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 σ=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 σ=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

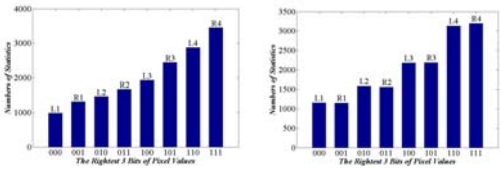
一般來說，若要能找出潛藏於多媒體影像中的機密訊息，並進一步解譯出嵌入訊息之內容，必須透過以下分析步驟的進行方能達成。

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：

$$n_i = |\{colour \mid sortedIndexOf(colour) = 2i\}|. \quad (14)$$

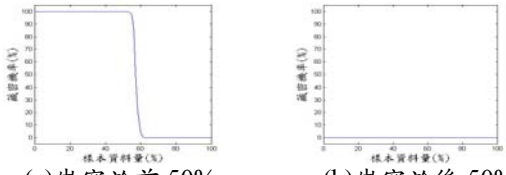
III. 以(15)式計算 χ^2 統計量：

$$x_{k-1}^2 = \sum_{i=1}^{k} \frac{(n_i - n_i^*)^2}{n_i^*}. \quad (15)$$

IV. 利用卡方分佈特性計算出影像藏密機率 p：

$$p = 1 - \frac{1}{2^{\frac{2k-1}{2}}\Gamma(\frac{k-1}{2})} \int_0^{x_{k-1}^2} e^{-\frac{x}{2}} x^{\frac{k-1}{2}-1} dx. \quad (16)$$

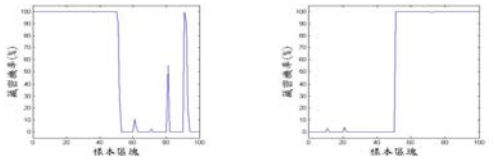
V. χ^2 偵測技術雖能有效地找出依序嵌入資料之影像；但若資料非以循序方式嵌入，則 χ^2 偵測技術將會失效，如圖 2 所示。



(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。

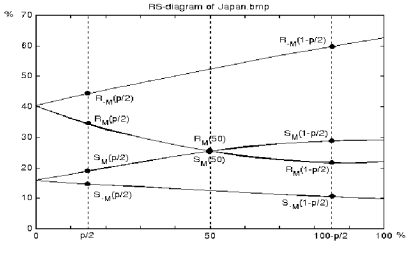
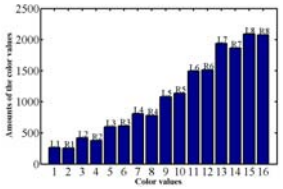


圖 4　RS 計算不同比率翻轉量之統計圖

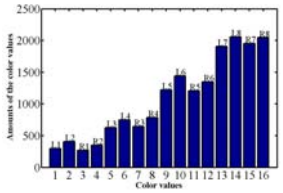
4. Min-Max 演算法安全性分析

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。

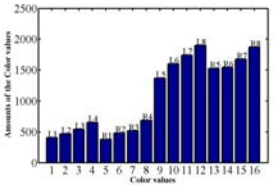
而 Yang 與 Hu 所提出之 Min-Max 演算法係將偽裝媒體待嵌入區塊之像素值與頻率係數，係運用乘數 k 來擾亂可能存在之相鄰像素對問題。當乘數 k 設定等於 2 時，經 Min-Max 演算嵌入之偽裝影像，雖存在像素對問題，如圖 5(b)所示，但已可有效躲過前述 χ2 與 RS 偵測技術仍可有效偵測及估算。若乘數設定為 4 時，則其像素對問題的區間將隨乘數增加而變大，且不再是以相鄰位置出現，將依乘數 k 的設定而形成不同群組，如圖 5(c)所示。因此 χ2 與 RS 偵測技術已經無法有效偵測運用 Min-Max 演算法所簽入之訊息及浮水印資料。



(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.