基於不同疊合距離的視覺雙重機密分享機制

Visual Two-secret Sharing Scheme by Different Superimposition Positions

李翼豪
銘傳大學資訊工程學系
john999970@gmail.com

徐熊健
銘傳大學資訊工程學系
sjshyu@mail.mcu.edu.tw

摘要

本研究提出了一種藉由多重距離疊合，來實現分享多重機密的視覺密碼機制。兩張機密影像可製作成兩張大小不同的投影片（分享影像），將兩張投影片分別放在遠近不同的對應位置上進行疊合，可利用人類視覺原理還原出兩張機密影像。此機制保留視覺密碼的安全特性，不同的疊合距離，使解密更具隱密性，機密系統也更具彈性。

一、簡介

隨著科技的進步與網際網路的普及，資訊數位化已經越來越普遍。這些數位化的資訊包含了許多私密資料需要被保護，因此產生了密碼學來對資料進行加密和解密。傳統密碼學下金鑰的長度將決定加密技術的強度，為了增加密文被破解的難度使得在解密過程中需要大量複雜的電腦計算。

視覺密碼 (visual cryptography) 最先由 Naor 與 Shamir 兩位學者所提出的一種新加密機制，其原理是直接使用人類視覺原理來解碼，解密者不需密碼學相關背景知識，並且解碼過程中不需要任何電腦計算，只需要透過疊合投影片動作便即時完成解碼。此機制改進了傳統密碼學在解密過程中需要大量複雜計算的缺點，也沒有加密資訊在網路傳輸過程中可能遭遇攔截並且被破解的風險。

而較新的研究 [1][2] 使用多機密視覺機密分享方法，我們可以更有效運用投影片空間，或是放入誤以為真的假還原影像來以欺騙為目的。其特殊解密技巧不同於傳統視覺密碼機制，讓機密即使落入間諜手中也不易被破解。

在這篇論文中，我們提出一個新的多機密之視覺機密分享機制，使用不同的解密距離關係來還原不同的機密影像。

二、相關文獻

2.1 視覺密碼概念

在機密影像 P 加密成 S_1 與 S_2 兩張分享影像中，像素點 $p \in P$ 若為白點，則隨機選擇前兩列之一作為 1×2 大小的分享影像區塊 $s_1 \in S_1$ 與 $s_2 \in S_2$，符號⊗意指“or”運算，s_1 與 s_2 疊合 ($s_1 \otimes s_2$) 後會呈現一黑一白的區塊；若 p 為黑點，則選擇後兩列作為 s_1 與 s_2，s_1 與 s_2 疊合後會呈現兩黑的區塊。在選擇 s_1 與 s_2 之前產生會各兩種組合，並且每種組合被選到的機率是一樣的，如此可以確保加密完成後的兩張分享影像黑白點分布是隨機的。Naor 與 Shamir [3] 的視覺密碼之基本原理如表 1 所示。

表 1 Naor 與 Shamir (2, 2) 視覺密碼分享機制

p	機率	s_1	s_2	$s_1 \otimes s_2$
□	0.5	■□	■□	■□
	0.5	□■	□■	□■
■	0.5	■□	□■	■■
	0.5	□■	■□	■■

2.2 安全訊息展示

Yamamoto 等人 [4-9] 首先提出了安全訊息展示 (secure information display) 的概念，使用顯示器 (display)、遮罩圖 (mask) 和有限可視區域 (limited viewing zone) 的技巧，可在不同的觀看位置下還原多張機密影像相關研究。Yamamoto 等人 [5][6] 使用一張遮罩與多張顯示影像還原多張彩色機密影像。[7] 分析不同觀看位置下還原機密影像的辨識結果。[8] 使用兩個有限可視區域還原兩張機密影像。[9] 提出使用多張遮罩來還原一張機密影像，提升機密的安全性。

Shyu 等人 [10] 延伸安全訊息展示的概念，提出使用一張投影片與 n 張不同位置遮罩圖來還原 n 張機密影像的視覺密碼機制。

2.3 視覺機密分享之多重距離概念

多個物體位置與人類視覺的關係，可以用大小知覺 (size perception) [11-13] 來求得。令 I_h 為眼睛視覺到的物體高度；A_h 為物體實際高度；d 為瞳孔到視網膜之間的距離；D 為眼睛到物體之間的距離，則物體大小知覺和距離之間的關係如下：

$$I_h = A_h \times d / D \tag{1}$$

考慮 I_w 為眼睛視覺到的物體寬度，A_w 為物體實

際寬度，同公式 (1) 得到：

$$I_w = A_w \times d / D \quad (2)$$

假設物體面為一矩形則根據公式 (1)(2) 可得眼睛視覺到的物體面積 $I_h \times I_w$ 為：

$$I_h \times I_w = A_h \times A_w \times d^2 / D^2 \quad (3)$$

由公式 (3) 得知眼睛視覺到的物體面積與物體實際面積成正比、與物體距離平方成反比，d 在此可視為一個常數。舉例說我們把同一物體放在眼前一倍距離處與兩倍距離處做比較，會感覺前者（近處）的物體面積是後者（遠處）物體面積的四倍大。

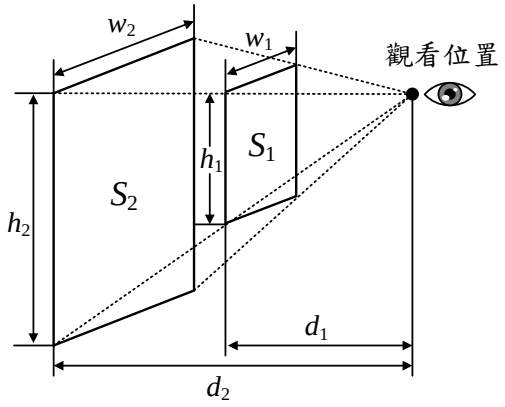
本研究與 [4-9] 及 [10] 不同的地方在於：我們提出的機制會產生兩張分享影像，而這兩張分享影像任意移動其中一張的前後位置可還原出兩張不同的機密影像。

三、本研究提出的方法

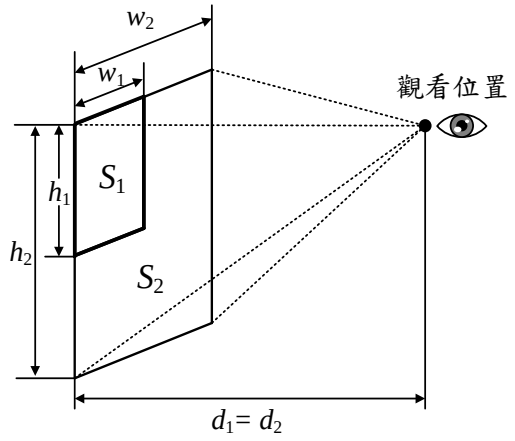
3.1 多距離疊合的多機密視覺分享機制

本機制的技巧如圖 1 所示。將兩張機密影像 P_1 和 P_2 編碼為兩張分享影像 S_1 和 S_2，分別放置在兩個不同的解密距離 d_1 與 d_2，S_1 和 S_2 的長度分別為 h_1 與 h_2，寬度分別為 w_1 與 w_2，且 $2w_1 = w_2$，$2h_1 = h_2$。

令 S_1 的位置要剛好能完全覆蓋 S_2（眼睛看到的 S_1 大小 = 眼睛看到的 S_2 大小）可還原 P_1，根據公式 (3) 可推得解密距離關係 $2d_1 = d_2$，如圖 1 (a) 所示。而令 S_1 與 S_2 對齊左上角疊合後可還原 P_2，根據公式 (1) 可推得解密距離關係 $d_1 = d_2$，如圖 1 (b) 所示。



(a)



(b)

圖 1、多重距離下還原機密影像：(a) 還原 P_1 的疊合方式，(b) 還原 P_2 的疊合方式

在定義好分享影像長度、寬度與解密距離關係後，接著舉例說明本機制 P_1, P_2 與 S_1, S_2，在兩個不同的解密距離關係下，透過疊合來還原機密影像所對應的區塊位置與大小。

假設兩張大小為 $h \times w$ 的機密影像 P_1, P_2 中的每一個像素 p_1, p_2 位於各 P_1, P_2 中的 (i, j) 處，如圖 2 (a)、(b) 所示。分享影像 S_1 中區塊 s_1 為 1×1 大小並位於 S_1 中的 (i, j) 處，如圖 2 (c) 所示。已知在解密距離 $2d_1 = d_2$ 下 $2w_1 = w_2$ 且 $2h_1 = h_2$，所以 S_2 中的每一個 s_2 會調整大小為 s_1 四倍大，也就是 2×2 大小並位於 S_2 中的 $(2i, 2j)$ 處，如圖 2 (d) 所示。在解密距離 $d_1 = d_2$ 關係下 $S_1 \otimes S_2$ 的區塊位於 (i, j) 處，還原出代表 p_2 的機密區塊，如圖 2 (e) A 區塊所示；在解密距離 $2d_1 = d_2$ 下 $S_1 \otimes S_2$ 的區塊位於 $(2i, 2j)$ 處，還原出代表 p_1 的機密區塊，如圖 2 (e) 中 B 區塊所示。

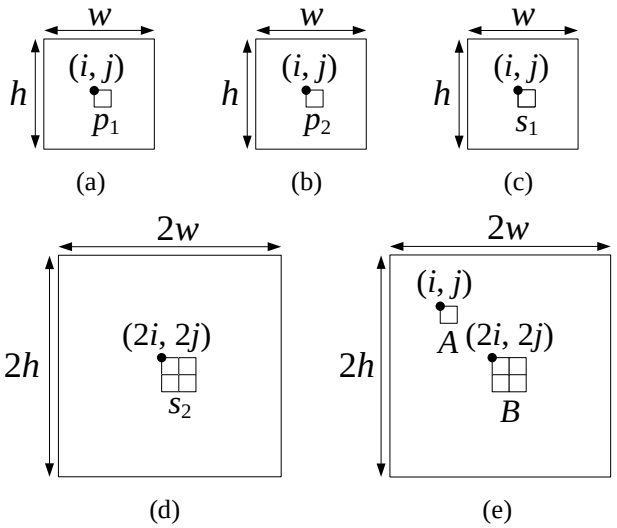


圖 2、機密影像與分享影像其對應像素間的位置關係：(a) $p_1 \in P_1$, (b) $p_2 \in P_2$, (c) $s_1 \in S_1$, (d) $s_2 \in S_2$, (e) 疊合後 $A \in S_1 \otimes S_2$ 當 $d_1 = d_2$、$B \in S_1 \otimes S_2$ 當 $2d_1 = d_2$

3.2 編碼分享影像

我們將機密影像 P_1 與 P_2 分別切割為 n 個不重疊區域 $P_{(1,n)}$與 $P_{(2,n)}$，其中 $P_{(1,n)}$與 $P_{(2,n)}$的位置 (i, j) 滿足 $(w / 2^{n-1} > i > w / 2^n) \parallel (h / 2^{n-1} > j > h / 2^n)$，$n \geq 1$，$P_{(1,n)}$與 $P_{(2,n)}$的編碼步驟如下：

1. 給定 $P_{(1,1)}$，$p_1 \in P_{(1,1)}$。當 p_1 為□，則 s_1 為隨機編碼□或■，在解密距離關係 $2d_1 = d_2$ 下，令 s_1 所對應的 2×2 區塊 s_2 根據已編的 s_1 設定為相同的顏色，亦即當 s_1 = □則 s_2 = ⊞，s_1 = ■則 s_2 = ■■。當 p_1 為■，s_2 根據 s_1 設定為互補的顏色，亦即當 s_1 = □則 s_2 = ■■，s_1 = ■則 s_2 = ⊞，令 $\updownarrow s_1 \otimes s_2$ 代表 s_1 與 s_2 是在 $2d_1 = d_2$ 下做有距離的疊合，如表 2 所示。

表 2、根據 p_1 編 s_1 與對應位置的 s_2

p_1	機率	s_1	s_2	$\updownarrow s_1 \otimes s_2$
□	0.5	□	⊞	⊞
	0.5	■	■■	■■
■	0.5	□	■■	■■
	0.5	■	⊞	■■

2. 給定 $P_{(2,n)}$，$p_2 \in P_{(2,n)}$和上階段已編碼的 $S_{(1,n)}$，$s_1 \in S_{(1,n)}$，在解密距離關係 $d_1 = d_2$ 編下階段所對應的 $S_{(2,n+1)}$，$s_2 \in S_{(2,n+1)}$，$n \geq 1$。當 p_2 為□，則 s_2 根據 s_1 設定為相同的顏色，若 p_2 為■，則 s_2 根據 s_1 設定為互補的顏色，如表 3 所示。

表 3、根據 p_2 和上階段已編碼的 s_1 編下階段 s_2

p_2	s_1	s_2	$s_1 \otimes s_2$
□	□	□	□
	■	■	■
■	□	■	■
	■	□	■

3. 給定 $P_{(1,n+1)}$，$p_1 \in P_{(1,n+1)}$和上階段已編碼的 $S_{(2,n+1)}$，$s_2 \in S_{(2,n+1)}$，在解密距離關係 $2d_1 = d_2$ 編下階段所對應的 $S_{(1,n+1)}$，$s_1 \in S_{(1,n+1)}$，$n \geq 1$。令 $H(s_2)$為 s_2 區塊的漢明值權重，即黑點的所有個數。當 p_1 為□，且 $H(s_2) < 2$（兩黑以下），則 s_1 = □。若 $H(s_2) > 2$（兩黑以上），則 s_1 = ■，若 $H(s_2) = 2$（兩黑兩白），則 s_1 為隨機編碼□或■，如表 4 所示。

表 4、根據 p_1 和上階段已編碼的 s_2 編下階段 s_1

p_1	s_2	機率	s_1	$\updownarrow s_1 \otimes s_2$
□	$H(s_2) < 2$	1	□	$H(\updownarrow s_1 \otimes s_2) < 2$
	$H(s_2) > 2$	1	■	$H(\updownarrow s_1 \otimes s_2) = 4$
	$H(s_2) = 2$	0.5	□	$H(\updownarrow s_1 \otimes s_2) = 2$
		0.5	■	$H(\updownarrow s_1 \otimes s_2) = 4$
■	$H(s_2) < 2$	1	■	$H(\updownarrow s_1 \otimes s_2) = 4$
	$H(s_2) > 2$	1	□	$H(\updownarrow s_1 \otimes s_2) > 2$
	$H(s_2) = 2$	0.5	□	$H(\updownarrow s_1 \otimes s_2) = 2$
		0.5	■	$H(\updownarrow s_1 \otimes s_2) = 4$

4. 將已編碼的 s_2 重新分配樣式，$s_2 \in S_{(2,1)}$，分配方式如表 5 所示。

表 5、重新分配 $s_2 \in S_{(2,1)}$

s_2	機率	*re*-s_2	s_2	機率	*re*-s_2
⊞	0.125		■	0.125	
	0.125			0.125	
	0.125			0.125	
	0.125			0.125	
	0.125			0.125	
	0.125			0.125	
	0.125			0.125	
	0.125			0.125	

重複步驟 2、3 直到兩張分享影像編碼完畢，最後執行步驟 4 使得 $S_{(2,1)}$與 $S_{(2,n)}$區塊分配樣式一致，$n \geq 2$。圖 3 畫出本機制的加密流程，步驟 1 中根據 $P_{(1,1)}$ 編碼 $S_{(1,1)}$與對應位置的 $S_{(2,1)}$，如圖 3 (a)。步驟 2 中根據已編碼的 $S_{(1,n)}$ 與 $P_{(2,n)}$ 編下階段 $S_{(2,n+1)}$，$n \geq 1$，如圖 3 (b)。步驟 3 中根據上階段已編碼的 $S_{(2,n+1)}$ 與 $P_{(1,n+1)}$ 編下階段 $S_{(1,n+1)}$，$n \geq 1$，如圖 3 (c)。

我們以演算法說明編碼步驟 [1-3]：

演算法 1：將機密影像 $P_{(1,\ 1)}$ 編碼為兩張分享影像 $S_{(1,\ 1)}$ 與 $S_{(2,\ 1)}$。

輸入：機密影像 $P_{(1,\ 1)}$。
輸出：兩張分享影像 $S_{(1,\ 1)}$與 $S_{(2,\ 1)}$。
for ($0 \le i < w, 0 \le j < h, i > w / 2 \,\|\, j > h / 2$)
{ if ($P_1[i, j] = 0$) //機密為白像素
{ $s_1[i, j]$ = *random_pixel*();
//隨機編碼白或黑像素
for ($0 \le k \le 1, 0 \le l \le 1$)
$s_2[2i + k, 2j + l] = s_1[i, j]$;
}
else //機密為黑像素
{ $s_1[i, j]$ = *random_pixel*();
//隨機編碼白或黑像素
for ($0 \le k \le 1, 0 \le l \le 1$)
$s_2[2i + k, 2j + l] = \overline{s_1[i, j]}$;
}
} output(S_1, S_2);

演算法 2：根據已編的 $S_{(1,\ n)}$將機密影像 $P_{(2,\ n)}$ 編碼為分享影像 $S_{(2,\ n+1)}$。

輸入：已編的分享影像 $S_{(1,\ n)}$與機密影像 $P_{(2,\ n)}$。
輸出：分享影像 $S_{(2,\ n+1)}$。
w /= 2;
h /= 2;
for ($0 \le i < w, 0 \le j < h, i > w / 2 \,\|\, j > h / 2$)
{ if ($p_2[i, j] = 0$) //機密為白像素
$s_2[i, j] = s_1[i, j]$;
else //機密為黑像素
$s_2[i, j] = \overline{s_1[i, j]}$;
} output(S_2);

演算法 3：根據已編的 $S_{(2,\ n+1)}$將機密影像 $P_{(1,\ n+1)}$ 編碼為分享影像 $S_{(1,\ n+1)}$。

輸入：已編的分享影像 $S_{(2,\ n+1)}$與機密影像 $P_{(1,\ n+1)}$
輸出：分享影像 $S_{(1,\ n+1)}$。
for($0 \le i < w, 0 \le j < h, i > w / 2 \,\|\, j > h / 2$)
{ $H(s_2) = 0$;
for ($0 \le k \le 1, 0 \le l \le 1$)
$H(s_2)$ += $s_2[2i + k, 2j + l]$;
//計算漢明值權重
if($p_1[i, j] = 0$) //機密為白像素
{ if($H(s_2) < 2$) $s_1[i, j] = 0$;
if($H(s_2) > 2$) $s_1[i, j] = 1$;
if($H(s_2) = 2$) $s_1[i,j]$=*random_pixel*();
//隨機編碼白或黑像素
}
else //機密為黑像素
{ if($H(s_2) < 2$) $s_1[i, j] = 1$;
if($H(s_2) > 2$) $s_1[i, j] = 0$;
if($H(s_2) = 2$) $s_1[i,j]$=*random_pixel*();
//隨機編碼白或黑像素
}
} output(S_1);

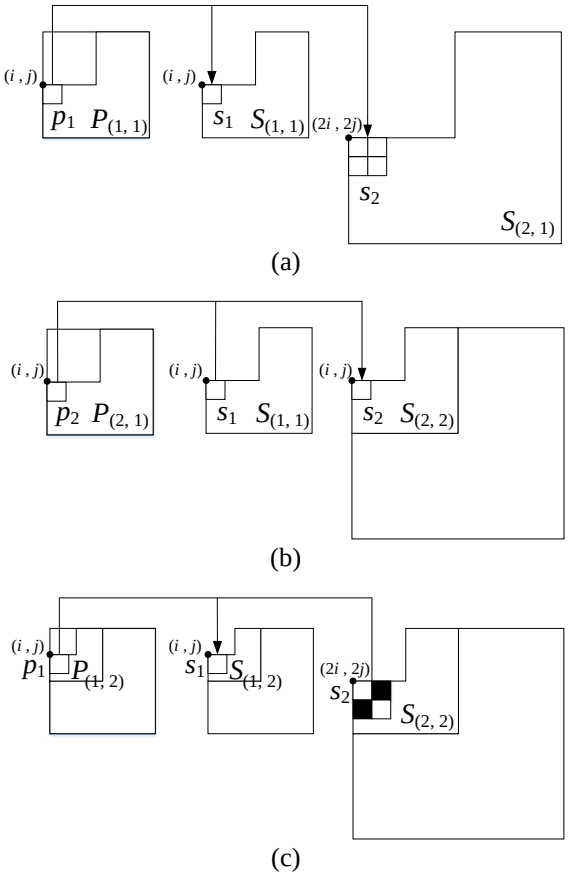


圖 3、多重距離原理的加密流程—根據兩張機密影像進行編碼：(a)將 $P_{(1,\ 1)}$編碼為兩張分享影像 $S_{(1,\ 1)}$與 $S_{(2,\ 1)}$,(b) 根據 $P_{(2,\ 1)}$和上階段 $S_{(1,\ 1)}$編 $S_{(2,\ 2)}$,(c) 根據 $P_{(1,\ 2)}$和上階段已決定的 $S_{(2,\ 2)}$編下階段 $S_{(1,\ 2)}$

3.3 改良對比度的編碼方案

在 3.2 節步驟 4 中提到重新分配 $S_{(2,\ 1)}$，使得 s_2 像素分配樣式與已編碼 $S_{(2,\ n)}$一致，$n \ge 2$，此步驟具有降低還原 P_1 之對比度特性。為了改善還原 P_1 的對比度損失，在此提出對 $S_{(2,\ 1)}$上區塊分配為 2 黑 2 白的樣式刪去，使得還原 P_1 之對比度增加，如表 6 所示。

表 6、改良之重新分配 $S_{(2,\ 1)}$上的區塊

s_2	機率	*re*-s_2	s_2	機率	*re*-s_2
	0.2			0.2	
	0.2			0.2	
	0.2			0.2	
	0.2			0.2	
	0.2			0.2	

改良對比度編碼方案在完成步驟 1、2 後，在解密距離關係 $d_1 = d_2$ 下，令 s_2 為 2×2 大小區塊，$s_2 \in S_{(2,n)}$，則 s_2 需要將 2 黑 2 白的樣式重新分配，分配規則是以 0.8 的機率將 s_2 上隨機一個白（黑）點改為黑（白）點，或是以 0.2 的機率將 s_2 改為 或 ，如表 7 所示，使得完成步驟 4 後 $S_{(2,1)}$上的區塊分配樣式（如表 6）與 $S_{(2,n)}$一致，$n \geq 2$。其中因為 $S_{(2,n)}$是還原 P_2 的區域，所以重新分配後會相對犧牲還原 P_2 之對比度，原始方案與改良方案的對比效果會在 3.4 節分析比較。

已知在步驟 1 中 s_2 編碼為 或 機率相同，並由表 6 可求得分配後 s_2 為 4 白、3 白 1 黑、3 黑 1 白與 4 黑的機率分別是 0.1、0.4、0.4 與 0.1，接著我們可以由表 7 驗算出 s_2 各種樣式編碼機率與表 6 所分配是相同的，因此可以確保 $S_{(2,1)}$與 $S_{(2,n)}$ 在不同分配規則下，所編碼的 s_2 仍然是樣式一致且機率相同的。

表 7、重新分配 $s_2 \in S_{(2,n)}$

s_2	機率	*re-*s_2	s_2	機率	*re-*s_2
	0.1			0.1	
	0.2			0.2	
	0.2			0.2	
	0.2			0.2	
	0.2			0.2	
	0.1			0.1	
	0.1			0.1	
	0.2			0.2	
	0.2			0.2	
	0.2			0.2	
	0.2			0.2	
	0.1			0.1	
	0.1			0.1	
	0.2			0.2	
	0.2			0.2	
	0.2			0.2	
	0.2			0.2	
	0.1			0.1	

3.4 模擬實驗結果

給定兩張大小 128 × 128 的機密影像 P_1 和 P_2 如圖 4 (a)、(b) 所示，經由 3.2 節原始方案所編碼的分享影像 S_1 和 S_2 如圖 4 (c)、(d) 所示，圖 (e) 是兩張分享影像疊合 $s_1 \otimes s_2$ 當 $2d_1 = d_2$；圖 (f) 是兩張分享影像疊合 $s_1 \otimes s_2$ 在 $d_1 = d_2$。由 3.2.1 節改良方案所編碼的分享影像 S_1 和 S_2 如圖 4(g)、(h) 所示，圖 (i)、(j) 分別是兩張分享影像疊合 $s_1 \otimes s_2$ 當 $2d_1 = d_2$ 與 $d_1 = d_2$。注意：在解密距離關係 $d_1 = d_2$ 下，S_1 疊合於 S_2 的 $0 \leq x < w_2/2, 0 \leq y < h_2/2$ 處為有效區域。

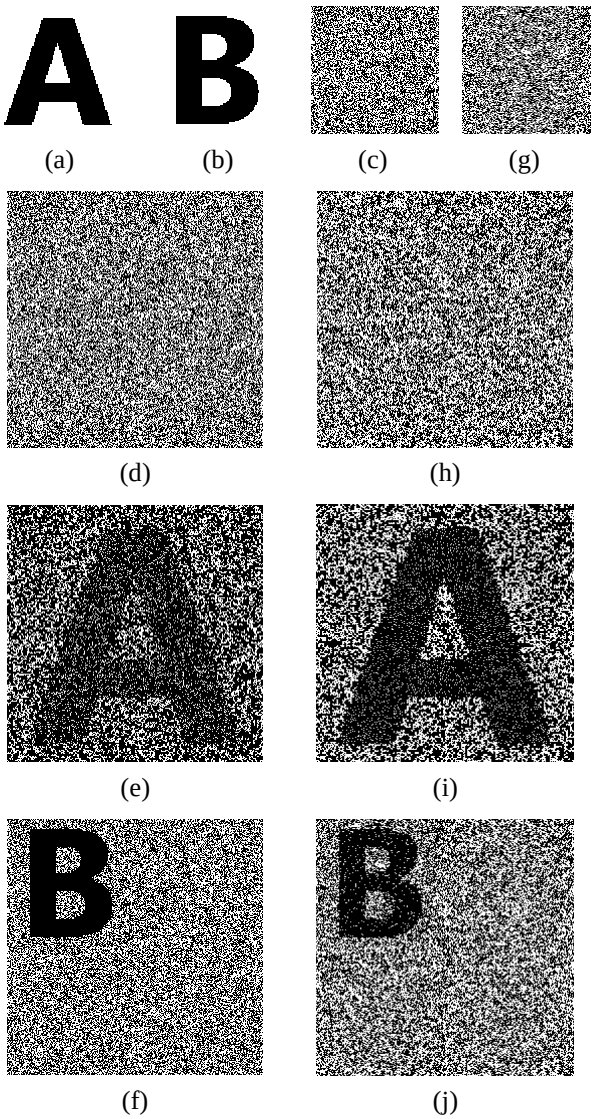


圖 4、實驗結果：(a) P_1 (b) P_2 (c-f) 原始方案之 S_1, S_2, $S_1 \otimes S_2$ 當 $2d_1 = d_2$, $S_1 \otimes S_2$ 當 $d_1 = d_2$ (g-j) 改良方案之 S_1, S_2, $S_1 \otimes S_2$ 當 $2d_1 = d_2$, $S_1 \otimes S_2$ 當 $d_1 = d_2$

在考慮還原機密辨識效果中，對比度可以當作是評判方法好壞的一個指標。根據以下公式 [2]：

$$C(S) = \frac{n_0(S[P(0)]) - n_0(S[P(1)])}{m}$$

其中 $n_0(S[P(0)])$、$n_0(S[P(1)])$分別代表還原白機密與黑機密區塊上所透光的像素個數，m 為像素擴張。

原始方案中還原 P_1 的 $n_0(S[P(0)]) = (4 \times 1 + 3 \times 4 + 2 \times 3) / 8 / 2 = 1.375$, $n_0(S[P(1)]) = (2 \times 3 + 1 \times 4 + 0 \times 1) / 8 / 2 = 0.625$, 於是當 $2d_1 = d_2$：

$$C(S_1 \otimes S_2) = \frac{1.375 - 0.625}{4} = 0.1875$$

還原 P_2 的 $n_0(S[P(0)]) = 0.5$, $n_0(S[P(1)]) = 0$, 於是當 $d_1 = d_2$：

$$C(S_1 \otimes S_2) = \frac{0.5 - 0}{1} = 0.5$$

改良方案中還原 P_1 的 $n_0(S[P(0)]) = (4 \times 1 + 3 \times 4) / 5 / 2 = 1.6$, $n_0(S[P(1)]) = (1 \times 4 + 0 \times 1) / 5 / 2 = 0.4$, 於是當 $2d_1 = d_2$：

$$C(S_1 \otimes S_2) = \frac{1.6 - 0.4}{4} = 0.3$$

還原 P_2 中 s_2 符合表 6 所編碼的比例為 10 / 16 ，其中 $n_0(S[P(0)]) = 0.5$, $n_0(S[P(1)]) = 0$，而 s_2 需要重新分配的比例為 6 / 16，其中 $n_0(S[P(0)]) = 0 \times 0.1 + 1 \times 0.4 + 2 \times 0.4 + 2 \times 0.1 = 1.4$, $n_0(S[P(1)]) = 0 \times 0.1 + 0 \times 0.4 + 1 \times 0.4 + 2 \times 0.1 = 0.6$, 於是當 $d_1 = d_2$：

$$C(S_1 \otimes S_2) = \frac{0.5 - 0}{1} \times \frac{10}{16} + \frac{1.4 - 0.6}{4} \times \frac{6}{16} = 0.3875$$

可得出改良方案對於與原始方案將還原 P_1 之對比度由 0.1875 提升至 0.3，還原 P_2 之對比度由 0.5 降低為 0.3875，因此改良方案的折衷特性能在兩個對比度間取得平衡。

四、結論

本論文提出使用雙重距離疊合來還原出兩個機密影像的方法，我們將進一步研究雙重以上的距離疊合機制、找出更具彈性的解密距離關係的編碼方法，或是結合平移概念的多機密視覺機密分享機制等，都是日後我們有興趣的研究方向。

參考文獻

[1] S. J. Shyu, S.-Y. Huang, Y.-L. Lee, R.-Z., Wang and K. Chen, “Sharing multiple secrets in visual cryptography,” *Pattern Recognition*, Vol. 40, Issue 12, Dec., pp. 3633-3651 (2007).

[2] S. J. Shyu and K. Chen, “Visual multiple secret sharing based upon turning and flipping,” *Information Sciences*, Vol. 181, Issue 15, Aug., pp. 3246-3266 (2011).

[3] M. Naor and A. Shamir, “Visual Cryptography,” *Advances in Cryptography — EUROCYPT’94, Lecture Notes in Computer Science* 950, pp. 1-12, Springer-Verlag (1994).

[4] H. Yamamoto, Y. Hayasaki, and N. Nishida, “Securing information display by use of visual cryptography,” *Opt. Lett.* **28**, 1564–1566 (2003).

[5] H. Yamamoto, Y. Hayasaki, and N. Nishida, “Secure information display with limited viewing zone by use of multi-color visual cryptography,” *Opt. Express* **12**, 1258–1270 (2004).

[6] H. Yamamoto, Y. Hayasaki, and N. Nishida, “Securing display of grayscale and multicolored images by use of visual cryptography,” *Proc. SPIE* **5306**, 716–724 (2004).

[7] H. Yamamoto and Y. Hayasaki, “Secure display that limits the viewing space by use of optically decodable encryption,” *Proc. SPIE* **6482**, 64820C (2007).

[8] H. Yamamoto, Y. Hayasaki, and N. Nishida, “Secure information display with two limited viewing zones using two decoding masks based on visual secret sharing scheme,” *Jpn. J. Appl. Phys., Part 1* **44**, 1803–1807 (2005).

[9] H. Yamamoto, Y. Hayasaki, and N. Nishida, “Secure information display by use of multiple decoding masks,” *Proc. SPIE* **5600**, 192–199 (2011).

[10] S. J. Shyu, M.-C. Chen, and K.-M. Chao, Securing information display for multiple secrets, *Optical Engineering*, Vol. 48, Issue 5, May, pp. 057005-1-057005-12 (2009).

[11] http://baike.baidu.com/view/2139426.htm

[12] http://staff.pccu.edu.tw/~tdl/percept7.htm

[13] 朱宝荣, “应用心理学教程, ” 清华大学出版社, pp. 64-66 (2004).