基因演繹式之關鍵性視覺判讀機制研究

王旭正
中央警察大學資訊管理系

王蕙禎
中央警察大學資訊管理系

林立群
中央警察大學資訊管理系

摘要

視覺安全是一種以視覺效果為辨識秘密的機制，其不需要計算大量的複雜數學，和其他傳統的密碼系統比較起來，方便許多。不過，視覺安全在使用上仍有許多議題有待研究與討論。其中，文獻(邱文怡等 2002)曾試圖運用善於搜尋問題的最佳解答之基因演算法，來解決視覺安全裡影像擴張與有意義性的問題。然而，我們發現用其方法所產生的秘密影像中，原應為黑色的像素，在某些時候可能變成白像素，或者白像素可能變成黑像素。這將造成使用者不容易判讀出正確的秘密訊息。因此，本文提出另一種做法，以改變基因演算法的運作方式，來解決此方面的議題。運用我們的方法，可以確保秘密訊息的正確性，並有效降低人眼判讀的錯誤。

關鍵字：科技應用、視覺密碼學、基因演算法、安全環境

Genetic Algorithms Highlighting the Target Secret in Visual Cryptography

Shiuh-Jeng Wang
Department of Information Management, Central Police University

Huei-Jhen Wang
Department of Information Management, Central Police University

Li-Cheng Lin
Department of Information Management, Central Police University

Abstract

Secure concern in visual cryptography is yet another cipher mechanism used in the lower computation requirements. Compared to the text-based cryptography, such as DES and RSA, the time cost in decryption is much saved due to the secret is gained directly by our human vision systems. In secure concerns, how to make visual cryptography practical applying in real cases in the computer systems, there are still open issues in this way. Accordingly, one of the studied literature in (邱文怡等 2002), the genetic-based algorithm was proposed to realize the visual cryptography in the shadow/share image generation, in such a way that the size of share image is able to remain the same one of target image showing the secret. It is great research work using the manner of the genetic-based algorithm. In this case, we further observed that the secret shown in the target image can be improved better in order to resolve the misconception in the recognition of critical secret reading. It is conducted the uniform generations of black-pixel and white-pixel in our proposed algorithms. As the experiments given in our scheme, the secret shown in the target image is really undoubtedly visible to make the confusions clear in the recognitions of critical view-points.

Key words: High-tech demands, visual cryptography, genetic algorithm, security

壹、緒論

隨著資訊時代的來臨，人與人之間的互動與溝通，對各種電腦與通訊技術的依賴日益加深。尤其是網際網路，早已成為人類生活的一部份。網路的無遠弗屆與便利性令人喜愛，卻也因此而衍生了安全性問題。駭客們正是利用網際網路方便的特性，完成他們不法竊取或竄改資料的目的。

為了讓重要的秘密訊息能夠在網路上安全地傳遞，也為了讓人們得以安心地使用網路進行各種活動，如網路拍賣、電子商務等，許多專家學者紛紛投入研究密碼系統的行列。然而，傳統上典型的密碼系統，加解密的過程大都建立在複雜的數學問題上，且必須進行大量的運算，在使用上並不容易。

視覺密碼學/視覺安全是許多密碼系統中的一種。其特點在於解密程序非常簡單。只要將數張分享影像疊合在一起，以人類的眼睛即可解讀出秘密訊息，同時仍然保有安全性(Naor & Shamir 1995)。此外，視覺密碼學亦符合門檻機制。所謂門檻機制，指的是秘密訊息需要超過一定數量之金鑰(Key)才可解出，也就是金鑰數量要達到一定門檻才行，否則無法解出秘密訊息(Shamir 1978)。

所以當秘密訊息不得由個人獨享，而必須是多人共同參與時，以視覺密碼系統為其安全性把關極為合適。舉例來說，核子武器的殺傷力極為強大，一旦發射將遺害千年。此時，下命發射核子彈的權力就必須慎重地交予多人控制，不能僅憑一己的思想。啟動核子發射系統的密碼可經由視覺密碼學加密成數個分享影像，分別發送給有權力的人。只有當一定人數的人同意發射核子武器，將各自擁有的分享影像疊合在一起，才能獲得密碼，啟動核子發射系統。如果其中一張分享影像不小心被不肖人士取得，並不會引起多大的危險。除非不肖人士已經各個擊破，掌握了足夠數量的分享影像，然而與只取得一張分享影像相較，取得多張分享影像是極其困難的。

雖然視覺密碼系統擁有上述多項好處，然而無可避免的，還是會有某些議題有待改進。例如分享影像的可攜性、有意義性，成本問題，以及秘密訊息的正確性等。在不同的議題上，目前已有不少相關的研究(沈伯成 2003；吳佳鴻 2003；邱文怡等 2002)。其中(邱文怡等 2002)利用基因演算法來改善分享影像的有意義性之議題。基因演算法是一種搜尋演算法(周鵬程 2002；候永昌 & 張雅惠 2003；黃昭平等 2000)，它模擬了自然界的演化機制，以數學的方式來找尋出問題的解答。由於其極富彈性的特點，能讓使用者針對自己的需求設計出不同的演算方式，因此已被廣為運用。文獻(邱文怡等 2002)即曾發表過應用基因演算法於視覺密碼學的相關研究。另外亦有學者利用基因演算法的概念來防範視覺密碼學的欺騙攻擊(Tasi et al. 2006)，其作法是將各分享子圖中之像素值組合做為母體，並代入適應函數，產生最佳化矩陣解。當偽裝攻擊發生時，受攻擊者在疊合分享子圖時，可發現疊合結果並不清晰，即可藉此查覺遭受攻擊，解密訊息並不正確。然而，在文獻(邱文怡等 2002)中我們發現用其方法所產生的秘密影像中，原應為黑色的像素，在某些時候可能變成白像素，或者白像素可能變成黑像素。如果不改善此一現象，

將使得使用者不容易判讀出正確的秘密訊息到底為何，甚至判讀錯誤。比如，將「i」誤以為「l」，細節將於後文做說明。此在重要情況下，將可能因判讀錯誤，造成嚴重的損失，例如密碼的讀取裡，「i」與「l」的不同判定，造成系統運作的待機。

為了延續視覺密碼學的加密能力，並且還能確保秘密訊息的正確性，降低人眼判讀錯誤的可能，本文提出新的應用基因演算法之方式。我們將採取不同以往的觀點，先固定秘密影像與一張分享影像，再據此尋找其他適合的分享影像。以此原理，再配合一些細節的修正，來達成我們的目標。

本文的編排說明如下：在第二節中，我們回顧視覺密碼與基因演算法的原理，並且簡單介紹文獻(邱文怡等 2002)之研究。在第三節中，我們將提出我們的方法，並且說明流程中的各個步驟。而在第四節隨即呈現出我們實驗的結果與討論。最後在第五節中做出結論。

貳、文獻探討

一、視覺密碼學

視覺密碼學(Visual Cryptography; VC)亦或視覺安全系統是由Naor和Shamir於1994年所提出的，其為秘密分享的技術(Secret Sharing)之一種形式表現(Noar & Shamir 1995)。所謂秘密分享的概念，是一個秘密的擁有者，要將秘密分給其他的參與者，但是又不要每個參與者獨自獲得這個秘密，而是要部分或全部的參與者集合起來，才能得到這個秘密，這種概念就叫做秘密分享。而視覺密碼學的主要概念，就是將一張擁有秘密訊息的影像，也就是秘密影像(Secret Image)，經由一些方法，分解出數張分享影像(Share)，這些動作在本文中，將之定義為加密(Encryption)。如果只擁有一張分享影像，是解讀不出其秘密資訊內容的，必須部分或者是全部的分享影像結合在一起，才可以看出其所要表達的秘密資訊。而可合成分享影像並得到內含的秘密訊息，在本文中，將之定義為解密(Decryption)。而VC的方法不需要複雜或大量的計算、也可以不需要電腦的輔助來完成解讀，只要藉由人眼便可直接解讀，即得出所隱藏的機密訊息。

一般的視覺密碼系統採用編碼表的方式來加密。所謂的編碼表的方式，以黑白的二元秘密影像要分成兩張分享影像來說，就是對秘密影像的白色和黑色的像素，個別按照如表1所示的編碼表之規則，對映出其在分享影像上所應呈現的樣子。拿白色像素來說，對映出的結果，可能兩張分享影像上，皆呈現前白後黑的兩相鄰像素。另一種情況是，兩張分享影像上，皆呈現前黑後白的兩像素。

然而，由上述我們可以得知，一張分享影像的像素數目會比原本秘密影像的像素數目，多出一倍。換句話說，即會使得影像擴張。如此一來，將會提高此密碼系統在使用及傳輸時的成本。不過，影像的擴張在另一方面，卻可以提高影像的對比性(Contrast)。對比性是讓秘密影像可從重疊的分享影像中，看出來的程度。對比性過低的話，設計此視覺安全系統就毫無意義了，因為根本看不出影像所要傳遞的秘密資訊。因此，如何在

成本與對比性之間取得平衡，是一個大議題。

另外，一般的視覺密碼機制所加密出的分享影像，可能是有意義的或是無意義的。圖1，2，3分別為Shares在視覺安全系統下對於秘密影像（機密影像標記）的效果呈現(在本文中，我們以〝logo〞為秘密訊息的範例)。如果分享影像是無意義的，則容易令有心偷窺秘密者產生懷疑，認為其中必有隱情。若對這些影像在網路傳輸的過程中做出攔截或攻擊的動作時，將破壞安全機制的完整性。藉由這些加強性需求，亦引發了相關的研究(沈伯成 2003；吳佳鴻 2003；邱文怡等 2002)。

表1：視覺密碼系統編碼表

影像	原機密影像（像素白， 大小：1*1）	原機密影像（像素黑，大小：1*1）
Share(2*2)一		
Share(2*2)二		
疊合結果		

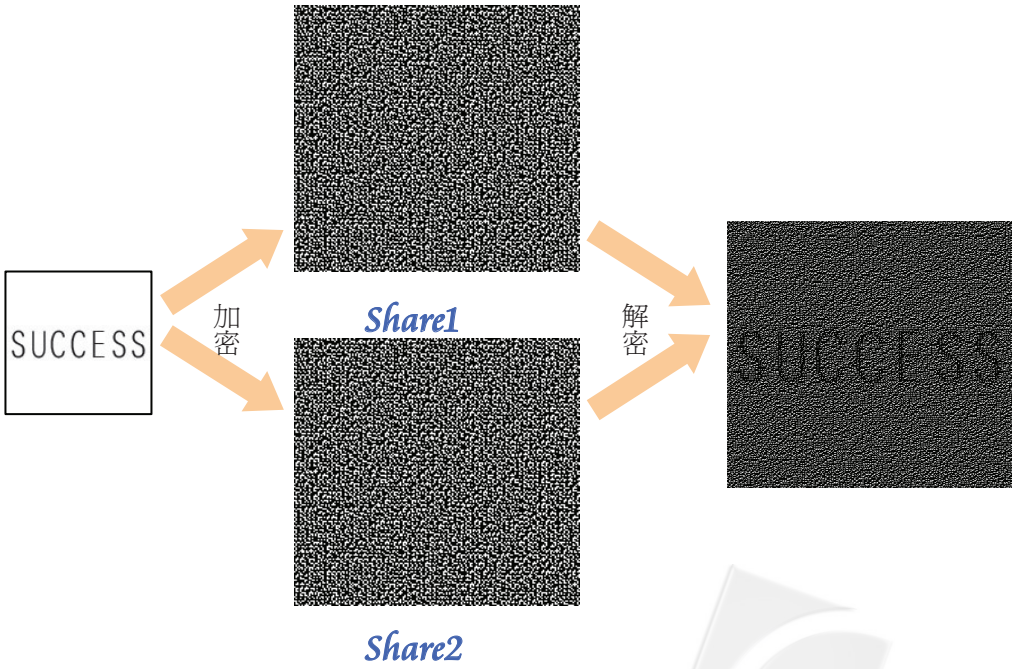


圖1：兩張無意義Shares在視覺密碼系統的疊合效果

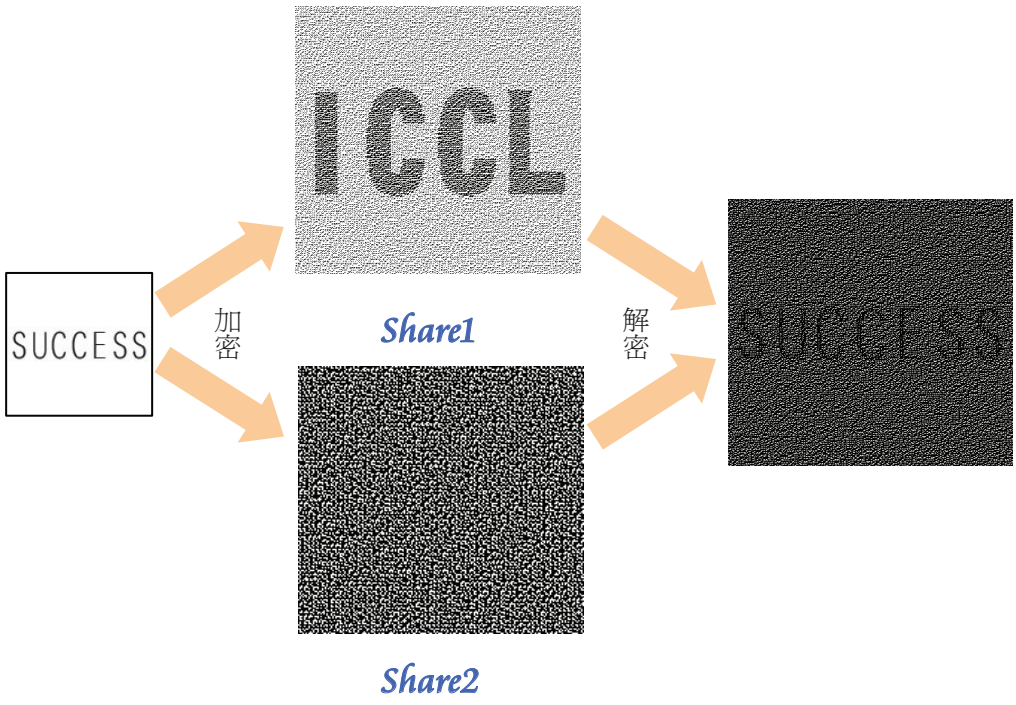


圖2：分別為有意義與無意義的Share在視覺密碼系統的疊合效果

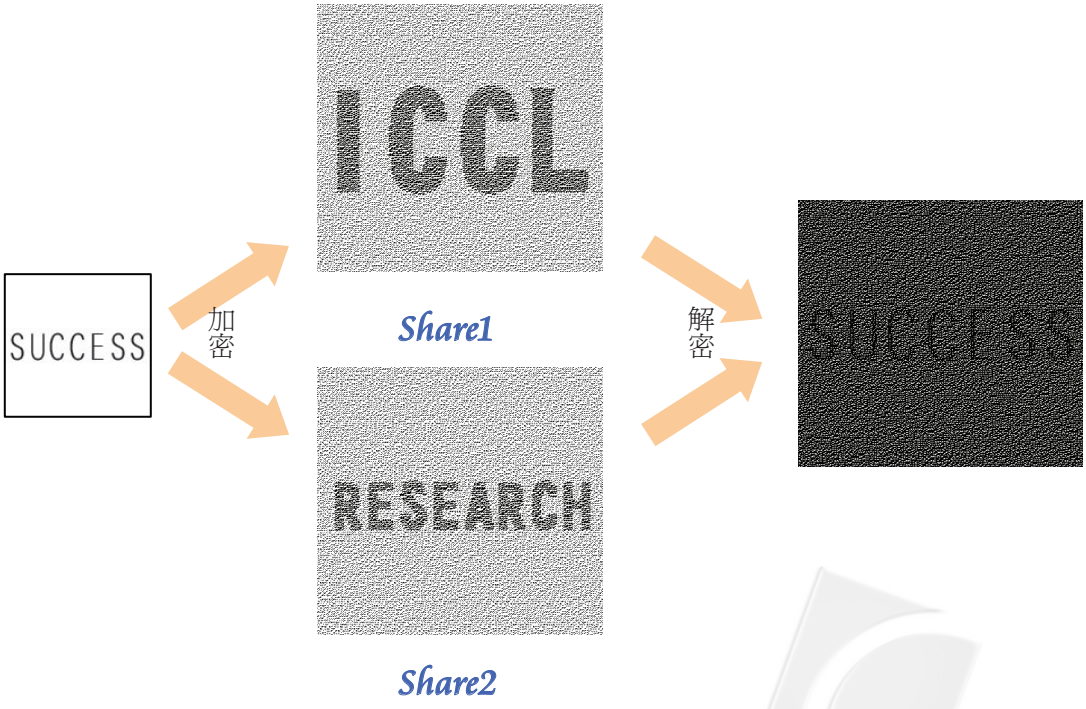


圖3：有意義的Shares在視覺密碼系統的疊合效果

二、基因演算法

1975年，賀蘭(John Holland)首度提出了基因演算法(Genetic Algorithm; GA)。GA模擬自然界生物的演化(Evolvement)，包括達爾文(Darwin)所提出的演化論，以及遺傳學中的基因(Gene)、染色體(Chromosome)等機制，以數學的方式將此轉化成一套流程，可用來搜尋問題之有效解(Solution)。只要設有合適的適應函數(Fitness Function)，母體(Population)在經過多次的繁衍之後，就會產生令人滿意的答案。以下為GA中常提及的名詞解釋，並將在本文的研究中使用：

（1）個體(Individual)：代表GA所求得的某一個解。

（2）母體(Population)：指共同生存於模擬環境中，所有同一代的個體，也就是一群解的集合。

（3）染色體(Chromosome)：每一個體以一條染色體表示，染色體中存有遺傳訊息(基因)，通常為編碼過的數據，這些訊息將影響個體於模擬環境中的表現。

（4）適應度(Fitness)：即個體在模擬環境中的適應程度。每個個體的適應度不同，GA將依此進行天擇，也就是把相對適應度低的個體淘汰，留下相對適應度高的個體。使用者通常須先定義一個適應函數(Fitness Function)，用以計算染色體在模擬環境中的適應程度。

GA的演化過程如圖4所示，其步驟如下：

（1）創造初始母體：以亂數產生初始母體。

（2）計算個體的適應度以判斷是否終止演化。

（3）進行繁衍：包括選擇(Selection)、交配(Crossover)和突變(Mutation)三個基因運算子。

（4）將新母體代入此演化機制中：重複步驟2~4，直到符合終止條件為止。

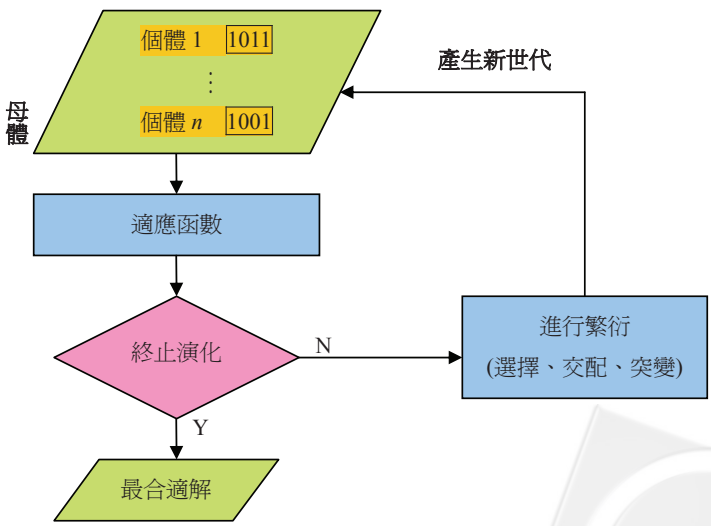


圖4：基因演算法演化過程示意圖

三、文獻(邱文怡等 2002)之研究

文獻(邱文怡等 2002)，使用了無性生殖模式的GA來解決視覺密碼學相關的議題。其先選出幾張灰階影像，用以作為分享影像的原圖。另外選定要加密的灰階影像，此即秘密影像。然後將這些灰階影像做適當灰度的分配。再將這些灰階影像進行半色調處理（Halftone），產生所需之半色調影像。接著，正式進入GA的部分。其將它分為七個步驟：影像分割、母體初始化、交換式突變、計算適應函數值、設立選擇策略、擬定演化策略，以及整合最佳解。簡單來說，此研究乃試圖用GA求得兩分享影像。此兩分享影像經過交換式的突變之後，將接受適應函數的評估。為了使分享影像重疊後，儘量產生相似於秘密影像的結果，將適應函數設計為，兩分享影像相同位置的疊合結果若等於秘密影像時，適應函數值加1。適應函數值越多，就越符合期待。

特別一提的是，所謂交換式突變，是為了確保分享影像整體的像素平均值之恆穩狀態，令其在演化過後不會和原圖差距過大，而採用了無性生殖的GA方式，僅在表示同一分享影像的染色體部分做交換式突變，來產生下一代。此交換式突變的方式如圖5所示，其中，個體 1010 1010 (Share1和Share2) 經過交換式突變將變成 1010 1010 。

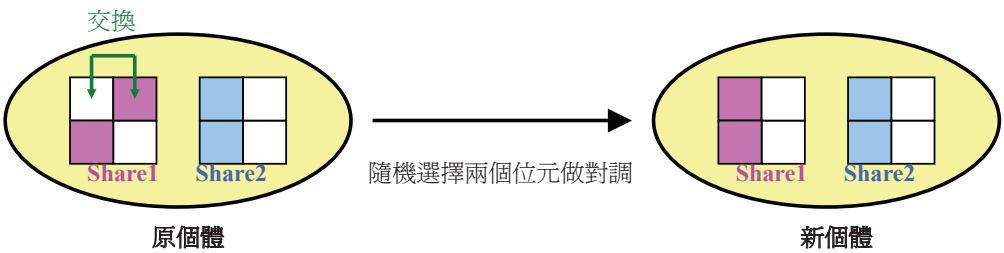
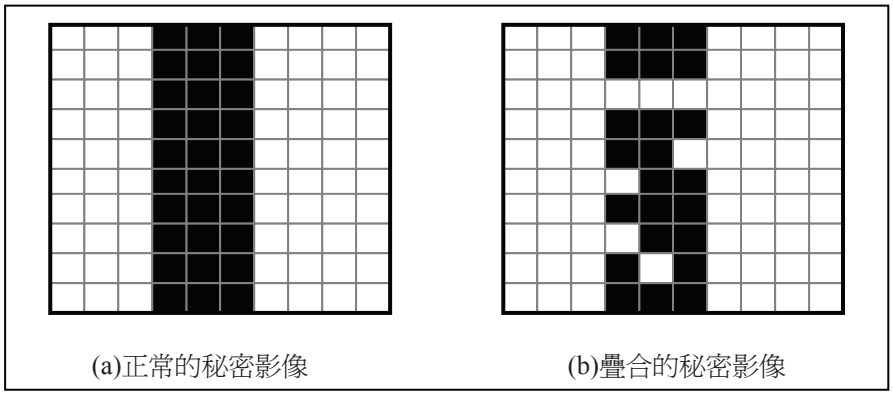


圖5：交換式突變示意圖

在交換式突變的步驟中，讓分享影像保留了原本親代的基因遺傳，僅做本身像素間位置的調換，如此一來，影像就不會產生擴張。至於分享影像是否具有意義，是可由一開始在選擇分享影像時，就先行決定。分享影像並不會因為基因演化後而產生太大的改變。

文獻(邱文怡等 2002)所提出的方法，雖然可以解決傳統視覺密碼學在成本與對比性兩者間抉擇的難處，亦即利用此方法所加密出的分享影像，並不需要擴張影像，即可使得分享影像有意義，但是在實際應用上，仍存在一些問題。將(邱文怡等 2002)的方法製造出來的分享影像疊合，所獲得的秘密影像中，其秘密訊息由大多數的黑像素與少數的白像素所組成。其中，白像素的位置，並非如同傳統運用編碼表的視覺密碼學一樣，位置有其一定的規則可循，而是隨著演化後的分享影像之像素而決定。也就是說，其疊合出的秘密訊息中，白像素的位置是雜亂無章、沒有規則的，而且無法事先得知或是獲得控制。此現象將可能造成秘密訊息不易辨識，甚至造成誤解。以圖6做說明。(a)是正常的秘密影像「｜」，(b)是(邱文怡等 2002)方法內疊合後的秘密影像(皆為10 ×10之影像，

背景部分不做討論)。疊合影像白像素的位置若沒有一定，而恰為(b)影像時，則人眼在判讀上，不容易辨識出秘密訊息究竟為英文字元「l」、「i」還是符號形式的「｜」。



(a)正常的秘密影像　　(b)疊合的秘密影像

圖6：秘密訊息辨識不易

參、關鍵性視覺判讀機制研究

本節為我們所提出之方法。為能清楚引導研究過程與帶來的實際效益，本文先討論此問題的原理為何，以利概念的形成，然後進行GA設計的描述，包括準備工作、編碼的描述規劃、初始母體的創造、適應度的計算、終止演化條件、選擇與突變的操作等。在本文裡提出了兩種做法，將陸續於後文介紹。運用GA的目的，在於提供一種有別於傳統編碼表的加密方式，運用此方式，可以使得視覺密碼系統更為安全、便利，且能確保秘密訊息的正確性。

一、原理

再考慮先前的情形：如何判讀「i」、「l」與「｜」的清晰性與正確判讀。基植於如此模糊的資料表示，將能造成安全機制設計的重大疏失，本文提出另一種做法，來改善這個問題，使得GA後的分享影像，可以疊合出完全吻合的機密訊息，使人一目了然，不必猜測。

事實上，秘密訊息會無預期出現白像素的原因，在於選出的分享影像雖然在一開始就已經經過半色調的處理，但還是會有些影像區塊再怎麼進行交換式突變，也無法疊合出機密影像。如圖7所示。兩張分別只有兩個與一個黑像素的2 ×2分享影像，絕無疊合出全黑秘密影像的可能，頂多只能疊合出三個黑像素的秘密影像，此時就會讓秘密訊息上出現無法預期的白點。

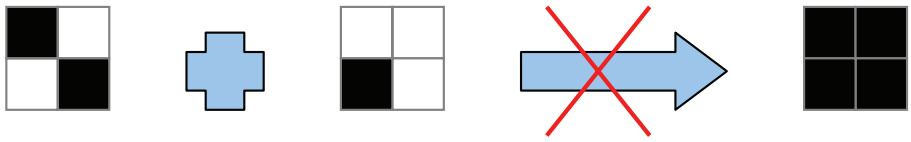


圖7：秘密訊息具有無預期的白像素之原因

為了避免上述情況的發生，我們的解決方法，在於改變GA的演化目標與範圍。以2 out of 2為例，先選定秘密影像與一張Share1，利用這兩者於堆疊規則中的關係，找出必可和Share1疊合出秘密影像的圖形有哪些，以這些圖形做為GA中，個體演化的範圍；另外，選擇另一張有意義/無意義的影像做為演化的目標，設計適當的適應函數，讓個體朝向與此影像相似的方向演化，如此一來，即可利用GA求得最佳的Share2，在絕對可以呈現原始秘密影像的風貌之狀態下，可進一步獲得有意義的Share2。根據上述原理，接下來，本文將應用GA，提出高判讀性視覺密碼加密方法。

二、研究方法

本文所提的研究方法的流程如圖8所示。其中，在進入GA之前，必須進行前置作業等步驟，此乃為了符合視覺密碼的需求，以及有利於進行基因演化，而對分享影像與秘密影像所做的一些處理(以(2,2) visual cryptography scheme為範例)。

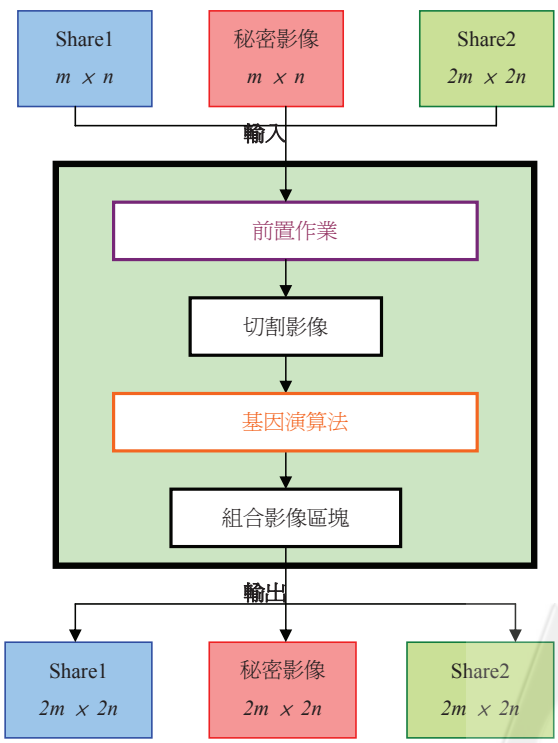


圖8：方法一流程圖

對於圖8的流程，說明如下：

步驟一：輸入影像

假設灰階機密影像大小為 $m \times n$，則選取一張大小 $m \times n$ 的灰階影像為Share1，另選取一張大小 $2m \times 2n$ 的灰階影像為Share2。灰階值範圍皆為0～255。

步驟二：前置作業

此步驟主要目的，在於將一般較常使用的灰階影像轉成半色調影像。所謂半色調影像是一種單位元影像，每個像素只用一個位元記錄，較暗的區域以較密的黑點表示，較亮的區域則以較疏的黑點表示，此讓影像產生一種層次感。因為其讓圖形有相對較不呆板的呈現，又像素的表示剛好符合視覺密碼學一般使用上的型態，故採用之。其前置作業的細部步驟如圖9所示，分述如下：

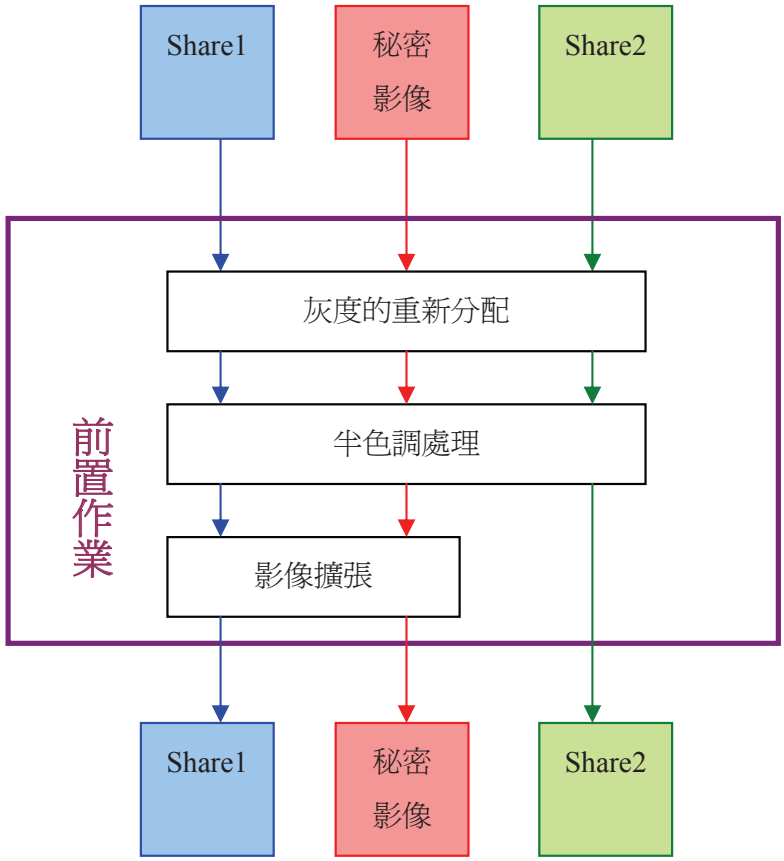


圖9：前置作業

（1）灰度的重新分配：

對秘密影像和分享影像如表2重新分配其灰階值，讓分享影像將來不需太多改變即可疊合成秘密影像。

表2：表度重分配

	原灰階值範圍	分配後灰階值範圍
秘密影像	0 ~ 255	191 ~ 255
Share1	0 ~ 255	128 ~ 192
Share2	0 ~ 255	127 ~ 191

（2）半色調處理：

採用錯誤擴散法(Error Diffusion)，讓灰階影像轉變為半色調影像，此亦符合視覺密碼一般所使用的黑白影像。

（3）影像擴張：

將Share1與秘密影像中的每個像素，分別按照表3擴張成2 ×2的影像區塊。

表3：影像擴張

Share1			**秘密影像**		
	原像素	擴張後		原像素	擴張後
白			白		
黑			黑		

步驟三：影像切割

將秘密影像、兩張分享影像切割成2 ×2的影像區塊。相同位置的區塊影像為一組，各組獨立進入一個基因演算系統。將有(2m ×2n) / (2 × 2) = m ×n組。例如，假設影像大小為100 × 100，則共有2500個影像組，分別進行基因演算。

步驟四：基因演算

經過前面步驟的處理之後，於本步驟正式進入GA的部分。其流程如圖10所示，包含編碼的描述規劃、初始母體染色體的建立、Fitness的計算、選擇和突變操作、終止演化條件等，分述如下：

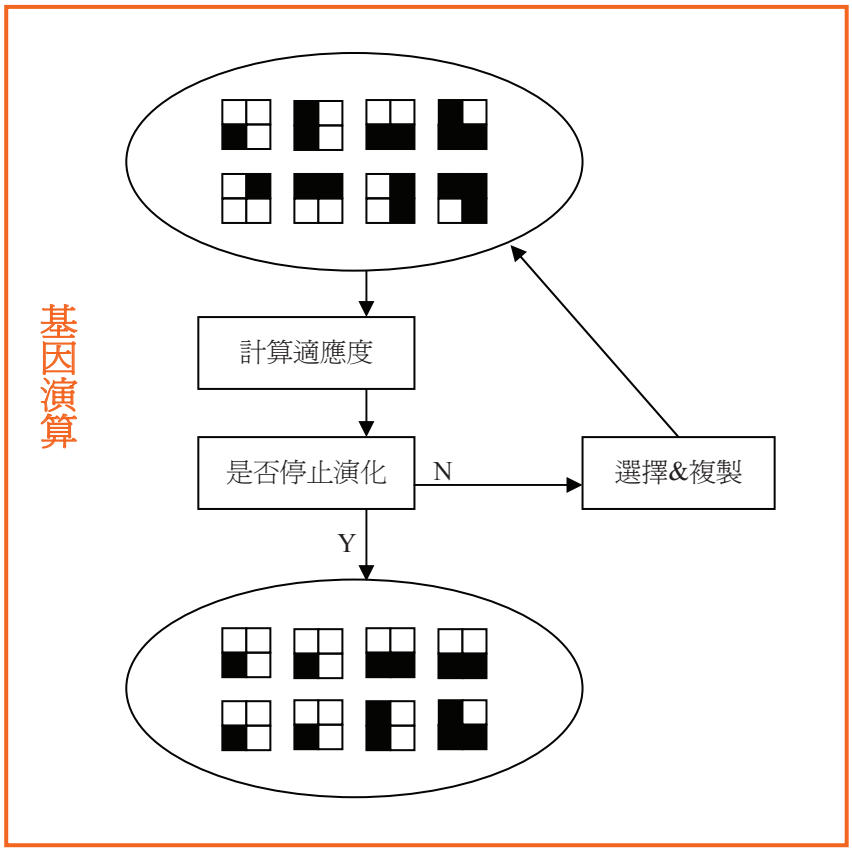


圖10：基因演算的流程

（1）Encode Schemes & Seeding策略：

在開始進行GA之前，須先設定母體大小，並幫這些數值訂定染色體的型式。訂定染色體的型式，需要考慮個體的性狀特徵、項目多寡、有幾種不同的表現方式等問題。二元字串(Binary Strings)就是一種簡單又方便計算的方式。例如，可將染色體以四個位元的二元字串來表示，例如1101。本方法的編碼方式以及初始母體染色體的建立方式如下：

a. 假設母體中共存在s個個體

b. 假設能夠和Share1疊合成秘密影像的圖形共有n種，則初始母體中，每種個體各有s / n個。如同本文上節所提出的原理，母體中，個體的種類將依據Share1與秘密影像而定。其和Share1疊合必定和原秘密訊息吻合才得以為個體的種類之一。以原秘密影像和Share1皆是白像素為例，則初始母體內，會有如圖11所示，有四種不同的個體。

c. 個體染色體的編碼採用二元字串的方式，如圖12所示。染色體的基因排序，依序代表著Share2影像區塊左上、右上、左下、右下的像素資訊。以「0」表示白像素，以「1」表示黑像素。

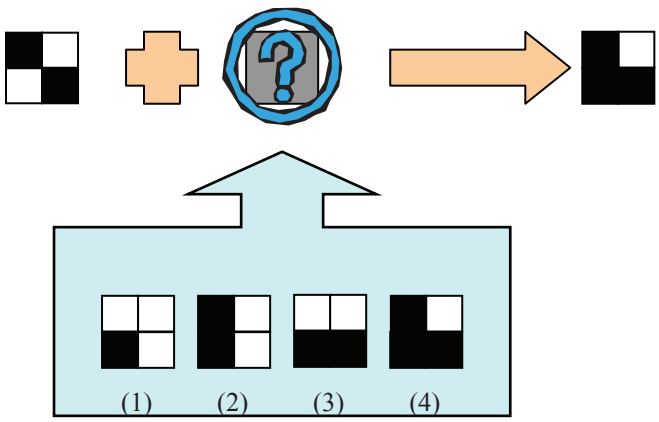


圖11：依據Sharel與秘密影像產生個體的種類

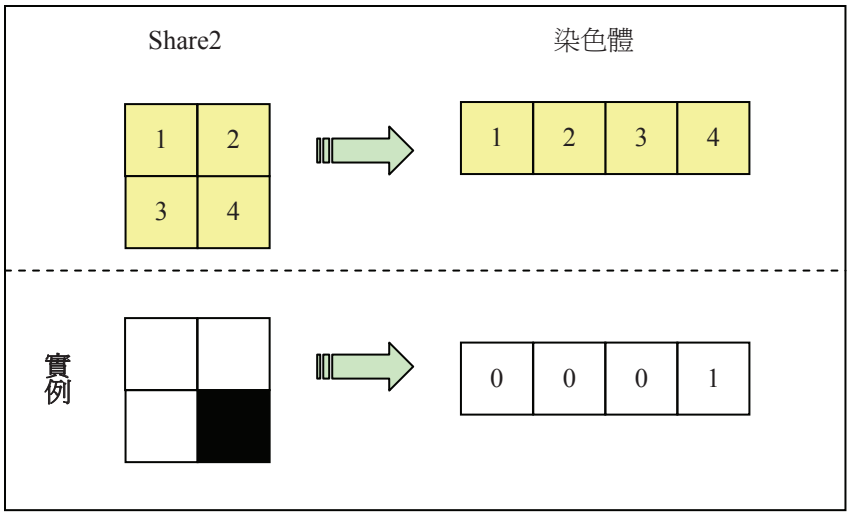


圖12：染色體編碼

（2）Fitness Function：

染色體不同，對於環境的適應程度也不同。故必須設計一個適應函數，以便將個體的適應程度以量化表示。將個體代入此適應函數計算，將得到一個值。值越大，代表此個體的適應度越強。根據此結果，即可對個體的優劣產生評估，因而可判斷其是否符合期待而終止演化。若個體群的優劣已達系統所求條件之程度，則終止演化，否則將進行繁衍。

本方法的適應函數的設計為，當個體中某一位元等於Share2相對應之位元時，適應度加1。也就是說，若四個位置的像素皆相同，則適應度為4；若僅有兩個相同，適應度為2。此做法是為了使經基因演算後的Share2能和原Share2最為相似。也就是說，如果一

開始選定的Share2為有意義之影像，則GA將盡其所能地挑選出最為有意義的影像做為結果。

（3）Selection策略 & Mutation策略：

若認為目前的母體，尚不滿足所期待的程度，就開始進行繁衍下一代的工作。繁衍的工作由三個主要的基因運算子：選擇(Selection)、交配(Crossover)以及突變(Mutation)所組成。選擇乃依據個體的適應程度，可訂定其將繁衍出下一代的機率，此機率亦決定個體將被複製的機率。交配乃選擇兩個個體，交換彼此部分的基因，進而產生新的兩個子代。此兩個子代將承接兩個親代個體的性狀特徵。而突變乃在個體的染色體上，隨機選擇一個或多個突變點，然後改變突變點上的基因，而產生了新個體。突變的動作在於可以確保演化的過程，不會太過侷限於某個方向，讓其他的性狀特徵也有機會登上舞台。對二元字串來說，突變就是將字串中的0變成1，或者將1變成0。

本方法僅選擇選擇與突變做為基因運算子，至於交配則不使用。進行選擇的做法，在於選出母體中，適應度排名在前50%的個體，使其留下來，得以複製出下一代；至於排名後50%的個體，則進行「全然的突變」。本文所謂「全然的突變」是指舊個體隨機變成所有個體種類之其中一種個體。如此一來，不同種類的個體皆有機會進行演化，且母體中，總是維持著一定的個體總數。以圖11為例，若原本為個體(1)，其進行全然的突變，則可隨機變為圖11裡個體(1)~(4)中的其中一種。

（4）終止演化條件：

當母體中，有某種個體佔總數半數以上時，或者演化世代數已到20代後，便終止演化，否則繼續。此終止條件的設立，一方面式為了適時選出最適合當作Share2的個體，另一方面是為了防止基因演算永無止日。新母體被產生之後，又將重複2~4的演化過程，直到符合終止條件為止。當終止基因演算後，以母體中所佔數量最多的種類之個體，為基因演算出之影像區塊。

步驟五：組合影像區塊

當所有的影像區塊都完成步驟四GA之後，則進入最後組合影像區塊的步驟，即將各組經基因演化求得的影像區塊組合回來，就獲得了經加密的Share2。而Share1與秘密影像在經過影像擴張的加工之後，已成為2m ×2n的黑白影像。

肆、實驗結果與討論

一、實驗結果

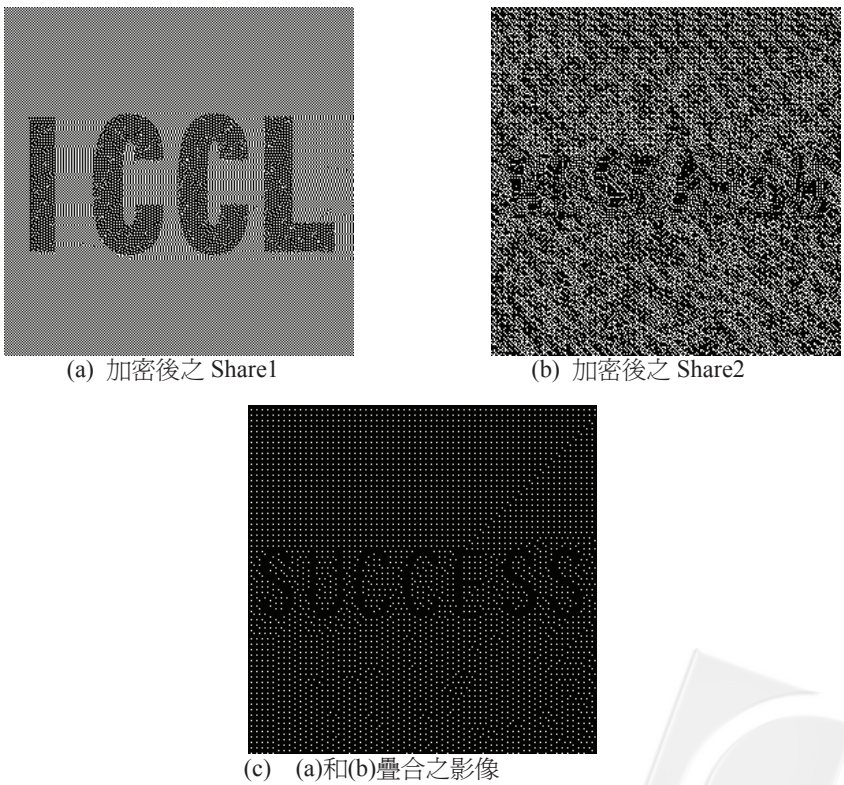
我們的實驗是使用個人電腦做為實驗平台，並利用Microsoft Visual Studio.NET 2003做為系統開發的程式工具。以下共呈現了三個實驗: 實驗一、實驗二和實驗三為本文所提方法的實驗結果。

（一）實驗一

選定如圖13中，(a)128 ×128像素大小的灰階影像「ICCL」做為Share1原圖，(b)256 × 256像素大小的灰階影像「RESEARCH」做為Share2原圖，(c) 128 × 128像素大小的灰階影像「SUCCESS」做為秘密影像。而實驗結果如圖14所示，(a)為加密過之Share1，(b)為加密過之Share2，(c)為(a)、(b)疊合之結果。

(a) Share1 原圖　(b) Share2 原圖　(c) 秘密影像

圖13：實驗一Share1、Share2和秘密影像原圖



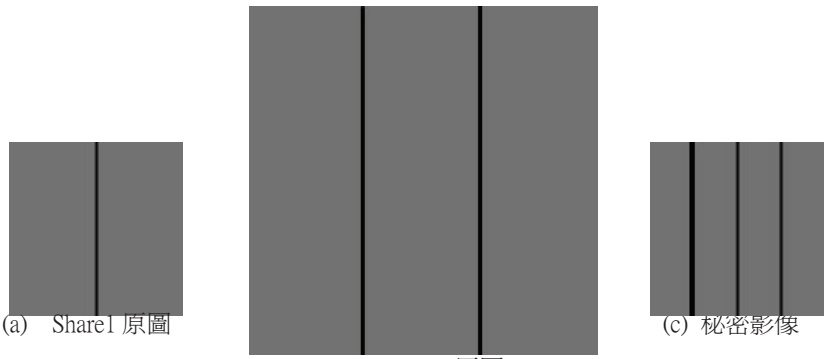
(a) 加密後之 Share1　(b) 加密後之 Share2

(c) (a)和(b)疊合之影像

圖14：實驗一結果

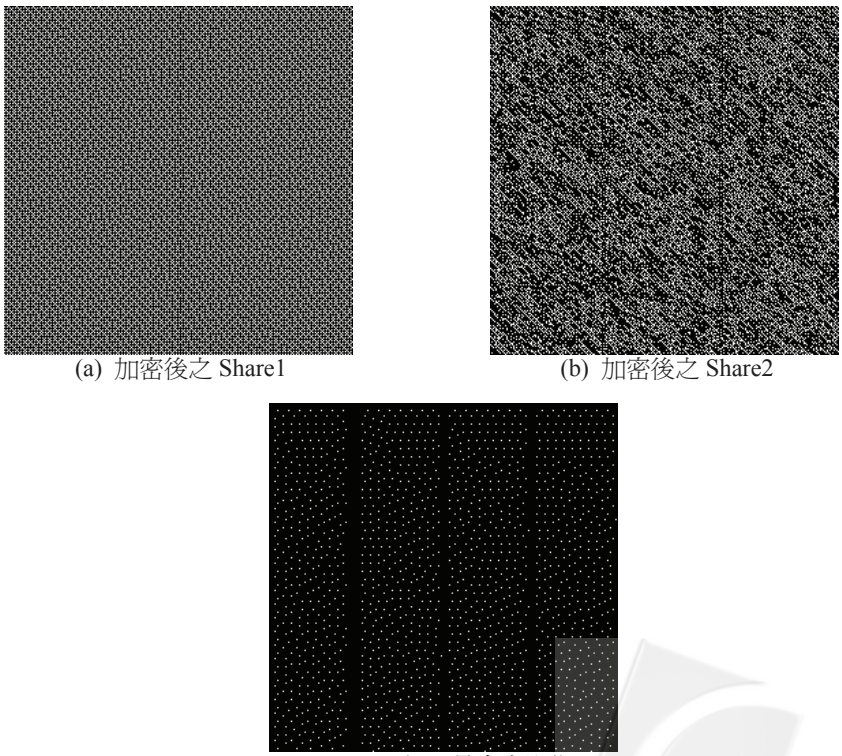
（二）實驗二：

選定如圖15中，(a)128 × 128像素大小的灰階影像「｜」做為Share1原圖，(b)256 × 256像素大小的灰階影像「｜｜」做為Share2原圖，(c) 128 × 128像素大小的灰階影像「｜｜｜」做為秘密影像。而實驗結果如圖16所示，(a)為加密過之Share1，(b)為加密過之Share2，(c)為(a)、(b)疊合之結果。



(a) Share1 原圖　(b) Share2 原圖　(c) 秘密影像

圖15：實驗二Share1、Share2和秘密影像原圖



(a) 加密後之 Share1　(b) 加密後之 Share2

(c) (a)和(b)疊合之影像

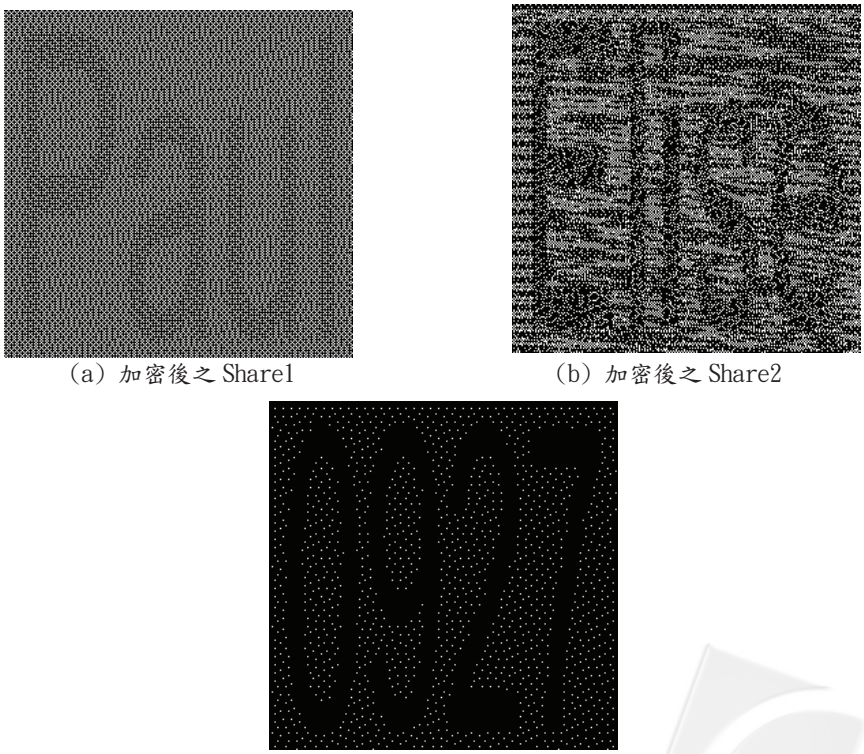
圖16：實驗二結果

（三）實驗三：

選定如圖17中，(a)128 × 128像素大小的灰階影像「Paul」做為Share1原圖，(b)256 ×256像素大小的灰階影像「Elise」做為Share2原圖，(c) 128 × 128像素大小的灰階影像「0927」做為秘密影像。而實驗結果如圖18所示，(a)為加密過之Share1，(b)為加密過之Share2，(c)為(a)、(b)疊合之結果。另外，附上文獻(邱文怡等2002)的實驗結果(圖19)，提供讀者比較。

(a) Share1 原圖　(b) Share2 原圖　(c) 秘密影像

圖17：實驗三Share1、Share2和秘密影像原圖



（a）加密後之 Share1　（b）加密後之 Share2

(c)： (a)和(b)疊合之影像

圖18：實驗三結果

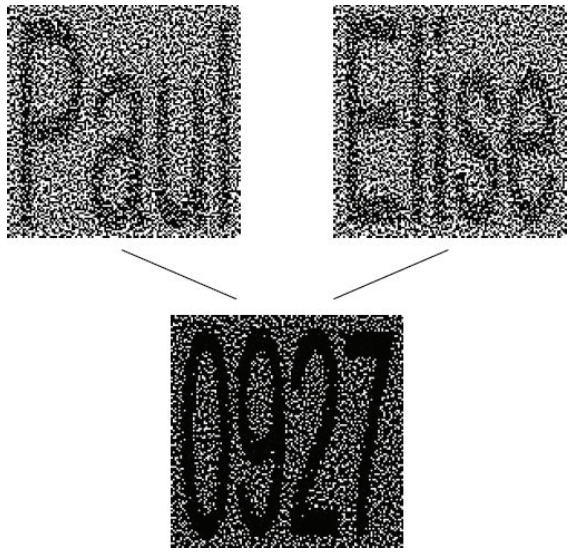


圖19：文獻(邱文怡等 2002)實驗結果

（四）實驗四：

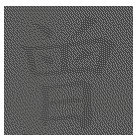
選定如圖20中，(a)128 × 128像素大小的灰階影像「曾」做為Share1原圖，(b) 256 × 256像素大小的灰階影像「經」做為Share2原圖，其中(c1)～(c5) 為128 × 128像素大小的灰階影像「滄」「海」「難」「為」「水」做為秘密影像。而我們所提出方法的實驗結果如圖21所示，其中(a)為加密過之Share1，(b1)～(b5)為加密過之Share2，(c1)～(c5)為(a)、(b1)～(b5)疊合之結果。另外，附上文獻(邱文怡等 2002)的實驗結果如圖22所示，提供讀者比較。

(a) Share1 原圖　　(b) Share2 原圖

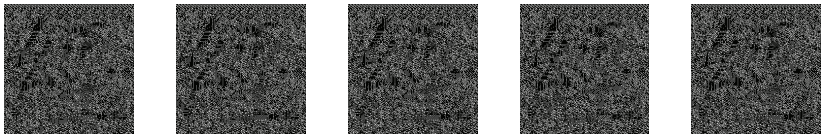
(c1)　(c2)　(c3)　(c4)　(c5)

秘密影像

圖20：實驗四Share1、Share2與秘密影像原圖

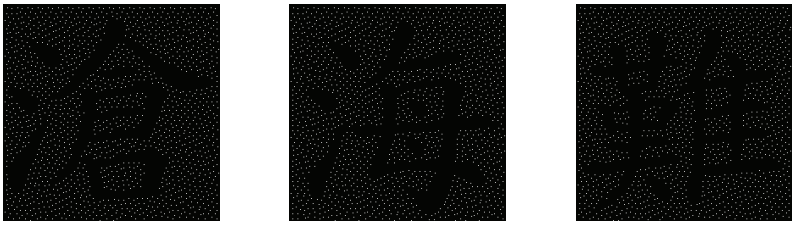


(a) 加密後之 Share1

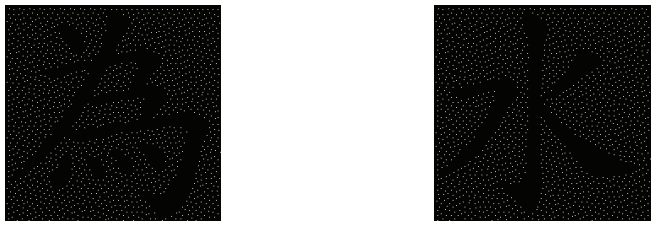


(b1) (b2) (b3) (b4) (b5)

加密後之 Share2



(c1): (a)和(b1)疊合影像 (c2): (a)和(b2)疊合影像 (c3): (a)和(b3)疊合影像



(c4): (a)和(b4)疊合影像 (c5): (a)和(b5)疊合影像

圖21：我們的方法實驗四裡疊合後之影像結果

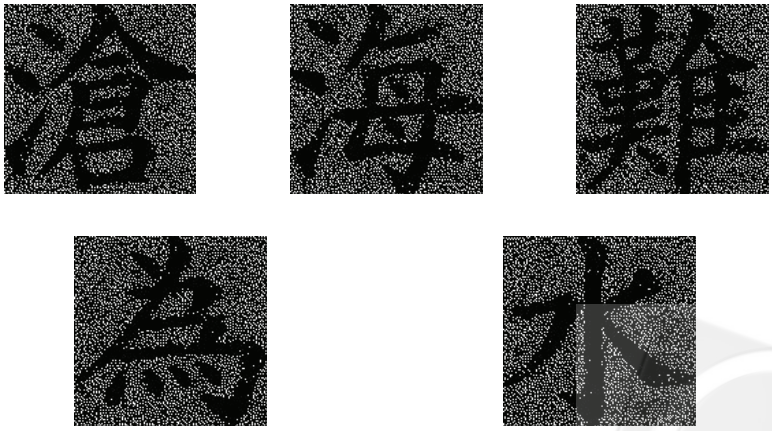


圖22：文獻(邱文怡等 2002)實驗結果

二、比較傳統視覺安全機制

傳統的視覺密碼學為了使分享影像有意義，使用編碼表(Code Book)來進行加密。此方式是針對秘密影像的每一像素，依照事先訂好的編碼表，將其擴張成數個像素，分享影像因此亦將比原秘密影像大數倍。然而，對於有經驗的人來說，只要擷取到利用此方式所加密出的任何分享影像，靠某些簡單分析的方式，還是有可能很容易就破解。以表4為例(取自(吳佳鴻 2003))，我們可以觀察出，只要Share2右上角像素為白，則秘密影像就是白，右上角像素為黑，秘密影像就是黑。以現代電腦技術的發達，只要將分享影像分割成，以2 ×2像素大小的影像區塊為單位，分別只讀取四個角的像素來顯示整張影像，不需花費很多時間，就可破解出秘密訊息。

表4：傳統Code Book (取自(吳佳鴻 2003))

秘密影像	Share1	Share2	疊合影像
白 □	白 ■ 白 ■ 黑 ■ 黑 ■	白 ■ 黑 ■ 白 ■ 黑 ■	■
黑 ■	白 ■ 白 ■ 黑 ■ 黑 ■	白 ■ 黑 ■ 白 ■ 黑 ■	■

而我們的方法採GA的方式進行加密，所產生的分享影像並沒有一定的規則可循，有心人士無法藉著上述的分析方式找到脈絡，取得秘密訊息。因此，使用我們的方法是較為安全的。

此外，傳統的視覺密碼經過許多專家學者的研究，提出了許多不同的編碼表，各有各的用途。因此也增添了編碼表的儲存與管理工作。而我們的方法不需要使用編碼表即可進行加密，省去了許多麻煩。

三、相關文獻比較

如同本文第三節所述，文獻(邱文怡等 2002)之方式，將可能造成疊合分享影像所獲

得的秘密訊息令人辨識不易，導致秘密訊息的判讀錯誤。雖然此並非其之常態，但在某些重要時刻，是決不容許有這樣的錯誤發生的。而我們的方法，從實驗結果中可知，即使原秘密訊息的字體非常的纖細，從Share1和Share2疊合出的影像中仍可很輕易地辨識出秘密訊息，以實驗二的數據:「｜」為例 ，在我們所提的方法下並不會有類似英文字元「i」與「l」因夾雜的白點導致分辨不清楚的情況(以Share1和Share2疊合出的影像「i」與「l」)。另外，從實驗三與從實驗四的結果與文獻(邱文怡等 2002)的實驗結果比較中可看出，我們的秘密訊息「0927」、「滄」、「海」、「難」、「為」、「水」字樣中，確實不存在著雜亂無章的白點。換言之，本研究之方法成功達到「確保秘密訊息的正確性，降低人眼判讀錯誤的可能」之研究目的。

伍、結論

GA本身解決問題的特點，讓視覺密碼系統在加密的過程中，不必多花時間在編碼表的製作、儲存與管理上，顯得方便許多。本文提出的做法，藉改良GA並降低錯誤判讀的機會。由本文實驗結果亦可看出，我們的方法確實可以保持秘密訊息的正確性，與更清晰判讀訊息，並且還能保有對比性與安全性。雖然犧牲了其中一張分享影像的有意義性，但卻能換來秘密訊息的正確無誤，對許多的情況來說，是很值得的。利用GA產生出的視覺密碼，較利用編碼表擁有許多的優點，更方便人們所使用，相信妥善利用本研究的成果，能增加更多的安全以及便利。

致謝

This work was supported in part by the National Science Council of the Republic of China under the Grant NSC 95-2221-E-015-002-MY2, and by the iCAST project sponsored, National Science Council under the Grants NSC 95-3114-P-001-001-Y02 and NSC 95-3114-P-001-002-Y02.

參考文獻

1. 沈伯成，2003，灰階視覺密碼浮水印，中央大學資訊管理學系碩士論文。
2. 吳佳鴻，2003，彩色影像之擴充型視覺密碼，中央大學資訊管理學系碩士論文。
3. 邱文怡、洪國寶、王乾隆、許琪慧，2002，『應用微小母體之基因演算法於視覺密碼學』，第十二屆全國資訊安全會議，307～314頁。
4. 周鵬程，2002，遺傳演算法原理與應用活用Matlab，全華科技圖書。
5. 侯永昌、張雅惠，2003，『應用遺傳演算法於向量量化之新編碼簿設計法』，電腦學刊，第十五卷．第二期。

6. 黃昭平、張克章、 侯永昌，2000，『基因密碼產生器之設計與研究』，中華管理評論，第三卷．第一期，173～186頁。
7. Naor, M. and Shamir, A.“Visual Cryptography,”*In Advances in Cryptology-EUROCRYPT ’94, LNCS 950, Springer-Verlag*, 1995, pp. 1-12.
8. Shamir, A.,“How to Share a Secret,”*Communications of the ACM* (22), 1978, pp. 612-613.
9. Tsai, D.S., Chen, T.H, and Horng, G.“A New Cheating Prevention Scheme for Visual Cryptography,”*Proceedings of the 16th National Conference on Information Security*, R.O.C., 2006, pp. 520-527.