Designs, Codes and Cryptography, 38, 219–236, 2006

Cheating in Visual Cryptography

GWOBOA HORNG gbhorng@cs.nchu.edu.tw
Department of Computer Science, National Chung Hsing University, 250 Kuo-Kuang Road, Taichung 40227, Taiwan, R. O. C.

TZUNGHER CHEN
Department of Computer Science, National Chung Hsing University, 250 Kuo-Kuang Road, Taichung 40227, Taiwan, R. O. C.

DU-SHIAU TSAI
Department of Information Management, Hsiuping Institute of Technology, 11, Gongye Rd., Dali City, Taichung County 412, Taiwan R. O. C.

Communicated by: P. Wild

Received June 30, 2003; Revised November 18, 2004; Accepted February 16, 2005

Abstract. A secret sharing scheme allows a secret to be shared among a set of participants, P, such that only authorized subsets of P can recover the secret, but any unauthorized subset cannot recover the secret. In 1995, Naor and Shamir proposed a variant of secret sharing, called visual cryptography, where the shares given to participants are xeroxed onto transparencies. If X is an authorized subset of P, then the participants in X can visually recover the secret image by stacking their transparencies together without performing any computation. In this paper, we address the issue of cheating by dishonest participants, called cheaters, in visual cryptography. The experimental results demonstrate that cheating is possible when the cheaters form a coalition in order to deceive honest participants. We also propose two simple cheating prevention visual cryptographic schemes.

Keywords: visual cryptography, cheating, secret sharing, visual authentication

AMS Classification: 94A62

1. Introduction

A secret sharing scheme is a method to protect a secret K, by distributing partial information, called *shares*, to a set of participants, $P = \{P_1, P_2, \ldots, P_n\}$, in a way that only authorized subsets of P can recover K, but any unauthorized subset cannot recover K. Such schemes are useful for protecting important secret data, such as cryptographic keys [1], from being lost or destroyed without accidental or malicious exposure. They are also useful in constructing shared control schemes [12] and fault tolerance

schemes [10]. Secret sharing schemes have been extensively investigated since their invention in 1979 [1,11]. A detailed bibliography can be found in [6].

In 1995, Naor and Shamir proposed a variant of secret sharing scheme, called visual cryptography (VC), where the shares given to participants are xeroxed onto transparencies [8]. If X is an authorized subset of participants, then the participants in X can visually recover the secret image by stacking their transparencies together without performing any cryptographic computation.

There are many practical applications based on VC. For example, assume there are two partners who keep jewels in a safe at a bank. A secret password is used for unlocking the safe. In order to ensure none of them can independently take out the jewels, a 2-out-of-2 VC can be adopted to create two transparencies. Then the bank delivers a transparency to each partner. In this case the partners need to stack their transparencies together to reveal the password and open the safe. There are other applications based on VC such as visual authentication and identification [7], and steganography [4,14].

In a secret sharing scheme, suppose the participants $P_{i1}, \ldots, P_{it}$ of an authorized subset want to determine the secret K. Then they can put their shares together and recover K. During the reconstruction of the secret, one participant, called *cheater*, may release a false share. In this case, only the cheater has the opportunity to decode the right secret, while the other participants will obtain the wrong secret. For example, Tompa and Woll [13] showed that Shamir's scheme [11] is insecure against cheating. It is very important to be able to detect cheating in secret sharing schemes. Otherwise, cheating activities could cause unpredictable damage to victims. Tompa and Woll improved Shamir's scheme to reduce the probability of a successful cheating. Brickell and Stinton [2] proposed a cheating detection scheme such that honest participants can detect cheating with high probability. There are other schemes, for examples [3, 5], which provide the function that cheaters can be identified.

Cheating in secret sharing schemes has been widely investigated for decades. In this paper, we show that cheating is also possible in VC. We also propose two simple methods to prevent cheating. The rest of this paper is organized as follows. In Section 2, we briefly describe the concepts of secret sharing and VC. Section 3 shows that cheating is possible in visual cryptography. Two simple methods to guard against cheating are proposed in Section 4. Finally, conclusions are given in Section 5.

2. Secret Sharing and Visual Cryptography

In a secret sharing scheme, there is a secret K to be shared among a set of participants. The secret is known to a special person called *dealer*. The

dealer generates and distributes partial information called *shares* to the participants. The family of authorized subsets of participants is called the *access structure*, $\mathcal{A}$, of the scheme. That is, $\mathcal{A} = \{Q : Q \subseteq P \text{ and } Q \text{ can recover the secret } K\}$. Shamir [11] and Blakley [1] proposed methods to construct secret sharing schemes realizing the threshold access structures $\mathcal{A} = \{Q : Q \subseteq P \text{ and } |Q| \geq t\}$ for some constant t such that $1 < t \leq n$ where $n = |P|$. Such schemes are also called t-out-of-n *threshold schemes*. That is, a t-out-of-n threshold scheme is to break a secret K into a number of shares and distribute them to the n participants in such a way that: any t or more participants can recover the secret K from their shares; and fewer than t participants cannot recover the secret K from their shares. The t-out-of-n threshold scheme proposed by Shamir is based on Lagrange interpolating polynomial. It goes as follows: The dealer randomly generates a secret polynomial $f(X) = \sum_{i=0}^{t-1} a_i x^i$ of degree at most $t-1$ with $f(0) = a_0 = K$. All arithmetic is done in $GF(p)$, where p is a large prime number. The values $f(i)$, for i=1 to n, are the shares to be distributed to the participants P_i respectively.

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 [8]. 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. 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 shares. We will call these m subpixels a *block*. Therefore, a pixel of the secret image corresponds to nm subpixels (n blocks). 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 jth subpixel of the ith share is black and $S_{ij} = 0$ if and only if the jth subpixel of the ith 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 participants as black if $H(V) \geq d$ and s 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 defines the color of the m subpixels in each one of the n transparencies. The solution is considered valid if the following three conditions are met:

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

The first two conditions are related to the contrast of the decoded image. The third condition is related to security since it implies that by inspecting fewer than k shares, even an infinitely powerful cryptanalyst cannot gain any advantage in deciding whether the shared pixel is white or black. The readers are referred to [8] for details.

3. Cheating in Visual Cryptography

3.1. Definitions and Assumptions

Definition 1. In VC, a participant is called a cheater if, during secret reconstruction, he releases a transparency, called fake share, different from the one he received from the dealer.

Definition 2. In VC, a reconstructed secret image is authentic if it is smooth in a sense that its boundary of black and white regions is clearly perceptible.

Definition 3. In VC, cheating is said to be successful if any honest participant, called victim, accepts a reconstructed secret image different from the actual secret image as authentic.

To be able to detect cheating we need the following assumptions.

Assumption 1. The appearance of each transparency is in a noise form and the brightness of each transparency is the same.

Assumption 2. The secret image is a binary image and it is smooth in a sense that its boundary of black and white regions is clearly perceptible. Furthermore, the secret image is large and there are many black pixels and many white pixels.

The reasons for making these assumptions are as follows. We require that the appearance of each transparency is in a noise form and the brightness of each transparency must be the same. In other words, the number of black subpixels in every block cannot be changed when creating a fake transparency. Otherwise, if collusive cheaters want to create a black block after stacking, he can simply increase more number of black subpixels in his block or create a white block by reducing the number of black subpixels in his block. Therefore, this assumption about fixed number of black subpixels is necessary. Furthermore, in order to decide the authenticity of the reconstructed image, we also need to assume that the secret image is smooth and the number of black pixels and there are many black pixels and many white pixels.

It is well known that VC suffers from a graying effect and the decoded image being much blurrier and darker than the original image. Furthermore, it is not easy to properly align two transparencies. To align more than two transparencies is much harder and impractical. Hence, instead of discussing general k-out-of-n VC, we will focus on the cheating problem in 2-out-of-n VC.

3.2. Overview of Cheating Process

Secret sharing schemes suffer from cheating where cheaters can submit false shares during secret reconstruction. In this subsection, we show that cheating is also possible in VC.

We first show that it is possible for collusive cheaters to convert transparencies into digital data with the help of a scanner. And they can analyze these data in order to infer the values of the important parameters that are used to generate their shares. Figure 1 illustrates a procedure to digitalize transparencies.

Let's discuss the digitalization procedure in details. It consists of three processes.

- Digitalizing process: This process transforms the white-and-black transparencies, Share1 and Share2 into 0-and-1 digital shares, DShare1′ and DShare2′. Black pixel is 1 and white (transparent) pixel is 0.
- Stacking process: This process creates a share, Share12, by XORing the shares, DShare1′ and DShare2′.
- Inferring process: This process should perform the following operations:

1. Estimate the block size m that is used as a unit to divide the share12 into blocks. By counting the number of black subpixels in every block,

we can find out the two values d and α.

2. Create an image by using black pixels to represent the blocks with the number of black subpixels $H(V) \geq d$ and use white pixel to represent the blocks with the number of black subpixels $H(V) \leq d - \alpha * m$.
3. If the image matches the secret image, output the predicted values. Otherwise, go to step 1.

Finally, all shares can be generated based on the share construction methods proposed by Naor and Shamir [8].

Now, we demonstrate the cheating process using a 2-out-of-3 scheme. Assume Alice, Bob, and Carol are three participants in a 2-out-of-3 VC. In the following, we will call an image a *message* since each image will represent a password. A secret message is transformed into three distinct shares, denoted S_A, S_B, and S_C. They are delivered to Alice, Bob, and Carol, respectively. Stacking two of the three shares will reveal the secret message. Figure 2 shows the whole cheating process.

Without lose of generality, Alice and Bob are assumed to be the collusive cheaters who intend to deceive the victim Carol.

The related parameters used are $B_V = 2, W_V = 1, H(S^1) = 1, H(S^0) = 1$ and $m = 3$, where

- m: the number of subpixels in a block.

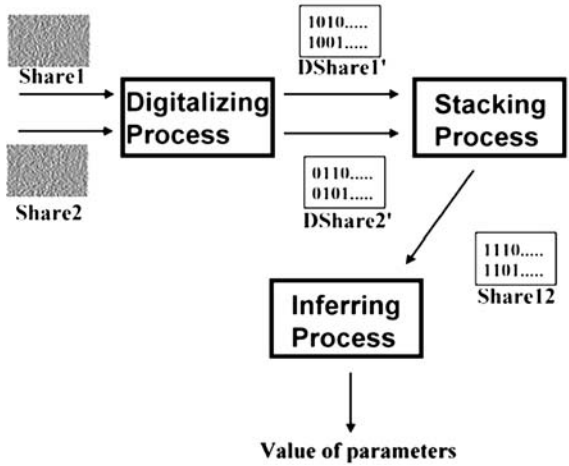


Figure 1. Digitalization procedure.

- B_V: the number of black subpixels in a block representing a black pixel of the reconstructed secret image.
- W_V: the number of black subpixels in a block representing a white pixel of the reconstructed secret image.
- $H(S^1)$: the number of black subpixels of any block in C^1.
- $H(S^0)$: the number of black subpixels of any block in C^0.

Let

$$C^0 = \begin{bmatrix} C_1^0 \\ C_2^0 \\ C_3^0 \end{bmatrix} = \left\{ \text{All the matrices obtained by permuting the columns of } \begin{bmatrix} 1\,0\,0 \\ 1\,0\,0 \\ 1\,0\,0 \end{bmatrix} \right\}$$

$$C^1 = \begin{bmatrix} C_1^1 \\ C_2^1 \\ C_3^1 \end{bmatrix} = \left\{ \text{All the matrices obtained by permuting the columns of } \begin{bmatrix} 1\,0\,0 \\ 0\,1\,0 \\ 0\,0\,1 \end{bmatrix} \right\}$$

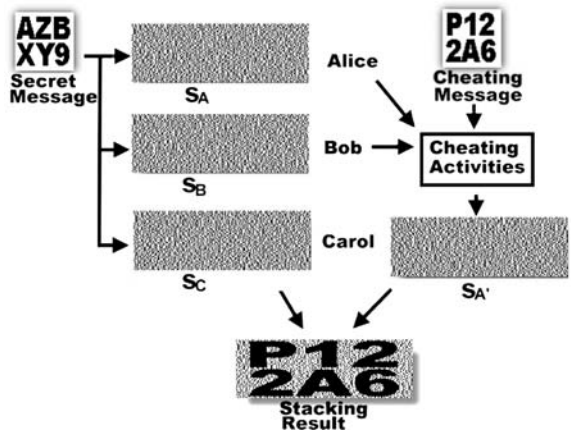


Figure 2. Cheating in visual cryptographic scheme.

Table 1. The basic concept of cheating in 2-out-of-3 VC.

	Pixel in Secret message	Block in Share S_A	Block in Share S_B	Block in Share S_C	Pixel in Cheating message	Block in Share S'_A	Block in Share S'_B
Case 1	white	[1 0 0]	[1 0 0]	[1 0 0]	white	[1 0 0]	[1 0 0]
Case 2	white	[1 0 0]	[1 0 0]	[1 0 0]	black	[0 1 0]	[0 0 1]
Case 3	black	[1 0 0]	[0 1 0]	[0 0 1]	white	[0 0 1]	[0 0 1]
Case 4	black	[1 0 0]	[0 1 0]	[0 0 1]	black	[1 0 0]	[0 1 0]

Based on C^0 and C^1, the dealer produces three shares $S_A, S_B,$ and S_C. For the ith pixel in the secret message, if the ith pixel is white, a matrix M^0 is chosen randomly from C^0 and M_1^0, M_2^0 and M_3^0 are assigned to $S_{Ai}, S_{Bi},$ and S_{Ci}, respectively. On the other hand, if the ith pixel is black, a matrix M^1 is chosen randomly from C^1 and M_1^1, M_2^1 and M_3^1 are assigned to $S_{Ai}, S_{Bi},$ and S_{Ci}, respectively. This operation will repeat until every pixel of the secret message is encoded. It does not matter the values of the parameters are public or not. As we have seen, collusive cheaters can derive the exact values from their shares.

The secret message is composed of many white or black blocks. If the cheaters intend to cheat someone, it is necessary for them to change the construction of their shares. First of all, they predict the positions of black and white subpixels in the victim's share. Then, based on the prediction, they change the positions of the black and white subpixels in the fake shares. Finally, after stacking the fake shares with the victim's shares, the cheating message will be revealed instead of the real secret message. The key step is how to predict the positions of black and white subpixels in the victim's share, and to rearrange the new positions of black and white subpixles in the cheaters' shares. There are four possible cases shown in Table 1.

It is easy to see that in case 1 and case 4, S_{Ai} (S_{Bi}) and S'_{Ai} (S'_{Bi}) are identical. In case 2, Alice and Bob compare their blocks $S_{Ai} = [1\,0\,0]$ and $S_{Bi} \overline{=} [1\,0\,0]$, and predict Carol's block $S_{Ci} = [1\,0\,0]$. This is because all rows in C^0 are identical. The blocks (S_{Ai}, S_{Bi}, S_{Ci}) in shares (S_A, S_B, S_C) are the same. Therefore, they create two modified blocks $S'_{Ai} = [0\,1\,0]$ and $S'_{Bi} = [0\,0\,1]$. Now, the stacked block of any two of the shares S'_{Ai}, S'_{Bi}, and S_{Ci} represents black. In case 3, Alice and Bob compare their blocks $S_{Ai} = [1\,0\,0]$ and $S_{Bi} = [0\,1\,0]$, and predict Carol's block $S_{Ci} = [0\,0\,1]$. This is because the rows in C^1 are pair-wise distinct and the blocks (S_{Ai}, S_{Bi}, S_{Ci}) in shares (S_A, S_B, S_C) are different. Therefore, they can create two mod-

ified blocks $S'_{Ai} = [0\,0\,1]$ and $S'_{Bi} = [0\,0\,1]$. Now, the stacked block of any two of the shares S'_{Ai}, S'_{Bi}, and S_{Ci} represents white.

The cheating process of the 2-out-of-3 VC can be extended to the 2-out-of-n VC which is constructed by the following collections of $n \times n$ matrices [9]:

$$C^0 = \left\{ \text{All the matrices obtained by permuting the columns of } \begin{bmatrix} 1\,0\,0\cdots 0 \\ 1\,0\,0\cdots 0 \\ \vdots \\ 1\,0\,0\cdots 0 \end{bmatrix} \right\}$$

and

$$C^1 = \left\{ \text{All the matrices obtained by permuting the columns of } \begin{bmatrix} 1\,0\,0\cdots 0 \\ 0\,1\,0\cdots 0 \\ \vdots \\ 0\,0\,0\cdots 1 \end{bmatrix} \right\}.$$

The related parameters used are $B_V = 2, W_V = 1, H(S^1) = 1, H(S^0) = 1$ and $m = n$. For the case of C^0, it is not necessary to predict the victim's blocks since all blocks are identical. Since C^1 is a $n \times n$ identity matrix and the cheaters have $n-1$ rows, the victim's block must be the remaining row. Therefore, for $n > 2, n-1$ collusive cheaters can deceive the remaining participant in a 2-out-of-n VC.

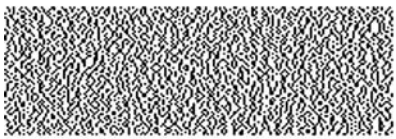
More generally, Table 1 can be extended to any visual cryptographic scheme for collusive cheaters to create the fake shares to deceive the victim in if they know the structure of black and white blocks of victim's share. Therefore, we can conclude this section with the following simple theorem.

THEOREM 1. *Cheating is possible in visual cryptography.*

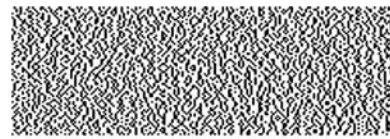
3.3. Experimental Results of Cheating Schemes

To demonstrate the feasibility of cheating, we conduct several experiments. The binary image shown in Figure 3(a) is employed as the original secret message and Figure 3(b)–(d) are the corresponding shares S_A, S_B, and S_C. The results of superimposing two of shares S_A, S_B, and S_C are shown in Figure 3(e)–(g). The cheating message is shown in Figure 4(a), and the two modified shares S'_A and S'_B, are shown in Figure 4(b)–(c). The result of superimposing S'_A and S_C (shown in Figure 4(d)) clearly reveals the cheating message. Figure 4(e) also shows the cheating message resulted from stacking S'_B and S_C.

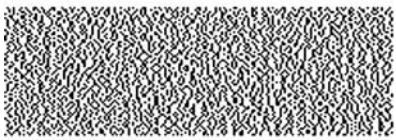
(a)Secret message *SM* (64*64)



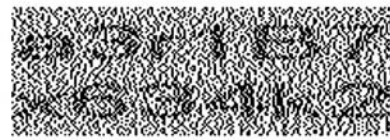
(b)Share S_A (64*192)



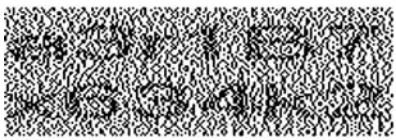
(c) Share S_B (64*192)



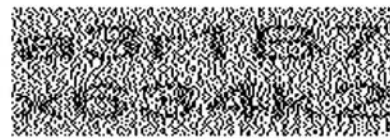
(d)Share S_C (64*192)



(e)Secret message by superimposing share S_A and share S_B (64*192)

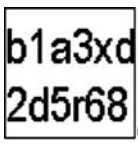


(f) Secret message by superimposing share S_C and share S_B (64*192)

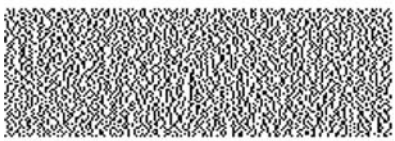


(g)Secret message by superimposing share S_C and share S_A (64*192)

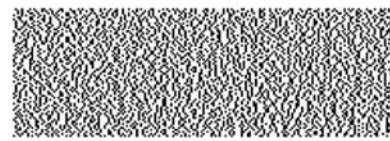
Figure 3. The experimental results based on a 2-out-of-3 VC.



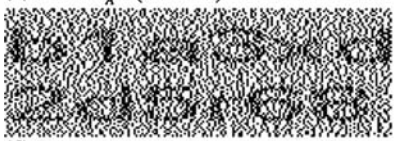
(a)Cheating message *CM* (64*64)



(b)Share S_A' (64*192)



(c)Share S_B' (64*192)



(d)Secret message by superimposing share $S_A'$and S_C (64*192)

(e)Secret message by superimposing share $S_B'$and S_C (64*192)

Figure 4. The experimental results under cheating attack.

4. Cheating Prevention Schemes

Definition 4. A VC scheme is a cheating prevention scheme if the probability of successful cheating is negligible.

Intuitively, cheating can be prevented if participants suspect that the transparencies or the decoded images are not genuine. Based on this observation, we propose two simple prevention schemes. One is designed to provide the participants the ability to verify the integrity of the transparencies before decoding secret messages. The other is designed to make it harder for the cheaters to predict the structure of the transparencies of the other participants.

4.1. An Authentication based Cheating Prevention Scheme

It is natural to solve the cheating problem by adopting the concept of authentication. Our approach is to use extra shares to verify the integrity of every participant's share.

An authentication based cheating prevention scheme consists of shares S_i and verification shares V_i. Shares S_i are generated by any visual cryptographic scheme. Verification shares V_i, for $i = 1, 2, \ldots, n$, generated by the verification shares generation process $f(\cdot)$ are used to verify the correctness of the shares S_j, for $j = 1, 2, \ldots, n$ and $i \neq j$. Each participant P_i should provide the dealer with a distinct verification logo L_i to be used for verifying the authenticity of other shares. All logos are confidential. The verification shares generation process is based on a 2-out-of-2 VC. Each verification share V_i is divided into $n-1$ regions, $R_{i,j}$ where $1 \leq j \leq n$, $j \neq i$ so that when stacking V_i and S_j the logo L_i appears in $R_{i,j}$. Figure 5 shows the verification shares generation process.

Let us carry on the scenario in Section 3. Besides possessing S_A, S_B, and S_C, Alice, Bob, and Carol also possess V_A, V_B, and V_C, respectively. V_A is the verification share to verify the correctness of S_B, and S_C. That is, the verification share is used to verify the correctness of the other two shares possessed by the other two participants. For simplicity, the scheme is divided into three phases: *Initialization*, *Authentication* and *decoding phases*.

A. *Initialization phase*
   First, the participants determine their individual logos L_A, L_B, and L_C, respectively. The logos are sent to the dealer securely.

B. *Authentication phase*
   In the authentication phase, Carol stacks V_C onto S_A (S_B) from Alice (Bob) and check if L_C appears on the stacked transparencies. If L_C does not appear, Carol refuses to accept the share.

C. *Decoding phase*

If authentication succeeds then Carol stacks S_C onto S_A (S_B) to decode the secret message.

THEOREM 2. *The scheme described above is a cheating prevention scheme.*

Proof. Since cheaters do not know the secret logo, the probability that they can create a fake share to pass the verification is negligible. Therefore, based on Definition 4, the scheme is a cheating prevention scheme. ■

Figure 6 illustrates the experiment results. L_C, shown in Figure 6(a), is used by Carol to verify Alice's share and Bob's share. Figure 6(b) and (c) demonstrate the results of stacking V_C and S_A and V_C and S_B. If there are cheatings, the results of stacking V_C onto S'_A and S'_B are shown in Figure 6(d) and (e).

The above scheme solves the cheating problem by using verification shares to ensure the shares from other participants are authentic and hence the recovered secret image is authentic. However, each participant is burden with a verification share. In the next subsection, we will proposed a 2-out-of-$(n+l)$ cheating prevention scheme without extra burdens.

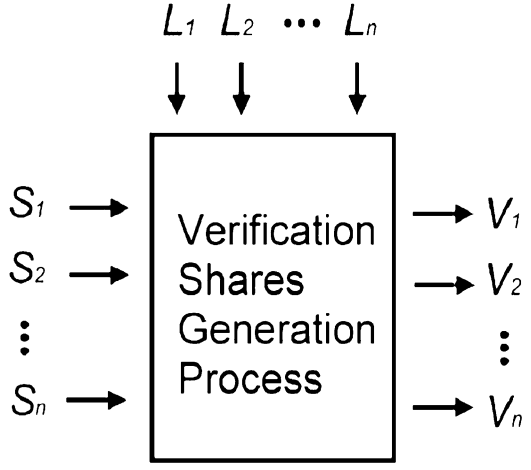


Figure 5. The verification shares generation process $f(\cdot)$.

4.2. A 2-OUT-OF-(N+L) Cheating Prevention Scheme

In this subsection, we propose a simple prevention scheme that is designed to make it harder for the cheaters to predict the structure of transparencies of the other participants. The method uses 2-out-of-$(n+l)$ VC instead of 2-out-of-n, where $l \geq 1$. The dealer creates $(n+l)$ shares but only delivers n shares to the n participants. The extra l shares are kept secret or destroyed by the dealer. For simplicity, we also demonstrate this scheme with three phases: *Initialization*, *distribution* and *decoding phases*.

A. *Initialization phase*
The dealer generates shares based on 2-out-of-(n+l) VC instead of 2-out-of-n .

B. *Distribution phase*

1. The dealer generates randomly and uniformly n pair-wise distinct numbers ω_i from the set $\{1, 2, \ldots, n+l\}$.

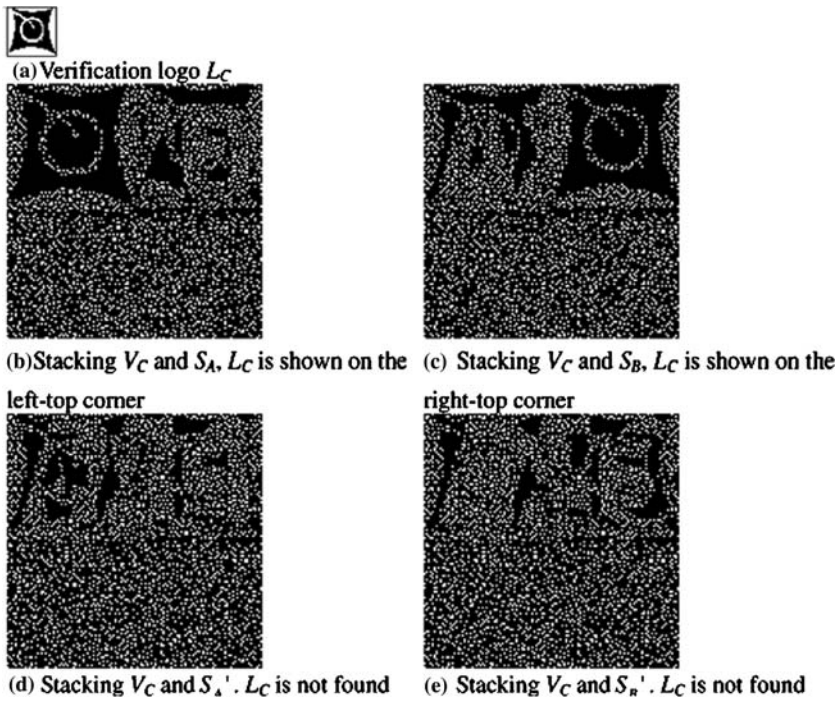


Figure 6. The experimental results of the scheme based on visual authentication.

2. The dealer distributes shares S_{ω_i} to participant P_i for $i = 1, 2, \ldots, n$.

C. *Decoding phase*
When at least 2 transparencies are stacked together; the secret message can be visually recovered by anyone.

Following the same scenario in Section 3.2, we use 2-out-of-4 VC instead of 2-out-of-3. The original construction matrices are replaced by the following two sets of 4×4 matrices:

$$C^0 = \left\{ \text{All the matrices obtained by permuting the columns of } \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \right\}$$

$$C^1 = \left\{ \text{All the matrices obtained by permuting the columns of } \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \right\}$$

The secret message and cheating message are shown in Figures 7(a) and 8(a), respectively. Shares S_A, S_B, S_C and S_D are shown in Figure 7(b)–(e). The dealer generates random numbers $\omega_i \in \{2, 1, 3\}$ and holds the share S_D, then distributes S_B to Alice, S_A to Bob, and S_C to Carol. The results of superimposing any two shares of S_A, S_B, and S_C are shown in Figure 7(f)–(h). Figure 8(b)–(c) illustrate fake shares S'_A and S'_B. Fortunately, after superimposing S'_A and S_C, shown in Figure 8(d), the revealed image is not smooth. That is, it is not perceptible. Figure 8(e) illustrates the same result.

The extra l shares in the initialization phase are used to ensure that the probability for the cheaters to change the shared black pixels in the secret image into white pixels without detection is small.

LEMMA 1. *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 guess the structure of B is* $1/(1+l)$.

Proof. In the scheme, B can be any row of an $(n+l) \times (n+l)$ matrix. The cheaters can determine $n-1$ rows if there are $n-1$ collusive cheaters. Any one of the remaining $l+1$ rows is equally likely to be B since the dealer

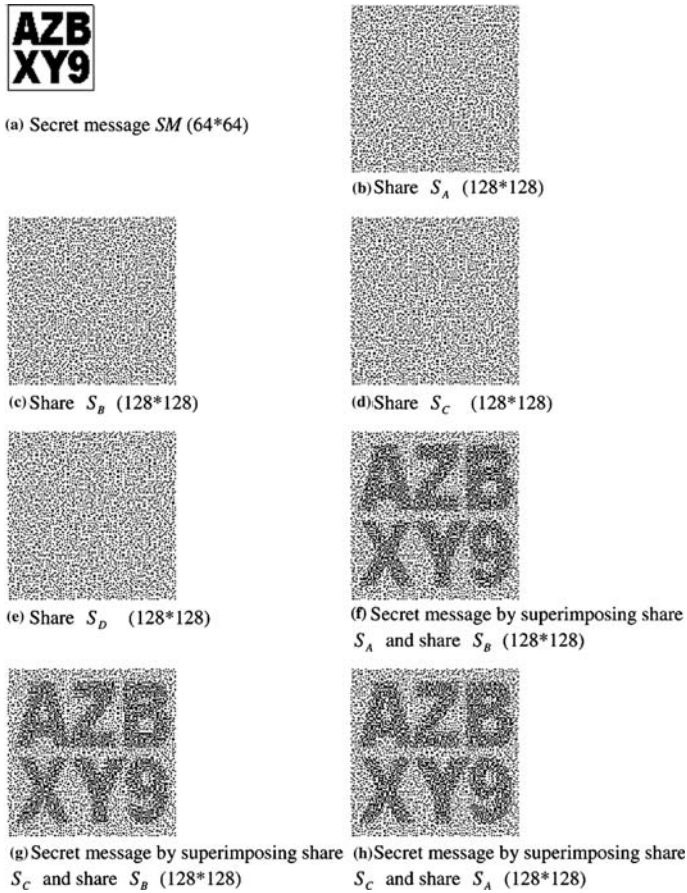


Figure 7. Example of a 2-out-of-(n+l) cheating prevention scheme.

distributes the shares to the participants randomly and uniformly. Therefore, the probability that cheaters can correctly guess the structure of B is $1/(1+l)$. ■

It is possible that the cheaters change only white pixels into black ones in order to create cheating messages. For example, they can change **P** into **B**. Nevertheless, we can resolve this weakness by requiring the secret image to consist of two complementary parts. Two binary images are said to be complementary to each other if and only if they have same size and, for all corresponding pixels, one is black the other is white. The decoded image is authentic only if the two parts represent the same message. In this

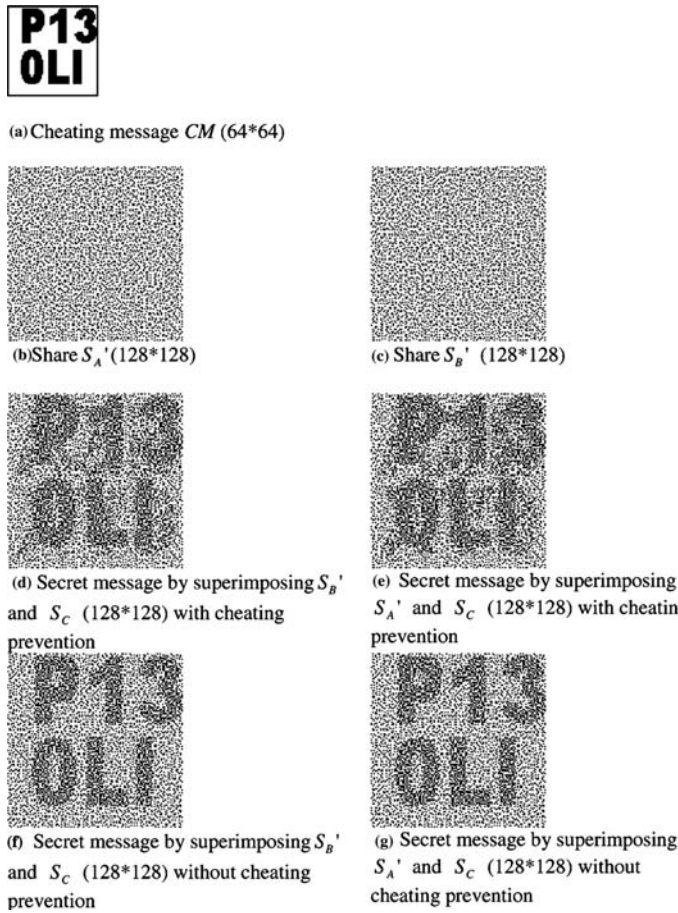


Figure 8. Experimental results of cheating prevention.

case, the cheaters are doomed to change black pixels in some part in order to create fake messages. Therefore, we have the following theorem.

THEOREM 3. *The 2-out-of-$(n+1)$ scheme is a 2-out-of-n cheating prevention scheme.*

Proof. Assume the cheaters need to change k black pixels of the secret image into white pixels in order to create the cheating message. Then, by Lemma 1, the probability that the cheaters can correctly guess the structure of the corresponding blocks in the victim's transparency is $(1/1+1)^k$.

By Assumption 2, there are many black pixels in the secret image. Therefore, k is large and hence the probability that the cheaters can guess the structure of the transparency of a victim in order to create a fake authentic image is negligible if $l > 0$. ■

5. Conclusions

VC is an interesting technique and has been widely investigated. In this paper, we show that cheating is possible when cheaters form a coalition in order to deceive honest participants. Therefore, applications based on VC are vulnerable. We also propose two cheating prevention schemes. Intuitively, one involves the concept of authentication to guarantee shares are unmodified. The other uses 2-out-of-$(n+l)$ VC instead of 2-out-of-n VC. The experiment results demonstrate the proposed schemes provide well protection against cheating.

Acknowledgment

The authors would like to thank the anonymous referees for their valuable comments.

References

1. G. Blakley, *Safeguarding Cryptographic Keys,* Proc. AFIPS 1979 Natl. Conf. New York, Vol. 48 (1979) pp. 313–317.
2. E. F. Brickell and D. R. Stinson, The detection of cheaters in threshold schemes, *SIAM J. Disc. Math.,* Vol. 4 (1991) pp. 502–510.
3. M. Carpenteri, A perfect threshold secret sharing scheme to identify cheaters, *Des. Codes Cryptogr.*, Vol. 5 (1995) pp. 183–187.
4. C. C. Chang and J. C. Chuang, An image intellectual property protection scheme for gray-level image using visual secret sharing strategy, *Pattern Recogn. Lett.*, Vol. 23 (2002) pp. 931–941.
5. C. C. Chang and R. J. Hwang, Efficient cheater identification method for threshold schemes, *IEE Proc.-Comput. Digit. Technol.*, Vol. 144 (1997), pp. 23–27.
6. http://www.cacr.math.uwaterloo.ca/~dstinson
7. M. Naor and B. Pinkas, Visual Authentication and Identification, In Burton S. Kaliski Jr. (ed.), *Advances in Cryptology—Proceedings of Crypto 97*, Lecture Notes in Computer Science, Springer-Verlag, New York, 1294 (1997) pp. 322–336.
8. M. Naor and A. Shamir, Visual cryptography, In Alfredo De Santis (ed.), *Advances in Cryptology—Proceedings of Eurocypto 94*, Lecture Notes in Computer Science, Springer-Verlag, New York, 950 (1995) pp. 1–12.
9. W. Ogata and K. Kurosawa, Optimum secret sharing scheme secure against cheating, In Ueli M. Maurer (ed.), *Advances in Cryptology—Proceedings of Eurocypto 96*, Lecture Notes in Computer Science, Springer-Verlag, New York, 1070 (1996) pp. 200–211.
10. M. Rabin, Efficient dispersal of information for security, load balancing, and fault tolerance, *J. ACM,* Vol. 36 (1989) pp. 335–348.

11. A. Shamir, How to share a secret, *Comm. ACM,* Vol. 22 (1979) pp. 612–613.
12. G. J. Simmons, An introduction to shared secret and/or shared control schemes and their applications, *Contemporary Cryptology,* IEEE Press, Piscataway (1991) pp. 491–497.
13. M. Tompa and H. Woll, How to share a secret with cheaters, *J. Cryptology,* Vol. 1 (1988) pp. 133–138.
14. C. C. Wang, S. C. Tai and C. S. Yu, Repeating image watermarking technique by the visual cryptography, *IEICE Trans. Fundamentals,* Vol. E83-A (2000) pp. 1589–1598.