一種 256 色機密影像分享的新技術

A New Approach on 256 Color Secret Image Sharing Technique

侯永昌* 林芳助* 張兆源*

Young-Chang Hou **Franz Lin** **Chao-Yuan Chang**

(Received Nov. 10, 1999; First Revised Feb. 27, 2000; Second Revised Apr. 13, 2000;

Accepted Apr. 15, 2000)

摘要

為了建立一個網路安全傳輸的環境，目前雖然有很多的方法能夠用來保護智慧財產及機密資料，但其加密及解密過程常需耗費很長的時間，並且其所產生的結果非常容易引起擷取者的懷疑，為了解決這些缺點，我們希望運用資料隱藏的觀念，只需透過少量的運算，將機密資料隱藏在另兩張有意義的資料如圖形中，讓人們視覺無法感覺到機密資料的存在，以建立安全的秘密通訊。

雖然目前所提出的彩色影像隱藏技術(張真誠等，民 88 年；侯永昌等，民 88 年)能夠分別隱藏五色或十色的彩色影像，也可產生有意義的偽裝影像，但是如果彩色機密影像的分享，只能限於分享五色或十色等少量的色彩，對於機密影像的品質及方便性，都大大的受到限制。在本文中我們提出能分享至少 256 色的方法，而且我們利用亂數與遮罩(MASK)的技巧，解決了彩色影像因為色彩的連續性，所造成在偽裝影像上顯露出機密影像區塊的邊界問題。因為亂數及 Key 值的關係，就算當兩張偽裝影像都被截取時，也無法順利的被解密而取出其中的機密影像，可以說是非常安全的技術。

關鍵詞：機密影像分享、彩色影像隱藏技術、遮罩、偽裝影像

Abstract

For developing a safety network transmission environment, there are many cryptography methods that can be used to protect intellectual property rights and secret data, but the time complexity of encryption and decryption are very long. And the encrypted message becomes clutter data that is easy to be suspected. For solving these disadvantages, we use data hiding concepts, and hide a secret image into another two meaningful images. This makes people do not suspect that any secret data will be existed in these two images. Hence it will create a safe secret communication channel.

Some researchers had introduced some color image hiding methods (Chang et al., 1999; Hou et al., 1999). But they only can hide a color image with five or ten colors at most. It is quite restricted especially in the multimedia environment.

In this paper, we present a scheme that can be used to share a secret image with at least 256 colors into

* 國立中央大學資訊管理系所 智慧型資訊系統實驗室
Intelligent Information Systems Laboratory
Department of Information Management, National Central University
E-mail: ychou@im.mgt.ncu.edu.tw

two meaningful cover images. We utilize random number generator and mask technology to solve the image boundary and color continuity problem to make cover images seem innocent and do not show any clue about the secret image block. Because of random number and secret key, even if two shares have been got by some unauthorized persons, it is hard to decrypt to reveal the secret image.

Keywords：secret image sharing, color image hiding technology , mask, cover images

壹、前言

由於電腦與通訊的結合，使得數位媒體快速成長，目前最熟知的數位媒體就是網際網路與光碟，並且由於數位儲存設備、媒體的價格下滑，使得多媒體的資料非常容易的傳播、複製、擷取及修改，並且很多的商業電子資料、機密文件等都已利用網路來傳輸，急需一個安全的資訊分享技術，能夠保護我們在網路上傳送的資料，不被非法者懷疑並且截取解密。

雖然資訊安全在近幾年來已被應用於各個領域中，可以利用加密的方法來保護機密資料，但其加密及解密過程常需耗費很長的時間，並且其所產生的結果容易引起擷取者的懷疑。因此有人想到了資訊隱藏的方法，利用影像特徵來加以僞裝，將機密影像的資料隱藏在另外一張明圖(Cover Image)中，透過明圖的傳遞可以將機密影像的資料傳送出去，即使明圖被別人所截取，也比較不容易造成截取者的懷疑。傳統上，在這個領域的研究可以分爲空間域與頻率域。

在空間域的資訊隱藏技術中，最簡單的就是 LSB 法(Schyndel et al., 1994)了，它是將機密資訊隱藏在位元組最低的幾個位元中。因爲改變最低的位元，對整個位元組影響是最小的，利用人眼無法察覺這麼細微的變化，而將機密資料傳送出去。還有些人利用 LSB 法配合一般資料的加密技術來達成另一種的安全保護。但是 LSB 法很容易被失真壓縮法(Lossy Compression)，例如：JPEG 或 Filtering process 所破壞(Anderson and Petitcolas, 1998; Johnson and Jajodia, 1998)。而且也不是明圖中的每一個 pixel 都適合用來隱藏資訊，因此，LSB 法也很容易被發覺在明圖中藏有機密的資料。透過 bit-plane steganalysis 可以找出利用 LSB 法來隱藏資料的圖形(Lee and Chen, 1999)。

爲了對抗失真壓縮，有人採用了重複隱藏資訊的方法(Redundancy)，例如 Patchwork(Bender et al., 1996)，將隨機選擇的大量 pixel pairs，分別加減同一個灰階值，利用統計的特性以隱藏一個 bit 的資料。但是 Patchwork 所能隱藏的資料量太少，截取者收集到多張相同大小、相同 key 值加密的圖形，就很容易偵測到 patch 的所在(Gruhl and Bender, 1998)，而且 Patchwork 對於 Cropping 或 Jitter 攻擊也沒有防禦的能力(Petitcolas et al., 1998)。

也有人利用向量量化(Vector Quantization)(Gersho and Gray, 1993)的方法來隱藏機密影像。向量量化法首先必需製造編碼書，將影像以固定大小的區塊加以切割，形成許多色階分布不同之小區塊。將其過濾、合併類似區塊而產生具代表性的小區塊，並將之建立一個索引陣列，做爲之後編碼的依據。再將欲壓縮之影像切割成固定大小之區塊，再和編碼書中各編碼區塊做影像比對，找出最接近之編碼區塊影像，以其索引值取代原先之小區塊，達到影像壓縮的目的。當要還原時，只需將壓縮過後影像的索

引值，由編碼書找出索引值所代表的小區塊影像即可。陳同孝等人(Chen et al., 1996)利用此原理提出 VQ 影像隱藏法，但本法的缺點就是還原後的影像會失真，且編碼書的建立並不容易，搜尋的時間也很長。

另一種利用偽裝影像來保護機密影像的方法是利用均質量化技術(Histogram Equalization)(Liaw and Chen, 1997)，它的作法是將 256 灰階的偽圖分爲 16 個等分的灰階區。估算每個灰階區是否足夠隱藏機密影像該灰階區的像點數量，若偽圖的灰階區內之像點個數大於機密影像該灰階區的像點個數，則偽圖在該灰階區足以隱藏機密影像的資料，因此不需調整該灰階區；若偽圖灰階區內之像點個數小於機密影像該灰階區的像點個數，則需用均質量化法的影像處理技術，將偽圖灰階值分佈調整成各灰階區的像點個數均大於或等於機密影像對應的灰階區，調整完畢後即可做像點的替代。利用均質量化法來隱藏資訊，機密影像還原後不失真，但偽圖需要比機密影像來的大，而且偽裝影像會失真在 16 灰階值內。

後來有人利用將影像轉換到頻率域的方式來隱藏資料，一般都是利用快速傅立葉轉換 (Fast Fourier Transform; FFT) (O'Ruanaidh et al., 1996)及數位餘弦轉換 (DCT-Discrete Cosine Transforms) (Memom and Wong, 1998)，將影像以 8*8 的區塊做切割，求出轉換後的係數找出影像的中頻帶，將浮水印藏入其中，使得加入的機密資料不易被察覺。頻率域的優點是非常適合用在 JPEG 失真影像的壓縮上，但是其運算處理通常都非常的複雜，是它的缺點。

除了影像以外，資訊隱藏的技術也大量的應用在其他的多媒體領域，例如：在 Video 或 Audio 中，可以利用 Discrete Cosine、Wavelet、Fractal transforms、Masking 或 Echo hiding 等技術(Anderson and Petitcolas, 1998; Petitcolas et al., 1998)來隱藏所有權人的資訊，其中的 Echo hiding 並且可以抵抗 Jitter 攻擊。

黑白視覺密碼學是另外一個研究方向，Naor 及 Shamir 在 1994 年提出了一個新的密碼學領域，即所謂的視覺密碼學 (Visual Cryptography)(Naor and Shamir, 1995)，將機密影像分散在兩張亂碼的圖像上，重要的目的在於還原機密影像時不需做任何的計算，而直接由人類的視覺系統將機密影像解讀出來，解決了傳統密碼學在解密過程中須大量複雜計算的缺點，而且其門檻機制（Threshold Scheme）使的視覺密碼應用更加廣泛，由 t out of n 的門檻機制，可將機密影像分解成 n 張投影片，分別給予 n 個人每人一張，其中只要有 t 位以上的人，將所持的投影片重疊起來，即可解出機密影像，只有一張投影片是無法破解的。

在視覺密碼學被提出後，一直應用在黑白的影像上，之後在 Naor 和 Shamir(1996)的文章中所提出的模型，能夠隱藏紅色，黃色和透明色，也就是說他們所提出的彩色視覺密碼，能夠隱藏三種顏色，但其方法所產生的 shares 有 2C 張之多，兩個人每人各持

有 C 張 shares，其中 C 代表一個 pixel 所分解的 subpixels 數目。在現今多媒體的世界中，對於彩色的影像來說，只能藏三種顏色是太少了一點，而且每個人持有多張 shares，也太過麻煩。

而 Rijmen 和 Preneel(1996)則提出了色彩分享視覺加密法，其所使用的方法是將一張彩色機密影像，利用視覺密碼的區塊編碼原理，將每一個機密影像的像點，分別建立兩個 2*2 的區塊，其中的一個區塊以隨機的方式填入紅綠藍及白色，共有 24 種組合，並且因爲人眼對於太小的顏色，會看成與鄰近顏色平均後的顏色，利用此原理，另一個區塊則依據機密影像的顏色，依據顏色重疊的原理，找出最適當的組合，完成了機密影像的加密，但此法只能有 24 種組合，所以在復原時會有顏色的失真。

視覺密碼學的缺點是產生的 share 爲雜亂的圖形，容易造成截取者的懷疑，爲了解決這些缺點，因此最近由張真誠等人(民 88)所提一種彩色影像的隱藏技術，其隱藏演算法是針對所給定的一張有 CI 個不同顏色的機密影像 S，將 S 中每一個不同顏色的色盤資料，分別建在一個 CIT 表格中。再任選兩張大小與機密影像同樣大小的掩蓋影像(O^1，O^2)，針對這兩張掩蓋影像中的每一像素，分別擴展成一個由 M(=k*k)個子像素組成的區塊，使得僞裝影像放大爲原來的 k 倍，其中 M 與 k 必需滿足不等式 CI ≦ ⌊ M/2 ⌋ + 1。將機密影像中每一個像素 S_{ij} 的顏色，分享到兩張掩蓋影像的方法是，由 CIT 表格中取得該顏色在 CIT 表中的位置編號 n，在兩張掩蓋影像中的每一像素所擴展的 M 個子像素區塊中，隨機選擇 ⌊ M/2 ⌋ + 1 個子像素，分別填入兩張掩蓋影像中對應的顏色值 O^{1C}_{ij} 與 O^{2C}_{ij}，選擇的條件是要讓這兩個擴展區塊所填入的位置有 n 個位置是重疊的，至於剩餘沒選擇到的子像素則保持透明色。重複這些步驟直到所有像素均處理完畢。而其復原的步驟只要從這兩張僞裝影像及分別針對每個 k*k 的區塊，求算出顏色重疊的子像素個數 n，再由 CIT 表格的第 n 個位置求出原來機密影像的顏色值即可復原。

根據以上的描述可以發現張真誠的方法有以下的缺點：

1. 所能隱藏機密影像的顏色數過少，只能隱藏 ⌊ M/2 ⌋+ 1 個顏色值，其中 M 爲擴展區塊的大小。
2. 固定使用 AND 運算來分解影像像素，因此當兩張掩蓋影像均被取得時，只要經過簡單的區塊檢查很容易就被取出機密影像的紋理，雖然顏色不見得對，但已被發現其中所藏機密影像的內容。

侯永昌等人(民 88)針對上述的缺點提出了一個改良的方法，去除了每個區塊都有固定的 ⌊ M/2 ⌋ + 1 個掩蓋影像顏色值的限制，而是有『隨機個數』的掩蓋影像顏色值，因此就算兩張掩蓋影像被取得，也無法從區塊分析而解密出機密影像的內容。其次我們隨機的利用交集(AND)和聯集(OR)的觀念，來計算掩蓋影像中每一個擴展區塊中顏

色重疊的子像素個數，因此可以得到 0 ~ M 的數值，代表能夠隱藏更多的機密影像顏色值達到 M+1 個顏色。但是隱藏的顏色數量只能到達 M+1 色，仍然是太少，並且會因爲機密影像如果有過多的顏色值爲 0 或 M 的編碼值，所產生的掩蓋影像會產生影像邊界的感覺。

在本文中，我們更進一步提出一種利用兩張明圖來隱藏 256 色、甚至更多顏色的模型，不限於只能分享五色或十色等少量的色彩，而必需降低機密影像的品質。僞裝後的影像具有不易察覺及安全性與可靠度，讓人們視覺無法感覺到機密資料的存在，並且所產生的掩蓋影像，不會因爲機密影像的像素編碼，有過多的擴展區塊中全爲 0 或是全爲 1，而有邊界產生，造成截取者的懷疑。並且因爲亂數、遮罩(MASK)及 Key 值的關係，就算當兩張僞裝影像都被截取時，也無法順利的破解而取出其中的機密影像，可以說是非常安全的技術。以下我們將描述所提模型的方法。

貳、理論基礎

針對所給定的一張 256 色的機密影像 S，另外再任選兩張大小與機密影像 S 同樣大小的影像，做爲 S 的掩蓋影像。256 色機密影像 S 中的每一個像素 S_{ij} 的像素值，只需要 8 個位元($B_7B_6B_5B_4B_3B_2B_1B_0$)即可表示。爲了避免另外傳送色盤資料的麻煩，我們將色盤資料分別藏在每一個像素的第 9 個位元上。色盤的資料量爲 256 色 * 3 分量/色 * 8 位元/分量 = 6144 位元，因此只要 S 的大小超過 80*80，即足以在 S 中藏入整個色盤的資料，而不需要透過另外的管道來傳送。

將每一個像素 S_{ij} 的 9 個位元分別排列成 3*3 的區塊，形成目標編碼區塊(圖 1)。

B7	B6	B5
B4	B3	B2
B1	B0	P

圖 1 S_{ij} 的目標編碼區塊，其中 P 代表色盤資料

接著對兩張掩蓋影像中的每一像素，分別擴展成一個由 M(=3*3)個子像素所組成的擴展區塊，以對應 S 中每一個像素的目標編碼區塊。

首先針對 S 中的每一像素 S_{ij} 的像素值，決定要如何分解到兩張掩蓋影像中。在機密影像分解到兩張掩蓋影像的過程中，爲了增加被破解的難度，我們隨機的決定 S_{ij} 像素值在兩張掩蓋影像的擴展區塊，它是以聯集還是交集的方式來產生。如果是聯集，我們希望讓掩蓋影像擴展區塊的聯集運算結果等於目標編碼區塊的值($B_7B_6B_5B_4B_3B_2B_1B_0P$)；如果是交集，我們希望讓掩蓋影像擴展區塊的交集運算結果也等於目標編碼區塊的值

($B_7B_6B_5B_4B_3B_2B_1B_0P$)。以圖二爲例，不同位置的位元代表不同的值，因此可以表達 256 不同的顏色值。

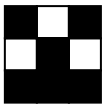
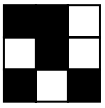
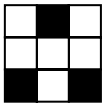
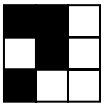
顏色索引值 色盤資料	目標區塊	運算型態	擴展區塊 1	擴展區塊 2
170 1	 101010101	交集	 101010111	 101111101
202 1	 110010101	聯集	 010000101	 110010100

圖 2　256 色隱藏法中，資訊分享的運算方式

假設目標編碼區塊中位元值爲 1 的個數爲 n，針對每個掩蓋影像的擴展區塊，其 M 個位置分配到 0 或 1 的規則如下：

如果是交集 兩張掩蓋影像的擴展區塊經過交集運算，必需有 n 個位置的值爲 1，並且這 n 個位置必需與目標編碼區塊相同。首先在掩蓋影像 1 的擴展區塊中隨機選擇 X_1 個位置，其中 X_1 必需大於 n 小於 M，將其填入 1 值，我們必需讓其中 n 個 1 的位置散佈在目標編碼區塊中原本就是 1 的位置上，其餘的位置則填入 0；而在掩蓋影像 2 的擴展區塊中，隨機選擇 X_2 個位置，其中 X_2 必需大於 n 小於 $n+M-X_1$，將其填入 1 值，我們必需讓其中 n 個 1 的位置散佈在目標編碼區塊中原本就是 1 的位置上，其餘的 X_2-n 個 1，則必需散佈在掩蓋影像 1 的擴展區塊值爲 0 的位置，剩餘的 $M-X_2$ 個位置則填入 0 值。

如果是聯集 兩張掩蓋影像的擴展區塊經過聯集運算，必需有 n 個位置的值爲 1，並且這 n 個位置必需與目標編碼區塊相同。首先在掩蓋影像 1 的擴展區塊中隨機選擇 X_1 個位置，其中 X_1 必需小於 n，將其填入 1 值，其 X_1 個 1 的位置必需散佈在目標編碼區塊中原本就是 1 的位置上，其餘的 $M-X_1$ 個位置則填入 0 值；而在掩蓋影像 2 的擴展區塊中，隨機選擇 X_2 個位置，其中 X_2 必需大於 $n-X_1$ 而小於 n，將其填入 1 值，我們必需讓其中的 $X_2-(n-X_1)$個位置散佈在掩蓋影像 1 的擴展區塊中原本就是 1 的位置上，其餘的

n-X_1 個位置，則必需散佈在掩蓋影像 1 的擴展區塊值爲 0，且目標編碼區塊值爲 1 的位置上，對剩餘的 M-X_2 個位置則填入 0 值。

在求出掩蓋影像的兩個擴展區塊後，編碼值爲 1 的位置上，分別填入O_{ij}^{1c}、O_{ij}^{2c}的顏色值，編碼值爲 0 的位置，分別填入透明色，即可完成顏色的分享。但是影像的顏色分佈具有連續性，爲了避免在一大片顏色爲 255(0)的區域，又剛好選擇到交集(聯集)的運算，以至於讓掩蓋影像上也產生一大片的 255(0)顏色，容易被截取者查覺機密影像的邊界，所以我們並不希望在擴展區塊中，固定的讓 0 就表示要在擴展區塊中加入透明色，1 就表示要在擴展區塊中加入掩蓋影像的顏色。我們設計了兩個 Mask(圖 3)，利用這兩個 Mask，我們隨機的與擴展區塊做 XOR 的運算，結果是 1 的位置才真正填入掩蓋影像O_{ij}^{1c}或O_{ij}^{2c}的顏色，如果是 0 就填入透明色，以增加顏色分佈的亂度，消除影像邊界的問題，增加了截取者破解的困難度。

1	0	1
0	1	0
1	0	1

0	1	0
1	0	1
0	1	0

圖 3 增加顏色亂度的 Mask

而復原的步驟只要將兩張經過擴展的掩蓋影像，分別與 Mask 做 XOR 的運算，以求得每一個擴展區塊的編碼值，再將這些擴展區塊執行適當的交集或是聯集運算，就可以求出機密影像的正確編碼值，其中前 8 個 bit 即爲機密影像的像素值，並將第 9 個 bit 收集成 6144 個 bits 的色盤資料，根據像素值及色盤資料，機密影像即可復原。

參、分享彩色機密影像演算法

一、隱藏 256 色機密影像演算法

以下即爲完整的 256 色機密影像隱藏演算法的詳細步驟：

1. 檢查機密影像 S 是否大於 80*80，若是則由機密影像中取出 256 個色盤資料，並將其轉爲 bit stream，則共有 6144 bits
2. 對機密影像中的每一像點 S_{ij}，求出其像素值的二進位表示法，並分配予一位元的色盤資料，湊成 9 個位元；若分配完 6144 個像點，則分配予 0。執行步驟 3-9，直到所有像點均處理完畢。
3. 將每一個像點的 9 個位元以 Row major 的方式建立一個 3*3 的目標區塊 T，並求位元值爲 1 的個數爲 n。
4. 針對兩張掩蓋影像O^1及O^2的每一像點O_{ij}^1與O_{ij}^2，建立一與目標區塊同樣大小(3*3)的擴展區塊 S^1、S^2。
5. 隨機選取 1 或 0，其中 1 表示這兩張掩蓋

影像的擴展區塊要做交集運算，0 表示這兩張掩蓋影像的擴展區塊要做聯集運算。

6. 如果是交集：在[n, M]之間產生一個隨機數 X_1，在掩蓋影像 1 的擴展區塊 S^1 中，隨機填入 X_1 個 1，其中的 n 個 1 的位置必需散佈在目標編碼區塊 T 中其值爲 1 的位置上，其餘的 M-X_1 個位置填入 0。
   在 [n, n+M-X1] 之間產生一個隨機數 X_2，在掩蓋影像 2 的擴展區塊 S^2 中，填入 X_2 個 1，其中的 n 個 1 的位置必需散佈在目標編碼區塊 T 中其值爲 1 的位置上，其餘的 X_2-n 個 1，則必需散佈在掩蓋影像 1 的擴展區塊 S^1 值爲 0 的位置，剩餘的 M-X_2 個位置則填入 0 值。
7. 如果是聯集：在[0, n]之間產生一個隨機數 X_1，在掩蓋影像 1 的擴展區塊 S^1 中，隨機填入 X_1 個 1，其 X_1 個 1 的位置必需散佈在目標編碼區塊 T 中其值爲 1 的位置上，其餘的 M-X_1 個位置則填入 0。
   在[n-X_1, n]之間產生一個隨機數 X_2，在掩蓋影像 2 的擴展區塊 S^2 中，填入 X_2 個 1，其中的 X_2-(n-X_1)個 1，必需散佈在掩蓋影像 1 的擴展區塊 S^1 中其值爲 1 的位置上，其餘的 n-X_1 個位置，則必需散佈在掩蓋影像 1 的擴展區塊 S^1 值爲 0，且目標編碼區塊 T 值爲 1 的位置上，剩餘的 M-X_2 個位置則填入 0。
8. 隨機選取系統所使用的 Mask(M)，由一半爲 0，一半爲 1 所組成，效果最好。
9. 對於掩蓋影像 1 的擴展區塊 S^1 中每一像素 S_{kl}^1，k, l = 1..3，若 S_{kl}^1 XOR $M_{kl}=0$ 則 S_{kl}^1 ＝掩蓋影像 1 的透明色；若 S_{kl}^1 XOR $M_{kl}=1$ 則 $S_{kl}^1=O_{ij}^1$ 的顏色值。

   對於掩蓋影像 2 的擴展區塊 S^2 中每一像素 S_{kl}^2，k, l = 1..3，若 S_{kl}^2 XOR $M_{kl}=0$ 則 S_{kl}^2 ＝掩蓋影像 2 的透明色；若 S_{kl}^2 XOR $M_{kl}=1$ 則 $S_{kl}^2=O_{ij}^2$ 的顏色值。

二、復原機密影像演算法

由隱藏演算法將 256 色機密影像隱藏在兩張掩蓋影像後，兩張掩蓋影像的透明色資料、交集或聯集的 Key 值、Mask 及這兩張區塊擴展的僞裝影像，可以由不同的管道傳送出去。若這兩張僞裝影像均被截取，沒有 Key 值、透明色資料、隨機所選擇的 Mask，截取者是無法用區塊分析來解開機密影像。以下即是復原演算法。

1. 由兩張大小相同的僞裝影像求出 256 色機密影像的大小。
2. 對兩張僞裝影像分別建立解碼區塊 S^1 及 S^2，其大小爲 3*3，並建立系統內定的 Mask(M)。

3. 將僞裝影像 1 切成 3*3 的區塊，對於每一區塊中的像點 S_{kl}^1，如果顏色值爲該僞裝影像的透明色，則 $S_{kl}^1 = \overline{M}_{kl}$，否則爲 $S_{kl}^1 = M_{kl}$。

   將僞裝影像 2 切成 3*3 的區塊，對於每一區塊中的像點 S_{kl}^2，如果顏色值爲該僞裝影像的透明色，則 $S_{kl}^2 = \overline{M}_{kl}$，否則爲 $S_{kl}^2 = M_{kl}$。

4. 根據 Key 值產生一序列的 1 與 0，其中 1 表示做交集運算，0 表示做聯集。
5. 如果是交集，則將兩個解碼區塊做 AND 邏輯運算。

   如果是聯集，則將兩個解碼區塊做 OR 邏輯運算。

6. 將運算結果的前 8 個位元，組合成機密碼影像的像素值，第 9 個位元就是色盤的資料。收集到前 6144 個解碼區塊運算結果的第 9 位元，然後可以組成完整的色盤資料。
7. 重複以上步驟直所有解碼區塊均處理完畢，最後再將機密影像的像素值對應 768 bytes 的色盤資料，就可以顯示出真正的 256 色的色彩。

三、全彩機密影像隱藏演算法

我們將影像擴展區塊放大成 5x5 的區塊大小，就可以使得所能隱藏顏色數量由 256 色變爲全彩，新的擴展區塊權值表如圖 4 所示。

2^{23}	2^{22}	2^{21}	2^{20}	2^{19}
2^{18}	2^{17}	2^{16}	2^{15}	2^{14}
2^{13}	2^{12}	2^{11}	2^{10}	2^9
2^8	2^7	2^6	2^5	2^4
2^3	2^2	2^1	2^0	0

圖 4 全彩擴展區塊位置權值圖

全彩影像的每個像點是由 3 bytes 所組成，Mask 的大小也需要改變成 5*5，並且因爲像點索引值即可用來表達所要顯示的顏色，因此全彩影像沒有色盤資料。全彩影像只需要 24 個 bits 就可以完全表達，多出來的一個 bit 如果用來儲存交集、聯集運算的指示，就可以減少傳送一個 key 值。其詳細之隱藏與復原演算法與第參章第一及第二節的演算法相同，可以自然的延伸到全彩影像。

肆、實驗結果與安全性分析

一、實驗環境

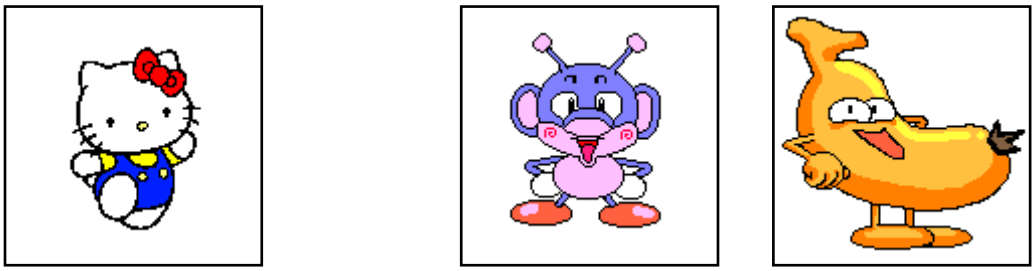
本研究實驗的電腦平台是以個人電腦 CPU Celeron-505，RAM 容量爲 64MB，作業系統採用 Windows 98，並以 Delphi 5.0 爲開發語言，影像資料方面則以 BMP 格式影像檔爲主，實驗影像大小均爲 128x128 像點的彩色與灰階影像。

二、實驗過程

(一) 實驗一：Mask 的作用

現以一張擁有 6 個顏色的彩色機密影像和兩張大小相同的彩色掩蓋影像如圖 5 所示。省略隱藏演算法的步驟 8 和 9 以後，得到兩張僞裝影像，如圖 6 所示。

但是在機密影像中，如果有過多的顏色值爲 0 或 M 的編碼值，所產生的僞裝影像會產生影像邊界的感覺，這是因爲當顏色值爲 0 值可能剛好選擇到聯集運算；而當顏色爲 M 時剛好選擇到交集運算，因此會有此種邊界產生的情形發生。以圖 6 爲例，在香蕉的影像中就可以隱約看到 kitty 頭飾和肚兜的輪廓。



(a)hellokitty(128x128x6 colors)　(b)機器娃娃(128x128)　香蕉(128x128)

圖 5 彩色機密影像和兩張彩色掩蓋影像

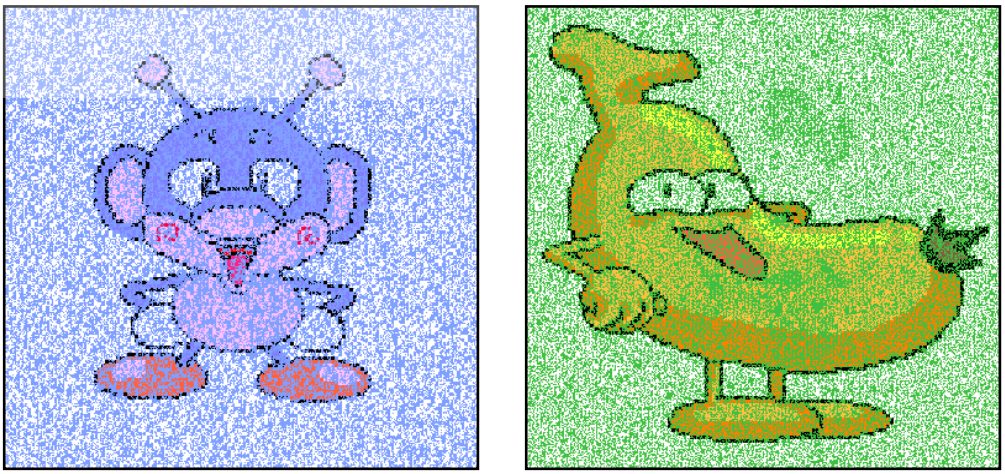


圖 6 兩張彩色僞裝影像：機器娃娃(384x384) 和香蕉(384x384)

我們先對之前的實驗加入隱藏演算法的步驟 8 和 9 以後，再隱藏一次，結果如圖 7，取出的機密影像如圖 8。從圖 7 中我們發現因爲加上了 Mask 以後，確實能夠打亂色彩的連續性，機器娃娃和香蕉圖中沒有任何的輪廓，因此解決了僞裝影像會有邊界的問題。說經由上述的過程，kitty 的影像就成功的藏入這兩張僞裝影像了。

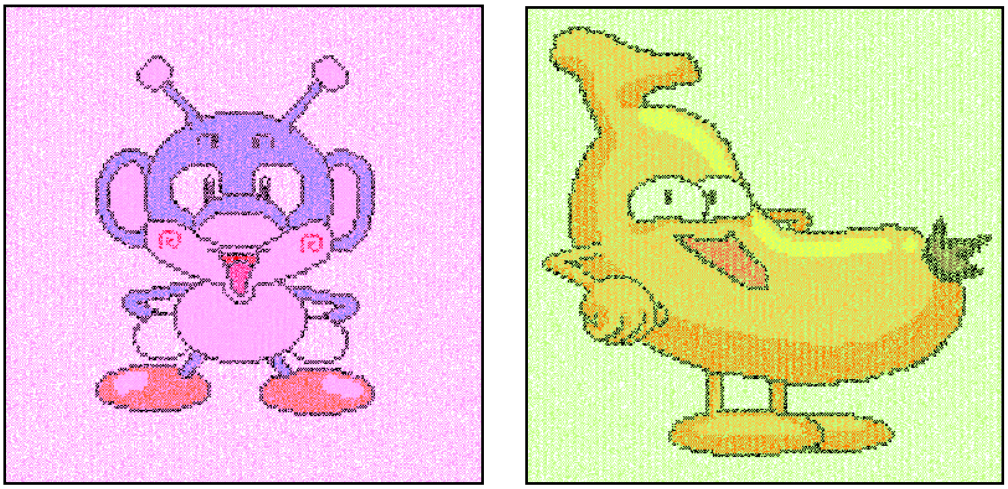


圖 7 兩張彩色僞裝影像：機器娃娃(384x384) 和香蕉(384x384)

圖 8 還原後的彩色 hellokitty 影像 (128x128x6 colors)

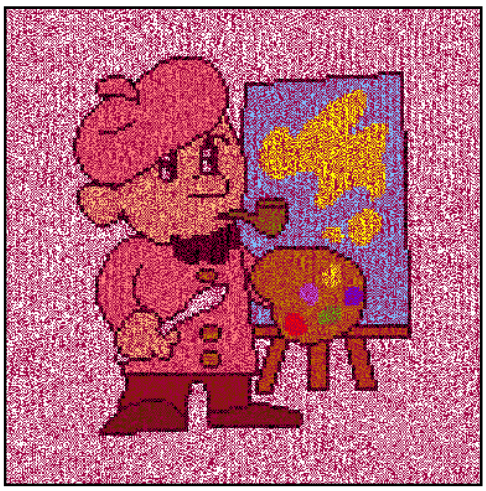
(二) 實驗二：256 色機密影像

現在我們就根據所提出的模型，實際的將一張 256 色的樹林彩色影像(圖 9)，隱藏到兩張普通的彩色影像中(圖 10)。經由我們所提模型的程序處理後，可得到兩張偽裝影像，如圖 11 所示。由上述的過程，樹林彩色影像就成功的藏入這兩張偽裝影像了。之後再由不同的祕密管道將這兩張偽裝影像、Key 值和兩張偽裝影像的透明色資料給接收者，如此即可根據復原程序而取出 256 色的機密影像了(如圖 12)。

圖 9 彩色機密影像 (128x128x255 colors)

圖 10 兩張彩色掩蓋影像 畫家(128x128)

小豬(128x128)



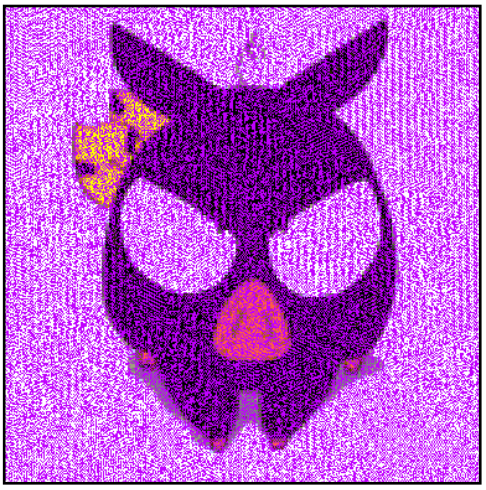


圖 11 兩張彩色偽裝影像：畫家(384x384)和小豬(384x384)

圖 12 還原後的樹林機密影像
(128x128x255 colors)

三、安全性分析

由以上的實驗結果可以發現，本方法確實可以隱藏任何 256 色的影像，能夠產生有意義的僞裝影像，並且因爲加入 Mask 的關係，所產生的僞裝影像不會有明顯邊界的產生。隱藏機密圖後的僞圖雖然與原委圖有明顯的差異，但是以卡通圖片作爲僞圖，尤其是如果截取者不知僞圖的原貌，就算僞圖中穿插有雜點雜訊的存在，但是這些雜訊並非一般的亂碼，而是構成有意義影像的一部份，感覺上也不會覺得太突兀。

關於利用本方法安全性如何？假設若被非法截取者取得其中一張掩蓋影像，則因爲隨機的產生 AND 與 OR 的運算，並且加上了一層 MASK 的轉換，更加讓截取者無法判讀色彩所代表的意義，使得同一顏色可能代表 0、也可能代表 1，並非固定的，而且就算知道區塊大小爲 3*3，也無法找出區塊內子像素的任何關係；若兩張皆被截取，截取者欲從這兩張僞裝影像找出某種關係，則被正確解密出來的可能性也很低。以本實驗而言，機密影像的大小爲 384*384，若知道區塊大小爲 3*3，則截取者必需猜對 128*128 個 AND 與 OR 運算，其猜對哪一種顏色代表 1 哪一種代表 0 的機率爲 1/2，因而解開機密影像的一個像點機率爲 2^{-8}，則截取者要解開整張機密影像的機率由此二者組合，所以其機率爲 $2^{-8*((384*384)/(3*3))}$，這個被解密的機率比(張真誠等，民 88；侯永昌等，民 88；Rijmem and Preneel, 1996)作法更低，幾乎是零。可以說只要截取者不知我們亂數的 Key 值及 MASK，就算有了兩張僞裝影像，仍無法取出機密影像，因此可以說本方法除了能夠分享更多顏色而且是更加安全的。

本研究是以視覺密碼的運算方式來分解機密影像，並且將它分配到兩張掩蓋影像上，這兩張掩蓋影像都是有意義的影像，以減少截取者的懷疑。在這兩張掩蓋影像上的 bit pattern 也是經過精心設計的，因此，當掩蓋影像被被攻擊(破壞、失真、或添加其他資訊)時，本方法就無法疊合出有意義的機密影像。但是只要掩蓋影像被人動了手腳，接收端就一定會發覺，不會造成誤用被篡改的資訊。因爲亂數的關係，截取者無法僞造機密資訊，因此，資訊的內容仍然是安全的。

伍、結論

在本論文中，我們採用資訊隱藏的觀念，將機密影像僞裝在兩張有意義的掩蓋影像中，利用視覺密碼學中的區塊擴展方法，並採用亂數及兩張僞裝影像區塊的 AND 與 OR 運算，先打亂機密影像分享到兩張僞裝影像上區塊之間的關係，再利用 MASK 來混淆截取者，讓其無法判讀色彩所代表的意義。這兩張僞裝影像經由網路傳送出去，即使中途被截取到了，也會因爲僞裝圖片爲普通的圖片並無異狀，而順利騙過截取者的注意，以達到安全祕密通訊的目的。即使截取者懷疑僞裝影像藏有機密而試著解密，其破解本模型而取出機密影像的機率幾乎爲零。只要這些僞裝影像被人動了手腳，接收端就一定會發覺。

由於本方法採用明圖做爲僞裝影像，解決了視覺密碼中僞裝影像是亂碼圖而造成截取者懷疑的問題，並且所能隱藏機密影像的顏色高達 256 色之多，相對於先前的相關研究(張真誠等，民 88；侯永昌等，民 88)，有大幅度的改進，不會因爲顏色數量的限制而影響到機密影像的品質。本研究的方法也可以輕易的將隱藏的顏色，由 256 色擴展到全彩影像，只需要將擴展區塊擴大爲 5*5 即可。而且加上了 Mask 的保護，可以大幅度改進影像物件的邊界問題，不僅提高了安全性，也增加了破解的複雜度。更重要的是本方法由於不需複雜的運算，更加適用於具備簡單計算的設備或是安全身份確認等系統上。

參考文獻

1. 侯永昌、林芳助與張兆源，「彩色機密影像分享技術改良與製作」，第五屆資訊管理研究暨實務研討會，世新大學，民國 88 年 11 月，頁 592-597。
2. 張真誠、蔡垂雄與陳同孝，「一種用來分享彩色機密影像的技術」，第九屆全國資訊安全會議論文集，台中，民國 88 年 5 月，頁 LXIII-LXXII。
3. Anderson, R.J. and Petitcolas, F. A. P. “On the Limits of Steganograpgy,” in *IEEE Journal on Selected Areas in Communications* (16:4), May 1998, pp. 474-481.
4. Bender, W., D. G., Morimoto, N. and Lu, A. “Techniques for data hiding,” *IBM Systems. J.*(35:3-4), 1996, pp.313-336.
5. Chen, T.S., Chang, C. C. and Hwang, M. S. “A Virtual Image Cryptosystem Using Vector Quantization,” *Proceedings of National Information Security Conference*, R.O.C., 1996, pp. 10-16.
6. Gersho, A. and Gray, R. M. *Vector Quantization and Signal Compression*, Kluwer Academic Publishers, MA. 1993.
7. Gruhl, D., and Bender, W. “Information Hiding to Foil the Causal Counterfeiter,” in *Information Hiding Working ’98*, pp.6-1 – 6-15.

8. Johnson, N. F., and Jajodia, S. "Steganalysis: The Investigation of Hidden Information," in *IEEE Information Technology Conference*, Syracuse, N.Y., Sep. 1998, pp. 113-116.
9. Lee, Y. K., and Chen, L. H. "An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement," *Proceedings of Ninth National Conference on Information Security*, Taichung, Taiwan, May 1999, pp. 8-15.
10. Liaw, M.S., and Chen, L.H. "An Effective Data Hiding Method," *Proceeding of the Sixth National Conference on Science and Technology of National Defense*, vol. 2, Taoyuan, Taiwan, Nov. 1997, pp. 534-540.
11. Memon, N., and Wong, P.W. "Protecting Digital Media Content," *Communications of the ACM* (41:7), July 1998, pp. 35-43.
12. Naor, M., and Shamir, A. "Visual Cryptography," Advances in Cryptology: *Eurpocrypt'94*, Springer-Verlag, Berlin, 1995, pp. 1-12.
13. Naor, M. and Shamir, A. "Visual Cryptography II: Improving the Contrast Via the Cover Base," Theory of Cryptography Library Report 96-07, ftp://theory.lcs.mit.edu.tw/pub/cryptol/96-07.ps
14. O'Ruanaidh, J. K., Dowling, W. J., and Boland, F. M. "Phase watermarking of digital images," *Proceedings of IEEE International Conference on Image Processing*, (3), 1996, pp.239-242.
15. Petitcolas, F. A. P., Anderson, R. J. and Kuhn, M. G. "Attacks on Copyright marking Systems," in *Second Workshop on Information Hiding*, Portland, Oregon, Apr. 1998, pp. 1-21.
16. Rijmen, V., and Preneel, B. "Efficient Colour Visual Encryption for Shared Colors of Benetton," presented at *Eurocrypto'96 Rump Session*. Available as http://www.iacr.org/conferences/ec96/rump/preneel.ps
17. van Schyndel, R. G., Tirkel, A. Z. and Osborne, C. F. "A Digital watermark," in *IEEE Int. Conf. Image Processing* (2), 1994, pp. 86-90.

作者簡介

侯永昌

國立交通大學資訊工程研究所博士。現任國立中央大學資訊管理系副教授，兼學生事務處僑生輔導室組長。研究領域爲資訊隱藏、浮水印技術與視覺密碼、模糊理論、軟體工程、演算法則。

林芳助

國立中央大學資訊管理系碩士。目前服役軍中，預計民國 90 年底退伍。研究領域爲資訊隱藏與浮水印技術。

張兆源

國立中央大學資訊管理系碩士。研究領域爲影像處理、資訊隱藏與視覺密碼。