On the Security of a Cheating Immune Visual Secret Sharing Scheme

Yu-Chi Chen[1], Du-Shiau Tsai[2], Gwoboa Horng [1]
Department of Computer Science and Engineering,
National Chung Hsing University[1]
Department of Information Networking Technology,
Hsiuping Institute of Technology[2]
Email[1] {s9756034, gbhorng}@cs.nchu.edu.tw
Email[2] dstsai@hit.edu.tw

Abstract

Visual Secret Sharing (VSS), first invented by Naor and Shamir, is a variant of secret sharing. In the literature, VSS schemes have many applications, including visual authentication and identification, steganography, and image encryption. Moreover, VSS schemes provide the secure services in communications. In 2010, De Prisco and De Santis deeply discussed the problem of cheating in VSS, gave the definition for deterministic cheating, and presented two cheating immune visual secret sharing schemes: 1) the simple scheme 2) the better scheme. However, we discover that the better scheme is not immune as they claimed. In this paper, we analyze this scheme is prone to deterministic cheating in theory and practice.

Keyword: Visual Cryptography; Visual Secret Sharing; Cheating; Cheating Prevention; Cheating Immune Scheme

1. Introduction

Naor and Shamir first proposed a variant of secret sharing called "visual secret sharing" (VSS) [3], where shares given to participants by the dealer 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 complicated cryptographic computation. More generically, in the k-out-of-n visual secret sharing (for short, (k,n)-VSS), there are totally n participants, and any k participants are in X which can obtain the secret image by stacking their transparencies. A VSS scheme is usually composed of three phases: (1) encoding (2) distributing (3) decoding. However, a special property to differ VSS from secret sharing [4] is that the security of VSS is achieved by losing the contrast and the resolution of the secret image. The quality of the reconstructed secret image is inferior to the original secret image. Due to the invention of VSS, many applications and techniques have been proposed.

Related works. Horng et al. [2] showed that cheating is possible in (k,n)-VSS, according to the cheaters in traditional secret sharing [5]. The cheating activity can cause unpredictable damage to victims while victims accept a fake secret image different from the actual secret image as authentic. De Prisco and De Santis also considered the problem of cheating, and they proved that in (n,n)-VSS and (2,n)-VSS, cheating is successful by n-1 collusive cheaters [1]. These n-1 cheaters want to fool the victim. They presented two cheating prevention VSS schemes (also called "cheating immune VSS schemes"). Conclusively, n-1 cheaters should be assumed, when we discuss the problem of cheating.

Normally, the cheating prevention schemes can be divided into two classes. One is share authentication where another additional transparency (verification transparency) is used to authenticate transparencies from other participants. The other is blind authentication, where cheaters predict the structure of transparencies of other participants is hard [1,2]. De Prisco and De Santis [1] gave the definition for deterministic cheating, and presented two cheating immune threshold visual secret sharing schemes: 1) the simple scheme 2) the better scheme. They also showed the better scheme is cheating immune to deterministic cheating in any black or white pixel. Additionally, their scheme can be used without relying on the complementary image to improve the security as compared to Horng et al.'s 2-out-of-(n+l) method [2].

In this paper, we find the better scheme is not as secure as the authors claimed. We then present a new cheating attack, named "deterministic white-to-black attack". The analysis and experimental result demonstrate that the better scheme suffers from the proposed attack in theory and practice.

The rest of the paper is organized as follows. Section 2 provides preliminaries with respect of the model of VSS and the definition of cheating. Section 3 briefly reviews De Prisco and De Santis's better (2,n)-VSS scheme. Section 4 shows deterministic white-to-black attack and the analysis of the better scheme. Finally, conclusions are given in Section 5.

2. Preliminaries

2.1 Model of Visual Secret Sharing

A VSS scheme is a special variant of a *k*-out-of-*n* secret sharing scheme, where the shares given to participants are xeroxed onto transparencies. A share in VSS is always called a "transparency". If *X* is a qualified subset, then the participants in *X* can decode the secret image by stacking their transparencies. Usually, the secret is an image, so we can regard it as the secret image (*SI*). To generate the transparencies, each black and white pixel of *SI* is handled separately. It appears as a collection of *m* black and white subpixels in each of the *n* transparencies. The *m* subpixels are denoted by a *block*. One pixel of the secret image corresponds to *nm* subpixels, and then the *nm* subpixels are denoted by an $n \times m$ boolean matrix, called a *base matrix*. $S=[S_{ij}]$ expresses the base matrix, 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 while if $H(V) \leq d-\alpha m$ for some fixed threshold *d* and relative difference α. We would hope *m* to be as small as possible and α to be as large as possible. Formally, a solution to the (*k*,*n*)-VSS consists of two collections C^0 and C^1 of $n \times m$ base 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 [3].

Definition 2.1. A solution to the (*k*,*n*)-VSS is composed of two collections C^0 and C^1 of $n \times m$ base matrices. The solution is considered valid if the following conditions are hold:

Contrast conditions:

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

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.

For convenience, let W_V be an integer which $W_V \leq d-\alpha m$ and B_V be an integer which $B_V \geq d$. W_V and B_V are used to judge a stacking block is black or white in a VSS scheme.

2.2 Definition of Cheating in VSS

Horng et al. proposed that cheating is possible in (*k*,*n*)-VSS [2]. We take a (2,3)-VSS scheme as an 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. Wlog, Alice and Bob are assumed to be collusive cheaters and Carol is the victim. In cheating, T_1 and T_2 to create forged 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 [3], collusive cheaters can predict the actual structure of the victim's transparency so as to create T'_2. C^0 is all the matrices obtained by permuting the columns of $\begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$, and C^1 is all the matrices obtained by permuting the columns of $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. By observing the above matrices, two rows of above 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 a white pixel or it is set to be [001] for a black pixel. Formally, the cheaters can construct a sub-base matrix (SBM) by T_1 and T_2, and then infer T_3. Practically, De Prisco and De Santis gave the following definitions of cheating in VSS [1].

Definition 2.2. For each pixel, if the probability of successful cheating for the cheaters is 1, the cheating is denoted as the deterministic cheating.

Definition 2.3. For a VSS scheme, the probability of successful cheating in any pixel is less than 1, hence this scheme is cheating immune to deterministic cheating.

These definitions are reasonable [1], and then make researchers more easily to consider the security for cheating immune VSS schemes.

3. Review of a Cheating Immune Threshold Visual Secret Sharing Scheme

De Prisco and De Santis proposed two cheating immune visual secret sharing schemes: the simple scheme and the better scheme. The simple scheme has been showed some inherent weaknesses by themselves, such that the white pixels are not protected without the complementary image. So they proposed a better scheme which is provably secure. They claimed this scheme for each black or white pixel is cheating immune to deterministic cheating. In the following, we will describe the better (2,*n*)-threshold scheme (for

short, the better scheme).

In this scheme, one pixel will be expanded to 2^n+n+1 subpixels. The base matrices are C^0 and C^1. Each of them is consisted of three parts: C^1, C^2, C^3. C^1 is all the possible 2^n binary column vectors of length n. C^2 is a column of all 0s. C^3 is the Naor-Shamir's base matrix [3]. We express $C^0 = [C_1^0 \mid C_2^0 \mid C_3^0]$C and $C^1 = [C_1^1 \mid C_2^1 \mid C_3^1]$. The following Fig 1 showed the base matrices for the better scheme (n=3,4).

$$C^0 = \left[\begin{array}{cccccccc|c|ccc} 0&1&0&1&0&1&0&1&0&1&0&0\\ 0&0&1&1&0&0&1&1&0&1&0&0\\ 0&0&0&0&1&1&1&1&0&1&0&0 \end{array}\right]$$

$$C^1 = \left[\begin{array}{cccccccc|c|ccc} 0&1&0&1&0&1&0&1&0&1&0&0\\ 0&0&1&1&0&0&1&1&0&0&1&0\\ 0&0&0&0&1&1&1&1&0&0&0&1 \end{array}\right]$$

(a) 2-out-of-3

$$C^0 = \left[\begin{array}{cccccccccccccccc|c|ccc} 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0 \end{array}\right]$$

$$C^1 = \left[\begin{array}{cccccccccccccccc|c|ccc} 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&1 \end{array}\right]$$

(b) 2-out-of-4

Fig. 1 The base matrices for the better scheme

Generically, we note that $B_V=2^{n-1}+2^{n-2}+2$ and $W_V=2^{n-1}+2^{n-2}+1$. In addition, they have proven the better scheme is cheating immune to deterministic cheating. For any black or white pixel, the cheaters cannot infer the actual value of victim's subpixels. The proof is definitely correct.

4. Analysis of the Better Scheme

We will show the weakness of De Prisco and De Santis's better scheme via our presented attack when $n\geq 3$. We then give the attack processes for the 2-out-of-n better scheme (n>3,4,5).

4.1 Deterministic White-to-Black Attack

This attack, named "Deterministic White-to-Black Attack", only occurs in white pixels for the better scheme. According to the attack for creating a fake black pixel, collusive cheaters generate a fake block (fb), then the victim will get a fake black one by stacking fb and T_v where T_v is the victim's corresponding block. In more details, this attack is illustrated as follows.

1. First, cheaters reconstruct the sub-base matrix (SBM) collusively.
2. They compute the numbers of different kinds of columns within the SBM, respectively.
3. Initially, let $fb=[a_1, a_2, ..., a_z]=[0, 0, ..., 0]$, where $z=2^n+1+n$.
4. If n is odd such as n=3, modify a_i=1 when a_i corresponds to the columns of all 0s in SBM; otherwise, modify a_i=1 if a_i corresponds to the columns of all 0s or all 1s in SBM. Here, we give an example of n=4 (Fig. 2) to show the process.
5. If $\sum_{j=1}^{z} a_j = 2^{n-1}+1$, the attack is done. Otherwise, in the case of $\sum_{j=1}^{z} a_j < 2^{n-1}+1$, the cheaters randomly choose x kinds of columns whose numbers are 2 where $\sum_{j=1}^{z} a_j + 2x = 2^{n-1}+1$, and then set a_i=1 when a_i corresponds to the columns of these x kinds of columns (the total number of x kinds of columns is $2x$). Finally, ensure $\sum_{j=1}^{z} a_j = 2^{n-1}+1$ after inserting 1s into $2x$ subpixels.

Let the stacking block of $fb+T_v$ be $[b_1, b_2, ..., b_z]$ ($z=2^n+1+n$). The cheater can make sure $\sum_{j=1}^{z} b_j = B_V + y$ where y is an integer and let $Y=B_V+y$ as the number of subpixels of 1 in the stacking block, so the victim will accept the fake black pixel.

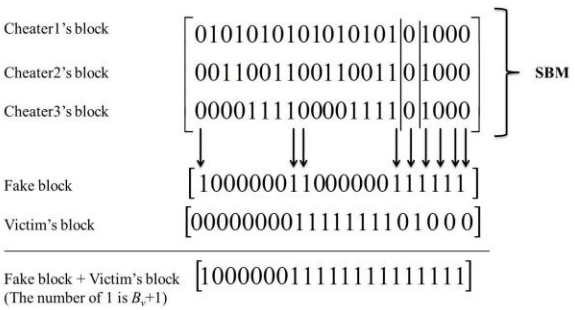


Fig. 2 A example of cheating process (n=4)

4.2 Analysis and Experiment

The processes of the deterministic white-to-black attack with respect to n=3,4 are simple. In the following, we show the process of the attack for n=5. First, the cheaters reconstruct the SBM and compute the numbers of different kinds of columns within SBM, and they can obtain the following results.

- The number of the column of all 1s is 3. This column we called the all 1s column.
- The number of the column of all 0s is 7. This column we called the all 0s column.
- The number of other each kind of columns is 2 (not all 0s and all 1s).

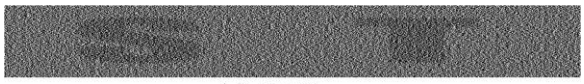
Since n=5 is odd, they set a_i=1 when a_i corresponds to the columns of all 0s. Now, we know $\sum_{j=1}^{z} a_j < 2^{5-1} + 1$. The cheaters continue to choose x(=5) kinds of columns (not all 0s and all 1s, $2x=2^{5-1}+1-\sum_{j=1}^{z} a_j$), and set a_i=1 when a_i corresponds to the columns of the 2x columns. This is, they ensure $\sum_{j=1}^{z} a_j = 2^{5-1} + 1 = 17$.

According to *fb*, we notice that 2x columns correspond to x subpixels of the victim's block are 1 and x subpixels of the victim's block are 0. And we also observe that 7 all 0 columns correspond to that 1 subpixel of the victim's block is 1 and the other 6 subpixels are 0. Thus, we can infer that $2^{5-1}+1-(x+1)=2^{5-1}+1-(5+1)=11$ subpixels of the victim's block are 1 correspond to 11 subpixels of *fb* are 0. Finally, the number of subpixels of 1 in the stacking block is $X=17+11=28=B_V+2> B_V$, hence the deterministic white-to-black attack is successful.

Because of no guessing with probability in the attack, the deterministic white-to-black attack is deterministic cheating. The better scheme is not cheating immune to the deterministic white-to-black attack. More formally, the generic result for the collusive cheaters' SBM is given as follows.

- The number of the column of all 1 is 3 for any n.
- The number of the column of all 0 is n+2 for any n.
- The number of each other kind of columns, except all 0 and all 1 columns, is 2 for any n.

Nevertheless, this attack is only suitable to the (2,n) better scheme, because the expansion of the better scheme is much bigger than other schemes such as Naor-Shamir's VC scheme [3].



(a) T_3+T_2

(b) T_3+CT

Fig. 3 Experiment result for the attack

For demonstrating the proposed cheating attack we conducted a experiment in the (2,3) better scheme. In this example, for creating each two adjacent fake black blocks, only one of the corresponding two blocks is changed by the attack and the other block is remained unchanged. The above method can ensure the reconstructed cheating image is normal, and Fig. 3 shows the experiment result that we can modify "**S T**" into "**SIT**".

5. Conclusions

In this paper, we have analyzed that a cheating immune visual secret sharing scheme is insecure without violating the original definitions of Naor-Shamir's visual cryptography. This scheme suffers from the deterministic white-to-black attack, while it is not cheating immune to deterministic cheating. To the best of our knowledge, the presented blind authentication cheating prevention schemes (Horng et al.'s and De Prisco and De Santis's) are insecure to protect black and white pixels at the same time without using a complementary image.

Acknowledgements

This work was partially supported by the National Science Council of the Republic of China under contract NSC 99-2221-E-005-078.

References

[1] R. De Prisco and A. De Santis, "Cheating Immune Threshold Visual Secret Sharing," Comput. J., Vol. 53, pp 1485-1496, 2010.

[2] G. Horng, T.H. Chen and D.S. Tsai, "Cheating in Visual Cryptography," Des. Codes Cryptogr., Vol. 38, pp. 219-236, 2006.

[3] M. Naor and A. Shamir, "Visual Cryptography," Proc. EUROCRYPT' 94, Perugia, Italy, May 9-12, Lecture Notes in Computer Science, Vol. 950, pp. 1-12. Springer, 1995.

[4] A. Shamir, "How to Share a Secret," Commun. ACM, Vol. 22, pp.612-613, 1979.

[5] M. Tompa and H. Woll, "How to Share a Secret with Cheaters," J. Cryptology, Vol. 1, pp.133-138, 1989.