視覺密碼學綜述

郭騰[1,2]，劉峰[1]，武傳坤[1]
[1]中國科學院信息工程研究所 信息安全國家重點實驗室
[2]中國科學院大學
{guoteng, liufeng, ckwu}@iie.ac.cn

摘要

視覺密碼方案將一張秘密圖片分解為多張分享圖片，使得被授權的參與者集合能夠獲得秘密資訊，而非授權的參與者集合不能夠獲得秘密資訊。視覺密碼的解密過程不依賴於計算設備，而且允許參與者通過簡單地對齊分享圖片來直接觀察到解密圖片。視覺密碼的研究吸引了越來越多的關注，本論文試圖總結一下視覺密碼的研究方向，為接觸該領域不久的研究人員提供一個有關視覺密碼研究的宏觀視圖。

關鍵詞： 視覺密碼，對比度，圖元擴張，灰度及彩色，隨機網格

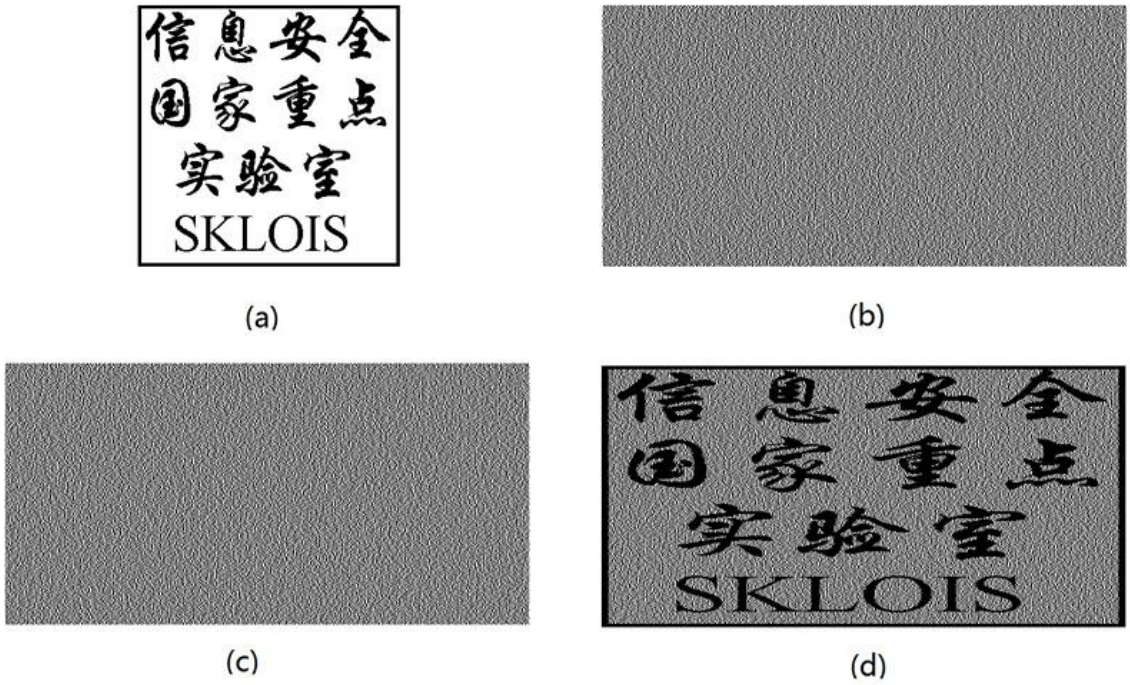
壹、前言

視覺密碼學（Visual cryptography, VC）是由 Naor 和 Shamir 在 1994 年的歐密會上首先提出來的，它與傳統密碼學的主要區別在於其解密過程只需要手工地疊加印刷著秘密資訊的透明膠片，而不需要進行複雜的計算，而參與者也不需要具備密碼學相關的知識。一個視覺密碼方案（Visual cryptography scheme, VCS）包含兩個階段：加密階段和解密階段。在加密階段，VCS 把需要分享的秘密圖片（Secret image）加密成多個分享圖片（Share image），並將其印刷到透明膠片（Transparencies）上。然後給每個參與者分配一個分享圖片，使得被授權的參與者集合能夠通過簡單的疊加獲得秘密資訊，而非授權的參與者集合不能夠獲得除了秘密圖片尺寸之外的任何資訊。下面我們給一個例子來說明上述過程：總共有兩個參與者，記為 P={1,2}。被授權的參與者集合定義為$\Gamma_{Qual} = \{1, 2\}$，而非授權的參與者集合定義為$\Gamma_{Forb} = \{\{1\}, \{2\}\}$。上面的存取結構又被簡稱為(2,2)門限存取結構（Threshold access structure）。

一個包含 n 個參與者的視覺密碼方案將一張秘密圖片 S 加密成了 n 張分享圖片 $S_1, S_2, \ldots, S_n$，使得分享圖片S_i看起來是雜訊圖片。下面我們給出一個(2,2)-VCS 來說明上述過程。假設秘密圖像上要加密的圖元為$w \in \{0, 1\}$（其中，0 表示白圖元，1 表示黑圖元）。為了分享該秘密圖元，我們選擇M_w作為分享矩陣，然後隨機地置換它的列向量，最後把第$i \in \{1, 2\}$行分配給參與者i。如果 w=0，那麼兩行疊加所得到向量的漢明重量為 1；如果 w=1，那麼兩行疊加所得到向量的漢明重量為 2，因此我們可以從分享圖片 1 和 2 的疊加結果中看到秘密圖片。

$$M_0 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

(2,2)-VCS 的詳細實驗結果見圖一。



圖一：(2, 2)-VCS 的實驗結果：(a)原始秘密圖片，大小300×300，(b)分享圖片 1，大小600×300，(c)分享圖片 2，大小600×300，(d)分享圖片 1 和 2 的疊加結果，大小600×300。

在圖一中，通過觀察(b)和(c)，我們不能得到關於原始秘密圖片(a)內容的任何資訊；通過觀察(d)，我們可以看到圖片(a)的內容。

通過以上的敘述和分析，不難看到視覺密碼具有如下幾個特點：

[1.] 屬於秘密共用系統，其中每張分享是一副圖片；

[2.] 解密過程無需複雜的計算，而僅需對齊所收集的分享圖片來完成。

[3.] 提供了無條件安全（Unconditional security）的保證。

視覺密碼方案在加密階段只需要一台連著印表機的普通電腦和若干張透明膠片就可以產生分享圖片，其中透明膠片可以像普通紙張一樣放入印表機中。視覺密碼方案在解密階段不需要依賴於電腦系統，僅需要手工地對齊印刷著秘密資訊的透明膠片就可以恢復出秘密資訊。總的來說，視覺密碼方案使用方便，不要求使用者具備密碼學知識，而其所需要的設備也容易獲得，成本低廉，很適合應用到人們的日常生活中。此外，視覺密碼方案加解密的物件是圖片，資訊容量大，所謂一圖勝千言，普通使用者也更加願意從圖像上獲取資訊，這為視覺密碼的發展和應用提供了良好的前景。文獻[1]通過視

覺密碼來保護使用者持有的口令。文獻[1]將視覺密碼應用到了安全兩方計算中，使得最終計算結果可以通過疊加透明膠片來得到。文獻[10][35]借助於視覺密碼技術來實現數位浮水印，從而保護數位媒體的版權。

貳、視覺密碼方案的形式化定義

視覺密碼方案屬於秘密共用（Secret sharing）系統，因而其方案是基於某個存取結構（Access structure）的。我們首先介紹存取結構的相關知識。

2.1 有關存取結構的基礎知識

在一個秘密共用系統當中，所有的參與者集合記為$P=\{1,2,\ldots,n\}$。一個存取結構就是對授權參與者集合（Qualified participant sets）$\Gamma_{Qual}\subseteq 2^P$和非授權參與者集合（Forbidden participant sets）$\Gamma_{Forb}\subset 2^P$的刻畫。任何的授權參與者集合$X\in\Gamma_{Qual}$ 能夠通過疊加他們的分享圖片來獲得秘密資訊，但是任何的非授權參與者集合$Y\in\Gamma_{Forb}$不能夠獲得除了秘密圖片尺寸之外的有關秘密圖片的任何資訊。最小的授權參與者集合（Minimal qualified sets）定義為$\Gamma_0=\{A\in\Gamma_{Qual}:A'\notin\Gamma_{Qual}$對於所有的$A'\subsetneq A\}$。如果$\Gamma_{Qual}$是單調遞增的，$\Gamma_{Forb}$是單調遞減的並且$\Gamma_{Qual}\cup\Gamma_{Forb}=2^P$，那麼我們稱 Γ 為強存取結構（Strong access structure）。在強存取結構 Γ 裡面 $\Gamma_{Qual}=\{A\subseteq P:A\supseteq B$ 對於某個$B\in\Gamma_0\}$，我們又稱Γ_{Qual}是Γ_0的*閉包*。如果$\Gamma_{Qual}=\Gamma_0$，那麼我們稱 Γ 為弱存取結構（Weak access structure）。對於*(k, n)*的門限存取結構，$\Gamma_0=\{B\subseteq P:|B|=k\}$ 而$\Gamma_{Forb}=\{B\subseteq P:|B|\leq k-1\}$。如果$\Gamma$是一個強的*(k, n)*的門限存取結構，那麼$\Gamma_{Qual}=\{B\subseteq P:|B|\geq k\}$。如果$\Gamma$是一個弱的*(k, n)*的門限存取結構，那麼$\Gamma_{Qual}=\Gamma_0=\{B\subseteq P:|B|=k\}$。因此，對於一個強的*(k, n)*-VCS，我們需要保證通過疊加多於或者等於 *k* 個分享圖片可以得到秘密資訊，而對於一個弱的*(k, n)*-VCS，我們僅需要保證通過疊加恰好 *k* 個分享圖片可以得到秘密資訊。最大非授權集合（Maximal forbidden sets）定義為$\Gamma_M=\{A\in\Gamma_{Forb}:A'\in\Gamma_{Qual}$,對於任意的$a\in P\setminus A, A'=A\cup\{a\}\}$。對於*(k, n)*的門限存取結構，$\Gamma_M=\{B\subseteq P:|B|=k-1\}$。

2.2 常用視覺密碼方案的定義及比較

宏觀上講，一個視覺密碼方案將一幅秘密圖片加密為多個分享圖片，並將其分配給多個參與者，使得被授權的參與者集合能夠通過疊加他們的分享圖片來獲得秘密資訊，而對於非授權參與者集合來講，他們不能從他們的分享圖片中獲得任何有關秘密的資訊。

在正式給出視覺密碼方案的定義之前，我們首先建立我們的符號系統。記 *X* 為$\{1,2,\cdots,n\}$的一個子集，同時記|*X*|為 *X* 的基數。記 *M* 為一個$n \times m$的矩陣。*M[X]*表示由集合 *X* 中的行構成的新的矩陣，易知 *M[X]*是一個$|X| \times m$的矩陣。記 *H(M[X])*為由 *M[X]*的所有行通過或（OR）運算得到的行向量的漢明重量（Hamming weight）。記 C_0 和 C_1 為兩個由$n \times m$布林矩陣（Boolean matrices）構成的多重集合，具體地將其分別記為$C_0[X] = \{M[X] : M \in C_0\}$和$C_1[X] = \{M[X] : M \in C_1\}$。

定義在通用存取結構上的視覺密碼方案是由 Ateniese 等人提出來的[5]。在一個 VCS 中，我們逐個圖元地加密原始秘密圖片。如果當前圖元為白色（resp. 黑色），我們從 C_0（resp. C_1）中隨機地選取一個分享矩陣，然後將其第 *j* $(1 \le j \le n)$ 行分配給分享圖片 *j*，其中 0 表示一個白圖元，而 1 表示一個黑圖元。下面我們給出其形式化的定義：

定義 1 [通用存取結構的視覺密碼方案[3]]

兩個由$n \times m$布林矩陣構成的多重集合*(C_0, C_1)*構成了一個 $(\Gamma_{Qual}, \Gamma_{Forb})$-VCS 如果其滿足下面的條件:

（對比度條件）對於任意的參與者集合$X \in \Gamma_{Qual}$，我們記$l_X = \max_{M \in C_0[X]} H(M)$，而記$h_X = \min_{M \in C_1[X]} H(M)$。那麼下面的不等式必須成立：$0 \le l_X < h_X \le m$。

（安全性條件）對於任意的參與者集合$Y \in \Gamma_{Forb}$，相同的矩陣以相同的頻率出現在 *C_0 [Y]* 和 *C_1 [Y]* 當中。

下面我們介紹定義當中的基本參數：

1）*m* 被稱為圖元擴張（Pixel expansion）。

2）l_X 和 h_X 是恢復出來的白色圖元和黑色圖元的閾值，其中 l_X 又被稱為暗度級（Darkness level），h_X 又被稱為亮度級（Whiteness level）。

3）$\alpha_X = \frac{h_X - l_X}{m}$ 被稱為授權集合 *X* 的對比度（Contrast），而 $\alpha = \min_{X \in \Gamma_{Qual}} \alpha_X$ 則被稱為視覺密碼方案 $(\Gamma_{Qual}, \Gamma_{Forb})$-VCS 的對比度。

對於比較特殊的存取結構，例如*(k, n)*的門限存取結構，其視覺密碼方案簡記為 *(k, n)*-VCS。當 $h_X = m$ 時，我們稱該方案為完美黑恢復（Perfect black recovery）的視覺密碼方案[6][16]。

如果兩個由$n \times m$布林矩陣構成的多重集合*(C_0, C_1)*可以通過以所有可能的方式置換對應的$n \times m$布林矩陣的列來得到(S_0對應C_0，而S_1對應C_1)，那麼我們稱這兩個$n \times m$布林矩陣為基矩陣（Basis matrices）[3]。在這種情況下，兩個多重集合*(C_0, C_1)*的大小相同(都等於 *m!*)。基於基矩陣的 VCS 僅需要很少的記憶體（僅存儲基矩陣S_0和S_1，而不必存儲兩個由基矩陣構成的多重集合*(C_0, C_1)*，而且在 C_0 (resp. *C1*) 中隨機的選取一個分享矩陣是很高效的，它僅需要產生一個 S_0（resp. S_1）的隨機列置換）。基矩陣被廣泛的應用於構造 VCS 或者證明 VCS 中參數的界（參考[3][26][8][9][28][24]）。下面我們形式化地給出基矩陣 $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, m, n)$-VCS 的定義:

定義 2[基矩陣視覺密碼方案[3]]

兩個$n \times m$布林矩陣(S_0, S_1)構成了一個視覺密碼方案$(\{\Gamma_{Qual}, \Gamma_{Forb}\}, m, n)$-VCS，如果其滿足下面的條件:

（對比度條件）對於任意的參與者集合$X \in \Gamma_{Qual}$，我們記$l_X = H(S_0[X])$，而記$h_X = H(S_1[X])$。那麼下面的不等式必須成立：$0 \leq l_X < h_X \leq m$

（安全性條件）對於任意的參與者集合$Y \in \Gamma_{Forb}$，$S_0[Y]$ 和 $S_1[Y]$ 在所有可能的列置換下生成的多重集合是相等的。

有時我們也稱 S_0 (resp. S_1)為黑(resp.白)基矩陣。為了消除圖元擴張，Ito.等人和 Yang 提出了無擴張的視覺密碼方案(Size invariant visual cryptography scheme，簡記為 SIVCS)。在 SIVCS 中，為了加密一個黑(resp.白)圖元，我們從黑(resp.白)基矩陣 當中隨機地選取一列，然後把此列的第 i 行分配給參與者 i。因為秘密圖片中的一個黑圖元恢復成一個黑圖元的概率要高於秘密圖片中的一個白圖元恢復成一個黑圖元的概率，因此我們可以從宏觀上看到秘密資訊。

下面我們形式化地給出無擴張的視覺密碼方案$(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n)$-SIVCS 的定義:

定義 3[無擴張的視覺密碼方案[21]]

兩個由 $n \times m$ 布林矩陣構成的多重集合(C_0, C_1)構成了一個 $(\{\Gamma_{Qual}, \Gamma_{Forb}\}, n)$-SIVCS，如果其滿足下面的條件:

（對比度條件）對於任意參與者集合$X \in \Gamma_{Qual}$，我們記$\bar{l}_X = \sum_{M \in C_0[X]} \frac{H(M)}{|C_0[X]|}$，而記

$\bar{h}_X = \sum_{M \in C_1[X]} \frac{H(M)}{|C_1[X]|}$。那麼下面的不等式必須成立：$0 \leq \bar{l}_X < \bar{h}_X \leq 1$。

（安全性條件）對於任意參與者集合$Y \in \Gamma_{Forb}$，相同的列向量以相同的頻率出現在 $C_0[Y]$ 和 $C_1[Y]$ 當中。

與 VCS 相比，SIVCS 的優勢在於沒有圖元擴張，而它的劣勢在於恢復出來的秘密圖片的視覺品質變差。除此之外，在 VCS 中，從秘密圖片中一個白圖元恢復出來的區塊的漢明重量一定嚴格小於從秘密圖片中一個黑圖元恢復出來的區塊的漢明重量，
因此我們可以精確地恢復秘密圖片（也就是說，可以恢復出秘密圖片的每一個圖元）。而對於 SIVCS，秘密圖片中一個白圖元或一個黑圖元都可能恢復成一個白圖元，也可能恢復成一個黑圖元。因此，在 SIVCS 中，雖然我們可以從宏觀上在恢復出來的秘密圖片中觀察到秘密資訊，但是我們並不能精確地恢復秘密圖片。

參、視覺密碼方案的評價指標

目前視覺密碼方案的評價指標包括對比度，圖元擴張和隨機性三方面。通常認為對

比度反映了所恢復出來的秘密圖片的視覺效果，對比度越大，所恢復圖片的視覺效果越好。因此，我們總是希望對比度越大越好。圖元擴張關係到分享圖片所需要的存儲空間的大小和幻燈片的尺寸，圖元擴張越大，所需要的存儲空間越多。因此，我們總是希望圖元擴張越小越好。隨機性是對分享一個圖元的過程當中所需的隨機比特數量的衡量，隨機性越大，分享一個圖元所需的隨機比特就越多。因此，我們也總是希望隨機性越小越好。由於對比度直接關係到恢復圖片的視覺效果，圖元擴張直接關係到分享圖片所需要的存儲空間的大小和所印刷的透明膠片的尺寸，因此針對這兩個參數的研究很多。而針對隨機性的研究則比較少，但是隨機性作為視覺密碼方案的一個固有屬性，從理論角度來看，也是一個很重要的參數。以上三個參數相互影響和限制，作為很長時間的公開問題，至今尚無確定的關係式來描述他們之間的相互限制關係。根據已知的結論，我們知道，對於 *(2,n)*-VCS，在對比度達到最優的條件下，最小的圖元擴張要大於無限制條件下的最優的圖元擴張。因此，從宏觀上來看，對比度的最大化與圖元擴張的最小化是兩個相互矛盾的最優化目標。但是對於*(n,n)*-VCS，最優的對比度和最優的圖元擴張可以同時達到，分別是2^{n-1}和$\frac{1}{2^{n-1}}$。

3.1 對比度

圖片對比度的定義最早是由 Naor 和 Shamir 提出的[26]，由參數$0 < \alpha \leq 1$來表示。但是由於研究人員不認同上述對比度定義恰好反映了圖片的真實視覺效果，因此上述對比度的定義尚存在爭議。例如，文獻[30]指出：在對比度一定的條件之下，當秘密圖片中的黑圖元所恢復出來的區塊全部由黑圖元構成時，該方案的視覺效果較好，這種方案被稱為完美黑恢復（Perfect black recovery）的視覺密碼方案。但是由於文獻[26]中對比度的定義比較簡單，相對比較容易分析，因此最廣泛應用的對比度的定義仍然是 Naor 和 Shamir 在文獻[26]中提出來的。

由於所恢復出來的秘密圖片與原始秘密圖片相比，有對比度上的損失，因此我們總是希望對比度越高越好，從而使得恢復出來的圖片與原始圖片在視覺品質上更加接近。目前，提高對比的研究方法有如下幾類：

1) 通過組合設計(Block design, BD)的理論來研究基矩陣的結構，從而得到某些（例如：*(n,n)*，*(2,n)*，*(3,n)*，*(4,n)*，*(5,n)*）特殊存取結構下對比度的最優值。但是由於基矩陣的組合結構非常複雜，因此此類方法通常需要很多數學知識與技巧。相應的研究可見[26][8][9][30][7]。
2) 通過線性規劃(Linear programming, LP)的理論來求解對比度的最優值，此類方法的難點在於將對比度用盡可能少的變數表示出來。相應的研究可見[17][23]。
3) 採用其他的最優化搜索演算法，搜索出具有最大對比度的方案。此類方法的難點也是在於將對比度用盡可能少的變數表示出來。此類方法的優點是其通用性，而缺點是搜索效率通常較低。相應的研究可見[22][19]。

3.2 圖元擴張

圖元擴張表示秘密圖片中的一個圖元對應分享圖片中的多少個圖元，通常用 m 來表示。從宏觀上來看，圖元擴張 m 表示分享圖片的尺寸比原始秘密圖片的尺寸大了多少倍。當圖元擴張 m 不是平方數時，圖片就難免有形變，因此，我們常常通過添加冗餘圖元來將圖元擴張變成一個平方數，或者採用類似拼版的技術來排列子圖元。目前，降低圖元擴張的研究方法有如下幾類：

1) 通過組合設計的理論來研究基矩陣的結構，從而得到某些（例如：(n,n)，$(2,n)$）特殊存取結構下圖元擴張的最優值。相應的研究可見[26][8][9][30]。
2) 通過整數規劃(Integer programming, IP)的理論來求解對比度的最優值，此類方法的難點在於將圖元擴張用盡可能少的變數表示出來。相應的研究可見[27]。
3) 採用其他的最優化搜索演算法，搜索出具有最大圖元擴張的方案。此類方法的難點也是在於將圖元擴張用盡可能少的變數表示出來。此類方法的優點是其通用性，而缺點是搜索效率通常較低。相應的研究可見[22][19]。

3.3 隨機性

隨機性表示分享一個秘密圖元需要多少個隨機比特，其做為視覺密碼方案的一個基本屬性，從理論角度來講具有很重要的意義。由於真正的隨機比特是很重要一種資源，我們期望一個視覺密碼方案的隨機性盡可能的小。

Bonis 等人給出了一個變換演算法，其可以將一個二元秘密共用方案（Binary secret sharing scheme，BSS）轉換為具有相同存取結構且隨機性相同的視覺密碼方案 [14]。Dupuy 等人從隨機性角度研究了視覺密碼與秘密共用之間的關係[15]。視覺密碼方案隨機性方面的研究與圖元擴張和對比度方面的研究相比要少得多。其中部分原因在於，從實踐角度來講，我們可以通過一個偽亂數產生器（Pseudo-random generator，PRG）從一個短的真隨機種子得到一個很長的偽隨機比特輸出流。

肆、視覺密碼的底層物理原理

4.1 基於 *OR* 運算的疊加模型

最早的視覺密碼模型是 Naor 和 Shamir 於 1994 年在歐密會上提出的，它是基於 *OR* 運算的。對應的物理模型可以簡述如下：將分享圖片列印到透明膠片上。當印有分享圖片的透明膠片進行疊加時，黑色圖元（用 1 來表示）和白色圖元（即透明圖元，用 0 來表示）疊加得到黑色圖元；兩個黑色圖元疊加也是得到黑色圖元；只有當兩個白色圖

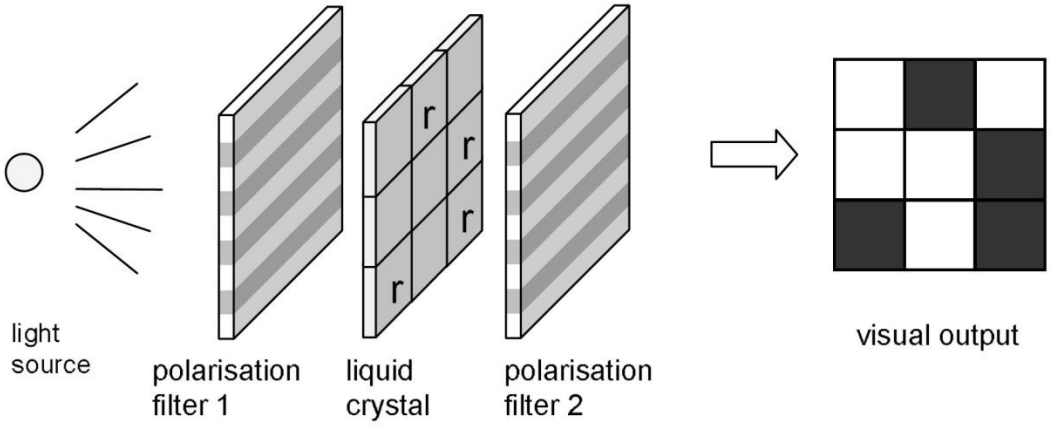
元進行疊加時，我們才得到白色圖元。因為疊加結果是透明的當且僅當兩個圖元都是白色的(即透明的)。因此，此種模型實現的運算可以在數學上抽象為定義在布林集合{0,1}上的 *OR* 運算。

4.2 基於 *XOR* 運算的偏振模型

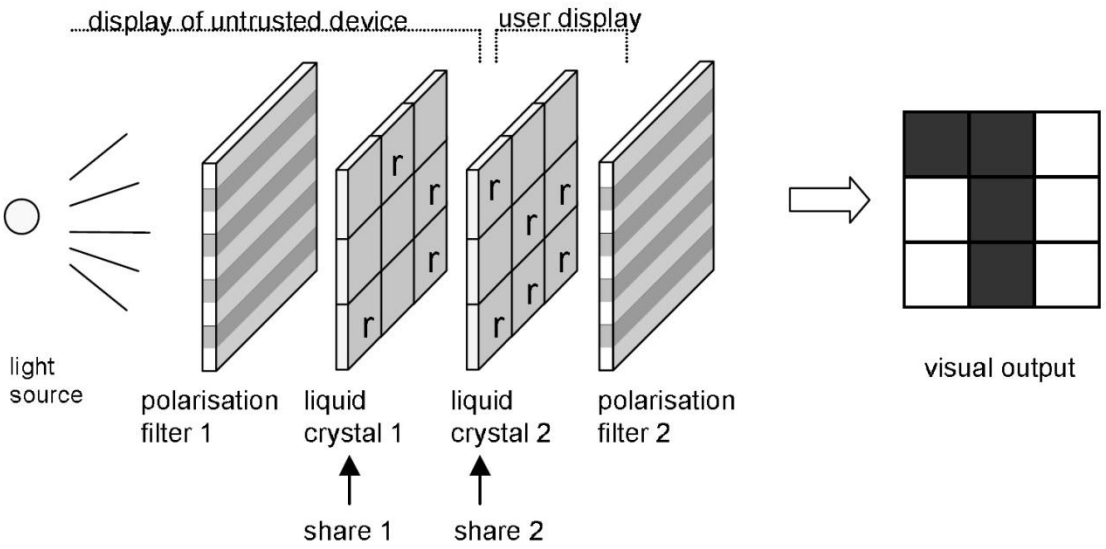
另外一種基於 *XOR* 運算的視覺密碼方案最早是由 Biham 等人於 1998 年在美密會的 RUMP session 上提出來的[5]。相對於基於 *OR* 運算的視覺密碼模型，這類模型需要更加複雜的硬體裝置來實現，比如偏振片，液晶層等。

比較典型的是 Tuyls 等人於 2002 年提出的基於光偏振的視覺密碼模型[29](如圖三所示)， 其方法就是在液晶顯示器（如圖二所示）中插入一個液晶層。這樣一來，新的液晶顯示器就包含如下五層：背景光源，偏振層 1，液晶層 1，液晶層 2，以及偏振層 2。偏振層只允許一個方向的電磁波通過，偏振層 1 和偏振層 2 的偏振方向是相同的。假設偏振光通過兩個液晶層之後分別偏轉的角度為α_1和α_2，並記偏振光通過偏振層 2 後的強度為I_r。我們有如下的強度函數：$I_r = \cos^2(\alpha_1 + \alpha_2)$, 當$\alpha_1, \alpha_2 \in \{0, \frac{\pi}{2}\}$時，由於$\cos(\pi) = cos(0) = 1$，且$\cos(\frac{\pi}{2}) = 0$, 該模型實現的運算可以在數學上抽象為定義在布林集合{0,1}上的 *XOR* 運算。由於兩個液晶層之間互相存在著電磁干擾，基於該原理所實現的顯示器還具有防止電磁洩漏的特點。基於該模型的研究還包括[32][12]。

由於 *OR* 運算具有單調遞增的特性，黑色圖元在透明膠片疊加的過程中不能被消除，因此所恢復出來的圖片就會有很多的黑圖元，從而降低了所恢復圖片的視覺效果。而 *XOR* 運算可以看做 *GF(2)*上的運算，從而避免了 *OR* 運算的上述缺點。基於 *XOR* 運算的視覺密碼方案通常比基於 *OR* 運算的視覺密碼方案 具有更高的對比度和更小的圖元擴張，例如對於*(n,n)*-VCS，基於 *OR* 運算的視覺密碼方案的最優對比度和最優圖元擴張分別是2^{n-1}和$\frac{1}{2^{n-1}}$，而基於 *XOR* 運算的視覺密碼方案的最優對比度和最優圖元擴張分別是 1 和 1，即完全恢復。



圖二：液晶顯示器模型：液晶元上的 *r* 表示，該液晶元旋轉所通過的偏振光的偏振方向
（圖片來源[29]）



圖三：基於 *XOR* 運算的視覺密碼模型：液晶元上的 *r* 表示，該液晶元旋轉所通過的偏振光的偏振方向（圖片來源[29]）

目前市場上的影印機通常具有反轉功能，即將圖片上的黑圖元變成白圖元，而將圖片上的白圖元變成黑圖元。實際上，該反轉功能實現了布林集合{0,1}上的"非"(*NOT*)運算。Viet et al.于 2004 年借助於影印機實現了可反轉視覺密碼方案（Reversing VCS）[31]，後續的研究工作包括文獻[13][33]。

從數學角度來講，*OR* 運算，*XOR* 運算和 *NOT* 運算滿足如下關係：$a \oplus b = (\neg a \wedge b) \vee (a \wedge \neg b) = \neg(a \vee \neg b) \vee \neg(\neg a \vee b)$其中，$\oplus$，$\wedge$，$\vee$和$\neg$分別表示 *XOR*，*AND*，*OR* 和 *NOT* 運算。從這個角度來看，可反轉視覺密碼方案與基於 *XOR* 運算的視覺密碼方案是可以互相類比的，即我們實現了其中一種方案，那麼另一種對應方案就可以從上式推得。

伍、視覺密碼的研究內容

視覺密碼學經過近二十年的發展，在多個研究分支取得了豐碩的成果，其也吸引了越來越多的關注。我們將其中比較重要的分支總結如下：

5.1 優化參數的視覺密碼方案

該分支包擴構造新的視覺密碼方案，使得其在對比度，圖元擴張和隨機性方面具有優勢。另外一個就是研究上面三個參數的最優值，以及在某個參數達到最優的條件之下，另外一個參數的最優值。因為對比度直接關係到所恢復圖片的視覺品質，而圖元擴張則

直接關係到分享圖片的尺寸，因此這兩個參數的研究比較多。隨機性雖然沒有直接限制方案的應用，但是其做為視覺密碼方案的一個基本屬性，從理論角度來講，也是很重要的一個研究課題。

理論上，對比度α必須滿足$0 < \alpha \leq 1$，圖元擴張 *m* 必須滿足$1 > m$且$m \in Z$。最理想的情況是$\alpha = 1$且 *m=1*，也就是說所恢復的秘密圖片和原秘密圖片完全一樣。但是，通常這是不可能達到的，例如對於*(n,n)*-VCS，最優的對比度和最優的圖元擴張可以同時達到，分別為$\frac{1}{2^{n-1}}$和2^{n-1}。此時的基矩陣可以表述如下：白基矩陣 M_0 包含所有漢明重量為偶數的 *n* 元列向量；黑基矩陣 M_1 包含所有漢明重量為奇數的 *n* 元列向量，參見[26]。但是對於*(2,n)*-VCS，最優的對比度和最優的圖元擴張是不能同時達到的，其最優的對比度為$\alpha = \frac{\lfloor \frac{n}{2} \rfloor \lceil \frac{n}{2} \rceil}{n(n-1)}$。當 *n* 為偶數時，在對比度達到最優的條件之下，*(2,n)*-VCS 的最小圖元擴張是 *2n-2*，參見[7]。

但是，對於*(2,n)*-VCS，我們有如下的構造方法：

$$M_0 = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}, M_1 = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

由上可知，在沒有限制條件之下，*(2,n)*-VCS 的最小圖元擴張一定不大於 *n*。因此，我們說對於*(2,n)*-VCS，最優的對比度和最優的圖元擴張是兩個相互矛盾的條件，它們不能同時達到。因此本文中優化參數的視覺密碼方案是指，構造出新的視覺密碼方案，使之具有盡可能大的對比度和盡可能小的圖元擴張，或者在這兩個相互矛盾的目標之間，得到一個較好的權衡。另外，研究在某些特殊存取結構之下的對比度的上界與圖元擴張的下界也是很重要的方向。由於對於通用存取結構，最優對比度和最優圖元擴張數值的確定，及其兩者之間關係的研究都非常複雜，因此目前優化參數的視覺密碼方案的構造主要是針對幾個特殊存取結構的，例如：*k=2,3,4,n-1,n* 時的*(k,n)*-VCS。

5.2 擴展的視覺密碼方案

Naor 和 Shamir 在最初的文獻[26]中就提出了一個*(2,2)*門限存取結構的有意義分享圖片的視覺密碼方案，在該文中他們又稱之為擴展的視覺密碼方案（Extended visual cryptography scheme，EVCS），這個名稱被後來的研究人員所廣泛接受[1][34]，並沿用至今。在 VCS 當中，分享圖片看起來像雜訊圖片（Noise-like），因此不同持有者（Holder）的分享圖片不容易區分，且容易混淆，也不方便分發者（Dealer）的管理；另外，雜訊圖片容易引起他人的懷疑，在通過海關時，容易被嚴格審查。與之相對，在 EVCS 當中，分享圖片是有意義的，使得不同持有者可以很容易識別出自己的分享圖片，便於分發者

進行管理；另外，有意義的分享圖片類似于普通的圖片，因而不容易引起他人的懷疑，也更加容易躲過海關人員的檢查。

一個有 *n* 個參與者的 EVCS 把 *n+1* 張輸入圖片$s_0, s_1, s_2, \ldots, s_n$加密成 *n* 張分享圖片$h_1, h_2, \ldots, h_n$，使得分享圖片 h_i 呈現出輸入圖片 s_i 的內容，其中輸入圖片s_0是需要分享的秘密圖片，而輸入圖片$s_1, s_2, \ldots, s_n$又被稱為掩蓋圖片（Cover images）。下面我們給出一個*(2,2)*-EVCS 來說明上述過程。假設秘密圖像上要加密的圖元為$w \in \{0,1\}$(其中，0 表示白圖元，1 表示黑圖元)，而掩蓋圖片 1 和 2 上的對應圖元分別為$u, v \in \{0,1\}$。為了分享該秘密圖元，我們選擇M_{uv}^{w}作為分享矩陣，然後隨機地置換它的列向量，最後把第$i \in \{1,2\}$行分配給參與者 *i*。如果 *u=0*，那麼第一行的漢明重量為 2；如果 *u=1*，那麼第一行的漢明重量為 3，因此我們可以從分享圖片 1 中看到掩蓋圖片 1 的內容。如果 *v=0*，那麼第二行的漢明重量為 2；如果 *v=1*，那麼第二行的漢明重量為 3，因此我們可以從分享圖片 2 中看到掩蓋圖片 2 的內容。如果 *w=0*，那麼兩行疊加的漢明重量為 3；如果 *w=1*，那麼兩行疊加的漢明重量為 4，因此我們可以從分享圖片 1 和 2 的疊加結果中看到秘密圖片的內容。

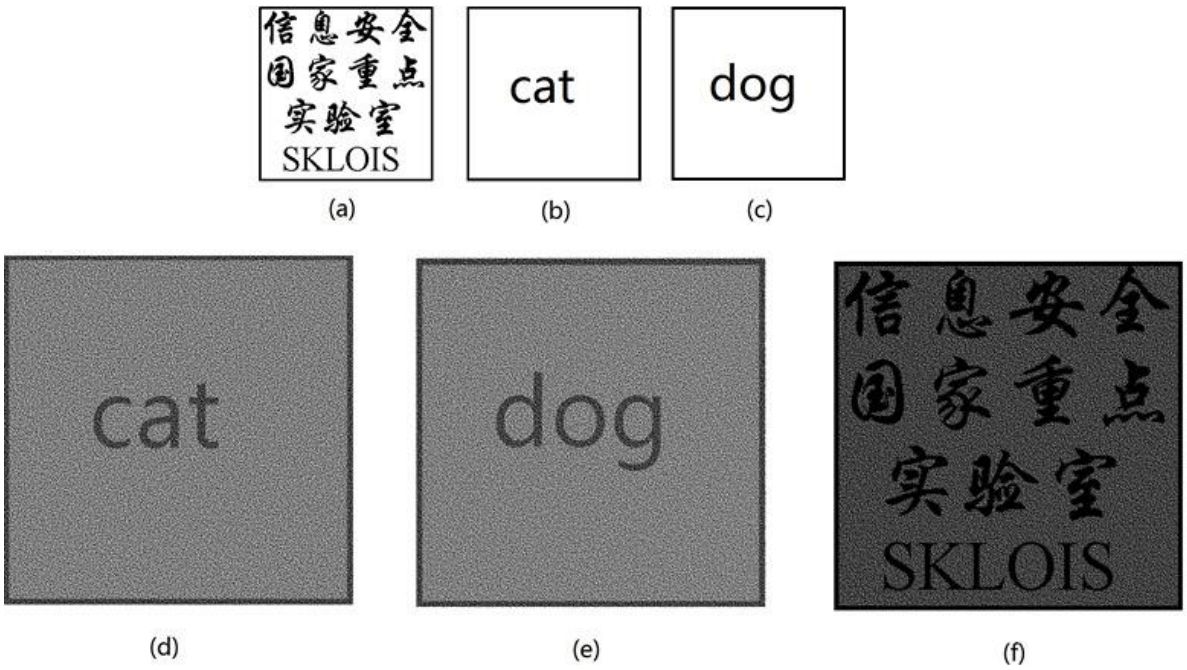
$$M_{00}^{0} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, M_{10}^{0} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

$$M_{01}^{0} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}, M_{11}^{0} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

$$M_{00}^{1} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, M_{10}^{1} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$M_{01}^{1} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, M_{11}^{1} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

詳細的實驗結果見圖四。



圖四：(2,2)-EVCS 的實驗結果：(a)原始秘密圖片300×300；(b)掩蓋圖片 1，大小300×300；(c)掩蓋圖片 2，大小300×300；(d)分享圖片 1，大小600×600；(e)分享圖片 2，大小600×600；(f)分享圖片 1 和 2 的疊加結果，大小600×600

在圖四中，(d)呈現了(b)的內容；(e)呈現了(c)的內容；但是通過觀察(d)和(e)，我們不能得到關於原始秘密圖片(a)內容的任何資訊；通過觀察(f)，我們可以看到圖片(a)的內容。

5.3 分享圖片大小不變的視覺密碼方案

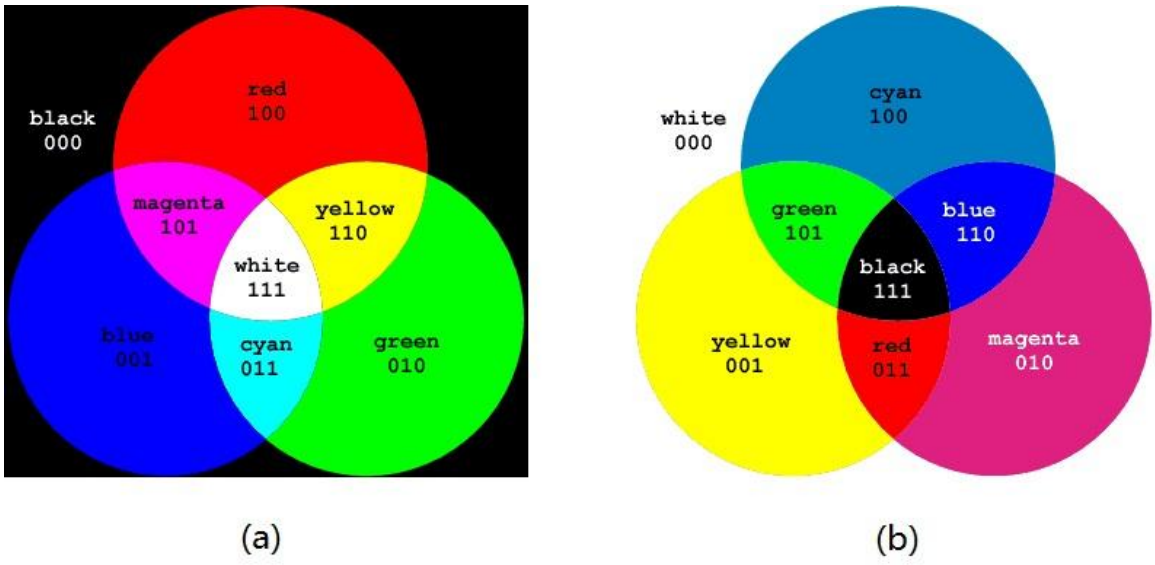
VCS，有時為了明確起見，又稱為確定型視覺密碼方案（Deterministic VCS，簡記為 DVCS），它的圖元擴張以指數增長。這為 VCS 的應用埋下了障礙。為了解決圖元擴張過於龐大的問題，Ito.et.al.於文獻[21]中提出了分享圖片大小不變的視覺密碼方案（Size-Invariant VCS，簡記為 SIVCS）。SIVCS 可以簡述如下，通過隨機地選取第二節中 S_0 和 S_1 中的一列來分別分享一個白圖元和一個黑圖元。類似的，我們可以得到有意義分享圖片且大小不變的視覺密碼方案。該類方法看起來非常簡單，但是卻成功地解決了確定型視覺密碼方案圖元擴張以指數增長的缺陷，為視覺密碼的應用開闢了一條新的路徑。從整體上來講，SIVCS 中所恢復出來的秘密圖片的視覺品質要比 DVCS 中所恢復出來的差，因此如何提高 SIVCS 所恢復圖片的視覺品質是一項重要的研究課題[25]。另外，由於 SIVCS 的構造是基於 VCS 的，因此最優 VCS 的構造仍然是一項基礎性的研究課題。

5.4 灰度及彩色視覺密碼方案

由於人眼不能夠分辨高頻的資訊，對於包含很多特別小的圖元點的區域，人眼自動將其做了一個平均，我們觀察到一個灰色的區域。這種利用黑圖元的疏密來表示一定灰度的技術被稱為半色調技術（Halftone technology）。灰度視覺密碼方案的通用技巧是：（1）將灰度圖片通過半色調技術轉換成二值圖片（Binary image）；（2）通過傳統的視覺密碼方案來分享該二值圖片。

由顏色理論，我們知道彩色可以分解為幾個不同的分量：加色模型下的紅綠藍（RGB）；減色模型下的青品紅黃（CMY）。電腦顯示器就是一個加色系統，分為紅（Red），綠（Green），藍（Blue）三個分量，每個分量又有從 0 到 255 的強度級別（Intensity level）。其中等強度的紅色光與綠色光混合可以得到黃（Yellow）色光；等強度的紅色光與藍色光混合可以得到品紅（Magenta）色光；等強度的藍色光與綠色光混合可以得到青（Cyan）色光；等強度的紅色光，綠色光與藍色光三者的混合可以得到白光。不同強度的白光可以構成不同階的灰度。當三個色光分量的強度不等時，我們就可以得到其他各種各樣的顏色[36][11]。該過程可見圖 5 中的（a）。

繪畫系統可以看做一個減色模型，白紙反射出來的白光作為背景光，青顏料會吸收其中的紅色分量，從而顯現出青色； 品紅顏料會吸收其中的綠色分量，從而顯現出品紅色；黃顏料會吸收其中的藍色分量，從而顯現出黃色。當等量青顏料與品紅顏料混合時，白光中的紅色與綠色分量會被吸收，從而顯現出藍色；當等量青顏料與黃顏料混合時，白光中的紅色與藍色分量會被吸收，從而顯現出綠色；當等量黃顏料與品紅顏料混合時，白光中的綠色與藍色分量會被吸收，從而顯現出紅色；當等量青顏料，黃顏料與品紅顏料混合時，白光中的紅色，綠色與藍色分量都會被吸收，從而顯現出黑色。不同量的黑色顏料可以構成不同階的灰度。當三個顏料的量不等時，我們就可以得到其他各種各樣的顏色[19]。該過程可見圖五中的（b）。



圖五：加色模型下三原色 RGB 與減色模型下三原色 CMY 的關係：(a) 將 CMY 由 RGB 來表示；(b) 將 RGB 由 CMY 來表示）

陸、結論

本文首先給出了視覺密碼的定義和評價指標，隨後介紹了視覺密碼的底層物理原理，最後給出了一些重要的研究方向。本文較為詳細地闡述了視覺密碼的基本原理和基礎知識，以使初學者能夠很快地對這個領域有個比較全面的認識，以便更快地步入研究工作。

[誌謝]

本研究受到資訊安全國家重點實驗室自主研究課題“安全顯示器的機理研究”的資助。

參考文獻

[1] P.D. Arco and R. De Prisco, "Secure Two-Party Computation: A Visual Way," ICITS 2013, LNCS 8317, pp. 18-38, 2014.

[2] G. Ateniese, C. Blundo, A. De Santis and D.R. Stinson, "Extended Capabilities for Visual Cryptography," Theoretical Computer Science, Vol. 250 Issue 1-2, pp. 143-161, 2001

[3] G. Ateniese, C. Blundo, A. De Santis and D.R. Stinson, "Visual Cryptography for General Access Structures," Information and Computation, Vol. 129, pp. 86-106,1996.

[4] R.A. Basavegowda and S.H. Seenappa, "Secret Code Authentication Using Enhanced Visual Cryptography," *Emerging Research in Electronics, Computer Science and Technology*, Vol. 248, pp. 69-76, 2014.

[5] E. Biham and A. Itzkovitz, "Visual Cryptography with Polarization," the Dagstuhl seminar on Cryptography, September 1997, and in the RUMP session of CRYPTO'97, 1997

[6] C. Blundo, A. De Bonis and A. De Santis, "Improved Schemes for Visual Cryptography," Designs, Codes and Cryptography,Vol.24, pp. 255-278,2001

[7] C. Blundo, A. De Santis and D.R. Stinson, "On the Contrast in Visual Cryptography Schemes," Journal of Cryptology, Vol. 12, No.4, pp. 261-289, 1999

[8] M. Bose and R. Mukerjee, "Optimal (k, n) visual cryptographic schemes for general k," Designs, Codes and Cryptography,Vol.55, pp. 19-35,2010

[9] M. Bose and R. Mukerjee, "Optimal (2, n) visual cryptographic schemes," Designs, Codes and Cryptography,Vol.40, pp. 255-267,2006.

[10] C.C. Chang and J.C. Chuang, "An Image Intellectual Property Protection Scheme for Gray-level Images Using Visual Secret Sharing Strategy," Pattern Recognition Letters, Vol. 23, pp. 931-941,2002.

[11] C.C. Chang, N.T. Huynh and H.D. Le, "Lossless and unlimited multi-image sharing based on Chinese remainder theorem and Lagrange interpolation," Signal Processing, Vol.99, pp. 159-170, 2014

[12] C.C. Chen and W.J. Wu, "A secure Boolean-based multi-secret image sharing scheme," The Journal of Systems and Software, http://dx.doi.org/10.1016/j.jss.2014.01.001

[13] S. Cimato, A. De Santis, A.L. Ferrara and B. Masucci, "Ideal Contrast Visual Cryptography Schemes With Reversing," Information Processing Letters, Vol. 93, pp. 199-206, 2005

[14] A. De Bonis and A. De Santis, "Randomness in secret sharing and visual cryptography schemes," Theoretical Computer Science, Vol. 314, pp. 351-374, 2004

[15] M. Dupuy and P. Paradinas, "Secret sharing and visual cryptography schemes," Sec '01:

Proceedings of the 16th international conference on Information security: Trusted information, pp. 123--137, 2001

[16] P.A. Eisen and D.R. Stinson, “Threshold Visual Cryptography Schemes with Specified Whiteness Levels of Reconstructed Pixels,” Designs, Codes and Cryptography,Vol.25, pp. 15-61,2002.

[17] T. Hofmeister, M. Krause and H.U. Simon, “Contrast-optimal k out of n Secret Sharing Schemes in Visual Cryptography,” COCOON '97, Berlin Springer LNCS, Vol. 1276, pp. 176-185, 1997

[18] T. Hofmeister, M. Krause and H.U. Simon, “Contrast-optimal k out of n Secret Sharing Schemes in Visual Cryptography,” Theoretical Computer Science, Vol. 240 Issue 2, pp. 471-485, 2000

[19] Y.C. Hou, “Visual cryptography for color images,” Pattern Recognition, Vol. 1773, pp. 1-11, 2003

[20] C.S. Hsu, S.F. Tu and Y.C. Hou, “An Optimization Model for Visual Cryptography Schemes with Unexpanded Shares,” The 16th International Symposium on Methodologies for Intelligent Systems, Vol. 4203, pp. 58-67, 2006

[21] R. Ito, H. Kuwakado and H. Tanaka, “Image Size Invariant Visual Cryptography,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, Vol. E82-A.No.10, pp. 2172-2177, 1999

[22] H. Koga, “A General Formula of the (t,n)-Threshold Visual Secret Sharing Scheme,” ASIACRYPT '2002, Springer-Verlag LNCS, Vol. 2501, pp. 328-345, 2002

[23] M. Krause and H.U. Simon, “Determining The Optimal Contrast For Secret Sharing Schemes In Visual Cryptography,” Combinatorics, Probability &Computing, Vol. 12, No.3, pp. 285-299, 2003

[24] F. Liu, C.K. Wu and X.J. Lin, “Step Construction of Visual Cryptography Schemes,” IEEE Transactions on Information Forensics & Security, Vol. 5, No. 1, pp. 27-38, 2010

[25] F. Liu, T. Guo, C.K. Wu and L.N. Qian, “Improving the visual quality of size invariant visual cryptography scheme,” Journal of Visual Communication and Image Representation, Vol.23, pp. 331-342, 2012

[26] M. Naor and A. Shamir, “Visual Cryptography,” EUROCRYPT '94, LNCS 950, pp. 1-12,1995.

[27] S.J. Shyu and M.C. Chen, “Optimum pixel expansions for threshold visual secret sharing schemes,” IEEE Transactions on Information Forensics and Security, Vol. 6, NO.3, pp. 960- 969, 2011

[28] P.B. Swadas, S. Pate and D. Darji, “A Comparatively Study on Visual Cryptography,” International Journal of Research in Engineering and Technology ، Vol.3, pp.

182-185,2014

[29] P. Tuyls, H.D.L. Hollmann, J.H.V. Lint and L. Tolhuizen, "XOR-based Visual Cryptography Schemes," Designs Codes and Cryptography, Vol. 37, pp. 169-186, 2005

[30] E. Verheul and H.V. Tilborg, "Constructions and Properties of k out of n Visual Secret Sharing Schemes," Designs Codes and Cryptography, Vol. 11, No.2, pp. 179-196, 1997

[31] D.Q. Viet and K. Kurosawa, "Almost Ideal Contrast Visual Cryptography with Reversing," Topics in Cryptology - CT-RSA, pp. 353-365, 2004

[32] D.S. Wang, L. Zhang, N. Ma and X.B. Li, "Two secret sharing schemes based on Boolean operations," Pattern Recognition, Vol. 40, pp. 2776-2785, 2007

[33] D.S. Wang, T. Song, L. Dong and C.N. Yang, "Optimal Contrast Grayscale Visual Cryptography Schemes With Reversing," IEEE Transactions on Information Forensics & Security, Vol. 8, No. 12, pp. 2059-2072, 2013

[34] D.S. Wang, F. Yi and X.B. Li, "On general construction for extended visual cryptography schemes," Pattern Recognition, Vol.42, pp. 3071-3082, 2009

[35] M.S. Wang and W.C. Chen, "A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography," Computer Standards & Interfaces, Vol. 31(4), pp. 757-762, 2009.

[36] C.N. Yang and T.S. Chen, "Colored visual cryptography scheme based on additive color mixing," Pattern Recognition, Vol.41, pp. 3114-3129, 2008