具有優先權概念之不擴展漸進式視覺密碼

侯永昌
淡江大學資訊管理系

官振宇
國立中央大學資訊管理系

蔡志豐
國立中央大學資訊管理系

摘要

在現行漸進式視覺密碼的研究假設中，是讓每一張分享影像都擁有相同的權限等級，因此在這個限制下，管理人員無法根據參與者的重要性，針對機密影像的還原而給予差異化的能力。為了改善這個限制，本研究提出漸進式且具有不同權限等級的不擴展視覺密碼分享方法，稱之為 (n, n)-priority and progressive visual sharing model ((n, n)-PPVSM)。在這個分享模型中，假設共有 n 位機密資訊分享的參與者，並且每一位參與者的權限都不相同，因此每一張分享影像都被賦予一個不同的還原機密影像的權限等級 (k)。

在本研究的設計中，第 k 個權限等級的分享影像 (WS^k) 上，每一個像素點被分配到黑點的機率是 $2k / (n^2+n)$，並且如果權限等級 k 大於權限等級 l，則 WS^k 還原機密影像的能力將優於 WS^l。當重疊所有的分享影像後，機密影像的白點部分被疊合出黑點的機率為 $2 / (n+1)$，而黑點部分則是會被疊合出全黑，在疊合影像上會產生 $(n-1) / (n+1)$ 的黑白色差，所以可以清晰地顯示機密影像的內容。

相較於其它學者的研究，(n, n)-PPVSM 的分享機制具備下列幾項優點：(1) 每一張分享影像具備不同的能力來還原機密影像。(2) 疊合影像的色差對比優於其它視覺密碼學的研究。(3) 權限機制更適合應用於灰階和彩色影像的漸進式分享環境中，可以清晰地辨識出機密內容。(4) 本研究的分享影像大小與機密影像相同。

關鍵字：視覺密碼、漸進式視覺密碼、機密資訊分享、優先權分享影像

(*n, n*)-priority and progressive visual sharing model

Young-Chang Hou
Department of Information Management, Tamkang University

Zen-Yu Quan
Department of Information Management, National Central University

Chih-Fong Tsai
Department of Information Management, National Central University

Abstract

In the recent studies of visual cryptography (VC) or progressive VC, every share created by above two schemas has same capabilities to recover the secret image. As a result, managers are unable to give proper advantage to participants according to their importance. Consequently, providing each share a suitable recovering capability will be an effective way to solve this problem. In this paper, we propose a novel secret sharing method namely (*n, n*)-priority and progressive visual sharing model ((*n, n*)-PPVSM), every participant will be assigned a distinct weighting value, assuming that each one's significance is different from each other.

Particularly, every pixel has the probability of $2k / (n^2+n)$ to be distributed as black in the *k*-th weighting share (WS^k), and this share has a better ability than the *l*-th weighting share (WS^l) to reveal the secret image if $k \geqq l$. When superimposing all shares, the upper bound of the white part in the secret image to be appeared as a black point will be $2 / (n+1)$, and the black part is fully black, the restored image's contrast is equal to $(n-1) / (n+1)$, and the contents will be clearly identified.

Comparing our work with others, (*n, n*)-PPVSM has the following advantages: (1) Every share has different abilities to reveal secret information. (2) The contrast of the restored image is better than traditional VC. (3) This mechanism is more suitable for gray-level and color images in progressive sharing, and the cryptographers can clearly identify confidential content visually. (4) The size of shares is the same as the one of the secret images.

Key words: Visual Cryptography, Progressive Visual Cryptography, Secret Sharing, Priority (Weighting) Share

壹、前言

隨著電腦和網際網路的興起與普及，許多日常行為因為方便、快速等理由，逐漸由實體世界轉移到虛擬的網路空間上去執行，因而發展出電子商務、電子化政府、電子付款等應用，使得每個人對於電腦及網際網路的依賴度日漸提高。然而在資訊化服務的快速發展下，如何確保資料在傳遞或分享時，不會面臨竊取、竄改與破壞等攻擊，一直是資訊安全的一大挑戰。目前最普遍的方法是使用密碼學的技術，透過加密 (encryption) 演算法將機密資訊轉換成雜訊式資料，並且必須要用對應的解密演算法 (decryption) 才能還原出原始資訊。藉此確保在有限的時間與資源下，攔截者無法經由窮舉法 (exhaustive attack) 或統計攻擊法 (statistical attack) 來破解機密資訊，而達到計算上安全 (computationally secure) 的目標。

視覺密碼 (visual cryptography) 是一種特殊的密碼學技術，首先是由 Naor 與 Shamir (1995) 於 EuroCrypt'94 會議中提出。其概念是將所要分享的機密影像經過加密程序後，會被分解為 n 張分享影像 (share，也可稱為 shadow image)，每一位參與機密分享的參與者均分別持有一張分享影像。當需要解譯機密資訊時，只要疊合一定數量的分享影像，在疊合影像上即可還原出機密影像的內容。視覺密碼的特點在於只需要透過人類的視覺系統，就可以判讀出疊合影像上的機密訊息，而不需要任何複雜的數學運算與金鑰置換過程，因此可以降低機密資訊分享的限制。傳統視覺密碼是植基於 (k, n)-threshold 的分享機制，而且它的還原過程是一種非有即無 (all-or-nothing) 的模式。當分享影像的數目少於 k 張時，疊合影像上會呈現出亂碼的形態，無法辨識出機密訊息的內容；但是重疊 k 張或 k 張以上的分享影像後，疊合影像上就能顯示出黑白區塊的色差，因而揭露出機密資訊的內容。漸進式視覺密碼 (progressive visual cryptography) 則是一個新的概念，其解密方式雖然也是藉由分享影像間的重疊，不過它的還原過程不再是非有即無的概念，而是隨著被重疊分享影像數目的增加，機密影像的輪廓會愈來愈清晰，以達到逐步還原機密資訊的目標。

在現行的漸進式視覺密碼的研究中 (Fang 與 Lin 2006；侯與官 2011)，是設定每一張分享影像都擁有相同的能力來復原機密資訊，這表示每一位機密分享的參與者，皆是被分配在同一個權限等級中。也就是說，每當疊合影像上再增加一張分享影像後，疊合影像上的黑白色差平均值就會提升某一個固定值。然而就管理層面而言，機密分享的參與者可能會有不同的重要性，不過在現行的漸進式視覺密碼的分享機制下，卻無法根據參與者的重要性來賦予適當的權限等級，藉此彰顯機密資訊還原的差異化能力，因而缺乏應用上的彈性。

本研究為了改善上述的限制，而提出一個漸進式且具有不同權限等級的不擴展視覺密碼分享方法，稱之為 (n, n)-PPVSM ((n, n)-priority and progressive visual sharing model)。在 (n, n)-PPVSM 的分享機制中，將會在分享影像上增加了優先權的概念，並且假設每一

張分享影像的優先權等級皆不相同，即是將 n 個機密分享的參與者劃分為 n 個相異的權限等級。當要還原機密資訊時，疊合影像的還原速率與視覺品質是根據參與者的權限等級而定，即是在較高權限的分享影像上，將會具有較充足的資訊來還原機密影像，因此能夠較快速來達成機密資訊的還原；反之，較低權限的分享影像則是被賦予較低的還原能力。根據實驗的結果顯示：本研究所設計的分享矩陣不僅能產生不擴展的分享影像，而且每一張分享影像會根據參與者的權限而具備不同的解密能力，當重疊 n 張分享影像後，疊合影像的色差對比是 $(n-1)/(n+1)$，這個結果優於傳統視覺密碼的 50% 色差對比。在下面的章節中，第二章是介紹相關參考文獻與技術，第三章是介紹本研究所提出的 (n, n)-PPVSM 的分享機制，而第四章則是實驗結果與分析討論，最後的第五章是本研究的結論。

貳、文獻探討

一、視覺密碼簡介

視覺密碼不同於以往的密碼學技術，除了加密過程中沒有複雜的演算法外，更重要的是當分享影像重疊後，就可以人眼直接對機密內容進行判讀，所以視覺密碼不需要額外的電腦輔助運算。其做法是將需加密的機密影像，根據黑白兩色的拆解和分享規則，製作出多張無意義的分享影像，使得人們無法從任何一張分享影像中解讀出機密圖像的內容，因而達成密碼學所要求的安全性目標。

在 Naor 與 Shamir (1995) 所提出的 (k, n)-threshold 分享機制中，需要兩個 $n \times m$ 的分享矩陣 C^0 與 C^1，用來分別代表機密影像上白點與黑點的拆解與分享方式，其中 n 代表參與機密分享的人數，m 代表像素擴展的倍率，而分享矩陣中的每一列代表每一個參與者所分配到的顏色分布 (0 代表白、1 代表黑)。我們以 (2, 2)-threshold 為例 (公式 1)，機密影像上的每一個像素點 (pixel)，會被分享為一白一黑的影像區塊。當要分享機密影像的白點時，兩個參與者都得到相同的影像區塊；反之，當要分享機密影像的黑點時，兩個參與者會得到互補的影像區塊。使得兩張分享影像在疊合時，機密影像上的白點會顯示為半黑白，而黑點的部份則為全黑，因此在疊合影像上會產生 50% 的黑白色差，只需要利用人類視覺系統就可以輕易解讀機密訊息。

$$C^0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}_{2\times 2}, \qquad C^1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}_{2\times 2} \tag{1}$$

黑白兩色的拆解和分享規則，無法呈現灰階或彩色影像中的色彩變化，因此傳統視覺密碼學只能應用於黑白影像。Hou (2003) 應用顏色分解與合成 (color decomposition / composition) 和數位半色調 (digital halftone) 技術，提出適用於彩色機密資訊的分享方法，使得視覺密碼的研究得以由黑白影像延伸至灰階與彩色的影像上。

二、像素不擴展技術

在 (*k*, *n*)-threshold 中，每一個像素點都會被擴展成數個子像素 (sub-pixel)，這種分享方法稱為像素擴展 (pixel-expansion)，雖然像素擴展可以造成疊合影像上有比較好的還原品質，但擴展後的分享影像將會造成網路頻寬與儲存空間的負擔。

Ito等 (1999) 從機率論的觀點，重新詮釋 (*k*, *n*)-threshold 的分享矩陣 (C^0、C^1)，提出一個像素不擴展的視覺密碼技術。Ito 等認為分享矩陣中的每一行代表一種視覺密碼的分配方式，而這一行中的每一列則代表每一個參與者所分配到的顏色。我們以公式 1 的 (2, 2)-threshold 為例，當機密影像的像素點是黑色時，從 C^1 矩陣中任選一行向量$\begin{bmatrix}1\\0\end{bmatrix}$或$\begin{bmatrix}0\\1\end{bmatrix}$，並將行向量中的值依序分配到兩張分享影像上。此時，在這兩張分享影像的相同像素點位置上，將會分配到相異的顏色，所以疊合後的結果一定是出現黑色；反之，當機密影像的像素點是白色時，則是從 C^0 矩陣中隨機取出一個行向量$\begin{bmatrix}1\\1\end{bmatrix}$或$\begin{bmatrix}1\\1\end{bmatrix}$，於是這兩張分享影像都會被分配到相同的顏色，並且於疊合後出現黑色或白色的機率各半 (50%)，因此可以產生出視覺密碼所需要的色差效果。

Hou 等 (2001) 利用顏色分解與合成、降低對比和半色調技術，提出了一種適用於灰階與彩色影像的不擴展機密分享技術。Hou 等的做法是利用分色技術，將彩色機密影像轉換成青、洋紅和黃三張連續色調的分色影像。再透過降低影像的對比與亮度，來讓分色影像中灰階值都調高到 127 以上，使得經半色調技術所產生的黑白二元影像，在每一個 2×2 的像素區塊內有兩個以上的黑點被產生，以滿足疊合分享影像時的情況。最後使用以 2×2 像素區塊為分享單位的視覺密碼模型來製作分享影像，達到不擴展分享影像的結果。

Yang (2004) 也是從機率的角度，針對 (2, *n*)-threshold 和 (*n*, *n*)-threshold 提出建構不擴展分享矩陣的新方法。但是在 Ito 等與 Yang 的分享方法中，皆是利用隨機挑選的方式來產生不擴展的分享影像，因為隨機亂度的關係，無法確保在分享影像上的每一個小區域內，顏色分佈都一定會保持在 50% 的黑和 50% 的白。因此，也就無法保證疊合影像上每一個小區域內的白色區域，在疊合後的顏色分布一定會是 50% 的黑和 50% 的白，這會使得疊合影像上白色區域的顏色分佈產生局部的變異，造成凌亂的視覺效果。因此 Tu 與 Hou (2007) 提出了多點加密法，即是一次選取機密影像上的連續 *m* 個白點 (黑點)作為加密對象，使得分享影像上每 *m* 個白點 (黑點) 的區域中出現黑色的機率都相等，以確保在分享影像上每一個小區域內的顏色亂度會受到控制，因此在疊合影像上可以得到較佳的視覺效果。

三、漸進式視覺密碼

傳統 (*k*, *n*)-threshold 視覺密碼的解密概念是一種「非有即無」的二元狀態，只有在

重疊 k 張或 k 張以上的分享影像時，疊合影像上才能產生足夠的色差，並且能夠以肉眼辨識出機密訊息的內容；若分享影像的數目少於 k 張時，疊合影像上只會呈現出亂碼的形態，無法顯示任何機密訊息的內容。漸進式視覺密碼不同於傳統視覺密碼，它的概念是在疊合較少張的分享影像時，只能顯現出粗略的機密影像資訊，當疊合的分享影像愈多，所還原的機密資訊會愈來愈清晰。這個概念可以延伸視覺密碼的應用性，使得視覺密碼的解密過程由過去非有即無的分享模式，轉變為逐步還原資訊的解密方式，因此增加機密分享機制的彈性。

Fang 與 Lin (2006) 首先提出一個應用於視覺密碼的漸進式分享方法，他們的作法是將機密影像的每一個黑色像素點，擴展為 2×2 的全黑影像區塊；而白色像素點則隨機擴展為兩白兩黑的影像區塊。在產生分享影像時，則根據擴展影像區塊中的顏色分布，隨機分配 0～2 個黑點到對應的分享影像區塊中。不過其分享模型是以像素擴展為基礎，因此會造成儲存空間和傳輸頻寬的浪費。當分享影像疊合時，因為分享影像上的影像區塊是隨機挑選，所以不能保證機密影像上的黑色像素，在疊合影像上也是 4 點全黑，而白色像素也有可能無法被疊合成兩白兩黑，所以在疊合影像上代表黑 (白) 的影像區塊，都有可能產生黑白密度不均勻的問題。更嚴重的問題是在每一張分享影像上，對應於機密影像的黑色部分出現黑點的機率，大於機密影像的白色部分，以致於在分享影像上會洩露出機密內容的邊緣輪廓，造成安全性的問題。

侯與官 (2011) 為了改善 Fang 與 Lin 在像素擴展、還原品質與安全性的問題，於是提出一個基於機率分配的像素不擴展之漸進式視覺密碼。其做法是採用兩個 $n\times n$ 的矩陣 (表 1)，分別代表白色像素與黑色像素的分享矩陣，其中矩陣內的每一列代表一種分享方式，而每一行則是代表每一個參與者被分配的內容。當要產生分享影像前，先隨機選取得一個亂數值 k ($1 \leqq k \leqq n$)，如果機密影像的內容為白色，是取出 C^0 矩陣中第 k 列的值，並依序分配給每一張分享影像；反之，黑色部分則是利用 C^1 矩陣，以同樣的方式進行加密。

表 1：侯與官的非擴展且漸進式之分享模型

□ (White pixel)	■ (Black pixel)
$C^0 = \begin{bmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 0 \end{bmatrix}_{n\times n}$	$C^1 = \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}_{n\times n}$

在他們的分享方法中，機密影像上的每一個像素點，在分享影像上也是以一個像素點來代表，因此分享影像的大小與機密影像相同。此外，在分享影像上的每一個像素點，出現黑點的機率都相等 ($=1/n$)，因此在每一張分享影像上都不會產生機密影像的輪廓。最後，由於該方法是透過隨機亂數來選取分享矩陣的列向量，因此針對機密影像

上的白點部份，如果它在某一張分享影像上出現黑點，它也會在其它每一張分享影像的相同位置出現黑點，因此重疊分享影像後，仍是在相同的位置上出現黑點；然而機密影像上的黑點部份，卻是在分享影像上的相異位置出現黑點，因此隨著重疊的分享影像數目增加，黑點的數目將會逐漸增加。當疊合所有的分享影像後，機密影像為白色的部份仍然保持 $1/n$ 的機率為黑色，而黑點部份則是被疊合成全黑，因此在疊合影像上會出現 $(n-1)/n$ 的色差對比。因此，侯與官的研究解決了 Fang 與 Lin 在分享影像大小、安全性、色差對比和黑點還原為全黑等方面的缺點。

四、具有優先權等級的視覺密碼

優先權概念是源自於電腦作業系統的排程問題，因為處理器 (processor) 無法同時處理多個行程 (processes)，所以處理器根據行程的執行時間或等待次數等資訊，來決定下一個被處理的行程 (Silberschatz et al. 2004)。隨著網際網路的發展，優先權概念被應用於排除網路壅塞 (congestion reduction) 等問題上 (Panko 2009)。例如當網路流量大於乙太網路 (Ethernet) 所能乘載時，將會造成資料遞延或遺失等問題的產生。因此新的網路協定中，是在網路訊框 (frame) 中加入優先等級欄位，使得優先權較高的資料不會受到網路擁塞而產生遞延，藉此增加資訊傳輸的彈性與效率。由於電腦影像的像素值是利用一個位元組 ($b_7 \cdots b_0$) 來儲存，但是在位元組中，每一個位元的權重皆不相同，因此 Chen 與 Lin (2005) 和 Wang 與 Shyu (2007) 皆透過這個特性，將優先權等級的概念帶入機密資訊分享的研究。

Chen 與 Lin 是延伸 Thien 與 Lin (2002) 的 (r, n)-threshold 的做法，將門檻值擴充為 k 個 r_i (其中 $r_1 \leqq r_2 \leqq \cdots \leqq r_k$)。其作法是同時取出機密影像上的 r ($r = r_1 + r_2 + \cdots + r_k$) 個像素點，並根據這些像素點的灰階值依位元平面由高至低的順序進行位元重組，產生 r 個新像素值。在資料加密時，是將這些新像素值分別填入 k 個多項式的 r 個係數上，每一位參與者依其 ID 分別產生 k 個函數值，成為他所擁有的分享影像上的像素值。當取得較少的分享影像時，只能解譯出每一個原始像素的較高位元平面值，而看到失真的機密影像。隨著分享影像的增加，機密影像將會愈來愈清晰，當取得 r_k 張以上的分享影像時，將可解譯出無失真的機密影像內容。Wang 與 Shyu 也是依位元平面重要性遞減的特性，將灰階影像的每一個像素點，根據位元平面切割成 j 個區段，藉此來進行漸進式機密資訊傳輸。然而 Chen 與 Lin 和 Wang 與 Shyu 的做法都不能透過直接疊合分享影像的方式來進行解密，並且需要電腦輔助才能還原機密資訊，因此無法應用於視覺密碼的應用中。

在 Naor 與 Shamir (1995) 所提出的機密資訊分享機制中，分享影像間並沒有權限等級的概念，每一張分享影像對於影像還原的貢獻度沒有任何差異。因此 Hou (2003) 基於管理的便利性，首先提出具備優先權等級的視覺密碼分享方法。Hou 的分享方法是利用隨機選擇的黑白遮罩 (Mask)，以及機密像素的青、洋紅、黃三個分色半色調值 ($CH_{i,j}$、$MH_{i,j}$、$YH_{i,j}$) 來產生四張分享影像，其中的一張是黑白的遮罩，用來掩蓋不希望出現在重疊影像中的顏色，另外三張分別代表青、洋紅、黃三個分色影像 (S_C、S_M、S_Y)。

在 Hou 的作法中，遮罩影像 (圖 1.(a)) 可以遮住我們不希望它出現的顏色，對於機密影像還原的重要性，顯然要比三個分色影像 (圖 1.(b)～1.(d)) 更為重要。因此依照分享影像的重要性，我們可以將遮罩影像交由一位管理者保管，而三張分色影像則交由其他三位從屬者保管。當要還原機密影像時，如果疊合影像上缺少了遮罩影像，在疊合影像上將會出現雜色來混淆機密影像的輪廓，而無法顯示出機密影像內容 (圖1.(h))，因此 Hou 的作法提供了一層特權或稽核的機制。反之，當管理者參與機密資訊的解譯時，如果疊合影像上只是缺少了某一個、甚至某兩個分色影像，雖然在疊合影像上無法正確地顯示機密影像的色彩，卻依然可以顯示出機密影像內容 (圖1.(e) ～1.(f))，因此在 Hou 的作法中也提供了一種漸進式還原機密影像的機制。[1]

圖1：(a～d) 四張分享影像，(e) 疊合Mask和青色分享影像，(f) 疊合Mask、青和洋紅色分享影像，(g) 疊合四張分享影像，(h) 移除Mask後的疊合影像

雖然 Hou 的作法可以提供具有權限等級的漸進式視覺密碼，但是 Hou 的作法仍有兩個限制，首先是分享影像是以像素擴展為基礎，這將會造成儲存空間與傳輸時間的浪費。第二，權限的劃分只有限定於管理與從屬兩層，並且只能分享成四張分享影像，因此無法適用於其他狀況。

Yang 與 Chen (2007) 則是基於機密影像的像素點有不同的重要性，提出一個考量優先權等級的機密資訊分享方法。他們的基本概念是認為影像中的邊緣輪廓對於影像內容的辨識非常重要，因此必須以較多的像素點來表示 (擴展倍率較大)，然而非輪廓區域則用較少的像素點來表示 (擴展倍率較小)。基於這個概念，分享影像上像素擴展的倍率不

[1] 本研究所有的彩色影像內容可至下述網址 http://mail.im.tku.edu.tw/~ychou/nnPPVSM.rar 下載

再是一個固定值，而是一個隨像素的重要性而變動的倍率。Yang 與 Chen 首先利用 Sobel 的影像邊緣測試法 (Sobel edge detector) 來找出機密影像的輪廓，將影像輪廓上的像素點視為擁有較高的權限等級，而非輪廓上的像素點則是較低權限，然後根據不同的權限等級來製作對應的分享影像。雖然 Yang 與 Chen 的作法可以在較小的擴展倍率上維持較佳的還原品質，但是他們的分享方法中也有幾項缺點，第一，權限等級的區分是根據像素點的重要性來設定分享影像上不同區域的擴展倍率，雖然可以彰顯出影像中不同的重要性和細膩程度，但是在不同的分享影像間，仍然無法區分權限與重要性。第二，分享方法仍是以像素擴展為基礎，而且機密影像與分享影像之間的像素對應 (mapping) 的計算變得非常複雜。

本研究是基於以往漸進式與不擴展視覺密碼的研究，提出漸進式且具有權限等級的不擴展視覺密碼分享方法，稱之為 (n, n)-PPVSM 機密分享機制。在 (n, n)-PPVSM 的分享機制中，機密影像的內容將會被分配到 n 張不擴展大小的分享影像上，每一張分享影像都隸屬於不同的權限等級。因此在還原機密資訊時，當疊合到較高權限的分享影像時，所揭露出的機密影像將會較為清晰；反之，所還原的機密影像就是較為模糊。

參、非擴展且具有優先權等級的漸進式分享模式

參在以往漸進式視覺密碼的研究中，每當在疊合影像上重疊另一張分享影像時，就會增加一個固定的黑白對比來達成漸進式解密的目的，因此對於機密影像的還原，每一張分享影像都擁有相同的復原能力。然而在現實生活中，機密分享的參與者可能會有不同的重要性，如果能夠賦予分享者不同的優先等級，使得權限較低分享者，對於機密影像的還原只有小幅度的貢獻，只有權限較高的分享影像才能顯示出更多機密影像的細部紋理。因此具有優先等級的漸進式分享模式，將可反應參與者在解密過程的重要性。

在視覺密碼的分享架構中，機密影像的還原是透過分享影投影片的重疊，而這個重疊的動作相當於邏輯運算上的 OR 運算。當重疊多張分享影像時，只要有一張分享影像的像素點內容為黑色 (1) 時，在疊合影像上就會顯示黑色，只有在每一張分享影像上的某一點像素都是白色 (0) 時，才會在疊合影像的那一個像素上顯示出白點。針對一張黑白影像，通常人們只會注意到影像中的黑色部份，因為它凸顯了機密影像的「真正」內容，而將白色的部份認為是影像中的背景，通常人們對於它是視而不見的。基於上述的觀察，我們可以調整分享影像中出現黑點的機率，讓權限等級比較高的分享影像中出現黑色的機率比較大，也就是在疊合時可以貢獻出比較多的黑點。反之，權限等級比較低的分享影像中出現黑色的機率比較小，也就是在疊合時能夠做出貢獻的黑點比較少。因此疊合較高權限的分享影像可以產生較高的黑白色差，也就是可以比較快速地呈現出機密影像的內容，達成依據參與者的權限來左右還原機密影像速率的目標。

在本研究中，我們假設 n 個機密分享的參與者都擁有不同的權限等級，我們設計了兩個 $m \times n$ 的矩陣 (C^0 和 C^1)，分別代表機密像素為白色或黑色的分享矩陣 (表 2)，矩陣中的每一行代表每一個參與者被分配的內容，而每一列則代表一種可能的分享方式。

假設參與者 k 的權限值為 k，則分享矩陣的第 k 行出現 1 的機率就設為 k / m，其中，$m=\sum_{k=1}^{n} k = n(n+1)/2$，使得權限等級比較高的分享影像 ($WS^k$, $k=1, ..., n$) 中出現黑色的機率比較大。在 C^1 矩陣中每一行的 1 都分配在不同的列上，而 C^0 矩陣中每一行的 1 則儘可能的出現在相同的列上。使得分享影像上因 C^1 矩陣所產生的相關像素，在疊合時出現黑點的機率會逐漸增加，而分享影像上因 C^0 矩陣所產生的相關像素，在疊合時出現黑點的機率則保持不變，因而擴大疊合影像上黑白像素間的色差，並在疊合的過程中逐漸顯現機密內容。由於在每一張分享影像上出現黑點的機率不同，使得還原機密影像中黑點的速率也不同，因此可以表現出不同權限的特性。

表 2： (n, n)-PPVSM的分享模型

□ (White pixel)	■ (Black pixel)
$C^0 = \begin{bmatrix} 1 & 1 & 1 & \cdots & \cdots & 1 \\ 0 & 1 & 1 & \cdots & \cdots & \vdots \\ \vdots & 0 & 1 & \cdots & \cdots & \vdots \\ \vdots & \vdots & 0 & 1 & \cdots & \vdots \\ \vdots & \vdots & \vdots & 0 & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & 1 \\ \vdots & \vdots & \vdots & \ddots & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 \end{bmatrix}_{\frac{n(n+1)}{2}\times n}$	$C^1 = \begin{bmatrix} 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & \cdots & 0 \\ \vdots & 1 & 0 & \cdots & \cdots & 0 \\ \vdots & 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & 0 & 1 & \ddots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & 1 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 1 \end{bmatrix}_{\frac{n(n+1)}{2}\times n}$

當要產生分享影像時，使用隨機亂數取得一個 $1 \sim m$ 之間的 t 值，如果是要拆解機密影像的白色部分，則將 C^0 矩陣中第 t 列上的值依序分配給每一張分享影像，也就是第 t 列的第 1 個值 ($C^0(t, 1)$) 分配給 WS^1，第 2 個值 ($C^0(t, 2)$) 分配給 WS^2，…，第 n 個值 ($C^0(t, n)$) 分配給 WS^n；反之，如果是要拆解機密影像的黑色部分，則利用 C^1 矩陣以同樣的方式進行加密，因而可以產生出 n 張相異權限的分享影像，詳細的分享影像製作流程請參考圖 2。

根據上述的演算法流程，我們可以得知 (n, n)-PPVSM 執行拆解機密影像的顏色，並將它分配到分享影像上的次數，是與機密影像的大小 ($W \times H$) 和機密分享的參與者個數 (n) 成正比，也就是說，整體演算法的時間複雜度是 $O(nWH)$。在空間複雜度上，分享矩陣 C^0 和 C^1 所需要的空間分別是 $n^2(n+1)/2$，每一張分享影像 WS^k 所需要的空間是 WH。通常影像的長寬大小遠大於參與分享機密的人數 ($W >> n$, $H >> n$)，因此，整個 (n, n)-PPVSM 演算法的空間複雜度為 $O(n^3 + nWH) \approx O(nWH)$。

(*n*, *n*)-PPVSM Algorithm:

Input：(1) 一張經半色調處理的機密影像 P，其大小為 $W \times H$

(2) 參與機密分享的參與者人數 n

(3) 分享矩陣 C^0、C^1

Output：n 張權限等級相異的分享影像 WS^k，$k = 1, 2, ..., n$

Process：

```
1    for   i ← 1 to W   do
2        for   j ← 1 to H   do
3            t ← Random number ( 1 ≦ t ≦ n(n+1)/2 )
4            if   P(i, j) is black
5                for   k ← 1 to n
6                    WS^k(i, j) = C^1(t, k)
7            else
8                for   k ← 1 to n
9                    WS^k(i, j) = C^0(t, k)
```

圖 2：(n, n)-PPVSM的分享模型

由於每一張分享影像的權限等級都不相同，假設部份參與者所組成的子集合 T 中，最大的權限等級為 M，所有權限等級的加總為 S，則疊合他們所擁有的分享影像後，機密影像中的白點部份有 M / m 的機率出現黑色，而黑點部份則有 S / m 的機率出現黑色，因此在疊合影像上會出現 $(S-M) / m$ 的黑白色差。以重疊兩張分享影像為例，如果重疊最低權限的 WS^1 和 WS^2，機密影像的白色和黑色部分分別有 $2 / m$ 和$3 / m$ 的機率被疊合出黑點，因此在疊合影像上只會產生 $1 / m$ 的黑白色差。反觀 WS^{n-1}、WS^n 重疊後，機密影像的白色部分有 n / m 的機率會被疊合出黑點，而黑色部分被疊合出黑點的機率則是提升到 $(2n-1) / m$，在疊合影像上會產生 $(n-1) / m$ 的色差對比，所以權限等級愈高的分享影像被疊合時，機密影像的還原效果愈好。隨著被疊合分享影像的數目增加，機密影像的白色部份被疊合出黑點的機率增加比較慢，而黑色部份則是增加比較快，因此黑白色差對比愈來愈明顯。當疊合所有的分享影像後，機密影像的白點部分被疊合出黑點的機率維持在 n / m，而黑點部分則是會被疊合出全黑，因此在疊合影像上會產生 $1-n / m=(n-1) / (n+1)$ 的黑白色差，所以可以清晰地顯示機密影像的內容。

在分享影像的安全性方面，由於 C^0 和 C^1 分享矩陣的第 k $(1 \leqq k \leqq n)$ 個行向量中都只有 k 個 1，因此無論機密像素是黑或白，第 k 張分享影像上的每一個像素點都只有 k / m 的機率呈現出黑色，不會因為機密影像上不同的顏色，而在分享影像上形成色差。使得攻擊者無法由任一張分享影像上的黑白分配，來反推機密影像上的顏色分布。除此之外，由於分享影像上的像素點顏色是透過隨機亂數來選取，隨機亂數將可以確保在每一張分享影像的黑白分佈是均勻的，黑點不會集中在機密影像的黑色部份，白點也不會集中在機密影像的白色部份，因而不會在分享影像上顯露出機密影像的邊緣輪廓。綜合上

述兩點，所以我們足以推論任一張分享影像都能夠視為是安全的。

當機密影像的型態轉變為彩色影像時，我們可以利用 Hou (2003) 所提出的顏色分解和半色調技術，產生出三張分色影像 (S_C、S_M、S_Y)。然後依照上述的方式，針對每一張分色影像製作出 n 張分色分享影像 (Share_C_1 ~ Share_C_n、Share_M_1 ~ Share_M_n、Share_Y_1 ~ Share_Y_n)，最後再運用色彩合成的概念，將三張分色分享影像 (Share_C_k、Share_M_k、Share_Y_k) 疊合後，即可得到具有權限等級為 k 的雜訊式彩色分享影像。

就安全性而言，在第 k 張分享影像上的每一個像素點產生出三個分色 (青、洋紅、黃) 點的機率皆為 (k / m)，而不會產生這三個分色 (白點) 的機率則分別為 (($m-k$) / m)。於是在第 k 張分享影像上出現黑點的機率是 (k / m)^3；出現紅、藍、綠點的機率皆是 (k / m)$^2\times$(($m-k$) / m) = ($k^2\times(m-k)$) / m^3；出現青、洋紅、黃點的機率皆為 (k / m)$\times$(($m-k$) / m)^2 = ($k\times(m-k)^2$) / m^3；而白點的出現機率則是 (($m-k$) / m)^3。由於顏色的分配是透過隨機亂數，因此彩色分享影像上會呈現出不規則色點分佈結果，而不會洩露出機密影像的資訊，所以彩色分享影像也可視為是安全的。

此外，我們利用 Hsu 與 Hou (2005) 所提出的改進式正規化相關係數法 (Normalized Correlation，NC) 值，來衡量重疊 r 張分享影像後與原影像間的相似程度，其定義如公式 2 所示。該公式的用意是計算原始機密影像 (I) 上的黑色點，在疊合影像上 (I') 上亦為黑色的比率，乘上原始機密影像 (I) 上的白點，在疊合影像上 (I') 上亦為白點的比率。NC 值是一個介於 0～1 之間的值，當 NC 值越接近 1，表示兩張影像的相似程度越高；NC 值越接近 0，則表示影像間的相似程度越低。

$$NC=\left[\frac{\sum_i\sum_j I(i,j)I'(i,j)}{\sum_i\sum_j[I(i,j)]^2}\times\frac{\sum_i\sum_j(1-I(i,j))(1-I'(i,j))}{\sum_i\sum_j[(1-I(i,j))]^2}\right]^{1/2} \tag{2}$$

因此，假設部份參與者所組成的子集合中，最大的權限等級為 M，所有權限等級的加總為 S，則疊合他們所擁有的分享影像後，機密影像中的白點部份有 $1-M/m$ 的機率出現白色，而黑點部份會有 S/m 的機率出現黑色，因此疊合影像上的 NC 理論值會趨近於 $\sqrt{S(m-M)}/m$。以 6 位參與者為例 (m=21)，若 T_1={1, 2}，則 S_1=3、M_1=2、NC_1=0.36；若 T_2={5, 6}，則 S_2=11、M_2=6、NC_2=0.61；若 T_3={1, 2, …, 6}，則 S_3=21、M_3=6、NC_3=0.85。這些 NC 理論值在 4.1 節中圖 6～8 的實驗，均可得到驗證。

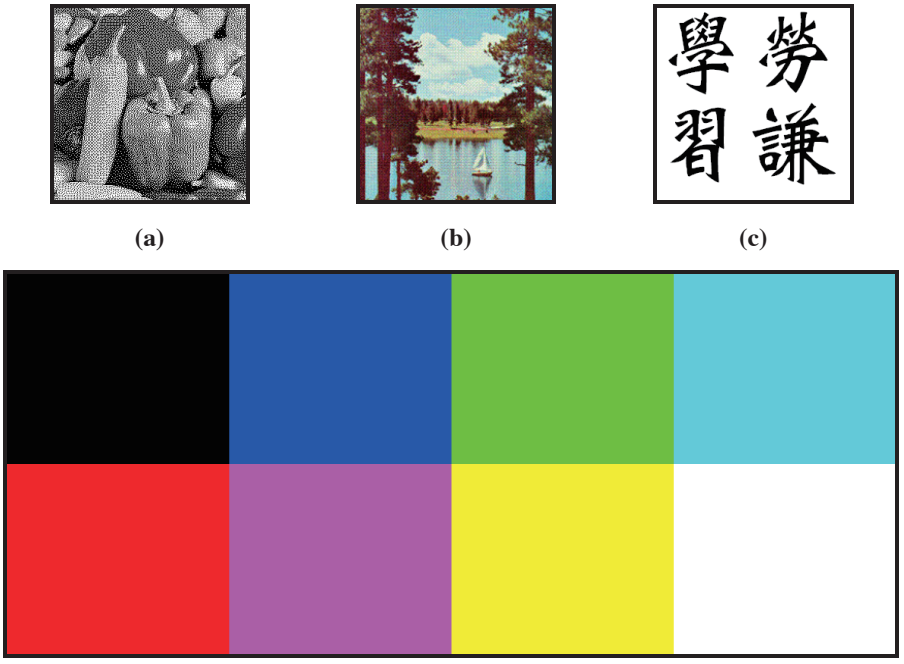
而彩色影像則依據顏色的分解與合成的概念，分別計算三個分色 NC 值後，以它們的平均值作為衡量的基準，如公式 3 所示。

$$NC_{Total}=\frac{(NC_C+NC_M+NC_Y)}{3} \tag{3}$$

肆、實驗結果與分析討論

一、實驗結果

本研究的實驗在 Windows XP 的作業系統、1.91GHz 的 AMD 處理器以及 256 MB 記憶體的環境下執行，使用 J2SE (JDK 1.6.7) 進行程式的寫作，而實驗影像大小為 256×256 且經過半色調與分色技術處理的機密影像 Pepper、Sailboat、Text，以及一張大小為 1176×504 的彩色影像 Block，如圖 3 所示。



(a) **(b)** **(c)**

(d)

圖 3：實驗影像 (a) Pepper，(b) Sailboat，(c) Text，(d) Block

以實驗影像為 Pepper 和 Sailboat 且產生 6 張分享影像為例 (圖 4～5)。在圖 4.(a) 的分享影像上，每一個像素點出現黑色的機率最低，將來它與別的分享影像疊合時，能夠貢獻的黑點最少，對於機密影像的還原能力也比較有限 (最低權限)，而在圖 4.(a) ~ 圖 4.(f) 的分享影像上，黑點的出現機率將由 1 / 21 增加到 6 / 21。依照機密分享矩陣 C^1 的設計，當某一分享影像上相應於機密影像的黑色部份被分配到黑點時，在其它分享影像上的那個位置上都會是白色，疊合這一張分享影像正好可以還原這一個位置的黑色。而圖 4.(f) 上有最多的黑點，因此它具有最大的能力來還原機密影像的黑色部份；反之，圖 4.(a) 上的黑點最少，因此它還原機密影像的黑色部份的能力就比較有限。在機密分享矩陣 C^0 的設計上，會使得在某一分享影像上產生相應於機密影像白色部份的黑點時，在其

它分享影像上的那個位置也很可能是黑色，因此就算疊合更多的分享影像，對於機密影像上白色部份增加更多黑色的速率會比較慢，也就是它會產生相對比較白的效果。

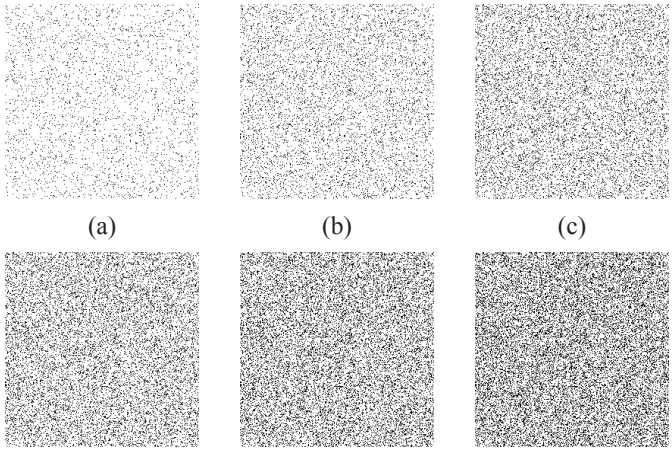


圖4：6張無意義且權限等級相異的分享影像。(a) ～ (f) 權限等級為由小到大

反觀彩色實驗影像 Sailboat 所產生的 6 張分享影像，分享影像上的像素點將會根據青、洋紅、黃三個分色的出現與否，而產生出八種 ($2^3 = 8$) 顏色變化，藉此來模擬彩色影像的色階變化，如圖 5 所示。

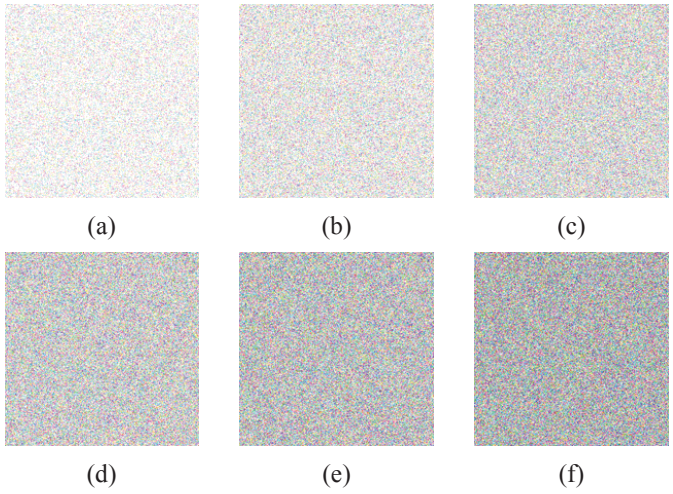


圖5：6張無意義且權限等級相異的分享影像。(a) ～ (f) 權限等級為由小到大

圖 6 是圖 4 分享影像的重疊結果，其中第一行是等級權限由小到大依序疊合的結果，而第二行則是權限依序由大到小的結果。根據圖 6 的實驗結果可以發現，在第一行

的疊合過程中，需要疊合五張分享影像後 (NC＝0.74)，才能隱約看到機密影像的輪廓；然而在第二行中，則是在疊合三張分享影像時 (NC＝0.72)，即可隱約看到機密影像的輪廓，當疊合四張分享影像後 (NC＝0.78)，即可清晰地看到機密影像的內容。由此可見，本研究所設計的機密分享矩陣確實可以達成賦予分享者不同的機密復原能力。圖 7則是根據圖 5 所產生的彩色分享影像，並依據權限等級的遞增與遞減，疊合 2～6 張分享影像的結果。從圖 7 的實驗結果中也可以發現，機密影像的還原結果是根據參與者的權限等級高低，當重疊權限較高的分享影像時，只需要 2 張分享影像即可在疊合影像上看到機密影像的內容，反觀權限較低的分享影像疊合時，則是需要較多張 (4 張) 的分享影像疊合後，才能看到機密影像的輪廓。

由於本實驗是採取漸進式的分享模式，因此隨著疊合影像的數目增加，機密影像的輪廓將會愈來愈清晰。在 (n, n)-PPVSM 的分享機制中，疊合影像上的對比色差是 (n − 1) / (n + 1)，這個結果優於傳統視覺密碼的 50% 的色差對比。根據改進式 NC 值的定義，當參與分享機密資訊的參與者人數 n＝6 時，疊合影像的 NC 理論上限值會等於 $(5 / 7)^{0.5}$，因此 NC 值將會介於 0.84～0.85 之間。從圖 6～8 中可以發現，本研究的實驗結果皆可以達到 NC 的理論上限值，顯示無論機密影像的型態為何，疊合影像上的還原品質都是最高的，並且能夠清晰地呈現出機密資訊的內容 (圖 6.(j) ~ 8.(j))。

此外，我們比較圖 6～8 左邊的實驗結果可以發現，黑白機密影像 (圖 8) 內容呈現非常規則的黑白分佈，因此只要疊合較少的分享影像，人眼就可以輕易地分辨出機密影像的輪廓。反觀灰階與彩色影像本身的顏色分佈較複雜，加上經過半色調處理後的圖案結構就更加不規律，因此圖 6、7 的左半部需要疊合比較多的分享影像後，才能夠辨識出機密影像的內容。因此，本研究所提出的 (n, n)-PPVSM分享模型，將更適合應用於需要賦予不同權限的灰階或彩色機密影像分享，並且在機密還原的過程中，疊合權限較高的分享影像可以加快機密影像的還原速率，如圖 6、7 右半部的機密資訊還原結果所示。

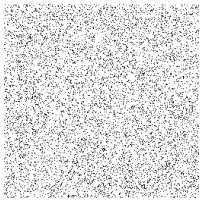
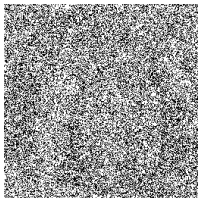
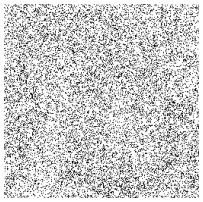
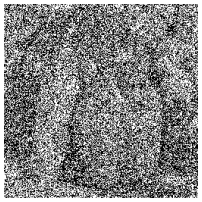
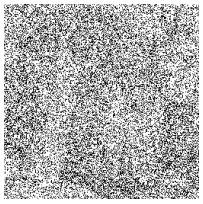
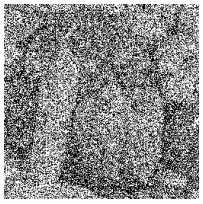
***r* = 2**		
	(a) *NC* = 0.36	(f) *NC* = 0.61
***r* = 3**		
	(b) *NC* = 0.49	(g) *NC* = 0.72
***r* = 4**		
	(c) *NC* = 0.62	(h) *NC* = 0.78
***r* = 5**		
	(d) *NC* = 0.74	(i) *NC* = 0.83
***r* = 6**		
	(e) *NC* = 0.85	(j) *NC* = 0.85

圖 6：2～6張 分享影像的疊合。

(a)～(e)權限由低到高依序疊合，(f)～(j)權限由高到低依序疊合

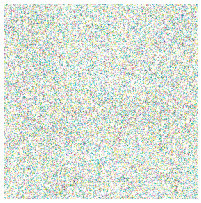
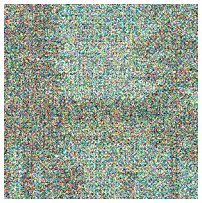
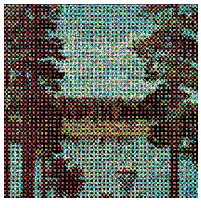
$r = 2$		
	(a) $NC = 0.36$	(f) $NC = 0.61$
$r = 3$		
	(b) $NC = 0.50$	(g) $NC = 0.71$
$r = 4$		
	(c) $NC = 0.62$	(h) $NC = 0.78$
$r = 5$		
	(d) $NC = 0.74$	(i) $NC = 0.83$
$r = 6$		
	(e) $NC = 0.85$	(j) $NC = 0.85$

圖7：2～6張分享影像的疊合。

(a)～(e)權限由低到高依序疊合，(f)～(j)權限由高到低依序疊合

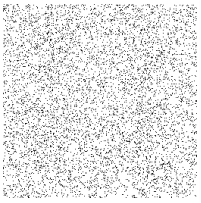
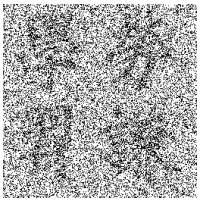
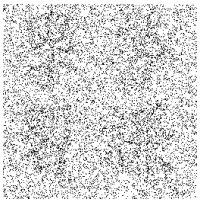
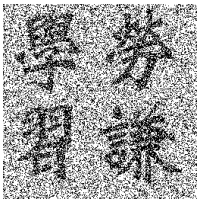
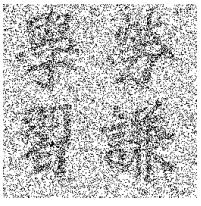
***r* = 2**		
	(a) *NC* = 0.36	(f) *NC* = 0.61
***r* = 3**		
	(b) *NC* = 0.49	(g) *NC* = 0.71
***r* = 4**		
	(c) *NC* = 0.62	(h) *NC* = 0.78
***r* = 5**		
	(d) *NC* = 0.73	(i) *NC* = 0.82
***r* = 6**		
	(e) *NC* = 0.84	(j) *NC* = 0.84

圖8：2 ~ 6 張分享影像的疊合。

(a)～(e)權限由低到高依序疊合，(f)～(j)權限由高到低依序疊合

二、安全性分析

為了驗證本研究所產生的每一張分享影像上，像素點都是根據表 2 的分享矩陣來進行分配，並且這些像素點的顏色會均勻地分布在整張分享影像上，使得分享影像呈現出雜訊式內容，而不會洩露出機密影像的邊緣輪廓，於是我們使用卡方檢定 (chi-square test) 中的適合度檢定 (goodness-of-fit test) 來進行驗證。適合度檢定是一種接受 (拒絕) 母體假設機率分配的統計檢定，它的概念是比較「觀察次數」與「期望次數」之間的差異值。如果達到差異顯著，那就表示樣本觀察資料所顯示的結果，足以拒絕母體所宣稱它滿足某一個機率分配的虛無假設 (Randles 與 Wolfe (1979))。

我們將實驗影像設定為一張大小為 1176×504 的彩色機密影像Block (圖 3.(d))，其中包含八個大小皆為 294×252 的單色區塊 (黑、藍、綠、青、紅、洋紅、黃和白)。本研究根據表 2 的分配模型，針對 Block 產生 6 張分享影像，每一張分享影像上都有 592,704 個像素。我們將分享影像上的每一種色點出現的個數與理論值整理成表 3，其中 O_k^j、E_k^j分別是代表實驗中第 k 張分享影像上的第 j 個色點 (j=黑、藍、綠、青、紅、洋紅、黃和白) 出現的個數與其對應的理論值。

第一個檢定的內容是驗證第 k 張分享影像的色點分佈，驗證黑點出現的機率是否滿足 $(k/21)^3$？紅、藍、綠點出現的機率是否都滿足 $(k/21)^2\times((21-k)/21)$？而青、洋紅、黃點出現的機率是否皆滿足 $(k/21)\times((21-k)/21)^2$？最後是白點的出現機率是否滿足 $((21-k)/21)^3$？這一個分佈檢定的卡方分佈自由度為 7，在 95% 信心水準下的臨界值為 $x_{0.05}^2(7)=14.067$，而檢定項目的虛無假設為

$$
\begin{aligned}
H_0:\ & p_{k_\text{black}}=(k/21)^3\\
& p_{k_\text{blue}}=p_{k_\text{green}}=p_{k_\text{red}}=(k/21)2\times((21-k)/21)\\
& p_{k_\text{cyan}}=p_{k_\text{magenta}}=p_{k_\text{yellow}}=(k/21)\times((21-k)/21)^2\\
& p_{k_\text{white}}=((21-k)/21)^3
\end{aligned}
$$

其檢定統計量如公式 4 所示：

$$Q=\sum_{j=1}^{8}\frac{(O_k^j-E_k^j)^2}{E_k^j} \tag{4}$$

根據表 3 的數據，我們可以得到第 1～6 張分享影像的檢定統計量分別為 3.144、7.862、5.446、11.028、6.331、3.871，這些數值均小於拒絕虛無假設的臨界值 14.067，因此沒有足夠的證據顯示在第 k 張分享影像上，色點的分佈機率不符合虛無假設 H_0 所宣稱的機率分配。另外，由於單一實驗可能會因為抽樣誤差而造成偏誤，無法證明本研究設計具有統計上的顯著性，因此我們以不同的亂數種子 (seed) 進行 1000 次上述的卡方適合度檢定測試。根據實驗結果顯示，本研究不拒絕虛無假設的次數介於 948～962 之間，因此，我們有很強的信心認為那些不服從模型假設 (也就是拒絕虛無假設) 的狀況是因為抽樣誤差所造成的，而不是在虛無假設上發生問題。

表 3：分享影像的單色點出現機率比較表

	j = Black	j = Blue	j = Green	j = Cyan	j = Red	j = Magenta	j = Yellow	j = White
$O_1{}^j$	70	1,323	1,281	25,699	1,282	25,669	25,697	511,683
$E_1{}^j$	64	1,280	1,280	25,600	1,280	25,600	25,600	512,000
$O_2{}^j$	538	4,971	4,908	46,284	4,742	46,057	46,142	439,062
$E_2{}^j$	512	4,864	4,864	46,208	4,864	46,208	46,208	438,976
$O_3{}^j$	1,731	10,361	10,455	62,253	10,168	62,011	62,283	373,442
$E_3{}^j$	1,728	10,368	10,368	62,208	10,368	62,208	62,208	373,248
$O_4{}^j$	4,158	17,320	17,514	74,287	17,710	73,616	74,084	314,015
$E_4{}^j$	4,096	17,408	17,408	73,984	17,408	73,984	73,984	314,432
$O_5{}^j$	7,853	25,699	25,643	82,092	25,520	82,313	81,829	261,755
$E_5{}^j$	8,000	25,600	25,600	81,920	25,600	81,920	81,920	262,144
$O_6{}^j$	13,808	34,601	34,653	86,691	34,576	86,680	86,168	215,527
$E_6{}^j$	13,824	34,560	34,560	86,400	34,560	86,400	86,400	216,000

上述的檢定，從巨觀的角度驗證了本研究所產生的每一張分享影像上的顏色會均勻地分布，使得分享影像上呈現出雜訊式的內容，因而不會洩露出機密影像的邊緣輪廓。不過機密影像 Block 的內容是由八個單色色塊所組成的，如果在某一 (幾) 個單色塊內的色點分布不均勻，也有可能會產生機密資訊內容被揭露的疑慮。因此我們想從微觀的角度驗證分享影像上的每一個單色區塊，其內容也符合分享模型的機率分配。因此我們的第二個檢定是將分享影像切割為不交集的 64 個區塊 (大小皆為147×63)，再使用上述的卡方適合度檢定進行實驗。由於機密影像被切割為 64 個區塊，並且在每一個區塊上的某一個像素點上，都會有出現 8 種不同顏色的可能性，因此這一個假設檢定的自由度為 441 (df =(64-1)×(8-1))，臨界值在 95% 的信心水準下為 $x_{0.05}{}^2(441)=490.96$。

根據實驗數據顯示，六張分享影像在 95% 信心水準下的檢定統計量分別是 433.77、382.28、394.71、428.50、442.01、439.15，均小於拒絕虛無假設的臨界值 490.96，因此我們沒有足夠的證據顯示在分享影像上的每一個影像區塊中，單色點的分佈機率不符合虛無假設。然後我們再以不同的亂數種子進行上述實驗 1000 次，發現不拒絕虛無假設的次數介於 929～942 之間，因此我們有很強的信心宣稱本研究所提出的分享模型，無論在任何一張分享影像上，每一個小的影像區塊內的色點分佈比例也都符合 H_0 的機率分佈。

此外，我們以第 1 張分享影像為例，藉此來觀察分享影像上是否會產生機密影像的邊界或色點集中的現象。從圖 9 的放大影像中可以發現，我們無法看出哪一種色點在哪一個單色的色塊中出現的個數較多，或是在分享影像上發現這 8 個色塊的邊界。這個結果顯示了本研究所產生的每一張分享影像上的顏色都會均勻地分布，不會出現機密影像的邊緣輪廓。

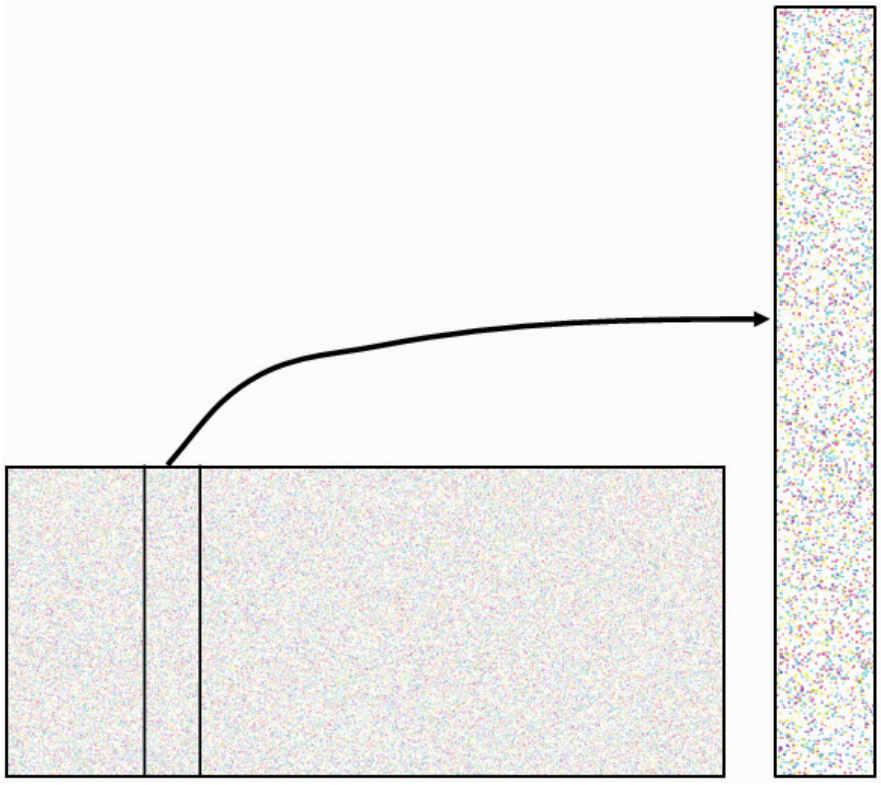


圖9：第 1 張分享影像的放大圖

伍、結論

依由於電腦科技日新月異，以及網際網路的盛行，使得大部分資料都轉為數位的方式儲存，並且藉由網際網路來傳遞與分享資訊。然而網際網路是一個開放的環境，因此所傳遞的資訊可能會遭受截取或盜用等安全性問題。為了確保機密資訊能安全地傳遞，一般是利用密碼學技術來加密機密資訊，被加密過的資訊通常不容易在短時間內被破解，因此可以降低資訊被擷取或被竄改的可能性。但是傳統密碼學的加解密都須要經過極為繁複的數學演算過程，所以必需借助電腦設備才能解決龐大的運算動作。而視覺密碼的優點在於解密時，不須要任何複雜的運算過程，只需要經由分享影像的疊合，並透過人類視覺系統即可辨識秘密資訊，因此可以降低資訊解密的複雜度。

傳統視覺密碼的分享方法是植基於 (k, n)-threshold 機制，當疊合大於或等於 k 張分享影像時才能解譯機密資訊，不然就無法得知機密資訊的內容。漸進式視覺密碼則是不同於以往「非有即無」的機制，其解密機密資訊的品質是決定於所擁有分享影像的數目，當獲得愈多的分享影像時，機密影像的還原品質愈好。不過在現行的漸進式視覺密碼的分享機制下，卻無法根據參與者的重要性來賦予適當的權限等級，藉此彰顯機密資訊還

原的差異化能力，因而缺乏應用上的彈性。

本研究設計出漸進式且具有權限等級的不擴展視覺密碼分享方法，稱之為 (n, n)-PPVSM 分享機制。相較於其他學者的研究結果，(n, n)-PPVSM 的分享機制具備下列幾項優點：(1) 每一張分享影像各自隸屬於一個權限等級，對於機密影像具備不同的還原能力。(2) 當重疊所有的分享影像後，疊合影像的色差對比是 (n－1) / (n＋1)，這個結果優於傳統視覺密碼的 50% 的色差對比。(3) 權限機制更適合應用於灰階和彩色影像的漸進式分享環境中，在疊合影像上可以清晰地辨識出機密內容。(4) 本研究的分享方法是基於像素不擴展，因此分享影像的大小與機密影像相同。未來我們將研究一種新的分享機制，當疊合的權限總和高於某一個門檻值時才開始顯現漸進式的特質，低於這個門檻值時重疊影像上就仍然顯示亂碼的外觀，使得具有權限等級的機密資訊分享更有彈性。

致謝

本論文為中華民國行政院國家科學委員會補助之研究計畫 NSC99-2221-E-032-051 的部份研究成果，謹此致謝。

參考文獻

1. 侯永昌、官振宇，2011，『像素不擴展之漸進式視覺密碼』，電子商務學報，第十三卷．第一期：99～116頁。
2. Chen, S. K. and Lin, J. C.“Fault-tolerant and progressive transmission of images,”*Pattern Recognition* (38:12), December 2005, pp. 2466-2471.
3. Fang, W. P. and Lin, J. C.“Progressive viewing and sharing of sensitive images,”*Pattern Recognition and Image Analysis* (16:4), 2006, pp. 638-642.
4. Hou, Y. C.,“Visual cryptography for color images,”*Pattern Recognition* (36:7), July 2003, pp. 1619-1629.
5. Hou, Y. C., Chang, C. Y., and Hsu, C. S.“Visual cryptography for color images without pixel expansion,”*in Proceeding of CISST'2001*, Vol. I, 2001, pp. 239-245.
6. Hsu, C. S. and Hou, Y. C.“Copyright protection scheme for digital images using visual cryptography and sampling methods,”*Optical Engineering* (44:7), July 2005, pp. 077003-1-077003-10.
7. 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.
8. Naor, M. and Shamir, A.“visual cryptography,”*in Advances in Cryptology- EUROCRYPT '94, LNCS 950, Springer-Verlag*, 1995, pp. 1-12.

9. Panko, R. R. *Business Data Networks and Telecommunications* (7th ed.), Pearson Prentice Hall, 2009.
10. Randles, R. H. and Wolfe, D. A. *Introduction to the Theory of Nonparametric Statistics,* Wiley, New York, 1979.
11. Silberschatz, A., Galvin, P. B., and Gagne, G. *Operating System Concepts* (7th ed.), John Wiley & Sons Inc, 2004.
12. Thien, C. C. and Lin, J. C. "Secret image sharing," *Computers & Graphics* (26:5), October 2002, pp. 765-770.
13. Tu, S. F. and Hou, Y. C. "Design of visual cryptographic methods with smooth-looking decoded images of invariant size for gray level images," *Imaging Science Journal* (55:2), June 2007, pp. 90-101.
14. Yang, C. N. "New visual secret sharing schemes using probabilistic method," *Pattern Recognition Letters* (25:4), March 2004, pp. 481-494.
15. Yang, C. N. and Chen, T. S. "Visual secret sharing scheme: prioritizing the secret pixels with different pixel expansions to enhance the image contrast," *Optical Engineering* (46:9), September 2007, pp. 097005-1-097005-19.
16. Wang, R. Z. and Shyu, S. J. "Scalable secret image sharing," *Signal Processing: Image Communication* (22:4), April 2007, pp. 363-373.