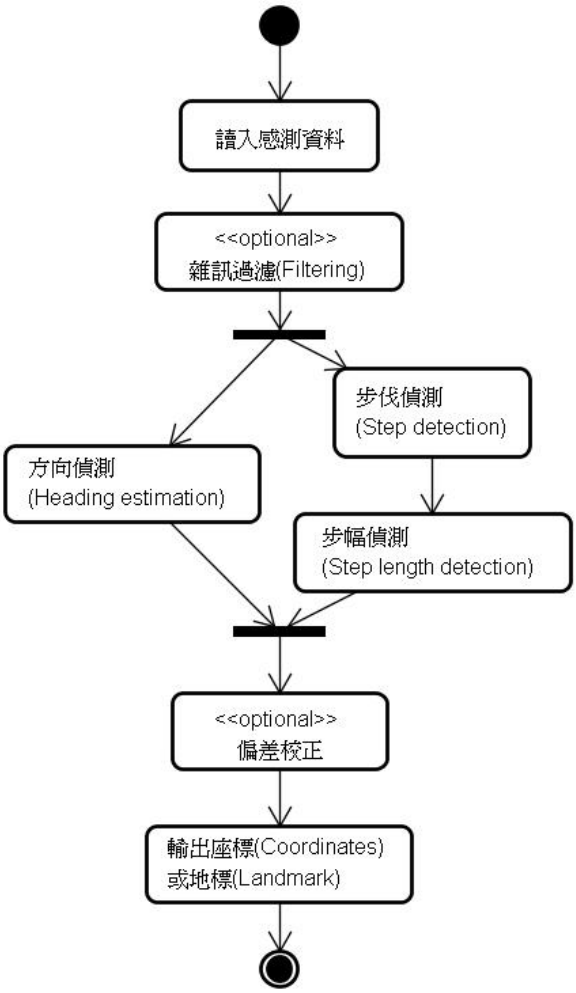


圖 1: PDR 室內定位系統資料處理步驟

2 研究背景

以智慧手機為基礎的 PDR 定位機制雖然採用的感 測器、演算法與精準度各有不同,但在設計上都有十 分類似之處。經過分析,PDR 定位系統共通的資料處 理流程可表示如圖 1的流程圖。首先,從感測器讀入 資料,接下來為增進後續辨識結果的穩定性,通常會引入各式雜訊過濾機制來對資料進行前處理,以求將 不正常的感測值去除。常被使用的方法包含 High pass 或 low pass filter [2] 及自動控制領域常用的 Kalman filter [10] 等。但並非所有 PDR 機制都具有此一步驟, 例如 Kang 等人提出的機制就沒有進行雜訊過濾 [3]。

接下來必須分別判讀人員的行走距離和行走方向,行走距離通常結合步數偵測 (Step Detection) 及步幅 偵測 (Step Length Detection)。步數偵測目前大部份 的研究都基於加速計讀值的趨勢來辨識步伐,例如 波動高峰偵測法 (Peak Detection) [11] 及波形急速下 降偵測法 (Sudden drop detection) [2],週期偵測法 (Zero-crossing detection) [12], 類神經網路 [13] 等。由 於加速計一般有 x、y、z 三個讀值,因此也有學者 認為應先整合為一個值再進行後續處理 (Synthetic acceleration) [3]。步幅偵測則包含了以加速度平均值 為主的 Kim 法 [14]、以加速度的振幅為主的 Weinberg 法 [15] 及以加速度值最大值、最小值以及平均值間關 聯的 Scarlet 法 [16]。此外,Shin 等人提出了根據步伐 頻率以及速度推估出來與步履長度的線性方程式的推 算步幅的方法 [7]。行走方向則和智慧手機平台有關, 有些透過加速計讀值與磁力計加以計算 [3],有些則直 接採用方位及手機姿態資訊。

最後,由於 PDR 定位機制具有誤差累積的問題 [2],因此可加入偏差校正措施,在適當時機將誤差縮小 [2, 10]。但如同雜訊過濾機制,並非所有 PDR 定位機 制都具有偏差校正模組。在取得一段時間的行走方向 與距離後,在平面上就形成一個有向性的線段,結合 多個線段即可形成人員位移的軌跡。圖 1 顯示了 PDR 定位系統的主要資訊處理流程及各個主要模組。根據 應用場合及所需解析度的不同,各個不同的 PDR 定 位系統在特定模組會採用不同的演算法。事實上許多 此類研究事實上只是針對各模組選取或提出適當的演 算法,再將之組成一個完整的定位系統。表 1 整理了 各重要模組常見的演算法。

表 1: PDR 室內定位系統主要步驟所使用的演算法

步驟	主要演算法
雜訊過濾 (Filtering)	High pass and low pass filter [2], Kalman filter [10]
步伐偵測 (Step detection)	Synthetic acceleration [3], Peak detection [11], Sudden drop detection [2], Zero-crossing detection[12], Neural network [13]
步幅偵測 (Step length detection)	Weiberg method [15], Scarlet method [16], Kim method [14], Linear combination [7]
方向偵測 (Heading estimation)	Direct reading, Kang method [3]
偏差校正 (Calibration)	GPS [10], Sequence alignment [2]

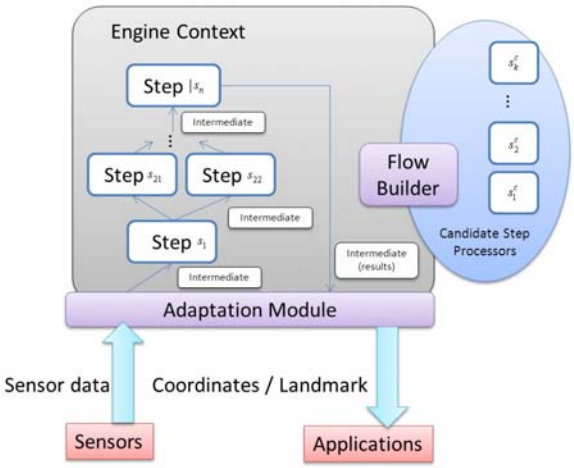


圖 2: 開發平台系統架構圖

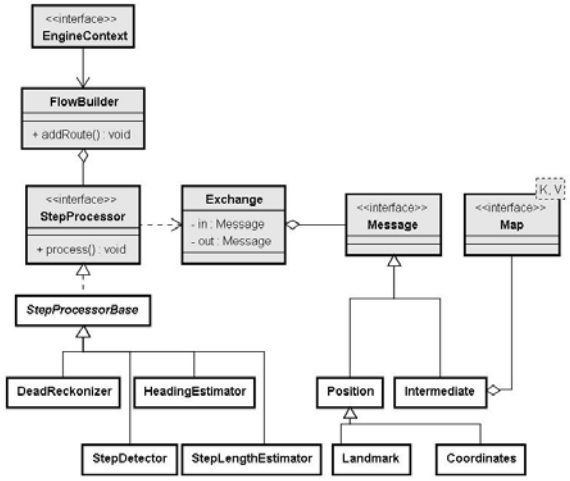


圖 3: 開發平台核心類別圖

3 平台系統架構與開發流程

本節將說明 PDR 室內定位系統快速模組化開發平 台的設計理念。如同第 2 節所述,室內 PDR 定位系 統雖然採用了不同的感測器及演算法模組,但資料處 理流程十分類似。以下我們首先將從軟體設計的角度, 分析此一開發平台的系統架構,接下來說明基於此一 平台的開發流程。

3.1 平台系統架構

本開發平台的系統架構如圖 2 所示,定位系統 從感測器中取得讀值後,透過轉換模組 (Adapta- tion module) 將讀值轉換為系統內部共通的格式 (稱為「中繼資料 (Intermediate)」)。考量中繼資料儲存結構的泛用性需求,我們將 Intermediate 定義 為聚合結構 (Aggregate) [17]。若令 p = (k,v) 為一 個鍵 -值組,則 P = {pj} 為鍵 -值組集合 (或稱 Map),且 Intermediate I = {Pi}。根據平台核心類 別圖 (圖 3),Intermediate 資料結構在實體上我們以 Set<Map<String,Object> > 來實作。

取得感測資訊並轉為 Intermediate 後,會經過多個 處理步驟單元 (Step Processors),每個 Step Processor 封裝了特定步驟的演算法,例如雜訊過濾、步伐偵測、 步幅偵測、方向偵測及偏差校正等步驟所包含的各個 演算法都可視為一個 Step Processor 加以模組化 (參 考圖 3)。將特定的 Step Processors 依照開發人員指 定的次序結合後,會成為「資料流 (Flow)」。每一個 由開發人員定義的 Flow 在本質上是一個擴充形式的 有向圖 F = (S, E, I),其中 F 代表資料流,也就是 定位系統的資料處理流程本身,S = (s1 , s2 , ..., sn) 是 處理步驟單元所形成的有序集合,而 E ⊆ S × S × I 是處理步驟單元的有向連結,且對所有的 e ∈ E 都 附屬一個特定格式的 Intermediate Ix 做為 sy 的輸 出或輸入介面。就直觀的意義來說,一個 Flow 就代 表了一個特定的定位系統。在定位系統執行時,Step Processor 會將輸入的 Intermediate 處理後,轉為另 一個 Intermediate 並加以輸出至下一步驟,到達最 後步驟之後,再透過轉換模組將 Intermediate 轉換 為應用程式 (Applications) 所需要定位資訊 (圖 3中 的 Position 類別),例如座標 (Coordinates) 或地標 (Landmark)。由於所有 Step Processors 都屬於同一 個介面 (StepProcessor),且輸出入都是 Intermediate, 因此開發人員可以基於 Builder 設計樣式構成的簡單 DSL 語法 (如圖 4) 自由組合 Step Processors 定義新 的定位系統。

```
EngineContext engine = new DefaultEngineContext();
engine.addFlow( new FlowBuilder(){
    public void configure() {
        from("direct:sensorGateway")
        .to(new SyntheticAccelerationDetector ())
        .parallel ().to(new WeibergStepLengthDetector(),
                        new MixMagnetGyroHeadingEstimator())
        .pdr(new CoordinatePositionResovler())
        .out("direct:myApplication");
    }
});
engine.start();
```

圖 4: 基於本平台開發的定位系統程式碼片段

此外,為了加快開發人員的開發速度,平台也提 供了預先實作好的 PDR 定位系統中各階段各式演算 法(請參考表 1) 的 Step Processor 模組,這些預先 提供的實作可預先在開發平台中登記成為候選處理步 驟單元(Candidate Step Processors),如果 Candidate Step Processors 不敷使用,開發人員也可以透過繼承 StepProcessorBase 類別,自訂新的 Candidate Step Processors。

這種架構最具彈性的地方是各式 Step Processors 可 以透過 Flow 的定義加以組裝,甚至可以表達平行處理的語意。原本開發 PDR 最耗時之處在於,在不同的資料處理階段 (請參考圖 1),根據應用程式特色,不 斷更換與測試各式演算法,而在此一開發平台上,只 要透過 Flow Builder 重新定義,開發人員可以快速測 試各種不同的組合。

3.2 開發流程

欲使用此一平台的開發人員,首先必須了解所要開發的定位系統要支援的應用服務需要的準確度,例如 需要正確的座標、需要軌跡、只需要地標,還是只要 知道有走幾步即可。事實上大部份智慧生活空間應用 服務不需要太高的精準度,例如自動照明、關燈,只 需正確辨識使用者在那個房間即可; 而健康照護用的 計步器,更只需透過步伐偵測模組得計算步數即可。 了解應用服務所需定位精準度,可以降低所使用模組 的數量,降低所需硬體成本,加快開發時間 (要達成 精準的定位必須重覆進行實驗與更換嘗式不同模組), 更可以降低軟體除錯的困難度。此外,若應用服務只 能依賴特定的硬體或作業系統版本,也必須事先列入 考量,例如可能會有某些智慧手機只不支援方向感測 器、或是一些作業系統上輸出的加速計不夠精準等狀況。

當服務精準度及軟硬體確定後,接下來可使用開 發平台依下列步驟進行開發:

表 2: 透過實測校正的方位感測讀值判斷表

讀值	判斷方位
337.5-360 或 0-22.5	北
22.5-67.5	東北
67.5-112.5	東
112.5-157.5	東南
157.5-202.5	南
202.5-247.5	西南
247.5-292.5	西
292.5-337.5	西北

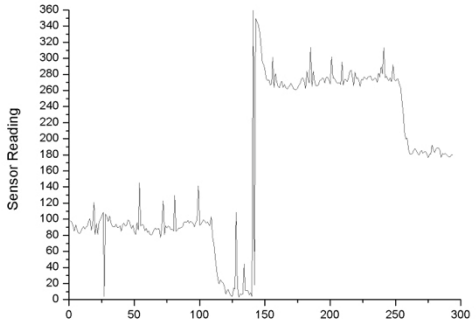


圖 5: 方向感測器實驗

1.初步考量與評估 PDR 的必要步驟,例如,若感 測器訊號輸入品質良好時,雜訊過濾與偏差校正 階段可以考慮先不實作。

2.針對每個 PDR 的必要步驟,初步選定「步伐偵 測、步幅偵測、方向偵測」的演算法模組。如果 所需要的演算法模組未提供,則必須自行透過寫 作 StepProcessorBase 的子類別實作。

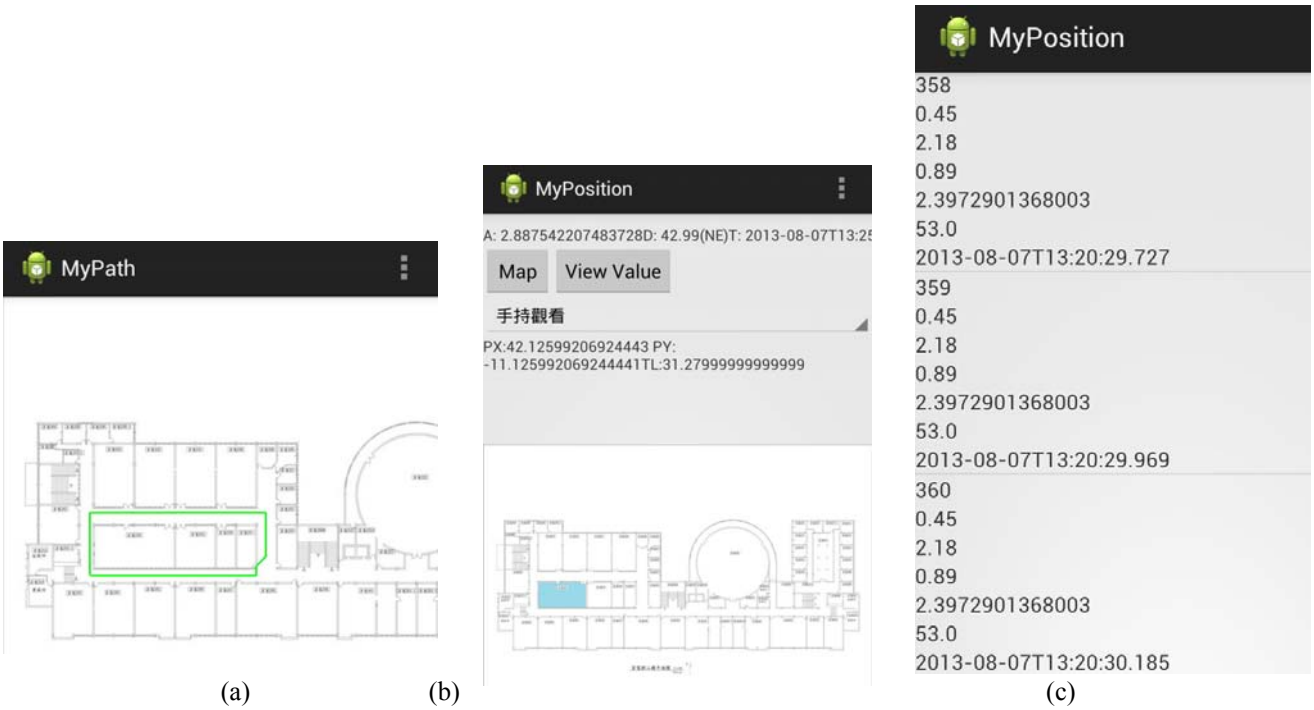
3.使用平台所提供 FlowBuilder 類別與 DSL,將選 定的演算法模組依所需要的次序建構為一 Flow。

4.編譯程式並佈署至手機,在需要佈署的空間中進 行實地步行測試。平台提供工具函式可將各階段 產生之資訊寫入手機上的本機資料庫。

5.根據資料庫計算定位準確度,若準確度達到理想 值則完成,否則回到步驟 2。

4 案例探討與實驗評估

為驗證平台設計,我們基於此平台實作了一個 PDR 定位系統初步雛型。以下將說明我們是如何基於此一 平台與開發流程,逐步改善此一 PDR 定位系統雛型。 本案例中,要開發的 PDR 定位系統將用於「影音如 影隨形」



(a) (b) (c)

圖 6: 基於本平台開啟之 PDR 定位系統雛型: (a) 軌跡模式; (b) 座標/地標並陳模式; (c)步行資料庫模式

應用服務,使用者在一個房間聽音樂或看影 片,當需要而移動到另外一個房間,也想聽到同一首 音樂或同一部影片,而且接著之前中斷的部份再繼續 播放。此一應用服務只需要地標 (Landmark) 層次的 解析度,定位精準需求約在 3 公尺以內。我們所使用 的開發硬體為 HTC One X 1.5Hz 四核心智慧型手機, 記憶體為 1G,儲存空間 16G,使用 Android 4.0.3。此 款手機上配備的感測器有陀螺儀、加速計、方向感測 器、環境光線感測器等。

初步評估,由於此應用服務需求的精準度不高,因 此我們選擇只實作步伐偵測、步幅偵測及方向偵測模 組。步伐偵測的演算法我們選用同時考慮三軸向加速 度的 Synthetic acceleration [3]。此方法主要的概念是 先從手機內的三軸加速計取得時刻 t 的 x、y、z 三軸的加速度值,再利用

$$a(t) = \sqrt{a_x^2 t + a_y^2 t + a_z^2 t} - g$$

計算一段時間內加速度的變化,利用 a(t) 的規律波動 週期計算步數。

步幅偵測部份則使用 Weiberg method [15]。其主要概念是取得 a(t) 波動週期的最大最小值,配合估算參數 η 來推算步伐長度。第 k 步的步幅可以下列公式計算:

$$l_k = \eta \cdot \sqrt[4]{(a_{max}(t) - a_{min}(t))}$$

其中$\eta = d_{real}/d_{estimated}$是一個需要預先設定好的常 數。最後,在方向偵測方面,我們直接藉由實際測試 結果,我們直接依據表 2將特定讀值對應到特定方向, 做為方向偵測模組的輸入值。在上述模組調整完成後, 我們透過如圖 4 中的程式碼將各模組整合。表 3顯示 了第一個版本的定位系統的精準度實驗結果。實驗場 地在逢甲大學資訊電機大樓,進行方式則為選定 4 條 方向不同的相連路線,其中路線 1、3 為 50 公尺,路線2、4 為 16 公尺。實驗時持手機步行,於步行時透過手 機即時定位,每次判定時間間隔為 0.2 秒 (t = 0.2s), 並將定位結果即時顯示於畫面 (圖 6a、b),定位結果 及收集到的資料則儲存於手機上的 SQLite 資料庫內 (圖 6c)。實驗完成後,離線進行準確度分析,實驗共 重覆進行 5 次,實驗的結果如表 3 所示,開發畫面則 如圖 6 所示。

由表 3可發現,雖然平均誤差在 1 公尺內,但路線 2 的誤差達到 50 公尺,即使是用來做房間定位,也屬於無法接受的精確度。其主要原因是在轉彎時,方向 偵測一旦有誤差,之後做航位推算時,此誤差會不斷 累積。因此,我們透過平台提供的組裝機制,將其它 模組拿掉,單單只對方向感測器做測試,其結果如圖 5 所示。我們發現,硬體的方向感測器讀值並不穩定, 如果轉彎時遇到不正常的讀值,就會產生很大的誤差。

基於此一發現,在第二個版本的定位系統中,我們 改用 Kang 等人提出來的方法 [3] 來改善方向偵測讀 取穩定度的問題。Kang method 主要的概念是額外參 考加速計讀值來輔助校正方向感測器的讀值。接下來 透過平台提供的 DSL,可以很容易地將原來的模組替 換為 KangOrientationDetector 類別來完成實作。改用 此方法後重新進行實驗的結果如表 4所示。可發現由 於轉彎時方向偵測誤差縮小,因此整體準確率也大幅 提高,因此也達成了應用服務所要求的精準度。

本節透過展現一個基於我們所提出的開發平台,實際為一個應用服務開發 PDR 室內定位系統的過程。 在依照 3.2節提出的流程的開發過程中,可發現開發人 員需要藉由不斷調整參數及更換測試不同模組來完成 一

個夠準確的 PDR 室內定位系統,而我們所提出的 平台,藉由彈性的模組組合及提供數個預設模組實作 成品的方式,可以大幅降低開發人員於此一持續改善 精準度過程的負擔。

表 3: 初步實驗結果

序號	路線1 累計誤差 (m)	路線2 累計誤差 (m)	路線3 累計誤差 (m)	路線4 累計誤差 (m)	平均量測誤差 (m/次)
1	0	8	51.4	9.6	0.522
2	0	0	50	0	0.379
3	0	6	50	0	0.424
4	0	0	50	0	0.379
5	0	6	50	2	0.515

表 4: 改用 Kang method 做方向偵測後的實驗結

序號	路線1 累計誤差 (m)	路線2 累計誤差 (m)	路線3 累計誤差 (m)	路線4 累計誤差 (m)	平均量測誤差 (m/次)
1	0	0	0	1	0.007
2	0	1.4	2.8	2	0.047
3	7	0	2.36	0	0.070
4	0	4	0	2	0.045
5	0	1.4	0	0	0.010

5 結論

本論文的主要從軟體工程的角度出發,發展一個可 快速建構 PDR 室內定位系統的開發平台。此平台將 PDR 各資料處理階段設計為具有相同輸出入介面的獨 立模組。開發人員可自由組合獨立模組,快速嘗試各 種演算法模組的組合,為其特定應用找到最好的搭配 方式。我們也基於此一平台實際開發出一個定位系統, 評估其精準度,並運用在一個典型的智慧生活空間應 用服務上,以驗證此一平台的可行性。PDR 定位技術 先天具有誤差累積問題,一旦開始發生偏差,則往後 的移動會產生更大的誤差。未來針對這一點,我們正 在研究利用 WiFi 訊號或是二維條碼來進行位置偏差 的修正。其次是手機在使用者身上的配戴位置不同, 會對定位產生影響,例如手機可能會拿在手上、放在 口袋或是放在包包裡,即使同樣是行走,也會因為擺 放位置不同而會產生不同的加速計波形,方向判斷也 會因此而難以判斷,未來我們也將透過手機內建的姿 態感應器,自動修正因手機放置位置所產生的誤差, 開發不需特定使用姿態的 PDR 定位機制。

參考文獻

[1] A.K.Dey, "Understanding and using context,"*Personal and Ubiquitous Computing Journal*, Vol.1, No. 5, 2001.

[2] J. A. B. Link, P. Smith, N. Viol, and K. Wehrle,"FootPath: Accurate Map-based Indoor Navigation Using Smartphones," in *Proc. International Conference on Indoor Positioning and Indoor Navigation*, 2011.

[3] W. Kang, S. Nam, Y. Han, and S. Lee, "Improved Heading Estimation for Smartphone-Based Indoor Positioning Systems," in *Proc. IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, 2012.

[4] M. Popa, J. Ansari, J. Riihijarvi, P. Mahonen, "Combining Cricket System and Inertial Navigation for Indoor Human Tracking," in *Proc. WCNC*, 2008.

[5] C. Lee, Y. Chang, G. Parkl, J. Ryu, S. G. Jeong, S. Park,J. W. Park, H. C. Lees, K. S. Hong, M. H. Lee, "Indoor positioning system based on incident angles of infrared emitters," in *Proc. Annual Conference of the IEEE Industrial Electronics Society*, 2004.

[6] A. R. Pratama, Widyawan, R. Hidayat, "Smartphone-based Pedestrian Dead Reckoning as an Indoor Positioning System," in *Proc. International Conference on System Engineering and Technology*, 2012.

[7] S.H. Shin, M. S. Lee, C. G. Park, H. S. Hyun, "Pedestrian dead reckoning system with phone location awareness algorithm, " in *Proc. IEEE/ION Position Location and Navigation Symposium*, 2010.

[8] C. Fischer, P. T. Sukumar, and M. Hazas, "Tutorial: Implementing a Pedestrian Tracker, Using Inertial Sensors," in *IEEE Pervasive Computing*, Vol. 12, No.2, 2013.

[9] M. Fowler, *Domain Specific Languages*, AW, 2010. [10] R. Jirawimut, P. Ptasinski, V. Garaj, F. Cecelja, W. Balachandran, "A Method for Dead Reckoning Parameter Correction in Pedestrian Navigation System," in *Proc. IEEE Instrumentation and Measurement Technology Conference*, 2001.

[11] Z. Sun, X. Mao, W. Tian, X. Zhang, "Activity Classification and Dead Reckoning for Pedestrian Navigation with Wearable Sensors," in *Measurement Science and Technology*, Vol.20, No.1, 2009.

[12] J. Kappi, J. Syrjarinne, and J. Saarinen. "MEMSIMU based pedestrian navigator for handheld devices," in *Proc.International Technical Meeting of the Satellite Division of The Institute of Navigation*, 2001.

[13] K. Aminian, P. Robert, E. Jequier, Y. Schutz, "Level, Downhill and Uphill Walking Identification using Neural Networks," in *Electronics Letters*, Vol.29, No.17, 1993.

[14] J. W. Kim, H. J. Jang, D-H. Hwang, and C. Park, "A Step, Stride and Heading Determination for the Pedestrian Navigation System," in *Journal of Global Positioning Systems*, Vol.1, No. 8, 2004.

[15] H. Weinberg, "Using the ADXL202 in Pedometer and Personal Navigation Applications," in *Analog Devices AN-602 Application Note*, 2002.

[16] J. Scarlet, "Enhancing the Performance of Pedometers Using a Single Accelerometer," *Analog Devices AN-900 Application Note*, 2005.

[17] E. Evan, *Domain-Driven Design: Tackling Complexity in the Heart of Software*, Addison Wesley, 2003.

融入基因演算法進化演算特性之進化式教師介聘多角調作業—以臺閩地區公立國民中小學暨幼兒園教師介聘他縣市為例

王 修
高雄市政府教育局資訊教育中心
hsiu@mail.kh.edu.tw

李文堂
高雄市政府教育局資訊教育中心
leewt@mail.kh.edu.tw

摘要

受到基因演算法（Genetic Algorithm, GA）應用於教師介聘多角調作業之研究的啟發，本研究提出一個以現行教師介聘作業為基礎、融入基因演算法之進化演算特性的多角調作業方式：「進化式多角調」，期能藉由改變介聘成功教師現職服務學校與應聘科別之循環媒合作業，增進介聘成功人數與介聘成功之志願學校排名。

現行教師介聘採電腦化作業，分成「單調、6 角調、5 角調、4 角調、3 角調、互調」等階段，各階段作業結束後，教師介聘作業即告完成。前述之「6 角調、5 角調、4 角調、3 角調、互調」統稱為「多角調」。

本研究所提出之「進化式多角調」，係於現行介聘作業結束後，以原介聘作業之「6 角調、5 角調、4 角調、3 角調、互調」等階段為一次媒合作業，每一次媒合作業中，已介聘成功但尚未介聘至最佳志願學校與科別之教師，改以介聘成功之學校與科別，作為現職服務學校與應聘科別，連同尚未介聘成功之教師，一同進行媒合作業。如此循環，直到媒合作業再無增益為止。

經以民國 99～102 年「臺閩地區公立國民中小學暨幼兒（稚）園教師介聘他縣市服務作業」之申請介聘教師進行實驗，結果發現本研究所提出之方法，確能有效增進介聘成功人數與介聘成功之志願學校排名，增益人數最高可達 384 人。

關鍵詞：教師介聘、多角調、進化演算。

Abstract

Inspired by “Application of Genetic Algorithm on Multiple Transfer Operation of Teacher Transfer”, this research proposes an approach of multiple transfer operation, Evolutionary Multiple Transfer Operation, which adapts current multiple transfer operation of teacher transfer as foundation, and integrates the evolutionary characteristics of Genetic Algorithm. We hope, by designing the cyclic matching procedures based on successful matched gains, to increase the numbers of effective matched teachers and school rankings.

Current operation of teacher transfer is computerized and is divided into phases of Single Posting, 6-sided Transfer, 5-sided Transfer, 4-sided Transfer, 3-sided Transfer and 2-sided Transfer. The operation is completed after each phase in is finished. The aforementioned transfer phases are collectively called “Multiple Transfer Operation”.

The “Evolutionary Multiple Transfer Operation” proposed in this research is, after the current transfer operation is completed, to conduct a single matching procedure by taking the original “6-sided Transfer, 5-sided Transfer, 4-sided Transfer, 3-sided Transfer and 2-sided Transfer” as a whole. In each procedure, teachers who are considered successfully matched but not transferred to the subjects and schools of their best choices, will, with the results from previous matching, join another single matching procedure that involves teachers who are not yet successfully matched. The cycles will not cease until there are no matched gains.

We conduct an experiment using the statics from “Operation of Application for Inter-City/County Transfer for Teachers of Public Junior High Schools, Elementary Schools and Kindergartens in Taiwan Area” database from 2010 to 2013, it shows that by implementing the approach proposed by this research, the numbers of successfully matched teachers and schools ascend and the maximum gain increases up to 384 persons.

Keywords: Teacher Transfer, Multiple Transfer, Evolutionary Computation.

1. 前言

「臺閩地區公立國民中小學暨幼兒園教師介聘他縣市服務作業」（以下稱臺閩教師介聘作業）是教育主管機關的年度重大事務，其目的在於服務每年數以千計、基於個人生涯規劃（進修）與生活不便（交通、照顧家人）等因素提出申請介聘的教師，能夠順利介聘至其理想的地區學校服務，使能安於教學，以謀教育工作之順遂推行。表 1 為民國 91～102 年臺閩教師介聘作業相關人數統計。

臺閩教師介聘作業自民國 55 年開始辦理、民國 76 年採用電腦化作業，經多年發展，作業方式分成「單調、6 角調、5 角調、4 角調、3 角調、互調」等階段[1, 4]，各階段作業結束後，教師介聘作業即告完成。前述之「6 角調、5 角調、4 角調、3 角調、互調」統稱為「多角調」。有關臺閩教師介

表 1 民國 91～102 年臺閩教師介聘作業申請暨成功人數統計表[3]

年度	國中		國小		幼兒(稚)園	
	申請人數	成功人數	申請人數	成功人數	申請人數	成功人數
91	2053	744	3359	1590	327	116
92	2091	800	3645	1779	364	154
93	2281	954	4061	1862	279	95
94	2308	905	3551	1392	252	103
95	2314	815	2986	1080	253	94
96	2462	978	2813	954	202	77
97	2640	868	2699	829	194	65
98	2576	746	2096	663	194	69
99	2633	763	2296	784	218	110
100	2330	753	2342	755	196	89
101	2493	786	2845	803	217	113
102	2499	813	2680	886	290	156

聘作業方式與單調、多角調等各階段作業之程式運作流程，請參閱本文所參考之文獻[2]。

現行臺閩教師介聘作業基於作業時效與連帶退回（該多角調介聘成功之教師中，如有某位教師不出席該介聘學校教評會審查，或經審查通過不到該校報到，則同屬介聘成功之其他教師無條件撤回）之考量，採取「分階段、一次性」且各階段介聘成功之教師不再參與剩餘階段作業之方式，雖可縮短作業時間與限制連帶退回之人數，卻也造成了介聘成功但非最佳志願學校的教師，失去了求得更佳介聘結果的機會，同時也限制了介聘成功人數。

基因演算法（Genetic Algorithm, GA）係源於自然界「物競天擇，適者生存」之特性，模擬生物相互競爭之概念，以類似基因（Gene）演化的循環過程而成，已證明為一可廣泛應用（物理、工程、醫學、建築……）之全域解最佳化搜尋方法，經研究實驗證明確可應用於臺閩教師介聘作業之多角調，有效突破其解空間限制，增進介聘成功人數，提供決策者多樣性解決方案的決策考量，惟因現行作業要點規範（積分高者優先、連帶退回）而難以發揮[2]。

本研究旨在提出一個以現行臺閩教師介聘作業模式為基礎、融入基因演算法之進化演算特性的多角調作業方式：「進化式多角調」，藉由改變介聘成功教師現職服務學校與應聘科別之循環媒合作業，並以民國 99～102 年臺閩教師介聘作業之申請介聘教師為例，進行增進介聘成功人數與介聘成功志願學校排名之探討。

本文將於次節描述本研究所探討之問題；本研究所提出之「進化式多角調」則於第 3 節說明；第 4 節為本研究之實驗結果；本文結論則於第 5 節提出；文末將列出本研究所參考之文獻來源。

2. 問題描述

假設有三位數學科教師申請介聘，相關資料與原介聘結果如表 2 所示。

表 2 模擬數學科教師原介聘作業結果

姓名	任職學校	積分	志願學校	介聘結果
張三	A 縣甲校	88	1.X 縣癸校 2.Y 縣壬校	單調 Y 縣壬校
李四	X 縣癸校	90	1.B 縣乙校 2.B 縣丙校	無
王五	B 縣乙校	85	1.Y 縣壬校 2.Z 縣辛校	無

表 3 模擬數學科教師進化式介聘作業結果

姓名	任職學校	積分	志願學校	介聘結果
張三	Y 縣壬校 ~~A 縣甲校~~	88	1.X 縣癸校 2.Y 縣壬校	X 縣癸校
李四	X 縣癸校	90	1.B 縣乙校 2.B 縣丙校	B 縣乙校
王五	B 縣乙校	85	1.Y 縣壬校 2.Z 縣辛校	Y 縣壬校

在介聘作業中，Y 縣壬校提出 1 個數學科缺額，經積分比序，由張三以「單調」方式介聘至該校（第 2 志願學校），李四、王五介聘失敗。

如能針對介聘成功但非最佳志願學校的教師，將其原任職學校與應聘科別，變更為介聘成功的學校與科別，連同尚未介聘成功的教師，一同進行多角調媒合作業，不僅可以提供已介聘成功之教師，能介聘至更佳志願學校的機會，同時也能增加尚未介聘成功之教師，能夠介聘成功的機會。

以表 3 為例，在原介聘作業結束後，如將張三的任職學校由原來的「A 縣甲校」變更為「Y 縣壬校」，連同張三、李四一同進行多角調媒合作業，結果將如表 3 所示，張三、李四、王五等三人可以「3 角調」方式介聘成功。張三不僅從原來的第 2 志願學校，介聘至更佳的第 1 志願學校，原介聘失敗的李四、王五，均能介聘成功。

3. 進化式多角調

本研究所提出之「進化式多角調」係以現行臺閩教師介聘作業模式為基礎，將基因演算法之進化演算特性，融入現行教師介聘作業之多角調，於現行介聘作業結束後，以原介聘作業之「6 角調、5 角調、4 角調、3 角調、互調」等階段為一次媒合作業，每一次媒合作業中，已介聘成功但尚未介聘至最佳志願學校與科別之教師，改以介聘成功之學校與科別，作為現職服務學校與應聘科別，連同尚未介聘成功之教師，一同進行媒合作業。如此循環，直到媒合作業再無增益為止。

加入進化式多角調之介聘作業流程如圖 1 所示，處理程序說明如下：

1. 單調作業
2. 多角調作業（6 角調、5 角調、4 角調、3

角調、互調）

3. 進化式多角調初始化：
   - 保留現行介聘結果
   - 排除已成功介聘至最佳志願學校與應聘科別之教師
   - 變更已介聘成功教師現職服務學校與應聘科別為介聘成功之志願學校與科別
4. 進化式多角調作業
   - 作業對象包括：
     - ◆ 已介聘成功但尚未介聘至最佳志願學校與科別之教師
     - ◆ 尚未介聘成功之教師
   - 作業邏輯與原多角調作業相同
5. 判斷介聘結果如有增益則回到步驟 3
6. 結束

對照於基因演算法，上述步驟 1、2 等同於「產生初始世代」；步驟 3、4 等同於「基因操作、建立新世代」；步驟 5 等同於「計算適應值（目標函數）」。

由於「進化式多角調」係以現行作業模式為基礎，作業邏輯與原多角調作業相同，故仍遵循「積分高者優先」的積分原則；融入基因演算法之進化演算特性，故可保有求得更佳介聘結果的機會。

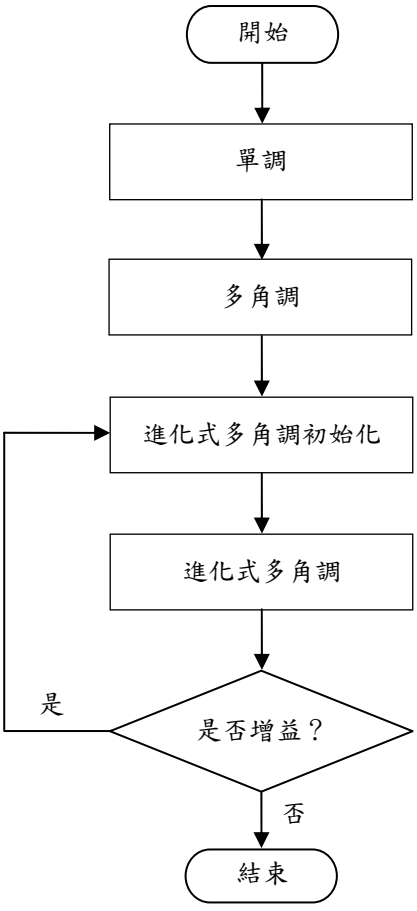


圖 1 加入進化式多角調之介聘作業流程

4. 實驗結果

本研究以民國 99～102 年臺閩教師介聘作業之申請介聘教師進行「進化式多角調」之實驗結果，與原作業結果之比較如表 4 所示，最多可增加介聘成功人數 92 人（102 年）、志願學校向前 305 人（101 年），增益人數高達 384 人（101 年）。

表 4 民國 99～102 年結果比較表

年度	階段別	原成功人數	加入進化式多角調介聘作業				
			循環次數	成功人數	增加人數	志願向前	增益人數
99	國中	763	2	790	27	87	114
	國小	784	3	826	42	160	202
	幼稚園	110	1	112	2	10	12
	合計	1657	6	1728	71	257	328
100	國中	753	2	779	26	68	94
	國小	755	2	781	26	189	215
	幼稚園	89	1	91	2	2	4
	合計	1597	5	1651	54	259	313
101	國中	786	2	815	29	64	93
	國小	803	3	849	46	234	280
	幼稚園	113	1	117	4	7	11
	合計	1702	6	1781	79	305	384
102	國中	813	2	859	46	89	135
	國小	886	3	929	43	160	203
	幼兒園	156	2	159	3	4	7
	合計	1855	7	1947	92	253	345

5. 結論

本研究所提出以現行教師介聘作業模式為基礎、融入基因演算法進化演算特性之「進化式多角調」，經以民國 99～102 年臺閩教師介聘作業之申請介聘教師進行實驗，結果發現確能有效增進介聘成功人數與介聘成功之志願學校排名，增益人數最高可達 384 人（101 年）。

「進化式多角調」係藉由改變介聘成功但尚未介聘至最佳志願學校與科別之教師現職服務學校與應聘科別之循環媒合作業，因此原介聘作業結果中介聘成功教師之介聘方式（單調成功或多角調成功）與介聘關連（多角調成功之教師關係）將不再具有意義，各縣市政府恐難依據現行作業要點之規範處理連帶退回作業。

臺閩教師介聘作業之目的，在於服務基於個人考量（生涯規劃、生活不便）申請介聘之教師，能夠順利介聘至其理想的地區學校服務。因此，在「連帶退回」與「增進介聘成功人數」二者權衡之下，應以後者為重。

本研究所提出之「進化式多角調」係以現行作業模式為基礎，故仍遵循「積分高者優先」的積分原則，容易為申請介聘教師所接受。為使能有更多的教師能夠介聘至其理想的地區學校服務，建議可針對現行作業要點中有關連帶退回的處理方式進行思考，目前雖以不影響已介聘成功教師之方式（協調開缺）處理，但各縣市仍難以全面配合執行；若可修改介聘辦法或作業要點，規定參與多角調教師必須到介聘學校報到，再配合「進化式多角調」作業，將可得到更佳的介聘作業結果。

參考文獻

[1] 王修、劉東官、楊中皇，應用基因演算法於教師介聘多角調作業之探討—以台閩地區公立幼稚園教師外縣市介聘為例，第十九屆國際資訊管理研討會，2008 年 5 月，國立暨南大學。

[2] 王修，應用基因演算法之最佳化教師介聘多角調作業—以台閩地區公立幼稚園教師介聘他縣市為例，國立高雄師範大學資訊教育研究所碩士論文，2010。

[3] 高雄市資訊教育中心，102 年臺閩地區公立國民中小學暨幼兒園教師申請介聘他縣市服務網，http://tas.kh.edu.tw/。

[4] Hsiu Wang, Tung-Kuan Liu, Chung-Huang Yang, "Multiple Teacher Transfer Optimization using Genetic Algorithms – Case Study on Kindergarten Teacher Transfer," The 2008 International Computer Symposium (ICS 2008), November 13-15, 2008, Tamkang University, Damsui, Taipei County, Taiwan.

我國「資訊素養與倫理」數位教材融入國小教學學習成效之研究—以國小五年級學生為例

李治慧[1]　林宜隆[2]　陳致穎[3]
[1]國立宜蘭大學 資訊工程研究所
n0043022@ms.niu.edu.tw
[2]元培科技大學 資訊管理學系
Cyberpaul747@gmail.com
[3]國立宜蘭大學 資訊工程研究所
n0043006@ms.niu.edu.tw

摘要

本研究主要目的在探討「資訊素養與倫理」數位教材融入教學對國小五年級學生在網路霸凌、網路交友及網路沉迷的認知態度及行動之學習成效，採用準實驗研究法，研究對象包含實驗組及對照組共六十位學生。本實驗教學使用臺北市教育局出版的國小「資訊素養與倫理」數位教材作為教學內容來進行實驗教學。教學前後採用「資訊素養與倫理」認知態度及行動量表進行前、後測，並將實驗組與對照組學生進行後測比較分析，以了解學生在資訊素養與倫理認知態度及行動上之學習成效。實驗過程並輔以教學活動回饋單、學習單、教室觀察記錄表、教師心得與省思等質性分析以了解學生在實驗教學過程中的學習歷程與成效。

關鍵詞：數位教材、資訊素養與倫理、鷹架學習理論、學習成效

Abstract

The purpose of this study was to explore the 「Information Literacy and Ethics」 digital materials intergrating into teaching for fifth grade students' learning effectiveness on cyberbullying, online dating and internet addiction. The use of quasi-experimental research study object contained the experimental group and the contrast group of sixty students. This experiment used the digital material—「Information Literacy and Ethics」, published by the Taipei City Department of Education, for experimental teaching. In addition, I used the scale of 「Information Literacy and Ethics」 for cognitive attitudes and actions to evaluate the students before teaching and after teaching, as well as did post-test comparison analysis for both the students from the experimental group and the control group, for understanding students' learning effectivness on information literacy, ethical cognitive attitudes and actions. During the experimental procedures, I also used qualitative analysis such as teaching feedback sheets, worksheets, classroom observation record sheet, and teacher's reflection, to know the learning process and the learning results of the students under the experimental teaching.

Keywords: digital textbooks, information literacy and ethics, scaffolding learning theory, learning effectiveness

1. 前言

近年來，網路引發的社會問題不勝枚舉，網路帶來的負面效應向下延伸，觸角已伸向國中小學童。目前國內的學生已經累積了許多因為不當使用網路的案例 這些不當使用資訊的案例著實令教育界擔憂！因此，教育部在 101 年 5 月提出「學生安全上網及不當使用網路資訊實施計畫」，特別針對大專院校、高中以及國中小學生推廣「資訊素養與倫理」課程，提升其正確的網路使用觀念，以降低並預防學生網路的不當使用，培養具有資訊倫理的現代國民！

2. 文獻探討

2.1 資訊素養與倫理的定義與意涵

資訊素養（Information Literacy）是「素養」一詞依時代需求演變而來。「素養」的要件與特質是「瞭解及與外界溝通的能力」，依不同期的需求標準有異（吳美美, 1996）。隨時代的演進，逐漸將「素養」內涵之二分法（有或無）進而轉為程度上的差異（吳美美, 1996），例如文學素養的高低。而「資訊素養」則是為符合資訊時代的需求應運而生的「產物」。

Mason（1986）認為資訊倫理是指發展和使用資訊科技有關的倫理議題，資訊倫理在處理資訊科技的使用者和提供者所引發的一些有關倫理的問題；他提出有關資訊倫理的四個範疇（PAPA）為：

資訊的隱私(Privacy)、資訊的正確性(Accuracy)、智慧財產（Property）和資訊的獲得（Access）。

根據臺北市教育局發行的「資訊素養與倫理高中國小第二版數位教材中對資訊素養與倫理的定義，包括正確的使用網路資訊與文字，要能夠做到克制自己、避免濫用網路，其內容包含數位達人、網路識讀、網路禮節、網路詐騙與色情、著作權合理使用、網路謠言與霸凌、不當資訊、網路交友、網路資料保護、線上遊戲與沉迷等重要議題。

2.2 臺北市教育局資訊素養與倫理網站與數位教材課程內容分析

本研究採用臺北市教育局資訊素養與倫理網站內之數位教材融入教學，本節將針對不同年級與不同對象，將此網站與數位教材的內容做詳細的比較分析。



http://ile.tp.edu.tw/

圖 1 臺北市政府教育局資訊素養與倫理網站

為了導引學生了解資訊倫理、電腦使用安全及資訊相關法律等議題。臺北市政府教育局資訊室於九十五年特委由中央警察大學林宜隆（現為元培科技大學資訊管理學系教授）教授擔任召集人，召集編輯小組進行編撰出版數位教材，提供國小、國中及高中學生與教師使用。並於九十八年針對第一版材進行編修，另增加線上動畫，提供學生自我學習。

表 1 網站內容簡介

適用年級	網頁封面	內容簡介
國小版	 http://ile.tp.edu.tw/ile/elementary/edu_web/ebook/ebook.htm	一、課程內容包含資訊素養與倫理十大主題單元。 二、十大單元以完整的電子書形式呈現。 三、國小版教材包含電子書、動畫、測驗及 PDF 四大部分。 四、電子書的使用活潑生動，可以做筆記的電子筆為其一大創新特色。
國中版	 http://ile.tp.edu.tw/ile/junior/	一、課程內容包含資訊素養與倫理導論與八大主題單元。 二、國中版教材包含電子書(PDF 格式)、動畫、學習單 DOC 及教學簡報 PPT 四大部分。
高中版	 http://ile.tp.edu.tw/ile/hischool/	一、課程內容包含資訊素養與倫理九大主題單元。 二、高中版教材包含電子書與動畫兩大部分。 三、每個主題單元都以三國歷史動畫故事導引，引起學生的學習興趣。 四、每個主題單元故事結束後皆提供測驗與詳細的解答。

3. 研究設計與實施

3.1 研究架構

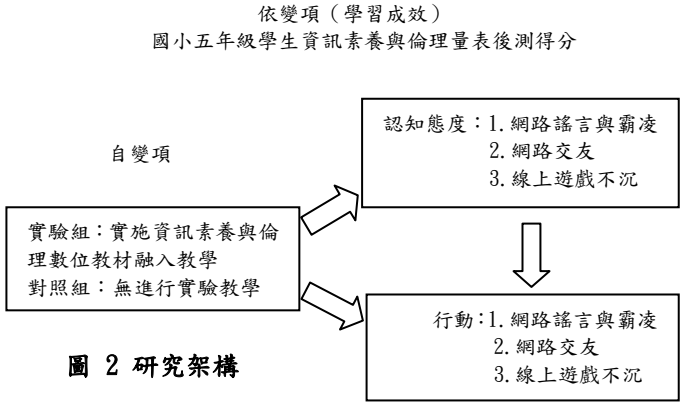
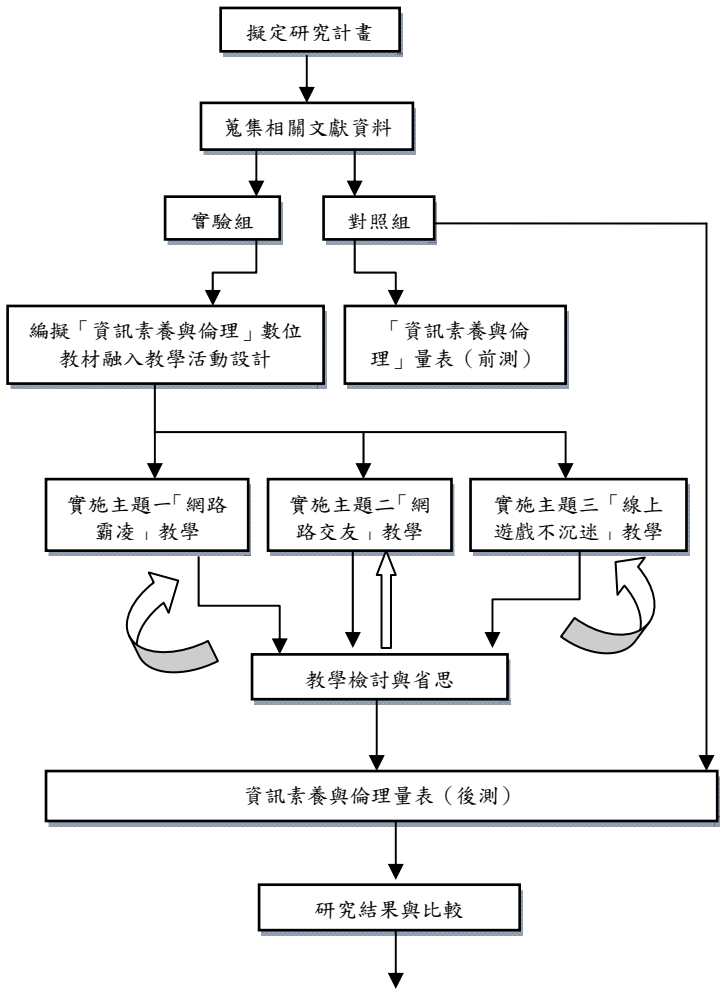


圖 2 研究架構

3.2 研究流程



研究結論與建議

圖 3 研究流程

4. 研究結果與討論

4.1 量化資料結果分析

實驗教學後，控制組與實驗組再次接受「資訊與倫理」問卷後測調查，旨在了解實驗教學結束之後，兩組學生在資訊素養與倫理之「認知態度」與「行動」的表現是否有顯著差異，以獨立樣本 t 檢定來檢驗後測問卷。

表 2 兩組學生資訊素養與倫理問卷後測分析

檢測項目	對照組		實驗組		t 值	顯著值
	平均	標準差	平均	標準差		
認知態度	3.49	.39	3.70	.27	2.32	.02*
網路霸凌	3.54	.56	3.78	.32	2.04	.04*
網路交友	3.60	.41	3.76	.33	1.66	.06
網路沉迷	3.34	.48	3.55	.33	1.95	.10
行動	3.42	.59	3.73	.27	2.55	.02*
網路霸凌	3.47	.67	3.76	.36	2.13	.04*
網路交友	3.35	.56	3.72	.32	3.17	.00**
網路沉迷	3.46	.66	3.70	.31	1.78	.08

*p < .05 , **p < .01; 註：對照組 N = 30；實驗組 N = 30

為了解實驗教學後實驗組資訊素養與倫理之「認知態度」、「行動」的改變情形，將實驗組的「資訊素養與倫理問卷」前測、後測進行相依樣本 t 檢定。

表 3 組內資訊素養與倫理分析

檢測項目	前測		後測		t 值	顯著值
	平均	標準差	平均	標準差		
認知態度	3.5976	.29540	3.6956	.26991	-4.331	.00**
網路霸凌	3.7467	.35982	3.7800	.31666	-1.720	.10
網路交友	3.6067	.35905	3.7600	.33384	-2.283	.03*
網路沈迷	3.3933	.47119	3.5467	.32772	-3.357	.00**
行動	3.5844	.46211	3.7267	.27311	-3.102	.00**
網路霸凌	3.5933	.63351	3.7600	.35777	-2.386	.02*
網路交友	3.5800	.47080	3.7200	.31775	-2.616	.01*
網路沈迷	3.5800	.46193	3.7000	.30962	-2.382	.02*

*p < .05 , **p < .01

4.2 質性量化結果討論分析

表 4 國小五年級資訊素養與倫理量表分析結果

研究工具	研究方法	研究單元主題		研究結果
國小五年級學生資訊素養與倫理量表	獨立樣本t檢定	認知態度面向	網路謠言與霸凌	實驗組>對照組 已達.05顯著水準
			網路交友	實驗組>對照組 未達.05顯著水準
			網路沉迷	實驗組>對照組 未達.05顯著水準
			整體量表	實驗組的各平均得分皆 高於對照組 以「網路謠言與霸凌」得分最高
		行動面向	網路謠言與霸凌	實驗組>對照組 已達.05顯著水準
			網路交友	實驗組>對照組 已達.05顯著水準
			網路沉迷	實驗組>對照組 未達.05顯著水準
			整體量表	實驗組的各平均得分皆 高於對照組 以「網路謠言與霸凌」得分最高
	相依樣本t檢定	認知態度面向	網路謠言與霸凌	實驗組後測>前測 未達.05顯著水準
			網路交友	實驗組後測>前測 已達.05顯著水準
			網路沉迷	實驗組後測>前測 已達.05顯著水準
			整體量表	實驗組後測各平均得分皆高於前測 以「網路謠言與霸凌」得分最高
		行動面向	網路謠言與霸凌	實驗組後測>前測 已達.05顯著水準
			網路交友	實驗組後測>前測 已達.05顯著水準
			網路沉迷	實驗組後測>前測 已達.05顯著水準
			整體量表	實驗組後測各平均得分皆高於前測 以「網路謠言與霸凌」得分最高

由上述實驗結果可知，在本研究的實驗教學之後，實驗組的資訊素養與倫理有顯著的正面發展，學習成效頗佳。實驗組學生在「認知態度」與「行動」兩個分向量表及「整體量表」前後測平均數，在經過相依樣本 t 考驗後，都達到.05 的顯著水準，表示實驗組學生在接受實驗教學後，前測與後測得分有顯著性的差異。

表 5 質量交叉比較分析小結

研究單元主題		量表研究結果	質性研究結果分析
認知態度面向	網路謠言與霸凌	實驗組後測>前測未達.05 顯著水準	1.實驗組學生在實驗教學前對網路謠言與霸凌已有了相當程度的認知。其原因可能為校內積極推動反霸凌活動，學生在教學前已具備相當的認知程度。 2.實驗組學生在經過實驗教學後，對有關在網路以言語攻擊他人或發表不當的言語可能涉及毀謗或公然侮辱罪的相關法律與刑責有了基本的認知。 3.知道不能隨便在臉書按讚，這是一種助長霸凌的行為。
	網路交友	實驗組後測>前測已達.05 顯著水準	1.實驗組學生在經過實驗教學後，對網路交友安全守則的認知概念有所提升。 2.加強個人在網路帳號密碼等隱私保護的認知。 3.透過新聞案例了解到網路交友所帶來的負面影響。
	線上遊戲不沉迷	實驗組後測>前測已達.05 顯著水準	1.實驗組學生中有 80%上網最常玩線上遊戲，也有學生曾在玩線上遊戲時被盜取帳號密碼。在實驗教學後，學生了解到網路沉迷帶來的負面影響。 2.了解虛擬世界易沉迷，不要以過份沉迷的態度當作唯一休閒娛樂。
	整體量表	實驗組後測各平均得分皆高於前測，並且達顯著水準	「線上遊戲不沉迷」的得分最低，大多數學生認為線上遊戲令人難以抗拒，破關具有挑戰性，會得到強大的成就感。
行動面向	網路謠言與霸凌	實驗組後測>前測已達.05 顯著水準	1.學生在社群網站或玩線上遊戲時會約束自己的行為並謹慎發言。 2.遇到霸凌事件時會主動告知父母及師長。 3.在網路上不會做出毀謗及侮辱他人的行為。
	網路交友	實驗組後測>前測已達.05 顯著水準	1.在面對網路交友時會謹慎小心，會告知父母自己的網路交友情形。 2.不會隨便向網友透露自己的隱私及帳號密碼。
	線上遊戲沉迷	實驗組後測>前測已達.05 顯著水準	1.願意培養其他的休閒活動，不把玩線上遊戲當作唯一的娛樂。 2.願意去遵守電腦軟體分級制度。
	整體量表	實驗組後測各平均得分皆高於前測 以「網路謠言與霸凌」得分最高	由實驗結果得知，小朋友未曾對別人網路霸凌。班上也僅有兩位同學被網路霸凌過。顯示在教學前小朋友以具備充份之認知。而僅有一位同學在臉書對霸凌他人的言語按讚，經過實驗教學後也了解其行為可能涉及的法律責任，並懂得約束自己的行為。

經過質量分析交叉比較的結果，實驗組學生在各方面的認知與表現都證明了利用「資訊素養與倫理」數位教材融入教學之學習成效頗高。臺北市政府教育局出版的「資訊素養與倫理」國小第二版數位教材由深具法學與資安素養的林宜隆教授（現為元培科技大學資管系教授）教授擔任召集人，與具備專業知識的各領域教師集結心血共同編撰完成。導引時下國小學生認識資訊素養與資訊倫理的相關議題，以資訊相關法律融入課程，配合學生日常生活經驗之案例故事，由實驗的量表分析及質性分析結果證明了活潑生動的教材不僅能引起學生的學習興趣，也收到了良好的學習成效！

5. 結論與建議

透過「課程計畫→教學行動→教學觀察→教學省思→修正→行動」的研究歷程探討如何透過資訊素養與倫理數位教材融入教學以提升學生在網路霸凌主題的學習成效。研究者以五年級的學生為教學對象，實施兩週的實驗教學活動課程，藉由教學歷程、教師省思日誌、五年級學童網路霸凌的認知態度與行動量表前後測、協同觀察者的教室觀察記錄、學生學習單與教學活動回饋單等資料，總結歸納其研究結論與研究建議。

(一)研究結論

透過資訊素養與倫理數位教材融入教學對國小五年級學童在網路霸凌主題之學習成效有明顯的提升，將其結果分述如下：

1. 提升學生資訊素養與倫理的認知
2. 培養面對網路霸凌時的正確態度
3. 建立良好與正向的行動

學生能確實遵守網路使用的倫理規範，在網路上表現出適當且合宜的行為。

(二)研究建議

1. 二十一世紀是資訊高度發展的時代，學生要面臨的資訊素養與倫理議題非常多，可以針對不同主題設計更多相關的課程，培養具有資訊倫理的現代國民。
2. 臺北市教育局資訊素養與倫理網站中的國小二版應普遍推廣，鼓勵其他縣市之國小教師進行資訊融入教學，將資訊教育向下紮根，減少因網路普及所帶來的負面影響！
3. 資訊素養與倫理的教學應該要融入各科教學，在國小各年段實施長時期的資訊教育，將正確的網路與資訊倫理觀念從小打好基礎！
4. 在基礎的相關課程實施後，應加強更深入的探討法律層面的問題，以實際發生的新聞案例每天隨機教學，加深學生的網路法律觀念，避免觸法。
5. 學校及教育行政機關，應該多辦理相關研習，對象包含家長、老師及社會人士，讓教師與家長具備正確的資訊素養與倫理認知態度與行動，以身作則，

作為學生與孩子學習的好榜樣！

資訊網路ｅ世代的莘莘學子，應該要培養正確之資訊素養與倫理概念！網路霸凌只是資訊倫理中的一個重要議題，本研究藉由網路霸凌的課程實施混成式的教學模式，並且導入以臉書成立社團的方式進行案例討論，企圖將網路霸凌高犯罪的場所導正為具教育意義的社群網站！由此研究得知，多媒體互動教材確實能有效引起學生的學習動機並達到有效之學習效果。台北市教育局資訊素養與倫理網站中的國小二版應普遍推廣，鼓勵其他縣市之國小教師進行資訊融入教學，落實網路建全國民之培養！

參考文獻

1. 吳清基・林宜隆等（2006）。資訊素養與倫理－國小版。
吳清基・林宜隆等（2006）。資訊素養與倫理－國中版。
吳清基・林宜隆等（2005）。資訊素養與倫理－高中版。

2.教育部數位學習網站
http://ups.moe.edu.tw/Teaching_Material/textbook_frame.php?content_cd=130313

3. 中小學網路素養與認知網站
http://www.eteacher.edu.tw

4. 朱家榮，資訊倫理研究初探，臺灣圖書館管理季刊，第6卷，第7期，2010，
頁 106-120。

5. 林維珉，國小高年級學生資訊倫理態度與行為意向之研究－以臺北市某國小
為例，臺北市立教育大學數學資訊教育學系碩士班，2008。

6. 林季謙，不同背景中/小學生網路成癮之相關研究，南華大學教社所，網路社會學通
訊期刊，第33期，2003，2010/10/13取自
http://www.nhu.edu.tw/~society/e-j/33/。

7. Belsey, B. (2005). Cyberbullying. Retrieved Feb. 28, 2009, from
http://www.cyberbullying.ca/pdf/feature_dec2005.pdf

8. Patchin, J. W. & Hinduja, S (2010). Changes in adolescent online social networking behaviors from2006 to 2009. Computers in Human Behavior, 26, 1818–1821.

9. Younes, W. (2007). A workshop by educators for students in middle and high schools. USA:Carnegie Mellon University.

10. 朱美瑰(2008)。網路犯罪新型態~看不見的拳頭：青少年網路霸凌現象初探。諮
商與輔導，268，6-10。

11. 兒童福利聯盟文教基金會（2012）。2012年台灣網路霸凌現象調查報告

中小學網路霸凌防治課程之教學：教學省思之內容分析研究

徐敏容[1]　周 倩[2]
國立交通大學 教育研究所
[1]arithamo@gmail.com, [2]cchou@mail.nctu.edu.tw

摘要

本研究旨在了解參與網路霸凌線上研習課程的中小學教師，實際將網路霸凌課程操作於教學現場後之回應。研究者使用內容分析法，分析與統整 119 位教師所撰寫的教學活動紀錄表，並針對學生態度、教學設計與教學省思進行探討。

研究結果發現，在學生態度部分，教師認為學生對於防治網路霸凌課程態度積極正面，但是在認知上仍有不足，尤以法律知識最為薄弱；在教學設計部分，教師多使用影片、案例式教學法與問題導向式教學等方式；在教學省思部分，教師認為雖然情意目標難以用教學達成，但應即早建立學生使用資訊媒體的正確觀念。最後，研究者根據內容分析提出具體建議，以作為學校、教師與家長日後參考。

關鍵詞：網路霸凌、教學省思、內容分析法

Abstract

This research aims to explore the integration of cyberbullying prevention curriculum in K-12 classrooms. The participants were 119 elementary and secondary school teachers who volunteered to take part in an online teacher workshop for cyberbullying program. Data were collected from participants' teaching record sheet; content analysis were conducted after the data collection.

Results of this study showed that those teachers' students had a positive attitude toward attending cyberbullying prevention curriculum, but they were insufficient of knowledge about cyberbullying, especially issues concerning related laws and regulations. Regarding instructional design, teachers usually used video, case method teaching, and problem-based learning, etc. Although the instructional goals of affective learning are difficult to reach, it is still necessary to teach students how to use the Internet safely in information education. Based on the findings, this study provides useful suggestions for school administrators, teachers, and parents; and the results could also be applied for future studies.

Keywords: cyberbullying; teaching reflection; content analysis

1. 前言

資訊科技的快速發展，帶來許多生活上的便利，Web2.0 世代的開始，使得社群網站、YouTube…等逐漸普及，人們可以在網路上分享新知、建立友誼，讓人際之間的互動與溝通變得更多樣化。然而，在正向的加值應用下，人們也有可能透過網路傳遞不當言論、不實資訊，使得霸凌種類與行為更勝以往，而在網路上進行的霸凌行為，我們稱之為「網路霸凌」。網路霸凌藉由網路的特性延伸甚至超越了傳統霸凌的行為與範圍，所造成的傷害雖非生理上的明顯外傷，但心理層面的傷害更是不容小覷。

過去研究指出，學生可能對於網路霸凌的認知不足，且不清楚網路霸凌與開玩笑的界線，而教師也未清楚告知該錯誤行為，因此學生容易忽視網路霸凌的嚴重性[1]。有鑑於此，教育部 eteacher 計畫提供了網路霸凌的線上研習課程，以協助教師提升資訊素養的專業發展。其中，教師必須在教學現場中實際發展防治網路霸凌的課程，並撰寫教學流程、教學設計以及教學反思等活動紀錄。

研究者透過助教身分參與本課程，並記錄教師於教學現場之現況。其研究目的在於探討教師實際教授網路霸凌防制課程後之情形，針對學生的反應、教學設計與教學省思，分為三部份進行內容分析，研究問題如下：(1) 探討中小學教師教授網路霸凌防治課程後的學生反應；(2) 探討中小學教師在網路霸凌防治課程的教學設計；(3) 探討中小學教師對於網路霸凌防治課程的教學省思。期盼研究結果能助於教師們未來在網路霸凌防治的課程教授與推廣，並瞭解資訊素養課程教學實況，並提出相關建議。

2. 文獻探討

2.1 網路霸凌的定義

網路霸凌是屬於傳統霸凌的其中一種方式，網路霸凌是透過手機、電腦或是其他電子裝置，不斷進行重覆性、蓄意性的傷害行為，因此又稱之為「電子霸凌（electronic bullying）」、「數位霸凌（digital bullying）」或「網路騷擾（cyber harassment）」等[2]。總結來說，只要關於威脅性、攻擊性或是具有性暗示等訊息，造成對方感到懼怕、生心理受到威脅或是感到不舒服等，都屬於網路霸凌的行為。

網路霸凌和傳統霸凌相似，霸凌者通常會藉著戲謔他人達到樂趣和滿足感的目的[3]；但不同於傳統霸凌，網路霸凌多在線上空間發生，不需要有直

接的身體接觸行為，而對於受害者的傷害多為心理和精神層面。正因使用媒介的不同，網路霸凌藉由網路的即時性、匿名性、快速傳播等特性，其勢力範圍會隨著網路 24 小時不受時間與空間的限制、公開且快速的傳播，再加上網路的訊息一旦發送出去後難以回收，因此會持續性造成受害者二度傷害[4]。

2.2 青少年網路霸凌現況與成因

Hinduja 與 Patchin[3]認為好發生網路霸凌的可能的原因在於，青少年較喜歡嘗試一些新的電子裝置和通訊平台等新興科技。因此，青少年結合了自己的電腦技術能力，以及網路沒有成年人監督的環境，很有可能成為網路犯罪的高危險群[1]。

此外，青少年時期的學子正處於身體發育和心理狀態轉換的階段，特別注重同儕關係與角色定位，許多研究者認為，青少年是屬於特別的族群，在青春期的時候，人身攻擊的頻率和強度會增加，因此容易被貼上叛逆期的標籤，特別是從小學到國中的階段[5,6]，而教師對於學生的影響力甚大，對於防治網路霸凌居於重要角色。

2.3 網路霸凌防治與九年一貫課程綱要

教育部[7]將資訊教育編列至國民中小學九年一貫課程綱要的重大議題中，亦即學童不只是在電腦與相關軟硬體的知識技能發展，也要具備網路禮節，瞭解相關的使用規範、以及認知不當使用網路後，需要負擔的法律責任，由此可看出資訊科技上的人文素養也是相當重要的一環。九年一貫課綱與資訊素養的相關能力指標中的「5-2-1 能遵守網路使用規範」、「5-3-1 能瞭解網路虛擬特性」，以及「5-3-2 能瞭解與實踐資訊倫理」，均與網路霸凌防制相關，都是為了應用資訊科技提升人文關懷，以及促進團隊和諧。

綜觀以上的文獻，網路霸凌文化和學校教育之資訊素養與倫理都是需要受到重視的議題，目前國內針對網路霸凌的文獻多半在探討青少年的行為調查，較少針對教師、家長面向與學校相關政策的調查。因此，本研究從教師的角度切入探討教師在網路霸凌防制課程實施後的學生反應、教學設計與教學省思。

3. 研究方法

3.1 研究場域與對象

本研究對象為參加網路進修研習課程的中小學在職教師，利用網路學習平台「K12 數位學校」（ds1.k12.edu.tw）進行線上學習。課程名稱為「看不見的拳頭：網路霸凌」，研習目標在於促進中小學教師網路霸凌的認知與素養，以及認識國內外網路霸凌的防治課程，教師亦可透過線上非同步方式進行案例與議題討論。圖 1 為 K12 數位學校的網頁畫面，左邊頁框為課程大綱，教師可點選後，至右方主要頁框閱讀線上教材。

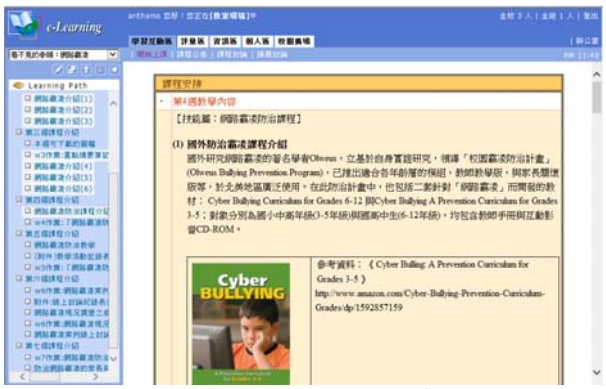


圖 1：K12 數位學校課程畫面

3.2 研究工具與資料蒐集

研習內容主要以觀看線上教材、議題討論、心得撰寫與分享的方式進行網路素養相關議題了解與討論，包括：網路霸凌的認識、網路霸凌防治課程的介紹、網路霸凌的現況調查和案例討論等。開課時間從 2013 年 4 月 8 日至 5 月 31 日，為期八週。調查的方法是本研究者以助教的身分進入系統觀看「網路霸凌防治課程」教學活動記錄表（如圖 2），並依據教師們實際教學後所撰寫之教學活動紀錄表，進一步針對研究問題，進行分類、歸納、比較等內容分析工作。

網路素養與認知教學活動紀錄表

學校：　　教學者：

教案名稱						
教案來源	□自編　□中小學網路素養與認知網站					
教學日期	年　月　日	節數		教學對象	年級:　人數:	
教學流程 (請簡述)						
教學心得	（可針對學生反應、教材設計、教學流程、省思……等方面描述）					
教學相片 或 學生作品	（請掃描後張貼一至二張,檔案請勿過大,謝謝!未有相片或學生作品者不核發研習時數）					

Ps.優秀作品將經過授權後刊登於 eteacher 網站供作觀摩。

圖 2：「網路霸凌防治課程」教學活動記錄表

參與本次研習課程共有 156 位（編號 T001 至 T156）在職教師，而其中有 28 位教師未教授網路霸凌防治課程；7 位教學活動紀錄過於簡陋；2 位教師未繳交教學活動紀錄表。因此，本研究之有效樣本數共 119 份。

4. 研究結果與討論

本節將研究結果分為三部分，第一節為教師知覺到的學生態度，包含班級氣氛、喚醒學生先備知識等；第二節為教師使用之教學設計，包含多媒體的使用及相關教學策略；第三節則呈現教師教學後之省思以及日後可改進之建議。

4.1 教師知覺到的學生態度

4.1.1 學生對於經驗分享的態度

分析結果顯示，共有 12 篇文章提到教室氣氛與學生反應，其中，有 10 篇文中認為學生反應熱烈，其原因在於教師與學生有較佳的互信感，且網路霸凌議題新鮮，許多學生本身或周遭有相符經驗，因此在討論中可以快速聚焦，也願意與其他人分享自身或曾聽聞的經驗。

學生對正式課程外的教學活動相當感興趣，尤其又是屬於學生常會見的網路相關話題。(T006)
學生對影片內容反應熱烈與高度興趣，許多人提到阿泰與阿傑的開玩笑感到生氣，認為他們把自己快樂建立別人痛苦上，另外也有同學認為被害的同學應該告訴家長與老師協助處理，而不是自己一個人痛苦。(T009)

然而，部分教師發現並不是每位學生都可以敞開心胸分享，若是學生有網路霸凌受害的相關經驗，學生可能流於嬉鬧、不願意透漏自身經驗。此時，為了不延伸學生的傷害，教師不須硬性要求學生分享，但並非不加以討論，可以視情況介入，讓學生正視此議題。

對於彼此經驗分享部分，學生較處於被動型式。(T067)
由於不是每位學生都有相關經驗，有時候學生在分享時其他學生，可能會覺得很有趣，反而對當事人造成二次傷害，針對學生同理心的建立需要再加強，教師應視情況隨時介入。(T119)

4.1.2 學生認識霸凌，但對網路霸凌不甚清楚

共有 11 篇文章提到，由於教育部近幾年的宣導與推廣，學生對於霸凌的認知算是熟悉，但在網路霸凌的認識卻非常模糊，且了解的部分也相當片面。

在教育部反霸凌的宣導下，一般學生對於「霸凌」一詞雖然知悉，但是概念上仍然模糊。在實際教學後，發現學生在上課前，對於自己在網路上的行為有些已經達到網路霸凌的情況，其實是一知半解；教學後學生才對自身在網路上的行為會有那些法律責任比較清楚，也有助於學生以後自我約束在網路上的言論或動作。(T014)
每年開學第一週為友善校園週，學生普遍對「霸凌」相當熟悉，但對「網路霸凌」這一區塊則顯陌生，許多學生以為網路是虛擬的，無需對自己的行為負責，也以為不會被抓到…等天真浪漫的想法。(T141)

4.1.3 學生自知法律常識不足

共有 13 篇文章提到，學生對於相關法律知識非常薄弱，而正因為教師開始教導這部分，學生才會開始重視，正所謂學而知不足。除了避免自己觸法，也可以讓受害者保護自己。

而學生對於網路霸凌可能觸犯的法律還頗有興趣，許多人的反應是「沒想到某些自認為無傷大雅的舉動竟已經觸犯法律，而且還挺嚴重的！」再看到確切的罰條時，「觸法」這件事對學生而言不再是那麼抽象，而能感受到嚴重性，除了增加法律常識外，也有嚇阻霸凌者與讓被霸凌者知道如何保護自己的作用。(T097)
剛開始學生都覺得好笑的心情來看待霸凌事件，但最後上到所需負的法律責任及對被霸凌者所產生的一些傷害，態度慢慢感受到事態嚴重，也比較正視這個議題。(T131)

4.2 教學設計

4.2.1 上課使用網路霸凌相關動畫／影片引導

共有 82 篇文章中提到教師使用動畫引起學生的學習動機，並透過影片內容進行討論與引導。這部分的影片多是採用「中小學教師網路素養與認知」網站或是教育部所提供防治霸凌等影片，內容有趣且皆符合學校生活的場景，教師認為影片觀賞可以幫助學生身歷其境，且比播放投影片更可以專注，而教師的角色從講述者轉換為引導者、價值澄清者的角色。

受學生歡迎，因為以學生實際生活為拍攝背景，更能引起共鳴，觀後討論及發表相當踴躍。(T005)
網路世界的發展對於國中而言感受更加深刻，老師們更是經常在處理因為網路而引起的糾紛，因此當看完影片後，很多學生的感受都很像是身歷其境般，因此杜絕網路霸凌是國中生該具備的基本禮儀。(T036)

然而，並非所有教師都認為動畫的加入能完整地達到教學目的，其中教師認為動畫的輕鬆詼諧確實可以吸引學生目光，但學生往往一笑置之，並沒有引導學生的同理心。

網路動畫，更加吸引學生的目光。但是往往在嘻笑之後，對於內容較難引起同理心。(T108)
藉由中小學網路素養與認知網站動畫「誠徵圓圓」的觀賞與探討，讓孩子知道有這些案例的發生，而

大家或許一笑置之，卻不了解其嚴重性；網路的影響層面與速度是超乎大家想像的，希望大家在使用社群網站時更要特別留意。(T109)

4.2.2 以同儕討論方式授課

共有 23 位教師提到，有時不會直接用講述的方式，而是請學生分組討論，特別是探討遇到網路霸凌的因應方式等，利用問題導向式學習引導，教師也會試圖進入討論並統整學生的想法。

分組討論若是發現有人遭受網路霸凌時應該採取的正確行動，各組上台發表，並請其他同學給予回饋。(T020)
各小組將今天討論過的主題與案例彙整，分別提出各小組看法，互相腦力激盪尋求解決或預防網路霸凌之方式，最後交由教師統整。(T116)

4.2.3 以案例教學方式授課

共有 43 位教師使用網路霸凌事件的新聞進行教學，除了讓學生實際了解網路霸凌所帶來的影響不容小覷，也可以分析霸凌者、受害者以及旁觀者等角色的不同特質，幫助學生設身處地體會不同角色的感受，並引發學生進行反思。

透過相關案例，讓學生了解遇到這樣的狀況要如何處理，如何保全證據。第二階段實際經驗論述及新聞相關內容時，較容易引起學生共鳴。(T108)
先以新聞片段引導學生覺察自己周遭存在著網路霸凌現象，再透過活動讓學生體驗關係霸凌中「攻擊者」、「被攻擊者」及「旁觀者」等角色，討論扮演各種角色時的感受，以及這些角色背後形成原因。接著藉由電影片段引導學生思考。(T116)

此部分建議教師若要使用案例教學法時，可以連帶提到相關的道德倫理與法律責任，提供學生更具深度的個案內容。

4.2.4 學生撰寫學習單／自評表

共有 35 位教師利用學習單或自評表的方式，讓學生藉由學習單反思課程中的學習歷程，教師也可以觀看學生的學習程度與自身狀況，除了在未來課堂上依照學生的程度進行調整，也可以觀察自己班上學生網路霸凌的情形後私下輔導。T014 教師請學生利用匿名的方式寫下自身經驗，此方式可以幫助學生更誠實地寫出自身經驗或想法。

利用空白紙條讓學生不記名寫下自己經驗，一方面引導學生自我省思，二方面可由學生分享的經驗，了解目前學生間的網路霸凌現況，作為老師未來輔導學生或是未來教學設計時的參考。(T014)
這次的教學以學生的回饋單來看，算是成功的教學，而且也讓教師知道，只要隨時遇到問題，或者是相關新知，都可以利用彈性課來加強與補充，預防勝於治療，讓學生在網路的世界裡，能夠獲得益處，並且懂得防範與保護自己。(T126)

4.2.5 提供學生口訣式記憶

有 5 位教師利用研習課程中所學的網路霸凌因應口訣「TELL KIDS TELL」(表 1)，由 Agatston、Kowalski 和 Limber 所編製給美國 3-5 年級學生的網路霸凌教材[8]，透過口訣幫助學生牢記面對網路霸凌的因應方式，例如 T060 教師提到，口訣的教導可以幫助學生可以藉由反覆背誦加深印象，也利用簡單的步驟保護自己的安全。

表 1：面對網路霸凌因應口訣及內容

口訣	內容
TELL（告知）	馬上告知你的家人。
Kick them off your friends list（把霸凌者從朋友清單刪除或封鎖）	從你的好友清單中刪除或封鎖散佈不當訊息的霸凌者。
Ignore the message（忽略這則訊息）	你可以檢舉或忽略這則訊息。
Don't respond（不要回應）	不要加入討論、引戰，也不要隨意按「讚」或分享。
Save the evidence（留下證據）	按下鍵盤的 print screen，將霸凌訊息保留下來，或請家人協助，留下證據。
TELL an adult（告訴師長或家人）	若是持續性看到不當訊息，請務必告知老師或家人。

與學生一起討論故事內容，討論霸凌的發生並思考解決方案。使用 ppt 教材「TELL KIDS TELL」，了解並利用簡單六步驟教導學生適時保衛自己。(T060)

由於此部分口訣是以國外教材翻譯而來，對於以中文為母語的學生而言，並不是容易於第一時間就能反應，此部分可以建議教師融入在英語課堂之中做機會教育。

4.2.6 提供學生體驗活動

有 7 位教師自己設計教學的體驗活動，例如角色扮演活動，或是藉由道具體會到霸凌的可怕。此部分的體驗活動以「做中學」為概念，可幫助學生藉由不同方式認識網路霸凌，且可以加深學生對此部分的印象。建議教師可以藉此引導學生的同理心，讓學生可以更深刻地體會到受害者的感受。

透過老師準備的保麗龍球與牙籤來讓學生借物體會感受言語霸凌者的殘酷與受害者的傷痕累累。

（T019）
在狀況模擬情境裡，學生想像力豐富，易於對各種狀況加油添醋，卻由不違背模擬劇的精神，可見國中階段的學生，富有創新與創意。（T096）

4.3 教學省思

4.3.1 課程時間不足

根據內容分析結果可知，有 12 篇文章表示課程內容豐富，難以在一節課（約 40~45 分鐘）的時間將網路霸凌的概念完整詳述，因而教學活動的部分就會被迫縮減，影響品質，期盼學生可以在課餘時間自主學習。

但一節課的時間只能讓他們感受的網路霸凌的存在及可怕，但是對於防治流程沒有實際體驗活動難以執行，所以教學時間宜調整為兩節課。（T074）
由於正式課程有進度上的規劃，因此只能暫時騰出一堂課的時間進行網路霸凌防治的課程，在內容方面，尚未進行到法律的責任，也未如課前預估的能說明開玩笑與霸凌的差異性，只能大約提到當自身對於同學的語言或舉動有不舒服的感受時，能事先向同學表達自身的感受，再觀察同學之後的言行。（T021）

研究者統整教師設計網路霸凌課程所預定花費的時間，由表 2 可知約有 75.63%中小教師只安排一堂課的時間教授網路霸凌課程，其中國小教師裡約 71.25%安排一節課；國高中教師約 84.62%安排一節課教授。可能的原因在於，相較於國中，國小教師較沒有教學進度的問題。因此，建議教師在沒有教學進度的壓力下，可以安排兩節以上的時間會較為充裕。

表 2：國中小教師教授網路霸凌課程所花費的時間

課程進行時間	授課年級		
	國小 1~6	國、高中 7~10	小計（%）
<一堂	1	0	1（0.84）
一堂（40／45 分鐘）	57	33	90（75.63）
兩堂（80／90 分鐘）	16	5	21（17.65）
三堂（120／135 分鐘）	3	1	4（3.36）
四堂（160 分鐘）	2	0	2（1.68）
五堂（200 分鐘）	1	0	1（0.84）
小計	80	39	119（100）

4.3.2 難以用評量方式檢測情意目標

共有 6 篇文章表示，教師反應雖然學生已具備網路霸凌的認知，但實際上行為的表現卻難以利用評量方式查看學生是否達到知行合一。

每年都在上網路素養的課程，感覺當下學生好像都聽進去了。時日久了看看學生的 fb 上的發言，再聽聽學生平日的交談內容，總覺好像不是那麼一回事。教學若流於說教，那講是講你的，要不要聽就由不得了。（T076）

因此，本研究建議教師可以安排相關的教學活動，以及更貼近學生生活的內容，不僅幫助學生產生遷移，也可以更加深學生的印象。其中，常見的活動包含角色扮演、案例教學法等，引導學生建立同理心。

4.3.3 加強家長宣導

共有 5 篇文章提到，教師若要推廣網路霸凌的防治，家長也是居於關鍵角色，亦即學生若有意願將網路霸凌的問題告知教師或家長，家長應該也要具備對網路霸凌基本的認知與相關資訊的協助。

上個禮拜做了霸凌問卷調查，發現如果遇到霸凌問題，學生向師長和父母求助意願頗高，因此我會向輔導主任爭取教師增能研習，或在親師座談會時加入相關議題宣導。（T052）
學校在班親會時，也可以找時間對家長做宣導，以獲得更好效果。（T123）

不同於過去的學者指出，學生反應網路霸凌是一個問題，鮮少的受害者會主動尋求成年人的協助，也沒有看到學校單位對於網路霸凌事件的處理提供相關資源[1]。對於 T052 教師的案例而言，學生會主動求助師長可能的原因在於教師平時就與學生建立互信感，或是具有良好的班級經營。

網路霸凌事件的發生，家長通常是最後知道的，在日常生活中，教師可藉班親會、親師日等機會加強家長對學童網路使用行為的重視，例如家用電腦放置位置、限制上網時間以及網站分級制度等，提供相關資訊與實用技巧，讓學校教育與家庭教育雙管齊下以降低網路霸凌的發生率。

4.3.4 即早建立學生資訊媒體使用的正確觀念

共有 5 篇文章提到，應讓學生即早建立正確使用資訊媒體的觀念，強調網路禮儀與現實生活的禮儀都應當相等重視，讓學生在面對網路上不適當的訊息可以有正確的判斷。

雖然他們離真正學習使用操作電腦的時間尚有一年多，但是能及早教導學生網路的規範與禮儀是絕對必要。（T019）

如何讓他們知道正確的網路禮儀是迫切的，甚至不正確的利用網路來散播謠言或人身攻擊，所需付出的行為結果都須知道，不可心存僥倖或以為網路是可以隱蔽的，並能夠知道保護自己及求救。(T034)

5. 結論與建議

本研究使用內容分析法，實際分析中小學教師教授網路霸凌課程之情況。研究問題一為探討中小學教師教授防治網路霸凌課程後的學生反應。其中，大部分學生願意正視網路霸凌的議題，但仍有少部分學生輕忽網路霸凌所帶來的嚴重性與法律常識。建議教師在面對網路霸凌的課程時，務必要注意班級氣氛的經營與內容範圍。本研究之多數教師選用影片或是動畫以引起學生動機，因為影片本身豐富有趣，且貼近學生生活，是合宜的教材。然而，某部分教師反應學生往往一笑置之，似乎並未從影片中獲得啟示與同理心。此部分建議教師在班級氣氛必須掌握得宜，避免 copycat（學生不以為意，而加以模仿）的情形發生。

研究問題二為探討中小學教師在網路霸凌防治課程的教學設計。建議教師將課程使用在中低年級時調整教學內容，避免使用過多艱深的詞語，而造成學生更不易理解。另外，部分教師使用體驗的方式讓學生體會受害者的感受，若是體驗活動較為隱喻，建議教師可以在最後幫助學生進行引導反思，統整學生的分享後，補充不足的部分。

研究問題三為探討中小學教師對於網路霸凌防治課程的教學省思。除了教師在課堂上加強學生對於網路霸凌的認知之外，家長的親子教育也居於重要地位。過去研究指出，網路霸凌是不受空間限制，且發生的地點多是在校外或是家裡，因此，教師跟家長之間應保持良好互信關係。除此之外，教師也可以藉此檢視學校資源，例如校園宣導、行政支持和學校的輔導機制等。建議教師可在學期初期安排一週為友善校園週等活動進行宣導，也可以和學校輔導老師互相討論如何因應校園網路霸凌事件，即使發生了網路霸凌，也可以及時地給予學生妥善的處理方式。

本研究提出以上建議，期盼可提供未來欲教導該主題的教師在教學實務上之增進，以及致力於校園間推廣的行政人員酌以參照。

6. 研究限制與未來發展

本研究使用內容分析法，分析教師之教學活動紀錄表，以了解教師們的教學狀況，由於內容為教師自行撰寫，因此難以看出實際的成效，若未來有相關主題之研究，可讓學生填寫評量與問卷，以測得實際的教學成效與課程滿意度。

另外，也可抽樣部分教師進行課堂觀察與深度訪談，輔以研究者更多面向分析並加以佐證，讓研究結果更加完善。

參考文獻

[1] Agatston, P.W., Kowalski, R. M., & Limber, S. P. (2007). Students' perspectives on cyber bullying. *Journal of Adolescent Health*, 41(6), S59-S60.

[2] Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2008). *Cyber Bullying*. Malden: Blackwell.

[3] Hinduja, S, & Patchin, J. W. (2008). Bullying beyond the schoolyard: Preventing and responding to cyberbulling Thousand Oaks, CA: Corwin Press.

[4] 吳明隆、簡妙如 （2009）。青少年網路霸凌行為探究。**中等教育，60** （3），90-109。

[5] Kwan, G. C. E., & Skoric, M. M. (2013). Facebook bullying: An extension of battles in school. *Computers in Human Behavior, 29*, 16-25.

[6] Perren, S., & Gutzwiller-Helfenfinger, E. (2012). Cyberbullying and traditional bullying in adolescence: Differential roles of moral disengagement, moral emotions, and moral values. *European Journal of Developmental Psychology*, *9*(2), 195-209.

[7] 教育部（2012）。**國民中小學九年一貫課程綱要重大議題**。台北市：教育部。

[8] Agatston, P. W., Kowalski, R. M., & Limber, S. P. (2009). *Cyber Bullying: A Prevention Curriculum for Grades 3-5*. Minnesota: Hazelden.

海洋污染防治管理系統 App 軟體之建置

游哲凱　　羅榮華
佛光大學資訊應用學系
992751@mail.fgu.edu.tw
jhlo@mail.fgu.edu.tw

摘要

「海洋污染防治管理系統 App 軟體」(Marine Pollution Prevention System App，以下簡稱本 App 軟體)，當海洋及河川污染事件發生油污及化學品溢漏事件時，需要把握黃金時間進行應變及處理，以避免油污及化學品的溢漏及污染擴大，故在第一時間將污染事件的狀況掌握極其重要。有鑑於此，本研究為了使海洋污染防治管理系統能便於在各種污染事件發生時，可以在應變人員到達現場後利用行動通訊設備，即時通報各項事件現場狀況的資訊或查詢附近的資材分布，將海洋污染及河川污染事件發生油污或化學品溢漏的即時狀況發布至海洋污染防治管理系統，讓行政院環境保護署(以下簡稱環保署)長官能即時掌握海洋污染及河川污染事件現場發生的情形，在最短時間內做適當的決策，下達正確的支援及調度。

關鍵詞：行動裝置開發(Mobile Device Development)、網際網路服務(Web Service)、海洋污染防治管理系統(Marine Pollution Prevention System)。

1. 前言

行政院環境保護署(以下簡稱環保署)於 90 年開始分階段建置「海洋污染防治管理系統(以下簡稱海污系統，網址為http://ocean.epa.gov.tw/)」，經由近 10 年的努力，現今的海污系統包含著大大小小近 700 件的海洋污染通報案件資料，也陸續整合污染應變資材、模擬及水質監測等資料或資訊，以供海洋污染應變使用，有效的管理、掌握、防止、排除並減輕海洋相關污染，為我國海洋污染防治業務上增添不少功績。

然隨著在時代變遷，資訊科技不斷進步，行動通訊技術不斷提升的情形下，資訊的方便性、時效性、正確性、完整性等需求的渴望，各種針對海洋污染防治及應變資源等相關的行動通訊需求也隨之接踵而來。海洋污染發生現場由於現場環境惡劣，除無法將現場狀況、照片等相關資訊立即通報外，海洋污染應變急需的應變資材資訊，也無法掌握，資材資源的規格、數量以及分布也無從得知，有鑑於此，本研究建置「海洋污染防治管理系統 App 軟體」(Marine Pollution Prevention System，以下簡稱 App 軟體)，系在讓應變人員能在海洋污染發生的現場，不管環境多惡劣都能把現場狀況及相關資訊立即通報，查詢最近資材資源所在位置。



圖 1-1 海洋污染防治管理系統主要元素示意圖

2. 系統規劃與設計

本 App 軟體著重在應變人員所需的兩大項功能：污染事件的通報與資材資源查詢。污染事件通報功能為相關應變人員抵達現場時，可以使用裝有本 App 軟體的行動通報相關設備，設備本身的相機及 GPS 定位功能可以在第一時間將現場位置、畫面及事件狀況，利用本 App 通報功能簡單的幾個步驟將污染事件通報給上級單位；資材查詢功能則是提供應變人員在掌握事件當下的狀況後，需要進一步

調度應變資材時，能在最短時間內找尋到其所需且距離該污染事件發生地最近的應變資材，並撥打電話聯絡調度。

2.1 App 軟體整體功能流程

由於海洋污染事件通報作業與河川污染事件通報作業的作業目的是在減少已發生事件的污染範圍及降低其影響性，並啟動對應的應變機制，為減少使用者應用上的學習，海洋及河川污染通報的方式及流程採用相同的設計概念，以利需要通報海洋及河川污染事件機關的推展。海洋事件通報以及河川事件通報以首報為例，其主要流程為填寫事件基本資料，以及利用行動通報的相關設備的照相及 GPS 功能，將事件現場狀況及照片依其發生地點記錄在首報中。

資材查詢則以資材的 10 大分類為主搜尋模式，在搜尋到所需資材後，系統會依據使用者所在位置做距離的運算，將搜尋到的資材依儲存場所位置的距離由近到遠列表，還包含資材格規及數量，並提供該資材所屬單位的聯絡人資料，讓使用者可即時撥打電話聯絡調度。查詢出來的資材資料還另外提供空間分布圖，讓使用者對附近的資材資源位置瞭若指掌。

依據前述所需開發的 App 需求，規劃其功能流程如圖 2.1-1 所示，海洋以及河川的作業及功能整體流程是相同的，但因其通報的項目不同，在實際通報系統設計時，仍必須依其特性分為海洋及河川通報功能，故本 App 軟體分為海洋事件通報、河川事件通報及資材查詢 3 大部分。

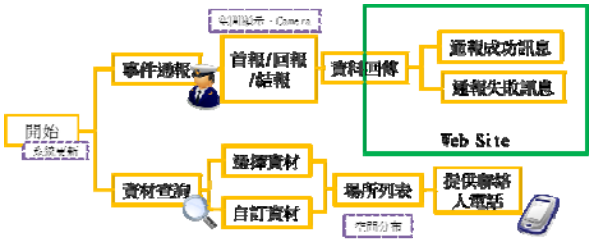


圖 2.1-1 App 功能流程示意

2.2 污染事件通報

污染事件通報功能乃是海洋污染防治系統中最基本且重要的工作，故本研究建置的 App 軟體功能首要重點工作即是污染事件通報功能的建置。系統通報作業分為 3 個階段，分別為「首報」、「回報」、「結報」，其關係如圖 2.2-1 所示。事件的「首報」的作業僅有 1 次，負責應變的單位必須立即進行通報；在首報作業完成後，相關應變單位也持續進行後續的應變及處理作業，每次處理完畢後必須上網進行「回報」的通報作業，故回報作業在系統設計上是可以多次性回報的，相關單位均可以利用系統進行各階段的通報作業；待整體事件處理完畢後，則上網進行「結報」的通報作業，用以描述本事件的最後處理結果。

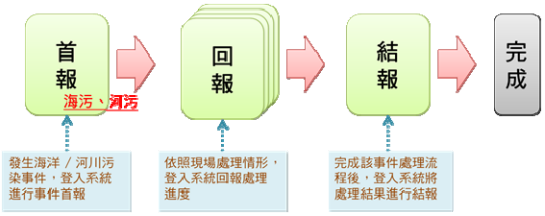


圖 2.2-1 線上系統污染事件通報流程

2.2.1 污染事件通報功能選擇介紹

在本 App 軟體中海洋以及河川事件通報方面和線上系統相同分為首報、回報和結報 3 項功能，在使用者點選海洋或河川事件通報後，系統將導引使用者進入通報功能，此時，系統提供「首報」、「回報」及「結報」3 項不同階段的功能選項，各階段的通報內容不完全相同如圖 2.2-2 所示的作業功能流程，用以設計各階段的通報功能。

在首報的通報階段，應變人員第一時間到達該事件地點時，填寫事件相關訊息，利用行動通報相關設備的定位及照相功能，將事件位置定位並提供拍攝畫面上傳至線上系統的功能；在回報處理的通報階段，相關應變單位每次進行應變處理作業完畢

後填寫相關作業內容，在結報處理的通報階段，則由應變單位確認事件處理結束後，利用系統進行事件「結報」的上網通報作業。

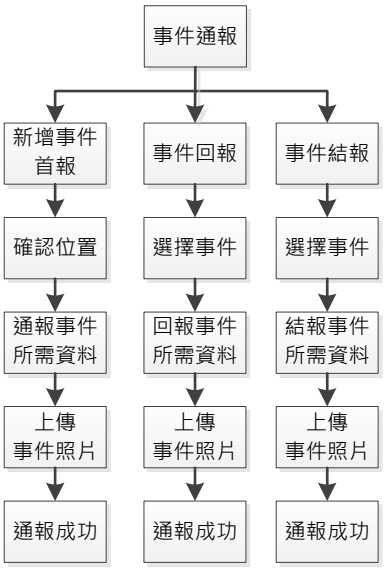


圖 2.2-2 應用程式設計流程圖

2.2.2 污染事件首報功能規劃

在首報的通報作業中，現場通報人員可以迅速提供的重點資訊包括：事件描述、事件照片以及事件地點等 3 項內容，系統的通報畫面如圖 2.2-3 所示，(1)為事件定位功能、(2)為事件描述、(3)為事件相片上傳功能。



圖 2.2-3 事件通報三大功能

2.2.3 資材查詢功能設計

各機關建立旗下的資材資料，不僅為了管理自身的資材數量，更進一步地是要提供跨部會或相關機關的查詢，以利環保署及各機關了解全國各類資材的內容及數量所在。海洋污染事件發生時，若應變人員所在機關的資材不夠需要調度其他部會機關的應變資材，本 App 軟體提供資材查詢功能，以便利使用者可以在最短時間內搜尋到距離自己最近的應變資材，並快速地進行資材調用的聯絡事宜設計。資材查詢系統介面，如圖 2.2-4 所示。



圖 2.2-4 資材查詢設計示意圖

3. 系統功能與運作

本 App 是利用 Phonegap 框架加上 html5、Javascript 及 CSS3 來建置 Android App 軟體，並提供下列功能：

(1)污染事件通報。
(2)提供相關空間資訊。
(3)提供污染現場照片傳輸功能。
(4)提供相關應變資材查詢。
(5)包括首報、回報以及結報等階段的通報作業。
(7)提供通報資料自動資料回傳功能。
(8)提供通報上傳狀況訊息。

3.1 系統功能架構

本 App 軟體，系利用手機本身所附載的 GPS 定位以及照相功能，在有網路訊號下，將海洋污染及河川污染通報資訊加上衛星定位資料以及現場拍攝圖片利用網際網路服務(Web Service)，以 JSON 資料交換格式與海洋污染防治管理系統做資料交換，

即時把現場位置、通報資料及現場畫面通至海洋污染防治管理系統，如圖 3.1-1 所示。

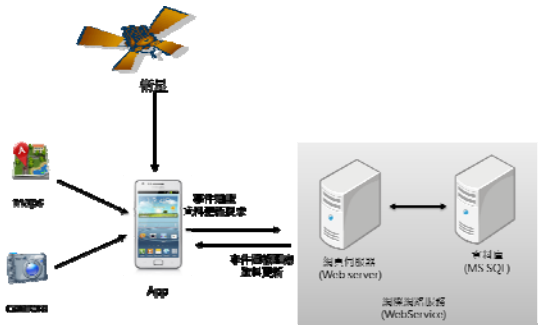


圖 3.1-1 系統架構示意圖

本 App 軟體除了主要的海洋污染及河川污染通報外，還設計了資材查詢功能，使應變人員得以在現在查詢到附近的資材資源，找到距離現場最近的資材資源，本 App 軟體所有功能，如圖 3.1-2 所示。

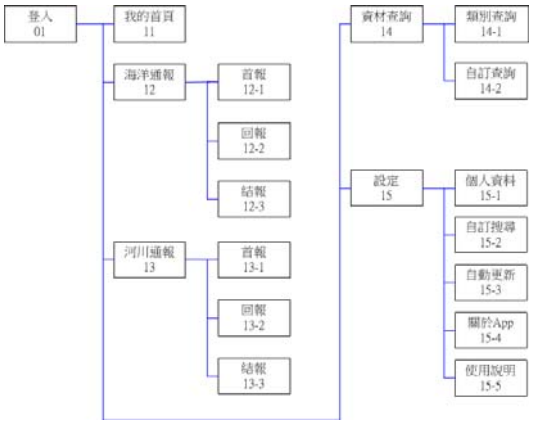


圖 3.1-2 功能架構圖

3.2 通報上傳運作模式

在本 App 軟體裡，所有通報上傳功能的運作模式，如圖 3.2-1。在海洋污染及河川污染通報的首報時，必須要在有網路訊號的情形下才能通報，回報及結報則無此限制，回報及結報如果在無網路訊號的情形下，本 App 軟體會將資料暫時儲存在手機內部，定時偵測網路訊號，偵測到有網路訊號，立即上傳通報資料。

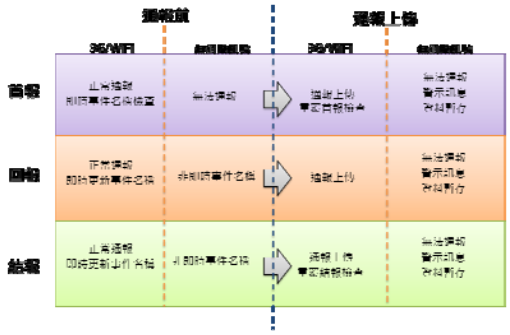


圖 3.2-1 通報上傳運作模式

3.3 事件定位功能

首先利用行動通報相關設備進行事件發生地點的標註，讓環保署應變業務負責人員能明確得知事件發生地點，提供快速應變與支援設備的投入，事件定位功能如圖 3.2-2 所示。



圖 3.2-2 事件定位功能

3.3.1 事件描述

在海洋及河川污染事件通報處理過程中，當務之急是進行事件狀況的應變處理，而填寫通報資料則是為了讓支援的相關單位能在短時間內了解現場狀況，使後續應變更為順利；事件描述的介面如圖 3.2-3 所示。

3.3.2 事件相片上傳功能

海洋污染通報的「首報」、「回報」和「結報」均設計上傳照片的功能，上傳照片分為處理前、中、後三個部分；在點上傳的功能鍵後，系統會開啟相機功能，讓使用者拍攝現場照片，拍攝完會顯示縮圖在通報頁面上。



圖 3.2-3 海洋通報首報之事件描述功能



圖 3.2-4 海洋通報首報之照相功能

3.4 搜尋功能規劃

資材查詢功能設計首重搜尋功能，以便提供使用者快速查到所需的資材設備項目，以及標示資材設備的所屬機關以及所在位置；本 App 軟體提供兩種資材查詢方式：資材類別查詢功能、自訂查詢功能。

3.4.1 資材分類查詢功能

資材的分類查詢功能主要是將資材分為攔油設備、吸附設備、儲存設備、除油設備、防護設備、海上運輸、陸上運輸、監測設備、通訊蒐證、以及其他設備共十大類；使用者可以依據此分類搜尋到所需資材，其系統設計畫面如圖 3.3-1 所示。



圖 3.3-1 資材查詢之資材分類搜尋功能

3.4.2 自訂查詢功能

在應變現場面臨要處理多項作業的狀況下，除了提供前述的資材分類查詢功能讓使用者依類別選擇及調閱各項資材，另一方面，在查詢方式的設計上，系統至少應再提供資材設備關鍵字查詢的功能，提供使用者可以直接設定常用的資材關鍵字後，由系統自動搜尋與使用者距離最近的資材清單，如圖 3.3-2 所示。



圖 3.3-2 自訂查詢畫面

3.5 資材查詢結果的呈現規劃

資材查詢結果的呈現上，本工作團隊的規劃重點在於如何讓使用者在行動通訊設備上，可以容易地閱覽資材的內容、掌握資材的分布、以及調閱資材所屬單位的聯絡資料，規劃概念如下面小節。

3.5.1 結合資材的分布概念的設計

不論使用者使用前述哪種搜尋方式來查詢資材資料，本 App 軟體將主動結合空間距離的概念來呈現系統的搜尋結果；查詢結果的呈現以資材所在的儲存場所與使用者所在位置間的距離為排序條件，呈現的順序以近到遠的距離來展現資材搜尋的結果。

3.5.2 提供容易閱覽資材搜尋結果的設計

系統設計提供「場所列表」及「空間分布」兩種設計方式來呈現資材的搜尋結果，「場所列表」可以清楚地將搜尋結果列出，呈現資材設備的所在位置、地址、數量、以及資材位置與使用者的距離；「空間分布」則可結合空間地理資訊，呈現資材分布的狀況。呈現方式如圖 3.4-1 所示。



圖 3.4-1 資材查詢之結果列表與分布



圖 3.4-2 資材查詢之聯絡方式

3.5.3 串接資材所屬單位的聯絡資料

使用者查詢資材的主要目的是希望在緊急狀況下可以了解哪些地方會有現場需要的資材設備，以便可以立即連絡取得資源，在此刻，資材所屬單位的聯絡資訊就顯得格外重要；在資材資料下方還提供資材所屬單位的聯絡方式，使用者可以直接對資材聯絡人進行撥號聯絡，減少使用者再次找尋電話資料的時間。

4. 結論與未來展望

在資訊的方便性、時效性、正確性、完整性等需求的渴望，在時代變遷，資訊科技不斷進步，行動通訊技術不斷提升的情形下，應變人員只要在污染現場，手持智慧型手機下載 App，就能即時上傳現場情形讓環保署長官知道現場狀況，並下達支援調度的指令，讓台灣寶貴的海洋資源不至於被污染給破壞。未來可以往地圖功能發展，可以將定位的功能再做提升，可以定位污染發生地點及污染範圍。

5. 致謝

本研究承蒙國科會（ 計畫編號：NSC100-2221-E-431 -002）及佛光大學「行動式旅遊導覽平台建置」專題計畫經費贊助，方達科技股份有限公司提供「海洋污染防治管理系統」之究研所需相關資料，使本研究得以順利完成，謹此致謝。

參考文獻

[1] “海洋污染防治法”,中華民國環保法規資料中心, http://law.epa.gov.tw/zh-tw/laws/759702163.html .

[2] “環保署海洋污染防治管理系統”,環保署, http://ocean.epa.gov.tw .

[3] 程榮祥、楊智鈞”植基於 Android 結合 GPS 與 Google 電子地圖開發的速度警示 App”, 崑山科技大學電腦與通訊研究所論文,2012

[4] 程榮祥、潘郁仁、林家鵬,”在 Android 系統上以 Google 電子地圖實作之手機定位 App”,崑山科技大學電腦與通訊研究所論文

[5] 鄉田 MARI 子、宅間俊志、近藤昭雄,”打卡還不簡單？APP 地圖定位模組設計實例”,PCuSER 電腦人文化,2012

[6] 黃崇明、盧尚群, ”適地性行動應用網路與數位內容製作技術”,易習圖書,2011

[7] 陳祥文、陳英一,” 以 PhoneGap 技術開發跨平台行動應用之研究”, 國立臺北科技大學資訊工程系研究所論文,2012

在 BSN 網路上建立與重組可靠反向路由樹的機制

蕭智仁　　許蒼嶺
電腦通訊網路實驗室
國立中山大學電機工程學系
sheu@ee.nsysu.edu.tw

摘要

本論文在人體感測網路(Body Sensor Networks, BSN)上建立與重組可靠的反向路由樹(Reversed Routing Tree, RRT)的機制，此一反向路由樹有兩個優點，一為使用 multi-hop 的樹狀架構去取代傳統的 one-hop 星狀架構以減少封包的碰撞機率，二為在選擇路徑時考慮到連線品質(Link Quality Indicator, LQI)可以讓封包遺失的比率(Packet Loss Ratio, PLR)降低。另外，我們建立的 RRT 可以針對人體姿勢的突然改變進行重組，使得移動位置的 sensor node 得以重新加入新的父節點，以顯著的減少 PLR。

關鍵詞：LQI 、BSN、PLR、碰撞、反向路由樹。

Abstract

This paper constructs a reconfigurable and reliable reversed-routing tree (RRT). There are two purposes of building the RRT: (i) to avoid packet collisions, we use multi-hop tree structure to replace traditional single-hop star structure; (ii) to reduce packet loss ratio (PLR), the RRT selects the routes based on the link quality indicator (LQI). Additionally, once there is a sudden human movement, the RRT can reconfigure itself such that a moving sensor node will re-connect to another parent node, which reduces PLR significantly.

Keywords: LQI、BSN、PLR、collision、RRT.

1. 前言

近年來人體感測網路(Body Sensor Network, BSN)已經開始蓬勃發展，而 BSN 網路的應用遍及了運動員的訓練、病人的看護、老年人的照料等等，因此藉由在人體上裝置 sensors 來收集各種資訊，例如心電圖(ECG)、肌電圖(EEG)、血壓等，由於這些資料都是與老人、病人的身體健康息息相關，所以降低 sensor nodes 收集資料的出錯機率也成為了一個重要課題。

2. 人體感測網路

2.1 IEEE 802.15.6

IEEE 802.15.6 [1]於 2007 年時便被提出討論，直到 2012 年才終於制定這項通訊標準，此標準是針對於人體周邊及人體內部的通訊協定，它的應用包括醫療、個人娛樂、消費電子等，而 IEEE 802.15.6 定義最遠為 3 公尺的工作範圍，最高可以達到 10 Mbps 的傳輸速率，它也提供 QoS 的功能。

2.2 BSN 拓樸

BSN 網路的拓樸約有 3 種：星狀(star)、網狀(mesh)、樹狀(tree)，而本論文針對樹狀拓樸來做研究，其中樹狀拓樸可分為兩種：正向路由樹(Forwarded Routing Tree, FRT)與反向路由樹(Reversed Routing Tree, RRT)，在樹狀拓樸中一般是由 root 開始往其他節點一圈一圈的建立一棵樹，每一圈在樹狀拓樸中稱為深度(depth)，正向路由樹是資料流傳送的方向與建立樹的方向相同；而反向路由樹是資料流傳送的方向與建立樹的方向相反，因為在 BSN 網路中有個特性，就是 sensors 收集資料後會將這些資料傳送給 hub ，所以必須採用反向路由樹，在 BSN 中我們考慮資料傳送路徑的連線品質，其目的是傳送資料時，能減少封包的遺失或是錯誤，因此建立反向路由樹時，我們必須收集周圍 sensors 的連線品質，然後依據連線品質建立反向路由樹，所以會增加建樹的 overhead 與 complexity。

2.3 相關研究

BSN 建立樹狀拓樸的研究主要都集中在如何建立路由協定，在建立路由協定時必須考慮網路的可靠度、減少封包的碰撞、省電、身體姿勢的改變等，與網路可靠度相關的協定，例如 H. Chebbo 等人[2]提出 Restricted Tree Topology (RTT)，RTT 修改了 MAC frame 格式，在 frame control 加入 relaying flag 表示拓樸圖為星狀或樹狀，建立樹狀拓樸是根據 node 連線期間 ACK 訊息遺失的情況選擇出 relaying node。在減少碰撞相關的協定有如 R. Annur 等人[3]提出應用樹演算法，此演算法將 BSN 網路的 sensor nodes 依據優先權先建立一棵選擇樹，sensor nodes 在樹中的位置都代表著競爭通道的優先權，而在樹中同一深度的 sensor nodes 其優先權高低是由左往右遞減，因此在最左邊的 sensor nodes 可以優先傳送資料，作者利用此優先權的方法減少碰撞的發生。

最後在 BSN 網路上，因為身體姿勢改變而提出的通訊協定有 2 篇，第一篇是 M. Quwaider 等人

[4] 提出的 On-body Store and Flood Routing (OBSFR)，它會在 sensor node 傳資料時，檢查目前的身體姿勢下有哪些鄰近 sensor nodes，並且選擇一個離 sink 最近的 sensor node，若沒有便先將資料暫存於 sensor node，當身體姿勢改變後，sensor node 有找到距離 sink 較近的 sensor node 時再傳送資料，最後作者使用嵌入式系統做實驗，從實驗結果發現，OBSFR 與現有的 probabilistic 路由協定比較，OBSFR 有比較小的 routing delay；第二篇是由 C. H. Wu 等人[5]所提出，他們的方法是去建立一個最小成本的路由樹，此方法是讓一個 sensor node 去 overhear 鄰近 sensor nodes 的資料傳輸，接著此 sensor node 會計算自己收集的資料與鄰近 sensor nodes 收集的資料的相似度，並將資料的相似度當作建立路由樹的成本，而資料的相似度越高則代表成本越小，然後為了傳輸每個 sensor node 所收集的資料，作者使用 Kruskal algorithm 建立一棵最小成本的路由樹。

3. 可靠的反向路由樹的建立與重組

在本章節中我們提出一個可靠的反向路由樹(reversed-routing tree)協定，因為我們建立樹的方向與資料傳送的方向相反，所以會增加建立樹的複雜度，此反向路由樹協定以 Link quality indicator (LQI)為基礎建立一棵樹，並且樹中的父節點會周期性地檢查自己與子節點的 LQI，然後適時地動態重組反向路由樹的結構，其目的是為了在 Body Sensor Network (BSN)網路傳送資料時，能夠減少封包的遺失以及降低封包的錯誤率。在本章節中我們會先介紹反向路由樹的系統架構，然後介紹我們如何設計反向路由樹協定。

3.1 反向路由樹系統架構

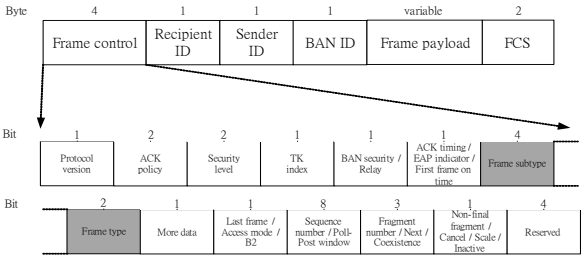
圖 1 BSN 的架構

如圖 1 所示，BSN 網路是由一個 hub、數個 sensors、外部的 sensor 以及個人電腦所組成，而 BSN 網路是以 IEEE 802.15.6 為通訊協定，如果醫生想要收集病患的健康資訊，例如 ECG、EEG、體溫、血壓…等，醫生會藉由個人電腦發出蒐集身體資訊的要求，當 hub 收到這個要求後，它會通知人體上的 sensors 開始收集此資料，並且 sensors 會將收集到的資料傳回給 hub，最後 hub 再將這些資料傳送給醫生的個人電腦，如此一來醫生便可以由這些資料判斷病患的身體情況。

3.2 反向路由樹協定

於 BSN 網路中，sensors 收集資料後，它們都是朝 hub 傳送，所以我們希望傳送的路徑都有好的 LQI，以確保封包不會遺失或出錯。我們建立一棵以 hub 為 root 的樹，然後樹中的父節點會周期性檢查子節點的 LQI，如果當子節點的 LQI 小於預設的 LQI threshold (LQI_TH)時，父節點會通知子節點要另尋新的父節點，如此可以動態重組反向路由樹(RRT)，以確保傳送路徑的連線品質。

於 IEEE 802.15.6 中我們新增了 8 個反向路由樹協定的控制封包，如圖 2，我們在 frame control 欄位中的 frame type 新增一個 RRT 的類別，然後在 RRT 類別下，我們在 frame subtype 欄位新加入 8 個 RRT 的控制封包，分別是：Build_Tree_Request (BTREQ)、Build_Tree_Reply (BTREP)、Parent_Selection (PS)、Member_Notification (MN)、Periodical_LQI_Measurement (PLM)、Bad_LQI (BL)、Joint_Request (JREQ)、Joint_Reply (JREP)，而它們對應的 frame subtype value 為 0000 到 0111，其中 MN 與 JREP 的 frame payload 中會紀錄 8-bit ΔLQI。



Frame type value	Frame type name
00	Management
01	Control
10	Data
11	RRT

Frame subtype value	Control packet name
0000	BTREQ
0001	BTREP
0010	PS
0011	MN
0100	PLM
0101	BL
0110	JREQ
0111	JREP
1000- 1111	Reserved

圖 2 MAC frame 中新增的控制封包

3.3 建立反向路由樹演算法

圖 3 為建立反向路由樹的演算法，首先 hub 會廣播 BTREQ 封包給鄰近 sensors，當鄰近 sensors 收到 BTREQ 時，如果它們已經是反向路由樹的節點，那那麼就會將封包丟棄，但如果它們不是反向路由樹的節點，則會回應 BTREP 封包。

如圖 4，當 S_i 收到 S_j 發送的 BTREP 封包時，S_i 會量測 LQI 值，並且判斷此 LQI 值是否大於 LQI_TH，如果大於，則 S_i 會送出 MN 封包給 S_j。接著如果 S_i 收到 MN 封包時，若 MN 是由 hub 發送的，則 S_i 會將

hub 設為父節點，然後送回 PS 封包給 hub，接著廣播 BTREQ 封包，最後它會周期性地傳送 PLM 封包給 hub；若當S_i收到非 hub 傳送的 MN 封包，S_i會在第一次收到 MN 封包時，紀錄下 MN 封包中的ΔLQI，並暫時將 MN 封包的發送端設為父節點，如果S_i非第一次收到 MN 封包，它會比較前一次的ΔLQI是否小於該封包的ΔLQI，若小於，那麼S_i便會更新父節點，但是如果前一次的ΔLQI 與該封包的ΔLQI相等時，S_i便會從具有相同ΔLQI的 sensors 中任意挑選一個 sensor 作為父節點，當確定了父節點後，S_i會送出 PS 封包通知父節點，接著S_i會周期性地傳送 PLM 封包給父節點，最後S_i繼續廣播 BTREQ 封包尋找下一個深度的子節點。

```
//At first, the hub broadcasts BTREQ.
If  Si  receives BTREQ from  Sj
      If  Si  is a tree member, it drops BTREQ.
      Else  Si  responses BTREP.

If  Si  receives BTREP from  Sj  , measures LQI.
      If  Sj_LQI > LQI_TH
            Si  sends MN to  Sj
      Else return

If  Si  receives MN
      If MN is from the hub
            Si  set the hub as parent
            Send PS to the coordinator
            Broadcast BTREQ
            Send  PLM  message  to  the  hub
      periodically
            Return
      Else          // MN is not from the hub
           If the first reception of MN
            PREV_ΔLQI  = MN_ΔLQI
            Set MN_SOURCE as parent
      Else
            If MN_ΔLQI  > PREV_ΔLQI
                  PREV_ΔLQI  = MN_ΔLQI
                  Set MN_SOURCE as parent
            If MN_ΔLQI  == PREV_ΔLQI
                  Randomly  choose  a  sensor  as
      parent
            //Parent has been chosen
            Send PS to  Si_parent
            Send PLM to  Si_parent  periodically
Broadcast BTREQ
```

圖 3 建立反向路由樹演算法

3.4 動態重組反向路由樹的演算法

圖 4 是動態重組反向路由樹的演算法，在演算法中，我們分成兩種情況來處理，分別為 sensor 是反向路由樹的成員以及非反向路由樹的成員，當S_i為反向路由樹的成員且為父節點時，S_i會收到由它的子節點S_j發送 PLM 封包，並且S_i會量測 LQI 值，如果此 LQI 值小於 LQI_TH，那麼S_i會送出 BL 封包通知子節點S_j，當子節點S_j收到 BL 封包後，它會廣播 JREQ 封包，並且進入重組反向路由樹(RECONSTRUCTION)的步驟；另一個情況是S_i為非反向路由樹的成員，當S_i已經收集好資料欲傳送時，它卻發現自己沒有父節點，於是S_i會廣播 JREQ 封包，然後進入重組反向路由樹的步驟。

最後介紹如何重組反向路由樹，當S_i接收到來自S_j的 JREQ 封包，而S_i會回覆 JREP 給S_j，當S_j第一次接收到 JREP 封包時，它會記錄下 JREP 封包中ΔLQI欄位的數值，並且S_j會先將S_i選為父節點，如果S_j非初次收到 JREP 封包時，它會比較前次記錄的ΔLQI與目前 JREP 封包的ΔLQI，如果目前的 JREP 封包的ΔLQI比較大時，S_j會記錄下目前 JREP 封包的ΔLQI，然後更新父節點為S_i，但是如果前次記錄的ΔLQI與目前 JREP 封包的ΔLQI相等時，S_j便會隨機挑選具有相同ΔLQI值的 sensors 為父節點，最後確定了新的父節點後，S_j就會送出 PS 封包給新的父節點，其用意是跟新的父節點講S_j為它的子節點，然後S_j會開始周期性地傳送 PLM 封包給新的父節點。

```
Tree member:
      // Si  is  Sj's  parent.
      If  Si  receives PLM message from  Sj
        If  Sj_LQI  < LQI_TH
            Si  sends BL message to  Sj
      If  Sj  receives BL message
        Broadcast JREQ   //Find a new parent.
        Go to RECONSTRUCTION()

Non Tree member:
   //When  Si  collects  data  and  is  ready  to
transmit.
   Si  found itself has no parent
      //After  the  construction  of
      //reversed-routing tree, some sensors not
      //in the tree.
      Broadcast JREQ        //Find a parent
      Go to RECONSTRUCTION()

RECONSTRUCTION:
  If  Sireceives JREQ from  Sj
    Si  responses JREP to  Sj
  If  Sj  receives JREP from  Si
    If the first reception of JREP
      PREV_ΔLQI  = JREP_ΔLQI
      Set  Si  as parent
    Else
      If PREV_ΔLQI  < JREP_ΔLQI
        PREV_ΔLQI  = JREP_ΔLQI
        Set  Si  as parent
      If PREV_ΔLQI  == JREP_ΔLQI
        Randomly choose a sensor as parent
  Send PS              //Send  PS  to  the  new
                       //parent.
  Send PLM periodically
```

圖 4 動態重組反向路由樹演算法

4. 模擬與分析

為了要分析使用反向路由樹建立 BSN 網路的效能，我們使用網路模擬器 NS-2，因為 NS-2 目前並沒有提供 IEEE 802.15.6 的功能，所以我們選擇 NS-2 有提供的 IEEE 802.15.4 當作 sensor nodes 之間的通訊協定。在本章節中，我們會先介紹 NS-2 的模擬環境，然後對模擬的結果進行分析討論。

4.1 模擬環境

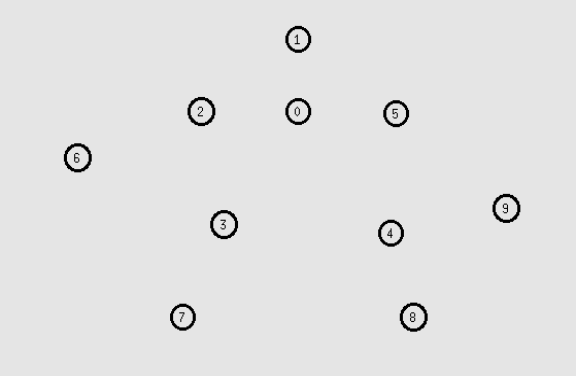


圖 5 使用 NS-2 建立的反向路由樹

圖 5 為我們使用 NS-2 所建立的人體感測網路(BSN)，我們建立的 BSN 有 10 個 sensor nodes，其中編號 0 的 sensor node 為 hub，其他的 sensor nodes 會以不同的速率(從 0.8 Kbps 增加到 4.8 Kbps)收集資料，sensor nodes 將收集的資料依照反向路由樹(RRT)的拓樸傳送給 hub。在我們建立的 RRT 拓樸中，sensor node ID=1, 2, 3, 4, 5 的只需要 1 個 hop 就可以送到 hub，然而 sensor node ID=6, 7, 8, 9 的卻需要 2 個 hops 才可以傳送至 hub。

為了簡單起見，我們在模擬 BSN 中人體各部位可能會移動的情境，只考慮到手的抬高，例如圖 6 中的 sensor node ID=9 會從 sensor node ID=5 的下方位置移動到 sensor node ID=5 的上方位置。表 1 為我們在 NS-2 中所設定的模擬參數。

4.2 模擬程式的架構

圖 6 是 NS-2 的物件架構，白色區塊是 NS-2 原來就有的模組，灰色區塊 RRT 則是我們新加入 NS-2 的模組。TclObject 是用來連結 C++與 Tcl 的程式；NsObject 繼承 TclObject，它為所有基本網路組件的父類別，而繼承 NsObject 的子類別能做參數傳遞給 Scheduler 來排程處理；Biconnector 類別具有承上啟下的作用，可以連接網路層與 MAC 層，它擁有連結網路層和 MAC 層的指標: uptarget 與 downtarget，藉由這兩個指標可以快速的找到網路層和 MAC 層的物件；MAC 類別繼承 Biconnector 類別，MAC 類別中描述基本的 MAC 功能，然後再衍生出不同的 MAC 協定，例如圖 6 中的 Mac802_15_4；另外 PHY 類別也是繼承 Biconnector 類別，在 PHY 類別中會模擬比較簡單的實體層，然後它會衍生 wirelessPhy 類別，在 wirelessPhy 類別中模擬無線的實體層功能，最後衍生出 Phy802_15_4。Connector 類別是從 NsObject 類別所衍生出來，它的作用是連接不同的 NsObjects 物件；Agent 類別為 Connector 類別的子類別，它代表了網路層的起點與終點，並用於實現各層級的協定，例如 TCP、UDP、AODV 等；最後 RRT 的模組是我們繼承 Agent 類別所新增的反向路由樹協定。

表 1 模擬參數的設定

參數	設定值
Sensor node	10
Packet size (Bytes)	50
Number of packets	1000
Bit rate (Kbps)	0.8 - 4.8
Moving speed of human body (m/s)	0.1 - 0.5

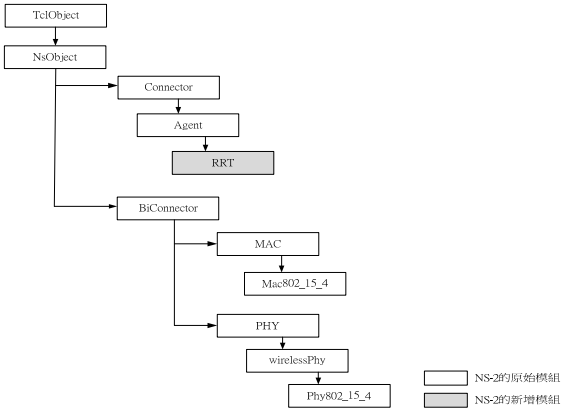


圖 6 NS-2 的架構

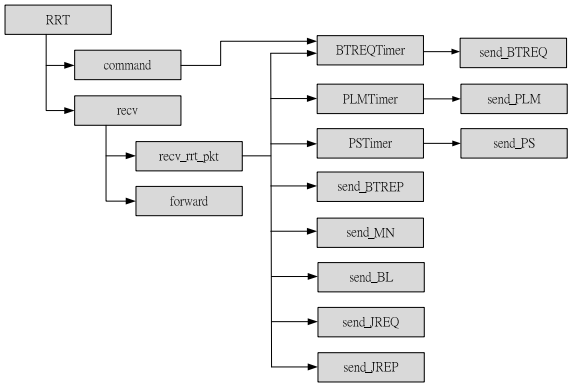


圖 7 RRT 的函式架構

新增的 RRT 模組其最大的貢獻是將原來 802.15.4 的 1 個 hop 的 STAR 拓樸擴充成 2 個 hops 的 TREE 拓樸，在 NS-2 的 802.15.4 環境上，從 1 個 hop 增加成 2 個 hops 的最大困難點在於建立封包轉傳的機制，為了詳細描述此一困難點我們以圖 7 的函式架構來說明，在 RRT 執行的時候會啟動 TCL_command 與 recv 的執行，TCL_command 函式

的目的是讓我們建立的 RRT 與 NS-2 的 TCL 設定建立連結，並且在模擬程式開始時，啟動 BTREQTimer，然後 timer 倒數結束後，hub 會呼叫 send_BTREQ 函式，開始建立以 hub 為 root 的 RRT 拓樸，另外 recv 函式負責接收傳輸層和 MAC 層的封包，它會先判斷收到封包的類型，如果收到的是 RRT 的控制封包，就會呼叫 recv_rrt_pkt 函式處理，若是非 RRT 的控制封包則呼叫 forward 函式。當 sensor node 呼叫了 recv_rrt_pkt 函式後，此函式會先判斷目前收到的封包是哪一種 RRT 的控制封包，如果收到 BTREQ 封包，則我們會判斷此 sensor node 是否已在 RRT 拓樸中，若是，我們會將收到的 BTREQ 封包丟棄，若否，我們會呼叫 send_BTREP 函式發送 BTREP 封包；如果 recv_rrt_pkt 函式收到 BTREP 封包，我們會檢查 LQI 是否大於 LQI_TH，若大於，我們會呼叫 send_MN 函式；如果 recv_rrt_pkt 函式收到 MN 封包時，若此 sensor node 已經在 RRT 拓樸中，那麼就會丟棄 MN 封包，若此 sensor node 不在 RRT 拓樸中，又收到來自 hub 的 MN 封包時，會呼叫 send_PS 函式和 send_BTREQ 函式，若它收到來自非 hub 的 MN 封包，會啟動 PLMTimer 與 BTREQTimer，在 timer 倒數結束前，這個 sensor node 會挑選出具有最佳 LQI 的 parent，然後 timer 倒數結束後，PLMTimer 會呼叫 send_PLM 函式，並開始周期性的量測 LQI，另外 BTREQTimer 會呼叫 send_BTREQ 函式，再去尋找下一個深度的 sensor node；如果此 sensor node 收到 PLM 封包，它會檢查 LQI 是否小於 LQI_TH，若小於，則它會取消 PLM 封包的周期性傳送，並且呼叫 send_BL 函式，送出 BL 封包給它的 child；如果 recv_rrt_pkt 函式收到 BL 封包，我們會將此 sensor node 標記為不在 RRT 拓樸中，並且呼叫 send_JREQ 函式為此 sensor node 尋找新的 parent；若 recv_rrt_pkt 函式收到 JREQ 時，此 sensor node 會呼叫 send_JREP 函式，回覆 JREP 封包；當 recv_rrt_pkt 函式收到 JREP 時，此 sensor node 便會啟動 PSTimer 和 PLMTimer，在 timer 倒數期間，此 sensor node 會挑選具最大 LQI 的 sensor node 為新的 parent，若是有多個 sensor node 具最大 LQI，那麼便從中隨機挑選一個 sensor node，最後 timer 倒數結束後，此 sensor node 便會呼叫 send_PS 函式及 send_PLM 函式。最後在 forward 函式中，此 sensor node 會判斷是否已經抵達目的地，若是，它會將封包往傳輸層傳遞，若否，則它會依據我們建立的 RRT 拓樸轉傳封包給它的父節點。

4.3 模擬結果

圖 8 是我們固定 bit rate (BR)為 4.8 Kbps 的情況下，比較 STAR 與 RRT 在每個 sensor node 的 packet loss ratio (PLR)，其中 PLR 是我們先統計每個 sensor node 遺失的封包個數，然後將遺失的封包個數除以這個 sensor node 傳出的封包總數。從圖 8 中，我們發現在 STAR 時，sensor node ID = 6, 7, 8, 9 的 PLR 都比較高，因為這些 sensor nodes 距離 hub 比較遠，較差的 LQI 會導致較高的 PLR；另外 RRT 的 PLR 都比 STAR 的 PLR 低，這是因為在 RRT 的拓樸中所有 sensor nodes 在選擇路徑時都有考慮到 LQI，因此可以導致比較低的 PLR。

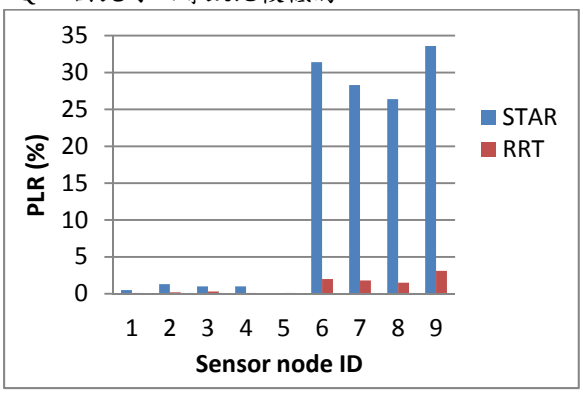


圖 8 個別的 PLR 在 STAR 和 RRT 比較

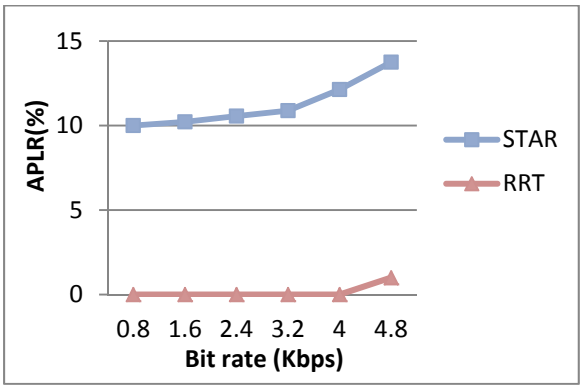


圖 9 所有的 APLR 在 STAR 與 RRT 的比較

圖 9 是我們將 BR 從 0.8 Kbps 增加到 4.8 Kbps 時，STAR 與 RRT 在 average packet loss ratio (APLR) 的比較，APLR 是將所有 sensor node 的 PLR 作平均。從圖 9 中我們發現 STAR 的 APLR 大約都在 10%以上，而且 STAR 的 APLR 總是高過 RRT 的 APLR，這是因為在 STAR 中的每個 sensor node 都是與 hub 直接相連，所以距離 hub 較遠的 sensor nodes 就會因 LQI 較差而導致資料的出錯而被丟棄；此外隨著 data rate 的增加，封包碰撞變多而導致封包遺失，因此 STAR 的 APLR 會逐漸上升，而 RRT 的 APLR 只有在 BR 上升到 4 Kbps 時，封包碰撞的次數才會突然上升，進而導致 APLR 上升。

圖 10 為我們固定 BR 為 4.8 Kbps 的情況下，比較 STAR 與 RRT 的每個 sensor node 在 average packet delay (APD)的變化，各別 sensor node 的 APD 是我們統計每個 sensor node 傳送給 hub 的 1000 個封包的平均延遲。從圖 10 中我們發現每個 sensor node 在 STAR 的拓樸中其 APD 都高於在 RRT 拓樸中的 APD，這是因為從圖 8 中我們發現每個 sensor node 的 PLR 在 STAR 拓樸中都比較高，封包遺失需要重傳，所以封包成功抵達 hub 的時間會增加；而在 RRT 的拓樸中，sensor node ID=6, 7, 8, 9 的 APD 都比較高，這是因為它們在 RRT 的拓樸中都

需要經過 2 個 hops 才能將資料傳到 hub，因此 APD 會比較高。

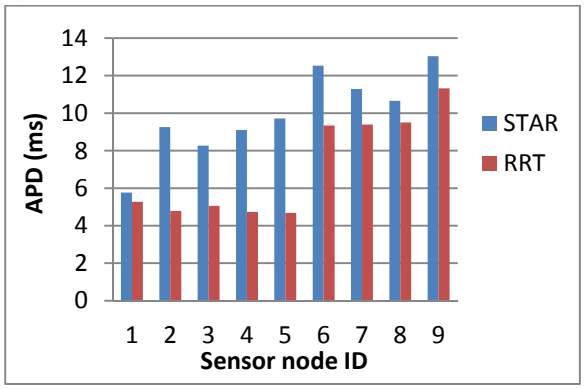


圖 10 個別的 APD 在 STAR 和 RRT 的比較

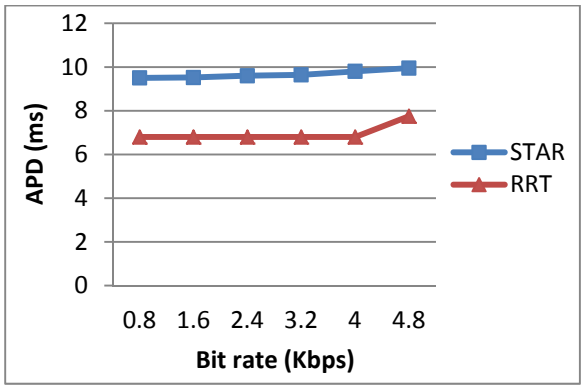


圖 11 所有的 APD 在 STAR 與 RRT 的比較

圖 11 是我們將 BR 從 0.8 Kbps 增加到 4.8 Kbps 時，STAR 與 RRT 在所有 sensor nodes 的 APD 比較，所有 sensor nodes 的 APD 是我們先統計每個 sensor node 傳送給 hub 的 1000 個封包的平均延遲，然後將每個 sensor node 的平均封包延遲再一起作平均。在圖 11 中我們發現在 STAR 拓樸中，所有 sensor nodes 的 APD 都高過在 RRT 拓樸中的 APD，因為在 STAR 拓樸中距離 hub 較遠的 sensor nodes 傳送的封包會因為 LQI 比較差而出錯，此時 sensor nodes 會重新傳送封包，所以使得 hub 成功接收到這些封包的時間變長；另外隨著 sensor node 的 BR 增加，封包產生碰撞的次數增加，碰撞的封包必須重新競爭傳送的機會，使得在 RRT 拓樸中的 APD 在 BR 上升到 4 Kbps 時會突然上升。

圖 12 是我們將人體移動速度從 0.1 m/s 增加到 1.1 m/s 時，RRT 重組時間(RT)的變化，我們觀察到 0.1 m/s 至 0.5 m/s 時，所有的曲線都呈現下降趨勢，這是因為藉由週期性的發送 PLM 封包給 parent，parent 可以較快的知道 child 的 LQI 不好，並通知 child 尋找新的 parent；當我們固定 BR 改變 PLM interval (PI)時，我們發現 PI=0.1 s 時 RRT 重組時間比較短，因為 PI 比較小時 parent 可以較快發現 child 的 LQI 變差，進而較快啟動重組；又當我們固定 PI 改變 BR 時，發現 BR=4.8 Kbps 時 RRT 重組時間比較長，因為 BR 較大的關係導致 PLM 封包會容易產生碰撞，所以延長了 RRT 的重組時間。在圖 12 中，我們觀察到在人體移動速度為 0.5 的時候，RRT 可以達到最短的重組時間。另外隨著人體移動速度繼續增加，我們發現 0.5 m/s 之後，重組的時間都開始變長，並且 PI=1 s 的 RRT 比 PI=0.1 s 的 RRT 較快上升，這是當 PI 較大時，child 移動太快，使得 child 收不到來自 parent 訊息，導致重組時間延長。

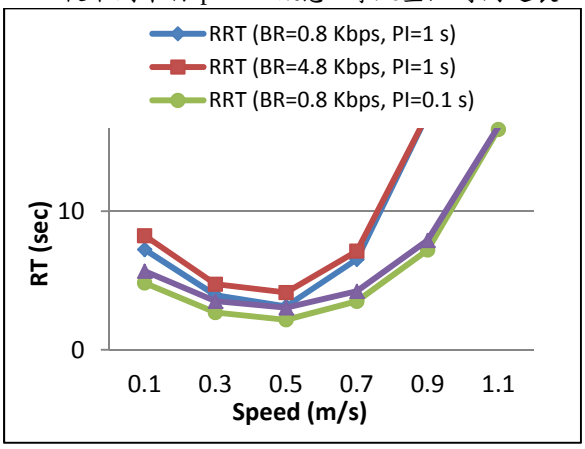


圖 12 RRT 的重組時間

5. 結論

我們在 BSN 網路上建立 RRT 拓樸，使得每個 sensor node 的資料傳送路徑都具有良好的 LQI，所以能夠有效減少 PLR，又因為 PLR 降低，減少封包重傳，所以 RRT 的 APD 比 STAR 的 APD 來的小，在人體動作改變時，我們能夠局部的進行 RRT 拓樸的重組以減少封包的遺失。但是當人體移動速度太快時，RRT 拓樸的重組時間會延長甚至失敗。

致謝

作者要感謝 NHRI, Taiwan. This work is supported under the grant number NHRI-EX102-10142EI.

參考文獻

[1] IEEE Standard for Local and Metropolitan Area Networks—Part 15.6: Wireless Body Area Networks, IEEE 802 LAN/MAN Standards Committee, Feb. 6, 2012.

[2] H. Chebbo, S. Abedi, T.A. Lamahewa, D.B. Smith, D. Miniutti, and L. Hanlen, “Reliable Body Area Networks Using Relays: Restricted Tree Topology,” 2012 International Conference on Computing, Networking and Communications (ICNC), Maui, Jan. 30, 2012.

[3] R. Annur, N. Wattanamongkhol, S. Nakpeeerayuth, and L. Wuttisittikulkij, “Applying the Tree Algorithm with Prioritization for Body Area Networks,” 2011 10th International Symposium on Autonomous Decentralized Systems (ISADS), Tokyo, Mar. 23-27, 2011.

[4] M. Quwaider and S. Biswas, “On-body Packet Routing Algorithms for Body Sensor Networks,” 2009 First International Conference on Networks and Communications (NETCOM 2009), Chennai, Dec. 27-29, 2009.

[5] C. H. Wu and Y. C. Tseng, “Data Compression by Temporal and Spatial Correlations in a Body-Area Sensor Network: A Case Study in Pilates Motion Recognition,” 2011 IEEE Transactions on Mobile Computing, vol. 10, no. 10, pp. 1459-1472, Oct. 2011.

應用於校園網路與監控系統網路整合之 CAN 與 TCP/IP 閘道器之設計

邱日清　王子昂　侯建和
國立中山大學電機工程學系
k781019@hotmail.com

摘要

TCP/IP 於 Ethernet 廣泛地使用在各種領域，亦是校園網路的主幹協定。對於校園網路環境而言，除了傳統的資料處理的應用外，校園安全監控系統的加入也日形重要，有效率地整合此兩種異質網路系統於一體，也是校園網路當前重要的課題之一。CAN 匯流排是當前應用於監控系統重要的匯流排協定，它採用訊息識別作為逐位仲裁的優先權機制，訊息傳遞能在有限的延遲之內完成，適合使用在即時環境當中。本研究透過 CAN 匯流排與 TCP/IP 網路的閘道器的設計，提供管道讓訊息來往於 CAN 匯流排與 TCP/IP 於 Ethernet 網路之間，以建構一個可靠且具有擴充性的自動化控制區域網路。

關鍵詞：控制器區域網路、自動化控制區域網路、CAN 與 TCP/IP 之閘道器

Abstract

TCP/IP on Ethernet is wildly using in various place, such as industry automation, commercial area networks, and campus area network, etc. In addition to the traditional data processing applications, campus safety monitoring system is becoming more and more important. The CAN bus uses the message identifier as a priority by-bit arbitration mechanism, message can be delivered within a limited delay, suitable for use in real-time environment, as an important basic layer protocol for the automation network. This study proposes a gateway model that provides message to transfer between CAN bus and TCP/IP on Ethernet.

Keywords: CAN, Controller Area Network, Automation network, CAN-to-TCP/IP on Ethernet Gateway

1. 前言

隨著微控制器和嵌入式系統的蓬勃發展，很容易透過編程的方式達到精確的時間與位置控制，許多特定行為的工作普遍都交由自動化設備執行，當控制器數量增加到一定的規模則很難再用人工的方式一一檢視設備，從而導入自動監控的機制，在車輛、航空、航海、建築、智慧家電、醫療、油氣、電力、水處理等各個領域都有所應用。隨這時代的進步與當前社會環境的變化，對於校園安全自動化監控系統，更是日形重要。

整合當前區域網路與自動化控制系統網路，作為數據採集與監控系統（Supervisory Control and Data Acquisition，SCADA）之用途，是提升校園網路系統功能的重要指標工作之一。對於一些控制系統且具有高度即時需求的系統，其網路架構的好壞會直接反應在傳輸時間上，嚴重者甚至產生錯誤，而任何一個錯誤的發生都可能導致財產損失或人員意外，更顯得自動監控系統中的錯誤處理機制格外重要。傳統採用 RS-485 作為控制區域網路控制訊號的載具雖然歷久不衰，卻不支援硬體的碰撞偵測或錯誤修正之解決方案。

現今自動控制通訊協定種類繁多，不同媒介之間無法直接互相通訊，使得整合不同媒介之間的溝通成為一個重要的課題。對於數據採集與監控系統的區域網路中，CAN 這種關鍵的通訊協定常被應用，若能將其與 TCP/IP 於 Ethernet 整合來提昇各網路之間的相容度，使得自動化監控系統區域網路的規劃更具有彈性。

本研究企圖建構一種可靠且低成本的應用模型，且期望可推廣至大型分散式的控制網路應用，於是提出 CAN 與 TCP/IP 於 Ethernet 之閘道器作為 CAN 匯流排網路向 TCP/IP 於 Ethernet 網路擴展的管道，達到有效率的整合校園網路與監控網路此兩種異質網路系統於一體。

2. CAN 與 TCP/IP 閘道器

閘道器又稱為協定轉換器，是一個面對兩種不同協定或不同實體介面的網路節點，可以運作在任何一個網路層級，當閘道器面對超過一個以上

的協定時，傳輸的轉傳機制可能比路由器或交換器還要複雜很多。

其工作內容包含協定轉換、裝置阻抗匹配、傳輸速率轉換、錯誤隔離或訊號轉換等。由於使用軟體處理協定轉換，相較於單純使用硬體的設備會造成更長的傳輸延遲，在實際使用上必須考慮傳輸延遲的問題，才能決定傳輸路徑中可存在的閘道器之最大數量。

CAN 匯流排與 TCP/IP 於 Ethernet 資料轉換機制的具體工作內容為訊息格式轉換、位址轉換和實體介面轉換。

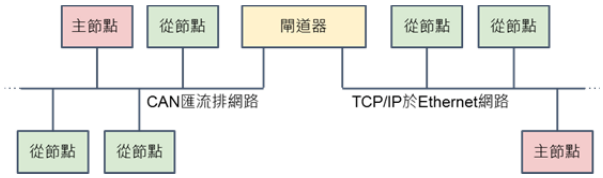


圖 1　閘道器與 CAN 匯流排網路、TCP/IP 於 Ethernet 網路

2.1　訊息格式轉換

對於上層協定和 CAN 的資料鏈結層之間而言，需要自行加入處理上層協定資料單元（Protocol Data Unit，PDU）片段的機制。

圖 2 為一個 17 位元組的上層 PDU 分解之例。一個 17 位元組的上層 PDU 依照 CAN 協定每次所能承載的最大容量 8 位元組分解程三個片段。

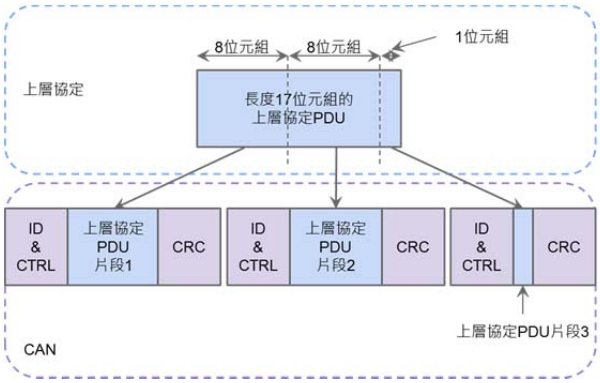


圖 2　17 位元組的上層協定資料單元分解之例

考慮支援上層 PDU 長度最大有 512 位元組，以 CAN 匯流排每次 8 位元組的方式傳送需要花費 64 次，需要使用 6 個位元（位元 0 到位元 5）作為上層 PDU 片段序號編碼。

參考圖 3，對於標準識別訊框的 CAN，利用 CAN 訊息識別的最小 6 個位元作為上層 PDU 片段之用，與 1 個位元（位元 6）的最末 PDU 片段識別（Final Bit Field，FIN）和 1 個位元（位元 7）的最首 PDU 片段識別（First Bit Field，FIR），最後 3 個位元（位元 8 到位元 10）保留作為 CAN 的訊息種類識別，也就是說明承載的資料屬於何種上層協定。

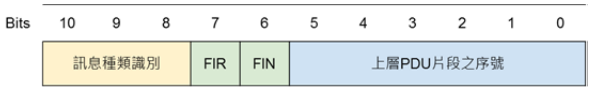


圖 3　CAN 訊息識別之用途規劃

2.2　位址轉換

位址轉換的目的在於訊息可以正確的送到接收端並且被辨識。CAN 匯流排與 TCP/IP 於 Ethernet 採用不同的定址模型，欲使 CAN 匯流排網路上的訊息能和 TCP/IP 於 Ethernet 網路上的訊息交換，閘道器必須具有位址轉換的機制。

CAN 匯流排網路上的資料內容類型由訊息識別定義，發送端的動作僅僅是把訊息識別（隱含資料內容類型）和資料往匯流排上送出，由接收端依據訊息識別（是否為感興趣的資料內容類型）決定接收後送往上層或丟棄。

參考圖 4，假設採用某種應用層通訊協定，在 CAN 匯流排上使用特定的訊息種類識別，二進制的「111」作為此種應用層通訊協定的訊息種類識別，即「0x7XX」的訊息識別，所以只要閘道器收到帶有此種應用層通訊協定的訊息種類識別的資料傳輸，就會往 TCP/IP 於 Ethernet 轉傳。



圖 4　對特定應用使用 CAN 訊息種類識別「111」的定址方法

TCP/IP 使用 IP 位址作為訊息傳輸來源與目標的依據，發送前需要先知道目標的 IP 位址，同時也要附上自己的 IP 位址作為回傳時之用。TCP/IP 使用 TCP 埠號作為不同應用程式的連接窗口，並且必須要先建立連線而後傳輸資料。

參考圖 5，假設採用某種應用層通訊協定，在 TCP/IP 於 Ethernet 上使用特定的 TCP 埠號「4183」作為此種應用層通訊協定的訊息種類識別，所以只要閘道器收到經由 TCP 4183 埠的資料傳輸，就會往 CAN 匯流排轉傳。

Bits	7	6	5	4	3	2	1	0
	0	0	0	1	0	1	1	1
Bits	15	14	13	12	11	10	9	8
	0	0	0	1	0	0	0	0

圖 5　對特定應用使用 TCP 埠號 4183 的定址方法

閘道器的位址轉換方法即是對於特定的應用程式使用特定的 CAN 訊息種類識別二進位的「111」和特定的 TCP 埠號「4183」。CAN 訊息種類識別二進位的「111」和 TCP 埠號「4183」並不是硬性規定的，是我們對一個自行規範的應用層協定的設定，實際應用上應考慮現有的使用常規來對特定應用程式設定對應的 CAN 訊息種類識別與 TCP 埠號。譬如 Modbus/TCP 使用 TCP 埠號 502 已經是公認的標準。

2.3 實體介面轉換

訊息通過閘道器的過程將於 CAN 匯流排與 Ethernet 兩種實體介質之間轉換。就像人們搭公車到車站轉乘鐵路一樣，到了車站時先下公車接著進入火車車廂。傳輸的訊息也是一樣，搭乘一種傳輸媒介到達閘道器時將其取出，轉載到另外一種傳輸媒介後繼續往前發送。實際的運作是由 CAN 收發器與 Ethernet 收發器處理訊息取出或載入的動作並完成阻抗匹配，而 CAN 控制器與 Ethernet 控制器會負責設置傳輸速率和處理位元編碼。

實體層通常被製造成晶片，如此一來，對於實體介面轉換的工作可以很容易地透過軟體的設計**來控制 CAN 控制器晶片和 Ethernet 控制器晶片來**達成。

依據現有的協定標準，CAN 裝置使用三條電線與匯流排網路相連，分別是 CAN_H、CAN_L 與接地線，對於線材或接頭沒有明確規範，而多使用無遮蔽雙絞線與 DB9 接頭等。CAN_H 與 CAN_L 是一組電壓振幅相同、相位相反的差動訊號，其電壓準位判別根據 ISO11898-2 [2] 標準的高速版本協定與 ISO11898-3 [3] 的低速版本協定略有不同。而 Ethernet 的版本眾多複雜，以 100Base-TX 為例，多以 TIA/EIA-568-B 的接線形式，使用兩對（1、2 及 3、6）第五類無遮蔽雙絞線（CAT.5 UTP）進行連接。

3. 實例操作

3.1 平台建立

在實作上採用帶有 PXA270 處理器的實驗板（XSBase270）[4] 作為閘道器的開發。XSBase270 是基於 Intel PXA270 之 ARM 架構處理器所建構的實驗板，整合了使用 LAN91C113 10Base-T 與 100Base-TX 的 Ethernet 控制器和 MCP2515 CAN 控制器 [5] 與 MCP2551 CAN 收發器 [6]。本研究將 Windows Embedded CE 6.0 R3 作業系統 [7] 搭載於 XSBase270 上的實驗發展板作為 CAN 與 TCP/IP 於 Ethernet 通訊模組的開發平台。

Ethernet 使用 XSBase270 核心板上的 LAN91C113 Ethernet 控制器，實驗板的製造廠商附有 LAN91C113 於 Windows Embedded CE 的驅動程式，是由 Standard MicroSystem Corporation 釋出的 2.1 版本。Ethernet 上的 TCP/IP 協定則以 Windows Sockets 2 [8] 實作。

CAN 模組位於 XSBase270 教學板上的 MCP2515 CAN 控制器與 MCP2551 CAN 收發器，MCP2551 以 SPI 為介面和 PXA270 連接，作為 PXA270 的 SPI 從裝置，經由 MCP2515 提供的 SPI 指令（表 1）達成對 CAN 控制器的操作。PXA270、MCP2515 CAN 控制器與 MCP2551 CAN 收發器之間的連線參考圖 6。

表 1　MCP2515 提供的 SPI 指令列表

指令格式	說明
1100 0000	重置，暫存器回覆預設值且進入配置模式
0000 0011	讀取，從指定位址的暫存器讀取資料
1001 0nm0	讀取接收緩衝器，n、m是指定暫存器的起始位址的編碼，對應的RX中斷旗標會被清除
0000 0010	寫入，在指定位址的暫存器寫入資料
0100 0abc	裝載發送緩衝器，a、b、c是指定暫存器起始位置的編碼
1000 0nnn	請求發送，n、n、n分別代表對第2、第1、第0個發送暫存器的請求，可同時發出請求
1010 0000	讀取狀態，讀取有關發送和接收功能的狀態
1011 0000	讀取接收緩衝器狀態，讀取接收緩衝器可知是否於已滿的狀態與相關資訊
0000 0101	位元修改，使用對特殊功能暫存器的特定位元修改

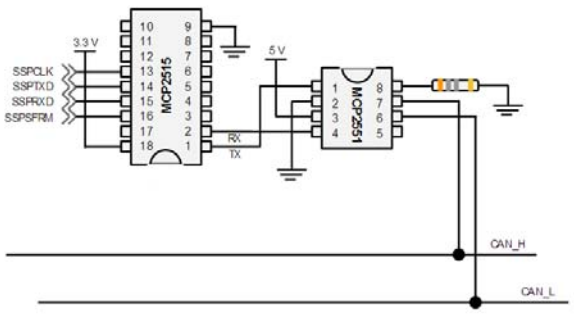


圖 6　PXA270、MCP2515 與 MCP2551 之連線圖

3.2 行為驗證

實例操作中對於訊息經過閘道的兩種方向均予以驗證。

從 CAN 匯流排收到帶有訊息種類識別 0x7XXX 的訊息要送往 TCP/IP 於 Ethernet（圖 7）時，閘道器會將訊息轉送給每一個以 TCP 埠號 4183 建立連線的裝置。

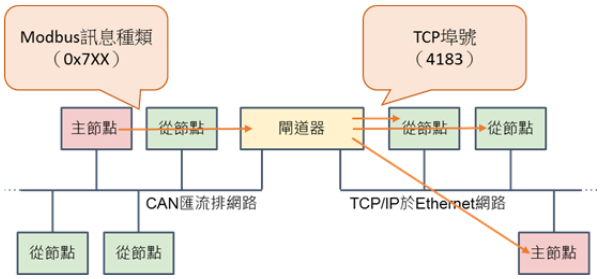


圖 7 訊息從 CAN 匯流排送往 TCP/IP 於 Ethernet

從 TCP/IP 於 Ethernet 經由 TCP 埠號 4183 傳來的訊息要送往 CAN 匯流排（圖 8）時，會將訊息種類識別設定為 0x7XX 以作為其特定應用層協定的識別，再送到 CAN 匯流排上。

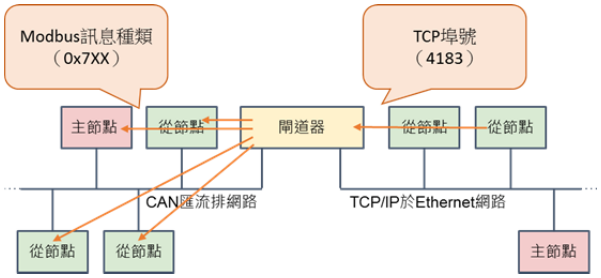


圖 8 訊息從 TCP/IP 於 Ethernet 送往 CAN 匯流排

不管是 CAN 匯流排傳往 TCP/IP 於 Ethernet 或是 TCP/IP 於 Ethernet 傳往 CAN 匯流排的情況，對於閘道器處理訊息格式轉換、位址轉換所花費的時間均小於 1 毫秒，對於一般的操作需求都沒有問題。

4. 結論與未來展望

4.1 結論

對於傳統的自動化控制區域網路採用 RS-485、RS-232 佈線改用 CAN 匯流排，其傳輸將更為可靠，一般以電話線即可作為線材容易建置，又 CAN 控制器與收發器價格低廉，幾乎是在不增加成本的情況下提昇可靠度。

將 CAN 匯流排區域網路與 TCP/IP 於 Ethernet 網路連結，即是將 TCP/IP 於 Ethernet 上的資源帶進 CAN 匯流排區域網路裡，譬如支援遠端的操作、建立資料庫等進階應用，將使得其數據採集與監控系統的功能更加完善。

本論文中提出並實現建構一種可靠且低成本的 CAN 與 TCP/IP 於 Ethernet 之閘道器，以做為達到有效率的整合校園網路與監控網路此兩種異質網路系統於一體的主要應用設備單元。

4.2 未來展望

本研究只是一個 CAN 與 TCP/IP 於 Ethernet 閘道器的雛型，預期可應用於分散式網路之中，譬如多個 CAN 匯流排網路與 TCP/IP 於 Ethernet 網路的網路拓樸。而目前實作的閘道器達成閘道器的基本工作內容，而未來還可以針對不同應用需求加入安全驗證等進階功能。

參考文獻

[1] CiA. (2001-2013). *CAN in Automation (CiA): Controller Area Network (CAN)* [Online]. Available:http://www.can-cia.org/

[2] International Organization for Standardization. (2003). *ISO 11898-2:2003 Road vehicles – Controller area network (CAN) – Part 2: High-speed medium access unit* [Online]. Availible: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=33423

[3] International Organization for Standardization. (2006). *ISO 11898-3:2006 Road vehicles – Controller area network (CAN) – Part 3: Low-speed, fault-tolerant, medium-dependent interface* [Online]. Availible: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=36055

[4] 華亨科技股份有限公司, XSBase270 (EELiod)ADS/Linux/WinCE 實驗開發與實務, 1 版. 高雄縣: 華亨科技股份有限公司, 2007.

[5] Microchip Technology Inc.. (2003-2012). *MCP2515 – Stand-Alone CAN Controller with SPI Interface* [Online]. Available:http://ww1.microchip.com/downloads/en/DeviceDoc/21801G.pdf

[6] Microchip Technology Inc.. (2007). *MCP2551 – High-speed CAN Transceiver* [Online]. Available:http://ww1.microchip.com/downloads/en/DeviceDoc/21667e.pdf

[7] Microsoft. (2009/10/29). *Windows Embedded CE 6.0 R3* [Online]. Availible:http://www.microsoft.com/en-us/download/details.aspx?id=14226

[8] Microsoft.(2013/07/11). Windows Socket 2 [Online]. Availible: http://msdn.microsoft.com/en-us/library/windows/desktop/ms740673%28v=vs.85%29.aspx

軟體定義網路下(SDN)跨網域之端對端自動拓樸與流量檢視

黃文源　　胡仁維　　劉德隆
國家高速網路與計算中心
{ wunyuan, hujw, tlliu }@nchc.narl.org.tw

摘要

未來網路為現今熱門的研究課題之一，許多研究人員為了能解決傳統網路的問題，提出了一些新的網路架構，其中 SDN(Software-defined networking)較為知名。SDN 的最大好處是讓使用者能夠在支援 SDN 的 switch 上自由開發所需策略，因此不再受限於實體機器廠商提供的有限功能，將能夠節省許多資金。實作 SDN 的架構，比較知名的軟體為 OpenFlow，現今有許多組織利用 OpenFlow 於它們的資料中心，例如:Google，因此對於 OpenFlow 網路的管理與維護將是很重要的一個工作，然而現今的 OpenFlow 網路不支援 Inter-domain，使用者從相關的 GUI 介面上無法得知其它網域的 host 與 OpenFlow switch 存在位置，執行 SLA 時，管理人員無法獲知正確的路由路徑，將造成管理與維運上的不便，故本篇文章，將利用先前實作的支援 Inter-domain 的網路拓樸與流量追蹤系統來研究與實作 host 與 host flow 的展示。

關鍵詞：未來網路，OpenFlow，NOX，ENVI，SDN。

1. 前言

在最近這幾年中，未來網路(Future Internet)[1][2][3][4][5]已經成為了研究網路方面的熱門主題之一了，眾多的專家學者們為了解決網路快速發展所衍生的問題，以及想發展一個能自由地設計所需協定或策略的新型態網路架構，紛紛熱情的針對未來網路進行相關研究。在住些研究當中，有專家學者提出了 SDN(Software-defined networking)[6][7][8][9]概念來解決現今網路上的問題。

在提出 SDN 之前，許多公司或住家在只有單一網路的情況下，會使用 switch 或 router 來讓眾多電腦能同時存取網路，然而傳統的 switch 與 router 其控制平台與資料平台是綁在一起，僅能使用廠商所提供的功能來制定策略，無法自由的開發所需的應用程式，再者現今網路規模越來越龐大，有許許多多的協定被使用，對於 switch 和 router 而言，它們就必須針對不同的協定來做正確的解封或是包裝封包，因而造成機器的負擔，使得網路效能不佳，而 SDN 的提出正好可以解決上述之問題。

SDN 跟傳統網路的差異是，控制平台與資料平台是分開的，資料平台的任務僅負責傳送資料，所有一切決策均在控制平台決定，而控制平台可能為裝著控制系統的電腦或伺服器，在此種架構下，對於網路管理人員而言，他們能夠根據自己的喜好在控制平台上開發程式，不用像傳統的 switch 或 router，想要額外的功能就得再花錢購置新的機器，如此一來也能節省金錢上的負擔。在架構 SDN 網路時，需要一些方法來讓控制平台能夠與資料平台聯繫，比較知名的是 OpenFlow，且現今 Google、Facebook 與 Amazon 在其資料中心上也套用 OpenFlow 來實作 SDN，有益於它們維護和管理所屬的資料中心。

由史丹佛大學開發的 OpenFlow，在資料平台中有著 Flow Table，當 Flow Table 中有對應的 Flow Entry，封包才能夠被 OpenFlow 所處理。在控制平台部分，使用者能依喜好安裝適合的控制軟體，例如：NOX[10]、POX[11]、Beacon[12] 與 Floodlight[13]，不管安裝哪套控制軟體，兩平台間均透過 OpenFlow 的協定來通訊。

OpenFlow[14][15][16]網路為中央式的網路控制，控制平台上會儲存著此 OpenFlow 網路的所有訊息，例如:flow 資訊、節點資訊與 link 資訊等，因此任何的決策和命令都是由控制平台來發布，並讓 OpenFlow switch 根據這些決策來處理封包。當不同組織有著各自的 OpenFlow 網路時，它們也會有著所屬的 flow 管理策略，當網路發生問題或是 flow 傳送不如預期時，依據 OpenFlow 的架構，這些組織們也僅能得知它們自己的 OpenFlow 網路狀況，無法確切知道問題發生在何處，在維修上將會耗費大量時間，若 OpenFlow 能支援跨網域所有節點與跨網域 Flow 顯示，對於任何組織來說，這樣能有益於網路管理與維護，而對於研究人員而言，也有益於快速與正確地開發所需之路由路徑與策略。

先前已完成 switch 自動拓樸與 switch 之間的流量檢視[17][18]，然而當 OpenFlow 網路需要執行 host QoS 與 SLA 時必須知道 host 的位置與 host 流量資訊，故我們擴充以前實作的系統，讓其能檢視 host 相關資訊。由於主控者平台原本的追蹤 host 機制的關係，在跨網域的系統上將會顯示錯誤的 host link 與 flow，故此擴充重點將在於如何在追蹤 host 機制的影響下，讓跨網域的系統能夠顯示正確的資訊。

本論文之架構與內容如下所述：第二章將介紹 OpenFlow 架構的跨網域的特點與方法，第三章詳細說明如何實作在跨網域的 OpenFlow 下正確顯示包含兩客戶端、link、flow 的完整拓樸，第四章說明如何架構跨網域的 OpenFlow 網路來展示實作之成果，最後為本論文結論與未來研發工作。

2. 背景知識

此章將分成兩小節簡單介紹 Inter-domain 與實作 Inter-domain 的相關文獻。第一節介紹 Inter-domain 以及它的重要性，第二節描述文獻中如何在 OpenFlow 網路上實作 Inter-domain 的技術。

2.1 Inter-domain introduction

在 OpenFlow 網路中，當控制平台控制著數台 OpenFlow switch，表示這些 OpenFlow switch 屬於同一個網域，反之若由不同的控制平台控制，則表示不同的網域，網域的多寡是依靠著控制平台的數量來決定的，而 Inter-domain Information 就是表示網域之間的資訊。

對於架設 OpenFlow 網路來合作與研究的任何組織而言，因為有著不同的控制平台，也沒有統一的網路 flow 策略，且管理人員也只能獲知自己所屬網域的 OpenFlow 網路狀況，無法得知 Inter-domain 的情況，這些因素將會在研究和管理上造成些許不便，然而現今 OpenFlow 已實作的軟體 NOX、Beacon 與 Floodlight，均尚無支援 Inter-domain 之技術，故需得於上述軟體上實作 Inter-domain。這四種軟體中，以 NOX 發展時間較早，且其所搭配的拓樸顯示的應用程式不僅能顯示節點分布情況與相關資訊外，也能在上面顯示各路由路徑，故本篇文章使用 NOX 來解說與實作 Inter-domain 技術。

ENVI[19]是與 NOX 搭配的拓樸顯示應用程式，它們的處理步驟如圖 1 所示。圖中 OF S/W_1 和 OF S/W_2 分別受 NOX_1 與 NOX_2 所控制，CL_A 和 CL_B 分別是 host，首先讓 CL_A 傳送 Flow 至 CL_B，接著 NOX_1 與 NOX_2 會設定拓樸資訊，此時 ENVI 傳送 Request 至 NOX_1，然後 NOX_1 傳送剛剛設定的拓樸資訊至 ENVI，最後 ENVI 處理所得到的資訊並以圖形化的方式顯示。從處理流程中得知，它們未存放與處理 Inter-domain Information，因此以圖 1 的例子而言，ENVI 尚無法觀察到 Inter-domain 的任何資訊，僅能觀察到 OF S/W_1，使用人員就沒辦法簡單地取得更多資訊。

若控制平台軟體能支援 Inter-domain 的技術，對各個組織而言，他們可以很方便的得知網路上所有的 flow 情況以及每個節點情況，若何處有異狀或是損毀，能夠馬上得知情報進而減少維修時間，而在開發路由或 flow 策略方面，也因為能夠觀察到整個網路的 flow 與拓樸，故能減少許多開發時間。

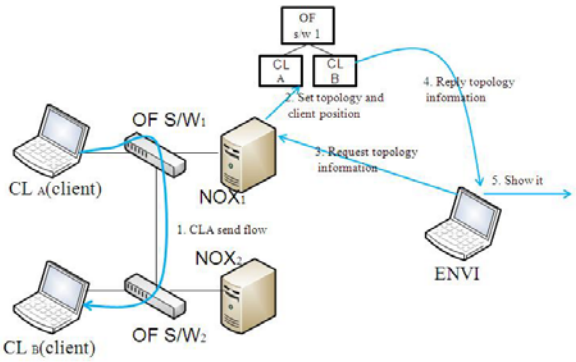


圖 1 NOX and ENVI processing step

2.2 Previous work

[17][18]均在 NOX 與 ENVI 上實作了 Inter-domain 技術，前者僅能夠顯示包含 Inter-domain 的 switch 拓樸分布，後者以前者為基礎，新增加 switch 之間的 Flow 與 Inter-domain flow 展示功能，使用者可以在 ENVI 上利用滑鼠點選任一 Flow 來觀看 Flow 方向、Flow 的起點與終點以及 host IP 資訊。

[17]此篇文章中 NOX 與 ENVI 流程如圖 2，紅色部分是新增與修改原本 NOX 與 ENVI 之處。圖 2 中的拓樸架構同圖 1，一開始讓 switch 間產生 Flow，此時 NOX_1 會接收到從 OF S/W_2 送過來的 LLDP，而這個 LLDP 也包含著 NOX_2 的 IP，故 NOX_1 設定拓樸時會將 OF S/W_2 加入拓樸之中並與 NOX_2 IP 配對，記錄至 switch ID 與 IP 配對表中，然後新增 OF S/W_1 與 OF S/W_2 間的 link，而 NOX_2 也會執行相同的做法來設定拓樸，接著讓 ENVI 先連接至 NOX_1 並取得拓樸資訊，這些資訊中有包含 NOX_2 的 IP，此 IP 將會被儲存至 IP 列表中，而其它資訊持續地被處理，然後於 ENVI GUI 上顯示處理完後的拓樸圖，當 NOX_1 資訊全部處理完畢後，將會根據 IP 列表中的 IP 連線至 NOX_2 上取得拓樸資訊，最後再將新取得的資訊跟原先 NOX_1 的資訊結合，並於 ENVI GUI 上顯示新增的資訊。

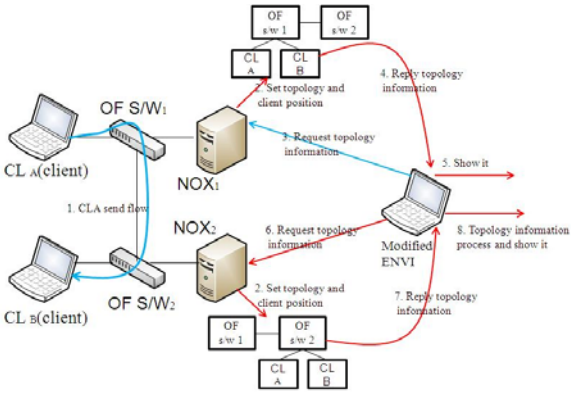


圖 2 Inter-domain implementation 1

圖 3 為[18]修改後的執行流程，與[17]的差異是，當 NOX 接收其他網域的 LLDP 時，不只會在拓樸新增節點外，也會標註接收此 LLDP 的 port 為 Inter-domain port。而原本 NOX 對於從 Inter-

domain port 進出的 Flow 不會有 Inter-domain flow 的紀錄，故 NOX 回應 flow request 時，於 Inter-domain flow 部分為空，ENVI 也就無法顯示 Inter-domain flow，因此[18]中，於回應 flow request 時，利用 Inter-domain port 來比對所有 flow，當確認 flow 由 Inter-domain port 進出後，即利用接收此 OF switch ID 與預定由哪一 port 進出等資訊再搭配 NOX 的 link 資料來找出 Inter-domain flow 的兩端點資訊，之後將這些資訊回應給 ENVI，如此一來 ENVI 就能顯示 Inter-domain flow。

利用上述文獻提供的方法，就能夠在 ENVI 上看到所有網域的 OpenFlow switch 節點，以及 switch 之間傳輸的 flow，然而卻無法得知 OpenFlow 網路上任何的 host，無法完全驗證網路的路由是否為正確，故 Inter-domain host 的顯示也需要被解決與實作。

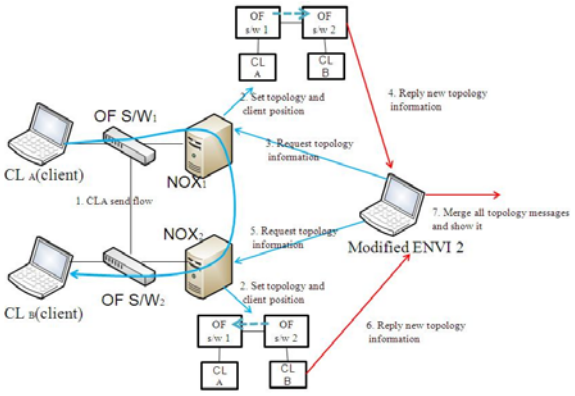


圖 3 Inter-domain implementation 2

3. INTER-DOMAIN HOST DISCOVERY

跨網域的環境中，使用前述支援跨網域顯示 switch 拓樸與 flow 的系統，能夠避免許多維修與管理的問題，然而原本的 OpenFlow 系統與前述的跨網域系統，尚無法正確顯示客戶端位置，對於 SLA(Service Level Agreement)將會造成困擾，故本節將針對此問題詳加說明並且也會提出相應的解決方法與實例。

3.1 問題定義

在跨網域的 NOX OpenFlow 網路中，雖然使用者可以透過 ENVI 來觀察封包傳送路徑，可是因為不支援跨網域的拓樸顯示，故無法得知其它網域的封包傳送路徑，例如下圖 4 的 OpenFlow 環境，有三台 OpenFlow switch OF_A、OF_B 與 OF_C 互相連接，且此三台 switch 分別受 NOX_1、NOX_2 與 NOX_3 控制，另外每台 switch 底下各接一台 host 分別是 1、2 與 3，若於此環境下，讓 1 送資料到 3，對於 NOX_1 而言，其會將 1 與 3 當成自己底下的 host，因此在 1 與 OF_A，3 與 OF_A 之間各自建立連結，使用者透過 ENVI 僅能得知如圖 5 的情形，卻無法得知封包是從 1->OFA->OFB->OFC->3 或是 1->OFA->OFC->3，如此一來對 SLA 而言將無任何幫助。

接著同樣使用圖 4 的拓樸環境，將原本的 NOX 用修改過可支援跨網域的的 NOX 來代替，同樣的讓 1 送資料至 3，假設 NOX_1 將資料由 OF_A 轉傳至 OF_C，NOX_3 再命令 OF_C 將資料送往 3，在此種的路徑下，NOX_1 與 NOX_3 均會得知 1 與 3 的存在，然後會如同前面敘述的，NOX1 會在 1 與 OF_A，3 與 OF_A 之間建立連結，而 NOX3 則是在 1 與 OF_C，3 與 OF_C 間建立連結，故會出現如圖 6 之情形。

雖然透過可支援 Inter-domain 的 NOX，可以得知 switch 間封包的傳輸路徑，可是在原本 NOX 決定客戶端機制的影響下，其形成的不正確 host 資訊將造成使用者的困擾。

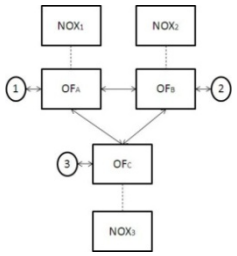


圖 4 SLA test topology

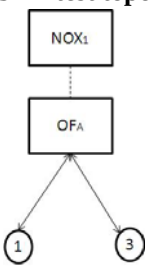


圖 5 SLA problem with default NOX

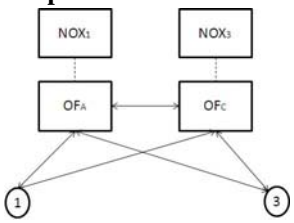


圖 6 SLA problem with inter-domain system

3.2 設計與實作

實作方面，主要分為 NOX 與 ENVI 兩大部分說明：

第一部分為 NOX 程式的修改，因為 NOX host 追蹤方法是根據 OpenFlow switch 從哪個 port 接收到 host 封包的資訊來設定位置，所以 Inter-domain 環境下，許多 host 雖然不在同一網域底下，可是每個網域的 NOX 卻會將所有 host 認定為自己所屬之 host，故為了要能取得正確的 host 位置，我們必須於 NOX 中辨識接收 host 封包的 port 的類型，如此才能順利的分析 host 是否存在於所屬之網域底下。

port 的類型分為 Inter-domain port 與 Intra-domain port，一般情況下 OpenFlow switch 的所有

port 均為 Intra-domain port，當某一 port 收到 Inter-domain 的 LLDP 封包時，NOX 將會從 LLDP 中取出節點相關資料於 Topology 中新增節點，同時也將接收的 OpenFlow switch ID 與接收此 LLDP 封包的 port 配對，然後放入用來確認是否為 Inter-domain port 的資料結構中。

接著修改 LAVI[20]中傳送 host 資訊的部分，首先須於回傳至 ENVI 的 Host Node JSON 中新增額外的辨識訊息，讓 ENVI 確認此為 host 而非 OpenFlow switch。然後 LAVI 中 host link 的部分，於 Host Link JSON 中的每條 link 資料內新增 InterDomain 欄位，用來讓 ENVI 判斷此 host link 是否為 Inter-domain link，若內容為 Yes 表示 Inter-domain host link，若為 No，表 Intra-domain host link。最後 Host Flow JSON 部分，我們於 Host Flow JSON 中新增些許欄位，讓 ENVI 能顯示更多的 Flow 資訊。

圖 7(a)(b)為修改成果的執行流程圖，流程圖中*表示為我們修改的部分，另外圖 7(b)處，由於 LAVI 中主要是修改 Host Link JSON 部分，故僅展示此部分的處理流程。圖 7(a)的流程中，當 NOX 收到 Inter-domain LLDP 後，於新增節點與 link 時也建立 Inter-domain 的 hash table，此 table 內容是 <Switch dp ID, port received LLDP >。圖 7(b)中，當 NOX 收到 ENVI 的請求時，會取得任一條 host link，然後使用 host link 中 switch 端的 switch id 至先前的 Inter-domain hash table 中查詢裡面紀錄的 Inter-domain port(port received LLDP)與 switch port 是否一樣，若一樣將會在 JSON message 新增的 interDomain 欄位上紀錄為 YES，不一樣則為 NO，最後再將此 Host Link JSON 回傳給 ENVI。

第二部分為 ENVI 程式的修改，因為我們有新增欄位於 JSON message 之中，故須修改 ENVI 中接收資訊的部分，讓所新增加的欄位資訊能正確地被讀取，這部分中最重要的是 host link 的處理，我們需在處理 host link 的部分新增一個辨識 Intra-domain host link 與 Inter-domain host link 的方法，當 ENVI 取得 Host Link JSON 中的資訊時，除了利用內部的資料建立 link 資料結構外，也利用資訊中的 interDomain 來判斷 host link 的類型，當為 Inter-domain host link 類型，表示它不直接與正連線的控制平台所控制的 switch 連接，故此處不會繼續進行 link 的處理，反之，Intra-domain host link 則會持續進行新增 link 的處理。

另外 Host Flow JSON 處理的部分，我們也需於此處增加一個判斷條件，當 ENVI 根據資訊建立新的 host flow 資料結構後，再利用其兩端點資料來判斷是否有此 link 的存在，若 host link 存在表示此為正常的 flow，然後繼續新增 flow，反之 host link 不存在則表示此為 Inter-domain host flow，故不應被儲存與顯示。

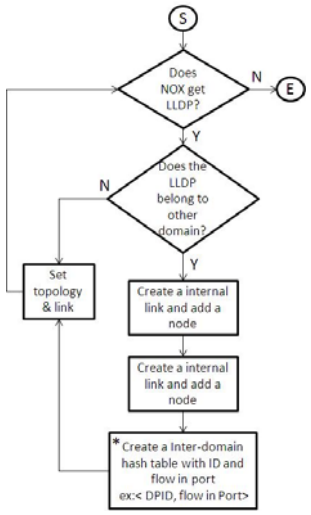


圖 7(a) Flow char of add an Inter-domain node

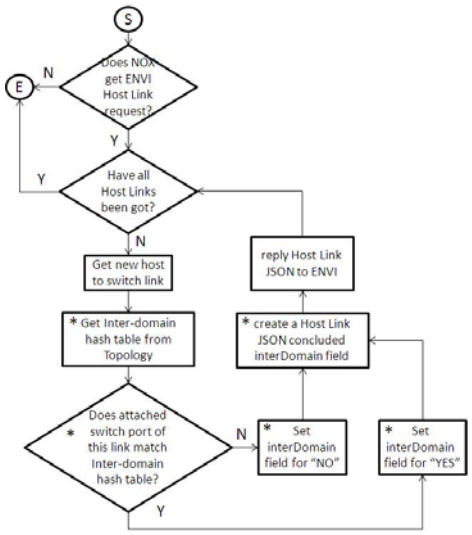


圖 7(b) Identify the Inter-domain host link within LAVI

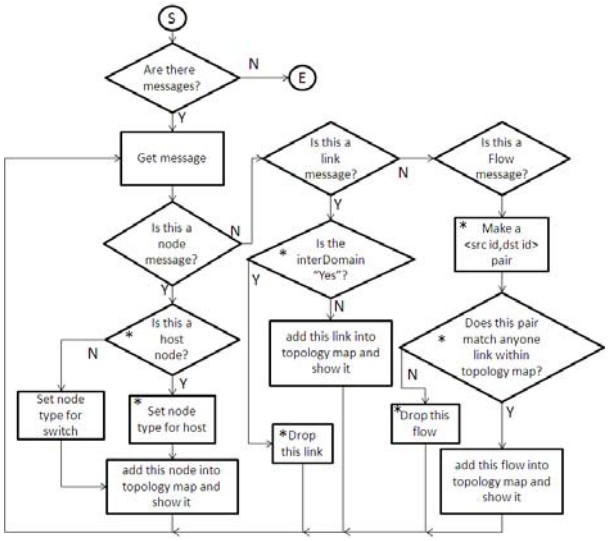


圖 8 The flow chart of ENVI handle messages

圖 8 為此階段修改後的執行流程圖，圖中*符號為修改的部分。ENVI 收到從 NOX 送來的 message 時，會先判斷 message 的型態，當為節點型態時，

會判斷此節點為 switch 或 host，然後將節點型態設成正確的類型，最後儲存入 topology map 之中並在 GUI 顯示。當 message 為 link 的資訊時，先判斷資訊中的 interDomain 是否為 Yes，Yes 則將資訊放入 topology map 並顯示，否則將此 link 丟棄。最後一種 message 類型為 flow 型態，一開始從 flow 資訊中取出來源端與目的端的 ID 做配對，然後至 topology map 中尋找對應的 link，如找到對應的 link，此 flow 資訊將被顯示並且儲存於 topology map 之中，反之則丟棄。

4. 實驗

接著利用 Oracle VM VirtualBox 建立如圖 9 的拓樸來進行測試。首先於 VirtualBox 中先建立三台 OS 為 Ubuntu 10.04 64bit 版本的 VM，並且安裝修改後的 NOX，此三台分別對應圖中的 NOX_1、NOX_2 與 NOX_3，而 OpenFlow switch 部分，則是建立四台 Ubuntu 10.04 32bit 版本的 VM，並在這四台 VM 上安裝 OpenFlow switch 軟體，此四台分別對應圖中的 OF_1、OF_2、OF_3 與 OF_4，最後 host 部分，建立四台任意 OS 且名為 CL_1、CL_2、CL_3 與 CL_4 的 VM，並且各自分配 10.0.0.1~10.0.0.4 的 IP 給它們。VM 間連線設定方面，NOX_1 管控 OF_1 與 OF_2，而 CL_1 與 CL_2 分別連接至此兩台 OpenFlow switch，NOX_2 管控 OF_3，CL_3 與 OF_3 連線，NOX_3 則是管控 OF_4，CL_4 與此 switch 連接

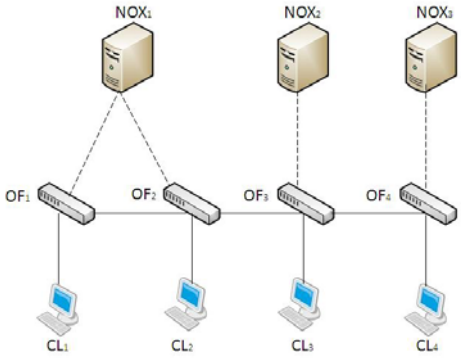
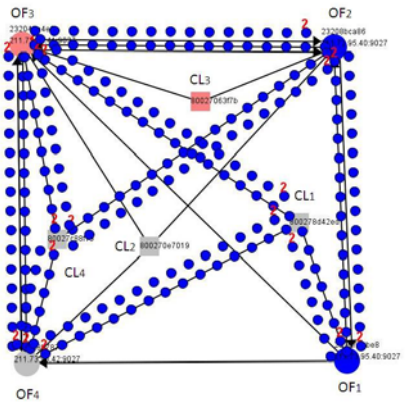


圖 9 Testbed topology

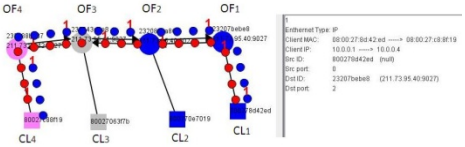
在測試方面，我們檢驗兩種不同的 flow 傳送路徑，第一種是由 CL_1 傳送 flow 至 CL_4， 第二種則是由 CL_2 傳送 flow 至 CL_3。首先先將文獻中的 Inter-domain ENVI Flow Viewer 系統顯示 host 與 host flow 功能開啟，然後執行第一種測試，測試結果如圖 10(a)，從圖中可以看到受 NOX 決定 host 位置的方法影響，對於 CL_1 和 CL_4，CL_1-OF_3、CL_1-OF_4、CL_4-OF_2 與 CL_4-OF_3 等 Inter-domain host link 以及 Inter-domain host flow 均被顯示出來，才會造成圖中網狀的拓樸。圖 10(b)為實作成果執行第一種測試的結果，可以從圖中觀察到 Inter-domain host link 以及 Inter-domain host flow 消失了，在 GUI 上的拓樸分布與實體上連接的線路分布一樣，flow 的路徑與資訊也為正確的結果。

在執行第二種測試方面，同樣的先利用 Inter-domain ENVI Flow Viewer 測試，圖 11(a)為測試結果，CL_2-OF_3 與 CL_3-OF_2 為 Inter-domain host link，而 link 之上的 flow 也為 Inter-domain host flow，與第一種測試的結果一樣，會顯示 Inter-domain host link 與 Inter-domain host flow，因此形成網狀的拓樸。圖 11(b)為實作的測試結果，測試結果與第一種測試相同，均能顯示正確的拓樸以及 flow 的情況。

另外我們也增加了兩種功能，第一種是可以藉由 host 顏色來分辨所屬的網域，例如：CL_1、OF_1 與 OF_2，它們屬於同一網域，故顯示的顏色是相同的。第二種是 host flow 資訊的顯示，藉由點選 host 與 switch 之間的 flow，可以從 GUI 右邊的 flow 視窗中看到此 flow 的內容，例如：兩端點 IP、MAC、port 與 flow type 等資訊，而這些新增的功能，有助於使用者管理與研究跨網域的 OpenFlow 網路。

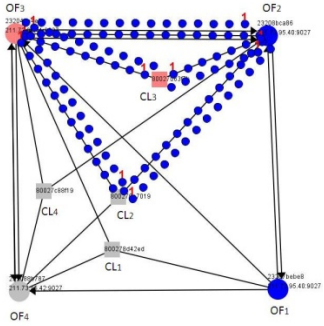


(a) Inter-domain ENVI Flow Viewer

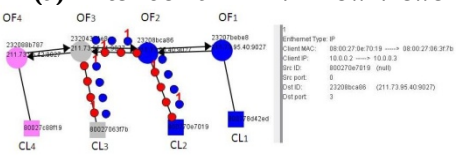


(b)The Implementation result of case 1

圖 10(a)(b) CL_2 forward flow to CL_3



(a) Inter-domain ENVI Flow Viewer



(b) The Implementation result of case 2

圖 11(a)(b) CL_1 florward flow to CL_4

5. 結論

在本篇中我們介紹如何解決 NOX 與 ENVI 顯示 host 與 host flow 的問題，藉由修改 NOX 的 LAVI 內的 host 相關元件，讓 NOX 能夠分辨出 host link 是否為 Inter-domain host link，並且藉著修改 ENVI 軟體，使其能從 NOX 上接收與處理新增的 Host JSON 資訊，並且在 GUI 上正確顯示 host 與 host flow。未來我們將研究並且擴展此系統，除了能進行未來網路管理之功能外，也將套用於其它控制平台軟體之上，如此將有益於跨單位及大型跨國未來網路平台之建置與維運。

參考文獻

[1] D. Cameron, "Internet2: The Future of the Internet and Next-Generation Initiatives, " Computer Technology Research Corp., February 1999.

[2] G. Fairhurst, B. Collini-Nocker, and L. Caviglione, "FIRST: Future Internet — a role for satellite technology," Satellite and Space Communications, 2008. IWSSC 2008. IEEE International Workshop on, pp. 160-164, Oct.2008.

[3] D. Y. Kim, L. Mathy, M. Campanella, R. Summerhill, J. Williams, S. Shimojo, Y. Kitamura, and H. Otsuki, "Future Internet: Challenges in Virtualization and Federation," Telecommunications, 2009. AICT '09. Fifth Advanced International Conference on, pp.1-8, May.2009.

[4] J. Lee, S. Kang, Y. Lee, and J. Lee, " A Study on the Future Internet Requirement and Strategy in Korea," Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on, Vol. 1, pp. 627-629, Feb.2008.

[5] P. Stuckmann, R. Zimmermann, "European research on future Internet design," IEEE Wireless Communications, Vol. 16, Issue 5, pp. 14-22, Oct.2009.

[6] SDN white paper, https://www.opennetworking.org/sdn-resources/sdn-library/whitepapers

[7] A.C. Risdianto, E. Mulyana, "Implementation and analysis of control and forwarding plane for SDN," Telecommunication Systems, Services, and Applications (TSSA), 2012 7th International Conference on, pp. 227-231, Oct. 2012.

[8] K. Bakshi, "Considerations for Software Defined Networking (SDN): Approaches and use cases," Aerospace Conference, 2013 IEEE, pp. 1-9, Mar. 2013.

[9] Myung-Ki Shin, Ki-Hyuk Nam, and Hyoung-Jun Kim, "Software-defined networking (SDN): A reference architecture and open APIs," ICT Convergence (ICTC), 2012 International Conference on, pp. 360-361, Oct. 2012

[10] N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown, and S. Shenker, "NOX: towards an operating system for networks," ACM SIGCOMM Computer Communication Review, Vol.38, Issue 3, pp. 105-110, July2008.

[11] POX, http://www.noxrepo.org/pox/about-pox/

[12] Beacon, https://openflow.stanford.edu/display/Beacon/Home

[13] Floodlight, http://floodlight.openflowhub.org/

[14] OpenFlow, http://www.openflow.org/

[15] OpenFlow white paper, http://www.openflow.org/documents/openflow-wp-latest.pdf

[16] OpenFlow Switch Specification, http://www.openflow.org/documents/openflow-spec-v1.0.0.pdf

[17] Wun-Yuan Huang, Jen-Wei Hu, Shu-Cheng Lin, Te-Lung Liu, Pang-Wei Tsai, Chu-Sing Yang, Fei I Yeh, Jim Hao Chen, and Mambretti, J.J., " Design and Implementation of an Automatic Network Topology Discovery System for the Future Internet Across Different Domains," Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on, pp. 903-908, Mar. 2012.

[18] Wun-Yuan Huang, Jen-Wei Hu, Ta-Yuan Chou, Te-Lung Liu, "Design and Implementation of Real-Time Flow Viewer across Different Domains. " Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on, pp. 619-624, Mar. 2013.

[19] ENVI, http://www.openflow.org/wk/index.php/Extending_ENVI

[20] LAVI, http://www.openflow.org/wk/index.php/LAVI

使用隧道技術實現網路虛擬化

曾惠敏　　胡仁維　　劉德隆
財團法人國家實驗研究院國家高速網路與計算中心
{ n00hmt00, hujw, tlliu }@narlabs.org.tw

摘要

近年來隨著雲端運算（Cloud Computing）的蓬勃發展，虛擬化（Virtualization）技術成為熱門的研究議題，其中主機虛擬化由於可將單一實體主機幻化為多部共同運作中的虛擬主機（Virtual Machine，VM），現已有多種商業與開放原始碼的虛擬化系統（Hypervisor）解決方案，可謂於雲端產業中最為成熟的技術之一；相較於虛擬主機可直接服務提供給終端使用者，位於底層的網路資源之虛擬化的需求度較為不高，但隨著跨機房的資源整合與大型虛擬環境的要求日漸成形，網路虛擬化（Network Virtualization）技術也在不斷摸索中逐漸成形，以隧道（Tunneling）技術動態提供虛擬網路資源已成為市場主流，在本篇論文中，我們將介紹網路虛擬化演進的過程，並分析目前主流的隧道技術，同時以開放原始碼的 Open vSwitch 結合 KVM 來實作出各種虛擬主機與網路配置的案例，提供整合虛擬網路與主機資源規劃之參考。

關鍵詞：網路虛擬化、雲端運算、Open vSwitch、軟體交換器、軟體定義網路。

1. 前言

隨著雲端時代的到來，隨用隨租的運作模式已徹底改變大眾對於數位服務的觀念，例如：可以依照自己的需求（CPU 數量、記憶體大小等）來訂製臨時使用的計算主機，使用完後歸還並依使用量或時間計費，省去自行購置及維護的成本與風險[1]。在雲端服務的背後，資源虛擬化被視為重要的技術之一，透過將實體資源虛擬化的技術，服務供應者方能對使用者的需要進行客製化，並可隨時動態地配置。主機虛擬化技術可以將實體主機依客戶需求同時配置成多部虛擬主機，市面上已有多個商業及開放原始碼的解決方案可採用，目前成為相當成熟的技術，並為大部份的基礎設施即服務（Infrastructure as a Service，IaaS）業者所採用，相對而言，網路資源由於位於底層，一般使用者較無客製化的需求，因此網路虛擬化的成長遲遲並未跟上雲端技術的發展[2][3][4]。

然而因應虛擬主機服務的擴展，虛擬主機間的動態網路配置益發顯示其重要性：如同一使用者所建之虛擬主機若跨不同的實體主機，則需要在實體主機間配置虛擬網路；以及不同使用者的虛擬主機之間需要區隔不同的網路網段等，為此網路虛擬化技術漸獲重視，但存在於實體主機內的軟體交換器與原先實體的硬體交換器間的互通模式需要由主機管理員與網路管理員彼此溝通，造成管理上的複雜度，為此已有不同陣營的網通廠商各自提出 IEEE 802.1Qbg[5]及 802.1BR[6]（取代 802.1Qbh[7]）等標準，試圖將網路設定的主導權自軟體交換器歸還給外部的硬體交換器[8]，但是由於缺乏統一標準，且仍需要與虛擬主機技術間整合，因此未獲大幅度之採用。

不論軟體或硬體式的交換器，基本上還是以 802.1Q 虛擬區域網路技術（Virtual Local Area Network，VLAN）來區分不同的使用者，然而 VLAN 的識別碼僅 12 位元，僅能區隔最多 4094 個用戶，無法因應大量需求；且第二層交換所使用的擴張樹路徑搜尋法也讓可用頻寬受限，無法發揮網路最大的使用率；同時數量龐大的虛擬機器也將會造成機架頂端（Top of Rack，ToR）之交換機過量的負荷，第二層位置表格的容量因受限記憶體大小將不敷使用，因此既有的 VLAN 方案無法滿足雲端環境所需要的虛擬網路需求，有鑑於此，虛擬機器透過軟體交換器間的虛擬隧道建立連線成為快速解決的途徑，相關設定均在伺服器端即可完成，底層網路僅為傳遞封包通透使用，無需額外設定。

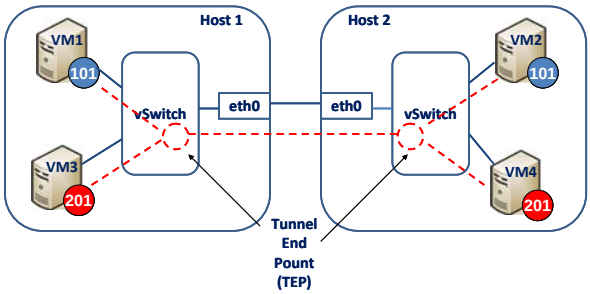


圖 1、 隧道技術示意圖

圖 1 為隧道技術的示意圖，兩個實體主機 Host1 與 Host2 內部的虛擬網路交換器透過底層網路建立起點對點的虛擬通道連線，通道兩端點通常稱為隧道終端節點（Tunnel End Point，TEP），各交換器在傳送封包到隧道之前會依照不同的使用者加註識別碼，如在圖 1 中 VM1 欲傳送封包至 VM2，Host1 內的軟體交換器會在包裝隧道封包時將使用者識別碼 101 填入，傳送到 Host2 後根據此識別碼正確地將封包送給 VM2，如此一來可有效地區隔使

用者識別碼為 101 的 VM1、VM2 與使用者識別碼為 201 的 VM3、VM4。

在本篇論文的第 2 節中，我們將綜覽目前主流的隧道技術並進行比較；第 3 節將介紹如何使用 Open vSwitch 實作出 GRE 隧道，同時進行簡單的效能實測；在第 4 節中，我們將針對雲端環境下的各種虛擬網路情境提出佈建之範例；並於第 5 節作出本篇論文的結論。

2. 隧道技術縱覽

本章節介紹目前三個主流的隧道技術，包括虛擬可擴展式區域網路（Virtual eXtensible Local Area Network，VXLAN）[9]、透過一般路由封裝實現網路虛擬化（Network Virtualization using Generic Routing Encapsulation，NVGRE）[10]、以及無狀態式傳輸層隧道（Stateless Transport Tunneling，STT）[11]，三者源自不同的公司，各自使用選擇不同的方式進行隧道封裝，目前均為 IETF 的 Internet Draft，以下各別敘述其細節，並整理三種技術間的比較。

2.1 VXLAN－虛擬可擴展式區域網路

VXLAN 為 VMWare 與 Cisco 等公司於 2011 年 8 月所草擬，目前最新版本為第四版，為三者當中最早提出的版本，點對點隧道的兩端點稱為 VXLAN 隧道終端節點（VXLAN Tunnel End Point，VTEP），並使用 UDP 進行隧道封裝，如圖 2 所示。

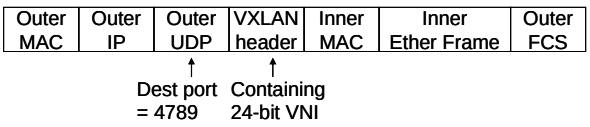


圖 2、 VXLAN 封包格式

被封裝的第二層封包由 VXLAN 表頭所包覆，在 VXLAN 表頭裡有個長度為 24 位元的 VXLAN 網路識別號碼（VXLAN Network ID，VNI），用來區隔使用該隧道的使用者，因此理論上可支援 2^{24} 超過一千六百萬個不同虛擬網路，遠大於 VLAN 4094 個的限制。整個 VXLAN 封包再由外層的 IP/UDP 封包透過第三層實體網路在兩個 VTEP 間傳遞，在 UDP 的表頭裡的目的地埠號已向 IANA 申請了 4789 作為辨識 VXLAN 的依據。而為了在多路徑的網路環境下達到負載平衡，即等價多路徑路由（Equal Cost Multi-Path，ECMP），建議 VTEP 在設定 UDP 的來源端埠號時參考內部被封裝的封包表頭的雜湊值，可依此區別不同資料流（flow），確保屬於相同資料流的封包在第三層傳輸的路徑相同，並讓不同資料流的封包分散至等價的路徑上。

在廣播（broadcast）與群播（multicast）的處理上，VXLAN 要求底層的第三層網路啟用 IP 群播功能，在 VTEP 上透過 VNI 與 IP 群播群組的對照表格處理各虛擬網路的廣播與群播封包，然而現今網際網路骨幹上大多並未開啟 IP 群播功能，這點可能會讓 VXLAN 在大規模佈建時受到限制。

2.2 NVGRE－透過一般路由封裝實現網路虛擬化

NVGRE 是由 Microsoft 為首的公司於 2011 年 9 月所提出，僅略晚 VXLAN 不到一個月，目前已修訂到第三版，不同於 VXLAN 使用 UDP 封包格式，NVGRE 採用現有的一般路由封裝（Generic Routing Encapsulation，GRE）之格式，隧道兩端點稱為網路虛擬化端點（Network Virtualization Edge，NVE）。

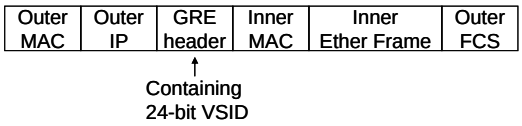


圖 3、 NVGRE 封包格式

NVGRE 封包格式如圖 3 所示，由 GRE 表頭來包覆被封裝的第二層封包，但是與 VXLAN 不同，內部的第二層封包並不支援 802.1Q VLAN 標籤功能，此部份可能會讓虛擬網路的上層應用受到限制，在 GRE 表頭裡定義的 32 位元 Key 欄位在此被拿來作為 24 位元的虛擬子網路識別碼（Virtual Subnet ID，VSID），以及 8 位元的網路流識別碼（FlowID），VSID 的用途與 VXLAN 裡的 VNI 相同，可區別超過一千六百萬個不同虛擬網路；FlowID 則是用來識別不同的資料流，然而現有的等價多路徑路由機制僅根據 TCP/IP 表頭來辨識資料流，並不支援 GRE 表頭，因此在底層設備並未支援 FlowID 的檢視之前，NVGRE 建議使用多個 NVE 實體 IP 位置來對應不同的資料流，在負載平衡上的處理仍然不夠細緻。

在廣播和群播的處理上，NVGRE 可使用 IP 群播的機制，若底層網路不支援 IP 群播，亦可用多重單點傳送來達成相同功能；同時考量隧道封包機制會將增加整體封包長度，若長度超過底層網路的最大傳輸單元（Maximum Transmission Unit，MTU）時封包會被強制分段（fragmentation）至零碎的封包，這些封包於隧道的另一端接收後再進行重組工作，將會增加隧道端點的負荷並降低網路傳輸效率，NVGRE 在內部封裝為 IP 封包時會辨識網路路徑 MTU（Path MTU），若大於封裝後的長度則會強迫封包維持原狀以避免此分段的情境，以上兩點均讓 NVGRE 適於在現有網際網路上傳遞。

2.3 STT－無狀態式傳輸層隧道

STT 是由新創公司 Nicira 於 2012 年 2 月所單獨提出，並被該公司申請專利，目前更新為第三

版，同時由於 Nicira 已於 2012 年 7 月被 VMWare 所併購，目前本 Internet Draft 也改為由 VMWare 所提案。STT 主要是要解決 2.2 節裡所述封包分段的問題，雖然 NVGRE 已盡量嘗試避免，但封包仍然會有被分段的可能，為此，STT 利用現今網路卡對 TCP 分段卸載（TCP Segmentation Offload，TSO）的支援功能，將欲封裝的封包包裝於類 TCP（TCP-like）的表頭之內，如此一來封包的分段及重組的工作均交由硬體網路卡處理，不會影響到隧道端點的運作效能，已有國外的技術網站[12]針對使 Open vSwitch 進行測試比較，發現 STT 完全不影響網路傳輸吞吐量與 CPU 效能，而相同情況下使用 GRE 封裝時傳輸吞吐量的表現僅 1/4 且 CPU 負載亦飆高到 97%，足見 STT 在技術上的優越性。

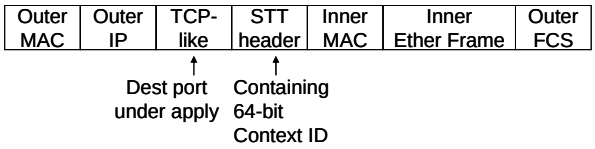


圖 4、 STT 封包格式

STT 封包格式如圖 4 所示，在 STT 表頭內保留了 64 位元的關聯識別碼（Context ID），因此可辨識的虛擬網路數量更為可觀，而在 TCP-like 表頭的目的地埠號正向 IANA 申請固定號碼中，以作為辨識 STT 的依據，來源埠號則是與 VXLAN 裡 UDP 來源埠號一樣，可用來作為等價多路徑路由的依據，在廣播與群播的處理上則是與 NVGRE 相同，底層的網路不必然一定要支援 IP 群播能力。

STT 的獨特設計讓 Nicira 公司大受矚目，並視為市場上其他雲端軟體公司的勁敵，因此在被 VMWare 收購時亦造成熱門之話題，目前 VMWare 同時擁有 XVLAN 與 STT 兩個相同的技術，未來是否會將兩者互相整合也受到市場的關注。

表 1、 三種隧道技術比較

	VXLAN	NVGRE	STT
Encapsulation	UDP	GRE	TCP-like
# of Virtual Networks	2^{24}	2^{24}	2^{64}
VLAN-tag allowed in inner Packet	Yes	No	Yes
IP Multicast Required	Yes	No	No
ECMP Granularity	Low	High	Low
Performance	Poor	Good only when inner packet is IP and path MTU allows	Good

綜合以上之討論，我們將三種隧道技術的比較整理如表 1，比較的項目分別為使用的封裝技術、支援虛擬網路之數量、內部封包是否可使用 VLAN 標籤、底層網路是否需要開啟 IP 群播功能、等價多路徑路由之細緻度、以及實際運作效能等。

3. 以 Open vSwitch 實作 GRE 隧道

Open vSwitch[13]為美國史丹福大學所開發的開放原始碼虛擬交換器軟體，可取代傳統 linux 內建橋接器（Bridge）模組，以取得更好的交換效能，同時 Open vSwitch 亦支援以 VLAN 標籤區隔不同用戶，以及 OpenFlow 這個重要的軟體定義網路（Software Defined Network，SDN）協定，因此頗受各界重視。

關於在第 2 節中所提到的三種隧道封裝格式，GRE 在 Open vSwitch 開發初期就已支援；而在今年 5 月最新的 1.10.0 版本裡亦正式支援了 VXLAN 格式；另外由於 Nicira 公司同為史丹福大學團隊所創立，STT 商業版本的實作亦選擇 Open vSwitch 為搭配之交換器，同時因專利擁有權之故，其他公司無法在自有的交換器上使用 STT 技術，因此成為目前唯一擁有三種封裝技術的解決方案。本節將以 GRE 封裝為例介紹如何在兩台 Open vSwitch 間組態專屬隧道，這邊要注意的是 Open vSwitch 僅分別支援 UDP 與 GRE 的封裝格式，並未完整實作出 VXLAN 與 NVGRE 的協定，因此我們僅能建立點對點隧道，需額外撰寫控制模組以使用 VNI 與 VSID 等欄位及其他相關功能，這部份可透過軟體定義網路 SDN 或自行設計控制層界面，而控制層軟體是否能夠統一標準也將是隧道技術未來發展的重要關鍵。

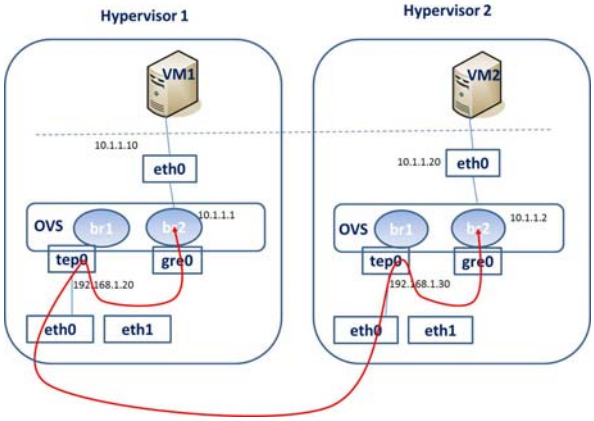


圖 5、點對點 GRE 隧道測試環境

圖 5 為實作的架構圖，在我們的測試環境中，包含兩台實體主機分別為 Hypervisor1 和 Hypervisor2，使用 KVM 配置虛擬主機，其中每台主機下各執行一個虛擬機器分別為 VM1 和 VM2，我們將測試透過 Open vSwitch 使用 GRE Tunneling 的技術來實作虛擬主機的網路配置以達到 VM1 和 VM2 互通目的。然而使用 libvirt 虛擬化管理介面建立的虛擬機器，預設網路介面會被自動地分配一個 vnetx 的網路名稱，經由 bridge(virbr0)連接出去，為了將其整合於 Open vSwitch 中管理，並指定須經由

OVS bridge(br2)連接出去。故須於/etc/libvirt/qemu 下產生之相關的 XML 描述檔修改設定，如圖 6，待修改後重新啟動虛擬主機時會載入新的 XML 描述檔，即完成該虛擬主機之網路介面整合於 Open vSwitch 中，如圖 7 所示。接著我們可依相關需求使用 Open vSwitch 指令進行相關 GRE Tunneling 的設定。

```
<interface type='bridge'>
  <mac address='52:54:00:84:13:17'/>
  <source bridge='br2'/>
  <virtualport type='openvswitch'>
    <parameters interfaceid='70b99bbf-edaf-b37c-c913-7be61997f61a'/>
  </virtualport>
```

圖 6、 Open vSwitch 指令

```
Bridge "br2"
    Port "gre2"
        Interface "gre2"
            type: gre
            options: {remote_ip="192.168.1.40"}
    Port "vnet0"
        Interface "vnet0"
```

圖 7、 整合於 Open vSwitch 之介面

建立 GRE Tunneling 有三個基本的步驟：

1. 新增一個獨立的 Bridge。
2. 在每一台 Hypervisor 上建立 GRE Tunneling 使用之 endpoint。
3. 建立欲連接使用之 GRE Tunneling。

這裡，我們需要在兩台實體主機上分別新增 OVS bridge(br1)和設定其使用之介面為 eth0，並且在該 OVS bridge(br1)上指定 GRE Tunneling 連接使用之 endpoint(tep0)，另外新增一個獨立的 OVS bridge(br2)，用來建立 GRE Tunneling (gre0)，圖 8 為所設定的 Open vSwitch 指令。

```
# sudo ovs-vsctl add-br br1
# sudo ovs-vsctl add-port br1 eth0
# sudo ovs-vsctl add-br br2
# sudo ifconfig br1 211.73.95.33 netmask 255.255.255.224
# sudo ifconfig br2 10.1.1.1 netmask 255.255.255.0
# sudo ovs-vsctl add-port br1 tep0 -- set interface tep0 type=internal
# sudo ifconfig tep0 192.168.1.20 netmask 255.255.255.0
# sudo ovs-vsctl add-port br2 gre0 -- set interface gre0 type=gre
options:remote_ip=192.168.1.30
```

圖 8、 Open vSwitch 指令

上列指令設定完成後，我們可以測試由 VM1 執行 Ping 指令到 VM2 驗證透過 GRE Tunneling 得到網路互通。實際上就像經由兩個 bridge 直接將網路互相連接，如圖 9。

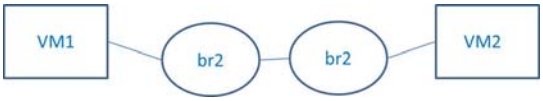


圖 9、 點對點虛擬連接拓樸圖

在 2.3 節裡我們提到[12]已有針對 STT 與 GRE 的效能進行測試，GRE 效能不彰的原因主要是在於封包分段所需的軟體處理上，使得網路吞吐量降低，也使 CPU 使用率飆高，雖然在 NVGRE 標準中為了避免此狀況有進行路徑最大傳輸單元的偵測，但並未詳述實作之細節，因此我們手動將兩實體主機和中間的交換器之最大傳輸單元依巨型封包的定義（Jumbo Frame）[14]設定為 9000，以確保來自 VM 的封包不會被分段，採用 iperf 軟體使用 TCP 單線傳輸，針對有無使用 GRE 隧道及最大傳輸單元為 1500 或 9000 共四種狀況進行測試，結果如表 2 所示。

由表 2 中我們可以看到在一般未經隧道技術及最大傳輸單元為 1500 的情況時，在 1Gbps 的網路環境下可到達 940 Mbps 的效能；當最大傳輸單元調高為 9000 時，可以看到效能隨著單一 TCP 封包傳遞的內容增加而增進到 990 Mbps，但頻繁的傳輸也讓 CPU 使用率由原來的 6%增加到 15%；若使用 GRE 隧道，在原先最大傳輸單元為 1500 的狀況下可以發現網路效能因封包分段的處理而降低到 710 Mbps，且 CPU 使用率也因軟體的隧道封裝增加到 22%；在設定最大傳輸單元為 9000 後，因為解決了封包分段的問題，效能可恢復到 978 Mbps，但 CPU 的使用率也因同時處理隧道及較高的傳輸速度而飆升至 30%。

藉由以上的實測，我們可知調整最大傳輸單元可以有效地解決隧道技術中傳輸效能不彰的問題，但是可能會加重 CPU 的負荷；同時在實務環境裡，目前除了研究網路骨幹外，一般的網際網路環境並未全面採用巨型封包的最大傳輸單元，所以此方式僅限於資料中心或是公司網路內部，若要建立跨網域的隧道，中間只要有一個網路設備沒有調整最大傳輸單元的話，所有長度超過大小的封包都會被丟棄導致無法通訊，所以斧底抽薪的解決方法仍待未來新一代硬體網路卡提供隧道封包的卸載功能，讓針對隧道的軟體處理均交由底層網卡負責，方能讓隧道技術的建置成熟。

表 2、 GRE 隧道效能測試

	TCP Throughput	CPU Utilization
w/o Tunnel MTU=1500	940 Mbits/sec	6%
w/o Tunnel MTU=9000	990 Mbits/sec	15%
GRE Tunnel MTU=1500	710 Mbits/sec	22%
GRE Tunnel MTU=9000	978 Mbits/sec	30%

4. 虛擬網路與主機整合情境案例探討

在本節我們將展示 Open vSwitch 結合 KVM 實作出各種虛擬主機與網路配置的案例。當使用者啟動虛擬機器時，透過動態配置 GRE Tunneling 的技

術讓虛擬機器間依客戶的需求以達到網路互連的目的。

4.1 情境一：兩部實體主機間新增多台虛擬主機

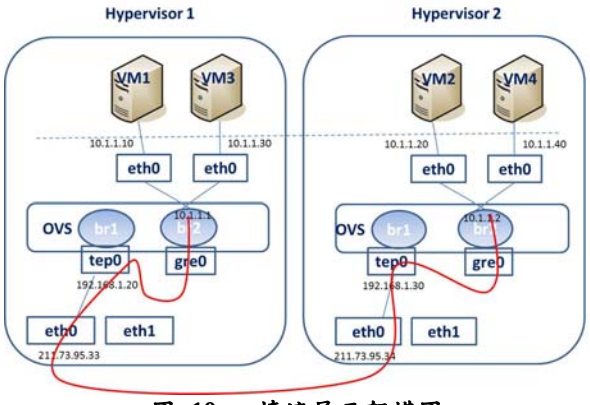


圖 10、 情境展示架構圖

在此情境中，我們延伸第 3 節的環境，原先是兩台虛擬主機分別位於兩部實體主機內部，透過底層虛擬交換器間的隧道互通，此時若配置多台新的虛擬主機，則僅需在實體主機內將這些虛擬主機與虛擬交換器互連即可，如圖 10 所示，此測試環境中，包含兩台實體主機分別為 Hypervisor1 和 Hypervisor2，每台主機下各執行兩個虛擬機器分別為 VM1、VM3 和 VM2、VM4，並屬於同一個網段，模擬經由相同的 bridge(br2)，透過建立專屬的 GRE Tunneling(gre0)讓四台虛擬機器彼此間網路互聯。實際上就像經由兩個 bridge 讓四台虛擬主機讓網路達到互連的目的，如圖 11。

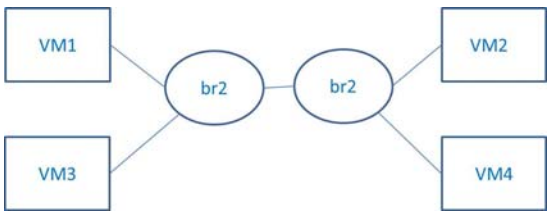


圖 11、 情境一虛擬連接拓樸圖

4.2 情境二：多台實體主機間之隧道互連

上述情境都是在兩台實體主機間建立點對點之隧道連線，若使用者的虛擬主機散佈於三台實體主機上，此時我們就需要建立多條隧道以串連這些實體主機，如圖 12，此測試環境中，包含三台實體主機分別為 Hypervisor1、Hypervisor2 和 Hypervisor3，每台主機下各執行一個虛擬機器分別為 VM1、VM2 和 VM3，並屬於同一個網段。其中 VM1 和 VM2 彼此模擬經由 OVS bridge(br2)，透過指向對端之 endpoint(tep0)所建立的 GRE Tunneling(gre0)讓兩台虛擬機器達到網路互聯。同樣的，VM2 和 VM3 彼此模擬經由 OVS bridge(br2)，透過指向對端之 endpoint(tep0)所建立的 GRE Tunneling(gre0)讓兩台虛擬機器達到網路互連目的。這裡，在 Hypervior2 上 GRE Tunneling 連接使用之 endpoint(tep0)，可同時提供給上述建立之兩條 GRE Tunneling 使用，毋須額外新增兩個 endpoint。就像 VM1 和 VM2 可經由各自的 bridge(br2)互連，VM2 和 VM3 經由各自的 bridge(br2)互連，而 VM1 和 VM3 會經由 VM2 之 bridge(br2)將彼此串起來，讓三台虛擬主機網路達到互連的目的，如圖 13。

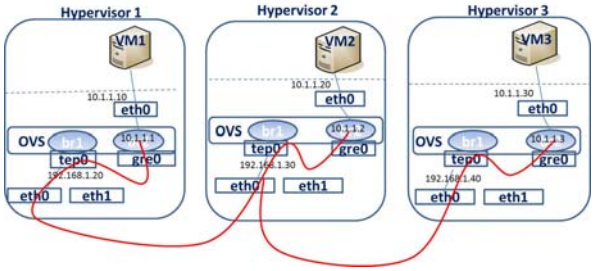


圖 12、 情境二展示架構圖

從圖 13 可看出本情境是將三個 br2 虛擬交換器透過兩條隧道互連，使用者亦可選擇建立三條隧道讓三個 br2 成為完全互連（fully-mesh），但如同第一節所述，第二層交換所使用的擴張樹路徑搜尋法無法有效運用所有的網路連結，在非擴張樹路徑上的連結均處於封閉狀態，待有斷線等狀況發生後才有可能被啟用。

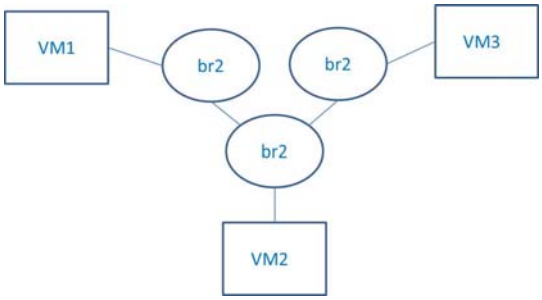


圖 13、 情境二虛擬連接拓樸圖

4.3 情境三：虛擬網路與實體網路互連

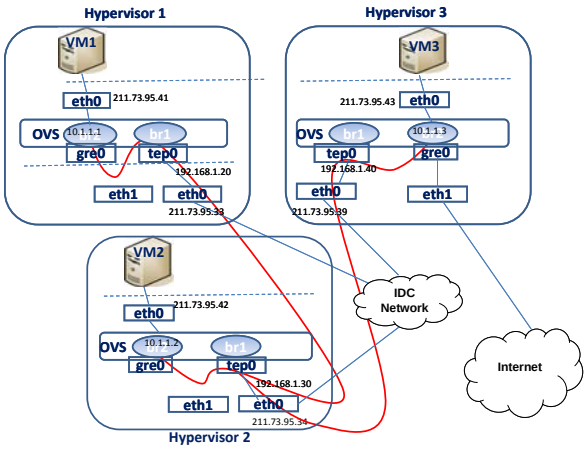


圖 14、 情境三展示架構圖

以上情境均為將虛擬機器置於私有網段內，如

使用者有與網際網路連接的需求，則我們需要在其中一部虛擬交換器與實體網路卡建立連結，以存取外部的網際網路，如圖 14，此測試環境中，包含三台實體主機分別為 Hypervisor1、Hypervisor2 和 Hypervisor3，每台主機下各執行一個虛擬機器分別為 VM1、VM2 和 VM3，假設均配置 Public 網段。我們模擬 Hypervisor3 上 OVS bridge(br2)將其設定使用之介面指定為 eth1(對外 public IP)，利用情境二之測試觀念，模擬讓 Hypervisor1 和 Hypervisor2 上之 VM1 和 VM2 可經由 Hypervisor3 上對外界接之介面(eth1)與外部 Internet 上之某一主機，達到對外網路互連目的，圖 15 為此情境之虛擬拓樸。

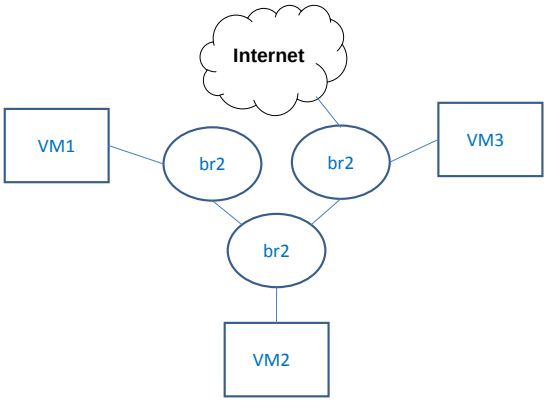


圖 15、 情境三虛擬連接拓樸圖

5. 結論

網路虛擬化技術最終需要與上層虛擬主機的整體配置整合，因此在發展的過程中除了既有網路設備商的規劃之外，尚要考量應用層的存取及操作的便利性，在網路與伺服器間尋求合作的過程中，雖然硬體網路設備嘗試著要主導網路交換的設定，但是在欠缺單一標準下讓使用者畏於投資，因此軟體交換器配合隧道技術隱然成為網路虛擬化的主流，然而隧道所需的表頭會造成額外的封包分割導致效能不彰，這部份也有賴將來新一代網路卡對於隧道封包的卸載功能提供解決方案，本論文整理了現有的隧道技術，並以實例方式對於各種可能的配置案例提供了佈建上的探討，可供整合虛擬主機與虛擬網路環境之參考；雖然網路設備的硬體式方案在此過程中未獲大量採用，但近年來興起的軟體定義網路 SDN 嘗試定義出網路控制的介面，統一的標準將可增加使用者採用之意願，屆時將可強化網路設備與伺服器間的合作關係，同時 SDN 與隧道技術的結合也將會是網路虛擬化下一個演進的方向。

參考文獻

[1] Ranjith Ramakrishnan, “What is cloud computing?,” CUMULUX, http://www.cumulux.com/Cloud Computing Primer.pdf

[2] J. Pettit, J. Gross, B. Pfaff, and M Casado, “Virtual Switching in an Era of Advanced Edges, “2nd Workshop on Data Center – Converged and Virtual Ethernet Switching (DC-CAVES), ITC 22, September 2010.

[3] J. Pettit, J. Gross, B. Pfaff, and M Casado, “Virtual Switching in an Era of Advanced Edges, “2nd Workshop on Data Center – Converged and Virtual Ethernet Switching (DC-CAVES), ITC 22, September 2010.

[4] Karsten Oberle, Marcus Kessler, Manuel Stein, Thomas Voith, Dominik Lamp, Sören Berger, “Network Virtualization: The missing piece,” ICIN conference, October 2009.

[5] IEEE 802.1Qbg - Edge Virtual Bridging, http://www.ieee802.org/1/pages/802.1bg.html

[6] IEEE 802.1: 802.1BR - Bridge Port Extension http://www.ieee802.org/1/pages/802.1br.html

[7] IEEE 802.1: 802.1Qbh - Bridge Port Extension http://www.ieee802.org/1/pages/802.1bh.html

[8] 曾惠敏、李慧蘭、胡仁維、劉德隆、張自恭、黃維誠，「使用雲端虛擬交換器進行網路虛擬化」，TANet2011 論文集，宜蘭，2011 年 10 月。

[9] VXLAN: A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks, Internet Draft, http://tools.ietf.org/html/draft-mahalingam-dutt-dcops-vxlan-04

[10] NVGRE: Network Virtualization using Generic Routing Encapsulation, Internet Draft, http://tools.ietf.org/html/draft-sridharan-virtualization-nvgre-02

[11] A Stateless Transport Tunneling Protocol for Network Virtualization (STT), Internet Draft, http://tools.ietf.org/html/draft-davie-stt-03

[12] The Overhead of Software Tunneling, Network Heresy http://networkheresy.com/2012/06/08/the-overhead-of-software-tunneling/

[13] Open vSwitch, http://www.openvswitch.org/

[14] Jumbo Frame, http://en.wikipedia.org/wiki/Jumbo_frame

TWAREN 網管 Flow 監控機制之設計與實作

梁明章
國家實驗研究院國家高速網路與計算中心
liangmc@narlabs.org.tw

摘要

本文將說明 TWAREN 在 FLOW 資料處理方面的目前已有的成果，包含常規統計分析與報表，特定條件的線上即時查詢機制，並說明嘗試以分散運算方法進行較為隨意條件的線上即時查詢等研究方向。

關鍵詞：TWAREN，FLOW，雲端運算。

1. 前言

TWAREN 網路屬於光電混合網路，設備含括多層，而學研網路的研究使命使得 TWAREN 網路必須時常換代提升讓國內學研界有接觸先進網路技術的機會，為節約國家經費，TWAREN 每次換代並非全面更新打造另一套骨幹，而僅是加入新技術設備，與前數代設備共同運作，幾次下來，TWAREN 網路越形複雜，因此數年前維運團隊就開始自行研發網路管理系統，主要目的就是期望能親自掌握網路管理的核心技術，才能因應頻繁更新的 TWAREN 網路架構與設備，使網路系統亦能隨之擴展成長，而不需要置辦越來越多套業界軟體或甚至全體撤換。

我們針對網管系統的研發主要分下列幾個方向：

狀態異常監測：主要工作就是「異常偵測」，想讓電腦系統判斷「何謂異常」，就必須告訴電腦「比較值」或稱「基準值」，狀態主要分兩類，第一類是二分狀態，例如線路通或斷(Up/Down)，這類判斷比較簡單，第二類則是量化數值，例如流量、溫度、電壓等等，這類判斷就必須定出基準數值，單一基準數，或是兩個基準數(上下水標線)，或甚至是多重基準數(多等級水標線)，因此網管系統對此類異常偵測的靈敏度與正確率，全看基準值是否適合，為了取得合適的基準值，我們將多種狀態數值長期記錄並透過類標準差算法每五至三十分鐘自動推測下次比對所需的基準值，而非使用人工設定固定數值的方法，針對一些波動較大的偵測標的，我們還加上緩衝判斷頻率機制，使得偵測靈敏度提升之際，也不至於損害太多準確率，這個動態臨界基準值計算我們曾發表於 TANet2009[1]。

品質效能監測：這類標的的異常判斷極為模糊，有些甚至是見仁見智，除利用動態臨界基準值計算之外，還需參考使用者感受進行調整。此外，我們發現藉由品質數據的長期變化趨勢，可能推測出品質劣化即將產生障礙，或是惡化趨勢加快可能表示劇烈波動(劇烈波動可視為異常)，因此我們也將此趨勢偵測預測方法應用至網管系統當中，相關成果也發表於 TANet2009[1]。

使用分析與查詢：傳統網路使用分析大部分指頻寬應用在哪些方面，通常是利用 Flow 資料進行分析與統計，常見應用是排序使用者用量 TopN，以及將每五分鐘的平均值送入 MRTG 或 RRD-Tools 做圖表呈現，站在骨幹維運者角度來看，由於 Flow 資料增量速度極快，若要即時監控，需要相當大的計算力才可能追上。我們在這幾年持續進行 Flow 相關的研發，先期開發可預先背景處理的分析與統計，近期則逐漸涉入 BigData 分散計算，嘗試網頁即時隨選查詢是否能實現。

自動控制設定變更：我們曾開發一些自動變更簡單設定的功能，例如當網管系統偵測到線路介面斷線時，自動登入該設備對該介面下達重啟指令，有時候故障會因此排除，無需等待工程師上線來處理。然而要自動進行更複雜的操作卻有極大的風險，因為透過網路連線下指令本身就有斷線的風險，若由工程師操作，萬一半途不幸斷線，以工程師的人類智慧可以應變並補救，然而程式要自動應變那麼多種可能性實在很困難，因此這部份我們暫時就不再深入開發了。

本文將把重點放在 Flow 相關的網管開發，說明我們在這方面已有的成果與未來的開發設計。

2. 設計與方法

我們將 Flow 的處理方式依照即時與非即時區分成三種：

2.1 完全預先處理

一般常規報表屬於這一類，例如每天輸出一次使用者用量排行表、各類應用排行表、連線單位用量排行表，各種 MRTG 與 RRD-Tools 圖表等等，這類事先制定的運算可以在背景定期執行，只要程式

能在定時周期內完成計算，不會拖累到下次的計算即可，這類程式最可能面臨的瓶頸在於讀取資料這一關，由於 Flow 資料量龐大，如果只存一份，要同時進行多組計算，資料讀取會形成瓶頸，解決的方法基本上就是用錢買空間來換取時間縮短，例如多買硬碟空間多存幾份，像 Hadoop 的 HDFS 就是同樣的資料多存幾份來協助加速，複製份數越多，加速就越明顯。

2.2 部分預先處理+部分即時運算

當我們開發好前述完全預處理機制後，有時候會需要查詢某特定時區間內的統計與分析，例如指定某日至某日之間或某時刻到某時刻之間的合計，這種可以事先規範好的查詢條件，可以事先做好前期資料準備，好在查詢條件確定後，能利用這些事先做好的部分資料快速完成計算。

由於近年來使用者習慣利用瀏覽器操作網頁程式，因此這種查詢會面對瀏覽器的接收逾時問題，一般預設是 15 秒，亦即網頁資料如果無法在 15 秒內傳輸完畢，有可能會被瀏覽器當作逾時而中斷，下面將說明我們為了這關鍵 15 秒做了哪些處理。

網管系統每天按照跨洋電路、Internet 互聯電路、連線單位等等個別進行用戶 IP 的用量統計、Port 應用量統計，以及目標地所屬 ASN (Autonomous System Number) 用量統計，下**表 1** 是一些統計數據，表示我們每天面對的 IP 用戶數量，當然這些 IP 日常就包含了不少 Fake-IP 的封包，所以像中山大學的 IP 總量雖然只有一個 Class-B，卻依然每天都統計到七萬多個 IP 用戶，而高屏澎區網在 6 月 3 日更是狂飆到平日的四倍多，也是超過分配 IP 總量，表示當日有比較多的 Fake-IP 疑似攻擊出現。

表 1 統計範圍與用戶 IP 數量舉例表

	歐美研網	亞太研網	高屏澎區網	中山大學
2013/6/1	5331694	956774	773551	70456
2013/6/2	5339895	971099	769770	70591
2013/6/3	5352203	939221	3224229	70786

我們用前述的用戶 IP 用量統計、Port 應用量統計，以及 ASN 用量統計按照每個 IP、PORT、ASN 做關鍵值進行計算，存成定時結算列表，目前儲存日結算表與月結算表，未來若儲存空間足夠的話，預計增加每小時結算表，甚至每十分鐘結算表，這些資料足以進行精確計算，然而，對於在網頁上進行即時查詢的功能來說，查詢者通常不會關心到每一個 IP 或每一個 PORT 的用量，一般查詢者只會關心前幾名，亦即排序後的結果。

數十萬或百萬筆資料的即時排序要在 15 秒內完成並不容易，因此我們必須先排序好，並儲存排序結果，然而考慮到節約儲存空間，我們放棄儲存完整的排序結果，從經驗來看，網路大部分的資源都被少數人用掉的，而下**表 2** 與下**圖 1** 也證實了這個經驗，若只儲存用量超過平均值的名次，則我們僅需儲存前面百分之五不到的名次資料，節省許多儲存空間。

表 2 用量高於平均值的 IP 用戶占比表

IP 占比	歐美研網	亞太研網	中山區網	中山大學
8 月 14 日	0.26%	1.74%	3.69%	5.08%
8 月 15 日	0.41%	1.97%	0.44%	4.34%

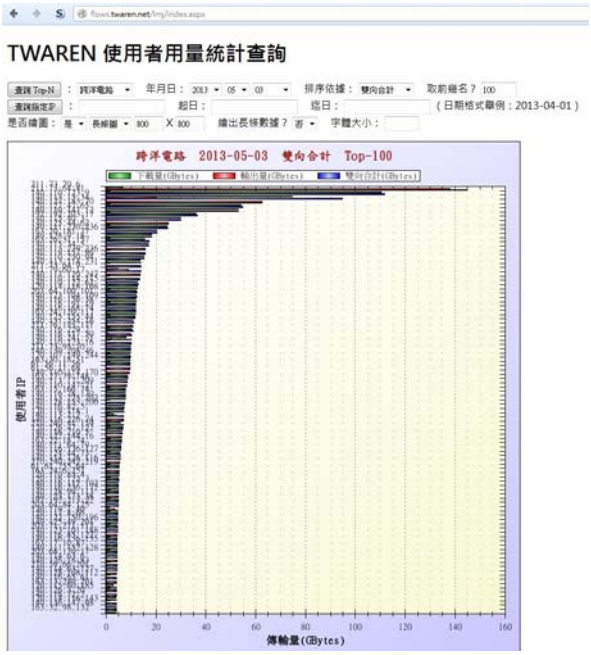


圖 1 頻寬用量集中於少數 IP 大戶的現象

預先處理的儲存結果，其資料大小遠小於 Flow 原始資料，因此在線上即時查詢時，所需消耗的讀取時間也大量減少，也能整批讀進記憶體中再運算，盡量減少等待硬碟的時間，使得一些線上即時查詢能進入關鍵 15 秒內，例如下**圖 2**，就可以線上查詢某特定 IP 在一個半月內的日用量而不會逾時，其實可以查詢更長的區間，只是圖表會拉得太長佔據太多篇幅，所以在此不舉例。

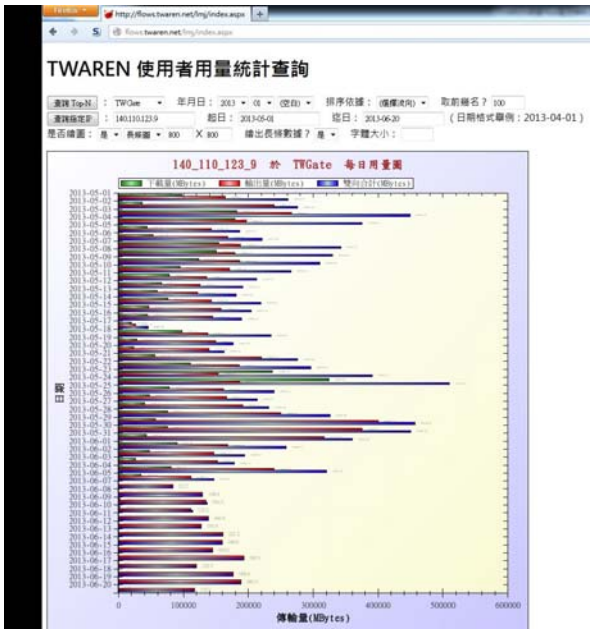


圖 2 特定 IP 用量查詢

目前我們仍持續研發更多利用局部預先處理方法來協助特定的線上查詢，而不會將全部希望都放在分散式雲端運算平台上，因為對我們來說雲端平台是蠻燒經費的一個選擇。

2.3 即時運算

儘管分散計算平台非常燒錢，然而不可否認的是，他確實是最有可能實現大部分線上即時查詢功能的方向，我們拜讀了一篇 IEEE Workshops 的論文[2]，該文探討透過 Hadoop 平台利用 Map-Reduce 方法運算 PORT 應用量統計，並量測時間比照，擷取該論文一張圖表如下**圖 3**，可以發現 Map-Reduce 的 data-node 逐步增加之後，其縮短的時間比率逐漸不如 node 數量之預期，以 TWAREN 跨洋電路一天的 Flow 筆數 300 個 million 來估計，Flow-Tools 約需 10 小時，按下圖比例若想要縮短到 15 秒內，可能需要出動 Google 資料中心那樣的貨櫃車。

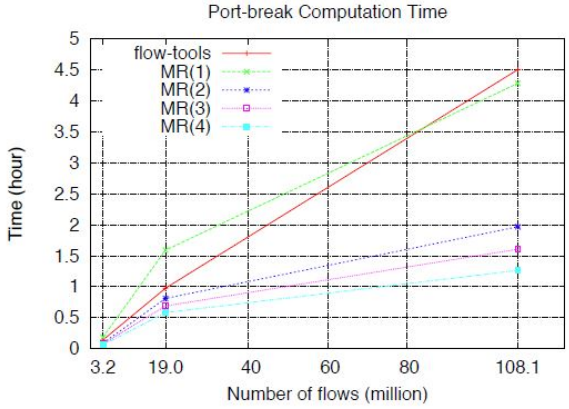


圖 3 Flow-Tools 與 Map-Reduce 耗時比較

因此，我們目前在 Hadoop 上的研究重點暫時不放在即時運算上，而是先將目標放在多種類的統計與分析上，例如，過往我們若想做一天的結算，譬如 IP 的用量排行，一天的資料由單機跑往往需要數小時，倒不是 CPU 太慢，而是因為讀取資料量的筆數迴圈太多次(每筆一次 I/O 要求是相當花費時間的)，而這一個問題若交給 HBase 就能比較快速解決，但問題是，大量的 Flow 資料要放進 HBase 卻需要相當多的時間，對於每日都需要計算新資料的情況來說，其實也要耗費不少時間，不過幸運的是，資料只要花時間進了 HBase，那麼後續不論做幾次不同的統計分析，都可以運用 Map-Reduce 來加速，而不用像傳統方法那樣每做一種不同的統計分析都得重新讀一遍 Raw Data 那麼久。

3. 未來工作

我們仍將繼續雲端分散計算的方向研究，畢竟他是目前最可能達成即時運算的方向，若輔以相當的預先處理，或許可以達成我們的目標，我們將先研究 Hadoop 以及 HBase 與 Flow 資料結合的方法，以及與之輔助的預先處理方式，希望能找到可以較少的 Data-Node 發揮足夠運算力的路。此外，Flow 資料常常是一個 Key (如 IP) 帶至少兩個 Value (In/Out 雙向流量) 甚至多重結構 (例如一個 IP 有 65536 個 PORT，每 PORT 各有 In/Out 雙向流量)，在做比較複雜的統計分析時，尤其是同時須對應多方 IP 與多 PORT 關聯時，要如何組合多個 Key 與值以符合 Map-Reduce 的 Key-Value pair，這也是我們目前研究的課題之一。

參考文獻

[1] 梁明章, 張聖翊, 林孟璋, 謝欣叡, “TWAREN 混合型網路管理系統之進階異常偵測與拓蹼監控技術,” TANet2009, 2009.

[2] Youngseok Lee, Wonchul Kang and Hyeongu Son, “An Internet Traffic Analysis Method with MapReduce,” 2010 IEEE/IFIP Network Operations and Management Symposium Workshops, 2010.

Cross domain VM migration over TWAREN OpenFlow testbed

李慧蘭　劉德隆　胡仁維　陳 敏
國家高速網路與計算中心
{gracelee, tlliu, hujw, minchen}@narlabs.org.tw

摘要

隨著雲端運算的快速發展，雲端應用服務的使用需求激增，為提高雲端服務的可靠度，因此對虛擬機器遷移的需求也因應而生。尤其，為確保雲端服務不中斷，首當其衝要面對的是虛擬機器跨不同網域遷移時的網路問題。OpenFlow 可程式化開放架構之特性，應用在雲端資料中心可以簡化對網路需求的複雜性與提高基礎架構的靈活性。在本文中，利用 OpenFlow 可以彈性依據使用者的定義快速過濾和導向封包的特性，設計一套 Layer3 跨網域之虛擬機器遷移機制，並在 TWAREN OpenFlow testbed 上實驗證明其可行性。

關鍵詞：虛擬機器遷移、跨網域、雲端資料中心、OpenFlow。

Abstract

While the cloud computing technology significantly progresses, it has been quickly gaining popularity at the same time. To ensure its service reliability against hardware and facility failure, the demand for live migrating virtual machines between different network domains is getting increasingly higher. OpenFlow's high programmability and its open architecture can be used to reduce the complexity of the cross domain IP migration and increase the overall architecture flexibility. This study proposed an OpenFlow based cross domain virtual machine migration mechanism and verified it in the TWAREN SDN testbed.

Keywords: VM Migration、VM Migration 、Cloud Data Center、OpenFlow.

1. 前言

近年來雲端服務的崛起， 各式各樣以雲端技術建構的基礎架構服務(IaaS)、平台服務(PaaS)及軟體服務(SaaS)等皆相繼推出，在這波熱潮下，帶動企業及相關業者快速建置雲端資料中心的腳步。根據 CISCO 發佈的 Global Cloud Index [1]報告，預估雲端資料中心的流量在 2016 年將達 4.3ZBs (Zettabytes)，屆時雲端資料中心的建置數量將比傳統資料中心多 1.5 倍，估算自 2011 年至 2016 年的網路流量的成長率將達 44%。

雲端服務業者利用虛擬化技術透過網際網路以服務的型態動態提供給使用者，讓每個使用者依需求取得虛擬資源，可降低資料中心建置成本並提高設備使用率。然而在營運過程中，數量龐大的虛擬機器可能面臨實體伺服機器超載、異地備援、資源分配和負載平衡[2]等問題。為解決上述問題，虛擬機器必須隨時可以遷移，而遷移的範圍不侷限於同一機櫃內、相同網域之資料中心內或跨資料中心之 Layer2 網域內，更擴及跨網域之資料中心，因此凸顯虛擬機器遷移是雲端服務管理上重要的議題。

在跨網域的遷移中需要打破不同網域異質網路架構的藩籬，為確保服務不中斷的無縫遷移，虛擬機器在來源網路的設定必須適用於搬遷至目地機器的網路設定，在[2]中提到利用 IP-in-IP Tunnel 技術可滿足上述虛擬機器跨網域遷移。虛擬機器遷移的許多問題已被正視，大部分虛擬機器遷移機制僅限 Layer2 網域間，如：VXLAN[3]、NVGRE[4]、TRILL[5] 、PortLand[6]等，並存在商業化的解決方案，但須全面佈署新功能之網路設備，成本過高且無法客制化。本文將探討以 OpenFlow[7]支援 Layer3 跨網域遷移的作法。

OpenFlow 技術是允許使用者自由設計創新的網路應用，經由傳送層和控制層分離的核心精神，將自由操控封包的工作交由獨立的控制平台，交換器則專責於封包的傳遞，基於 flow table 上記載的 flow entry 來傳送封包，因此只要將自行開發相關功能載入控制平台，如此即能打造一應用 OpenFlow 技術作到跨網域之虛擬機器遷移。

2. 研究背景

許多研究針對雲端資料中心之虛擬機器遷移提出相關的解決方法，其中也針對雲端資料中心的網路拓撲架構探討，隨著軟體定義網路(Software-Defined Network, SDN[8]) 的崛起，OpenFlow 技術獲得重視，如何應用 OpenFlow 技術，降低雲端資料中心之虛擬機器遷移管理的複雜度，將是未來熱門的研究議題。

2.1 相關研究

傳統網路技術在鋪建新興的雲端資料中心時，應用在雲端運算時略顯不足，例如：STP (生成

樹協議)收斂時間在大型資料中心就顯得過長；此外，STP 為確保無迴圈，而將有些路徑阻斷，也降低頻寬使用率和遏止虛擬機器遷移的便利性。有鑒於此 IETF 制定 TRILL (Transparaent Interconnection of Lots of Links)[5]標準，來取代 IEEE 802.1D 在 LAN 環境避免迴圈的角色。TRILL 是利用路由技術作為 Layer 2 網路的控制平台，在資料中心內的各交換器彼此交換鏈路狀態路由協議(link-state routing protocol)。當有封包須要傳送時，交換器透過路由表做最佳路徑選擇到達目地交換器。另 FabricPath[9]技術與 TRILL 協定相近。

PortLand[6]提出一隨插即用、易於管理和容錯性高的雲端資料中心架構，為進行有效率的封包轉送，每個虛擬機器會根據本身在拓樸中的位置分配到一個 PMAC (Pseudo MAC)位址編碼，交換器根據自行定義的 PMAC 位址查找傳送，當封包要往出口交換器轉送時再由中央控管系統 fabric manger 進行 PMAC 位址和傳統 AMAC (Actual MAC)位址的轉換。因此 PorLand 支援同 Layer2 網域內的虛擬主機遷移。

VL2[10]也採用新定址方式，主機上的應用編址稱為 AA (Application Address)，位置編址為 LA(Locator Address)。在主機上必須額外安裝代理軟體，以將要送出的封包封裝在 LA 位址中，導向負責管理的目錄系統(Directory System)，由該系統進行 LA 位址轉換成 AA 位址並計算路由。當虛擬機器遷移到他處時，雖 LA 位址更動但 AA 位址不變，虛擬機器遷移後仍可正常存取。

VXLAN(Virtual eXtensible LAN)[11]的作法是將虛擬機器的乙太訊框封裝在 IP 封包內(MAC-in-UDP)，新增 24 位元的 VNI 欄位來擴充可使用的 VLAN 個數，僅有相同 VNI 的虛擬機器可以彼此互通，虛擬機器唯一的代號是 VNI 加 MAC 位址，因此即使同一台虛擬機器由於搭配不同 VNI 而屬於不同的 VXLAN，藉此區隔多個租用戶(multi-tenancy)的資料流。資料中心之間以 Layer2 Tunnel 串連， 提供相同 Layer2 網域之虛擬機器遷移。而 OTV(Overlay Transport Virtualization)[12]是 MAC-in-IP 的作法，利用 MAC 位址路由建立 MAC 位址與 IP 位址對應表，其技術與 VXLAN 相仿，但支援 Layer3 網域之虛擬機器遷移，缺點是成本過高和缺乏彈性。

2.2 雲端資料中心網路拓樸

Fat Tree[13]如圖 1，是典型的資料中心三層式(three-tiered)網路架構，該架構自底層往樹根的鏈路頻寬越來越大，有別於一般 tree 架構的鏈路頻寬階相同。PortLand[6]採用 Fat Tree 網路架構。VL2[10]採用 Clos Netwoks 架構，作法是存取層(access layer)交換器以兩條鏈路介接匯聚層(aggregation layer)交換器，每一台匯聚層交換器與每一台核心層(在論文中稱 Intermediate Switch)介接，後者為多對多鏈路，該架構也是三層式網路架構，如圖 2所示。

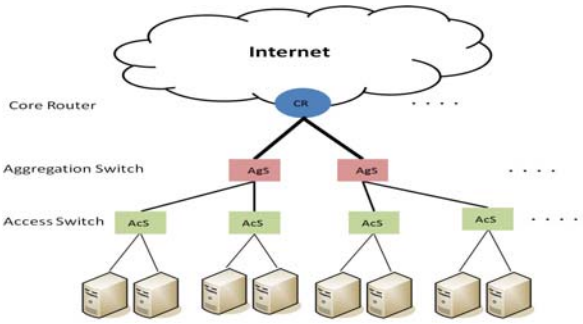


圖1 Fat Tree 架構

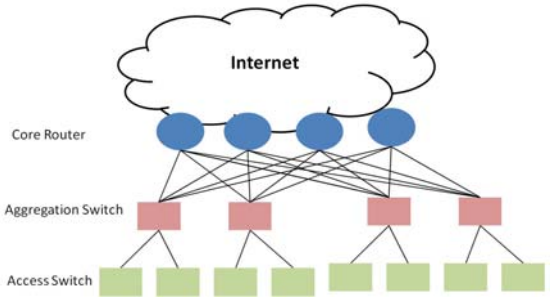


圖2 Clos Network 架構

3. 系統設計與架構

在本節中我們將展示在 TWAREN OpenFlow testbed 上應用 OpenFlow 建構跨網域之虛擬機器遷移的網路架構、方法設計和以實驗情境證明其方法可行性。

3.1 實驗架構

本研究所設計的架構圖如圖 3所示。網域 1 和網域 2 為不同網域且具 L2+L3 混合型網路架構的雲端資料中心。核心層通常是路由器或高階交換器，為資料中心介接至網際網路的邊界，負責 Layer 3 IP 路由查詢與交換工作。匯聚層與存取層則負責 Layer 2 封包轉送，匯聚層把存取層交換器連結匯合聚集後與核心層連結，存取層交換器供伺服器介接。我們設計匯聚層與存取層的交換器為 OpenFlow 交換器，兩個網域之間透過匯聚層供裝之 Tunnel 技術串連成 TWAREN OpenFlow 網路。

本實驗所建置的 OpenFlow 交換器是搭建在 NetFPGA[14]平台上，採用由美國史丹佛大學(Standford University)為了研究下一世代網路技術而開發的實驗平台 NetFPGA。NetFPGA 包含了四個 1Gbps 高速乙太網路通訊埠，使用 Xilinx Virtex-II Pro 50 場域可程式化閘陣列(Field-Programmable gate array, FPGA)為系統晶片，配備兩個 18Mb 的 SRAM 和 64MB 的 DDR2 DRAM，此外也提供兩個 Serial ATA(SATA)接口，可以串連多張 NetFPGA 卡板達成多埠數的交換器與路由器系統設計。本實驗是將 NetFPGA 卡板安裝於 CentOS 5.6 以上作業系

統，該 NetFPGA 是一張 PCI 介面卡，載入 openflow 1.0.4 軟體之後就是一台四埠網路介面 OpenFlow 交換器。

3.2 控制平台

本實驗控制平台採用的控制器是以 Floodlight Controller[15]建置。提供兩種 flow entry 建立方式：

- 主動式 flow 插入(Proactive Flow Insertion, PFI)：為 OpenFlow 標準所支援。可事先撰寫 flow entry 於 Static Flow Pusher 模組中，啟動該模組即可將 flow entry 派送至 OpenFlow 交換器。或以 REST API 提供之介面，手動新增 flow entry 到 OpenFlow 交換器。如表 2中 flow1 和 flow2。
- 回應式 flow 插入(Reactive Flow Insertion, RFI)：為 OpenFlow 標準所支援。當封包到達 OpenFlow 交換器時，比對 flow table 結果為沒有符合的 flow entry，則送往控制平台控制管理，控制平台載入 Forwarding 模組，再依據該模組定義即刻派送適用的 flow entry 到 OpenFlow 交換器，目前於 Forwarding 模組中預設定義有 ARP 請求和 ARP 回應封包皆以回應式 flow 插入(RFI)處理。

本文中除了使用上述兩種 flow entry 建立方式之外，我們也設計 On-demand Flow Insertion(OFI)方式：

- 隨選式 flow 插入(On-demand Flow Insertion, OFI)：利用 Floodlight Controller 內的 LearningSwitch 模組，如圖 4右下方塊所示，可將目的端 IP 位址、MAC 位址和 Switch Port 資訊記錄到 Switch Table。當收到封包後，擷取封包中 DIP 欄位(DIP：目的端 IP 位址)當成搜尋字串，便可獲知 MAC 位址和交換器介接之埠號。最後以 REST API 方式將撰寫好的 flow entry 派送至交換器。

在本架構圖圖 3中，存取層之 OpenFlow 交換器控制端由各別區域內的控制平台控制控：控制平台 1(controller1)和控制平台 2(controller2)，匯聚層之 OpenFlow 交換器則由共同之控制平台控制：控制平台 0(controller0)。

3.3 實驗情境

本實驗將展示位於異地跨網域之資料中心內的虛擬機器遷移到目標主機後，為保持對外服務不中斷，必須維持原有的 IP 位址、閘道和 MAC 位址不變，我們應用 OpenFlow 達到無縫遷移，為便於描述以下網路實驗的三種情境。本文定義以下概念：

- Home Domain (HD)：虛擬機器原本所在的網域，又可稱為虛擬機器的 Home Network。
- Foreign Domain (FD)：虛擬機器遷移到新的網域，又可稱為虛擬機器的 Foreign Network。
- Home Domain VM (HDVM)：位於 Home Network 的虛擬機器。
- Foreign Domain VM (FDVM) ：位於 Foreign Network 的虛擬機器。

下文以圖 3為實驗情境說明，位於網域 1 的虛擬機器有 R 和 S；位於網域 2 的虛擬機器有 U 和 T，當原來位於網域 1 的虛擬機器 VM-S 遷移至網域 2 後，網域 1 對虛擬機器 VM-S 而言是 HD，網域 1 內未曾遷移過的虛擬機器群均屬 HDVM。然而，網域 2 對虛擬機器 VM-S 而言是 FD，虛擬機器 VM-S 在網域 2 內被視為 FDVM。表 1為實驗架構中使用到的設備 IP 位址、MAC 位址資訊，CR1 為網域 1 的閘道；CR2 為網域 2 的閘道等。

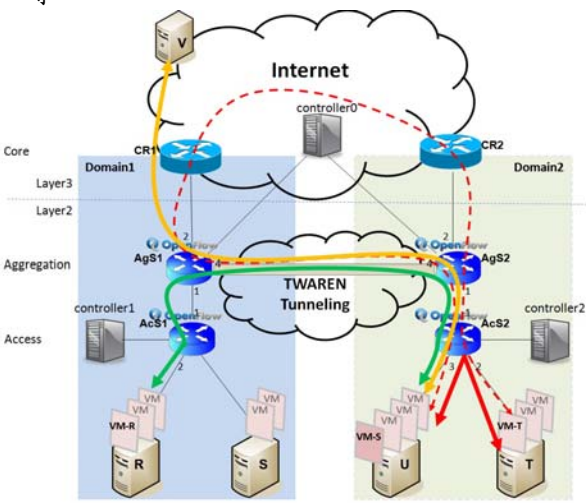


圖3 網路架構與情境示意圖

表1 實驗設備資訊

網域 1		
CR1	IP:192.168.1.254	MAC:00:15:fa:fe:34:41
AgS1	Switch ID: 11:11:11:11:11:11	
R	IP:192.168.1.2	MAC:08:00:27:94:9e:3d
網域 2		
CR2	IP:10.27.82.254	MAC:00:15:fa:fe:34:42
AgS2	Switch ID: 22:22:22:22:22:22	
AcS2	Switch ID: 04:96:52:21:3d	
VM-S	IP:192.168.1.101	MAC:00:15:17:8f:ca:37
VM-T	IP:10.27.82.101	MAC:08:00:27:9b:b3:12

情境一：

虛擬機器 VM-S 遷移至網域 2 後，VM-T 要與 VM-S 通訊時，由於分別屬於不同網域之 IP 位址，因此封包被傳遞到網域 2 的閘道 CR2，如表 1紅色虛線所示，再經由 Internet 上路由表查找，最後送到網域 1 的入口路由器 CR1，再往介接其下之 Layer2 交換器轉送。在本架構中匯聚層交換器 AgS1

和 AgS2 以 Tunnel 連接後，網域 1 的 AgS1 和 AcS1 交換器與網域 2 的 AgS2 和 AcS2 交換器，均屬於同一個 Layer2 廣播網域，於控制平台 2 上啟動預設 Forwarding 模組，當有 ARP 封包經過時，觸發 RFI 建立 VM-S 的 MAC 和對應埠號的 flow table，因此封包一路傳送到目的端。這樣的繞路就是三角路由(Triangle Routing)，這種非對稱性的路徑對於通訊延遲與網路資源浪費帶來了顯著與額外的負擔。尤其資料中心的流量特徵以東西向流量居多，更凸顯其封包傳送延遲造成的效能不彰。

我們在 AcS2 上應用 OpenFlow 可自由操控網路封包流向的技術，縮短通訊延遲與改善頻寬使用率。以下詳述當 VM-S 開始遷移到目的機器 Y 時，步驟如圖 4所示，說明如下：

❶網域 2 的控制平台 2 接收到虛擬機器遷移的 Event 通知，該通知包含 VM-S 的 IP 位址、MAC 位址和閘道的 MAC 位址。

❷將設計好的 flow entry 資訊寫進 Static Flow Pusher 模組。

❸flow entry 被派送到 AcS2 交換器(switch id: 04:96:52:21:3d)的 flow table，即表 2的 flow1 和 flow2。

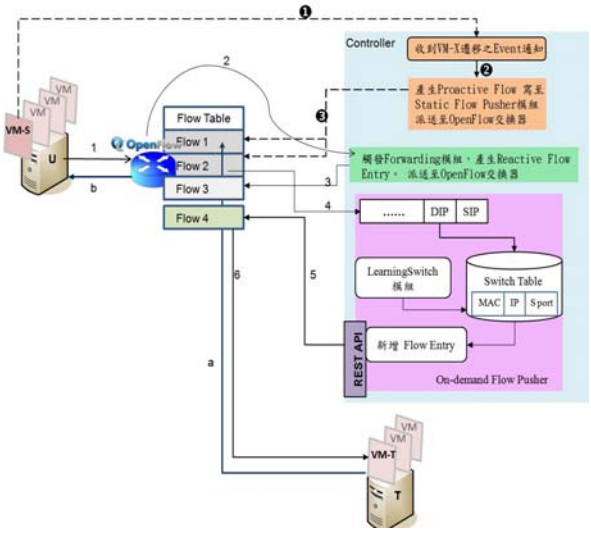


圖4 封包傳送示意圖

flow1 可將目的位址是 VM-S ("dst-ip":"192.168.1.101")，但必須送給網域 2 路由器 CR2("dst-mac":"00:15:fa:fe:34:42")的封包轉向直接給埠號 3。然而，VM-S 要丟往網域 2 的封包，由於目的位址無法事先得知，因此設計 flow2 規則為：來源位址是 VM-S("src-ip":"192.168.1.101")送出的封包轉向給控制平台處理。

接著， VM-S 送出第一個封包給目的機器 VM-T 如圖 4所示，步驟如下：

1. VM-S 發送 ARP 詢問 CR1 之閘道 MAC 位址，封包進到 OpenFlow 交換器，Flow Table 內無符合的 flow entry，送至控制平台處理。
2. 控制平台觸發 Forwarding 模組，以回應式 flowt 插入(RFI) 產生 ARP 廣播用之 flow3，以幫助 VM-S 取得 CR1 之閘道 MAC 位址。
3. VM-S 取得 CR1 之閘道 MAC 位址之後，VM-S 開始送出的封包目的 IP 是 VM-T 的位址("dst-ip":"10.27.82.0/24")，目的 MAC 是 CR1 之閘道 MAC ("dst-mac":"00:15:fa:fe:34:41")，符合 flow2 規則，操作行為(action)是將封包轉向送至控制平台 2。
4. 進入隨選式 flow 插入(OFI) 模組，擷取封包之目的 IP 位址(DIP)當成關鍵字串，進到 Switching Table 的資料庫進行搜尋，便可獲知 MAC 位址和與交換器 AcS2 介接之埠號。
5. 透過 REST API 寫一筆 flow entry 如**表 2** 中的 Flow4 到 AcS2 交換器。
6. 最後傳輸路徑依據 flow4 定義，原應送到網域 1 閘道的封包，直接修改為 VM-T 之目的 MAC 位址並轉向至埠號 2。

VM-S 與目的機器 VM-T 通訊的第一個封包將被送至控制管道的控制平台處理，依上述流程(step1~5)轉送。之後的封包到達 AcS2 交換器時，由於可成功比對 flow4，則不需再送至控制平台處理。亦即忽略優先順序較低 flow2 (priority=3000)。

當 VM-T 反向傳送封包給目的端 VM-S 時，由於目的端 VM-S 資訊在上述步驟❶~❸時，已根據 Event 資訊建立好 flow1，流程如圖 4：

a. 封包進到 AcS2 交換器，比對 Flow Table，符合 flow1 的 flow entry，操作行為是修改目的 MAC 位址為 VM-S，並轉向送到 VM-S 所介接的埠號。
b. AcS2 交換器送出封包。

最後，AcS2 交換器的 Flow Table 有三筆 flow entry，為 flow1、flow2 和 flow4，而 flow3 僅在 ARP 請求時使用，固定時間後會被移出 flow table。因此 VM-S 送包封給 VM-T 的路徑(datapath)最後只會比對 flow4；反向 VM-T 送包封給 VM-S 的路徑(datapath)最後只會比對 flow1，如圖 3紅色實線所示，改善了三角路由的問題。

表 2 控制平台 2 之 Flow 資訊

```
flow1= {
'switch':"00:00:00:04:96:52:21:3d",
"ether-type":“0800",
"priority":"32768",
"src-ip":"10.27.82.0/24",
"dst-mac":"00:15:fa:fe:34:42",
"dst-ip":"192.168.1.101"
"active":"true",
"actions":"set-dst-mac=00:15:17:8f:ca:37, output=3"
}
```

```
flow2= {
'switch':"00:00:00:04:96:52:21:3d",
"ether-type":“0800",
"priority":"30000",
"src-ip":"192.168.1.101",
"src-mac":"00:15:17:8f:ca:37",
"dst-mac":"00:15:fa:fe:34:41",
"dst-ip":“10.27.82.0/24",
"active":"true",
"actions":" output=controller2"
}
```

```
Flow3 = {
 'switch':" 00:00:00:04:96:52:21:3d ",
"ether-type":“0806",
"dst-mac":"ff:ff:ff:ff:ff:ff",
"dst-ip":"192.168.1.254"
"actions":"output=1"
}
```

```
flow4 = {
'switch':"00:00:00:04:96:52:21:3d",
"ether-type":“0800",
"priority":"32768",
"src-ip":"192.168.1.101",
"src-mac":"00:15:17:8f:ca:37",
"dst-mac":"00:15:fa:fe:34:41",
"dst-ip":"10.27.82.101",
"active":"true",
"actions":"set-dst-mac=08:00:27:9b:b3:12,output=2"
}
```

情境二：

與情境一相同的網路架構，如綠色線所示，VM-S 與 VM-R 均屬相同網域，因此與 VM-S 通訊時，傳輸路徑是 AcS1-AgS1-AgS2-AcS2。在情境二中，控制平台 0、控制平台 1 和控制平台 2 載入 Forwarding 模組之後，可自動以回應式 flow 插入模式(RFI)正常通訊。但當數量龐大的虛擬機器需要遷移時，Layer2 廣播網域將拖垮效能，因此本實驗也撰寫主動式 flow 插入(PFI)如圖 5、圖 6所示，並證明可運行。

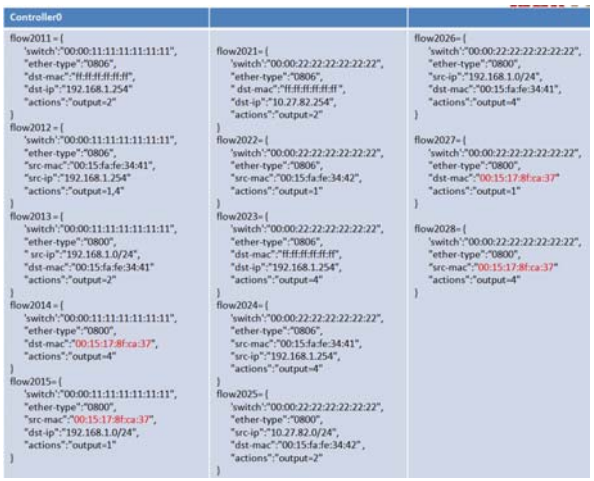


圖5 控制平台 0 之 Flow 資訊(應用於情境二、三)

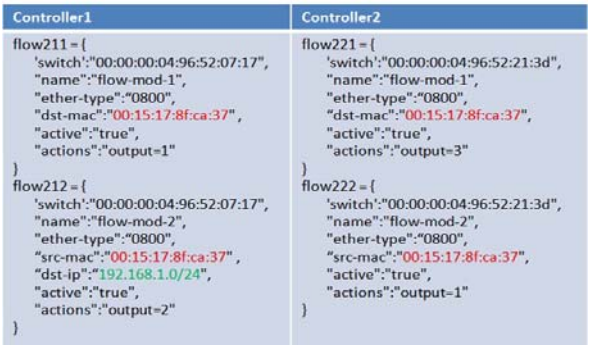


圖6 控制平台 1、2 之 Flow 資訊 (應用於情境二、三)

情境三：

如圖 3黃色線所示，其他網域的機器 V 要與 VM-S 通訊時，由於 VM-S 的網路 IP 位址未異動，經路由表上查找最佳路徑是往網域 1 的邊界路由器 CR1 走，再往 AgS1-AgS2-AcS2 到達目的端。flow entry 設計與情境二相同。

4. 架構分析與評估

由第三章跨網域虛擬機器遷移的情境中所述，我們設計的機制是混合式控制，每個網域之存取層有一專屬的分散式控制平台，因為網域之間的距離可能達數百公里，且虛擬機器遷移後伺服器對伺服器間的東西向流量佔 75%[16]，若由同一個控制平台分送 flow entry 到交換器，將有通訊延遲(latency)過長、彈性不足和服務中斷問題。但為維持 IP tunnel 的建立，匯聚層控制平台則採集中控制，面臨的問題是每一個控制平台之間必需彼此同步。IETF 工作小組提出 SDNi 協定草稿[17]，是 SDN 控制平台同步的初步構想，以 BGP 和 SIP over SCTP 協定的概念作同步交換訊息。

本設計架構以一階層的一對一網域為例，虛擬機器由 HD 遷移至 FD。並經實驗證明可運行。當有兩個以上的雲端資料中心需要交互進行多對多虛擬機器遷移時，如圖 7四個網域為例說明，網域 1 內有 VMx 和 VMa 遷移出去，也會有其他虛擬機器遷移進來。而多階層式的遷移，例如，兩階層的遷移：VMb 位於網域 1 遷移至網域 2(VMB)再遷移至網域 3(VMB')。三階層的的遷移：VMc 位於網域 1 遷移至網域 2(VMC)再遷移至網域 3(VMC')最後再遷移到網域 4(VMC")。多階層式遷移中網域內匯聚層交換器須建立 fully mesh tunnel 連線。

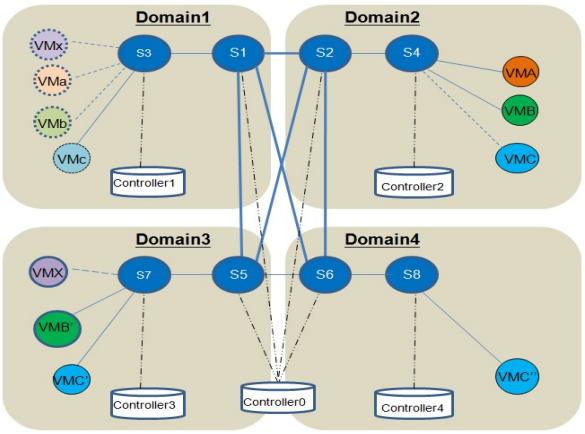


圖7 多對多虛擬機器遷移示意圖

由 3.3 節實驗情境結果可知，情境一時僅須在位於目的端之控制平台 2 撰寫 flow entry，由實驗統計當 FDVM=1 時，新增 2 主動式 flow 插入(PFI)，新增 1 筆隨選式 flow 插入(OFI)。情境二和三：FDVM=1 時，在控制平台 0 上新增 4 筆主動式 flow 插入(PFI)，新增 9 筆回應式 flow 插入(RFI)。在控制平台 1 和 2 上新增 1 筆主動式 flow 插入(PFI)，新增 2 筆回應式 flow 插入(RFI)。表 3和表 4為須要新增到控制平台的 flow 個數。

表3 情境 1 - 控制平台 0 的 flow 個數

Flow Insertion Type	Flow entry number
Proactive Flow Insertion	N+1
On-demand Flow Insertion	N

N = 網域中 FDVM 的虛擬機器個數

表4 情境 2 和 3 -控制平台 0、1、2 的 flow 個數

	Con0	Con1	Con2
Flow Insertion Type	Flow entry number		
Proactive Flow Insertion	3*K+1	K	M
Reactive Flow Insertion	9	2*K	2*M

K = 網域中被遷移出去的虛擬機器個數

M = 網域中 FDVM 的虛擬機器個數

5. 結論與未來工作

在本文中，我們檢視了目前虛擬機器遷移的各種解決方案；PortLand 解決了 Layer2 網域內遷移，VXLAN 解決了跨資料中心的 Layer2 網域內遷移，OTV 解決了跨網域的遷移。而廠商所提供的商業化解決方案，一致性的均須全面佈署支援新協定的網路設備，建置成本過高且缺乏彈性。OpenFlow 可以彈性的根據使用者的需求快速定義網路應用服務，最著名的成功案例是 Google 研發之 OpenFlow 交換器和 OpenFlow 軟體控制平台，可依流量工程計算出最佳路徑，提升 Google 全球資料中心之間傳輸效能至近乎 100%[18]。OpenFlow 應用將會越來越廣泛。而我們在 TWAREN OpenFlow Testbed 上驗證所設計之主動式 flow 插入(Proactive Flow Insertion,PFI)和隨選式 flow 插入(On-demand Flow Insertion, OFI)機制滿足跨網域之虛擬機器遷移的最短路徑。未來將依目前實作之結果，發展出一套自動化的 flow entry 派送軟體安裝於控制平台上，以減少人為設定失誤。尤其，如果遷移的規模更大，需要管理的控制平台複雜度將更高。

參考文獻

[1] http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.html

[2] http://datatracker.ietf.org/doc/draft-khasnabish-vmmi-problems/

[3] Mahalingam, Mallik, et al. "VXLAN: A framework for overlaying virtualized layer 2 networks over layer 3 networks." draftmahalingam-dutt-dcops-vxlan-01. txt (2012).

[4] Sridharan, Murari, et al. "NVGRE: Network virtualization using generic routing encapsulation." (2013).

[5] Touch, Joe, and Radia Perlman. "Transparent interconnection of lots of links (TRILL): Problem and applicability statement." (2009).

[6] R. Niranjan Mysore, A. Pamboris, N. Farrington, N. Huang, P. Miri, S. Radhakrishnan, V. Subramanya, and A. Vahdat. Portland: a scalable fault-tolerant layer 2 data center network fabric. In SIGCOMM, 2009.

[7] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson,J. Rexford, S. Shenker, and J. Turner, “OpenFlow: enabling innovation in campus networks,” ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69–74, 2008.

[8] Lantz, Bob, Brandon Heller, and Nick McKeown. "A network in a laptop: rapid prototyping for software-defined networks." Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks. ACM, 2010.

[9] Scarfo, Antonio. "The evolution of Data Center networking technologies." Data Compression, Communications and Processing (CCP), 2011 First International Conference on. IEEE, 2011.

[10] A. Greenberg, J. R. Hamilton, N. Jain, S. Kandula, C. Kim, P. Lahiri, D. A. Maltz, P. Patel, and S. Sengupta. VL2: a scalable and flexible data center network. In SIGCOMM, 2009.

[11] Mahalingam, Mallik, et al. "VXLAN: A framework for overlaying virtualized layer 2 networks over layer 3 networks." draftmahalingam-dutt-dcops-vxlan-01. txt (2012).

[12] http://www.cisco.com/en/US/netsol/ns1153/index.html

[13] C. E. Leiserson. Fat-Trees: Universal Networks for Hardware-E_cient Supercomputing. IEEE Transactions on Computers, 34(10):892- 901, 1985.

[14] J. W. Lockwood, N. McKeown, G. Watson, G. Gibb, P. Hartke, J. Naous, R. Raghuraman, and J. Luo. NetFPGA-An Open Platform for Gigabit-Rate Network Switching and Routing. In Proceedings of the 2007 IEEE International Conference on Microelectronic Systems Education, pages 160-161, Washington, DC, USA, 2007. IEEE Computer Society.

[15] http://docs.projectfloodlight.org/display/floodlightcontroller/Static+Flow+Pusher+API

[16] Benson, Theophilus, Aditya Akella, and David A. Maltz. "Network traffic characteristics of data centers in the wild." Proceedings of the 10th ACM SIGCOMM conference on Internet measurement. ACM, 2010.

[17] http://tools.ietf.org/html/draft-yin-sdn-sdni-00

[18] http://opennetsummit.org/talks/ONS2012/hoelzle-tue-openflow.pdf

以 ETL 方式建構半導體業 B2B 系統之方法

張永昌　　范金鳳
元智大學資訊工程系
chang.pepper@gmail.com　　csfanc@saturn.yzu.edu.tw

摘要

半導體業上下游廠商的企業流程(Business processes)資訊包括訂單、工單、生產、入庫、出貨、請款對帳款單等。目前多數此類企業流程使用 B2B 平台、點對點開發方式。但此作法面臨兩大挑戰：(1)對外導入時，各客戶有各自不同的 B2B 系統檔案交換規格與需求；(2)對內，因應客戶規格所需要的資料將橫跨各異質性環境系統。所以，供應鏈B2B垂直整合與廠內多元系統的水平整合愈顯重要、挑戰亦愈高。本研究針對此議題，建構一個全方位企業流程資訊整合系統的架構，設計了企業流程資訊通用之 E-R Model Data Mart 結構(schema)，運用 ETL 實作整合異質性系統，能有效地處理半導體企業供應鏈資訊交換與企業內系統整合的問題。初步實作結果顯示此方法可成功地增加資訊分享效益、並提升服務之深度及廣度。

關鍵詞：半導體產業，企業間電子商務，企業應用系統整合。

Abstract

The business processes among the supply chain in semiconductor companies include product order, work order, production, inventory, delivery, bill, etc. Currently most companies use the Peer to Peer B2B platform to perform information transfer and integration. However, this approach faces two major challenges：(1) Externally, different customers may have different B2B system format for exchange. (2) Internally, the data required by the customer may spread in different heterogeneous systems. Therefore, it is essential to integrate B2B supply chain vertically for external partners, and horizontally across internal systems.

This research develops an integrated framework for business process in semiconductor industry. It first designs generic E-R model Data Mart schema for business processes, and then uses an ETL tool to implement the integration of heterogeneous systems so as to effectively handle the supply-chain information exchange. The preliminary case study results show that this approach is successful in enhancing information sharing and IT (Information Technology) service.

Keywords: Semiconductor industry, B2B, enterprise application integration

1. 前言

半導體產業變化急遽、分工專業、競爭激烈，半導體工廠必須達成快、準、好、省的經營方針，因此企業需強化和客戶與供應商之間緊密的關係，以提升競爭力。企業利用網際網路進行與合作夥伴之間企業流程(Business processes)的資訊，如訂單、工單、生產、入庫、出貨、請款、對帳單等狀態資訊溝通，使參與的夥伴間皆能即時獲得相關訊息，以充分協同作業。

過去尚未有眾所接受的 B2B 整合標準，客戶往往自定標準，造成各廠商引用標準之紛雜。導入B2B時面臨內外的兩大挑戰：(1) 對外導入時因各家客戶有各自不同的 B2B 檔案規格與需求，將面臨一大挑戰 ； (2)對內因應客戶規格所需要的資料橫跨各異質性環境系統，又是另一大挑戰。本研究針對此議題，發展半導體封裝廠企業流程之 B2B 系統導入的資料模組與架構技術。

過去半導體導入 B2B 系統是透過點對點方法，大部份只是單純的將客戶的資料匯進來與匯整資料給客戶，如此方式會造成 B2B 系統變成複雜的網狀架構，往往導致成本過高與整體效率過低。所以本研究發展了整合異質系統的共用資料模組與架構的技術，規劃設計整合資料模組的 Data Mart 概念，並運用開放原始碼的 ETL (Extract-Transform-Load)工具來實作完成整合異質性系統的建構方法，可以彈性且較低成本，來達到系統的一致性、擴充性、、及執行效率等好處。

2. 相關背景及研究

2.1 資料市集(Data Mart)

資料市集(Data Mart，以下縮寫為 DM)可視為資料倉儲 (Data Warehouse，縮寫為 DW)縮影或元件。資料市集的重點是只支援某些特定的部門需求或單一目的要求；面向某個特定的主題。若將企業組織內或多個部門的 DM 整合，可發展成完整企業體的資料倉儲 DW，以提供企業重要決策者完整且廣泛的訊息。

本研究利用到 DM 常用的星狀綱要(Star Schema)與雪花綱要(Snowflake Schema) [1]。星狀綱要 (Star schema)，是一種簡單的資料庫設計，有一個主要物件在中央(Fact table)，包含著大量的資料但不重複，其輻射狀地連接其他物件，看似星狀，

故稱之為星狀綱要。

雪花綱要(Snowflake Schema)與星狀綱要類似，差別只在於雪花綱要將各維度資料表正規化(Normalized)，將重複的地方分別以獨立的表格儲存，因此形成多階的資料結構狀態，資料表增加；在查詢時，會因為需連結多個表而影響效率(如圖 1 所示)。

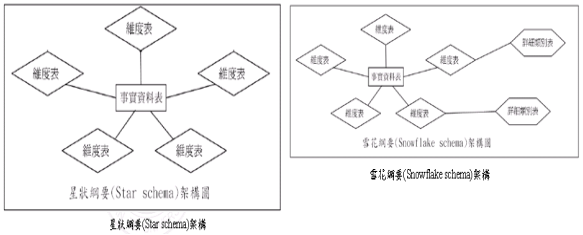


圖 1 DM 資料的結構

2.2 ETL(Extract-Transform-Load)

ETL 即資料數據抽取（Extract）、轉換（Transform）、裝載（Load）的程序。在整合系統架構建置過程中，資料整合轉換(ETL)是最花費時間與人力，也是導入中關鍵要素之一。本研究在 B2B 系統導入中，使用 ETL 工具使企業應用易於更改資料，ETL 程序方式可將不同的系統與來源資料檔案或資料庫所擷取的資料，依據企業之需求及 ER-Model 的設計加以 轉換、整理、清除不需要的資料，將洗淨後的資料轉至目的地 DM 資料庫中，以保留在企業內以利後續使用。

IT(Information Technology)系統資料與 DM 資料除了在記錄不同產品成長階段所留下來歷史資料，還包括使用者所產生的大量資料，及對外部所取得的資料，這些資訊可能來自不同的資料平臺，或一些特定的檔案格式。隨著時間與系統增加，而累計資料越來越多，尤其是在 DM 的資料中心，如此大量資料將造成系統變慢。本研究提出的策略也可針對此部份也一併處理，透過整合的模組與 DM 架構，使用 ETL 的方式並依據訂定的規則來規劃資料保留與封存策略。

2.3 資料交換現況

早期電子資料交換 EDI(Electronic Data Interchange)[2]，透過雙方定義好的規定和格式交換，其後演變成透過網際網路利用 XML[3]格式來傳送資料，但面臨到各企業間各自有不同的商業字彙，有不同的交易規格和不同的 XML。軟體間轉換格式無統一標準，以致於有後續相關的國際電子商務標準，如 RosettaNet[4]與 ebXML[5]等，這些都是以 XML 為基礎來制定電子商務標準。下面簡述 RosettaNet 標準化 B2B 標準[6] 和 ebXML 國際標準[5]。

RosettaNet 協會針對全球資訊、電子元件、及半導體業者發展了產業供應鏈商務標準，旨在形成共同的電子商務語言。RosettaNet B2B 標準具有上層商業處理與下層技術服務的整體架構。依其結構分為三塊：(1)詞典(Dictionary)： 定義交易夥伴與產品描述字典的標準語言，將供應鏈中組織運作的術語標準化。(2) 執行架構標準 (RosettaNet Implementation Framework ，RNIF)：規範了傳輸、通信協定、安全、路由及訊息包裝的方式。(3) 作業程序標準(Partner Interface Processes， PIP)：將商品資訊之收集、維護，產品資訊加以分類、標準化、及電子化。

RosettaNet 標準因使用方式複雜、牽涉技術繁複，給企業『高單價、難導入、維護與學習成本高』的印象，以致許多企業仍然裹足不前。

ebXML (Electronic Business using eXtensible Markup Language) 是由聯合國 (UN/CEFACT) 與 OASIS(The Organization for the Advancement of Structured Information Standards) 兩大國際組織於 1999 年 11 月共同發起了一項名為 ebXML 的計畫，企圖建構一個全球互通性之電子交易基礎架構和電子商務標準。其使用流程如下：參與 ebXML 式企業間電子商務的交易夥伴將其商業處理細節及能力記載在一份稱為「合作協定細節」(Collaboration Protocol Profile,CPP) 的 XML 文件中，並公佈在註冊服務處，以供其他有興趣的交易夥伴查詢。 透過 CPP 的查詢，ebXML 交易夥伴透過協商達到共識，協商後的結果紀錄在另一份稱為「合作協定契約」(Collaboration Protocol Agreement， CPA)的標準 XML 文件中，以做為雙方商業交談的依據。

ebXML 最大困難在於企業需與每一客戶取得協定契約 CPA，來實現交易夥伴間的 B2B 導入；每個不同的客戶，CPA 可能都不一樣。客戶也需要導入 ebXML，而且對於企業內整合效益不大。

3. 研究設計與方法

本研究針對半導體後段封裝廠 B2B 系統企業流程，提出了一個模組化的架構，建置共用 E-R Model 結構來達到 B2B 系統企業流程之整合，並透過 ETL 工具實作。研究的模組架構圖，如圖 2 所示，在半導體上游各家晶圓廠與下游封裝廠資訊，皆透過 ETL 匯整到下游封裝廠企業 DM 內，並共用 E-R Model 結構表。本研究各步驟在下面子節中敘述。

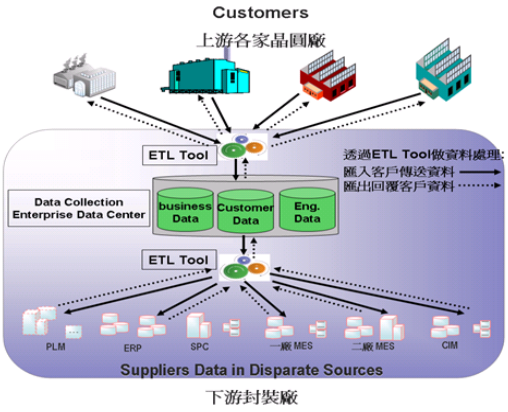


圖 2 上游與下游廠 B2B 系統與對內系統整合架構

3.1 步驟一：需求規格分析

本研究首先分析 B2B 系統在半導體上游晶圓廠與下游封裝廠的企業間通用性的 B2B 企業流程。此企業流程 B2B 系統需求(Business needs)一般包括了訂單資訊、產品資訊、工單資料、下線生產資訊、WIP(Work In Process)在製品流程資訊、成品入庫、出貨、工程資訊、與帳單資訊等傳遞資訊(如圖 3 所示)。若以 UML 使用者案例說明，主動者(actor)為上游晶圓廠 B2B 系統，相關的使用者案例為下訂單、訂單異動、工單通知，在下游封裝廠 B2B 系統角色，相關使用者案例為訂單回覆、在製品 WIP、相關生產 Event 通知、及月初的帳款訊息等。

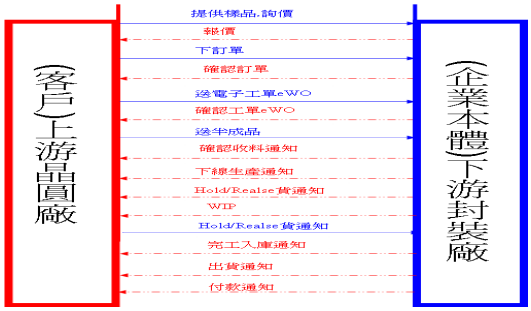


圖 3 半導體 B2B 系統企業流程資訊傳遞需求分析

至於交易流程細節方面，上游晶圓廠與下游封裝廠間 B2B 系統及企業本體內部流程皆以產品批號(LOT_NO)為控管單位，所以系統相關資料傳送及企業流程皆以產品批號(LOT_NO)為出發控管。交易流程如圖 4 所示。從上游客戶開立工單給下游封裝廠通知開使生產，庫存收到上游廠晶圓半成品，在 ERP 系統上做收料確認，記錄客戶批號與數量等資訊、生管依據主生產排程 MPS (Master Production Schedule) 開始用 MES (Manufacture Execution System)系統投入下線生產製造，此時 MES 即開始產生企業本體的生產批號，在生產製造中有各種的生產製造狀況，如生產中 Run、等待 Wait、報廢 Scrap、客戶要求終止生產 Terminate、暫停與釋放 Hold/Release 等，後續經產品檢驗，入成品庫、出貨、以及帳款等都是以產品批號去做系統資料交易，呈現產品以批號的交易流狀態的生命週期(如圖 4 所示)，後續整合 B2B 系統的 Data Model 設計也將用產品批號(LOT_NO)為控管單位。

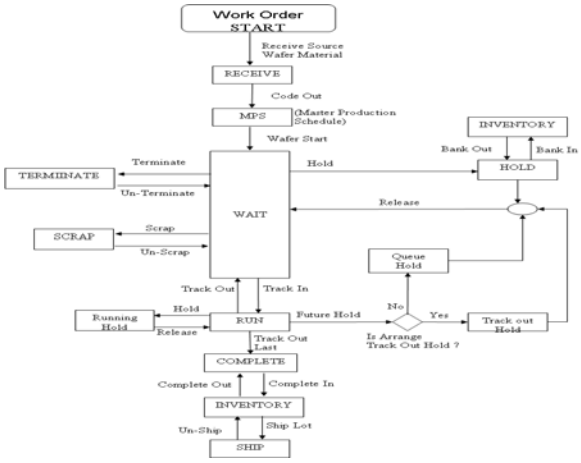


圖 4 生產批號狀況交易圖

3.2 步驟二：資料模型設計開發

此 B2B 系統在整合異質資料庫上有著不同於以往的設計與規劃，不同於傳統直接使用各系統的 OLTP(On-Line Transaction Processing)資料，而是將從不同來源的資料，以半導體產業(產品生產批號)的角度將資料反正規化，匯整成星狀綱要架構 (Star schema)。

此研究將以半導體產業(產品批號)的需求為出發，將所有資料的資訊分為以下兩大類，即不會變動的事件檔(Event Data)，與一直變動現況檔(WIP Data)。其中訂單資訊、訂單回覆、收料通知、工單、下線生產通知、成品完工入庫通知、送貨通知、出貨通知、及最後月初帳單通知這一些都歸納於不會變動事件檔(Event Data)。另一類如在生產製造中客戶會想知道目前當下在製品(WIP)資訊的相關資訊，因為此資料內容會一直變動。以上這資訊都須依據客戶的需求於第一時間傳送資訊給客戶。另有一種報表資訊是客戶生產完所要的即產品生產的歷史資料(Lot history Report)從收料，到下線生產，生產中包含各製造站點的進站(Track In)與出站(Track Out)時間與相關資訊如良品數量、報廢數量、異常時的 Hold/Release 等，最後成品入庫與出貨資訊。當然最重要需要有生產批的基本資料檔供參考。故在設計 Data Model 時可以，以反正規方式分成三類的 DM 星狀綱要架構：(1)事件檔(Receipt Note 收料資訊、Wafer Start 開始下線生產資訊等)。(2) 現況檔(WIP 在製品資訊)。(3) 基本資料檔(PO (Purchase Order) 訂單資訊、WO(Work Order)工單資訊) (如表 1 所示) 。

表 1 產品生產批號分類設計表

	事件檔	現況檔	基本資料檔
(PO)訂單資訊			V
(WO)工單資訊			V
(Receipt Note)收料資訊	V		
(Wafer Start)開始下線生產資訊	V		
(WIP)在製品資訊		V	
(SCRAP)報廢資訊	V		
(Inventory)成品入庫資訊	V		
(Delivery note)送貨單資訊	V		
(Shipping)出貨資訊	V		
(Bill)帳單	V		

其中現況檔，例如生產批現況資料，主要解決上游晶圓廠要求下游封裝廠提供即時的生產現況資料。本研究設計以半導體產業(產品生產批號)的角度將資料反正規化，故在 E-R Model 架構的中間建立一事實資料表（fact table）來呈現封裝廠生產批即時資料現況，故建立生產批即時在製品現況檔(B2B_LOT_WIP_C)，其欄位資訊包括在製品時間的生產批號(LOT_NO)，在那一廠(SITE_ID)與站點(STAGE)，目前良品(WAFER_QTY)、不良品(LOSSQTY)等，都可以詳細記錄匯整後提供給上游晶圓廠。為了更加快速所以建立相關索引參考資料，包含批號報廢記錄(B2B_LOT_SCRAP_H)、異常原因明細記錄(B2B_LOT_ERR_H)、晶圓明細檔記錄(B2B_Lot_WaferContent_H)，這些資訊都與生產現況有關(如圖 5 所示)。

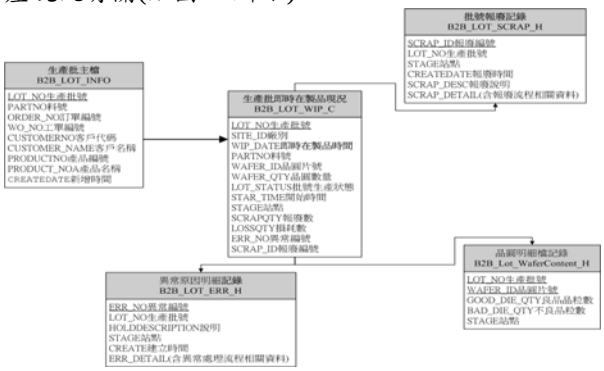


圖 5 WIP 生產批現況資料之 E-R Model

至於事件檔，例如生產批事件，主要記錄上游晶圓廠要求下游封裝廠提供產品的生產事件的資料通知。如圖 6 所示。本研究設計在生產批事件 E-R Model 架構中間建立生產批過帳交易記錄表(B2B_LOT_STEP_H)來呈現封裝廠生產批歷史資料與相關事件，其欄位資訊包括產品生產批號(LOT_NO)在那一廠(SITE_ID)與站點(STAGE)，開始進站時間(STAR_TIME)與有多少數量進站點(INPUTQTY)，完成後出站時間(END_TIME)與有多少數量出站點(GOODQTY)，生產中有無異常或報廢及其數量(SCRAPQTY)與說明，都詳盡記錄下游封裝廠的產品生產歷程，最後則建立維度參考資料表，包含批號報廢記錄(B2B_LOT_SCRAP_H)、異常原因明細記錄(B2B_LOT_ERR_H)、晶圓明細檔記錄(B2B_Lot_WaferContent_H) 等生產歷史資料有關(如圖 6 所示)。

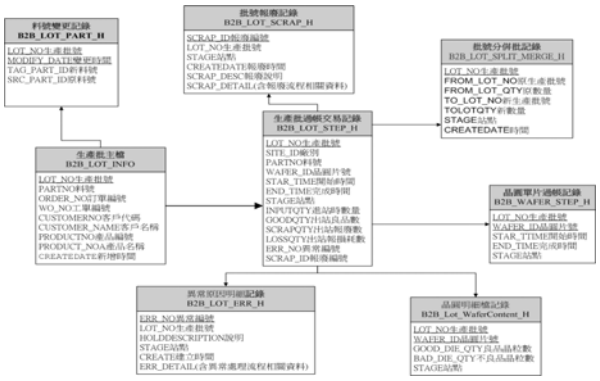


圖 6 EVENT 生產批事件資料 E-R Model

至於基本資料，此部份的來源依據上游晶圓廠提供的工單資訊來設計架構，工單資訊可分為檔頭的主資料表與明細資料表其間的主鍵 PK(Primary Key)與外來鍵 FK(Foreign Key)為工單編號 WO_NO，其主檔欄位資訊包含上游供應商相關資訊與此工單總數量(B2B_EWO_M.WAFER_QTY)與工單時間(B2B_EWO_M. WO_DATE)，工單明細欄位資訊包含工單型態(B2B_EWO_D. WO_TYPE)，(如量產、實驗或工程)等 (如圖 7 所示)。

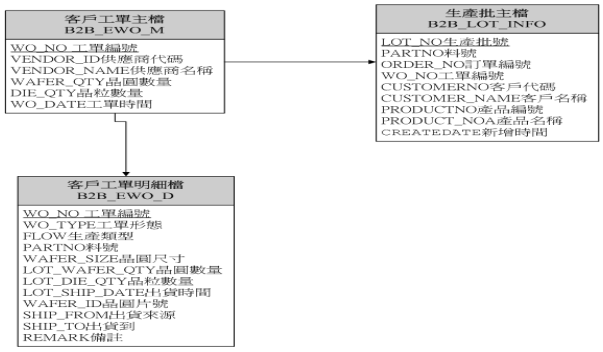


圖 7 生產批基本資料之 E-R Model

3.3 步驟三：ETL 工具並評估

B2B 於整合需求與所需技術可分為三類：應用系統的整合(企業內部異質系統之間的整合)、組織內流程的整合(企業內部異質且分散的商業流程整合)、商業社群的整合(整體供應鏈上下游整合)，其所需要的整合技術各有不同，在對內與外部資料傳輸與轉換技術，介面整合與附加服務技術都不同。本研究研議透過開放原始碼 ETL 工具[7,8,9]支來援系統建構 Data Mart。理想的 ETL 工具需要有下列特性：在資料傳輸技術上 ETL 工具可以支援系統(FTP 或 ODBC 等)、在資料轉換技術上可支援不同資料格式並可處理轉換成所需要的檔案格式(如

XML 或 Excel 格式)、附加服務可外掛自行開發或外購模組(如 Java 或已編譯執行檔)、在商業流程支援技術上可透過 Data Mart 當中介溝通橋樑。根據這些原則，本研究最後選定了 Pentaho kettle ETL[9]工具來實作。

3.4 步驟四：資料庫與系統架構

半導體產業 B2B 系統整合的資料流程圖如圖 8 所示。如企業將依據規範透過 FTP Server 存放客戶檔案，並透過 ETL System 取得檔案將之處理清理轉換匯入 Data Mart，各系統依據需要透過 ETL System 取得所需要的資料，如 ERP 與 MES 皆需要客戶資料，Work Order 工單，透過 ETL System 被 MES 取得所有生產的資料提供給 MPS 主生產計畫排定生產的下線時間，當中有相關的生產事件也會透過 ETL System 寫入到 Data Mart 給相關系統運用，則 MES 系統產品報廢與原因資料皆需給廠內 ERP 系統與客戶 B2B 系統知悉，產品經檢驗符合品質要求後做成品入庫流程，此舉將成品入庫資訊透過 ETL 寫入到 Data Mart，以便提供給 ERP 取用做後續出貨動作，最後依據客戶需求將 Data Mart 的資訊透過 ETL System 處理後傳送到客戶(如圖 8 所示)。

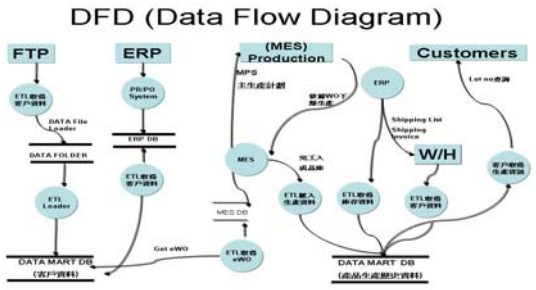


圖 8 設計資料流程圖

本研究建立兩組 DM 匯總資料庫，對外各上游晶圓廠提供下游封裝廠不同來源客戶資料表的匯總資料庫與企業本體內不同系統來源的產品生產相關資料表匯整資料庫，再透過四部份不同目的 ETL System 來處理匯整與傳送資料(如圖 9 所示)。

步驟1. 依據 DFD 及建立 Data Mart。

a. 不同來源上游晶圓廠客戶資料表的匯總資料庫，客戶相關資料 DM(如工單基本資料)。

b. 封裝廠企業本體內不同系統來源產品生產資料匯總資料庫，產品生產相關資料 DM(如事件、在製品資料)。

步驟2. 建構 ETL System 主機來處理資料。

a. 建立 ETL System 主機匯整上游來源晶圓廠客戶資料到 Data Mart，並轉提供相關資訊給工廠生產使用。

b. 建立 ETL System 主機匯整封裝廠企業本體內不同系統來源的產品生產資訊，並依據客戶需求轉拋給客戶。

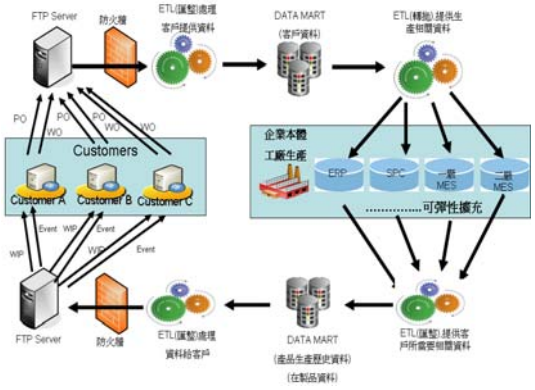


圖 9 上游晶圓廠與下游封裝廠整體系統架構

3.5 資料保存與歸檔

透過 ETL 處理資料建構 Data Mart (DM)會隨著時間與客戶數量增加會導致效能低落且成本負擔增加，故將透過 ETL 處理，並依據符合政府電子法規明確規範資訊保留原則，企業會清楚知道哪些資訊應該保留多久，哪些資訊應該要刪除，以及應該要如何保留資訊。流程說明：

(1)以 IT 基礎設施角度，將企業儲存底層分級，制定保留原則，目前規劃 Disk to Disk to Tape 備份架構。

(2)以客戶批號(LOT_NO)來查詢稽核生產歷程資料的角度重新檢視各類型資料的保存期限。

圖 10 為 一範例。

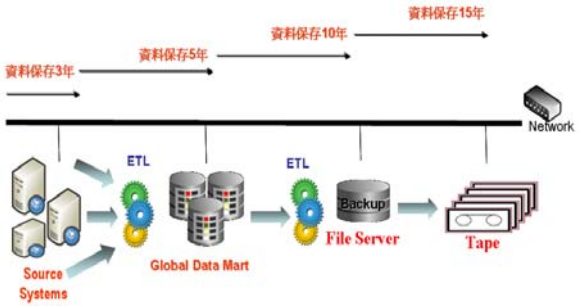


圖 10 資料保留與封存架構

4. 案例實作與效率評估

為應用上章之方法，我們以一實際個案評估所提方法之有效性。個案為半導體供應鏈的上游晶圓廠與下游晶圓封裝廠的 B2B 資料交換為例，提供兩個面向實作：(1)從上游晶圓廠提供 WO(Work Order)電子給下游晶圓封裝廠。(2)下游晶圓封裝廠匯整企業內各系統生產製造中資訊，提供在給上游晶圓廠在製品 WIP(Work In Process)報告[10]。圖 11 顯示部份實作畫面，初步結果令人滿意。

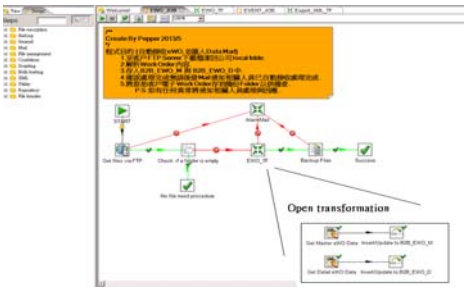


圖 11 ETL 實作取得客戶 FTP 工單資料流程

最後，我們評估傳統點對點的 B2B 方式與本研究整合方式，本研究方式好處如下:

1. 點對點的資料交換往返數減少(如圖 12 所示)。
2. 從開發週期來看，傳統點對點的開發約 4 週，使用整合的架構約 1~2 週，故可縮短開發週期 50%～75%。
3. 從系統維護來看，每年維護傳統點對點分散式 B2B 系統的人力，需 3 個人力， 使用標準整合的架構每年用於維護人力約 2 位人力。
4. 從開發品質來看，自行開發點對點 B2B 系統資料分散在各個異質系統，通常是根據系統的當前客戶與開發需求與模組人員各自規劃，應用系統每增加一個新的模組，這一類需求相關系統常常需要隨之進行相應改動。而使用資料整合的架構及清楚 E-R Model 策略，可以有效保證系統品質，並減少資料不一致與錯誤。

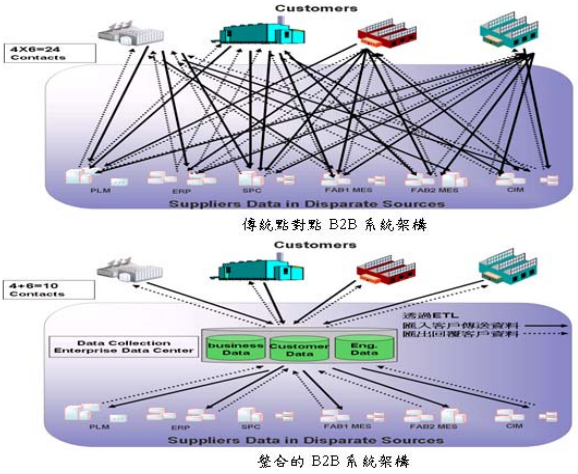


圖 12 上游晶圓廠與下游封裝廠整體系統架構

5. 結論與未來展望

半導體業的企業流程 B2B 系統傳統使用點對點的方法，此方法面臨到上下游垂直整合與企業本體內多元系統的水平整合挑戰；此傳統方法往往無法滿足企業的需求並導致開發成本過的現象，需要撰寫大量的程式碼並進行長時期的系統維護。本研究針對半導體封裝廠的企業流程 B2B 系統設計通用星狀綱要架構的E-R Model (生產批現況資料E-R Model 等)，整合相關企業流程資料並建立 Data Mart， 使半導體上游晶圓廠與半導體下游封裝廠的企業流程資料都可以含蓋，且可以減少 B2B 系統需要不斷與各個廠內系統連線取得資料，降低企業內系統負載。本研究透過開放原始碼 ETL 工具來實作整合異質系統與資料，可快速導入 B2B 系統，且使封裝廠只需短時間，即可建構完整與上游廠企業流程與資訊整合。企業內部流程發生變化後，也不會影響到上游晶圓廠，對於封裝廠內部系統而言也可解決各異質應用系統的難題，亦容許內部應用系統延伸。當然 DM 的資料中心隨著時間與系統增加，而累計資料越來越多，將造成系統變慢。本研究提出的策略也可針對此部份也一併處理，透過整合的模組與 DM 架構，使用 ETL 的程序方式並依據訂定的原則來實作資料保留與封存。總結本方法效率有:節省系統維護成本、整合系統導入完成後，不易受企業流程變動影響。未來將在資安的管理、認證、授權上進一步探討。

參考文獻

[1] 許智誠，資料倉儲的資料建制,中央大學資訊管理學系,2012.

[2] EDI 資訊服務網，http://edi.csd.org.tw/index.htm.

[3] XML 簡介，http://www.xml.org.tw/Plan/XML.

[4] 林玉凡，EB 前瞻產品-企業應用程式整合(EAI)產品之探討，資策會電子商務應用推廣中心-FIND 研究群， 2001.

[5] ebXML.org, “ebXML Technical Architecture Specification,” http://www.ebxml.org/specs/.

[6] 資策會電子商務應用推廣中心，”RosettaNet Overview,” http://www.rosettanettaiwan.org.tw，2002.

[7] 資策會 EB 研究小組，製商整合資訊網企業應用整合，http://ciis.cdri.org.tw/.

[8] T. Jun, C. Kai, F, Yu, T. Gang, ”The Research & Application of ETL tool in Business Intelligence Project,” May, 2009.

[9] The Best Open-Source ETL Tool , http://www.ask.com/explore/opensource-etl-tools-3962.

[10] Yen-Yun Feng，”Development of WIP Monitoring Process Applications in Semiconductor Engineering Chain,” May 2008.

基於 3D 列印技術與社群工藝的文化創意產業生態系

周忠信、張哲綜、陳丁加、楊尚仁、謝翰誼
資訊工程學系數位創意組
東海大學
{jwo, onepot, chencat}@thu.edu.tw

王立志、陳怡文
工業工程與經營資訊學系
東海大學
{wanglc, evinchen}@thu.edu.tw

摘要

本研究提出基於 3D 列印技術所建構的社群工藝概念，發展一個在網際網路上支持文化創意產業的新形態生態系。在此生態系下，創作者可以擺脫預先製作文創作品所需投入的成本，同時又可透過社群工藝，跨技術領域並 3D 列印技術快速製作交付作品。創作者在此生態系下可更專注於作品設計，提供更多文創作品，進而創造更多營收。本論文最後以一實際製作，說明本研究所提之創新生態系特性。

關鍵詞：3D 列印、文化創意產業、社群工藝、生態系。

Abstract

Based on the new concept called social crafting enabled by 3D printing technology, an ecosystem built upon Internet for cultural and creative industry is proposed. Under this ecosystem, cultural and creative designers only need to focus on their designing jobs. Cross discipline production of the design is achieved through social crafting. In this paper, a real implementation is given to show how the ecosystem works.

Keywords: 3D printing, cultural and creative industry, social crafting, ecosystem.

1. 文化創意產業與價值鏈

文化創意產業，或簡稱”文創產業”，近年來頗受全球各國重視，儼然成為繼農漁礦業、工業與服務業之後的第四產業。這個產業的特色，主要在於結合文化、生活體驗、個人創意與工藝技術等，從而製作出具銷售潛力的文化創意商品，或簡稱”文創商品”。

事實上文創商品從其製作與銷售方式，可進一步區分為”文創產品”與”文創作品”。文創產品是指可被量化製造與銷售的商品；文創作品則是由創作者透過工藝技術製作，不是經由量化製造與銷售的產品。一般而言，文創產品可被視為一般商品，其商務模式與傳統產業的製造、銷售等類似。本研究中所討論的文創產業，則是以文創作品為對象。

文創產業的特徵，參考楊燕枝與吳思華論文[1]，主要包括以下幾項：

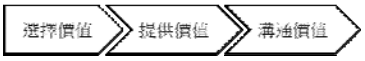
- 多數文創作品的發展過程極為耗時，而且非知名的文創作品，其創作人也無法預測消費者對其作品的好惡反應，同時更無法掌握可能需求量。
- 文創作品的創作者通常較關注創作作品本身而非消費者的需求，反之消費者對文創作品評價卻又極為主觀。因此，消費者對文創作品的感受將決定購買該作品與否，從而導致多數創作者不易獲利。
- 消費者購買文創作品的原因並非基於生理或物質上的需求，而是一種”理性沈溺”的心理需求[2]。換言之，文創作品必須讓消費者產生有助於對其生活享受的認同，而這有時需要作品配合情境體驗與展示。
- 跟其他產業相比，文創作品的消費者存在更明顯的”從眾行為”與”理性跟風”[3]。顯然文創作品的行銷與銷售不同於一般產業，創作者必須面對更大的挑戰。

除了上述特徵外，文創產業與一般產業的差異，更可從價值鏈角度來探討[4]。圖一為大家耳熟能詳的一般產業價值鏈。在此價值鏈下，首先必須從用戶出發，發掘顧客真實需求。再來則依此需求研發設計產品。當研發設計出來的產品被確認滿足需求後，則進一步進入量產製造，大量生產符合品質目標的產品。而生產出來的產品，必須經由市場行銷介紹給廣大用戶，從而順利銷售給所需顧客。而為確保該產品用戶的權益與對產品的滿意度，價值鏈最終仍需提供對產品的維修或使用詢問等後續服務。



圖一、一般產業價值鏈

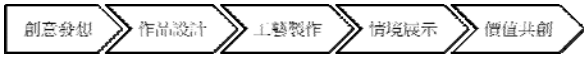
上述價值鏈可以有效解釋高科技產業或民生用品等傳統製造相關產業的價值創造過程，但對於服務業則明顯不足。事實上，服務業的價值創造過程，用行銷價值鏈更容易說明。圖二即為一個行銷價值鏈的示意圖[5]。



圖二、行銷價值鏈

在此價值鏈下，首先評估顧客對價值的認知。所謂價值，是指將顧客眼中對服務渴望所認定的利益，減去顧客自身認知的總付出成本。依據上述價值公式，定位出顧客期望的服務價值。服務提供者再根據顧客渴望獲得的價值需求，設計並提供對應服務。當服務提供者面對廣大顧客時，其過程不只在讓用戶知曉其服務而已，還必須透過行銷廣告或公關等手段，與顧客溝通並幫助他們體認該服務的價值，從而吸引顧客使用該服務。

根據前述對文創產業的特徵描述，文創產業在追求經濟規模上，明顯與一般製造業不同。事實上，消費者購買某文創作品時的動機，也可看成是對該作品體認後而渴望獲得的價值。然而，此價值的計算並不同於服務價值的計算。文創作品究竟不是以解決顧客問題為目的，因此文創作品已也不能視為是一種服務。換言之，前述兩個價值鏈並無法有效說明文創產業的價值創造過程。圖三中所示，是我們進一步提出的文創產業價值鏈。



圖三、文創產業價值鏈

在此價值鏈中，創作者根據自己的創意以及對文化與生活的體驗而發想，再加上對呈現形式的設計與使用的工藝技術等，最終實際設計出獨特的作品。文創作品的價值認定，並不同於一般產品或服務，而是與作品的創意、製作技能、時尚趨勢、文化意涵等有關[6]。換言之，文創作品是因顧客的不同體驗與認知，而有不同的價值認定。因此在價值鏈中，針對製作完成作品提供情境展示，可幫助顧客進一步體驗或認知到該作品所想傳達的創意、時尚、文化或美感等，從而促進顧客對該作品產生渴望。跟一般價值鏈不同的是，一般價值鏈的供應商更注重對顧客售後商品的關注與服務。文創價值鏈則是作品的擁有顧客，會持續關注該作品的創作者，當該創作者、或是創作者的新作品、或是原來作品等越獲矚目，則擁有該作品的顧客將獲得越高價值。因此我們可以說在此價值鏈下，創作者與顧客雙方乃是一種"價值共創"的關係。

2. 文化創意產業的挑戰

有鑑於前述文創產業價值鏈的特殊性，同時考慮文創作品以下四個特性：

1. 由創作者的創意而非消費者的需求主導作品；
2. 作品不是以大量製造方式生產，而是透過工藝技術打造，具明顯獨特性；
3. 創作者規模通常不大，無法有效觸及潛在消費者並誘發其對作品的感受。
4. 作品的價值不在實際應用，而在引起顧客的心理渴望與沉溺；

若再特別考慮作品的獨特性，對於知名的創作者而言，事先完成實體作品並不構成問題。因為從眾性與理性跟風，可以確保該作品最終賣出。但對於一般創作者而言，卻難以依此維生。因為該作品若無法獲得青睞，則對事先投入製作作品的成本，將可能造成無法回收的窘境。因此，文創產業確實很難依據一般產業模式經營。面對上述挑戰，本論文認為唯有創新文創產業的經營思維，才有機會使得文創產業真正成熟。

在討論可能的創新作法前，首先根據價值鏈來看，文創作品的產出過程可分為兩個階段，分別是尚未被實體化的"作品設計" (intangible design)以及工藝製作出來後的"實體作品" (tangible work)。將文創作品分成非實體設計以及實體作品兩面向，將有助於以下討論。

首先，在網際網路時代下，儘管單一文創作品非名家設計，但在"長尾理論" (long-tail theory) [7]支持下，即使再無名氣或是特殊的作品，只要有機會在網路上被發現，那麼網路世界的某個角落，始終存在著某個可能購買該作品的顧客。甚至即使實體作品尚未被實際製作出來前，只要可以將非實體的設計在網際網路上，透過虛擬技術將之情境化地呈現出來，仍可能吸引消費者並誘發其對該作品的心理渴望。當作品以非實體的設計被購買後再進行實體作品的製作，將可大大降低預先投入的實際成本。此模式改變作品作為實體的獨特性限制，讓創意本身即可獲利，而非因為作品實體的唯一性才能獲利。

上述創新模式存在兩個關鍵挑戰：其一在於如何確保非實體的設計與實體作品的一致性；其二，實體作品受限於工藝製作過程，如何快速產出已被顧客購買的實體作品。這兩個挑戰本來並不易克服，但是在"3D 列印技術" (3D printing)的快速成熟下[8]，卻變得頗為可行。首先，3D 列印技術是基於 3D 設計模型而列印出成品，因此可與原始設計幾乎不存在任何落差；同時，若將 3D 列印技術與近幾年快速興起的"社群網路服務"(Social Network Service, SNS)相結合，將可利用社群網路力量，發展出支持快速且具彈性工藝的"社群工藝"(social crafting)概念。換言之，在 3D 列印技術以及社群工藝下，同時借助網際網路力量結合文創作品的創作者、製作者以及消費者，我們可以為文創產業創新發展出一個全新的生態系(ecosystem)概念。

本文往下首先介紹 3D 列印技術與社群工藝，緊接著解說本文所提出的創新文創產業生態系，並以一實際案例輔以說明。

3. 3D 列印與社群工藝

2011 年 6 月美國啟動"先進製造夥伴計畫"

(Advanced Manufacturing Partnership, AMP) [9]。此計畫目的在於建立美國在先進製造技術的領導地位，從而創造高附加價值的工作機會，並期望將現況大量 out-sourcing 的美國製造業轉型而成 in-sourcing。其中 AMP 計畫最優先被選出的主題，就是被”經濟學人”(The Economist)稱為第三次工業革命的”先進加法製造技術”(Additive Manufacturing, AM) [10]。

先進加法製造技術又可稱為 3D 列印技術，是一種數位列印製作三維固態物件的技術。其製作方式是透過多層堆疊方式，一層一層的來構建目標物。3D 列印技術起源於 1970 年代，技術包含選擇性雷射燒結(Selective Laser Sintering, SLS)、直接金屬雷射燒結(Direct Metal Laser Sintering, DMLS)、電子束熔融(Electron Beam Melting, EBM)、光固化成型 (Stereolithography, SLA)、層疊實體製造(Laminated Object Manufacturing, LOM)、以及融熔沉積成型(Fused Deposition Modeling, FDM)等[11]。隨著近幾年 3D 列印技術的進展成熟，材料的選用逐漸由紙材、樹脂、陶瓷至金屬。不同的 3D 列印技術有其對應選用的材料。同時不是所有的 3D 設計模型，皆可被任一 3D 列印技術與材料製作出來。3D 設計模型基本上要先被轉化成 3D 列印模型，才能被驗證是否可以製作。

3D 列印技術的出現，改變過去傳統浪費材料的切割或去除加工技術，取而代之以材料的堆疊及後續固化技術來形成產品。3D 列印此一創新性技術，將會帶動許多產業供應鏈的重大轉變[11-13]。3D 列印技術在改變傳統製造問題上，更擁有以下的創新價值：

- 快速：例如 Shapways 運用 3D 列印技術，2010 年 ipad 上市後第四天，就生產並上市第一個 ipad 保護套。
- 降低風險：搭配社群媒體的擴散效應與使用者互動機制，商品上市前可以先做市場調查，上市後可以依照消費者回饋調整商品設計，因為錯估而造成的庫存風險大幅降低。
- 特殊設計商品化：3D 列印技術的堆疊製造方式，可讓一些因特殊設計而無法開模製造的產品也能被生產出來。

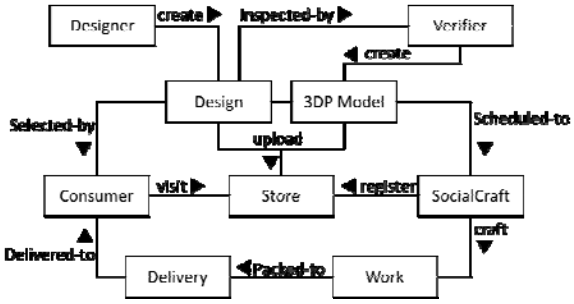
根據上述 3D 列印技術特性，近年來”社群製造”(social manufacturing)或”協同製造”(collaborative manufacturing)也越受矚目[10]。這些新創製造業的特色在於高技術密集而非人力密集，強調”用戶體驗”(user experience)的價值服務而非純粹生產製造。3D 列印技術成為社群製造的關鍵核心，主要在於透過該項技術可大量改善產品從設計到製造過程中，複雜的鑄模成本、大量卻無法客製化的製造程序、以及最終產品與原設計差異無法預估等問題。

將社群製造的精神用於文創產業，如前一節所述我們將之稱為社群工藝。社群工藝強調社群中的各式工藝提供者，根據消費者對文創作品所展現的價值渴望，提供特殊化的工藝製作服務。同樣地，面對無法事先投入的高成本模具開發或是客製化製作，同時又需保障最終作品與原設計豪無差異等，3D 列印技術在社群工藝上更顯優勢。

4. 基於社群工藝的文創產業生態系模型

圖四是本研究以領域物件模型(domain object model)技術所建立的創新文創產業生態系模型。在此模型中，矩形代表參與本生態系的領域物件；連線代表兩領域物件間的關聯與意義；關聯上的箭號則指出兩領域物件間的關聯方向。

在此圖中，Design 代表某一文創作品的非實體設計，而 Work 則是該非實體設計的對應實體作品。另外，Store 是此生態系中各式文創作品設計的集中商店，同時也是文創作品設計者(Designer)、文創作品消費者(Consumer)、文創作品社群工藝(SocialCraft)、與 3D 列印模型檢驗者(Verifier)的共同合作處。

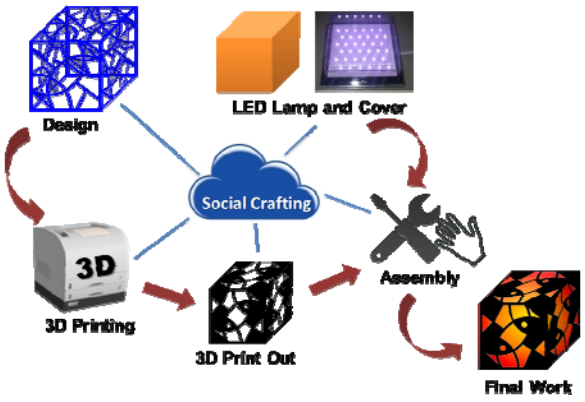


圖四、創新文創產業生態系模型

在此模型下，設計者首先創作其文創作品的非實體設計，並將尺寸、材料等資訊一併上載至商店。生態系中的檢驗者獲得設計者同意後，根據設計與相關選定的尺寸與材料等，將原始設計轉化成 3D 列印模型 3DP Model，從而確認其設計可被選定的 3D 列印技術與材料正確無誤地製作出來。若該 3D 列印模型經檢驗確認無法被 3D 列印，檢驗者將回復設計者其設計的瑕疵處，再由設計者重新修改設計，直至順利通過檢驗始可上架。由於 3D 列印模型涉及對 3D 列印技術限制的理解，因此並非文創作品設計者所在意。

消費者從已上架的作品中，透過虛擬情境展示選定其喜好作品後，商店將提供多個可為此設計代為 3D 列印與相關工藝製作的社群工藝服務。消費者根據各服務所提供的費用與交期等資訊，選擇服務提供對象。消費者所需付出費用，包括作品設計者、3D 列印模型檢驗者、運送包裝以及所有的社群工藝服務等費用。在此生態系下，不同專業者彼此間，可以各盡所能、各取所需。

為進一步說明此生態系模型，圖五是一個基於 LED 燈的室內文創作品生態系架構圖。在此生態系裡，除了燈外觀的文創作品設計外，尚涉及數位技術創新的 LED 燈底座設計。消費者可以選配燈與燈座，待確認後再行 3D 列印與組裝交付。圖六所示，是此案例的實際作品呈現。



圖五、案例架構圖

在此案例中，消費者從作品設計原稿中，選擇一個雙魚座的非實體設計。同時，該消費者也選定某一燈座後，透過此生態系媒合，首先經檢驗者設計並確認 3D 列印模型無誤、並與選配的 LED 燈座正確搭配後，生態系透過虛擬技術提供該作品之網路虛擬情境展示。當消費者對該作品產生心理渴望並確認價錢與交期後，此作品即刻正式進入工藝製作。透過 3D 列印技術，從選定到完成整個作品的製作週期，可於一日內即順利完成。



圖六、案例實際作品

5. 結論與未來方向

本研究首度利用 3D 列印技術搭配社群工藝，並利用社群網路技術創新發展一個可以支持文創產業的新形態生態系。在此生態系下，文創作品的創作者可以擺脫預先製作作品所需投入的成本，同時又可快速交付消費者購買的作品。創作者因為可以更專注於作品設計，所以可以提供更多的文創作品，進而創造更多的營收。而生態系中的社群工藝者，透過運用 3D 列印技術，可以開設類似過去到處都有的影印店，提供 3D 列印代工服務。消費者除可獲得更多的設計選擇外，同時也可以依自己所好指定 3D 列印服務。

本論文針對文創產業生態系進行初期探討。未來應可更進一步結合軟體技術，針對各種文創作品，提供消費者於選定作品後，自行再次客製設計與製作的能力，真正發揮 3D 列印技術的高彈性、快速、以及高度客製生產的特性，進一步讓廣大庶民參與文創作品的設計與製作。

ACKNOWLEDGMENTS

This research was supported by the program of Global Research & Education on Environment and Society (GREEnS) of Tunghai University.

參考文獻

[1] 楊燕枝，吳思華，“文化創意產業的價值創造形塑之初探，” 行銷評論, 2005, 第 2 卷, 第 3 期, pp. 313-338.

[2] Caves, R. E., Creative Industries: Contracts between Art and Commerce, Cambridge, Massachusetts: Harvard University Press, 2000.

[3] Devenow, A. and I. Welch, “Rational Herding in Financial Economics,” European Economic Review, 1996, Vol.40, pp.603-615.

[4] Porter, M., Competitive Advantage: Creating and Sustaining Superior Performance, New York: Free Press, 1985.

[5] Anterasian, C. and L. Phillips, “Discontinuities, Value Delivery, and the Share-Returns Association: A Re-examination of the “Share-Causes-Profits” Controversy,” The Marketing Science Institute, MA, 1998, pp. 88-109.

[6] Crossland, P. and F. I. Smith, “Value Creation in Fine Arts: A System Dynamics Model of Inverse Demand and Information Cascades,” Strategic Management Journal, 2002, Vol.23, pp.417-434.

[7] Anderson, C., The Long Tail: Why the Future of Business Is Selling Less of More, New York: Hyperion Books, 2006.

[8] Bird, J., "Exploring the 3D Printing Opportunity," The Financial Times, Retrieved, 2012-08-30.

[9] Executive Office of the President, “Report to the President on Ensuring American Leadership in Advanced Manufacturing,” President’s Council of Advisors on Science and Technology, June 2011.

[10] The Economist, “A Third Industrial Revolution,” April, 2012.

[11] David L. Bourell, Ming C. Leu, David W. Rosen, “Roadmap for Additive Manufacturing Identifying the Future of Freeform Processing,” Published by The University of Texas at Austin, Laboratory for Freeform Fabrication Advanced Manufacturing Center, 2009.

[12] Bak, D., "Rapid Prototyping or Rapid Production? 3D Printing Processes Move Industry Towards the Latter," Assembly Automation, 2003, Vol. 23, Iss. 4, pp. 340-345.

[13] Dimitrov, D., K. Schreve, and N. de Beer, "Advances in Three Dimensional Printing – State of the Art and Future Perspectives," Rapid Prototyping Journal, 2006, Vol. 12, Iss. 3, pp. 136-147.

相容於 NFC 之匿名行動付款協定

羅嘉寧[1]　楊明豪[2]　黃思穎[2]　蔡卓倫[1]
[1]銘傳大學電腦與通訊工程學系
[2]中原大學通訊工程碩士學位學程
deer@mail.mcu.edu.tw, mhyang@cycu.edu.tw, kobebryand76@gmail.com, luen19881015@gmail.com

摘要

從電子付款服務已廣泛的被人們所使用。演進到行動付款服務，手機構物、轉帳、NFC 付款等。NFC 付款服務，則可能曝露許多敏感的個人資訊，危害使用者之權益。個人隱私問題實為行動付款服務之一大課題。

本論文提出一個以 NFC 為基礎之匿名行動付款協定，以匿名行動付款方式結合 NFC 手機，具有以下特點：(1)便利性：使用者僅需擁有 NFC 手機取代信用卡、現金，減輕消費者出門的負擔，加快結帳速度。(2)不可連結性：商家只會拿到一具短時效之虛擬信用卡資訊，無法從多次交易紀錄分析並連結至使用者身份。TSM 雖擁有使用者之消費資訊，然而其僅擁有使用者提供之銀行匿名帳戶，無法得知真實使用者之銀行帳戶資訊。而銀行端亦僅能得知使用者利用 TSM 付款，並無法得知使用者之消費紀錄。(3)匿名性：除銀行知曉使用者之真實身分外，使用者對 TSM 及商店皆匿名。(4)不可否認性：所有之帳戶註冊訊息、虛擬信用卡之製作及交易訊息皆須進行數位簽名，達成不可否認性。

本論文之 NFC 為基礎之匿名行動付款協定，利用 TEE 和 MTM 解決 NFC 行動裝置之軟硬體執行的安全性問題，NFC 手機中的安全元件(Secure element, SE)結合發展出一個具備認證(Authentication)、授權(Authorization)及稽核(Audit)的匿名行動付款系統。

關鍵詞：NFC、MTM、TEE、EMV、匿名付款系統

1. 前言

隨著無線網路和行動通訊的快速發展，及智慧型手機、平板電腦之大量普及，行動電子商務(Mobile Commerce, M-commerce)[1][2]亦隨之盛行。行動電子商務[3]使用者可利用隨身攜帶之智慧型手機或平板電腦於開放的網路環境下進行各種商貿活動，如網路購物、網路拍賣、影音租賃、線上電子付款等。

對於一般使用者而言，行動電子商務之導入將會提高個人生活的方便化、自由化、與個人化；對於企業而言，導入行動電子商務將增加顧客資訊的正確性與效率性，並藉著準確的顧客分析進而得以提高顧客的忠誠滿意度。

然而在行動電子商務中，付款機制一直是一個重要議題。雖然現今之智慧型手機已可提供強大運算能力和存儲能力，然而付款機制大部分仍沿用傳統付款方式：如使用貨到付款、自動提款機(ATM)轉帳、信用卡、小額電子貨幣儲值等。近年來許多學者提出行動付款[3][4][5][6][7][8]機制，希望使用者能透過簡單的操作並能夠進行個性化的應用程序，以滿足使用者的快速付款需求，以取代信用卡或現金等傳統付款機制，增加消費者於付款上之便利性。此外行動付款服務同時也增加了商家和消費者互動的管道：商家可以藉由行動付款，推出更加豐富、個人化的廣告和折扣方案；行動付款也將進一步刺激行動商務，創造更多的應用和商業模式。

在各種行動付款之機制中，Chen 等人[5]提出以 3G-UMTS 為基礎之付款機制，方法側重於傳統的店內付款環境，與實體和隨後的值得信賴的交易正在通過 3G 和 USIM 安全服務之間的相互驗證。用簡單的方法來實施，同時提供合理的安全保護，以及便於用戶使用的移動支付系統。行動付款應用程序正在開發的在線和店內購買，近場通信(NFC)技術允許在現有的非接觸式應用的基礎設施，如銷售點終端（POS）用手機付款為一體的移動設備。結合現有的 3G 加密演算法，除了 USIM 卡的標識和認證功能的，與 NFC 技術來實現一個行動付款系統。系統可以用當前的 3G 基礎設施，並提供更好的可擴展性和無處不在的行動付款服務。使用交易正在通過 3G 和 USIM 安全服務之間的相互驗證，因此消費交易隱私全曝露在電信業者，電信業者可從多次交易紀錄分析並連結至使用者身份。

Toorani 等人[9]提出一個安全的簡訊行動付款協議，以簡訊付款則是另一種經由手機購物的方式。以小額交易，沒有能力設置專屬的金流服務平台，就可以透過簡訊付款來交易。消費者只要鍵入手機號碼，商家將會利用交換簡訊的方式，讓消費者確認交易金額。這筆金額最後會出現在消費者的手機帳單，消費者不需要動用現金或信用卡。交換簡訊缺點重覆傳送交易訊息、偽造的交易簡訊。

另外 NFC（近場通訊）是時下最受矚目的行動付款技術，如電子錢包，為用戶提供行動付款服務，還得保證隱私安全性。

Martínez-Peláez 等人[7] 提出小額行動付款協議：提款和付款匿名，利用匿名電子現金基礎上使用小額行動付款的實用的協議，為客戶提供匿名性和不可連結性。移動在協議中使用的現金，可以是不同的價值及面額。經由銀行簽署它與特定的私鑰。該銀行存儲電子現金的值和對應的公鑰之間的關係。該協議避免重複消費和偽造攻擊。客戶可以使用匿名證書進行身份驗證使用 WTLS 協議不透露個人信息。銀行擁有使用者之消費資訊，得知客戶消費資訊的隱私。

Kungpisdan 等人[10]基於安全帳戶的行動付款協議，提出一個安全帳戶為基礎的付款協議，這是適用於無線網絡。擬議的協議採用對稱密鑰的操作要求較低的計算在所有參與方比現有的支付協議。擬議的協議也滿足基於公共密鑰的付款協議，如 SET 和 IKP 交易安全性能。

廖等人[11]跨網域之匿名行動付款機制，提出有關行動付款機制，在行動通訊中讓使用者與不同商家進行消費，消費方式用可分割的電子現金，提供使用者匿名性需求，在手機網域進行消費付款，也讓電信業者保有電子現金發行權，提升現實環境的可行性，採用離線驗證和支後追蹤達成付款驗證。電信業者知道使用者的付款記錄，存放手機電子現金安全保護。商家從多次交易紀錄分析並連結至使用者身份。

Molloy 等人[12]提出虛擬信用卡機制，提出一個動態的虛擬信用卡號碼，減少所造成的損失由偷來的信用卡號碼。用戶可以使用現有的信用卡帳戶生成多個虛擬信用卡號碼，是一個單一的交易中使用或特定商戶。

廖等人[13]提出整合型電子票證機制之研究，整合電子票卷與電子錢幣之應用，提出具有電子票卷與電子錢幣功能之票證機制，結合行動設備與資訊安全技術的應用，讓原有行動設備晶片卡，擁有儲存電子票卷的資訊，節省實體票卷交付過程，消費者隱私權的完整保障。

目前行動付款在安全隱私與信任、及行動付款機制牽涉了手機硬體、軟體、金融業、電信業、零售商家、消費者各個層面上的整合，使系統能與其他系統的交互應用是為討論話題，一位使用者必須能夠信任的行動付款應用程序的供應商，信用卡或卡片信息不被濫用。當這些交易成為記錄客戶的隱私是否應該為優先，客戶的信用記錄和消費模式的不應該公開給公眾的監督。

NFC 的通訊晶片，已經有詳細的規格制定；相反地，安全元件和軟體方面，則提供相當大的發揮空間。尤其是安全元件 SE 決定了 NFC 手機的功用和效能，因此我們硬體基於安全硬體平台的安全性使用可信任執行環境 TEE 確保安全元件 SE 環境安全。MTM 要求行動通訊裝置的安全性，檢查行動裝置測量系統完整性。兼容 EMV 支付款系統。

由於 NFC 付款也牽涉到資訊安全、資料處理架構、硬體基於安全硬體平台的安全性等各方面的技術。

本論文提出以 NFC 為基礎之匿名行動付款協定。在我們的協定中，使用者必須先向其往來銀行註冊帳戶，銀行會配發虛擬帳戶給使用者並存在使用者 NFC 手機之安全元件中。使用者利用該虛擬帳戶向公信的第三者 (TSM) 申請具有特定信用額度之虛擬信用卡。TSM 會向使用者之往來銀行確認虛擬帳戶之正確性及有效性，接著簽發一張具有短時效及少於使用者之信用額度之虛擬信用卡並存在使用者之安全元件中。該配發之虛擬信用卡須滿足 EMV 協定之所有要求。隨後，使用者可以使用 NFC 之 Card-Emulation Mode 進行交易。TSM 將維護使用者之虛擬信用卡帳戶之餘額及有效期限。當虛擬信用卡之有效期限將至時，TSM 會重新配發另一虛擬信用卡給使用者。而當帳戶之餘額低於銀行之授信額度時，TSM 將要求使用者提供另一銀行之虛擬帳戶以重新進行授信。

本論文預期達到以下特性：(1)便利性：使用者僅需擁有 NFC 手機取代信用卡、現金，減輕消費者出門的負擔，加快結帳速度。(2)不可連結性：商家只會拿到一具短時效之虛擬信用卡資訊，無法從多次交易紀錄分析並連結至使用者身份。TSM 雖擁有使用者之消費資訊，然而其僅擁有使用者提供之銀行匿名帳戶，無法得知真實使用者之銀行帳戶資訊。而銀行端亦僅能得知使用者利用 TSM 付款，並無法得知使用者之消費紀錄。(3)匿名性：除銀行知曉使用者之真實身分外，使用者對 TSM 及商店皆匿名。(4)不可否認性：所有之帳戶註冊訊息、虛擬信用卡之製作及交易訊息皆須進行數位簽名，達成不可否認性。

2. 以 NFC 為基礎之匿名行動付款協定

本章我們提出我們的方法-以 NFC 為基礎之匿名行動付款協定，適用 NFC 手機進行匿名行動付款協議機制，我們的方法用 TEE、MTM、EMV、PKI 等方式作延伸，整個機制包含(1)系統初始化 2. 遠端軟體驗證 3. 申請銀行虛擬帳戶階段 4. 服務帳號註冊 5. 虛擬信用卡簽發。

系統角色介紹如下：

- 軟體供應商 SP：提供軟體下載。
- 銀行 B:銀行提供使用者帳戶與驗證軟體合法性，銀行與可信服務管理進行請款與付款之行為。
- 使用者 U：持有 NFC 手機使用者簡稱使用者，使用者個人身份、資訊，與銀行申請帳戶，主要利用 NFC 手機模擬信用卡，並使用利用 NFC 手機進行匿名的行動付款。
- 安全元件 SE:NFC 手機中的安全元件，通常與使用者綁在一起，SE 提供安全的存放空間及運算並產生金鑰。

- 可信服務管理 TSM：提供匿名信用服務並管理，為公信的第三方，與使用者進行認證並簽發信用卡匿名授權；與銀行取得驗證匿名授權及請款；與商家進行認證提供交易服務。
- 商家 M：商家。

我們提出之以 NFC 為基礎之匿名行動付款協定架構具備以下五個部分：

1. 系統初始化：協定初始化設定，主要是產生此交易付款系統於運作中所需之參數和資訊。
2. 遠端軟體驗證：交易軟體下載安裝於 NFC 手機時，須先通過 MTM 架構之軟體驗證程序，並將驗證碼存放於銀行端。每次手機啟動軟體時，皆會進行遠端軟體驗證以確保使用者是使用未經竄改之軟體與合法的 NFC 手機。
3. 申請銀行虛擬帳戶階段：使用者向銀行申請一虛擬帳戶，並取得授權。
4. 服務帳號註冊：使用者向 TSM 提出交易帳號註冊需求，並提供銀行所簽發之虛擬帳戶資訊以供驗證。TSM 向銀行驗證使用者之授信額度後，配發一服務帳號給使用者。
5. 虛擬信用卡簽發：使用者請求 TSM 配發一短時效之虛擬信用卡，並將其存放在 SE 之中。

2.1 名詞定義表

表 1 名詞定義表

IDx	x 身份識別碼如：ID_{SE} 為使用者(安全元件)身份識別碼，ID_U 使用者的身份識別碼，ID_B 銀行業者的身份識別碼。
AIDi	銀行給使用者的匿名識別碼
TIDi	使用者給 TSM 的匿名識別碼
PKx	每個角色 x 的公開金鑰
SKx	每個角色 x 的私密金鑰
SID	會議身份識別碼
$CERT^{X}_{IDX}$	x 角色發行的憑證：如 CA 發給銀行的憑證$CERT^{CA}_{B}$，銀行發給使用者的匿名識別碼的憑證$CERT^{B}_{AIDi}$
$K_{x,y}$	角色通訊者 x 與角色通訊者 y 角色之間的通訊金鑰
$SIGN(SK_x,M)$	用 x 私密金鑰將訊息 M 簽章
$Nonce_Z$	隨機數
||	訊息連接符號
E(key,M)	用 key 加密訊息 M 的加密函式
D(key,M)	用 key 解密訊息 M 的解密函式
X_ExpTime	X 的憑證到期時間
X_Limit	X 的信用額度
BINFO	給 X 的訊息
TSMINFO	給 TSM 的訊息
TSMBINFO	TSM 給 B 的訊息
AuthDATA	驗證訊息
Status	驗證訊息狀態，成功/失敗
TIDi_CerditINFO	憑 EMV 發行信用卡的訊息
TIDiList	TSM 用來記錄匿名帳號信用授權表
Quote	舉證訊息

2.2 系統初始化

在初始化設定時，安全元件、使用者、銀行和可信服務管理 TSM，都各自擁有唯一的識別碼：ID_{SE}、ID_U、ID_B、ID_{TSM}。每一個角色的識別碼皆有一組非對稱式金鑰對(PK_{ID}, SK_{ID})，且公開金鑰皆經過 CA 所簽署，並存放於 PKI 架構中。

在系統開始時，使用者需要先向其往來銀行開立信用卡帳號，並持 NFC 手機至銀行註冊。銀行會透過安全通道將 NFC 手機平台檢查碼用 SK_{SE} 簽名過的 PCR 驗證通行碼和 Measurement List 訊息與安全元件所產生之公開金鑰 PK_U 存放於放置於銀行伺服器中，銀行並會為此公開金鑰 PK_U 簽發一憑證 $CERT^{B}_{U}$ 並建立彼此之間的通訊金鑰 $K_{B,U}$。使用者有 NFC 手機在 TEE 的環境下與 SE 通訊，SE 提供安全的存放空間及運算並產生金鑰。可信服務管理 TSM 則擁有銀行經過 CA 所簽署的憑證$CERT^{CA}_{B}$，軟體供應商 SP：軟體驗證碼、提供軟體。

以下是各角色系統初始化所擁有的資訊：

軟體供應商 SP：軟體驗證碼 $SIGN(SK_B, Quote)$、提供軟體。

銀行 B：ID_B 為銀行的 ID 識別碼、(PK_B, SK_B) 銀行的非對稱式金鑰對、$K_{B,U}$ 銀行與使用者建立的通訊金鑰、$CERT^{CA}_{B}$ 皆經過 CA 簽署公開金鑰 PK_B 的憑證。

使用者 U：ID_U 為使用者的 ID 識別碼、(PK_U, SK_U) ID 使用者的非對稱式金鑰對、$K_{B,U}$ 銀行與使用者建立的通訊金鑰、$CERT^{CA}_{U}$ 皆經過 CA 簽署公開金鑰 PK_U 的憑證。

安全元件 SE：ID_{SE} 為 SE 的 ID 識別碼、(PK_{SE}, SK_{SE}) SE 的非對稱式金鑰對、$CERT^{CA}_{SE}$ 皆經過 CA 簽署公開金鑰 PK_{SE} 的憑證。

可信服務管理 TSM：ID_{TSM} 為 TSM 的 ID 識別碼、(PK_{TSM}, SK_{TSM}) TSM 的非對稱式金鑰對、$CERT^{CA}_{TSM}$ 經過 CA 簽署公開金鑰 PK_{TSM} 的憑證。

2.3 遠端軟體驗證

在使用手機進行行動付款前，NFC 手機必須具備行動可信模組的 MTM 架構。當 NFC 手機從軟體供應商(如 Google Play Market 或 Apple AppStore)下載特定軟體並執行安裝。本階段包含兩部分: 軟體下載驗證及軟體啟動驗證，分述如下:

2.3.1 軟體下載驗證

NFC 手機要執行軟體安裝時，MTM 平台之 Application Measurement 須先確認軟體是否經過簽名，並由 Attestation Service 詢問 Trusted Platform 確認其軟體驗證碼(fingerprint) 是否正確，驗證軟體為可信不可信。

若軟體可信賴，則於安裝後計算該軟體之 PCR 值，除存放於安全元件 SE 中，亦將 PCR 簽名後傳送至銀行，存放於銀行伺服器中。詳細步驟如下:

1. Application Measurement 下載軟體時會，收到軟體識別碼，產生隨機數 Nonce 給 Attestation Service。
2. Attestation Service 產生 Quote Request 去詢問 Trusted Platform
3. MTM 算出 Quote，Quote 為 MTM 簽名過的 PCRs 驗證通行碼、Nonce、軟體識別碼。
4. Attestation Service 向 Measurement Agent 請求平台驗證訊息。
5. Measurement Agent 會將平台驗證訊息傳給在 Measurement List 存放，報告 MTM，並回傳給 Application Measurement 透過 Attestation Service。
6. Application Measurement 平台驗證訊息、Quote 和軟體識別碼傳給銀行。
7. 銀行驗證手機平台和軟體識別碼，並通知 Application Measurement 安裝。

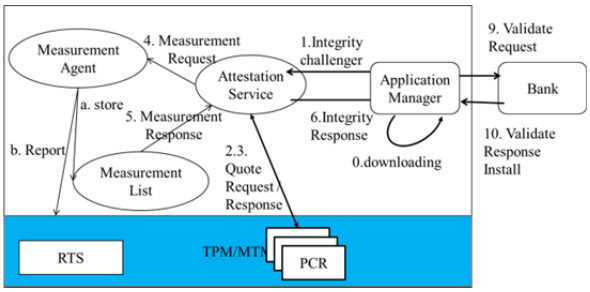


圖 1 軟體下載驗證流程圖

2.3.2 軟體啟動驗證

每次手機執行軟體時，Attestation Service 亦會計算軟體驗證碼，除與存放於安全元件中之 PCR 比對外，亦會加以簽名後傳送至銀行端請求驗證，若銀行確認該驗證碼與之前存放於伺服器中之驗證碼相同，則會允許使用者執行該軟體。詳細步驟如下：

1. 軟體啟動驗證，產生隨機數 Nonce。
2. Attestaion Service 產生 Quote Request 去尋問 Trusted Platform。
3. MTM 算出 Quote，Quote 為 MTM 簽名過的 PCRs 驗證通行碼與 Nonce。
4. Attestaion Service 向 Measurement Agent 請求平台驗證訊息。
5. Measurement Agent 會將平台驗證訊息傳給在 Measurement List 存放，報告 MTM，並 Measurement List 回傳給 Attestaion Service。
6. 軟體驗證訊息 Measurement List 訊息、Quote 和 Nonce 簽名回傳銀行驗證。

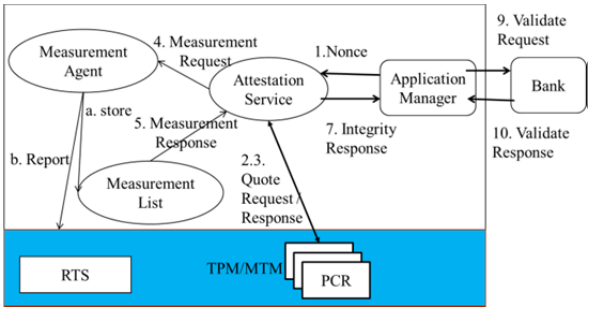


圖 2 軟體啟動驗證流程圖

2.4 申請銀行虛擬帳戶階段

為了保護使用者的隱私，使用者於確認軟體之正確性後，向銀行請求建立一虛擬帳戶識別碼 AIDi，此時使用者 NFC 手機之安全元件將產生一組新的公開金鑰對(PK_{AIDi}, SK_{AIDi})後，利用其中之祕密金鑰(SK_{AIDi})將相對應之公開金鑰(PK_{AIDi})執行自我簽署(Self-Signed) 後，傳送至銀行確認。當銀行確認使用者之身分後，將簽發一相對應 AIDi 的公開金鑰之數位憑證給予使用者，以供後續交易使用。其步驟如下所示：

1. 使用者身份 ID_U 向銀行發出請求 Request，將 ID_U 產生虛擬帳號 AIDi 與通訊金鑰 $K_{AIDi,B}$。
2. 銀行回應 ID_U 給與 AIDi 並建立通訊金鑰 $K_{AIDi,B}$。
3. 使用者得到 AIDi 時向 SE 提出產生一新公開金鑰對的請求。
4. SE 建立的 AIDi 金鑰對 (PK_{AIDi}, SK_{AIDi})，並以 SK_{AIDi} 進行自我簽章後送回給使用者。
5. 使用者將 AIDi 金鑰簽章訊息與申請的虛擬帳號 AIDi 使用通訊金鑰 $K_{AIDi,B}$ 加密傳回給銀行進行驗證。
6. 銀行解開訊息，得到 AIDi 的公開金鑰，將產生虛擬帳號 AIDi 銀行 B 所發行的 AIDi 憑證、AIDi 的到期時間 AIDi_ExpTime 、AIDi 帳戶的信用額度 AIDi_Limit 及與 AIDi 與通訊金鑰 $K_{AIDi,B}$，回傳給 IDU 訊息為到期時間、信用額度及加密過要給 SE 的 AIDi 通訊金鑰 $K_{AIDi,B}$。

7. IDU 將加密傳送到 SE
8. SE 用產生的 AIDi 的私密金鑰解開，得到 AIDi 產生的通訊金鑰 $K_{AIDi,B}$ 及銀行發行的 AIDi 憑證，完成申請。

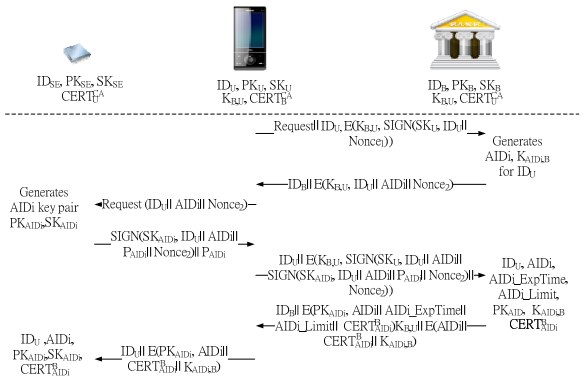


圖 3 銀行帳戶授權協定

2.5 申請 TSM 服務帳號註冊階段

當使用者向銀行註冊後，亦須向可信服務管理 TSM 註冊，以取得實際交易所使用之虛擬信用卡。在此階段中，使用者將於 TSM 建立一預儲帳戶，並可自訂一最高交易額度。該預儲帳戶將使用銀行之虛擬帳戶進行電子付款。為了確保付款之安全性，使用者將付款訊息 BINFO 包含虛擬帳戶名稱 AIDi、虛擬帳戶到期時間 AIDi_ExpTime 、虛擬帳戶信用額度 AIDi_Limit、以與銀行共享之金鑰 $K_{AIDi,B}$ 加密後並以 SKAIDi 簽名後，透過 TSM 傳送至銀行。使用者亦會將付款訊息以與 TSM 共享之金鑰 $K_{TIDi,TSM}$ 加密後並以 SK_{TIDi} 簽名後，一併傳送給 TSM。TSM 僅知交易銀行，但無法解開使用者傳送給銀行之付款訊息。

隨後 TSM 將解開之付款訊息 TSMINFO，經重新以與銀行公開金鑰 PK_B 加密及 SK_{TSM} 私鑰簽名後，連同使用者傳送給銀行之加密付款訊息 TMSBINFO 傳送至交易銀行。交易銀行將使用者傳送之付款訊息解開後，比對 TSM 所傳送之付款訊息是否一致。若銀行比對結果兩者一致則將虛擬帳戶之信用資訊傳送至 TSM，詳細步驟如下:

1. 使用者發出請求註冊
   - ID_U 建立帳號 TIDi，產生金鑰對(PK_{TIDi}, SK_{TIDi})，使用金鑰簽章並用 PKTSM 加密訊息 E(PK_{TSM}, SIGN(SK_{TIDi}, TIDi|| PK_{TIDi}|| TimeStamp))，請求建立 TIDi 訊息 E(PK_{TID}, SID|| TIDi || $K_{TIDi,TSM}$)並傳送 TSM。
   - ID_{TSM} 收到 TIDi 請求訊息解開，建立通訊金鑰 $K_{TSM,TIDi}$ 並且回傳給使用者並要求帳號提供信用證明，才可開通服務。
2. 使用者相關證明

ID_U 收到 ID_{TSM} 立建 TIDi，需提供信用證明才可啟用服務，建立給 ID_{TSM} 的訊息與給銀行訊息，銀行訊息需由 AIDi 與銀行之間的通訊金鑰 $K_{AIDi,B}$ 做出加密訊息並用 AIDi 的私鑰簽章；給可信服務管理訊息由 TIDi 與可信服務管理之間的通訊金鑰 $K_{TSM,TIDi}$ 做出加密訊息，並用 TIDi 的私鑰簽章。

- ID_U 請求 SID 會議身份識別碼、AIDi、和 AIDi 的銀行和隨機數 Nonce1 送給 IDSE。
- ID_SE 做出銀行給 AIDi 的相關訊息 BINFO、$Nonce_1$ 交給 IDU。BINFO=SIGN(SAIDi, E($K_{AIDi,B}$, SID || AIDi || ID_{TSM} || IDB || AIDi_ExpTime || AIDi_Limit || $Nonce_2$))。
- IDU 做出 IDTSM 給 TIDi 的相關訊息 TSMINFO。TSMINFO=SIGN(SK_{TIDi}, E($K_{TIDi,TSM}$, SID || AIDi || ID_{TSM} || ID_B|| $Nonce_2$ || AIDi_ExpTime || AIDi_Limit))。
- 將訊息 BINFO、TSMINFO、$Nonce_1$ 加密並使用 SK_{TIDi} 簽名傳送給 ID_{TSM}。
- TSM 收到 TIDi 提出的身份證明訊息。

3. 可信服務管理向銀行驗證

收到 TIDi 提出的身份證明訊息向銀行驗證。

- 將得到的訊息解密，得到 TSMINFO 解開取得 AIDi、IDB、SID、與 AIDi_ExpTime 到期間|| AIDi_Limit 信用額度。
- 將要銀行確認的 AIDi 身份和到期間時間、信用額度做出驗證訊息 TMSBINFO，TSMBINFO=SIGN(SK_{TSM}, E(PK_B, SID || AIDi || $Nonce_2$ || AIDi_ExpTime || AIDi_Limit || $K_{TSM,B}$))。
- 將 AIDi、BINFO 和 TMSBINFO 驗證的加密訊息傳送到 ID_B
- 解開訊息，比對 BINFO 和 TMSBINFO，內容是否一制，並將 AIDi 的信用資訊傳送給可信服務管理。

4. 可信服務管理接受 TIDi 是合法的使用都並取得服務，傳送給使用者，TIDi 的到期時間、信用額度。

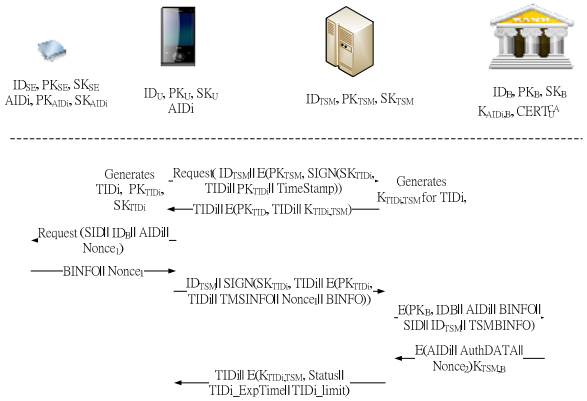


圖 4 TSM 申請帳戶協定

2.6 虛擬信用卡簽發

使用者隨後即可向可信服務管理申請虛擬信用卡，可信服務管理將簽發一具有效期限較短、信用額度較低且符合 EMV 規範之信用卡資訊，傳送給使用者後存放於安全元件中。當該虛擬信用卡過期時，則使用者須重新進行此階段之步驟以取得另一張虛擬信用卡。詳細步驟如下：

1. 使用者與 ID_{SE} 請求 TIDi 的金鑰對(PK_{TIDi}, SK_{TIDi})，用來向可信服務管理簽發信用卡卡片金鑰。
2. 使用者傳送請求給 ID_{SE}，產生 TIDi 的金鑰對(PK_{TIDi}, SK_{TIDi})
3. 使用者傳送申請訊息，使用者申請服務帳 TID 與 ID_{SE} 產生金鑰簽章送給 ID_{TSM}，簽發憑證。
4. TSM 簽發虛擬信用卡訊息資料，由 SE 保護。收到訊息，產生 $CERT_{TIDi}^{TSM}$ 和虛擬信用卡資訊 TIDi_CreditINFO 存放在安全元件內。
5. 後序交易流程遵照 EMV 交易流程用 NFC 手機的卡片模擬方式，產生虛擬信用卡進行交易。

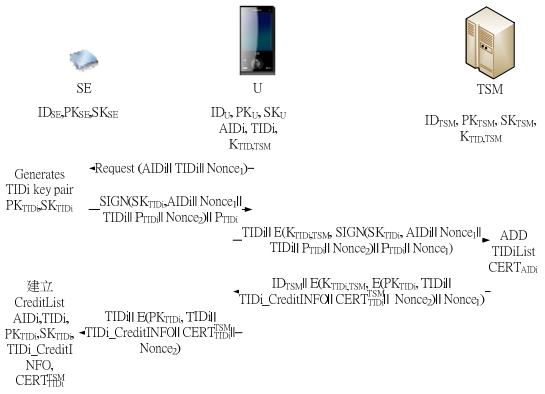


圖 5 虛擬信用卡協定

表 2 TSM 用來記錄匿名帳號信用授權表

TIDi	AIDi	PK_{TIDi}	$CERT_{TIDi}^{TSM}$
TIDi_CreditINFO	AIDi_ExpTime	AIDi_Limit	

3. 結論

本論文以基於 TEE、MTM、及 EMV 的規範結合 NFC 手機並加入 TSM 公信的第三方，實現安全且便利的匿名行動付款系統。銀行及 TSM 兩個匿名機制方式保有信用卡特色且改善不可匿名、可連結性問題。本方法保護使用者個人隱私與增加消費便利性與安全性。就使用者隱私而言，使用者匿名向 TSM 進行註冊，利用銀行帳戶身份驗證，而 TSM 只知道像銀行帳戶請款，而銀行無法得知使用者進行交易訊息，商家像 TSM 請款也無法得知使用者的銀行資訊，進而無法假冒使用者身份及分析使用者的交易習慣，然而當有消費紛爭或信用問題時，TSM 可像銀行申請追蹤帳戶使用者的真實身份。就交易方面而言，使用者只需使用 NFC 手機取得 TSM 授權虛擬信用卡即可完成整個付款流程。

參考文獻

[1] C.I. Fan and V.M. Huang, “Provably secure integrated on/off-line electronic cash for flexible and efficient payment,” in IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 40, pp. 567-579, 2010.

[2] Y. Chen, J.S. Chou, H.M. Sun, and M.H. Cho, “A novel electronic cash system with trustee-based anonymity revocation from pairing,” Electronic Commerce Research and Applications, 2011, vol. 10, pp. 673-682.

[3] M. Carr, "Mobile Payment systems and services: An introduction, “ in Mobile Payment Forum, 2007, pp. 1-12.

[4] W. Chen, G. Hancke, K. Mayes, Y. Lien, and J.H. Chiu, “NFC mobile transactions and authentication based on GSM network,” in Second International Workshop on Near Field Communication (NFC), 2010, pp. 83-89.

[5] W. D. Chen, G. P. Hancke, K. E. Mayes, Y. Lien, and J. H. Chiu, “Using 3G network components to enable NFC mobile transactions and authentication,” in IEEE International Conference on Progress in Informatics and Computing (PIC), 2010, pp. 441-448.

[6] Z. Kabir, “User Centric Design of an NFC Mobile Wallet Framework,” KTH, 2011.

[7] R. Martínez-Peláez, F. Rico-Novella, and C. Satizábal, “Mobile payment Protocol for micropayments: withdrawal and payment anonymous,” in New Technologies, Mobility and Security, NTMS'08., 2008, pp. 1-5.

[8] M. Hassinen, K. Hyppönen, and E. Trichina, “Utilizing national public-key infrastructure in mobile payment systems,” Electronic Commerce Research and Applications, 2008, vol. 7, pp. 214-231.

[9] M. Toorani, A. Beheshti, “SSMS-A secure SMS messaging protocol for the m-payment systems,” Computers and Communications , 2008.

[10] S. Kungpisdan, B. Srinivasan, and P. D. Le, “A secure account-based mobile payment protocol,” in International Conference on Information Technology: Coding and Computing (ITCC), 2004, pp. 35-39.

[11] 廖鴻圖, “跨網域之匿名行動付款機制,” 電子商務學報, vol. 9, pp. 779-799, 2007.

[12] I. Molloy, J. Li, and N. Li, “Dynamic virtual credit card numbers,” in Financial Cryptography and Data Security, ed: Springer, 2007, pp. 208-223.

[13] 廖鴻圖, 廖偉鵬, 郭明煌, and 陳志瑋, “整合型電子票證機制之研究,” 2008.

結合安全測試與異常偵測之防範架構降低電子商務安全風險

賴森堂　　羅翊萱
實踐大學資訊科技與管理學系
stlai@mail.usc.edu.tw

摘要

在網際網路的年代，日常的各種活動都與網路適度結合，商業的各種交易活動更是需要網路的服務，凡是透過網際網路進行的商業交易行為都統稱電子商務(Electric Commerce)。電子商務具備網路的優勢，在各式各樣商業行為與活動中，確實提昇許多的效益，不過，卻也隱含了許多急需改善的問題和缺失，其中又以交易與個人資料安全對於組織及利害關係人的影響最大。本文針對電子商務安全相關議題進行討論，且探究與剖析電子商務的例行性安全測試與異常事件偵測作業，進而提出一套結合安全測試與異常偵測兩層式之電子商務安全防範架構(EC Security Prevention Scheme, ECSPS)，定期的例行性弱點掃描及滲透測試找出電子商務安全的漏洞及缺失，再搭配安全事件偵測作業即時阻斷安全事件的衝擊減少損失擴大，以有效降低電子商務安全風險。

關鍵詞：電子商務、安全測試、安全事件、安全防範架構、ECSPS

Abstract

In the network and digital age, the high efficiency and high profit activities have to incorporate with the internet. E-commerce is an important system in the internet fever. However, the network intrusion, malicious users, virus attack and system security vulnerabilities have continued to threaten the operation of the e-commerce, making e-commerce security encounter serious test. In order to avoid security flaws and defects of the system caused user significant loss, how to improve e-commerce security has become a topic worthy of further exploration. Combining security test procedure and exception detection procedure, in this paper proposes an E-Commerce Security Prevention Scheme (ECSPS). Applying ECSPS, no security event before, routine security test procedure can identify security vulnerability and defect, and develop repair operations. Security event occurred, abnormal detection procedure can quickly detect and identify event, develop security defects revision step, and recover e-commerce system normally operation. Two-layer security prevention scheme can effectively enhance e-commerce security and concretely reduce e-commerce security risk.

Keywords: e-commerce, security test, exception detection, security event, ECSPS

1. 緒論

在網際網路與數位化的年代，促使各種追求高效率與高效益的活動都必須與網際網路適當的結合，如此才能在網路熱潮下提昇其競爭力以延續其生存空間，商業的各項行為與活動一直都是追求高效益與高利潤的先驅，因此，配合網際網路而改變的各種商業行為與活動，更是積極且快速的被開發與推動，凡是透過網路進行的商業活動都統稱電子商務(Electric Commerce; EC)[4, 5]，依據研究調查機構 eMarketer 的調查數據顯示，全球電子商務銷售首度超越 1 兆美元，且預估 2013 年電子商務銷售將成長至 1.3 兆美元，其中亞太區銷售額將超越北美[1]。而根據「新網路時代電子商務發展計畫」之調查顯示，2011 年我國 B2C 市場規模為新台幣 3,226 億元，預測至 2013 年可望達到新台幣 4,781 億元[8]。不過，Gartner 的研究報告指出，由於消費者擔心安全上的問題，使得電子商務的銷售額因而短少 20 億美元之多[15]。從以上的研究報告中，可以得知電子商務銷售額將持續的成長，而影響銷售額成長的關鍵因素就是電子商務的安全性。

電子商務具備了網路的優勢，在各式各樣商業行為與活動中，提昇許多的效益與競爭力，不過，卻也隱含了許多急需改善的問題和缺失，包括執行效率、網路交易安全、系統運作的特性及配合環境調整與異動的維護能力等問題，所涉及的因素非常多，其中又以交易資訊與個人資料的安全對於組織及利害關係人的影響最大，其衝擊已經超越功能與效能的需求，電子商務安全性是一項必須重視的議題。電子商務出現的安全漏洞或缺失幾乎都非主動被發現的，反之大部份異常事件屬於被告知後才發現的，因此，一旦查覺系統被入侵或資料外洩等事件，對組織所造成的損失以及對用戶所形成的衝擊，是難以評估與預期的，即使後續採取耗費人力與成本的修補作業或改善措施，也無法有效彌補，為此本文針對如何以安全防範措施有效提昇電子商務系統的安全性進行探討，且以「預防重於治療」的觀念，於電子商務安全事件發生前後，主動測試與偵測電子商務的安全缺失，以安全防範為基礎，提昇電子商務安全性。

電子商務系統除了必須搭配複雜的網路環境及更新頻繁的硬體設施外，還要協助運作中的各項

任務能夠滿足組織與用戶所提出的各項需求，另外為了協助企業/組織達成永續經營的目標，電子商務系統應該具備可以持續改善、高擴充能力、高完整性及高安全性等基本特質，其中又以高安全性的基本特質是各種商業交易活動或行為必須重視且加強的關鍵項目。本文針對電子商務的安全相關議題進行探討，且探究與剖析電子商務的例行性安全測試與異常安全事件偵測作業，進而提出一套結合安全測試與異常偵測兩層面之電子商務安全防範架構(EC Security Prevention Scheme, ECSPS)，在安全事件發生前後，即時標示出安全漏洞與缺失，適時進行安全缺失調整與改善措施，具體降低電子商務的安全風險，有效提昇電子商務安全性。本文共分成五節，第二節將探討電子商務系統的安全議題及其特質。找出運作中電子商務的安全漏洞是改善電子商務安全性的首要步驟，第三節從例行性安全測試與異常安全事件偵測作業兩個層面探討電子商務的安全性。安全測試與異常偵測是防範電子商務安全風險的必要步驟，第四節將提出一套結合安全測試與異常偵測兩層面之電子商務安全防範架構(ECSPS)。第五節將彙整電子商務安全防範程序在降低電子商務安全風險的貢獻，且針對本主題作個結論。

2. 電子商務安全之重要性

網路的熱潮改變了商業交易方式，為電子商務系統帶來許多商機，卻也隱含了難以預期的安全危機。

2.1 電子商務安全相關議題

凡是利用網路進行的商業活動或交易行為都稱為電子商務(EC)，電子商務的各項活動或行為都會涉及關鍵的個人資料與交易資訊，這些重要的資訊成為電子商務安全性的一大隱憂。根據 104 市調中心對於網路購物的安全性及影響調查的結果顯示，有 84%的民眾，擔心使用網路購物而導致「個人資料外洩」(如圖 1 所示)，也有 42%的民眾發生過「個資外洩」或遇到「詐騙事件」[7]。而近年來，個資外洩以及交易安全的問題更是越來越頻繁，從 2011 年日本 Sony 公司的 PlayStation Network 遭駭客入侵竊走 7,700 萬筆 PS3, Qriocity 音樂隨選服務使用者的個人資料[9]，及南韓線上業者 SK Communications 維運的 Nate.com 入口網站、CyWorld 部落格網站遭駭客入侵造成約 3,500 萬會員個資外洩 [11]，到 2012 年 3 月美國線上交易付款服務公司 Global Payments 遭駭客入侵恐致上千萬筆 Visa、萬事達、美國運通與 Discover 持卡人的個資外洩甚至遭人盜刷[10]等安全事件。因此，各大公司無不採取各種方法以避免客戶個人資料因駭客入侵而外洩。其中，除了透過防火牆(Firewall)、網路偵防系統(Intrusion Detection and Prevention, IDP)等硬體設備加強網路安全防護外[2]，還應該採取弱點掃描工具與滲透測試技術檢測軟體系統與應用程式的安全漏洞與缺失，以降低被駭客入侵的風險。

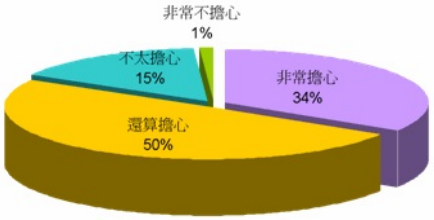


圖 1 84%的民眾擔心網路購物個人資料外洩
***資料來源：104 市調中心**

2.2 電子商務應具備的安全項目

當單位或組織規劃的電子商務系統未能關注安全上的議題時，不但會讓使用者對於該單位或組織所提供的系統產生安全上的質疑，還會大幅降低對於該單位或組織的信任度與系統的使用意願。因此，電子商務系統必須在開發前，就擬訂一套完善的安全需求，以強化系統的安全性 [3, 5, 13, 14]。Holcombe 認為任何電子商務系統都必須滿足四個安全需求[16](如圖 2)：

(1) 授權(Authorization)：對於電子商務驗證完成的使用者，必須確認該使用者的功能權限。
(2) 完整性(Integrity)：在電子商務資料交換的過程中，必須確保資訊不會遭到變更或篡改，以確定資訊內容的完整性。
(3) 隱私性(Privacy)：在電子商務資料交換的過程中，必須避免未經授權人員的接觸及參與，以善加保護用戶的個人資料與交易資訊。
(4) 不可否認性(Non-Reputation)：各種電子商務的交易行為中，均能夠具體證明且記錄交易雙方都已經確實收到對方的交換資訊，以達到不可否認性。

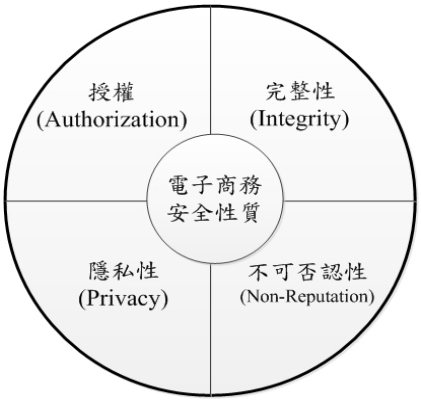


圖 2 Holcombe 電子商務四項不可分割的安全性質

Web App 系統的安全問題受到許多國際性團體與組織(SANS(安全訓練、認證與研究機構)，OWASP (開放 Web App 安全計畫，Open Web Application Security Project)的重視，陸續公佈 Web App 的關鍵安全漏洞與弱點：SANS Top-20 Security Risks [19] 與 OWASP Top 10 [16]，以協助降低電子商務軟體的安全風險。根據 SANS Top-20 Security Risks，OWASP Top 10 以及 Holcombe 提出之電子商務系統不可分割的四項安全需求[13]，將安全缺失與漏洞分為五種類型：

(1) 授與之權限之缺失：電子商務系統的維運人員必須規範明確的權限，系統無法掌控人員使用權限，將造成嚴重的安全缺失與漏洞。
(2) 完整性之缺失：當電子商務系統運作過程中，必須確保資訊或資料不會遭受到變更或篡改，以確定資訊內容的完整性，系統無法確保資料完整性，將是一項關鍵的安全缺失與漏洞。
(3) 隱私性之缺失：用戶個人資料與交易資訊是系統一項重要隱私，系統必須有能力保護用戶個人資料與交易資訊，當發生個人資料與交易資訊外洩，將形成嚴重的安全事件。
(4) 不可否認性之缺失：電子商務的交易行為中，當發生交易糾紛時，系統必須詳細記載交易行為的各項資料，且有能力分析且判斷交易行為的執行細節，以達到不可否認性，否則，將形成交易糾紛的安全事件。
(5) 入侵與攻擊手法之缺失：入侵與攻擊手法五花八門且持續創新，像是無線網路的入侵手法(封包竊聽、中間人攔截、拒絕存取、偽冒基地台攻擊...等)或是網路釣魚等，系統無法防範入侵與攻擊手法，將形成難以預期的安全事件。。

3. 安全測試與異常偵測

電子商務的安全性應該從例行性安全測試與異常事件偵測作業兩個層面進行探討。

3.1 例行性安全測試作業

電子商務系統必須擬訂一套例行性的安全測試作業以確保電子商務能夠在安全的環境中正常運作，安全測試作業大致分成弱點掃描與滲透測試兩種方式[6, 17]：

(1) 弱點掃描(Vulnerability Scan)：屬於系統內部安全漏洞與缺失的檢測作業，可交由電子商務軟體系統維護人員執行，至少應該半年執行一次，利用弱點掃描工具的協助找出電子商務軟體系統的安全漏洞與缺失，再由維護人員進行後續的修補作業，免費或開放原始碼的掃描工具包括 NetCat, NIKTO, Paros Proxy 等。由於弱點掃描只能針對程式碼可能存在的安全缺失與漏洞進行檢視，無法達成全面性的安全環境測試作業，能夠處理的範圍與改善的能力較為有限，此外免費的弱點掃描工具出現誤判率過高的狀況，也造成安全漏洞修補人員的一大困擾。為了彌補弱點掃描的缺陷，滲透測試成為安全防範措施不可缺少的重要作業[6]。
(2) 滲透測試(Penetration Test)：是一項正式的安全漏洞與缺失的檢測作業，它是模擬惡意攻擊者的攻擊手法，來去評估整個系統的安全性，而滲透測試一般都委託顧問公司且由專業人員來執行，測試的時間與檢視項目的多寡有關，且至少需要五個工作天以上，完成的滲透測試報告，除了詳述測試的執行過程外，最重要的是完整記錄發現的安全漏洞與缺失，若經費預算之許可，更可以交由顧問公司協助企業或組織進行後續的安全改善措施[6]。

使用弱點掃描及滲透測試等檢測作業，或多或少還是會有小部分的漏洞與缺失是沒辦法找出來的，所以，最後還需依靠人工針對所列舉出來的電子商務安全清單一一去做審核的工作。Racquel 針對電子商務的安全性提出了人工檢視的清單，其目的是幫助企業或組織提供一個安全且可靠的環境給使用該電子商務軟體系統的客戶，使企業或組織的系統與網站的信任度能夠提升[18]。最後，將弱點掃描、滲透測試及人工檢視針對其特性整理如下表(如表 2)。

表 1 安全測試方法相關特性比較表

測試方法 / 特性	弱點掃描	滲透測試	人工檢視
執行頻率	三個月或半年	半年或一年	依需求
執行時間	短	長	長
成本	低	高	中等
執行人員	維護人員	專業技術人員	維護人員
改善方式	自行改善	顧問公司協助完成	自行改善

3.2 異常安全偵測作業

安全測試作業可以有效提昇電子商務系統的安全性，卻無法保證系統不會被駭客或惡意使用者的入侵，更無法確認系統本身不會發生例外的安全事件，因此必須規劃一套安全事件的偵測作業，即時發現安全事件且阻止事件與損失的擴大。安全事件的偵測作業可以廣泛蒐集各種資訊安全事件的發生原因，透過歷史資料與數據制定出安全事件的判斷法則，以下為本文整理的六項安全事件判斷法則：

(1) 存取量異常：系統用戶的個人資料出現超出正常的存取現象。
(2) Log 檔異常：資料庫存取的 Log 檔出現不正確、不完整或不一致等異常現象。

(3) 交易行為異常：客戶在特定期間的交易行為出現數量過多或金融龐大的異常現象。
(4) 非法使用者：系統於運作過程中，發現非法使用者進行資料存取或竄改的異常現象。
(5) 銀行通報：信用卡發卡銀行以緊急訊息通報客特定客戶信用卡止付。
(6) 客戶通報：客戶透過相關管道告知，存放在系統的個人資料已遭竊取或竄改的現象。

這些法則具有高度的調整彈性，可以依實際的安全事件發生狀況進行新增、修訂或調整，能夠即早發現難以避免的安全事件，就可以減少事件帶來的嚴重衝擊，也可以大幅降低，因客戶個人資料外洩所造成的損失，更可以有效提高用戶對於企業或組織的信賴度。

4. 安全防範架構與運作流程

本節以例行性的安全測試與異常事件偵測作業提出一套電子商務安全防範架構，且從運作流程說明安全防範架構如何降低電子商務安全風險。

4.1 安全防範架構

企業或組織對於電子商務個人資料與交易資訊的隱私，必須規劃一套完善的安全防範措施以善盡保護個人資料與交易資訊的安全。電子商務的安全防範措施可以從兩個層面進行強化，第一層面為安全事件未發生前的測試與修補作業，網路與資訊相關設備日新月異，不斷有新的技術或產品被推出，電子商務系統必須配合這些新的技術或產品持續的調整與精進，以滿足市場的需求。此外駭客與惡意使用者的入侵手法與資訊竊取技術也不斷翻新，促使電子商務系統必須擬訂一套例行性的安全測試作業，在安全事件未發生前，識別出系統因調整與精進所導入的安全漏洞與缺失，或是翻新入侵手法與竊取技術所衍生的安全風險，例行性的安全測試作應該於 3 至 6 個月至少執行一次弱點掃描，6 至 12 個月至少進行一次滲透測試，及時找出安全漏洞與缺失，以協助後續的修補與改善作業。

第二層面為安全事件發生後的偵測與補救作業，電子商務屬於持續運作中的資訊系統，因此任何時段都有可能出現異常的安全事件，一旦發生安全事件，不僅將危及系統的正常運作，更可能波及客戶個人資料與交易活動細部資訊等重要隱私，因此，電子商務系統必須擬訂一套異常事件偵測與補救作業，此項作業屬於持續運作中的程序，在安全事件發生後，能夠透過安全偵測主動且及時得知事件發生，且依事件情節的輕重進行後續補救措施，以有效減低安全事件所造成的各項損失。

結合第一層面安全測試與修補作業，及第二層面安全事件偵測與補救作業，我們稱此安全防範措施為電子商務安全防範架構 (EC Security Prevention Scheme, ECSPS)，在安全事件未發生前，識別出系統的安全漏洞與缺失，適時找出安全漏洞與缺失，以進行後續的修補與改善作業。在安全事件發生後，主動且及時發現安全異常事件，且依安全事件情節的輕重進行後續補救措施，以有效降低安全事件造成的擴大衝擊。

4.2 ECSPS 運作流程

ECSPS 的第一層面必須制訂一套例行性安全測試程序，透過例行性的弱點掃描、滲透測試及人工檢視等方法找出電子商務系統的安全漏洞或缺失，在安全事件未發生前，即針對系統安全漏洞或缺失進行修補及改善作業，可有效降低駭客入侵、惡意使用者或系統異常等安全事件。例行性安全測試程序包括四個作業階段(參閱圖 3 所示)，說明如下：

(1) 測試規劃階段：
- 廣泛蒐集且分析現今 Web App 可能出現的安全漏洞與缺失，及駭客任入侵與新攻擊的手法。
- 針對行性安全測試作業擬訂一套完善的測試計畫。

(2) 測試執行階段：
- 規劃且設計安全測試的相關個案。
- 依據測試計畫執行安全測試且標示系統出現的各種安全漏洞與缺失。

(3) 問題識別階段：
- 剖析標示出的各種安全漏洞與缺失，且刪除誤判的項目。
- 依據確認後的安全漏洞與缺失，判斷系統受影響的功能與模組。

(4) 修補作業階段：
- 修補確認後的安全漏洞與缺失。
- 評估安全漏洞與缺失的修補作業。

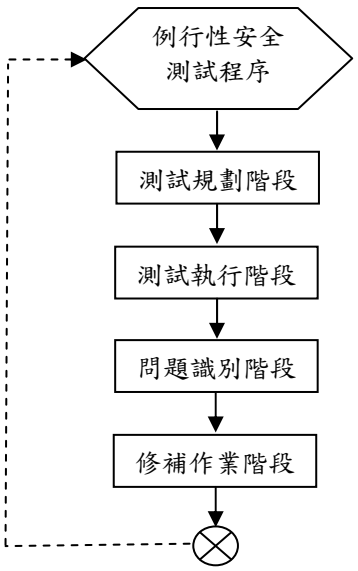


圖 3 例行性安全測試程序作業流程圖

第二層面是擬訂一套異常事件偵測程序，持續且即時的監測各種可能的安全異常事件，一旦發現資訊安全的異常狀況，經過進一步確認後，必須立即進行採取行動阻止安全事件的擴大，以有效減少安全事件的衝擊與損失，最後再針對系統的安全漏洞或缺失提出修補與改善措施，盡快恢復電子商務系統的正常運作。安全事件偵測程序包括五個作業階段(參閱圖 4 所示)，說明如下：

(1) 事件偵測階段：
- 在電子商務運作過程中，持續監控所有的交易行為與資料傳輸等活動。
- 依據事先擬訂的法則判斷方法，識別可能出現的安全事件。

(2) 事件確認階段：
- 深入分析可能出現的安全事件，進一步確定真正的安全事件。
- 剖析安全事件嚴重性，了解事件對用戶個人資料的影響程度及對系統的影響範圍。

(3) 暫停運作階段：
- 依據安全事件的嚴重性，決定停止某些功能的運作或暫時停止整個電子商務系統的運作，以減少的影響成範圍。

(4) 事件識別階段：
- 識別出安全事件發生的原因，且針對安全漏洞與缺失擬定與規劃安全事件修補與電子商務系統復原策略。
- 完整記錄安全事件發生的時間、原因、如何發現、受損的範圍及修補與復原策略。

(5) 修補恢復階段：
- 依策略修補造成電子商務安全事件的安全漏洞與缺失。
- 盡快恢復電子商務系統的正常運作。

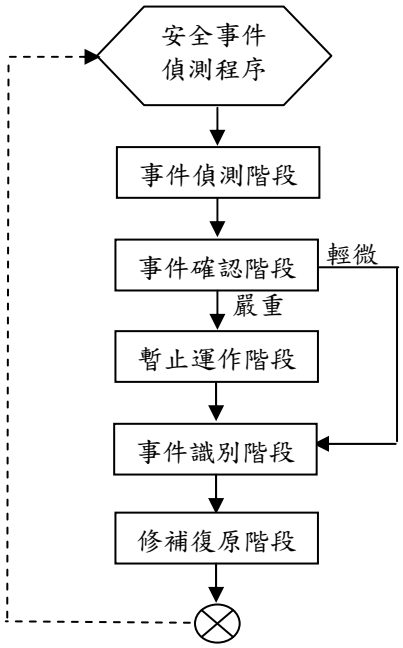


圖 4 安全事件偵測程序作業流程圖

為了具體且有效的降低電子商務系統個人資料與交易資訊的安全風險，本文規劃兩層面的安全防範架構，結合例行性安全測試程序與異常安全事件偵測程序 (參閱圖 5 所示)，例行性安全測試程序主要目的是標示潛在的安全漏洞與缺失，在未發生安全事件前，即針對電子商務安全漏洞與缺失進行修補與改善作業，大幅降低異常安全事件發生率。大部份電子商務異常事件屬於被告知後才發現的，因此，安全事件經常對組織與用戶造成重大的損失，異常安全事件偵測程序主要目的是即時偵測異常事件，且針對異常安全事件發生後，採取適時的補救措施，以降低安全事件的擴大與損失。

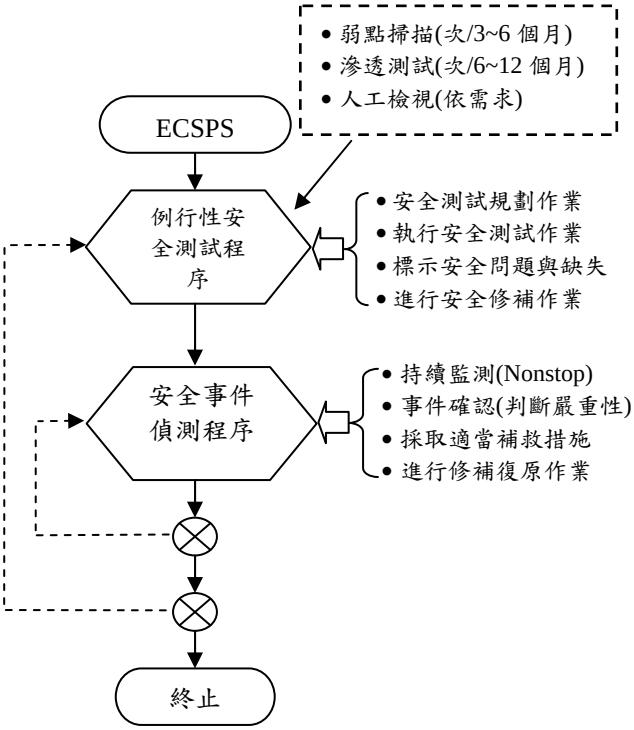


圖 5 電子商務安全防範架構運作流程圖

4.3 ECSPS 之優勢

駭客與惡意使用者入侵手法與技術持續成長，系統調整與精進過程中，因為人員的疏忽，經常造成系統本身的安全漏洞與缺失，這是電子商務系統必須面臨的問題，例行性的安全測試程序可以有效標示安全漏洞與缺失，增強電子商務的安全性，異常事件偵測程序可以即將發現異常安全事件，有效降低電子商務衝擊與損失，進而提昇個人資料與交易資訊的安全性。ECSPS 三項優勢說明如下：

- 安全事件發生前：例行性的安全測試程序可以針對事件發生前的安全漏洞與缺失，進行識別與確認，且及時提出漏洞修補與缺失改善作業。
- 安全事件發生後：異常事件偵測程序可以即時發現異常安全事件，且判斷事件的狀況，進而

採取後續的補救與強化作業。

- 降低安全風險：兩層面的安全程序可以達到互補效果，強化相互程序的漏洞與缺失判斷能力，以有效降低電子商務安全風險。

5 結論

在網際網路的年代，促使電子商務的應用範圍越來越廣泛，電子商務系統的交易行為及金額更是逐年持續增加，人們的日常生活幾乎無法擺脫電子商務的應用範疇，也因此電子商務的安全性成為一項值得深入探討與重視的議題。電子商務系統應具備可以持續改善、高擴充能力、高完整性及高安全性等基本特質，其中又以高安全性的基本特質是各種電子商務活動或行為必須重視且加強的關鍵項目。本文結合安全測試作業與異常偵測作業，提出一套電子商務安全防範架構 (EC Security Prevention Scheme, ECSPS)，在安全事件未發生前，識別出系統的安全漏洞與缺失，適時找出安全漏洞與缺失，以進行後續的修補與改善作業。在安全事件發生後，主動且及時發現事件，且依事件情節的輕重進行後續補救措施，以有效降低安全事件的風險。兩層面的安全防範架構，可以有效降低電子商務安全風險。ECSPS 具備的三項優勢為：

- 例行性的安全測試程序在安全事件發生前，及時提出漏洞修補與缺失改善作業，以降低安全事件發生率。
- 異常事件偵測程序可以即時發現異常安全事件，進而採取後續的補救與強化作業，以減輕安全事件的衝擊與損失。。
- 漏洞與缺失的判斷及安全事件的確認，可以強化兩安全程序對問題的識別能力，以達到互補效果。

參考文獻

[1] 李思萱，全球電子商務銷售首度超越 1 兆美元，預測 2013 亞太區銷售超越北美，2013/02/07-DIGITIMES，中文網。(http://www.digitimes.com.tw/tw/dt/n/shwnws.asp)

[2] 黃于珊，[觀點] 惡魔藏在細節中-- 個資外洩的四大漏洞，2012/08/14- 網路資訊雜誌 (http://news.networkmagazine.com.tw/magazine/2012/08/14/42204/)

[3] 陳政龍，軟體開發之資訊安全管理問題探討，資通安全專論，2008 年 4 月。

[4] 梁定澎主編，電子商務理論與實務，華泰文化事業公司，2000 年 5 月。

[5] 賴森堂，“電子商務軟體品質量測模式”，企業管理學報，第 53 期，53-72 頁，國立臺北大學企業管理學系，2002 年 6 月。

[6] 賴森堂，“以弱點掃描結合修補函數提昇 Web App 安全品質”，電腦稽核，第 25 期，158-168 頁，2012 年 1 月。

[7] 八成民眾，擔心網路購物遇到【詐騙事件】，104 市調中心，2010 年 04 月。(http://www.104survey.com/faces/newportal/viewPointCtx.xhtml;jsessionid=70AFB339F7F99D2503FBD40CBF199DD4.syyweb202?researchId=254)

[8] 我國電子商務發展狀況，2012 中華民國電子商務年鑑，2011 年 10 月。(http://ecommercetaiwan.blogspot.tw/2012/10/blog-post_29.html)。

[9] SONY 又出包 已逾 1 億人個資外洩，2011/05/04-自由時報電子報。(http://www.libertytimes.com.tw/2011/new/may/4/today-int10.htm)

[10] Visa、萬事達卡遭駭 台灣百張信用卡遭殃、已通知換卡，2012/03/31-NOWnews 今日新聞網。(http://www.nownews.com/2012/03/31/320-2800410.htm#ixzz2ZTZOAQFe)

[11] M. Bishop, Computer Security: Art and Science, Addison-Wesley, 2003

[12] D. Evans and D. Larochelle, “Improving Security Using Extensible Lightweight Static Analysis,” IEEE Software, January/February, pp.42-51, 2002.

[13] C. Holcombe, Advanced Guide to eCommerce, LitLangs Publishing, 2007.

[14] G. McGraw, “Software Security”, IEEE Security & Privacy, vol. 2, no.2, 2004, pp. 80–83.

[15] E. Schuman, Gartner: $2 Billion in E-Commerce Sales Lost Because of Security Fears, 2006/11/27-pcmag (http://www.pcmag.com/article2/0,2817,2064021,00.asp)

[16] OWASP Top 10 (https://www.owasp.org/index.php/Top_10_2013-Table_of_Contents)

[17] Penetration Testing vs. Vulnerability Scanning (http://www.tns.com/PenTestvsVScan.asp)

[18] Racquel, 15 Point e-Commerce Security Checklist,2013/3(https://www.swipehq.com/blog/post/15-point-e-commerce-security-checklist/1395)

[19] SANS Top-20 Security Risks (http://www.sans.org/critical-security-controls/)(2013)

以科技接受模式探討智慧型手機與 QR Code 結合的購買行為意圖之研究

王俊嘉
資訊管理系
臺北城市科技大學
toshihitowang@gmail.com

陳美鐘
資訊處
修平科技大學
srachen@hust.edu.tw

曾珈儒
資訊管理系
臺北城市科技大學
ruby24682002@yahoo.com.tw

周珉如
資訊管理系
臺北城市科技大學
s22301089@yahoo.com.tw

摘要

近年來，在日常生活中，無論是在捷運車廂的廣告內容，用來感應通過高鐵的驗票閘門，或是商品型錄、雜誌包裝上，QR Code(Quick Response Code)的應用已愈來愈廣泛。本研究結合智慧型手機與 QR Code 的特性之便利性，擴充至 Davis 的科技接受模式(Technology Acceptance Mode, TAM)，提出概念架構模式，以探討影響 QR Code 接受度之因素以及 QR Code 之使用對消費者行動購買意願之影響。本研究問卷採用便利抽樣方法，針對曾使用過 QR Code 進行線上購物的消費者為對象，共發放 233 份問卷樣本資料，回收並扣除無效問卷後，實際可用之有效樣本為 219 份，有效回收率達 93.99%。並且採用結構方程模式(Structural Equation Modeling, SEM)驗證本研究所提出之假設。結果顯示認知便利性及認知有用性是影響 QR Code 接受的前置因素。其中，認知便利性正向影響認知有用性；認知便利性及認知有用性正向影響朝向使用態度；認知有用性及朝向使用態度正向顯著影響購買行為意圖。整體來說，本研究所提出之研究模式對 QR Code 接受度之預測和解釋力良好。

關鍵詞：智慧型手機、QR Code、認知便利性、科技接受模式

Abstract

In recent years, the applications of QR Code have been widely accepted. According to the combination of smartphones with QR Code, this study extends perceived convenience to Davis' Technology Acceptance Model (TAM) to discuss the factors influencing QR Code acceptance and the usage of QR Code to influence the on-line shopping intention. The convenience sampling method would be conducted for consumers used to on-line shopping through QR Code. There were 233 people replied it. After excluding incomplete questionnaires, 219 out of 233 were deemed valid samples-representing a response ratio of 93.99%. Through the valid questionnaires and Structural Equation Modeling (SEM), our study's hypotheses have all be support. Research findings show that perceived convenience and perceived usefulness are the antecedents of QR Code acceptance. Specifically, perceived convenience and perceived usefulness positively influence attitude toward using; perceived usefulness and attitude toward using positively affect behavior intention to purchase. Overall, this study's findings showed fine predictive and explanatory power of QR Code acceptance.

Keywords: Smartphones, QR Code, Perceived Convenience, Technology Acceptance Model

1. 緒論

條碼(Barcode)的使用幾乎在日常生活當中，所有商品都印有零售標籤。從 60 年代末所出現只有黑白的直線形線條的一維條碼，其儲存資訊容量小，僅能用來記錄商品的編號卻無法描述商品，如少了預先建立的資料庫，資訊就無法被存取；再者，條碼如稍有損壞便無法準確辨認及讀取。因此，導致一維條碼的應用層面受到了限制。幸好豐田集團子公司 Denso Wave 於 1994 年研發出 QR Code 二維條碼，作為優化自動機件的存貨追蹤，之後這種資料儲存容量與一維條碼相較下多達 100 倍的二維條碼便一直在全球被大量運用。

近年來，智慧型手機已成為人人出門必備的隨身物品之一。隨著通訊科技不斷地創新與發展，智慧型手機受到青睞的原因，除了基本的通訊及拍照功能外，還附帶許多應用程式可以在智慧型手機上執行，而這些應用程式不僅具有娛樂效果幫助人們打發空閒時間，也讓人們上網購物變得十分便利。也因為智慧型手機的流行，QR Code 將現實生活與虛擬世界結合，讓 QR Code 成為智慧型手機流行後的產物，無形助長行動商務的趨勢，讓消費者可以在智慧型手機上完成購物前的準備工作，減少購物的往返時間，也不用收集各家的宣傳單後才進行比價的動作，不僅提高消費者的吸引力，更創造新的行銷契機。

目前已有許許多多業者將其販售的商品在包裝上使用 QR Code 二維條碼來儲存網站位址，讓消費者在戶外或是宣傳海報上看到感興趣的商品，不需要記住一長串的網址，只需要將裝有解碼軟體的智慧型手機對準商品型錄上的 QR Code 條碼，待程式讀取條碼成功後，就會自動轉換到相對應的網址，自然會提高消費者瀏覽商品網站或是活動首頁的意願。國外學者[24]在其研究中指出，掃描 QR Code 的動機在於「促銷訊息」的提供，例如：折價券、抽獎或是產品樣本試用；同時亦可透過此

方式將流量導入網站，提高消費者註冊的意圖。國內有研究學者利用 QR Code 設計行動電子商務平台推薦商品，讓消費者可快速瞭解相關商品[2]以及分析消費者個人偏好，建立個人化推薦機制，透過手機的普遍性，建構個人化行動購物系統[5]。然而，較少文獻研究運用智慧型手機的操作便利性，整合 QR Code 二維條碼，培養消費者使用 QR Code 的習慣，探討消費者行動商務之行為態度與意願。因此本研究之主要研究目的包含：

1. 以 Davis 的科技接受模式(Technology Acceptance Model, TAM)為基礎[16]，結合智慧型手機操作方便性與 TAM 易用性後，以認知便利性為外部變數，提出本研究之概念架構模式。
2. 實施問卷設計與調查，經由量表收集消費者使用智慧型手機讀取商品型錄上的 QR Code 條碼後的感受程度。
3. 以 SPSS 19 統計軟體進行建構信度檢定，並以 AMOS 19 軟體作為結構方程模式(Structural Equation Modeling, SEM)之統計分析工具，以實證認知便利性與 TAM 變數以及 TAM 變數之間的關係；並期望發現，商品型錄上的 QR Code 二維條碼可以提高消費者購買商品的意願。

2. 文獻探討

誠如上述，本研究以科技接受模式為基礎，探討消費者利用智慧型手機掃描 QR Code 二維條碼進行行動購物之意圖；並實施問卷調查，藉以了解智慧型手機的操作便利與 TAM 變數之關係，分析與探討智慧型手機與 QR Code 之結合有正向影響使用態度及購買行為意圖。因此，以下分別回顧與探討(1)二維條碼；(2)科技接受模式；以及(3)認知便利性。

2.1 二維條碼 (2D Bar Code)

近年來，使用條碼來儲存與呈現資訊內容的應用需求與日俱增。而原先所使用的一維條碼，因其資料儲存容量太小(約僅能儲存 15 個文數字)，以致於一維條碼在交易資料的直接傳輸應用上受到了限制[4,21]；且一維條碼也因為儲存容量小，僅能作為物品標識，而不能描述物品。因此，一維條碼通常被應用於儲存資料庫的關鍵索引值[26]；它必須透過電腦網路和資料庫的連結以取得更多的資訊。若無法與資料庫相配合，一維條碼即變得毫無意義可言。因此，無法攜帶資料的缺點使得一維條碼其應用範圍受到了極大的限制[8]。

為了解決儲存容量太少以及需要網路及資料庫連結等缺點，於是乎促使了二維條碼的發展與成熟。二維條碼是由一維條碼的概念所發展出來的，而且是為了資料收集自動化的目的所衍生成的技術，其優越性可完全取代一維條碼[6,7]。[9]曾針對二維條碼與一維條碼之特性做一比較，如表 1 所示。

表 1 二維條碼與一維條碼之特性比較

特性	二維條碼	一維條碼
儲存性	1100 個文數字(含中文)	15 文數字(不含中文)
安全性	可於編解碼時加上密碼	無，立刻可讀出
追蹤性	包含產品資訊，同產品一起攜帶	僅為關鍵字，須連結資料庫
抗損性	50%磨損者皆可讀出	無法順利讀出
備援性	可立即支援讀出完整資料	無
效益性	經傳真和影印後可使用	經傳真和影印後無法使用

QR Code(Quick Response Code)是由日本 Denso wave 於 1994 年 9 月所發表出來，其屬於矩陣類型的二維條碼。QR 來自英文「Quick Response」的縮寫，即快速反應的意思。因為發明者希望 QR Code 可讓其內容快速被解碼。它的形狀是正方形的，在 3 個角落，印有像「回」字的正方形圖案，這 3 個正方形圖案可幫助解碼軟件定位，使用者無論以任何角度掃描，資料仍可正確被讀取。因此，QR Code 是一個被發展成能夠高速讀取、高速處理及快速回應的二維符號條碼[1]，如圖 1 所示。QR Code 除以上主要特性外，進而考慮到能夠編碼中文、日文、韓文字元的能力，其應用將會有龐大的亞洲市場潛力。同時 QR Code 能容錯，且有錯誤修正能力，即使被弄髒或是受潮，還是能夠被讀取。二維條碼對於行動商務市場有很大的幫助，所以行動上網聯盟(Open Mobile Internet Alliance, OMIA)於 2007 年提出的行動條碼應用共通規範可分為 4 類：(1)自動化文字傳輸；(2)數位內容下載；(3)網址快速連；(4)身分鑑別與商務交易[13]。

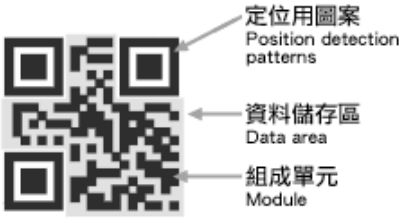


圖 1 QR Code 圖樣

近年來，由於智慧型手機已廣泛地被持用，尤其配合高像素相機功能整合於手機中，QR Code 已逐漸且明顯地可透過手機掃描及讀取使用[2]。QR Code 最明顯的優點在於取代冗長網址或大量資料的輸入動作。使用者可以輕易地使用智慧型手機掃描讀取 QR Code，立即使用或儲存資料[14]。本研究基於二維條碼自動連結網站、容錯和錯誤修正等能力，讓使用者利用智慧型手機判讀商品型錄

上的 QR Code 二維條碼，快速連結到商品網站，完成商品購買，以探討 QR Code 之接受度。

2.2 科技接受模式 (Technology Acceptance Model, TAM)

科技接受模式(TAM)是 Davis 於 1989 年以理性行動理論(Theory of Reasoned Action, TRA)為基礎，發展出解釋和預測使用者接受資訊系統的模式。TAM 假定認知易用(perceived ease of use)和認知有用(perceived usefulness)兩個內在信念，和電腦系統的接受行為有關。認知有用是使用者預期使用特定的應用系統，可以提升工作效率的程度；認知易用是使用者預期使用特定的系統，心智免於努力的程度。TAM 假設電腦系統的實際使用是由使用的為意願決定；而使用的行為意願由使用者使用系統的態度和認知有用共同決定；使用者使用系統的態度則由認知有用和認知易用共同決定；認知易用影響認知有用，而且認知有用中介認知易用對使用意願的影響[16]。此外，TAM 假設某些外部變數會影響認知有用和認知易用，而且認知有用和認知易用中介外部變數對系統使用意願的影響。因此，TAM 可提供外部變數、內在信念、態度、使用意願和實際使用之間關係的基礎[16,22]。Davis 的科技接受模式，如圖 2 所示。

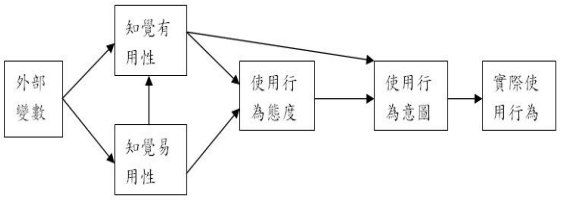


圖 2 Davis 的科技接受模式

2.3 認知便利性 (Perceived Convenience)

對消費者而言，便利可分為商品及服務的便利。而評估便利的方式包含時間和努力[11]。當商品及服務可以節省消費者的時間愈多，則商品及服務的便利性愈高；當商品及服務可以減輕消費者在身體、認知或情感上的能量花費或努力，則商品及服務的便利性愈高。[12]以時間、地點、取得、使用和執行五個面向來衡量商品及服務的便利性。而[29]基於[12]所提出的便利性，去除取得及使用兩個面向，只以時間、地點及執行三個面向評估無線區域網路之便利性；並將認知便利定義為使用無線區域網路完成任務時，認知在時間、地點及執行過程中便利之程度[3]。

本研究參考[3,29]之先前研究，在商品型錄上利用 QR Code 二維條碼的研究中，將認知便利定義為消費者知覺使用智慧型手機進行二維條碼掃描而完成行動購物時，在時間、地點及執行過程中便利的程度。其中，時間的便利是每次使用智慧型手機進行二維條碼掃描而完成行動購物程序時，消費者對使用時間便利程度的感知。換言之，如果在任何時間都能使用智慧型手機完成行動購物時，消費者感知使用時間的便利程度最大；地點的便利是使用智慧型手機進行二維條碼掃描而完成行動購物程序時，消費者對使用地點便利程度的感知。亦即，如果在任何地點都能使用智慧型手機完成行動購物的任務，則消費者感知使用地點的便利程度最佳；執行的便利是指消費者使用智慧型手機進行二維條碼掃描而完成行動購物程序時，感知完成商品購買過程的便利程度。

[28]在其研究中發現，便利性的評價是影響網購的功利動機，而且功利動機是影響消費者網購意願的決定因素。而且在 RFID 行動科技產品[19]，以及線上購物服務的研究中[18]，均發現認知便利是影響使用者對行動科技產品或系統服務使用意願的前置因素。

3. 研究模式與假設

由於操作方便性是智慧型手機的特性之一，在手機操作與容易上手之本質上，與 TAM 模式的易用性變數相近，亦都是指消費者操作智慧型手機可以容易掃描二維條碼，完成行動購物之能力。因此，本研究將兩者結合為認知便利性構面，當作科技接受模式之外部變數；再者，以朝向使用態度及購買行為意圖作為科技接受之指標，提出一個擴充的科技接受模式；進而在商品型錄採用 QR Code 二維條碼的脈絡下，探討認知便利性、認知有用性、朝向使用態度及購買行為意圖之間的關係。本研究以文獻探討的相關理論及相關研究為基礎[12]，提出本研究之研究模式，如圖 3 所示。

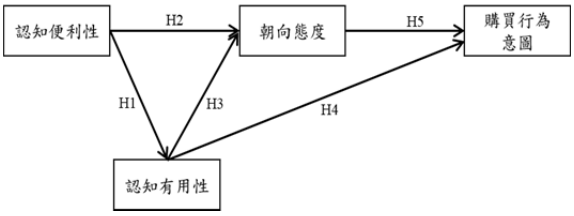


圖 3. 擴充的科技接受模式

3.1 認知便利性和科技接受模式變數之間關係的假設

[29]在無線區域網路的接受模式中發現，認知便利性正向影響認知有用性。因此，本研究提出假設 1。

假設 1：認知便利性正向影響認知有用性。

[3]在行動英語學習的研究中發現，認知便利性正向影響朝向使用態度。因此，本研究提出假設 2。

假設 2：認知便利性正向影響朝向使用態度。

3.2 科技接受模式變數之間關係的假設

依據 Davis 的 TAM 研究架構模式，[12,25,29]的研究結果顯示，認知有用性、朝向使用態度及使用意願的關係如下：認知有用性正向影響朝向使用態度；認知有用性和朝向使用態度正向影響

使用意願。因此，本研究在消費者持用智慧型手機直接掃描商品型錄上的 QR Code，進行行動購物的脈絡下，假設認知有用性、朝向使用態度及購買行為意圖的關係如下：

假設3：認知有用性正向影響朝向使用態度。

假設4：認知有用性正向影響購買行為意圖。

假設5：朝向使用態度正向影響購買行為意圖。

4. 研究方法

4.1 研究樣本與資料蒐集

本研究問卷採用便利抽樣方法，於2013年6月共計發出233份問卷，回收並扣除無效問卷後，實際可用之有效樣本為219份，有效回收率達93.99%。本研究樣本資料分析，受測對象女生103人(47%)，男生116人(53%)；在年齡上，以20至29歲佔38.8%居多；教育程度為大學高達69.4%；職業類別以學生42%居多；曾接觸二維條碼年資以半年佔65.3%居多；每月線上購物金額以1000至1999元佔25.1%居多，所得結果如表2所示。

表2 樣本分析

	排序	人數	%
性別	男	116	53
	女	103	47
年齡	19以下	25	11.4
	20~29	85	38.8
	30~39	60	27.4
	40~49	32	14.6
	50~59	17	7.8
教育程度	高中職以下	13	5.9
	專科	25	11.4
	大學	152	69.4
	研究所以上	29	13.2
職業	學生	92	42
	農林漁牧業	2	0.9
	製造業	5	2.3
	資訊產業	15	6.8
	工商服務業	5	2.3
	大眾傳播業	15	6.8
	軍公教	14	6.4
	法律服務業	3	1.4
	醫療服務業	12	5.5
	金融保險服務業	16	7.3
	運輸通信業	2	0.9
	社會服務業	27	12.3
	其他	11	5.0
接觸二維條碼年資	半年以內	143	65.3
	一年	55	25.1
	二年	17	7.8
	三年	2	0.9
	四年以上	2	0.9
每月購物平均金額	900元以下	129	58.9
	1000~1999元	55	25.1
	2000~2999元	22	10.0
	3000~3999元	7	3.2
	4000~4999元	2	0.9
	5000元以上	4	1.8

4.2 問卷設計與資料分析

本研究問卷之內容包含兩部分，第一部分係有關衡量變項方面；經由研究文獻探討與整理，本研究選擇之潛在變數為：認知便利性(Perceived Convenience, PC)、認知有用性(Perceived Usefulness, PU)、朝向態度(Attitude Toward Using, ATU)、購買行為意圖(Behavior Intention to Purchase, BITP)等四項。第二部分為填答者之基本資料，包括性別、年齡、教育程度、職業、接觸二維條碼年資、每月購物平均金額等。本研究以結構方程模式(Structural Equation Modeling, SEM)進行資料分析，目的在探討變數間之因果關係並以驗證所提理論[20,23]。採AMOS 19進行資料分析工作，並以內定之最大概似估計法(Maximum Likelihood, ML)估計參數，而模式鑑定度屬過度鑑定值(Over identified)，是不會引起參數估計問題 [15,27]。第一階段以信度與效度分析來檢驗研究架構中的每一變數；第二階段以模型檢定來分析研究模型的配適度(Model Fitness)與估計參數顯著性；第三階段係作假設檢定，估計結構模式中研究變數與研究變數之間的路徑，決定其顯著性以及模式的預測能力。

5. 研究結果

5.1 信度與效度

本研究的信度與效度包括觀察變數間的信度、潛在變數的組成信度(Composite Reliability, CR)、收斂效度及區別效度。本研究每一潛在變數之觀察變數間Cronbach's alpha係數均大於0.8，表示觀察變數間具有高度的內部一致性。本研究觀察變數的標準化因素負荷量均在0.6以上、各潛在變數的CR值均在0.6標準以上，符合學者建議值[17]、以及各潛在變數的平均變異抽取量(Average Variance Extracted, AVE)均在0.5標準值上，也符合標準值須大於0.5的建議值。因此，本研究模式中的潛在變數具有高度的信度與收斂效度，如表3所示。表4為相關係數矩陣，其對角線上之數值是各變數之平均變異抽取量的平方根，而在相關係數矩陣中，非對角線上之數值為各不同變數間的相關係數。由表4得知，雖認知便利性和認知有用性之間的相關係數(0.753)略大於認知有用性之平均變異抽取量的平方根(0.749)，但認知有用性和朝向態度與認知有用性和購買行為意圖之間的相關係數分別為0.579與0.659，均未大於認知有用性之平均變異抽取量的平方根。因此，認知有用性與朝向態度及購買行為意圖兩潛在變數之間具有區別效度。除此之外，其餘的每一變數的平均變異抽取量的平方根均大於此變數與其他變數之間的相關係數。因此，可以判定本研究具有相當之區別效度。綜合以上信度與效度之分析得知，整體而言，本研究所有衡量均具有相當良好的測量屬性。

表3 研究變數的信度及收斂效度

潛在變數	題項編號	因素負荷量	Cronbach's alpha	CR	AVE
認知便利性	PC1	0.682	0.857	0.859	0.605
	PC2	0.809			
	PC3	0.797			
	PC4	0.816			
認知有用性	PU1	0.827	0.824	0.834	0.561
	PU2	0.671			
	PU3	0.849			
	PU4	0.622			
朝向態度	ATU1	0.800	0.886	0.887	0.663
	ATU2	0.803			
	ATU3	0.859			
	ATU4	0.793			
購買行為意圖	BITP1	0.836	0.824	0.84	0.639
	BITP2	0.887			
	BITP3	0.657			

表4 相關係數矩陣與區別效度

變項	認知便利性	認知有用性	朝向態度	購買行為意圖
認知便利性	**0.778**			
認知有用性	0.753	**0.749**		
朝向態度	0.581	0.579	**0.814**	
購買行為意圖	0.575	0.659	0.746	**0.799**

註：對角線之值為此一潛在變數之平均變異抽取量的平方根。

5.2 模型檢定

模型檢定包含研究模型的配適度分析(Model Fitness)與估計參數顯著性。由表5所示，p=0.000<0.05，整體模型檢定是顯著的，表示模型與樣本資料並不一致。然因，SEM在大樣本分析下，p值就容易顯著。[10]建議改採用實務上的顯著性，佐以模型配適度指標作為參考。表5呈現模型檢定配適度指標及理想的標準值，包含χ^2、χ^2/df、GFI、AGFI、RMSEA、TLI、IFI、CFI等，所有配適度指標均符合一般學者建議的經驗法則標準，故本研究模型可以達到配適度標準。

表5 研究模型的配適度指標

配適指標	理想要求標準	研究模型
χ^2 (Chi-square)	愈小愈好	196.828 (p=0.000)
χ^2/df	1~3	2.316
(degree of freedom)		
GFI (Goodness of Fit Index)	>0.8 可接受 >0.9 配適良好	0.893
AGFI (Adjusted Goodness of Fit Index)	>0.8 可接受 >0.9 配適良好	0.849
RMSEA (Root Mean Square Error of Approximation)	<0.08	0.078
TLI (NNFI) (Non-normed Fit Index)	>0.9	0.928
IFI (Incremental Fit Index)	>0.9	0.942
CFI (Comparative Fit Index)	>0.9	0.942

5.3 假設檢定

本研究之路徑係數 (path coefficients)與預測能力(predictive ability)方面，如圖4所示。在路徑係數的顯著性部分，由t值來判別，五條路徑均達到顯著水準(p<0.01)。因此，本研究之所有假設均獲得支持成立。在分析結果中，認知有用性之R^2值為0.57，表示認知有用性受到認知便利性(β= 0.75)潛在變數之影響，可解釋57%的結果，具有相當的影響性。朝向態度之R^2值為0.38，表示朝向態度受到認知便利性(β= 0.33)與認知有用性(β= 0.33)二項潛在變數之影響，可解釋38%的結果，解釋力將近40%，具有相當的影響性。購買行為意圖之R^2值為0.63，表示購買行為意圖受到認知有用性(β= 0.34)與朝向態度(β= 0.55)二項潛在變項的影響，可解釋63%的結果，也具有相當的影響性。由上述得知，本研究具有良好的預測能力。

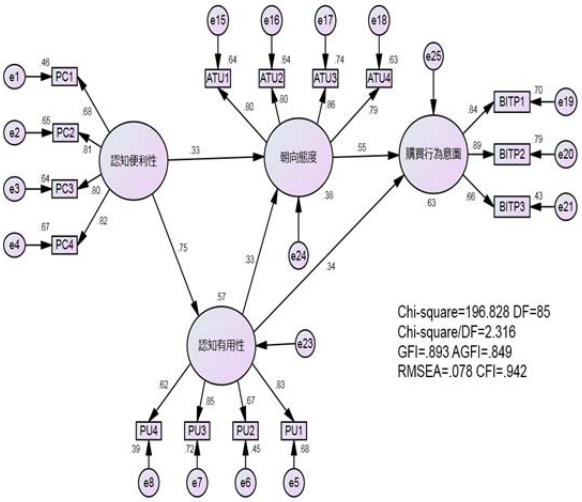


圖4 結構模式分析結果

6. 結論

本研究以Davis 科技接受模式為基礎，利用智慧型手機的容易操作特性，結合QR Code之優點，加入認知便利性至TAM模式中，提出本研究概念架構模式，經過實證分析得知：

(一) 整體而言，本研究所提的研究模式的驗證性因素分析配適度良好，經轉換為結構模式後，其整體模式配適度GFI、AGFI、RMSEA、TLI、IFI、CFI分別為0.893、0.849、0.078、0.928、0.942、0.942。χ^2與自由度的比值為2.316，本研究模式是一個可接受的模式。

(二) 研究結果顯示便利性是智慧型手機與QR Code結合下，可帶動行動商務線上消費的特性之一。認知便利性正向影響認知有用性；認知便利性正向影響朝向態度；認知有用性正向影響朝向態度；認知有用性與朝向態度正向影響購買行為意圖。

(三) 因此，在智慧型手機與QR Code結合下，認知便利性與認知有用性是影響朝向態度及購買行為意圖的前置因素。本研究所提出的研究模式，可以解釋消費者朝向利用智慧型手機掃描QR Code的態度63%之變異，以及解釋進行線上購物的行為意圖38%之變異。整體而言，本研究的模式預測和解釋消費者對QR Code接受度的能力良好。

參考文獻

[1] 林政宏、李宜庭、邱莉婷，"綠色科技新知"，生活科技教育月刊，第 41 卷，第 7 期，3-12，2008。

[2] 吳志祥、張博閔、黃鏗永、黃柏齊、黃國禎，"以 QR Code 為基礎之個人化行動商務系統-以台糖量販店為例"，TANET2010 臺灣網際網路研討會，台南市，台灣，2010 年 10 月。

[3] 張基成、顏啟芳，"以擴充的科技接受模式探討行動英語學習之接受度"，Journal of e-Business，第 14 卷，第 1 期，97-120，2012。

[4] 張勝茂、高翊峰、陳馨雯， "條碼知多少－淺談條碼的演進與二維條碼的應用"， 生活科技教育月刊，第 42 卷，第 6 期，157-168，2009。

[5] 陳富川，應用 QR Code 設計手機個人化行動購物系統，碩士論文，大同大學資訊工程研究所，台北市，2007。

[6] 蔡宛栩，"QR Code 於農產品產銷履歷之應用"，科技發展政策報導，第 4 卷，91-95，2008。

[7] 趙怡晴、陳玲慧，"資料收集自動化的新利器：二維條碼"，電腦與通訊，第 85 卷，31-36，2000。

[8] 晁瑞明、藍大勝、張佳楠、陳雍宗，"以行動載具結合二維條碼與數位學習平台建構無所不在的 STS 合作學習環境"，國立屏東教育大學資訊科學應用期刊，第 2 卷，第 2 期，173-189，2007。

[9] 黃慶祥，資料自動收集與商業自動化，台北：松崗出版社，1997。

[10] J.C., Anderson and D.W., Gerbing, "Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach," *Psychological Bulletin*, Vol. 103, No. 3, pp. 411-423, 1988.

[11] L.L., Berry, K., Seiders, and D., Grewal, "Understanding service convenience," Journal of Marketing, Vol. 66, No. 3, pp. 1-17, 2002.

[12] L.G., Brown, "Convenience in services marketing," Journal of Services Marketing, 4(1), 53-59, 1990.

[13] CamReader, available at http://www.camreader.jp/ (accessed on 12 June 2013).

[14] P., Chaisatien, P. and K., Akahori, "Introducing QR code in Classroom Management and Communication via Mobile Phone Application System," *Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications*, 2181-2187, 2006.

[15] W.R., Davis, "The FCI Rule of Identification for Confirmatory Factor Analysis: A General Sufficient Condition," *Sociological Methods and Research*, Vol. 21, pp. 403-437, 1993.

[16] F.D., Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, Vol. 13, No. 3, pp. 319-340, 1989.

[17] C., Fornell and D.F., Larcker, "Evaluating Structural Equation Models with Unobservable and Measurement Error," *Journal of Marketing Research*, Vol. 18, pp. 39-50, 1981.

[18] S., Gupta and H.W., Kim, "The moderating effect of transaction experience on the decision calculus in on-line repurchase," *International Journal of Electronic Commerce*, Vol. 12, No.1, pp.127-158, 2007.

[19] M.M., Hossain and V.R., Prybutok, "Consumer acceptance of RFID technology: An exploratory study," *IEEE Transactions on Engineering Management*, Vol. 55, No. 2, pp. 316-328, 2008.

[20] M., Igbaria, T., Guimaraes, and G.B., Davis, "Testing the Determinants of Microcomputer Usages via a Structural Equation Model," *Journal of Management Information Systems*, Vol. 11, No. 4, pp. 87-114, 1995.

[21] R.B., Johnston and A.K.C., Yap, "Two Dimensional Bar Code as a Medium for Electronic Data Interchange," *International Journal of Electronic Commerce*, Vol. 3, No. 1, pp. 86-101, 1998.

[22] P., Legris, J., Ingham, and C., Collerette, "Why do people use information technology? A critical review of the technology acceptance model," *Information & management*, 40, 191-204, 2003.

[23] R.C., MacCallum, M., Roznowski, C.M., Mar, and J.V., Reith, "Alternative Strategies for Cross-Validation of Covariance Structure Models," *Multivariate Behavioral Research*, Vol. 29, No. 1, pp. 1-32, 1994.

[24] S., Okazaki, H., Li, and M., Hirose, "Benchmarking the use of QR code in mobile promotion: three studies in Japan," *Journal of Advertising Research*, Vol. 52, No. 1, pp. 102-117, 2012.

[25] C.S., Ong, J.Y., Lai, and Y.S., Wang, "Factors affecting engineers' acceptance of asynchronous e-learning systems in high-tech companies," *Information & Management*, Vol. 41, No. 6, pp. 795-804, 2004.

[26] T., Pavlidis, J., Swartz, and Y.P., Wang, "Information Encoding with 15 Two-Dimensional Bar Codes," *Computer*, Vol. 25, No.6, pp. 18-28, 1992.

[27] T., Reilly, "A Necessary and Sufficient Condition for Identification of Confirmatory Factor Analysis Models of Factor Complexity One," *Sociological Methods and Research*, Vol. 23, No. 4, pp. 421-441, 1995.

[28] P.L., To, C., Liao, and T.H., Lin, "Shopping motivations on Internet: A study based on utilitarian and hedonic value," *Technovation*, Vol. 27, No. 12, pp. 774-787, 2007.

[29] C., Yoon and S., Kim, "Convenience and TAM in a ubiquitous computing environment: The case of wireless LAN," *Electronic Commerce Research & Applications*, Vol. 6, No. 1, pp. 102-112, 2007.