以機率為基礎之像素不擴展的視覺式秘密分享模型

侯永昌、許慶昇
國立中央大學資訊管理研究所

摘要

視覺密碼是一個密碼學的新興研究領域，它與傳統密碼學的主要差異在於解密過程的不同。視覺密碼的方法是將一份機密影像加密成 N 份分享影像，參與機密分享的每個人都可以持有一份分享影像。一群被允許還原秘密的人將她們所持有的分享影像重疊在一起後，便可以直接透過肉眼看到機密訊息；而被禁止還原機密訊息的一群人便無法利用分享影像獲得任何機密訊息。視覺密碼學的主要精神在於解密的方法是透過人類視覺系統，而不需使用任何密碼學知識與計算機資源。在視覺密碼的研究中，降低像素擴展與提高對比是兩個重要的研究主題。大部分的視覺密碼方法都使用像素擴展的技巧，其結果是分享影像的大小被擴展成機密影像的 M 倍。像素擴展的結果不但使影像產生變形，同時也會產生不易攜帶與消耗更多儲存空間的問題。在本研究中，我們提出一個不需像素擴展的新方法。我們的方法結合機率的觀念，並考量安全性與對比兩項指標，建構出最佳化問題的模型。此外，我們應用遺傳演算法來求解最佳化的問題。實驗結果顯示我們的方法不但有效，而且還具有處理單一機密影像之任意使用結構(access structure)的能力。

[1] 原中文題目「以機率為基礎之像素不擴展的視覺式秘密分享機制最佳化模型」刪除"機制最佳化"等五字，更改為「以機率為基礎之像素不擴展的視覺式秘密分享模型」；原英文題目「A Probability-based Optimization Model for Visual Secret Sharing Schemes without Pixel Expansion」刪除 "Optimization"一字，更改為「A Probability-based Model for Visual Secret Sharing Schemes without Pixel Expansion」。

關鍵字：視覺密碼、視覺式秘密分享、遺傳演算法

A Probability-based Model for Visual Secret Sharing Schemes without Pixel Expansion

Young-Chang Hou、Ching-Sheng Hsu
Department of Information Management, National Central University

Abstract

Visual cryptography, which is characterized by its decryption process in comparison with the traditional ones, is an emerging cryptographic field. The method of visual cryptography is to encrypt a secret image into N shares such that any qualified set of participants can recover secret by their eyes. Any forbidden set of participants cannot obtain any secret information. In the study of visual cryptography, pixel expansion and contrast are two important issues. Most visual cryptographic methods are based on the technique of pixel expansion, and the result is that the size of each share is larger than that of the secret image. Pixel expansion not only results in distortion of the shares, but also consumes more storage space. In this paper, we propose a new method without pixel expansion. Our method combines concepts of probability with considerations of security and contrast to construct an optimization model. To solve the optimization problems, genetic algorithms are employed. Experimental results show that our method is effective and is able to cope with general access structures.

Keywords: visual cryptography, visual secret sharing, genetic algorithms.

壹、導論

視覺密碼的觀念是由 Naor 與 Shamir (1995)首先提出來的，它與傳統密碼學的主要差異在於解密過程的不同。(K, N)-threshold VCS 是一個視覺密碼的方法，它將一張機密影像加密後，產生 N 張看起來雜亂無章的分享影像。想要還原機密影像時，只要將這 N 張分享影像中的任意 K 張或大於 K 張的分享影像重疊，就可以透過人眼辨識出機密訊息。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(Ateniese et al. 1996a, 1996b, 2001)。Ateniese et al. (1996b)將(K, N)-threshold 的使用結構(access structure)加以擴充為$(\Gamma_{Qual}, \Gamma_{Forb}, M)$的形式。任何一個合格的集合(qualified set) $Y \in \Gamma_{Qual}$ 都可以還原機密影像，而任何一個禁止的集合(forbidden set) $X \in \Gamma_{Forb}$ 都無法獲得一絲機密訊息。這樣的結構可以定義出單一機密影像的任何機密分享規則。Droste (1996)提出多重機密影像的觀念，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。在視覺密碼的研究中，像素擴展與對比是兩個重要的研究主題(Blundo and De Santis 1998)。大部分的視覺密碼方法都使用像素擴展的技巧(Ateniese et al. 1996a, 1996b, 2001; Blundo and De Santis 1998; Blundo et al. 1999, 2001; Droste 1996; Eisen and Stinson 2002; Hofmeister et al. 2000; Naor and Shamir 1995; Tzeng and Hu 2002; Verheul and van Tilborg 1997)，其結果是分享影像的大小被擴展成機密影像的 M 倍。像素擴展的結果不但使影像產生變形，同使也會產生不易攜帶與消耗更多儲存空間的問題。而為了要解決影像變形的問題，就必須將影像再擴展以維持長與寬的比例，如此就更不易攜帶也更耗費儲存空間了。Ito et al. (1999)提出一個不需要像素擴展的方法，並將它應用在(K, N)-threshold 的使用結構上。在本研究中，我們將提出一個不需像素擴展的新方法。我們的方法結合機率的觀念並考量安全性與對比兩項指標，以建構出最佳化問題的模型。我們的方法不但可以應用在(K, N)-threshold 的使用結構上，還可以應用在單一機密影像的任何使用結構上。在本研究中，我們將使用遺傳演算法來解最佳化的問題，並產生加密用的機率矩陣。此外，我們也將展示實驗的結果，並驗證我們的方法的能力。

貳、無須像素擴展的視覺密碼方法

一、名詞與符號

在介紹無須像素擴展的視覺密碼方法之前，我們首先說明何謂使用結構，並定義一些符號，以方便後續的說明。令 $P = \{1, 2, \ldots, N\}$為參與者(participants)的集合。令 2^P 代表 P 的冪集(power set)，也就是 P 的全體子集合的集合。$\Gamma = (P, F, Q)$稱為一個使用結構(access structure) (Tzeng and Hu 2002)，它定義了機密訊息的分享規則，其中 F, Q 是 2^P 的子集合，分別代表禁止集合(forbidden sets)與合格集合(qualified sets)的集合，而且 $Q \cap F = \varnothing$。在本研究中，我們假設機密影像與分享影像為皆為黑白影像，我們以 0 代表白點，

1 代表黑點。假設 E 為一個集合，我們以$|E|$代表 E 中元素的個數。我們以符號 "$\vee$"代表邏輯運算子"OR"。假設 S 為一個布林矩陣(Boolean matrix)，我們以 S_i 表示 S 的第 i 個列向量，S_j^c 表示 S 的第 j 個欄向量。我們以 $S_i^c \vee S_j^c$ 代表兩個欄向量的"OR"運算結果。令 $X = \{i_1, i_2, \ldots, i_q\} \subseteq P$，我們定義 $\mathrm{OR}(S, X) = S_{i_1}^c \vee S_{i_2}^c \vee \ldots \vee S_{i_q}^c$ 。函數 OR(S, X)代表取出矩陣 S 中對應於集合 X 內的每一個參與者的欄向量，然後做"OR"運算之後的結果。假設 A 與 B 為矩陣，我們以 $A||B$ 表示兩個具有相同列數的矩陣的結合(concatenation)。假設 Share1, Share2, ..., ShareN 皆代表分享影像，我們以(Share1 + Share2 + ... + ShareN)表示 Share1, Share2, ..., ShareN 的重疊影像(stacked share)。

二、模型概念

以半色調影像技術的觀點而言，在一個影像區域中，如果均勻分佈的黑點密度愈高，則這一個影像區域看起來就會愈黑；反之，如果均勻分佈的黑點密度愈低，則這一個影像區域看起來就會愈白。因此，透過控制黑點分佈的密度，就可以創造出不同程度的灰階值(我們以 0 代表全白，1 代表全黑)。舉例而言，如果我們在一個 10×10 的白色影像區塊中，隨機挑選 70 個點塗成黑色，則這一個影像區塊看起來就會像是具有 70%的黑(相對於全黑)。換個角度來看，如果在這個區塊中的每一個點都有 70%的機會被塗成黑色，則這一個影像區塊看起來也會像是具有 70%的黑。因此在一個影像區域中，如果每一個點都具有相同的黑點出現機率，則這個機率值就可以做為這個影像區域的灰階值的代表。如果我們以一個黑點密度為 80%的影像區塊 B'來取代具有相同大小的黑色影像區塊 B，另外再以一個黑點密度為 50%的影像區塊 W'來取代具有相同大小的白色影像區塊 W。雖然 B'看起來沒有 B 來得黑，而 W'看起來也沒有 W 來得白，不過我們還是可以區別 B'和 W'之間的差異。視覺密碼的特色在於利用人眼來進行解密，只要眼睛能辨別黑與白的差異，就能還原機密訊息。因此，我們可以利用控制影像區塊中黑點出現機率的概念，使得不作像素擴展的視覺密碼技術變得可行。

在不作像素擴展之黑白視覺密碼中，機密影像上的每一個點經過加密後，在每一張分享影像上都只能產生一個相對應的黑點或白點。因此，針對$|P|$個參與者，機密影像上的每一個點，在$|P|$張分享影像上就有 $2^{|P|}$種可能的加密方式。以(2, 2)-threshold 使用結構($P = \{1, 2\}, F = \{\{1\}, \{2\}\}, Q = \{\{1, 2\}\}$)為例，機密影像上每一個白點或黑點加密後，分享影像 1 與分享影像 2 上相對應的點共有"白白"、"白黑"、"黑白"與"黑黑"四種可能的情況；而這四種情況重疊的結果分別為"白"、"黑"、"黑"與"黑"，如表 1 所示。在本文中，我們將稱每一種可能的加密方式為"加密規則"(Encryption Rule)。在確保安全性與提高對比的前提之下，如何決定這些加密規則被使用的機率是一個值得探討的關鍵問題。以安全性的觀點而言，在禁止集合 $X \in F$ 所構成的重疊影像上，如果代表機密影像中白點的區域與代表機密影像中黑點的區域，都具有相同的黑點出現機率，則無法產生色差的感覺，因而安全性可以得到確保。以對比的觀點而言，在合格集合 $Y \in Q$ 所構成的重疊影像上，如果代表機密影像中白點的區域與代表機密影像中黑點的區域，兩者黑點出現機率差異夠大，我們就可以透過眼睛分辨白色與黑色的差異，進而還原機密影像。

表 1：(2, 2)-threshold 的加密規則

像素顏色	分享影像 S1	分享影像 S2	重疊影像 (S1+S2)
□	□	□	□
	□	■	■
	■	□	■
	■	■	■
■	□	□	□
	□	■	■
	■	□	■
	■	■	■

表 2 與表 3 分別顯示(2, 2)-threshold 的兩種不同加密規則機率值設定對安全性與對比的影響，其結果如圖 1 與圖 2 所示。在表 2 與表 3 中，(S_{j1}, S_{j2})代表分享影像 1 (Share1)與分享影像 2 (Share2)上第 j 個可能的加密規則，而 S_{j3} 則代表將 S_{j1} 與 S_{j2} 作"OR"運算之後的結果，其中 0 代表白點，1 代表黑點。C_{0j} 代表以第 j 個加密規則來加密一個白點的機率值；C_{1j} 代表以第 j 個加密規則來加密一個黑點的機率值。表 2 顯示在 Share1 上，密圖上的白點經過加密後，出現黑點的機率為 $FC_{01} = S_{11}\times C_{01} + S_{21}\times C_{02} + S_{31}\times C_{03} + S_{41}\times C_{04} = 0.5$；而密圖上的黑點經過加密後，出現黑點的機率 FC_{11} 也是 0.5 ($FC_{11} = S_{11}\times C_{11} + S_{21}\times C_{12} + S_{31}\times C_{13} + S_{41}\times C_{14} = 0.5$)。因為密圖上的黑點與白點經過加密程序後，在 Share1 上都具有相同的黑點出現機率($FC_{01} = FC_{11}$)，也就是沒有出現色差，因此安全性可以得到確保。在 Share2 上的情況也是一樣($FC_{02} = 0.5, FC_{12} = 0.5$)，因此 Share2 的安全性也可以得到確保。但是在重疊影像(Share1+Share2)上，密圖上的白點經過加密後，出現黑點的機率為 $QC_{01} = S_{13}\times C_{01} + S_{23}\times C_{02} + S_{33}\times C_{03} + S_{43}\times C_{04} = 0.5$；密圖上的黑點經過加密後，出現黑點的機率為 $QC_{11} = S_{13}\times C_{11} + S_{23}\times C_{12} + S_{33}\times C_{13} + S_{43}\times C_{14} = 1$。因為黑點經過加密後的黑點出現機率，比白點經過加密後的黑點出現機率高($QC_{11} > QC_{01}$)，因此可以透過黑與白的色差，進而辨識出機密影像的內容(見圖 1)。

表 2：具有良好的安全性與良好的對比之機率值設定

像素顏色	分享影像 S1	分享影像 S2	重疊影像 (S1+S2)	加密規則使用機率	黑點出現機率		
					S1	S2	(S1+S2)
0	$S_{11} = 0$	$S_{12} = 0$	$S_{13} = 0$	$C_{01} = 0.5$	$FC_{01} = 0.5$	$FC_{02} = 0.5$	$QC_{01} = 0.5$
	$S_{21} = 0$	$S_{22} = 1$	$S_{23} = 1$	$C_{02} = 0.0$			
	$S_{31} = 1$	$S_{32} = 0$	$S_{33} = 1$	$C_{03} = 0.0$			
	$S_{41} = 1$	$S_{42} = 1$	$S_{43} = 1$	$C_{04} = 0.5$			
1	$S_{11} = 0$	$S_{12} = 0$	$S_{13} = 0$	$C_{11} = 0.0$	$FC_{11} = 0.5$	$FC_{12} = 0.5$	$QC_{11} = 1.0$
	$S_{21} = 0$	$S_{22} = 1$	$S_{23} = 1$	$C_{12} = 0.5$			
	$S_{31} = 1$	$S_{32} = 0$	$S_{33} = 1$	$C_{13} = 0.5$			
	$S_{41} = 1$	$S_{42} = 1$	$S_{43} = 1$	$C_{14} = 0.0$			

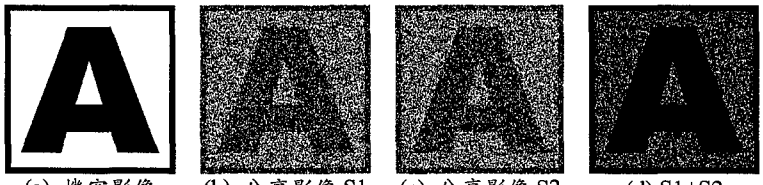
(a) 機密影像 (b) 分享影像 S1 (c) 分享影像 S2 (d) S1+S2

圖 1：具有良好的安全性與良好的對比之範例

表 3 的機率值設定雖然可以在重疊影像(Share1+Share2)上呈現白與黑的差異($QC_{01} < QC_{11}$)，但是在 Share1 與 Share2 上，代表白與黑的黑點出現機率並不相同($FC_{01} < FC_{11}$, $FC_{02} < FC_{12}$)，因此其安全性無法得到確保(見圖 2)。我們的目標是在滿足安全性的條件下，求解白點與黑點的所有加密規則的機率值(C_{0j}, C_{1j})，使得對比能達到最佳化。

表 3：具有不良的安全性與普通的對比之機率值設定

像素顏色	分享影像 S1	分享影像 S2	重疊影像 (S1+S2)	加密規則使用機率	黑點出現機率		
					S1	S2	(S1+S2)
0	$S_{11}=0$	$S_{12}=0$	$S_{13}=0$	$C_{01}=0.25$	$FC_{01}=0.5$	$FC_{02}=0.5$	$QC_{01}=0.75$
	$S_{21}=0$	$S_{22}=1$	$S_{23}=1$	$C_{02}=0.25$			
	$S_{31}=1$	$S_{32}=0$	$S_{33}=1$	$C_{03}=0.25$			
	$S_{41}=1$	$S_{42}=1$	$S_{43}=1$	$C_{04}=0.25$			
1	$S_{11}=0$	$S_{12}=0$	$S_{13}=0$	$C_{11}=0.00$	$FC_{11}=0.75$	$FC_{12}=0.75$	$QC_{11}=1.0$
	$S_{21}=0$	$S_{22}=1$	$S_{23}=1$	$C_{12}=0.25$			
	$S_{31}=1$	$S_{32}=0$	$S_{33}=1$	$C_{13}=0.25$			
	$S_{41}=1$	$S_{42}=1$	$S_{43}=1$	$C_{14}=0.50$			



(a) 機密影像 (b) 分享影像 S1 (c) 分享影像 S2 (d) S1+S2

圖 2：具有不良的安全性與普通的對比之範例

三、(2, 2)-threshold 的模型

在本節中，我們將介紹(2, 2)-threshold 的模型。它的使用結構可以寫成$\Gamma=(P, F, Q)$，其中 $P=\{1, 2\}$，$F=\{\{1\}, \{2\}\}$，且 $Q=\{\{1, 2\}\}$。在本例中，因為參與者的個數為$|P|=2$，且影像中的每個點只有白與黑兩種顏色，所以共有 $2^2=4$ 種加密規則。因此，密圖上的白點與黑點都分別有(0, 0)、(0, 1)、(1, 0)、與(1, 1)等四種加密規則。令(S_{j1}, S_{j2})代表在分享影像 1 與分享影像 2 上的第 j 個加密規則，其中 $j=1, 2, 3, 4$。令 FC_{01} 與 FC_{11} 分別代表白點與黑點經過加密後，在分享影像 1 (Share1)上出現黑點的機率；令 FC_{02} 與 FC_{12} 分別代表白點與黑點經過加密後，在分享影像 2 (Share2)上出現黑點的機率。令 QC_{01} 與 QC_{11} 分別代表白點與黑點經過加密後，在(Share1+Share2)上出現黑點的機率。在表 4 中，有

關 FC_{ik} 與 QC_{ih} 的計算如下：

$FC_{01} = S_{11}\times C_{01} + S_{21}\times C_{02} + S_{31}\times C_{03} + S_{41}\times C_{04} = C_{03} + C_{04}$，
$FC_{11} = S_{11}\times C_{11} + S_{21}\times C_{12} + S_{31}\times C_{13} + S_{41}\times C_{14} = C_{13} + C_{14}$，
$FC_{02} = S_{12}\times C_{01} + S_{22}\times C_{02} + S_{32}\times C_{03} + S_{42}\times C_{04} = C_{02} + C_{04}$，
$FC_{12} = S_{12}\times C_{11} + S_{22}\times C_{12} + S_{32}\times C_{13} + S_{42}\times C_{14} = C_{12} + C_{14}$，
$QC_{01} = (S_{11}\vee S_{12})\times C_{01} + (S_{21}\vee S_{22})\times C_{02} + (S_{31}\vee S_{32})\times C_{03} + (S_{41}\vee S_{42})\times C_{04} = C_{02} + C_{03} + C_{04}$，
$QC_{11} = (S_{11}\vee S_{12})\times C_{11} + (S_{21}\vee S_{22})\times C_{12} + (S_{31}\vee S_{32})\times C_{13} + (S_{41}\vee S_{42})\times C_{14} = C_{12} + C_{13} + C_{14}$。

表 4：(2, 2)-threshold 模型之分析表格

Pixel	S_{in}		C_{ij}	FC_{ik}		QC_{ih}
				$X_1 = \{1\}$	$X_2 = \{2\}$	$Y_1 = \{1, 2\}$
0	$S_{11} = 0$	$S_{12} = 0$	C_{01}	$FC_{01} = C_{03} + C_{04}$	$FC_{02} = C_{02} + C_{04}$	$QC_{01} = C_{02} + C_{03} + C_{04}$
	$S_{21} = 0$	$S_{22} = 1$	C_{02}			
	$S_{31} = 1$	$S_{32} = 0$	C_{03}			
	$S_{41} = 1$	$S_{42} = 1$	C_{04}			
1	$S_{11} = 0$	$S_{12} = 0$	C_{11}	$FC_{11} = C_{13} + C_{14}$	$FC_{12} = C_{12} + C_{14}$	$QC_{11} = C_{12} + C_{13} + C_{14}$
	$S_{21} = 0$	$S_{22} = 1$	C_{12}			
	$S_{31} = 1$	$S_{32} = 0$	C_{13}			
	$S_{41} = 1$	$S_{42} = 1$	C_{14}			
				$\sigma_1 = \lvert FC_{11} - FC_{01}\rvert$	$\sigma_2 = \lvert FC_{12} - FC_{02}\rvert$	$\alpha_1 = QC_{11} - QC_{01}$

就"安全性"的角度而言，密圖上的白點與黑點經過加密後，在 Share1、Share2 上必須有相同的黑點出現機率，也就是 $FC_{01} = FC_{11}$, $FC_{02} = FC_{12}$。如果它們不相等，則在 Share1、Share2 上就可能會透露出機密影像的訊息，如此安全性便無法得到確保。在此，我們分別以 $\sigma_1 = \lvert FC_{11} - FC_{01}\rvert$ 與 $\sigma_2 = \lvert FC_{12} - FC_{02}\rvert$ 來代表 Share1 與 Share2 的安全性指標。就"對比"的角度而言，密圖上的白點與黑點經過加密後，在重疊影像(Share1+Share2)上，兩者出現黑點的機率(QC_{01} 與 QC_{11})其差異必須要夠大，才能透過人眼辨識機密訊息。因此，我們希望($QC_{11} - QC_{01}$)愈大愈好。在此，我們以 $\alpha_1 = QC_{11} - QC_{01}$ 來代表重疊影像的對比指標。我們的目標是在滿足安全性的限制條件之下，求解白點與黑點的各個可能的加密規則的使用機率，使對比能達到最佳化。我們所建構的(2, 2)-threshold 模型如第(1)式所示。

$$\left.\begin{array}{ll} \max & \alpha_1 = (C_{12} + C_{13} + C_{14}) - (C_{02} + C_{03} + C_{04}), \\ \text{s.t.} & \sigma_1 = \lvert (C_{13} + C_{14}) - (C_{03} + C_{04})\rvert = 0, \\ & \sigma_2 = \lvert (C_{12} + C_{14}) - (C_{02} + C_{04})\rvert = 0, \\ & \sum_{j=1}^{4} C_{ij} = 1, \text{ for } i = 0, 1, \\ & 0 \le C_{ij} \le 1, \text{ for } i = 0, 1, \text{ and } j = 1, 2, 3, 4. \end{array}\right\} \quad (1)$$

第(1)式為一個單目標最佳化模型，其目標是在確保 Share1 與 Share2 的安全性的限

制條件之下(即$\sigma_1 = 0$，且$\sigma_2 = 0$)，求解 8 個機率值 C_{ij}，其中 $i = 0,1, j = 1, 2, 3, 4$，使得(Share1+Share2)的對比α_1極大化。

四、(2, 3)-threshold 的模型

在本節中，我們將介紹(2, 3)-threshold 的模型。它的使用結構可以寫成$\Gamma = (P, F, Q)$，其中 $P = \{1, 2, 3\}$，$F = \{\{1\}, \{2\}, \{3\}\}$，且 $Q = \{\{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 2, 3\}\}$。在本例中，因為參與者的個數為$|P| = 3$，且影像中的每個點只有白與黑兩種顏色，所以共有 $2^3 = 8$ 種加密規則。因此，密圖上的白點與黑點都分別有(0, 0, 0)、(0, 0, 1)、(0, 1, 0)、(1, 0, 0)、(0, 1, 1)、(1, 1, 0)、(1, 0, 1)、與(1, 1, 1)等八種加密規則。令(S_{j1}, S_{j2}, S_{j3})代表第 j 個加密規則，其中 $j = 1, 2, \ldots, 8$。令 C_{0j} 與 C_{1j} 分別代表白點與黑點的第 j 個加密規則的使用機率。在表 5 中，有關 C_{ij}、FC_{ik} 與 QC_{ih} 的意義與前一節相同，其計算方式不再贅述。我們所建構的(2, 3)-threshold 模型如第(2)式所示。在表 5 中，α_1、α_2、α_3 與α_4 分別代表合格集合 Y_1、Y_2、Y_3 與 Y_4 所構成的重疊影像(Share1+Share2)、(Share2+Share3)、(Share1+Share3)與(Share1+Share2+Share3)的對比。此外，σ_1、σ_2 與σ_3 分別代表禁止集合 X_1、X_2 與 X_3 所構成的重疊影像 Share1、Share2 與 Share3 的安全性。第(2)式為一個多目標最佳化模型，其目標是在確保 Share1、Share2 與 Share3 的安全性限制條件之下(即$\sigma_1 = 0$, $\sigma_2 = 0$, $\sigma_3 = 0$)，求解 16 個機率值 C_{ij}，其中 $i = 0, 1, j = 1, 2, \ldots, 8$，使得(Share1+Share2)、(Share2+Share3)、(Share1+Share3)與(Share1+Share2+Share3)的對比α_1、α_2、α_3、與α_4 極大化。

表 5：(2, 3)-threshold 模型之分析表格

Pixel	S_{i1}	S_{i2}	S_{i3}	C_{ij}	FC_{ik}			QC_{ih}			
					$X_1=\{1\}$	$X_2=\{2\}$	$X_3=\{3\}$	$Y_1=\{1,2\}$	$Y_2=\{2,3\}$	$Y_3=\{1,3\}$	$Y_4=\{1,2,3\}$
0	S_{11}=0	S_{12}=0	S_{13}=0	C_{01}	$FC_{01} = C_{04}+C_{06}+C_{07}+C_{08}$	$FC_{02} = C_{03}+C_{05}+C_{06}+C_{08}$	$FC_{03} = C_{02}+C_{05}+C_{07}+C_{08}$	$QC_{01} = C_{03}+C_{04}+C_{05}+C_{06}+C_{07}+C_{08}$	$QC_{02} = C_{02}+C_{03}+C_{05}+C_{06}+C_{07}+C_{08}$	$QC_{03} = C_{02}+C_{04}+C_{05}+C_{06}+C_{07}+C_{08}$	$QC_{04} = C_{02}+C_{03}+C_{04}+C_{05}+C_{06}+C_{07}+C_{08}$
	S_{21}=0	S_{22}=0	S_{23}=1	C_{02}							
	S_{31}=0	S_{32}=1	S_{33}=0	C_{03}							
	S_{41}=1	S_{42}=0	S_{43}=0	C_{04}							
	S_{51}=0	S_{52}=1	S_{53}=1	C_{05}							
	S_{61}=1	S_{62}=1	S_{63}=0	C_{06}							
	S_{71}=1	S_{72}=0	S_{73}=1	C_{07}							
	S_{81}=1	S_{82}=1	S_{83}=1	C_{08}							
1	S_{11}=0	S_{12}=0	S_{13}=0	C_{11}	$FC_{11} = C_{14}+C_{16}+C_{17}+C_{18}$	$FC_{12} = C_{13}+C_{15}+C_{16}+C_{18}$	$FC_{13} = C_{12}+C_{15}+C_{17}+C_{18}$	$QC_{11} = C_{13}+C_{14}+C_{15}+C_{16}+C_{17}+C_{18}$	$QC_{12} = C_{12}+C_{13}+C_{15}+C_{16}+C_{17}+C_{18}$	$QC_{13} = C_{12}+C_{14}+C_{15}+C_{16}+C_{17}+C_{18}$	$QC_{14} = C_{12}+C_{13}+C_{14}+C_{15}+C_{16}+C_{17}+C_{18}$
	S_{21}=0	S_{22}=0	S_{23}=1	C_{12}							
	S_{31}=0	S_{32}=1	S_{33}=0	C_{13}							
	S_{41}=1	S_{42}=0	S_{43}=0	C_{14}							
	S_{51}=0	S_{52}=1	S_{53}=1	C_{15}							
	S_{61}=1	S_{62}=1	S_{63}=0	C_{16}							
	S_{71}=1	S_{72}=0	S_{73}=1	C_{17}							
	S_{81}=1	S_{82}=1	S_{83}=1	C_{18}							
					$\sigma_1 = \lvert FC_{11}-FC_{01}\rvert$	$\sigma_2 = \lvert FC_{12}-FC_{02}\rvert$	$\sigma_3 = \lvert FC_{13}-FC_{03}\rvert$	$\alpha_1 = QC_{11}-QC_{01}$	$\alpha_2 = QC_{12}-QC_{02}$	$\alpha_3 = QC_{13}-QC_{03}$	$\alpha_4 = QC_{14}-QC_{04}$

$$
\left.\begin{array}{ll}
\max & \alpha_1 = (C_{13}+C_{14}+C_{15}+C_{16}+C_{17}+C_{18})-(C_{03}+C_{04}+C_{05}+C_{06}+C_{07}+C_{08}).\\
\max & \alpha_2 = (C_{12}+C_{13}+C_{15}+C_{16}+C_{17}+C_{18})-(C_{02}+C_{03}+C_{05}+C_{06}+C_{07}+C_{08}).\\
\max & \alpha_3 = (C_{12}+C_{14}+C_{15}+C_{16}+C_{17}+C_{18})-(C_{02}+C_{04}+C_{05}+C_{06}+C_{07}+C_{08}).\\
\max & \alpha_4 = (C_{12}+C_{13}+C_{14}+C_{15}+C_{16}+C_{17}+C_{18})-(C_{02}+C_{03}+C_{04}+C_{05}+C_{06}+C_{07}+C_{08}).\\
\text{s.t.} & \sigma_1 = \left|(C_{14}+C_{16}+C_{17}+C_{18})-(C_{04}+C_{06}+C_{07}+C_{08})\right| = 0,\\
& \sigma_2 = \left|(C_{13}+C_{15}+C_{16}+C_{18})-(C_{03}+C_{05}+C_{06}+C_{08})\right| = 0,\\
& \sigma_3 = \left|(C_{12}+C_{15}+C_{17}+C_{18})-(C_{02}+C_{05}+C_{07}+C_{08})\right| = 0,\\
& \sum_{j=1}^{8} C_{ij} = 1, \textit{ for } i = 0, 1,\\
& 0 \le C_{ij} \le 1, \textit{ for } i = 0, 1, \textit{ and } j = 1, 2, ..., 8.
\end{array}\right\} \quad (2)
$$

參、任意使用結構之模型

一、加密規則矩陣與機率矩陣

令 $\boldsymbol{S} = [S_{jn}]$為一個 $2^{|P|}\times|P|$的二元矩陣，其中 $S_{jn} \in \{0, 1\}$。我們稱 $\boldsymbol{S}$ 為加密規則矩陣，用以表達在參與者集合 P 之下的所有可能的加密規則。加密規則矩陣 $\boldsymbol{S}$ 中的每一個列向量 $\boldsymbol{S_j} = [S_{j1}, S_{j2}, \ldots, S_{j|P|}]$代表一個加密規則。例如，當$|P| = 3$ 時，$\boldsymbol{S_j} = [1, 0, 0]$表示第 j 的加密規則為在第一、第二與第三個分享影像上分別產生黑點、白點與白點。令 $\boldsymbol{C} = [C_{ij}]$為一個 $2\times2^{|P|}$的矩陣，其中 $C_{ij} \in [0, 1]$，$i = 0, 1, j = 1, 2, \ldots, 2^{|P|}$, 且

$$\sum_{j=1}^{2^{|P|}} C_{ij} = 1$$

我們稱 $\boldsymbol{C}$ 為機率矩陣，C_{0j} 與 C_{1j} 分別代表白點與黑點的第 j 個加密規則 $\boldsymbol{S_j}$ 的使用機率值。以表 2 的(2, 2)-threshold 為例，其加密規則矩陣與機率矩陣可以表示成：

$$S = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} C_{01} & C_{02} & C_{03} & C_{04} \\ C_{11} & C_{12} & C_{13} & C_{14} \end{bmatrix} = \begin{bmatrix} 0.5 & 0.0 & 0.0 & 0.5 \\ 0.0 & 0.5 & 0.5 & 0.0 \end{bmatrix}$$

在這個機率矩陣 $\boldsymbol{C}$ 中，C_{01} 代表使用第一個加密規則[0, 0]來加密一個白點(0)的機率；而 C_{12} 則代表使用第二個加密規則[0, 1]來加密一個黑點(1)的機率。

二、安全性

令 FC_{0k} 與 FC_{1k} 分別表示白點與黑點經過加密後，在對應於禁止集合 X_k 的重疊影像上出現黑點的機率。以安全性的角度而言，白點與黑點經過加密後，在由禁止集合所構

成的重疊的影像上，必須具有相同的黑點出現機率。因此當 $FC_{0k}=FC_{1k}$ 時，就代表對應於 X_k 的重疊影像是絕對安全的。反之，如果 $FC_{0k}\neq FC_{1k}$，則頻率上的變化就可能會透露出機密影像的訊息，如此安全性便無法得到確保。因此，我們定義對應於禁止集合 X_k 的重疊影像的安全性為

$$\sigma_k = |FC_{1k} - FC_{0k}| \tag{3}$$

安全性指標 σ_k 的值愈大，代表由 X_k 所構成的重疊影像的安全性愈差；反之，安全性指標 σ_k 的值愈小，代表由 X_k 所構成的重疊影像的安全性愈好。當 $\sigma_k = 0$ 時，代表由 X_k 所構成的重疊影像是絕對安全的。關於 FC_{ik} 的計算方式如下：

$$[FC_{ik}] = C \times \left(\mathrm{OR}(S,X_1)||\mathrm{OR}(S,X_2)||...||\mathrm{OR}(S,X_{|F|})\right) \tag{4}$$

其中 OR($\boldsymbol{S}$, X_k)代表由加密規則矩陣 $\boldsymbol{S}$ 中取出對應於禁止集合 X_k 內的每一個參與者的欄向量，然後做"OR"運算之後的結果；這個結果代表每一個可能的加密規則在對應於 X_k 的重疊影像上疊合的結果。假設 $\boldsymbol{\Gamma}=(P,F,Q)$，其中 $P=\{1,2,3\}$，$F=\{\{1\},\{2\},\{3\},\{1,3\}\}$，$Q=\{\{1,2\},\{2,3\},\{1,2,3\}\}$，且加密規則矩陣 $\boldsymbol{S}$ 與機率矩陣 $\boldsymbol{C}$ 分別為

$$S=\begin{bmatrix}0&0&0&1&0&1&1&1\\0&0&1&0&1&1&0&1\\0&1&0&0&1&0&1&1\end{bmatrix}^T,\quad C=\begin{bmatrix}C_{01}&C_{02}&C_{03}&C_{04}&C_{05}&C_{06}&C_{07}&C_{08}\\C_{11}&C_{12}&C_{13}&C_{14}&C_{15}&C_{16}&C_{17}&C_{18}\end{bmatrix}$$

則針對第一個禁止集合{1}而言，OR($\boldsymbol{S}$, {1})代表 $\boldsymbol{S}$ 中的第一欄$[0,0,0,1,0,1,1,1]^T$，針對第二個禁止集合{2}而言，OR($\boldsymbol{S}$, {2})代表 $\boldsymbol{S}$ 中的第二欄$[0,0,1,0,1,1,0,1]^T$，針對第三個禁止集合{3}而言，OR($\boldsymbol{S}$, {3})代表 $\boldsymbol{S}$ 中的第三欄$[0,1,0,0,1,0,1,1]^T$，而針對第四個禁止集合{1,3}而言，OR($\boldsymbol{S}$, {1,3})則是將 $\boldsymbol{S}$ 中的第一欄與第三欄作 bit-wise "OR"運算，得到的為結果$[0,1,0,1,1,1,1,1]^T$；因此 OR(S, X_1)|| OR(S, X_2)||...|| OR(S, $X_{|F|}$)可以表示為下列的矩陣

$$\begin{bmatrix}0&0&0&1&0&1&1&1\\0&0&1&0&1&1&0&1\\0&1&0&0&1&0&1&1\\0&1&0&1&1&1&1&1\end{bmatrix}^T$$

三、對比

令 QC_{0h} 與 QC_{1h} 分別表示白點與黑點經過加密後，在對應於合格集合 Y_h 的重疊影像上出現黑點的機率。QC_{ih} 的計算方式如下：

$$[QC_{ih}] = C \times \left(\mathrm{OR}(S, Y_1) \,||\, \mathrm{OR}(S, Y_2) \,||\, \ldots \,||\, \mathrm{OR}(S, Y_{|Q|})\right) \tag{5}$$

我們定義對應於合格集合 Y_h 的重疊影像的對比為

$$\alpha_h = QC_{1h} - QC_{0h} \tag{6}$$

對比指標 α_h 的絕對值愈大，代表由合格集合 Y_h 所構成的重疊影像的對比愈大，表示愈容易看清楚機密影像的內容；反之，如果對比指標 α_h 的絕對值愈小，則代表由合格集合 Y_h 所構成的重疊影像的對比愈小，表示愈不容易看清楚機密影像的內容。當對比指標 α_h 為負值時，表示影像呈現反白(inverse)的結果。如果考慮反白的情況(Tzeng and Hu 2002)，則對比指標可以修改為

$$\alpha_h = |QC_{1h} - QC_{0h}| \tag{7}$$

在本研究中，我們使用第(6)式的定義，也就是不考慮反白的情況。因為對比愈大人眼愈容易辨識機密訊息，因此我們的目標是求對比極大化。

四、模型之一般式

我們以 $\boldsymbol{\Gamma} = (P, F, Q)$ 的形式表示單一機密影像的任意使用結構。對於任何一個使用結構而言，我們希望在滿足安全性的限制條件之下，求解一個機率矩陣，使得對比達到極大化。$\boldsymbol{\Gamma} = (P, F, Q)$ 形式的模型如第(8)式所示。在第(8)式中，因為白點與黑點都各有 $2^{|P|}$ 種加密規則，而一種加密規則需要一個相對應的機率值，因此總共有 $2\times 2^{|P|}$ 個變數需要求解。每一個變數都是介於 0 到 1 之間的實數，且白點與黑點的所有加密規則的使用機率之總合必須分別為 1。在安全性方面，因為每一個禁止集合 $X \in F$ 所構成的重疊影像的安全性都必須被確保，因此總共有 $|F|$ 個關於安全性的限制條件。在對比方面，因為每一個合格集合 $Y \in Q$ 所構成的重疊影像的對比必須夠大，因此總共有 $|Q|$ 個最佳化的目標。這個模型可以適用在單一機密影像的任何使用結構上，前述之第(1)式與第(2)式為本模型之特例。

$$\left.\begin{array}{ll} \max & \alpha_h = QC_{1h} - QC_{0h},\ for\ h = 1,2,...,|Q|. \\ \text{s.t.} & \sigma_k = |FC_{1k} - FC_{0k}| = 0,\ for\ k = 1,2,...,|F|, \\ & \sum_{j=1}^{2^{|P|}} C_{ij} = 1,\ for\ i = 0,1, \\ & C_{ij} \in [0,1],\ for\ i = 0,1,\ and\ j = 1,2,...,2^{|P|}. \end{array}\right\} \quad (8)$$

第(8)式的模型在本質上是一個多準則決策(multiple criterion decision-making)問題或多目標最佳化模型(multi-objective optimization model)。觀察此一多目標最佳化模型，我們發現模型中所有的目標函數與限制函數皆為線性函數；因此，這是一個典型的多目標線性規劃模型(multi-objective linear programming model)。

肆、遺傳演算法的應用

一、遺傳演算法

遺傳演算法(Genetic Algorithms; GAs)是在 1970 年代由 Holland (1975)所首先提出的。它是一種模仿自然界中「適者生存，不適者淘汰」之演化法則與遺傳機制的一種搜尋演算法。GAs 是由一個族群(population)的染色體(chromosomes)與遺傳運算元(genetic operators)所構成的。在一個族群中，一個染色體所代表的是某一特定問題之解答空間中的一個答案。此外，GAs 使用適合度函數(fitness function)來評估每一個解答的好壞，並引導它在解答空間中的搜尋方向。GAs 包含三個重要的運算元：複製(reproduction)、交配(crossover)與突變(mutation)。複製運算元根據適合度來選出存活機率高的染色體，並將它們複製到交配池(mating pool)中，等待後續的遺傳運算程序。交配運算元負責將兩個染色體中的部分基因作交換，並產生新一代的染色體。突變運算元可以使染色體中的基因有機會被改變；因此，它不但能使某些原本不存在的重要基因有機會出現，還能使一個已經趨於收斂的族群，仍然有機會產生新的解答。由於 GAs 同時處理一個族群的染色體，因此，這個多點搜尋的能力使得它非常適合應用在多型態(multi-modal)與多目標(multi-objective)的最佳化問題上。再者，GAs 所處理的對象為將參數集(parameter set)編碼後的染色體(或字串)，而不是參數集本身，同時它唯一需要的資訊為適合度函數，而不需要其他輔助資訊或限制；因此，它可以很容易地被應用在各種不同的最佳化問題上。由於 GAs 所具備的這些特性，近年來，它已經被廣泛地應用到許多領域的最佳化問題上，例如影像處理、財務管理、策略規劃、機器學習、環境工程...等(Back et al. 1997; Chaiyaratana and Zalzala 1997; Srinivas and Patnaik 1994)。

二、染色體編碼與解碼

由於第(8)式的模型的變數為實數型態，因此，我們在遺傳演算法中使用實數編碼

法，即染色體上的每個基因都以實數表示。實數編碼法不但可以避免因使用二元編碼法所產生的"Hamming cliffs"與精確度的問題(Deb 2001; Srinivas and Patnaik 1994)；同時，較短的染色體長度也能獲得較佳的執行效率(Deb 2001)。在第(8)式中，我們需要求解 $2^{|P|+1}$ 個機率值：C_{ij}，其中 $i = 0, 1, j = 1, 2, \ldots, 2^{|P|}$。為了滿足第(8)式中的最後兩個限制條件，我們在 0 到 1 的實數範圍之間由小到大依序取 $2^{|P|}$-1 個數$(x'_{i1}, x'_{i2}, \ldots, x'_{i,2^{|P|}-1})$當作分割點，然後利用這 $2^{|P|}$-1 個分割點將此一範圍切割成 $2^{|P|}$段，第一段的長度代表 C_{i1}，第二段的長度代表 C_{i2}，以此類推(如圖 3 所示)。因此，我們將染色體編碼為 $\boldsymbol{x} = (x_{01}, x_{02}, \ldots, x_{0,2^{|P|}-1}, x_{11}, x_{12}, \ldots, x_{1,2^{|P|}-1})$。接著，我們分別將$(x_{01}, x_{02}, \ldots, x_{0,2^{|P|}-1})$與$(x_{11}, x_{12}, \ldots, x_{1,2^{|P|}-1})$由小到大排序後，就可以形成 0 到 1 之間的 $2^{|P|}$-1 個分割點。令$(x'_{01}, x'_{02}, \ldots, x'_{0,2^{|P|}-1}) = \text{Sort}(x_{01}, x_{02}, \ldots, x_{0,2^{|P|}-1})$，$(x'_{11}, x'_{12}, \ldots, x'_{1,2^{|P|}-1}) = \text{Sort}(x_{11}, x_{12}, \ldots, x_{1,2^{|P|}-1})$，$x'_{00} = 0$，$x'_{0,2^{|P|}} = 1$，$x'_{10} = 0$，$x'_{1,2^{|P|}} = 1$。透過這些分割點，我們可以將染色體的解碼方式設定為 $C_{ij} = x'_{ij} - x'_{i,j-1}$。

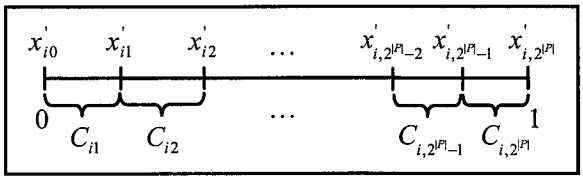


圖 3：染色體編碼方式示意圖

三、適合度函數

基於前述之染色體編碼與解碼方法，我們將對比函數寫成：$f_h(\boldsymbol{x}) = \alpha_h, for\ h = 1, 2, \ldots, |Q|$。另外，為了處理第(8)式中的第一個限制條件，我們使用懲罰函數法(penalty function approach)。我們定義的懲罰函數為$\Omega(\boldsymbol{x}) = \sum\sigma_k$，因此將限制條件考慮在內的適合度函數就可以寫成 $F_h(\boldsymbol{x}) = f_h(\boldsymbol{x}) - \theta\Omega(\boldsymbol{x})$。係數$\theta$的值會影響到滿足限制條件的程度以及收斂性。當$\theta$的值較小時，GA 較不容易因過早收斂而無法找到最佳解，但是另外一方面卻也較不容易滿足限制條件。反之，當θ的值較大時，GA 較容易滿足限制條件，但卻會有過早收斂而無法找到最佳解的問題。為了同時克服上述問題，我們在剛開始的一代設定一個較小的θ值，然後隨著代數的增加慢慢地將θ值加大。這樣的做法不但可以使得 GA 不至於太早收斂，還能使得 GA 在演化的後期能盡量在滿足限制條件的情況下來做搜尋。當演化進行到後期時，違反限制條件的懲罰會變得很大，因此那些違反限制條件的染色體存活的機率將會變得很小。我們所要求解的問題為具有$|Q|$個目標的多目標最佳化問題，在此，我們使用兼具效率與容易實作特性的加權總合法(weighted-sum approach)來解求這個問題。經過加權總合的適合度函數為 $F(\boldsymbol{x}) = \sum F_h(\boldsymbol{x})$。

四、複製

為了考量適合度可能為負值的情況，我們使用二元競賽選擇法(binary tournament selection)來進行染色體複製的程序。二元競賽選擇法的做法為：由族群中隨機挑選兩個染色體，並比較兩者的適合度，適合度較高的染色體即被複製到交配池中，重複這個隨機挑選、比較與複製的程序，直到交配池填滿染色體為止。

五、交配

為了進行實數編碼字串的交配程序，我們採用模擬二元交配法(Simulated Binary Crossover; SBX) (Deb and Agrawal 1995)。SBX 是一種模擬二元編碼字串之單點交配運作原理的實數字串交配法。其特色為父代解答附近的答案有比較高的機會成為子代解答，同時，SBX 還可以透過調整分配索引(distribution index)參數η_c，來控制遺傳演算法的搜尋能力(search power)。

六、突變

在實數編碼字串中進行突變運算最簡單的方法，就是將基因進行隨機初始化。令 y_i 代表實數編碼字串中的第 i 個基因 x_i 經過突變運算後的結果，而 $x_i^{(U)}$ 與 $x_i^{(L)}$ 則分別代表 x_i 的上限與下限。以隨機初始化來進行突變運算的方法為：

$$y_i = r_i\left(x_i^{(U)} - x_i^{(L)}\right) + x_i^{(L)} \tag{9}$$

其中 r_i 代表介於 0 與 1 之間的任意實數。此外，我們假設染色體中的每一個基因的突變機率是獨立的。

伍、實驗結果與討論

一、(2, 2)-threshold 的實驗結果

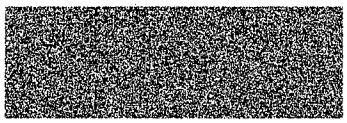
在本實驗中，有關遺傳演算法之相關參數設定如表 6 所示，其實驗結果如表 7 與圖 4 所示。在表 7 中，機率矩陣 $\boldsymbol{C}$ 顯示白點的加密規則(0, 0)、(0, 1)、(1, 0)與(1, 1)的使用機率分別為 0.5、0.0、0.0 與 0.5；而黑點的加密規則(0, 0)、(0, 1)、(1, 0)與(1, 1)的使用機率則分別為 0.0、0.5、0.5 與 0.0。在安全性方面，以這個機率矩陣 $\boldsymbol{C}$ 所產生的分享影像 Share1 與 Share2 的安全性指標分別為$\sigma_1 = 0$ 與$\sigma_2 = 0$，也就是代表 Share1 與 Share2 是絕對安全的。在對比方面，(Share1+Share2)的對比指標為$\alpha_1 = 0.5$，其中白色部分為 50%的黑($QC_{01} = 0.5$)，而黑色部分則為 100%的黑($QC_{11} = 1.0$)。

表 6：遺傳演算法之相關參數設定(一)

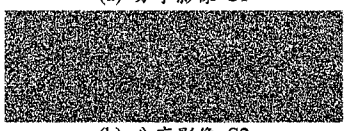
參數	設定值
族群大小	140
染色體長度	6
交配率	0.9
突變率	0.01/per gene
複製方法	二元競賽選擇法
交配法	SBX，$\eta_c = 2$
停止條件	150 代

表 7：(2, 2)-threshold 之機率矩陣及其安全性與對比分析

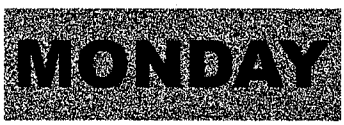
機率矩陣	
$C = \begin{bmatrix} 0.5 & 0.0 & 0.0 & 0.5 \\ 0.0 & 0.5 & 0.5 & 0.0 \end{bmatrix}$	
安全性	對比
$\sigma_1 = 0.0$ $\sigma_2 = 0.0$	$\alpha_1 = 0.5$ ($QC_{01} = 0.5$, $QC_{11} = 1.0$)



(a) 分享影像 S1



(b) 分享影像 S2



(c) S1+S2

圖 4：(2, 2)-threshold 的實驗結果

二、(2, 3)-threshold 的實驗結果

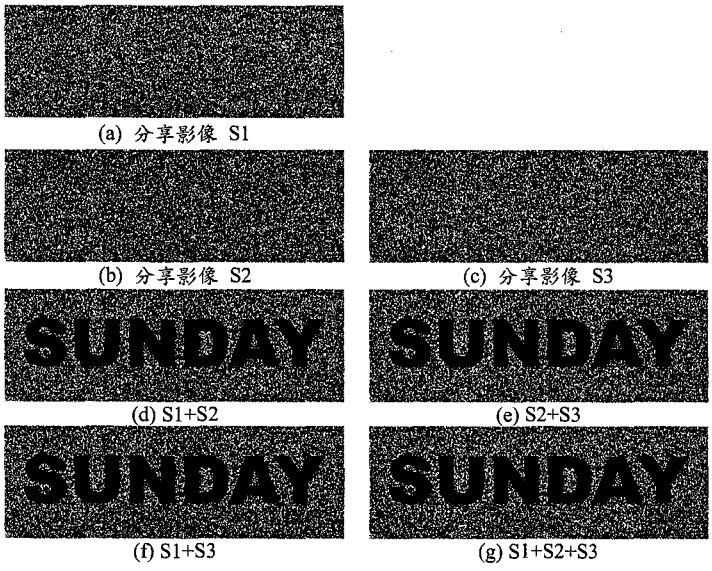
在本實驗中，有關遺傳演算法之相關參數設定如表 8 所示，其實驗結果如表 9 與圖 5 所示。在表 9 中，機率矩陣 C 顯示白點的加密規則(0, 0, 0)、(0, 0, 1)、(0, 1, 0)、(1, 0, 0)、(0, 1, 1)、(1, 1, 0)、(1, 0, 1)與(1, 1, 1)的使用機率分別為 0.33、0.0、0.0、0.0、0.01、0.0、0.0 與 0.66；而黑點的各個加密規則的使用機率則分別為 0.0、0.0、0.0、0.0、0.34、0.33、0.33 與 0.0。在安全性方面，以這個機率矩陣 C 所產生的分享影像 Share1、Share2 與 Share3 的安全性指標分別為 $\sigma_1 = 0$、$\sigma_2 = 0$ 與 $\sigma_3 = 0$，也就是代表 Share1、Share2 與 Share3 是絕對安全的。在對比方面，(Share1+Share2)、(Share2+Share3)、(Share1+Share3)與(Share1+Share2+Share3)的對比指標分別為 $\alpha_1 = 0.33$、$\alpha_2 = 0.33$、$\alpha_3 = 0.33$ 與 $\alpha_4 = 0.33$，其中白色部分皆為 67%的黑，而黑色部分皆為 100%的黑。

表 8：遺傳演算法之相關參數設定(二)

參數	設定值
族群大小	300
染色體長度	14
交配率	0.9
突變率	0.01/per gene
複製方法	二元競賽選擇法
交配方法	SBX，$\eta_c = 2$
停止條件	300 代

表 9：(2, 3)-threshold 之機率矩陣及其安全性與對比分析

機率矩陣	
$C = \begin{bmatrix} 0.33 & 0.00 & 0.00 & 0.00 & 0.01 & 0.00 & 0.00 & 0.66 \\ 0.00 & 0.00 & 0.00 & 0.00 & 0.34 & 0.33 & 0.33 & 0.00 \end{bmatrix}$	
安全性	對比
$\sigma_1 = 0.0$ $\sigma_2 = 0.0$ $\sigma_3 = 0.0$	$\alpha_1 = 0.33$ ($QC_{01} = 0.67$, $QC_{11} = 1.0$) $\alpha_2 = 0.33$ ($QC_{02} = 0.67$, $QC_{12} = 1.0$) $\alpha_3 = 0.33$ ($QC_{03} = 0.67$, $QC_{13} = 1.0$) $\alpha_4 = 0.33$ ($QC_{04} = 0.67$, $QC_{14} = 1.0$)



(a) 分享影像 S1

(b) 分享影像 S2　(c) 分享影像 S3

(d) S1+S2　(e) S2+S3

(f) S1+S3　(g) S1+S2+S3

圖 5：(2, 3)-threshold 的實驗結果

三、討論

根據 Blundo et al.(1999)的研究，(2, N)-threshold VCSs 的最佳對比為

$$\alpha^*(N)=\frac{\left\lfloor \frac{N}{2} \right\rfloor \left\lceil \frac{N}{2} \right\rceil}{N(N-1)} \tag{10}$$

而達成最佳對比的像素擴展 M 為

$$M \geq \begin{cases} 2N-2, & if\ N\ is\ even \\ N, & if\ N \equiv 3\ mod\ 4 \\ 2N, & if\ N \equiv 1\ mod\ 4 \end{cases} \tag{11}$$

因此，(2, 2)-threshold 之最佳對比為α^* = 1/2，而最小像素擴展為 M = 2；而(2, 3)-threshold 之最佳對比為α^* = 1/3，而最小像素擴展為 M = 3。為了解決影像變形的問題，分享影像的長與寬必須同時擴展為機密影像的 M 倍，也就是實際的分享影像大小為機密影像的 M^2 倍。因此，在確保影像不會產生變形的情況之下，(2, 2)-threshold 之最小像素擴展為 M = 4，而(2, 3)-threshold 之最小像素擴展則為 M = 9。本實驗結果顯示，在不作像素擴展的情況之下，在(2, 2)-threshold 與(2, 3)-threshold 這兩個使用結構上，我們所求解出的機率矩陣都能達成最佳之對比(1/2 與 1/3)。實驗證明，我們的模型不但可以達成像素不擴展的目標，也能在確保安全性的前提之下，使得重疊影像有很好的對比。

雖然我們的模型目前只適用於單一機密影像的使用結構上，但是如果稍作修改，它也是可以應用在多重機密影像的情況的。在單一機密影像的情況下，我們只需要針對白點與黑點兩種狀態進行加密。但是如果在 t 張機密影像的情況之下，我們需要考量 2^t 種加密的對象。例如，當 t = 2 時，我們會有(0, 0)、(0, 1)、(1, 0)與(1, 1)等四種加密的對象。在多重機密影像情況下，針對$|P|$個參與者，每一種加密的對象都有 $2^{|P|}$種可能的加密規則。如同單一機密影像的做法一般，我們也分別為每一個加密對象的每一個加密規則指定一個使用機率值。如此，便可建構出多重機密影像的模型。

陸、結論

在視覺密碼的研究領域中，大部分的方法都是以像素擴展為基礎的。使用以像素擴展為基礎的視覺密碼方法進行加密，其結果會導致產生出來的的分享影像的尺寸比機密影像大 M 倍。影像尺寸經過擴大後的分享影像，不但會造成儲存空間的浪費與攜帶不易的問題，同時也會導致影像的變形問題。為了解決影像變形的問題，又必須將分享影像

的長與寬同時擴展為機密影像的 M 倍。這樣的結果更進一步使得分享影像的大小變為機密影像的 M^2 倍。本研究中，我們提出一個不需要像素擴展的視覺密碼方法，來改進以像素擴展為基礎的方法的缺點。我們的方法利用機率的觀念，並且結合安全性與對比兩項指標，建構出任意使用結構的模型。我們所提出的模型可以適用於單一機密影像的任何使用結構上。在本研究中，我們使用遺傳演算法來求解最佳化的問題並產生加密用的機率矩陣。我們只要透過這個機率矩陣就可以很容易進行機密影像的加密程序。實驗結果顯示我們的方法是有效的，而且遺傳演算法在本研究中也能找到令人滿意的解答。在未來，我們將致力於研究如何改進我們的模型，使它能進一步應用於多重機密影像的使用結構上。

參考文獻

1. 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), LNCS 1099, 1996a, pp. 416-428.
2. 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.
3. Ateniese, G., Blundo, C., De Santis, A., and Stinson, D. R. "Extended Capabilities for Visual Cryptography," Theoretical Computer Science (250:1-2), 2001, pp. 143-161.
4. Back, T., Hammel, U., and Schwefel, H. P. "Evolutionary Computation: Comments on the History and Current State," IEEE Transactions on Evolutionary Computation (1:1), 1997, pp. 3-17.
5. Blundo, C., De Bonis, A., and De Santis, A. "Improved Schemes for Visual Cryptography," Designs, Codes and Cryptography (24), 2001, pp. 255-278.
6. Blundo, C., and De Santis, A. "Visual Cryptography Schemes with Perfect Reconstruction of Black Pixels," Computer & Graphics (12:4), 1998, pp. 449-455.
7. 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.
8. Chaiyaratana, N. and Zalzala, A. M. S. "Recent Developments in Evolutionary and Genetic Algorithms: Theory and Applications," Second International Conference on Genetic Algorithms in Engineering Systems: Innovations and Applications (2-4), 1997, pp. 270-277.
9. Deb, K. Multi-Objective Optimization using Evolutionary Algorithms, John Wiley & Sons, West Sussex, 2001.
10. Deb, K. and Agrawal, R. B. "Simulated Binary Crossover for Continuous Search Space," Complex Systems (9:2), 1995, pp. 115-148.
11. Droste, S. "New Results on Visual Cryptography," in Advances in

Cryptology-CRYPTO '96, LNCS 1109, Springer-Verlag, 1996, pp. 401-415.

12. Eisen, P. A., and Stinson, D. R. "Threshold Visual Cryptography Schemes with Specified Whiteness Levels of Reconstructed Pixels," Designs, Codes and Cryptography (25), 2002, pp. 15-61.
13. Hofmeister, T., Krause, M., and Simon, H. U. "Contrast-optimal k out of n Secret Sharing Schemes in Visual Cryptography," Theoretical Computer Science (240), 2000, pp. 471-485.
14. Holland, J. H. Adaptation in Natural and Artificial Systems, Ann Arbor: The University of Michigan Press, 1975.
15. Ito, R., Kuwakado, H., and Tanaka, H. "Image Size Invariant Visual Cryptography," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences (E82-A:10), 1999, pp. 2172-2177.
16. Naor, M., and Shamir, A. "Visual Cryptography," in Advances in Cryptology-EUROCRYPT '94, LNCS 950, Springer-Verlag, 1995, pp. 1-12.
17. Srinivas, M. and Patnaik, L. M. "Genetic Algorithms: A Survey," IEEE Computer (27:6), 1994, pp. 17-26.
18. Tzeng, W. G., and Hu, C. M. "A New Approach for Visual Cryptography," Designs, Codes and Cryptography (27), 2002, pp. 207-227.
19. Verheul, E. R., and van Tilborg, H. C. A. "Constructions and Properties of k out of n Visual Secret Sharing Schemes," Designs, Codes and Cryptography (11), 1997, pp. 179-196.