國 立 政 治 大 學 資 訊 科 學 系

碩 士 學 位 論 文

A Study on Multiple Visual Cryptography via Rotation

視覺密碼技術旋轉與立體旋轉之研究

指導教授：左瑞麟

研 究 生：謝孟諺

100 年 7 月 1 日

視覺密碼技術旋轉與立體旋轉之研究

摘要

視覺密碼是一種特別的密碼系統,在 1994 由 Noar 與 Shamir 所提出的概念,透過設計好的模型，加密時將原始機密分散成數張雜亂無章的分享影像，解密時，不需要任何大量複雜的數學運算，只需結合所有分散影像，透過人類的視覺系統，即可解讀原始機密的方法，而此種方式不需要用到任何密碼學專業知識，且具有視覺化、操作容易、高度保密等優點。現今網路日益發達與開放的社會，視覺密碼可以增加我們資料的安全性。

在本研究中將引用視覺密碼的基本概念，透過結合 1998 年 Wu 所提出旋轉式視覺密碼以及 2001 年 Wu 所提出平移視視覺密碼兩種概念，進而提出 "立體旋轉"的視覺密碼以增加解碼的困難度，可確保不易查出機密影像的資訊。

關鍵詞　視覺密碼；多秘密分享；

Visual Cryptography Techniques for

Abstract

Visual cryptography is considered as a special encryption system that can be decrypted by human vision in a way without any type of computing process. This technique was proposed by Noar and Shamir in 1994.It also increases safety for our information in today's increasingly open network environment.

Visual cryptography uses two transparent images and both of them reveal the information. One image contains random pixels and the other image contains the secret information. This research adopts the concepts of basic idea of visual cryptography and introduces a method that increases the complexity of decryption by wrapping up one layer of images so that one can not perceive the secret information from one single share images.

Keywords visual cryptography; multiple secrets;

目錄

圖目錄

表目錄

第一章　緒論

1.1 研究背景

科技的進步造就資訊時代的來臨，資訊獲得是如此輕而易舉，不管是工作或是消費、休閒等，都離不開使用電腦的需求，然而網際網路的成熟，更加速了這方面的發展。但也因此造成網路犯罪的發生，資訊安全無疑成為一個重要安全議題。舉例來說，當傳送機密文件至網路的同時，為了避免於無授權情況下被存取、竊取，機密文件通常會做加密動作，用以保護機密文件。因此資訊安全漸漸被社會大眾重視，也產生了許多這方面的議題，像是密碼學、鑑定機制、電子簽章、資訊隱藏等各式各樣的安全機制。但是這些機制都需要複雜的計算，幾乎都須要靠電腦來完成，因此有學者提出了一種稱為視覺密碼，藉由人類的雙眼(視覺系統)來解讀秘密。

視覺密碼學最早在1994 年由Naor 和Shamir 所提出[1-2]，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，依據人類視覺系統對於色差的反應，而賦予影像意義的基礎，例如健康檢查時，檢測色盲所用的卡片即是以人眼視覺的反應來判斷多個不同色彩的雜點所包含的訊息。而Naor 及Shamir透過設計好的模型，將機密影像編碼為兩張看似雜亂無意義的分享影像，再將分享影像印在透明的投影片上，解密時只需要將兩張投影片疊在一起，即可利用人類的視覺系統(眼睛)進行解密的工作，如此在解密的時候就不再需要透過電腦的幫忙，在沒有電腦的場合之下，也能讓合法的使用者輕易的還原出機密影像，這種做法具有視覺化、操作簡易、高度保密等優點使得密碼學邁向另一種不同層面。

2.2 、研究動機、方式

Naor與Shamir 首先將視覺密碼的觀念應用在(K, N)-threshold的門檻使用結構(threshold access structure)上。(K, N)-threshold是定義在N個參與者的集合P = {1, 2, …, N}之上的使用結構，只有疊合K或大於K個參與者的分享影像才可以獲得機密訊息；小於K個參與者則無法獲得任何機密訊息。後來的許多研究都以Naor與Shamir的觀念為基礎，再加以進一步擴充發展[3-5]。Ateniese et al. [4]將(K, N)-threshold的使用結構加以擴充為(Γ_{Qual}, Γ_{Forb}, M)的形式。任何一個合格的集合(qualified set) Y ∈ Γ_{Qual}都可以還原機密影像，而任何一個禁止的集合(forbidden set) X ∈ Γ_{Forb}都無法獲得一絲機密訊息。而視覺密碼的研究中，像素擴展(pixel expansion)與對比是兩個重要的研究主題[6]，其中許多研究是關於如何提高對比的[6, 8]。大部分的視覺密碼方法都使用像素擴展的技巧[3-5, 6-8, 9] 。就分享影像的形式而言，雖然大部分的視覺密碼方法的產出都是雜亂無章的分享影像；然而，有一些視覺密碼方法的產出卻是有意義的影像。雜亂無章的分享影像雖然可以確保安全性，但是卻容易遭受懷疑、竊取與破壞。因此，分享影像本身為有意義影像的秘密分享方式，有其實際的應用價值。Droste [9]提出多機密影像的觀念，使得參與機密分享的N個人中，不同人的組合，可以分享不同的機密訊息。

這些相關的研究主題概括分類如下：

1. **灰階機密影像**：主要是針對灰色機密影像研究其編碼機制。
2. **對比設定**：在視覺密碼的機制中，疊合後還原影像中白色的點與原始機密影像中白色的點相比，其實不是純白，而是半黑半白，遠遠的看會像是灰色，如此會使人對影像的辨識能力降低，此主題是希望能讓黑色與白色的對比落差能越大越好，希望能達成與原始機密影像相同的完美對比。
3. **像素擴張**：Noar 與Shamir 所提機制，因編碼機制的關係，編碼後的投影片會比原始的機密影像還要大，此議題主要希望編碼後的分享投影片能盡量的小，希望能達到與

原始機密影像一樣的大小，即像素無擴張。

綜觀以上所提的議題都是在探討疊合還原的機密影像的視覺密碼機制，然而本研究將針對藏入機密影像的領域提出新的方法，使得兩張分享投影片，可利用旋轉角度，顯示出多張不同的機密影像。

第二章 文獻探討

2.1 視覺機密分享機制

視覺機密分享(Visual Secret Sharing，簡稱：VSS)機制，主要目的是將機密影像P編碼成兩張分享投影片(Shares) S_1和S_2，在P中的每個像素p皆會編碼成兩個分享像素S_1和S_2，由於投影片上黑點和白點重疊會有表2-1 中所列之特性，這裡S_1和S_2疊在一起的結果我們用$S_1 \otimes S_2$來表示。譬如，在表2-1 中第三列，表示當S_1為黑色、S_2為白色，其$S_1 \otimes S_2$的結果為黑色，由表2-1 可觀察出其疊合(⊗)可相當於布林運算中的 “OR”運算。

表2.1 投影片疊合編碼表

S_1	S_2	$S_1 \otimes S_2$
■	■	■
■	□	■
□	■	■
□	□	□

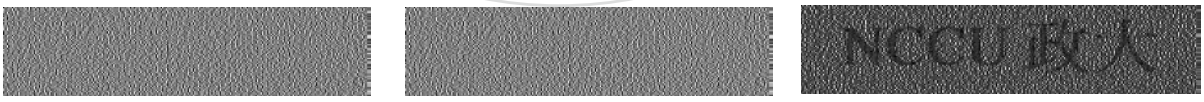
分享影像製成投影片時，白點即為透明的點，黑點則為不透光的點。在解密時，將兩張投影片疊合在一起，若在上方的投影片為白點(即透明無色)則會透出下方投影片的顏色，再根據兩張投影片疊合後所顯示出的影像，利用人的視覺系統分辨出其中的機密影像，即能達成視覺解密的目的。

2.2 (1,2) 、(2,2) 視覺祕密分享機制

視覺安全的原理在於人類視覺系統在辯識影像時，是以像素與周圍像素所產生的對比效果，並且無法清楚的辨識出每一個像素值，只能感覺出來一塊區域的效果。而輸出通常為投影片，黑色像素以全黑看待，黑白影像之白色像素以透明看待，像素重疊的特點：黑點疊合黑點產生黑點,白點疊合黑點產生黑點，白點疊合白點產生白點，黑點疊合白點產生黑點。

2.2.1 (1,2) 視覺祕密分享機制

以Naor 及Shamir[1-2]發表1×2視覺密碼可以發現到每個像素p將會編碼為兩個像素，也就是若機密影像大小為 h × w，編碼完後的分享影像大小為h × 2w，其分享影像的寬長度會等於機密影像寬長度的兩倍，我們將此性質稱其為像素擴張(Pixel Expansion) 。舉例來說機密影像大小為100x100，在編碼完後還原的機密影像大小為100 x200，此時還原後的機密影像會比起原始機密影像看起來會被拉長壓扁如圖2.1所示，然而為了不使還原後的機密影像變形。後來將像素擴張調整為4(=2x2)，來保持還原後影像的長寬比與原始機密影像相同。



(a) (b) (c)

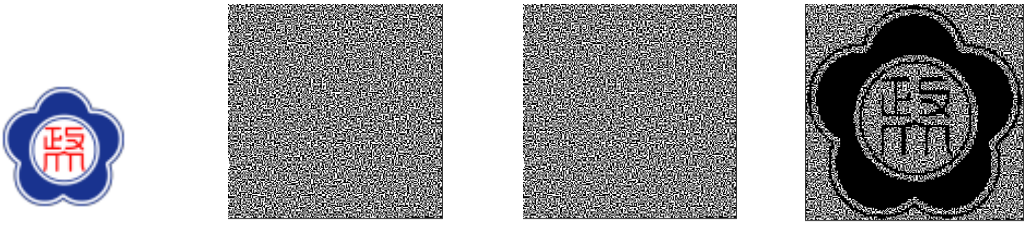
圖 2.1 根據表 2.2 實做 1X2 視覺秘密分享

表 2.2　1x2 視覺密碼編碼表

P	矩陣	S_1	S_2	$r = S_1 \otimes S_2$
□	$M_0=\begin{pmatrix}1&0\\1&0\end{pmatrix}$	■□	■□	■□
		（1，0）	（1，0）	（1，0）
	$M_0=\begin{pmatrix}0&1\\0&1\end{pmatrix}$	□■	□■	□■
		（0，1）	（0，1）	（0，1）
■	$M_1=\begin{pmatrix}1&0\\0&1\end{pmatrix}$	■□	□■	■
		（1，0）	（0，1）	（1，1）
	$M_1=\begin{pmatrix}0&1\\1&0\end{pmatrix}$	□■	■□	■
		（0，1）	（1，0）	（1，1）

2.2.2　(2,2) 視覺祕密分享機制

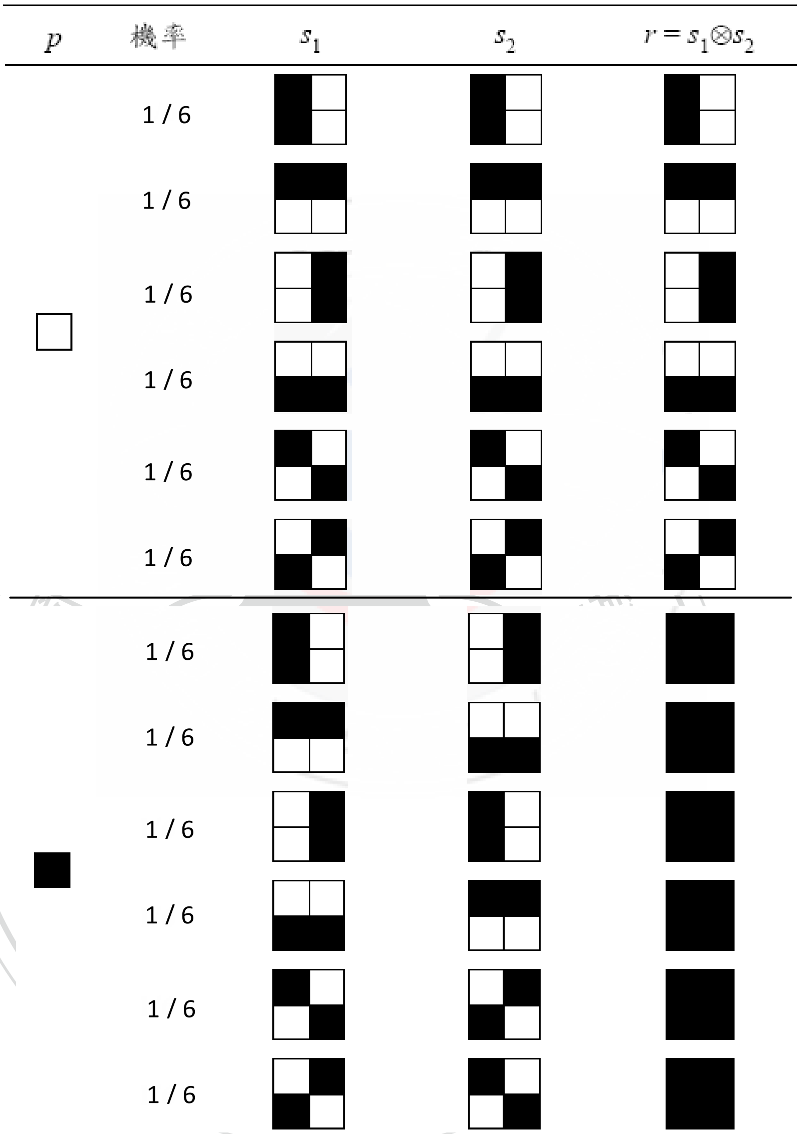
由於像素擴張調整為2x2 後，S_1和S_2將會有六種不同的區塊樣式可供編碼，如表2.3所示。當p為白(黑)點時，將從表2.3 前(後)六列隨機挑選一列來編碼S_1和S_2，且每列挑選到的機率為1/6，其還原像素$r = S_1 \otimes S_2$可由表2.3 最後一行得知，當p為白點時，r則顯示出二黑二白；當p 為黑點時，r 則為全黑(四黑)。如此將P中所有像素皆依此方法編碼，當所有p 皆編碼完成，即可得到兩張完整的分享影像S_1和S_2，而S_1和S_2看起來會像似張雜亂無意義的影像。圖2.2 為根據表2.3 實作後之結果，其圖2.2(a)為機密影像，圖2.2(b)、(c)為編碼後的兩個分享投影片S_1和S_2，這兩張分享投影像看起來像是張雜亂無意義的影像。圖2.2(d)為S_1和S_2疊合後的還原影像，其此還原影像可以明顯看的出來就是圖2.2(a)的機密影像。



(a)P　(b)S_1　(c)S_2　(d) $S_1 \otimes S_2$

圖 2.2　根據表 2.3 實作成果

表 2.3 (2, 2)-VSS 機制實作時所採用之編碼表



2.3 視覺多重機密分享機制

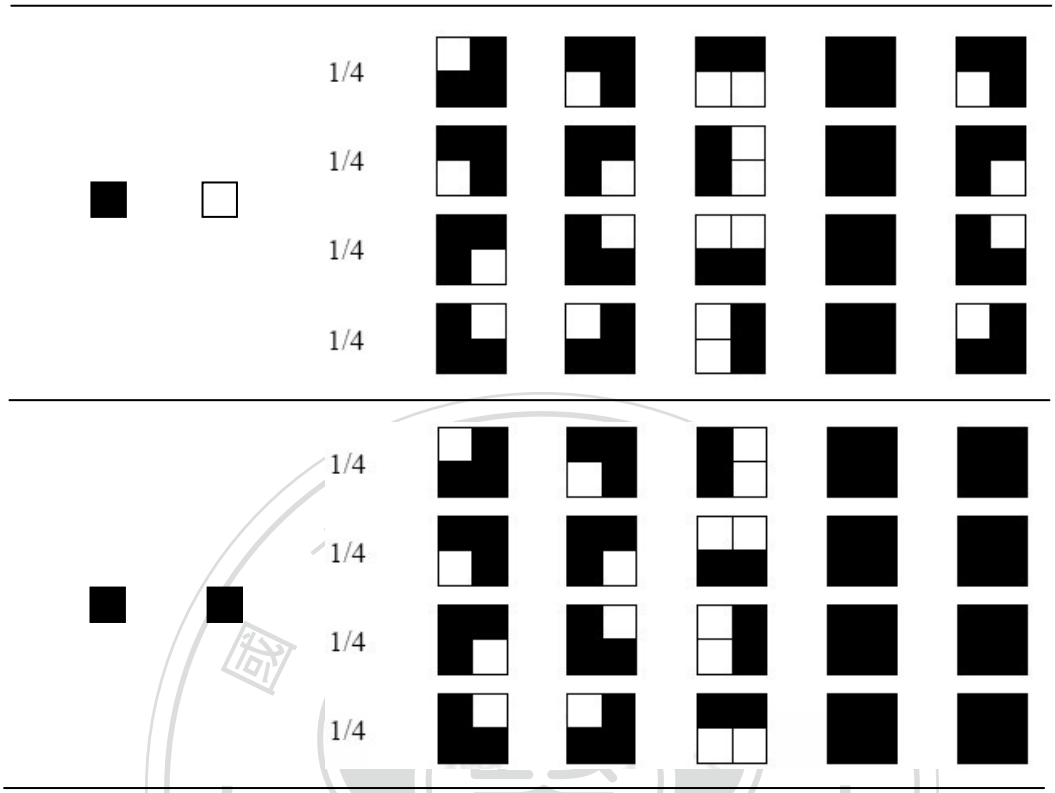
VSS 機制在還原影像時，其分享投影片疊合後皆可還原出一張機密影像。而視覺多重機密分享 (Visual Multi-Secret Sharing，簡稱：VMSS) 機制，則是希望分享投影片的疊合，還原出多種不同的機密影像，令q為可顯示的機密影像個數，其中由兩張分享影像還原出q張機密影像的機制，我們稱(2, q)-VMSS 機制，接下來針對(2, q)-VMSS 機制介紹一些學者所做的相關研究。

2.3.1 旋轉式視覺機密分享機制

1998 年，Wu的碩士論文[10]中，提出一種(2, 2)-VMSS 的編碼機制，可以隱藏兩張機密影像在兩張分享投影片上，也就是給兩張大小N×N的黑白機密影像P_1和P_2，可產生兩張分享投影片S_1和S_2，單看其中一張S_1或是S_2時，無法看出任何有關P_1或P_2的資訊。但當S_1和S_2疊在一起時，可看到P_1的資訊。另外，當S_1逆時針旋轉90°後再和S_2相疊合時則可看到P_2，這裡以$S_1^{90^\circ}$來表示S_1逆時針旋轉90°後的影像。再來考慮兩個對應的像素p_1和p_2，令p_1屬於P_1中座標為 [i, j] 的像素，記作$p_1 \in P_1[i, j]$，令$p_2 \in P_2[u, v]$。當p_1與p_2位於相同座標時(也就是 i = u 且 j = v)，即表示在解密時，還原影像中座標為 [i, j] 的區塊，同時要顯示出p_1，再經過某些角度的旋轉後也要顯示出p_2。如此將p_1和p_2的組合及吳振彰所提之編碼表整理於表2.4。

表 2.4 旋轉式視覺密碼編碼表

p_1	p_2	機率	S_1	$S_1^{90^\circ}$	S_2	$S_1 \otimes S_2$	$S_1^{90^\circ} \otimes S_2$
□	□	1/4					
		1/4					
		1/4					
		1/4					
□	■	1/4					
		1/4					
		1/4					
		1/4					



這裡用個簡單的例子說明旋轉式視覺密碼的編碼方法。假設p_1和p_2的影像大小為8 × 8，而將S_1區分為四個像三角形的區域，如圖2.3(a) 將四個區域用不同的顏色表示，並且以k = I, II, III, IV 來表示各區域，而每個區域皆由2×2的像素區塊所組成，所有像素區塊都各別標上號碼，如圖2.3(b)。在區域k中的第i個像素區塊我們用b_i^k 來表示，其中 i = 1, 2, …, 16。其S_1與S_2的編碼方法如下：編碼分享影像S_1：將區域I內的所有b_j^I 隨機從圖2.3(c)中所列的四個像素區塊任挑選一個填入。而其它區域II、III、IV 內的第i 個像素區塊皆填入同b_j^I 一樣的像素區塊，即$b_j^t = b_j^I$，t = II, III, IV，j = 1, 2, …, 16，如此即可將S_1編碼完成。

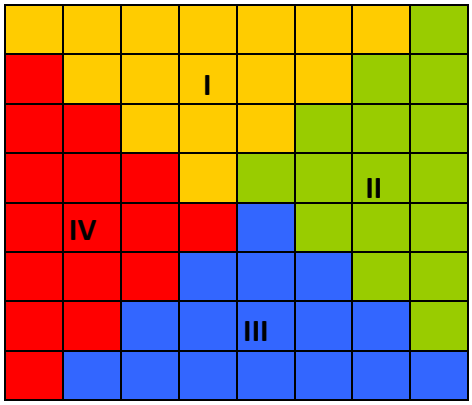


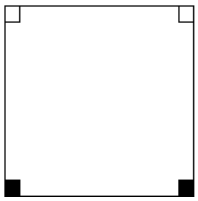
圖 2.3(a) 分割四個區域

1	2	3	4	5	6	7	1
7	8	9	10	11	12	8	2
6	12	13	14	15	13	9	3
5	11	15	16	16	14	10	4
4	10	14	16	16	15	11	5
3	9	13	15	14	13	12	6
2	8	12	11	10	9	8	7
1	7	6	5	4	3	2	1

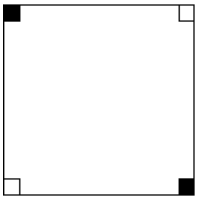
圖 2.3(b) 四個區域區塊標號

圖 2.3(c) 編碼指定四個區塊

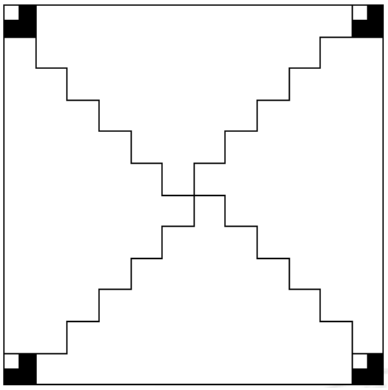
編碼分享影像S_2：S_1編碼完成後，再來根據P_1和P_2如圖2.2(a)、(b)，來編碼S_2。這裡針對右上、左上、左下、右下這四個點，簡單來說明如何編碼S_2，假設$P_1(P_2)$這四個點依序為：□. □. ■. ■ (□. ■. □. ■)，再假設S_1中b_1^l 挑選到 因此b_1^k皆為  ，k= I, II, III, IV，整個S1編碼如圖2.2(c)所示，再編碼S2 前，先看P1和P2 所對應的點有(□. □) (□. ■), (■. □), (■. ■)，由於b_1^k =  其S_2之編碼可以參考表2.1依序編成  、  、  和  (見表2.4 中 1, 5, 9, 13 列)，圖2.4(d) 即為S_2編碼完成的結果。當$S_1 \otimes S_2$時，如圖2.4(e) 所示，可依序用眼睛辨識出 □、□、■、■，當S_1旋轉90°後就如圖2.4 (f) 所示，而$S_1^{90^\circ} \otimes S_2$的結果如圖2.4 (g)，可依序辨識出□、■、□、■。此機制雖然可利用兩張分享投影片，利用旋轉的方式，同時顯示出兩張不同的機密影像，但分享投影片S_1及S_2必需為正方形，礙於分享投影片為正方形其旋轉的角度只可能有0°、90°、180° 和270°，並無法利用其它角度來旋轉。



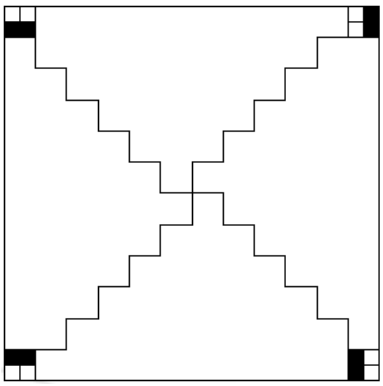
(a) P_1



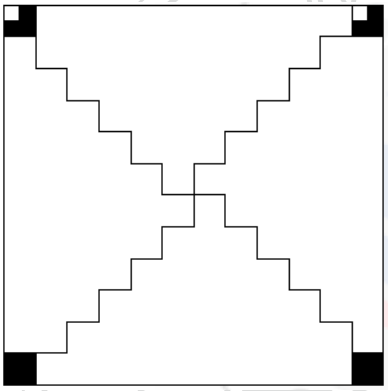
(b) P_2



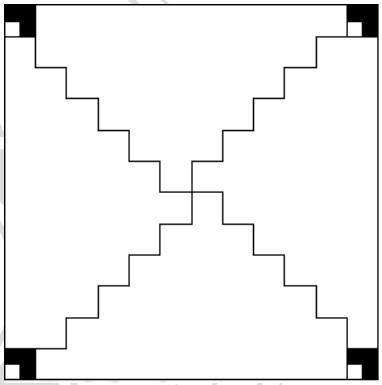
(c) S_1



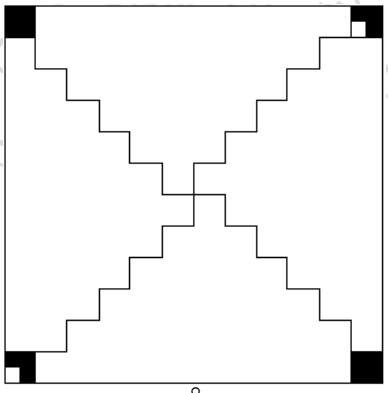
(d) S_2



(e)$S_1 \otimes S_2$



(f) $S_1^{90°}$



(g) $S_1^{90^\circ} \otimes S_2$

圖 2.4 旋轉式視覺密碼機制之編碼範例

2.3.2 平移式視覺秘密分享技術

2001 年，在 Wu 的碩士論文[11]中，提出一種 (2, 2, X)-VSS 的編碼機制，可以隱藏 q 張機密影像在兩張分享投影片上，當給 q 張影像 P_1、P_2、…、P_q，隱藏於兩張投影片 S_1和 S_2，當 S_1以 q 種不同的位置平移且相疊到 S2 則可以看出 q 種不同的機密資訊。

這裡用個簡單範例來的說明平移式視覺秘密如何分享如圖 2.5，假設 X= 2 、分享圖為 S_1和 S_2、兩張機密影像 P_1、P_2，令 P_1為 S_1直接與 S_2疊合之結果如圖 2.6，故 P_1擁有所有機密影像的最大面積 $w \times h$，而 P_2為 S_1向右下方向位移 [x, y] 個座標再與 S_2疊合之結果如圖 2.6，其中 $1 \le w, 1 \le y \le h$，如圖 2.5 所示，故 P_2的機密影像面積為(w-x)×(h-w)。

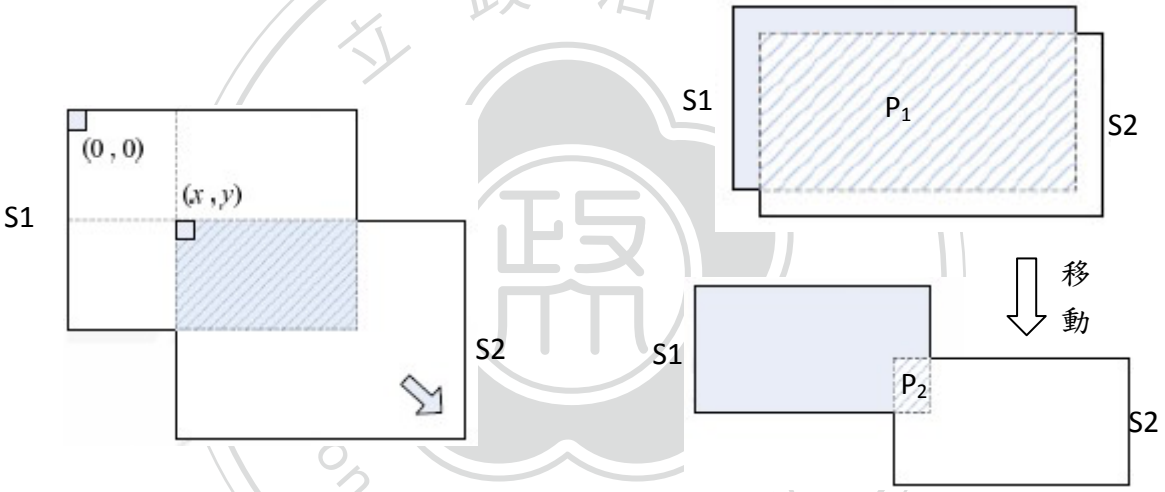


圖 2.5 平移式視覺機密分享　　圖 2.6 Wu 的做法

這裡用個簡單的例子說明 Wu 的平移式視覺密碼，假設有 5 張秘密影像使用 Wu 的編碼機制，並且產生兩張分享投影片 S_1和 S_2。(2, 2, 5)-VSS 編碼方式如下，首先我們需要將每個像素分成五個區塊，S_1像素裡的第一個區塊與 S_2的第一個區塊重疊後適用於第一個影像、S_1像素裡的第二個區塊與 S_2的第二個區塊重疊後適用於第二個影像、因此 S_1、S_2第三、四、五區塊重疊後適用於第三、四、五個影像分別如圖 2.7，每一個機密影像都有它像素裡單獨的區塊。接著選擇五種不同的位置恢復五個機密影像，舉例來說第一個秘密影像解密位置定義(0,0)，則 S_1和 S_2重疊後將解出第一個影像，如果第二個秘密影像解密位置定義(80,100) ，則 S_2向右移動 100 行與向下移動 80 列後與 S_1重疊後將

解出第二個秘密影像如圖 2.8，第三、四、五的秘密影像也將以這方式解出秘密。

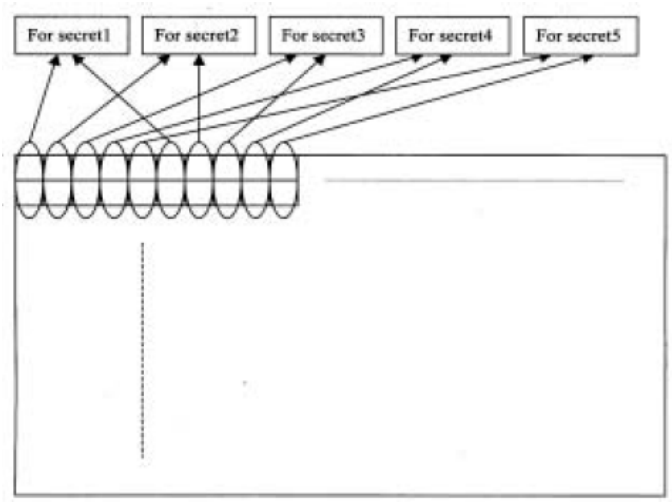


圖 2.7 (2, 2, 5)-VSS 編碼區塊

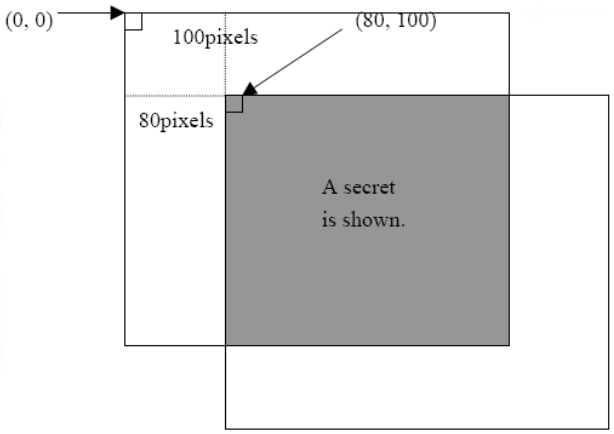


圖 2.8 S_1 和 S_2 在指定位置解出第二張影像

假設我們的秘密影像為 Y、C、N、5、9，使用(2, 2, 5)-VSS 編碼，圖 2.9(a)與(b)為分享影像 S_1 和 S_2，圖 2.9(c) 為 S_1 和 S_2 在(0,0)的位置重疊，圖 2.9(d) 為 S_1 和 S_2 在(100,80)的位置重疊，圖 2.9(e) 為 S_1 和 S_2 在(100,-80)的位置重疊，圖 2.9(f) 為 S_1 和 S_2 在(-100,-80)的位置重疊，圖 2.9(g) 為 S_1 和 S_2 在(-100,80)的位置重疊，實驗成果如下所示：

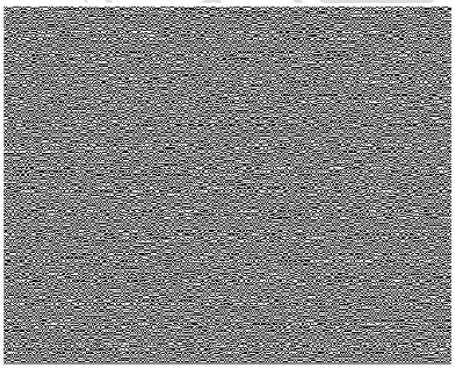


圖 2.9(a) 分享影像 S_1

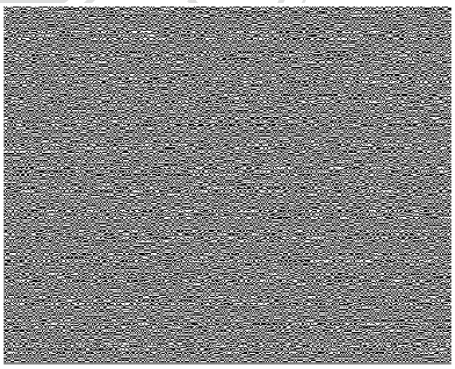


圖 2.9(b) 分享影像 S_2

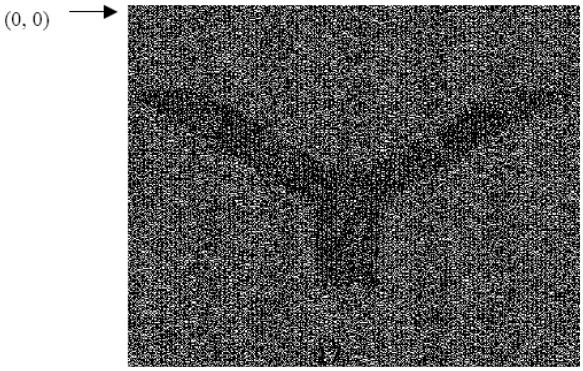


圖 2.9(c) S_1 與 S_2 重疊(0,0)

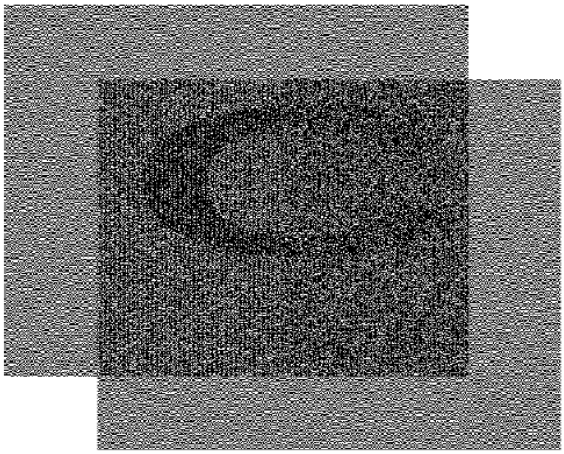


圖 2.9(d) S_1 與 S_2 重疊(100,80)

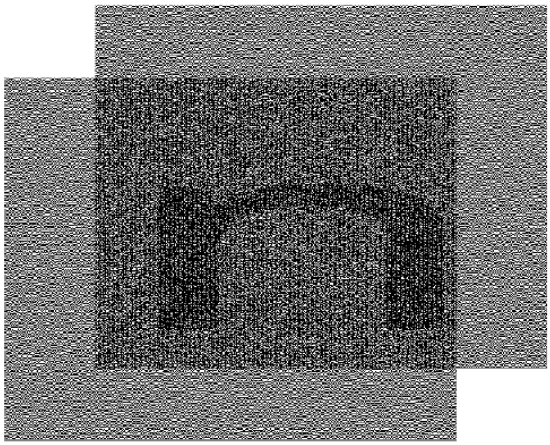


圖 2.9(e) S_1 與 S_2 重疊(100,-80)

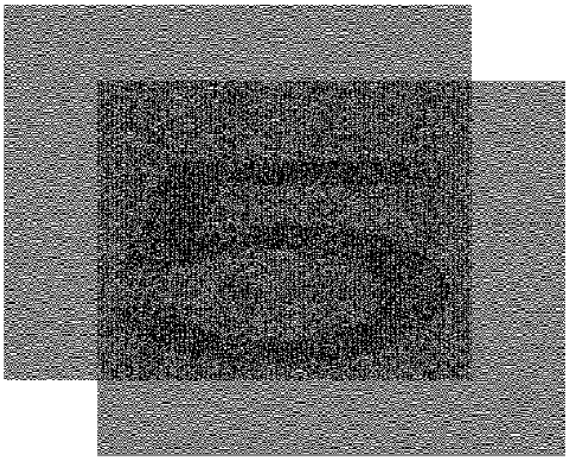


圖 2.9(f) S_1 與 S_2 重疊(-100,-80)

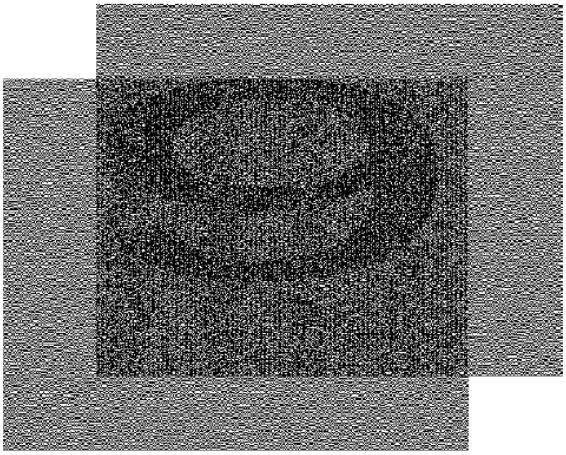


圖 2.9(g) S_1 與 S_2 重疊(-100,80)

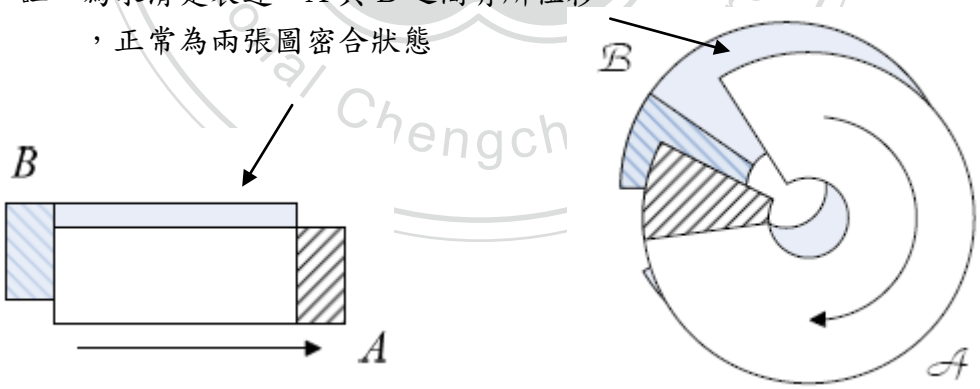
但此機制雖然可將兩張分享投影片以不同的平移方式，疊出 q 種不同機密影像，然而在無重疊到的區域將無法藏入任何機密，因此當平移的範圍越大，疊合的面積就會越小，可隱藏機密的範圍便跟著縮小。

第三章 平移、旋轉為基礎之立體旋轉視覺多重機密分享機制

立體旋轉的視覺密碼的編碼機制，可隱藏 n 張機密影像在兩張分享投影片上，當 n 張影像 S_1、S_2.....S_n，藏於兩張投影片分享圖 A 與分享圖 B，當投影片捲起來時相疊至指定的位置時即可以解出的機密資訊。

3.1 平移與旋轉關係

假設有兩張相同大小的矩形影像 A、B，當 A 向右平移後(如圖 3.1 (a)所示)，A 的最右端與 B 的最左端將無法重疊，若能使 A 的最右端該塊移到 A 之最左端，如此便能使得重疊面積與原圖一樣大。所以我們將 A 與 B 轉換成立體環形影像 A、B (如圖 3.1(b)所示)，當順時針旋轉時，就好像 A 為向右平移一樣，此時在 A、B 無法重疊的區域，在 A、B 就能重疊在一起。平面旋轉正方形影像只能順時針旋轉 4 次，且每次旋轉的角度只能為 90°，而立體環形影像就不受此限制，旋轉角度可在 0°到 360°之間，實際應用上將有更大空間。



(a)矩形影像 A 與 B 向右平移　　(b)立體環型影像 A、B 旋轉

圖 3.1 平移與旋轉關係

3.2 圖例說明如何立體旋轉

我們利用範例圖來說明如何立體旋轉解密方法，假設有 2 張機密影像 S_1 與 S_2，我們將 2 張圖疊合後將 A 與 B 捲起來(如圖 3.2(a))，S_1 為 A 與 B 疊合後解出的第一個秘密(如圖 3.2(b))，而 S_2 的解密方式為解出第一個祕密後，再將 A 向右方向位移 r 個位置，即可解出 S_2 的機密訊息（如圖 3.2(c)）。

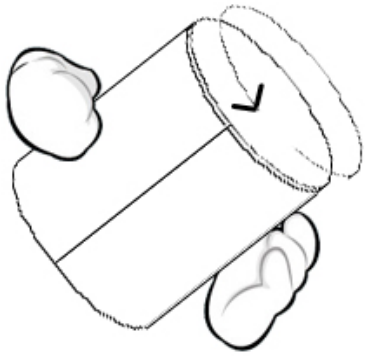


圖 3.2(a)

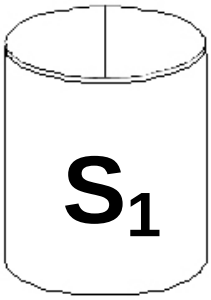


圖 3.2(b)

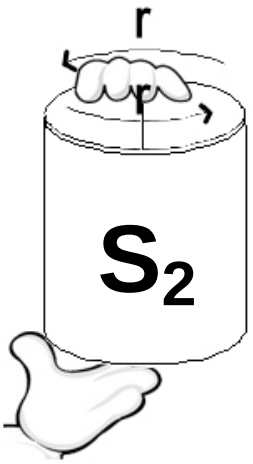


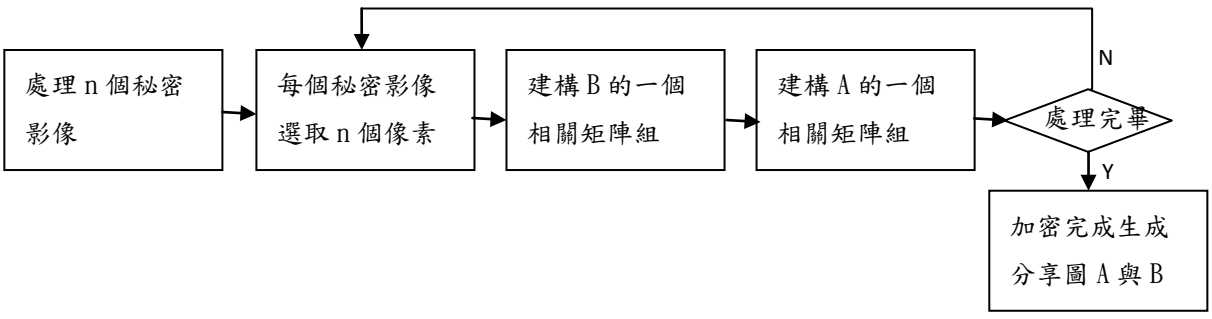
圖 3.2(c) 旋轉 r 位置得機密 S_2

3.3 立體旋轉視覺多重機密基本概念

一般多張視覺密碼方案對祕密影像的多個像素點同時進行加密，一次加密過程處理每個祕密影像的 n 個像素點，即 n^2 像素點，但本方案不同於的是既不是基於基礎矩陣，也不是通過 4 種視覺模式完成旋轉方案的設計，而是通過建構相關矩陣完成加密過程。

3.3.1 建構方法

分享圖中的 2×n 的矩陣對應著秘密影像的一個像素點，所以秘密圖像也可以劃分 n 個區域而一次加密過程涉及 n^2 像素點，整個加密操作流程如下圖



3.3.2、立體旋轉視覺多重機密基本概念

假設待加密的圖像為 S_1、S_2..... S_n，在本文的方案中，分享圖 A 與 B 都由 m × n 的像素區塊組成，每個像素區塊使用 2xn 的布林矩陣來表示，一個像素區塊對應秘密圖像中的一個像素，其中像素區塊在解密時，兩個產生的分享圖像 A 和 B 需要首尾接成環形，通過固定 B 且旋轉 A 不同的角度來恢復不同的祕密圖像。

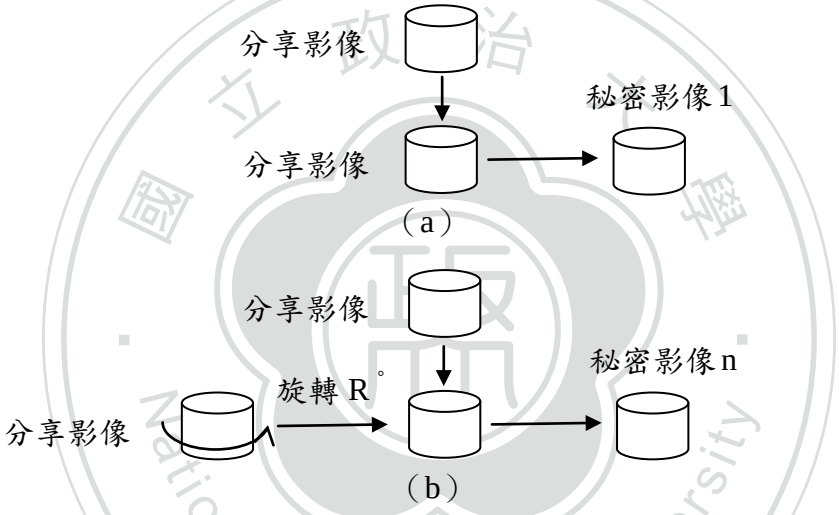


圖 3.3 立體旋轉解密過程

3.3.3 立體旋轉視覺多重機密方式

本研究所能隱藏的（最多）秘密影像個數由秘密影像之像數而定。若秘密影像之像數值為 m × n，則本研究方法將最多可影藏 n 個秘密影像。令視覺密碼白像素的影像為 0，黑像素的影像為 1，提案方式之詳細演算法如下：

Input: n 個秘密影像, $S_0, S_1, S_2, \cdots, S_{n-1}$. 每個秘密影像由 m × n 個像數所組成。
Output: 分享影像 A 及 B. A 及 B 由 $2m \times n^2$ 個像數所組成。

符號定義

定義一：$S_t^{(i,j)}$為第 t 個秘密影像的第 i 行 j 列之像數, $0 \le t \le n-1$, $0 \le i \le m-1$, $0 \le j \le n-1$。

$S_t^{(0,0)}$	$S_t^{(0,1)}$	...	$S_t^{(0,n-1)}$
$S_t^{(1,0)}$	$S_t^{(1,1)}$	...	$S_t^{(1,n-1)}$
...	...	...	...
$S_t^{(m-1,0)}$	$S_t^{(m-1,1)}$	...	$S_t^{(m-1,n-1)}$

圖 3.3 第 t 個秘密影像像數之排列方式

定義二：$A_{(i,j)}$指在分享影像 A 中，對應到秘密影像 S_l 的第 i 行 j 列之像數區塊，其區塊大小為 2 x n。(如圖 3.4)

1	2	...	n
n+1	n+2	...	2n

圖 3.4 第 i 行 j 列之像數區塊

定義三：$B_{(i,j)}$ 指在分享影像 B 中，對應到秘密影像 S_l 的第 i 行 j 列之像數區塊，其區塊大小為 2 x n。(如圖 3.4)

定義四：$A_{(i,j)}^{(u,v)}$ 指在 $A_{(i,j)}$區塊中之第 u 行 v 列之像數, $0 \le u \le 1$, $0 \le v \le n-1$(如圖 3.5)

$A_{(i,j)}^{(0,0)}$	$A_{(i,j)}^{(0,1)}$	$A_{(i,j)}^{(0,2)}$	....	$A_{(i,j)}^{(0,n-1)}$
$A_{(i,j)}^{(1,0)}$	$A_{(i,j)}^{(1,1)}$	$A_{(i,j)}^{(1,2)}$	....	$A_{(i,j)}^{(1,n-1)}$

圖 3.5 $A_{(i,j)}$區塊第 u 行 v 列之像數編號

定義五：$B_{(i,j)}^{(u,v)}$ 指在 $B_{(i,j)}$區塊中之第 u 行 v 列之像數，$0 \le u \le 1$，$0 \le v \le n-1$(如圖 3.6)

$B_{(i,j)}^{(0,0)}$	$B_{(i,j)}^{(0,1)}$	$B_{(i,j)}^{(0,2)}$	....	$B_{(i,j)}^{(0,n-1)}$
$B_{(i,j)}^{(1,0)}$	$B_{(i,j)}^{(1,1)}$	$B_{(i,j)}^{(1,2)}$	....	$B_{(i,j)}^{(1,n-1)}$

圖 3.6 $B_{(i,j)}$區塊第 u 行 v 列之像數編號

執行步驟：

Step 1: 在分享影像 A 與 B 中,將秘密影像的每個像數擴張為 2 × n 個像素，每個 2 × n 的像素即為一個區塊。

Step 2: 令 i=0，t=0，然後對所有 $A_{(i,j)}$及 $B_{(i,j)}$區塊執行以下步驟。

Step 3: 從集合{0,1,2,…,n-1}中隨機選取 n 個值,$r_0, r_1, \cdots, r_{n-1}$。其中，$r_\alpha \neq r_\beta$當 $\alpha \neq \beta$ 時，$0 \le \alpha \neq \beta \le n-1$。

Step 4: For $0 \le j \le n-1$，從{0,1}中隨機選取一值予 u_j ，並在每個 $B_{(i,j)}$區塊中，給定像數 $\mathbf{B}_{(i,j)}^{(u_j,r_j)} = 0$，其餘為 1。

Step 5: For $0 \le j \le n-1$，set $\mathbf{A}_{(i,j)}^{(u_{j+t \,(\mathrm{mod}\, n)}, r_{j+t \,(\mathrm{mod}\, n)})} \leftarrow S_t^{(i,j)}$

Step 6:Set t=t+1, if t<n, 條件不符回到步驟 5，條件符合執行步驟 7

Step 7:Set i=i+1, if i<n, 條件不符回到步驟 5，條件符合執行步驟 8

輸出分享影像 A 及 B

將分享影像 A 與 B 疊合，可得秘密影像 S_l

將分享影像 B 左旋 t 個區塊後與 A 疊合，可得秘密影像 S_t

第四章範例示範與實驗結果

4.1 範例示範

以下加密 3 個秘密影像 S_0=｛1,0,1｝、S_1=｛1,1,0｝、S_2=｛0,1,0｝，首先從集合{0, 1, 2}中隨機選取 3 個值, 取出的值為 r_0=2, r_1=0, r_2=1，根據加密規則產生分享圖 A 與 B，最後重疊 R(A, C)(0≤ C ≤3)和分享圖 B 完成解密過程，過程如圖 4.1 所視。

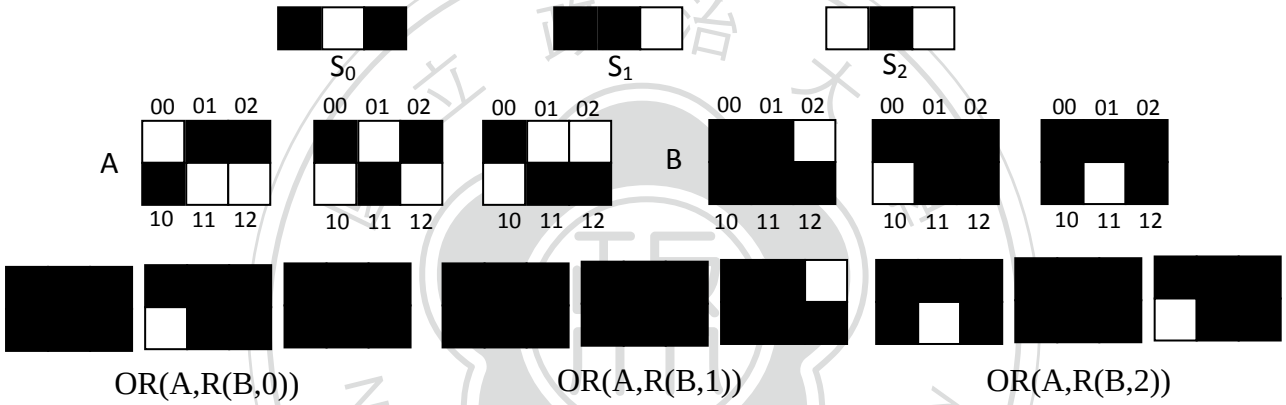


圖 4.1 加密 3 幅秘密影像的例子

4.2 實驗結果

本章將針對本論文提出的研究方法之實作結果呈現，對實作結果進一步探討。

本實驗用3張30×60 pixels的影像（圖4.2）當作秘密影像，再根據我們的研究方法產生2張分享圖像A與B（圖4.3）。固定B旋轉A不同的角度{ 0°、45°、135°}即可恢復機密影像。首先將分享影像A與分享影像B做疊合，即可恢復原秘密影像S_1（圖4.4）；若固定影像B且旋轉影像A角度45°後的影像做疊合，即可還原秘密影像S_2（圖4.5），若固定影像B且旋轉影像A角度135°後的影像做疊合，即可還原秘密影像S_3(圖4.6)。

圖 4.2 秘密影像 S_1、S_2、S_3

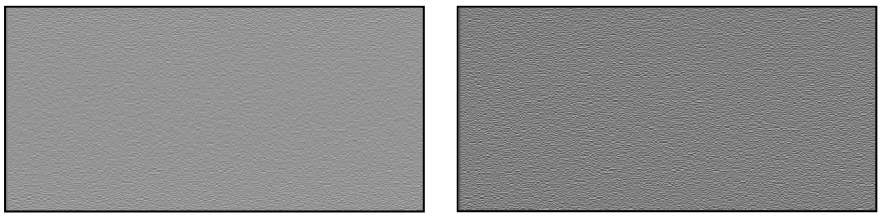


圖 4.3 分享影像 A 與 B

圖 4.4 解密後秘密影像 S_1

圖 4.5 旋轉 45° 解出秘密影像 S_2

圖 4.6 旋轉 135° 解出秘密影

第五章 結論

本文提出的一種基於立體旋轉的視覺秘密分享技術，首先，先對影像轉換成二元黑白影像，並調整每一區塊黑點數量，之後再將二元黑白影像透過平移環型角度分享方式，分解成兩張不具任何意義的二元圖。由我們的實驗結果發現，兩張偽裝影像中，任何人皆無法從自身得到的單張偽裝影像獲得隱藏資訊，在安全性中有不錯的效果，期許將來可改良為彩色型立體旋轉的視覺秘密分享研究，做為未來的研究方向。

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.

[3] Ateniese, G., Blundo, C., De Santis, A. and Stinson, D. R., "Constructions and Bounds for Visual Cryptography," In 23rd International Colloquium on Automata, Languages and Programming (ICALP '96), Springer-Verlag, 1996a: pp. 416-428.

[4] Ateniese, G., Blundo, C., De Santis, A. and Stinson, D. R., "Visual Cryptography for General Access Structures," Information and Computation (129:2), 1996b: pp. 86-106.

[5] Ateniese, G., Blundo, C., De Santis, A. and Stinson, D. R., "Extended Capabilities for Visual Journal of Information, Technology and Society 2003(2) 37 Cryptography," Theoretical Computer Science (250:1-2), 2001: pp. 143-161.

[6] Blundo, C., De Bonis, A. and De Santis, A., "Improved Schemes for Visual Cryptography," Designs, Codes and Cryptography (24), 2001: pp. 255-278.

[7] Blundo, C. and De Santis, A., "Visual Cryptography Schemes with Perfect Reconstruction of Black Pixels," Computer & Graphics (12:4), 1998: pp. 449-455.

[8] Blundo, C., De Santis, A. and Stinson, D. R., "On the Contrast in Visual Cryptography Schemes," Journal of Cryptology (12:4), 1999: pp. 261-289.

[9] Droste, S., "New Results on Visual Cryptography," In Advances in Cryptology-CRYPTO '96, Springer-Verlag, 1996: pp. 401-415.

[10]C.C. Wu, "A Study on Visual Cryptography," Master thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C, 1998.

[11]T.L. Wu, "Two New Visual Cryptography Schemes: Visual Multi-Secrets Sharing Scheme And Colored Visual Secret Sharing Scheme," Master thesis, Department of Computer Science and Information Engineering, National Dong Hwa University, Taiwan, R.O.C, 2001.