具完美對比之(2,n)視覺秘密分享機制

李南逸
南台科技大學 資訊管理系
教授
e-mail：nylee@mail.stut.edu.tw

黃資真
南台科技大學 資訊管理系
碩士研究生
e-mail:m9690106@webmail.stut.edu.tw

摘要

傳統密碼學通常需要複雜運算以對資料進行保護，並防止機密資料的外洩。在 1994 年 Naor 與 Shamir 提出視覺秘密分享機制，最大特色是在解密時，只需利用人類視覺系統來解密機密資訊，所以不需任何運算。目前視覺秘密分享機制中，常用半色調技術先對灰階或彩色影像進行處理，因此在重疊影像時，難以達成完美對比。本文擬提出(2,n)視覺秘密分享機制，運用二進位轉換、亂數與布林運算來分享機密影像，在重疊影像時可產生完美對比，以達到最佳辨識效果。

關鍵字：視覺密碼、視覺秘密分享機制、加密、影像分享

Abstract

Traditional cryptography usually involves complex operations on data protection in order to prevent the leakage of confidential information. Naor and Shamir first proposed visual secret sharing scheme in 1994. The main characteristic on decipherment is to decode confidential information by human's visual system. So, it does not need any computation. VSS often uses half toning technology to deal with gray images or color images, but it cannot provide perfect contrast. This paper proposes (2,n) visual secret sharing scheme, which uses bit-level decomposition, random numbers and Boolean operations to share secret images. Our scheme provides perfect contrast to enhance the result of distinguishability.

Keywords: Visual cryptography; Visual secret sharing scheme; Encryption; Image sharing

1. 前言

近年來，網際網路的發達，導致多媒體的傳送相當普遍，且隨著電子商務的來臨，如何在開放的網際網路中，確保多媒體資料的安全，變成相當重要的議題。

傳統密碼學中，加密技術是目前最常被運用來保護資料安全的方法。經由複雜的數學運算來進行加密產生密文，必須透過正確金鑰（Key）才能將密文進行解密還原原本資料。因此資料加密後，即使被未授權者盜取，也因沒有解密金鑰，而無法取得原始資料，因此可以達到資料保密的目的。但傳統密碼學的缺點是必須運用大量且複雜的數學運算，因此無論加解密都必須運用電腦來輔助。

Naor 與 Shamir [7]在 1994 年提出了一套新的技術，稱為視覺密碼（Visual Cryptography）。其最大特色就是還原秘密影像時不需做任何運算，而透過人類視覺系統從重疊影像中，直接解讀機密資訊。最初是運用在黑白影像上，稱為視覺秘密分享機制(Visual Secret Sharing Scheme, VSS) [2,4,5,7,10]，指機密影像會分成 n 張分享影像，並授權給 n 個成員，每個人一張。只要有 k 個以上成員將影像重疊，便可得出原來的機密影像，相反的；當小於 k 張分享影像時，將無法得到任何資訊。

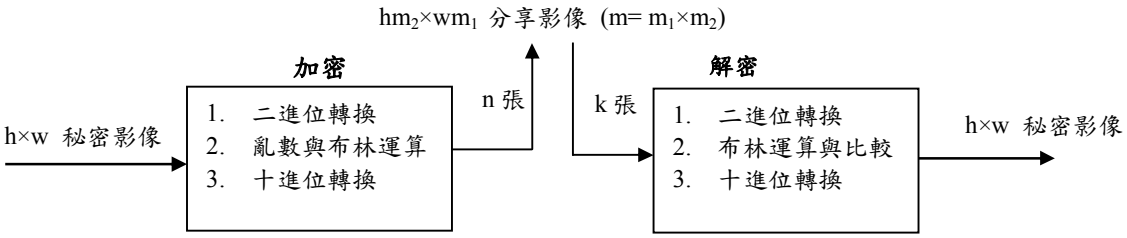
傳統視覺秘密分享機制只用於黑白影像，現今則擴大至灰階影像與彩色影像，主要先利用半色調技術處理[2,3,5,6]，將影像變成二進位影像，再經由視覺密碼技術去加密，產生分享影像，可是重疊後的影像無法達到完美的對比。

目前有些學者[1,8-10]主要在研究如何將重疊後的對比提升，讓人類視覺系統可以很清楚的分辨出訊息，其中，在 2005 年 Lukac 與 Platantions [4]提出的演算法可達到完美對比，可是在恢復影像資訊時，需要少許計算量，且必須自行建構 codebook，然自訂 codebook 必須考量所建構 codebook 是否安全，若不安全，則可能讓攻擊者有機會取得秘密資訊。而且依照分享的 n 不同，每個 codebook 就會不一樣，導致使用上不方便。

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

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

圖一：(2,2)VSS 的 codebook



圖二：Lukac-Platantions 演算法流程圖

用於黑白影像、灰階影像與彩色影像，主要運用[4]與[8,9]的概念。首先會將每個像素進行二進位轉換，再利用亂數與布林運算的方式將資料進行加密，擴張產生 m 個子像素。在重疊影像時，則將分享影像利用布林運算恢復成原始影像大小以產生完美對比。

2.研究背景

2.1 Lukac-Platantions 演算法

Lukac 與 Platantions [4]提出(k,n)秘密分享機制可用於各種影像中，此分享機制主要依 codebook 的不同來進行編碼，在此以(2,2)VSS 來介紹，首先將每個像素進行二進位轉換，因此每個像素會轉換成 8 位元，然後自訂 codebook [7]（如圖一），當位元為 1 時，則從 C1 中取得一組來進行編碼;若當位元為 0 時，則從 C0 中取得一組來進行編碼，因此每個位元會擴張為 4 位元，最後再反轉為十進位，而每個像素將會擴張成 4 個像素。解密是先將分享影像轉換為二進位資料,再進行 AND 運算，若擴張後之 4 個位元總和為 0,則此位元為 0，若總和大於或等於 1，則此位元為 1，最後再進行十進位轉換，恢復回原始影像（如圖二）。

2.2 Wang 等人的(2,n)VSS 演算法

Wang 等人 [8,9]提出（2,n）視覺秘密分享機制可使用於黑白影像、灰階影像與彩色影像，此方法基於布林運算（Boolean Operations）中 XOR 和 AND 運算，且利用亂數來產生分享影像。此方法先假設輸入一個整數 n 與一張秘密影像 A，輸出 n 個$A_1,\dots,A_n$之分享影像，而建構與恢復方法如下：

建構方法：

1. 產生 n+1 個亂數影像$B_1,\dots,B_{n+1}$。
2. 計算 n 個中間值$C_1,\dots,C_n$：
   $C_i=B_i\&A$，其中$i=1,\dots,n$。
3. 計算 n 個分享影像$A_1,\dots,A_n$：
   $A_i=B_{n+1}\oplus C_i$，其中$i=1,\dots,n$。

恢復方法：

$A'=A_i\oplus A_j$，且$i,j\in\{1,2,\dots,n\}$與$i\neq j$ 。

3.本論文的方法

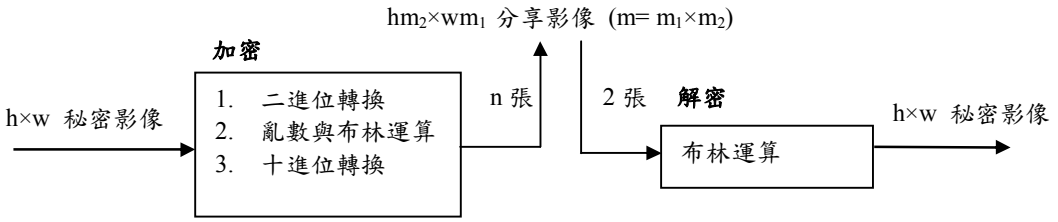
我們所提出來的(2,n)視覺秘密分享機制，乃植基於[4]及[8,9]兩種概念上，可使用於黑白影像、灰階影像與彩色影像。首先我們會輸入一張秘密影像並進行二進位轉換，然後進行亂數與布林運算來進行加密，最後再反轉為十進位資料。解密時，我們只用布林運算來進行重疊，流程如圖三。

3.1 符號定義

本文所使用之符號定義，如表一。

3.2 加密演算法

本文提出之加密演算法是建立在[4]及[8,9]兩種技術上，首先會利用[4]的概念對每個像素進行二進位轉換成 0 或 1，再用[8,9]的概念針



圖三：所提方法之流程圖

表一：符號定義

符號	說明
S	秘密影像。
$h \times w$	影像之像素總數，其中 h 為影像的高，w 為影像的寬。
n	分享影像數目，其中$n \geq 2$。
$P_{(i,j)}$	影像中第 i 列與第 j 行的像素，其中$1 \leq j \leq h$，$1 \leq i \leq w$。
m	原始影像中每個像素將會擴張成 m 個像素，在每張分享影像中（$m = m_1 \times m_2$，m_1為影像寬擴張像素，m_2為影像高擴張像素）。
$P_{(i,j,b)}$	$P_{(i,j)}$經二進位轉換成 8 位元之資料中，第 b 個位元，其中$1 \leq j \leq h$，$1 \leq i \leq w$，$1 \leq b \leq 8$。
Ran(m)	產生 m 個位元亂數之函數。
$C_{(i,j,b)}^{k}$	對第 i 列、第 j 行、第 b 位元，利用 *Ran(m)*產生 n 個亂數$C_{(i,j,b)}^{k}$，其中$1 \leq k \leq n$，$1 \leq b \leq 8$，$1 \leq j \leq h$，$1 \leq i \leq w$。
$C_{(i,j,b)}^{k,v}$	在$C_{(i,j,b)}^{k}$中之第 v 個位元，其中$1 \leq k \leq n$，$1 \leq b \leq 8$，$1 \leq j \leq h$，$1 \leq i \leq w$，$1 \leq v \leq m$。
A^k	第 k 張分享影像，其中$1 \leq k \leq n$。
$A_{(x,y)}^{k}$	第 k 張分享影像中第 x 列與第 y 行像素，其中$1 \leq y \leq h \times m_2$，$1 \leq x \leq w \times m_1$，$1 \leq k \leq n$。
$X_{(x,y)}$	每張分享影像中第 x 列與第 y 行的像素利用 AND 重疊找出相同值，其中$1 \leq y \leq h \times m_2$，$1 \leq x \leq w \times m_1$。
$D_{(x,y)}$	用$X_{(y,x)}$對每張分享影像中第 x 列與第 y 行的像素進行 XOR 的值，其中$1 \leq y \leq h \times m_2$，$1 \leq x \leq w \times m_1$。

對每個位元去產生亂數值，經過布林運算後，產生 m 個位元，而這些位元即為每張分享影像所擴張像素的二進位的值，再將之反轉為十進位的數值後，即可得分享之影像資料。所有加密演算法過程如下步驟：

輸入：一個整數 n 與秘密影像 S

輸出：$A^1, \ldots, A^n$為分享影像

Step 1：計算擴張 m 個像素值。

(a) 若$2 \leq n < 4$，則$m = n$。

(b) 若$4 \leq \mathrm{n} < 2^4$，則$m = 4$。

(c) 若$2^i \leq n$，則 m=i+1，其中$i \geq 4$。

Step 2：將秘密影像 S 的像素$P_{(i,j)}$進行二進位轉換，可得 $P_{(i,j,b)}$，其中 $1 \leq j \leq h$，$1 \leq i \leq w$，$1 \leq b \leq 8$。

Step 3：針對每個位元$P_{(i,j,b)}$，利用$Ran(m)$產生 n 個亂數$C_{(i,j,b)}^{k}$，其中$1 \leq k \leq n$，$1 \leq b \leq 8$，$1 \leq j \leq h$，$1 \leq i \leq w$，且$Ran(m)$所產生的亂數不得重複。

(1) 先產生一個 m 位元亂數 *I=Ran(m)*。

(2) 根據$P_{(i,j,b)}$的值做以下計算：

(a) 若$P_{(i,j,b)} = 0$，則$C_{(i,j,b)}^{k} = I$。

(b) 若$P_{(\mathrm{i,j,b})} = 1$，則 $C_{(i,j,b)}^{k} = Ran(m) \oplus I$。

Step 4：$C_{(i,j,b)}^{k}$有 m 個位元，取出第 v 個

位元$C_{(i,j,b)}^{k,v}$，將此 b 位元連結在一起，如$C_{(i,j,8)}^{k,v}C_{(i,j,7)}^{k,v}C_{(i,j,6)}^{k,v}C_{(i,j,5)}^{k,v}C_{(i,j,4)}^{k,v}C_{(i,j,3)}^{k,v}C_{(i,j,2)}^{k,v}C_{(i,j,1)}^{k,v}$，再進行十進位轉換成$A_{(x,y)}^{k}$，其中$1 \le k \le n$，$1 \le b \le 8$，$1 \le j \le h$，$1 \le i \le w$，$1 \le \mathrm{v} \le \mathrm{m}$，$1 \le \mathrm{y} \le \mathrm{h} \times \mathrm{m}_2$，$1 \le \mathrm{x} \le \mathrm{w} \times \mathrm{m}_1$。

我們以（2,4）VSS 為例，來解釋整個加密演算法流程，假設秘密影像之第 1 個像素為$P_{(1,1)}$ =148，則流程如下：

Step 1：因n=4，可得知 m=4。

Step 2：將$P_{(1,1)}$進行二進位轉換，148=10010100_2，故$P_{(1,1,8)}$=1、$P_{(1,1,7)}$ =0、$P_{(1,1,6)}$ =0、$P_{(1,1,5)}$=1、$P_{(1,1,4)}$=0、$P_{(1,1,3)}$=1、$P_{(1,1,2)}$=0、$P_{(1,1,1)}$=0。

Step 3：針對每個位元$P_{(1,1,b)}$，利用$Ran(m)$產生 4 個亂數$C_{(1,1,b)}^{k}$，其中$Ran(m)$所產生亂數不得重複。

(1) 先產生 I=0010。

(2) 因$P_{(1,1,8)} = 1$，則

$$C_{(1,1,8)}^{1} = Ran(m) \oplus I = 0000 \oplus 0010 = 0010、$$

$$C_{(1,1,8)}^{2} = Ran(m) \oplus I = 1000 \oplus 0010 = 1010、$$

$$C_{(1,1,8)}^{3} = Ran(m) \oplus I = 1111 \oplus 0010 = 1101、$$

$$C_{(1,1,8)}^{4} = Ran(m) \oplus I = 0001 \oplus 0010 = 0011，$$

其他位元同理，其中$1 \le k \le 4$，$1 \le b \le 8$，$1 \le j \le h$，$1 \le i \le w$。

Step 4：若 v=4，則取出$C_{(1,1,b)}^{1}$中第 4 個位元連結在一起，再轉成十進位，如

$C_{(1,1,8)}^{1}$={ 0010 }、$C_{(1,1,7)}^{1}$={ 0000 }、$C_{(1,1,6)}^{1}$={ 1001 }、$C_{(1,1,5)}^{1}$={ 0101 }、$C_{(1,1,4)}^{1}$={ 0101 }、$C_{(1,1,3)}^{1}$={ 1110 }、$C_{(1,1,2)}^{1}$={ 1011 }、$C_{(1,1,1)}^{1}$={ 1101 }，則第 1 個擴張像素二進位為$C_{(1,1,8)}^{1,4} \dots C_{(1,1,1)}^{1,4}$={ 00100111 }，再進行十進位轉換可得$A_{(1,1)}^{1}$=39。

3.3 解密演算法

解密演算法主要利用簡單布林運算，來進行解密。首先將 2 張分享影像作 AND 運算（&）計算出相同值，再利用此值對每張分享影像進行 XOR 運算（⊕），最後再取得擴張 m 個像素做 OR 運算（|），還原成原始秘密影像，過程如下：

輸入：分享影像A^l, A^k，且$l, k \in \{1,2,\dots,n\}$與$l \ne k$

輸出：S

Step 1：$X_{(y,x)}$為 2 張分享影像作 AND 運算後所得之值，$X_{(y,x)} = A_{(y,x)}^{l} \& A_{(y,x)}^{k}$。

Step 2：$D_{(y,x)}$為每張分享影像與$X_{(y,x)}$做 XOR 運算，再作 OR 運算後，所得之值，$D_{(y,x)} = \left(A_{(y,x)}^{l} \oplus X_{(y,x)}\right) | \left(A_{(y,x)}^{k} \oplus X_{(y,x)}\right)$。

Step 3：再將$D_{(y,x)}$作 OR 運算，恢復成原始秘密影像，$P_{(i,j)} = (D_{(i,j)} | D_{(i,j+1)} | \dots | D_{(i+m_2,j+m_1-1)} | D_{(i+m_2,j+m_1)})$，其中$1 \le y \le h \times m_2$，$1 \le x \le w \times m_1$，$1 \le j \le h$，$1 \le i \le w$。

本文以（2,4）VSS 為例，假如秘密影像之像素$P_{(1,1)}$=148，經由 3.2 節加密演算法產生每張分享影像，將會擴張成 4 倍，如表二。而本文從表二中，選擇分享影像 2 與 4 的像素來進行解密，計算過程如下：

Step 1：

$$X_{(1,1)} = 183\&51 = 10110111_2\&00110011_2 = 00110011_2 = 51$$

$$X_{(1,2)} = 29\&13 = 00011101_2\&00001101_2 = 00001101_2 = 13$$

$$X_{(2,1)} = 146\&150 = 10010010_2\&10010110_2 = 10010010_2 = 146$$

$$X_{(2,2)} = 63\&187 = 00111111_2\&10111011_2 = 00111011_2 = 59$$

Step 2：

$$D_{(1,1)} = (183 \oplus 51) | (51 \oplus 51) = (10110111_2 \oplus 00110011_2) | (00110011_2 \oplus 00110011_2) = 10000100_2 = 132$$

$$D_{(1,2)} = (29 \oplus 13)|(13 \oplus 13)$$
$$= (00011101_2 \oplus 00001101_2)| (00001101_2 \oplus 00001101_2)$$
$$= 00010000_2 = 16$$
$$D_{(2,1)} = (146 \oplus 146)|(150 \oplus 146)$$
$$= (10010010_2 \oplus 10010010_2)| (10010110_2 \oplus 10010010_2)$$
$$= 00000100_2 = 4$$
$$D_{(2,2)} = (63 \oplus 59)|(187 \oplus 59)$$
$$= (00111111_2 \oplus 00111011_2)| (10111011_2 \oplus 00111011_2)$$
$$= 10000100_2 = 132$$

Step 3：故

$$P_{(1,1)} = (D_{(1,1)}|D_{(1,2)}|D_{(2,1)}|D_{(2,2)})$$
$$=132|16|4|132$$
$$= 10000100_2|00010000_2| 00000100_2|10000100_2$$
$$=10010100_2 = 148$$

表二：4 張分享影像中由$P_{(1,1)}$擴張後之像素

像素 / 分享影像	$A_{(1,1)}$	$A_{(1,2)}$	$A_{(2,1)}$	$A_{(2,2)}$
1	39	29	134	59
2	183	29	146	63
3	179	141	2	171
4	51	13	150	187

3.4.實驗結果

用(2,4)VSS 進行實驗如圖四，假設輸入一張 256×256 像素 Lena 灰階影像如（a），產生四張 512×512 像素分享影像分別為(b)(c)(d)(e)，假設使用分享影像（I）(II）進行重疊可產生（f）之影像，分享影像（III）(IV）進行重疊可產生（g）之影像。

4.安全性分析與比較

4.1 安全性分析

本研究所提之方法，是將秘密影像像素進行二進位轉換，在對每個位元產生 m 個位元的亂數並且利用 XOR 運算進行加密。如果是合法成員取得兩張分享影像，則會利用分享影像，進行布林運算，恢復成原始秘密影像。如果是攻擊者得到任何一張分享影像，是無法取得秘密影像的。因為分享影像中的值是利用亂數函數產生，所以分享影像中的值是無法預測的，因此攻擊者無法從分享影像中取得秘密影像，而達成高安全性之保護。

4.2 比較

本研究和 Yang [10]的(2,n)ProbVSS、Wang 等人 [8,9] 的 (2,n)VSS 與 Lukac-Platantions [4](2,n)VSS 方案進行比較。首先針對對比 α 進行比較，如表三。Yang 學者是利用機率的方式進行編碼，因此當分享影像越多，則對比效果相對變得越差。Wang 等人學者所提之方法，假設以黑白影像來進行分享，將所產生 2 張分享影像進行重疊時，當像素為黑點時，則重疊像素一定為黑點，可是當像素為白點時，則重疊出的像素可能是黑點或白點，因此對比為 1/2。但本研究與 Lukac-Platantions 學者所提之方法，是將秘密資料經過編碼或運算產生 m 個像素的分享影像，將分享影像進行重疊時，會利用 m 個像素來進行回復運算，讓重疊後資料跟原始影像一模一樣，因此對比為 1。

在 codebook 部分，Lukac-Platantions 學者所提之方法必須自行建構 codebook，但自行建構 codebook 時，必須考量到所建構的 codebook 是否安全，若不安全，則可能讓攻擊者，有機會取得秘密資訊。且依照分享影像張數不同，則每個 codebook 就有所不同，導致使用上不方便。而本研究方法是利用亂數，來取代 codebook，因此不需要自行建構 codebook，也讓使用者使用上較便利。

在重疊恢復取得秘密資訊效率上，本研究所提之方法須進行四次布林運算，比 Yang 與 Wang 等人所提之方法只需要一次布林運算差，但在對比效果上比他們還要完美。而 Lukac-Platantions 學者所提之方法在對比上與本研究所提之方法都一樣可產生完美對比，但在恢復秘密資訊時，Lukac-Platantionss 學者所

表三：對比 α 的比較表

	n=2	n=3	n=4	…	n=100
Yang [10]之方法 2	1/2	1/3	1/4	…	1/100
Wang 等人 [8,9]	1/2	1/2	1/2	…	1/2
Lukac-Platantions [4]	1	1	1	…	1
本論文之方法	1	1	1	…	1

表四：(2,n)VSS 方法之比較

	Yang [10] 之方法 2	Wang 等人 [8,9]	Lukac-Platantions [4]	本論文所提之方法
對比 α	1/n	1/2	1	1
Codebook	不須自訂	不須自訂	須自訂	不須自訂
分享影像像素擴張（m）	1	1	m	m
影像種類	黑白影像	All	All	All
重疊效率	Boolean(1 次)	Boolean(1 次)	二進位轉換	Boolean(4 次)

提之方法必須經過二進位與十進位轉換，與本研究所提之方法做比較，本研究重疊恢復影像效率較佳。

在分享影像像素擴張上，Yang 與 Wang 等人學者所提之方法都不會擴張，可是他們重疊後對比都無法達到 1。而 Lukac-Platantions 學者與本研究所提之方法，雖然分享影像會擴張成 m 倍，可是在重疊分享影像時，會恢復成原始影像的大小且對比可達到 1。

5. 結論

由於目前視覺秘密分享機制中，在灰階影像或彩色影像，常利用半色調技術，將影像變成二進位影像後，再進行編碼產生分享影像。而本研究提出(2,n)視覺秘密分享機制，主要是利用二進位轉換取代半色調技術，再利用亂數與布林運算來取代 codebook，雖每個像素會擴張成 m 個像素；但在重疊影像時，可利用簡單布林運算，將重疊影像恢復成原來大小且產生完美對比，以達到最佳辨識效果。

6. 誌謝

感謝國家科學委員會計畫編號 NSC 96-2628- E-218-002-MY2 對於本論文的支持與協助。

參考文獻

[1] Cimato, S., De Prisco, R. and De. Santis, A., ***Probabilistic visual cryptography schemes***, Computer Journal, Vol. 49 No. 1, pp. 97-107, 2006.

[2] Hou, J.C., ***Visual cryptography for color images*,** Pattern Recognition, Vol. 36, No. 7, pp. 1619–1629, 2003.

[3] Hou, Y.C. and Tu, S.F., ***A Visual Cryptographic Technique for Chromatic Images Using Multi-pixel Encoding Method***, Journal of Research and Practice in Information Technology, Vol. 37, No. 2, pp. 179-191, 2005.

[4] Lukac, R. and Platantions, K.N., ***Bit-level based secret sharing for image encryption***, Pattern Recognition, Vol. 38, pp. 767-772, 2005.

[5] Lin, C.C. and Tsai, W.H., ***Visual cryptography for gray-level images by dithering techniques***, Pattern Recognition Letter, Vol. 24, No1–3, pp. 349–358, 2003.

[6] Lin, C.C. and Tsai, W.H., ***Visual cryptography for gray-level images by dithering techniques***, Pattern Recognition, Vol. 24, No. 1–3, pp. 349–358, 2003.

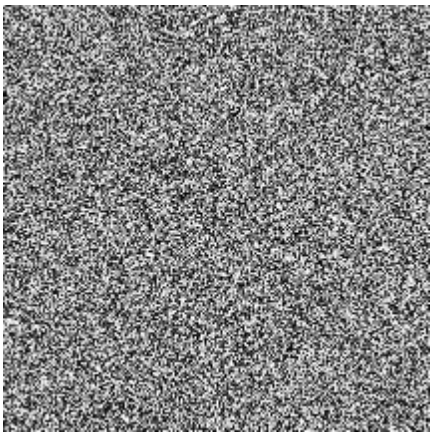
[7] Naor, M. and Shamir, A., ***Visual Cryptography***, In: Advances in Cryptology-EUROCRYPT '94, LNCS 950, Springer-Verlag, pp. 1-12, 1995.

[8] Wang, D., Zhang, L., Ma, N., and Li, X., ***Two secret sharing schemes based on Boolean operations***, Pattern Recognition, Vol. 40, pp. 2776-2785, 2007.

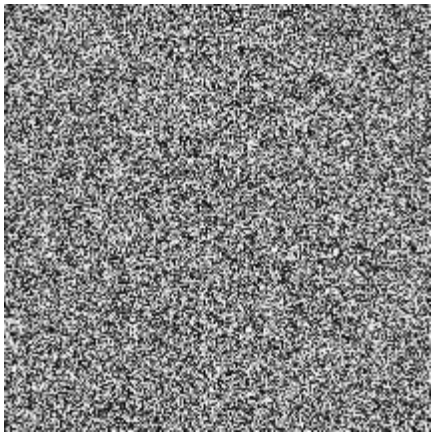
[9] Wang, D., Zhang, L., Ma, N., and Li, X., ***Secret color images sharing schemes based on XOR operation***, Cryptology ePrint Archive: Report 2005/372, 2005.

[10] Yang, C.N., *New* ***visual secret sharing schemes using probabilistic method***, Pattern Recognition Letters, Vol. 25, No. 4, pp.481-494, 2004.

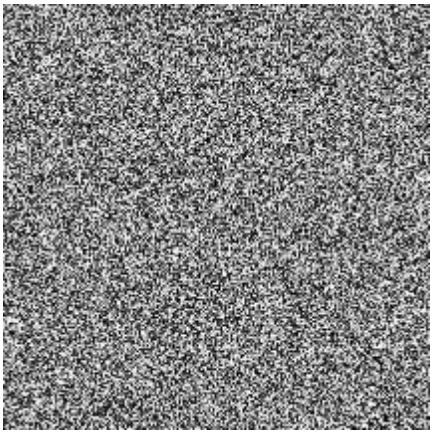
（a）秘密影像 256×256 Lena



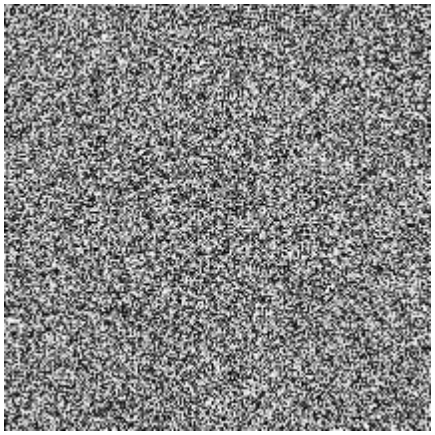
（b）分享影像（I）



（c）分享影像（II）



（d）分享影像（III）



（e）分享影像（IV）

（f）使用兩張分享影像 I、II 所恢復之影像

（g）使用兩張分享影像 III、IV 所恢復之影像

圖四：（2,4）VSS 實驗結果