Cheating Human Vision in Visual Secret Sharing

Yu-Chi Chen[1,*], Gwoboa Horng[1] and Du-Shiau Tsai[2]
[1]Department of Computer Science and Engineering
National Chung Hsing University, Taiwan
[2]Department of Information and Networking Technology
Hsiuping University of Science and Technology, Taiwan
[*]email: wycchen@ieee.org

Abstract

Visual Secret Sharing (VSS), first introduced by Naor and Shamir, is a variant form of secret sharing; especially, secret decoding is stacking shares together without performing any complicated cryptographic computation. The recovered secret is visible by human vision system (HVS). However, Horng et al. showed cheating is possible in VSS, which is inspired from cheating in secret sharing. Since then many cheating activities and cheating immune schemes have been proposed, whereas all presented cheating activities only take cheating in any pixel as a unit into consideration. In this paper, we analyze some presented cheating activities, and we propose a new kind of cheating: *Region Cheating Attack* (RCA) as a result of the properties of HVS. Differently, RCA involves with cheating in a region which is several adjacent pixels as a unit. We therefore use RCA to enhance effect of several attacks which has been proposed. Moreover, a new attack, deterministic white-to-black attack (DWtBA), is proposed to point out that a well-known cheating immune scheme, proposed by De Prisco and De Santis, will suffer from RCA and DWtBA. Finally, we propose a remedy to overcome the problem of the scheme.

1 Introduction

Naor and Shamir first proposed a variant of secret sharing called "visual secret sharing" (VSS) [11], where shares given to participants by the dealer

are xeroxed onto transparencies. The participants in $\mathcal{X}$ can visually recover the secret image by stacking their transparencies together without performing any complicated cryptographic computation if $\mathcal{X}$ is an authorized subset. 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 in $\mathcal{X}$ can obtain the secret image by stacking their transparencies. A VSS scheme is usually composed of three phases: (1) encoding (2) distributing (3) decoding. Encoding is performed by the dealer to get all transparencies, then he distributes those transparencies to participants. Finally, the participants in $\mathcal{X}$ can decode the secret image by stacking their transparencies.

However, the security of VSS is achieved by loosing the contrast and the resolution of the secret image is a special property to differ VSS from secret sharing [12]; indeed, the quality of the reconstructed secret image is inferior to the original secret image. Many applications and techniques have been proposed, including visual authentication and identification, steganography, and image encryption which are attributed to the invention of VSS.

Related work. Horng et al. [9] showed that cheating is possible in (k,n)-VSS, according to the cheaters in traditional secret sharing [14]. The cheating activity can cause unpredictable damage to victims, when 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 $(2,n)$-VSS, cheating is successful by $n-1$ collusive cheaters, and in (n,n)-VSS, by 1 cheater. The collusive cheaters want to *fool* the victim for some reasons. The authors gave the definition for deterministic cheating, and presented two cheating immune threshold visual secret sharing (CIVSS) schemes: 1) the simple scheme and 2) the better scheme. They also declare the better scheme is cheating immune to deterministic cheating in any black or white pixel, and based on the security model, it is provably secure in theory. In particular, the better scheme can be used without relying on the complementary image to improve the security as compared to 2-out-of-$(n+l)$ method [9].

Contribution and organization. There are four significant contributions of this paper as follows.

1. NOVEL CONCEPT. We analyze some presented cheating activities regarding Hoeng et al.'s cheating activity [9] and Hu and Tzeng's cheating activities (as well as CA-1 and CA-2) [10]. All of the attacks only take cheating in any pixel as a unit into consideration. According to HVS, we propose a new kind of cheating: *region cheating at-*

tack (RCA) in which we consider cheating in several adjacent pixels, whereas a region is composed of several adjacent pixels. Moreover, we also give the formal definition of security of RCA.

2. ENHANCEMENT. The well-know attacks, CA-1 and CA-2, are easy to be detected by HVS in some cases. For improving this disadvantage, we enhance effect of CA-1 and CA-2 upon cheating, which combines CA-1/CA-2 with the proposed RCA.

3. CRYPTANALYSIS. We find the better scheme, proposed by De Prisco and De Santis, is not as secure as the authors claimed. Therefore, we present another cheating attack, named *deterministic white-to-black attack* (DWtBA). The cryptanalysis and experimental result are attached to demonstrate that the better scheme suffers from DWtBA and RCA undoubtedly.

4. REMEDY. Cryptanalysis is used to point out potential weaknesses in a cryptographic scheme, while, straightly, it can help us to present an improvement. Thus, we give a remedy to overcome the problem of the insecure better scheme.

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 presents a new cheating activity with HVS, then illustrates the results with experiments of human's vision. Section 4 briefly reviews De Prisco and De Santis's better $(2, n)$-VSS scheme, and shows the deterministic white-to-black attack and the cryptanalysis of the better scheme. Finally, conclusions are given in Section 5.

2 Visual Secret Sharing (VSS)

In this section, we will briefly review the model of VSS and describe the formal definition of cheating in VSS.

2.1 Model

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". The participants in $\mathcal{X}$ would decode the secret image by stacking their transparencies if $\mathcal{X}$ is a qualified subset. Usually, the secret is an image, so we can regard it as

the secret image (*SI*). To generate the transparencies, each 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 a $n \times m$ boolean matrix, called a *base matrix*. Let $S = [S_{ij}]$ be the base matrix, while $S_{ij} = 1$ 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. Here, α is the contrast and m is the pixel expansion. We 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 [11].

Definition 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 would 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. The stacking results in Naor-Shamir's (2,3)-VSS are showed in Fig. 1.

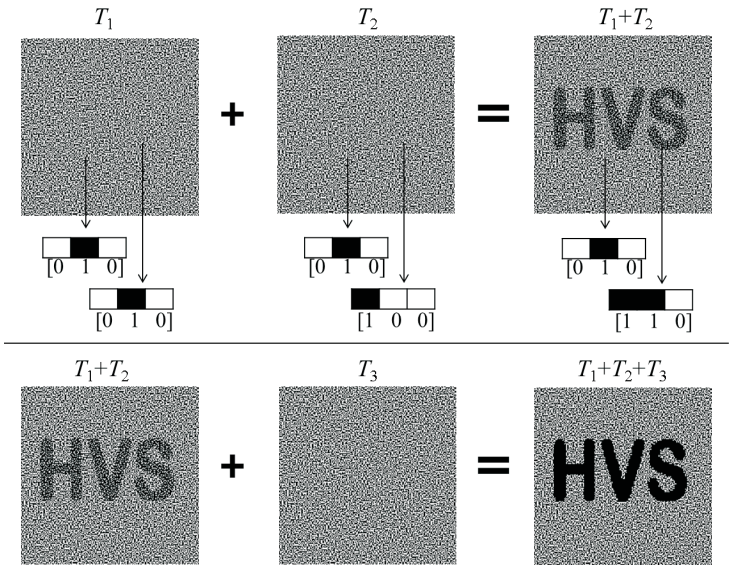


Figure 1: The stacking results in Naor-Shamir's (2,3)-VSS

Example 1. *In (2,3)-VSS,* 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* $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$*. Conveniently, we always write* $C^0 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ *and* $C^1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$*. In (3,3)-VSS, the base matrices are* $C^0 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$ *and* $C^1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$.

2.2 Cheating for a Block

Cheating is possible in (k,n)-VSS [9]. 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. Without lose of generality, Alice and Bob are

assumed to be collusive cheaters and Carol is the victim.[1] In cheating, T_1 and T_2 to create forged transparency/cheating transparency CT, whereas superimposing CT 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 [11], collusive cheaters can predict the actual structure of the victim's transparency so as to create CT. 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 CT is set to be the same structure of T_3. For presenting a black pixel of cheating image, the block of CT is set to be the different structure of T_3. For example, if the block of T_3 is [0 1 0], CT is set to be [0 1 0] for a white pixel or [0 0 1] 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. Here, we give another example as Fig 2, and show the generalization of this cheating activity below.

1. $n-1$ cheaters stack their transparencies to recover the secret image.
2. According to the reconstructed secret image, the cheaters will infer the victim's transparency.
3. Taking a cheating image (CI) as an input, they can generate several cheating transparencies to the victim. The CTs and the victim's transparency will recover CI, not SI.
4. Finally, the victim will be fooled if he accept the reconstructed cheating image as SI.

Practically, De Prisco and De Santis gave the following definitions of cheating in VSS [7].

Definition 2. *A cheating attack (activity) is denoted as the deterministic cheating if the probability of successful cheating for the cheaters is 1 for each pixel/block.*

[1] The cheaters are assumed to collude w.r.t cheating in VSS [4, 7, 9, 10].

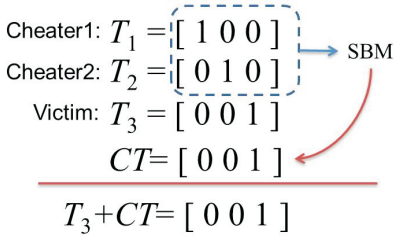


Figure 2: Cheating in (2,3)-VSS for a block

Definition 3. *A VSS scheme is cheating immune to deterministic cheating if the probability of successful cheating in any pixel is less than 1.*

These definitions are reasonable [7] for a block, and then make researchers more easily to consider the security for cheating immune VSS schemes for a block (pixel).

2.2.1 CA-1 and CA-2

In 2007, Hu and Tzeng showed three cheating activities: CA-1, CA-2, and CA-3 [10]. We first give a definition about "perfect black", and then briefly describes CA-1 and CA-2. CA-3 is omitted to show, because it is a extended method for extended VSS.

Definition 4. *A block in a stacking result is perfect black if and only if all subpixels of the block are black.*

Example 2. *A block of a stacking result is [1 1 1 1] is perfect black, but the block is [1 1 1 0] is not. The block of [1 0 0 0] or [1 1 0 0] is also not perfect black.*

CA-1 and CA-2 are performed by a malicious participant (MP) and a malicious outsider (MO), respectively. MP or MO sets a cheating image and generates CTs, whereas the stacking result of the victim's transparency and CTs reveals the cheating image.

In CA-1, with the MP's transparency T_1, we assume that each block in T_1 has x black and y white subpixels. The MP then chooses a cheating image and prepares r fake transparencies, CT_1, ..., CT_r, where $r = \lceil \frac{m}{x} \rceil - 1$.

Example 3. *In a (3,3)-VSS scheme with* 3×4 *base matrices, MP creates only one* CT*, because of* $r = \lceil \frac{4}{2} \rceil - 1 = 1$*. The base matrices is the same as Section 2.1. For each white pixel of the cheating image, the MP copies the corresponding subpixels of the block in* T_1 *to the* CT*. Assume the block is [1 0 1 0] in* T_1*. The corresponding*

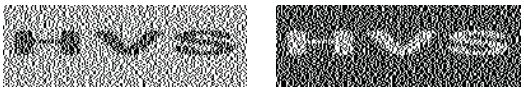


Figure 3: An example of complementary images

block in the CT is set to be [1 0 1 0]. For each black pixel of the cheating image, the MP randomly assigns 2 black and 2 white subpixels to the CT, whereas the block in the stacking of CT and T_1 is perfect black. *We assume the block is [1 0 1 0] in T_1 when the MP wants to form a black pixel of the cheating image, therefore, the corresponding block in the CT is set to be [0 1 0 1].*

In CA-2, with the same scenario, the MO only knows the share construction algorithm, and it does not hold any transparency. In a (3,3)-VSS scheme, the MO can generate two fake transparencies, CT_1 and CT_2, and then makes the stacking result of CT_1, CT_2, and T_v be black.

Example 4. *For each white pixel of the cheating image, the corresponding subpixels of the block in CT_1 and CT_2 is set to be the same. Assume the block in CT_1 is [1 0 1 0], then the block in the CT_2 will be [1 0 1 0]. For each black pixel of the cheating image, the corresponding subpixels of the block in CT_1 and CT_2 is set to be complement. Assume the block in CT_1 is [1 0 1 0], then the block in CT_2 is [0 1 0 1].*

2.3 Cheating Immune Visual Secret Sharing

Cheating would be prevented if participants find out or detect some transparencies or the reconstructed secret images are not genuine. Based on this intuition, there are two approaches for designing CIVSS schemes, first introduced by Horng et al. [9]. One is based on share authentication where another additional transparency (verification transparency) is used to authenticate transparencies from other participants. The other is based on blind authentication, where cheaters infer the structure of transparencies of other participants is hard. The goal of share authentication is to provide the participants the ability to verify the integrity of the shares before reconstructing secret images and the goal of blind authentication is to make it harder for the cheaters to predict the structure of the shares of the other participants.

Usually, in a share authentication based CIVSS scheme, each participant receives two transparencies: one transparency and one verification transparency. The first one is used to reconstruct the secret image and the

verification transparency is used to check the integrity of the transparencies held by other participants. Hu and Tzeng's scheme is share authentication, but this scheme is insecure [5].

In a blind authentication based CIVSS scheme, the transparencies must be inherently immune to cheating. In (k,n)-VSS, $k < n$, because the structures of black block and white block are different, a participant must hold two transparencies. One is the original transparency (referred to as T_1), and the other is the complementary transparency (referred to as $\overline{T_1}$). Thus, $T_1 + T_2$ displays the secret image, while $\overline{T_1} + \overline{T_2}$ will display the complementary secret image. As known, two results of $T_1 + T_2$ and $\overline{T_1} + \overline{T_2}$ are given in Fig. 3.

2.3.1 Review of De Prisco and De Santis's Better Scheme

De Prisco and De Santis proposed two CIVSS schemes: the simple scheme and the better scheme. The simple scheme has been showed some inherent weaknesses by the authors, as well as 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 block/pixel is cheating immune to deterministic cheating.

In the better 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_{bin}, C_{all0}, C_{ns}. C_{bin} is all the possible 2^n binary column vectors of length n. C_{all0} is a column of all 0. C_{ns} is the Naor-Shamir's base matrix [11]. We express $C^0 = [C_{bin}|C_{all0}|C^0_{ns}]$ and $C^1 = [C_{bin}|C_{all0}|C^1_{ns}]$.

For example, C^0 and C^1 of the better $(2,3)$ scheme are showed as follows:

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

$$C^1 = \left[\begin{array}{cccccccc|c|ccc} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right] \tag{2}$$

C^0 and C^1 of the better $(2,4)$ scheme are showed as follows:

$$C^0 = \left[\begin{array}{cccccccccccccccc|c|cccc} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{array}\right] \tag{3}$$

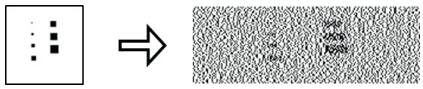


Figure 4: The stacking result for 1×1 black pixel, 2×2 black pixels, ..., 7×7 black pixels

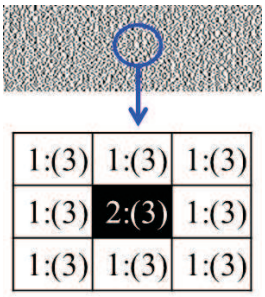


Figure 5: A region composed of one black block and eight white blacks and $m = 3$

$$C^1 = \left[\begin{array}{c|c|c} 0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1 & 0 & 1\,0\,0\,0 \\ 0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1 & 0 & 0\,1\,0\,0 \\ 0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1 & 0 & 0\,0\,1\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1 & 0 & 0\,0\,0\,1 \end{array}\right] \tag{4}$$

It is clarified that $B_V = 2^{n-1} + 2^{n-2} + 2$ and $W_V = 2^{n-1} + 2^{n-2} + 1$. The pixel expansion, m, is $2^n + n + 1$ and the contrast, α, is $1/m$. Moreover, the authors 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 blocks. The proof is definitely correct.

3 Region Cheating Attack

Previous cheating for a block in VSS has been discussed by the papers of Horng et al., Hu and Tzeng, and De Prisco and De Santis [7, 9, 10]. They presented different cheating activities, where those kinds of cheating activities are for a block. However, in practical, many published papers used a set of blocks instead of one block for increasing visibility of secret. Fig 4 illustrates how to increase visibility of one secret pixel by a set of 1×1 blocks, 2×2 blocks, ..., 7×7 blocks. In this paper, we name a set of

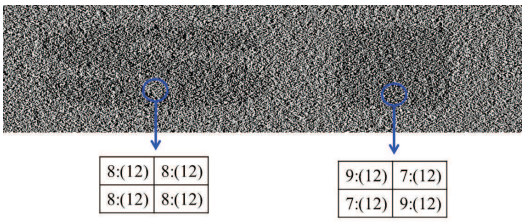


Figure 6: A region, $m = 12$

blocks a region. Fig. 4 evidences the following definition.

Definition 5. *For a VSS scheme, HVS does not observe the secret image on each block. It observes on regions.*

In addition, Fig. 4 shows the stacking result for 1×1 black pixel, 2×2 black pixels, ..., 7×7 black pixels in (2,3)-VSS.

3.1 RCA: Region Cheating Attack

We denote that a black block consists of μ_B 1s and $m - \mu_B$ 0s in a stacking result, while a white block consists of μ_W 1s and $m - \mu_W$ 0s. In Fig 5, $\rho : (m)$ is used to recognize the block is black or white, where $\rho \in \{\mu_W, \mu_B\}$ and m is the pixel expansion. In Fig 5, the region is composed one black block and eight white blocks, but we cannot observe any black block in the stacking result. This experiment confirms that HVS observes the secret image on regions.

Let $d_\mu = \mu_B - \mu_W$. We define a "black plus block" is a block which is composed of $\mu_B + t \times d_\mu$ 1s in the stacking result for an integer t. The new cheating activity with human vision system (RCA: White-to-Black) performs as follows.[2]

RCA: White-to-Black

1. The cheaters replace a white block (of μ_W 1s) with a black plus block (of $\mu_B + t \times d_\mu$ 1s).

2. The t adjacent white blocks near the black plus block do not change.

[2]Here, we do not consider how the cheaters to replace, because different VSS schemes may suffer from different cheating activities for a block described in Section 2.2. Our RCA can be used with any cheating activity for a block.

3. Finally, in HVS, a cheating region, composed of t white blocks and one black plus block, looks like a black region, composed of $t+1$ black blocks.

For HVS, the presented RCA is actually existing as well as Fig. 6 shows a stacking result with $m = 12$ which consists of different kinds of regions: **S** is for all 8:(12), but **I** is for 9:(12) and 7:(12). If a victim cannot observe **I** is not in the true secret in HVS, he will accept the secret image, **S I**.

However, on the contrary, we also have RCA: Black-to-White. Let $d_\mu = \mu_B - \mu_W$. We define a "white plus block" is a block which is composed of $\mu_W - t \times d_\mu$ 1s in the stacking result for an integer t. This cheating activity performs as follows.

RCA: Black-to-White

1. The cheaters replace a black block (of μ_B 1s) with a white plus block (of $\mu_W - t \times d_\mu$ 1s).
2. The t adjacent black blocks near the white plus block do not change.
3. Finally, in HVS, a cheating region, composed of t black blocks and one white plus block, looks like a white region, composed of $t+1$ white blocks.

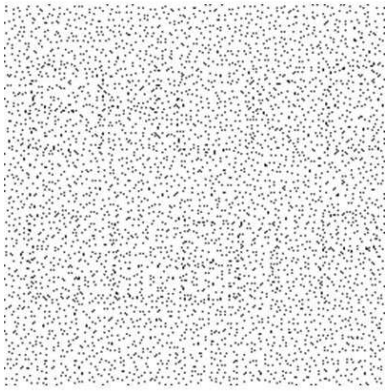
Definition 6. *A scheme is not cheating immune to RCA if and only if the probability of RCA is 1 where cheaters find a correct integer t.*

Example 5. *If the cheaters consider $t = 1$ with $Pr[t = 1] = 5/6$ and $t = 2$ with $Pr[t = 2] = 1/6$, the scheme is cheating immune to RCA; Otherwise, the cheaters consider $t = 1$ with $Pr[t = 1] = 1$, the scheme is not.*

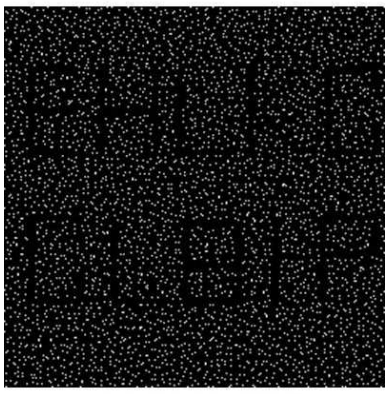
3.2 Enhancing CA-1 and CA-2

Cheaters can make the victim to accept the fake secret by setting perfect black blocks in CA-1 and CA-2 [10]. Except (n,n)-VSS schemes, other schemes do not ensure that the stacking results contain perfect black blocks. However, for other schemes, CA-1 and CA-2 will be detected, whereas the perfect black blocks is *sensitive* by HVS, which means the perfect black blocks are observed easily. We give an experiment in Fig. 7 where two stacking results with the same contrast, $\alpha = 1/16$. The first one is (2,16)-VSS, and the second one is (5,5)-VSS. We find the second one is clearer than the other, while it contains the perfect black blocks. We thus conclude that original CA-1 and CA-2 are detected when $k \neq n$ in (k,n)-VSS.

(a) Secret image



(b) (2, 16)-VSS



(c) (5, 5)-VSS

Figure 7: The stacking result of (5,5)-VSS is more visible than of (2,16)-VSS

Accordingly, we can use the above concept of RCA with CA-1 and CA-2. Let CA-1 or CA-2 be the cheating method for Step 1 of RCA: White-to-Black. Other steps are the same as before. Finally, even the stacking result contains the perfect black blocks, HVS does not detect them, because these blocks are interfered with the adjacent blocks (not perfect black blocks) in a sense.

4 Cryptanalysis of a Cheating Immune Visual Secret Sharing Scheme

In Section 2.3.1, we have described the better $(2,n)$-threshold scheme (for short, the better scheme). Now we propose deterministic white-to-black attack (DBtWA) in Section 4.1, and further, we also give the cryptanalysis to indicate how to cheat HVS for this scheme by DBtWA and RCA in Section 4.2.

4.1 Deterministic White-to-Black Attack (DWtBA)

This attack, named "Deterministic White-to-Black Attack" (for short, DWtBA), only occurs in a white pixel for the better scheme. Collusive cheaters generate a fake block (fb) according to the attack for creating a fake black pixel. The victim will get a black one by stacking fb and T_v where T_v is the victim's corresponding block. We illustrate this attack as follows for more details.

(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 0 in SBM (Fig. 8); otherwise, smodify $a_i = 1$ when a_i corresponds to the columns of all 0 or all 1 in SBM (Fig. 9).

(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

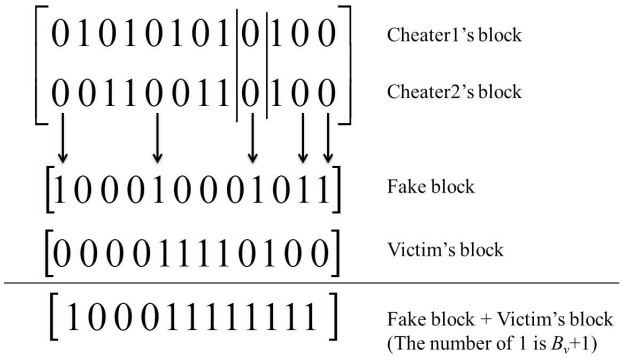


Figure 8: The process of this attack for the (2,3) better scheme.

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 $2x$ subpxiels.

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 $y > 0$ is an integer and let $X = B_V + y$ as the number of subpixels of 1 in the stacking block, so the victim will accept the fake black block.

Definition 7. *A scheme is not cheating immune to the deterministic white-to-black attack if and only if the probability of the attack is 1 where the cheaters can generate a fake black block.*

We straightly conclude that DWtBA is the deterministic cheating as a result of Definition 2 and 7.

4.2 Cryptanalysis

The processes of DWtBA with respect to $n = 3, 4$ are showed in Fig. 8 and 9, separately. We know the attack for $n = 3$ and 4 is very simple.

We have to further discuss cases of $n \geq 5$. We take $n = 5$ as example, where $B_V = 2^{5-1} + 2^{4-1} + 2 = 26$ and $W_V = 2^{5-1} + 2^{4-1} + 1 = 25$. First, the cheaters reconstruct the SBM and compute the numbers of different kinds of columns within SBM, and they can obtain the following result as Fig 10.

- The number of the columns of all 1s is 3. This column we called the all 1 column.
- The number of the columns of all 0s is 7. This column we called the all 0 column.

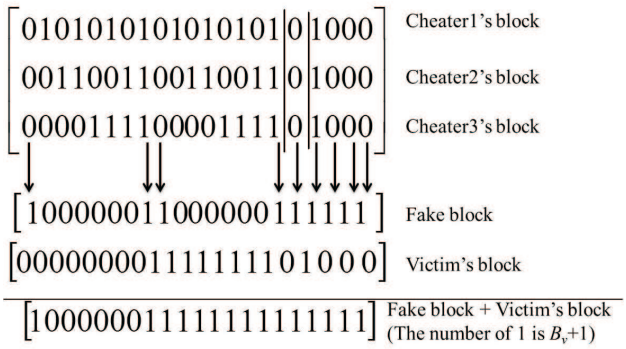


Figure 9: The process of this attack for the (2,4) better scheme.

Table 1: The presented attack for $n = 3, 4, ..., 8$ ($y = X - B_V$)

n:odd	B_V	X	y	n:even	B_V	X	y
3	8	9	1	4	14	15	1
5	26	28	2	6	50	52	2
7	98	101	3	8	194	197	3

- The number of each other kind of columns is 2 (not all 0 and all 1).

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

From the fake block 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. We thus 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 DWtBA is successful without violating Definition 1. Fig. 10 shows the result of this attack for the (2,5) better scheme with respect of the correspondence of subpixels, where 1(7) denotes that the number of subpixels of 1 is 7, and $x_1, ..., x_5$ denotes five different kinds of columns except the all 0 and all 1 columns.

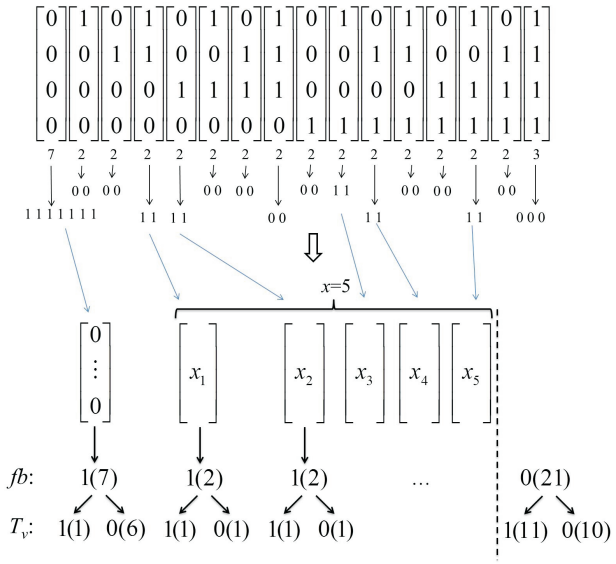


Figure 10: The result of this attack for the (2,5) better scheme.

In terms of Table 1, if $X = B_V + y > 2^n + n + 1$, the attack will fail. However, $y > 2^n + n + 1 - 2^{n-1} - 2 = 2^{n-1} + n - 1$ ($n \geq 3$) is impossible. DWtBA is deterministic cheating, because the probability of the attack is 1. The cheaters absolutely know an integer, t, to generate a region which is composed of a fake black block and t normal white blocks. As a result, we can have the following theorem.

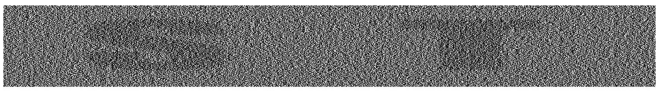
Theorem 1. *The better scheme is not cheating immune to the deterministic white-to-black attack and RCA.*

The generic result from the collusive cheaters' SBM is given as follows.

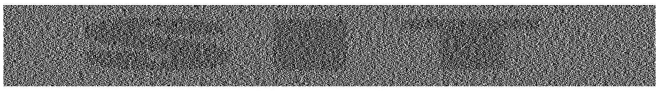
- The number of the all 1 columns is 3 for any n.
- The number of the all 0 columns is $n+2$ for any n.
- The number of each other kind of columns, except all 0 and all 1 columns, is 2 for any n.

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 VSS scheme [11].

For demonstrating the proposed cheating attack we conducted a experiment in the (2,3) better scheme. In this example, for creating each two



(a) T_3+T_2



(b) T_3+CT

Figure 11: The results of $T_3 + T_2$ and $T_3 + CT$.

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. 11 shows the experiment results that we can modify "**S T**" into "**SIT**", where T_3 is the victim's transparency and CT is the fake transparency for cheating.

For example of (2,3) better scheme [7], the proof of the scheme only ensures that cheaters cannot change 8 from $W_V = 7$. Indeed, cheaters cannot change 9 from 7. A block of 9 and an adjacent block of 7 looks like two block of 8 (Fig. 6 and 11).

4.3 Remedy

In the paper of De Prisco and De Santis [7], the base matrices of the better scheme, C^0 and C^1, are proven to be an optimal structure, thus we cannot decrease the number of columns of C^0 and C^1. Based on the better scheme, we attempt to find an improvement via increasing the number of columns of C^0 and C^1.

According to the attack, the cheaters usually choose the subpixels of the fake block and set them as 1s which correspond to all 0 columns in SBM. The main idea of the improvement is to add all 0 columns to the original base matrices (described as Section 2.3.1). Unfortunately, we find the improvement is still impossible to withstand DWtBA, but it can resist RCA partially.

We have known that, in SBM, the number of the all 1 columns is 3, whereas the number of the all 0 columns is $n+2$ for any n due to the inference in Section 4.2. In addition, the number of 1s of a block is $2^{n-1}+1$ (referred to as $w = 2^{n-1}+1$), and the pixel expansion is $m = 2^n + 1 + n$; for example, in the (2,3) better scheme, the block is [1 1 1 1 1 0 0 0 0 0 0 0]. In the

following, we give a possible improved (2,3) scheme. The improved better scheme holds the following base matrices, $C^0 = \left[\begin{array}{c|c} 0 & 010101010100 \\ 0 & 001100110100 \\ 0 & 000011110100 \end{array}\right]$ and $C^1 = \left[\begin{array}{c|c} 0 & 010101010100 \\ 0 & 001100110010 \\ 0 & 000011110001 \end{array}\right]$. Now we show how the cheaters perform DWtBA.

$$
\begin{array}{rll}
T_1: & [0\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,0] & \triangleright\ \mathsf{Cheater1} \\
T_2: & [0\,0\,0\,1\,1\,0\,0\,1\,1\,0\,1\,0\,0] & \triangleright\ \mathsf{Cheater2} \\
\hline
\multicolumn{3}{l}{\textbf{Case 1}} \\
CT1: & [1\,1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,1\,0] & \Pr[CT1] = \frac{5}{6} \\
T_3: & [0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,1\,0\,0] & \triangleright\ \mathsf{Victim} \\
\mathsf{Stack}: & [1\,1\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,0] & \\
\hline
\multicolumn{3}{l}{\textbf{Case 2}} \\
CT2: & [1\,1\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,1] & \Pr[CT2] = \frac{1}{6} \\
T_3: & [0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,1\,0\,0] & \\
\mathsf{Stack}: & [1\,1\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1] &
\end{array}
$$

The improved scheme can resist RCA, because the cheaters do not know how many normal white blocks should be collocated with the fake block. As the above, we know the probability of Case 1 is 5/6, and the probability of Case 1 is 1/6. In Case 1, the cheaters should set a normal white block with a fake block, whereas in Case 2, they should set two normal white block with a fake block.

For more general, the base matrices must be $C^0 = \left[\begin{array}{c|c} 0\ldots0 & \\ \vdots\ddots\vdots & C^0_{dd} \\ 0\ldots0 & \end{array}\right]$ and $C^1 = \left[\begin{array}{c|c} 0\ldots0 & \\ \vdots\ddots\vdots & C^1_{dd} \\ 0\ldots0 & \end{array}\right]$, where C^0_{dd} and C^1_{dd} are the base matrices of the original better scheme. Here, the number of added all 0 columns is more than $w-(n+2) = (2^{n-1}+1)-(n+2)$. We would like the number of added all 0 columns is $w-(n+2)+1 = (2^{n-1}+1)-(n+2)+1 = 2^{n-1}-n+4$ for minimal pixel expansion.

Theorem 2. *This scheme is insecure against the deterministic white-to-black attack, but it resists RCA.*

Proof. For a block, according to the structure of SBM, there are totally $2^{n-1}+2$ all 0 columns in the $(2,n)$ improved better scheme, where $(2^{n-1}+2)$ is denoted by W. Particularly, one of all 0 columns corresponds to 1 of subpixels of the victim's block, and the other $2^{n-1}+1$ correspond to 0s. Therefore, as the above two cases, the cheaters should set a normal white block with a fake block with $\mathsf{Pr}[CT1] = \frac{W-1}{W}$ in Case 1, whereas they should set two normal white block with a fake block with $\mathsf{Pr}[CT2] = \frac{1}{W}$ in Case 2. However, this scheme attributes to that the number of normal white blocks is unknown, because the cheaters do not infer that the stacking result is Case 1 or Case 2. The correct integer t may be one of two cases, and the probability is less than 1. □

To the best of our knowledge, the presented blind authentication cheating immune 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 the complementary image. The better scheme is also insecure due to DWtBA and RCA. Our improved better scheme is only one scheme can be cheating immune to the presented attack and RCA without using the complementary image, whereas the pixel expansion of our scheme is $m = 2^n + 2^{n-1} = 3(2^{n-1})$.

5 Conclusions

Seeing is not believing that, in visual secret sharing, we see a black region, then we cannot ensure that it is made up of all black blocks. We are devoted of a new kind of cheating activities: RCA based on the properties of HVS. With the main concept of it, the previous cheating methods will bring better results. Additionally, we have analyzed De Prisco and De Santis's better scheme suffers from the deterministic white-to-black attack (DWtBA) and RCA. Even this scheme is provably secure based on its security model in theory, which does not imply being secure for HVS. Finally, we attach a remedy to withstand RCA.

References

[1] C. Blundo, P. D'Arco, A. De Santis, and D.R. Stinson, "Contrast optimal threshold visual cryptography schemes," *SIAM Discret. Math.*,

vol. 16, pp. 224-261, 2003.

[2] C.C. Chang, C.C. Lin, T.H.N. Le, and H.B. Le, "Self-verifying visual secret sharing using error diffusion and interpolation techniques," *IEEE Trans. Inf. Forensic Secur.*, vol. 4, pp. 790-801, 2009.

[3] T.H. Chen and K.H. Tsao, "Visual secret sharing by random grids revisited," *Pattern Recognit.*, vol. 42, pp. 2203-2217, 2009.

[4] Y.C. Chen, G. Horng, and D.S. Tsai, "Cheating prevention in visual cryptography," In Cimato, S. and Yang, C.N. (eds), *Visual Cryptography and Secret Image Sharing*, 2011. CRC Press / Taylor & Francis, Boca Raton, FL.

[5] Y.C. Chen, G. Horng, and D.S. Tsai, "Comment on "Cheating Prevention in Visual Cryptography"," IEEE Transactions on Image Processing (Accepted), 2012.

[6] S. Cimato, R. De Prisco, and A. De Santis, "Probabilistic visual cryptography schemes," *Comput. J.*, vol. 49, pp. 97-107, 2006

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

[8] T. Hofmeister, M. Krause, and H. U. Simon, "Contrast-optimal k out of n secret sharing schemes in visual cryptography," *Theor. Comput. Sci.*, vol. 240, pp. 471-485, 2000.

[9] G. Horng, T.H. Chen, and D.S. Tsai, "Cheating in visual cryptography," *Des. Codes Cryptogr.*, vol. 38, pp. 219-236, 2006.

[10] C.M. Hu and W.G. Tzeng, "Cheating prevention in visual cryptography," *IEEE Trans. Image Process.*, vol. 16, pp. 36-45, 2007.

[11] 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, 1994.

[12] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, pp. 612-613, 1979.

[13] S.J. Shyu and M.C. Chen, Optimum pixel expansions for threshold visual secret sharing schemes. *IEEE Trans. Inf. Forensic Secur.*, vol. 6, pp. 960-969, 2011.

[14] M. Tompa and H. Woll, "How to share a secret with cheaters," *J. Cryptology*, vol. 1, pp. 133-138, 1989.

[15] D.S. Tsai, T.H. Chen, and G. Horng, "A cheating prevention scheme for binary visual cryptography with homogeneous secret images," *Pattern Recognit.*, vol. 40, pp. 2356-2366, 2007.

[16] C.N. Yang and T.H. Chung, "A general multi-secret visual cryptography scheme," *Opt. Commun.*, vol. 283, pp. 4949-4962, 2010.

[17] C.N. Yang, A.G. Peng, and T.S. Chen, "MTVSS: (M)isalignment (T)olerant (V)isual (S)ecret (S)haring on resolving alignment difficulty," *Signal Process.*, vol. 89, pp. 1602-1624, 2009.

[18] C.N. Yang, C.C. Wang, and T.S. Chen, "Visual cryptography schemes with reversing," *Comput. J.*, vol. 51, pp. 710-722, 2008.