以機率為基礎之像素不擴展的多機密影像視覺密碼最佳化模型

A Probability-based Optimization Model for Sharing Multiple Secret Images without Pixel Expansion

侯永昌
國立中央大學資訊管理研究所
320 桃園縣中壢市五權里 2 鄰中大路 300 號
E-mail: ychou@mgt.ncu.edu.tw

許慶昇
國立中央大學資訊管理研究所
320 桃園縣中壢市五權里 2 鄰中大路 300 號
E-mail: cshsu60@ms52.hinet.net

摘要

視覺密碼方法的特色在於其解密過程是透過人類視覺系統，而不需要利用任何計算機資源與複雜的解密演算法。因此，在一些無法使用電腦解密的情況下，視覺式的秘密分享方法是一個很好的解決方案。大部分的視覺密碼方法都是使用像素擴展的技巧；因此，分享影像的大小會被擴展成機密影像的若干倍。像素擴展的結果不但使得分享影像不易攜帶，也會造成儲存空間的浪費。此外，大部分的視覺密碼方法只允許分享單一機密影像，而無法分享多張機密影像。在本文中，我們提出一個不需要像素擴展，又能分享多張機密影像的視覺密碼方法。我們的方法使用機率的觀念，並且結合安全性與對比兩項指標，建構出多機密影像視覺密碼方法的多目標最佳化模型。此外，我們利用遺傳演算法來求解多目標最佳化的問題。實驗結果顯示，我們的方法不但能達成像素不擴展與分享多張機密影像的目的；同時，遺傳演算法也能找到令人滿意的解答。

關鍵詞：視覺密碼、視覺機密分享、遺傳演算法。

Abstract

Visual cryptography is characterized by its decryption process that is done by human eyes; that is, there is no need for computers and complex decryption algorithms. Consequently, it is a good solution while computers are not available for decryption. Most visual cryptography methods are based on the technique of pixel expansion; therefore, the size of each share is larger than that of the secret image. Pixel expansion not only results in distortion of shares, but also consumes much more storage space. Besides, most visual cryptography schemes are limited to share only one secret image, whereas the ability to share multiple secret images is not available. In this paper, we propose a method to share multiple secret images without pixel expansion. Our method uses the concept of probability and considers both security and contrast to construct a multi-objective optimization model. To solve the optimization problems, we employ genetic algorithms. Experimental results show that our method is effective in sharing multiple secret images without pixel expansion. Additionally,

experimental results also indicate that genetic algorithms can find satisfactory solutions.

Keywords: Visual Cryptography, Visual Secret Sharing, Genetic Algorithms

一、簡介

視覺密碼的觀念是由 Naor 與 Shamir [17]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。一個視覺密碼方法(visual cryptography scheme)可以將一張機密影像加密成 N 張分享影像，一群參與機密分享的每一個參與者(participants)分別持有一張分享影像。在這一群參與者中，被允許獲得機密訊息的一群人，將他們所持有的分享影像全部重疊在一起之後，就可以透過眼睛在這個重疊影像上看到機密訊息；然而，未被允許獲得機密訊息的一群人，便無法透過它們所持有的分享影像來獲得任何一絲機密訊息。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的知識與計算機資源。因此，在一些無法使用電腦解密的情況下，視覺式的秘密分享方法是一個很好的解決方案。

Naor 與 Shamir [17]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 $P = \{1, 2, \ldots, N\}$ 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[1-3]。Ateniese et al. [2]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) $Y \in \Gamma_{Qual}$ 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。在視覺密碼的研究中，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[5, 7, 12, 13, 17, 19, 20]。大部分的視覺密碼方法都使用像素擴展的技巧[1-3, 5-7, 11-13, 17, 19, 20]，只有少數的研究是關於像素不擴展的[15, 16]。像素擴展的方法將機密影像上的一個點，分解成具有 M 個點的子像素群；因此，分享影像的大小被擴展為機密影像的 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原先的長與寬的比例，因此就更不易攜帶也更耗費儲存空間了。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[3, 17]。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的影像的秘密分享方式，有其實際的應用價值。就機密影像數目來看，大部分的視覺密碼方法都只探討單機密影像的分享方式，只有少數的研究是關於多機密影像的分享方法。Droste [11]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。多機密影像的觀念不但能使秘密分享方式更富於變化；同時，也使得所需的資訊量大為降低。

綜觀視覺密碼學的研究，關於不需要像素擴展，而又能分享多張機密影像的方法可謂付之闕如。在本文中，我們提出一個不需要像素擴展的多機密影像視覺密碼方法。我們使用機率的觀念，並且結合安全性與對比兩項指標，建構出視覺密碼方法的多目標最佳化模型。在不作像素擴展的前提之下，我們的最佳化模型不但可以處理單機密影像

與多機密影像的任意使用結構；同時，它也可以處理有意義之分享影像的任意使用結構。實驗結果顯示，我們的方法不但能達成像素不擴展與分享多張機密影像的目的；同時，遺傳演算法也能找到令人滿意的解答。

二、無須像素擴展的多機密影像視覺密碼方法

1. 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。$\boldsymbol{\Gamma} = (P, F, Q)$稱為一個使用結構(access structure) [19]，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 $Q \cap F = \varnothing$。$\boldsymbol{\Gamma} = (P, F, Q)$的形式只能表達單一機密影像的分享規則，為了表達多機密影像的分享規則，我們將 $\boldsymbol{\Gamma} = (P, F, Q)$進一步擴充為$\Psi = (T, P, F, Q, \Omega)$的形式，其中 $T = \{1, 2, \ldots, m\}$代表機密影像的集合，而$\Omega(Y \in Q) \in T$則代表解密目標影像，也就是說Ω決定合格集合 Y 中的所有參與者可以獲得哪一張機密影像的訊息。

在本文中，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"∨"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 $X = \{i_1, i_2, \ldots, i_q\} \subseteq P$，我們定義函數 $\mathrm{OR}(S, X) = S_{i_1}^c \vee S_{i_2}^c \vee \ldots \vee S_{i_q}^c$。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 S1, S2, …, SN 皆代表分享影像，我們以(S1 + S2 + … + SN)表示 S1, S2, …, SN 的重疊影像(stacked share)。

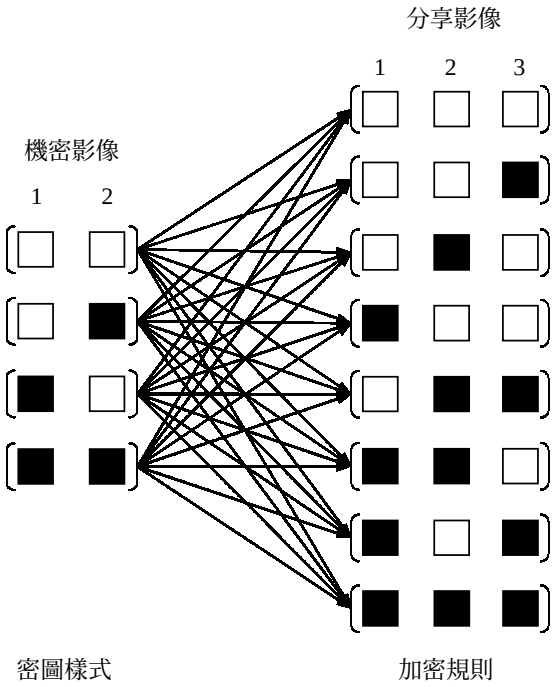
在本文中，我們將利用一個使用結構範例 AS_T2P3，來說明不需要像素擴展的多機密影像視覺機密分享的做法。為了方便後續的說明，我們在此定義這個使用結構如下：

使用結構範例 AS_T2P3：

$\Psi = (T, P, F, Q, \Omega)$，其中 $T = \{1, 2\}$，$P = \{1, 2, 3\}$，$F = \{\{1\}, \{2\}, \{3\}\}$，$Q = \{\{1 ,2\}, \{2, 3\}, \{1, 3\}\}$，且

$$\Omega(Y) = \begin{cases} 1, & \text{if } Y = \{1, 2\} \text{ or } Y = \{1, 3\} \\ 2, & \text{if } Y = \{2, 3\} \\ 0, & \text{otherwise} \end{cases} \quad 。$$

AS_T2P3 定義了兩張機密影像($|T| = 2$)與三個參與者($|P| = 3$)的機密分享規則。其中禁止集合的集合 F 表示，第一、第二與第三張分享影像皆為雜亂無章的影像；合格集合的集合 Q 與函數Ω則表示，將第一與第二或是第一與第三張分享影像重疊後皆可重建第一張機密影像，而將第二與第三張分享影像重疊後則可重建第二張機密影像。



圖一：兩張機密影像與三個參與者的密圖樣式與加密規則

2. 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。

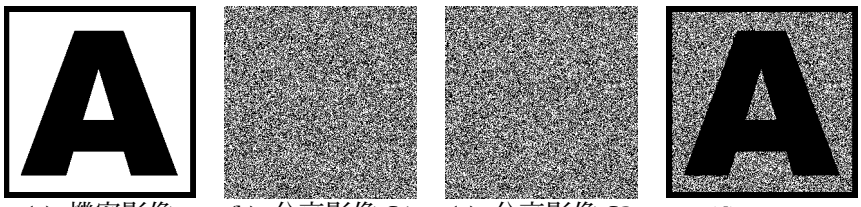
對於$|T|$張相同大小的黑白機密影像而言，由於影像上的每一個點只可能為白色或黑色，所以在同一個影像位置座標上，其$|T|$個點的顏色排列方式一共有 $2^{|T|}$種可能的情況。例如，當機密影像個數為$|T| = 2$ 時，在第一張與第二張影像的同一個位置座標上，所有可能的顏色排列方式包含(白，白)、(白，黑)、(黑，白)與(黑，黑)等四種可能的情況。因此，在加密時應該考量這 $2^{|T|}$種情況應如何被分解成分享影像。在本文中，我們稱$|T|$張黑白機密影像的每一個可能的顏色排列方式為「密圖樣式」(secret pattern)。在不作像素擴展的情況下，當一個密圖樣式被加密之後，在每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，如果要產生$|P|$張分享影像的話，則一共會有 $2^{|P|}$種可能的加密方式。例如當分享影像個數為$|P| = 3$ 時，對於任何一個密圖樣式而言，我們都可以使用(白, 白, 白)、(白, 白, 黑)、(白, 黑, 白)、(黑, 白, 白)、(白, 黑, 黑)、(黑, 黑, 白)、(黑, 白, 黑)與(黑, 黑, 黑)等八種可能的加密方式的其中一種來將它放置到三個分享影像上。在本文中，我們稱每一個可能的加密方式為「加密規則」(encryption rule)。$|T|$張密圖有 $2^{|T|}$種密圖樣式，每一種密圖樣式在分享影像上又可以由 $2^{|P|}$種加密規則所建構而成，因此可以產生 $2^{|T|}\times 2^{|P|}$種配對方式。圖一即顯示出在兩張機密影像與三張分享影像的情況下，其密圖樣式與加密規則的關係。每一種配對方式出現的機率就可以影響到分享影像疊合的結果。

因為不同加密規則機率值的設定對安全性與對比會產生不同程度的影響；因此，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。表一與表二分別顯示(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，其結果如圖二與圖三所示。在表一與表二中，(S_{j1}, S_{j2})代表分享影像 S1 與分享影像 S2 上第 j 個可能的加密規則，而 S_{j3} 則代表將分享影像 S1 與 S2 疊合之後的結果$(S_{j1} \vee S_{j2})$，其中 0 代表白點，1 代表黑點；C_{1j} (C_{2j})代表以第 j 個加密規則來加密一個白點(黑點)的機率值。表一顯示在 S1 上，密圖上的白點經過加密後，出現黑點的機率為 $FC_{11} = S_{11}\times C_{11} + S_{21}\times C_{12} + S_{31}\times C_{13} + S_{41}\times C_{14} = 0.5$；而密圖上的黑點經過加密後，出現黑點的機率 FC_{21} 也是 0.5 ($FC_{21} = S_{11}\times C_{21} + S_{21}\times C_{22} + S_{31}\times C_{23} + S_{41}\times C_{24} = 0.5$)。因為密圖上的黑點與白點經過加密程序後，在 S1 上都具有相同的黑點出現機率($FC_{11} = FC_{21}$)，也就是沒有出現色差，因此安全性可以得到確保。在 S2 上的情況也是一樣($FC_{12} = 0.5$, $FC_{22} = 0.5$)，因此 S2 的安全性也可以得到確保。但是在重疊影像(S1+S2)上，密圖上的白點經過加密後，出現黑點的機率為 $QC_{11} = S_{13}\times C_{11} + S_{23}\times C_{12} + S_{33}\times C_{13} + S_{43}\times C_{14} = 0.5$；密圖上的黑點經過加密後，出現黑點的機率為 $QC_{21} = S_{13}\times C_{21} + S_{23}\times C_{22} + S_{33}\times C_{23} + S_{43}\times C_{24} = 1$。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

表一：具有良好的安全性與良好的對比之機率值設定

機密影像像素顏色	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	$S_{11} = 0$	$S_{12} = 0$	$S_{13} = 0$	$C_{11} = 0.5$	$FC_{11} = 0.5$	$FC_{12} = 0.5$	$QC_{11} = 0.5$
	$S_{21} = 0$	$S_{22} = 1$	$S_{23} = 1$	$C_{12} = 0.0$			
	$S_{31} = 1$	$S_{32} = 0$	$S_{33} = 1$	$C_{13} = 0.0$			
	$S_{41} = 1$	$S_{42} = 1$	$S_{43} = 1$	$C_{14} = 0.5$			
1	$S_{11} = 0$	$S_{12} = 0$	$S_{13} = 0$	$C_{21} = 0.0$	$FC_{21} = 0.5$	$FC_{22} = 0.5$	$QC_{21} = 1.0$
	$S_{21} = 0$	$S_{22} = 1$	$S_{23} = 1$	$C_{22} = 0.5$			
	$S_{31} = 1$	$S_{32} = 0$	$S_{33} = 1$	$C_{23} = 0.5$			
	$S_{41} = 1$	$S_{42} = 1$	$S_{43} = 1$	$C_{24} = 0.0$			

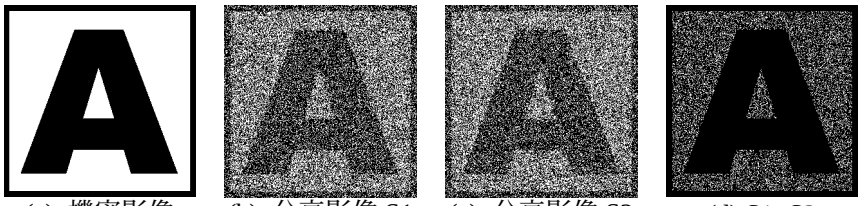


(a) 機密影像 (b) 分享影像 S1 (c) 分享影像 S2 (d) S1+S2

圖二：具有良好的安全性與良好的對比之範例(300×300 pixels, 300 dpi)

表二：具有不良的安全性與普通的對比之機率值設定

機密影像像素顏色	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	$S_{11} = 0$	$S_{12} = 0$	$S_{13} = 0$	$C_{11} = 0.25$	$FC_{11} = 0.5$	$FC_{12} = 0.5$	$QC_{11} = 0.75$
	$S_{21} = 0$	$S_{22} = 1$	$S_{23} = 1$	$C_{12} = 0.25$			
	$S_{31} = 1$	$S_{32} = 0$	$S_{33} = 1$	$C_{13} = 0.25$			
	$S_{41} = 1$	$S_{42} = 1$	$S_{43} = 1$	$C_{14} = 0.25$			
1	$S_{11} = 0$	$S_{12} = 0$	$S_{13} = 0$	$C_{21} = 0.00$	$FC_{21} = 0.75$	$FC_{22} = 0.75$	$QC_{21} = 1.0$
	$S_{21} = 0$	$S_{22} = 1$	$S_{23} = 1$	$C_{22} = 0.25$			
	$S_{31} = 1$	$S_{32} = 0$	$S_{33} = 1$	$C_{23} = 0.25$			
	$S_{41} = 1$	$S_{42} = 1$	$S_{43} = 1$	$C_{24} = 0.50$			



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

圖三：具有不良的安全性與普通的對比之範例(300×300 pixels, 300 dpi)

高($QC_{21} > QC_{11}$)，因此可以透過黑與白的色差，進而辨識出機密影像的內容(見圖二)。

表二的機率值設定雖然可以在重疊影像(S1+S2)上呈現白與黑的差異($QC_{11} < QC_{21}$)，但是在 S1 與 S2 上，代表白與黑的黑點出現機率並不相同($FC_{11} < FC_{21}$, $FC_{12} < FC_{22}$)，因此會洩露出機密影像的蛛絲馬跡，而使其安全性無法得到確保(見圖三)。

3. AS_T2P3 的最佳化模型

在本節中，我們將介紹 AS_T2P3 的最佳化模型。因為在 AS_T2P3 的使用結構中，機密影像個數為$|T| = 2$ 且參與者個數為$|P| = 3$，所以一共有 $2^{|T|} = 4$ 個密圖樣式與 $2^{|P|} = 8$ 個加密規則。在表三中，(R_{i1}, R_{i2})代表第 i 個密圖樣式，(S_{j1}, S_{j2}, S_{j3})代表第 j 個加密規則，而 C_{ij} 則代表使用第 j 個加密規則來加密第 i 個密圖樣式的機率，其中 $i = 1, 2, 3, 4$，且 $j = 1, 2, \ldots, 8$。另外，FC_{i1}、FC_{i2} 與 FC_{i3} 分別代表第 i 個密圖樣式經過加密後，在對應於禁止集合 $X_1 = \{1\}$、$X_2 = \{2\}$與 $X_3 = \{3\}$的分享影像上出現黑點的機率，而 QC_{i1}、QC_{i2} 與 QC_{i3} 則分別代表第 i 個密圖樣式經過加密後，在對應於合格集合 $Y_1 = \{1, 2\}$、$Y_2 = \{2, 3\}$ 與 $Y_3 = \{1, 3\}$的重疊影像上出現黑點的機率，其中 $i = 1, 2, 3, 4$。

就安全性的角度而言，兩張機密影像上的所有可能的密圖樣式(0, 0)、(0, 1)、(1, 0)與(1, 1)經過加密後，在分享影像 S1、分享影像 S2 與分享影像 S3 上必須有相同的黑點出現機率；也就是 $FC_{11} = FC_{21} = FC_{31} = FC_{41}$、$FC_{12} = FC_{22} = FC_{32} = FC_{42}$ 且 $FC_{13} = FC_{23} = FC_{33} = FC_{43}$。如果它們不相等，則在 S1、S2 與 S3 上就可能因為黑點出現頻率的變化，而透露出機密影像中的訊息；如此，安全性便無法得到確保。在此，我們分別以$\{FC_{11}, FC_{21}, FC_{31}, FC_{41}\}$、$\{FC_{12}, FC_{22}, FC_{32}, FC_{42}\}$與$\{FC_{13}, FC_{23}, FC_{33}, FC_{43}\}$的標準差$\sigma_1$、$\sigma_2$ 與 σ_3 來代表 S1、S2 與 S3 的安全性指標。安全性指標σ_1、σ_2 與σ_3 的值愈大，代表在 S1、S2 與 S3 上，對應於所有可能的密圖樣式的黑點出現機率的差異愈大；當黑點的出現頻率產生較大的變化時，就有可能會透露出機密訊息。因此，σ_1、σ_2 與σ_3 的值愈大，代表 S1、S2 與 S3 愈不安全。反之，當安全性指標σ_1、σ_2 與σ_3 的值愈小，代表 S1、S2 與 S3

表三：AS_T2P3 的最佳化模型分析表格

R_{im} (i=1,…,$2^{\|T\|}$, m=1,…,$\|T\|$)		S_{jn} (j=1,…,$2^{\|P\|}$, n=1,…,$\|P\|$)			C_{ij}	FC_{ik} (k = 1, …, $\|F\|$)			QC_{ih} (h = 1, …, $\|Q\|$)		
						X_1={1}	X_2={2}	X_3={3}	Y_1={1,2}	Y_2={2,3}	Y_3={1,3}
R_{11}=0	R_{12}=0	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}
		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}						
R_{21}=0	R_{22}=1	S_{11}=0	S_{12}=0	S_{13}=0	C_{21}	FC_{21} = C_{24}+C_{26}+C_{27}+C_{28}	FC_{22} = C_{23}+C_{25}+C_{26}+C_{28}	FC_{23} = C_{22}+C_{25}+C_{27}+C_{28}	QC_{21} = C_{23}+C_{24}+C_{25}+C_{26}+ C_{27}+C_{28}	QC_{22} = C_{22}+C_{23}+C_{25}+C_{26}+ C_{27}+C_{28}	QC_{23} = C_{22}+C_{24}+C_{25}+C_{26}+ C_{27}+C_{28}
		S_{21}=0	S_{22}=0	S_{23}=1	C_{22}						
		S_{31}=0	S_{32}=1	S_{33}=0	C_{23}						
		S_{41}=1	S_{42}=0	S_{43}=0	C_{24}						
		S_{51}=0	S_{52}=1	S_{53}=1	C_{25}						
		S_{61}=1	S_{62}=1	S_{63}=0	C_{26}						
		S_{71}=1	S_{72}=0	S_{73}=1	C_{27}						
		S_{81}=1	S_{82}=1	S_{83}=1	C_{28}						
R_{31}=1	R_{32}=0	S_{11}=0	S_{12}=0	S_{13}=0	C_{31}	FC_{31} = C_{34}+C_{36}+C_{37}+C_{38}	FC_{32} = C_{33}+C_{35}+C_{36}+C_{38}	FC_{33} = C_{32}+C_{35}+C_{37}+C_{38}	QC_{31} = C_{33}+C_{34}+C_{35}+C_{36}+ C_{37}+C_{38}	QC_{32} = C_{32}+C_{33}+C_{35}+C_{36}+ C_{37}+C_{38}	QC_{33} = C_{32}+C_{34}+C_{35}+C_{36}+ C_{37}+C_{38}
		S_{21}=0	S_{22}=0	S_{23}=1	C_{32}						
		S_{31}=0	S_{32}=1	S_{33}=0	C_{33}						
		S_{41}=1	S_{42}=0	S_{43}=0	C_{34}						
		S_{51}=0	S_{52}=1	S_{53}=1	C_{35}						
		S_{61}=1	S_{62}=1	S_{63}=0	C_{36}						
		S_{71}=1	S_{72}=0	S_{73}=1	C_{37}						
		S_{81}=1	S_{82}=1	S_{83}=1	C_{38}						
R_{41}=1	R_{42}=1	S_{11}=0	S_{12}=0	S_{13}=0	C_{41}	FC_{41} = C_{44}+C_{46}+C_{47}+C_{48}	FC_{42} = C_{43}+C_{45}+C_{46}+C_{48}	FC_{43} = C_{42}+C_{45}+C_{47}+C_{48}	QC_{41} = C_{43}+C_{44}+C_{45}+C_{46}+ C_{47}+C_{48}	QC_{42} = C_{42}+C_{43}+C_{45}+C_{46}+ C_{47}+C_{48}	QC_{43} = C_{42}+C_{44}+C_{45}+C_{46}+ C_{47}+C_{48}
		S_{21}=0	S_{22}=0	S_{23}=1	C_{42}						
		S_{31}=0	S_{32}=1	S_{33}=0	C_{43}						
		S_{41}=1	S_{42}=0	S_{43}=0	C_{44}						
		S_{51}=0	S_{52}=1	S_{53}=1	C_{45}						
		S_{61}=1	S_{62}=1	S_{63}=0	C_{46}						
		S_{71}=1	S_{72}=0	S_{73}=1	C_{47}						
		S_{81}=1	S_{82}=1	S_{83}=1	C_{48}						

愈安全。

此外，由表三之分析得知，兩張機密影像上的所有可能的密圖樣式經過加密後，在重疊影像(S1+S2)上，對應於解密目標影像Ω({1, 2}) = 1 之黑色區域的黑點出現機率為 QC_{31} 與 QC_{41}；對應於白色區域的黑點出現機率為 QC_{11} 與 QC_{21}。為了表達(S1+S2)上代表黑色區域與代表白色區域的黑色程度，我們以 QC_{31} 與 QC_{41} 的平均值 b_1 來表示黑點的黑色程度；另外，我們以 QC_{11} 與 QC_{21} 的平均值 w_1 來表示白點的黑色程度。就對比的角度而言，b_1 與 w_1 的差異必須要夠大，才能透過人眼辨識機密訊息。因此，我們希望對比(b_1 - w_1)愈大愈好。在此，我們以$\alpha_1 = b_1 - w_1 = 0.5(QC_{31} + QC_{41} - QC_{11} - QC_{21})$來代表(S1+S2)的對比指標。對比指標$\alpha_1$的值愈大，代表重疊影像(S1+S2)的對比愈大；反之，如果對比指標α_1的值愈小，則代表 (S1+S2)的對比愈小。另外有一點值得注意的是，如果 QC_{31} 與 QC_{41} (QC_{11} 與 QC_{21})的差異太大，則在(S1+S2)上代表黑色(白色)的區域，其黑點的分布將會不夠均勻，進而影響重疊影像的影像品質；此外，由於頻率上的變化可能會透露出機密影像的訊息，所以重疊影像的安全性也會因此降低。因此，我們以 $\sigma_1^b = \left|QC_{31} - QC_{41}\right|$ 來代表(S1+S2)上代表黑色區域的黑點分布均勻程度與安全性，而

$\sigma_1^w = |QC_{11} - QC_{21}|$則代表白色區域的黑點分布均勻程度與安全性。因此，當σ_1^b (σ_1^w)的值愈大，表示在(S1+S2)上代表黑色(白色)的區域的黑點分布愈不均勻，其安全性也愈差；反之，當σ_1^b (σ_1^w)的值愈小，表示在(S1+S2)上代表黑色(白色)的區域的黑點分布愈均勻，其安全性也愈好。

同樣地，在重疊影像(S2+S3)上，對應於解密目標影像Ω({2, 3}) = 2 之黑色區域的黑點出現機率為 QC_{22} 與 QC_{42}；對應於白色區域的黑點出現機率為 QC_{12} 與 QC_{32}。因此，我們以$\alpha_2 = 0.5(QC_{22} + QC_{42} - QC_{12} - QC_{32})$來代表(S2+S3)的對比指標；以$\sigma_2^b = |QC_{22} - QC_{42}|$來代表黑色區域的黑點分布均勻程度與安全性；以$\sigma_2^w = |QC_{12} - QC_{32}|$來代表白色區域的黑點分布均勻程度與安全性。最後，在重疊影像(S1+S3)上，對應於解密目標影像Ω({1, 3}) = 1 之黑色區域的黑點出現機率為 QC_{33} 與 QC_{43}；對應於白色區域的黑點出現機率為 QC_{13} 與 QC_{23}；因此，我們以$\alpha_3 = 0.5(QC_{33} + QC_{43} - QC_{13} - QC_{23})$來代表(S1+S3)的對比指標；以$\sigma_3^b = |QC_{33} - QC_{43}|$來代表黑色區域的黑點分布均勻程度與安全性；以$\sigma_3^w = |QC_{13} - QC_{23}|$來代表白色區域的黑點分布均勻程度與安全性。

基於安全性與對比的考量，我們的目標是在滿足安全性的限制條件之下(也就是$\sigma_1 = 0, \sigma_2 = 0, \sigma_3 = 0$, $\sigma_1^b = 0$, $\sigma_2^b = 0$, $\sigma_3^b = 0$, $\sigma_1^w = 0$, $\sigma_2^w = 0$ 且$\sigma_3^w = 0$)，求解每個密圖樣式的所有可能的加密規則的使用機率(C_{ij}，其中 $i = 1, 2, 3, 4$，且 $j = 1, 2, \ldots, 8$)，使對比(α_1、α_2 與α_3)能達到極大化。根據以上的分析，我們建構出的 AS_T2P3 的最佳化模型如第(1)式所示，其中函數 STD(A)代表集合 A 中的所有元素的標準差。

$$
\left.\begin{array}{ll}
\max. & \alpha_1 = 0.5(QC_{31} + QC_{41} - QC_{11} - QC_{21}). \\
\max. & \alpha_2 = 0.5(QC_{22} + QC_{42} - QC_{12} - QC_{32}). \\
\max. & \alpha_3 = 0.5(QC_{33} + QC_{43} - QC_{13} - QC_{23}). \\
\text{s.t.} & \sigma_1 = \mathrm{STD}(\{FC_{11}, FC_{21}, FC_{31}, FC_{41}\}) = 0, \\
& \sigma_2 = \mathrm{STD}(\{FC_{12}, FC_{22}, FC_{32}, FC_{42}\}) = 0, \\
& \sigma_3 = \mathrm{STD}(\{FC_{13}, FC_{23}, FC_{33}, FC_{43}\}) = 0, \\
& \sigma_1^b = |QC_{31} - QC_{41}| = 0, \\
& \sigma_2^b = |QC_{22} - QC_{42}| = 0, \\
& \sigma_3^b = |QC_{33} - QC_{43}| = 0, \\
& \sigma_1^w = |QC_{11} - QC_{21}| = 0, \\
& \sigma_2^w = |QC_{12} - QC_{32}| = 0, \\
& \sigma_3^w = |QC_{13} - QC_{23}| = 0, \\
& \sum_{j=1}^{8} C_{ij} = 1, \; for\; i = 1, 2, 3, 4, \\
& C_{ij} \in [0, 1], \; for\; i = 1, 2, 3, 4, \; and \; j = 1, 2, \ldots, 8.
\end{array}\right\} \quad (1)
$$

三、任意使用結構之最佳化模型

1. 密圖樣式矩陣、加密規則矩陣與機率矩陣

令 $\boldsymbol{R} = [R_{im}]$為一個 $2^{|T|} \times |T|$的二元矩陣，其中 $R_{im} \in \{0, 1\}$。我們稱 $\boldsymbol{R}$ 為密圖樣式矩陣，用以表達在機密影像集合 T 之下的所有可能的密圖樣式。$\boldsymbol{R}$ 中每一個列向量 $\boldsymbol{R_i} = [R_{i1},$

$R_{i2},\ldots, R_{i|T|}$]代表一個密圖樣式，是加密的基本單位。例如，當$|T| = 2$時，$\boldsymbol{R_i} = [0, 1]$表示在第一張與第二張機密影像的相對應的位置上分別為白點與黑點。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，$\boldsymbol{S_j} = [1, 0, 0]$表示以第 j 個加密規則來加密一個密圖樣式後，會在第一、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 $2^{|T|}\times2^{|P|}$的矩陣，其中 $C_{ij} \in [0, 1]$且

$$\sum_{j=1}^{2^{|P|}} C_{ij} = 1。$$

我們稱 $\boldsymbol{C}$ 為機率矩陣，C_{ij} 代表使用第 j 個加密規則 $\boldsymbol{S_j}$ 來加密第 i 個密圖樣式 $\boldsymbol{R_i}$ 的機率。以 AS_T2P3 的使用結構為例，其密圖樣式矩陣、加密規則矩陣與機率矩陣可以分別表示成：

$$R = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}^T, \tag{2}$$

$$S = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}^T, \tag{3}$$

$$C = \begin{bmatrix} C_{11} & C_{12} & C_{13} & C_{14} & C_{15} & C_{16} & C_{17} & C_{18} \\ C_{21} & C_{22} & C_{23} & C_{24} & C_{25} & C_{26} & C_{27} & C_{28} \\ C_{31} & C_{32} & C_{33} & C_{34} & C_{35} & C_{36} & C_{37} & C_{38} \\ C_{41} & C_{42} & C_{43} & C_{44} & C_{45} & C_{46} & C_{47} & C_{48} \end{bmatrix}。 \tag{4}$$

2. 禁止集合的安全性

令 FC_{ik} 代表第 i 個密圖樣式經過加密後，在對應於禁止集合 $X_k \in F$ 的重疊影像上出現黑點的機率。FC_{ik} 的計算方式如下：

$$\left[FC_{ik}\right] = C \times \left(\mathrm{OR}(S, X_1) \,\|\, \mathrm{OR}(S, X_2) \,\|\, \ldots \,\|\, \mathrm{OR}(S, X_{|F|})\right)。 \tag{5}$$

以安全性的角度而言，如果$|T|$張機密影像上的每一個密圖樣式經過加密後，在對應於 X_k 的重疊的影像上都具有相同的黑點出現機率，則由於無法透過頻率變化的分析來窺探機密訊息，因而使安全性可以得到確保。因此，當 $FC_{1k} = FC_{2k} = \ldots = FC_{2^{|T|}k}$ 時，就代表對應於 X_k 的重疊影像是絕對安全的。反之，如果它們不相等，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 X_k 的重疊影像的安全性為 $FC_{1k}, FC_{2k}, \ldots, FC_{2^{|T|}k}$ 的標準差σ_k。安全性指標σ_k的計算如下：

$$\overline{FC_k} = \frac{\sum_{i=1}^{2^{|T|}} FC_{ik}}{2^{|T|}}, \tag{6}$$

$$\sigma_k = \sqrt{\frac{\sum_{i=1}^{2^{|T|}} \left(FC_{ik} - \overline{FC_k}\right)^2}{2^{|T|}}}。 \tag{7}$$

安全性指標σ_k的值愈大，代表在對應於 X_k 的重疊影像上，其相對於所有可能的密圖樣式的黑點出現頻率產生愈大的變化；當黑點的出現頻率產生愈大的變化時，就愈有可能會因為頻率的變化而透露出機密訊息，因而使得應於 X_k 的重疊影像的安全性變的愈差。因此，當σ_k的值愈大，代表對應於 X_k 的重疊影像愈不安全。反之，當σ_k的值愈小，代表對應於 X_k 的重疊影像愈安全。當$\sigma_k = 0$ 時，代表對應於 X_k 的重疊影像是絕對安全的。

3. 對比

令 QC_{ih} 代表第 i 個密圖樣式經過加密後，在對應於合格集合 $Y_h \in Q$ 的重疊影像上出現黑點的機率。QC_{ih} 的計算方式如下：

$$[QC_{ih}] = C \times \left(\mathrm{OR}(S, Y_1) \,||\, \mathrm{OR}(S, Y_2) \,||\, ... \,||\, \mathrm{OR}(S, Y_{|Q|})\right)。 \tag{8}$$

$\{QC_{1h}, QC_{2h}, ..., QC_{2^{|T|}h}\}$可以進一步區分成兩部分：一部分對應於解密目標影像$\Omega(Y_h)$為黑點的部分

$$B_h = \left\{QC_{ih} \middle| R_{ig} = 1, where\ g = \Omega(Y_h), i = 1, 2, ..., 2^{|T|}\right\};$$

另一部分對應於解密的目標影像$\Omega(Y_h)$為白點的部分

$$W_h = \left\{QC_{ih} \middle| R_{ig} = 0, where\ g = \Omega(Y_h), i = 1, 2, ..., 2^{|T|}\right\}。$$

我們定義對應於 Y_h 的重疊影像的黑點灰階值的平均數 b_h 和白點灰階值的平均數 w_h 為：

$$b_h = \frac{1}{2^{|T|-1}} \cdot \sum_{i=1}^{2^{|T|}} \left(QC_{ih} \cdot R_{ig}\right), where\ g = \Omega(Y_h), \tag{9}$$

$$w_h = \frac{1}{2^{|T|-1}} \cdot \sum_{i=1}^{2^{|T|}} \left(QC_{ih} \cdot \left(1 - R_{ig}\right)\right), where\ g = \Omega(Y_h)。 \tag{10}$$

因此，對應於 Y_h 的重疊影像之對比可被定義為：

$$\alpha_h = b_h - w_h。 \quad (11)$$

對比指標α_h的絕對值愈大，表示在對應於 Y_h 的重疊影像上，代表白色區域與代表黑色區域的黑點出現機率的差異愈大，也就是白色與黑色的差異會顯得愈明顯；因此，就可很容易透過眼睛來辨識機密訊息。反之，如果對比指標α_h的絕對值愈小，代表白色區域與代表黑色區域的黑點出現機率的差異愈小，也就是白色與黑色的差異會顯得愈不明顯；因此，就不容易透過眼睛來辨識機密訊息。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[19]，則對比指標可以修改為：

$$\alpha_h = |b_h - w_h|。 \quad (12)$$

在本研究中，我們使用第(11)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α_h極大化。

4. 合格集合的安全性

針對不同的密圖樣式，如果 B_h 的變異程度太大，在對應於 Y_h 的重疊影像上代表黑色的區域，其黑點的分佈將會不夠均勻；同樣地，如果 W_h 的變異程度太大，在對應於 Y_h 的重疊影像上代表白色的區域，黑點的分佈也會不夠均勻。B_h 與 W_h 的變異程度除了會影響重疊影像的品質之外，由於頻率上的變化可能會透露出機密影像的訊息，進而影響重疊影像的安全性；因此，為了使安全性能被確保，B_h 與 W_h 的變異程度應該愈小愈好。令σ_h^b與σ_h^w分別代表 B_h 與 W_h 的標準差，其計算方式如下：

$$\sigma_h^b = \sqrt{\frac{\sum_{i=1}^{2^{|T|}} \left(QC_{ih} - b_h\right)^2 \cdot R_{ig}}{2^{|T|-1}}}, where\ g = \Omega\left(Y_h\right), \quad (13)$$

$$\sigma_h^w = \sqrt{\frac{\sum_{i=1}^{2^{|T|}} \left(QC_{ih} - w_h\right)^2 \cdot \left(1 - R_{ig}\right)}{2^{|T|-1}}}, where\ g = \Omega\left(Y_h\right)。 \quad (14)$$

為了使對應於 Y_h 的重疊影像有較佳的影像品質與安全性，我們應該使σ_h^b與σ_h^w的值愈小愈好。當$|T| = 1$，也就是只有一張密圖時，σ_h^b與σ_h^w的值必然為 0，因此這兩項指標可以不予考慮。

5. 最佳化模型之一般式

我們以$\Psi = (T, P, F, Q, \Omega)$的形式表示多張機密影像的任意使用結構。對於任何一個使用結構Ψ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。$\Psi = (T, P, F, Q, \Omega)$形式的最佳化模型如第(15)式所示。在第(15)式中，因為每一個密圖樣式都各有 $2^{|P|}$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 $2^{|T|}\times 2^{|P|}$個變數需要求解。每一個變數都是介於 0 到 1 之間的實數，且每一個

密圖樣式所有加密規則的機率總和必須分別為 1。在安全性方面，因為每一個對應於禁止集合 $X \in F$ 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。此外，為了確保對應於合格集合 $Y \in Q$ 的重疊影像的影像品質與安全性，因此有 $2\times|Q|$ 個相對應的限制條件。在對比方面，因為每一個對應於合格集合 $Y \in Q$ 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。這個最佳化模型可以適用在多機密影像的任何使用結構上，而單機密影像使用結構的模型為本模型之特例。

$$\left.\begin{array}{ll} \max. & \alpha_h = b_h - w_h, \; for\; h = 1, 2, ..., |Q|. \\ \text{s.t.} & \sigma_k = 0, \; for\; k = 1, 2, ..., |F|, \\ & \sigma_h^b = 0, \; for\; h = 1, 2, ..., |Q|, \\ & \sigma_h^w = 0, \; for\; h = 1, 2, ..., |Q|, \\ & \sum_{j=1}^{2^{|P|}} C_{ij} = 1, \; for\; i = 1, 2, ..., 2^{|T|}, \\ & C_{ij} \in [0,1], \; for\; i = 1, 2, ..., 2^{|T|}, \; j = 1, 2, ..., 2^{|P|}. \end{array}\right\} \quad (15)$$

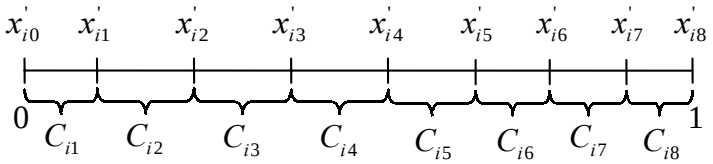
四、遺傳演算法的應用

1. 遺傳演算法

遺傳演算法(Genetic Algorithms; GAs)是在 1970 年代由 Holland [14]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 所處理的對象是參數集(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[4, 8, 18]。

2. AS_T2P3 最佳化問題的做法

(1) 染色體編碼與解碼



圖四：染色體編碼方式示意圖

由於第(1)式的變數為實數型態，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[9, 18]，而其較短的染色體長度也能獲得較佳的執行效率[9]。在這個問題中，我們需要求解 32 個機率值：C_{ij}，其中 i = 1, 2, 3, 4, j = 1, 2, …, 8。為了滿足第(1)式中的第 10 與第 11 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 7 個數(x'_{i1}、x'_{i2}、x'_{i3}、x'_{i4}、x'_{i5}、x'_{i6} 與 x'_{i7})當作分割點，然後利用這 7 個分割點將 0 到 1 的範圍切割成 8 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(如圖四所示)。因此，我們將染色體編碼為 (x_{11} .. x_{17}, x_{21} .. x_{27}, x_{31} .. x_{37}, x_{41} .. x_{47})。接著，我們分別將(x_{i1}, x_{i2}, x_{i3}, x_{i4}, x_{i5}, x_{i6}, x_{i7})由小到大排序後，就可以形成 0 到 1 之間的 7 個分割點。令(x'_{i1}, x'_{i2}, x'_{i3}, x'_{i4}, x'_{i5}, x'_{i6}, x'_{i7}) = Sort(x_{i1}, x_{i2}, x_{i3}, x_{i4}, x_{i5}, x_{i6}, x_{i7})，x'_{i0} = 0，x'_{i8} = 1，其中 i = 1, 2, 3, 4。透過這些分割點，我們可以將染色體的解碼方式設定為 $C_{ij} = x'_{ij} - x'_{i,j-1}$，其中 i = 1, 2, 3, 4, j = 1, 2, …, 8。

(2) 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：$f_1(x) = \alpha_1 = 0.5(QC_{31} + QC_{41} - QC_{11} - QC_{21})$、$f_2(x) = \alpha_2 = 0.5(QC_{22} + QC_{42} - QC_{12} - QC_{32})$與 $f_3(x) = \alpha_3 = 0.5(QC_{33} + QC_{43} - QC_{13} - QC_{23})$，而 f_1、f_2 與 f_3 即是我們要追求最大化的目標。另外，我們使用懲罰函數法(penalty function approach)來處理第 1 至第 9 個限制條件。我們定義的懲罰函數為：

$$\Phi(x) = \sum_{i=1}^{3} \sigma_i + \sum_{i=1}^{3} \sigma_i^b + \sum_{i=1}^{3} \sigma_i^w \text{。} \tag{16}$$

懲罰函數$\Phi(x)$代表模型中違反安全性限制條件的程度。所以，考慮限制條件的適合度函數可以分別寫成：$F_1(x) = f_1(x) - \Phi(x)$，$F_2(x) = f_2(x) - \Phi(x)$，$F_3(x) = f_3(x) - \Phi(x)$。我們所要求解的問題為具有 3 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：$F(x) = F_1(x) + F_2(x) + F_3(x)$。

(3) 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。

(4) 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) [10]。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。其特色為兩個子代解答(offspring solutions)之間的距離與兩個父代解答(parent solutions)之間的距離具有比例關係；此外，父代解答附近的答案有比較高的機會成為子代解答。使用 SBX 的好處是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)。

(5) 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：

$$y_i = r_i\left(x_i^{(U)} - x_i^{(L)}\right) + x_i^{(L)}, \tag{17}$$

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。

五、實驗結果與討論

1. 多機密影像視覺密碼方法

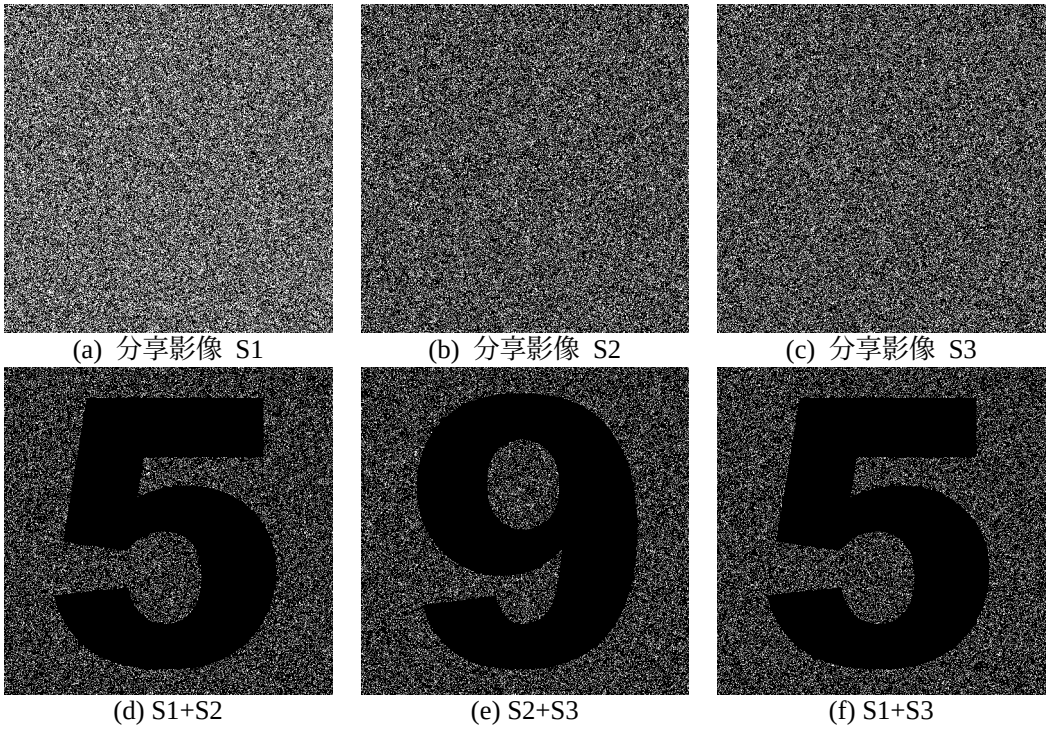
在本實驗中，我們以遺傳演算法來求解 AS_T2P3 的最佳化問題。有關遺傳演算法之相關參數設定如表四所示，其實驗結果如表五與圖五所示。在表五中，機率矩陣 $\boldsymbol{C}$ 顯示對應於密圖樣式(0, 0)的加密規則(0, 0, 0)、(0, 0, 1)、(0, 1, 0)、(1, 0, 0)、(0, 1, 1)、(1, 1, 0)、(1, 0, 1)與(1, 1, 1)的使用機率分別為 0.1、0.1、0.1、0.1、0.1、0.0、0.0 與 0.5；對應於密圖樣式(0, 1)的各個加密規則的使用機率則分別為 0.0、0.2、0.2、0.0、0.0、0.1、0.1 與 0.4；對應於密圖樣式(1, 0)的各個加密規則的使用機率則分別為 0.0、0.0、0.0、0.2、0.4、0.1、0.1 與 0.2；對應於密圖樣式(1, 1)的各個加密規則的使用機率則分別為 0.0、0.0、0.0、0.0、0.4、0.3、0.3 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 S1、分享影像 S2 與分享影像 S3 的安全性指標分別為$\sigma_1 = 0$、$\sigma_2 = 0$ 與$\sigma_3 = 0$，也就是代表 S1、S2 與 S3 是絕對安全的(見圖五(a)-(c))。在對比方面，(S1+S2)、(S2+S3)與(S1+S3)

表四：遺傳演算法之相關參數設定

參數	設定值
族群大小	400
染色體長度	28
交配率	1.0
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	100 代

表五：AS_T2P3 之機率矩陣及其安全性與對比分析

機率矩陣		
$C = \begin{bmatrix} 0.1 & 0.1 & 0.1 & 0.1 & 0.1 & 0.0 & 0.0 & 0.5 \\ 0.0 & 0.2 & 0.2 & 0.0 & 0.0 & 0.1 & 0.1 & 0.4 \\ 0.0 & 0.0 & 0.0 & 0.2 & 0.4 & 0.1 & 0.1 & 0.2 \\ 0.0 & 0.0 & 0.0 & 0.0 & 0.4 & 0.3 & 0.3 & 0.0 \end{bmatrix}$		
安全性		對比
$\sigma_1 = 0.0$	$\sigma_1^b = 0.0$ $\sigma_1^w = 0.0$	$\alpha_1 = 0.2$ ($w_1 = 0.8$, $b_1 = 1.0$)
$\sigma_2 = 0.0$	$\sigma_2^b = 0.0$ $\sigma_2^w = 0.0$	$\alpha_2 = 0.2$ ($w_2 = 0.8$, $b_2 = 1.0$)
$\sigma_3 = 0.0$	$\sigma_3^b = 0.0$ $\sigma_3^w = 0.0$	$\alpha_3 = 0.2$ ($w_3 = 0.8$, $b_3 = 1.0$)



(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

圖五：AS_T2P3 的實驗結果(512×512 pixels, 300 dpi)

的對比指標分別為$\alpha_1 = 0.2$、$\alpha_2 = 0.2$ 與$\alpha_3 = 0.2$，其中黑色部分皆為 100%的黑，代表黑點的重建結果是完美的。此外，由於$\sigma_1^b = 0$，$\sigma_2^b = 0$，$\sigma_3^b = 0$，$\sigma_1^w = 0$，$\sigma_2^w = 0$ 且$\sigma_3^w = 0$，因此在重疊影像(S1+S2)、(S2+S3)與(S1+S3)中，代表機密影像中的黑色區域與白色區域，其黑點的分布也都是均勻的(見圖五(d)-(f))；因此，影像的品質可以得到確保。

根據以上實驗結果可知，在不作像素擴展的條件下，我們的方法對於處理多機密影像的使用結構是有效的。此外，實驗結果也顯示遺傳演算法能夠找到令人滿意的解答。我們所求解的機率矩陣不但能夠確保絕對的安全性；同時，也能夠確保完美的黑點重建結果。我們只要將分享影像重疊，就可以透過眼睛輕易地進行解密，完全不需要使用任何計算機資源。

2. 單機密影像視覺密碼方法

觀察第(15)式的最佳化模型可以發現，在單機密影像的情況下，因為所有可能的密圖樣式只有(0)與(1)兩種，且σ_h^b與σ_h^w的值必然為 0；因此，除了$\sigma_h^b = 0$與$\sigma_h^w = 0$這兩組限制條件可以不必考慮之外，單機密影像視覺密碼方法的最佳化模型，可以簡化為下列的多目標線性規劃最佳化模型：

$$\left.\begin{array}{ll} \max. & \alpha_h = QC_{1h} - QC_{0h},\ for\ h = 1, 2, ..., |Q|. \\ \text{s.t.} & \sigma_k = |FC_{1k} - FC_{0k}| = 0,\ for\ k = 1, 2, ..., |F|, \\ & \sum_{j=1}^{2^{|P|}} C_{ij} = 1,\ for\ i = 0, 1, \\ & C_{ij} \in [0, 1],\ for\ i = 0, 1,\ and\ j = 1, 2, ..., 2^{|P|}. \end{array}\right\}, \tag{18}$$

其中 QC_{0h} (QC_{1h})代表白點(黑點)經過加密後，在對應於合格集合 $Y_h \in Q$ 的重疊影像上出現黑點的機率，而 FC_{0k} (FC_{1k})代表白點(黑點)經過加密後，在對應於禁止集合 $X_k \in F$ 的重疊影像上出現黑點的機率。基本上，單機密影像的模型(第(18)式)為多機密影像的模型(第(15)式)的特例。透過第(18)式的單機密影像最佳化模型，我們只要給定一個使用結構 $\boldsymbol{\Gamma}$ = (P, F, Q)，便可建構出相對應的最佳化問題；透過求解最佳化問題，便可得到加密用的機率矩陣。假設使用結構為Γ = (P, F, Q)，其中 P = {1, 2, 3}，F = {{1}, {2}, {3}, {1, 3}}，Q = {{1, 2}, {2, 3}, {1, 2, 3}}，且加密規則矩陣如第(3)式，而機率矩陣為

$$C = \begin{bmatrix} C_{01} & C_{02} & C_{03} & C_{04} & C_{05} & C_{06} & C_{07} & C_{08} \\ C_{11} & C_{12} & C_{13} & C_{14} & C_{15} & C_{16} & C_{17} & C_{18} \end{bmatrix}, \tag{19}$$

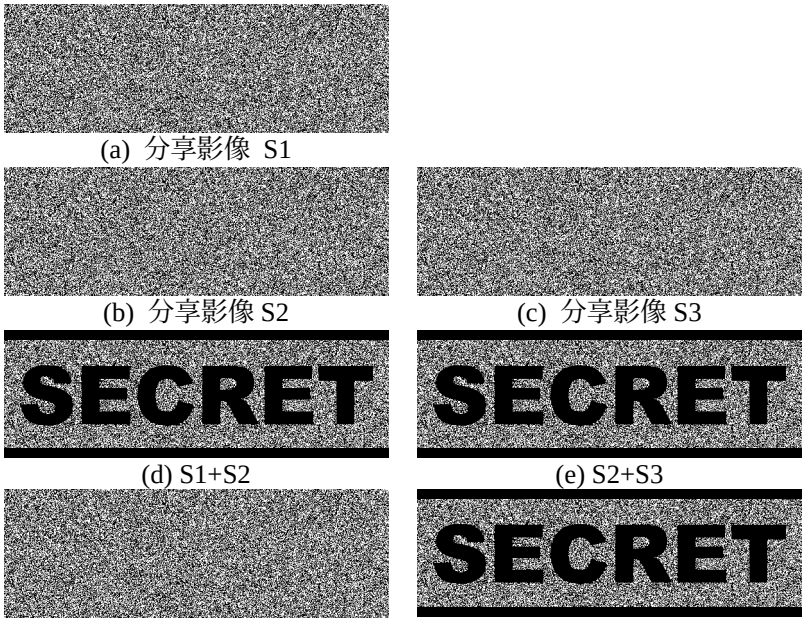
則其最佳化問題可以寫成

$$\left.\begin{array}{ll} \max. & \alpha_1 = (C_{13} + C_{14} + C_{15} + C_{16} + C_{17} + C_{18}) - (C_{03} + C_{04} + C_{05} + C_{06} + C_{07} + C_{08}). \\ \max. & \alpha_2 = (C_{12} + C_{13} + C_{15} + C_{16} + C_{17} + C_{18}) - (C_{02} + C_{03} + C_{05} + C_{06} + C_{07} + C_{08}). \\ \max. & \alpha_3 = (C_{12} + C_{13} + C_{14} + C_{15} + C_{16} + C_{17} + C_{18}) - (C_{02} + C_{03} + C_{04} + C_{05} + C_{06} + C_{07} + C_{08}). \\ \text{s.t.} & \sigma_1 = |(C_{14} + C_{16} + C_{17} + C_{18}) - (C_{04} + C_{06} + C_{07} + C_{08})| = 0, \\ & \sigma_2 = |(C_{13} + C_{15} + C_{16} + C_{18}) - (C_{03} + C_{05} + C_{06} + C_{08})| = 0, \\ & \sigma_3 = |(C_{12} + C_{15} + C_{17} + C_{18}) - (C_{02} + C_{05} + C_{07} + C_{08})| = 0, \\ & \sigma_4 = |(C_{12} + C_{14} + C_{15} + C_{16} + C_{17} + C_{18}) - (C_{02} + C_{04} + C_{05} + C_{06} + C_{07} + C_{08})| = 0, \\ & \sum_{j=1}^{8} C_{ij} = 1,\ for\ i = 0, 1, \\ & 0 \le C_{ij} \le 1,\ for\ i = 0, 1,\ and\ j = 1, 2, ..., 8. \end{array}\right\}。 \tag{20}$$

以上述之遺傳演算法求解第(20)式所得到的一個可能的機率矩陣如表六所示，而其實驗結果則如圖六所示。

表六：單機密影像視覺密碼方法之機率矩陣及其安全性與對比分析

機率矩陣	
$C = \begin{bmatrix} 0.5 & 0.0 & 0.0 & 0.0 & 0.0 & 0.0 & 0.0 & 0.5 \\ 0.0 & 0.0 & 0.5 & 0.0 & 0.0 & 0.0 & 0.5 & 0.0 \end{bmatrix}$	
安全性	對比
$\sigma_1 = 0.0$ $\sigma_2 = 0.0$ $\sigma_3 = 0.0$ $\sigma_4 = 0.0$	$\alpha_1 = 0.5$ ($QC_{01} = 0.5$, $QC_{11} = 1.0$) $\alpha_2 = 0.5$ ($QC_{02} = 0.5$, $QC_{12} = 1.0$) $\alpha_3 = 0.5$ ($QC_{03} = 0.5$, $QC_{13} = 1.0$)



(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

圖六：單機密影像視覺密碼方法的實驗結果(600×200 pixels, 300 dpi)

3. 討論

綜觀以上的討論，我們所探討的分享影像都是雜亂無章的影像。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的影像的使用結構，就有其實際的應用價值。第(15)式的最佳化模型的特色在於，只要給定一個使用結構$\Psi = (T, P, F, Q, \Omega)$，就可以建構出相對應的最佳化問題。因此，我們的模型也可以應用在分享影像本身是有意義的影像的結構。例如，我們可以將$\Psi = (T, P, F, Q, \Omega)$建構成 $T = \{1, 2, 3\}$，$P = \{1, 2\}$，$F = \varnothing$，$Q = \{\{1\}, \{2\}, \{1, 2\}\}$，且

$$\Omega(Y) = \begin{cases} 1, & if\ Y = \{1\} \\ 2, & if\ Y = \{2\} \\ 3, & if\ Y = \{1, 2\} \\ 0, & otherwise \end{cases}.$$

這個使用結構即定義了將兩張有意義的分享影像重疊後，可以重建一張機密影像的秘密分享規則，其中集合 T 包含了三張機密影像($|T| = 3$)，而集合 P 則包含了兩個參與者($|P| = 2$)。此外，合格集合的集合 Q 與函數Ω定義{1}與{2}分別代表合格集合，其中第一張分享影像本身就可以重建機密影像 1，而第二張分享影像本身則可以重建機密影像 2，也就是第一與第二張分享影像本身都是有意義的影像；將第一與第二張分享影像重疊後則可重建機密影像 3。這樣的模型就如同 Ateniese et al. [3]與 Naor and Shamir [17]所提出之有意義的分享影像的概念。透過Ψ與第(15)式的最佳化模型，我們就可以建構出關於有意義的分享影像的最佳化問題，只要求解最佳化問題就能得到加密用的機率矩陣。在未來，我們將更深入研究如何運用這個模型於有意義之分享影像的秘密分享方法。此外，我們也將進一步探討如何將我們的模型進一步應用在灰階與彩色的影像上。

六、結論

視覺密碼方法的特色在於其解密過程是透過人類視覺系統，而不需要利用任何計算機資源與複雜的解密演算法。因此，在一些無法使用電腦解密的情況下，視覺式的秘密分享方法是一個很好的解決方案。大部分的視覺密碼方法都是使用像素擴展的技巧；因此，分享影像的大小會被擴展成機密影像的若干倍。像素擴展的結果不但使得分享影像不易攜帶，也會造成儲存空間的浪費。此外，大部分的視覺密碼方法只允許分享單一機密影像，而無法分享多張機密影像。多機密影像的視覺密碼方法不但能使秘密分享方式更富於變化；同時，也可以使得所需的資訊量大為降低。就分享影像的形式而言，大部分的視覺密碼方法的產出都是雜亂無章的分享影像。雜亂無章的分享影像的缺點為容易遭受懷疑、竊取與破壞；因此，分享影像本身為有意義的影像的秘密分享方式，有其實際的應用價值。

綜觀視覺密碼學的研究，關於不需要像素擴展，而又能分享多張機密影像的方法可謂付之闕如。在本文中，我們提出一個不需要像素擴展的多機密影像視覺密碼方法。我們使用機率的觀念，並且結合安全性與對比兩項指標，建構出視覺密碼方法的最佳化模型。在不作像素擴展的前提之下，我們的最佳化模型不但可以處理單機密影像與多機密影像的任意使用結構；同時，它也可以處理有意義之分享影像的任意使用結構。透過 $\Psi = (T, P, F, Q, \Omega)$的使用結構形式，我們可以建構出單機密影像、多機密影像與有意義之分享影像的任何使用結構。我們只要給定一個Ψ的使用結構，就可以透過我們的模型建構出相對應的最佳化問題，進而求解加密用的機率矩陣。實驗結果顯示，我們的方法確實可以達成像素不擴展與分享多張機密影像的目標。在未來，我們將更深入研究如何運用這個模型於有意義之分享影像的秘密分享方法。此外，我們也將進一步探討如何將我們的模型進一步應用在灰階與彩色的影像上。

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] Hou, Y. C., Lin, F. and Chang, C. Y., "Visual Cryptography for Color Images without Pixel Expansion", *Journal of Technology* (16:4), 2001: pp. 595-603.

[16] 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.

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

[18] Srinivas, M. and Patnaik, L. M., "Genetic Algorithms: A Survey," *Computer* (27:6), 1994: pp. 17-26.

[19] Tzeng, W. G. and Hu, C. M., "A New Approach for Visual Cryptography," *Designs, Codes and Cryptography* (27), 2002: pp. 207-227.

[20] 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.

38 以機率為基礎之像素不擴展的多機密影像視覺密碼最佳化模型