具有優先權概念之通用型視覺機密分享

侯永昌[1]　官振宇[2*]　蔡志豐[2]

[1]淡江大學資訊管理系
[2]國立中央大學資訊管理系

摘　要

在侯永昌等 [11] 所提出的 (*n*, *n*)-PPVSM 分享模型中，雖然已經可以達成根據使用者的重要性來設計分享模型，不過這個分享模型仍有違反權限等級與多數決精神的情況發生。為了改善這些問題，於是本研究提出一個新的具有優先權概念之通用型漸進式視覺機密分享模型。本研究具備下列幾項優點：(1) 分享矩陣可以根據實際狀況，視優先權等級的個數和人數進行調整。(2) 參與解密的人數愈多或權限的組合愈大，疊合影像上的黑白色差值將會愈高，使得黑白色差的設計符合根據多數決和權限等級還原的原則。(3) 當重疊所有的分享影像後，還原影像黑白色差值都是 $(n-2)/(n-1)$，優於現行其他的研究。(4) 分享影像的大小與機密影像相同，不須擴展。

關鍵詞：視覺機密分享，漸進式視覺機密分享，優先權分享影像

General Model for the Priority-based Progressive Visual Secret Sharing

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

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

ABSTRACT

Hou et al. [11] proposed the (*n, n*)-PPVSM in which every participator is assigned a unique privilege to recover the secret message. However, their schema may violate the spirits of priority and the majority decision most in some situations. In order to improve these problems, this study proposes a novel method called the general model for the priority-based progressive visual secret sharing (GPPVSS). Our study has the following advantages: (1) the number of participants in each priority level can be adjusted based on the actual situation. (2) as the number of the stacked shares or the sum of the corresponding privileges increases, the black-white contrast is risen. That is to say, this schema conforms to the principles of majority decision most and priority-based. (3) after all of transparencies are stacked, the contrast of restored images are $(n-2)/(n-1)$, and it is better than other studies. (4) the size of transparencies is the same as the secret image.

Keywords: visual secret sharing, progressive visual secret sharing, priority (weighting) share

文稿收件日期 101.1.16; 文稿修正後接受日期 101.5.30;*通訊作者
Manuscript received January 16, 2012; revised May 30, 2012;* Corresponding author

一、前　言

公平性和合理性是任何組織在建立制度中的重要參考準則，如果一個組織能夠公平且合理地分派組織資源給各個商務功能(Business function)，將可使各功能均衡發展，進而為組織創造最大獲利與績效。儘管公平性是一個普世價值，不過在真實世界裡卻有很多情境需要應用到「優先權」概念。在醫院裡，急診室的病患需要優先診治；在生產排程中，急單需要立即被滿足；在商務環境中，高階管理者為了有效且快速地做出正確決策，因而需要擁有較高的權限來取用更多、更重要的資訊。

在資訊安全領域中，當重要資訊掌握在少數人手中，一旦這個人離職或意圖不軌，將會造成機密資訊遺失與洩露等風險。為了提升資訊分享的安全性，因而資安領域發展出機密分享的模式。其作法是把機密資訊分散為多份雜訊式資料，再將這些雜訊式資料交付給多人共同保管，而機密資訊還原必須藉由多位保管人員共同參與，藉此達成分散風險的目的。機密分享 (Shamir [1]；Thien 與 Lin [2]) 是一種應用於影像資料的機密資訊分享模式，其作法是將一張機密影像分散為多張分享影像，並且將這些分享影像分配給多位參與者共同保管。如果想要還原機密影像的內容，在獲得 k 張以上的分享影像後，將可以透過多項式求解的方式，來計算出機密影像的資訊；反之，則無法獲得任何機密資訊。

當資訊由多位參與者共同保管與分享時，資訊的分配保管亦需考量參與者的角色，根據參與者的職責與重要性，分配不同的資訊保管量，使得高階人員被分配到的資訊比低階人員要多。例如：在影像的位元平面上，每一個位元所代表的像素值皆不相同，因此較高位元平面值改變後對於像素值的更動，會比較低位元平面值來得劇烈。根據這一個特性，Chen 與 Lin [3] 和 Wang 與 Shyu [4] 將較高位元平面值的資訊分配給較高權限的參與者，而將較低位元平面值的資訊分配給較低權限的參與者，因此在機密資訊的還原品質上會產生差異，於是衍伸出具有優先權等級的機密分享研究。

視覺機密分享 (Naor 與 Shamir [5]) 是一個應用在影像資料上的新密碼學方法，其目的是希望透過人類的視覺系統，便可直接對加密資訊進行解讀。然而上述兩篇研究的做法都需要電腦輔助才能還原機密資訊，因此無法透過直接疊合分享影像的方式來進行解密。Hou [6] 基於顏色分解與合成的原理產生四張分享影像，分別是一張黑白遮罩影像 (S_{mask})，以及三張分別是代表青、洋紅、黃的分色影像 (S_{c}、S_{m}、S_{y})，並且將遮罩影像交由一位管理者保管，而三張分色影像則交由其他三位從屬者保管。雖然 Hou 的作法可以達成具有優先權的視覺機密分享，不過所產生的分享影像是機密影像的 4 倍，於是造成儲存空間與傳輸時間的浪費。此外，權限的劃分只有限定於管理與從屬兩層，並且只能分享成四張分享影像，因此無法適用於其他狀況。漸進式視覺機密分享 (Fang and Lin [7]；Fang [8]；侯與官 [8]；Hou and Quan [10]) 是一種新的資訊分享概念，機密影像的內容將會隨著疊合的分享影像數目增加而愈來愈清晰。侯永昌等 [11] 為了能夠賦予分享者不同的優先等級，於是又提出一個具有權限等級的非擴展型漸進式視覺機密分享模型，稱之為 (n, n)-PPVSM 機密分享機制。

雖然 (n, n)-PPVSM 已經可以達成根據使用者的重要性來設計分享模型，不過這個分享模型仍有幾個問題而無法完全符合優先權分享的概念。例如：(1) 當參與解密的人數相同時，在疊合影像上的黑白色差值將受限於較低權限等級的參與者。(2) 當權限值總和的組合相同時，有時參與解密的人數較多的組合，疊合影像上的黑白色差值卻是較低。(3) 每一個權限等級內的參與者人數只能限定為一人，使得分享模型不夠彈性 (請參見 2.2 節)。為了改善這三個問題，於是本研究提出一個新的具有優先權概念之不擴展漸進式視覺密碼，稱之為具有優先權概念之通用型漸進式視覺機密分享模型。在下面章節中，第二章將簡單說明漸進式視覺機密分享的相關研究，第三章說明本研究所提出的兩個視覺機密分享模型，第四章則是實驗結果與分析討論，最後在第五章是本研究的結論。

二、文獻探討

2.1 漸進式視覺機密分享

傳統 (k, n)-threshold 視覺機密分享是一種「門檻式」的解密概念，當門檻值設定為 k 值後，當重疊 k 張或 k 張以上的分享影像後，疊合影像因為機密資訊的黑點部分與白點部份產生出黑白色差，於是還原出機密資訊。反之，如果重疊少於 k 張分享影像時，疊合影像上仍然是呈現出雜訊式的外觀，而無法還原出機密資訊的內容。漸進式視覺密碼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。

Jin 等 [12] 提出一個多解析度的機密分享方法，其作法是將機密影像的像素點擴展為 3×3 的影像區塊，其中的 8 個位置分別代表像素灰階值的 8 個位元平面，另外 1 個像素則用來儲存機密影像的半色調影像值。為了以這 8 個位置的位元平面值來模擬機密影像的灰階值，Jin 等首先需要調整機密影像的灰階值，將灰階值比較大的像素調整為它在這 8 個位置中擁有比較多的 1 (代表疊合後它會變得比較黑)；反之，灰階值比較小的像素調整為它在這 8 個位置中擁有比較少的 1 (代表疊合後它會變得比較白)。Jin 利用傳統視覺密碼的方法，來分別處理 1 - 8 和第 9 個位元的值，就可以用疊合方式來產生兩種不同解析度的視覺密碼的效果。如果利用第 9 個位置上的半色調影像值，藉由電腦設備的 XOR 計算，也可以完全還原機密影像的半色調內容(第三種解析度)。雖然 Jin 等人的方法可以產生不同解析度的還原影像，不過其模型需要額外的空間來儲存灰階值的轉換表 (look-up table)，而且分享影像要擴展到 6×6 倍之多，因此造成儲存空間和傳輸頻寬的浪費。

Fang 與 Lin [7] 和 Fang [8] 分別針對無意義和有意義的分享影像提出兩篇有關漸進式視覺密碼的研究，雖然他們的做法確實可以藉由重疊分享影像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共同的缺點。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 [10] 和侯與官 [9] 為了改善這些問題，設計了兩組新的 $n\times n$ 的矩陣來產生出 n 張不擴展型的分享投影片。實驗結果顯示在分享投影片上不僅不會顯露出機密資訊，而且重疊所有分享投影片後，在疊合影像上可以分別產生出 $(n-1)/n$ 和 $(n-1)/(2n)$ 的黑白色差，使得機密內容可以清楚地被辨識。

Wang 等 [13] 應用漸進式分享概念，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 ($n \geqq 3$) 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 ($1 \leqq i \leqq n$) 個機密區塊。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 等 [14] 為了改善像素擴展的缺點，於是他們運用隨機網格 (random grid) 的概念，重新提出三個非擴展型的視覺分享模型，稱之為 n-level IVCRG。不過這三個分享模型所產生的還原影像黑白色差值都不明顯，尤其是當 n 值變得比較大的時候，機密影像的黑白色差會隨之大幅度降低，因而產生視覺品質不佳的問題。此外，在第一個分享模型的第 $1 \sim n-1$ 個影像區塊的還原結果，以及第二與第三個分享模型中所有影像區塊的還原結果，機密影像的黑點部分被還原出黑點的機率都會比機密白點部分低，於是在這些區塊上的機密內容會被還原出黑白顛倒的「陰刻」結果。因此，Wang 等所提出的這三個分享模型，機密影像內容都只適合選用結構簡單的黑白影像。

Chen 與 Lee [15] 也是運用隨機網格而提出了一個有意義偽裝分享投影片的漸進式視覺密碼。他們的做法是先輸入 n 張偽裝影像與 1 張機密影像，然後利用隨機亂數 i ($1 \leqq i \leqq n+1$) 來決定 n 張分享投影片上每一個像素的顏色。如果 i 值等於 $n+1$ 時，他們先用一個隨機網格來產生第 1 張偽裝分

享影像 (G_1) 某一個像素的顏色，當對應的機密像素是白色時，第 j ($2 \leqq j \leqq n$) 張分享投影片 (G_j) 上相對應像素的顏色都與 G_1 相同；反之，G_j 的顏色則是各自利用一個隨機網格來挑選顏色，其中挑中白色與黑色的機率皆為 50%。如果 i 值小於 $n+1$ 時，第 i 張投影片上的顏色則是由第 i 張偽裝影像上相對應像素的顏色來決定；也就是說，G_i 的內容將會與第 i 張偽裝影像的顏色相同，而其他投影片上相對應像素的顏色則是全都設定為黑色，使得這一部份在重疊後的結果都是黑色。在這一個分享模型中，偽裝分享投影片的白點部分出現黑點的機率是接近 $(2n-1)/[2(n+1)]$，而黑點部分出現黑點的機率則是接近 $(2n+1)/[2(n+1)]$，因此每一張偽裝分享投影片的黑白色差值約為 $1/(n+1)$。重疊任意兩張分享投影片後，重疊影像上被重疊出白點的機會就只會出現在隨機亂數 $i=n+1$ 的時後，其他的時刻無論機密影像的顏色為何，在重疊影像上都是被疊出黑色。當重疊所有的分享投影片後，機密白點部分被重疊出黑點的機率是接近於 $(2n+1)/[2(n+1)]$，而黑點部分被重疊出黑點的機率則是接近於 1，因此機密影像的黑白色差值接近於 $1/[2(n+1)]$。由於機密影像的黑白色差值過低，因此這一個分享模型會發生還原品質不佳的問題。

2.2 具有優先權等級的漸進式視覺密碼

在傳統的漸進式視覺密碼研究，每一位參與者都視為是相同權限等級，因此對於機密影像的還原，每一張分享影像都擁有相同的復原能力。然而在現實生活中，參與視覺機密分享的參與者可能會有不同重要性，為了能夠賦予分享者不同的優先等級，使得還原機密資訊的能力會根據權限等級的不同而有所調整，於是 侯永昌等 [11] 提出漸進式且具有權限等級的不擴展視覺密碼分享方法，稱之為 (n, n)-PPVSM 機密分享機制。

(n, n)-PPVSM 機密分享機制的做法是假設 n 個機密分享的參與者都擁有不同的權限等級，於是設計了兩個 $m\times n$ 的矩陣 (C^0 和 C^1)，分別代表機密像素為白色或黑色的分享矩陣 (表 1)。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 (1 代表黑點，0 代表白點)，此外，他們假設參與者 k 的權限值為 k，則分享矩陣的第 k 行出現 1 的機率就設為 k/m，其中，$m=\sum_{k=1}^{n}k=n(n+1)/2$，使得權限等級比較高的分享影像中出現黑色的機率比較大。由於在每一張分享影像上出現黑點的機率不同，使得還原機密影像中黑點的速率也不同，因此可以表現出不同權限的特性。

根據表 1 的分享模型，分享投影片的大小將會與機密影像相同，並且矩陣 C^0 和 C^1 的第 k ($1 \leqq k \leqq n$) 個行向量中都只有 k 個 1，因此無論機密像素是黑或白，第 k 張分享投影片上的每一個像素點都只有 k/m 的機率呈現出黑色，於是投影片上不會顯露出機密資訊。在重疊影像的還原品質上，假設部份參與者所組成的子集合 T 中，最大的權限等級為 M，所有權限等級的加總為 S，則疊合子集合 T 的所有分享影像後，機密影像中的白點部份有 M/m 的機率出現黑色，而黑點部份則有 S/m 的機率出現黑色，因此在疊合影像上會出現 $(S-M)/m$ 的黑白色差。當重疊所有的分享影像後，疊合影像的色差對比是 $(n-1)/(n+1)$，這個結果優於傳統視覺密碼的 50% 的色差對比，使得機密內容可以清楚地被辨識。

雖然 (n, n)-PPVSM 可以達到優先權等級的概念，不過在這個分享模型的設計規則上，仍有某些情況無法完全地符合優先權等級的需求。我們以產生六張分享影像為例 ($m=21$，$n=6$)，將結果整理如表 2 所示，將可以發現下列幾個問題。

問題 1：當參與解密的人數相同時，在疊合影像上的黑白色差值將受限於較低權限等級的參與者。

範例 1：疊合影像的黑白色差值等於 $(S-M)/m$，當最小權限值的分享影像與其他任一張分享影像重疊後，疊合影像 1+2、1+3、1+4、1+5、1+6 的黑白色差值的分子部分 $(S-M)$ 皆是等於 1，因此這些疊合影像的黑白色差值都是呈現出 1/21，因此即使最高權限的參與者拿出他的投影片，疊合後的結果也不會比其他較低權限的參與者要好。從表 2 的結果中，我們可以發現：2+3、2+4、…；3+4、3+5、…；4+5、4+6、…；1+2+3、1+2+4、…；

1+2+3+4、1+2+3+5、…，都是最低權限的參與者主導了整個還原的結果，這違反了根據權限等級還原的原則。

問題 2：當權限值加總和的組合相同時，有時參與解密的人數較多的組合，疊合影像上的黑白色差值卻是較低。

範例 2：疊合影像的黑白色差值等於 $(S-M)/m$，當使用者設定權限值的加總和相等時，有時重疊多張分享影像後的黑白色差值反而小於重疊較少張分享影像的結果，使得黑白色差的設計無法符合多數決的精神 (見表 2 中之陰影區)。例如：$S = 9$，疊合影像 1+2+6 的黑白色差值等於 $(9 - 6) / 21 = 3 / 21$ (0.143)，疊合影像 4+5 的黑白色差值則是 $(9 - 5) / 21 = 4 / 21$ (0.190)；$S = 12$，疊合影像 1+2+3+6 的黑白色差值等於 $(12 - 6) / 21 = 6 / 21$ (0.286)，疊合影像 3+4+5 的黑白色差值則是 $(12 - 5) / 21 = 7 / 21$ (0.333)。

問題 3：在侯永昌等 [11] 的分享模型中，是設定每一位參與者都隸屬於不同權限等級。然而在現實生活中，每一個權限等級內的參與者人數可能不只一人。不過他們的分享模型卻無法根據實際狀況而進行調整，使得分享模型不夠彈性。

表 1. (n, n)-PPVSM 的分享模型

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

三、本研究所提出的分享模型

為了改善上述的問題，於是本研究提出一個新的具有優先權概念之不擴展漸進式視覺密碼，稱之為具有優先權概念之通用型漸進式視覺機密分享模型。

3.1 基本模型

本研究所提出的第一個分享模型，是為了改善 (n, n)-PPVSM 機密分享機制在問題 1 與問題 2 的限制，因此假設 n 個機密分享的參與者都擁有不同權限等級，並且設計了兩個 $m \times n$ 的矩陣 (C^0 和 C^1)，分別代表機密像素為白色或黑色的分享矩陣，分享矩陣的設計規則如下所示：

建構 1：有 n 位參與者加入機密分享的工作，且每一位參與者的權限等級都不相同。假設參與者 i 的權限值為 i，因此在分享矩陣上出現 1 的機率要大於比他權限低的參與者，使得權限等級比較高的分享影像 (WS^i, $i = 1, ..., n$) 中出現黑色的機率比較大。

1. C^0 矩陣的內容可以分為上下兩個半部 (CU^0 和 CL^0)。在 C^0 矩陣的上半部 (CU^0)，所有的 0 都分配在不同的列上，其中，第 i 行出現 0 的個數為 $n - i$ 個，其他位置的內容皆為 1。因此 CU^0 矩陣至

少需要 $\Sigma_i (n-i) = n(n-1)/2$ 的位置來存放 0，於是我們設定 CU^0 矩陣的大小是 $m_1 \times n$，其中 $m_1 = n(n-1)/2$。矩陣 CU^0 中出現 1 的個數依序遞增，矩陣第 i 行 $(CU^0{}_i)$ 出現 1 的個數 (A_i) 為 $m_1 - (n-i) = (n^2 - 3n + 2i)/2$，使得權限等級比較高的分享影像中出現黑色的機率比較大。

$$m_1 = n(n-1)/2 \tag{1}$$

$$A_i = (n^2 - 3n + 2i)/2 \tag{2}$$

2. 為了不在分享影像上洩露出機密影像的蛛絲馬跡，矩陣 $C^1{}_i$ 出現 1 的個數要和矩陣 CU^0 的第 i 行 $(CU^0{}_i)$ 相同，也就是有 $(n^2 - 3n + 2i)/2$ 個 1。另外，為了擴大 C^1 矩陣在疊合時能夠產生更多的黑點，所有的 1 都是分配在不同的列上，而其他位置的內容則皆為 0。因此矩陣大小是 $m \times n$，其中 $m = \Sigma_i (n^2 - 3n + 2i)/2 = n(n-1)^2/2$。

$$m = n(n-1)^2/2 \tag{3}$$

3. 為了不讓分享影像上洩露出機密影像的蛛絲馬跡，C^0 矩陣的大小必須與 C^1 矩陣相同，使得分享影像的像素內容不論是由機密影像的黑點或白點所分配而來，出現黑點的機率將會相同。因此，C^0 矩陣的下半部 (CL^0) 大小是 $m_2 \times n$，並且矩陣的內容都設為 0，其中 $m_2 = m - m_1 = n(n-1)^2/2 - n(n-1)/2 = n(n-1)(n-2)/2$。

$$m_2 = n(n-1)(n-2)/2 \tag{4}$$

4. 根據上述建構過程，我們定義四個變數來控制矩陣內容，其中 $\sigma^{1,i} = (n-i-1) \times (n-i)/2$、$\sigma^{2,i} = A_i - \sigma^{1,i}$、$\sigma^{3,i} = \Sigma_i (A_{i-1})$ 和 $\sigma^{4,i} = m_2 - \Sigma_i (A_i)$，並假設 $A_0 = 0$，因此 $CU^0{}_i = \{\overbrace{1,\cdots,1}^{\sigma^{1,i}},\overbrace{0,\cdots,0}^{n-i},\overbrace{1,\cdots,1}^{\sigma^{2,i}}\}$、$CL^0{}_i = \{\overbrace{0,\cdots\cdots,0}^{m_2}\}$、$C^1{}_i = \{\overbrace{0,\cdots,0}^{\sigma^{3,i}},\overbrace{1,\cdots,1}^{A_i},\overbrace{0,\cdots,0}^{\sigma^{4,i}}\}$。

表 2. 重疊 2 張與 3 張分享影像後的疊合影像黑白色差表

疊合影像	出現黑點機率		黑白色差	疊合影像	出現黑點機率		黑白色差
	W	B			W	B	
1+2	2/21	3/21	1/21	1+3+4	4/21	8/21	4/21
1+3	3/21	4/21	1/21	1+3+5	5/21	9/21	4/21
1+4	4/21	5/21	1/21	1+3+6	6/21	10/21	4/21
1+5	5/21	6/21	1/21	⋮	⋮	⋮	⋮
1+6	6/21	7/21	1/21	2+3+4	4/21	9/21	5/21
2+3	3/21	5/21	2/21	2+3+5	5/21	10/21	5/21
2+4	4/21	6/21	2/21	2+3+6	6/21	11/21	5/21
2+5	5/21	7/21	2/21	⋮	⋮	⋮	⋮
2+6	6/21	8/21	2/21	3+4+5	5/21	12/21	7/21
3+4	4/21	7/21	3/21	3+4+6	6/21	13/21	7/21
3+5	5/21	8/21	3/21	⋮	⋮	⋮	⋮
3+6	6/21	9/21	3/21	1+2+3+4	4/21	10/21	6/21
4+5	5/21	9/21	4/21	1+2+3+5	5/21	11/21	6/21
4+6	6/21	10/21	4/21	1+2+3+6	6/21	12/21	6/21
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
1+2+3	3/21	6/21	3/21				
1+2+4	4/21	7/21	3/21				
1+2+5	5/21	8/21	3/21				
1+2+6	6/21	9/21	3/21				

定義 1：隨機變數 X 和 Y 分別是代表機密影像與分享影像的顏色，機密影像上出現黑點和白點的機率分別以 P(X = 1) 和 P(X = 0) 來表示，而分享影像上出現黑點和白點的機率則是 P(Y=1) 和 P(Y=0)。

定理 1：無論機密影像的內容為何，第 i 張分享影像上 (WS^i) 出現黑點的機率是 $\beta_i = A_i / m$。

證明：當機密影像為黑點時，分享影像上出現黑點的機率是 $P(Y = 1 \mid X = 1)$；機密影像為白點時，分享影像上出現黑點的機率是 $P(Y = 1 \mid X=0)$。根據條件機率的定義可以得知，第 i 張分享影像上出現黑點的機率是 $\beta_i = P(Y_i = 1 \mid X = 1)\times P(X = 1) + P(Y_i = 1 \mid X = 0)\times P(X = 0) = P(Y_i = 1, X = 1) + P(Y_i = 1, X = 0) = P(Y_i = 1) = A_i / m$。得證。

當要產生分享投影片時，是透過隨機亂數 (u) 來選取分享矩陣內的一個列向量，並依序將列向量內的每一個值分配到對應的投影片上 (第 v 個值分配給第 v 張投影片)，其中 $1 \le u \le m$ 和 $1 \le v \le n$，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，將第 u 列的第 1 個值 ($C^0_{u,1}$) 分配給 WS^1，第 2 個值 ($C^0_{u,2}$) 分配給 WS^2，…，第 n 個值 ($C^0_{u,n}$) 分配給 WS^n；反之，如果機密影像像素點的顏色為黑色，則利用 C^1 矩陣以同樣的方式進行加密，因而可以產生出 n 張相異權限的分享影像。

在安全性的考量下，C^0 和 C^1 矩陣的第 i 列有 A_i 個元素是出現 1，這代表無論機密影像的內容是白點或黑點，第 i 張分享影像 (WS^i) 被分配到黑點的機率都是等於 $\beta_i = A_i/m$。假設 B(0) 和 B(1) 分別是代表 WS^i 上的白點和黑點的面積，因此 $WS^i = B(0) \cup B(1)$ 和 $B(0) \cap B(1) = \varnothing$。根據 Shyu [16] 的平均透光值 (average light transmission) 定義，$T(B(0)) = T(B(1)) = 1 - A_i/m = (m - A_i)/m$，因此 WS^i 的黑白色差值等於 $(T(B(0)) - T(B(1)) / (1+T(B(1))) = 0$。由於在白色 (黑色) 區域上的平均透光值都是相同的，因此在分享影像上不會揭露出任何機密影像的訊息，加上分享影像的內容是根據隨機亂數 u 來選取，隨機亂數將可以確保在每一張分享影像的黑白分佈是均勻的，黑點不會集中在機密影像的黑色部份，白點也不會集中在機密影像的白色部份，因而不會在分享影像上顯露出機密影像的邊緣輪廓。綜合上述兩點，所以我們足以推論任一張分享影像都能夠視為是安全的。

範例 3：以 4 個分享者為例，CU^0_i 擁有 $4 - i$ 個 0，而且 CU^0 矩陣中每一行的 0 都分配在不同的列上，因此，CU^0 矩陣共佔有 $\Sigma_i (4 - i) = 6$ 列，其他位置的內容皆為 1；CL^0 矩陣有 $n(n - 1)(n - 2)/2 = 4\times3\times2/2 = 12$ 列，其內容則全部都是 0；C^1 矩陣中每一行都擁有 $(n^2 - 3n + 2i)/2 = (16 - 12 + 2i)/2 = 2 + i$ 個 1，也就是第 1 - 4 行分別擁有 3 - 6 個 1。因為每一行的 1 都是分配在不同的列上，因此 C^1 矩陣一共佔有 18 列，而其他位置的內容則是皆為 0。這樣設計的分享矩陣，使得分享影像 i 上的像素，不論是由 C^0 或 C^1 分配而來，都有 $(2 + i)/18$ 的機率產生黑點，有 $(16 - i)/18$ 的機率產生白點，因此，分享影像上不會洩露出機密影像的蛛絲馬跡，使用者也無法由分享影像來判斷機密影像的內容。其分享矩陣如表 3 所示。

視覺密碼學中分享影像重疊的動作相當於邏輯運算上的 OR 運算。當重疊多張分享影像時，只要有一張分享影像的像素點內容為黑色 (1) 時，在疊合影像上就會顯示黑色，只有在每一張分享影像上的某一點像素都是白色 (0) 時，才會在疊合影像的那一個像素上顯示出白點。根據上述的觀察，我們將分享矩陣設計為，C^0 矩陣中每一行的 1 都出現在矩陣的上半部，並且儘可能的重疊在一起；而 C^1 矩陣中每一行的 1 都分配在不同的列上，使得分享影像上因 C^1 矩陣所產生的相關像素，在疊合時出現黑點的機率會逐漸增加，而分享影像上因 C^0 矩陣所產生的相關像素，在疊合時出現黑點的機率則維持在 $m_1 / m = 1 / (n - 1)$，不會改變，因而擴大了疊合影像上黑白像素間的色差，造成在疊合的過程中逐漸顯現機密內容。由於在每一張分享影像上出現黑點的機率不同，使得它能還原機密影像中黑點的速率也不同，因此可以表現出不同權限的特性。假設在 |T| 位參與者所組成的子集合

T 中，所有權限等級的加總和為 S，則疊合他們所擁有的分享影像後，機密影像中的色點分布滿足下列的定理。

表 3. 兩個 $m \times n$ 的分享模型 (以 $n = 4$ 為例)

C^0	C^1
$\begin{bmatrix} 1&1&0&1 \\ 1&0&1&1 \\ 1&0&1&1 \\ 0&1&1&1 \\ 0&1&1&1 \\ 0&1&1&1 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{bmatrix}_{18\times4}$	$\begin{bmatrix} 1&0&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \\ 0&1&0&0 \\ 0&1&0&0 \\ 0&1&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&1&0 \\ 0&0&1&0 \\ 0&0&1&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 0&0&0&1 \\ 0&0&0&1 \\ 0&0&0&1 \\ 0&0&0&1 \\ 0&0&0&1 \end{bmatrix}_{18\times4}$

定義 2：OR(·) 為邏輯上的 OR 運算，其中 $\mathrm{OR}(Y_1, Y_2, \ldots, Y_{|T|})$ 代表重疊任意 |T| 張分享影像後的疊合影像顏色，Y_h 是疊合影像上的第 h 張分享影像的顏色 ($h = 1, 2, ..., |T|$)。此外，疊合影像上被重疊出白點和黑點的機率，分別為 $\mathrm{P}(\mathrm{OR}(Y_1, Y_2, \ldots, Y_{|T|}) = 0)$ 與 $1 - \mathrm{P}(\mathrm{OR}(Y_1, Y_2, \ldots, Y_{|T|}) = 0)$。

$$\begin{cases} OR(Y_1, Y_2, \cdots, Y_{|T|}) = 0 & if\ (Y_1 = Y_2 = \cdots = Y_{|T|} = 0) \\ OR(Y_1, Y_2, \cdots, Y_{|T|}) = 1 & otherwise \end{cases} \quad (5)$$

定理 2：在重疊影像上，機密影像的白點部份有 m_1 / m 的機率出現黑色，而黑點部份則有 $[(n^2 - 3n)|T| + 2S] / (2m)$ 的機率出現黑色，因此在疊合影像上會出現 $[(n^2 - 3n)|T| + 2S - 2m_1] / (2m)$ 的黑白色差。

證明：

1. 根據定義 2，當機密像素點的顏色是白點時，重疊影像被重疊出白點的機率是：

$$\begin{aligned} &P(OR(Y_1, Y_2, \cdots, Y_{|T|}) = 0 \mid X = 0) \\ &= P(Y_1 = 0, Y_2 = 0, \cdots, Y_{|T|} = 0 \mid X = 0) \\ &= P(Y_1 = 0 \mid X = 0) \times P(Y_2 = 0 \mid Y_1 = 0, X = 0) \times \cdots \\ &\quad \times \cdots \times P(Y_{|T|} = 0 \mid Y_1 = Y_2 = \cdots Y_{|T|-1} = 0, X = 0) \end{aligned}$$

Case 1：當任意兩張分享影像重疊後 (在不失普遍性的原則下，我們假設是參與者 1 與 參與者 2)

根據分享矩陣可以得知第 1 張分享影像出現白點的機率是 $\mathrm{P}(Y_1 = 0 \mid X = 0) = (m - A_1) / m$，而第 2 張分享影像出現白點的條件機率是 $\mathrm{P}(Y_2 = 0 \mid Y_1 = 0, X = 0) = m_2 / (m - A_1)$，因此疊合影像出現白點的機率是 $\mathrm{P}(\mathrm{OR}(Y_1, Y_2) = 0 \mid X = 0) = m_2 / m$。

Case 2：當任意 |T| 張分享影像重疊後 (|T| > 2)

根據 Case 1 可以得知，在重疊前兩張分享影像後，重疊影像上出現白點的機率為 m_2 / m。根據分享矩陣的設計可以得知，CU^0 矩陣的列向量只有一個 0，而 CL^0 矩陣的列向量則是全部內容皆為 0，因此當前兩張分享影像某一個像素點都是出現白點時，第 $h = 3 \sim |T|$ 張分享影像的該像素點的內容也一定是白色；也就是 $\mathrm{P}(Y_h = 0 \mid Y_1 = 0, Y_2 = 0, \ldots, Y_{h-1} = 0, X=0) = 1$，因此，疊合 h 張分享影像後出現白色的條件機率值等於 $\mathrm{P}(\mathrm{OR}(Y_1, Y_2, \ldots, Y_{|T|}) = 0 \mid X = 0) = \mathrm{P}(\mathrm{OR}(Y_1, Y_2) = 0 \mid X = 0) \times 1 \times \ldots \times 1 = m_2 / m$。因此，當機密影像是白點時，疊合影像上出現黑點的機率為 $\mathrm{P}(\mathrm{OR}(Y_1, Y_2, \ldots, Y_{|T|}) = 1 \mid X = 0) = 1 - m_2 / m = m_1 / m$。

$$\mathrm{P}(\mathrm{OR}(Y_1, Y_2, \ldots, Y_{|T|}) = 1 \mid X = 0) = m_1 / m \quad (6)$$

2. 根據分享矩陣 C^1 的行向量內容可以得知，C^1 中所有的 1 都在不同的列中，當疊合 2 張以上的分享影像後，都可以增加疊合影像中出現黑點的機會。分享矩陣 $C^1{}_i$ 中出現 1 的個數為 $(n^2 - n + 2i) / 2$，因此疊合 |T| 張分享影像，其所有權限等級的加總為 S 時，疊合影像中出現黑點的個數就變成為 $\Sigma_i\ (n^2 - 3n + 2i)/2 = [(n^2 - 3n)|T| + 2S] / 2$。因此當機密影像是黑點時，疊合影像上出現黑點的機率為 $\mathrm{P}(\mathrm{OR}(Y_1, Y_2, \ldots, Y_t) = 1 \mid X = 1) = [(n^2 - 3n)|T| + 2S]/(2m)$。

$$P(OR(Y_1, Y_2, \ldots, Y_{|T|}) = 1 \mid X = 1)$$
$$= [(n^2 - 3n)|T| + 2S]/(2m) \quad (7)$$

3. 因此，疊合影像的黑白色差值 $\alpha = P(OR(Y_1, Y_2, \ldots, Y_{|T|}) = 1 \mid X = 1) - P(OR(Y_1, Y_2, \ldots, Y_{|T|}) = 1 \mid X = 0) = [(n^2 - 3n)|T| + 2S]/(2m) - m_1/m = [(n^2 - 3n)|T| + 2S - 2m_1]/(2m)$。得證。

$$\alpha = [(n^2 - 3n)|T| + 2S - 2m_1]/(2m) \quad (8)$$

定理 3：當疊合所有的分享影像以後，機密影像中的白點部份有 $1/(n-1)$ 的機率出現黑色，而黑點部份則有 100% 的機率出現黑色，因此在疊合影像上會出現的黑白色差值是 $\alpha = (n-2)/(n-1)$。

證明：根據建構 1 的第 1 點，我們知道 $m_1 = n(n-1)/2$，由建構 1 的第 2 點，我們知道 $m = n(n-1)^2/2$，因此，$m_1 / m = 1 / (n-1)$。當重疊所有的分享影像後 ($|T| = n$、$S = n(n+1)/2$)，$P(OR(Y_1, Y_2, \ldots, Y_n) = 1 \mid X = 0) = 1/(n-1)$，而 $P(OR(Y_1, Y_2, \ldots, Y_n) = 1 \mid X = 1) = [(n^2 - 3n)\times n + 2\times n(n+1)/2] / (2\times n(n-1)^2/2) = 1$，因此疊合影像的黑白色差 $\alpha = 1 - 1/(n-1) = (n-2)/(n-1)$。得證。

$$\alpha = (n-2)/(n-1) \quad (9)$$

範例 4：仍然是以 4 個分享者為例，當要還原機密資訊時，機密影像的白點部分無論重疊幾張分享影像後，被重疊出黑點的機率均然保持為 6/18。反觀機密影像的黑點部分，當重疊參與者 1 和參與者 2 的分享影像後 ($|T_1| = 2$、$S = 3$)，被重疊出黑點的機率是 $[(16-12)\times 2 + 2\times 3]/(2\times 18) = 7/18$，疊合影像的黑白色差是 1/18 (0.06)；當重疊參與者 1 和參與者 4 的分享影像後 ($|T_2| = 2$、$S = 5$)，機密影像的黑點部分被重疊出黑點的機率是 $[(16-12)\times 2 + 2\times 5]/(2\times 18) = 9/18$，於是疊合影像的黑白色差提升為 3/18 (0.17)，藉此顯示出不同權限分享影像所還原出機密資訊的黑白色差結果有所差別，權限等級愈高的分享影像被疊合時，機密影像的還原效果愈好。隨著被疊合分享影像的數目增加，機密影像的白色部份被疊合出黑點的機率維持不變，而黑色部份則是逐漸遞增，因此黑白色差對比愈來愈明顯。當重疊所有的分享影像後，機密影像的白點部分被重疊出黑點的機率仍然是 6/18，而黑點部分被重疊出黑點的機率為 1，因此在還原影像上可以產生出 2/3 (0.67) 的黑白色差。

推論 1：根據等式 (8) 可以發現一旦參與者的人數決定了以後，n、m_1、m 皆為常數，因此黑白色差與被重疊的分享影像數目 ($|T|$) 和分享影像的權限值加總和 (S) 成正比。因此，參與解密的人數愈多或權限的組合愈大，疊合影像上的黑白色差值將會愈高。

推論 2：根據等式 (8) 可以發現當參與解密的人數相同時 ($|T_x| = |T_y|$)，權限值加總和愈大的組合 ($S_x > S_y$)，疊合影像上的黑白色差值將會愈高，使得黑白色差的設計符合根據權限等級還原的原則。

推論 3：根據等式 (8) 可以發現當權限值加總和的組合相同時 ($S_x = S_y$)，參與解密的人數愈多 ($|T_x| > |T_y|$)，疊合影像上的黑白色差值將會愈高，使得黑白色差的設計符合多數決的精神。

此外，本研究使用 Hsu 與 Hou [17] 所提出的改進式正規化相關係數 (Normalized Correlation，*NC*) 值來衡量重疊 r 張分享影像後 (I') 與原影像 (I) 間的相似程度，其定義如公式 (10) 所示。*NC* 等式中的左半部代表原影像中的黑點在疊合影像中還是黑點的比率，如果分子部分有值存在是表示原影像與疊合影像的值都是 1 (黑點)；而 *NC* 等式中的右半部則是代表原影像中的白點在疊合影像中還是白點的比率，其中分子部分有值存在是表示原影像和疊合影像的值都是 0 (白點)。*NC* 值必定介於 0 到 1 之間，當 *NC* 值愈大時，表示原影像和疊合影像之間的相似度愈高；當 *NC* 值愈小時，表示兩者間之相似度愈低。另一方面，彩色影像必須依據顏色的分解與合成的概念，分別計算三個分色 *NC* 值後，再以它們的平均值作為衡量的基準，如公式 (11) 所示。

$$NC = \sqrt{\frac{\sum_{x\in W}\sum_{y\in H} I(x,y)I'(x,y)}{\sum_{x\in W}\sum_{y\in H}[I(x,y)]^2} \times \frac{\sum_{x\in W}\sum_{y\in H}(1-I(x,y))(1-I'(x,y))}{\sum_{x\in W}\sum_{y\in H}[1-I(x,y)]^2}} \quad (10)$$

$$NC_{Total} = \frac{(NC_C + NC_M + NC_Y)}{3} \quad (11)$$

定理 4：在重疊影像上，機密影像的白點部份有 $1 - m_1/m = m_2/m$ 的機率出現白色，而黑點部份則有 $[(n^2 - 3n)|T| + 2S] / (2m)$ 的機率出現黑色，因此在疊合影像上的 NC 理論值會趨近於 $\{2m_2[(n^2 - 3n)|T| + 2S]\}^{0.5} / (2m)$。

證明：根據定理 2 可以得知當重疊 $|T|$ 張分享影像後，機密影像的白點部分被重疊出白點的機率是 $P(OR(Y_1, Y_2, \ldots, Y_{|T|}) = 0 \mid X = 0) = m_2/m$，而黑點部分被重疊出黑點的機率 $P(OR(Y_1, Y_2, \ldots, Y_{|T|}) = 1 \mid X = 1) = [(n^2 - 3n)|T| + 2S]/(2m)$。因此，疊合影像上的 NC 理論值等於 $NC = [P(OR(Y_1, Y_2, \ldots, Y_{|T|}) = 0 \mid X = 0) \times P(OR(Y_1, Y_2, \ldots, Y_{|T|}) = 1 \mid X = 1)]^{0.5} = [(m_2/m) \times [(n^2 - 3n)|T| + 2S]/(2m)]^{0.5} = \{2m_2[(n^2 - 3n)|T| + 2S]\}^{0.5}/(2m)$。得證。

$$NC = \{2m_2[(n^2 - 3n)|T| + 2S]\}^{0.5}/(2m) \quad (12)$$

範例 5：以 6 位參與者為例 ($m = 75$、$m_1 = 15$)，這些 NC 理論值可以從圖 3 – 4 的實驗均可得到驗證。若 $T_1 = \{1, 2\}$，則 $S_1 = 3$、$|T_1| = 2$、$NC_1 = 0.469 \sim 0.478$ (圖 3.(a)、圖 4.(a1) ~ 4.(d1))；若 $T_2 = \{5, 6\}$，則 $S_2 = 11$、$|T_2| = 2$、$NC_2 = 0.558$ (圖 3.(f))；若 $T_3 = \{1, 2, \ldots, 6\}$，則 $S_3 = 21$、$|T_3| = 6$、$NC_3 = 0.893 \sim 0.896$ (圖 4.(a5) ~ 4.(d5))。

3.2 通用模型

在基本模型中，每一位參與者被分配到權限等級都不相同，因此當確定參與機密分享的人數後，就決定了視覺機密分享的權限等級個數。然而在現實生活中，權限等級的個數必須根據不同情境而有所調整，並且每一個權限等級所擁有的參與者個數可能會大於一人。因此本研究所提出的第二個分享模型 (通用模型)，是為了改善 (n, n)-PPVSM 機密分享機制在問題 3 的限制，因此設定 n 位參與者被分配到 p 個權限等級中，其中 $2 \le p \le n - 1$，並且重新設計了兩個 $m \times n$ 的矩陣 (C^0 和 C^1)，藉此提升分享模型的彈性。分享矩陣的設計規則如下所示：

建構 2：有 n 位參與者加入機密分享的工作，並且參與者被劃分為 p $(2 \le p \le n - 1)$ 個權限等級，每個權限等級具有 W_j $(1 \le W_j \le n - 1)$ 位參與者，使得 $\Sigma_j W_j = n$。此外，為了要顯示優先權限的特性，因此我們設定權限值為 j 的參與者在分享矩陣上出現 1 的機率，會比權限值為 $j - 1$ 的參與者來的大。

1. 在 C^0 矩陣的上半部，所有的 0 都分配在不同的列上，其中，權限值 j 的行向量出現 0 的個數為 $p - j$ 個，其他位置的內容皆為 1。因此 CU^0 矩陣至少需要 $\Sigma_j W_j \times (p - j)$ 的位置來存放 0，於是我們設定 CU^0 矩陣的大小是 $m_1 \times n$，其中 $m_1 = \Sigma_j W_j \times (p - j)$。分享矩陣 C^0 中出現 1 的個數根據權限等級值而依序遞增，權限值為 j 的矩陣行向量出現 1 的個數 (A_j) 為 $m_1 - (p - j) = m_1 - p + j$，使得權限等級比較高的分享影像中出現黑色的機率比較大。

$$m_1 = \Sigma_j W_j \times (p - j) \quad (13)$$

$$A_j = m_1 - p + j \quad (14)$$

2. 為了避免在分享影像上出現機密影像的輪廓，分享矩陣 $C^1{}_i$ 出現 1 的個數要和 $CU^0{}_i$ 相同，也就是有 $m_1 - p + j$ 個 1。另外，為了擴大 C^1 矩陣在疊合時能夠產生更多的黑點，所有的 1 都是分配在不同的列上，而其他位置的內容則皆為 0。因此矩陣 C^1 的大小是 $m \times n$，其中 $m = \Sigma_j W_j \times (m_1 - p + j)$。

$$m = \Sigma_j W_j \times (m_1 - p + j) \quad (15)$$

3. 為了不讓分享影像上洩露出機密影像的蛛絲馬跡，C^0 矩陣的大小必須與 C^1 矩陣相同，因此，CL^0 矩陣的大小是 $m_2 \times n$，其中 $m_2 = m - m_1 = \Sigma_j W_j \times (m_1 - p + j) - \Sigma_j W_j \times (p - j) = \Sigma_j W_j \times (m_1 - 2p + 2j)$，並且矩陣的內容都設為 0。

$$m_2 = \Sigma_j W_j \times (m_1 - 2p + 2j) \quad (16)$$

4. 根據上述建構過程，我們可以根據建構 1 的矩陣排列方式來製作出兩個分享矩陣 C^0 和 C^1。

範例 6：以 6 位分享者且劃分為 3 個權限等級值為例 $(n = 6, p = 3)$，每一個權限值的參與者個數分別為 $W_1 = 2$、$W_2 = 3$、$W_3 = 1$，在上半部第 j 個權限等級的矩陣行向量擁有 $3 - j$ 個 0，並且每一行的 0 都分配在不同的列上。因此，CU^0 矩陣一共佔有 $m_1 = \Sigma_j W_j \times (3 - j) = 7$ 列來存放 0，其他位置的內容皆為 1；CL^0 矩陣有 $m_2 = \Sigma_j W_j \times (7 - 6 + 2j) = \Sigma_j W_j \times (2j + 1) = 28$ 列，其內容則全部都是 0；C^1 矩陣中的第 j 個權限擁有 $m_1 - p + j = j + 4$ 個 1，並且每一行的 1 都是分配在不同的列上，因此 C^1 矩陣一共佔有 $m = \Sigma_j W_j \times (j + 4) = 35$ 列來存放 1，而其他位置的內容則是皆為 0。這樣設計的分享矩陣，使得權限 j 分享影像上的像素點，不論是由 C^0 或 C^1 分配而來，都有 $\beta_j = (j + 4)/35$ 的機率產生黑點，$1 - \beta_j = (31 - j)/35$ 的機率產生白點，因此使用者無法由分享影像來判斷機密影像的內容。

當 n 位參與者被劃分為 p $(2 \le p \le n - 1)$ 個權限等級，每個權限等級具有 W_j $(1 \le W_j \le n - 1)$ 位參與者，則 $|T|$ 位參與者所組成的子集合 T 中，所有權限等級的加總為 S，疊合他們所擁有的分享影像後，機密影像中的色點分布滿足下列的定理。

定理 5：機密影像中的白點部份有 m_1/m 的機率出現黑色，而黑點部份則有 $[(m_1 - p)|T| + S]/m$ 的機率出現黑色，因此在疊合影像上會出現 $[(m_1 - p)|T| + S - m_1]/m$ 的黑白色差。

證明：

1. 建構 2 在 C^0 的上半部 (m_1 列) 中所有的 0 都在不同的列中，當疊合 2 張以上的分享影像後，這一部份都會呈現出 1 的狀況，也就是有 m_1 個機會它會出現 1。相同於定理 2 的證明方式，我們可以得知當機密影像是白點時，疊合影像上出現黑點的機率是 $P(OR(Y_1, Y_2, \ldots, Y_{|T|}) = 1 \mid X = 0) = m_1 / m$。

$$P(OR(Y_1, Y_2, \ldots, Y_{|T|}) = 1 \mid X = 0) = m_1/m \quad (17)$$

2. 在 C^1 中所有的 1 都在不同的列中，當疊合 2 張以上的分享影像後，都可以增加疊合影像中出現黑點的機會。權限值為 j 的行向量出現 1 的個數為 $m_1 - p + j$，因此疊合 $|T|$ 張分享影像，其所有權限等級的加總為 S，則疊合影像中出現黑點的個數就變成為 $\Sigma_{|T|} (m_1 - p + j) = (m_1 - p)|T| + S$。因此當機密影像是黑點時，疊合影像上出現黑點的機率為 $P(OR(Y_1, Y_2, \ldots, Y_{|T|}) = 1 \mid X = 1) = [(m_1 - p)|T| + S]/m$。

$$P(OR(Y_1, Y_2, \ldots, Y_{|T|}) = 1 \mid X=1) = [(m_1 - p)|T| + S]/m \quad (18)$$

3. 疊合影像的黑白色差值 $\alpha = P(OR(Y_1, Y_2, \ldots, Y_{|T|}) = 1 \mid X = 1) - P(OR(Y_1, Y_2, \ldots, Y_{|T|}) = 1 \mid X = 0) = [(m_1 - p)|T| + S]/m - m_1/m = [(m_1 - p)|T| + S - m_1]/m$。得證。

$$\alpha = [(m_1 - p)|T| + S - m_1]/m \quad (19)$$

定理 6：當疊合所有的分享影像以後，機密影像中的白點部份有 $1 / (n - 1)$ 的機率出現黑色，而黑點部份則有 100% 的機率出現黑色，因此在疊合影像上會出現 $(n - 2) / (n - 1)$ 的黑白色差。

證明：由建構 2 的第 1 點，我們知道矩陣 C^0 的 1 都在前 m_1 列，機密影像的白點部分有 m_1 / m 的機率被重疊出黑色，其中 $m_1 = \Sigma_j W_j \times (p - j)$、$m = \Sigma_j W_j \times (m_1 - p + j)$ 和 $n = \Sigma_j W_j$，於是 $m = \Sigma_j W_j \times m_1 - \Sigma_j W_j \times (p - j) = m_1 \times (\Sigma_j W_j - 1) = m_1 \times (n - 1)$，所以機密影像的白點部分有 $1/(n-1)$ 的機率被重疊出黑色；由建構 2 的第 2 點，我們知道矩陣 C^1 的 1 都在不同列，$m = \Sigma_j W_j \times (m_1 - p + j)$，所以機密影像的黑點部分有 $[(m_1 - p)|T| + S]/m$ 的機率被重疊出黑色。當重疊所有的分享影像後 ($|T| = n = \Sigma_j W_j$、$S = \Sigma_j W_j \times j$)，$P(OR(Y_1, Y_2, \ldots, Y_n) = 1 \mid X=1) = [(m_1 - p)n + S] /m = [\Sigma_j W_j(m_1 - p) + \Sigma_j W_j \times j] /m = [\Sigma_j W_j(m_1 - p + j)] / m = m/m = 1$，因此疊合影像的黑白色差值等於 $\alpha = 1 - 1/(n-1) = (n - 2)/(n - 1)$。得證。

$$\alpha = (n-2)/(n-1) \tag{20}$$

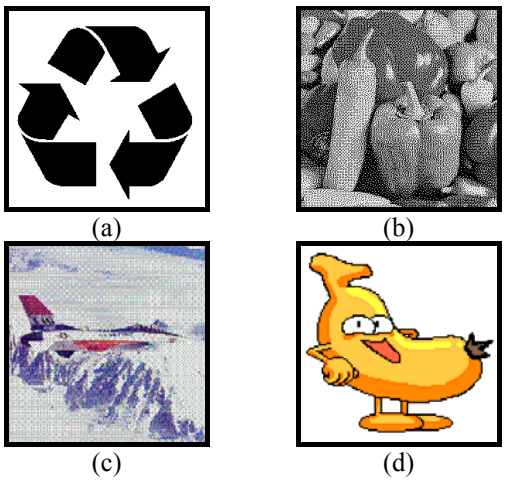
定理 7：在重疊影像上，機密影像的白點部份有 $1 - m_1/m = m_2/m$ 的機率出現白色，而黑點部份則有 $[(m_1 - p)|\mathrm{T}| + S]/m$ 的機率出現黑色，因此在疊合影像上的 NC 理論值會趨近於 $\{m_2[(m_1-p)|\mathrm{T}| + S]\}^{0.5}/m$。

證明：根據定理 6 可以得知機密影像的白點部分被重疊出白點的機率是 $1 - m_1/m = m_2/m$，而黑點部分被重疊出黑點的機率 $[(m_1-p)|\mathrm{T}| + S]/m$。根據公式 (10) 的定義，疊合影像上的 NC 理論值是等於原影像中的黑點在疊合影像中還是黑點的比率，再乘以原影像中的白點在疊合影像中還是白點的比率後的開根號值。因此，通用模型的 $NC = \{m_2/m \times [(m_1-p)|\mathrm{T}| + S]/m\}^{0.5} = \{m_2[(m_1-p)|\mathrm{T}| + S]\}^{0.5}/m$。得證。

$$NC = \{m_2[(m_1-p)|\mathrm{T}| + S]\}^{0.5}/m \tag{21}$$

四、實驗結果與分析討論

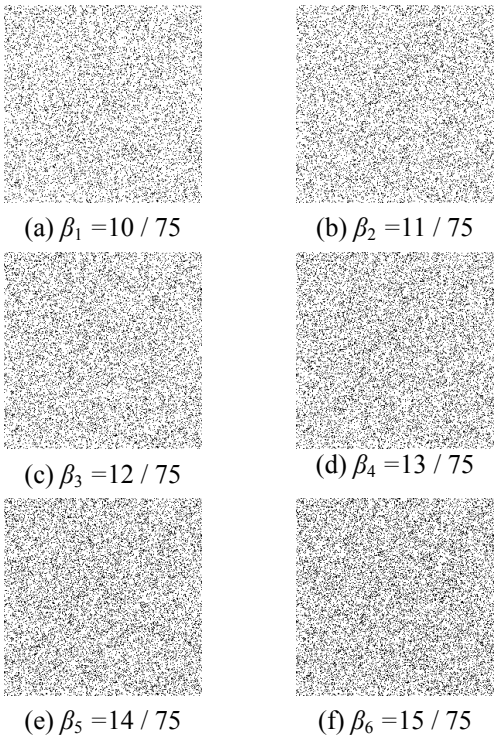
本實驗是在作業系統 Microsoft Windows XP 下，以 Java (JDK 1.6.10) 程式語言作為開發環境，硬體設備為個人桌上型電腦 CPU AMD Athlon(tm) X2 240 和 RAM 2 GB。實驗圖像是四張經過半色調處理後的 BMP 格式影像，分別是大小為 256×256 的黑白影像 Recycle、灰階影像 Pepper 與彩色影像 Airplane 和 Banana (圖 1.(a) ~ 圖 1.(d))。



(a) (b) (c) (d)

圖 1. 本研究所使用的實驗圖像

本研究首先利用黑白影像 Recycle 來進行實驗，然後根據建構 1 的分享矩陣來產生出六張雜訊式的分享投影片 (m = 75、m_1 = 15)，其結果如圖 2 所示。圖 2.(a) 的分享投影片上，每一個像素點出現黑色的機率約等於 10 / 75，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。圖 2.(b) ~ 圖 2.(f) 的分享影像上，黑點的出現機率將由 11 / 75 增加到 15 / 75，將來在機密資訊還原時，所能夠貢獻的黑點隨之增加，因而呈現機根據優先權等級還原機密資訊的特點。

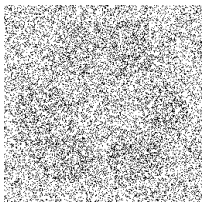


(a) β_1 =10 / 75 (b) β_2 =11 / 75
(c) β_3 =12 / 75 (d) β_4 =13 / 75
(e) β_5 =14 / 75 (f) β_6 =15 / 75

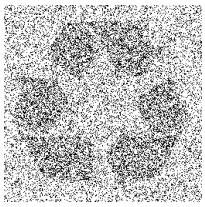
圖 2. 6 張無意義且權限等級相異的分享影像。(a) ~ (f) 權限等級為由小到大

圖 3 是根據圖 2 的六張分享影像，且重疊不同組合分享影像後的結果，其中圖 3.(a) ~ 圖 3.(e) 分別是重疊 1+2、1+3、… 和 1+6 的結果。根據公式 (8) 的定義，因此疊合影像的 α 值是隨著權限值總和 (S) 的上升而增加，因此較高權限值的參與者擁有還原機密資訊的主控權。根據圖 3.(a) ~ 圖 3.(e) 的實驗結果顯示，α 值從 0.08 提升到 0.13，而 NC 值則是從 0.475 提升到 0.520，因此符合推論 2 的結果。此外，圖 3.(f) ~ 圖 3.(j) 分別是權限加總值等於 11 (5+6、1+4+6、

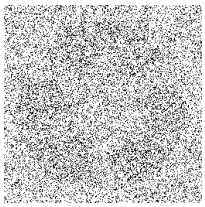
2+3+6、2+4+5 和 1+2+3+5) 的結果，我們可以發現，重疊四張分享影像的結果 (圖 3.(j)，$\alpha = 0.43$，*NC* 值趨近於 0.706) 優於重疊三張的結果；而重疊三張分享影像的還原結果 (圖 3.(g) ~ 圖 3.(i)，$\alpha = 0.31$，*NC* 值趨近於 0.639) 又優於重疊兩張的結果 (圖 3.(f)，$\alpha = 0.19$，*NC* 值趨近於 0.558)，隨著疊合影像的數目增加，機密影像的輪廓將會愈來愈清晰，這個結果符合多數決的精神 (推論 3)。最後，在相同參與人數、相同權限組合的條件下，重疊影像的還原結果也都近似 (圖 3.(g) ~ 圖 3.(i)，$\alpha = 0.31$，*NC* 值趨近於 0.639)，符合推論 1 的結果。



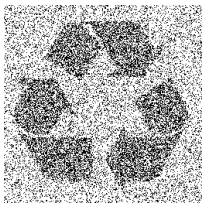
(a) 重疊 Share 1+2
$\alpha = 0.08$, $NC = 0.475$



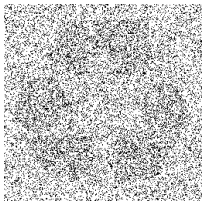
(f) 重疊 Share 5+6
$\alpha = 0.19$, $NC = 0.558$



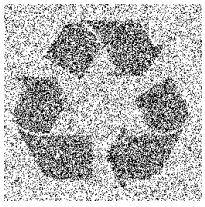
(b) 重疊 Share 1+3
$\alpha = 0.09$, $NC = 0.481$



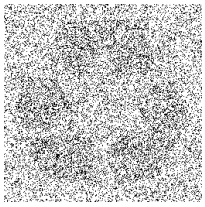
(g) 重疊 Share 1+4+6
$\alpha = 0.31$, $NC = 0.640$



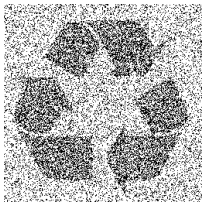
(c) 重疊 Share 1+4
$\alpha = 0.11$, $NC = 0.496$



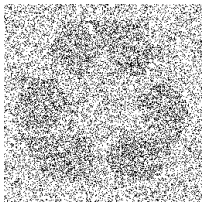
(h) 重疊 Share 2+3+6
$\alpha = 0.31$, $NC = 0.639$



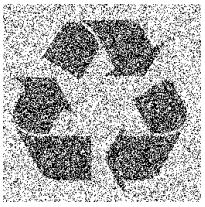
(h) 重疊 Share 1+5
$\alpha = 0.12$, $NC = 0.504$



(i) 重疊 Share 2+4+5
$\alpha = 0.31$, $NC = 0.638$



(e) 重疊 Share 1+6
$\alpha = 0.13$, $NC = 0.520$



(j) 重疊 Share 1+2+3+5
$\alpha = 0.43$, $NC = 0.706$

圖 3. (a) ~ (e) $|T| = 2$ 的相關重疊組合，權限由 S = 3 - 7 依序疊合，(f) ~ (j) S = 11 的相關重疊組合，參與者由 $|T| = 2 - 4$ 依序疊合

圖 4 是三張機密影像重疊 2 ~ 6 張分享影像，並且根據權限等級由小到大依序疊合的結果 (1+2, 1+2+3, …, 1+2+…+6)。根據黑白色差值 (α) 和 *NC* 值定義，當參與分享機密資訊的參與者人數 $n = 6$ 時，基本模型的疊合影像 α 值等於 $[(n^2 - 3n)|T| + 2S - 2m_1]/(2m)$，而 *NC* 值等於 $\{2m_2[(n^2-3n)|T|+2S]\}^{0.5}/(2m)$。從圖 4 中可以發現，實驗結果的 α 值與 *NC* 值都隨著 $|T|$ 值與 S 值而快速增加。當重疊所有的分享影像後 (圖 4.(a5) ~ 4.(d5))，*NC* 理論上限值會等於 $(60 / 75)^{0.5}$，因此 *NC* 值將會接近於 0.894，顯示無論機密影像的型態為何，疊合影像上的還原品質都是最高的，並且能夠清晰地呈現出機密資訊的內容。並且本研究的還原品質(*NC* 值介於 0.893 ~ 0.896) 都優於 (n, n)-PPVSM 的研究成果 (*NC* 值介於 0.843 ~ 0.845)，這個結果顯示本研究所提出的分享模型不僅可以完全地符合優先權的分享概念，在機密資訊的還原上也擁有不錯的視覺品質。

此外，圖 4 也顯示出機密影像的還原品質與機密影像型態的關係。當機密影像的型態為簡單的黑白二元影像 (Recycle) 或不連續色調的卡通圖像 (Banana) 時，由於影像的構圖簡單且有大範圍相同的色塊，於是在機密資訊還原的過程中，較為容易顯示出顏色的差異，因而機密資訊的還原速度比較快，視覺品質也比較好，如圖 4.(a) 和圖 4.(b) 的還原過程。反之，當機密影像的型態是連續色調的灰階 (Pepper) 或彩色影像 (Airplane) 時，必須重疊多張分享影像後才能呈現連續色調上細微的差異，因此機密資訊的還原速度比較慢，視覺品質也比較差，如圖 4.(c) 和圖 4.(d) 的還原過程。

本研究的第三個實驗是以 6 位分享者劃

分為 3 個權限等級值為例 ($n = 6, p = 3$)，其中每一個權限值的參與者個數分別為 $W_1 = 2$、$W_2 = 3$、$W_3 = 1$，然後根據建構 2 的分享矩陣來產生出 6 張雜訊式的分享投影片 ($m = 35$、$m_1 = 7$)。這樣設計的分享矩陣，使得分享影像上的像素，不論是由 C^0 或 C^1 分配而來，權限 j 的分享影像有 $(j + 4)/35$ 的機率產生黑點，有 $(31 - j)/35$ 的機率產生白點，因此使用者無法由分享影像來判斷機密影像的內容，其結果如圖 5 所示。圖 6 則是根據圖 5 分屬於 3 個不同權限等級的 6 張分享影像疊合後的結果。從圖 6 的實驗結果可以發現，α 值與 *NC* 值都隨著參與者人數與權重總和的增加而快速增加，並且還原影像能夠清晰地呈現出機密資訊的內容 (圖 6.(e))。

根據上述三個實驗結果可以得知，本研究所提出的兩個分享模型確實可以達成基於優先權的視覺機密分享，並且在分享影像上都不會顯露出機密資訊的輪廓。此外，通用模型延伸了基本模型的設計概念，使得權限等級的個數與每一個權限內的參與者人數可以根據使用者需求進行調整，因而擴充了具有權限等級概念之不擴展型漸進式視覺密碼的彈性。

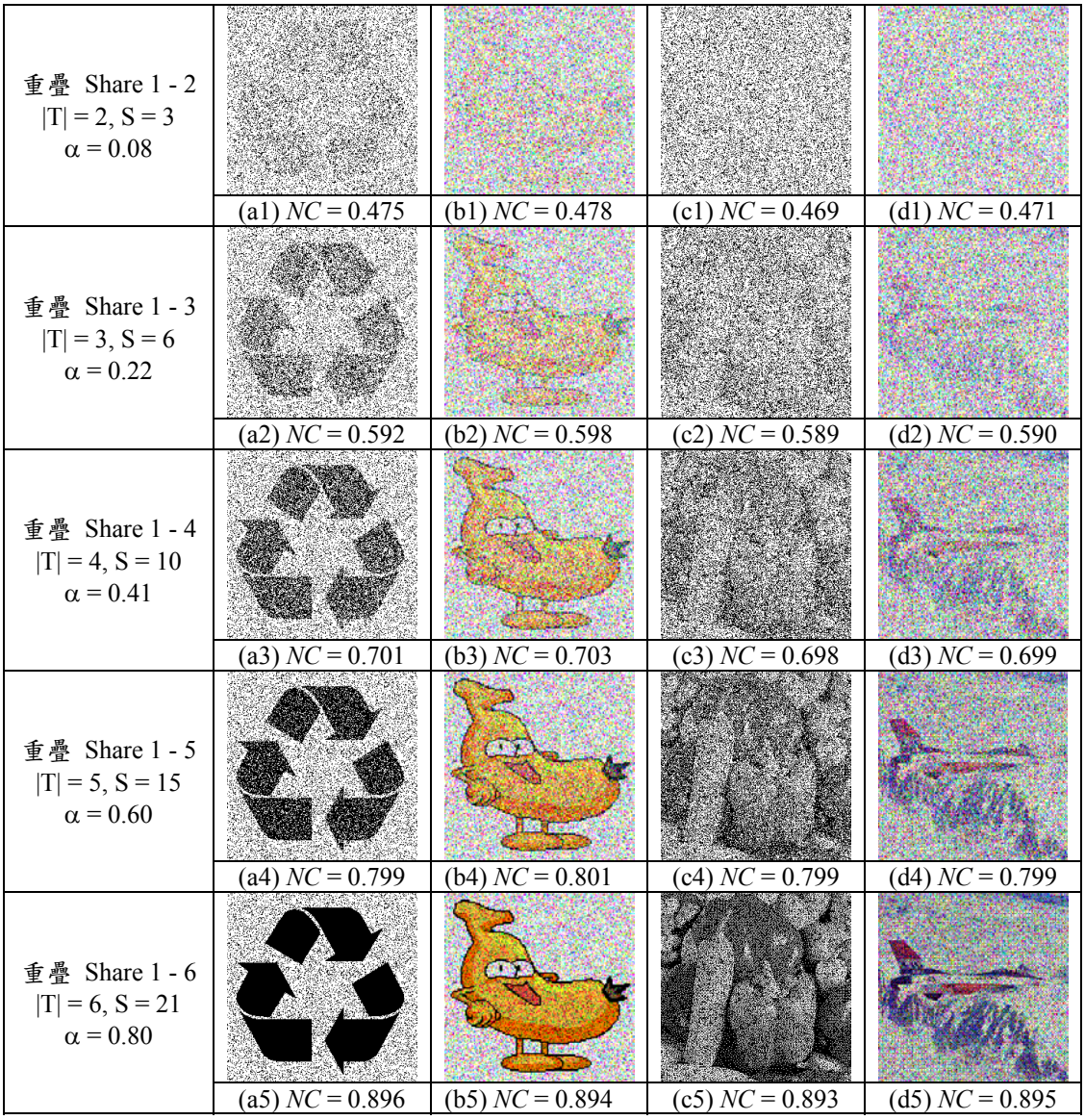
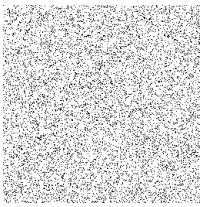


圖 4. 不同機密影像的還原過程：(a) Recycle，(b) Banana，(c) Pepper，(d) Airplane

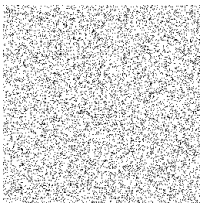
五、結　論

漸進式視覺密碼不同於傳統視覺機密分享的傳輸概念，當愈來愈多分享影像重疊後，疊合影像的黑白色差值將會愈來愈高，使得機密影像的輪廓逐漸地變為清晰。不過在傳統漸進式視覺密碼的研究中，是假設每一個參與者都擁有相同的能力來還原機密資訊，因此侯永昌等 [11] 基於優先權概念的考量而提出了一個具有優先權概念的分享模型，稱之為 (n, n)-PPVSM。雖然這個模型可以根據優先權等級來配置不同的分享影像給每一位參與者，不過這個分享模型卻有三個現象無法完全地符合優先權等級的概念 (請參見 2.2 節)，於是本研究提出兩個新分享模型設計法，藉此來補足 (n, n)-PPVSM 的研究限制。

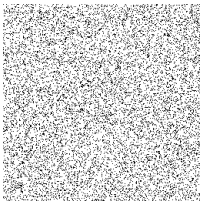
相較於侯永昌等的研究成果，本研究具備下列幾項優點：(1) 分享矩陣可以根據實際狀況，調整優先權等級的個數和每一個權限等級內的參與者人數，並且在相同權限等級內的參與者，具有相同的能力來還原機密資訊。(2) 根據推論 1 到推論 3 的結果顯示，參與解密的人數愈多或權限的組合愈大，疊合影像上的黑白色差值將會愈高，使得黑白色差的設計符合根據多數決和權限等級還原的原則。(3) 當重疊所有的分享影像後，基本模型和通用模型的還原影像黑白色差值都是 $(n-2)/(n-1)$，這個結果優於 (n, n)-PPVSM 的 $(n-1)/(n+1)$。(4) 本研究的分享方法是基於像素不擴展，因此分享影像的大小與機密影像相同。



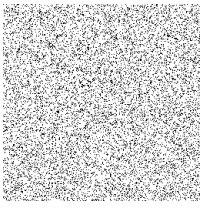
(a) β_1 =5/35



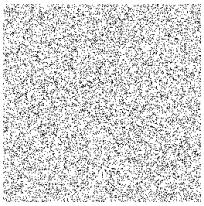
(b) β_1 = 5/35



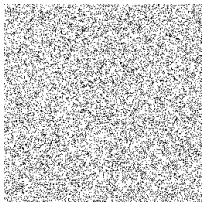
(c) β_2 = 6/35



(d) β_2 = 6/35

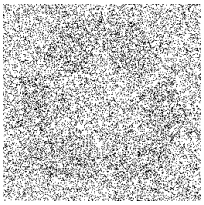


(e) β_2 = 6/35

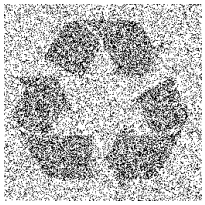


(f) β_3 = 7/35

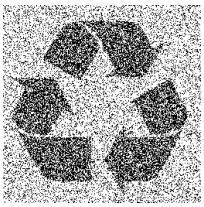
圖 5. (a) ~ (b) 權限等級 1；(c) ~ (e) 權限等級 2；(f) 權限等級 3



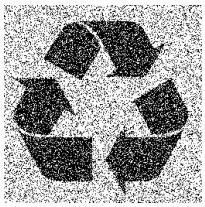
(a) 重疊 Share 1 - 2
|T| = 2, S = 2
α = 0.09, *NC* = 0.474



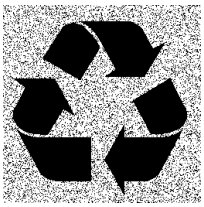
(b) 重疊 Share 1 - 3
|T| = 3, S = 4
α = 0.26, *NC* = 0.603



(c) 重疊 Share 1 - 4
|T| = 4, S = 6
α = 0.43, *NC* = 0.708



(d) 重疊 Share 1 - 5
|T| = 5, S = 8
α = 0.60, *NC* = 0.798



(e) 重疊 Share 1 - 6
|T| = 6, S = 11
α = 0.80, *NC* = 0.893

圖 6. 根據權限由低到高依序重疊 2 ~ 6 張分享影像的結果

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 NSC99-2221-E-032-051 的部份研究成果，並感謝 M. C. Liao 於論文初稿期間提供寶貴之意見，謹此致謝。

參考文獻

[1]. Shamir, A., “How to share a secret,” Communications of the ACM, Vol. 22, No. 11, pp. 612-613, 1979.

[2]. Thien, C. C. and Lin, J. C., “Secret image sharing,” Computers & Graphics, Vol. 26, No. 5, pp. 765-770, 2002.

[3]. Chen, S. K. and Lin, J. C., “Fault-tolerant and progressive transmission of images,” Pattern Recognition, Vol. 38, No. 12, pp. 2466-2471, 2005.

[4]. Wang, R. Z. and Shyu, S. J., “Scalable secret image sharing,” Signal Processing: Image Communication, Vol. 22, No. 4, pp. 363-373, 2007.

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

[6]. Hou, Y. C., “Visual cryptography for color images,” Pattern Recognition, Vol. 36, No. 7, pp. 1619-1629, 2003.

[7]. Fang, W. P. and Lin, J. C., “Progressive viewing and sharing of sensitive images,” Pattern Recognition and Image Analysis, Vol. 16, No. 4, pp. 638-642, 2006.

[8]. Fang, W. P., “Friendly progressive visual secret sharing,” Pattern Recognition, Vol. 41, No. 4, pp. 1410-1414, 2008.

[9]. 侯永昌、官振宇，“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，第十七卷，第三期，第 131–154 頁，2010。

[10].Hou, Y. C. and Quan, Z. Y. “Progressive visual cryptography with unexpanded shares,” IEEE Transactions on Circuits and Systems for Video Technology, Vol. 21, No. 11, pp. 1760-1764, 2011.

[11].侯永昌、官振宇、蔡志豐，“具有優先權概念之不擴展漸進式視覺密碼”，資訊管理學報，第十八卷，第三期，第 125–148 頁，2011。

[12].Jin, D., Yan, W. Q., and Kankanhalli, M. S., “Progressive color visual cryptography,” Journal of Electronic Imaging, Vol. 14, No. 3, pp. 077003-1-077003-10, 2005.

[13].Wang, R. Z., Lee, Y. K., Huang, S. Y., and Chia, T. L., “Multilevel visual secret sharing,” in Proceeding of ICICIC’07, pp. 283-286, 2007.

[14].Wang, R. Z., Lan Y. C., Lee, Y. K., Huang, S. Y., Shyu, S. J., and Chia, T. L., “Incrementing visual cryptography using random grids,” Optics Communications, Vol. 283, No. 21, pp. 4242-4249, 2010.

[15].Chen, T. H. and Lee Y. S., “Yet another friendly progressive visual secret sharing scheme,” in 5-th International Conference on Intelligence Information Hiding and Multimedia Signal Processing, pp. 353-356, 2009.

[16].Shyu, S. J., “Image encryption by random grids,” *Pattern Recognition*, Vol. 40, No. 3, pp. 1014–1031, 2007.

[17].Hsu, C. S. and Hou, Y. C., “Copyright protection scheme for digital images using visual cryptography and sampling methods,” Optical Engineering, Vol. 44, No. 7, pp. 077003-1-077003-10, 2005.