具驗證能力之視覺機密分享技術

李正吉[2] 陳國瑋[1] 劉泓廷[1] 蔡垂雄[1]
國立中興大學 資訊管理學系[1]
Email: tsaics@nchu.edu.tw, peteryam131@gmail.com, hover_g@hotmail.com
亞洲大學 光電與通訊學系[2]
Email : cclee@asia.edu.tw

摘要 **– 視覺密碼與機密分享主要功能在於將一機密影像分成多份無法辨識內容之分享影像，然後藉由分享影像的疊合而重新建構出機密影像。本論文提出兩個影像加密以及驗證的方法。兩種加密方式皆是經由多項式運算去決定分享影像之構成組合。而兩種驗證方式除了傳統藉由分享影像疊合獲得正確機密圖像的方法之外，亦藉由分享影像所提供的資訊經由運算後與當初藏入之機密資訊比對確認，若經由比對之後確認無誤則代表該分享影像為有效之分享影像。**

關鍵詞**—視覺密碼、機密分享、多項式運算、影像**

Abstract **- The main functions of visual cryptography and secret sharing are distributing the secret image to several recognizable sharing images and reconstructing the secret image by overlapping the sharing images. This paper provides two methods to encrypt the secret image and authenticate whether the secret image and the sharing images are correct. Both methods of encryption decide the composition of sharing images by computing with polynomial function. And both methods of authentication use the traditional method that checks the secret image with eyes and also check the information which are hidden in the sharing images and are computed with polynomial function additionally. If the data after checked are all correct, we can identify the sharing images are valid.**

Keyword**—Visual encryption, secret sharing, polynomial computing, image**

一、 前言

在現在這個資訊發達的時代，機密資料的保護是一件非常重要的課題，無論是在商業、軍事以及醫療……等各個方面。此外，也很重要的是我們要確保資料在傳遞過程當中不會遭到他人竄改，為了達到這個目的，對機密資訊加密是一個保護資料完整性的有效方法，但是我們如果對機密資訊加密只加密成唯一資料還是有其風險存在，而這個風險就是一旦這個資料被破解，而整個機密也就洩漏出去了。此外，如果解密這一份加密資訊的鑰匙只有一把的話，萬一這把鑰匙遺失或者損壞，那麼這份機密可能會因此永遠解不開。而且萬一加密的資訊是集會重要的軍事影像、衛星圖像又或者是極重要的醫療影像，如果遇到以上所述之問題將可能遇到重大災害，因此為了解決上述之問題，視覺機密分享機制是一種解決這種問題的好方法[2, 3, 10, 11]。

所謂的*(k,n)*-機密分享機制就是指將一份機密資訊分成 n 份分享資訊，然而要解開機密資訊的內容必須至少有 k 份分享資訊才能解回機密資訊，如果只有$(k-1)$份分享資訊也是無法解密，其中這k份分享資料必須是從n中挑選出來的才行，否則無法解密。例如：公司裡面有一份機密文件被上鎖，而這個鎖有五個孔，分別

各有固定的鑰匙可以插入，然而要解開鎖至少必須要有這五把鑰匙之中的三把才能解鎖，只有一把鑰匙或兩把鑰匙皆無法開鎖。然後在西元 1979 年時，Blakley [1] 和 Shamir [7] 個別提出一種(k,n)-機密分享機制，而他們一般的想法就是如同前面所敘述一樣。

西元 1983 年 Karnin 與 Greene 以及 Hellman [6] 提出了一個完美機密分享 (perfect secret sharing , PSS) 的概念，這個概念主要是在說明如果有一個少於 k(等同於 $\leq k$-1)個有效解密因子為不合格集合，它將只能獲得「零資訊」，也就是無法獲得任何資訊，例如：一個不合格的群組可能會知道機密資訊是一個偶數，但是這個不合格的群組卻無法進一步得知精確的數值，在這 Karnin 等人提出了 $H(s)$去表示一個機密資訊轉換的函式，其中 s 表示一個被分為 n 個分享資訊的機密資訊。而 Karnin 等人提出 PSS 機制必須滿足以下兩個條件：

1. 一個大於等於 k 個因子或者說是 key 所組成的合格集合 C 可以解回機密資訊 s：
   $H(s|C) = 0 \quad \forall |C| \geq k,$

2. 一個小於等於(k–1)個因子所組成的不合格集合 C 無法得知機密 s 的資訊：
   $H(s|C) = H(s) \quad \forall |C| < k.$

在符合上述兩個 PSS 機制中的條件的情況之下，如果擁有大於或等於 k 個合格分享資訊，那麼將可以完全解出機密；相反地，如果只擁有小於或等於(k-1)個分享資訊，那麼將無法成功解密，因此就不會有只擁有(k-1)或者少於(k–1)個分享資訊就洩漏任何機密資訊的情況發生。

之後，Noar 和 Shamir[8, 9]將機密分享的概念延伸到影像方面，並將它歸類在視覺密碼，而視覺密碼是符合 PSS 機制的，也就是說他們的機密資訊為一張影像，而他們將此影像分為 n 張看不出任何資訊的分享影像，如果想要得知機密影像的資訊，則必須至少擁有 n 張分享影像之中的 k 張疊合才可得知機密影像的資訊；同理，如果只擁有 n 張分享影像之中的(k-1)張分享影像或者還比(k–1)張少，那麼將無法疊合出機密影像中所藏的資訊。而這種技術主要是藉由分享影像的疊合來獲取機密影像的資訊，而且不需要任何的計算，但是因為這個方法驗證的方法就只有利用肉眼觀察分享影像疊合出來的結果，而沒有其他的驗證方法，也就是說機密資訊有可能遭人竄改，可是只依賴肉眼卻無法完全保證其機密資訊之正確性，所以我們可能還是得依靠一些數學方法去進一步驗證資訊的正確性。

因此，本論文提出兩個數學方法在將影像加密時，可以將影像的資訊藏入分享影像之中，之後將分享影像疊合之後，除了利用肉眼觀察其疊合後機密影像之正確性之外，亦利用隱藏在分享影像的資訊去作運算，並利用其運算結果確認分享影像是否為正確之分享影像，如果分享影像皆確認無誤，那麼疊合出來的機密影像我們也可以確保其正確性。首先，利用我們想加密的原始圖像的像素值分別以兩個、兩個為一對，然後再帶入多項式去運算，之後我們將運算過後的值存入一個陣列 M 當中，其中這個陣列 M 將是之後要用來比對分享影像中的資訊是否正確之用，之後再將陣列 M 中的資料化為四個數字為一組的六進位數字再存入另一個陣列 R，其中陣列 R 中 0~5 的數字分別代表黑白像素的組合形式，其組何種類白色共有 6 種，而黑色共 6×4 = 24 種，之後的步驟將是本論文提出的兩個方法的不同之處，我們將在後面的章節更詳細的描述。而從實驗中我們也可以觀察到我們確實可以藉由隱藏資訊的比對有效地檢驗分享影像以及分享影像疊合後所獲得的機密影像的正確性。

本篇論文在內容架構上一共分為五個章

節，在下一章節將介紹 Shamir 提出的機密分享機制以及 Shamir 與 Noar 提出的視覺機密分享機制；在第三個章節我們將詳細介紹本論文提出的兩個方法；第四個章節將會展示實驗的結果；最後為本篇論文的結論。

二、 文獻探討

2.1 Shamir 的機密分享機制

前面我們提到了許多(*k*,*n*)-機密分享機制，而且也介紹到 Noar 與 Shamir 如何將機密分享機制運用到視覺密碼。在這裡我們要介紹一個 Shamir [7]在 1979 年提出的機密分享機制，Shamir 在這個機制中提出了一個(*k*, *n*)-機密分享技術的想法，其中 $k \le n$。這項技術運用到一個多項式的公式，而公式如下[4, 5]：

$$f(x) = s_0 + s_1 x + s_2 x^2 + \ldots + s_{k-1} x^{k-1} \pmod{p}$$，

而上式中的 s_0 代表的是機密，p 代表的則是一個質數，機密分享則是一對值(x_i, y_i)，其中 $y_i = f(x_i)$，$1 \le i \le n$，$0 < x_1 < x_2 < \cdots x_n < p - 1$。

當每個有權獲得分享資訊的持有者都獲得一對值(x_i, y_i)之後，多項式 $f(x)$將被破壞，也將導致如果只擁有單一分享資訊是無法解出機密值 s_0的。如果想要解出機密值 s_0的話，則必須至少擁有 k 組或者 k 組以上的有效分享資訊，並將這些分享資訊代入 k 個線性方程式 $y_i = f(x_i)$ 去解出各個未知數 s_i，然後藉由這些線性方程式的唯一解再利用 Lagrange interpolation 我們便可以很容易地解出機密值 s_0；相反地，如果我們擁有的有效分享資訊如果只有$(k-1)$組，或者甚至比$(k-1)$組還要少，那麼我們將無法解出機密資訊 s_0。

因此，由前面敘述我們可以得知 Shamir 的機密分享機制是屬於 PSS 機制，因為我們必須知道多於 k 個線性方程是去求解才解得出機密資訊 s_0，否則即使我們知道$(k-1)$個線性方程式，我們依舊無法得知機密資訊。

2.2 Shamir 與 Noar 的視覺機密分享機制

在這個部分我們要回顧 Shamir 與 Noar [9]在 1994 年提出的(2,2) -視覺機密分享機制，而這項視覺加密技術主要的貢獻在於我們只需要藉由肉眼便可以辨認出隱藏的機密圖像，不需要依靠任何的計算。而(2,2) –視覺機密分享機制是指將機密影像分為兩張分享影像，而且任何人如果只擁有其中一張分享影像是無法從中獲得任何資訊的，一定得同時具備這兩張分享影像才可以解出機密圖像。

假設我們有一張像素大小為 $M \times N$ 黑白機密影像 *BS*，*BS* 是由分享影像 1 與分享影像 2 這兩張黑白分享影像所組成的，而這兩張黑白分享影像大小皆為 $2M \times 2N$。首先，我們要將分享影像分成許多沒有重疊且像素值大小為 2×2 的正方形區塊，而且每一個正方形區塊都必須等分為四等分，而且每個區塊都必須擁有 2 黑 2 白，也就是說這四個等分必須有兩個等分是黑兩個是白。而由前面我們可以知道在兩張分享影像之中我們會有 $M \times N$ 個 2×2 的正方形區塊，而這 $M \times N$ 個區塊分別依序代表 *BS* 中 $M \times N$ 個像素的值，因此接下來就是依序判斷 *BS* 中的像素值為黑或者是白，然後在兩張分享影像相對應的位置放入 2×2 的正方形區塊，而無論 *BS* 中的值為白或黑，兩張分享影像所應放入的相對應的正方形區塊皆有六種情形，而這六種情形我們將列於下列表Ⅰ與表Ⅱ當中，而表Ⅲ與表Ⅳ分別為表Ⅰ與表Ⅱ之矩陣表示法。

表Ⅰ 此為當 *BS* 為白時兩張分享影像所放入區

塊組合圖以及疊合之後的圖

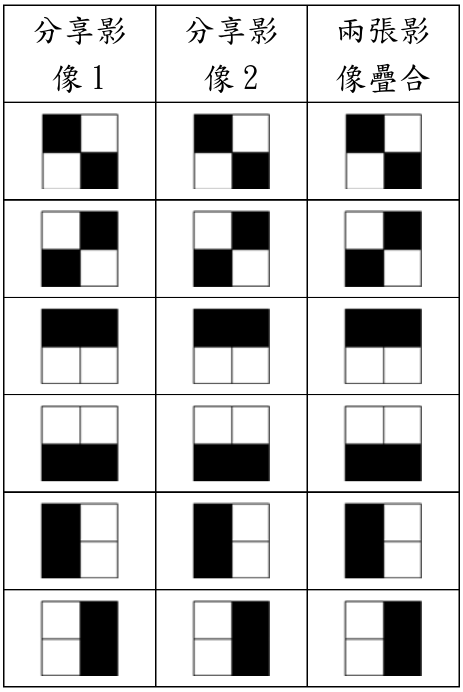


表 II 此為當 *BS* 為黑時兩張分享影像所放入區塊組合圖以及疊合之後的圖

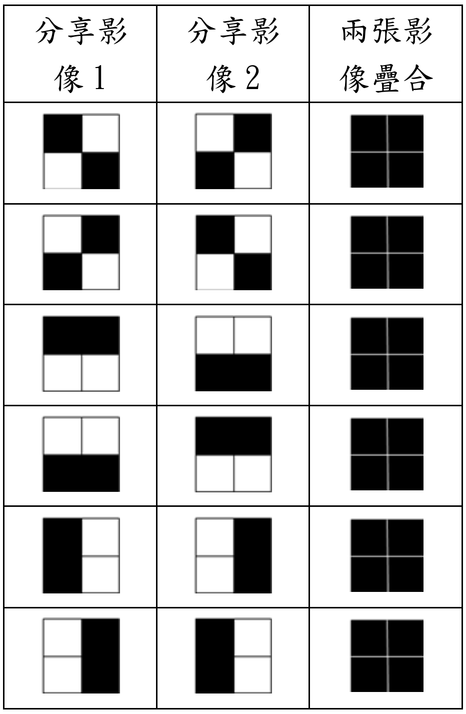


表 III 此為表 I 中六種疊合方式之矩陣表示法

$\begin{bmatrix}1001\\1001\end{bmatrix}$	$\begin{bmatrix}0110\\0110\end{bmatrix}$	$\begin{bmatrix}1100\\1100\end{bmatrix}$
$\begin{bmatrix}0011\\0011\end{bmatrix}$	$\begin{bmatrix}1010\\1010\end{bmatrix}$	$\begin{bmatrix}0101\\0101\end{bmatrix}$

表 IV 此為表 II 中六種疊合方式之矩陣表示法

$\begin{bmatrix}1001\\0110\end{bmatrix}$	$\begin{bmatrix}0110\\1001\end{bmatrix}$	$\begin{bmatrix}1100\\0011\end{bmatrix}$
$\begin{bmatrix}0011\\1100\end{bmatrix}$	$\begin{bmatrix}1010\\0101\end{bmatrix}$	$\begin{bmatrix}0101\\1010\end{bmatrix}$

三、 本論文提出之方法

3.1 原始圖像前置處理

(1) 步驟一：將原始大小為 $i\times j$ 之灰階圖像的像素值資訊存入一個大小為 $i\times j$ 之一維陣列 x_1 中，其中圖像大小為 $i\times j$ 代表共有 i 列 j 行個像數值。

(2) 步驟二：將原始灰階圖像作半色調處理，並將圖像半色調後之像素資訊存入另一個大小為 $(i+2)\times(j+2)$ 之一維陣列 x_2 中。

3.2 兩個加密方法共同之步驟

(1) 步驟一：將陣列 x_1 中的相鄰的值兩個為一組劃分清楚，因此將可以分為 $\theta = \lfloor \frac{i\times j}{2} \rfloor$ 組。

(2) 步驟二：我們用以計算出加密(比對驗證)資訊的式子如下：

$$f_n(x) = \alpha_{(n,1)} + \alpha_{(n,2)}x \pmod{251},\ 1 \le n \le \theta \quad (1)$$

方程式(1)中，$f_n(x)$代表第 n 組函式，$\alpha_{(n,1)}$代表步驟一中分組完後第 n 組的第 1 個數值；同理，$\alpha_{(n,2)}$代表第 n 組中的第 2 個數值。

(3) 步驟三：如果我們要將機密影像分成 β 張分享影像，那麼就將 $x = 0 \sim x = (\beta-1)$的整數分別代入式子(1)中計算。換句話說，(1)中的 θ 組函式均要代入 β 個 x 值下去計算，因此會產生($\theta \times \beta$)個數據。

3.3 第一個加密方法後續處理

(1) 步驟一：因為本論文第一個方法實作是採(2,3) - 機密分享機制，所以將 $x = 0$~2 的整數依照 3.2 步驟三去作計算，最後算出的每一個十進位數據存入一維陣列 δ_1 中且再將 δ_1 中的值轉換成四個六進位數值，並將這些數值存入另一個一維陣列 γ_1 之中。

(2) 步驟二：判斷一維陣列 x_2 中的值代表著黑或白，來決定三張分享影像應該放入何種組合。其中，三張分享影像之大小皆為 $2\times(i+2)\times 2\times(j+2)$。

(3) 步驟三：若判斷 x_2 之像素值為白，則三張分享影像的組合方式會有 6 種組合情形，而組合的情況我們列在下面表Ⅴ當中，其中表Ⅴ所列出的矩陣中的 1 代表黑色、0 代表白色，而每個矩陣中有三列的值，這三列值分別代表三張分享影像分別要填入的情況。此外，這 6 種組合情形之中三張分享影像填入的情況必須符合每兩張分享影像或者三張分享影像疊合之後，必為 2 黑 2 白的情況。

表Ⅴ x_2 中的值為白三張分享影像 6 種疊合方式之矩陣表示法

組合形式	$\begin{bmatrix}1100\\1100\\1100\end{bmatrix}$	$\begin{bmatrix}1001\\1001\\1001\end{bmatrix}$	$\begin{bmatrix}1100\\0110\\0101\end{bmatrix}$
編號	(1)	(2)	(3)
組合形式	$\begin{bmatrix}1010\\1010\\1010\end{bmatrix}$	$\begin{bmatrix}0101\\0101\\0101\end{bmatrix}$	$\begin{bmatrix}0011\\0011\\0011\end{bmatrix}$
編號	(4)	(5)	(6)

若判斷 x_2 之像素值為黑則三張分享影像的組合方式會有 24 種組合情形，而這些組合情況我們列在下面表Ⅵ之中，表Ⅵ當中矩陣的值以及每一列代表的意義皆與表Ⅴ相同。不過表Ⅵ當中所列出的 24 種組合情況有其必須遵守的規則，也就是這 24 種組合情況必須符合兩張分享影像疊合必須符合 3 黑 1 白的條件，而三張影像疊合必須符合 4 黑 0 白的條件。

在前面表Ⅴ與表Ⅵ的說明中我們提到 3 個條件：2 黑 2 白、3 黑 1 白、4 黑 0 白，主要是由於影像疊合之後，我們分辨黑白的方式是藉由對比的關係去判別，也就是我們在疊合之後的影像所看到的黑與白是「相對的黑」以及「相對的白」，而並非絕對性的。除此之外，表Ⅴ與表Ⅵ中每個陣列的第一列將會是後面我們解密的關鍵，因此我們稱此列為「main row」。

表Ⅵ x_2 中的值為黑時三張分享影像 24 種疊合方式之矩陣表示法

組合形式	$\begin{bmatrix}1100\\1010\\1001\end{bmatrix}$	$\begin{bmatrix}1100\\1001\\1010\end{bmatrix}$	$\begin{bmatrix}1100\\0101\\0110\end{bmatrix}$	$\begin{bmatrix}1100\\0110\\0101\end{bmatrix}$
編號	(1-1)	(1-2)	(1-3)	(1-4)
組合形式	$\begin{bmatrix}1001\\0101\\0011\end{bmatrix}$	$\begin{bmatrix}1001\\0011\\0101\end{bmatrix}$	$\begin{bmatrix}1001\\1100\\1010\end{bmatrix}$	$\begin{bmatrix}1001\\1010\\1100\end{bmatrix}$
編號	(2-1)	(2-2)	(2-3)	(2-4)
組合形式	$\begin{bmatrix}0110\\0011\\1010\end{bmatrix}$	$\begin{bmatrix}0110\\1010\\0011\end{bmatrix}$	$\begin{bmatrix}0110\\0101\\1100\end{bmatrix}$	$\begin{bmatrix}0110\\1100\\0101\end{bmatrix}$
編號	(3-1)	(3-2)	(3-3)	(3-4)
組合形式	$\begin{bmatrix}1010\\1100\\1001\end{bmatrix}$	$\begin{bmatrix}1010\\1001\\1100\end{bmatrix}$	$\begin{bmatrix}1010\\0011\\0110\end{bmatrix}$	$\begin{bmatrix}1010\\0110\\0011\end{bmatrix}$
編號	(4-1)	(4-2)	(4-3)	(4-4)
組合形式	$\begin{bmatrix}0101\\1100\\0110\end{bmatrix}$	$\begin{bmatrix}0101\\0110\\1100\end{bmatrix}$	$\begin{bmatrix}0101\\1001\\0011\end{bmatrix}$	$\begin{bmatrix}0101\\0011\\1001\end{bmatrix}$
編號	(5-1)	(5-2)	(5-3)	(5-4)
組合形式	$\begin{bmatrix}0011\\1010\\0110\end{bmatrix}$	$\begin{bmatrix}0011\\0110\\1010\end{bmatrix}$	$\begin{bmatrix}0011\\0101\\1001\end{bmatrix}$	$\begin{bmatrix}0011\\1001\\0101\end{bmatrix}$
編號	(6-1)	(6-2)	(6-3)	(6-4)

(4) 步驟四：由於此方法之實驗有三張分享影像，因此我們將三張影像分為上、中、下三個部分，在「上面」的部分，陣列第一列的值填入第一張分享影像，其餘依序填入另外兩張分享影像；在「中間」部分，陣列第一列值填入第二張分享影像，其餘亦依序填入另外兩張分享影像；最後依此類推。

(5) 步驟五：經過步驟三的判斷之後，如果判斷 x_2 中的值為白，再藉由陣列 γ_1 中的值 ρ 下去決定要從表Ⅴ之中選擇編號(ρ+1)的陣列，並依照步驟四的方式填入；反之，如果是黑色則根據陣列 γ_1 中的值 ρ 然後再隨機選取一個範圍從1~4的正整數 μ，最後從表Ⅵ中挑出編號((ρ+1)–μ)的陣列，並依照步驟四的方法填入，則方法一之影像加密就完成了。

3.4 第二個加密方法後續處理

(1) 步驟一：與 3.3 步驟一類似，不過第二個方法是實作是採(2,2)-機密分享機制，因此，我們將 x=0~1 的整數依照 3.2 步驟三去作計算，最後算出的每一個十進位數據存入一維陣列 δ_2 中且再將 δ_2 中的值轉換成四個六進位數值，並將這些數值存入另一個一維陣列 γ_2 之中。

(2) 步驟二：判斷一維陣列 x_2 中的值代表著黑或白，來決定兩張分享影像應該放入何種組合。其中，兩張分享影像之大小皆為 $2\times(i+2)\times 2\times(j+2)$。

(3) 步驟三：若判斷 x_2 之像素值為白，則兩張分享影像的組合方式有 6 種情況，這些組合情形我們將列於表Ⅶ之中，而表Ⅶ之中每個矩陣中的 1 代表黑色、0 代表白色，矩陣中的第一列值代表第一張分享影像所要填入的情況。同理，第二列值代表第二張分享影像所要填入的情況。

若判斷 x_2 之像素值為黑則兩張分享影像的組合方式亦有 6 種情況，我們亦將組合方式列於下列表Ⅷ之中，而表Ⅷ之中矩陣的每列以及其值所代表的意義皆與表Ⅶ相同。

表Ⅶ x_2 中的值為白時兩張分享影像 6 種疊合方式之矩陣表示法

組合形	$\begin{bmatrix}1100\\1100\end{bmatrix}$	$\begin{bmatrix}1001\\1001\end{bmatrix}$	$\begin{bmatrix}0110\\0110\end{bmatrix}$

式			
編號	(1)	(2)	(3)
組合形式	$\begin{bmatrix}1010\\1010\end{bmatrix}$	$\begin{bmatrix}0101\\0101\end{bmatrix}$	$\begin{bmatrix}0011\\0011\end{bmatrix}$
編號	(4)	(5)	(6)

表Ⅷ x_2 中的值為黑時兩張分享影像 6 種疊合方式之矩陣表示法

組合形式	$\begin{bmatrix}1100\\0011\end{bmatrix}$	$\begin{bmatrix}1001\\0110\end{bmatrix}$	$\begin{bmatrix}0110\\1001\end{bmatrix}$
編號	(1)	(2)	(3)
組合形式	$\begin{bmatrix}1010\\0101\end{bmatrix}$	$\begin{bmatrix}0101\\1010\end{bmatrix}$	$\begin{bmatrix}0011\\1100\end{bmatrix}$
編號	(4)	(5)	(6)

(4) 步驟四：我們將表Ⅶ以及表Ⅷ中編號(6)之陣列定為特殊矩陣，因為之後我們解密將利用到這特殊矩陣。

(5) 步驟五：依照 γ_2 中的值 ω 來決定特殊矩陣在兩張分享影像之中的放置位置，且兩兩特殊矩陣放置的位置中間理應有 ω 個空格。

(6) 步驟六：決定好特殊矩陣放置的位置之後，其餘空格則隨機挑選特殊矩陣之外的其他編號矩陣來填補。

(7) 步驟七：在經過步驟五與六確定好兩張分享影像每個位置所要填放之編號組合之後，我們再配合 x_2 之黑白像素值來決定分享影像應該放表Ⅶ或者表Ⅷ之中的該編號之矩陣，則方法二之加密就完成了。

3.5 方法一之解密與驗證

(1) 步驟一：首先將三張分享影像分別兩兩疊合以及三張疊合，檢驗是否可以看得出有意義的資訊，如果可以再進行下一個驗證工作。如果疊合無法看出圖像資訊便不需要再進行下一步，因為代表分享影像為不合法分享影像。

(2) 步驟二：通過步驟一之檢驗後，接下來我們要更進一步去驗證分享影像，我們可以藉由分享影像一之前三分之一部分與分享影像二之中間三分之一部分以及分享影像三之最後三分之一部分之中以 2×2 為一個單位之正方格黑白矩陣，去對照表Ⅴ與表Ⅵ之中 main row 的組成，決定其正方格為表Ⅴ或表Ⅵ之中哪一編號矩陣，若為表Ⅴ中之矩陣則將編號減 1 的值存入陣列 ε_1，若為表Ⅵ之中之矩陣則將編號第一個數字減 1 的值存入陣列 ε_1，之後將陣列 ε_1 之六進位值四個為一組化為十進位存入陣列 ε_2。

(3) 步驟三：比對 ε_2 與 δ_1 中的值是否相同，若相同代表分享影像為合法分享影像；反之，代表分享影像為不合法分享影像。

3.6 方法二之解密與驗證

(1) 步驟一：先將兩張分享影像疊合之後，檢查是否可疊出機密資訊，如果可以呈現有意義的資訊我們再進到下一階段的驗證工作；反之，

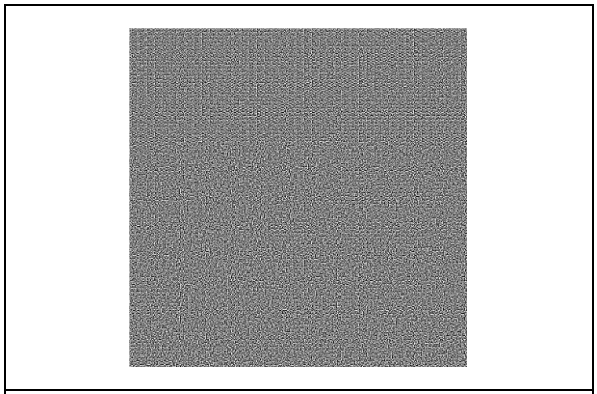
則代表分享影像為不合法分享影像。

(2) 步驟二：對照表Ⅶ與表Ⅷ之中的矩陣組合，找出分享影像一與分享影像二之中編號六的矩陣位置所在並記錄下來，之後計算每兩個矩陣六之間有幾個空格並將結果記錄在陣列 ε_3，再來將陣列 ε_3 之中的六進位值四個為一組化為十進位存入陣列 ε_4 之中。

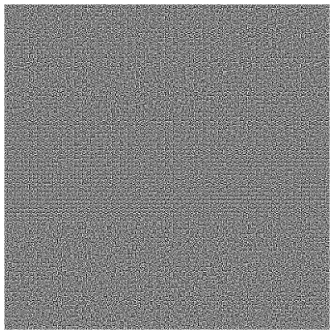
(3) 步驟三：比對陣列 ε_4 與 δ_2 中的值是否相同，若比對無誤代表分享影像為合法分享影像；反之，代表分享影像為不合法分享影像。

四、 實驗結果

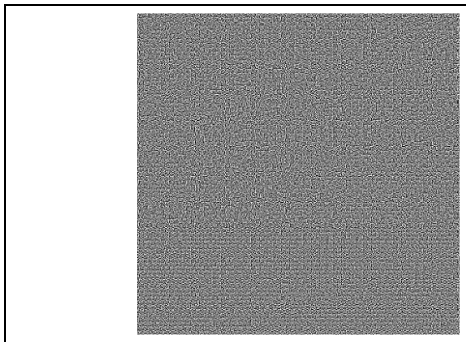
4.1 方法一之實驗結果



分享影像 1



分享影像 2



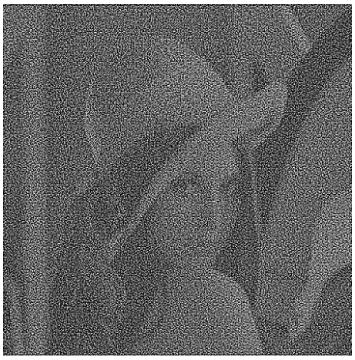
分享影像 3

圖一

圖一為利用方法一加密方法所形成的分享影像呈現之結果。如圖所示，我們利用肉眼無法從分享影像無法得知機密資訊。

分享影像 1、2 疊合

分享影像 1、3 疊合



分享影像 2、3 疊合

三張分享影像疊合

圖二

圖二中的圖為方法一之解密圖像，我們可以看出機密圖像為 lena，而且結果是符合(2,3)-機密分享機制的。雖然我們看到無論是兩張分享影像疊合或者是三張分享影像疊合都可以看出機密影像，但是兩張分享影像疊合的結果感覺較沒有三張分享影像疊合之後的影像清晰，這是由於在 3.3 步驟三我們有提到在這裡我們所看到疊合後影像中的黑與白是相對的，而兩張分享影像疊合的結果由於其中的白是由 2 黑 2 白所構成，其中的黑是由 3 黑 1 白所構成；相對地，三張分享影像疊合後之影像中的白一樣是由 2 黑 2 白所構成，黑是由 4 黑 0 白所構成。因此，我們可以知道三張分享影像疊合造成的對比效果較兩張分享影像所造成的效果顯著，所以我們才會看到三張分享影像疊合出來比兩張分享影像疊合出來之影像清晰。

此外，我們將存有利用分享影像 1、2、3 所提供的隱藏資訊經計算後之結果的陣列 ε_2 與存有機密資訊的陣列 δ_1 作比對動作，我們發現 ε_2 中之資訊為正確機密資訊，因此可以判定分享影像為合法分享影像。

4.2 方法二之實驗結果

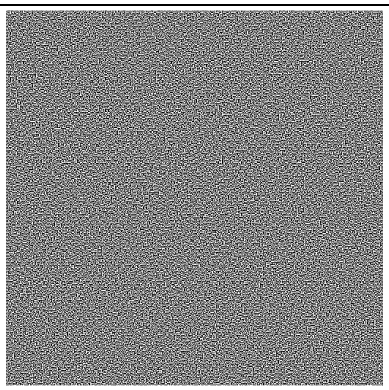
圖三為利用方法二所實作出來的分享影像，我們無法單獨從分享影像得到任何有關機密資訊的訊息。

圖四為方法二之解密圖像，我們可以看出機密圖像為 lena。

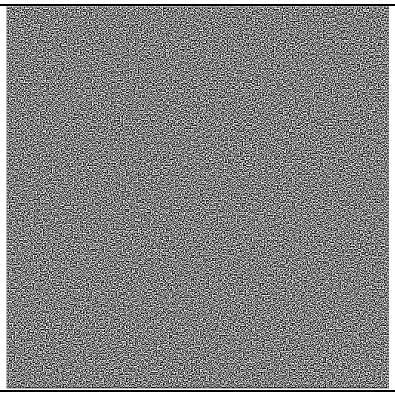
此外，我們將存有利用分享影像 1、2 所提供的隱藏資訊經計算後之結果的陣列 ε_4 與存有機密資訊的陣列 δ_2 作比對動作，我們發現 ε_4 中之資訊為正確機密資訊，因此可以判定分享影像為合法分享影像。

4.3 方法一與方法二藏入資訊量之對照

除了上述之實驗結果，我們亦經由實驗得知利用方法一與方法二所藏入的機密資訊量。在實驗中我們所採用的的原圖為 256×256 像素的 lena 圖，經由實驗後我們得知方法一所藏入的機密資訊量為 133128 bits，方法二所藏入的機密資訊量為 46334 bits。而經由計算後，我們亦證實解密出的資訊量與藏入的資訊量一致。



分享影像 1



分享影像 2

圖三

兩張分享影像疊合之結果

圖四

五、 結論

本論文提出的兩個以計算方式加密並藉由藏在判斷分享影像之中的資訊，去作計算且加以比對驗證的方法，並不會破壞視覺密碼的基本原則，也就是在不滿足解密條件的情況之下，機密圖像是不會被發現的。而本論文解密除了具備只需肉眼就可看出機密資訊的功能之外，亦利用了計算的方式算出藏在分享影像中的資訊，並比對其正確性，這更加提高了機密資訊的正確性與安全性。

誌謝

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no: NSC 96-2628-E-005-008-MY2 and NSC98-2221-E-468-002.

參考文獻

[1] G. Blakley, “Safeguarding cryptographic keys,” presented at Proceedings of the AFIPS 1979 National Computer Conference, vol . 48, Arlington, VA, pp. 313-317, June 1997.

[2] C. C. Chang and J. C. Chuang, “An image intellectual property protection scheme for gray-level images using visual secret sharing strategy,” Pattern Recognition Letters, vol. 23, no. 8, pp. 931-941, June, 2002.

[3] Y. F. Chen, Y. K. Chan, C. C. Huang, M. H. Tsai, and Y. P. Chu, “A multiple-level visual secret-sharing scheme without image size expansion,” Information Sciences, vol. 177, no. 21, pp. 4696-4710, November 1, 2007.

[4] J. B. Feng, H. C. Wu, C. S. Tsai, and Y. P. Chu, “A new multi-secret images sharing scheme using Largrange’s interpolation, Journal of Systems & Software, vol. 76, no. 3, pp. 327-339, June, 2005.

[5] H. F. Huang and C. C. Chang, “A novel efficient (t,n) threshold proxy signature scheme, “ Information Sciences, vol. 176, no. 10, pp. 1338-1349, May 22, 2006.

[6] E. D. Karnin, J. W. Greene, and M. E. Hellman,

"On secret sharing systems," IEEE Tran. On Information Theory, vol. IT-29, no. 1 , pp.35-41, Jan. 1983.

[7] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612-613, Nov. 1979.

[8] M. Noar and A. Shamir (June,1996) Visual cryptography II: Improving the contrast via the coverbase.[Online]. Available:http://philby.ucsd.edu/cryptolib/1996/96-07.html. Last accessed: March 2005.

[9] M. Noar and A. Shamir, "Visual cryptography," presented at the Proceedings of the Conference on Advances in Cryptology – Eurocrypt '94, A. De Santis, Ed, Berlin, Germany, pp. 1- 12., 1994.

[10] C. S. Tsai, C. C. Chang, and T. S. Chen, "Sharing multiple secrets in digital images," Journal of Systems and Software, vol. 64, no. 2, pp. 163-170, November 15, 2002.

[11] H. C. Wu and C. C. Chang, "Sharing visual multi-secrets using circle shares," Computer Standards & Interfaces, vol. 28, no. 1, pp. 123-135, July, 2005.