基於 3D 人臉辨識之使用者數位版權管理方案
A Smart-monitor-Device-Based User Authentication Scheme For DRM

詹昭文　　莊政儒　　林詠章
國立台中科技大學資訊工程系
ccwen@ntit.edu.tw; megasyscloud@gmail.com
國立中興大學資訊管理系
iclin@nchu.edu.tw

摘要

近年來科技發展非常迅速，電子閱讀裝置愈來越盛行，例如智慧型手機及平板電腦市場目前一片火熱，其背後的核心技術即是螢幕顯示技術。在 MP3 興起的年代，DRM 開始被大家所注意。現在則是因為電子閱讀裝置再度引起關注。DRM 由於牽涉到商業利益，所以變得很重要，本論文著重在利用螢幕嵌入多微型攝影鏡頭，進而辨識使用者人臉特徵，並直接在雲端做辨識運算，提出一個新的辨識系統，架構出理想的數位版權保護架構。

關鍵詞：可攜式電子裝置、數位版權管理、雲端運算

Abstract

The technology is developing very fast in recent years. Electronic reading device is therefore very popular. For examples Smart phone and tablet PC markets are very hot. Their core technology is based on the nowadays screen display technology. DRM had been public at the rise in the era of MP3. It becomes popular again because the popularity of the electronic reading device. So, DRM has become a focus of research area. DRM is important. Because it was involved the most important-「Commercial interests」. In this paper, we propose an embedded multi-camera screen-based user identification scheme that uses cloud computing to perform the recognition operation. The presented paper proposes a new scheme to perform user identification in DRM.

Keywords: Cloud computing, DRM, portable electronic device.

1. 前言

面對傳播更為容易的數位內容，為保護這些內容的智慧財產權，數位版權管理是關鍵技術。數位版權管理（Digital Right Management，DRM）是一種用來保護數位內容使用的管理機制。透過加密、認證來管理使用者對數位內容的存取權限。透過在文件上加浮水印來證明數位內容的所有權。

依據李彥璋(2006)。電子書的守門員-談 DRM 的保護機制[1]。DRM 功能與模式應用一般分為三個階段，從電子出版物的生產，上架後進行電子出版物的權限保護，並於線上購買與下載服務。

使用者經過身分驗證與權限檢驗後，就可進行電子出版物的閱讀或使用，甚至可進行版權交易。以目前數位版權管理大致上可分為兩個部分

a 提供可視或不可視的數位浮水印加密機制：

加密方法主要是將一張圖檔放入需要加密的數位內容中，一旦有被盜用的嫌疑時，便可以透過浮水印檢視的機制來取出數位浮水印，作為智慧財被盜用的證明。此方法可有效證明其數位內容的所有權，但缺乏使用者認證過程，需與其他加密及認證方式搭配，才能建構出較理想的數位版權保護系統。

b 存取控制：

主要目的為對於數位內容的存取保護，防止任何未經授權的存取或破壞。存取控制的範圍很多，主要指的是允許或禁止某人使用某項資源的能力。驗證方法有密碼輸入驗證、智慧卡驗證、使用硬體設備驗證…等。如蘋果電腦公司的 iTunes 在方法上，可以在雲端提供數位內容的永久儲存記憶體，而使用者端設備的記憶體較少，所以下載下來的數位內容可以隨時從記憶體裡刪除，反之透過身分認證及存取控制，也可以隨時再從雲端上下載下來使用。

對數位內容的存取控制在某種程度上，防止了非法的使用，但相反的，合法的使用者反而可能因為這些限制，而降低購買正版的意願。

本篇提出創新的身分驗證方式。基於 3D 人臉辨識的方法透過螢幕裡的多微型攝像鏡頭辨識並至雲端做及時辨識運算以架構出適用於各種類型的數位內容為本研究之目的。期望透過此方法，在硬體規格可達到前，建構出創新的數位版權管理方法。

2. 背景知識及相關研究之探討

不同於傳統媒體以文字敘述來宣告版權，數位版權管理系統除了可以宣告版權之外，還可以描述數位內容的特性與相關訊息，例如：使用權限以及相關責任等。另外，數位版權管理系統也能與密碼學、浮水印等保護技術結合，增加數位內容的安全性。本章將對數位版權管理系統的基本架構、之前使用的方法分析以及在系統中會使用到的各項技術做探討。

2.1 數位浮水印加密機制

數位浮水印根據人類的視覺系統可分為可視(Visible)與不可視(Invisible)，不管是哪種浮水印都是為了保護或證明被嵌入浮水印的數位內容其所有或使用權。可視或不可視的數位浮水印對於多媒體來說可能是標記、圖案或是一串訊息文字。而不可視的數位浮水印除了上述意義外，也有可能是無特定意義的標記、圖案或是一串訊息文字。因為不可視數位浮水印是看不見得，對於數位內容所造成的破壞比可視的數位浮水印來的小，加上數位浮水印不可視，所以無法知道其嵌入的位置與內容，故可提升安全性。數位浮水印為之前數位版權管理常用的技術，本研究並未涉及數位浮水印，但可使用此方法選擇一個最安全且效率最好的數位浮水印技術來架構更完整的系統，此將可供使用者後續研究之參考。

2.2 存取控制

存取控制通常為使用者(或可稱 subjects)對伺服器所管理的資源(objects)的存取控管。在伺服器端都存有一份清單，使用者與權限記錄在清單上，使用者跟使用者要取出的資源通常都有個識別碼。當使用者要存取數位內容時，伺服器會查核清單上的使用者與權限，作為控管機制，判斷使用者要取出的數位內容。如通過認證，則允許使用者使用其資源，反之則予於限制。

2.3 3D 人臉辨識

人臉辨識主要可以分為兩種方法，一是整體特徵方法，一是局部特徵方法。整體特徵方法為將整張人臉當作個人資訊，計算出一個特徵並以資料庫中所存之特徵，進行相似度比對，如相似度夠高，則可通過認證。局部特徵方法先找出局部特徵，通常是眼睛、鼻子和嘴巴，然後根據這些局部特徵以向量的方式來呈現個人資訊，再以資料庫中所存的特徵，進行相似度比對，若相似度夠高，則可通過認證。

人臉辨識比對相似性目前仍有很多問題，其中最顯著的兩個問題為：1. 光源不同的問題，2. 角度不同的問題。在做辨識的時候，同一張人臉在不同光線及不同角度下，通常都會有很大的差異，這對於辨識率影響嚴重，是近幾年來人臉辨識研究要克服的難題之一。

人臉辨識已有不少的研究及可行的方法。如 Meng Joo Er 與 Shiqian Wu[2]提出 Principal Component Analysis(PCA)、Fisher’s Linear Discriminant(FLD)以及 Radial Basis Function(RBF)來對於人臉做辨識的動作，這些方法可提高系統的速度，但使用 RBF 的唯一缺點便是需要較大的記憶體空間[3]。

另外，如Y. Mitsukura, M. Fukumi, N. Akamatsu[4]在人臉建模的方法為利用基因演算法去定義染色體再進行代數演化，此方法用來搜尋出人臉輪廓的實際效能不錯[3] [5]，可以不用在乎背景影響的因素，因此本架構在雲端運算的實作人臉辨識也參考此演算法來加速辨識的運算。

為了解決前面辨識的種種問題，我們建議以人臉的3D模型做為人臉特徵。亦即將第一次拍攝的多張照片所建之3D模型存入特徵資料庫中，作為人臉辨識的依據。當進行存取控制時再擷取使用者的多張照片建立3D人臉模型，並以之與特徵資料庫中所存之3D人臉模型進行相似度比對，若足夠相似則通過認證，否則不通過認證。(目前3D建模技術或演算法已非常進步，以此技術建立出來的3D人臉模型，做相互比對，並設一個門檻值，如相似度高於門檻值，便可通過認證。)。在此研究我們所稱的3D人臉辨識指的就是如上所述的過程。

2.4 電子時戳

在網路或電子設備中「電子時戳」可以為任何數位內容提供準確的時間證明。在本文所建議的方法中，我們以強固之數位浮水印的技術將電子時戳植入相片中，以提供準確的時間證明，可驗證出數位內容從加上電子時戳後是否曾被人修改過，並用來避免在使用者與伺服器傳輸過程中被截取資料之後作為重播(Replay)用途使用。

2.5 本文中所使用的簡易資料庫

在存取控制的機制中，伺服器會查核清單上的使用者與權限，所以會有欄位名稱定義及存取權限的索引表，伺服器會依照這樣的索引資料，來執行存取控制的機制。如圖(1)，ID_{U1}跟ID_{U2}各自的權限就不相同，能獲得對資料庫的權限就不一樣。

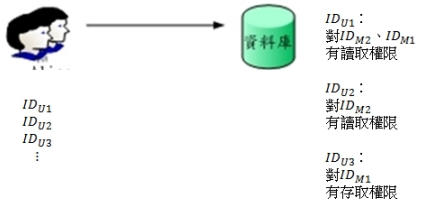

圖 1

在此資料庫的欄位型態表示可為表 1：

使用者U的識別碼	權限	數位內容M的識別碼
ID_{U1}	對ID_{M2}、ID_{M1}有讀取權限	ID_{M1} ID_{M2} ID_{M3} ⋮ ⋮
ID_{U2}	對ID_{M2}有讀取權限	
ID_{U3}	對ID_{M1}有存取權限	

表 1

3. 數位版權管理應用於智能顯示器辨識系統

我們提出一套DRM的認證方案，利用多微型攝影鏡頭嵌入螢幕像素及像素間空餘的空間，用於智能顯示器來辨識使用者臉部特徵，進而達到認證使用者之真實身分的目的，辨識完後，決定是否給予使用權，來達成存取控制之權限管理的目的。

3.1 系統架構

在現今解析度越來越高的顯示器中，如蘋果電腦公司的視網膜螢幕(Retina Display)[6]，在超過其解析度一定程度後，肉眼便分辨不出兩個單獨的像素，所以在像素跟像素之間便有多的空間可嵌入微型鏡頭。

隨著科技的進步和製程改善，微型鏡頭可做越小，日後我們將微型攝影鏡頭嵌入在螢幕，並以一定數量遍佈在其的任意位置中，藉此拍攝使用者特徵。

一個像素通常被視為影像的最小的完整採樣，一幅影像中的像素個數有時被稱為影像解析度，在解析度越來越高的顯示器其像素可被嵌入微型攝影鏡頭的空間會越來越多，也越不影響圖像的品質。

智能顯示器辨識系統我們定義可以有幾個模組：

視訊模組（Video Model）主要是利用嵌入在螢幕裡面的微型攝影鏡頭用來取得影像。

影像模組（Image Model）主要是接收視訊模組的動態連續影像，然後依照時間順序儲存為每張影像畫面，視畫面品質對影像作前處理，例如：去除畫面雜訊、影像強化…等等。

偵測模組（Detection Model），根據系統的目的和應用會有不同的功能，為了系統效能考慮，起初會對複雜的畫面先偵測區分為前景和背景，然後針對包含目標物的前景做主要的處理。

追蹤模組（Tracking Model）為偵測模組的後續處理，因為偵測模組主要是偵測整個畫面的情況，當偵測到正確的目標物後，就可以交給追蹤模組來局部且持續的取得目標物的資訊。

辨識模組（Recognition Model）當有目標物資訊之後，我們可以交給辨識模組來判定為何種目標物，此模組主要功能是抽取目標物的特徵，然後和資料庫中所建立的 3D 人影像模型進行特徵的建立和比對。

3.2 數位內容的保護機制架構

本架構提出數位內容存取控制之架構，數位內容被下載到使用者的電腦端前，其保護機制除了限定使用者的行為之外，另外就是加密數位內容，其在加密模組內的運作流程註冊階段如圖，我們定義多微型攝像鏡頭螢幕為下列設備：

1. 此設備為螢幕，可顯示數位內容
2. 其微型攝像鏡頭有N個，此N個鏡頭以亂數方式，分布於螢幕的像素間。其中N足夠大。
3. 多微型攝像鏡頭螢幕在初始階可隨機從N個鏡頭中，選取n個鏡頭，並從這n個鏡頭，取得n張螢幕前的相片，其中n大於0，小於N。

一個具有可防讀之簡易資料庫且可閱讀數位內容並配備多微型鏡頭螢幕的設備，我們稱之為智能顯示器(Smart Monitor)。(可防讀記憶體是指使用者須輸入正確密碼始可讀取其內容之記憶體)。智能顯示器與授權中心(authorization Center)之資料庫欄位型態表示為表2：

欄位說明	欄位名稱	欄位型態	長度
使用者U的識別碼	ID_U	字元	5
授權中心建立的3D影像模型	P_U	字元	30
授權中心產生的機密數值	x_U	數值	1
數位內容M的識別碼	ID_M	字元	10

表2

3.2.1 註冊階段

在此註冊階段，符號說明意義為：

使用者U的識別碼：ID_U

數位內容M的識別碼：ID_M

M的版權資訊：R_M

註冊階段步驟如下，流程如圖 2：

Step 1. 假設使用者U準備購買數位內容M。U以智能顯示器產生 n 個亂數$(r_1, r_2, \ldots, r_n)$後，智

能顯示器依照此n個亂數挑選 n 個鏡頭，即時拍攝n張使用者相片$p_1, p_2, \ldots, p_n$，其中$p_1, p_2, \ldots, p_n$擁有相同的時戳及各自的相機編號。並將$ID_U, p_1, p_2, \ldots, p_n$及$ID_M$傳給授權中心。

Step 2　授權中心先檢查$p_1, p_2, \ldots, p_n$的時戳之合法性與適時性，若通過檢查則以$p_1, p_2, \ldots, p_n$為U建立 3D 影像模型(稱此 3D 影像模型為P_U)。授權中心同時為U產生一個機密數值x_U。並將機密數值x_U及M的版權資(R_M)傳給U。並將ID_U, P_U, x_U, ID_M寫入機密資料庫。

Step 3　U的智能顯示器將機密數值x_U及M的版權資訊(R_M)存入其資料庫中。

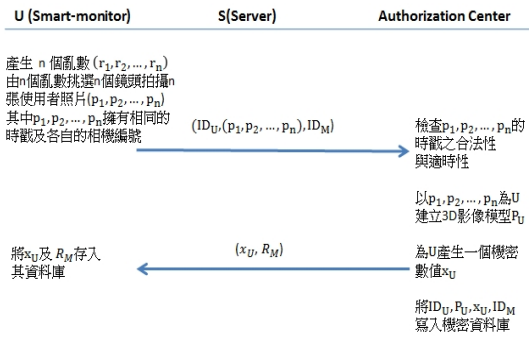

圖 2 註冊階段

3.2.2 使用者要求取出數位內容M階段

假設伺服器(簡稱S，其識別碼為ID_S)擁有受保護的數位內容M。流程如圖3：

Step 1. U取出智能顯示器並輸入ID_S, ID_M，智能顯示器隨機選取 n 個鏡頭，並拍攝U的照片$(q_1, q_2, \ldots, q_n)$，其中$q_1, q_2, \ldots, q_n$擁有相同的時戳及各自的相機編號，然後再將$q_1, q_2, \ldots, q_n$及ID_M傳給 S。

Step 2.　S將$q_1, q_2, \ldots, q_n$及ID_M透過安全通道轉送給授權中心。

Step 3.　授權中心先檢查$q_1, q_2, \ldots, q_n$的時戳之合法性與適時性，若通過檢查則以$q_1, q_2, \ldots, q_n$建立 3D 影像模型(稱此 3D 影像模型為q_U)，再跟機密資料庫中的各個 3D 影像模型P_U做比對。若比對不成功，則拒絕請求。若比對成功，則可取出ID_U及x_U並檢查ID_U是否擁有ID_M，若無則拒絕請求。否則利用$q_1, q_2, \ldots, q_n$算出一個亂數y。若 y 曾經為U計算過則拒絕請求，否則將y存入ID_U的紀錄中及計算金鑰$k = x_u \oplus y$。最後將 k 及ID_M回傳給S。

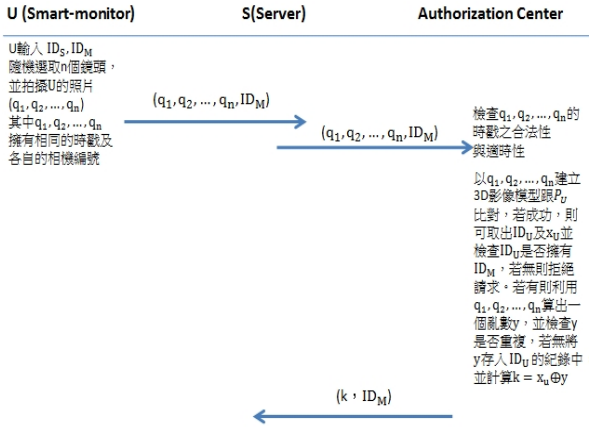

圖 3 使用者要求取出數位內容M階段

3.2.3 回傳數位內容階段

S依授權中心做人臉辨識比對完的結果，決定是否將數位內容回傳給U。流程如圖 4：

Step 1.　S若收到授權中心傳回的拒絕請求訊息，則將其轉送給U，並停止服務。

Step 2.　S根據ID_M取出M並以 k 加密，假設密文為$E_k(M)$，其中E為安全的對稱加密演算法。S將ID_M及$E_k(M)$轉送給U的智能顯示器。

Step 3.　U的智能顯示器收到ID_M及$E_k(M)$後，利用$q_1, q_2, \ldots, q_n$算出同一個亂數y並以資料庫中的x_U計算金鑰$k = x_u \oplus y$，然後解出$M = D_k(E_k(M))$，其中D是E的對應解密演算法。

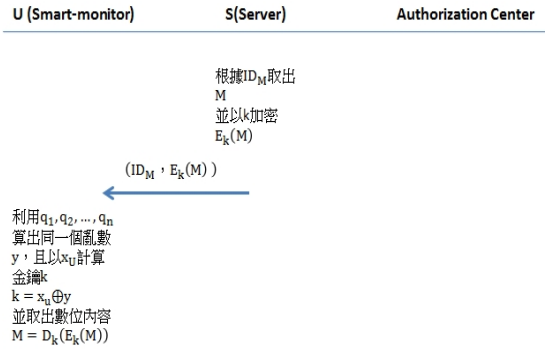

圖 4 回傳數位內容階段

4. 安全性分析

本章探討了五個假設性的弱點分析及系統運作防禦方法：

1. 假設使用者可控制x_U，若使用者將x_U設為0，便可算出k，進而拿到M。但x_U為授權中心產生，U無法控制此亂數便無法拿到M。

2. U如果將智能顯示器借給其他非法使用者去存取數位內容，但拍攝的照片經認證中心進行人臉辨識，經3D影像模型P_U比對不成功則中止服務。

3. 如非法使用者攔截$q_1, q_2, \ldots, q_n$經過計算比對後，所得出來的y會是重複的，則回傳終止服務訊息給U的智能顯示器。

4. 若使用者可事先攔截到x_U，但拍攝的照片經認證中心進行人臉辨識，經3D影像模型P_U比對不成功，則會中止服務。

5. 多微型攝像鏡頭以亂數分布在智能顯示器中，故使用者無法得知是用哪些多微型攝像鏡頭拍攝相片，所以如果使用U的相片在螢幕前，所拍出的相片亦無法通過3D影像模型P_U比對。

5. 結論

為了防止盜版的情況日益嚴重，各家廠商研發出來的數位版權管理系統種類眾多，但由於目的與保護的數位內容類型不盡相同，所以也就沒有一致的標準性。數位內容應該不能被鎖在同一個DRM系統下無法脫身。數位版權管理原始動機良好，但卻可能造成使用者很多不便及不公平。現今的數位版權管理系統應越來越朝向類似紙張書時代的傳統模式發展，用紙張傳統邏輯來思考保護機制。

本研究建議一個新的人臉辨識方法並將之應用於數位版權管理（Digital Right Management，DRM）的使用中，一方面有效的應用於數位內容的存取控制，另一方面同時兼顧DRM所需之安全性與即時性。透過雲端運算辨識結果，我們可以節省在使用者手上的智能顯示器之硬體需求並提高其安全性。此方法如果未來微型攝影鏡頭可達到要求的技術即可廣泛的運用在智能顯示器，如平板電腦、多功能顯示器中並將之發展成資訊安全管理系統中的重要設備。

本研究所建議之創新身分驗證方式。基於 3D 人臉辨識的技術越來越先進，我們可更深入研究其使用的數位浮水印技術及 3D 建模的技術，可探討使用更為安全及有效率數位浮水印技術的可能性並在 3D 建模的技術上更為擬真使其辨識率更高。透過這些技術，建構出創新的數位版權管理方法。

6. 參考文獻

[1] 李彥璋（2006）。電子書的守門員－談 DRM 的保護機制。在陳碧鐘編著，2006 出版年鑑（頁 369-374）。臺北市：新聞局。

[2] Meng Joo Er, S.Wu, j.Lu, and H. Lye, “Face recognition with Radial Basis Function (RBF) Neural Networks,”IEEE Transaction on Neural Networks, Vol. 13, No. 3, PP. 697-710, 2002

[3] 曾郁展（2005）。「DSP-Based 之及時人臉辨識系統」。國立中山大學碩士論文。

[4] Y. Mitsukura, M. Fukumi, N. Akamatsu, “A design of face detection system Using evolutionary computation “,TENCON 2000. Proceedings, Volume: 2 ,24-27 Sept. 2000

[5] H. Yokoo, M. Hagiwara,”Human faces detection method using genetic algorithm” , The Journal of The Institute of Electrical Engineers of Japan, Vol. 117, no.9, pp. 1245-1552, 1997

[6] MoneyDJ 財經知識庫，視網膜螢幕(Retina Display)，
http://www.moneydj.com/kmdj/wiki/wikiViewer.aspx?keyid=38552f1e-d27a-4850-b22f-e26c4bae7f35#ixzz2WjjOtPkM