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

Quan, Zen-Yu\textsuperscript{1}, Hou, Young-Chang\textsuperscript{2*}, and Tsai, Chih-Fong\textsuperscript{1}

\textsuperscript{1}Department of Information Management, National Central University
\textsuperscript{2}Department of Information Management, Tamkang University

\textbf{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.

\textbf{Keywords:} secret sharing, visual cryptography, (3, n)-threshold visual cryptography, combinatorics.
一、前言

密码学（cryptography）是一門研究如何隱藏資訊的學問，其作法是透過加密算法將明文（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，使得攜帶者在有限時間內無法破解密文，不過傳統密碼學的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和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，使用者不必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個機密影像分解成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效用。當要解譯機密時，只要任意k張（2 ≤ k ≤ n）其中k張重疊時，就可以產生出足以人眼所辨認的黑白色差，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=1時，將會造成重疊影像的識別效果愈來愈差，使得視覺密碼學的應用性受到侷限。而在（k,n）-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×m基礎矩陣（basis matrices）M’與M來加密機密影像的白點與黑點（m是機密影像的擴展倍率）的加密方法是將機密影像上的白點（或黑點）逐一處理，如果為白點（黑點）的話，就將M’（M）做欄向量隨機重排，然後將第i列的內容放入第i張分享投影片中，因此可以產生出n張分享投影片。Naor和Shamir[1]的分享模型是將每個機密像素點擴展為（2n–2）倍的像素區塊，並且每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機密資訊。當重疊任意張以上的分享投影片後，無論機密影像的內容為何，機密影像部分出現黑點的機率將會等於機密影像黑色部分，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，將會高於機密影像黑色部分，並且產生出α=1/（2n–2）的黑白色差。

Blundo和De Santis[2]將每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×（n–1）²的基礎矩陣來製作分享投影片。在任意重疊三張以上的分享投影片時，機密影像黑色部分被重疊出黑點的機率為（n²–2n–1）/（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α=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差值也會愈來愈小。Hofmeister[3]和Blundo et al.[4]為了改善（3,n）-門檻式視覺密碼學在黑白差不佳的問題，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α=n²/(16(n–1)(n–2))和α=(n–2)(n+1)/4。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1.5C₄ⁿ和2Cⁿ⁺¹/(n+1)/4，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和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，其中每個網格內容必須符合隨機變數的要求。所謂隨機規則就是網格內容可隨機挑選，以黑白影像而言，每個網格內容不是透明像素（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
明像素与不透明像素之个数应为相等，即平均透光率为1/2，其优点是分享模型不需要再建立积分矩阵，且在所产生的分享影像皆与密影像一致大。Chen and Taso [6] 应用 Kafri and Keren [5] 的设计概念，而提出无须像素扩展的(3, n)-门框式视觉密码学模型。其作法是先根据任一随机像素内容来产生两个随机网络 r_1 和 r_2，然后根据随机网络 r_3 的内容来产生另外两个随机网络 r_2 和 r_3，且将 r_1、r_2 和 r_3 三个随机网络的分配给任意三张分享投影片。而其他 (n-3) 张分享投影片的内容则是随机的填充 0 或 1。依照上述的原则将每个随机像素点加密完毕后，就可以得到 n 张与密影影像大小相同的分享投影片，并且重叠任意三张分享投影片后就可以产生出 $a = \frac{12}{9(n-1)(n-2)-6}$ 的黑白色差。

Yang et al. [7] 以 Naor and Shamir [1] 所提出的 (κ, n)-门框式视觉密码学模型为基础，配合在 (n-κ) 列中的各种 0-1 的组合，产生出一个超过庞大的基础共享矩阵，再经过化简的步骤，以产生最后的分享矩阵。

Lin and Chung [8] 为了让 (3, n)-门框式视觉密码学模型利用在大量密影分享参与者的情境下，于是透过随机的方式来设计新型态的分享模型。其优点是可以任意调整与密影分享的使用者，使得密影分享无论某些参与者输入或离开时，分享投影片仍然不需要重新制作。无论参与密影分享的使用者数目为何，当重叠任意 r 张分享投影片时，重叠图案上可以产生 $a = \frac{4^r-2^3+2}{3^r}$ 的黑白色差。因此重叠任意三张分享投影片后，重叠影像的黑白色差值为 $\alpha = 1/16$。不过这个分享模型在密影分享参与者较少的情况下，会比 Naor and Shamir [1] 的结果差。

在上述的 (3, n)-门框式视觉密码学的分享模型中，虽然在重叠三张分享分享投影片后即可还原密影资讯，不过还原影像的黑白色差会随著参与密影分享的参与者人数增加而降低，因此密影影像的难读大多只适合黑白影而无法推展到灰阶或彩色影像上。为了改善上述的缺点，于是本研究运用组合数学公式 (combinatorics) 来设计出一个新形态的非扩展型 (3, n)-门框式视觉密码学的分享模型，使得在重叠 3 张分享投影片时，重叠影像的黑白区域出现最佳的黑白色差，也因还原影像产生极佳的视觉效果。

二、本研究所提出的分享模型

一个典型的 (3, n)-门框式视觉密码学，是运用一张随机影像来产生 n (n≥3) 张分享投影片，其中密影投影片上的每个像素，在分享投影片上是用 m (m≥1) 像素点所形成的像素区域来代表，且也符合下列条件：

条件 1 (安全性)：为了确保密影影像的安全性，在重叠任意三张以下的分享投影片时，叠合影像上 (包括可能只有单一的分享投影片) 的像素区域内无法产生出黑白色差 (也就是每一个像素区域被重叠出黑点的比例均相等)，使得在重叠影像上无法显示出密影资讯的轮廓。

条件 2 (对比性)：为了确保重叠影像的对比性，在重叠任意三张及三张以上的分享投影片后，在代表密影影像的黑点部分的像素区域内，被重叠出黑点的百分比将大於密影影像的白点部分。因此在重叠影像上会呈现出不同的黑白色差，因此可以用目视解释出密影资讯的内容。

在 Naor and Shamir [1] 的 (3, 7)-门框式视觉密码学模型中 (表 1)，设计了两个 7×12 的基础矩阵 M^1 和 M^2 来分别加密黑白随机像素与黑色随机像素。在基础矩阵中第 i 列的值，代表要分配给第 i 张分享投影片的内容 (其中 0 代表白色，1 代表黑色)，因此在分享投影片上每一个像素区域点将被扩展为 12 像素的像素区域。此外，由於两个矩阵的列向量内容皆为 6 个 1 和 6 个 0，使得每一个像素区域的内容皆为六黑六白，因此在分享投影片上不会洩漏出自密影资讯的轮廓，借此确保视觉密影资讯分享的安全性。当任意重叠两张分享投影片后，叠合影像上的每一个像素区域的内容皆为七黑五白，使得重叠影像上不会显现出密影资讯；当任意重叠三张以上的分享投影片后，代表密影白点的像素区域内容仍
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，使得重疊影像上能夠產生黑的色差，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

<table>
<thead>
<tr>
<th>M^0</th>
<th>0 1 1 1 1 1 1 0 0 0 0 0 1 0 1 1 1 1 0 0 0 0 1 1 0 1 1 1 1 0 0 0 0 1 1 1 0 1 1 0 0 0 0 1 1 1 1 0 1 0 0 0 0 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>M^1</td>
<td>0 1 0 0 0 0 0 0 1 1 1 1 1 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0 1 0 1 0 0 0 0 1 1 1 1 1 0 0 0 0 0 1 0 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1</td>
</tr>
</tbody>
</table>

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，使得在任意重疊兩張以上分享段影片後，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×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_n>) 和非遞減數列 (<A^j_n>)，而矩陣右半部 (CR_0 、CR_1) 則是為了調整分享段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×m 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，矩陣內的每一個行向量的漢明權重值 (Hamming weight) 等於 \binom{n}{i} - \binom{n-i}{p}，並且任意 i (1 ≤ i ≤ n) 個矩陣向量進行邏輯 OR 運算後，所產生的漢明權重值等於 \binom{n-i}{p} 。因此在分享段影片疊合時，針對機密影像的白點部分所產生出非遞減數列為 <A^j_n > = \left< \binom{n}{p} - \binom{n-2}{p}, ..., \binom{n-p}{p}, \binom{n}{p}, ..., \binom{n}{p} \right>。

3. 為了讓每一張分享段影片，以及重疊任意兩張分享段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 \( \text{DIF} = A_2 - A_1 = \left[ \binom{n}{p} \binom{n-2}{p} - \binom{n-1}{p} \right] \)

\(= \binom{n-1}{p} \binom{n-2}{p} \)。因此如果我們運用 \( \text{DIF} \)
作為差值來產生一個等差遞增數列 \( A_1 \),

\[ < \binom{n}{p} \binom{n-1}{p}, \binom{n}{p} \binom{n-1}{p} + \binom{n}{p} \binom{n-2}{p}, \ldots, \binom{n}{p} \binom{n-1}{p} + (n-1) \binom{n-2}{p} > \]，就可
在重疊三張以上分享投影片後，使得鏡頭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第一白色差。由於等差數列的每個等差數都等於

\( \binom{n-1}{p} \binom{n-2}{p} \)，因此 \( \text{CL}_1 \) 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. 爲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 \( \text{CL}_0 \) 的每一個
列向量出現 \( 1 \) 的個數是 \( \binom{n}{p} \binom{n-1}{p} \)，而
矩陣 \( \text{CL}_1 \) 的列向量出現 \( 1 \) 的個數是

\( \binom{n-1}{p} \binom{n-2}{p} \)，因此矩陣 \( \text{CR}_1 \) 是一個大
小為 \( n \times m_1 \)，其中 \( m_1 = \left[ \binom{n}{p} \binom{n-1}{p} - \binom{n-1}{p} \binom{n-2}{p} \right] = \left[ \binom{n-2}{p} + \binom{n-2}{p} \right] \)，且矩陣內的所有元
素皆為 \( 1 \)。此外，由於矩陣 \( \text{CL}_1 \) 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 \( \text{CL}_1 \) 的大小為 \( n \times m_2 \)，
其中 \( m_2 = \left[ \binom{n-1}{p} \binom{n-2}{p} \right] \)。因此矩陣 \( \text{C}_1 \)
是一個大小為 \( n \times m \)，其中 \( m = m_1 + m_2 =

\( \binom{n}{p} - \binom{n-1}{p} + \binom{n-2}{p} + \binom{n-1}{p} + \binom{n-2}{p} \) \]

\(= \binom{n}{p} - \binom{n-1}{p} + (n-1) \binom{n-1}{p} + \binom{n-2}{p} \)。為了讓
\( \text{C}_0 \) 和 \( \text{C}_1 \) 的矩陣大小相同，於是矩陣 \( \text{CR}_0 \)
的大小為 \( n \times m_3 \)，其中 \( m_3 = m - m_0 =
\left[ \binom{n}{p} - \binom{n-1}{p} + (n-1) \binom{n-1}{p} + \binom{n-2}{p} \right] - \binom{n}{p} \)

\(= \binom{n}{p} + (n-1) \binom{n-1}{p} + \binom{n-2}{p} \)，且矩陣內的
所有元素皆為 \( 0 \)。

綜合上述的分析，矩陣 \( \text{C}_0 = [\text{CL}_0, \text{CR}_0] \) 和 \( \text{C}_1 = [\text{CL}_1, \text{CR}_1] \) 的大小為 \( n \times m \)，其中 \( n \) 為參與視覺機密分享的人數，\( m = m_0 + m_3 = m_1 + m_2 + m_3 = \left[ \binom{n}{p} - \binom{n-1}{p} + (n-1) \binom{n-1}{p} + \binom{n-2}{p} \right] - \binom{n}{p} \)，

其內容如下：

1. \( \text{CL}_0 \) 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

\( \text{CL}_0 \) 的大小為 \( n \times m_0 \)，其中 \( m_0 = \binom{n}{p} \)。

2. \( \text{CR}_0 \) 內所有的元素皆為 \( 0 \)，矩陣的大小為

\( n \times m_3 \)，其中 \( m_3 = \left[ (n-1) \binom{n-1}{p} + \binom{n-2}{p} \right] - \binom{n}{p} \)。

3. \( \text{CL}_1 \) 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 \( \text{CL}_1 \) 的大小
為 \( n \times m_2 \)，其中 \( m_2 = \binom{n-1}{p} - \binom{n-2}{p} \)。

4. \( \text{CR}_1 \) 內所有的元素皆為 \( 1 \)，矩陣的大小為

\( n \times m_3 \)，其中 \( m_1 = \binom{n}{p} - \binom{n-1}{p} + \binom{n-2}{p} \)。

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 \( m_0 = \binom{5}{3} = 10 \cdot \)

\( m_1 = \binom{5}{3} - 2 \times \binom{4}{3} + \binom{3}{3} = 3 \) 、 \( m_2 = \)

\( 5 \times \binom{4}{3} - \binom{3}{3} = 15 \) 、 \( m_3 = \)

145
4×\left[ \begin{array}{c} 4 \\ 3 \\ -3 \\ 3 \\ 3 \end{array} \right] = 8m = m_1 + m_2 + m_3 = 18。我們可以根據上述的分享模型設定

根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 \( R (0 \leq R < 1) \) 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 \( R \times m \) 行所對應的內容，並且將矩陣第 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 \( R \times m \) 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的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 \( WH \)，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事務矩陣的空間。每張分享投影片所需的空间是 \( WH \)，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，使得空間複雜度也為 \( O(nWH) \)。
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 \( 2 \leq p \leq (n-1) \) 情況下，當重疊 \( q (1 \leq q \leq n) \) 張分享投影片後，在重合影像上對應機密影像黑色部分有

\[
\frac{\binom{n}{p} - \binom{n-1}{p}}{m} \]

的機率被重疊出黑點，因此重疊影像上的黑白對比度為

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

\[
= \frac{\binom{n-2}{p} + (q-2)\binom{n-1}{p}}{\binom{n}{p} - (n-2)\binom{n-1}{p} + (n-1)\binom{n-2}{p}}
\]

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

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

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

(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，重疊影像的黑白對比度會大於 0，因此可以解答出機密資訊的內容，而達成 \( (3, n) \)-門檻式視覺密碼學的目標。
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 $\alpha_p^3$ 是一個由參數 n 和 p 所組成的連統函數，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 $\alpha_p^3$ 對 p 值進行偏微分後，所得到的一階導數等於 0 的位置，就是 $\alpha_p^3$ 的極值，如等式 (3) 所示。

由等式 (4) 的結果可以發現，$\alpha_p^3$ 二階導函數值小於 0，表示以 $p = n - n_{0.5}^0 + 1$ 帶入 (2) 式確實可以讓還原影像的黑白色差 ( $\alpha_p^3$) 達到極大值。也就是說，在設計 CL0 時，應該要選擇「在 n 個位置中填入 1 個」的設計，才能重疊 3 張分享投影片時，得到最大的色差對比。當 p 值離中心 $n_{0.5}^0$ 越遠，$\alpha_p^3$ 的值就越小。因為 p 必須是整數，因此本研究就採用最接近的整數，$[n - n_{0.5}^0]$ 或 $[n - n_{0.5}^0 + 1]$ 來代替，就可以求到最接近理論上的最大值。
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 $x^2 \leq n \leq (x + 0.5)^2 = x^2 + x + 0.25$，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 $p = \left\lceil n-n^{0.5}+1 \right\rceil = n+1-\left\lceil n^{0.5} \right\rceil$；如果 $n^{0.5}$ 值是介於 $x + 0.5$ 到 $x + 1$ 之間，也就是 $(x + 0.5)^2 \leq n \leq (x + 1)^2$，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 $p = \left\lceil n-n^{0.5}+1 \right\rceil = n+1-\left\lceil n^{0.5} \right\rceil$。

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

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

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」的方法來設計分享矩陣的 $CL_0$ 的話，本研究所提出的分享模型就可以在重疊 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度差，也讓原像產生極佳的視覺效果。

四、實驗結果與分析討論

![Tai-chi, Indians, Mena, Lena](149)

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 256x256 且經過半調處理後的 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灰階影影 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，無論視覺影像的參數（$p$ 值）為何，在分享投影片上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，因此每張分享投影片都可被視為是安全的（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同。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積累黑點的機率是呈
具有高色差對比之 (3, n)-門檻式視覺密碼學

現出等差遞增數列，而機密白色像素點則是呈現出等差遞減數列，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.(c3) 所示。當 \( p = n - n^{0.5} + 1 = 5 \) 時，重疊影像黑白色差值 \( \alpha_3 = 8.89\% \) 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，可以在重合 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。隨著重疊的分享投影片的數目增加，重疊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。

<table>
<thead>
<tr>
<th>( q = 1 )</th>
<th>( p = 2 )</th>
<th>( p = 3 )</th>
<th>( p = 4 )</th>
<th>( p = 5 )</th>
<th>( p = 6 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a1) ( \alpha_2^1 = 0 )</td>
<td>(b1) ( \alpha_3^1 = 0 )</td>
<td>(c1) ( \alpha_4^1 = 0 )</td>
<td>(d1) ( \alpha_5^1 = 0 )</td>
<td>(e1) ( \alpha_6^1 = 0 )</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( q = 2 )</th>
<th>( p = 2 )</th>
<th>( p = 3 )</th>
<th>( p = 4 )</th>
<th>( p = 5 )</th>
<th>( p = 6 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a2) ( \alpha_2^2 = 0 )</td>
<td>(b2) ( \alpha_3^2 = 0 )</td>
<td>(c2) ( \alpha_4^2 = 0 )</td>
<td>(d2) ( \alpha_5^2 = 0 )</td>
<td>(e2) ( \alpha_6^2 = 0 )</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( q = 3 )</th>
<th>( p = 2 )</th>
<th>( p = 3 )</th>
<th>( p = 4 )</th>
<th>( p = 5 )</th>
<th>( p = 6 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a3) ( \alpha_2^3 = 0.028 )</td>
<td>(b3) ( \alpha_3^3 = 0.053 )</td>
<td>(c3) ( \alpha_4^3 = 0.075 )</td>
<td>(d3) ( \alpha_5^3 = 0.089 )</td>
<td>(e3) ( \alpha_6^3 = 0.083 )</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( q = 4 )</th>
<th>( p = 2 )</th>
<th>( p = 3 )</th>
<th>( p = 4 )</th>
<th>( p = 5 )</th>
<th>( p = 6 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a4) ( \alpha_2^4 = 0.083 )</td>
<td>(b4) ( \alpha_3^4 = 0.147 )</td>
<td>(c4) ( \alpha_4^4 = 0.188 )</td>
<td>(d4) ( \alpha_5^4 = 0.200 )</td>
<td>(e4) ( \alpha_6^4 = 0.167 )</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( q = 5 )</th>
<th>( p = 2 )</th>
<th>( p = 3 )</th>
<th>( p = 4 )</th>
<th>( p = 5 )</th>
<th>( p = 6 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a5) ( \alpha_2^5 = 0.167 )</td>
<td>(b5) ( \alpha_3^5 = 0.267 )</td>
<td>(c5) ( \alpha_4^5 = 0.313 )</td>
<td>(d5) ( \alpha_5^5 = 0.311 )</td>
<td>(e5) ( \alpha_6^5 = 0.250 )</td>
<td></td>
</tr>
</tbody>
</table>
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 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，展現影像黑白差值 $\alpha_4^4 = 12.5\%$ 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 張分享影像時得到最佳的色差對比。

<table>
<thead>
<tr>
<th>$q$</th>
<th>$p=2$</th>
<th>$p=3$</th>
<th>$p=4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(a1) $\alpha_2^1 = 0$</td>
<td>(b1) $\alpha_3^1 = 0$</td>
<td>(c1) $\alpha_4^1 = 0$</td>
</tr>
<tr>
<td>2</td>
<td>(a2) $\alpha_2^2 = 0$</td>
<td>(b2) $\alpha_3^2 = 0$</td>
<td>(c2) $\alpha_4^2 = 0$</td>
</tr>
<tr>
<td>3</td>
<td>(a3) $\alpha_2^3 = 0.063$</td>
<td>(b3) $\alpha_3^3 = 0.111$</td>
<td>(c3) $\alpha_4^3 = 0.125$</td>
</tr>
<tr>
<td>4</td>
<td>(a4) $\alpha_2^4 = 0.188%$</td>
<td>(b4) $\alpha_3^4 = 0.167$</td>
<td>(c4) $\alpha_4^4 = 0.250$</td>
</tr>
</tbody>
</table>
官振宇等
具有高色差對比之 (3, n)-門檻式視覺密碼學

\[ q = 5 \]

<table>
<thead>
<tr>
<th></th>
<th>( p = 2 )</th>
<th>( p = 3 )</th>
<th>( p = 2 )</th>
<th>( p = 3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( q = 1 )</td>
<td>( a_2^1 = 0 )</td>
<td>( a_3^1 = 0 )</td>
<td>( a_2^1 = 0 )</td>
<td>( a_3^1 = 0 )</td>
</tr>
<tr>
<td>( q = 2 )</td>
<td>( a_2^2 = 0 )</td>
<td>( a_3^2 = 0 )</td>
<td>( a_2^2 = 0 )</td>
<td>( a_3^2 = 0 )</td>
</tr>
<tr>
<td>( q = 3 )</td>
<td>( a_2^3 = 0.111 )</td>
<td>( a_3^3 = 0.167 )</td>
<td>( a_2^3 = 0.111 )</td>
<td>( a_3^3 = 0.167 )</td>
</tr>
</tbody>
</table>

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重合影像黑白差差值為 \( \alpha_3^5 = 8.89\% \) (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 \( \alpha_3^5 = 53.33\% \) (圖 3.(d7)) 和 \( \alpha_3^4 = 37.50\% \) (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，無論機密影像的形態為何，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，重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，重疊影像黑白差差值 \( \alpha_3^3 = 16.7\% \) 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。
圖 5. (3, 4)-門檻式密碼學模型的機密還原結果，以灰階影像 Lena 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 \( p = \lceil n - n^{0.5} \rceil = n - 1 \) 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 \( p = \lceil n - n^{0.5} \rceil = n - 2 \) 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，確實可以在重合 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

<table>
<thead>
<tr>
<th>( n )</th>
<th>( p = 2 )</th>
<th>( p = 3 )</th>
<th>( p = 4 )</th>
<th>( p = 5 )</th>
<th>( p = 6 )</th>
<th>( p = 7 )</th>
<th>( p = 8 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>11.11%</td>
<td>16.67%</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>5</td>
<td>6.25%</td>
<td>11.11%</td>
<td>12.50%</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6</td>
<td>4.00%</td>
<td>7.50%</td>
<td>10.00%</td>
<td>10.00%</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>7</td>
<td>2.78%</td>
<td>5.33%</td>
<td>7.50%</td>
<td>8.89%</td>
<td>8.33%</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>8</td>
<td>2.04%</td>
<td>3.97%</td>
<td>5.71%</td>
<td>7.14%</td>
<td>7.94%</td>
<td>7.14%</td>
<td>—</td>
</tr>
<tr>
<td>9</td>
<td>1.56%</td>
<td>3.06%</td>
<td>4.46%</td>
<td>5.71%</td>
<td>6.70%</td>
<td>7.14%</td>
<td>6.25%</td>
</tr>
</tbody>
</table>

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 \( a^1 \) 及 \( a^n \) 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大。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，\( a^1 \) 及 \( a^n \) 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，\( a^5 = 5/63 (\approx 7.94\%) \) 和 \( a^8 = 5/9 (\approx 55.56\%) \)。當 \( n \) 值趨近於無限大時，\( a^n \) 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。

官振宇等
具有高色差對比之 (3, n)-門檻式視覺密碼學

表 4. 本研究與相關 (3, n)-門檻式視覺密碼學模型之比較表

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

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 $k (k \leq n)$ 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
矩阵，使得重叠影像的黑白区域出现最佳的黑白色差，也使形变影像产生最佳的视觉效果。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. 設計概念十分簡單，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 \(CH\) 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 \((3, n)\)-閾值密碼學的研究成果。
3. 本研究所提出的分享模細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

官振宇等
具有高色差對比之 (3, n)- 門檻式視覺密碼學