階層式多重視覺秘密分享機制於灰階影像之研究與應用

廖惠雯　　林秀蓓
嶺東科技大學資訊科技應用研究所
hwliao@mail.ltu.edu.tw　sendohpei@hotmail.com

摘　要

視覺密碼學最大的優點在於解密過程僅需將分享影像重疊，不需任何複雜的電腦計算，也無需任何的密碼學知識。本文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，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。若將 2n 個機密分解成 n+1 張分享影像，管理者可授權於 n 個成員，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，任何其他成員皆無法解讀出機密影像，必須和管理者所持的分享影像疊合，才可解讀出機密影像。此外，此建構機制適用於黑白視覺密碼中，亦適用於灰階影像之中，不因色調上的不同阻礙此建構機制。所以，此建構機制於灰階影像之應用，除了每個成員可擁有兩種機密影像外，原始分享影像並不需重新計算、成員數具有高度的擴充性，且不因成員數量龐大，造成金鑰(分享影像)管理的問題及不增加加密的複雜度。

關鍵字：視覺密碼學、階層式視覺機密分享機制、分享影像、機密影像、灰階影像

Abstract

The key advantage of visual cryptography is in the decryption process that is to decrypt the share image stacks, does not require complex computation nor any cryptographic knowledge is needed. Based on the interaction operation of share images of odd level, which has two black pixels and two while pixels, and share images of even level, which has three black pixels and one while pixel, this article establishes a hierarchical, multiple visual secret sharing scheme. And this article demonstrated the usage of rotating the share image to allow manager and members to hold two kinds of confidential messages.

When separating 2n secret images into n+1 share images, the manager can authorize them to n members, and more; furthermore, any member can not decrypt the secret images, but only manager can obtain the content of secret images by combining the original share images with member share image. This paper establishes the scheme of black-and-white visual cryptography, which extended gray-level. All kind of the hues can also be able to apply to the scheme, such as gray-level easily.

This scheme provides that features, such as each member can have two kind of secret images, this is no need to re-calculate them original share images, the number of members is highly expandable, even with large number of members, this system can be easily managed, and this scheme does not add complexity to the cryptography.

Keyword：Visual Cryptography, Hierarchical Visual Secret Sharing Scheme, Share Image, Secret Image, Gray-Level Image

1. 前言

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，但擁有者在解密的過程中，所需的運算、複雜度及有限的設備下也是一大問題，而視覺密碼(Visual Cryptography)便在此環境下產生。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。

視覺密碼學[1-2]最早在 1994 年由 Naor and 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，而是直接重疊所有分享影像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。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≦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，如圖 1。在分享影像小於 t 張時(1~t-1)，就無法取得機密訊息，這就是視覺密碼中典型的(t,n)t out of n Threshold Scheme 門檻機制。

Akl and Taylor 於 1983 年的論文中，首先提出一個密碼階層式存取控制的方法[3]，在一個由上而下的階層中，每一個節點代表一群使用者，若所有的使用者可分為$\{C_1,C_2,\cdots,C_n\}$等 n 個群組，這些使用者群組間存在著由上而下的隸屬關係。金鑰中心(Key Center，KC)負責金鑰之製作與分配，每一個機密群組 C_i 擁有一個由金鑰中心製作的金鑰 K_i，而且可以使用這個金鑰 K_i 去計算 K_i 所管轄之所有群組的秘密金鑰。另外，一個 K_i 或某幾個群組 K_i 絕無法推算出管轄它(或它們)的群組(即上司)的金鑰，如圖 2。但一旦群組數量龐大，則上位者貯存之金鑰數量由於過度龐大而有安全上與應用上之危機。

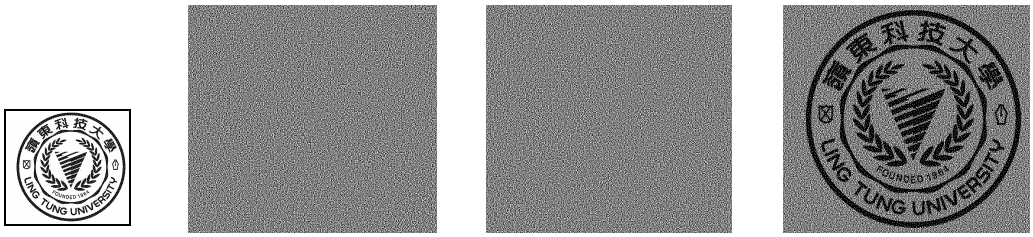
Harn & Lin 於 1990 年提出一個階層式存取控制的方法[4]是由下而上(Bottom-Up)的方式金鑰去推算每一個安全層級的秘密金鑰。當一個新的層級要加進原來的階層時，需要重新推算的金鑰較少；系統只需要重新計算在這個新層級上面每個層級的金鑰。

Floyd and Steinberg 於 1976 年提出誤差擴散法[5]，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內眼可察覺的程度，其結果如圖 3。

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，提出幾種灰階影像和彩色影像的視覺密碼作法[6]，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，對於先前有關黑白視覺密碼的研究(如 t out of n Threshold Scheme)亦可以套用在他的方法上，而應用於灰階及彩色影像的製作上。

Hsien-Chu Wu 等人於 2005 年提出改變傳統的方形分享影像，使用圓形有 360 度特色的分享技術[7]，機密訊息可隱藏在任一選擇的角度。兩張分享影像重疊後可得到機密資訊，再旋轉某一張分享影像 x 度後和另一分享影像重疊後，即可得到第二張分享影像。與傳統的視覺密碼比較，這技術有更多的彈性、可伸展性和安全性。

Chin-Chen Chang 等人於 2002 年提出保護智慧財產權的方法[8]，它的第一張分享影像是管理者指定特定的圖片，且不更改第一張分享影像的任何一個像素，另一張分享影像是由使用者任意產生，且還可承受模糊、失真壓縮(例：JPEG)、剪裁、縮小等攻擊，在不同的攻擊下，依然可得到機密影像。



原始影像 1　　Share A　　Share B　　還原影像 1

圖 1. (2,2)視覺密碼加密與解密

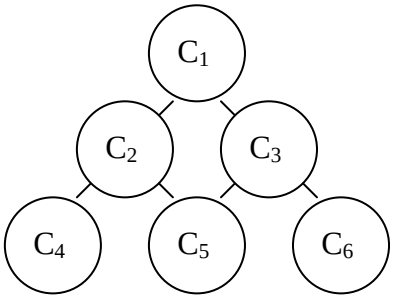
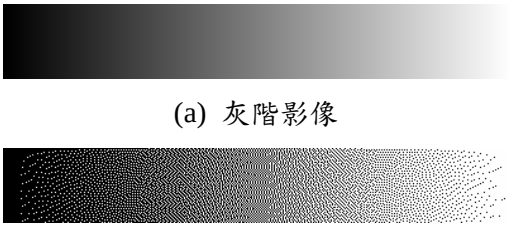


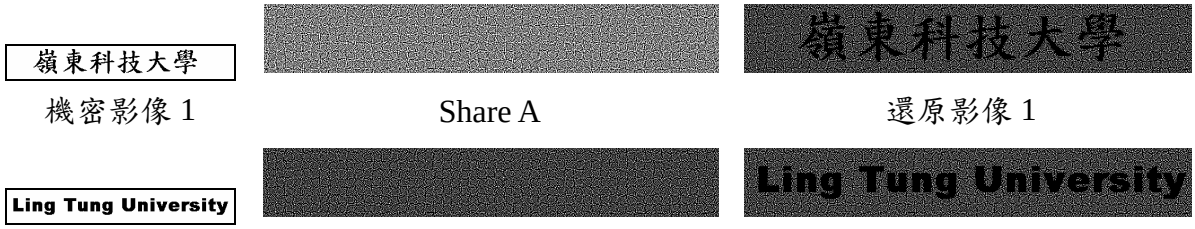
圖 2. 密碼階層式存取控制



(a) 灰階影像

(b) 半色調影像

圖 3. 灰階色調和半色調色階



機密影像 1　　Share A　　還原影像 1

機密影像 2　　Share B　　還原影像 2

圖 4. 新的視覺密碼加密與解密

陳玲慧等人於 2000 年提出一個新的視覺密碼技術[9]，解決傳統密碼方法須要計算繁複以及大量的資料量的缺點。基於(2,2)2 out of 2 的視覺密碼方法所建構出來的系統，利用三點與兩點黑點的變化，將分享影像(Share A)的每個區塊(Block)逆時鐘旋轉 90 度的方式，再與分享影像(Share B)重疊，得到第二張機密影像，它不但可保護原始機密影像，且儲存機密訊息的容量較其他方法加倍，如圖 4。

2. 研究方法

在 Naor and Shamir[1-2]的視覺密碼中，所提出的方法在每一次加密時，只能擁有一種機密影像，所以加密的資料量相當地少。使用陳玲慧等人所提出的新的視覺密碼技術[9]，便可增加隱藏機密資訊的容量，另外，所建構出來的方法也不需要大量的計算，且保有原始資料的安全性。

利用密碼學的方法來管制使用者對資料的讀取，一個比較基本的作法是先由系統和使用者之間執行一樣認證的協商程序(Authentication Protocols)，以確認使用者的身份並在協商的過程中決定出一把金鑰(Key)；如此一來，系統傳送給使用者的資料便可利用這把金鑰加密(Encryption)後再傳送；使用者收到封包之後，可以利用金鑰解密(Decryption)，得到原來的資訊。至於其他的人員，因為沒有金

鑰或是其他足夠訊息來還原這些加密的資訊，所以僅能竊聽到傳送的密文，而無法得到真正的訊息。

傳統上金鑰管理者必須擁有多把的金鑰，造成金鑰管理上的問題。所以，透過「金鑰推導」(Key Derivation)的方式，能達到多層級資料安全的基本要求。每個安全層級都配置一把加、解密的金鑰，用來對每個層級所能讀取的資料做加、解密；因此必須擁有解密金鑰的使用者才能在收到密文後，將其還原成真正的機密訊息。層級之間如果有高低的相對關係，那麼層級比較高的使用者可以利用他的金鑰推導出層級比較低的使用者之金鑰。因為同樣的一份資訊不需要針對每個層級的金鑰做加密；高層級的使用者如果要讀取低層級的資料，僅需先推導出該份資料的解密金鑰即可得到還原的資訊，而系統則可以免去對同一份資料重複儲存的空間效率問題；同時，高層級的使用者也不需擁有太多的金鑰，造成管理上的不便。

半色調技術有很多種方法，其中，誤差擴散法(Error Diffusion)是 Floyd and Steinberg 在 1976 年所提出[5]，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，擴散的方式是將所計算出的誤差，以誤差的 1/16、3/16、5/16、7/16 加到緊鄰的點，而處理的順序由左而右、由上而下。使得鄰近的像素值差異可以盡量低於肉眼可察覺的程度，圖 3 即為灰階影像轉為黑白影像及半色調影像之差異。依此方式將整張灰階影像轉換後可得到二元影像，但是又不失去灰階影像的明暗效果，比直接轉換成黑白值的方式改善很多。

本文先將灰階影像經過半色調處理，再利用金鑰推導的觀念及秘密分享交互建構機制，建立階層式多重視覺秘密分享機制，其階層關係如圖 5 及交互建構機制如表 1。

假設 A 是第一層，B_i 是第二層(即 A 附屬之成員)，由機密影像 S1 及機密影像 S2 產生分享影像 A(Share A)及分享影像 B_1(Share B_1)，可

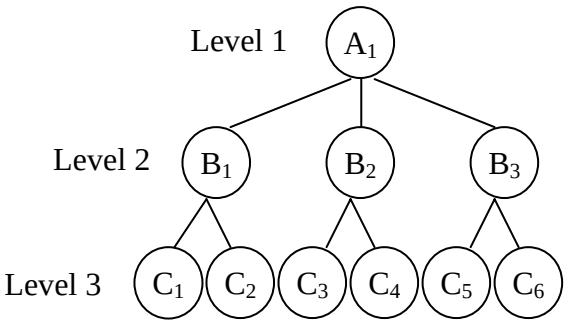


圖 5. 階層式金鑰管理

根據已產生的 Share A 和機密影像 S3 及機密影像 S4 產生分享影像 B_2(Share B_2)，如此，A 不用改變 ShareA 即可不斷的增加 Share B_3、Share B_4…等。每個成員僅須保存自己的分享影像，即可與 Share A 或旋轉 90 度後的 ShareA(即 Share A')疊合，得到 2 種機密影像，而管理者 A 也僅須保存自己的 Share A 及旋轉後之 Share A'，皆可與所有成員擁有各別的機密訊息。C_i 是第三層，由 B_i 與 C_i 之間的兩種機密影像及 Share B_i 產生分享影像 C_i (Share C_i)，Share B_i 為原始分享影像，並不須重新計算，如同 A 產生 Share B_i 相同，B_i 可不斷增加 Share C_i，故可持續地擴增成員組織。

此種方式，每個成員僅須保存自己的分享影像，若須兩種機密，管理者僅須將自己的分享影像旋轉 90 度，即可與使用者多一個機密，且每增加一個成員，其機密建構模型中區塊組合型僅 16 種(如表 1)，並不須要擴增其模型。再由 2 黑 2 白區塊及 3 黑 1 白區塊的交互變換，可設計出階層式分享影像，例如：第一層分享影像是 2 黑 2 白區塊所組成，第二層分享影像是 3 黑 1 白區塊所組成，則第三層分享影像回到 2 黑 2 白區塊所組成，第四層分享影像回到 3 黑 1 白區塊所組成。即奇數層分享影像由 2 黑 2 白像素所組成，偶數層分享影像由 3 黑 1 白像素所組成(如表 1)。

第一層 A 可與第二層 B_i 共享機密，若欲與第三層 C_i 共享機密，僅須根據第二層分享影像(第二層由第一層授權，所以 A 可推出第二層 B_i 的分享影像)即可與第三層 C_i 共享機密。

表 1：階層式秘密分享交互建構機制

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

機密圖 1	W	W	B	B	W	W	B	B	W	W	B	B	W	W	B	B
機密圖 2	W	B	W	B	W	B	W	B	W	B	W	B	W	B	W	B
Share A																
Share B																
A+B																
Share A’																
A’+B																

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

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

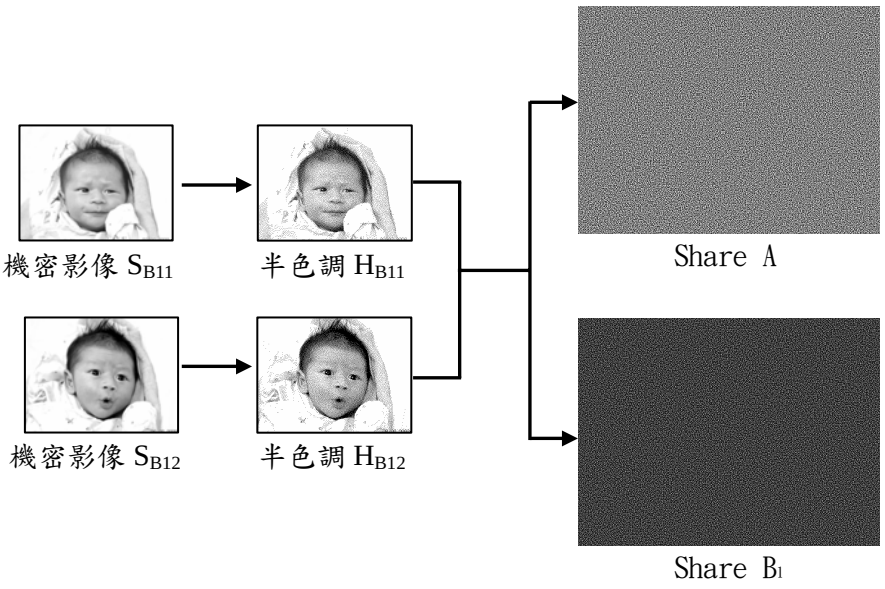
本文所提出階層式多重視覺秘密分享機制，除了可不斷增加成員數，亦可不斷增加階層數；而階層較高的管理者可與所屬階層較低的成員共享機密，跨階層時，僅須推導出低階層之分享影像，即可與跨階層成員共享機密；再利用旋轉關係，管理者可與每個成員分別擁有兩種機密。

3. 實驗步驟

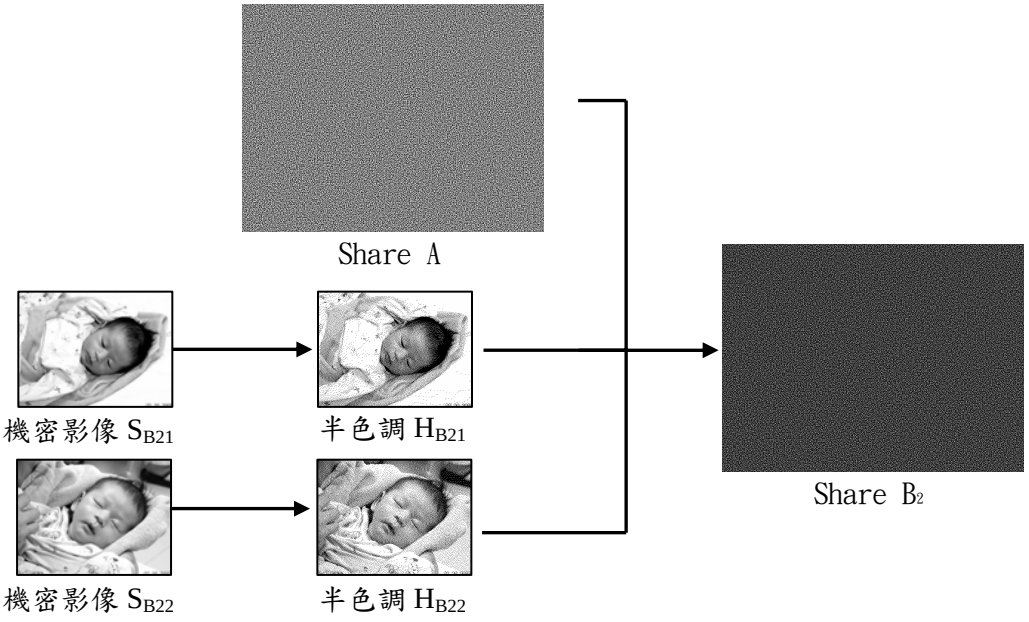
本文提出階層式秘密分享交互建構機制於灰階影像之應用，先利用半色調處理技術，分別將二個機密圖，轉換成相同大小 n×m 像素的機密影像 S_{B11} 及 S_{B12} (S_{B11} 與 S_{B12} 為第一層 A 與第二層 B_1 之間的機密影像)，再將機密影像經半色調處理為 H_{B11} 及 H_{B12}，根據 H_{B11} 和 H_{B12} 產生兩個分享影像 Share A 和 Share B_1 如圖 6(a)，若欲增加第二層成員與第一層之間之機密，一樣將機密圖轉換成和 S_{B11} 及 S_{B12} 相同大小 n×m 像素的機密影像 S_{B21} 及 S_{B22} (S_{B21} 與 S_{B22} 為第一層 A 與第二層 B_2 之間的機密影像)，經半色調處理後為半色調機密影像 H_{B21} 及 H_{B22}，再依據 Share A、H_{B21} 和 H_{B22} 產生 Share B_2，如圖 6(b)，而 Share A、Share B_1 和 Share B_2 是由表 1(a)所產生，舉例來說，如果第一個半色調機密影像的第 i 個像素為黑色，第二個半色調機密影像相同的位置第 i 個像素為白色，共有四種可能性，再以隨機選擇的方式選取一種，如果 Share A 的 i 個區塊為  ，而 Share B_1 的第 i 個區塊如果為  ，Share A 和 Share B_1 重疊後得到  ，而 Share A 經過順時針旋轉 90 度，區塊變為，再與 Share B_1 重疊後得到  ；若欲增加第二層的成員，假設第三個半色調機密影像 H_{B21} 為白色及第四個半色調機密影像 H_{B22} 為白色，根據 Share A 的機密影像，判斷出 Share B_2 為，如表 1(a)，並不須重新產生 Share A、Share B_2 和原始的 Share A(即 Share A’)重疊後，得到第三個半色調機密影像 H_{B22}  ，Share B_2 再與 Share A’重疊後，即可得到第四個半色調機密影像 H_{B22}  。

當進行解密時，將 Share A 和 Share B_1 重疊後可得到第一個半色調機密影像 H_{B11}，再將 Share A 的每個 2×2 區塊旋轉 90 度後為 Share A’和 Share B_1 重疊，可產生第二個半色調機密影像 H_{B12}；Share A 和 Share B_2 重疊後可得到第三個半色調機密影像 H_{B21}，再以 Share A’和 Share B_2 重疊後可得到第四個半色調機密影像 H_{B22}。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，半色調機密影像中的白色由二個黑色像素和二個白色像素所構成，而半色調機密影像中的黑色由三個黑色像素和一個白色像素所構成。而疊合成的 2×2 區塊中，三個黑色像素和一個白色像素代表為白色，四個皆為黑色像素的區塊代表為黑色。

假設第五個及第六個半色調機密影像 H_{C11} 及 H_{C12} 為第三層 C_1 與第二層 B_1 之間的半色調機密影像，欲產生分享影像 C_1 (ShareC_1)，根據 Share B_1 和 H_{C11} 與 H_{C12}，利用表 1(b)之建構模型即可產生 Share C_1，如圖 7，Share B_1 並不須重新計算。



(a)機密影像 S_{B11}、S_{B12} 加密模型(S_{B11} 與 S_{B12} 為第一層 A 與第二層 B_1 之間的機密影像)



(b)機密影像 S_{B21}、S_{B22} 加密模型(S_{B11} 與 S_{B22} 為第一層 A 與第二層 B_1 之間的機密影像)

圖 6. 第一層 A 與第二層 B_1 及 B_2 之加密流程

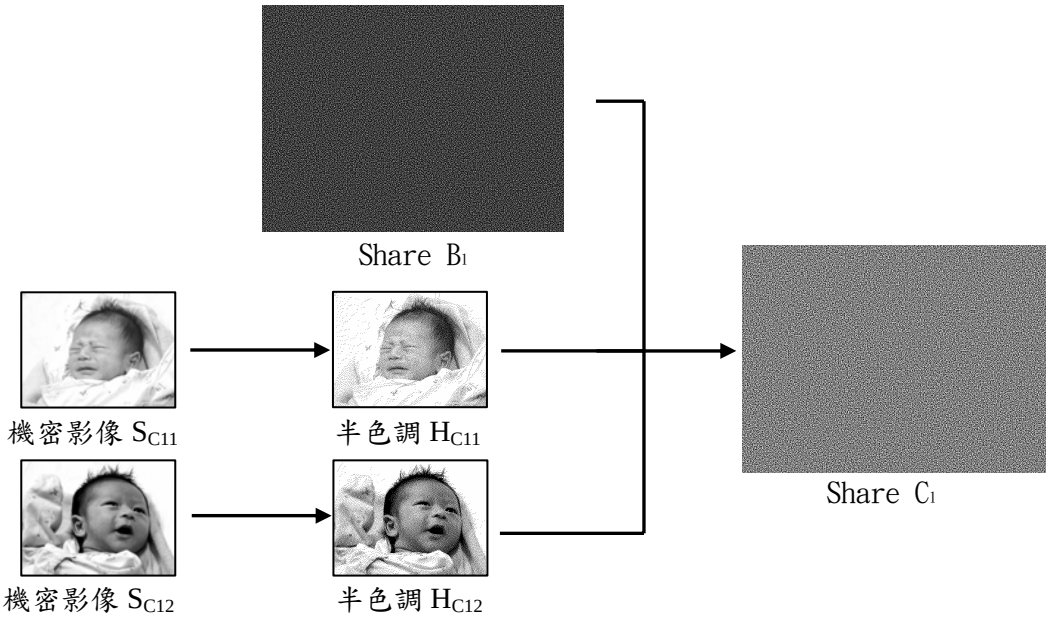


圖 7. 第二層 B_1 及第三層 C_1 之加密流程(S_{C11} 與 S_{C12} 為第二層 B_1 與第三層 C_1 之間的機密影像)

4. 實驗結果與應用

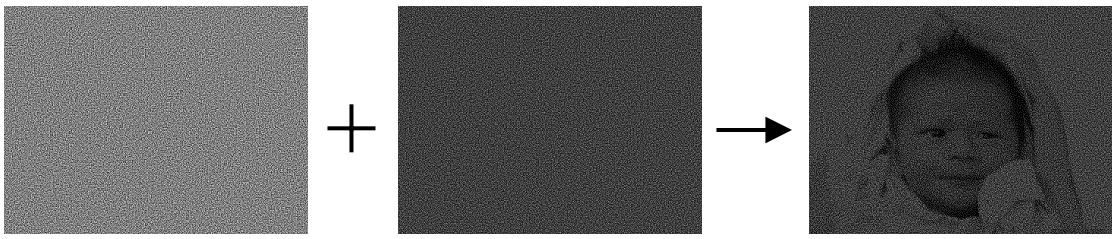
本實驗中以六張灰階圖樣做為機密影像，影像大小皆為 400×300 的像素，每個影像皆有 2 張分享影像，分享影像產生透過階層式祕密分享交互建構機制(如表 1)，分享影像疊合結果如圖 8 及 9。A 為第一層的管理者，B_1 及 B_2 為第 2 層成員，A 及 B_1 之機密影像為 S_{B11} 和 S_{B12}，Share A 與 Share B_1 疊合為「還原影像 1」，Share A 旋轉 90 度後為 Share A'，Share A' 及 Share B_1 疊合為「還原影像 2」，如圖 8(a)所示。管理者 A 與第二層 B_2 之機密影像為 S_{B21} 和 S_{B22}，同理 Share A(Share A 並不須重新計算)與 Share B_2 可得機密「還原影像 3」，Share A' 與 ShareB_2 可得機密「還原影像 4」，如圖 8(b)所示。假設 B_1 為第二層管理者，其所屬成員為第三層之 C_1，B_1 與 C_1 之機密影像為 S_{C11} 及 S_{C12}，Share B_1(Share B_1 不須重新計算)與 Share C_1 疊合還原「機密影像 5」，Share B_1 旋轉 90 度後為 Share B_1'，Share B_1'與 Share C_1 疊合還原「機密影像 6」，如圖 9 所示。

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 B_1、B_2、B_3；而 Level 2 每個成員 B_1、B_2、B_3 也可分別管理第三層(Level 3)中的成員，B_1 可管理 C_1、C_2；B_2 可管理 C_3、C_4；B_3 可管理 C_5、C_6，且 B_i 不須改變原始的分享影像，透過表 1(b)產生分享影像 C_i，並可不斷的擴增成員與階層。在 Level 1 中，A 可透過機密影像推導出 Level 2 的分享影像與共享 Level 2 與 Level 3 成員之機密。

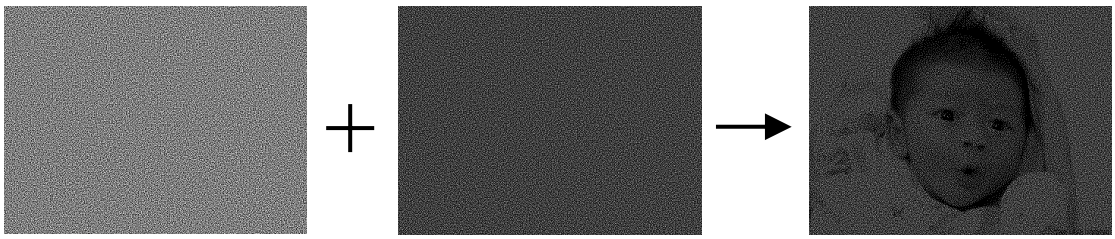
管理者與每個成員只能隱藏 2 個機密影像，欲增加更多的機密影像，透過此研究模型，根據管理者的分享影像和欲增加的機密影像，再利用階層式秘密分享交互建構機制，產生新的分享影像，即可增加更多的機密影像。此機制可不斷的增加機密影像，不管增加幾張機密影像，每增加二張機密影像，建構模型區塊組合僅 16 種(如表 1)，加密時不須擴充區塊組合，所以建構模型不需擴展。在此研究模型中，每一個分享影像相當於金鑰(由 Key Center 製作後分配)，上位者有權知道受其管轄之每個分享影像之金鑰，如圖 5 的階層關係，若第一層為 A(管理者)，第二層為 B_1(管理者)及 B_2，第三層為 C_1，其每成員間握有金鑰及機密如表 2 所示。

表 2：金鑰與機密影像的配置

階層成員	分享影像(金鑰)	機密影像
第一層 A	Share A、Share A’	S_{B11},S_{B12} ; S_{B21},S_{B22} ; S_{C11},S_{C12}(須與 Share C 及 Share C’疊合)
第二層 B_1	Share B_1、Share B’	S_{B11},S_{B12}(須與 Share A 及 Share A’疊合) ; S_{C11}、S_{C12}
第二層 B_2	Share B_2	S_{B21},S_{B22}(須與 Share A 及 Share A’疊合)
第三層 C_1	Share C_1	S_{C11},S_{C12}(須與 Share B_1 及 Share B_1 疊合)

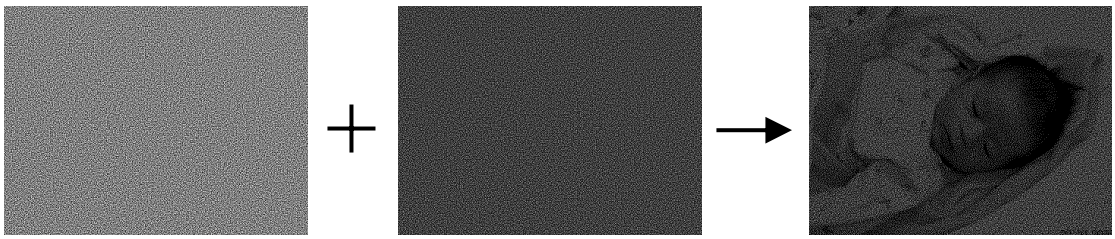


Share A　　Share B_1　　還原影像 1

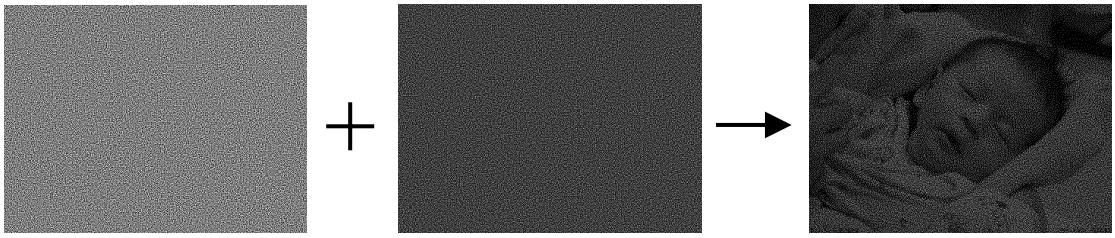


Share A’　　Share B_1　　還原影像 2

(a).第一層 A 之 Share A 與 ShareA’和第二層 B_1 之 Share B_1 的解密流程



Share A　　Share B_2　　還原影像 3



Share A’　　Share B_2　　還原影像 4

(b). 第一層 A 之 Share A 與 ShareA’和第二層 B_2 之 Share B_2 的解密流程

圖 8. 第一層 A 與第二層 B_1 及 B_2 之解密流程

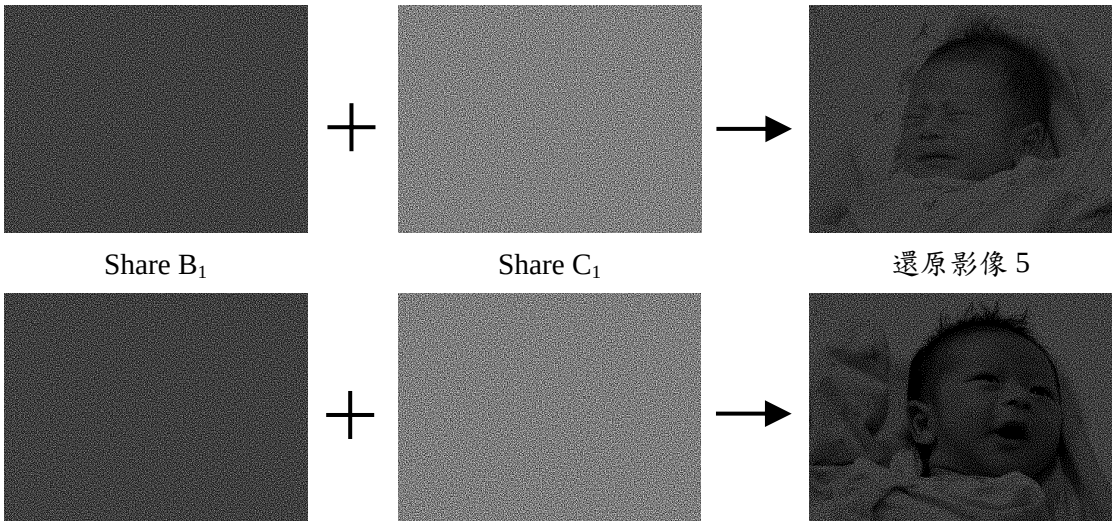


圖 9. 第二層 B_1 之 Share B_1 與 Share B_1'和第三層 C_1 之 Share C_1 的解密流程

5. 結論

資訊的爆破及網際網路的普及化，使得資訊的傳遞愈來愈快速與便利，然而卻衍生了資訊安全的問題，而視覺密碼的技術，無庸至疑的提供了影像在網路上傳送的另一種安全作法，它的優點在於解密時無需大量的運算，可直接用人類視覺特性來取得機密資訊。

分享影像相當於金鑰，而每一個成員僅須管理自己的分享影像，管理者亦僅須保存自己的分享影像及由自己分享影像順時針旋轉 90 度後的分享影像，即可和所屬群組分享機密影像。

本文提出一種階層式多重視覺祕密分享機制，可將其方式應用於金鑰(分享影像)製作及管理上，每增加一個分享影像，即可增加 2 張的機密影像，且不需要擴充機密模型和管理者也不需要更改原持有的分享影像，解決了金鑰數量過度龐大而有安全上與管理上的危機。在安全性方面，疊合機密影像時，必須和管理者之分享影像進行疊合，才可得知機密影像，延續了無須大量運算的優點，而疊合任何其他分享影像，均無法得知機密影像。

總而言之，此建構機制具有以下幾個特性及優點：

- 每個成員可擁有兩種機密影像
- 原始分享影像並不需重新計算
- 成員數(分享影像數)具有高度的擴充性
- 不因成員數量龐大，造成金鑰(分享影像)管理的問題
- 此機制之建構模型區塊組合僅 16 種，加密時不須擴充區塊組合，故不增加加密的複雜度
- 半色調處理技術，改善灰階影像直接轉換的視覺效果。

參考文獻

[1] Naor, M. and Shamir A. (1994), ***Visual Cryptography, Advances in Cryptology : Eurpocrypt'94,*** Springer-Verlag, Berlin, pp. 1-12.

[2] Naor, M. and Shamir A. (1996), ***Visual Cryptography II：Improving the Contrast via the Cover Base***, Cambrdge workshop on Cryptographic Protocols. ftp://theory.lcs.mit.edu/pub/tcrypto/96-07.ps

[3] Akl, S.G. and Taylor (1983), P.D.,Cryptography solution to a

problem of access control in a hierarchy, ***ACM Transactions on Computer System***, 1(3), pp. 239-248.

[4] L. Harn and H.Y. Lin. (1990),A cryptographic key generation scheme for multilevel data security, ***Computers & Security 9***,pp.539-546.

[5] R.W. Floyd and L. Steinberg, “An adaptive algorithm for spatial grayscale,” ***Proceedings of the Society for Information Display***, Vol. 17, No. 2, pp. 75-77, 1976.

[6] Young-Chang Hou(2003), Visual Cryptography for color images, ***Pattern Recognition*** 36, pp.1619-1629.

[7] Hsien-Chu Wu and Chin-Chen Chang(2005), Sharing visual multi-secrets using circle shares, ***Computer Standards & Interfaces*** 28, pp.123-135.

[8] Chang Chin-Chen and Jun-Chou Chuang(2002), An image intellectual property protection scheme for gray-level images using visual secret sharing strategy, ***Pattern Recognition Letters*** 23, pp.931-941.

[9] 陳玲慧(2000)，視覺化密碼之研究及其應用，***89 學年度國科會技術報告***。