Journal of Science and Engineering Technology, Vol. 10, No. 1, pp.35-43 (2014)

灰階影像藏匿彩色浮水印採用（2, 2）門檻秘密分享策略

程于芳　林宗德
國立彰化師範大學工業教育與技術學系
50007 彰化市進德路 1 號

摘　要

隨著資訊科技的日新月異，數位資料的編輯、修改以及複製的方便性，使得如何保障產權就變成十分重要的議題。Visual secret sharing strategy 是基於數位影像產權所產生的一種隱藏式浮水印技術。在過去，基於視覺密碼模型之浮水印技術，對於嵌入的浮水印僅黑白或者是簡單的幾個顏色文字。因此本文研究採用（2, 2）門檻秘密分享策略，實現灰階圖像嵌入彩色的浮水印並結合 Toral automorphism 來達到對於影像攻擊如剪裁、模糊、雜訊、銳化、JPEG 壓縮的強韌性，在實際實驗我們以剪裁 10%、20%、30%、模糊化、雜訊、銳化、JPEG QF=90、50、10 作爲影像攻擊手段。實驗結果表示，裁 20%與 30%攻擊下之還原浮水印 NC 值分別爲 0.857 與 0.808，其餘攻擊的 NC 值皆在 0.934 以上。最後，增加水平/垂直的扭曲攻擊與旋轉攻擊實驗，本研究所提出的方法，能夠有效抵禦水平/垂直扭曲攻擊以及 15 度以下的旋轉攻擊。

關鍵詞：門檻秘密分享策略，視覺密碼，彩色浮水印。

Color Watermarking for a Grayscale Image Based on （2, 2）Threshold Secret-Sharing Schemes

YU-FANG CHENG and TZUNG-DE LIN
Department of Industrial Education and Technology, National Changhua Universily of Education
No.1, Jin-De Road, Changhua 50007, Taiwan, R.O.C.

ABSTRACT

Computer and communication technology has increased the transmission and exchange of digital data and created an environment in which digital information is easy to spread, copy, and modify, necessitating effective copyright protection techniques. Previous watermark studies have used only binary, grayscale, or a four-color images for visual cryptography. In this study, the RGB color watermark was embedded into a grayscale image based on (2, 2) threshold secret-sharing schemes. We propose two strategies: combining binarzation and toral automorphism, and combining “neighboring relations” and toral automorphism. In the experiment, the attack resilience was evaluated it contained 10% clipping, 20% clipping, 30% clipping, blurring, noise, sharpening, scaling, JPEG QF = 90, JPEG QF = 50, and JPEG QF = 10. The neighbor relations approach reduces the destruction of the image that is embedded information. The watermark NCs under 10% clipping and 20% clipping attacks

were 0.857 and 0.808, and the remaining NCs exceeded 0.934. Finally, we added horizontal/vertical distortions and rotation attack to the experiment. The results show that the proposed method effectively resists horizontal/vertical distortion and rotation attacks below 15°.

***Key Words*:** threshold secret sharing schemes, visual cryptography, watermarking.

一、文獻探討

隨著資訊科技的日新月異，網路科技的普及，使得多媒體資料的傳遞變得十分迅速。由於數位資料編輯、修改以及複製的方便性，導致原創者對於創作的智慧財產權的憂慮。因此，對於數位資料進行一些訊息的嵌入，以供未來可以驗證其產權也就變成十分重要的研究議題了。其中對於數位影像資料產權驗證方法稱爲浮水印。

浮水印分爲兩種，一種是浮現式，這一種是可以被看到的浮水印（visible watermarking），其資訊可在觀看影片或者圖片時同時被看見。另一種則爲隱藏式，是以數位資料的方式加入音訊、圖片或影片中，但是這在未做任何處理的情況下是不會被看到。而這種隱藏式浮水印的重要應用就是爲了保護智慧財產權，避免數位資料未經授權進行複製或拷貝甚至使用。

因此，對於一些常規的影像處理方式，隱藏式浮水印必然須在這些處理後，還能夠將藏入的浮水印抽取並且擁有一定比例的可辨識度或者完整性。這些常規的影像處理大致分爲旋轉（rotation）、縮放（scaling）、剪裁（cropping）、壓縮（compression），而避免這類的處理則爲浮水印重要的課題。

「視覺密碼」，1995 年由 Naor 與 Shamir[1]提出的加密技術，視覺密碼在加密過程，將機密影像分解成 n 張分享影像，這些分享影像看起來是雜亂無章的內容。解密過程，不需要複雜的運算只要有 k 張或者 k 張以上的分享影像重疊，便可還原機密影像，但若低於 k 張的分享影像重疊，機密影像則無法還原，這就是所謂的（k, n）門檻機制（k-out-of-n threshold）。

Hou 與 Chen [6]將視覺密碼應用於浮水印，受保護的灰階圖像透過像素的增減將 Share-1 的資訊藏入，利用這種方式完成浮水印的嵌入。Hwang 與 Chang[8]爲了包含更多的意義，將每一個像素擴展成 3x3 區塊，這些方法的缺點，無法抵禦剪裁的攻擊，第二點則是修改了受保護的圖像，第三點，嵌入的浮水印爲黑白影像。

Chang 與 Chuang [5]提出了改良的 Hou 與 Chen 的方法，他們認爲頻率域的處理[3, 7, 9, 11]須要相當複雜的計算，因此 Chang 與 Chuang 採用 Voyatzis 與 Pitas[14]所提出的 Toral Automorphisms 方法，Toral Automorphisms 方法是將須受智慧財產權保護的圖像將整圖所有的像素進行位置上的置換（或稱打亂動作），這個方法有兩種特點：第一點利用參數 k 與處理次數 t 作爲嵌入與抽取浮水印的關鍵鑰匙；第二點在抽取浮水印的方式並不是運用反函數而是繼續以嵌入相同的函式做還原動作。最重要的，這種方式對於裁剪的攻擊是具有強健性的。

由於這個方法的計算簡單，經過幾次的處理其浮水印已經變成無法判斷近乎雜訊的圖像，因此成爲許多浮水印處理必然會使用的技術。以下是 Toral Automorphism 處理定義：

$$\begin{pmatrix} X_t \\ Y_t \end{pmatrix} = A \begin{pmatrix} X \\ Y \end{pmatrix} (mod\ N) \qquad (1)$$

其中 X、Y 爲原圖的座標，X_t、Y_t 是經過 t 次 Toral Automorphosm 處理後的新座標，A 是轉換矩陣，N 爲影像的尺寸。而矩陣 A 常見的有下列五種：

$$\begin{bmatrix} k+1 & 1 \\ k & 1 \end{bmatrix}、\begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix}、\begin{bmatrix} k+1 & k \\ 1 & 1 \end{bmatrix}、\begin{bmatrix} 1 & k \\ 1 & k+1 \end{bmatrix} or \begin{bmatrix} k+1 & k \\ k+2 & k-1 \end{bmatrix} \qquad (2)$$

Tsai 與 Chang[13]認爲彩色的浮水印提供了更好的視覺效果，因此他們提出了灰階影像使用視覺密碼藏入四個顏色文字的浮水印，將傳統黑白視覺密碼的延伸，將重疊的涵義變成四種顏色。

吳佳鴻[1]利用半色調與 CMY 系統實現兩張彩色影像藏入一張彩色影像的視覺密碼系統。半色調技術，這是一種模擬連續調的一種視覺感覺，CMY 系統爲青色（Cyan）、洋紅（Magenta）、與黃色（Yellow）三色所組成的，所以又稱 CMY 顏色模型，通常指顏料、染料、或是墨水的混合情況，隨著混合的顏色越多，每一個顏色會減去（或稱吸收）光度，最後會趨近於黑色。此研究的缺點在於對影像的攻擊，吳所提的系統屬於脆弱性的系統，同時疊合影像對比降低，這也由於採用半色調的技術所導致的，雖然半色調技術

可以使圖像資訊量降低，也使得對於低對比的圖像在使用半色調技術時，會變成較難以辨識。後續的研究如增強對比度的研究[2, 4, 15]，使識別品質提高，但是仍然會使原圖失真情況嚴重。

Surekha 與 Swamy [12]灰階影像藏入黑白影像使用色彩對比表（Color Correlation Table, CCT），利用同像素之間的「最大距離」作爲 Table 以及平均距離 A，假如兩個相同的像素座標分別爲（x1,y1）與（x2,y2），最大距離爲 Max={|x1-x2|,|y1-y2|}並從中取得 30 組與浮水印相同尺寸的資料，相同座標的各 30 組數據平均值 a，若 a（x, y）≥A 則 share-1（x, y）=1，反之爲 0。最後的 share-1 與黑白浮水印進行比較形成 share-2 使 share-1 或 share-2 能夠符合黑白浮水印。這個方法，同樣是不修改受產權保護的圖像，同時不使用擴增處理，因此沒有失真性，但是缺點在於另一張作爲認證收藏的圖像爲雜亂無章的圖像。

本研究意旨嘗試將一張 RGB 全彩的浮水印結合 Toral Automorphisms，利用視覺秘密策略實現受產權保護的灰階圖像不做任何修改，並且利用常見的影像攻擊作爲驗證其強韌性。第二節爲本研究所提出嵌入彩色浮水印之策略，第三節爲實驗設置，第四節爲實驗結果與比較，第五節爲結論。

二、提出之策略

此章節，我們將利用 Toral Automorphisms 與視覺密碼將在兩張灰階影像 M_1 與 M_2 藏入一張彩色浮水印 W，其中一張灰階影像 M_1 爲受財權保護的影像，另一張則是爲了重疊效果而需要進行改變的 M_2，M_1 與 M_2 分別使用二值化與本實驗所提出的「相鄰關係」形成 Share-1 與 Share-2，研究當 M_1 受到影像攻擊的強韌性與 M_2 經過嵌入之後的影像之影響性。

（一）Share-1 之形成

爲了使 M_1，也就是受產權保護的灰階影像不做任何影響圖像品質，所以這個階段利用 Toral Automorphisms 與二值化。爲了提高強韌性與安全性，因此我們從 M_1 選取某一座標點作爲形成 Share-1 的起始點，來提高破解的難度與對於一些影像處理的強韌性。

輸入：灰階影像 M_1，嵌入起始座標（α, β），TA 採用矩陣 $\begin{bmatrix} k+1 & 1 \\ k & 1 \end{bmatrix}$，且 k 參數爲 γ，與執行次數 p，其中 $0<p<P$，其中 P 爲 M_1 經過 P 次 Toral Automorphisms 會回復爲 M_1。

輸出：Share-1。

Share-1 形成之步驟：

步驟一：將從 M_1 中選擇從座標（α, β）開始取得 $M' \times M'$ 大小的 M'_1，其中 $\sqrt{N \times N \times 2} \leq M' \leq M$，$N$ 爲浮水印 W 之長與寬，如圖 1。

步驟二：依據二值化程序，當值大於 127 則爲 1，小於等於 127 爲 0。其中 1 爲黑點，0 爲白點，如圖 2。

步驟三：使用利用公式（1）進行 Toral Automorphisms 處理。經過二值化的 M'_1 進行打亂 p 次數形成 Share-1，輸出 Share-1，如圖 3。

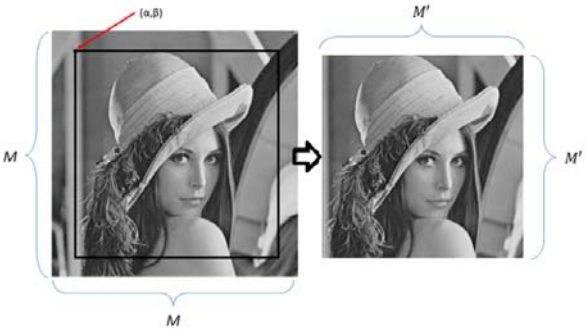


圖 1. Share-1 的範圍取得過程

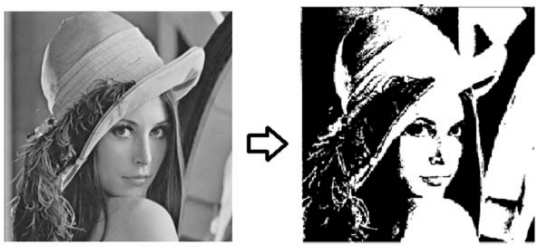


圖 2. 二值化處理

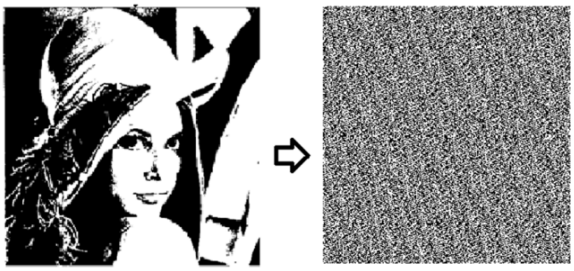


圖 3. Toral Automorphisms 轉換結果

（二）Share-2 之形成

Share-2 的形成使用本研究所提出的「相鄰關係」方法，本研究在 M_2 要嵌入 W，也就是爲了 W=Share-1⊕Share-2 時，會尋找 3×3 區塊內 9 個數值，尋找出作爲中間位置是改變 3×3 區塊區塊內 9 個數值爲最少次數的，將此數值取代原本中間值，並且依據中間值與 W=Share-1⊕Share-2 結果進行修改相鄰值。最後形成 Share-2。

輸入：灰階影像 M_2，嵌入起始座標浮（α,β），圖 Share-1，浮水印 W，Toral Automorphisms 參數 γ，W執行 Toral Automorphisms 次數 h，其中 H 爲W執行 Toral Automorphisms 還原原圖的次數，0 < h < H。

輸出：完成嵌入的 Share-2

相鄰關係 Share-2 處理流程如下：

步驟一：從 M_2 取某一座標（α,β）作爲嵌入的起始點開始取得 $M'\times M'$ 大小的 M'_2，其中 $\sqrt{W\times W\times 27}\le M'\le M$。

步驟二：M'_2 [x][y]，其中 x=1+3i，且 0≤ i < $M'/3$，y=1+3j，且 0≤ j < $M'/3$ 劃分 3×3 區塊，每一個 3×3 區塊獨立進行二質化，以 M'_2 [x][y]像素值做爲閾值，相鄰 8 個點大於等於 M'_2 [x][y]爲 1，小於 M'_2 [x][y]爲 0，形成未嵌入的 Share-2。

步驟三：浮水印 W，使用公式（1）進行 Toral Automorphisms 將浮水印 W 進行 h 次的打亂動作其中 K 參數爲 γ，其中 0<h<H，H 則還原影像所需次數，形成 W'。

步驟四：W'中每一個座標依序由左而右由上而下將像素 RGB 數值轉換成二進制 3 個 8bits，如下 $W_R^{(0,0)}=(r_7r_6r_5r_4r_3r_2r_1r_0)_2$、$W_G^{(0,0)}=(g_7g_6g_5g_4g_3g_2g_1g_0)_2$、$W_B^{(0,0)}=(b_7b_6b_5b_4b_3b_2b_1b_0)_2$。

步驟五：每一個區塊 Share-1[x][y]& Share-2[x][y]四周的八個點進行 xor 處理並依序與所對應的 W_R、W_G 或 W_B 比較並修改 share-2 值，直到 Share-1⊕Share-2 完全符合 W_R, W_G, W_B。最後輸出Share-2。

步驟六：M'_2[x][y]之 3×3 區塊中 9 個值分別帶入區塊中央並且執行步驟二之二值化，並與 Share-2[x][y]相對應的 3×3 區塊進行比較 0 與 1，取得最少改變次數 S 之情況之中央值 ω，將 M'_2 之 3×3 區塊中央值帶入 ω，改變相鄰值直到步驟二處理後與 Share-2 相同。

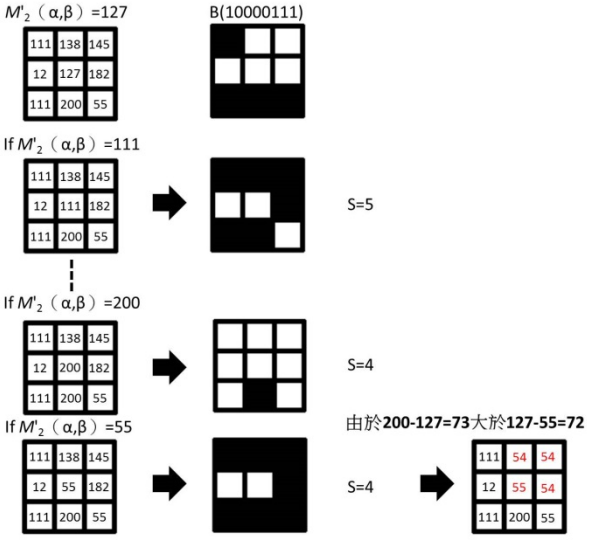


圖 4. 範例修改圖例

舉例來說，以 Share-1 與 Share-2 第一個 3×3 區塊以及 W'第一個座標 R 值作爲例子。W'[0][0]中 RGB 中 R 值爲 10，也就是說 W_R 爲（00001010）2，對應的 Share-1 與 Share-2 爲 Share-1[α][β]與 Share-2[α][β]四周的八個點（左上、上、右上、左、右、左下、下與右下），序列值爲 A（10001101）與 B（01101010），爲了實現 A ⊕ B=WR，將 B 序列值改成（10000111），M'_2（α,β） 中 3×3 區塊中相鄰的 9 個值爲{111,138,145,12,127,182,111,200,55}分別帶入區塊中央並且執行步驟二之二值化，比較 B 序列值 （10000111），直到取得當 200 代入與帶入 55，分別只要針對四個值進行修改，但原本中央值 127 變成 200 或者 55 分別需要變動 73 與 72 數值，故以 55 爲中央值只需改變四個值分爲分別爲上（111）改成 54，右上（145）改成 54，右（182）改爲 54，及中央（127）改爲 55。所有區塊處理完，形成新的 M'_2 並且輸出。圖 4 爲範例修改情況。

（三）浮水印抽取

輸入：兩張灰階影像 T_1與 T_2，Toral Automorphisms 矩陣 $\begin{bmatrix}k+1 & 1\\ k & 1\end{bmatrix}$，$k$ 參數 γ、h、H、p，起始座標 α 與 β

輸出：一張彩色浮水印 I

復原彩色浮水印之步驟：

步驟一：於 T_1與 T_2分別從座標（α,β）開始取得藏匿浮水印之位置形成 T'_1與 T'_2，T'_1進行 TA 處理，形成新的 T'_1。。

步驟二：T'_1 與 T'_2，每一個區塊 3×3 依序化分，如下

$T'_1[x][y]$& $T'_2[x][y]$，其中 x=1+3i，且 $0 \le i < M'/3$，y=1+3j，且 $0 \le j < M'/3$。中央值 $T'_1[x][y]$& $T'_2[x][y]$ 分別爲閾值，相鄰 8 個點執行二值化形成 Share-1 與 Share-2

步驟三：Share-1 與 Share-2 進行 xor 處理，最後形成的圖形 T_3 依據 3×3 劃分，每一個 3×3 區塊依序由左而右由上而下（左上、上、右上、左、右、左下、下、右下）取得 8 個 1 與 0 的數據，最後轉換成 10 進制依序 R→G→B 形成一張由 RGB 所構成的圖像*最後執行* Toral Automorphisms，執行 *H-h* 次數還原原圖。

舉例來說，假如 T_3（1,1）、T_3（4,1）、T_3（7,1）相鄰的點由左而右由上而下分別爲（10101111）$_2$、（01100000）$_2$、（01100000）$_{296}$，轉成 10 進制爲 175、96、130，分別等於 I（0,0）之 RGB 分別爲 175、96、130。如圖 5 所示。

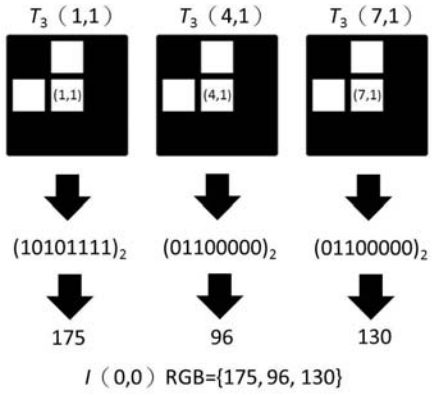


圖 5. 還原的浮水印之範例

圖 6. 產權保護的灰階測試影像，Lena

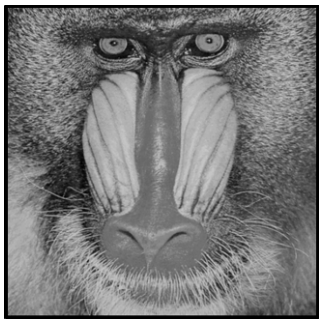


圖 7. 產權認證的測試圖，Mandrill

圖 8. 浮水印的側視圖，數位學習研究所所徽

三、實驗設置

（一）測試圖與參數

本實驗使用 512×512，灰階 Lena 圖像作爲須受產權保護的測試圖像圖 6，以及作爲以後產權認證的圖 7 Mandrill，圖 8 作爲浮水印圖像的彰師大數位學習研究所所徽，其尺寸爲 98 × 98。

Toral Automorphisms 中 k 參數 γ 爲 4、浮水印實驗所打亂次數 h 與 H，分別爲 30 與 42 次，灰階影像 M_1 實驗所採用的打亂次數 p 與還原次數 P 分別爲分別 13 與 25。起始座標（α,β）爲（1,1），取出的尺寸 M'爲 510。

（二）強韌性測試設計

本研究，使用 Ulead PhotoImpact X3 針對可能的對產權保護圖像進行各種影像處理的結果，分別有剪裁、JPEG、模糊化、銳化、縮放、雜訊、顯示浮水印、水平扭曲、與垂直扭曲、旋轉處理。其中剪裁與 JPEG 壓縮分有三種，分別爲剪裁 10%、20%、30%，JPEG QF=90、50、10，旋轉 1 度、5 度、8 度、15 度。縮放是指將圖像縮小然後再放大。顯示浮水印，則是模擬受產權保護的圖像增加了其他可見式浮水印。水平扭曲與垂直扭曲則是將產權保護圖像進行水平座標與垂直座標的置換，並且分爲兩種情況，一種是微幅的，是以肉眼看不至於覺得奇怪的情況，另一種爲幅度增大，以肉眼看會感覺明顯怪異的情況下。旋轉攻擊圖像的形成是先旋轉然後再縮小成 512×512，因此表 1 共 20 種影像處理的圖像作爲檢驗強韌性之影像，分別爲 JPEG 壓縮、可

見式浮水印、模糊化、銳化、縮放、剪裁、水平、垂直扭曲、以及旋轉所使用的圖。

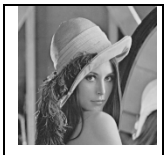
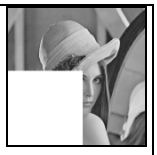
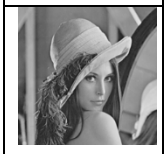
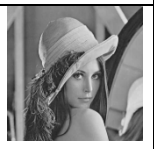
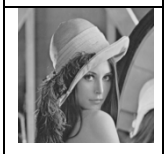
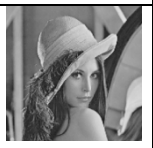
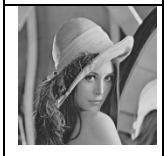
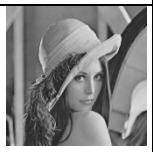
實驗平台，CPU 爲 Xeon Processor 5345/ 2.33GHz，RAM 爲 4GB DDRII，OS 爲 WinXP Professional SP3 並使用 Borland C++ Builder 6.0 作爲開發工具。

（三）檢驗設計

假如影像受攻擊程度越大，則與原圖的差異性則越大，但在這種情況下若所抽取的浮水印與嵌入的相似性越高，則代表這個浮水印技術對於影像攻擊的強韌性越高。但由於人類視覺的可察覺性並沒有那麼高，因此對於某些影像處理的攻擊是無法發覺的，爲了能夠清楚定義受攻擊影像的失真程度，本實驗採用峰值信噪比（Peak signal-to-noise ratio，*PSNR*）其公式如下：

$$PSNR = 10 \times \log_{10}(MAX^2 / MSE), 0 \le PSNR \le 48 \quad (3)$$

表 1. 實驗採用之攻擊圖像

 原始影像	 剪裁 10%	 剪裁 20%	 剪裁 30%
 JPEG QF=90	 JPEG QF=50	 JPEG QF=10	 顯式浮水印
 模糊	 銳化	 縮放	 雜訊
 水平扭曲（小）	 水平扭曲（大）	 垂直扭曲（小）	 垂直扭曲（大）
 旋轉 1 度	 旋轉 5 度	 旋轉 8 度	 旋轉 15 度

其中 MAX^2 代表圖像像素顏色的最大值，也就是 255。當兩張圖相似性越高，*PSNR* 越接近 48，反之則越趨近於 0。*MSE* 爲均方差（Mean Square Error, MSE），如公式（4）：

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left\| I(\mathrm{i},\mathrm{j}) - K(\mathrm{i},\mathrm{j}) \right\|^2 \quad (4)$$

其中 *m* 與 *n* 爲圖像大小，*I* 與 *K* 爲比對的兩個圖像。當 *PSNR* 值越大則代表兩張影像相似性越高;反之若 *PSNR* 越小，則表示兩張影像相似性越低。

最後實驗使用正規化關連值（Normalized correlation，NC）作爲檢驗取出的浮水印與原來浮水印的相似程度。公式（5）爲 *NC*：

$$NC = \frac{\sum_{i=1}^{Wm} \sum_{j=1}^{Wn} \left[W(\mathrm{i},\mathrm{j}) \times W'(\mathrm{i},\mathrm{j}) \right]}{\sum_{i=1}^{Wm} \sum_{j=1}^{Wn} \left[W(\mathrm{i},\mathrm{j}) \times W(\mathrm{i},\mathrm{j}) \right]}, 0 \le NC \le 1 \quad (5)$$

其中，*Wm* 與 *Wn* 爲浮水印的長跟寬，*W*(*i*,*j*)爲原始的浮水印，*W'*(*i*,*j*)爲抽取的浮水印。*NC* 值的範圍介於 0~1 之間，*NC* 趨近於 1 則代表抽取的浮水印與原浮水印越相似，反之，*NC* 值越接近 0 則代表抽取的浮水印與原來的浮水印越不相似。由於浮水印爲全彩，因此分別對於 Red、Green 以及 Blue 的 *NC* 值個別比較以及三值平均值。

四、實驗結果與比較

（一）實驗結果

所有攻擊圖像的 *PSNR* 值以表 2 所示。影像受攻擊程度越大，則與原圖的差異性則越大，*PSNR* 值越低，因此可從表 2 得知各種影像處理的攻擊程度，其中 JPEG 的 *PSNR* 相較於其他影像處理高，因爲 JPEG 是一種將影像的區塊從空間域轉換成頻率域，並且針對高頻部分進行量化處理來產生較爲模糊的影像，以影像來說高頻部分比例是小很多的，所以實際對於影像的影響也小多的。

實驗結果所抽取的浮水印，表 3 所示。從實驗結果來看對於各種攻擊所抽取的浮水印皆能明確的分辨出浮水印的樣貌與顏色，然而對於扭曲攻擊，從水平扭曲（大幅度）與剪裁 30%所抽取出來的浮水印有較爲模糊的浮水印影像，不

過卻仍然保有一定的識別度。如表 3 爲各個攻擊所抽取的浮水印，表 4 爲各個攻擊的浮水印之 NC 值。剪裁攻擊上，以 *PSNR* 來說僅有 10%剪裁與 20%剪裁只有 13.88 dB 與 10.64 dB 甚至 30%剪裁僅剩下 9.29 dB 然而浮水印的抽取結果卻能夠清楚辨別其浮水印，平均 *NC* 分別爲 0.934、0.857 與 0.808。JPEG 壓縮對於 QF=10 仍然有 0.961 的平均 *NC* 值，因此本實驗提出的方法對於 JPEG 極爲有效的強韌性。

垂直扭曲與水平扭曲是將圖像像素進行垂直與水平的位移，小幅度的水平/垂直變化，若不與原始圖像放在一起作爲比較，可能完全無法發現其變化。但在這種攻擊底下，小幅度水平扭曲與小幅度垂直扭分別有平均 0.869 與 0.911 的平均 *NC* 值，而大幅度的水平/垂直扭曲，垂直與水平分別爲 0.858 與 0.757，尤其水平僅剩下 0.757，但是以抽取浮水印圖像來看依然能夠有效的識別其浮水印。最後對於整體所有攻擊的平均 *NC* 爲 0.916，可以說對於各種攻擊都有一定水準的強韌性。

本研究測試了旋轉 1 度、5 度、8 度與 15 度，旋轉攻擊圖像的形成是先旋轉然後再縮小成 512×512。實驗結果發現當我們對於旋轉大概到 8 度 *NC* 值分別剩下 0.648，15 度更爲模糊，*NC* 僅只有 0.582，但仍可看到浮水印的外型。

本實驗「相鄰關係」目的在於改善經過嵌入的 M_2，從圖 9 來看在不仔細看的情況下實際上是看不太出來差異性，然而仔細看與原圖還是有些許的差異，如較爲模糊且有些地方似乎多了些雜訊的感覺。若不將兩者圖像放於一塊比較，很難發現其中的變化。

表 2. 各攻擊圖像之 PSNR

攻擊名稱	*PSNR*	攻擊名稱	*PSNR*
剪裁 10%	13.88	銳化	23.98
剪裁 20%	10.64	縮放	27.92
剪裁 30%	9.29	雜訊	28.35
JPEG QF=90	37.34	水平扭曲 1	18.46
JPEG QF=50	35.58	水平扭曲 2	14.86
JPEG QF=10	30.65	垂直扭曲 1	20.93
浮水印	19.85	垂直扭曲 2	17.35
模糊	32.69	旋轉 1 度	16.93
旋轉 5 度	11.10	旋轉 8 度	10.18
旋轉 15 度	8.53		

表 3. 影像攻擊所抽取之浮水印

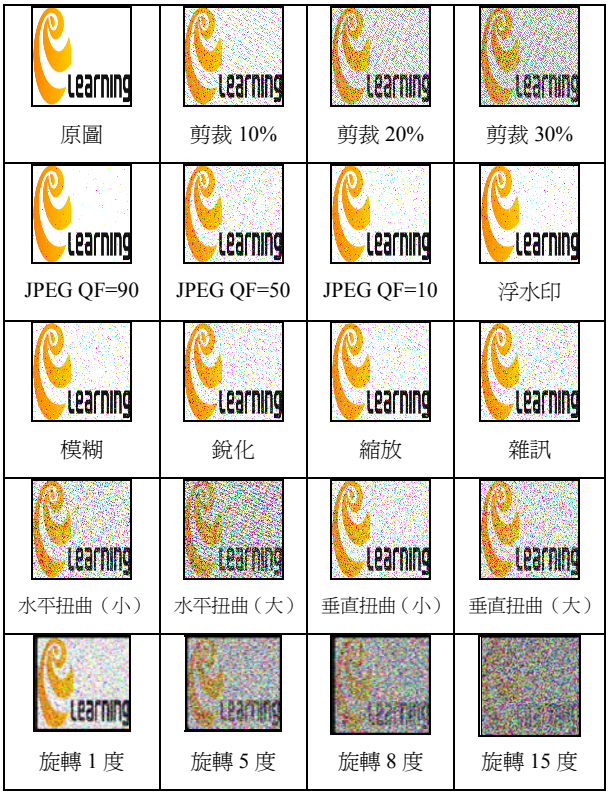


表 4. 實驗結果之 NC 數據

攻擊名稱	*NC*	攻擊名稱	*NC*
剪裁 10%	0.934	雜訊	0.943
剪裁 20%	0.857	水平扭曲 1	0.869
剪裁 30%	0.808	水平扭曲 2	0.757
JPEG QF=90	0.997	垂直扭曲 1	0.911
JPEG QF=50	0.980	垂直扭曲 2	0.858
JPEG QF=10	0.961	旋轉 1 度	0.883
浮水印	0.984	旋轉 5 度	0.694
模糊	0.975	旋轉 8 度	0.648
銳化	0.948	旋轉 15 度	0.582
縮放	0.962		

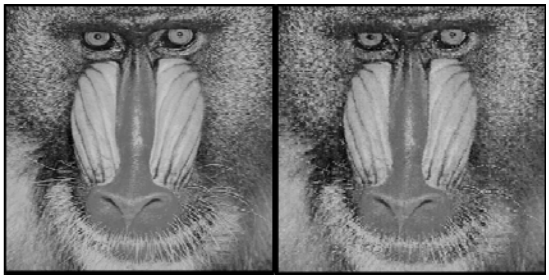


圖 9. 實驗結果 M_2 與原圖差異性（左圖爲原圖，右圖爲實驗二嵌入圖）

本實驗選取某一座標點作爲藏入資料的起始點，來提高破解的難度與對於一些影像處理的強韌性。但由於藏入資料量過大，幾乎使用了整個 Lena，使得對於像剪裁之類的攻擊則沒有明顯的抵禦效果。

（二）相關研究之文獻比較

Surekha 與 Swamy 使用 512×512 的灰階影像，藏入一張 170×100 的黑白浮水印，而我們是 512×512 灰階影像，藏入一張 98×98 的彩色浮水印，可以視爲藏入一張約 480×480 的黑白浮水印。本實驗比較所測試的攻擊影像的 PSNR 值，表 5 與浮水印抽取後的 *PSNR* 值，表 6 *NC* 比較結果。

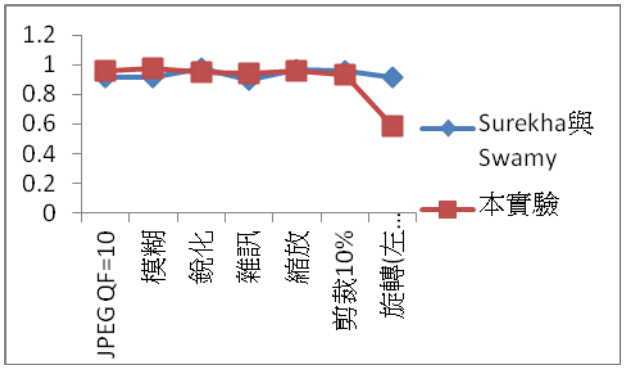
表 5. 攻擊影像的 *PSNR* 值差異

Attacks	Surekha 與 Swamy（2012）	本實驗
JPEG QF=10	35.36	30.65
模糊	32.64	32.69
銳化	32.54	23.98
雜訊	27.89	28.35
縮放	36.81	27.92
剪裁 10%	36.21	13.88
旋轉（左 15 度）	27.94	8.53

表 6. *NC* 比較結果

Attacks	Surekha 與 Swamy（2012）	本實驗
JPEG QF=10	0.913	0.961
模糊	0.914	0.975
銳化	0.978	0.948
雜訊	0.899	0.943
縮放	0.970	0.962
剪裁 10%	0.958	0.934
旋轉（左 15 度）	0.917	0.582

表 7. 折線圖分析



比較發現，對於 JPEG QF=10、模糊與雜訊，本研究兩種方法是較爲好的，而銳化與剪裁，則較爲弱項，縮放攻擊則差異不大。唯一問題在於旋轉攻擊的強韌性，Surekha 與 Swamy 的方法在旋轉（左 15 度攻擊下 *NC* 仍有 0.917，本研究兩個方法僅有 0.582。

以 *PSNR* 來說，本研究所使用的模糊與雜訊影像與 Surekha 與 Swamy 相似，而其他攻擊影像本研究所使用則以極大的差距低於 Surekha 與 Swamy 所使用的。雖然原因不明，但以「假如影像受攻擊程度越大，則與原圖的差異性則越大，但在這種情況下若所抽取的浮水印與嵌入的相似性越高，則代表這個浮水印技術對於影像攻擊的強韌性越高」概念來看，本研究對於 JPEG QF=10、模糊與雜訊確實優於 Surekha 與 Swamy 所提出的方法。而銳化、剪裁、縮放與左旋 15 度，本研究與 Surekha 與 Swamy 有些數據不能嚴格比較，因爲所採用的攻擊圖像與原圖的 PSNR 差異過大。

最後，雖然本研究旋轉角度的攻擊強韌性較不理想，但是 Surekha 與 Swamy 所提出的方法作爲保存以作爲認證依據的圖像卻是一張雜亂毫無意義的圖像，而我們則是一張看不出受到攻擊的影像，並且我們藏入的資料大於 Surekha 與 Swamy 所提的方法。

五、結論

本實驗攻擊的整體效能以 NC 平均值可達 0.857，可以說我們方法對於各種攻擊的強韌性是足夠的，但旋轉角度僅限於 15 度以下。

雖然本實驗對於各種攻擊的強韌性皆有一定的水準，但是仍舊有一些需要改進的地方，以提高浮水印方法的效果。以下幾點是我們可以改善的地方，如下所示：

一、如何提高藏量，如每一個 3x3 區塊有一點並沒有藏入資料。

二、研究如何提高對於旋轉攻擊的強韌性。

三、「相鄰關係」的影像降低破壞性與對於攻擊的強韌性都有改善的地方，利用像素之間的變化量作爲依據，並且研究像素之間變化與攻擊強韌性的關聯性。

四、降低彩色浮水印的資料量。

參考文獻

1. 吳佳鴻（民 91）彩色影像之擴充型視覺密碼，中央大

學資訊管理研究所碩士論文，桃園。

2. 張淑貞（民 98）在半色調圖像中隱藏視覺圖案，國立臺北大學電機工程研究所碩士論文，台北。
3. 黃酩閔（民 95）基於視覺密碼學之影像浮水印技術，屏東教育大學資訊科學系碩士論文，屏東。
4. Chang, C. C., W. L. Tai, and C. C. Lin (2005) Hiding a secret colour image in two colour images. *Imaging Science Journal*, 53(4), 229-240.
5. Chang, C. C. and J. C. Chuang (2002) An image intellectual property protection scheme for gray-level images using visual secret sharing strategy. *Pattern Recognition Letters*, 23(8), 931-941.
6. Hou, Y. C. and P. M. Chen (2000) An asymmetric watermarking scheme based on visual cryptography. Signal Processing Proceedings, WCCC-ICSP 2000. 5th International Conference, 2, 992-995.
7. Hsu, C. T. and J. L. Wu (1999) Hidden digital watermarks in images. *IEEE Transactions on Image Processing*, 8(1), 58-68.
8. Hwang, R. J. and C. C. Chang (2001) Hiding a picture in two pictures. *Optical Engineering*, 40(3), 342–351.
9. Kim, W. S., O. H. Hyung, and R. H. Park (1999) Wavelet based watermarking method for digital images using the human visual system. *Electronics Letters*, 35(6), 466-468.
10. Naor, M. and A. Shamir (1995) Visual cryptography. *Advances in Cryptology - EUROCRYPT'94*, 950, 1-12.
11. Shieh, C. S., H. C. Huang, F. H. Wang, and J. S. Pan (2004) Genetic watermarking based on transform-domain techniques. *Pattern Recognition*, 37(3), 555-565.
12. Surekha, B. and G. N. Swamy. (2012) Visual Secret Sharing Based Digital Image Watermarking. *International Journal of Computer Science Issues*, 9(2), 312-317.
13. Tsai, C. S. and C. C. Chang (2004) A new repeating color watermarking scheme based on human visual model. *EURASIP J. Appl. Signal Process*, 1965-1972.
14. Voyatzis, G. and I. Pitas (1996) Applications of toral automorphisms in image watermarking. *International Conference on Image Processing, Proceedings*, 1, 237-240.
15. Yang, C. N. and T. S. Chen (2008) Colored visual cryptography scheme based on additive color mixing. *Pattern Recognition*, 41(10), 3114-3129.

收件：102.07.31　修正：102.09.02　接受：102.11.21