使用隨機網格設計之可調整光透率與片段張數的視覺密碼

A random Grid-based Visual Cryptography to Adjust Light Transmission and the Number of Shares

陳瀅羽
國立暨南國際大學
資訊工程學系
s95321011@ncnu.edu.tw

阮夙姿*
國立暨南國際大學
資訊工程學系
jsjuan@ncnu.edu.tw

李明政
國立暨南國際大學
資訊工程學系
s3321908@ncnu.edu.tw

***摘要*－視覺密碼 (Visual Cryptography) 是一種可由人眼解密的機密分享方法，在無法使用電腦運算的情況之下，他是一個可選擇的加密方法。多數的視覺密碼技術是將一張祕密影像加密，分製成數張毫無意義的片段 (Share)，由於每張片段上的影像皆是雜亂無章的，因此無法從中得知原秘密影像。解密時則只需將多張片段疊合，即可利用人的視覺辨識出原秘密影像。在這個過程中，不需要經由電腦複雜運算。**

本研究藉由隨機網格 (Random Grids) 的概念，設計出數種不同的演算法，提供使用者任意選擇片段張數以及光透率 (Light Transmission)，使每張片段在不會透露出任何原始機密影像的同時，也確保還原影像有好的視覺效果，藉以達成視覺密碼在使用上有更多元及更彈性的應用。

***Abstract*－Visual cryptography is a way that can decrypt the secret image by the human's eye rather than decrypt by the computer. Visual cryptography encrypts a secret image into many shares. We can't recognize the secret image from a share because the shares are chosen randomly. When the shares are superimposed together, we can recognize the secret image by human's vision. In the process, we don't need complicatedly calculate by means of the computer.**

This research applies the concept of random grids. We propose many different algorithms according to difference number of the shares and difference light transmission of the share. In which, every shares were produced that can't be figured out any information about the secrete image, but it will be identified the when all the shares are superimposed.

***關鍵詞*—視覺密碼 (Visual Cryptography)、影像加密 (Image Encryption)、片段 (Share)、隨機網格 (Random Grids)。**

一、簡介

由於現今的社會中，網路技術十分的發達，為了確保透過網路所傳輸的秘密影像不被竊取，我們必須對此機密影像做加密，此法則稱為影像加密法 (Image Encryption)。在許多的影像加密的文獻中 [5, 6, 7, 8]，不少研究探討視覺密碼學 (Visual Cryptography，簡稱 VC)，視覺密碼是將秘密影像加密，即可輸出得到隨機網格，或稱為片段 (Share)，只需將片段疊合，即可由人的視覺辨識出原圖形。其中將長 h、寬 w 的圖片中的每一點像素區分成透明與不透

* Corresponding author. Tel.: +886-49-2910960 ext.4875.

明，其中透明代表白色和 0，不透明代表黑色和 1，本文只討論黑白二階圖，其中光透率的定義為全部的像素量分之透明的像素量。

R_1，R_2 分別為片段 1 與片段 2，$R_1 \otimes R_2$ 代表將 R_1，R_2 做疊合的結果：

R_1	R_2	$R_1 \otimes R_2$
0	0	0
0	1	1
1	0	1
1	1	1

Kafri 和 Keren [4] 於 1987 年首先提出隨機網格的概念，設計出三種演算法。其每一個像素只分為透明或是不透明。且每一個像素是由亂數產生，所以透明像素量平均會等於不透明像素量。因此隨機網格的平均光透率 ($\Im$) 為 1/2。然而，此三種演算法都只能產生兩張片段。此外，大部分方法不但加密後的影像大小會變大，且光透率 ($\Im$) 必固定為 1/2。

在 2005 年，白璟霖提出以隨機亂數為基礎之影像機密分享。他們利用多張隨機亂數網格與 XOR 運算，產生出多張分享的機密片段，並宣稱使用者可任意產生 n 張機密片段。2008 年，Chen 與 Tsao 等學者也提出基於 (n, n) 的隨機網格之影像加密法。然而，無論是白璟霖的方法或是 Chen 與 Tsao 等學者的研究，本文皆發現當分享的片段張數大於五張時，則會有疊合後看不清影像的問題存在。

基於上述缺失，本文的研究之動機將針對機密影像做加密，同時設計出能依使用者之希望，產生任意張片段，並且也可以依照使用者的喜好調整這些片段的光透率。使得祕密影像之加密有更多層面之應用。

以下，本文將簡介相關研究之文獻探討。

(一) Kafri 和 Keren 之方法

1987 年 Kafri 和 Keren 提出下列三個演算法以加密一張黑白的祕密影像。在他們的演算法中，輸入所要加密的影像 B，將輸出得到兩張片段 R_1、R_2。詳細演算法步驟如下：

Algorithm 1
Generate a random grid R_1// $\Im$ (R_1) = 1/2
for (i = 0; i<w; i++)
  for (j = 0; j<h; j++)
    if ($B[i][j]$ == 0) $R_2[i][j] = R_1[i][j]$;
    else $R_2[i][j] = \overline{R_1[i][j]}$;
output (R_1, R_2)

Algorithm 2
Generate a random grid R_1// $\Im$ (R_1) = 1/2
for (i = 0; i<w; i++)
  for (j = 0; j<h; j++)
    if ($B[i][j]$ == 0) $R_2[i][j] = R_1[i][j]$;
    else $R_2[i][j]$ = random(0, 1);
output (R_1, R_2)

Algorithm 3
Generate a random grid R_1// $\Im$ (R_1) = 1/2
for (i = 0; i<w; i++)
  for (j = 0; j<h; j++)
    if ($B[i][j]$ == 0) $R_2[i][j] = \underline{\text{random}}(0, 1)$;
    else $R_2[i][j] = \overline{R_1[i][j]}$;
output (R_1, R_2)

表 1：演算法 1、2、3 疊合後的光透率。

	B	R_1	R_2	$R_1 \otimes R_2$	光透率
1	□	□ ■	□ ■	□ ■	1/2
	■	□ ■	■ □	■ ■	0
2	□	□ ■	□ ■	□ ■	1/2
	■	□ □ ■ ■	□ ■ □ ■	□ ■ ■ ■	1/4
3	□	□ □ ■ ■	□ ■ □ ■	□ ■ ■ ■	1/4
	■	□ ■	■ □	■ ■	0

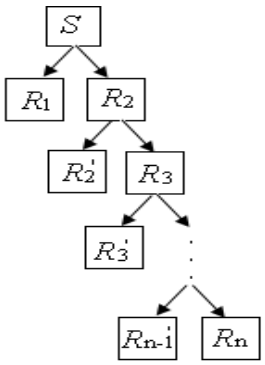
我們於表 1 列出演算法 1、2、3 與光透率的關係。其中 B 代表原始祕密影像的像素值，R_1 代表第一張片段，R_2 代表第一張片段。可看出此三種演算法都只能產生兩張片段。由於只能產生兩張隨機網格，而無法產生多張以利更多應用，因此，此法尚有改進空間。

(二) Chen 與 Taso 之方法

2008 年，Tzung-Her Chen 與 Kai-Hsiang Tsao 等學者，從 [3] 中延伸出第四種演算法，此時隨機網格的平均光透率 (ℑ) 仍為 1/2，但已可以產生多張片段。演算法步驟如下。

Algorithm 4
n-out-of-*n*_ RandomGrids(S){
//Create R_1, R_2 as two cipher grids
$R_1, R_2 \leftarrow$ Random_Grids(S)
//Create R_3 to R_n as cipher grids recursively
if ($n > 2$){
for $k = 2$ to $(n - 1)$
$R'_k, R_{k+1} \leftarrow$ Random_Grids(R_k)
}
}

其中的 Random_Grids(S) 可用演算法 1 至演算法 3 任一個代入，此法所產生的多重隨機網格樹狀圖如下所示：



(三) 白璟霖之方法

接著白璟霖在 2005 年又設計出演算法五 [1] 如下，其中 $f_y(x)$ 是 XOR 的運算，a 為二維陣列，random(2) 為隨機選擇一白與一黑。

Algorithm 5
Define $a_0 = 0$
for $k \leftarrow 1$ to $n - 1$ do
for (each $b \in B[i, j]$, $1 \le i \le w$, $1 \le j \le h$) do
$R_k[i, j]$ = random(2)
$a_k[i, j] = f_{a_{k-1}}(R_k[i, j])$
endfor
endfor
for (each $b \in B[i, j]$, $1 \le i \le w$, $1 \le j \le h$) do
$R_n[i, j] = f_b(a_{n-1}[i, j])$
endfor

此結果與演算法四相同，皆可分出每張光透率為 1/2 之多張片段，只是使用了不同的方法。此演算法先產生一個空的二維陣列 a，依序 a 與每一張亂數產生出的隨機網格做 XOR 運算，不斷的產生新的二維陣列 a，這是為了最後一張片段而作的準備。換句話說，前面 $n - 1$ 張片段皆是由亂數所產生的，只有最後一張片段，是根據二維陣列及原影像再做一次 XOR 運算所產生出來。而產生的任何一張片段都無法看出被加密的祕密影像為何，必須要全部隨機網格做疊合，才能看到原本所加密的祕密影像。然而，演算法 4 與演算法 5 兩者，皆有同一缺失，則為分出來的片段張數大於或多於 5 張，就越會有疊合後影像看不清楚的問題。因為疊合後的影像中，無論原圖中的透明像素 (0) 或是不透明像素 (1) 的光透率，將越來越小 (近乎全黑)，並且此五種演算法所產生的每個片段的光透率都只能固定為 1/2。因此，本論文將設計出新的三種演算法，不但能任意選定片段的張數之外，也可以選定片段的光透率，使得多張疊合後的影像仍舊清晰可辨識。藉由此法，相信將能使視覺密碼更有彈性的被多方應用。

本論文組織架構如下：在下節中將提出本文主要研究成果，將分為三種方法討論，並在第三節中，分別針對本論文架構提出三種方法之實驗結果。在第四節中，進行本架構的分析與相關研究之比較。最後，則是本論文之結論

與未來研究方向。

二、主要研究成果

此研究共有三個主要成果，分別述敘如下。

(一) 方法一

在演算法 5 中，產生 n 張片段，前 $n-1$ 張片段皆是亂數產生，只有最後一張片段是經過計算而來。然而此方法只能改變片段的張數，並不能改變片段的光透率。因此，本方法將利用一個新的函數 $h_y(x)$，如表 2 所示，如此不但能改變片段的張數，且能改變片段的光透率。本研究為了方便敘述，將定義光透率 $\Im = (\alpha-1)/\alpha$，而 random(α) 則表示為隨機選擇一個黑點與 $\alpha-1$ 個白點，例：random(3) 為選擇一黑或二白；random(4) 為選擇一黑與三白，以此類推。當光透率為 $\Im = (\alpha-1)/\alpha$ 時，方法一將由亂數去產生 0 到 $\alpha-1$ 的數字，0 到 $\alpha-2$ 代表白色，$\alpha-1$ 則代表黑色，例：$\Im = 2/3$，則 0 到 1 為白色，2 則為黑色，即可表示成 (白、白、黑)。

在方法一中，每一張片段的光透率皆為一致，其演算法步驟如下。

表 2：函式 $h_y(x)$、y、x 的關係表

y	x	$h_y(x)$
0	0	0
0	1	1
1	0	random($\alpha-1$)
1	1	0

Algorithm 6
Define $a_0 = 0$
for $k \leftarrow 1$ to n do
  for (each $b \in B[i, j]$, $1 \le i \le w, 1 \le j \le h$) do
    if (($B[i, j]$ == 1) or ($k < n$))
      $R_k[i, j]$ = random(α)
      $a_k[i, j] = h_{a_{k-1}}(R_k[i, j])$
    else
      $R_n[i, j] = h_b(a_{n-1}[i, j])$
  endfor
endfor

表 3：Algorithm 6 之例子；$\Im = 2/3$，$n = 3$。

B	R_1	a_1	R_2	a_2	R_3	$R_1 \otimes R_2 \otimes R_3$
□	□	□	□	□	□	□
			□	□	□	□
			■	■	■	■
	□	□	□	□	□	□
			□	□	□	□
			■	■	■	■
	■	■	□	□	□	■
				■	■	■
			□	□	□	■
				■	■	■
			■	□	□	■
■	□	□	□	□	□	□
					□	□
					■	■
			□	□	□	□
					□	□
					■	■
			■	■	□	■
					□	■
					■	■
	□	□	□	□	□	□
					□	□
					■	■
			□	□	□	□
					□	□
					■	■
			■	■	□	■
					□	■
					■	■
	■	■	□	■	□	■
					□	■
					■	■
			□	■	□	■
					□	■
					■	■
			■	□	□	■
					□	■
					■	■

舉例如下，當片段張數 $n = 3$，光透率 $\Im = 2/3$

時。如表 3 所示，每張片段的光透率都為 2/3，因此每張片段看不出任何原秘密影像，而全部片段重疊將可看出影像，其光透率比為白：黑 = 4/9：8/27 = 3：2。由此可知，白色數量約為黑色的 1.5 倍之多。因此，使用者可透過肉眼辨識原始影像。

(二) 方法二

經由演算法五與方法一，為求使影像更明顯，將混和使用此兩種方法的精神，利用函數 $h_y(x)$ 以及 XOR，產生演算法如下:

Algorithm 7
Define $a_0 = 0$
Define count = 0
for $k \leftarrow 1$ to $n-1$ do
  for (each $b \in B[i, j]$, $1 \le i \le w$, $1 \le j \le h$) do
    if (($B[i, j]$ == 0) && (count!= 0))
      $R_k[i, j] = R_1[i, j]$
    else
      $R_k[i, j]$ = random(α)
      $a_k[i, j] = f_{a_{k-1}}(R_k[i, j])$
  endfor
  count = 1;
endfor
for (each $b \in B$, $B[i, j]$, $1 \le i \le w$, $1 \le j \le h$) do
  $R_n[i, j] = h_b(a_{n-1}[i, j])$
endfor

舉例如下，當 $n = 3$，$\Im = 2/3$ 時，原圖像素為白色部分，片段的像素值都一樣，黑色部分的像素值就是利用 $h_y(x)$ 以及 XOR 產生。如表 4 所示，每一張片段的光透率都為 2/3，因此每張片段看不出任何原秘密影像，而全部片段重疊將看的出影像，其光透率比為白：黑 = 2/3：4/18 = 3：1。由於白色數量約為黑色的 3 倍之多。由此可知，方法二比方法一更能讓使用者容易透過肉眼辨識原始影像。

從表 4 可知，每一張片段的光透率都幾乎等於 2/3。由於白色部分的值每張都一樣，疊合的差別在於黑色部分的光透率。因此任兩張疊合就可以看出影像，但疊合多張將得到愈清晰的因素，並且無論分幾張片段皆可。

表 4：Algorithm 7 之例子；$\Im = 2/3$，$n = 3$。

B	R_1	a_1	R_2	a_2	R_3	$R_1 \otimes R_2 \otimes R_3$
□	□	□	□	□	□	□
	□	□	□	□	□	□
	■	■	■	■	■	■
■	□	□	□	□	□	□
					■	■
			□	□	□	□
					■	■
			■	■	□	■
	□	□	□	□	□	□
					■	■
			□	□	□	□
					■	■
			■	■	□	■
	■	■	□	■	□	■
			□	■	□	■
			■	□	□	■
					■	■

(三) 方法三

將每個 *pixel* 值原本只有 0、1 兩個數字來做改變。當光透率為 $\Im = (\alpha - 1)/\alpha$ 時，將原影像黑色部分代表數字 $\alpha - 1$，白色部分代表數字 0。前 $n-1$ 張片段取亂數，由亂數去產生 0 到 $\alpha - 1$ 的數字，0 到 $\alpha - 2$ 代表白色，$\alpha - 1$ 代表黑色，再由一個二維陣列存前 $n-1$ 張片段數字的總和。當片段張數只有兩張或光透率為 1/2 時，最後一張片段的黑色部份會是前 $n-1$ 張數字的總和 mod(α) 後，同餘為 $\alpha - 1$ 的數字，其餘數字則皆為白色 (範例請見表 5)。若當片段大於 2 張以上時，則最後一張片段的黑色部份會是前 $n-1$ 張數字的總和 mod(α) 同餘為 $\alpha - 3$ 的數字，其餘皆為白色，其演算法如下。

Algorithm 8
for $k \leftarrow 1$ to $n-1$ do
  for (each $b \in B[i,j]$, $1 \le i \le w$, $1 \le j \le h$) do
    $R_k[i,j] = \text{random}(\alpha)$
    $B[i,j] = B[i,j] + R_k[i,j]$
  endfor
endfor
for (each $b \in B[i,j]$, $1 \le i \le w$, $1 \le j \le h$) do
  if (($n <= 2$) or ($\Im == 1/2$))
    if ($B[i,j] \bmod(\alpha) \equiv \alpha - 1$)
      $R_n[i,j] = 1$
    else
      $R_n[i,j] = 0$
  else
    if ($B[i,j] \bmod(\alpha) \equiv \alpha - 3$)
      $R_n[i,j] = 1$
    else
      $R_n[i,j] = 0$
endfor

舉例如下，當 $n = 3$，$\Im = 2/3$ 時，將原圖與前 2 張片段像素白色用數字 0 與 1 表示，黑色用數字 2 表示，最後一張片段的像素是前 2 張片段數字總和 mod 3 產生，結果等於 0 代表像素是黑色，其餘為白色。從表 5 所示，每一張片段的光透率都為 2/3，且每張片段看不出任何原秘密影像的樣子，但是由於疊合後的原白色部分和原黑色部分的光透率差異不是很大，所以片段張數較多，疊合後的結果會變的不清楚，但此方法必須要全部片段重疊才可看出原始影像。其方法三之光透率比為白：黑 = 1/3：2/9 = 3：2。

三、實驗結果

本文的實驗環境於 Windows XP 作業系統，使用 Visual Studio 2005 for C# 程式開發環境，實作本文所提出的三種方法。本研究將上述三個研究成果，利用電腦實際模擬實驗，結果如下。

(一) 方法一的實驗結果

由圖 1 實驗結果所示，每張片段都看不出任何影像，且任兩張片段重疊也看不出秘密影像，必須將全部片段重疊才可看出秘密影像。雖然此法可以將片段的透明度及張數任意改變

表 5：Algorithm 8 之例子；$\Im = 2/3$，$n = 3$。

B	R_1	R_2	總和	R_3	$R_1 \otimes R_2 \otimes R_3$
0 □	0 □	0 □	0	■	■
		1 □	1	□	□
		2 ■	2	□	■
	1 □	0 □	1	□	□
		1 □	2	□	□
		2 ■	3	■	■
	2 ■	0 □	2	□	■
		1 □	3	■	■
		2 ■	4	□	■
2 ■	0 □	0 □	2	□	□
		1 □	3	■	■
		2 ■	4	□	■
	1 □	0 □	3	■	■
		1 □	4	□	□
		2 ■	5	□	■
	2 ■	0 □	4	□	■
		1 □	5	□	■
		2 ■	6	■	■

，但只要片段的張數較多，則疊合後的結果就會變的不清楚。因此，本文接著進一步提出新的演算法 (方法二)，使得原白色部分和原黑色部分的光透率差別擴大，以讓影像更明顯的可辨識。

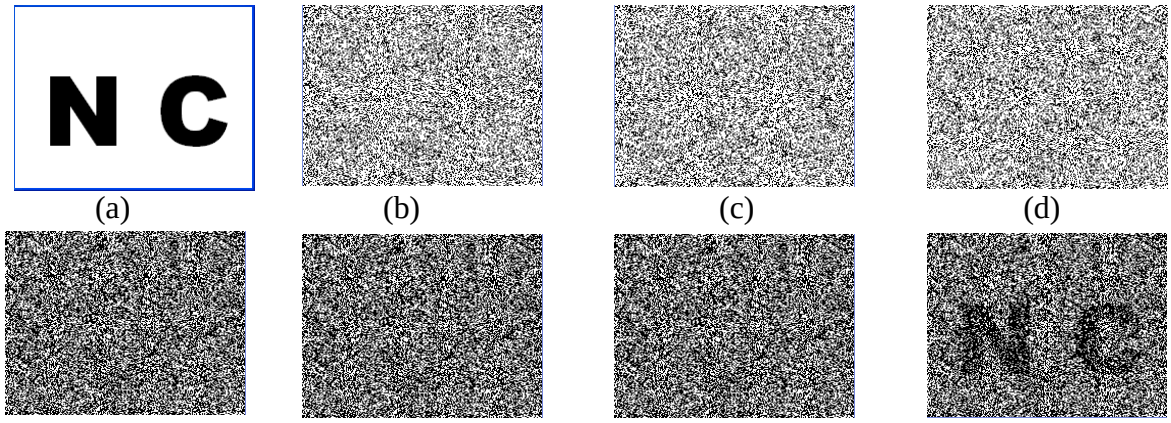
(二) 方法二的實驗結果

由圖 2 實驗結果所示，可看出每張片段都看不出任何影像，但兩張片段重疊就可略看出影像。而疊合越多張片段，則原影像就會越明顯。本文方法二解決方法一中，當多張片段重疊，影像會不清楚的問題。然而，當任選兩張片段疊合時，卻會略看出影像。由於此法較不適用於任何情境之中，因此本文提出下一個演算法 (方法三) 作改進。

(三) 方法三的實驗結果

由圖 3 所示，可看出每張片段及任兩張片

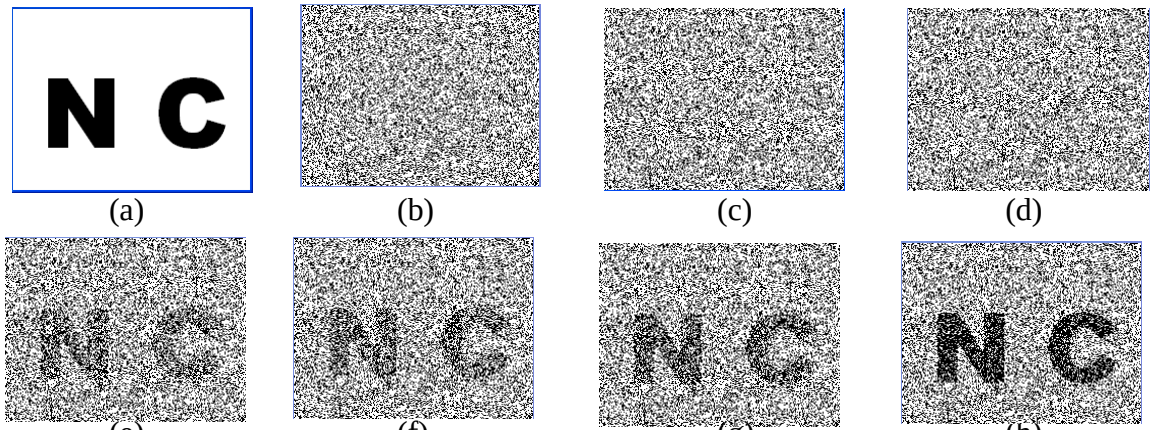
段重疊都看不出秘密影像，必須要全部片段重疊才可看出秘密影像。藉由此方法，可了解到片段光透率和片段張數關係的上限值。但是此方法卻存在另一個問題，就是當片段的張數較多時，疊合後的結果黑白之間的光透率會過於接近，以致無法以肉眼辨識。



(a) (b) (c) (d)

(e) (f) (g) (h)

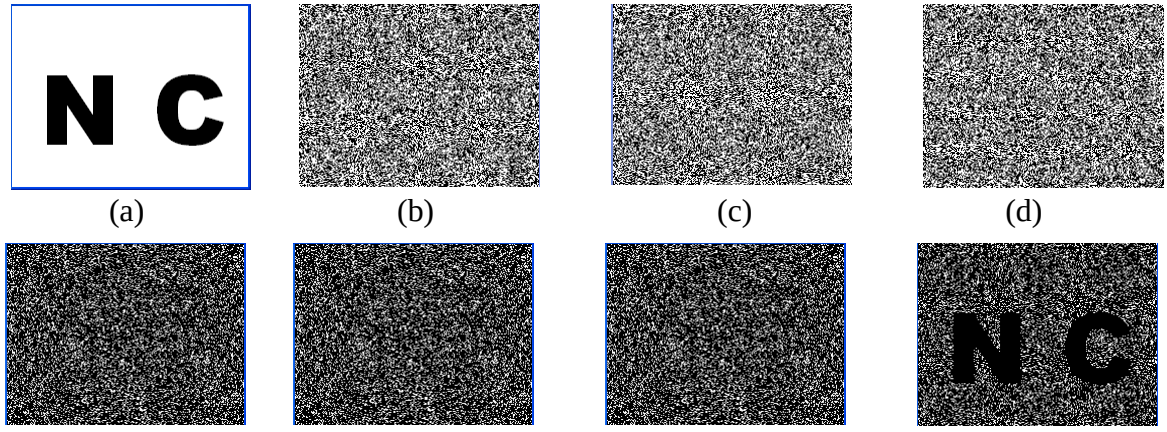
圖 1 方法一的實驗結果，當光透率 2/3，片段的張數為 3，(a) 祕密影像 B，(b) R_1，(c) R_2，(d) R_3，(e) $R_1 \otimes R_2$，(f) $R_1 \otimes R_3$，(g) $R_2 \otimes R_3$，(h) $R_1 \otimes R_2 \otimes R_3$。



(a) (b) (c) (d)

(e) (f) (g) (h)

圖 2 方法二的實驗結果，當光透率 2/3，片段的張數為 3，(a) 祕密影像 B，(b) R_1，(c) R_2，(d) R_3，(e) $R_1 \otimes R_2$，(f) $R_1 \otimes R_3$，(g) $R_2 \otimes R_3$，(h) $R_1 \otimes R_2 \otimes R_3$。



(a) (b) (c) (d)

(e) (f) (g) (h)

圖 3 方法三的實驗結果，當光透率 1/2，片段的張數為 3，(a) 祕密影像 B，(b) R_1，(c) R_2，(d) R_3，(e) $R_1 \otimes R_2$，(f) $R_1 \otimes R_3$，(g) $R_2 \otimes R_3$，(h) $R_1 \otimes R_2 \otimes R_3$。

四、分析與比較

在表 6 中，逐一列出本方法與先前之相關研究之間的比較。其中 (*s, p, r*)：*s* 代表片段的光透率、*p* 代表片段的張數、*r* 代表重疊幾張片段可還原秘密影像。從表 6 可清楚的發現 Kafri 與 Keren 的方法只能產生兩張片段，且光透率必須固定為 1/2；而 Chen 與 Tsao 的方法雖然宣稱可分成多張片段，然而實際上當片段數大於等於五張時，使用者將已無法透過肉眼辨識出秘密影像，此外光透率也同樣必須固定為 1/2；而白璟霖的方法，則與 [3] 擁有相同的問題。至於本文提出的三種方法，不但可提供使用者隨意選擇片段的光透率，方法二更可確實疊合多張片段後，仍能肉眼辨識成功。因此，本文將比先前的相關研究更具有使用彈性與實用性。

表 6：本研究與前者之比較

相關研究	成果大小:(*s, p, r*)
Kafri 與 Keren [4]	(1/2, 2, 2)
Chen 與 Tsao [3]	(1/2, 2, 2)、(1/2, 3, 3)、(1/2, 4, 4)
白璟霖 [1]	(1/2, 2, 2)、(1/2, 3, 3)、(1/2, 4, 4)
本研究之方法一	(1/2, 2, 2)、(1/2, 3, 3)、(1/2, 4, 4)、(2/3, 2, 2)、(2/3, 3, 3)、(3/4, 2, 2)、(4/5, 2, 2)
本研究之方法二	(1/2~8/9, *n*, 2~*n*) *n* : 2~∞ (9/10~19/20, *n*, 3~*n*) *n* : 3~∞ (20/21~29/30, *n*, 4~*n*) *n* : 4~∞ ..... (((*t*-2)*10)/((*t*-2)*10+1)~ ((*t*-1)*10)-1/((*t*-1)*10), *n*, *t*~*n*)*n* : *t*~∞
本研究之方法三	(1/2, 2, 2)、(1/2, 3, 3)、(1/2, 4, 4)、(2/3, 2, 2)、(3/4, 2, 2)、(4/5, 2, 2)、(5/6, 2, 2)

五、結論與未來研究方向

先前的相關研究中，片段的光透率只能固定為 1/2，且疊合片段張數只要 5 張以上就會看不清秘密影像，在實用上存在許多限制。有鑑於此，本文提出三種演算法，提供使用者可任意改變片段的光透率以及張數，同時也找出此兩參數對於每種方法的關係值，說明當分配的片段張數多大時，光透率若大於某值將會導致圖像不易辨識。此外，當光透率固定為某數時，若要求圖像的辨識清晰則片段的張數時，則可選擇的範圍為何。如表 7 與表 8 所示。

本文未來研究方向可分為以下三點：一、目前的研究成果多半需要全部片段重疊，才能顯示秘密影像。然而，在許多現實環境應用上，並非需要全部片段重疊才可看出秘密影像，如：門檻值的方式。二、本研究以僅提供加密一張影像，未來將做改進，提供可加密多張秘

表 7：固定片段光透率，張數可達的範圍

光透率	方法一	方法二	方法三
s = 1/2	2~5	2~∞	2~6
s = 2/3	2~3	2~∞	2
s = 3/4	2	2~∞	2
s = 4/5	X	2~∞	2
s = 5/6	X	2~∞	2
s >= 6/7	X	2~∞	X

密影像的演算法。三、本文只針對黑白影像提出方法，希望未來能夠往灰階以及彩色方面再進行深入的研究。

表 8：固定片段張數，光透率可達的範圍

張數	方法一	方法二	方法三
n= 2	1/2~4/5	1/2~8/9	1/2~5/6
n = 3	1/2~2/3	9/10~19/20	1/2
n = 4	1/2	20/21~29/30	X
n >= 5	X	((n–2)*10)/((n–2)*10+1) ~ ((n–1)*10–1)/((n–1)*10)	X

致謝

本研究感謝行政院國家科學委員會（NSC 98-2815-C-260 -009 -E）的補助。

六、參考文獻

[1] 白璟霖，“以隨機亂數為基礎的影像機密分享，”*銘傳大學資訊工程系碩士論文*，2005。

[2] 陳宗和，魏國珍，曹凱翔，“使用隨機網格加密多重秘密影像，” *Proceedings of 18th Information Security Conference*, Hualien, May 29-30, 2008.

[3] T.-H. Chen and K.-H. Tsao, “Image encryption by (*n*, *n*) random grids,” *Proceedings of 18th Information Security Conference*, Hualien, May 29-30, 2008.

[4] O. Kafri and E. Keren, “Encryption of pictures and shapes by random grids,” *Optics Letters*, Vol. 12, No. 6, pp. 377-379, 1987.

[5] R. Lukac and K. N. Plataniotis, “Bit-level based secret sharing for image encryption,” *Pattern Recognition*, Vol. 38, No. 5, pp. 767-772, 2005.

[6] M. Naor and A. Shamir, “Visual cryptography,” *Eurocrypt’ 94*, LNCS 950, pp. 1-12, 1995.

[7] S.-J. Shyu, “Image encryption by random grids,” *Pattern Recognition*, Vol. 40, No. 3, pp. 1014-1031, 2007.

[8] S.-J. Shyu, “Image encryption by multiple random grids,” *Pattern Recognition*, Vol. 42, No. 7, pp. 1582-1596, 2009.