像素不擴展之彩色視覺密碼技術

Visual Cryptography Techniques for Color Images without Pixel Expansion

侯永昌
國立中央大學資訊管理研究所
桃園縣中壢市320五權里2鄰中大路300號
ychou@mgt.ncu.edu.tw

杜淑芬
國立中央大學資訊管理研究所
桃園縣中壢市320五權里2鄰中大路300號
arieltu@ms52.hinet.net

摘要

視覺密碼是一種依靠人眼解密的一種秘密分享方法，在無法使用電腦解密的情況下，它是一個很好的解決方案。大部分的視覺密碼方法由於像素擴展的關係，所以產生的分享影像大小會比原來的機密影像大上許多倍，尤其是應用在灰階和彩色影像上，其擴展的倍數更是驚人。本研究提出一種不需要像素擴展的灰階和彩色視覺密碼的技術；我們的方法利用多點同時加密的概念，每次取連續的m個點做為加密序列進行加密，我們的方法可以確保在m個具有b個黑點的加密序列中，一定會有b個加密序列是使用黑點基礎矩陣加密，另外的$(m-b)$個則使用白點基礎矩陣加密，因此在疊合影像上黑與白的變化很規律。因此，我們不但能達成像素不擴展的目標，而且也能確保重疊影像的視覺效果。針對彩色影像，我們應用色彩模型的原理，將影像分解成青、洋紅、黃三張不同色調的影像，將這三張單一色調的連續調影像，利用半色調技術轉換成二元影像，再利用本研究所提的多點加密法，來加密這些半色調影像。由實驗結果可以證明，在不作像素擴展的前提之下，分享影像仍然具有足夠的安全性，而且也能確保還原影像有很好的視覺效果，同時我們的方法可以很容易地延伸至任意的使用結構上。

關鍵詞: 視覺密碼、半色調技術、色彩模型。

Abstract

Visual cryptography is a visual secret sharing method which encodes a secret into several shares and decodes a secret with human eyes; therefore, it is a good solution to decrypt secrets without computers. Most visual cryptographic methods need to expand pixels and hence enlarge the size of shares. This situation is more serious for gray-level and chromatic images. In this paper, we propose a new visual cryptographic method for gray-level and chromatic images without pixel expansion. We simultaneously encrypt m successive pixels (called an "encryption sequence") each time in accordance with two basis matrices. In every m encryption sequences

with *b* blacks, we make sure that b encryption sequences are encoded by black basis matrix, and the other (*m* − *b*) ones are encoded by white basis matrix. Therefore we can not only attain the aim of not expanding the pixels, but also ensure good visual effect of the stacked image. Additionally, we utilize the color model to decompose a chromatic image into three monochromatic images in tones of cyan, magenta, and yellow, respectively. These three images are transformed into halftone images and then encrypted by the proposed method. The experimental results show that the security of shares is still maintained though pixels are not expanded, and the visual effect of the stacked images is good. With appropriate basis matrices, our method can be easily extended to general access structure.

Keywords: Visual Cryptography, Halftoning, Color Model

一、簡介

傳統密碼學主要是將機密訊息的內容，經由複雜的數學運算，將其轉換成無意義的訊息。要還原原來的機密訊息，除非有解密的金鑰，否則在有限的時間和資源下，加密過的訊息是無法被破解的，因此可以避免機密被駭客得知。但是傳統密碼學的缺點也就在於需要透過大量且複雜的數學運算，因此無論是加密或解密都需要有電腦的協助。

1994年Naor與Shamir兩位學者提出一個應用在影像資料上的新的密碼學方法，稱為視覺密碼(Visual Cryptography)[17]。它是一種依靠人眼解密的一種秘密分享方法，在無法使用電腦解密的情況下，它是一個很好的解決方案。視覺密碼技術最初被提出時，是應用在黑白機密影像的分享上，稱為(*k*, *n*)-threshold視覺式秘密分享機制(visual secret sharing scheme, VSS)，意指*n*張分享影像中至少取*k*張加以疊合，便可得出原來的機密影像。視覺密碼的加密方式，一般都是使用像素擴展的技巧 [1-7,9,10,12,14,17,19,20]，也就是說機密影像上的每個像素，在分享影像上會被擴展成*m*個像素($m \geq 2$)，因此分享影像的大小會是機密影像的*m*倍。表一為(2, 2)-threshold視覺式秘密分享機制，機密影像上的白點和黑點都各有兩列的加密規則，而且每個加密規則被選用的機率是一樣的。假設要加密的機密影像像素是白點，並且隨機選取了白點加密規則的第一列，則在分享影像1上依序填入一黑點一白點，在分享影像2上依序填入一黑點一白點，當兩張分享影像疊合時便會呈現一黑點一白點；假設要加密的機密影像像素為黑點，並且隨機選取了黑點加密規則的第二列，則在分享影像1上依序填入一白點一黑點，在分享影像2上依序填入一黑點一白點，當兩張分享影像疊合時便會呈現兩個連續的黑點。從表一很明顯地可以看出，機密影像上的每個像素在分享影像上皆被擴展成兩個像素，使得疊合影像的大小變成原機密影像的兩倍，有些(*k*, *n*)-threshold視覺式秘密分享機制其像素擴展的倍數甚至

表一: 傳統的(2, 2)-threshold 視覺式秘密分享機制

機密影像的像素	機率	加密規則		疊合結果
		分享影像 1	分享影像 2	
□	0.5	■□	■□	■□
	0.5	□■	□■	□■
■	0.5	■□	□■	■
	0.5	□■	■□	■

超過兩倍。像素擴展的結果不但使得影像產生變形，也造成分享影像的不易攜帶以及儲存空間的浪費。儘管像素擴展具有這些缺點，大部分的視覺密碼的研究還是以像素擴展的技術為基礎，並將它延伸至灰階影像或彩色影像上。

Ateniese等人[2]和Tzeng與Hu [19]則將門檻式的使用結構擴充為$\boldsymbol{\Gamma} = (P, F, Q)$的形式，稱之為任意使用結構(general access structure)，其中$P = \{1, 2, \ldots, N\}$為參與者(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，F, Q是2^P的子集合，分別代表禁止集合的集合(forbidden sets)與合格集合的集合(qualified sets)，而且$Q \cap F = \varnothing$。任何一個合格集合$Y \in Q$都可以還原機密影像，而任何一個禁止集合$X \in F$都無法獲得一絲機密訊息。所謂的「使用結構」是指定義如何分享機密的一種規則，而(k, n)-threshold便是屬於任意使用結構的一種特例。例如(2, 2)-threshold可以表示成下列的使用結構：$\boldsymbol{\Gamma} = (P=\{1, 2\}, F=\{\{1\},\{2\}\}, Q=\{\{1, 2\}\})$。每一個禁止集合與合格集合皆代表一種分享影像的疊合結果，也就是說，分享影像1或分享影像2都無法得出機密影像，當分享影像1與分享影像2疊合時，才能看到機密影像。不論是(k, n)-threshold或是任意使用結構，在實作上都要先設計黑點與白點的基礎矩陣，這兩個基礎矩陣便代表實現使用結構的分享機制，方程式(1)便是可實作出(2, 2)-threshold使用結構的基礎矩陣：

$$M_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \quad , \quad M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{1}$$

其中M_0 (M_1)代表白(黑)點的基礎矩陣，矩陣中的'1'代表黑色，'0'代表白色。當要加密的像素為白(黑)點時，便將M_0 (M_1)做欄向量隨機重排，將重排後的矩陣第一列的顏色填入分享影像1，第二列的顏色填入分享影像2。至於基礎矩陣要如何設計，則有許多相關的文獻可以參考[2,7,17,19,20]。

雖然視覺密碼發展至今已有一段時間，但是大部份的研究都是針對黑白影像，關於灰階和彩色影像的研究則十分有限。最早有關彩色視覺密碼的研究是由Verheul與van Tilborg [20]兩位學者所提出，稱為k out of n c-color VSS scheme，也就是具有c種顏色的機密影像，被分解成n張分享影像，取其中k張加以疊合，便可還原機密影像。他們的分享機制是使用c個$n \times b$的基礎矩陣$(C_0, C_1, \ldots, C_{c-1})$，其中$b$代表像素擴展的倍數。每個基礎矩陣$C_i$取$k$列以上疊合的向量$\boldsymbol{V}$中，只會有一個子像素顯示出顏色$i$，其餘子像素皆為黑色，而不足$k$列所疊合出的向量$\boldsymbol{V}$中，每種顏色的分佈頻率皆相同。當要分享機密影像上一個顏色為i的像素時，則將矩陣C_i進行欄向量隨機重排，並將每一列填入不同的分享影像上，藉此完成機密影像的分享。Yang與Laih [21]兩位學者則利用傳統的黑白視覺密碼中，分別對應於白點與黑點的兩個$n \times m$的基礎矩陣B_0和B_1，轉換成c個大小為$n \times (c \times m)$的基礎矩陣C_i。Yang與Laih宣稱在大部份的情況下，他們的像素擴展參數$b(= c \times m)$皆比Verheul與van Tilborg的像素擴展參數來得小。由於Verheul與van Tilborg以及Yang與Laih的方法都是使用像素擴展的技巧，而且當所要分享的顏色數目愈多時，像素擴展的愈嚴重。此外，他們的方法基本上都是利用黑色來遮住疊合時所不想顯露的顏色，使得他們

的疊合影像上的每個區塊，很可能有極大的部份會顯現出黑色，因此無法產生好的視覺效果。

Rijmen與Preneel [18]提出另外一種應用在彩色影像上的(2, 2)-threshold視覺密碼方法，他們將機密影像上的每個像素擴展成一個2×2大小的區塊，每個區塊分別填入紅(red)、綠(green)、藍(blue)、白(white)等四種顏色，因此在任何單一張分享影像上，是無法顯露出有關機密影像的訊息。Rijmen與Preneel認為四種顏色在2×2大小的區塊中，就會呈現出24種可能的排列(permutation)方式，將兩張分享影像疊合後，便會有24^2種顏色的變化。我們可以發現，若將相對應的兩個區塊上的顏色同時往同一方向移位，雖然所呈現的是另外一種排列，但是因為人眼並非針對單一像素的顏色做解釋，而會自動將整個區塊的顏色混合起來解釋，因此疊合後所產生的顏色與位移前的疊合結果是相同的，所以顏色上的變化並沒有Rijmen與Preneel兩位學者所宣稱的這麼多。Yang [22]亦曾針對此點進行探討。

Hou [14]利用CMY色彩模型與半色調的原理，提出一個(2, 2)-threshold的彩色視覺密碼模型。Hou將彩色機密影像分解成三張色調為青、洋紅、黃的影像，並且利用半色調技術將這三張連續調的影像分別轉換成二元的半色調影像。之後便依傳統的黑白視覺密碼方法，將這三張半色調影像各自分解成兩張分享影像。最後將所有的第一張分享影像合併成為一張分享影像，所有的第二張分享影像亦合併成另外一張分享影像，便可得出這個彩色機密影像的兩張分享影像。Hou也採用像素擴展的方法，為了維持影像的長寬比，機密影像上的每個點都被擴展成$m\times m$倍。

Chang等人[8]利用視覺密碼和數位餘弦轉換(Discrete Cosine Transform, DCT)設計了以彩色浮水印來保護彩色影像所有權的機制，實體上浮水印並未真正嵌入影像當中，而是藉由比對從彩色影像萃取出的Master Share和影像所有人持有的Ownership，來顯現出浮水印。Ownership的產生及將來浮水印的還原，便是Chang等人宣稱使用視覺密碼方法的部份。由於文中的浮水印只有四種顏色，所以他們將這四種顏色分別以不同的3×3黑白區塊來代表，Master Share和Ownership Share上每個3×3的區塊便對應於浮水印的每個像素，而Ownership Share的設計，便是令同樣是黑白影像的Master Share與Ownership Share進行OR運算後，可以得出符合浮水印像素顏色的區塊。所以本質上，Chang等人的方法是應用了與視覺密碼相同的OR運算，與視覺密碼以視覺解密的精神不符，對於浮水印每個像素的顏色，也是必須經過電腦對於影像區塊型態的判讀才能還原。

關於像素不擴展的黑白視覺密碼的研究非常少見。Hou等人[13]則針對灰階影像提出一種像素不擴展的方法，他們將灰階的連續調影像先行降低對比，然後再轉換成半色調影像，使得半色調影像上的每個固定大小的區塊內，都包含一半以上的黑點；要加密機密影像上的一個區塊B時，就在第一張分享影像上相對應的區塊B_1上隨機填入一半的黑點，然後配合機密影像區塊中黑點的分佈，在第二張分享影像上相對應的區塊B_2中也是填入一半的黑點，使得B_1和B_2重疊後所產生的黑點分佈，與機密影像區塊B中的黑點分佈相同。同時他們亦利用分色的原理，將彩色機密影像分解成青、洋紅、黃三張單一色調的影像，再將其方法套用在這三張單一色調影像，來達成像素不擴展的彩色視覺密碼。上述方法雖然實現了不擴展的目標，但是卻只適用在(2, 2)-threshold的視覺式秘密分享機制，而無法推廣到(k, n)-threshold以及任意使用結構的視覺式秘密分享機制。事實上

(a) 連續調影像　　(b) 半色調影像

圖一: 半色調轉換 (512×512 pixels, 300 dpi)

在Hou [14]的方法中，如果以像素不擴展的黑白視覺密碼方法來分享半色調影像，便可達到彩色視覺密碼分享影像不擴展的目的。Ito等人[15]針對黑白機密影像提出了一種不擴展的(*k*, *n*)-threshold視覺式秘密分享方法，當要分享一個黑(白)點時，便從對應於黑(白)點的基礎矩陣中隨機挑選一行，並且將這個行向量的第*i*列分配給第*i*個分享影像。由於不論是黑點或白點的基礎矩陣，其每一列0與1分佈的比例皆相同，所以分享影像上每一個像素，會填上黑點或白點的機率也都一樣，因此無法從分享影像上猜測到有關機密影像的資訊。而還原影像則靠第(2)式來產生對比。

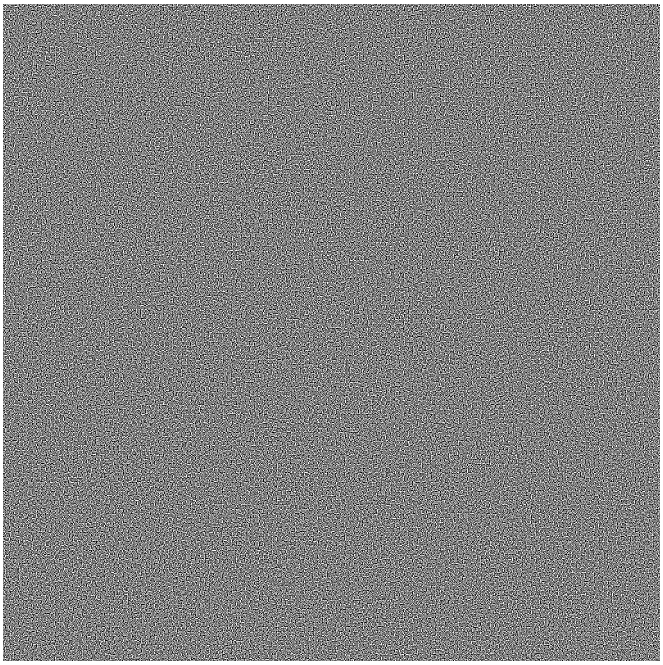
$$\beta = |p_0 - p_1| \tag{2}$$

在第(2)式中，p_0和p_1分別代表白點和黑點在疊合影像上產生黑點的機率。只要這兩個機率值差別夠大，人眼便可自動區分疊合影像上黑色與白色的區域。Ito等人所提出的不擴展模型，在分享一個像素時，是完全隨機地從基礎矩陣中挑選一行，雖然在整張疊合影像上，能夠達到(2)式的對比，但是在小區域上，黑點與白點的分佈就可能無法達到p_0與p_1的比率。因此在疊合影像上會有不好的視覺效果，尤其是當此模型應用在灰階和彩色影像上時，疊合影像看起來會太過雜亂，而嚴重影響到視覺效果。

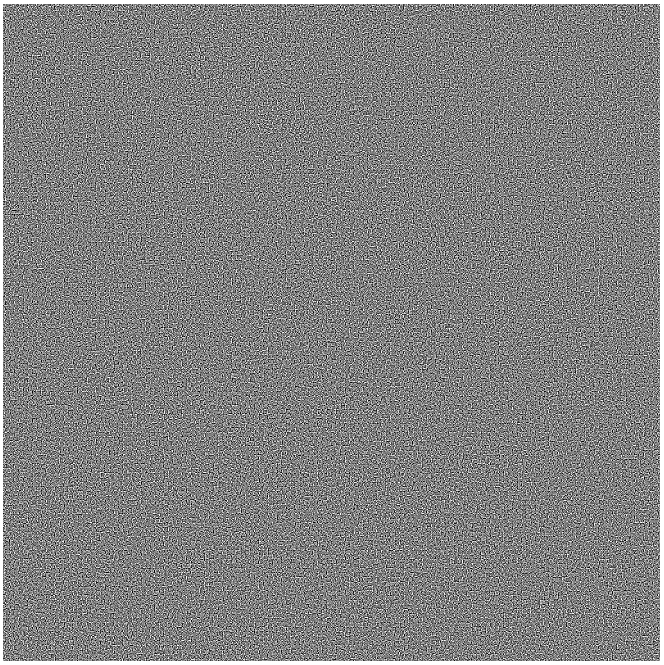
由於彩色視覺密碼的研究非常有限，而且大部份都是以像素擴展的技巧為主，因此本研究的目的便是在於提出一套不需像素擴展的彩色視覺密碼方法。我們的方法利用CMY色彩模型將彩色機密影像分解成三張單一色調的影像，這些單一色調的影像便相當於灰階影像，因此我們可以利用半色調技術，將這三張單一色調的影像轉換成三張二元影像。另外，本研究配合半色調影像的特性，提出一套像素不擴展的多點加密的方法，配合兩個代表黑點與白點的基礎矩陣，分別處理這三張單一色調的二元影像，最後利用色彩合成的原理，就可以疊合出我們所需要的分享影像。實驗結果證明，我們的方法所產生的分享影像，具有足夠的安全性；與Ito等人的方法相比，我們的疊合影像有較佳的視覺效果，同時，配合適當的基礎矩陣，我們的方法便可以很容易地推廣到其它使用結構上。

二、不擴展的灰階視覺密碼方法

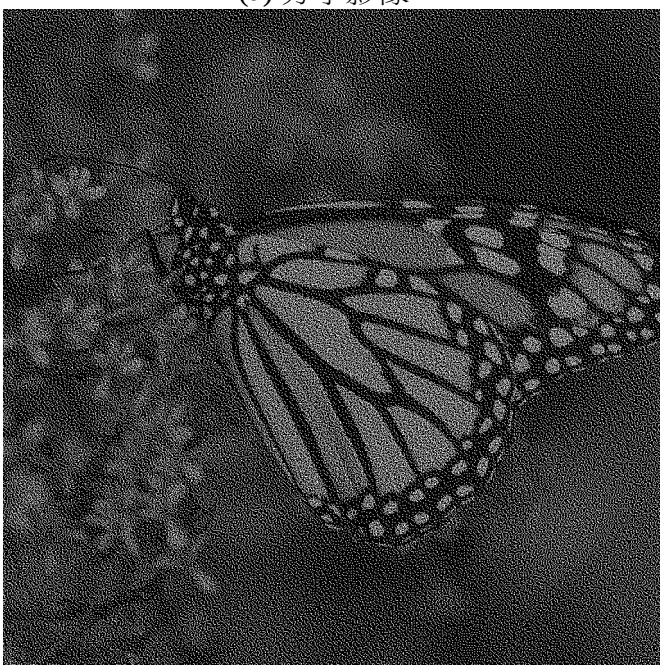
1. 半色調



(a) 分享影像1



(b) 分享影像 2



(c) 疊合影像

圖二: 以圖一(b)為機密影像的視覺密碼實驗 (1024×1024 pixels, 300 dpi)

半色調技術(halftoning)是一種將連續調影像(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。人類視覺系統對高頻的變化具有不敏銳性；因此，一塊均勻分佈的網點會被眼睛解釋為一塊單一灰階值的區域，而忽略其間網點的變化。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，我們只需要使用黑白兩種顏色，就可以模擬一個連續的色階。以灰階影像(圖一(a))為例，經過半色調轉換後，其結果為一張僅具有黑點與白點的半色調影像(圖一(b))。雖然圖一(b)為一張黑白影像，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

表二: 隨機式的不擴展(2, 2)-threshold 視覺式秘密分享機制

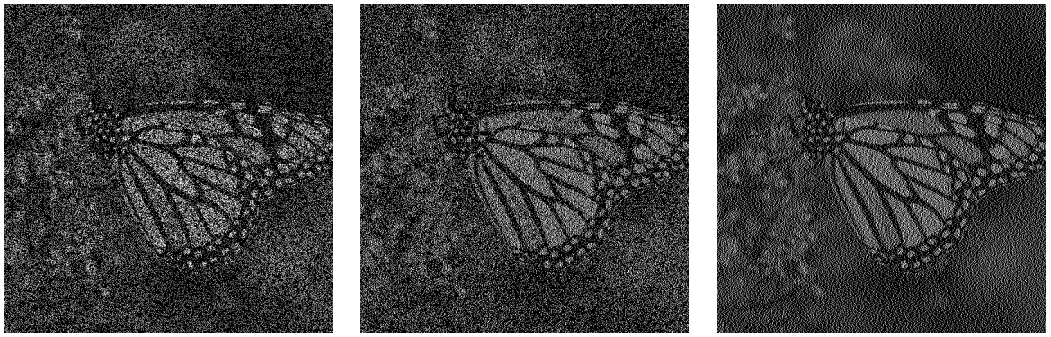
加密序列	機率	加密規則		疊合結果
		分享影像1	分享影像2	
□□	0.5	□■	□■	□■
	0.5	■□	■□	■□
■■	0.5	■□	□■	■■
	0.5	□■	■□	■■
■□	0.25	■□	□■	■■
	0.25	□■	■□	■■
	0.25	□■	□■	□■
	0.25	■□	■□	■□
□■	0.25	■□	□■	■■
	0.25	□■	■□	■■
	0.25	□■	□■	□■
	0.25	■□	■□	■□

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[16]。

大部分的視覺密碼技術都是以黑白影像為基礎的；如果我們利用半色調技術，將灰階影像轉換為黑白影像，那麼以黑白影像為基礎的視覺密碼方法便可以直接應用在半色調影像上。以圖一(b)為機密影像為例，利用Naor與Shamir的(2, 2)-threshold模型[17]製作出兩張分享影像(圖二(a)和圖二(b))，圖二(c)便為兩張分享影像重疊後的結果。由圖二(c)的結果可以證明，利用半色調技術來建構灰階視覺密碼方法是可行的。

2. 像素不擴展的多點加密法

由於半色調技術是利用網點的疏密來模擬灰階影像的灰階程度， Ito等人單點加密的方法，有可能破壞了半色調影像上網點分佈的規則，造成疊合影像上凌亂的視覺效果(見圖三(a))，因此並不適合應用在半色調影像的加密上。為了達成分享影像不擴展的目標，並且改進Ito等人方法的缺點，本研究提出一套新的黑白視覺密碼方法，再結合上述的半色調技術，便可應用在灰階影像的加密上，同時疊合影像也有較好的視覺效果。首先，我們以(2, 2)-threshold的視覺式秘密分享機制來說明本研究所提的加密方法，我們一次選取機密影像上的連續兩個點做為加密的對象，我們將這兩個點稱為「加密序列」，在一張黑白影像上便會有四種不同的加密序列型態，如表二所示。當加密序列為連續兩白點(黑點)時，我們可以沿用如表一的白點(黑點)加密規則，在分享影像上對應於加密序列的位置，隨機選擇白點(黑點)加密規則的其中一列，並依所選的加密規則在分享影像上填入一白一黑的點。當分享影像疊合時，對應連續兩白點的加密序列的疊合結果為一白一黑的兩個點，對應連續兩黑點的加密序列其疊合結果為兩個黑點，由於對應這兩種加密序列的疊合結果有對比上的差異，因此人眼還是能從疊合影像上分辨黑白之間的不同。當加密序列為另外兩種型態時(即黑白各半)，由於黑點和白點皆佔整個加密序列的



(a) Ito等人的方法　　(b)隨機式的方法　　(c)本研究的方法

圖三: Ito等人的方法、隨機式的方法與本研究方法之比較(512×512 pixels, 300 dpi)

一半，其中一種可能的解決方式便是，先隨機決定要使用的是連續兩白點或連續兩黑點的加密規則，再從所選的加密規則中隨機選取一列來使用，即表二所顯示的分享機制。雖然這種作法將這兩種加密序列做了失真的處理，但由於是隨機決定的結果，在疊合影像上仍是能表現出黑色區域和白色區域之間的對比。我們以圖一(b)做為機密影像，並以表二所示的視覺式秘密分享機制來加密，解密後的疊合影像如圖三(b)所示。

由圖三(b)可以看出隨機決定的結果造成疊合影像上雜亂的視覺效果，為了解決這種雜亂的視覺效果，針對這種黑白各半的加密序列，我們設定了下列的規則，來決定加密規則的使用：

if e **mod** 2 < 1 **then**
　　從連續兩黑點的加密規則中隨機選用其中一列
else 從連續兩白點的加密規則中隨機選用其中一列

其中，e代表機密影像上已加密過的黑白各半的加密序列的個數。我們的方法主要是依照加密序列中黑點與白點的比例，來分配連續兩黑點的加密規則和連續兩白點的加密規則使用頻率。由於黑點個數在黑白各半的加密序列中佔1/2，所以較合理的作法，機密影像上所有黑白各半的加密序列，其中的1/2使用連續兩黑點的加密規則來加密。因此，我們的方法會使每2個黑白各半的加密序列中，其中一個是使用連續兩黑點的加密規則，另一個則使用連續兩白點的加密規則。由於按照黑白點分佈的比例來決定加密規則的使用，所以疊合影像有較平順的視覺效果，如圖三(c)所示。

之前我們曾經提過，任何一種視覺式秘密分享的使用結構，都是利用兩個基礎矩陣實作出來，因此我們只要利用適當的基礎矩陣，便可將我們的方法從(2, 2)-threshold延伸至(k, n)-threshold視覺式秘密分享機制。令M_0與M_1分別代表對應於白點與黑點的$n \times m$基礎矩陣，加密序列的長度為m，亦即我們一次取機密影像上的連續m個點來加密，b代表加密序列中的黑點個數($0 \le b \le m$)，e_b則代表具有b個黑點的加密序列已加密過的個數，則本研究的多點加密法加密程序如下：

a) 令$e_b = 0$ **for** $b = 1, 2, \ldots, m$。
b) 由機密影像SI中取出尚未加密的加密序列，記錄其位置($p_1, p_2, \ldots, p_m$)，並計算其黑點個數b。

c) 將基礎矩陣M做欄向量隨機重排，再將重排後的矩陣中第i列上的m個顏色，依序填入第i張分享影像的$p_1, p_2, \ldots, p_m$位置上，其中矩陣M根據下列規則決定：

if e_b **mod** $m < b$ **then** $M = M_1$
else $M = M_0$

d) $e_b = e_b + 1$。

e) 重覆步驟(b) – (d)直到機密影像上的所有像素皆加密完畢。

以(2, 2)-threshold視覺式秘密分享機制為例，其黑點與白點的基礎矩陣如第(1)式所示。假設機密影像上的所有的點為D = (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)，其中'0'代表白點，而'1'則代表黑點。我們由機密影像中取出第一組加密序列的位置為(p_1, p_2) = (1, 2)，其黑點個數b = 1，此時e_1 = 0，由於e_1 **mod** 2 = 0 < 1，所以我們將M_1做欄向量隨機重排後得到的矩陣為

$$M = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

重排後的矩陣M的第一列為[1, 0]，所以在第一張分享影像上的位置1與位置2分別填上黑點與白點，而M中的第二列為[0, 1]，所以在第二張分享影像上的位置1與位置2分別填上白點與黑點。接著，再依序取出第二組加密序列的位置為(p_1, p_2) = (3, 4)，其黑點個數b = 1，此時e_1 = 1，由於e_1 **mod** 2 = 1，所以我們將M_0做欄向量隨機重排後得到的矩陣為

$$M = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

所以在第一張分享影像上的位置3與位置4分別填上白點與黑點，而在第二張分享影像上的位置3與位置4分別填上黑點與白點。依此類推，直到所有的加密序列都加密完畢為止。

3. 安全性和對比分析

令$\boldsymbol{\Gamma} = (P, F, Q)$為一個任意使用結構，$C_0$和$C_1$分別代表將基礎矩陣$M_0$和$M_1$做欄向量隨機重排後的所有$n \times m$布林矩陣的集合。假如存在一個值$\alpha(m)$與一個門檻值集合$\{(X, t_X)\}_{X \in Q}$，則$C_0$和$C_1$構成一個視覺密碼方法必須滿足下列條件[2]：

(1) 任何一個合格集合$X = \{i_1, i_2, \ldots, i_p\} \in Q$可以藉由疊合對應於集合中的所有分享影像來還原機密影像。也就是說，將任何一個矩陣$M \in C_0$的第$i_1, i_2, \ldots, i_p$列做OR運算所得到的m-向量$\boldsymbol{V}$，必須滿足$w(\boldsymbol{V}) \le t_X - \alpha(m) \cdot m$；然而，將任何一個矩陣$M \in C_1$的第$i_1, i_2, \ldots, i_p$列做OR運算所得到的$m$-向量$\boldsymbol{V}$，必須滿足$w(\boldsymbol{V}) \ge t_X$。

(2) 任何一個禁止集合$X = \{i_1, i_2, \ldots, i_p\} \in F$無法獲得機密影像中的任何機密訊息。也就是說，將$C_t$ ($t \in \{0, 1\}$)中所有的$n \times m$矩陣限制在第$i_1, i_2, \ldots, i_p$列所得到的$p \times m$矩陣的集合D_t，則在D_0與D_1中相同的矩陣會有相同的出現次數，因此D_0與D_1是無法區分的(indistinguishable)。

其中$w(\boldsymbol{V})$代表向量$\boldsymbol{V}$中的'1'的個數(即Hamming weight)，t_X代表將矩陣$M \in C_1$的第$i_1, i_2, \ldots, i_p$列做OR運算所得到的m-向量$\boldsymbol{V}$中黑點個數的門檻值，$\alpha(m)$為疊合影像的相對對比。

第一個條件稱為對比條件，代表白點的分享影像上的m個點重疊後，其黑點的個數必須小於$t_X - \alpha(m) \cdot m$；代表黑點的分享影像的m個點重疊後，其黑點的個數必須大於門檻值t_X。因此，代表白點的分享影像的m個點重疊後，就會與代表黑點的分享影像的m個點有一定的色差。也就是說，Q中的任一個合格集合的成員將他們所持有的分享影像疊合在一起，可以產生黑白之間的對比，從而看出機密影像。第二個條件稱為安全條件，也就是任何人都不可能從屬於禁止集合的分享影像上，獲得任何有關機密影像的資訊。

本研究的方法是架構在基礎矩陣之上，因此亦能滿足視覺密碼所要求的安全性與對比兩個條件。藉由下列命題1與命題2的證明，便可了解本研究方法的安全性和對比。

命題1：屬於禁止集合的分享影像疊合後，無法洩露出機密影像的訊息。

證明：機密影像上的每個加密序列，不論其是何種型態，不是使用矩陣$M \in C_0$加密，就是使用矩陣$M \in C_1$加密。又C_0和C_1必須滿足上述之安全性條件，因此本研究的方法與C_0和C_1有相同的安全等級。

命題2：屬於合格集合的分享影像疊合後，疊合影像的最大對比為$\alpha(m)$。

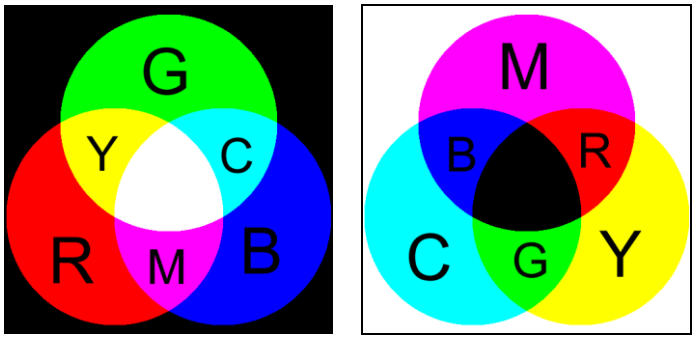
證明：令$X = \{i_1, i_2, \ldots, i_p\} \in Q$，$M \in C_t$ ($t \in \{0, 1\}$)，OR(M, X)代表將矩陣M的第$i_1, i_2, \ldots, i_p$列做OR運算所得到的m-向量。$E^{(b)}$代表機密影像上具有b個黑點的加密序列，在m個$E^{(b)}$加密序列中，有b個使用$M \in C_1$加密，其餘的$(m - b)$個$E^{(b)}$加密序列則使用$M \in C_0$加密，因此在將X的分享影像重疊後的疊合影像上，在對應於這m個$E^{(b)}$加密序列的區域將會有$[b \times r_1 + (m - b) \times r_0]$個黑點，其中 $r_1 = w(\mathrm{OR}(M \in C_1, X))$，$r_0 = w(\mathrm{OR}(M \in C_0, X))$；因此，這$m$個$E^{(b)}$加密序列在疊合影像上的黑色程度(blackness)或灰階值(gray-level)可以表示成$[b \times r_1 + (m - b) \times r_0]/m^2$。在最極端的情況下，當加密序列全為白點(即$b = 0$)時的灰階值為$r_0/m$，加密序列全為黑點($b = m$)時的灰階值為$r_1/m$，因此疊合影像的最大對比為$(r_1 - r_0)/m$，此對比與基礎矩陣的對比$\alpha(m)$相同。

三、不擴展的彩色視覺密碼方法

1. 彩色的基本原理

色彩模型(color model)是一個描述顏色的方法[11]，色彩模型可以表示成一個三度空間的座標系統，在這空間上的每個點就代表一種顏色。色彩模型有很多種，最常見的兩種色彩模型便為RGB與CMY。

在RGB色彩模型中，每個顏色都是利用紅(red)、綠(green)、藍(blue)三種顏色混合產生，這三個顏色亦是光的三原色。因此RGB色彩模型通常是應用在利用光來產生顏色的



(a) (b)

圖四: (a)光的三原色及其混色；(b)顏料的三原色及其混色

硬體上，例如螢幕或是攝影機。當全紅、全綠、和全藍的光混合在一起時，便會產生白光，因此RGB色彩模型又稱為增色模型。在CMY色彩模型中，每個顏色則是利用青(cyan)、洋紅(magenta)、黃(yellow)三種顏色混合所產生，這三個顏色亦為顏料的三原色，因此CMY色彩模型通常是應用在彩色列印上。光的波長決定了光的顏色，當光照在顏料上時，顏料會吸收部份光的波長，未被吸收的部份便反射(reflect)出來，成為顏料的顏色。不同顏色的顏料則吸收不同波長的光，愈多種顏色的顏料混合在一起，所吸收的光愈多。當全青、全洋紅、和全黃三種顏色的顏料混合在一起時，由於所有波長的光都被吸收了，因此混合後的顏料便形成黑色，所以CMY色彩模型又稱為減色模型。我們由圖四可以觀察到，不論是RGB色彩模型或CMY色彩模型，當我們分別混合其中兩種顏色時，便會產生另外一個模型的原色，因此RGB和CMY之間是為互補的關係，青、洋紅、黃為光的補色(secondary colors)，而紅、綠、藍則為顏料的補色。

從上面對色彩模型的描述我們可以知道，我們可將彩色影像進行分色處理，利用RGB或CMY色彩模型將影像分成三張單一色調的影像，再將這三個不同色調的影像混合在一起後，就可以還原原來的彩色影像。例如在列印彩色影像時，便是利用CMY色彩模型，將不同程度半透明的青、洋紅、黃三種顏料一層層地印在紙上。當光照在塗有顏料的紙上反射回來，每一層的顏料都會吸收部份波長的光，最後未被吸收的光，便是這三層顏料混色後所顯現的顏色。由於彩色視覺密碼最後所產生的分享影像，是列印在投影片上，將投影片疊合後便產生混色效果，與彩色列印的原理相同。所以本研究亦使用CMY色彩模型，將彩色機密影像分解成三張分別具有青、洋紅、黃色調的影像。每一張分解影像其中的顏色皆為同一色調但強度(intensity)不同，其顏色分佈的範圍皆為0–255，所以也可以將之視為三張單色的灰階影像。由於每一張影像都是屬於連續調的影像，所以同樣可以利用半色調技術將這三張連續調影像轉換成二元影像，之後再利用本研究所提的多點加密法來產生相對應的分享影像。

2. 彩色影像的多點加密法

令M_0與M_1分別代表對應於白點與黑點的兩個$n \times m$的基礎矩陣。為了使這兩個基礎矩陣可以直接應用在彩色機密影像上，我們利用CMY色彩模型將彩色機密影像分解成三張青、洋紅、黃的單一色調影像。之後再將每一張分解的影像由連續調轉換成半色調，使得每張影像上的每個像素只有兩種值：空白(blank)或非空白(not blank)。為了方便說明

起見，我們將這兩種值分別以白點和黑點稱之。轉換後的半色調影像，便可以利用我們的多點加密法來處理，因此整個彩色影像視覺密碼方法的加密程序如下：

a) 將彩色機密影像*SI*利用CMY色彩模型分解成青、洋紅、黃三張單一色調的影像，分別為*C, M, Y*。
b) 將*C, M, Y*分別轉換成三張半色調影像*C', M', Y'*。
c) 將這三張半色調影像*C', M', Y'*，分別利用多點加密法加密。
d) 將半色調影像*C', M', Y'*的第*i*張分享影像利用色彩合成的原理合併成為一張分享影像，合併後的影像便成為彩色機密影像*SI*的第*i*張分享影像。

我們將彩色機密影像分解成青、洋紅、黃三張單一色調的影像，使得我們可以很容易地利用上一節所提的灰階視覺密碼的方法，來處理彩色機密影像。而在灰階視覺密碼中，我們利用半色調的技術，將連續調的影像轉換成二元影像。所以我們可以很容易地將傳統黑白影像的視覺密碼方法，應用在彩色視覺密碼上。在此我們以本研究所提出的多點加密法，將三張不同色調的半色調影像*C', M', Y'*，分別分解出*n*張分享影像：C_1, C_2, …, C_n、M_1, M_2, …, M_n、Y_1, Y_2, …, Y_n，再將C_i, M_i, 與Y_i合併成彩色機密影的第*i*張分享影像，而分享影像上的每個像素的顏色，便為C_i, M_i, 與Y_i中對應於同一像素的顏色的混色結果。

由於基礎矩陣的安全條件，因此在每張半色調影像所分解出的分享影像上，是看不出任何蛛絲馬跡的，當不同色調的分享影像混合後，亦無法從中窺得任何有關機密影像的訊息。而基礎矩陣的對比條件，使得屬於合格集合的分享影像疊合後，可以在顏色上產生深淺不同的對比。從實驗結果亦可看出，禁止集合的分享影像是有足夠的亂度，無法從中看出一絲有關機密影像的訊息，而合格集合的分享影像疊合後的結果，不僅可以看出機密影像的內容，亦具有不錯的視覺效果。

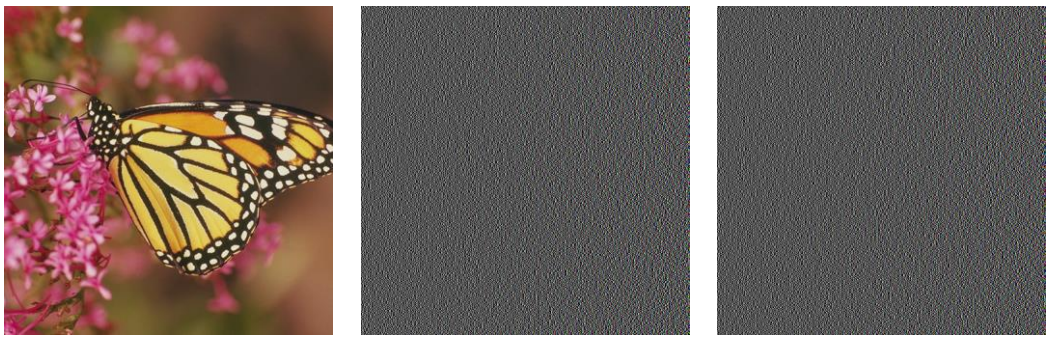
四、實驗與討論

1. (2, 3)-threshold使用結構

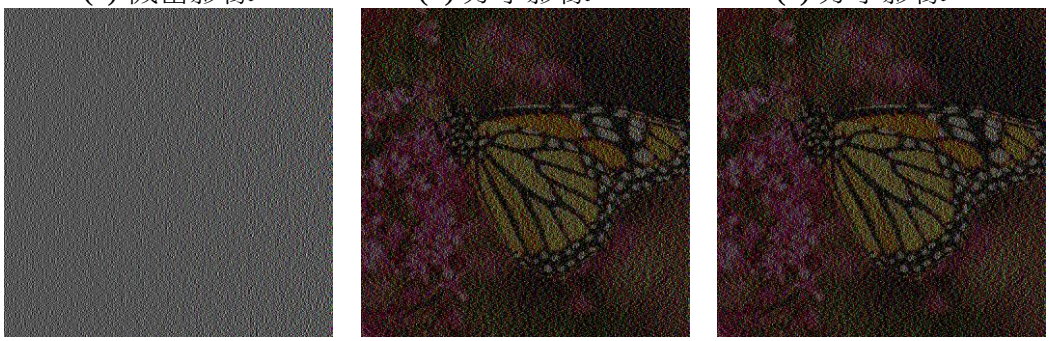
在這個實驗當中，我們實作一個(2, 3)-threshold使用結構的彩色視覺密碼，其任意使用結構的形式可表示成$\Gamma = (P=\{1, 2, 3\}, F=\{\{1\},\{2\}, \{3\}\}, Q=\{\{1, 2\}, \{2, 3\}, \{1, 3\},\{1, 2, 3\}\})$。我們所使用的基礎矩陣如下所示：

$$M_0 = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \quad M_1 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}。 \tag{3}$$

我們所使用的實驗影像如圖五(a)所示，這個使用結構會產生三個分享影像(見圖五(b)–(d))，至少取兩張分享影像便可還原機密影像(見圖五(e)–(h))。從實驗結果來看，在對應於禁止集合的疊合影像上，都無法窺探出機密影像的訊息。



(a) 機密影像 (b) 分享影像 S1 (c) 分享影像 S2



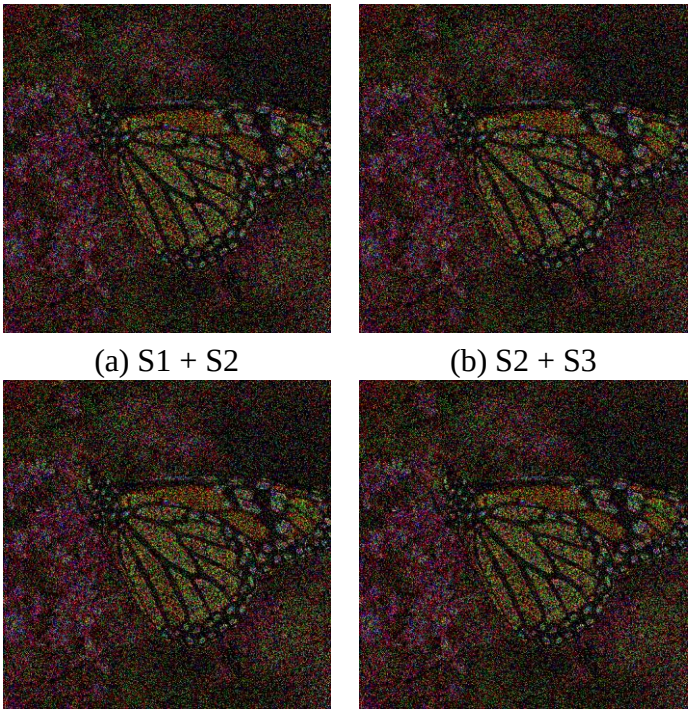
(d) 分享影像 S3 (e) S1 + S2 (f) S2 + S3

(g) S1 + S3 (h) S1+ S2 + S3

圖五: 彩色影像之(2, 3)-threshold實驗結果 (512×512 pixels, 300 dpi)

2. 討論

本研究應用色彩模型的原理，將彩色機密影像分解成青、洋紅、黃三張單一色調的影像，並且利用半色調技術將這三張連續調影像轉換成二元影像。而本研究所所提的多點加密法，可針對這些二元影像產生不擴展的分享影像。再將不同色調的分享影像合併後，便成為彩色機密影像的分享影像，而這些合併的分享影像自然也是與原始機密影像大小相同的。大部份的視覺密碼的研究，都需要擴展分享影像的像素，尤其是灰階或彩色的視覺密碼更是如此。事實上，彩色視覺密碼的研究非常有限，其中Verheul與van Tilborg [20]以及Yang與Laih [21]的方法不但需要擴展像素，而且還需要利用黑色來將疊合後不想顯現出來的顏色遮住，可以想見其疊合影像的視覺效果是非常的差。Hou等人[13]雖然提出了一個不擴展的彩色視覺密碼方法，但是他們的方法只限於(2, 2)-threshold的使用結構，而無法推廣到其它使用結構上。雖然在本研究中實作的是(2, 3)-threshold的使用結構，事實上我們可以取用任意使用結構的基礎矩陣，便可以產生任意使用結構的分享影像，因此本研究的方法可以很容易地延伸至任意使用結構。



(a) S1 + S2　(b) S2 + S3

(c) S1 + S3　(d) S1+ S2 + S3

圖六: 使用Ito等人的方法所得出的疊合影像 (512×512 pixels, 300 dpi)

如果我們應用Ito等人[15]的方法將像素不擴展的黑白視覺密碼方法推廣到灰階或彩色影像上，則疊合影像顯得有點凌亂(見圖六(a)–(d))。由於Ito等人的作法是針對每一點去做加密，因此雖然在大範圍上可以達到其設計上的期望值，但是在小範圍內的黑點與白點的分佈可能無法達到(2)式中的p_0與p_1的比率，使得小範圍內的灰階值有可能產生極大的變動，造成疊合影像看起來雜亂無章。本研究所提的多點加密法保證在每m個$E^{(b)}$加密序列中，有b個加密序列是使用黑點基礎矩陣加密，另外的$(m - b)$個使用白點基礎矩陣加密，因此在疊合影像上黑與白的變化很規律。此外，半色調影像是以網點的疏密來模擬色階的變化，其網點的設計皆有一定的規則，一旦此一規則被嚴重破壞，將可能導致影像視覺品質的下降。因此，加密時如能有效降低原半色調影像網點分佈被破壞的程度，將可提高視覺密碼疊合影像的視覺品質。我們的方法由於在小範圍內能維持一定的黑與白的比例，因此可以有效維持原半色調影像上網點的分佈規則，這也就是將我們的方法應用在半色調影像上，可以維持較好的視覺效果的原因。然而Ito等人的方法完全是以隨機的方式來產生分享影像，因此可能嚴重破壞原半色調影像的網點分佈規則，導致重疊後旳影像視覺效果不佳，這個現象可以由圖五和圖六的比較看出其差異。

五、結論

視覺密碼的方法可以將一張機密影像，加密成n張分享影像，參與秘密分享的n個參與者都分別持有一張分享影像。一群被允許可以獲得機密訊息的參與者，只要將他們所持有的分享影像全部重疊在一起，就可以直接透過眼睛在重疊的影像上看到機密訊息；相反地，一群不被允許獲得機密訊息的參與者，便無法透過將分享影像重疊的方式來取得機密訊息。因此，視覺密碼學與傳統密碼學最大的不同，就在於其解密的方式是透過

人眼來完成，而不需要其它的電腦設備或是複雜的解密演算法。由於這樣的一個特殊解密方式，使得視覺式的秘密分享方式，非常適用於無法使用電腦來解密的情況。

在視覺密碼學的研究領域中，大部分的方法都是以像素擴展為基礎的，然而以像素擴展技術為基礎的視覺密碼方法，卻會導致分享影像變形、不易攜帶以及浪費儲存空間等問題。此外，大部份的視覺密碼方法是以黑白機密影像為主，少有研究提出灰階和彩色影像的視覺密碼方法。在本研究中，我們提出一個不需要像素擴展的灰階和彩色視覺密碼方法。每次選取影像上連續的m個點同時加密加密m個連續的點，可以避免單點加密造成疊合影像視覺效果雜亂的缺點，同時達成像素不擴展的目標。我們的方法架構在兩個$n \times m$的黑點與白點基礎矩陣上，因此可以保有與基礎矩陣相同的安全性。對於灰階機密影像而言，我們利用半色調技術，將原始機密影像轉換成黑白影像，再針對黑白影像以同樣的方法進行加密，由於本研究的方法對於基礎矩陣M_0和M_1的使用，是配合影像中黑點的比例，因此不易破壞半色調影像網點分佈的規律性，進而可以確保疊合影像的視覺效果。對於彩色機密影像則進行分色的處理，將它分成青、洋紅、黃三張不同色調的影像，每個色調的影像便可視為一張灰階影像，因此就可利用本研究所提的灰階視覺密碼方法來加密。

視覺密碼的方法除了有像素擴展的問題外，尚存在著另一個對比損失的問題，亦即疊合影像的對比往往比原始影像的對比來得低，造成疊合影像的內容不夠清晰，尤其是灰階影像其灰階度的動態範圍(dynamic range)有可能很狹窄，轉換後的半色調影像對於對比損失的容忍程度，會比一般的黑白影像來得差。因此，未來我們將進一步擴充本研究的方法，來解決視覺密碼中對比損失的問題。

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 Naor, M., “Visual Cryptography for Grey Level Images”, *Information Processing Letters* (75), 2000: pp.255-259.

[7] 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.

[8] Chang, C. C., Yeh, J. C., and Hsiao, J. Y., “A Color Image Copyright Protection Scheme Based on Visual Cryptography and Discrete Cosine Transform”, *Imaging Science Journal* (50), 2002: pp. 133-140

[9] Droste, S., “New Results on Visual Cryptography” , in *Advances in Cryptology-CRYPTO ’96*, LNCS 1109, Springer-Verlag, 1996: pp.401-415

[10] 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.

[11] Gonzalez R. C. and Woods, R. E., *Digital Image Processing*, 2nd Edition, Prentice-Hall, New Jersey, 2002.

[12] 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.

[13] Hou, Y. C., Lin, C. F. and Chang, C. Y., "Visual Cryptography for Color Images without Pixel Expansion", *Journal of Technology* (16:4), 2001: pp. 595-603.

[14] Hou, Y. C., "Visual Cryptography for Color Images", *Pattern Recognition* (36), 2003: pp. 1619-1629.

[15] Ito, R., Kuwakado, H., and Tanaka, H., "Image Size Invariant Visual Cryptography", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science* (E82-A:10), 1999: pp. 2172-2177.

[16] 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.

[17] Naor, M. and Shamir, A., "Visual Cryptography", in *Advances in Cryptology-EUROCRYPT '94*, LNCS 950, Springer-Verlag, 1995: pp. 1-12.

[18] Rijmen, V. and Preneel, B., "Efficient Colour Visual Encryption for Shared Colors of Benetton", *Eurocrypto '96*, Rump Session, Berlin, 1996, Available at http://www.iacr.org/conferences/ec96/rump/preneel.ps

[19] Tzeng, W. G. and Hu, C. M., "A New Approach for Visual Cryptography", *Designs, Codes and Cryptography* (27), 2002: pp. 207-227.

[20] 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* (11:2), 1997: pp. 179-196.

[21] Yang, C. N. and Laih, C. S., "New Colored Visual Secret Sharing Schemes", *Designs, Codes and Cryptography* (20), 2000: pp. 325-335.

[22] Yang, C.N., "A Note on Efficient Color Visual Encryption", *Journal of Information Science and Engineering* (18), 2002: pp. 367-372.