像素不擴展之灰階視覺密碼方法

An Unexpanded Visual Cryptography Method for Gray-level Images

侯永昌
Young-Chang Hou
國立中央大學資訊管理研究所
Department of Information Management, National Central University

許慶昇
Ching-Sheng Hsu
國立中央大學資訊管理研究所
Department of Information Management, National Central University

摘要

視覺密碼的方法將一張機密影像加密成 *n* 張分享影像，參與機密分享的每個人都可以持有一張分享影像。一群被授權的人將他們所持有的分享影像重疊後，就可以在重疊的影像上看到機密訊息；而不被授權的一群人便無法利用分享影像獲得任何機密訊息。視覺密碼學的主要精神在於解密的方法是透過人類視覺系統，而不需使用任何密碼學的知識與計算機資源；因此，在一些無法使用電腦解密的情況下，視覺式的秘密分享方法是一個很好的解決方案。許多視覺密碼方法都使用像素擴展的技巧來進行加密，因此使得分享影像被擴展為機密影像的好幾倍；如此不但造成儲存空間的浪費，也使攜帶更為不方便。此外，大部分的視覺密碼研究都是關於黑白影像的，而較少關於灰階影像的研究。在本文中，我們提出一個可以應用在單一機密影像之任意使用結構，且不需要像素擴展的灰階視覺密碼方法。我們的方法結合機率的觀念來達成分享影像不擴展的目標；同時，我們利用半色調技術，使得黑白視覺密碼技術能夠很容易地被應用在灰階影像上。此外，我們也考量對比損失的問題，提出一個適用於半色調影像的對比補償方法，使重疊影像能達到更好的視覺效果。實驗結果顯示，我們的方法不但有可能達到更好的對比，同時透過對比補償的方法，我們也能獲得更好的重疊影像視覺效果。

關鍵詞：視覺密碼、視覺式秘密分享、半色調技術、灰階影像

Abstract

Visual cryptography is a method to encrypt a secret image into *n* shares so that any qualified set of shares can recover the secret, whereas any forbidden set of shares cannot leak out any secret information. Since visual cryptography uses human visual system to decrypt the secret, it becomes an appropriate scheme while computers or other decryption devices are not available. Most visual cryptographic methods use the concept of pixel expansion; therefore, the size of shares is larger than that of the secret image. Pixel expansion not only results in distortion of shares, but also consumes more storage space. In addition, most studies of visual cryptography were about black-and-white images, whereas few studies were made on gray-level images. In this paper, we proposed an unexpanded visual cryptography method for gray-level images. Our method used the concept of probability to achieve the goal of non-pixel-expansion. Moreover, we employed digital image halftoning to deal with gray-level images. Finally, we also proposed a method to cope with the problem of loss of contrast in visual cryptography. Experimental results showed that our method might get better contrast and better visual effect of the stacked images.

Keywords: visual cryptography, visual secret sharing, halftoning, gray-level images

壹、簡介

視覺密碼是由Naor與Shamir (1995)所提出來的一個新興的密碼學研究領域，它與傳統密碼學最大的不同在於解密的過程。一個視覺式秘密分享方法(visual secret sharing scheme; VSSS)可以將一張機密影像加密成*n*張分享影像，一群參與機密分享的每一個參與者(participants)分別持有一張分享影像。在這一群參與者中，被允許獲得機密訊息的一群人，將他們所持有的分享影像列印成投影片後全部重疊在一起，就可以透過眼睛在這個重疊影像上看到機密訊息；然而，未被允許獲得機密訊息的一群人，便無法透過它們所持有的分享影像來獲得任何一絲機密訊息。視覺密碼學的主要精神在於解密的方法是透過人類視覺系統，而不需使用任何密碼學的知識與計算機資源；因此，在一些無法使用電腦解密的情況下，視覺式的秘密分享方法是一個很好的解決方案。一般而言，視覺式秘密分享方法是透過對應於白點與黑點的兩個$n \times m$布林矩陣(Boolean matrices) M_0與M_1來達成的，這兩個矩陣稱爲基礎矩陣(basis matrices)；加密的方法是將機密影像上的點(白點或黑點)逐一處理，如果是白點(黑點)

的話，就將M_0 (M_1)做欄向量隨機重排，然後將第i列的m個值(顏色)填入第i個分享影像中。至於基礎矩陣的設計則必須要滿足對比與安全性這兩個條件(Ateniese et al 1996b; Naor and Shamir 1995)。

綜觀整個視覺密碼學的研究，可以分別由使用結構(access structures)、技術、色彩模型、機密影像數目與分享影像形式等方面來探討其發展。就使用結構的角度來看，視覺式秘密分享方法可以區分爲門檻使用結構(threshold access structures)與任意使用結構(general access structures)。Naor與Shamir (1995)首先將視覺密碼的觀念應用在(k, n)-threshold的門檻使用結構上。(k, n)-threshold是定義在n個參與者的集合P = {1, 2, …, n}之上的使用結構，表示只有k或大於k個參與者才可以獲得機密訊息，小於k個參與者則無法獲得任何機密訊息。Ateniese et al. (1996b)將(k, n)-threshold的使用結構加以擴充爲(Γ_{Qual}, Γ_{Forb})的形式。任何一個合格的集合(qualified set) $Y \in \Gamma_{Qual}$都可以還原機密影像，而任何一個禁止的集合(forbidden set) $X \in \Gamma_{Forb}$都無法獲得一絲機密訊息。就分享影像的形式而言，分享影像可以是雜亂無章的影像，也可以是具有意義的影像(Ateniese et al. 2001; Naor and Shamir 1995)。雜亂無章的分享影像雖然可以確保安全性，但是卻容易遭受懷疑、竊取與破壞；因此，分享影像本身爲有意義的影像的秘密分享方式，有其實際的應用價值。就機密影像數目來看，視覺式秘密分享方法可以區分爲單機密影像與多機密影像兩類。多機密影像的方法允許參與機密分享的n個人中，不同人的組合可以分享不同的機密訊息(Droste 1996; Iwamoto and Yamamoto 2003)。就技術面來看，視覺式秘密分享方法可以區分爲像素擴展(pixel-expansion)與像素不擴展(non-pixel-expansion)兩類。大部分的視覺密碼方法都使用像素擴展的技巧來達成機密影像的分享(Ateniese et al. 1996a, 1996b, 2001; Blundo and De Santis 1998; Blundo et al. 1999; Blundo et al. 2001; Droste 1996; Eisen and Stinson 2002; Hou 2003; Hofmeister et al. 2000; Naor and Shamir 1995; Tzeng and Hu 2002; Verheul and van Tilborg 1997)，只有少數的方法可以不需要像素擴展(Hou and Hsu 2004; Hou et al. 2001; Ito et al. 1999)。像素擴展的方法將機密影像上的一個點，分解成具有m個點的子像素群，所以分享影像會被擴展成機密影像的m倍。像素擴展的方法不但使影像產生變形，同使也會產生不易攜帶與消耗更多儲存空間的問題。而爲了要解決影像變形的問題，就必須將影像再擴展以維持長與寬的比例，因此就更不易攜帶也更耗費儲存空間了。爲了解決影像擴張的問題，Ito et al. (1999)利用隨機的觀念來達成影像不擴展的效果。他們的方法以對應於白點與黑點的兩個$n \times m$基礎矩陣M_0與M_1爲基礎，每次要加密一個白點(黑點)時，便隨機由M_0 (M_1)中挑選一欄向量，然後將欄向量中第i列的值(顏色)填入第i個分享影像中。這個方法的對比與安全性完全與基礎矩陣的對比與安全性相同，

因此要有好的對比就必須仰賴良好的基礎矩陣的設計。就色彩模型的角度來看，視覺式秘密分享方法可以區分爲黑白、灰階與彩色三類。大部分的研究都是關於黑白影像的(Ateniese et al. 1996a, 1996b, 2001; Blundo and De Santis 1998; Blundo et al. 1999; Blundo et al. 2001; Droste 1996; Eisen and Stinson 2002; Hofmeister et al. 2000; Hou and Hsu 2003; Ito et al. 1999; Naor and Shamir 1995; Tzeng and Hu 2002)，只有少數的研究是關於灰階與彩色影像的(Hou 2003; Hou et al. 2001; Koga and Yamamoto 1998; Lin and Tsai 2003; Verheul and van Tilborg 1997)。Verheul與van Tilborg (1997)針對灰階影像，提出一套(k, n)-threshold的視覺式秘密分享方法，他們使用像素擴展的技巧，爲每一個灰階值j = 0, 1, …, g − 1 建構一個相對應的$n \times m$的基礎矩陣A_j；每次要加密一個點時，就將對應於這個點的灰階值j的基礎矩陣A_j，做欄向量的隨機重排，然後將A_j的第i列分配給第i個分享影像。這個方法雖然可以處理灰階影像，但是因爲分享影像會被嚴重擴展，因而大大地降低了它的實用性。Hou et al. (2001)的方法則是結合半色調的觀念與對比調整的技巧，使得(2, 2)-threshold的灰階與彩色視覺密碼方法變得可行，不過它的缺點是無法處理(2, 2)-threshold以外的任何結構的問題。

在本研究中，我們將以機率的觀念來建構單一機密影像的視覺密碼模型，並且以Hou 與 Hsu (2004)的方法來求解基率矩陣。我們同時考量對比損失(loss of contrast)的問題(Naor and Shamir 1995)，爲了解決對比損失的問題，我們提出了一個對比補償的方法來改善重疊影像的視覺效果。針對灰階的機密影像，我們的方法不但能保有像素不擴展的優點，同時還能使用在單一機密影像的任何使用結構上。利用我們的方法所產生的分享影像都具有絕對的安全性；同時，在重疊影像上，我們也可以輕易地透過眼睛清楚辨識灰階機密影像中的秘密訊息。我們的方法不但具有視覺密碼直接以人眼解密的優點；同時，藉由機率的觀念與半色調技術的結合，本研究使得任意使用結構之像素不擴展的灰階視覺密碼變得可行。

貳、不擴展的視覺密碼模型

一、名詞與符號

在介紹無須像素擴展的視覺密碼方法之前，我們首先說明何謂使用結構，並定義一些符號，以方便後續的說明。令P = {1, 2, …, n}爲參與者(participants)的集合。令 2^P代表P的冪集(power set)，也就是P的全體子集合的集合。$\boldsymbol{\Gamma} = (P, F, Q)$稱爲一個使用結構(access structure) (Tzeng and Hu 2002)，它定義了機密訊息的分享規則，其中F, Q是 2^P的子集合，分別代表禁止集合(forbidden sets)與合格集合(qualified sets)的集合，而且$Q \cap F = \varnothing$。令每一個$X \in F$爲一個禁止的參與者集合，每一個$Y \in Q$爲一個合格的參與者集合。如果$Q = 2^P - F$則(P, F, Q)稱爲完整的(complete)。如果$X \in F$隱含著所有的$X' \subseteq X$都滿足$X' \in F$，則

F是單調遞減(monotonically decreasing)；如果$Y \in Q$隱含著所有的$Y' \supseteq Y$都能使$Y' \in Q$成立，則Q是單調遞增(monotonically increasing)。如果F是單調遞減且Q是單調遞增，則Γ是單調的(monotonic)。對於一個任意的使用結構而言，F不必然爲單調遞減，Q也不必然爲單調遞增。在本文中，我們規定Γ是單調的，但不必是完整的。

在本研究中，我們以 0 代表影像中的白點，1 代表影像中的黑點。假設X爲一個集合，我們以$|X|$代表X中元素的個數。我們以符號"∨"代表邏輯運算子"OR"。假設E爲一個矩陣，符號E_i代表E的第i個列向量。假設SH_1, SH_2, …, SH_n皆代表分享影像，則$(SH_1 + SH_2 + \ldots + SH_n)$表示將$SH_1$, SH_2, …, SH_n疊合後的重疊影像。

二、模型概念

以半色調影像技術的觀點而言，在一個影像區域中，如果均勻分佈的黑點密度愈高，則這一個影像區域看起來就會愈黑；反之，如果均勻分佈的黑點密度愈低，則這一個影像區域看起來就會愈白。因此，透過控制黑點分佈的密度，就可以創造出不同程度的灰階值(我們以 0 代表全白，1 代表全黑)。舉例而言，如果我們在一個 10×10 的白色影像區塊中，隨機挑選 70 個點塗成黑色，則這一個影像區塊看起來就會像是具有 70%的黑(相對於全黑)。換個角度來看，如果在這個區塊中的每一個點都有 70%的機會被塗成黑色，則這一個影像區塊看起來也會像是具有 70%的黑。因此在一個影像區域中，如果每一個點都具有相同的黑點出現機率，則這個機率值就可以做爲這個影像區域的灰階值的代表。如果我們以一個黑點密度爲 80%的影像區塊B'來取代具有相同大小的黑色影像區塊B，另外再以一個黑點密度爲 50%的影像區塊W'來取代具有相同大小的白色影像區塊W。雖然B'看起來沒有B來得黑，而W'看起來也沒有W來得白，不過我們還是可以區別B'和W'之間的差異。視覺密碼的特色在於利用人眼來進行解密，只要眼睛能辨別黑與白的差異，就能還原機密訊息。因此，我們可以利用控制影像區塊中黑點出現機率的概念，使得不作像素擴展的視覺密碼技術變得可行。

表 1 (2, 2)-threshold 的加密規則

機密影像上的像素顏色	分享影像 SH_1	分享影像 SH_2	重疊影像 (SH_1+SH_2)
□	□	□	□
	□	■	■
	■	□	■
	■	■	■
■	□	□	□
	□	■	■
	■	□	■
	■	■	■

在不作像素擴展之黑白視覺密碼中，機密影像上的每一個點經過加密後，在每一張分享影像上都只能產生一個相對應的黑點或白點。因此，針對n個參與者，機密影像上的每一個點，在n張分享影像上就有 2^n種可能的加密方式。以(2, 2)-threshold使用結構(P = {1, 2}, F = {{1}, {2}}, Q = {{1, 2}})爲例，機密影像上每一個白點或黑點加密後，分享影像 1 與分享影像 2 上相對應的點共有“白白”、“白黑”、“黑白”與“黑黑”四種可能的情況；而這四種情況重疊的結果分別爲“白”、“黑”、“黑”與“黑”，如表 1 所示。在本文中，我們將稱每一種可能的加密方式爲“加密規則”(encryption rule)。在確保安全性與提高對比的前提之下，如何決定這些加密規則被使用的機率是一個值得探討的關鍵問題。以安全性的觀點而言，因爲禁止集合$X \in F$中的所有分享影像的某個相對應的點上，其所有可能的顏色排列方式可以表示成$\{0, 1\}^{|X|}$，如果將機密影像上的白點與黑點加密後，在這$|X|$張分享影像上出現顏色排列$U_X \in \{0, 1\}^{|X|}$的機率皆相等，那麼禁止集合X中的分享影像就不可能洩漏任何秘密影像中的訊息，因而安全性可以得到確保。以對比的觀點而言，在合格集合$Y \in Q$所構成的重疊影像上，如果代表機密影像中白點的區域與代表機密影像中黑點的區域，兩者黑點出現機率差異夠大，我們就可以透過眼睛分辨白色與黑色的差異，進而還原機密影像。

三、(2, 2)-threshold 的最佳化模型

在本節中，我們將介紹(2, 2)-threshold的最佳化模型，它的使用結構可以寫成Γ = (P, F, Q)，其中P = {1, 2}，F = {{1}, {2}}，且Q = {{1, 2}}。在本例中，因爲參與者的個數爲n = 2，且影像中的每個點只有白與黑兩種顏色，所以共有 2^2 = 4 種加密規則。因此，密圖上的白點與黑點都分別有(0, 0)、(0, 1)、(1, 0)與(1, 1)等四種加密規則。令($e_{j,1}$, $e_{j,2}$)代表在分享影像 1 (SH_1)與分享影像 2 (SH_2)上的第j個加密規則，其中j = 1, 2, 3, 4。令$p_0(U_X)$與$p_1(U_X)$分別代表白點與黑點加密後，在對應於禁止

表 2 (2, 2)-threshold 最佳化模型之分析表格

Pixel	e_{jn}		c_{ij}	$p_i(U_X)$		$q_i(Y)$
				$X = \{1\}$	$X = \{2\}$	$Y = \{1, 2\}$
0	$e_{1,1} = 0$	$e_{1,2} = 0$	$c_{0,1}$	$p_0(0) = c_{0,1} + c_{0,2}$ $p_0(1) = c_{0,3} + c_{0,4}$	$p_0(0) = c_{0,1} + c_{0,3}$ $p_0(1) = c_{0,2} + c_{0,4}$	$q_0(\{1, 2\}) = c_{0,2} + c_{0,3} + c_{0,4}$
	$e_{2,1} = 0$	$e_{2,2} = 1$	$c_{0,2}$			
	$e_{3,1} = 1$	$e_{3,2} = 0$	$c_{0,3}$			
	$e_{4,1} = 1$	$e_{4,2} = 1$	$c_{0,4}$			
1	$e_{1,1} = 0$	$e_{1,2} = 0$	$c_{1,1}$	$P_1(0) = c_{1,1} + c_{1,2}$ $P_1(1) = c_{1,3} + c_{1,4}$	$P_1(0) = c_{1,1} + c_{1,3}$ $P_1(1) = c_{1,2} + c_{1,4}$	$q_1(\{1, 2\}) = c_{1,2} + c_{1,3} + c_{1,4}$
	$e_{2,1} = 0$	$e_{2,2} = 1$	$c_{1,2}$			
	$e_{3,1} = 1$	$e_{3,2} = 0$	$c_{1,3}$			
	$e_{4,1} = 1$	$e_{4,2} = 1$	$c_{1,4}$			
				Security: $c_{0,1} + c_{0,2} = c_{1,1} + c_{1,2}$ $c_{0,3} + c_{0,4} = c_{1,3} + c_{1,4}$	Security $c_{0,1} + c_{0,3} = c_{1,1} + c_{1,3}$ $c_{0,2} + c_{0,4} = c_{1,2} + c_{1,4}$	Contrast: $\alpha = q_1(\{1, 2\}) - q_0(\{1, 2\})$

集合$X \in F$的所有分享影像上出現顏色排列$U_X \in \{0, 1\}^{|X|}$的機率。令$q_0(Y)$與$q_1(Y)$分別代表白點與黑點經過加密後，在合格集合$Y \in Q$的重疊影像上出現黑點的機率。有關$p_0(U_X)$、$p_1(U_X)$、$q_0(Y)$與$q_1(Y)$的計算如表 2 所示。

就“安全性”的角度而言，爲了確保禁止集合X的安全性，密圖上的白點與黑點經過加密後，必須滿足$p_0(U_X) = p_1(U_X)$的條件。因此，爲了確保SH_1的安全性必須滿足$c_{0,1} + c_{0,2} = c_{1,1} + c_{1,2}$與$c_{0,3} + c_{0,4} = c_{1,3} + c_{1,4}$的條件；同樣地，爲了確保$SH_2$的安全性必須滿足$c_{0,1} + c_{0,3} = c_{1,1} + c_{1,3}$與$c_{0,2} + c_{0,4} = c_{1,2} + c_{1,4}$的條件。如果它們不相等，則在$SH_1$與$SH_2$上就可能會透露出機密影像的訊息，如此安全性便無法得到確保。由於$c_{0,1} + c_{0,2} + c_{0,3} + c_{0,4} = 1$ 且$c_{1,1} + c_{1,2} + c_{1,3} + c_{1,4} = 1$，因此我們只需要考慮$c_{0,3} + c_{0,4} = c_{1,3} + c_{1,4}$與$c_{0,2} + c_{0,4} = c_{1,2} + c_{1,4}$這兩個條件便足以保證安全性。就“對比”的角度而言，密圖上的白點與黑點經過加密後，在重疊影像(SH_1+SH_2)上，兩者出現黑點的機率$q_1(\{1, 2\})$與$q_0(\{1, 2\})$的差異必須夠大，才能透過人眼辨識機密訊息。因此我們以$\alpha = q_1(\{1, 2\}) - q_0(\{1, 2\}) = (c_{1,2} + c_{1,3} + c_{1,4}) - (c_{0,2} + c_{0,3} + c_{0,4})$來代表重疊影像的對比。我們的目標是在滿足安全性的限制條件之下，求解白點與黑點的各個可能的加密規則的使用機率，使對比能達到最佳化。根據以上之分析，(2, 2)-threshold的最佳化模型可表示成第(1)式的線性規劃模型。

$$\left.\begin{array}{ll} \max. & \alpha = (c_{1,2} + c_{1,3} + c_{1,4}) - (c_{0,2} + c_{0,3} + c_{0,4}). \\ \text{s.t.} & (c_{0,3} + c_{0,4}) - (c_{1,3} + c_{1,4}) = 0; \\ & (c_{0,2} + c_{0,4}) - (c_{1,2} + c_{1,4}) = 0; \\ & \sum_{j=1}^{4} c_{i,j} = 1, \text{for } i = 0, 1; \\ & 0 \le c_{i,j} \le 1, \text{for all } i, j. \end{array}\right\} \quad (1)$$

我們以線性規劃的方法可以很容易求得(2,

2)-threshold 加密規則機率值的最佳解爲

$$\begin{bmatrix} c_{0,1} & c_{0,2} & c_{0,3} & c_{0,4} \\ c_{1,1} & c_{1,2} & c_{1,3} & c_{1,4} \end{bmatrix} = \begin{bmatrix} 0.5 & 0.0 & 0.0 & 0.5 \\ 0.0 & 0.5 & 0.5 & 0.0 \end{bmatrix}, \quad (2)$$

其重疊影像的對比爲$\alpha = 0.5$。接下來，我們將以(2, 2)-threshold 的模型爲基礎，探討如何建構任意使用結構的模型。

四、加密規則矩陣與機率矩陣

令$E = [e_{j,k}]$爲一個 $2^n \times n$的矩陣，其中$e_{j,k} \in \{0, 1\}$。我們稱E爲加密規則矩陣，用來表達在參與者集合P之下的所有可能的加密規則。加密規則矩陣E中的每一個列向量$E_j = [e_{j,1}, e_{j,2}, \ldots, e_{j,n}]$代表一個加密規則。例如，當$n = 3$ 時，$E_j = [1, 0, 0]$表示第j的加密規則爲在第一、第二與第三個分享影像上分別產生黑點、白點與白點。令$C = [c_{i,j}]$爲一個 2×2^n的矩陣，其中$c_{i,j} \in [0, 1]$，$i \in \{0, 1\}$，$j \in \{1, 2, \ldots, 2^n\}$且

$$\sum_{j=1}^{2^n} c_{i,j} = 1 \text{。} \quad (3)$$

我們稱C爲機率矩陣，$c_{0,j}$與$c_{1,j}$分別代表使用第j個加密規則E_j來加密白點與黑點機率值。以表 2 的(2, 2)-threshold爲例，其加密規則矩陣與機率矩陣可以表示成：

$$E = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad (4)$$

$$C = \begin{bmatrix} c_{0,1} & c_{0,2} & c_{0,3} & c_{0,4} \\ c_{1,1} & c_{1,2} & c_{1,3} & c_{1,4} \end{bmatrix} \text{。} \quad (5)$$

在這個機率矩陣C中，$c_{0,1}$代表使用第一個加密規則[0, 0]來加密一個白點的機率；而$c_{1,2}$則代表使用第二個加密規則[0, 1]來加密一個黑點的機率。

五、安全性

令$p_0(U_X)$與$p_1(U_X)$分別代表白點與黑點加密後，在對應於禁止集合$X = \{l_1, l_2, \ldots, l_r\} \in F$的所有分享影像上出現顏色排列$U_X \in \{0, 1\}^{|X|}$的機率。就“安全性”的角度而言，爲了確保禁止集合$X$的安全性，密圖上的白點與黑點經過加密後，對於所有的$X \in F$，$U_X \in \{0, 1\}^{|X|}$必須滿足$p_0(U_X) = p_1(U_X)$的條件。當$p_0(U_X) = p_1(U_X)$時，代表無法由禁止集合X中的分享影像來反推機密影像中的訊息。反之，如果$p_0(U_X) \neq p_1(U_X)$，則頻率上的變化就可能會透露出機密影像的訊息，如此安全性便無法得到確保。以(k, n)-threshold爲例說明，在$k = 3$的情況下，任意兩張分享影像SH_i與SH_j上的相對應的點的顏色排列的有(0, 0)、(0, 1)、(1, 0)與(1, 1)等四種可能的情況。爲了確保SH_i與SH_j不會洩漏任何關於機密影像的訊息，我們必須保證在SH_i與SH_j的任何區域中，出現(0, 0)、(0, 1)、(1, 0)與(1, 1)的機率分佈必須要相同。假設白點加密後，在SH_i與SH_j上出現(0, 0)、(0, 1)、(1, 0)與(1, 1)的機率分佈爲$\boldsymbol{x} = (x_1, x_2, x_3, x_4)$，且黑點加密後的機率分佈爲$\boldsymbol{y} = (y_1,$

y_2, y_3, y_4)，如果$\boldsymbol{x} = \boldsymbol{y}$則可確保$SH_i$與$SH_j$的安全性。關於$p_0(U_X)$與$p_1(U_X)$的計算方式，我們以下列式子表示：

$$p_i(U_X) = \sum_{j=1}^{2^n} c_{i,j} \cdot g(U_X, V_j) \ , \qquad (6)$$

其中$i \in \{0, 1\}$，$V_j = (e_{j,l_1}, e_{j,l_2}, \ldots, e_{j,l_r})$且

$$g(U_X, V_j) = \begin{cases} 1 & \text{if } U_X = V_j \\ 0 & \text{else} \end{cases} 。 \qquad (7)$$

六、對比

令$q_0(Y)$與$q_1(Y)$分別表示白點與黑點經過加密後，在對應於合格集合$Y = \{ l_1, l_2, \ldots, l_r\} \in Q$的重疊影像上出現黑點的機率，其計算方式如下：

$$q_i(Y) = \sum_{j=1}^{2^n} c_{i,j} \cdot (e_{j,l_1} \vee e_{j,l_2} \vee \ldots \vee e_{j,l_r}) \ , \qquad (8)$$

其中 $i \in \{0, 1\}$。我們定義對應於合格集合 Y 的重疊影像的對比爲

$$\alpha_Y = q_1(Y) - q_0(Y)。 \qquad (9)$$

對比指標α_Y的絕對值愈大，代表由合格集合Y所構成的重疊影像的對比愈大，表示愈容易看清楚機密影像的內容；反之，如果對比指標α_Y的絕對值愈小，則代表由合格集合Y所構成的重疊影像的對比愈小，表示愈不容易看清楚機密影像的內容。當對比指標α_Y爲負值時，表示影像呈現反白(inverse)的結果。如果考慮反白的情況(Tzeng and Hu 2002)，則對比指標可以修改爲

$$\alpha_Y = |q_1(Y) - q_0(Y)|。 \qquad (10)$$

在本研究中，我們使用第(9)式的定義，也就是不考慮反白的情況。因爲對比愈大人眼愈容易辨識機密訊息，因此我們的目標是求對比極大化。

七、任意結構的模型

我們以$\boldsymbol{\Gamma} = (P, F, Q)$的形式表示單一機密影像的任意使用結構。對於任何一個使用結構而言，我們希望在滿足安全性的限制條件之下，求解一個機率矩陣，使得對比達到極大化。$\boldsymbol{\Gamma} = (P, F, Q)$形式的模型如第(11)式所示。在第(11)式中，因爲白點與黑點都各有2^n種加密規則，而一種加密規則需要一個相對應的機率值，因此總共有 2^{n+1}個變數需要求解。每一個變數都是介於 0 到 1 之間的實數，且白點與黑點的所有加密規則的使用機率之總合必須分別爲 1。在安全性方面，因爲每一個禁止集合$X \in F$的安全性都必須被確保，而且每個禁止集合X都有 $2^{|X|}$個限制條件，因此總共有$\Sigma_{X \in F} 2^{|X|}$個關於安全性的限制條件。在對比方面，因爲每一個合格集合$Y \in Q$所構成的重疊影像的對比都必須做最佳化，因此總共有$|Q|$個最佳化的目標。這個模型可以適用在單一機密影像的任何使用結構上，前述之第(1)式式爲本模型之特例。

$$\left.\begin{array}{ll}\max & \alpha_Y = q_1(Y) - q_0(Y), \text{for all } Y \in Q. \\ \text{s.t.} & p_0(U_X) = p_1(U_X), \text{for all } X \in F, U_X \in \{0,1\}^{|X|}; \\ & \sum_{j=1}^{2^n} c_{i,j} = 1, \text{for } i = 0, 1; \\ & c_{i,j} \in [0,1], \text{for all } i, j.\end{array}\right\} \quad (11)$$

第(11)式是一個多目標最佳化模型(multi-objective optimization model)，其中所有的目標函數與限制函數皆爲線性函數，因此這是一個典型的多目標線性規劃模型(multi-objective linear programming model)。

八、實驗與討論

Droste (1996)曾經針對多機密影像的視覺密碼問題提出一個演算法，稱爲*S*-Extended *n* out of *n* Schemes，這個演算法利用*n* out of *n*的方法來建構每一個合格集合的基礎矩陣，最後再將所有的矩陣結合成最終的基礎矩陣。由於*n* out of *n* 的問題必定能找到一個對比爲 $1/2^{n-1}$的基礎矩陣(Naor and Shamir 1995)，且Droste的方法也適用於單一機密影像，因此對於任何一個使用結構，必定能找到一個視覺密碼的解。此外，由於我們的機率矩陣與基礎矩陣可以相互轉換，因此我們的模型也必定有解。

在本模型中，變數個數有 2^{n+1}個，它將隨著參與者個數*n*的增加而成指數型的成長，因此使得問題的複雜度隨之增加。當*n*的值很大的時候，大部分的線性規劃方法的效率都普遍不佳，因此Hou & Hsu (2004)針對此類最佳化問題，曾經提出一個以遺傳演算法爲基礎的解題方法，在考慮解題效率的前提下可以得到不錯的結果。考慮P = {1, 2, 3, 4}，Q = {{1, 4}, {3, 4}, {1, 2, 3}, {1, 2, 4}, {1, 3, 4}, {2, 3, 4}, {1, 2, 3, 4}}且$F = 2^P - Q$的問題，假設加密規則矩陣E爲

$$E = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}^T,$$

我們利用 Hou & Hsu 的方法求解的機率矩陣C爲

$$C = \begin{bmatrix} 0.3 & 0.0 & 0.0 & 0.0 & 0.1 & 0.0 & 0.0 & 0.1 & 0.0 & 0.0 & 0.0 & 0.4 & 0.0 & 0.1 & 0.0 & 0.0 \\ 0.0 & 0.2 & 0.0 & 0.1 & 0.0 & 0.2 & 0.0 & 0.0 & 0.0 & 0.1 & 0.3 & 0.0 & 0.0 & 0.0 & 0.1 & 0.0 \end{bmatrix},$$

其對比爲$\alpha_{\{1,4\}} = 0.4$、$\alpha_{\{3,4\}} = 0.4$、$\alpha_{\{1,2,3\}} = 0.1$、$\alpha_{\{1,2,4\}} = 0.3$、$\alpha_{\{1,3,4\}} = 0.4$、$\alpha_{\{2,3,4\}} = 0.3$與$\alpha_{\{1,2,3,4\}} = 0.3$，且合格集合{1, 4}、{3, 4}、{1, 2, 4}、{1, 3, 4}、{2, 3, 4}與{1, 2, 3, 4}的黑點重建結果皆爲 100%的黑(如圖 1 所示)。比較Ateniese et al. (1996b)的結果，其對比爲$\alpha_{\{1,4\}} = 0.2$、$\alpha_{\{3,4\}} = 0.2$、$\alpha_{\{1,2,3\}} = 0.2$、$\alpha_{\{1,2,4\}} = 0.2$、$\alpha_{\{1,3,4\}} = 0.2$、$\alpha_{\{2,3,4\}} = 0.2$與$\alpha_{\{1,2,3,4\}} = 0.4$，且只有一個合格集合{1, 2, 3, 4}的黑點重建結果爲 100%的黑。在這個例子上，我們的機率矩陣的平均對比要比Ateniese et al.的平均對比高出 37.5%，而且有更佳的黑點重建效果。另外，我們利用機率矩陣加密不會產生影像擴張的問題，也就是分享影像與機密影像有完全相同的影像尺吋；然而，Ateniese et al.的方法在這個使用結構上必須將影像擴展 5 倍，如果要維持影像的長寬比

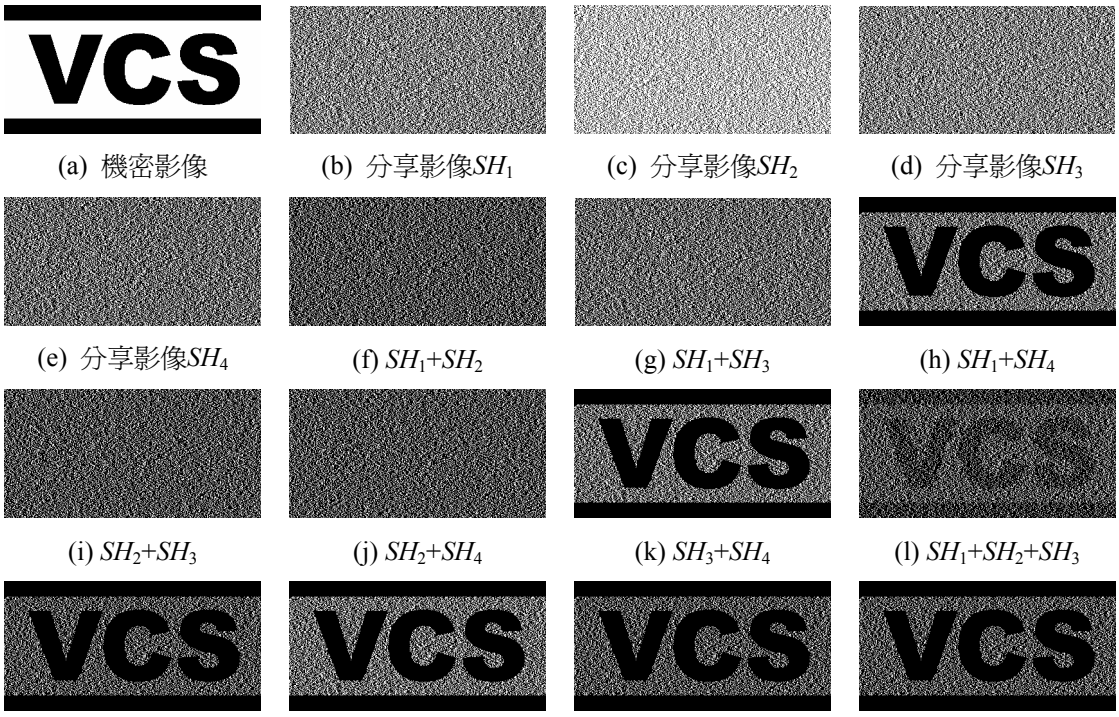


圖 1 任意結構的實驗結果(400×200 pixels, 300 dpi)

例，必須要擴展高達 25 倍，因此其實用性將大打折扣。利用機率矩陣加密的方法也很簡單，如果要加密一個白點(黑點)，就根據機率矩陣C的第一列(第二列)的機率值隨機決定一個加密規則，然後將加密規則的n個值(顏色)填入相對應的n張分享影像中，其加密複雜度與傳統視覺密碼方法相同。解密時，只需要將分享影像重疊在一起就可以透過眼睛來看到機密訊息，完全不需要使用到電腦與複雜的解密演算法。就安全性而言，我們的模型保證未被授權的影像絕對不會含有任何可以反推機密影像的訊息，因爲在未被授權的幾張分享影像的相對應的位置上，任何一種顏色的排列方式其來自機密影像上的白點與黑點的機率完全相同，因此由未被授權的分享影像要完全到算回機密影像的機率只有 $1/2^{xxy}$，其中x與y分別爲影像的寬與高。以圖 1 中的影像爲例，因爲其影像大小爲 400×200 pixels，所以要由未被授權的若干張分享影像(例如SH_1與SH_2)倒算回原來的機密影像(圖 1(a))的機率只有 $1/2^{80000}$。

參、不擴展的灰階視覺密碼方法

一、半色調技術

半色調技術(halftoning)是一種將連續調

(a) 連續調影像　　(b) 半色調影像

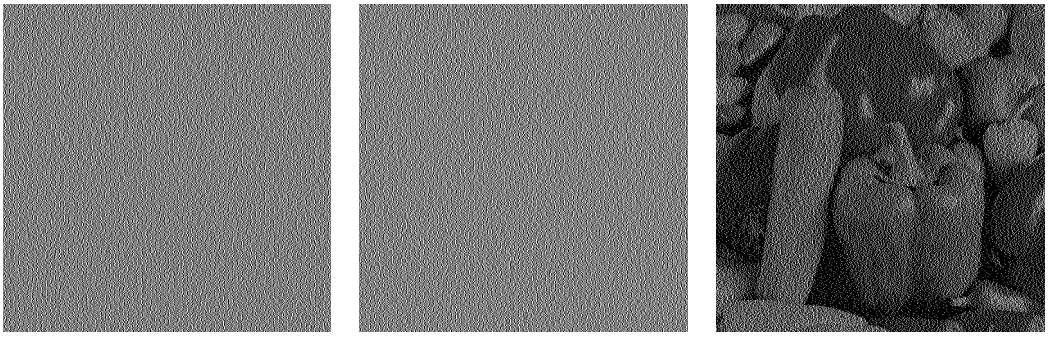
圖 2　連續調影像與半色調影像 (512×512 pixels, 300 dpi)

影像(continuous-tone image)轉換成二元影像(bi-level image)的一種影像處理技術。它的工作原理主要是透過網點的疏密來表現色階的程度。由於人類視覺系統對高頻具有不敏銳性，因此，一塊均勻的網點會被眼睛解釋爲某一灰階值的區域。如果網點愈密，則影像會顯得愈黑(暗)；反之，如果網點愈疏，則影像就顯得愈白(亮)。基於視覺系統的這個特性，我們只需要使用兩種顏色，就可以模擬一個連續的色階。透過半色調轉換，一張連續調的影像可以被轉換成一張二元影像。以灰階影像爲例，一張灰階影像(圖 2(a))經過半色調轉換後，其結果爲一張僅具有黑點與白點的半色調影像(圖 2(b))。雖然圖 2(b)爲一張半色調影像，但是我們還是可以感覺到色階的變化，就好像是灰階影像一般；因此，透過半色調技術，我們只要利用黑點與白點，就可以模擬出灰階影像的效果。半色調技術已經被廣泛應用於列印設備，目前已有許多半色調技術相繼被提出，例如 ordered dither、error diffusion、blue noise masks、green noise halftoning、direct binary search、dot diffusion 等(Mese and Vaidyanathan 2002)。

大部分的視覺密碼技術都是以黑白影像爲基礎的，如果我們能以利用半色調技術，將灰階影像轉換爲半色調影像來模擬灰階的色階，那麼以黑白影像爲基礎的視覺密碼方法便可以直接應用在半色調影像上。以圖 2(b)的半色調影像爲例，我們利用第(2)式的機率矩陣C將半色調影像加密後，可以製作出如圖 3 的分享影像與重疊影像。觀察圖 3(c)的結果可以發現，重疊影像(SH_1+SH_2)仍然保留相當程度的色階變化，就人眼的感受而言，它仍然保有圖 2(a)之灰階影像的大部分特徵。由此結果可以證明，利用半色調技術來建構灰階視覺密碼方法是可行的。

二、對比損失的補償方法

所有的視覺密碼技術都有一個的共同的特色，那就是重疊影像的對比會比原始機密影像的對比來得低。假設原機密影像的對比爲α，而重疊影像的對比爲α'，則$|\alpha - \alpha'|/\alpha$就稱之爲對比損失。例如，(2, 2)-threshold之最佳對比爲$\alpha^* = 1/2$，因此其對比損失爲 50%(比較圖 2(b)與圖 3(c)即可看出其差異)；而(2, 3)-threshold之最佳對比爲$\alpha^* = 1/3$ (Blundo et al. 1999)，因此其對比損失爲 67%。對比損失的程度影響了人類視覺系統在解密時，對於機密訊息辨認的精確度。較低的對比損失將使得重建後的影像較容易被人眼辨識；相反地，較高的對比損失則較不利於人眼的辨識。對於黑白機密影像而言，因爲原來黑與白之間的對比爲 100%，因此能夠容忍較高的對比損失。也就是說，雖然重建後的影像對比被降低了，我們依然能夠透過人眼辨識機密訊息。然而，對於灰階機密影像而言，影像本身的灰階度的動態範圍(dynamic range)可能很寬廣，也可能很狹窄。在灰階影像本身就具有較狹窄的動態範圍的情況之下，將灰階影像轉換成半色調影像後，它對於對比損失的容忍程度就會變得比較差；也就是說，狹窄的動態範圍加上對比損失之後，秘密訊息將變得模糊不清而難以被人眼辨識。因此，爲了解決對比損失的問題，我們將大



(a) 分享影像 SH_1　(b) 分享影像 SH_2　(c) SH_1+SH_2

圖 3　利用半色調技術與機率矩陣所產生的視覺密碼影像(512×512 pixels, 300dpi)

小爲$x\times y$的半色調影像劃分爲$(x\times y)/(t\times t)$個$t\times t$的區塊，我們每次以一個區塊爲單位來加密，如果區塊內的黑點個數$b < t^2/2$的話，那我們就將區塊內的每一個點都當作白點來加密；如果$b > t^2/2$的話，那我們就將區塊內的每一個點都當作黑點來加密；如果$b = t^2/2$的話，那我們就根據區塊內的每一個點的顏色來加密。這個加密的流程可以表示如下：

a) 將大小爲 $x\times y$ 的半色調影像 HI 劃分爲 $(x\times y)/(t\times t)$個 $t\times t$ 的區塊。

b) 由 HI 中依序取出一個尚未加密的 $t\times t$ 區塊 B，並計算其黑點個數 b。

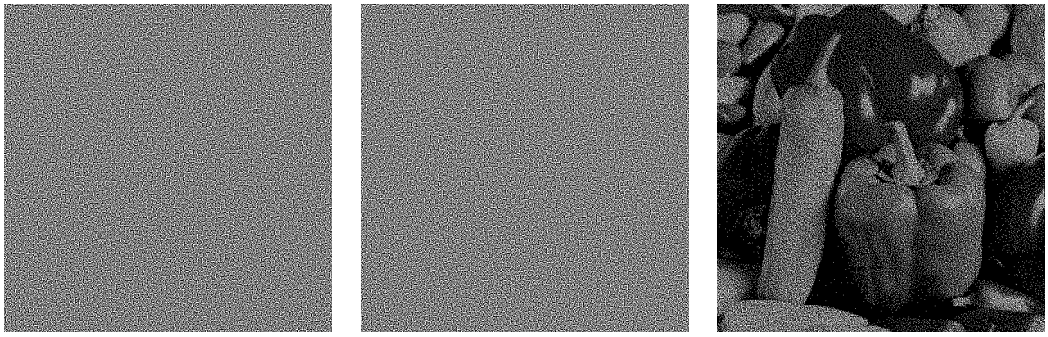
c) 根據下列規則將 B 中的每一個點加密：

```
if   b < t^2/2   then
        將 B 中的每一個點都當作白點，並根據機率矩陣 C 來加密每一個點
else if   b > t^2/2   then
        將 B 中的每一個點都當作黑點，並根據機率矩陣 C 來加密每一個點
    else
        根據 B 中的每一個點的顏色，以機率矩陣 C 來加密
```

d) 重覆步驟(b)-(c)直到機密影像上的所有區塊皆加密完畢。

在這個方法的作用之下，半色調影像中比較白的區域會被當作全白色來處理，比較黑的區域會被當作全黑色來處理，因此拉大了黑白之間的距離，這個效果正好可以用來彌補對比損失，進而改進重疊影像的視覺效果。

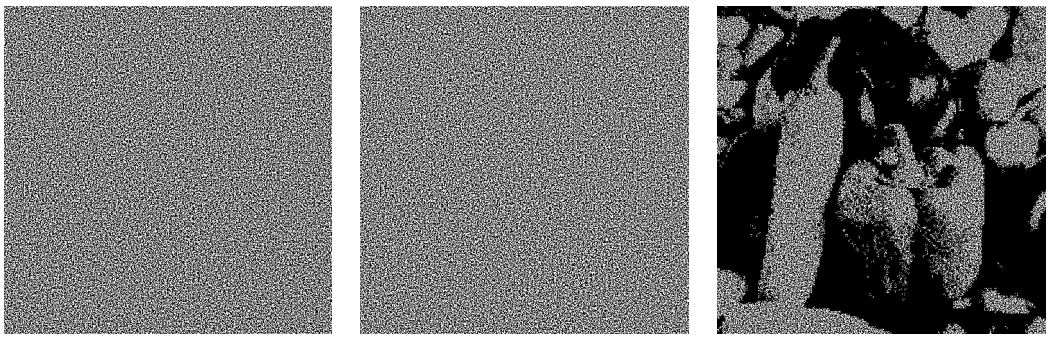
三、實驗與討論



(a) 分享影像 SH_1　　(b) 分享影像 SH_2　　(c) SH_1+SH_2

圖 4　2×2 區塊的實驗結果(512×512 pixels, 300dpi)

我們將圖 2(b)中大小爲 512×512 pixels 的半色調影像，劃分成 65536 個 2×2 的區塊，針對每一個 2×2 的區塊都利用前述的區塊加密準則，以第(2)式的機率矩陣 C 來加密，所得到的結果如圖 4 所示。另外，我們也將半色調影像，劃分成 16384 個 4×4 的區塊，針對每一個 4×4 的區塊，我們同樣利用區塊加密準則，以第(2)式的機率矩陣 C 來加密，所得到的結果如圖 5 所示。圖 3(c)爲不作區塊對比補償的原始結果，而圖 4(c)與圖 5(c)爲進行區塊對比改善後的結果，比較圖 3(c)、圖 4(c)與圖 5(c)可以發現，有進行區塊對比改善的重疊影像會產生比較強烈的對比，這個對比的改善可以彌補一部分加密時所損失的對比。就視覺效果而言，區塊大小爲 2×2 的效果看起來比較接近原圖，但是又有對比改善的效果，而區塊大小爲 4×4 的效果看起雖然有比較強烈的對比，但與原圖相比其失真的程度就比較大一些。根據我們的觀察，區塊愈大則對比愈強烈且失真度也愈大；相



(a) 分享影像 SH_1　　(b) 分享影像 SH_2　　(c) SH_1+SH_2

圖 5　4×4 區塊的實驗結果(512×512 pixels, 300dpi)

反地，區塊愈小則對比改善的效果也愈有限，不過與原圖相比的失真度也愈小。根據我們的經驗，我們認爲 2×2 的區塊是比較恰當的。

肆、結論

在本文中，我們以機率的觀念建構了一個單一機密影像的視覺密碼模型，爲了求解效率的考量，我們以Hou & Hsu (2004)的方法來求解機率矩陣。實驗結果顯示，我們的方法有機會在對比與黑點重建品質上獲得比較好的結果。此外，利用隨機挑選加密規則的方法來加密，我們可以完全不須要擴張影像，因此可以避免像素擴展所帶來的缺點。對於灰階機密影像而言，傳統的做法是使用像素擴展的技巧，爲每一個灰階值$j = 0, 1, \ldots, g - 1$建構一個相對應的$n \times m$的基礎矩陣A_j；每次要加密一個點時，就將對應於這個點的灰階值j的基礎矩陣A_j，做欄向量的隨機重排，然後將A_j的第i列分配給第i個分享影像。這樣的做法是以m個點中所佔的黑點數目來模擬灰色的色階度，在本質上，還是以黑白的概念在處理灰階影像的問題。這個方法雖然說可以處理灰階影像，但是因爲分享影像會被嚴重擴展，因而大大地降低了它的實用性。在本文中，我們是以半色調技術將灰階影像轉換成半色調影像，然後再以機率矩陣加密，達成不擴展的灰階影像視覺密碼。雖然半色調影像本質上也是一個二元影像，不過它與純粹黑白的影像最大的差異就在於它使用網點疏密來模擬連續調的色階，因此可以表達比較複雜的連續調影像。基於半色調影像對於灰階影像有很好的模擬效果，而且又能夠直接使用黑白視覺密碼方法來加密，因此利用半色調技術來解決灰階影像的視覺密碼問題是一個很好的方法。

在本研究中，我們也探討了對比損失的問題；對比損失的影響在半色調影像中會顯得特別嚴重，尤其是在那些原本就具有狹窄色階動態範圍的灰階影像，將其轉換成半色調影像後，就更難忍受對比損失的影響了。爲了解決對比損失的問題，我們提出了一個對比補償的方法來改善重疊影像的視覺效果。我們以區塊的黑點數來決定到底要使用黑點還是白點的加密規則，其中區塊的大小會影響重疊影像的對比與失真程度，根據我們的經驗，我們建議使用 2×2 大小的區塊會得到比較好的重疊影像視覺效果。

藉由結合機率的觀念、半色調技術與對比補償的技巧，對於灰階影像而言，我們的方法可以同時達到像素不擴展、對使用結構的通用性與維持良好的影像重建品質等三個目標。我們的方法不但能夠確保絕對的安全性，同時也保有視覺密碼的優點；我們只要將分享影像重疊，就能夠很輕易地透過人眼辨識出灰階機密影像的訊息，其解密過程完全不需要使用任何計算機資源，也沒有任何複雜的解密程序。在未來，我們將延續此一研究，使這個方法能進一步應用於彩色機密影像上。

參考文獻

1. Ateniese, G., Blundo, C., De Santis, A., and Stinson, D. R. "Constructions and Bounds for Visual Cryptography," in *23rd International Colloquium on Automata, Languages and Programming (ICALP '96)*, LNCS 1099, 1996a, pp. 416-428.
2. Ateniese, G., Blundo, C., De Santis, A., and Stinson, D. R. "Visual Cryptography for General Access Structures," *Information and Computation* (129:2), 1996b, pp. 86-106.
3. Ateniese, G., Blundo, C., De Santis, A., and Stinson, D. R. "Extended Capabilities for Visual Cryptography," *Theoretical Computer Science* (250:1-2), 2001, pp. 143-161.
4. Blundo, C., De Bonis, A., and De Santis, A. "Improved Schemes for Visual Cryptography," *Designs, Codes and Cryptography* (24), 2001, pp. 255-278.
5. Blundo, C., and De Santis, A. "Visual Cryptography Schemes with Perfect Reconstruction of Black Pixels," *Computer & Graphics* (12:4), 1998, pp. 449-455.
6. Blundo, C., De Santis, A., and Stinson, D. R. "On the Contrast in Visual Cryptography Schemes," *Journal of Cryptology* (12:4), 1999, pp. 261-289.
7. Droste, S. "New Results on Visual Cryptography," in *Advances in Cryptology-CRYPTO '96*, LNCS 1109, Springer-Verlag, 1996, pp. 401-415.
8. Eisen, P. A., and Stinson, D. R. "Threshold Visual Cryptography Schemes with Specified Whiteness Levels of Reconstructed Pixels," *Designs, Codes and Cryptography* (25), 2002, pp. 15-61.
9. Gonzalez, R. C., and Woods, R. E. *Digital Image Processing*, 2nd Edition, Prentice-Hall, New Jersey, 2002.
10. Hofmeister, T., Krause, M., and Simon, H. U. "Contrast-optimal *k* out of *n* Secret Sharing Schemes in Visual Cryptography," *Theoretical Computer Science* (240), 2000, pp. 471-485.
11. Hou, Y. C. "Visual Cryptography for Color Images," *Pattern Recognition* (36), 2003, pp. 1619-1629.
12. Hou, Y. C., and Hsu, C. S. "A Probability-based Model for Visual Secret Sharing Schemes without Pixel Expansion," accepted by *Journal of Information Management*, 2004 (In Chinese).
13. Hou, Y. C., Lin, F., and Chang, C. Y. "Visual Cryptography for Color Images without Pixel Expansion," *Journal of Technology* (16:4), 2001, pp. 595-603 (In Chinese).
14. Iwamoto, M. and Yamamoto, H. "A Construction Method of Visual Secret

Sharing Schemes for Plural Secret Images," *IEICE Transactions on Fundamentals* (86-A:10), 2003, pp. 2577-2588.

15. Ito, R., Kuwakado, H., and Tanaka, H. "Image Size Invariant Visual Cryptography," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* (E82-A:10), 1999, pp. 2172-2177.
16. Koga, H., and Yamamoto, H. "Proposal of a Lattice-Based Visual Secret Sharing Scheme for Color and Gray-Scale Images," *IECE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* (E82-A:6), 1998, pp. 1262-1269.
17. Lin, C. C., and Tsai, W. H. "Visual Cryptography for Gray-level Images by Dithering Techniques," *Pattern Recognition Letters* (24), 2003, pp. 349-358.
18. Mese, M., and Vaidyanathan, P. P. "Recent Advances in Digital Halftoning and Inverse Halftoning Methods," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* (49:6), 2002, pp. 790-805.
19. Naor, M., and Shamir, A. "Visual Cryptography," in *Advances in Cryptology-EUROCRYPT '94*, LNCS 950, Springer-Verlag, 1995, pp. 1-12.
20. Tzeng, W. G., and Hu, C. M. "A New Approach for Visual Cryptography," *Designs, Codes and Cryptography* (27), 2002, pp. 207-227.
21. Verheul, E. R., and van Tilborg, H. C. A. "Constructions and Properties of *k* out of *n* Visual Secret Sharing Schemes," *Designs, Codes and Cryptography* (11), 1997, pp. 179-196.

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教授，兼學生事務處諮商輔導中心組長。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。

許慶昇

國立中央大學資訊管理研究所博士班研究生。研究領域爲資訊隱藏、浮水印技術與視覺密碼、柔性計算技術、智慧型電腦輔助教學與評量。