A new deterministic algorithm based cheating prevention scheme for Visual Cryptography

Du-Shiau Tsai, Chang-Chin Huang

Abstract

In 1995, Naor and Shamir proposed the *k*-out-of-*n* Visual Cryptography scheme such that only more than or equal to *k* participants can visually recover the secret through superimposing their transparencies. In 2006, Horng et al. indicated that cheating is possible when some participants create forged transparencies to deceive the remaining participants. In 2007, Tsai et al. proposed another cheating prevention scheme which was redesigned and extended by Generic Algorithms. This scheme was shown more secure in comparison with previous cheating prevention schemes in the literature. However, the major limitation of it is the case when the secret image consists of much more white pixels than black pixels, the secret shared by Generic Algorithms could be decoded incorrectly. In this paper, a new scheme is given to solve the cheating problem without extra burdens by adopting multiple distinct secret images and Generic Algorithms. Finally, experimental results and security analysis demonstrate the feasibility of the proposed scheme.

Keywords: Visual Cryptography, Cheating, Cheating Prevention Scheme.

Du-Shiau Tsai, Department of Information Networking Technology, HIT.
Chang-Chin Huang, Ph.D. Student, Department of Computer Science and engineering, National Chung Hsing University.
投稿日期：980804 接受刊登日期：980915

植基於決定型演算法的視覺密碼學欺騙攻擊防範機制

蔡篤校、黃暢卿

摘 要

於西元 1995 年，Naor 與 Shamir 兩位學者從有別於一般祕密分享方法的機制中提出(k, n)門檻值視覺密碼學(Visual Cryptography)，當有 k 位以上（含）的參與者一起重疊 k 張投影片時，直接藉由人類視覺解密重疊投影片時所產生的還原圖像，即可以完成解碼的動作。於西元 2006 年，洪教授等人提出於門檻值視覺密碼學可能出現欺騙攻擊，其方式爲部份參與者藉由僞造投影片使其它參與者遭受欺騙攻擊。蔡學者等人於西元 2007 年提出結合基因演算法的欺騙攻擊防範機制，這一個機制被證明能比其它防範機制提供更加安全的使用環境。但是這一個機制也存在一個限制，當要分享的秘密影像是由較多的白色像素和較少的黑色像素所構成時，使用基因演算法產生的投影片可能無法完成解碼的動作。因此這篇論文將提出一個新的機制除了能防範欺騙攻擊外，將較基因演算法欺騙攻擊防範機制，減少因使用多重秘密影像及基因演算法所產生的各項缺點。最後，實驗結果和安全性分析證明所提出機制的可行性。

關鍵詞：視覺密碼學、欺騙攻擊、欺騙攻擊防範機制。

蔡篤校：修平技術學院資訊網路技術學系專任助理教授
黃暢卿：國立中興大學資訊科學與工程學系研究生

1. INTRODUCTION

In 1995, Naor and Shamir proposed a variant of secret sharing called Visual Cryptography (VC) [12], where the shares given to participants are xeroxed onto transparencies. If X is an authorized subset, then the participants in X can visually recover the secret image by stacking their transparencies together without performing any computation. One of special properties distinguishes VC from secret sharing scheme [4,15] is that the security of VC is obtained by loosing contrast and resolution of secret images. Since the invention of VC, many researchers have devoted themselves to enhancing the contrast and resolution of the recovered images [3, 14] and to extending VC to general access structures [1]. Many non-binary secret image schemes were also proposed [2, 5, 8, 11, 13]. There are lots of applications based on VC such as visual authentication, steganography, and image encryption [6, 7, 10, 17].

In 2006, Horng et al. proposed that cheating is possible in the *k*-out-of-*n* VC [9]. Victims accept recovered images different from the actual secret image as authentic. The cheating activity could cause unpredictable damage to victims. Meanwhile, Horng et al. also proposed two cheating prevention schemes: the *Authentication Based Cheating Prevention scheme* (ABCP) and the *2-out-of-(n+l) VC*. Next year, the same authors proposed another cheating prevention scheme: *cheating prevention scheme with homogeneous secret images* (CPHS) by using homogenous secret images with Genetic Algorithms [16]. This scheme was proven more secure in comparison with previous two cheating prevention schemes. But, in CPHS, the secret shared by Generic Algorithms could be decoded incorrectly when the secret image consists of much more white pixels than black pixels. Because of the adoption of Genetic Algorithms, CPHS requires more computational power than traditional VC in encoding phase.

According to the above properties of VC and limitations of CPHS, the study recommends three guidelines to propose a new cheating prevention scheme:

1. When decoding, every recovered image should be visually recognized as the authentic secret.
2. To protect honest participants from cheating. This scheme should be a secure cheating prevention scheme.
3. This scheme requires lower computational power than CPHS does in encoding phase.

In this work, we assume that k is 2 since it is hard enough to correctly align the subpixels while k is larger than 2. That is, we will discuss 2-out-of-n scheme instead of the general problem of constructing k-out-of-n visual cryptography scheme. The rest of the paper is organized as follows. Section 2 gives a brief review of VC and Horng et al.'s cheating activity. Section 3 presents construction details for the proposed scheme. Section 4 demonstrates experimental results. Discussion and conclusions are given in Sections 5 and 6, respectively.

2. PRELIMINARIES

2.1 VISUAL CRYPTOGRAPHY

In 1995, Naor and Shamir proposed a variant of t-out-of-n secret sharing scheme where the shares given to participants are xeroxed onto transparencies. Therefore, a share is also called a transparency. If X is a qualified subset, then the participants in X can visually recover the secret image by stacking their transparencies without performing any cryptographic computation. Usually, the secret is an image. To create the transparencies, each black and white pixel of the secret image is handled separately. It appears as a collection of m black and white subpixels in each of the n transparencies. We will call these m subpixels a *block*. Therefore, a pixel of the secret image corresponds to nm subpixels. We can describe the nm subpixels by an $n \times m$ boolean matrix $S=[S_{ij}]$ such that $S_{ij}=1$ if and only if the j^{th} subpixel of the i^{th} share is black and $S_{ij}=0$ if and only if the j^{th} subpixel of the i^{th} share is white. The grey level of the stack of k shared blocks is determined by the Hamming weight $H(V)$ of the "or"ed m-vector V of the corresponding k rows in S. This grey level is interpreted by the visual system of the users as black if $H(V) \geq d$ and as white if $H(V) \leq d - \alpha * m$ for some fixed threshold d and relative difference α. We would like m to be as small as possible and α to be as large as possible.

More formally, a solution to the k-out-of-n VC consists of two collections C^0 and C^1 of $n \times m$ boolean matrices. To share a white pixel, the dealer randomly chooses one of the matrices from C^0, and to share a black pixel, the dealer randomly chooses one of the matrices from C^1. The chosen matrix determines the m subpixels in each one of the n transparencies.

Definition 1 A solution to the k-out-of-n VC consists of two collections C^0 and C^1 of $n \times m$ boolean matrices. The

solution is considered valid if the following conditions are met:

Contrast conditions:

1. For any matrix S^0 in C^0, the "or" V of any k of the n rows satisfies $H(V) \le d - \alpha * m$.
2. For any matrix S^1 in C^1, the "or" V of any k of the n rows satisfies $H(V) \ge d$.

Security condition:

3. For any subset $\{i_1, i_2, \ldots, i_q\}$ of $\{1,2,\ldots,n\}$ with $q < k$, the two collections D^0, D^1 of $q \times m$ matrices obtained by restricting each $n \times m$ matrix in C^0, C^1 to rows $i_1, i_2, \ldots, i_q$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Contrast conditions are related to the contrast of the decoded image. Security condition indicates that by inspecting fewer than k transparencies, even an infinitely powerful cryptanalyst cannot gain any advantage in deciding whether a shared pixel is white or black. The following serves as an example of how to implement a 2-out-of-n VC. It can be constructed by the following collections of $n \times n$ matrices:

C^0={all the matrices obtained by permuting the columns of

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ \vdots & & & & \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}\}$$

C^1= {all the matrices obtained by permuting the columns of

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}\}$$

The properties of each transparency are (1) in the decoding phase, every m, $m = n$, adjacency subpixels of the stacking result is united as a block for representing a pixel. (2) A block consisting of two black and n-2 transparent subpixels is for representing a black pixel; on the contrary, a block consisting of one black and n-1 transparent subpixels is for representing a white pixel. Therefore, the contrast is $\frac{1}{n}$.

2.2 THE HORNG ET AL.'S CHEATING ACTIVITY

In [9], Horng et al. proposed that cheating is possible in k-out-of-n VC. Take a 2-out-of-3 VC for example. A secret image is encoded into three distinct transparencies, denoted T_1, T_2

and T_3. Then, the three transparencies are respectively delivered to Alice, Bob, and Carol. Without loss of generality, Alice and Bob are assumed to be collusive cheaters and Carol is the victim. In the cheating activity, T_1 and T_2 are used to create fake transparency T_2' such that superimposing T_2' and T_3 will visually recover the cheating image. Precisely, by observing the following collections of 3×3 matrices which are used to generate transparencies, collusive cheaters can predict the actual structure of the victim's transparency for creating T_2'.

C^0={all the matrices obtained by permuting the columns of S^0= $\begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$}

C^1= {all the matrices obtained by permuting the columns of S^1= $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$}

By observing above matrices, two rows of C^0 or C^1 matrix are determined by collusive cheaters. Therefore, the structure of each block of T_3 is exact the remaining row. For presenting a white pixel of cheating image, the block of T_2' is set to be the same structure of T_3. For presenting a black pixel of cheating image, the block of T_2' is set to be the different structure of T_3. For example, if the block of T_3 is [010], then T_2' is set to be [010] for white pixel or it is set to be [001] for black pixel.

3. THE PROPOSED SCHEME

In this section, we first analyze the cheating activity. On the basis of the analysis results, a new deterministic algorithm based cheating prevention scheme (DACP) is proposed.

The following notations are defined for the rest of this paper.

- n : the number of shares;
- m : the number of subpixels in a block;
- SM (CM): secret message (cheating message);
- Sc (Sv): cheater's share(victim's share);
- $H(\mathrm{x})$, $\mathrm{x}\in\{S^1, S^0, v\}$: the number of black subpixels of any block in S^1,S^0 or of block v;
- c : the number of collusive cheaters;
- B_V (W_V): the number of black subpixels in a block to represent

black(white);

- $OR(\ )$: logical OR operation;
- $Block_i^m(\ )$: divide the input message into blocks and output the ith block;
- $Color_B(\ )(\ Color_W(\ ))$: Output "true" if the number of black subpixels in the input block is equal to $B_V(W_V)$, otherwise output "false";
- $R(\ )$: rearrange the positions of black and white subpixels in a block; and
- $\Psi(\ )$: output the number of black subpixels in the same position of two blocks.

3.1 *WTOB* AND *BTOW* ATTACK

By observing the proposed cheating activity [9], it can be represented by two cheating attacks: *WTOB* attack and *BTOW* attack. *WTOB* attack is an attack tries to change the color of blocks from authentic white to fake black while recovering the secret. On the contrary, *BTOW* attack is an attack tries to change the color of blocks from authentic black to fake white while recovering the secret. Both algorithms are illustrated as follows:

WTOB attack algorithm:

IF $Color_W(\ Block_i^m(SM)\ )$ ***AND***

$Color_B(\ Block_i^m(CM)\ )$

REPEAT

$$Sc' = R(\ Block_i^m(Sc)\ )$$

UNTIL $Color_B(\ Block_i^m(OR(Sc', Sv)\ )$

BTOW attack algorithm:

IF $Color_B(\ Block_i^m(SM)\ )$ ***AND***

$Color_W(\ Block_i^m(CM)\ )$

REPEAT

$$Sc' = R(\ Block_i^m(Sc)\ )$$

UNTIL $Color_W(\ Block_i^m(OR(Sc', Sv)\ )$

We propose new parameters $\psi^0(\psi^1)$ and two constraints to prevent *WTOB attack* and *BTOW attack*. By two constraints the actual structure of victim's shares in the proposed scheme is harder to be determined by collusive cheaters than that in VC.

Definition 2

$\psi^0(\psi^1)$: the number of 1's in the same position of any two blocks for any S^0 in C^0(S^1 in C^1)

Constraint 1

The value of parameter ψ^0 is set to be $0<\psi^0<H(S^0)$.

Constraint 2

The value of parameter m is set to be $m>H(S^1)\times n$.

For example, C^0 is generated by following matrix in a 2-out-of-2 VC:

C^0={all the matrices obtained by

permuting the columns of $S^0=\begin{bmatrix}1&1&0&0\\1&1&0&0\end{bmatrix}\}$

The probability that cheaters can correctly guess the structure of victim's block is 100%. By constraint 1, after setting the value of parameter ψ to be 1, the probability becomes 1/4 with the following modified matrix:

C^0={all the matrices obtained by permuting the columns of $S^0=\begin{bmatrix}1&1&0&0\\0&1&1&0\end{bmatrix}\}$

By observing the following matrix in a 2-out-of-2 VC:

C^1={all the matrices obtained by permuting the columns of $S^1=\begin{bmatrix}1&1&0&0\\0&0&1&1\end{bmatrix}\}$

In this example, $m=4$, $H(S^1)=2$, $n=2$. The probability that cheaters can correctly guess the structure of victim's block is still 100%. By constraint 2, the probability becomes 1/3 with the following modified matrix:

C^1={all the matrices obtained by permuting the columns of $S^1=\begin{bmatrix}1&1&0&0&0\\0&0&1&1&0\end{bmatrix}\}$

The proposed DACP prevents the victim from cheating even when the worst case happens. Any two of the participants can reveal the secret message and form a coalition to deceive the victim, i.e. the protection scheme should be robust under the coalition with two collusive cheaters (c=2). More than that we assume even the number of collusive cheaters is n-1, the proposed scheme still guarantee the victim's safety.

3.2 CONSTRUCTION OF DACP

3.2.1 CONSTRUCTION OF C^1

We adopt the ideal of 2-out-of-(n+l) *VC* that basically uses extra l shares to prevent the victim from being deceived. In 2-out-of-(n+l) *VC*, the dealer generates (n+l) shares and randomly chooses l shares that is kept secretly or is destroyed. The remaining n shares are distributed to the n participants. Therefore, this construction of C^1 satisfies constraint 2.

Definition 3

In DACP, C^1 is all the matrices obtained by permuting the columns of $S^1=\{\mathcal{T}^1\cup\mathcal{B}^1\}$.

For S^1, we define a base block $\mathcal{B}^1$ and set $\mathcal{T}^1$ that is inferred from set $\mathcal{R}^1$, and $\mathcal{U}^1$.

- $\mathcal{B}^1=[1^{H(S^1)}0^{m-H(S^1)}]_{1*m}$, $\mathcal{B}^1$ is composed of consecutive $H(S^1)$ 1's and consecutive (m- $H(S^1)$) 0's;
- $\mathcal{R}^1=\{[a_1\cdots a_m]_{1*m}$:

$a_i \in \{0,1\}, \forall i = 1,2,\cdots,m$, the number of 1's is $H(S^1)$ };

- $\mathcal{U}^1$={A:A$\in \mathcal{R}^1$ and Ψ(A,$\mathcal{B}$) =*0*};
- $\mathcal{T}^1$={A:A$\in \mathcal{U}^1$,$\forall$B$\in \mathcal{U}^1$ and A≠B such that Ψ(A, B) =*0*}.

When $|\mathcal{T}^1|$ is greater than or equal to *n*, $\mathcal{T}^1$ is used to construct S^1. S^1={$\mathcal{T}^1 \cup \mathcal{B}^1$}.

The construction of C^1 satisfies constraint 2 by adding an undistributed block. The security analysis of this construction of C^1 will be demonstrated in section 5.

3.2.2 CONSTRUCTION OF C^0

When it comes to construct the structure of C^0, the worst case will be the (*n-1*) participants form a coalition to deceive victim. Therefore, even the worst case does happen, the collusive cheaters still can't exactly locate the positions of black and white subpixels in the victim's block.

Definition 4

In DACP, C^0 is all the matrices obtained by permuting the columns of S^0={$\mathcal{T}^0 \cup \mathcal{B}^0$}.

For S^0, we define a base block $\mathcal{B}^0$ and set $\mathcal{T}^0$ that is inferred from set $\mathcal{R}^0$, and $\mathcal{U}^0$.

- $\mathcal{B}^0$=$[1^{H(S^0)}0^{m-H(S^0)}]_{1*m}$, $\mathcal{B}^0$ is composed of consecutive $H(S^0)$ 1's and consecutive (*m*- $H(S^0)$) 0's;
- $\mathcal{R}^0$={$[a_1 \cdots a_m]_{1*m}$: $a_i \in \{0,1\}, \forall i = 1,2,\cdots,m$, the number of 1's is $H(S^0)$ };
- $\mathcal{U}^0$={A:A$\in \mathcal{R}^0$ and Ψ(A,$\mathcal{B}$) =ψ};
- $\mathcal{T}^0$={A:A$\in \mathcal{U}^0$,$\forall$B$\in \mathcal{U}^0$ and A≠B such that Ψ(A, B) =ψ}.

When $|\mathcal{T}^0|$ is greater than or equal to *n*, $\mathcal{T}$ is used to construct S^0. S^0={$\mathcal{T}^0 \cup \mathcal{B}^0$}.

The value of ψ determines the contrast of the revealed secret message. The contrast of the secret message is $\frac{B_V - W_V}{m}$. Since $W_V = B_V$-ψ, the contrast of the secret message is $\frac{\psi}{m}$ in the proposed DACP. The higher value ψ is the better contrast of the revealed secret message will be.

In the following part, we demonstrate a simple construction of C^0. For better contrast of the revealed secret message, we here maximize the value of ψ=$H(S^0)$-1. And the structure of $\mathcal{U}$ and $\mathcal{T}$ are defined as followings:

- $\mathcal{U}$={$[a_1 \cdots a_{H(S^0)} a_{H(S^0)+1} \cdots a_m]$: $[a_1 \cdots a_{H(S^0)} a_{H(S^0)+1} \cdots a_m] \in \mathcal{R}$ and the number of 1's in the substring of $a_1 \cdots a_{H(S^0)}$ is ψ}.

Then divide $\mathcal{U}$ into several subsets that satisfy the property of $\mathcal{T}$.

- $\mathcal{T}_i$={$[a_1 \cdots a_{H(S^0)} a_{H(S^0)+1} \cdots a_m]$: $[a_1 \cdots a_{H(S^0)} a_{H(S^0)+1} \cdots a_m] \in \mathcal{U}$ and $a_{H(S^0)+i}$=1} where i=1,2,$\cdots, m - H(S^0)$

Hence $|\mathcal{T}_i| = \dfrac{|\mathcal{U}|}{m - H(S^0)}$

Therefore, the structure of S^0={$\mathcal{T}_i \cup \mathcal{B}$} is done in the proposed scheme.

Take 2-out-of-3 DACP for instance, where $H(S^0)$ =3, m=12, W_V=4, ψ=2, $\mathcal{B}$=[111000000000]

$\mathcal{U}$=

$$\begin{bmatrix} 1&1&0&1&0&0&0&0&0&0&0&0 \\ 1&1&0&0&1&0&0&0&0&0&0&0 \\ & & & & & &\vdots & & & & & \\ 1&1&0&0&0&0&0&0&0&0&0&1 \\ 1&0&1&1&0&0&0&0&0&0&0&0 \\ 1&0&1&0&1&0&0&0&0&0&0&0 \\ & & & & & &\vdots & & & & & \\ 1&0&1&0&0&0&0&0&0&0&0&1 \\ 0&1&1&1&0&0&0&0&0&0&0&0 \\ 0&1&1&0&1&0&0&0&0&0&0&0 \\ & & & & & &\vdots & & & & & \\ 0&1&1&0&0&0&0&0&0&0&0&1 \end{bmatrix}$$

$\mathcal{T}_1$=

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

,

$\mathcal{T}_2$=

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

,…,

$\mathcal{T}_9$=

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

C^0=all the matrices obtained by permuting the columns of S^0={$\mathcal{T}_i \cup \mathcal{B}$}, where $i = 1, 2, \cdots, 9$

4. EXPERIMENTAL RESULTS

Experiments were conducted to prove that the proposed scheme is robust against cheating attacks. Although examples about *k*-out-of-*n* VC are abundant, for simplicity we will take a 2-out-of-3 example to demonstrate the prevention ability of the proposed scheme. These experiments are conducted with following two matrices and parameters, where m=12, $H(S^0)$=3, $H(S^1)$=3, W_V=4, B_V=6, ψ=2.

C^0=all the matrices obtained by permuting the columns of

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

C^1= all the matrices obtained by permuting the columns of

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

The secret message and cheating message are shown in Figure 1 (a) and Figure 1(h), respectively. Shares S_A, S_B, and S_C are shown in Figure 1 (b)-(d). The results of superimposing any two shares of S_A, S_B, and S_C are shown in Figure 1 (e)-(g). The simulated cheating attack is given as follows: Assume that two participants, holding shares S_A,and S_B, respectively, are the collusive cheaters. The honest participant with share S_C is assumed to be the victim. The collusive cheaters create a forging share S_A' in order to deceive the victim. Figure 1 (i) illustrate fake shares S_A'. Fortunately, after superimposing S_A' and S_C, shown in Figure 1 (j), the revealed image is not smooth. That is, it is not perceptible and the simulated cheating attack is not a successful one.

5. DISCUSSION

In this section, the security of the proposed scheme is analyzed.

Lemma 1 *Let T be the transparency of a victim and let B be a block of T that corresponds to a white pixel of the secret image. Then the probability that cheaters can correctly determine the structure of B is* $\frac{1}{\left|\mathcal{T}^0\right|+1-c}$.

Proof: In the scheme, *B* can be any row of $S^0=\{\mathcal{T}^0 \cup \mathcal{B}^0\}$ matrix. The cheaters can determine *c* rows if there are *c* collusive cheaters. Any one of the $\left|\mathcal{T}^0\right|+1-c$ remaining rows is equally likely to be *B* because the dealer distributes transparencies to participants randomly and uniformly. Therefore, the probability that cheaters can correctly determine the structure of *B* is $\frac{1}{\left|\mathcal{T}^0\right|+1-c}$. □

Lemma 2 *Let T be the transparency of a victim and let B be a block of T that corresponds to a black pixel of the secret image. Then the probability that cheaters can correctly determine the structure of B is* $1 \Big/ C^{(m-H(S^1)*c)}_{H(S^1)}$.

Proof:

By definition 3, the victim's block might be one of the $C^m_{H(S^1)}$ blocks, but collusive cheaters could reduce many impossible blocks based on the

information of their corresponding blocks and the structure of C^1. Collusive cheaters could infer that the victim's block is one of $C_{H(S^1)}^{(m-H(S^1)*c)}$ blocks. Therefore the probability that cheaters can correctly determine the structure of B is $1/C_{H(S^1)}^{(m-H(S^1)*c)}$. □

Theorem 1 The proposed scheme is a 2-out-of-n cheating prevention scheme.

Proof: Assume that cheaters need to change r white pixels and r' black pixels of the unknown secret image to create the cheating message. Then, by Lemma 1 and Lemma 2, the probability that the cheaters can correctly guess the structure of the corresponding blocks of T is $\left(\frac{1}{|\mathcal{T}|+1-c}\right)^r * \left(\frac{1}{C_{H(S^1)}^{(m-H(S^1)*c)}}\right)^{r'}$. Since secret image consists of a lot of black and white pixels, the value of r and r' are both large. Therefore, even with n-1 collusive cheaters, the probability to determine the structure of T in order to create a fake authentic image is negligible. □

6. CONCLUSIONS

In this paper, a new cheating protection for visual cryptography has been proposed without extra burdens by adopting multiple distinct secret images and Generic Algorithms. By using deterministic algorithm for generating shares, this scheme requires lower computational power than CPHS. It is guaranteed that the secret can be visually recovered. The experimental results and security analysis show that the proposed scheme does prevent victims from cheating activity.

REFERENCES

[1] Ateniese, G., Blundo, C., De Santis, A., and Stinson, D. R.(1996) Visual Cryptography for General Access Structures. *Information and Computation,* pp. 86-106.

[2] Blundo, C., De Santis, A., and Naor, M. (2000). Visual cryptography for grey level images. *Information Processing Letters*, Vol. 75, No.6, pp. 255-259.

[3] Blundo, C., D'Arco, P., De Santis, A., Stinson, D. R.(2003) Contrast optimal Threshold Visual Cryptography Schemes. *SIAM J. Discrete Math*. 16(2) pp.224-261.

[4] Blakley, G. (1979) Safeguarding cryptographic keys. *Proc. AFIPS 1979 Natl. Conf.*, New York , Vol.

48 pp. 313-317.

[5] Chang, C.C., and Chuang, J.C. (2002) An image intellectual property protection scheme for gray-level image using visual secret sharing strategy. *Pattern Recognition Letters*, Vol. 23, pp. 931-941.

[6] Chen,T.H. and Tsai, D.S. (2006) Owner-Customer Right Protection Mechanism using a Watermarking Scheme and a Watermarking Protocol. *Pattern Recognition*, Vol. 39, Issue 8, pp. 1530-1541.

[7] Chen,T.H., Hung,T.H., Horng, G., and Chang, C.M.(2008)Multiple Watermarking Based on Visual Secret Sharing. *International Journal of Innovative Computing Information and Control*, Vol. 4, No. 11, pp. 3005-3026.

[8] Hou, Y.C. (2003) Visual cryptography for color images. *Pattern Recognition*, Vol. 36 pp. 1619 – 1629.

[9] Horng, G., Chen T.H., and Tsai, D.S. (2006) Cheating in Visual Cryptography. *Designs, Codes and Cryptography*, Vol. 38, No. 2 pps.219-236.

[10] Lukac, R., and Plataniotis, K.N. (2005) Bit-level based secret sharing for image encryption. *Pattern Recognition* Vol. 38(5) pp. 767-772.

[11] Lin, C.C., and Tsai, W.H. (2003) Visual cryptography for gray-level images by dithering techniques. *Pattern Recognition Letters*. Vol. 24 (1-3) pp. 349-358.

[12] Naor M., and Shamir, A. (1995) Visual Cryptography. *In Proceedings of Advances in Cryptography- EUROCRYOT'94*, 1-12.

[13] Rijmen,V., and Preneel, B. (1996) Efficient colour visual encryption or shared colors of Benetton. *Eurocrypto'96, Rump Session, Berlin*.

[14] Shamir, A., and Naor, M. (1997). Visual Cryptography II: Improving the Contrast via the Cover Base, *Security Protocols*, LNCS 1189, pp.197–202.

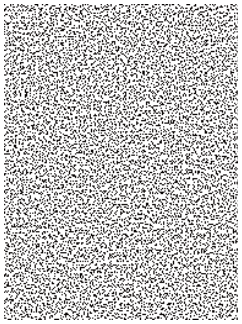
[15] Shamir, A. (1979).How to share a secret. *Comm. ACM*, Vol. 22, pp. 612-613.

[16] Tsai, D.S., Chen T.H., and Horng, G. (2007) A Cheating Prevention Scheme for Binary Visual Cryptography with Homogeneous Secret Images. *Pattern Recognition*. Vol. 40, Issue 8, pp.

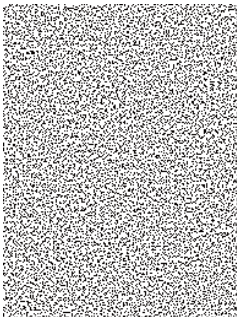
2356-2366.

[17] Wang, C.C., Tai, S.C., and Yu, C.S. (2000) Repeating image watermarking technique by the visual cryptography. *IEICE Transactions on Fundamentals*, Vol. E83-A pp. 1589-1598.

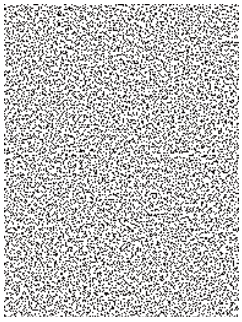
(a)Secret message *SM* (64*64)



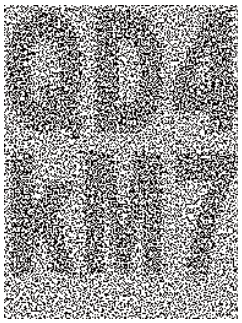
(b)Share S_A 192*256 50%



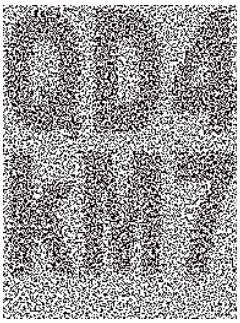
(c)Share S_B 192*256 50%



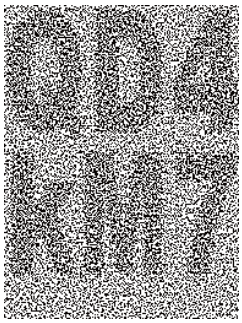
(d)Share S_C 192*256 50%



(e)Secret message by superimposing share S_A and share S_B 192*256 50%

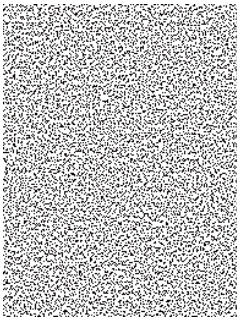


(f)Secret message by superimposing share S_C and share S_B 192*256 50%

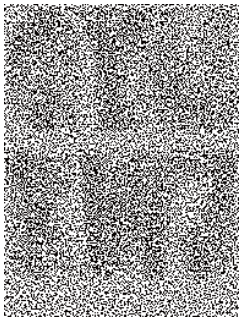


(g)Secret message by superimposing share S_C and share S_A 192*256 50%

(h)Cheating message *CM* (64*64)



(i)Share S_A' 192*256 50%



(j) Secret message by superimposing S_A' and S_C 192*256 50%

Figure 1: An example of a DACP