具有高色差對比之 (3, n)-門檻式視覺密碼學

官振宇[1] 侯永昌[2*] 蔡志豐[1]

[1]國立中央大學資訊管理系
[2]淡江大學資訊管理系

摘 要

本研究運用組合數學來設計 (3, *n*)-門檻式視覺分享模型，使得重疊影像的黑白區域出現最佳的黑白色差，也讓還原影像產生極佳的視覺效果。相較於 (3, *n*)- 視覺分享機制的相關研究，本研究具備下列幾項特點：(1) 設計概念十分單純，易於實作。(2) 以「在 *n* 個位置中任選 $n–n^{0.5}+1$ 個位置來填入 1 值」的方式來設計視覺密碼學所需之分享矩陣的內容，可以在重疊任意 3 張分享投影片時出現最佳的黑白色差，並且在還原影像上產生極佳的視覺效果，優於其他 (3, *n*)-門檻值密碼學的研究成果。(3) 本研究所提出的分享模型適合任何型態的機密影像。(4) 分享投影片的大小將與機密影像相同。

關鍵詞：機密分享、視覺密碼學、(3, n)-門檻式視覺密碼學、組合數學

A novel approach for (3, n)-threshold visual cryptography

Quan, Zen-Yu[1], Hou, Young-Chang[2*], and Tsai, Chih-Fong[1]

[1]*Department of Information Management, National Central University*
[2]*Department of Information Management, Tamkang University*

ABSTRACT

In this study, we propose a novel design for (3, *n*)-threshold visual cryptography by using the theory of the combinatorics to achieve an excellent contrast (visual effects) in the stacked image. Compared to the related works, this study has the following advantages: (1) the design concept is simple and easy to implement; (2) the stacked image's contrast is optimal when we choose $n–n^{0.5}+1$ positions to fill 1 in the columns of the dispatching matrices that are needed in applying the theorem of visual cryptography and the restored image's contrast is better than other researches in the field of (3, *n*)-threshold visual cryptography; (3) our method is suitable for any types of images; (4) the size of the transparencies are the same as the secret image.

Keywords: secret sharing, visual cryptography, (3, *n*)-threshold visual cryptography, combinatorics.

文稿收件日期 102.12.3; 文稿修正後接受日期 103.7.16;*通訊作者
Manuscript received December 3, 2013; revised July 16, 2014;* Corresponding author

一、前　言

密碼學 (cryptology) 是一門研究如何隱藏資訊的學問，其作法是透過加密演算法將明文 (plaintext) 轉換為無意義的密文 (ciphertext)，並且透過對應的解密演算法來還原明文的內容。傳統密碼學為了確保機密資訊的安全性，於是運用大量數學運算與複雜演算流程來產生密文，使得擷取者在有限時間內無法破解密文，不過傳統密碼學的加解密過程需要電腦設備輔助，並且使用者必須具備密碼學知識，因而將降低分享機密資訊的便利性。

視覺密碼學 (visual cryptography，VC) 是由 Naor and Shamir [1] 所提出，其主要精神在於解密方法是透過人類視覺系統，使用者不需具備密碼學知識與計算機資源，因此，在一些無法使用電腦解密的情況下，視覺密碼學是一個很好的解決方案。視覺密碼學的作法是將一張機密影像分散成 n 張雜亂無章的分享投影片 (transparency)，並且將這些分享投影片分別交付給 n 個參與者保管，因而達到機密資訊分散風險的功效。當要解譯機密資訊時，只要任意 k ($2 \le k \le n$) 位參與者重疊本身所持有的分享投影片後，在重疊影像上就可以產生出足以為人眼所辨識的黑白色差，而這個機制稱之為 (k, n)-門檻式視覺密碼學。在 (k, n)-門檻式視覺密碼學的研究中，當 k 值愈大時，將會造成重疊影像的視覺效果愈來愈差，使得視覺密碼學的應用性受到侷限。因此，在門檻式視覺密碼學的研究大多是著重於討論 (2, n)-門檻式視覺密碼學和 (3, n)-門檻式視覺密碼學。

典型的 (3, n)-門檻式視覺密碼學是透過兩個大小為 $n \times m$ 基礎矩陣 (basis matrices) M^0 與 M^1 來加密機密影像的白點與黑點 (m 是機密影像的擴展倍率)，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 列的內容填入第 i 張分享投影片中，因此可以產生出 n 張分享投影片。Naor and Shamir [1] 的分享模型是將每一個機密像素點都擴展為 $(2n–2)$ 倍的像素區塊，並且每一個像素區塊出現黑點的機率是 $(n–1)/(2n–2)$，因此在分享投影片上不會洩漏出機密資訊。當重疊任意三張以下的分享投影片後，無論機密影像的內容為何，機密影像黑色部分出現黑點的機率將會等於機密影像白色部分，因此重疊影像上無法解譯出機密資訊。在重疊三張分享投影片時，機密影像黑色部分出現黑點的機率，將會高於機密影像白色部分，並且產生出 $\alpha = 1/(2n–2)$ 的黑白色差。Blundo and De Santis [2] 將每一個機密像素點都擴展為 $(n–1)^2$ 倍的像素區塊，並且透過兩個 $n \times (n–1)^2$ 的基礎矩陣來製作分享模型。在任意重疊三張以上的分享投影片後，機密影像白色部分被重疊出黑點的機率為 $(n^2–2n)/(n–1)^2$，而機密影像黑色部分被重疊出黑點的比例為 1，因此在重疊影像上將會顯示出 $\alpha = 1/(n–1)^2$ 的黑白色差。

不過在上述兩個分享機制中，機密影像的擴展倍率會隨著參與機密分享的人數 (n 值) 增加而愈來愈大，並且重疊影像的黑白色差值也會愈來愈低。Hofmeister [3] 和 Blundo et al. [4] 為了改善 (3, n)-門檻式視覺密碼學在黑白色差不佳的問題，於是透過整數線性規劃法 (integers linear programming，ILP) 來計算出重疊任意三張分享投影片時的最佳黑白色差值分別為 $\alpha = \dfrac{n^2}{[16(n-1)(n-2])}$ 和 $\alpha = \dfrac{\left(n-2\left\lfloor\frac{n+1}{4}\right\rfloor\right)\left\lfloor\frac{n+1}{4}\right\rfloor}{2(n-1)(n-2)}$。雖然他們的分享模型在參與機密分享的人數眾多時能到達到趨近於 1/16 的黑白色差值，不過這兩個分享模型的像素擴展倍率卻增加為 $1.5\,C^n_{n/4}$ 和 $2C^{n-1}_{\lfloor(n+1)/4\rfloor}$，使得視覺機密分享只適合在參與機密分享的人數較少的情況下使用。

傳統 (3, n)-門檻式視覺密碼學在製作分享投影片都是使用像素擴展的方法，像素擴展的結果將會造成傳輸時間與儲存空間的浪費，為了解決像素擴展的問題，於是有學者使用隨機網格 (random grids) 和機率配置 (probability) 的做法來加密機密影像。Kafri and Keren [5] 所提出的隨機網格是以隨機亂數為基礎的機密影像分享機制，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。所謂隨機的意思就是網格內容可以隨機挑選，以黑白影像而言，每一個網格的內容不是透明像素 (0) 就是不透明像素 (1)，各有 50% 的出現機率。因此，加密後的分享投影片上所產生之透

明像素與不透明像素之個數應為相等，即平均透光率為 1/2，其優點是分享模型不需要再建置分享矩陣，並且所產生的分享影像皆與機密影像一樣大。Chen and Tsao [6] 應用 Kafri and Keren [5] 的設計概念，而提出無須像素擴展的 (3, *n*)-門檻式視覺密碼學模型。其作法是先根據每一個機密像素內容來產生兩個隨機網格 r_1 和 r'_2，然後根據隨機網格 r'_2 的內容來產生另外兩個隨機網格 r_2 和 r_3，並且將 r_1、r_2 和 r_3 這三個網格隨機的分配給任意三張分享投影片，而其他 (*n*–3) 張分享投影片的內容則是任意的填入 0 或 1。依照上述的原則將每一個機密像素點加密完畢後，就可以得到 *n* 張與機密影像大小相同的分享投影片，並且重疊任意三張分享投影片後就可以產生出 $\alpha = \frac{12}{9(n)(n-1)(n-2)-6}$ 的黑白色差。Yang et al. [7] 以 Naor and Shamir [1] 所提出的 (*k*, *k*)-門檻式視覺密碼學分享模型為基礎，配合在 (*n*–*k*) 列中的各種 0、1 的組合，產生出一個過於龐大的基礎分享矩陣，再經過化簡的步驟，以產生最後的分享矩陣。

Lin and Chung [8] 為了讓 (3, *n*)-門檻式視覺密碼學適用於大量機密分享參與者的情況下，於是透過機率的方式來設計新型態的分享模型，其優點是可以任意調整參與機密分享的使用者，使得機密分享無論某些參與者新加入或離開時，分享投影片仍然是不需要重新製作。無論參與機密分享的使用者數目為何，當重疊任意 *t* 張分享投片後，在疊合影像上可以產生 $\alpha_t = \frac{4^t - 2\times 3^t + 2}{3\times 4^t}$ 的黑白色差，因此重疊任意三張分享投影片後，疊合影像的黑白色差值為 $\alpha = 1/16$。不過這個分享模型在機密分享參與者較少的情況下，會比 Naor and Shamir [1] 的結果差。

在上述的 (3, *n*)-門檻式視覺密碼學的分享模型中，雖然在重疊三張分享投影片後即可以還原機密資訊，不過還原影像的黑白色差會隨著參與機密分享的參與者人數增加而降低，因此機密影像的型態大多只適合黑白影像，而無法推廣到灰階或彩色影像上。為了改善上述的缺點，於是本研究運用組合數學公式 (combinatorics) 來設計出一個新形態的非擴展型 (3, *n*)-門檻式視覺密碼學的分享模型，使得在疊合 3 張分享投影片時，讓重疊影像的黑白區域出現最佳的黑白色差，也讓還原影像產生極佳的視覺效果。在下面的章節中，第二章是介紹本研究所提出的分享模型，第三章是對本研究所提出的分享模型進行最佳化的設計與討論，第四章是本研究的實驗結果與討論，本篇論文的結論則是第五章。

二、本研究所提出的分享模型

一個典型的 (3, *n*)-門檻式視覺密碼學，是運用一張機密影像來產生 *n* ($n \geq 3$) 張分享投影片，其中機密影像上的每一個像素點，在分享投影片上是用 *m* ($m \geq 1$) 個像素點所形成的像素區塊來代表，並且符合下列條件：

條件 1 (安全性)：為了確保機密影像的安全性，在重疊任意三張以下的分享投影片時，疊合影像上 (包括可能只有單一的分享影片) 的像素區塊內無法產生出黑白色差 (也就是每一個像素區塊被重疊出黑點的比例均相等)，使得在重疊影像上無法顯露出機密資訊的輪廓。

條件 2 (對比性)：為了確保重疊影像的對比性，在重疊任意三張及三張以上的分享投影片後，在代表機密影像的黑點部分的像素區塊內，被重疊出黑點的比例將會大於機密影像的白點部分，因此在重疊影像上會呈現出不同的黑白色差，因此可以利用目視解譯出機密資訊的內容。

在 Naor and Shamir [1] 的 (3, 7)-門檻式視覺密碼學模型中 (表 1)，設計了兩個 7×12 的基礎矩陣 M^0 與 M^1 來分別加密白色機密像素與黑色機密像素。在基礎矩陣中第 *i* 列的值，代表要分配給第 *i* 張分享投影片的內容 (其中 0 代表白色，1 代表黑色)，因此在分享投影片上每一個機密像素點將被擴展為 12 個像素的像素區塊。此外，由於兩個矩陣的列向量內容皆是 6 個 1 和 6 個 0，使得每一個像素區塊的內容皆是六黑六白，因此在分享投影片上不會洩漏出機密資訊的輪廓，藉此確保視覺機密資訊分享的安全性。當任意重疊兩張分享投影片後，疊合影像上的每一個像素區塊的內容皆是七黑五白，使得重疊影像上不會顯露出機密資訊；當任意重疊三張以上的分享投影片後，代表機密白點的像素區塊內容仍

然保持七黑五白，而代表機密黑點的像素區塊內容分別是八黑四白、九黑三白、...、和十二黑零白等種狀況，使得重疊影像上能夠產生黑白的色差，因此重疊影像能夠透過人類的視覺系統直接辨識出機密資訊的內容。

表 1. (3, 7)-門檻式視覺密碼學模型

□	$M^0=\begin{bmatrix}0&1&1&1&1&1&1&0&0&0&0&0\\1&0&1&1&1&1&1&0&0&0&0&0\\1&1&0&1&1&1&1&0&0&0&0&0\\1&1&1&0&1&1&1&0&0&0&0&0\\1&1&1&1&0&1&1&0&0&0&0&0\\1&1&1&1&1&0&1&0&0&0&0&0\\1&1&1&1&1&1&0&0&0&0&0&0\end{bmatrix}$
■	$M^1=\begin{bmatrix}1&0&0&0&0&0&0&1&1&1&1&1\\0&1&0&0&0&0&0&1&1&1&1&1\\0&0&1&0&0&0&0&1&1&1&1&1\\0&0&0&1&0&0&0&1&1&1&1&1\\0&0&0&0&1&0&0&1&1&1&1&1\\0&0&0&0&0&1&0&1&1&1&1&1\\0&0&0&0&0&0&1&1&1&1&1&1\end{bmatrix}$

表 1 的分享模型在製作分享投影片時是使用像素擴展法，因此每一個機密像素被擴展為 12 倍，這個結果除了造成傳輸時間與儲存空間的浪費之外，也會造成被還原的機密影像的外觀扭曲。此外，從表 1 分享模型在還原機密資訊的過程中我們可以發現，機密資訊的黑點部分的黑點出現機率，是隨著疊合分享投影片數目的增加而呈現出等差遞增數列 (6/12、7/12、8/12、9/12、10/12、11/12、12/12)，而機密資訊的白點部分則是呈現出非遞減數列 (6/12、7/12、7/12、7/12、7/12、7/12、7/12)。因此，當要設計一個非擴展型的 (3, n)-門檻式視覺密碼學模型，必須符合下列需求：

需求 1：分享投影片上每一個像素點出現黑點的機率皆相等，並且在機密資訊還原的過程中，機密資訊的黑點部分的黑點出現機率是呈現出等差遞增數列，而機密資訊的白點部分則是呈現出非遞減數列。

需求 2：兩個數列的首項和第二項內容必須相等，使得在任意重疊兩張分享投影片後，疊合影像上每一個像素區塊被重疊出黑點的機率也相等，因此在疊合影像上不會洩露出機密資訊的輪廓。

需求 3：等差遞增數列的第 3 ~ n 項的內容必須大於非遞減數列的內容，使得在任意重疊三張以上分享投影片後，疊合影像上可以產生黑白色差，以解譯出機密資訊的輪廓。

為了達成上述的目標，因此我們設計兩個大小為 $n\times m$ 的分享矩陣 (C^0 和 C^1)，其中每一個行向量皆是一種分享方法，分享模型設計法如下所示：

1. 矩陣 C_0、C_1 分別是代表機密資訊的白點和黑點部分的分享矩陣，其中兩個分享矩陣都包含左右兩個部分，依序是 CL_0、CR_0 和 CL_1、CR_1，矩陣左半部 (CL_0、CL_1) 是為了設計出等差遞增數列 ($<A_i^1>_{i=1}^n$) 和非遞減數列 ($<A_i^2>_{i=1}^n$)，而矩陣右半部 (CR_0、CR_1) 則是為了調整分享投影片的黑點出現機率。
2. 為了在機密影像的白點部分產生出非遞減數列，於是我們設計大小為 $n\times m_0$ 的 CL_0，且內容為利用在 n 個位置中任選 p 個位置的各種排列組合來填入 1 值，因此 $m_0=\binom{n}{p}$。根據漢明編碼 (Hamming code) 的定義可以得知，矩陣內的每一個列向量的漢明權重值 (Hamming weight) 等於 $\binom{n}{p}-\binom{n-1}{p}$，並且任意 i ($1\le i\le n$) 個矩陣列向量進行邏輯 OR 運算的結果，所產生的漢明權重值等於 $\binom{n}{p}-\binom{n-i}{p}$。因此在分享投影片疊合時，針對機密影像的白點部分所產生出非遞減數列為 $<A^2_i>$ = $<\binom{n}{p}-\binom{n-1}{p}, \binom{n}{p}-\binom{n-2}{p}, \ldots, \binom{n}{p}-\binom{p}{p}, \binom{n}{p}, \ldots, \binom{n}{p}>$。
3. 為了讓每一張分享投影片，以及重疊任意兩張分享投影片後皆無法產生出黑白色差，不會暴露機密影像的輪廓，在機密影像的黑點部分所產生出的遞增數列，其中的首項和第二項必須是等於 $\binom{n}{p}-\binom{n-1}{p}$

和 $\binom{n}{p}-\binom{n-2}{p}$，這兩項的差值為 $DIF = A^2{}_2 - A^2{}_1 = \left[\binom{n}{p}-\binom{n-2}{p}\right] - \left[\binom{n}{p}-\binom{n-1}{p}\right] = \binom{n-1}{p}-\binom{n-2}{p}$。因此如果我們運用 DIF 作為差值來產生一個等差遞增數列 $<A^1{}_i> = < \binom{n}{p}-\binom{n-1}{p}$，$\binom{n}{p}-\binom{n-1}{p}+\binom{n-1}{p}-\binom{n-2}{p}$，…，$\binom{n}{p}-\binom{n-1}{p}+(n-1)\left[\binom{n-1}{p}-\binom{n-2}{p}\right]>$，就可在重疊三張以上分享投影片後，使得機密影像的黑色部分更快速的累積黑點，於是可以在重疊影像上產生出所需要的黑白色差。由於等差數列的每一個等差值都等於 $\binom{n-1}{p}-\binom{n-2}{p}$，因此 CL_1 的內容是大小為 $\binom{n-1}{p}-\binom{n-2}{p}$ 個 $n\times n$ 的單位矩陣，使得每一列都有 $\binom{n-1}{p}-\binom{n-2}{p}$ 個 1。

4. 為了讓分享投影片上的每一個像素點出黑點的機率相等，其中矩陣 CL_0 的每一個列向量出現 1 的個數是 $\binom{n}{p}-\binom{n-1}{p}$，而矩陣 CL_1 的列向量出現 1 的個數是 $\binom{n-1}{p}-\binom{n-2}{p}$，因此矩陣 CR_1 是一個大小為 $n\times m_1$，其中 $m_1 = \left[\binom{n}{p}-\binom{n-1}{p}\right] - \left[\binom{n-1}{p}-\binom{n-2}{p}\right] = \binom{n}{p}-2\binom{n-1}{p}+\binom{n-2}{p}$ 且矩陣內的所有元素皆為 1。此外，由於矩陣 CL_1 是一個大小為 $\binom{n-1}{p}-\binom{n-2}{p}$ 個 $n\times n$ 的單位矩陣(主對角線元素為 1，其餘元素為 0，相當於在每一行的 n 個元素中，任選一個位置填入 1)，因此矩陣 CL_1 的大小為 $n\times m_2$，其中 $m_2 = n\left[\binom{n-1}{p}-\binom{n-2}{p}\right]$。因此矩陣 C_1 是一個大小為 $n\times m$，其中 $m = m_1 + m_2 = \binom{n}{p}-2\binom{n-1}{p}+\binom{n-2}{p} + n\left[\binom{n-1}{p}-\binom{n-2}{p}\right] = \binom{n}{p}-\binom{n-1}{p}+(n-1)\left[\binom{n-1}{p}+\binom{n-2}{p}\right]$。為了讓 C_0 和 C_1 的矩陣大小相同，於是矩陣 CR_0 的大小為 $n\times m_3$，其中 $m_3 = m - m_0 = \binom{n}{p}-\binom{n-1}{p}+(n-1)\left[\binom{n-1}{p}+\binom{n-2}{p}\right]-\binom{n}{p} = (n-1)\left[\binom{n-1}{p}+\binom{n-2}{p}\right]-\binom{n-1}{p}$，且矩陣內的所有元素皆為 0。

總結上述的分析，分享矩陣 $C_0 = [CL_0、CR_0]$ 和 $C_1 = [CL_1、CR_1]$ 的大小為 $n\times m$，其中 n 為參與視覺機密分享的人數，$m = m_0+m_3 = m_1+m_2 = \binom{n}{p}-\binom{n-1}{p}+(n-1)\left[\binom{n-1}{p}+\binom{n-2}{p}\right]$，其內容如下：

1. CL_0 的內容為在 n 個位置中任選 p 個位置來填入 1 值的各種排列組合，因此 CL_0 的大小為 $n\times m_0$，其中 $m_0 = \binom{n}{p}$。
2. CR_0 內所有的元素皆為 0，矩陣的大小為 $n\times m_3$，其中 $m_3 = (n-1)\left[\binom{n-1}{p}+\binom{n-2}{p}\right] - \binom{n-1}{p}$。
3. CL_1 是一個大小為 $\binom{n-1}{p}-\binom{n-2}{p}$ 個 $n\times n$ 的單位矩陣，因此矩陣 CL_1 的大小為 $n\times m_2$，其中 $m_2 = n\left[\binom{n-1}{p}-\binom{n-2}{p}\right]$。
4. CR_1 內所有的元素皆為 1，矩陣的大小為 $n\times m_1$，其中 $m_1 = \binom{n}{p}-2\binom{n-1}{p}+\binom{n-2}{p}$。

範例 1：以 (3, 5)-門檻式分享模型且參數值設定為 $p = 3$ 為例，使得 $m_0 = \binom{5}{3} = 10$、$m_1 = \binom{5}{3}-2\times\binom{4}{3}+\binom{3}{3} = 3$、$m_2 = 5\times\left[\binom{4}{3}-\binom{3}{3}\right] = 15$、$m_3 =$

$4\times\left[\binom{4}{3}-\binom{3}{3}\right]-\binom{4}{3}=8$、$m=m_1+m_2=m_0+m_3=18$。我們可以根據上述的分享模型設計法來產生出兩個 5×18 的分享矩陣，如表 2 所示。

表 2. (3, 5)-門檻式視覺密碼學模型 (p = 3)

□	$C_0=\begin{bmatrix}1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\1&1&1&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0\\1&0&0&1&1&0&1&1&0&1&0&0&0&0&0&0&0&0\\0&1&0&1&0&1&1&0&1&1&0&0&0&0&0&0&0&0\\0&0&1&0&1&1&0&1&1&1&0&0&0&0&0&0&0&0\end{bmatrix}_{5\times18}$
■	$C_1=\begin{bmatrix}1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&1&1\\0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&1&1&1\\0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&1&1&1\\0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&1&1&1\\0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&1&1&1\end{bmatrix}_{5\times18}$

依據這個視覺機密分享模型的設計流程，假設 p = 6，讀者也可以很容易的推導出 Naor and Shamir 的 (3, 7)-門檻式視覺密碼學模型 (表 1)。

當要分享機密影像的每一個像素點時，我們每一次都選取一個機率值 R ($0 \le R < 1$) 作為挑選分享內容的參數，當被分享的機密內容是黑色時，我們將選取矩陣 C_1 中第 $\lfloor R\times m \rfloor$ 行所對應的內容，並且將行向量第 1 個值分配給第 1 張分享投影片，第 2 個值分配給第 2 張分享投影片，以此類推，將第 n 個值分配給第 n 張分享投影片；當被分享的機密內容是白色時，我們將選取矩陣 C_0 中第 $\lfloor R\times m \rfloor$ 行所對應的內容，並且用同樣的方法來進行像素點分配，詳細的分享投影片製作流程請參考圖 1。

根據上述的演算法流程，我們可以得知本研究所提出分享模型的執行速度，是根據視覺機密分享的參與者個數 (n) 與機密影像的大小 ($W\times H$)，於是演算法的時間複雜度是 O(nWH)。在空間複雜度上，需要配置分享投影片與分享矩陣的空間。每一張分享投影片所需要的空間是 WH，通常影像的大小遠大於 C_0 和 C_1 兩個分享矩陣的大小，因此分享矩陣的空間可以忽略不計，使得空間複雜度也是 O(nWH)。

Algorithm:
Input: a halftoned secret image P which size is $W\times H$ and n participators
Output: n transparencies T_s, s = 1, 2, ..., and n
Process：
1. Construct two sharing matrixes C_0 and C_1
2. For $i \leftarrow 1$ to W do
3. For $j \leftarrow 1$ to H do
4. $R \leftarrow$ Randomize Probability value ($0 \le R < 1$)
5. $u \leftarrow \lfloor R\times m \rfloor$
6. IF $P(i, j)$ is black
7. For $v \leftarrow 1$ to n
8. $T_v(i, j) = C_1(v, u)$
9. ELSE
10. For $v \leftarrow 1$ to n
11. $T_v(i, j) = C_0(v, u)$

圖 1. 演算法。

三、效能評估

根據第三章的矩陣設計，在 n 位視覺機密分享參與者且 $2 \le p \le (n–1)$ 的情況下，當重疊 $q\,(1 \le q \le n)$ 張分享投影片後，在疊合影像上對應機密影像黑色部分有 $\left\{\binom{n}{p}-\binom{n-1}{p}+(q-1)\left[\binom{n-1}{p}-\binom{n-2}{p}\right]\right\}\Big/m$ 的機率被重疊出黑點，而機密白點部分會有 $\left[\binom{n}{p}-\binom{n-q}{p}\right]\Big/m$ 的機率被重疊出黑點，因此重疊影像上的黑白對比度為 $\alpha_p^q = \left\{\binom{n}{p}-\binom{n-1}{p}+(q-1)\left[\binom{n-1}{p}-\binom{n-2}{p}\right]\right\}\Big/m - \left[\binom{n}{p}-\binom{n-q}{p}\right]\Big/m$，其中 $m = \binom{n}{p}-\binom{n-1}{p} + (n-1)\left[\binom{n-1}{p}+\binom{n-2}{p}\right]$。

$$\alpha_p^q = \frac{\binom{n}{p}-\binom{n-1}{p}+(q-1)\left[\binom{n-1}{p}-\binom{n-2}{p}\right]-\left[\binom{n}{p}-\binom{n-q}{p}\right]}{\binom{n}{p}-\binom{n-1}{p}+(n-1)\left[\binom{n-1}{p}-\binom{n-2}{p}\right]}$$

$$= \frac{(q-2)\binom{n-1}{p}-(q-1)\binom{n-2}{p}+\binom{n-q}{p}}{\binom{n}{p}-(n-2)\binom{n-1}{p}+(n-1)\binom{n-2}{p}} = \frac{\frac{(q-2)(n-1)!}{p!(n-p-1)!}-\frac{(q-1)(n-2)!}{p!(n-p-2)!}+\frac{(n-q)!}{p!(n-p-q)!}}{\frac{n!}{p!(n-p)!}-\frac{(n-2)(n-1)!}{p!(n-p-1)!}+\frac{(n-1)(n-2)!}{p!(n-p-2)!}}$$

$$= \frac{\frac{(n-2)!}{p!(n-p-1)!}\left[(q-2)(n-1)-(q-1)(n-p-1)\right]+\frac{(n-q)!}{p!(n-p-q)!}}{\frac{(n-1)!}{p!(n-p)!}\left[n+(n-2)(n-p)-(n-p)(n-p-1)\right]}$$

$$= \frac{\frac{(n-2)!(qp-p-n+1)}{(n-p-1)!}+\frac{(n-q)!}{(n-p-q)!}}{\frac{(n-1)!\,p(n-p+1)}{(n-p)!}} \qquad (1)$$

根據上述的分析可以得知，將 $q = 1$ (代表只有一張分享投影片) 帶入等式 (1)後，分享投影片上的黑白對比度等於 0，因此在每一張分享投影片上都不會洩漏出機密資訊的輪廓。將 $q = 2$ (代表重疊任意兩張分享投影片) 帶入等式 (1) 後，重疊影像上的黑白對比度也是等於 0，因此在疊合影像上無法解譯出任何機密資訊。當任意重疊三張以上的分享投影片 (將 $q \ge 3$ 帶入等式 (1) 後)，疊合影像的黑白對比度將會大於 0，因此可以解譯出機密資訊的內容，而達成 $(3, n)$-門檻式視覺密碼學的目標。

$$\alpha_p^3 = \frac{\frac{(n-2)!(3p-p-n+1)}{(n-p-1)!}+\frac{(n-3)!}{(n-p-3)!}}{\frac{(n-1)!\,p(n-p+1)}{(n-p)!}}$$

$$=\frac{\frac{(n-1)!}{p!(n-p-1)!}-\frac{2(n-2)!}{p!(n-p-2)!}+\frac{(n-3)!}{p!(n-p-3)!}}{\frac{n!}{p!(n-p)!}-\frac{(n-1)!}{p!(n-p-1)!}+(n-1)\left[\frac{(n-1)!}{p!(n-p-1)!}-\frac{(n-2)!}{p!(n-p-2)!}\right]}$$	
$$=\frac{\frac{(n-3)!}{(n-p-1)!}\left[(n-2)(2p-n+1)+(n-p-1)(n-p-2)\right]}{\frac{(n-1)!\,p(n-p+1)}{(n-p)!}}$$	
$$=\frac{\frac{(n-3)!\,p(p-1)}{(n-p-1)!}}{\frac{(n-1)!\,p(n-p+1)}{(n-p)!}}=\frac{(p-1)(n-p)}{(n-1)(n-2)(n-p+1)}=\frac{1}{(n-1)(n-2)}\left[p-\frac{n}{(n-p+1)}\right]$$	(2)

當重疊 3 張分享投影片後 ($q = 3$)，等式 (1) 可以改寫成等式 (2)。經過等式 (2) 的推導過程可以發現，重疊影像的黑白色差值 α_p^3 是一個由參數 n 和 p 所組成的連續函數，其中 n 為常數，代表參與視覺機密分享的人數，p 為在 n 個位置中填入 1 的個數，是本研究唯一的變數。當 α_p^3 對 p 值進行偏微分後，所得到的一階導函數值等於 0 的位置，就是 α_p^3 的極值，如等式 (3) 所示。

$$\frac{\partial\alpha_p^3}{\partial p}=\frac{\partial}{\partial p}\left(\frac{1}{(n-1)(n-2)}\left[p-\frac{n}{(n-p+1)}\right]\right)=\frac{1}{(n-1)(n-2)}\frac{\partial}{\partial p}\left(p-\frac{n}{(n-p+1)}\right)$$ $$=\frac{1}{(n-1)(n-2)}\left[1-\frac{0-n(-1)}{(n-p+1)^2}\right]=\frac{1}{(n-1)(n-2)}\left[\frac{(n+1-p)^2-n}{(n-p+1)^2}\right]=0$$	
$\therefore (n-p+1)^2-n=0 \Rightarrow p=n-n^{0.5}+1$	(3)

當連續函數 α_p^3 對 p 值進行二次偏微分後，以 $p = n–n^{0.5}+1$ 帶入所得到的二階導函數，如果二階導函數值小於 0，就代表以 $p = n–n^{0.5}+1$ 帶入 α_p^3 所求到的值就是極大值，也就是重疊三張分享投影片時所產生的黑白色差值是最佳的結果。

由等式 (4) 的結果可以發現，α_p^3 二階導函數值小於 0，表示以 $p = n–n^{0.5}+1$ 帶入 (2) 式確實可以讓還原影像的黑白色差 (α_p^3) 達到極大值。也就是說，在設計 CL_0 時，應該要選擇「在 n 個位置中填入 $p\,(= n–n^{0.5}+1)$ 個 1」的設計，才能在重疊 3 張分享投影片時，得到最大的色差對比。當 p 值離開中心 $n–n^{0.5}+1$ 越遠，α_p^3 的值就越小。因為 p 必須是正整數，因此本研究就採用最接近的整數，$\lceil n–n^{0.5}+1\rceil$ 或 $\lfloor n–n^{0.5}+1\rfloor$ 來代替，就可以求到最接近理論上的最大值。

$$\frac{\partial^2\alpha_p^{3\,\text{L}}}{\partial^2 p}=\frac{\partial}{\partial p}\left(\frac{1}{(n-1)(n-2)}\left[1-\frac{n}{(n-p+1)^2}\right]\right)=\frac{1}{(n-1)(n-2)}\frac{\partial}{\partial p}\left(\left[1-\frac{n}{(n-p+1)^2}\right]\right)$$	
$$=\frac{-n}{(n-1)(n-2)}\frac{\partial}{\partial p}\left(\frac{1}{(n-p+1)^2}\right)=\frac{-n}{(n-1)(n-2)}\frac{(-2)(n-p+1)(-1)}{(n-p+1)^4}$$	
$=\frac{-2n}{(n-1)(n-2)(n-p+1)^3}<0$ (以 $p = n–n^{0.5}+1$ 帶入上式)	(4)

假設 x 是正整數，如果 $n^{0.5}$ 值是介於 x 到 $x+0.5$ 之間，也就是 $x^2 \le n \le (x+0.5)^2 = x^2+x+0.25$，因為 n 必須是整數，因此當 n 是介於 x^2 到 x^2+x 之間的整數時，$n^{0.5}$ 值比較接近 x，我們可以取 $p = \lceil n-n^{0.5}+1 \rceil = n+1-\lfloor n^{0.5} \rfloor$；如果 $n^{0.5}$ 值是介於 $x+0.5$ 到 $x+1$ 之間，也就是 $(x+0.5)^2 \le n \le (x+1)^2$，因此當 n 是介於 x^2+x+1 到 x^2+2x+1 之間的整數時，$n^{0.5}$ 值比較接近 $x+1$，我們可以取 $p = \lfloor n-n^{0.5}+1 \rfloor = n+1-\lceil n^{0.5} \rceil$。

當重疊所有的分享投影片後 ($q = n$)，等式 (1) 可以改寫成等式 (5)。以 $p = n-n^{0.5}+1$ 帶入等式 (5)，就可以得到疊合所有的分享投影片後的黑白色差對比。此外，由等式 (5) 還可以發現還原影像的黑白色差值 α_p^n 會隨著參與者 (n 值) 的增加而越來越大，最後當 n 值趨近於無窮大時，α_p^n 將會逐漸趨近於 1，而這個還原影像的黑白色差優於其他 (3, n)-門檻式視覺密碼學的相關研究。

$$\alpha_p^n = \frac{\frac{(n-2)!(np-p-n+1)}{(n-p-1)!} + \frac{(n-n)!}{(n-p-n)!}}{\frac{(n-1)!p(n-p+1)}{(n-p)!}} = \frac{\frac{(n-2)!(np-p-n+1)}{(n-p-1)!}}{\frac{(n-1)!p(n-p+1)}{(n-p)!}}$$

$$= \frac{\frac{(n-2)!(n-1)(p-1)}{(n-p-1)!}}{\frac{(n-1)!p(n-p+1)}{(n-p)!}} = \frac{(n-p)(p-1)}{p(n-p+1)} = \frac{np-p^2-n+p}{p(n-p+1)} = 1-\frac{n}{p(n-p+1)} \quad (5)$$

因此，如果我們以「選擇在 n 列中任選 $p = n-n^{0.5}+1$ 個位置來填入 1 值」的各種排列組合的方式，來設計分享矩陣的 CL_0 的話，本研究所提出的分享模型就可以在疊合 3 張分享投影片時，讓重疊影像的黑白區域出現最佳的黑白色差，也讓還原影像產生極佳的視覺效果。

四、實驗結果與分析討論

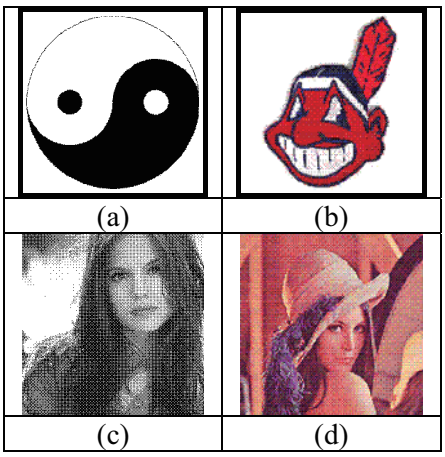
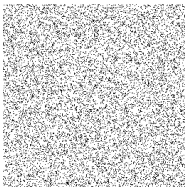
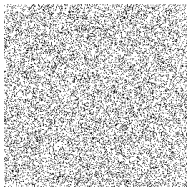
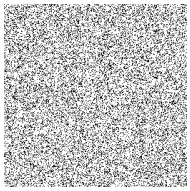
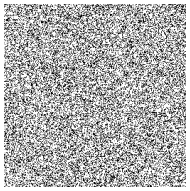
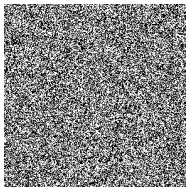
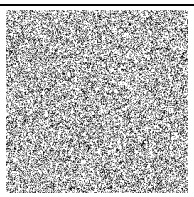
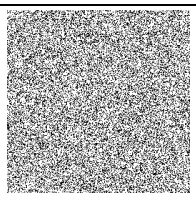
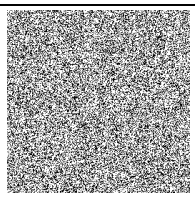
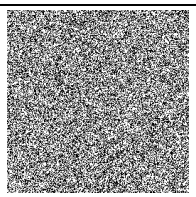
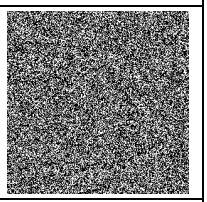
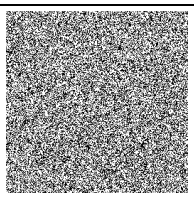
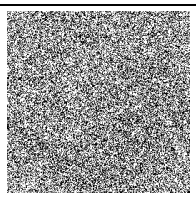
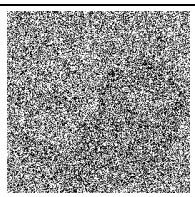
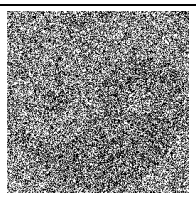
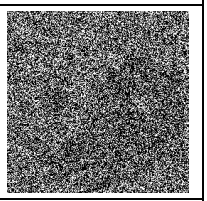
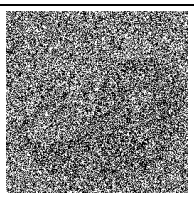
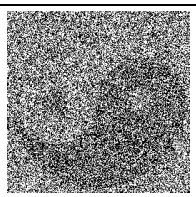
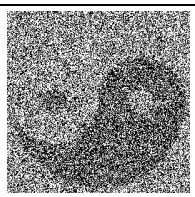
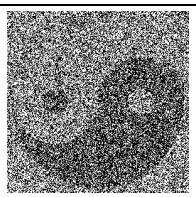
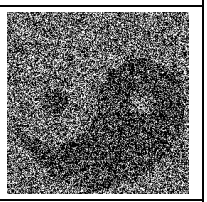
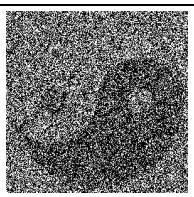
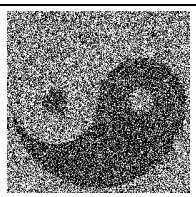
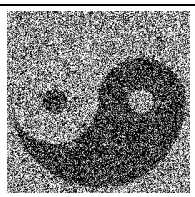
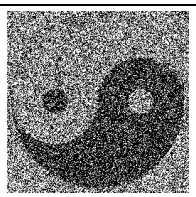
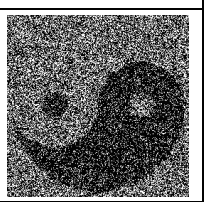


圖 2. (a) Tai-chi，(b) Indians，(c) Mena，(d) Lena。

本實驗是在作業系統 Microsoft Windows 7 的環境下，以 Java (JDK 1.6.21)程式語言作為開發環境，硬體設備為個人桌上型電腦 CPU Intel Core(tm) i7-920 2.67GHz 和 RAM 24GB。實驗圖像是四張大小為 256×256 且經過半色調處理後的 BMP 格式影像，分別是黑白影像 Tai-chi、彩色卡通影像 Indians、灰階影像 Mena 和彩色影像 Lena，如圖 2.(a) ~ 圖 2.(d)所示。

本研究首先選取黑白機密影像 Tai-chi 來製作 (3, 7)-門檻式密碼學模型，而圖 3 是不同參數設定下的機密資訊還原結果。根據圖 3 的實驗結果可以發現，無論視覺機密分享的參數 (p 值) 為何，在分享投影片上的每一個像素點出現黑點的機率都是相同的，並且顏色的分配是透過隨機亂數，因此每一張分享投影片都可以被視為是安全的 (圖 3.(a1) – (e1))。當任意重疊兩張分享投影片後，無論機密影像的像素點內容為何，重疊影像上的每一個像素點被重疊出黑點的機率也相等，因此在重疊影像上也無法辨識出機密影像的內容 (圖 3.(a2) – (e2))。當任意重疊三張的分享投影片後，由於機密黑色像素點累積黑點的機率是呈

現出等差遞增數列，而機密白色像素點則是呈現出非遞增數列，因此機密黑色部分出現黑點的機率將會高於機密白色部分，使得重疊影像能夠可以產生出黑白色差而解譯出機密資訊的內容，如圖 3.(a3)～圖 3.(e3) 所示。當 $p = n–n^{0.5}+1 = 5$ 時，重疊影像黑白色差值 $\alpha^3_5 = 8.89\%$ 將會優於其他參數設定的結果 (圖 3.(d3))，表示採用「在 7 個位置中任選 5 個位置來填入 1 值」的方式來設計 CL_0 的內容，可以在疊合 3 張分享投影片時得到最佳的色差對比，達到 (3, n)-門檻式視覺密碼學的要求。隨著被重疊的分享投影片的數目增加，疊合影像的黑白色差值逐漸提升，當重疊所有的分享投影片後，還原影像的黑白色差值大於或等於 41.67%，使得機密資訊能夠清晰地被人眼所辨識，如圖 3.(a7)～ 圖 3.(e7) 所示。

	$p = 2$	$p = 3$	$p = 4$	$p = 5$	$p = 6$
$q = 1$					
	(a1) $\alpha^1_2 = 0$	(b1) $\alpha^1_3 = 0$	(c1) $\alpha^1_4 = 0$	(d1) $\alpha^1_5 = 0$	(e1) $\alpha^1_6 = 0$
$q = 2$					
	(a2) $\alpha^2_2 = 0$	(b2) $\alpha^2_3 = 0$	(c2) $\alpha^2_4 = 0$	(d2) $\alpha^2_5 = 0$	(e2) $\alpha^2_6 = 0$
$q = 3$					
	(a3) $\alpha^3_2 = 0.028$	(b3) $\alpha^3_3 = 0.053$	(c3) $\alpha^3_4 = 0.075$	(d3) $\alpha^3_5 = 0.089$	(e3) $\alpha^3_6 = 0.083$
$q = 4$					
	(a4) $\alpha^4_2 = 0.083$	(b4) $\alpha^4_3 = 0.147$	(c4) $\alpha^4_4 = 0.188$	(d4) $\alpha^4_5 = 0.200$	(e4) $\alpha^4_6 = 0.167$
$q = 5$					
	(a5) $\alpha^5_2 = 0.167$	(b5) $\alpha^5_3 = 0.267$	(c5) $\alpha^5_4 = 0.313$	(d5) $\alpha^5_5 = 0.311$	(e5) $\alpha^5_6 = 0.250$

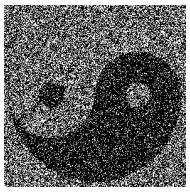
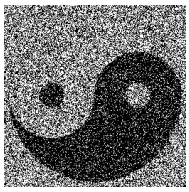
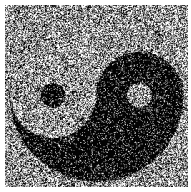
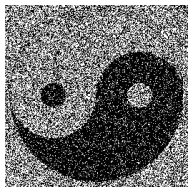
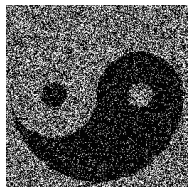
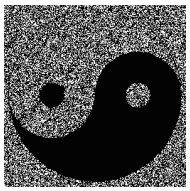
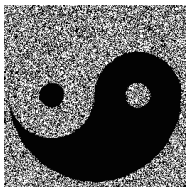
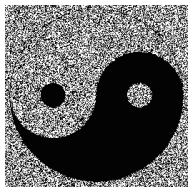
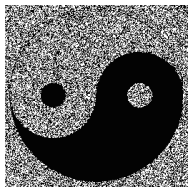
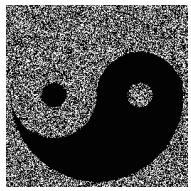
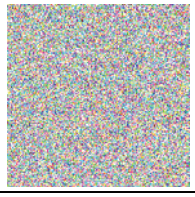
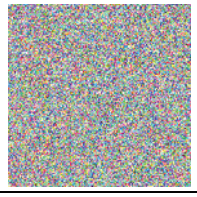
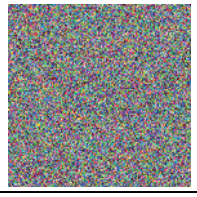
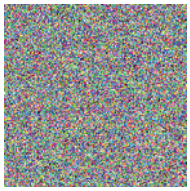
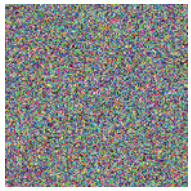
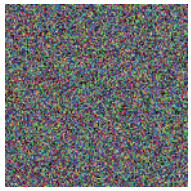
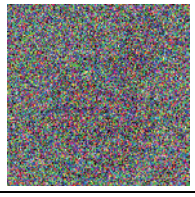
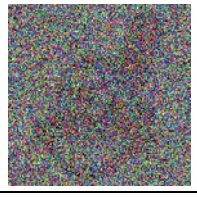
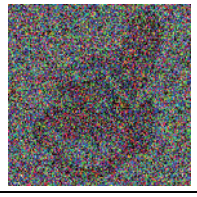
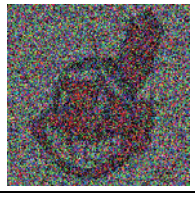
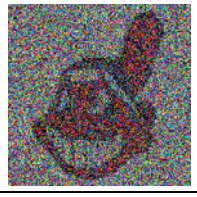
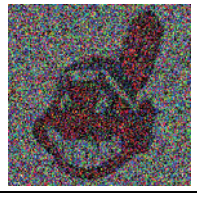
$q = 6$					
	(a6) $\alpha^6_2 = 0.278$	(b6) $\alpha^6_3 = 0.400$	(c6) $\alpha^6_4 = 0.438$	(d6) $\alpha^6_5 = 0.422$	(e6) $\alpha^6_6 = 0.333$
$q = 7$					
	(a7) $\alpha^7_2 = 0.417$	(b7) $\alpha^7_3 = 0.533$	(c7) $\alpha^7_4 = 0.563$	(d7) $\alpha^7_3 = 0.533$	(e7) $\alpha^7_6 = 0.417$

圖 3. (3, 7)-門檻式密碼學模型的機密還原結果，以黑白影像 Tai-chi 為例。

圖 4 是選取彩色卡通影像 Indians 來製作 (3, 5)-門檻式密碼學模型的實驗結果。由實驗的結果可以發覺當 $p = n–n^{0.5}+1 = 4$ 時，重疊影像黑白色差值 $\alpha^3_4 = 12.5\%$ 將會優於其他參數設定的結果 (圖 4. (c3))，表示採用「在 5 個位置中任選 4 個位置來填入 1 值」的方式來設計 CL_0 的內容，確實可以在疊合 3 張分享投影片時得到最佳的色差對比。

	$p = 2$	$p = 3$	$p = 4$
$q = 1$			
	(a1) $\alpha^1_2 = 0$	(b1) $\alpha^1_3 = 0$	(c1) $\alpha^1_4 = 0$
$q = 2$			
	(a2) $\alpha^2_2 = 0$	(b2) $\alpha^2_3 = 0$	(c2) $\alpha^2_4 = 0$
$q = 3$			
	(a3) $\alpha^3_2 = 0.063$	(b3) $\alpha^3_3 = 0.111$	(c3) $\alpha^3_4 = 0.125$
$q = 4$			
	(a4) $\alpha^4_2 = 0.188\%$	(b4) $\alpha^4_3 = 0.167$	(c4) $\alpha^4_4 = 0.250$

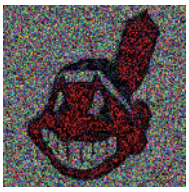
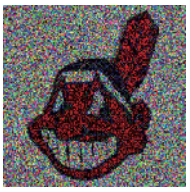
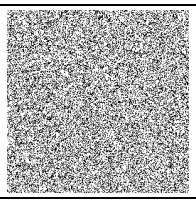
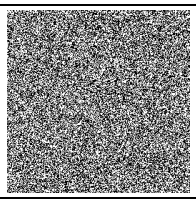
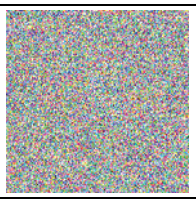
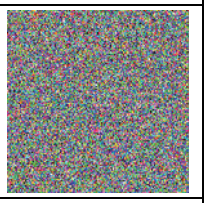
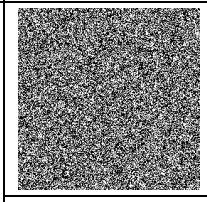
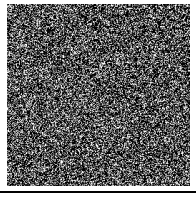
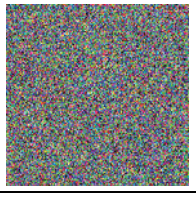
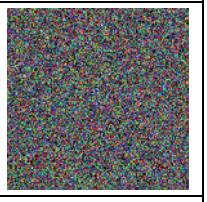
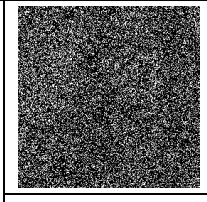
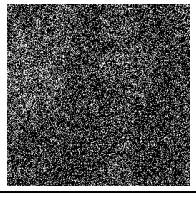
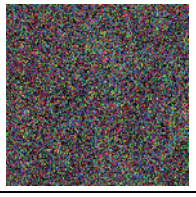
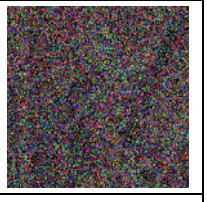
$q = 5$			
	(a5) $\alpha^5_2 = 0.375$	(b5) $\alpha^5_3 = 0.444$	(c5) $\alpha^5_4 = 0.375$

圖 4. (3, 5)-門檻式密碼學模型的機密還原結果，以彩色影像 Indians 為例。

根據上述兩個實驗的結果可以發現下列事實：第一，根據等式 (3) 來挑選實驗參數後，這兩個實驗所選取的參數分別是 $p = 5$ 和 $p = 4$，使得重疊三張分享投影片後的疊合影像黑白色差值為 $\alpha^3_5 = 8.89\%$ (圖 3.(d3)) 和 $\alpha^3_4 = 12.50\%$ (圖 4.(c3))，將會優於其他參數設定的結果，並且在還原影像上產生極佳的視覺效果 $\alpha^7_5 = 53.33\%$ (圖 3.(d7)) 和 $\alpha^5_4 = 37.50\%$ (圖 4.(c5))，使得機密資訊能夠清晰地被人類視覺系統所辨識。第二，無論機密影像的型態為何，本研究所產生的分享投影片大小都會與機密影像相同，因此不會造成儲存空間的浪費。第三，隨著被重疊的分享投影片數目的增加，疊合影像的色差值將會愈來愈高，因此本研究所提出的分享模型也屬於漸進式視覺密碼學的範疇。

此外，為了驗證本研究所提出的分享模型對於圖形結構較為複雜的灰階影像和彩色影像也具有同樣的效果，於是我們以灰階影像 Mena 和彩色影像 Lena 為對象，來實作 (3, 4)-門檻式密碼學模型。根據圖 5 的實驗結果可以發現，重疊任意三張分享影像後即可解譯機密資訊，而且當 $p = n - n^{0.5} + 1 = 3$ 時，重疊影像黑白色差值 $\alpha^3_3 = 16.7\%$ 將會優於 $p = 2$ 的結果 (圖 5. (a3) ~ 圖 5.(d3))。因此，可以驗證本研究所提出的分享模型適合任何型態的機密影像。

	$p = 2$	$p = 3$	$p = 2$	$p = 3$
$q = 1$				
	(a1) $\alpha^1_2 = 0$	(b1) $\alpha^1_3 = 0$	(c1) $\alpha^1_2 = 0$	(d1) $\alpha^1_3 = 0$
$q = 2$				
	(a2) $\alpha^2_2 = 0$	(b2) $\alpha^2_3 = 0$	(c2) $\alpha^2_2 = 0$	(d2) $\alpha^2_3 = 0$
$q = 3$				
	(a3) $\alpha^3_2 = 0.111$	(b3) $\alpha^3_3 = 0.167$	(c3) $\alpha^3_2 = 0.111$	(d3) $\alpha^3_3 = 0.167$

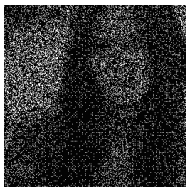
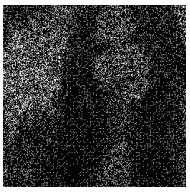
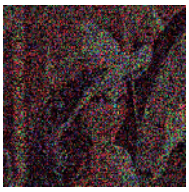
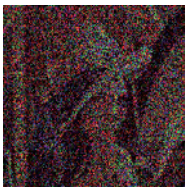
$q = 4$				
	(a4) $\alpha^4_2 = 0.333$	(b4) $\alpha^4_3 = 0.333$	(c4) $\alpha^4_2 = 0.333$	(d4) $\alpha^4_3 = 0.333$

圖 5. (3, 4)-門檻式密碼學模型的機密還原結果，以灰階影像 Mena 和彩色影像 Lena 為例。

表 3 是不同參數設定後，重疊任意三張分享投影片後的黑白色差結果比較表。當 n 值介於 4 ~ 6 之間時，由於 $n^{0.5}$ 值的結果是比較接近正整數 2 ($2< n^{0.5}<2.5$)，因此我們選取 $p = \lceil n - n^{0.5} + 1 \rceil = n - 1$ 作為實驗參數；當 n 值介於 7 ~ 9 之間時，由於 $n^{0.5}$ 值的結果是比較接近正整數 3 ($2.5< n^{0.5}<3$)，因此我們選取 $p = \lfloor n - n^{0.5} + 1 \rfloor = n - 2$ 作為實驗參數。根據上述的參數選擇結果可以發現，在 $p = n - n^{0.5} + 1$ 時，重疊影像的黑白色差都會優於其他參數設定的結果，顯示本研究所提出的「在 n 個位置中任選 p 個位置來填入 1 值」的方式來設計 CL_0 的內容，確實可以在疊合 3 張分享投影片時，讓重疊影像的黑白區域出現最佳的黑白色差。

表 3. 重疊三張分享投影片的黑白色差結果

	$p = 2$	$p = 3$	$p = 4$	$p = 5$	$p = 6$	$p = 7$	$p = 8$
$n = 4$	11.11%	**16.67%**	—	—	—	—	—
$n = 5$	6.25%	11.11%	**12.50%**	—	—	—	—
$n = 6$	4.00%	7.50%	10.00%	**10.00%**	—	—	—
$n = 7$	2.78%	5.33%	7.50%	**8.89%**	8.33%	—	—
$n = 8$	2.04%	3.97%	5.71%	7.14%	**7.94%**	7.14%	—
$n = 9$	1.56%	3.06%	4.46%	5.71%	6.70%	**7.14%**	6.25%

最後，為了驗證本研究分享模型的效能，於是我們將本研究與相關研究比較整理成表 4，其中 α^3、α^n 分別是代表重疊 3 張和 n 張分享投影片的重疊影像黑白色差，m 則是代表分享模型的擴展倍率。

在黑白色差對比度方面，當 n 值逐漸變大時，重疊影像的黑白色差值將會愈來愈差。由 Blundo and De Santis [2] 和 Chen and Tsao [6] 的實驗結果可以發現，當 n 值逐漸變大時，α^3、α^n 將會逐漸趨近於 0，使得機密資訊無法被人眼所辨識。反觀在 Hofmeister [3]、Blundo et al. [4] 和 Lin and Chung [8] 的分享模型中，α^3、α^n 將會逐漸收斂於一個常數值，因此重疊影像上能夠產生出足以為人眼辨識的黑白色差。在本研究所提出的分享模型中，當 $n = 8$ 時，$\alpha^3 = 5/63$ (≒7.94%) 和 $\alpha^n = 5/9$ (≒55.56%)，並且當 n 值趨向於無限大時，α^n 將會逐漸趨近於 1，而這個還原影像的黑白色差優於其他 (3, n)-門檻式視覺密碼學的相關研究。

在分享模型的擴展倍率方面，Naor and Shamir [1]、Blundo and De Santis [2]、Hofmeister [3] 和 Blundo et al. [4] 都是透過像素擴展來製作分享投影片，像素擴展的倍率隨著參與者 (n 值) 的增加而越來越大，最後當 n 值趨近於無窮大時，m 值也會逐漸趨近於無窮大。Chen and Tsao [6] 是使用隨機網格來設計分享模型，Yang et al. [7]、Lin and Chung [8] 和本研究則是使用機率的方法來設計分享模型，因此像素擴展的倍率隨著參與者的增加仍然保持不變 ($m = 1$)，使得分享投影片的大小將會與機密影像相同。

表 4. 本研究與相關 (3, *n*)-門檻式視覺密碼學模型之比較表

	n	**3**	**4**	**5**	**6**	**7**	**8**
Naor and Shamir [1]	α^3	1/4	1/6	1/8	1/10	1/12	1/14
	α^n	1/4	1/3	3/8	2/5	5/12	3/7
	m	4	6	8	10	12	14
Blundo and De Santis [2]	α^3	1/4	1/9	1/16	1/25	1/36	1/49
	α^n	1/4	1/9	1/16	1/25	1/36	1/49
	m	4	9	16	25	36	49
Hofmeister et al. [3]	α^3	1/4	1/6	1/8	1/10	1/10	2/21
	α^n	1/4	1/3	3/8	2/5	3/10	1/3
	m	4	6	8	10	30	42
Blundo et al. [4]	α^3	1/4	1/6	1/8	1/10	1/10	2/21
	α^n	1/4	1/3	3/8	2/5	3/10	1/3
	m	4	6	8	10	30	42
Chen and Tsao [6]	α^3	1/4	1/8	1/16	1/32	1/64	1/128
	α^n	1/4	1/8	1/16	1/32	1/64	1/128
	m	1	1	1	1	1	1
Yang et al. [7]	α^3	1/4	1/6	1/8	1/10	1/12	1/14
	α^n	1/4	1/3	3/8	2/5	5/12	3/7
	m	1	1	1	1	1	1
Lin and Chung [8]	α^3	1/16	1/16	1/16	1/16	1/16	1/16
	α^n	1/16	1/8	45/256	55/256	1001/4096	273/1024
	m	1	1	1	1	1	1
本研究的實驗結果	*p*	2	3	4	5	5	6
	α^3	1/4	1/6	1/8	1/10	4/45	5/63
	α^n	1/4	1/3	3/8	2/5	8/15	5/9
	m	1	1	1	1	1	1

五、結論

視覺密碼技術是機密分享領域下的一個新興領域，其主要的特色在於還原機密影像時，不需要任何計算方式即可進行解密，而是直接重疊所有分享投影片即可以視覺系統進行解密，改進了傳統密碼學在解密過程中須大量複雜運算的缺點。視覺密碼學的加密過程是將一張機密影像分散成 n 張無意義的分享投影片，並分別給 n 個成員保管，若要解得機密訊息，只要有 k ($k \le n$) 個以上的成員將自己所持有的投影片正確重疊後，由人類視覺系統判讀即可以還原機密影像。反之，如果只有 $1 \sim k-1$ 張分享投影片時，重疊影像就無法取得機密訊息，這就是視覺密碼中的 (k, n)-門檻式視覺密碼學。

本研究運用不同的排列組合來設計分享

矩陣，使得重疊影像的黑白區域出現最佳的黑白色差，也讓還原影像產生極佳的視覺效果。相較於 (3, n)-視覺分享機制的相關研究，本研究具備下列幾項特點：

1. 設計概念十分單純，易於實作。
2. 以「在 n 個位置中任選 $p = n - n^{0.5} + 1$ 個位置來填入 1 值」的方式來設計 CL_0 的內容，可以在重疊任意 3 張分享投影片時出現最佳的黑白色差，並且在還原影像產生極佳的視覺效果，優於其他 (3, n)-門檻值密碼學的研究成果。
3. 本研究所提出的分享模型適合任何型態的機密影像。
4. 分享投影片的大小將與機密影像相同。

誌謝

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 NSC101-2221-E-032-047 的部份研究成果，謹此致謝。

參考文獻

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

[2] Blundo, C., and De Santis, A., “Visual cryptography schemes with perfect reconstruction of black pixels,” Computer Graphics, Vol. 22, No. 4, pp. 449-455, 1998.

[3] Hofmeister, T., Krause, M., and Simon, H. U., “Contrast-optimal k out of n secret sharing schems in visual cryptography,” Theoretical Computer Science, Vol. 240, No. 2, pp. 471-485, 2000.

[4] Blundo, C., D’Arco P., De Santis, A., Stinson, D. R., “Contrast optimal threshold visual cryptography schemes,” SIAM Journal on Discrete Mathematics, Vol. 16, No. 2, pp. 224-261, 2003.

[5] Kafri, O. and Keren, E., “Encryption of pictures and shapes by random grids,” Optics Letters, Vol. 12, No. 6, pp. 377-379, 1987.

[6] Chen, T. H. and Tsao K. H., “Threshold visual secret sharing by random grids,” Journal of Systems and Software, Vol. 84, No. 2, pp. 1197-1208, 2011.

[7] Yang, C. N., Wu, C. C., and Liu F., “Construction of general (k, n) probabilistic visual cryptography scheme,” Journal of Electronic Science and Technology, Vol. 9, No. 4, pp. 317-324, 2011.

[8] Lin, S. J. and Chung W. H., “A probabilistic model of (t, n) visual cryptography scheme with dynamic group,” IEEE Transactions on Information Forensics and Security, Vol. 7, No. 1, pp. 197-207, 2012.