Journal of e-Business
第十四卷　第四期　2012 年 12 月（pp.575～596）

植基於區塊漸進還原之非擴展式視覺機密分享 [1]

侯永昌 [a]　官振宇 [b,*]　蔡志豐 [b]
[a] 淡江大學資訊管理系　[b] 國立中央大學資訊管理系

摘要

在目前漸進式視覺機密分享（PVSS）的研究中，Wang et al.（2007）和 Wang（2009）都是採用逐步還原不同機密影像區塊的方式來進行，不過在他們所提出的分享模式中，都會產生分享矩陣的設計沒有規律性、浪費儲存空間、還原影像品質不佳，以及不適合應用於灰階或彩色影像等缺點。為了解決上述的缺點，本研究提出一個應用影像區塊進行漸進式還原的非擴展式視覺機密分享模型，稱之為 Block-based Progressive Visual Secret Sharing（BPVSS）。其做法是將機密影像切割成 n 個不重疊的影像區塊，當重疊 t（$2 \le t \le n$）張投影片後，疊合影像上會有 t 個影像區塊內的機密內容會被完全還原。相較於其他學者的研究成果，本研究具備下列幾項優點：(1) 本研究的分享模型的概念簡明、容易實作，並且參與機密資訊分享的人數不會受到限制。(2) 在分享投影片為雜訊式的內容時，還原影像上可以產生出 50% 的黑白色差，使得機密資訊能清楚地為人眼所辨識。(3) 分享投影片也可以轉換成有意義的偽裝影像，因此可以提高分享投影片的安全性，並且在偽裝影像與還原影像上皆有 25% 的黑白色差。(4) 本研究的機密影像適用於灰階與彩色影像。(5) 每一張分享投影片大小皆與機密影像相同，不需要擴展。

關鍵詞：視覺機密分享、漸進式視覺機密分享、機密影像區塊、藏密學技術

Block-based Progressive Visual Secret Sharing

Young-Chang Hou[a]　Zen-Yu Quan[b]　Chih-Fong Tsai[b]
[a] Department of Information Management, Tamkang University
[b] Department of Information Management, National Central University

Abstract

In the related works of progressive visual secret sharing (PVSS), Wang et al. (2007)

[1] 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，並竭誠感謝 M. C. Liao 於論文初稿期間提供寶貴意見，使得本論文更臻完善，謹此致謝。

[*] 通訊作者
電子郵件：984403005@cc.ncu.edu.tw

and Wang (2009) all have the following drawbacks: (1) The design of the dispatching matrices is not regular. (2) Shares are m-times larger than the original secret image. (3) Restored image's quality is poor. (4) Their schemes are not suitable to apply in grayscale and color secret images. In order to solve the above limitations, we propose a non-expanded PVSS approach, in which the recovery method is based on secret blocks, namely Block-based Progressive Visual Secret Sharing (BPVSS). We divide a secret image into n non-overlapped image blocks, and an additional portion of secret will be restored after superimposing one more transparency. When superimposing any t shares, there have t ($2 \leq t \leq n$) secret blocks being restored. Compared with other related works, BPVSS has several advantages: (1) The concept of this model is concise, easy to implement, and the number of participants will not be restricted. (2) In the situation of noise-like shares, the contrast of the restored image is 50%, which means that the hidden message can be clearly recognized by the naked eyes. (3) When transparencies are shifted from noise-like into meaningful, the contrast of the stego-image and the restored image will be 25% which is still superior to other related studies. (4) Our scheme is more suitable for grayscale and color secret images than previous related studies. (5) The size of transparencies is the same as the size of secret image.

Key Words: Visual Secret Sharing, Progressive Visual Secret Sharing, Secret Block, Steganography

1. 前言

視覺機密分享（visual secret sharing，VSS）是 Naor and Shamir（1995）所提出一個應用在影像資料上的密碼學技術，其主要的概念是將一張機密影像，轉換成 n 張看似由雜點所組成的黑白投影片，再將這些黑白投影片分配給參與機密分享的成員。若是其中 k 張以上（$k \leq n$）的投影片被重疊，將可以單純地憑藉人類的視覺系統來辨識機密資訊；反之，疊合影像上仍然是呈現出無意義的影像內容，因此這個機制被稱之為 (k, n)-threshold scheme。Ateniese et al.（1996）則是針對重疊的組合做出限制，因而提出任意使用結構的分享架構（general access structure，GAS），其模型可以表示為 $\Gamma = (P, F, Q)$，分別代表參與者（P）、禁止（F）與合法（Q）三個集合。其做法是將投影片的重疊組合劃分為兩個互斥的禁止與合法集合。所謂的禁止集合，是指集合內任何一個元素中的所有分享投影片重疊後，在疊合影像上仍然是呈現出雜亂

無章的內容，無法解譯機密資訊；反觀在合法集合中，則是每一個元素都可以疊合出機密資訊，使得機密資訊的還原結果，可以根據使用者的需求來做出不同的設定。相較於傳統密碼學的加解密過程，視覺機密分享的優點是不需要繁複的數學運算與電腦輔助，只要透過人類視覺系統即可進行解密。

雖然視覺機密分享可以安全地分享機密資訊，不過它的分享投影片卻是透過像素擴展來產生，即是機密影像上的每一個像素點，在投影片上會被擴展成 m 個點（$m \geq 2$）的像素區塊，因此投影片的大小會是機密影像的 m 倍。像素擴展不僅會導致機密內容的影像扭曲，也會造成分享投影片的不易攜帶和儲存空間浪費，為了解決這個問題，Ito et al.（1999）與 Yang（2004）基於機率的觀點，分別提出一個像素不擴展的分享方法。Tu and Hou（2007）為了改善因機率上的隨機挑選影像內容，而造成疊合影像上凌亂的視覺效果，於是提出了一個利用多點加密的不擴展視覺機密分享模型。隨機網格（random grid）是 Kafri and Keren（1987）所提出的一種加密方法，其中每一個網格內容必須符合隨機變數的要求，也就是服從統計學上獨立且分配一致（independent and identically distributed，IID）的要求，因此每一個網格點上黑點與白點的出現機率皆為 1/2。Shyu（2009）利用這個概念來設計一種 (n, n)-threshold 的分享機制，稱之為 VCRG-n。但是隨著參與者和被重疊分享投影片數目的增加，機密影像的白點部份，在疊合影像上仍是出現白點的機率將會下降，使得疊合影像上無法產生出足夠的色差對比值，因此造成了還原品質不佳的問題。

此外，上述的研究在疊合影像上所呈現的不是雜訊內容，就是被解密後的機密資訊，這是一種非有即無（all-or-nothing）的概念。而漸進式視覺機密分享（progressive visual secret sharing，PVSS）的做法則是隨著重疊的投影片數目增加，機密影像的內容會漸漸地被還原，因而達成逐步地還原機密資訊的目標。在目前漸進式視覺機密分享的研究中，可以分為兩種分享模式。第一種分享模式是將整張機密影像視為被還原的對象（Fang and Lin, 2006; Fang, 2008; Chen, 2009; 侯永昌與官振宇，2010；Hou and Quan, 2011），因此只要在疊合影像上再重疊另一張分享投影片，疊合影像的黑白色差就會增加一個固定比例，因此達到漸進式機密還原的目標。第二種分享模式是將機密影像切割為多個不重疊的影像區塊（Wang et al., 2007; Wang, 2009），當疊合影像上再重疊另一張分享投影片後，被還原的影像區塊範圍將會愈來愈多，因而達成漸進式還原的目標。不過在 Wang et al.（2007）和 Wang（2009）所提出的分享模式中，都會產生了下列幾個缺點：(1) 分享矩陣的設計沒有規律性而造成不容易配置，使得參與機密分享的數目（n 值）受到限制。(2) 使用像素擴展法來產生分享投影片，使得分享投影片比機密影像大上很多倍。(3) 隨著參與者的數目逐漸增加，還原影像的黑白色差值將會愈來愈低，造成還原影像的品質不佳。(4) 不適合應用於灰階或彩色影像上。

為了解決上述 Wang et al.（2007）和 Wang（2009）的研究限制，本研究提出一個應用影像區塊進行漸進式還原的非擴展式視覺機密分享模型，稱之為 Block-based Progressive Visual Secret Sharing（BPVSS）。其概念是將一張機密影像切割成 n 個任意大小且不重疊的機密影像區塊（secret block），當 t（$2 \le t \le n$）張投影片重疊後，機密影像上就會有 t 個影像區塊被復原，並且隨著被重疊的投影片數目增加，機密影像上被還原的影像區塊也隨之遞增，藉此達成基於影像區塊來還原機密資訊的目標。在下面的章節中，第 2 節將簡單說明漸進式視覺機密分享的相關研究。第 3 節是介紹本研究所提出的兩個分享模型，第 4 節是實驗結果與其他學者的比較，最後在第 5 節則是本篇論文的結論。

2. 漸進式還原之機密分享

機密分享（Shamir, 1979）和視覺機密分享（Naor and Shamir, 1995）的研究都是以分散風險的觀念來避免機密資訊遭到濫用。他們分別將機密資訊分散成 n 張分享影像或分享投影片，並且分別將這些分享影像（或投影片）分配給每一位參與者。要解讀機密資訊時，必須透過一個門檻值（k）來決定機密資訊是否可以被還原。要獲得 k 張或 k 張以上的分享影像（或投影片）後才可計算（或疊合）出機密影像的資訊；反之，則無法獲得任何機密資訊，因此可以提升機密資訊的安全性。不過門檻值機制卻會受到門檻值的限制，當 k 值過大時，機密分享會因為參與者過多而降低其便利性，因此發展出漸進式機密資訊分享的研究。

漸進式機密分享（Chen and Lin, 2005; Wang and Shyu, 2007; Hung et al., 2008）不再是運用門檻值機制，而是透過「協同合作」的概念來解譯機密資訊。換句話說，在這一個新的分享機制中，每一位參與者都擁有部分的解密訊息，隨著提供解密訊息人數的增加，機密資訊被還原的幅度也會逐漸增加。漸進式視覺機密分享延伸這一個概念，將機密資訊分解成多張外觀為雜訊內容的分享投影片，當重疊分享投影片的數目逐漸增加，機密內容的整體黑白色差將會愈來愈大，或者是機密內容被揭露的區塊範圍愈來愈多，這表示機密內容的細部紋理將會愈來愈清晰，因此達到透過人眼來直接解譯機密資訊的目標。

2.1 基於整張機密影像

在 Fang and Lin（2006）的研究中，雖然可以藉由重疊分享投影片來達成漸進式還原機密資訊的目標，不過他們的研究有下列幾個缺點。第一，利用像素擴展的方式來設計分享模型，因此造成傳輸頻寬與儲存空間的浪費。第二，分享投影片上代表每

一個像素點的影像區塊內，被分配到黑點的機率並不一致，使得在分享投影片上會顯露出機密資訊的輪廓。第三，機密影像上的黑點（白點）部份，在還原影像上無法被完全還原為全黑（兩黑兩白）的區塊。Hou and Quan（2011）為了改善這些問題，使用兩個 $n \times n$ 的矩陣 C_0、C_1 來產生出 n 張不擴展型的分享投影片，其中矩陣中的每一列是代表一種分享方式，每一行則是代表每一張投影片被分配的內容（其中 1 代表黑點，0 代表白點），如表 1 所示。

▼ 表 1　n×n 的機密影像分享矩陣

□	■
$C_0 = \begin{bmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 0 \end{bmatrix}_{n \times n}$	$C_1 = \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}_{n \times n}$

根據矩陣的內容可以得知，無論機密資訊的像素點顏色為何？每一張投影片被分配到黑點的機率皆維持相等（$= 1 / n$），再加上每一個像素點的內容，都是根據隨機選取矩陣內的列向量而產生，因而在分享投影片上不會顯露出機密資訊的邊緣輪廓。此外，機密影像上的白點將會在每一張投影片的相同位置上出現黑點；反之，機密影像上的黑點則分別出現在不同投影片的相異位置上。因此，當重疊分享投影片後，機密影像上的白點部份仍是在同一個位置被疊合出黑點；而黑點部分被疊合出的黑點數目會逐漸增加，因而擴大疊合影像的黑白色差，所以在疊合影像上會逐漸顯現出機密影像的內容。當重疊所有的投影片後，機密影像上的黑點保證還原為全黑，使得還原影像上的黑白色差增加為（$n - 1$）/ n。

2.2　應用藏密學技術

經過密碼學技術所處理過的資訊，常常呈現出雜訊式的外觀，容易引起竊取者試圖破解的意願。藏密學（steganography）是一種資訊隱藏技術，將機密資訊嵌入在偽裝影像（stego-image）之中，使人不易讓人察覺其中藏有額外資訊，因此可以增加機密資訊傳輸的安全性。一般藏密學技術是將機密資 以微調影像灰階值的方式，藏入灰階或彩色影像中，其中以最小位元置換法（Moulin and O'sullivan, 2003）與鄰近像素值差異法（Wu and Tsai, 2003）最常被使用。由於視覺機密分享所處理的像素點內容只有黑或白兩種，所以無法利用微調灰階值的方式來隱藏資訊。因此，當要應用藏密學的概念時，視覺機密分享是運用黑點出現的疏密來製造出影像的黑白色差，藉

此呈現出偽裝影像與機密影像的輪廓。也就是偽裝影像上較黑的部份，在投影片上也會顯得比較黑，而白點部份則是比較白，因此可以在投影片上顯示出有意義的偽裝影像。當要還原機密資訊時，機密影像上的黑點部份，在疊合影像上也會比較黑，而白點部份則會比較白，因而還原出機密資訊的內容。

Fang（2008）應用藏密學的概念，提出了一個有意義分享投影片的漸進式分享模型。不過其分享模型是利用像素擴展法，因此投影片的大小會是機密影像的 4 倍。此外，投影片上的色塊分配會受到機密像素顏色和亂數隨機性的影響，於是產生分享投影片的安全性不足及疊合影像色差不佳等問題。Chen（2009）則是利用隨機網格來製作有意義的偽裝分享投影片，雖然這個作法可以解決像素擴展的問題，不過當重疊分享投影片後，機密影像上的黑色（白色）區域被還原為黑色（白色）的機率，會因為所對應的偽裝影像顏色而有所不同，並且機密影像的黑點部份無法被還原為全黑，因此造成還原影像品質不佳的結果。

為了改善上述的問題，侯永昌與官振宇（2010）設計了四個基本矩陣 $C_0 \sim C_3$（表 2），用來合成出四種分享矩陣 $M^0 \sim M^3$（表 3），分別是代表偽裝與機密影像的像素點內容為（白，白）、（黑，白）、（白，黑）、（黑，黑）四種可能的分享機制。根據表 3 的分享模型，分享投影片的大小將會與機密影像相同，並且每一張投影片上的色塊分配只會與偽裝影像的白色與黑色有關，於是投影片上不會顯露出機密資訊。但是在重疊所有分享投影片後，在疊合影像上可以產生出（$n-1$）/（$2n$）的黑白色差，使得機密內容可以清楚地被辨識。

▼ 表 2　4 個 n×n 的基本矩陣

$C_0 = \begin{bmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 0 \end{bmatrix}_{n\times n}$	$C_1 = \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}_{n\times n}$
$C_2 = \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}_{n\times n}$	$C_3 = \begin{bmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 1 & 1 & \cdots & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & \cdots & \cdots & 1 \end{bmatrix}_{n\times n}$

▼ 表 3　4 個 2n×n 的機密影像分享矩陣

（偽裝白，機密白）	（偽裝黑，機密白）	（偽裝白，機密黑）	（偽裝黑，機密黑）
$M^0 = \begin{bmatrix} C_2 \\ C_0 \end{bmatrix}_{2n\times n}$	$M^1 = \begin{bmatrix} C_3 \\ C_0 \end{bmatrix}_{2n\times n}$	$M^2 = \begin{bmatrix} C_2 \\ C_1 \end{bmatrix}_{2n\times n}$	$M^3 = \begin{bmatrix} C_3 \\ C_1 \end{bmatrix}_{2n\times n}$

2.3　基於機密影像區塊

Wang and Shyu（2007）首先提出一個基於影像區塊還原的加密方法。這個分享模型將機密影像分割為 n 個不重疊的影像區塊，每一個參與者分別主控一個影像區塊的還原工作。他們的做法是採用 Thien and Lin（2002）的 (2, n)-threshold 機制，每次將 2 個像素值分別隱藏在一次多項式的 2 個係數中，以完成資訊的分享，日後在取得 t 張分享投影片時，將會有 t 個影像區塊的內容被完全還原。不過 Wang and Shyu（2007）的分享模型是藉由多項式來隱藏資料，因此在解密過程中必需電腦的輔助運算，才能求解出隱藏在一次多項式的 2 個係數，完成機密影像的解密工作，所以無法像視覺機密分享一般，以利用目視的方式來進行解密。

Wang et al.（2007）應用這一個分享概念，提出一個基於影像區塊還原的漸進式視覺機密分享，稱之為 n-level VSS。其做法是先將機密影像分割為 n（$n \geq 3$）個不重疊的影像區塊，並且分別以 (i + 1, n + 1)-threshold 的模型來加密第 i（$1 \leq i \leq n$）個機密區塊，因此總共需要利用 2n 個分享矩陣，以產生出 n + 1 張分享投影片。當要解譯機密資訊時，只要任意 i + 1 張分享投影片重疊後，疊合影像上就會顯示出機密資訊中編號為 1 ～ i 的區塊內容。不過相異的 (i + 1, n + 1)-threshold 分享模型，像素點的擴展倍率並不一致，因此為了維持原始機密影像的長寬比例，以及在保護分享影上不會顯露出機密資訊的邊界，於是他們將每一個分享矩陣都擴展為相同的大小，並且在分享矩陣內填入冗餘資料。這個做法雖然可以使得每一個像素點都維持相同的機率出現黑點，但是卻增加了分享投影片的擴展倍率，使得機密資訊傳輸更不方便。

Wang（2009）又提出了另一個基於影像區塊還原的分享模型，稱之為 n-level RIVC。其做法是先運用 (n + 1, n + 1)-threshold 來決定第 n 層機密影像區塊的白黑兩色的分享矩陣 L_n^0 和 L_n^1，並且為了簡化分享矩陣的設計，於是在第 1 ~（n – 1）層影像區塊上的白點部份，將會都被分配到相同的分享矩陣（$L_1^0 = L_2^0 = \cdots = L_{n-1}^0 = L_n^0$）。在設計影像區塊黑點部份的分享矩陣時，Wang 是任意選擇 L_n^0 上的一個列向量來配置第 1 層影像區塊內的參考矩陣，並且運用一個 n + 1 階的單位矩陣（主對角線元素為 1，其餘元素為 0），和反單位矩陣（主對角線元素為 0，其餘元素為 1）來配置出第 2 ~（n – 1）層影像區塊的黑點分享矩陣。此外，為了要保持每個分享矩陣有相同的擴展倍率，以及每個分享矩陣的每一列有相同數目的 1，於是 Wang 在分享

矩陣內填入適當的冗餘內容。這一個分享模型需要使用 $n + 1$ 個分享矩陣以產生出 $n + 1$ 張分享投影片。

雖然上述兩個做法可以直接透過重疊投影片，來達成基於影像區塊漸進式還原的目標。不過在這些分享模型中，每一個分享矩陣都需要經過特殊的設計，因而造成分享矩陣變得複雜且不易實做。其次，運用像素擴展來製作分享投影片，因此在傳輸效率與機密資訊的視覺品質考量下，分享投影片的數目（n 值）將會受到限制。第三，還原影像上的黑白色差不明顯，而造成部份影像區塊內的機密內容不易辨識的結果。最後，在 Wang（2009）年的作法中，由於機密影像上的白點部份是採取相同的分享矩陣，因此在機密影像上的第 1 ~（$n - 1$）個影像區塊內，機密影像的白點部份被疊合成黑色的機率反而比黑點部份高，因此在疊合影像的影像區塊內會被還原出黑白顛倒的「陰刻」結果；只有第 n 個影像區塊內，黑點部份被疊合成黑色的機率比白點部份高，因此會被還原出「陽刻」的結果。由於在還原影像上無法忠實地還原出機密影像的內容，因此這個分享模型比較不適合應用於灰階或彩色機密影像的情況。

為了改善上述相關研究的缺點，於是本研究提出一個非擴展且應用於影像區塊漸進還原的視覺機密分享模型。在這個分享機制中，機密影像的內容將會被分配到 n 張不擴展大小的分享投影片上，只要任意 2 張投影片重疊後，就可以解譯部分區塊內的機密資訊，並且隨著被重疊的投影片數目增加，被還原的影像區塊也會愈來愈多。此外，本研究也將分享投影片由雜訊影像延伸到有意義的偽裝影像，因此可以降低分享投影片遭受攻擊的可能性。

3. 本研究所提出的分享模型：BPVSS

本研究提出一個以還原機密影像區塊為基礎的非擴展型漸進式視覺機密分享模型，每一位參與者都如同是拼圖遊戲上的一塊子圖片，如果想要還原機密資訊時，必須依賴每一位參與者提供自己的子圖片，並且隨著提供子圖片的參與者數目愈來愈多，被還原的機密內容將會愈來愈完整。只要有某一（幾）位參與者沒有提供自己的子圖片，它所對應到的機密影像區塊將無法被還原，因此這個分享模型稱之為 Block-based Progressive Visual Secret Sharing（BPVSS）。

在 BPVSS 的分享模型中，首先是根據參與視覺機密分享的人數，將一張機密影像（SI）劃分為 n 個任意大小且不重疊的影像區塊 $P_1, P_2, \cdots, P_n$，這些影像區塊滿足公式 (1) 的定義。

$$\begin{cases} SI = \bigcup P_i & for \quad 1 \le i \le n \\ P_i \cap P_j = \varnothing & for \quad 1 \le i \ne j \le n \end{cases} \tag{1}$$

每一位參與者各自擁有一個特定影像區塊的還原金鑰，即是只要在疊合影像上加上第 m（$1 \le m \le n$）位參與者的分享投影片後，在機密影像上對應的區塊內容就會被還原，因而顯示出機密資訊的部份內容。當任意重疊 t（$2 \le t \le n$）張投影片後，這 t 個參與者所對應的 t 個影像區塊內的機密內容就都會被還原，然而其他影像區塊的內容仍是保持雜訊式影像，藉此達成基於機密影像區塊而逐步還原的效果。

3.1　模型 1 －無意義分享投影片的 BPVSS

為了達成上述的要求，本研究設計了 $n + 1$ 個大小為 $2 \times n$ 的分享矩陣 $C^0, C^1, \cdots, C^n$（公式 (2)），其中 C^0 是一個代表機密內容為白色的分享矩陣，而 C^m 則分別代表影像區塊 m 內黑色機密的分享矩陣。

$$C^0 = [\theta_{xy}]_{2\times n} = \begin{cases} 0, \ if\ x = 1, \ 1 \le y \le n \\ 1, \ if\ x = 2, \ 1 \le y \le n \end{cases}$$

$$C^m = [\theta_{xy}]_{2\times n} = \begin{cases} 1, \ if\ x = 1, \ 1 \le y = m \le n \\ 1, \ if\ x = 2, \ 1 \le y \ne m \le n \ \text{ where } m = 1, 2, \cdots, \text{and } n \\ 0, \ otherwise \end{cases} \qquad (2)$$

在 C^0 矩陣上，第一列的值會全部被設為 0，而第二列的內容則是皆被設為 1；在 C^m 矩陣上，第一列的第 m 個值將會被設為 1，其他位置上的值則是被設為 0，第二列的第 m 個值將會被設為 0，其他位置則被設為 1。矩陣中的每一列是代表一種分享方式，而每一行則是代表每一個參與者被分配的像素點內容，其中 0 代表白點、1 代表黑點。

當要產生分享投影片時，是透過隨機亂數（l）來選取分享矩陣 $C^0 \sim C^m$ 內的一個列向量，並依序將列向量內的每一個值分配到對應的投影片上（第 m 個值分配給第 m 張投影片），所以每一張投影片的大小將會與機密影像相同。如果機密影像的像素點顏色為白色，就從 C^0 矩陣中任意選取一個列向量做為分配內容；反之，如果機密影像像素點的顏色為黑色，則是根據影像區塊的位置（block m）來選取 C^m 分享矩陣，並且以同樣的分配方法來產生分享投影片。詳細的分享投影片製作流程請參考圖 1。由於各個分享矩陣上的每一個行向量都保持一白一黑，加上投影片是根據隨機亂數來選取分享矩陣的內容，所以不論機密像素是白是黑，在分享投影片上的每一個對應的像素點都有 1/2 的機率會出現黑點。因此，黑點會均勻地散佈在投影片上，確保在每一張投影片上都不會洩露出機密資訊的輪廓。

BPVSS Algorithm:
Input：
(1) 一張經半色調處理的機密影像 SI，其大小為 $W \times H$
(2) 參與機密分享的參與者人數 n
(3) $n + 1$ 個大小為 $2 \times n$ 的分享矩陣 $C^0, C^1, \cdots, C^n$
Output：n 張大小為 $W \times H$ 的分享投影片 S_m，$m = 1, 2, \cdots,$ and n
Process：

```
FOR each row on the SI
  FOR each column on the SI
    Set a random number l (l = 1, 2)
    FOR m = 1 to n
      IF secretPosition (row, column) is White THEN
        S_m (row, column) is C^0 (l, m)
      ELSE
        S_m (row, column) is C^m (l, m)
      END IF
    END FOR
  END FOR
END FOR
```

▲ 圖 1　BPVSS 演算法

由於 C^0 矩陣列向量的內容都相同，因此針對機密影像上的白色像素，在每一張分享投影片的對應位置上都會被分配到相同的顏色（出現黑點或白點的機率皆是 50%）。因此，機密影像的白點部分無論重疊多少張投影片後，在疊合影像的對應位置上仍然會保持相同的顏色，使得疊合結果仍然維持黑白各半的機率（50% 的黑）。然而 C^m 矩陣則是在列向量上的第 m 個值與其他內容相異，也就是在第 m 張投影片上出現黑點（白點）時，在其他分享投影片上都會出現白點（黑點），形成投影片 m 與其他投影片互補的狀態。因此 C^m 矩陣可以讓參與者 m 擔任還原影像區塊 m 的主控角色：在沒有第 m 張投影片參與機密解譯的情況下，無論其他的投影片再怎麼疊合，在疊合影像上都無法增加影像區塊 m 中的黑點數目，使得機密影像上的黑點部份不會更黑（仍然只能保持 50% 的黑點和 50% 的白點），無法與機密影像為白色的部份產生色差，自然不會洩漏出影像區塊 m 的機密資訊；但是只要有第 m 張投影片與其他的投影片疊合，機密影像上區塊 m 的黑點部份就會被重疊出全黑（100% 的黑），與區塊內的白色部份產生 50% 的黑白色差，因此靠視覺就可以還原第 m 個影像區塊的機密內容。

當重疊第 i 張與第 j 張分享投影片（S_i、S_j）後，由於機密影像的白點會在投影片的相同位置上被分配到黑點，於是在編號為 i 和 j 的兩個影像區塊上將不會產生任何變化（仍然保持 50% 的黑點和 50% 的白點）。相反地，機密影像的黑點部份在投

影片的這兩個影像區塊內，將會被分配到互補的內容，於是在疊合影像上將會出現全黑，因此可以利用色差來還原影像區塊 i 和影像區塊 j 的機密資訊。反觀機密影像上的其他影像區塊，無論機密影像上的像素點內容為何，每一個像素點被分配到的內容都是相同的，其中有 50% 的機率會出現黑點，有 50% 的機率會出現白點。因此在重疊 S_i、S_j 兩張投影片後，其他區塊內黑點的個數並不會因此增加，也沒有辦法產生黑白色差，於是這些區塊內的機密內容將無法被還原。

在任意重疊 t（$2 \le t \le n$）張分享投影片的情況下，由於每一張投影片所解譯的影像區塊都不相同，因此根據組合公式（combination formula）的定義，將可以產生出 $\frac{n!}{t!(n-t)!}$ 種不同的還原結果。而隨著被重疊的投影片數目增加，所能還原機密影像的區塊將會愈來愈大，達成漸進式還原的目標。由於參與者的組合不同，將會產生不同的還原結果，根據二項式定理（binomial theorem），當重疊的投影片數目從 2 張增加到 n 張後，疊合影像一共會產生出 $2^n - n - 1$ 種的還原結果。

3.2　模型 2 －有意義偽裝投影片的 BPVSS

當我們想要在分享投影片上呈現出偽裝影像的內容，那麼投影片上每一個像素點被分配到黑點的機率必須變得不同，使得偽裝影像的黑色部分在分享投影片會顯得比較黑，而白點部份顯得比較白，於是可以產生顯現偽裝內容的黑白色差。此外，機密影像的白（黑）點部份可能是由偽裝影像上的白點所疊合而成，也可能是黑點的重疊結果，因此我們需要四個分享模型，分別代表偽裝與機密影像的內容為（白，白）、（白，黑）、（黑，白）、（黑，黑）等四種組合狀況。此外，為了保持機密影像是以影像區塊為漸進還原的目標，每一個影像區塊 m 都有一組主控的分享矩陣 $M_0^m \sim M_3^m$，如公式 (3) 所示。

$$M = \begin{cases} M_0^m = \begin{bmatrix} C^m \\ C^0 \end{bmatrix}_{4\times n}, \ if \text{ 偽裝} = white, \text{ 機密} = white \ and \text{ 區塊} = m \\ M_1^m = \begin{bmatrix} C^m \\ C^m \end{bmatrix}_{4\times n}, \ if \text{ 偽裝} = white, \text{ 機密} = black \ and \text{ 區塊} = m \\ M_2^m = \begin{bmatrix} C^{n+1} \\ C^0 \end{bmatrix}_{4\times n}, \ if \text{ 偽裝} = black, \text{ 機密} = white \ and \text{ 區塊} = m \\ M_3^m = \begin{bmatrix} C^{n+1} \\ C^m \end{bmatrix}_{4\times n}, \ if \text{ 偽裝} = black, \text{ 機密} = black \ and \text{ 區塊} = m \end{cases} \tag{3}$$

其中，C^0 和 C^m 如公式 (2) 所示，C^{n+1}（公式 (4)）為一個新的分享矩陣，其矩陣內的值全部都設為 1。

$$C^{n+1}=[\theta_{xy}]_{2\times n}=\begin{cases}1, & for\ 1\le x\le 2,\ 1\le y\le n\\ 0, & otherwise\end{cases} \tag{4}$$

為了能在分享投影片上顯示偽裝影像的內容，我們將 C^m 放置在代表偽裝影像為白色的相關矩陣（M_0^m, M_1^m）中，而在偽裝影像為黑色的相關矩陣（M_2^m, M_3^m）內則是放置矩陣 C^{n+1}，使得在偽裝影像上黑點部份被分配到黑點的機率，會大於偽裝影像的白點部份，因此可以在分享投影片上顯露出偽裝影像的輪廓。為了能清楚看到機密影像的內容，我們利用矩陣 C^0 和 C^m 來控制疊合影像上的色差，於是將 C^0 放置在機密影像為白色的相關矩陣（M_0^m, M_2^m）中，而矩陣 C^m 放置在機密影像為黑色的相關矩陣（M_1^m, M_3^m）中，使得在疊合影像上也可以顯示出機密影像的輪廓。

根據公式 (3) 的設計，當要在分享投影片上顯示出偽裝影像上的白色部分時，不論這些像素點在疊合影像上是代表機密影像的黑點或白點，每一個像素點都有 50% 的機會被分配到黑點；反之，偽裝影像的黑點被分配到黑點的機率則是保持 75%。因此，分享投影片除了不會產生機密資訊的邊界外，而且在每一張投影片上都可以產生出 25% 的黑白色差，可以清楚地辨識出偽裝影像的內容。由於本研究是基於影像區塊的內容來進行還原，因此在重疊分享投影片後，對應的影像區塊中機密內容為白點的部份，在疊合影像上會有 75% 的機會被疊合出黑點，而黑點部份則是被疊合出全黑的內容，因此在疊合影像上對應的影像區塊中也會顯示出 25% 的黑白色差。隨著被重疊的投影片數目逐漸增加，被還原的範圍將會愈來愈大，因而逐漸顯露出完整的機密影像內容。

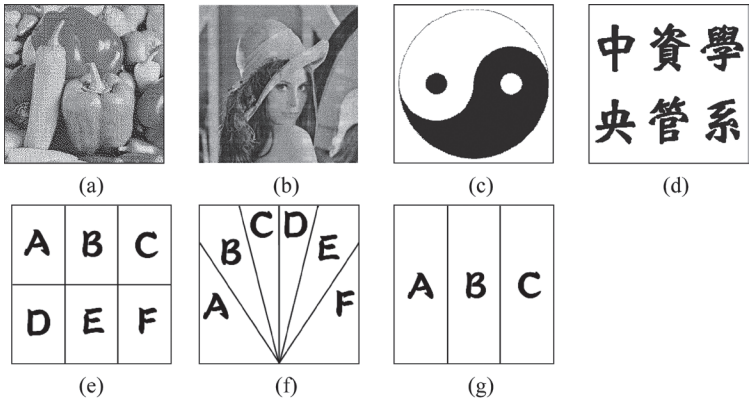
以 4 個影像區塊的視覺機密分享為例，我們必須產生 1 個代表機密影像白點的分享矩陣 C^0，4 個代表機密影像黑點和偽裝影像白點的分享矩陣 $C^1 \sim C^4$（分別是用來還原影像區塊 1 ～ 4 的分享矩陣），以及 1 個代表偽裝影像黑點的分享矩陣 C^5，其內容如表 4 所示。

▼ 表 4　4 個影像區塊的視覺機密分享矩陣

$C^0=\begin{bmatrix}0&0&0&0\\1&1&1&1\end{bmatrix}_{2\times4}$	$C^1=\begin{bmatrix}1&0&0&0\\0&1&1&1\end{bmatrix}_{2\times4}$	$C^2=\begin{bmatrix}0&1&0&0\\1&0&1&1\end{bmatrix}_{2\times4}$
$C^3=\begin{bmatrix}0&0&1&0\\1&1&0&1\end{bmatrix}_{2\times4}$	$C^4=\begin{bmatrix}0&0&0&1\\1&1&1&0\end{bmatrix}_{2\times4}$	$C^5=\begin{bmatrix}1&1&1&1\\1&1&1&1\end{bmatrix}_{2\times4}$

4. 實驗結果與分析比較

本實驗是在作業系統 Microsoft Windows XP 下，以 Java（JDK 1.6.10）程式語言作為開發環境，硬體設備為個人桌上型電腦 CPU AMD Athlon（tm）X2 240 和 RAM 2 GB。實驗圖像是四張經過半色調處理後的 BMP 格式影像，分別是大小為 256×256 的灰階影像 Pepper、彩色影像 Lena 與黑白影像 Tai_chi 和 Faculty（圖 2(a) ～圖 2(d)）。此外，由於本研究是基於影像區塊來進行漸進式還原，因此我們將機密影像切割為三種樣式（圖 2(e) ～圖 2(g)）。在 4.1 節，本研究運用四張實驗圖像來實做 BPVSS 的兩個分享模型，而 4.2 節則是比較本研究與其他學者的實驗結果。

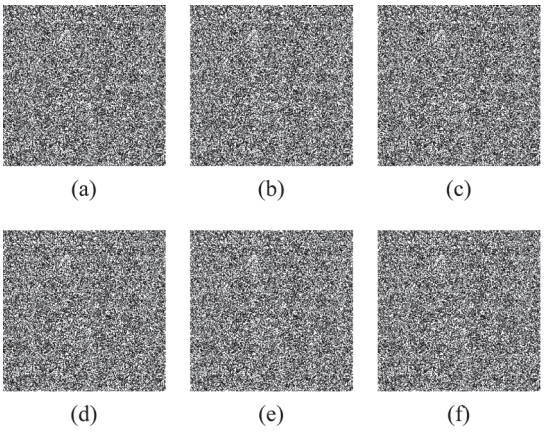


▲ 圖 2　實驗影像與機密影像的切割方式

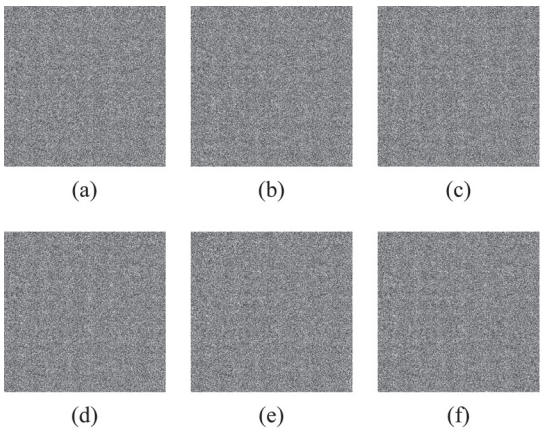
4.1　BPVSS 的實驗結果

本研究首先利用黑白影像 Faculty 來進行實驗，機密影像將會被切割為第一種影像區塊樣式（圖 2(e)），然後根據公式 (2) 的分享矩陣來產生出六張雜訊式的分享投影片（圖 3）。在圖 3 的每一張投影片上，每一個像素點出現黑色的機率約等於 1/2，並且這些黑點是均勻地散佈在整張投影片上，於是攔截者無法從任何一張投影片上獲取機密資訊的內容。當機密影像轉換成彩色影像 Lena 後，我們將機密影像切割成另一種影像區塊的樣式（圖 2(f)），再利用公式 (2) 與 Hou（2003）的色彩分解與合成方法來產生六張彩色分享投影片（圖 4）。彩色分享投影片上的每一個像素點顏色，是根據三個分色是否出現來決定，並且隨機選擇分享矩陣上的列向量，於是出現八種色點的機率都約略等於 1/8，使得攔截者無法輕易地從任一張分享投影片的顏色，來猜中（解譯出）機密資訊的顏色（內容）。因此，無論機密影像的像素內容為何，在本研究所產生的每一張分享投影片都可以被視為是安全的。無論機密影像被切

割的樣式為何，圖 3 和圖 4 中的分享投影片 $Share_1$ ～ $Share_6$，分別被視為是影像區塊編號 A ～ F 的解密金鑰。

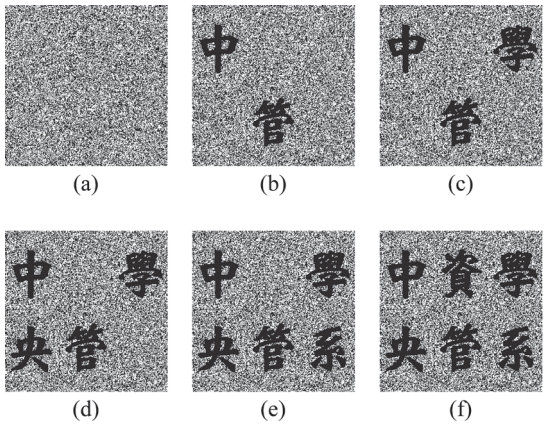


▲ 圖 3　以 Faculty 為例所產生的 6 張雜訊式投影片



▲ 圖 4　以 Lena 為例所產生的 6 張彩色雜訊式投影片

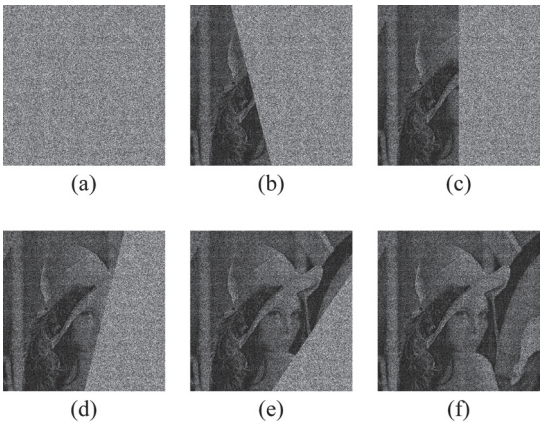
圖 5 是圖 3 投影片的重疊結果。當重疊 $Share_1$ 與 $Share_5$ 兩張投影片後，只有區塊 A 和區塊 E 的內容被還原，其餘區塊仍保持雜訊式內容（圖 5(b)）；重疊 $Share_1$、$Share_3$、$Share_5$ 三張投影片時，則是區塊 A、C、E 的內容會被完全還原，其餘位置仍然是雜訊式內容（圖 5(c)）。隨著被重疊的投影片數目逐漸增加，被還原的機密影像內容將會愈來愈完整，藉此達成漸進式還原的效果。



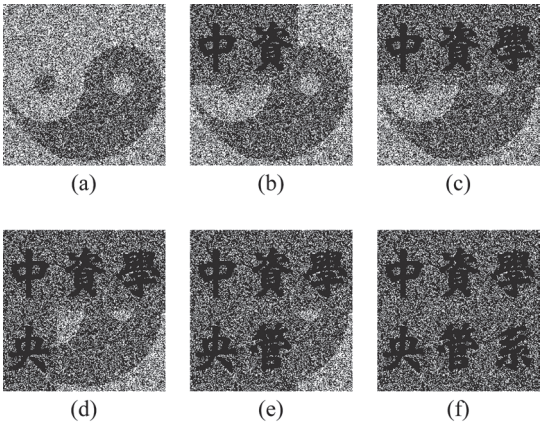
▲ 圖 5　以 Faculty 為例的漸進式還原結果

根據公式 (2) 可以得知機密影像 Faculty 的白點部份，不論分享投影片 m 上第 m 個區塊的內容是白色或黑色，在其他分享投影片的對應位置上也會出現相同內容，因此無論重疊幾張投影片後，疊合影像上的第 m 個區塊出現黑點的機率仍然保持是 50%；反觀機密影像的黑點部份，不論在編號 m 分享投影片的第 m 個區塊上被分配到的內容為何，在其他分享投影片上的對應位置上都會出現互補色，因此當重疊投影片後，在第 m 個區塊出現黑點的機率將會提升為 100%，因此在疊合影像上會出現 50% 的黑白色差。由於本研究是透過影像區塊來達成漸進式還原機密資訊的目標，因此在任意重疊第 i 張與第 j 張分享投影片後，只有在編號 i 和編號 j 上的機密影像內容會被還原，因此根據組合公式可以產生出 $C_2^6 = 15$ 種還原結果。隨著被重疊的投影片數目逐漸增加，機密影像內容被還原的區域也隨之豐富，最後當重疊所有的分享投影片後，機密影像上的每一個影像區塊都會被還原，因此在疊合影像上會顯示出機密影像 Faculty 的完整圖樣（圖 5(f)）。圖 6 則是彩色機密影像 Lena 的漸進式還原結果。

根據公式 (3) 的矩陣設計，我們設定機密與偽裝影像分別為 Faculty 和 Tai_chi，而影像的切割樣式則是運用圖 2(e) 的方法。在偽裝影像的白點部份，分享投影片上會有 50% 的機率出現黑點，而偽裝影像的黑點部份則是有 75% 的機率出現黑點，因此在每一張投影片上都會呈現出偽裝影像 Tai_chi 的圖樣（25% 的黑白色差），如圖 7(a) 所示。當要還原機密資訊時，機密資訊被還原的範圍會隨著被重疊的投影片數目增加而逐漸擴大（圖 7(b) ～圖 7(e)）。最後當重疊所有的投影片後，在機密影像的白點部份，疊合影像上會有 75% 的機率被重疊出黑色，而黑點部份的重疊結果將會是全黑，因此在疊合影像上顯示出機密影像 Faculty（25% 黑白色差），如圖 7(f) 所示。



▲ 圖 6　以 Lena 為例的漸進式還原結果

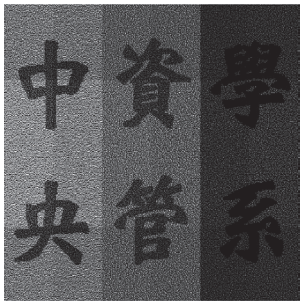
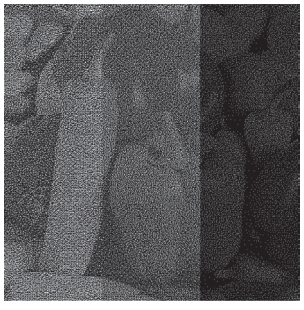
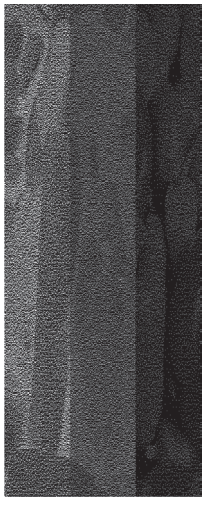
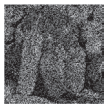


▲ 圖 7　有意義分享投影片的漸進式還原結果

4.2　本研究與其他學者的實驗結果比較

我們利用黑白影像 Faculty 與半色調灰階影像 Pepper 來進行實驗，將影像切割成 3 個區塊（如圖 2(g)），並且將本研究與其他學者（Wang et al., 2007; Wang, 2009）的實驗結果整理成表 5。

▼ 表 5　本研究與其他學者的實驗比較表

	Wang et al.（2007）	Wang（2009）	本研究
黑白機密影像的疊合結果			
	(a)	(b)	(c)
灰階機密影像的疊合結果			
	(d)	(e)	(f)
分享矩陣個數	$2n$ 個分享矩陣	$n + 1$ 個分享矩陣	$n + 1$ 個分享矩陣
分享矩陣設計	複雜且沒有規律性	複雜且沒有規律性	具有規律性
投影片大小	768×768（擴展 9 倍）	512×1280（擴展 10 倍）	256×256（原始大小）
機密影像內容	較適用於黑白機密影像	只適用於黑白機密影像	任何型態的機密影像
疊合影像內容	顯露出機密影像區塊個數	扭曲的機密影像	沒有區塊邊界輪廓

在 Wang et al.（2007）的分享模型中，機密影像上的每一點都擴展為 9 個點的像素區塊，因此分享投影片大小會是機密影像的 9 倍，這將造成傳輸與儲存上的負擔。其次，分享投影片疊合後，機密影像區塊的黑白色差分別是 3 / 9、2 / 9 和 1 / 9。使得在疊合影像的區塊邊界上會因為兩者的色差值不同而產生色階不連續的結果，而且有些影像區塊會因為色差太小，而無法清楚地顯現出機密影像的內容（表 5(a) 和 表 5(d)）。

在 Wang（2009）的分享模型中也有同樣的問題，機密影像上的每一個像素點都必須被擴展為 10（2×5）倍，這不僅會造成傳輸與儲存上的負擔，也會造成疊合影像的扭曲。其次，分享投影片疊合後，機密影像區塊內的黑白色差值分別為 3 / 10、1 / 10 和 1 / 10，也會產生因色差不足而無法清晰地顯示機密內容的問題，使得機密影像較適合於簡單結構的影像（表 5(b) 和 表 5(e)）。此外，Wang（2009）針對機密影像上的白點部份是採取相同的的分享矩陣（L_n^0），因此在機密影像上的第 1 ~（n – 1）個影像區塊內，機密影像的白點部份被疊合成為黑色的機率比黑點部份高。這造成了在被還原的機密影像區內，前兩個機密影像區塊是還原出「陰刻」效果的機密內容（表 5(b) 和 表 5(e) 的左邊兩個區塊，機密影像的疊合結果是黑白顛倒），而在第三個影像區塊內則是還原出「陽刻」效果的機密內容（表 5(b) 和 表 5(e) 最右邊的一個區塊，疊合結果的顏色與機密影像相同），使得還原影像無法忠實地表現出機密影像的內容。

由於 Wang et al.（2007）和 Wang（2009）的分享矩陣是根據機密影像的區塊數目（n 值），來決定矩陣的設計方式與矩陣內容，因此當 n 值逐漸增加後，這兩個模型的分享矩陣就會變得難以實做。反觀本研究的分享矩陣設計具有規律性（公式 (2) ～公式 (4)），並且無論分享投影片的數目為何，分享矩陣的設計方法與內容都是一致的。於是 BPVSS 可以適用於任何 n 值的狀況，使得機密資訊分享更加具有彈性。其次，本研究的分享矩陣是採取非擴展型，因此每一張投影片的大小都與機密影像相同，使得機密資訊的傳輸更具有效率。此外，在疊合影像的還原品質上，模型 1 使得每一個影像區塊內的黑白色差值都是 50%，因此能夠清晰地呈現出機密影像的內容（表 5(c)）。即使當機密影像轉換為有色調變化的半色調影像後，疊合影像上依然可以清楚地呈現出機密內容，因此 BPVSS 適用於任何機密影像的型態（表 5(f)）。最後，本研究也可以採用有意義的偽裝影像來製作分享投影片的內容（模型 2），使得機密影像的傳輸更為安全，並且在分享投影片與疊合影像上都能夠顯示出 25% 的黑白色差，可以清晰地被人眼所辨識（圖 7(a) 與圖 7(f)）。

為了讓讀者更了解漸進式視覺機密分享的研究，本研究將 BPVSS 與相關研究整理成表 6。根據表 6 可以得知，BPVSS 無論在擴展倍率、分享投影片的安全性與內容，以及還原影像品質等評估標準上，都有不錯的表現。

▼ 表 6　本研究與其他漸進式視覺機密分享研究的實驗比較表

	漸進還原類型		擴展倍率	分享投影片安全性	分享投影片的內容	還原影像品質
	整張影像	影像區塊				
Fang and Lin（2006）	✓		4	不佳	雜訊式	不佳
Wang et al.（2007）		✓	≥ 6	佳	雜訊式	不佳
Fang（2008）	✓		4	不佳	有意義	不佳
Chen（2009）	✓		1	佳	有意義	不佳
Wang（2009）		✓	≥ 4	佳	雜訊式	不佳
侯永昌與官振宇（2010）	✓		1	佳	有意義	佳
Hou and Quan（2011）	✓		1	佳	雜訊式	佳
本研究的模型 1		✓	1	佳	雜訊式	佳
本研究的模型 2		✓	1	佳	有意義	佳

5. 結論

漸進式機密分享是一種新的分享概念，機密資訊將會隨著所獲得分享影像數目的增加，機密資訊的內容將會逐步地被還原。漸進式視覺機密分享延伸這個分享概念，機密資訊的黑白色差會隨著重疊分享投影片的數目增加而變大，或者是被解譯的區塊範圍變多，藉此達成漸進式還原的效果。不過現行以機密影像區塊做為還原目標的相關研究中，都有分享矩陣設計法繁複、增加儲存空間負擔、還原影像品質不佳，以及機密影像不適合延伸到灰階或彩色影像上等缺點。

本研究為了改善上述的問題，於是提出一個以影像區塊還原的漸進式視覺機密分享模型，稱之為 BPVSS。相較於其他學者的研究成果，本研究具備下列幾項優點：(1) 本研究的分享模型的概念簡明且容易實作，不需要複雜的矩陣設計與像素點匹配，並且分享投影片的數目大小不會受到限制。(2) 模型 1 在還原影像上可以產生出 50% 的色差（黑點部分為全黑，白點部份為半黑白），使得機密資訊能清楚地為人眼所辨識。(3) 模型 2 可以讓分享投影片採用有意義偽裝影像，因此可以提高分享投影片的安全性，並且在偽裝影像與還原影像上皆有 25% 的黑白色差。(4) 本研究的機密影像可以擴展至灰階與彩色影像。(5) 每一張分享投影片大小於機密影像相同，可以降低資訊傳遞與儲存的負擔。

參考文獻

侯永昌、官振宇（2010），“有意義且不擴展分享影像之漸進式視覺密碼”，《資訊管理學報》，17 (3) ，131-154。

Ateniese, G., Blundo, C., De Santis, A., and Stinson, D.R. (1996), “Visual cryptography for general access structures,” *Information and Computation*, 129 (2), 86-106.

Chen, S.K. (2009), “Friendly progressive visual secret sharing using generalized random grids,” *Optical Engineering*, 48 (11), 1-7.

Chen, S.K. and Lin, J.C. (2005), “Fault-tolerant and progressive transmission of images,” *Pattern Recognition*, 38 (12), 2466-2471.

Fang, W.P. (2008), “Friendly progressive visual secret sharing,” *Pattern Recognition*, 41 (4), 1410-1414.

Fang, W.P. and Lin, J.C. (2006), “Progressive viewing and sharing of sensitive images,” *Pattern Recognition and Image Analysis*, 16 (4), 632-636.

Hou, Y.C. (2003), “Visual cryptography for color images,” *Pattern Recognition*, 36 (7), 1619-1629.

Hung, K.H., Chang, Y.J., and Lin, J.C. (2008), “Progressive sharing of an image,” *Optical Engineering*, 47 (4), 1-14.

Hou, Y.C. and Quan, Z.Y. (2011), “Progressive visual cryptography with unexpanded shares,” *IEEE Transactions on Circuits and Systems for Video Technology*, 21(11), 1760-1764.

Ito, R., Kuwakado, H., and Tanaka, H. (1999), “Image size invariant visual cryptography,” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E82-A (10), 2172-2177.

Kafri, O. and Keren, E. (1987), “Encryption of pictures and shapes by random grids,” *Optics Letters*, 12 (6), 377-379.

Moulin, P. and O’sullivan, J.A. (2003), “Information-theoretic analysis of information hiding,” *IEEE Transactions on Information Theory*, 49 (3), 563-593.

Naor, M. and Shamir, A. (1995), “Visual cryptography,” in *Advances in Cryptology-EUROCRYPT ’94, LNCS 950*, Springer-Verlag, 1-12.

Shamir, A. (1979), “How to share a secret,” *Communications of the ACM*, 22 (11), 612-613.

Shyu, S.J. (2009), “Image encryption by multiple random grids,” *Pattern Recognition*, 42 (7), 1582-1596.

Thien, C.C. and Lin, J.C. (2002), "Secret image sharing," *Computers & Graphics*, 26 (5), 765-770.

Tu, S.F. and Hou, Y.C. (2007), "Design of visual cryptographic methods with smooth-looking decoded images of invariant size for gray level images," *Imaging Science Journal*, 55 (2), 90-101.

Wang, R.Z. (2009), "Region incrementing visual cryptography," *IEEE Signal Processing Letters*, 16 (8), 659-662.

Wang, R.Z. and Shyu, S.J. (2007), "Scalable secret image sharing," *Signal Processing: Image Communication*, 22 (4), 363-373.

Wang, R.Z., Lee, Y.K., Huang, S.Y., and Chia, T.L. (2007), "Multilevel visual secret sharing," in *Proceeding of ICICIC'07*, Kumamoto: Kumamoto City International Center, 283-286.

Wu, D.C. and Tsai, W.H. (2003), "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, 24 (9-10), 1613-1626.

Yang, C.N. (2004), "New visual secret sharing schemes using probabilistic method," *Pattern Recognition Letters*, 25 (4), 481-494.