不擴展階層式多重視覺秘密分享技術

廖惠雯 助理教授
嶺東科技大學資訊科技應用研究所
hwliao@mail.ltu.edu.tw

張紋莉 碩士生
嶺東科技大學資訊科技應用研究所
t051@lths.tc.edu.tw

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。大部分的視覺密碼方法,都以像素擴展為基礎,造成所產生的分享影像會比原來的機密影像大上許多倍,本文提出不需像素擴展的視覺技術,以固定區塊為加密基本矩陣,每次選取 2x2 區塊作為加密區塊來進行加密判別,將此判別規則應用於階層式多重視覺秘密分享機制,即可建立不擴展階層式多重視覺秘密分享技術。此外,本文除了提出不擴展技術改善了階層式多重視覺秘密分享機制之分享影像及還原影像皆為機密影像的 4 倍之缺點外,並在還原機密影像時,提出以『分享影像判別方法』來,提高還原影像之影像品質。

關鍵詞：視覺密碼學、分享影像、不擴展階層式視覺秘密分享技術、機密影像

Abstract

The biggest merit of visual cryptology lies in that the decryption process only involves overlapping image shares without the requirement of any complex computation or any knowledge on cryptology.

The majority of methods in visual cryptology are based on the concept of pixel expansion. The image shares generated this way are a several-fold magnification of the original secret images. This article proposes a visual technique that does not require pixel expansion. By using a fixed block as the fundamental encryption matrix, this technique selects a block of 2x2 as the encryption block each time to differentiate encryption. A non-expansion hierarchical multiple visual secret sharing technique is then established by applying this differentiation rule to multiple visual secret sharing mechanism.

This proposal not only improves the disadvantage that the image shares and restored image is a 4-fold enlargement of the original secret image when multiple visual secret sharing mechanism is applied, this research also proposes an “image share differentiation method” to enhance the image quality of the restored image when restoring a secret image.

Keywords: Visual Cryptography, Share Image, Hierarchical Visual Secret Sharing Scheme, Secret Image,

1. 前言

由於資訊科技的快速發展,造就網際網路的迅速流通,人們利用網際網路傳遞各式各樣的電子資料,但在互相傳遞過程中,難保不被有心人士擷取資料,造成電子資料機密外洩,如何讓所傳遞的電子資料能確保安全性及保密性,更形重要。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,在有限的時間及資源下也是一大問題,而視覺密碼(Visual Cryptography)便在此環境下產生。

2. 文獻探討

視覺密碼學[2-3](Naor and Shamir,1994；1996)最早在 1994 年由 Naor and Shamir 兩位學者所提出,加密方法很簡單,主要特色是在於解密,在還原機密影像時,不需要任何計算方式來進行解密,而是直接將所有的分享影像重疊起來,即可以人類視覺系統進行解密,改善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 張機密影像,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,將機密影像正確重疊,由人類視覺系統判讀即可以還原機密影像,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) 門檻機制(t out of n Threshold Scheme)。

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[1],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{C1,C2,…,Cn}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 Ci 擁有一個由金鑰中心製作的金鑰 Ki,而且可以使用這個金鑰 Ki 去算 Ki 所管轄之所有群組的秘密金鑰。另外,一個 Ki 或某幾個群組 Ki 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。

陳玲慧等人於 2000 年提出一個新的視覺密碼技術[6],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 3。

侯永昌和杜淑芬於 2004 年提出一種多點同時加密式的不擴展視覺密碼方法[5],利用多點同時加密的概念,每次取 m 個點進行加密,在這 m 個點上出現的黑點,則是依黑點在基礎矩陣中出現的比例而定,來達成像素不擴展的目標,再以提高對比的方式,來解決還原影像中對比損失的問題。

洪維恩和黃敏慧於 2005 年提出使用區塊加密的概念[4],每次依序選擇 2x2 的區塊作為加密區塊來進行加密,並透過限制規則,使分享影像的製作過程為亂中有序,序中有亂,確保加密過程中,像素不擴展。而且,在不影響疊合還原影像結果的情況下,以 3x3 區塊來判別是否加入雜訊干擾,產生新的分享影像,多一份安全性的防護。

廖惠雯及林秀蓓於 2007 年提出階層式多重視覺秘密分享機制[7-8],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(如表 1),建立階層式視覺秘密分享機制,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。

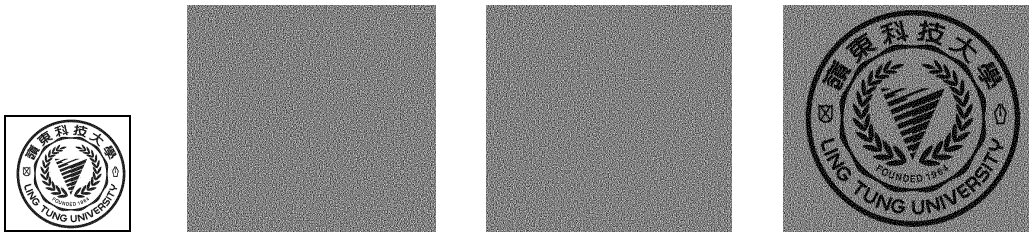


圖 1. (2,2) **Naor and Shamir** 視覺密碼加密與解密

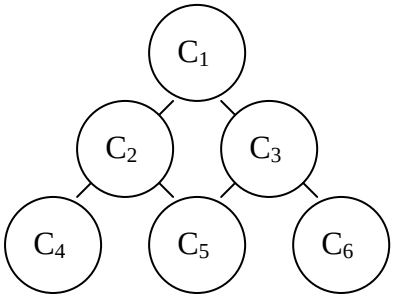


圖 2. **Akl and Taylor** 密碼階層式存取控制

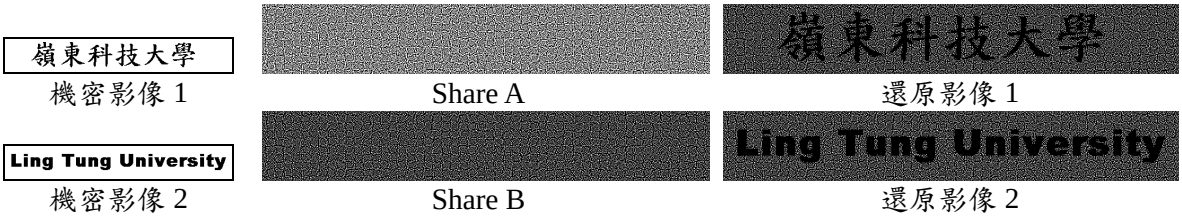


圖 3. **陳玲慧** 新的視覺密碼加密與解密

3. 研究方法

本文所提出不擴展階層式多重視覺秘密分享技術,研究方法以 2x2 區塊為加密基本矩陣,0 表示為白色,1 表示為黑色,每次選取 2x2 區塊作為加密區塊來進行加密判別,2x2 區塊會呈現 16 種黑白像素之組合情況,先把它區分為三類,如表 2,區塊裡若有四個白色像素或是有一個黑色像素及三個白色像素的區塊視為白色(W)；區塊裡若有四個黑色像素或是有一個白色像素及三個黑色像素的區塊視為黑色(B)；二個黑色像素及二個白色像素的區塊則以隨機亂數選取,亂數值大於 0.5 視為白色,亂數值小於 0.5 視為黑色。判別 2 個機密影像相對應的 2x2 區塊位置,再利用表 1,建立不擴展階層式多重視覺秘密分享技術。

若階層關係如圖 4,假設 A 是第一層,B_i 是第二層(即 A 附屬之成員),先將機密影像 S1 及機密影像 S2,一次選取 2x2 區塊像素,根據區塊分類表規則(表 2)及交互建構機制模型(表 1),產生分享影像 A(Share A)及分享影像 B_1(Share B_1),可根據已產生的 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。再由奇數層 2 黑 2 白區塊,及偶數層 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區塊 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。

第一層 A 可知第二層 B_i 之機密,若欲知第三層 C_i 之機密,僅須根據第二層 B_i (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。

要得到兩張機密影像時,直接將分享影像 A(Share A)及分享影像 B_1(Share B_1)疊合,就得到機密影像 S1,再把分享影像 A(Share A)旋轉 90 度與分享影像 B_1(Share B_1)疊合即可得到機密影像 S2。

此外,本研究利用『分享影像判別方法』,來得到兩張機密影像,依序選取 Share A 及 Share B_1 相對應之 2x2 區塊像素,若疊合後為 3 黑 1 白則視為第一類及第三類,若為 4 黑則視為第二類及第三類,再依區塊分類表(表 2),以亂數隨機選取方式填入 2x2 區塊像素,得到第一張機密影像 S1。同理,依序選取 Share A'(及 Share A 旋轉 90 度)及 Share B_1 相對應之 2x2 區塊像素,依上述規則,可得到第二張機密影像 S2。

由於奇偶數層之分享影像分別為 2 黑 2 白及 3 黑 1 白,直接疊合影像為 3 黑 1 白或 4 黑,而 3 黑 1 白代表原機密影像在 2x2 區塊中為白,比實際為影像偏暗,此『分享影像判別方法』可提高機密影像之清晰度。

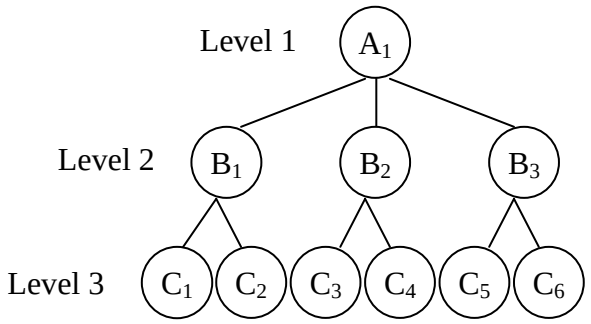


圖 4. 階層式金鑰管理

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																
Share A'																
Share A+ Share B																
Share A'+ Share 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																
Share B'																
Share B+ Share C																
Share B'+ Share C																

表 2：區塊加密分類表

類別	機密影像 2x2 區塊	分類規則	說明
第一類	$\begin{bmatrix}0&0\\0&0\end{bmatrix}$ $\begin{bmatrix}1&0\\0&0\end{bmatrix}$ $\begin{bmatrix}0&1\\0&0\end{bmatrix}$ $\begin{bmatrix}0&0\\0&1\end{bmatrix}$ $\begin{bmatrix}0&0\\1&0\end{bmatrix}$	W	左列五種 2x2 區塊，4 白或 1 黑 3 白像素視為白色(W)
第二類	$\begin{bmatrix}1&1\\1&1\end{bmatrix}$ $\begin{bmatrix}0&1\\1&1\end{bmatrix}$ $\begin{bmatrix}1&0\\1&1\end{bmatrix}$ $\begin{bmatrix}1&1\\0&1\end{bmatrix}$ $\begin{bmatrix}1&1\\1&0\end{bmatrix}$	B	左列五種 2x2 區塊，4 黑或 1 白 3 黑像素視為黑色(B)
第三類	$\begin{bmatrix}1&0\\1&0\end{bmatrix}$ $\begin{bmatrix}0&0\\1&1\end{bmatrix}$ $\begin{bmatrix}0&1\\0&1\end{bmatrix}$ $\begin{bmatrix}1&1\\0&0\end{bmatrix}$ $\begin{bmatrix}0&1\\1&0\end{bmatrix}$ $\begin{bmatrix}1&0\\0&1\end{bmatrix}$	W， $r \geq 0.5$ B， $r < 0.5$	左列六種 2x2 區塊，2 黑 2 白像素，以隨機亂數 r 分類，大於等於 0.5 視為白色(W)，小於 0.5 視為黑色(B)

4. 實驗步驟

本實驗中,以「嶺東科技大學」、「Ling Tung Univerity」、「嶺東高級中學」、「Ling Tung High School」、「資訊科技應用所」、「Information Technology」的字樣分別做為機密影像 S_{B11}、S_{B12}、S_{B21}、S_{B22}、S_{C11} 及 S_{C12},六張影像大小皆為 400×60 的像素。

此階層式架構如圖 4 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。

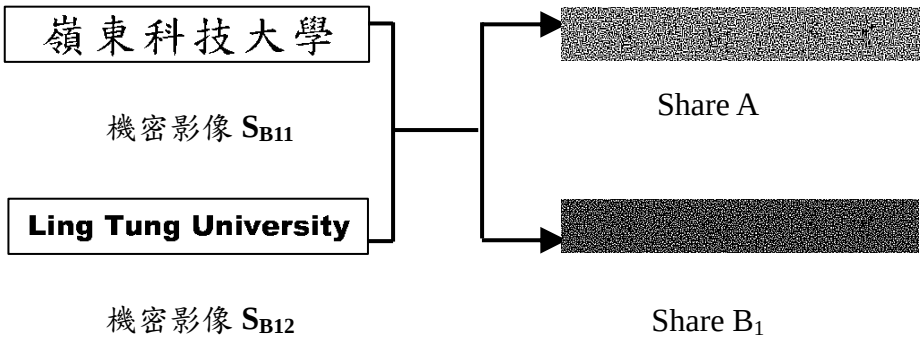
4.1 加密實驗過程

本研究提出不擴展階層式多重視覺秘密分享技術,依序選取 2x2 區塊作為加密區塊來進行加密判別。首先,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),根據區塊分類規則(表 2)及階層秘密分享交互建構機制(表 1(a))產生兩個分享影像 Share A 和 Share B_1 如圖 5(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

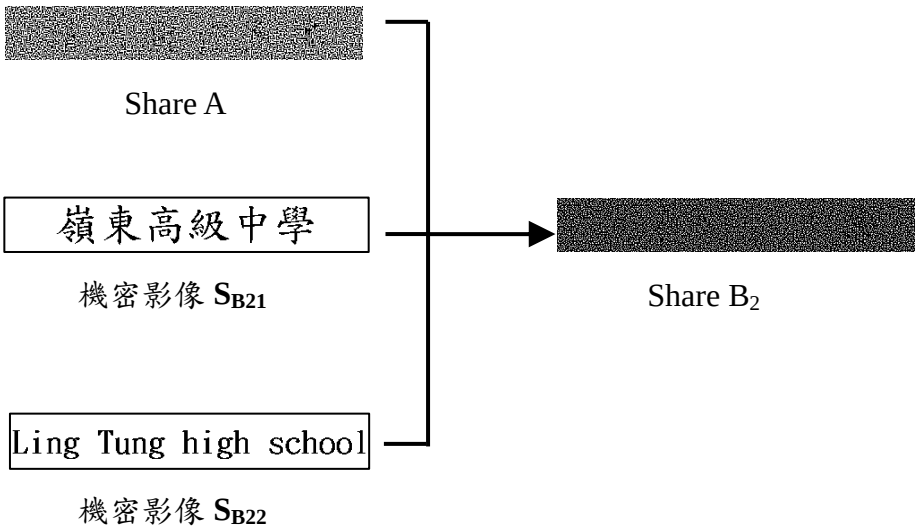
層 B_2 之間的機密影像),再依據 Share A、S_{B21} 和 S_{B22} 產生 Share B_2,如圖 5(b)。

Share A、Share B_1 和 Share B_2 是由表 1(a)所產生,舉例來說,如果第一個機密影像 S_{B11} 的 2x2 區塊,根據區塊分類表規則(表 2)判斷為黑色,第二個機密影像 S_{B12} 相同的區塊位置判斷為白色,根據表 1(a)機密建構模型,共有四種可能性,再以隨機選擇的方式選取一種,就可產生分享影像 Share A 和 Share B_1,若欲增加第二層的成員,假設第三個機密影像 S_{B21} 為白色及第四個機密影像 S_{B22} 為白色,不須重新產生 Share A,根據 Share A 判斷出 Share B_2(由表 1(a))。

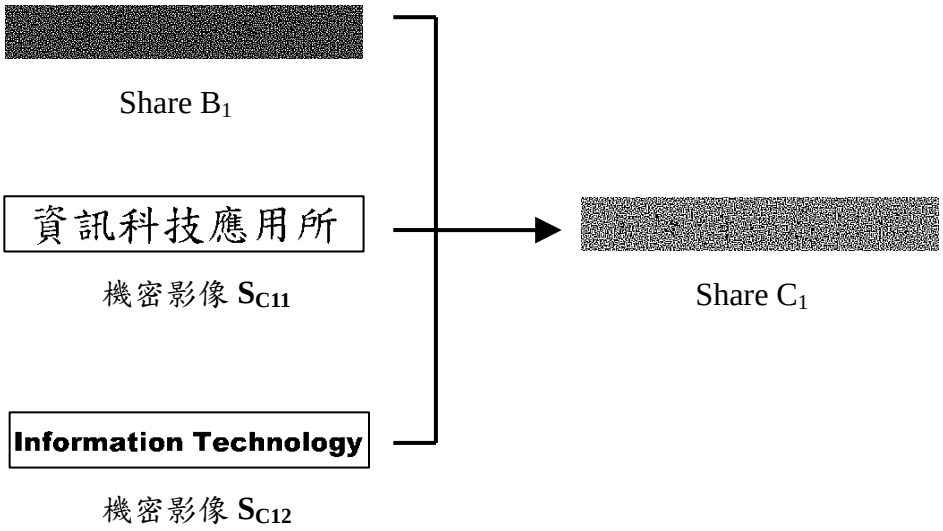
假設第五個及第六個機密影像 S_{C11} 及 S_{C12} 為第三層 C_1 與第二層 B_1 之間的機密影像,欲產生 Share C_1,根據 Share B_1 和機密影像 S_{C11} 與 S_{C12},利用表 1(b)之建構模型即可產生 Share C_1,如圖 5(c)。



(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_{B21} 與 S_{B22} 為第一層 A 與第二層 B_1 之間的機密影像)



(c) 機密影像 S_{C11}、S_{C12} 加密模型(S_{C11} 與 S_{C12} 為第二層 B_1 與第三層 C_1 之間的機密影像)

圖 5. 加密模型

4.1 解密實驗結果

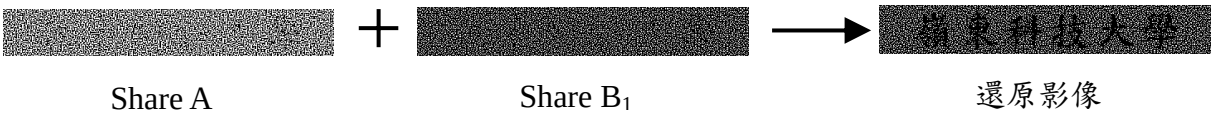
當進行解密時,如果 Share A 的 2×2 區塊為◧,而 Share B_1 的 2×2 區塊如果為◨,Share A 和 Share B_1 重疊後得到■,而 Share A 經過順時針旋轉 90 度,區塊變為◧,在與 Share B_1 重疊後得到◨。

將 Share A 和 Share B_1 重疊後可得到第一個機密影像 S_{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,可產生第二個機密影像 S_{B12}。Share B_2 和原始的 Share A 重疊後,得到第三個機密影像 S_{B22}◨,Share B_2 再與旋轉 90 度後的 Share A(即 Share A')重疊後,即可得到第四個機密影像 S_{B22}◨。

Share A 和 Share B_2 重疊後可得到第三個機密影像 S_{B21},再以 Share A'和 Share B_2 重疊後可得到第四個機密影像 S_{B22}。每一個機密影像中 2×2 區塊的白色由二個黑色像素和二個白色像素所構成,而機密影像中 2×2 區塊的黑色由三個黑色像素和一個白色像素所構成。而疊合而成的 2×2 區塊中,三個黑色像素和一個白色像素代表為白色,而四個皆為黑色像素的區塊代表為黑色。

4.2.1 分享影像直接疊合

A 為第一層的管理者,B_1、B_2 為第 2 層成員,A 及 B_1 之機密影像為「嶺東科技大學」和「Ling Tung Univerity」,Share A 與 Share B_1 疊合還原影像為「嶺東科技大學」,Share A 旋轉 90 度後為 Share A',Share A' 及 Share B_1 疊合還原影像為「Ling Tung Univerity」,如圖 6 所示。管理者 A 與第二層 B_2 之機密影像為「嶺東高級中學」、「Ling Tung High School」,同理 Share A(Share A 並不須重新計算)與 Share B_2 可還原影像「嶺東高級中學」,Share A'與 ShareB_2 可還原機密影像「Ling Tung High School」,如圖 7 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「資訊科技應用所」及「Information Technology」,Share B_1(Share B1 不須重新計算)與 Share C_1 疊合還原機密影像「資訊科技應用所」,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「Information Technology」,如圖 8 所示。



Share A　　Share B_1　　還原影像

Share A'　　Share B_1　　還原影像

圖 6.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

Share A'　　Share B_2　　還原影像

圖 7. 第一層 A 之 Share A 與 ShareA'和第二層 B_2 之 Share B_2 的解密流程

Share B_1　　Share C_1　　還原影像

Share B_1'　　Share C_1　　還原影像

圖 8. 第二層 B_2 之 Share B 與 ShareB'和第三層 C_1 之 Share C_1 的解密流程

4.2.2 分享影像判別

由於直接疊合還原機密圖影像時,白色區塊會有對比度降低,造成機密影像清晰度降低的情形,在此,提出「分享影像判別方法」來提高影像品質,將兩張分享影像依序選取 2×2 區塊,根據區塊分類表規則(表 2)及機密建構模型(表 1)中區塊組合規則,判斷所選取的 2×2 區塊是白色或黑色,再依隨機方式還原機密圖影像。

假設 A 為第一層的管理者,B1、B2 為第 2 層成員,A 及 B1 之機密影像為「嶺東科技大學」和「Ling Tung Univerity」,Share A 與 Share B1 分別為 A 及 B1 的分享影像,每次選取 2×2 區塊,根據「分享影像判別方法」,還原機密影像「嶺東科技大學」,Share A 旋轉 90 度後為 Share A';同理 Share A' 及 Share B1 依據「分享影像判別方法」還原機密影像為「Ling Tung Univerity」,如圖 9 所示。第一層管理者 A 與第二層成員 B2 之機密影像為「嶺東高級中學」和「Ling Tung High School」,同理 Share A(Share A 並不須重新計算)與 Share B2,分別為 A 及 B2 的分享影像,可還原機密影像「嶺東高級中學」,Share A'與 Share B2 分別為 A 旋轉 90 度及 B2 的分享影像,可還原機密影像「Ling Tung High School」,如圖 10 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「資訊科技應用所」及「Information Technology」,同理,Share B_1(Share B_1 不須重新計算)與 Share C_1,分別為 B_1 及 C_1 的分享影像,可還原機密影像「資訊科

技應用所」,Share B_1 旋轉 90 度後為 Share B_1',Share B_1'與 Share C_1 分別為 B_1 旋轉 90 度後及 C_1 的分享影像可還原機密影像「Information Technology」,如圖 11 所示。

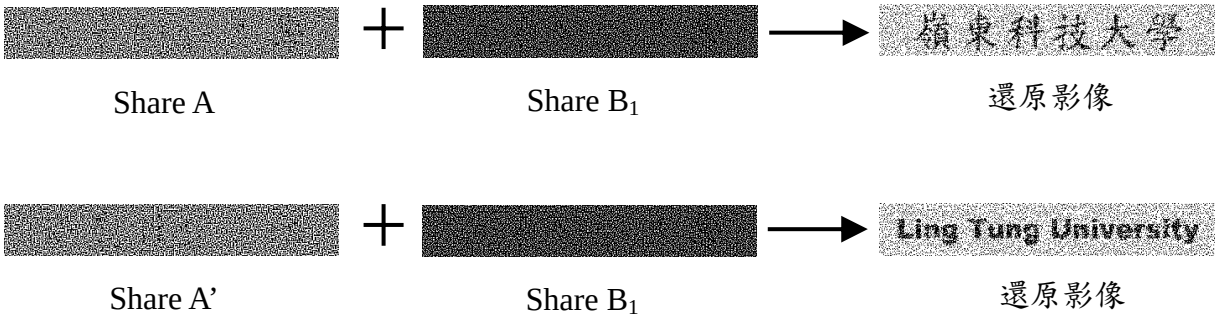


圖 9.第一層 A 之 Share A 與 ShareA'和第二層 B_1 之 Share B_1 的解密流程

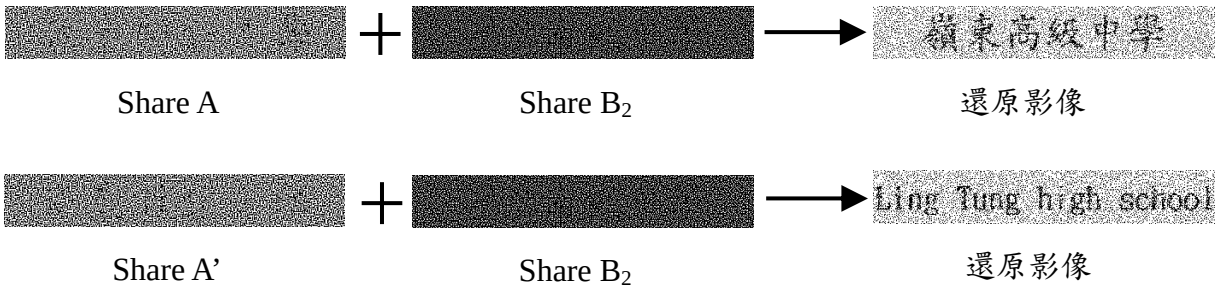


圖 10. 第一層 A 之 Share A 與 ShareA'和第二層 B_2 之 Share B_2 的解密流程

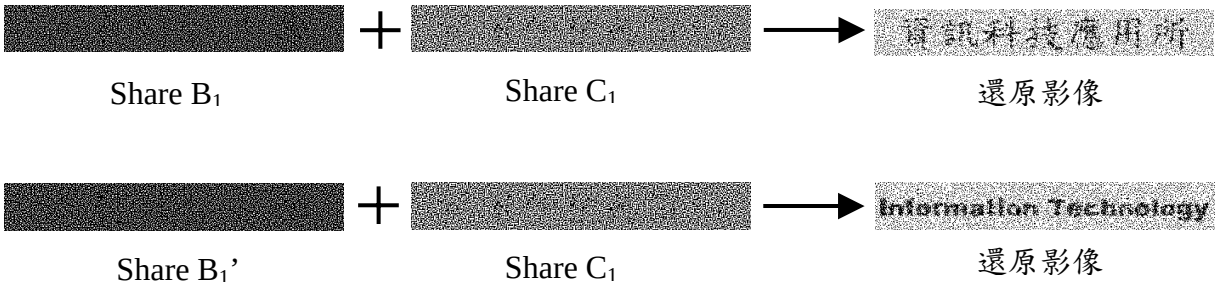


圖 11. 第二層 B_2 之 Share B 與 ShareB'和第三層 C_1 之 Share C_1 的解密流程

5. 分析與討論

經解密實驗後,把還原的影像與原始影像做比對,發現還原影像會產生失真現象,因此我們參考 PSNR 公式值,來比較影像品質。PSNR 公式的定義如下：

$$PSNR = 10 \times \log\left[\frac{255^2}{MSE}\right]$$

$$MSE = \frac{\sum_{k=1}^{n \times m} (I_k - P_k)^2}{n \times m}$$

公式說明：

I_k ：機密圖影像像素值

P_k ：還原影像像素值

MSE ：均方誤差

$n \times m$ ：機密圖跟還原影像寬度及高度

使用 PSNR 公式,將兩種解密方法所產生的還原影像與原始機密影像作比較,如表 3,PSNR 值越大,代表失真越少,可以發現兩種方法的 PSNR 值皆超過 30,且利用「分享影像判別」的方法,PSNR 值超過 54,可得到較好效果。

表 3：機密影像與還原影像 PSNR 值之比較

原始機密影像	PSNR 值比較	
	分享影像直接疊合	分享影像判別
嶺東科技大學	 PSNR=49.8496	 PSNR=54.5913
Ling Tung University	 PSNR=50.0529	 PSNR=54.7355
嶺東高級中學	 PSNR=49.9001	 PSNR=54.3446
Ling Tung high school	 PSNR=50.0574	 PSNR=54.4526
資訊科技應用所	 PSNR=49.7869	 PSNR=54.6170
Information Technology	 PSNR=49.7900	 PSNR=54.6170

6. 結論

資訊的爆炸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,未來此技術可應用於銀行郵局的密碼識別系統,門禁出入系統,及相關使用者身份確認系統。

本文提出一種不擴展階層式多重視覺祕密分享技術,以 2x2 區塊分類規則,達成像素不擴展的目的,並且使用兩種不同的解密方法還原影像,提高影像品質。利用階層式多重視覺秘密分享機制[7-8],管理者與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、讓成員數具有高度的擴充性。

此研究模型,具有以下幾個特性及優點:

- 不擴展技術使分享影像與機密影像大小相同
- 可使用傳統視覺密碼直接疊合還原機密影像
- 可利用「分享影像判別方法」提高還原影像清晰度

參考文獻

[1] Akl, S.G. and Taylor, P.D., "Cryptography solution to a problem of access control in a hierarchy", ***ACM Transactions on Computer System***, 1(3), pp. 239-248,1983

[2] Naor, M. and Shamir, A., "Visual cryptography, Advances in Cryptology,Eurpocrypt'94", ***Springer-Verlag, Berlin***, pp. 1-12, 1994.

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

[4] 洪維恩、黃敏慧,"使用區塊加密法於視覺密碼之研究",***育達商業技術學院資訊管理研究所***,碩士論文,2005。

[5] 侯永昌、杜淑芬,"一種多點同時加密式的不擴展灰階視覺密碼方法",***資訊管理學報第十一卷第四期***,pp.229-249,2004。

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

[7] 廖惠雯、林秀蓓,"階層式多重視覺祕密分享機制於灰階影像之研究與應用", ***資訊科技國際期刊***,Vol 1, pp. 56-66, 2007。

[8] 廖惠雯、林秀蓓,"階層式多重視覺祕密分享機制之研究與應用",***嶺東科技大學資訊科技應用研究所***,碩士論文,2007。