

基於位元層技術於彩色影像之階層式多重視覺秘密分享機制 之研究與應用

A Study of Bit-level Processing Based on Color Imagines of Hierarchical Multiple Visual Secret Sharing Schemes and Applications

廖惠雯(H.W. Liao)、黃信維(S.W. Huang)、陳立忠(L.J. Chen)、
王培任(P.R. Wang)、黃志仁(J.R. Huang)、劉佳政(C.C. Liu)

嶺東科技大學資訊科技系

hwliao@mail.ltu.edu.tw

摘要

視覺密碼學最早在1994年由Naor和Shamir所提出，彩色影像之階層式多重視覺秘密分享機制，先將彩色影像分解為三個減色影像CMY，再分別利用半色調處理技術，使其將減色影像CMY 疊合後，可以得到原本的彩色影像，其分享影像及還原後的機密影像之長與寬均擴展為原始影像之2倍，無法維持原本機密影像的大小，且產生影像失真的情況。本文提出利用位元平面層技術應用於彩色影像之階層式多重視覺秘密分享機制，每一階層的成員仍擁有兩種機密影像，且彩色機密影像利用位元層技術分解及疊合替代傳統的半色調處理技術，並利用Lukac 和Plataniotis所提出的解密規則，即可將分享影像恢復成原始機密影像，改善了失真及無法恢復原始機密影像之缺點。

關鍵字：視覺密碼學、階層式多重視覺秘密分享機制、減色影像、半色調處理技術、位元層技術。

Abstract

The concept of visual secret sharing

scheme was first proposed by Naor and Shamir in 1994; many secret sharing schemes were published afterward; one of them, the color images of hierarchical multiple visual secret sharing schemes, which first decomposed the color images into three subtractive primaries colors, CMY, then applied the halftone process technique to these subtractive primary colors and stacked them to obtain the original images; even though this process made the stacks returned to the original secret images; however, the process made the original images distorted to 2×2 times their sizes.

This article utilized the bit-level processing and applied it to the color images of hierarchical multiple visual secret sharing schemes; with this approach, replaces the traditional halftone technique with the bit-level decomposition / stacking process, and each hierarchical affiliate maintains two sets of secret images, then applied the process proposed by Lukac and Plataniotis to restore the original images to their sizes

without distortion.

Thus when replacing the traditional halftone processing with bit-level share technology and applying it to the color images will not only resolve the deficiency that distorts the original share images, but also restore them to their original sizes.

Keyword : Visual Cryptography, Hierarchical Multiple Visual Secret Sharing Scheme, Subtractive Primary, Halftone Technology, Bit-level Processing.

前言

隨著網際網路世界的蓬勃發展，網路已成為現代人所不可或缺的日常工具，數位多媒體的傳輸日益廣闊，資訊媒體安全的研究亦備受重視。

傳統密碼學中的加密技術是目前最普遍用來保護資料安全的方法，雖然傳統密碼學可以保護電子資料的安全，但在解密的過程中，所需的運算、複雜度及有限的設備下也是一大問題，如 PDA 及手機...等，而視覺密碼(Visual Cryptography)便在此環境下因應而生。

視覺密碼學是依據人類視覺系統對於影像色差的反應，將機密影像分成數張分享影像(Share Images)，其主要目的為保護機密訊息，機密訊息可為文字、數字、符號或圖形等，再將影像重疊進行解密，解密過程中不需任何複雜的電腦計算，也無需任何的密碼學知識。

2. 文獻探討

視覺密碼學[5-6]最早在 1994 年由 Naor 和 Shamir 所提出，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，而是直接重疊分享影像即可視覺系統進行解密，改進了傳統密碼

學在解密過程中須大量複雜運算的缺點。其方法是產生 n 張分享影像，並分別授權給 n 個成員，若要解得機密訊息，只要有 t ($t \leq n$) 個以上的成員，將分享影像正確重疊，由人類視覺系統判讀即可還原機密影像，在分享影像小於 t 張時($1 \sim t-1$)，就無法取得機密訊息，這就是視覺密碼中典型的 $\{t, n\}$ 門檻機制 (t out of n Threshold Scheme)。

在 Naor 和 Shamir 的視覺密碼中，為使分享影像疊合後，能保有原始比例之型態，常將機密影像中每一個像素擴展成 2×2 的區塊，若原機密影像為白色，所分解出的分享影像疊合起來是二黑二白的像素區塊；若原機密影像為黑色，所分解出來的分享影像疊合起來則為四黑零白的區塊，如圖 1 即為黑白影像於 $\{2, 2\}$ 門檻機制像素擴展為 2×2 之視覺密碼的加密與解密。

Floyd 和 Steinberg 於 1976 年提出誤差擴散法(Error Diffusion)[3]，此種方法能將整個半色調影像的能量集中在高頻的部份。對於人類的視覺系統而言，具有這種能量分布的半色調影像可以產生很好的視覺效果。其做法是當像素的色彩改變時，將色彩的差值分散到周圍其他像素上，使得鄰近的像素值差異可以儘量低於肉眼可察覺的程度。

色彩基本上是眼睛察覺到光所產生的反應。在日常生活中，由於彩色影像的使用率大於黑白或灰階影像，色彩模型常用的有 RGB(Red、Green、Blue)和 CMYK(Cyan、Magenta、Yellow、Black)...等。

RGB 模型是由紅(Red)、綠(Green)、藍(Blue)三原色所組成。利用這三種顏色的不同比例和強度來產生各種顏色，色光混合的愈多，光度愈增加，愈趨近白色光，所以亦稱增色模型[7]如圖2。

利用這三種顏色的不同比例和強度來產生各種顏色，日常生活中如電視、電腦螢幕等都是使用這種模型的實際運用。

色彩印刷仍利用顏料的吸光特性顯示色調，而CMYK模型是由青色(Cyan)、洋紅(Magenta)、黃色(Yellow)為印刷三原色，是利用物體表射的色光組合來呈現色彩，分別吸收各自的補光色；青色吸收紅光，洋紅色吸收綠光，黃色吸收藍光。也利用這三種顏色的不同比例和強度來產生各種顏色，這三種原色混合會產生出近似黑色(K)，顏料的混合愈多，光度愈減少，愈趨近於黑色，亦稱為減色模型[7]如圖3。在色彩系統中，RGB與CMY彩色系統為互補色如圖4。而彩色印表機就是利用減色模型的原理來列印彩色影像。

Young-Chang Hou 於 2003 年根據以往視覺密碼的研究，加上半色調技術及分色原理 C、M、Y 顏料三原色，再對其子影像做處理，提出灰階影像和彩色影像的視覺密碼作法[8]，和傳統上的黑白影像視覺密碼模型一樣，將機密影像上的每一個像素擴展至分享影像上的 2x2 區塊，而區塊中皆保持 2 個色點的狀態。它不但延續了黑白視覺密碼直接利用視覺系統解密，無須大量運算的優點，利用在他的方法上，亦可應用於灰階及彩色影像的製作上。

分色影像 CMY 中的每一分色為 8 個位元可以描述 256 色階(從 0 到 255)，如下二進位公式(1)所示：

(i, j) 表示圖像素位置； $O_{(i,j)}$ 表示色階值；

$$O_{(i,j)} = O_{(i,j)}^1 2^7 + O_{(i,j)}^2 2^6 + \dots + O_{(i,j)}^7 2 + O_{(i,j)}^8 \quad (1)$$

$O_{(i,j)}^1, O_{(i,j)}^2, \dots, O_{(i,j)}^8$ 表示位元值。圖 5 即為分色影像分解為八張二元圖。

Lukac 和 Plataniotis 於 2005 年利用 Bit-level(位元層)提出新的秘密分享機制

[4]，利用位元層技術的分解和疊合及傳統的視覺秘密分享加密技術，如公式(2)：

$$f_e(r_{(i,j)}) = \begin{cases} [S_1, S_2]^T \in C_0 & \text{for } r_{(i,j)} = 0, \\ [S_1, S_2]^T \in C_1 & \text{for } r_{(i,j)} = 1. \end{cases} \quad (2)$$

$$C_0 = \begin{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix} \\ \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \end{bmatrix},$$

$$C_1 = \begin{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \\ \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \end{bmatrix},$$

$f_e(\cdot)$ 為加密函數， $r(i, j)$ 為原始圖位置 (i, j) 之像素值， $r(i, j)=0$ 表黑色， $r(i, j)=1$ 表白色， C_0 與 C_1 為原始像素值所對應之 2x2 擴展之分享影像 1(S_1)及分享影像 2(S_2)的矩陣表示方式，其區塊表示如表 1 和其所提出之解密規則，能完整的重建及還原機密影像，如公式(3)：

$$O_{(i,j)}^b = f_d(S_1^b, S_2^b) = \begin{cases} 0 & \text{for } [S_1^b, S_2^b]^T \in C_0 \\ 1 & \text{for } [S_1^b, S_2^b]^T \in C_1 \end{cases} \quad (3)$$

b 表位元層，每一分色(C、M、Y)影像是 256 色階，共 8 個位元層($b=1, 2, \dots, 8$)， $O_{(i,j)}^b$ 為還原像素值， S_1^b, S_2^b 為分享影像 1 及分享影像 2， (i, j) 表還原像素位置， $S_1^b(2i-1, 2j-1) = S_2^b(2i-1, 2j-1)$ 即為 C_1 ，可還原 $O_{(i,j)}^b = 1$ ； $S_1^b(2i-1, 2j-1) \neq S_2^b(2i-1, 2j-1)$ 即為 C_0 ，可還原 $O_{(i,j)}^b = 0$ 。圖 6 為利用 Lukac 和 Plataniotis 方式將灰階影像應用於 {2, 2} 視覺秘密分享。

廖惠雯及林秀蓓於 2007 年提出利用奇數層分享影像為 2 黑 2 白像素及偶數層分享影像為 3 黑 1 白像素之交互運作，建立階層式視覺機密分享機制[1-2]，其青(C)分色建構機制如表 2 及階層關係如圖 7，(減色模型洋紅(M)與黃色(Y)之階層式秘密分享交互建構機制和青色(C)之階層式秘密分享交互建構機制模型相同)，再運用旋轉分享影像的方式，管理者與每個成員

皆可擁有 2 種機密影像，且可不斷的增加成員數，管理者並不須要改變原始分享影像，即可和成員所持的分享影像疊合，讀出機密影像的內容。

本文提出利用位元層技術應用於彩色之階層式多重視覺秘密分享機制，每一階

層的成員仍擁有兩種機密影像，且彩色機密影像利用位元層技術分解及疊合替代傳統的半色調處理技術，並利用 Lukac 和 Plataniotis 所提出的解密規則，即可將分享影像恢復成原始機密影像，改善了失真及無法恢復原始機密影像之缺點。

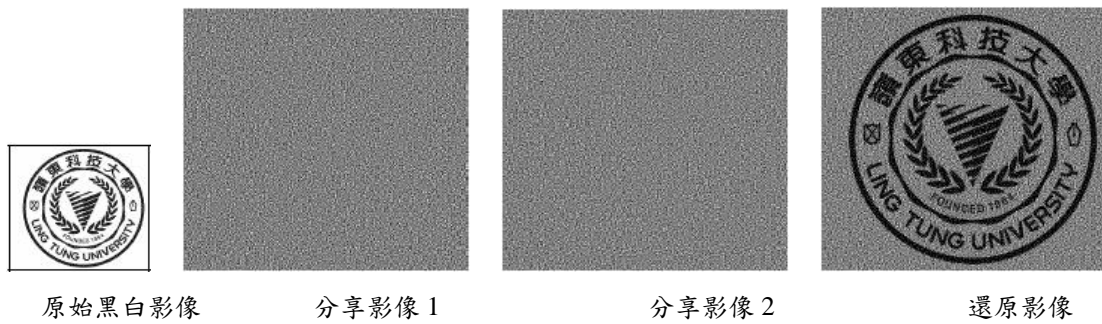


圖 1. {2, 2}黑白影像之視覺密碼加密與解密

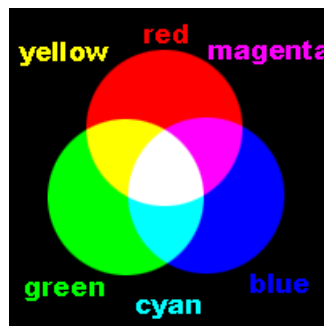


圖 2. 增色模型

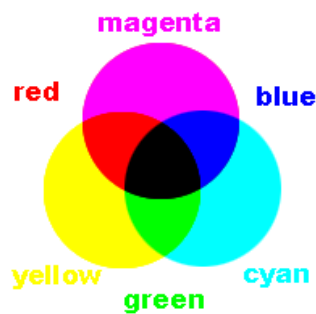


圖 3. 減色模型

$$\begin{pmatrix} C \\ M \\ Y \end{pmatrix} = \begin{pmatrix} 255 - R \\ 255 - G \\ 255 - B \end{pmatrix}$$

圖 4. RGB 與 CMY 之對應圖

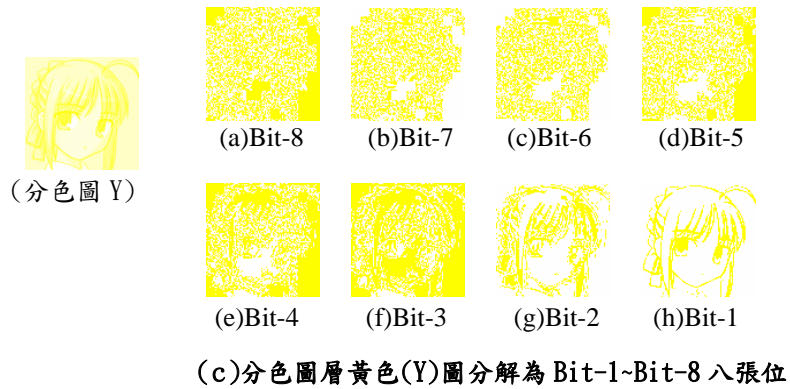
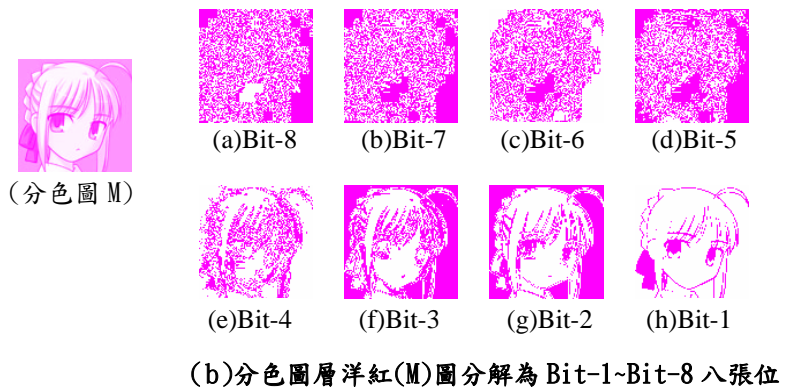
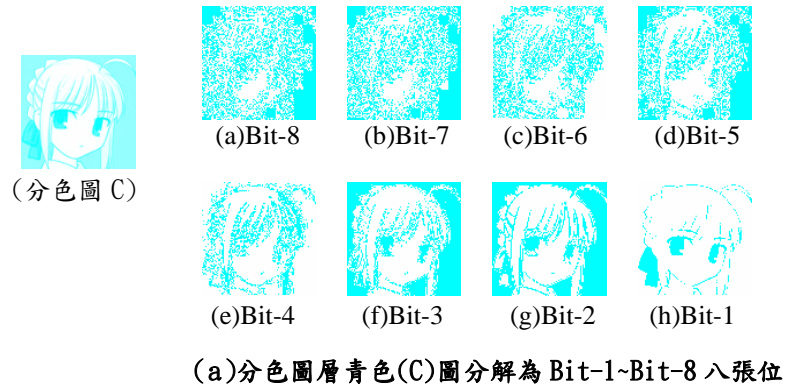


圖 5. CMY 三色分色圖

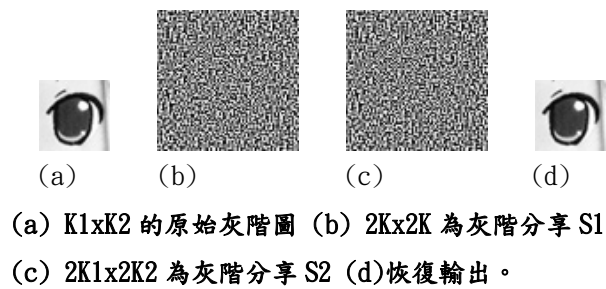


圖 6. 灰階影像 $\{2, 2\}$ 視覺機密分享

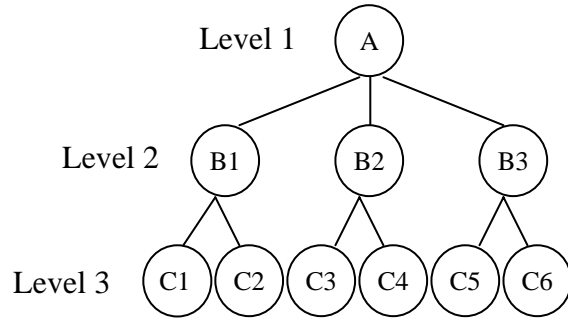


圖 7. 階層式架構

表 1. 2x2 像素擴展模型

	機密影像(白)	機密影像(黑)
分享影像 1		
分享影像 2		
疊合結果		

表 2 (2,2)青色(C)之階層式秘密分享交互建構機制

(a)奇數層 Share A 為 2 青 2 白區塊與偶數層 Share B 為 3 青 1 白區塊之機密建構模型

機密圖 1	W	W	C	C	W	W	C	C	W	W	C	C	W	W	C	C
機密圖 2	W	C	W	C	W	C	W	C	W	C	W	C	W	C	W	C
Share A																
Share B																
A+B																
Share A'																
A'+B																

(b)偶數層 Share B 為 3 青 1 白區塊與奇數層 Share C 為 2 青 2 白區塊之機密建構模型

機密圖 3	W	W	C	C	W	W	C	C	W	W	C	C	W	W	C	C
機密圖 4	W	C	W	C	W	C	W	C	W	C	W	C	W	C	W	C
Share B																
Share C																
B+C																
Share B'																
B'+C																

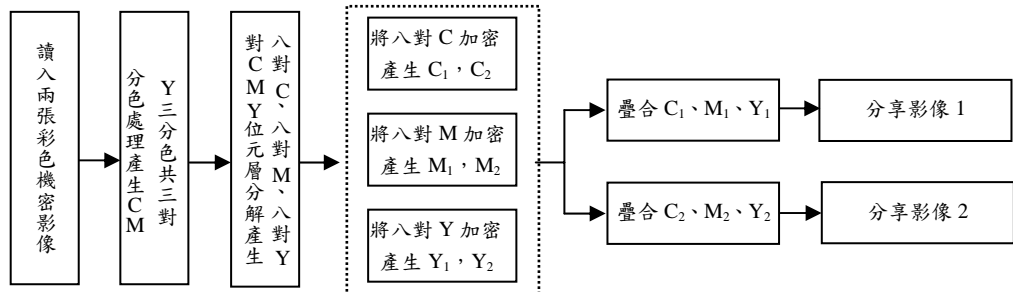
3. 研究方法

本文提出利用位元層技術於彩色影像之階層式多重視覺秘密分享機制之研究與應用，其加密流程如圖 8(a)，A 與 B1 若要共享兩張機密時，先將兩張機密影像分色處理，產生 CMY 三分色共三對，對 CMY 做位元層分解，每分色機密圖可分解為八張位元層圖，三分色共二十四對，將此二十四對位元層圖利用階層式交互建構機制加密，每對位元層圖分別產生兩張分享影像 S_{1C}^b 、 S_{1M}^b 、 S_{1Y}^b 及 S_{2C}^b 、 S_{2M}^b 、 S_{2Y}^b ($b=1, 2, \dots, 8$)，再將 C 分色 S_{1C}^b 八張位元層圖疊合即為 C_1 ， S_{2C}^b 八張位元層圖疊合即為 C_2 ，M 分色 S_{1M}^b 八張位元層圖疊合即為 M_1 ， S_{2M}^b 八張位元層圖疊合即為 M_2 ，Y 分色 S_{1Y}^b 八張位元層圖疊合即為 Y_1 ， S_{2Y}^b 八張位元層圖疊合即為 Y_2 ，疊合 C_1 、 M_1 、 Y_1 可得分享影像 1，疊合 C_2 、 M_2 、 Y_2 可得分享影像 2；若增加第二層成員與第一層之間的機密，其加密流程如圖 8(b)，讀入兩張彩色機密影像，如圖 8(a) 產生 S_{1C}^b 、 S_{1M}^b 、 S_{1Y}^b 、 S_{2C}^b 、 S_{2M}^b 、 S_{2Y}^b 的方法產生 S_{3C}^b 、 S_{3M}^b 、 S_{3Y}^b 、 S_{4C}^b 、 S_{4M}^b 及 S_{4Y}^b ，再讀入分享影像 1，將分享影像 1 做分色處理及位元層分解產生 S_{1C}^b 、 S_{1M}^b 、 S_{1Y}^b ，根據該層 S_{1C}^b 、 S_{3C}^b 及 S_{4C}^b 經表 2(a) 加密疊合得 C_3 ，如同產生 C_3 方式產生 M_3 及 Y_3 ，再疊合 C_3 、 M_3 、 Y_3 可得分享影像 3；若欲增加第三層成員 C1，根據分享影像 2 及 B1 與 C1 之間的 2 個機密影像，參照表 2(b) 加密方式，即可產生 C1 的分享影像，不需重新產生分享影像 2。

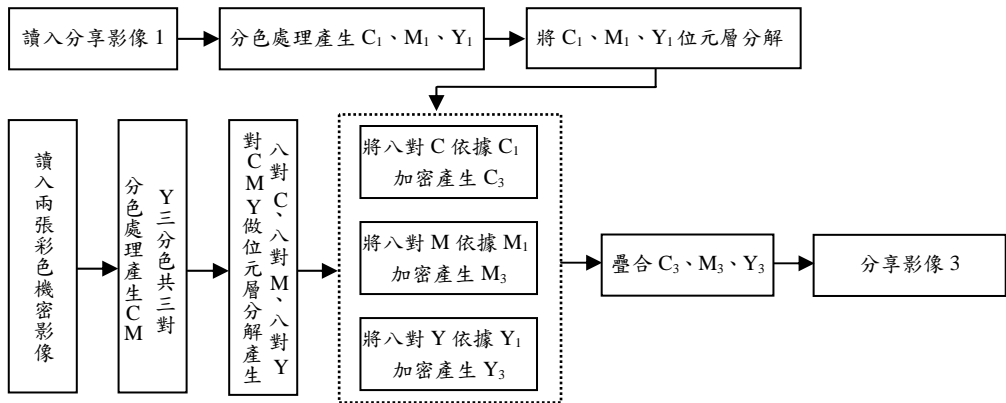
解密時，如流程圖 8(c)，將分享影像 1、分享影像 2 分別分色處理產生 CMY 三

分色共三對，對 CMY 三分色做位元層分解共二十四對，分別對每分色 (S_{1C}^b , S_{2C}^b)、(S_{1M}^b , S_{2M}^b) 及 (S_{1Y}^b , S_{2Y}^b)，依公式(2)解回 $n \times m$ 之八張位元層圖共 24 張，疊合 C 分色八張位元層圖可得 C_1 ，疊合 M 分色八張位元層圖可得 M_1 ，疊合 Y 分色八張位元層圖可得 Y_1 ，疊合 C_1 、 M_1 、 Y_1 可得還原影像 1；令 CMY 三分色之 S_{1C}^b 、 S_{1M}^b 及 S_{1Y}^b 旋轉 90 度與 S_{2C}^b 、 S_{2M}^b 、 S_{2Y}^b ，依公式(2)解回 $n \times m$ 之八張位元層圖，疊合 C 分色八張位元層圖可得 C_2 ，疊合 M 分色八張位元層圖可得 M_2 ，疊合 Y 分色八張位元層圖可得 Y_2 ，疊合 C_2 、 M_2 、 Y_2 可得還原影像 2；若要還原第二層 B2 與第一層 A 的機密影像，如流程圖 8(c) 分享影像 1 和分享影像 3 做分色處理產生 CMY 三分色共三對，對 CMY 三分色做位元層分解共二十四對，分別對每分色之 (S_{1C}^b , S_{3C}^b)、(S_{1M}^b , S_{3M}^b) 及時 (S_{1Y}^b , S_{3Y}^b)，依公式(2)解回 $n \times m$ 之八張位元層圖，疊合 C 分色八張位元層圖即可得 C_3 ，疊合 M 分色八張位元層圖即可得 M_3 ，疊合 Y 分色八張位元層圖即可得 Y_3 ，疊合 C_3 、 M_3 、 Y_3 可得分還原影像 3；每分色之 S_{1C}^b 、 S_{1M}^b 及 S_{1Y}^b 旋轉九十度和每分色之 S_{3C}^b 、 S_{3M}^b 及 S_{3Y}^b ，依公式(2)解回 $n \times m$ 之八張位元層圖，疊合 C 分色八張位元層圖即可得 C_4 ，疊合 M 分色八張位元層圖即可得 M_4 ，疊合 Y 分色八張位元層圖即可得 Y_4 ，疊合 C_4 、 M_4 、 Y_4 可得分還原影像 4。

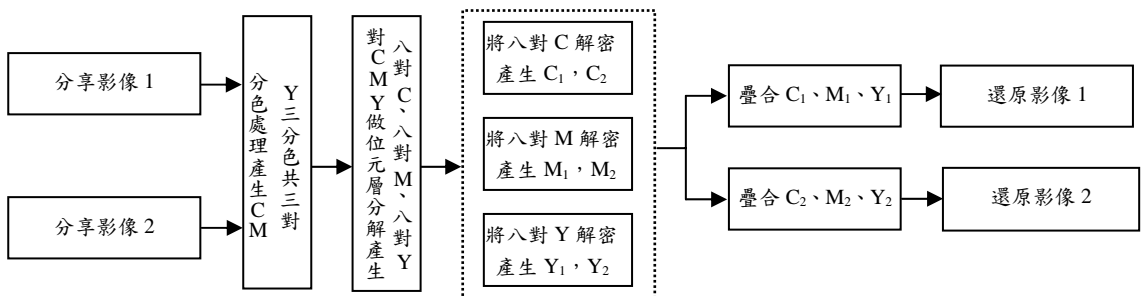
第二層與第三層解密規則和第一層與第二層的解密規則圖 8(c) 相同，根據圖 8(c) 之流程可得還原影像 5 及還原影像 6。



(a) 彩色階層式位元層加密流程圖 I



(b) 彩色階層式位元層加密流程圖 II











(c) 彩色階層式位元層解密流程圖

圖 8. 彩色階層式位元層加密/解密流程圖

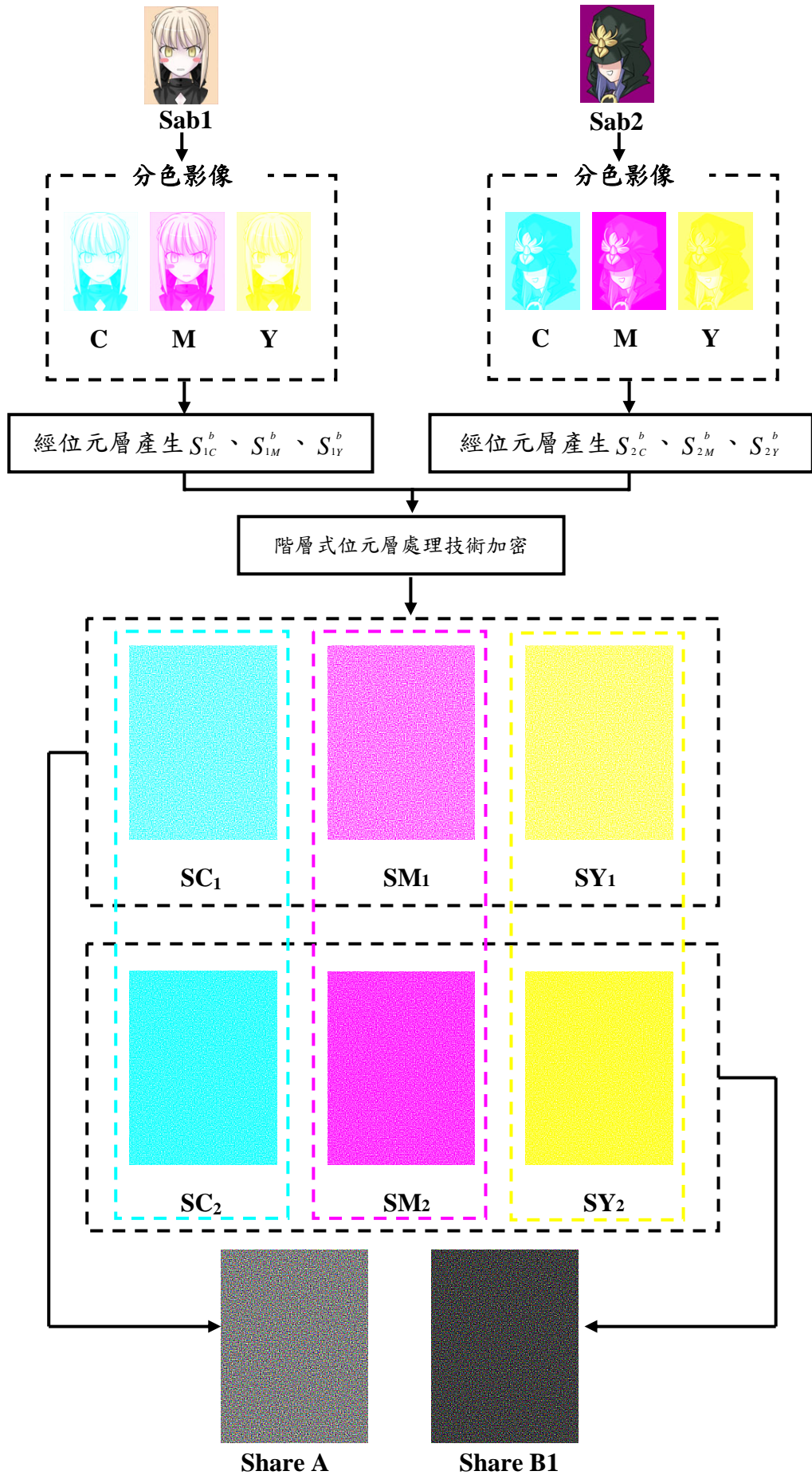
4. 實驗步驟

本文提出階層式位元層秘密分享交互建構機制於彩色視覺密碼之應用，首先對 Sab1 和 Sab2 個別分色成 3 張分色影像 CMY，對 CMY 各分色做位元層處理產生 S_{1C}^b 、 S_{1M}^b 、 S_{1Y}^b 及 S_{2C}^b 、 S_{2M}^b 、 S_{2Y}^b ($b=1, 2, \dots, 8$)，每分色分解為各八張 $n \times m$ 位元層圖，每分色八對共二十四對，再將每分色八對位元層圖分別加密，利用階層式多重秘密分享機制，產生 $2n \times 2m$ 的分享影像 SC₁、SM₁、SY₁ 及 SC₂、SM₂、SY₂，疊合 SC₁、SM₁、SY₁ 後即為分享影像 Share A，疊合 SC₂、SM₂、SY₂ 即為分享影像 ShareB1 如圖 9(a)，若欲增加第二層成員與第一層之間之機密，一樣將機密圖轉換成和 Sab1 及 Sab2 相同大小 $n \times m$ 像素的機密影像 Sab3 及 Sab4 (Sab3 與 Sab4 為第一層 A 與第二層 B2 之間的機密影像)，依據 ShareA、Sab3 和 Sab4 經階層式位元層處理技術產生 Share B2，如圖 9(b) 而 ShareA、ShareB1 和 ShareB2 是由表 2(a) 方式所產生。假設第五個及第六個機密影像 Sab5 及 Sab6，為第三層 C1 與第二層 B1 之間的機密影像，欲產生分享影像 Share C1，根據 Share B1 和 Sab5 與 Sab6，經階層式位元層處理技術，即可產生 Share C1，如圖 8(b)，Share B1 並不須重新計算。

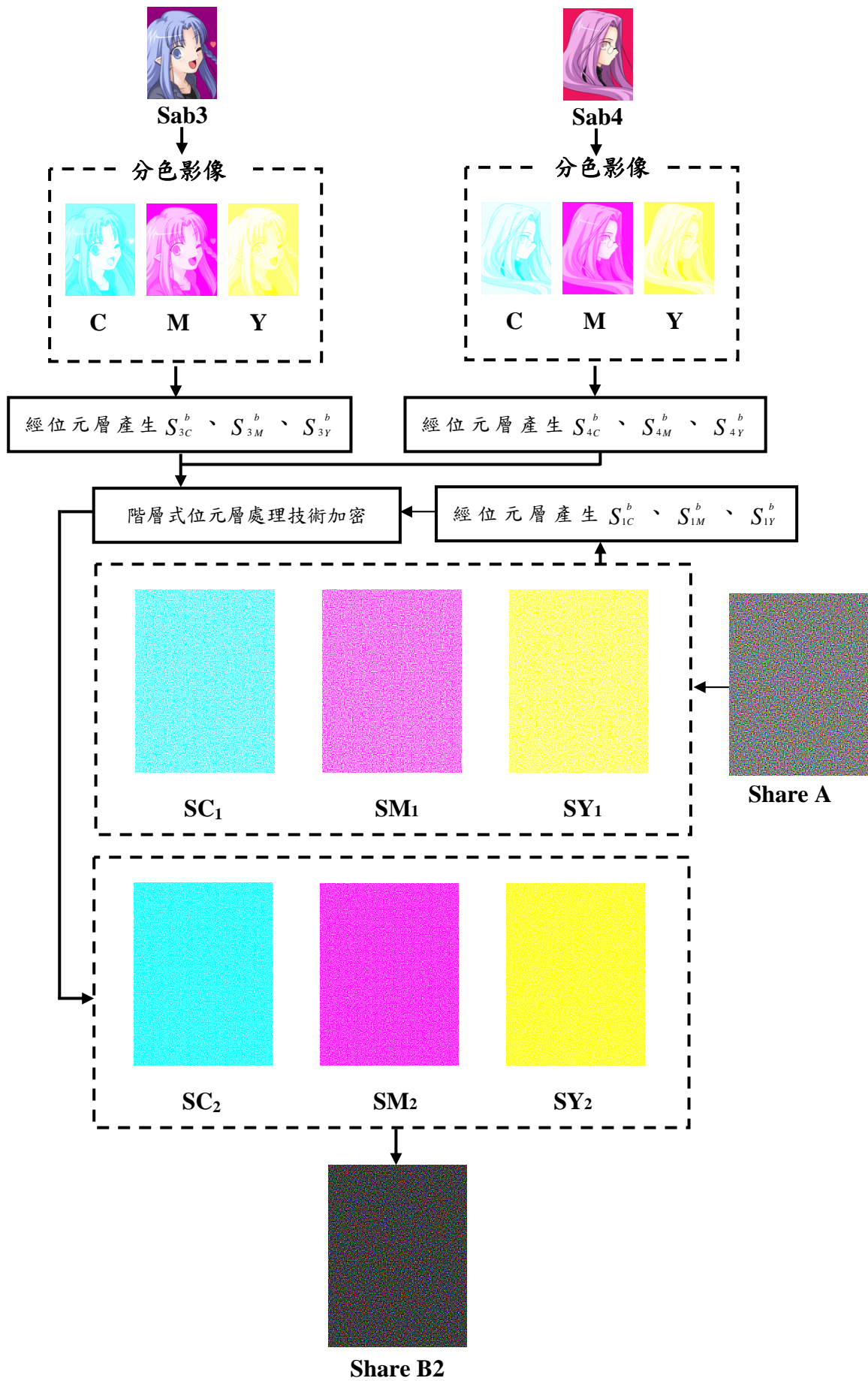
舉例來說，如果分色 C 第一個位元層機密影像 1 的第 i 個像素為青色，第一個分色位元層機密影像 2 相同的位置第 i 個像素為白色，由表 2(a) 共有四種可能性，以隨機選擇的方式選取一種，如果 Share A 分色 C 第一個位元層的 i 個區塊為 ，而

Share B1 分色 C 第一個位元層的第 i 個區塊如果為 ，階層式位元層解密技術可還原分色 C 第一個位元層機密影像 1 第 i 個像素為青色；而 Share A 分色 C 第一個位元層的第 i 個區塊順時針旋轉 90 度，區塊變為 ，再與 Share B1 分色 C 第一個位元層的第 i 個區塊  經階層式位元層解密技術可還原分色 C 第一個位元層機密影像 2 第 i 個像素白色；若欲增加第二層的成員，假設第一個分色位元層機密影像 3 的第 i 個像素為白色及第一個分色位元層機密影像 4 的第 i 個像素為白色，根據 Share A 分色 C 第一個位元層區塊為 ，由表 2(a) 可得 Share B2 分色 C 第一個位元層的第 i 個區塊為 ，經階層式位元層解密技術可還原分色 C 第一個位元層機密影像 3 的第 i 個像素為白色；同理旋轉 90 度後的 Share A 分色 C 第一個位元層第 i 個區塊  與 Share B2 分色 C 第一個位元層的第 i 個區塊 ，經階層式位元層解密技術可還原分色 C 第一個位元層機密影像 4 為白色。

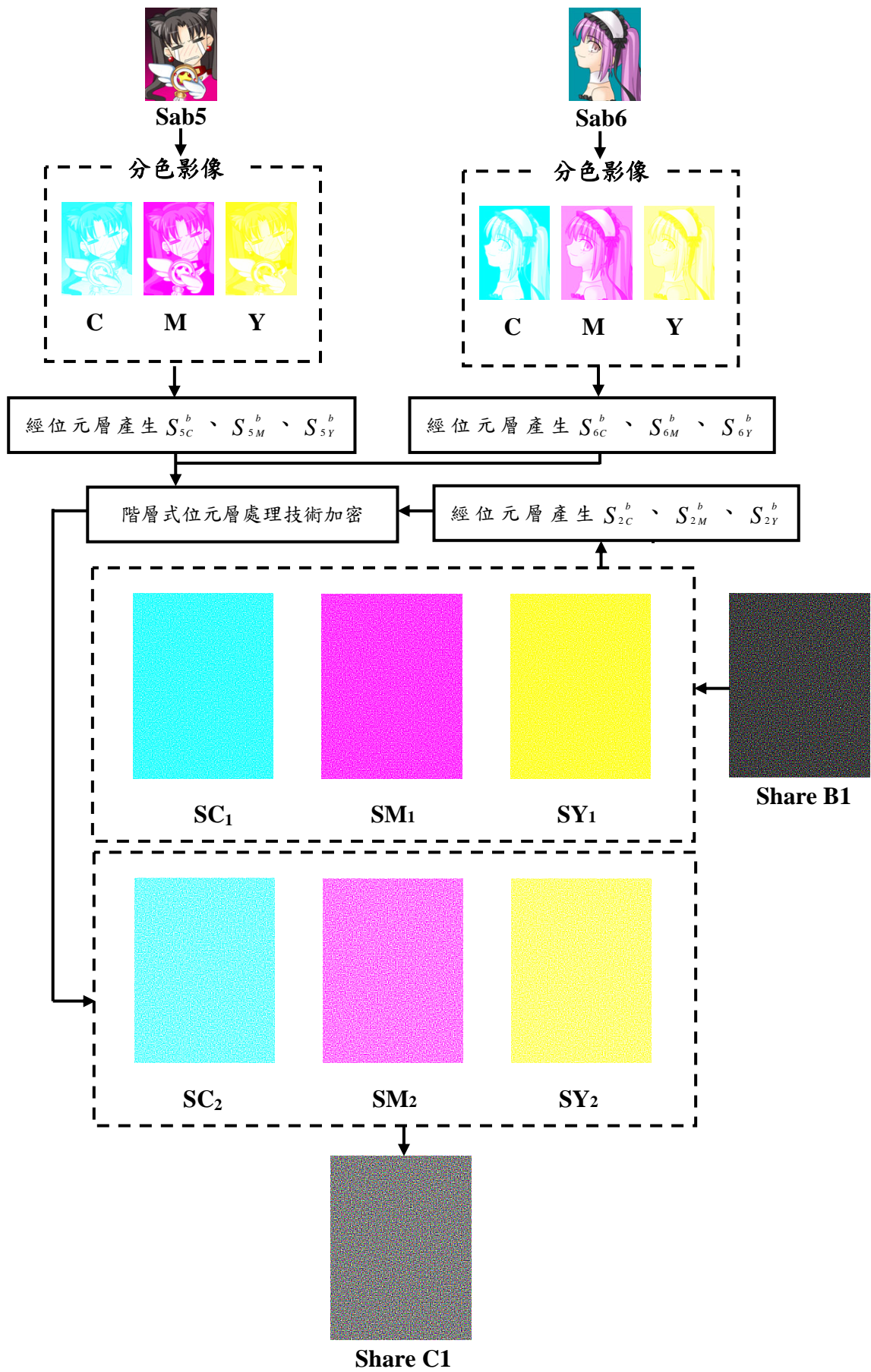
每一個機密影像的像素代表每一個 2×2 的區塊，每一個 2×2 區塊中，青分色機密影像中的白色由二個青色像素和二個白色像素所構成，青色由三個青色像素和一個白色像素所構成；洋紅分色機密影像中的白色由二個洋紅色像素和二個白色像素所構成，洋紅色由三個洋紅色像素和一個白色像素所構成；黃色位元層機密影像中的白色由二個黃色像素和二個白色像素所構成，黃色由三個黃色像素和一個白色像素所構成。



(a)機密影像 Sab1、Sab2 加密模型(Sab1 與 Sab2 為第一層 A 與第二層 B1 之間的機密影像)



(b) 機密影像 Sab3、Sab4 加密模型 (Sab3 與 Sab4 為第一層 A 與第二層 B2 之間的機密影像)



(c)機密影像 Sab5、Sab6 加密模型(Sab5 與 Sab6 為第二層 B₁與第三層 C₁之間的機密影像)

圖 9. 階層式位元層加密流程圖

5. 實驗結果與應用

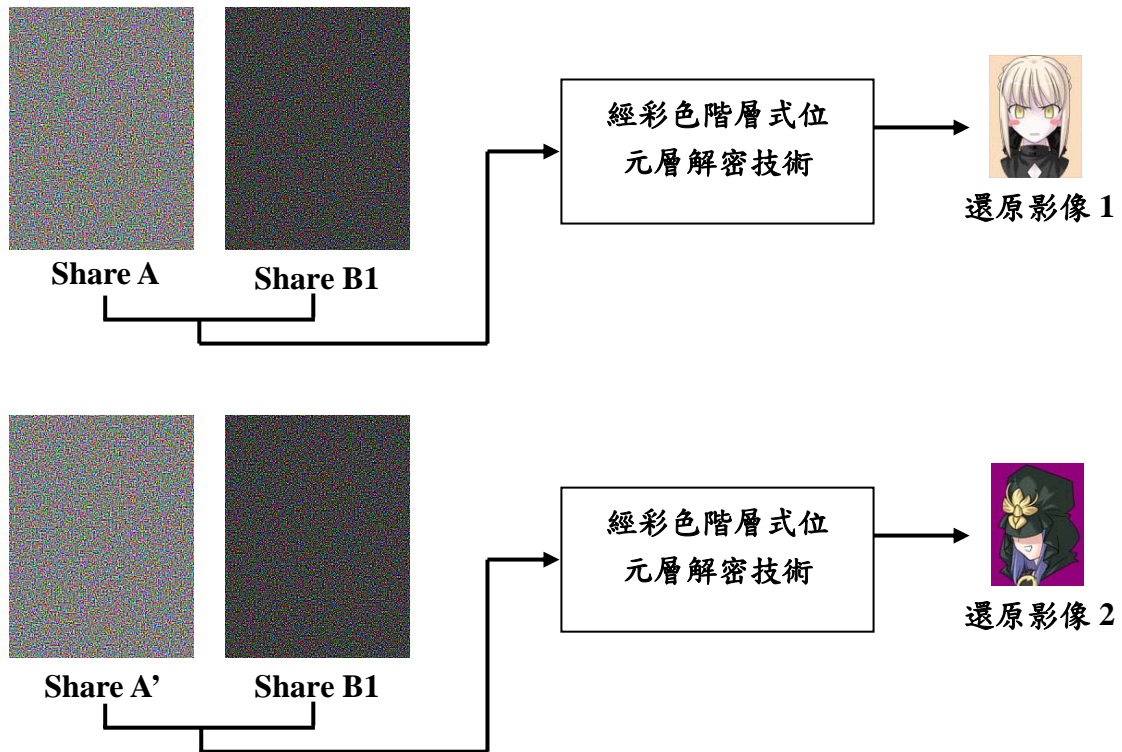
本實驗中以六張彩色圖樣做為機密影像，分享影像產生透過彩色階層式秘密分享交互建構機制如表 2 表式，欲解出 A 層與第二層 B1 之機密圖，將 ShareA 與 ShareB1 經彩色階層式位元層解密技術可得「還原影像 1」，將 ShareA 旋轉 90 度後為 ShareA'，ShareA' 及 ShareB1 經彩色階層式位元層解密技術可得為「還原影像 2」如圖 10(a)。

欲解 A 層與第二層 B2 之機密圖，同理將 ShareA 與 ShareB2 經彩色階層式位元層解密技術，可得機密圖「還原影像 3」，ShareA' 與 ShareB2 經彩色階層式位元層解密技術可得為機密圖「還原影像 4」如圖 10(b)。假設 B1 為第二層管理者，其所屬成員為第三層之 C1，欲解出之間的機密圖，需將 ShareB1 與 ShareC1 經彩色階層式位元層解密技術可得還原「還原影像 5」，ShareB1 旋轉 90 度後為 ShareB1'，

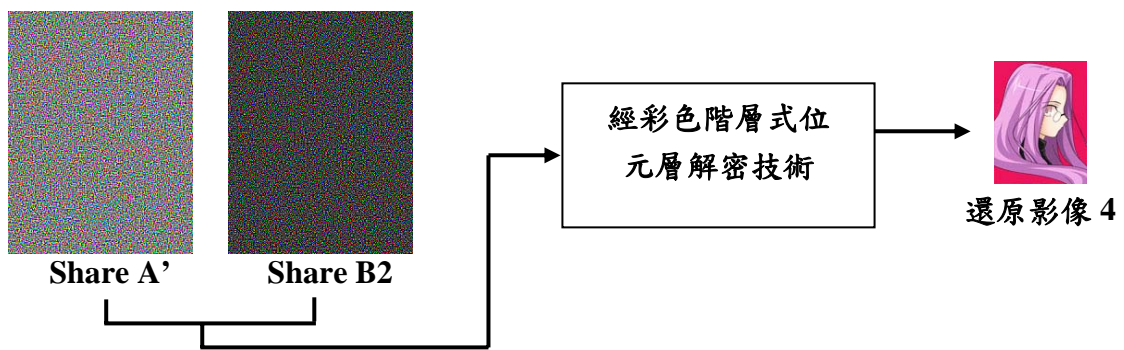
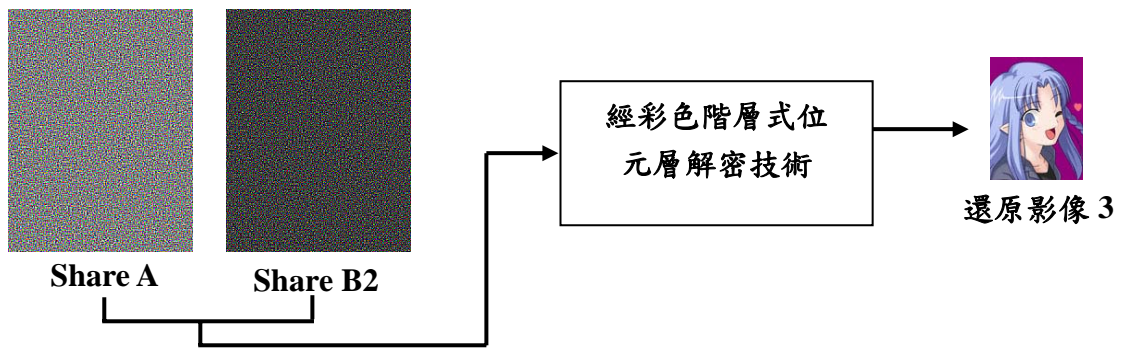
ShareB1' 與 ShareC1 經彩色階層式位元層解密技術可得還原「還原影像 6」如圖 10(c)。

此階層式架構如圖 5 所示，第一層 (Level 1) 為金鑰管理者，A 只須持有一把金鑰，即可管理第二層 (Level 2) 每個成員 B1、B2、B3；而 Level 2 每個成員 B1、B2、B3 也可分別管理第三層 (Level 3) 中的成員，B1 可管理 C1、C2；B2 可管理 C3、C4；B3 可管理 C5、C6，且 Bi 不須改變原始的分享影像，透過表 3(b) 方式產生分享影像 Ci，並可不斷的擴增成員與階層。在 Level 1 中，A 可透過機密影像推导出 Level 2 的分享影像與共享 Level 2 與 Level 3 成員之機密。

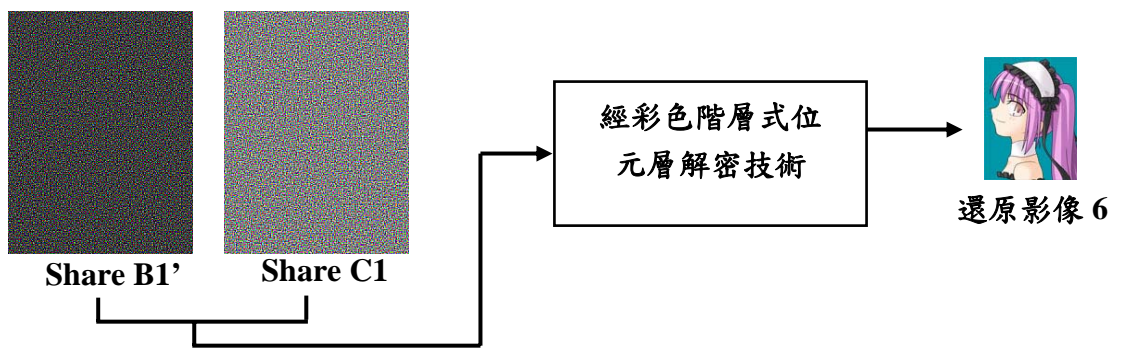
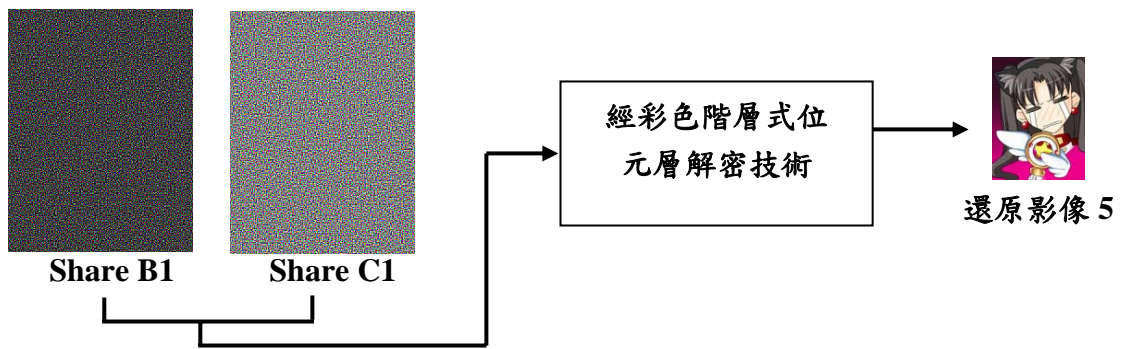
管理者與每個成員只能隱藏 2 個機密影像，欲增加更多的機密影像，透過此研究模型，根據管理者的分享影像和欲增加的機密影像，再利用階層式秘密分享交互建構機制，產生新的分享影像，即可增加更多的機密影像。



(a) 第一層 A 之 ShareA 與 ShareA' 和第二層 B1 之 ShareB1 的解密流程



(b)第一層 A 之 ShareA 與 ShareA'和 第二層 B2 之 ShareB2 的解密流程



(c)第二層 B1 之 ShareB1 與 ShareB1'和 第三層 C1 之 ShareC 的解密流程

圖 10. 階層式位元層解密流程圖

6. 結論

本文提出位元層技術應用於彩色階層式多重視覺秘密分享機制，利用為元層分解/疊合取代半色調處理技術，每個成員仍可擁有兩種機密影像，防止圖片失真並能還原影像大小，此彩色階層式位元層技術具有以下幾個特性及優點：

- 解密後影像為原始大小。
- 可解決傳統視覺密碼技術失真問題。
- 利用位元層分解取代半色調處理技術。
- 每個成員皆可擁有兩種機密影像。
- 可應用於彩色影像。

參考文獻

- [1] 廖惠雯、林秀蓓(2007)，階層式多重視覺秘密分享機制於灰階影像之研究與應用，資訊科技國際期刊，1，pp. 56-66。
- [2] 廖惠雯、林秀蓓(2007)，階層式多重視覺秘密分享機制於彩色影像之研究與應用，雲林縣，2007/05/04，2007 資訊管理暨商務科技研討會，p.239-p.256。
- [3] Floyd, W. and Steinberg,L.,(1976), “An adaptive algorithm for spatial grayscale”, Proceedings of Society for Information Display, 17(2),pp75-77.
- [4] Lukac, R. and Plataniotis, K. N.,(2005), “ Bit-level based secret sharing for image encryption”, Pattern Recognition 38, 767 – 772.
- [5] Naor, M. and Shamir A. (1994), *Visual Cryptography, Advances in Cryptology : Eurpocrypt’94*, Springer-Verlag, Berlin, pp. 1-12.
- [6] Naor, M. and Shamir A. (1996), *Visual Cryptography II :Improving the Contrast via the Cover Base*, Cambridge workshop on Cryptographic Protocols.
- [7] R.C. Gonzalez, R.E. Woods, “Digital Image Processing 2/e”, *Prentice Hall*,2002.
- [8] Young – ChangHou , (2003) , *Visual Cryptography for color images*, *Pattern Recognition* 36, pp.1619-1629.