A Cheat-Prevention Visual Secret Sharing Scheme with Minimum Pixel Expansion

Shenchuan Liu, Masaaki Fujiyoshi, and Hitoshi Kiya

The authors are with the Graduate School of System Design, Tokyo Metropolitan University, Hino-shi, 191–0065, Japan. {liu-shenchuan@sd.tmu.ac.jp, mfujiyoshi@ieee.org,kiya@sd.tmu.ac.jp}

Abstract. A visual secret sharing (VSS) scheme with minimum pixel expansion is proposed to prevent malicious participants from deceiving an honest participant. A VSS scheme encrypts a secret image into pieces referred to as shares where each participant keeps a share so that stacking sufficient number of shares recovers the secret image. A cheat prevention VSS scheme provides another piece for each participant for verifying whether the shares presented by other participants are genuine. The proposed scheme improves the contrast of the recovered image and cheat-prevention functionality by introducing randomness in producing pieces for verification. Experimental results show the effectiveness of the proposed scheme.

Keywords: Visual secret sharing, cheat prevention, visual cryptography

1 Introduction

In recent years, powerful computers offer even ordinary users the encryption of secret information. To encrypt and decrypt secret information, a key (or a key pair) is used and should be securely and safely guarded. This straightforward key protection, however, still has the risk of key loss and leakage. On the other hand, with the development of fast network technologies, many people collaborate on secret projects over the public Internet. Information should be secret even a few member collude to leak the secret information. To overcome such situations, secret sharing (SS) has been proposed [1].

A SS scheme [1] divides a secret into n pieces referred to as shares. n shares are held by no more than n different participants and the secret is recovered if and only if k or more shares are gathered. This scheme is called as a (k, n)-threshold SS scheme. Even computer technology is highly developed, it is not always possible to use computer. In order to share a secret without computers, visual SS (VSS) in which decryption can be done by human eyes has been proposed for binary images [2].

Later, VSS has been extended to non-binary images [3, 4]. Color VSS have also been proposed [5–7]. Instead of generating random-noise share images [2], meaningful shares are employed in a scheme [8]. Some schemes [9, 10] allow to embed multi-secret within one image. A weaken security scheme [11, 12] is also

proposed to improve the visuality of recovered image. Other direction reduces the pixel expansion size and improves the contrast of the recovered image [13, 14].

On the other hand, it is assumed in a scenario that malicious participants deceive an honest participant, and cheat-prevention VSS schemes have been proposed to fight it [15–18]. This paper focus on cheat-prevention VSS. A literature [17] found that the original cheat-prevention VSS scheme [16] is not well function in some circumstances. The literature [17] also proposes a new scheme, but pixel expansion is sacrificed significantly. Later, the same authors proposed another scheme [18] with less pixel expansion, but its application is limited to $(2, n)$-threshold VSS and it introduces a further restriction.

This paper proposes a new cheat-prevention VSS scheme which solves the problem in the original cheat-prevention VSS scheme [16] without sacrificing pixel expansion. By introducing randomness into share generation, it simultaneously overcomes the above mentioned two problems in the conventional schemes [16, 17]. In addition, the proposed scheme can be applied to (k, n)-threshold VSS, whereas a latest scheme [18] which is only applicable to $(2, n)$-threshold VSS.

The rest of this paper is arranged as follows. In Section 2, SS [1], VSS [2], and the concept of cheat-prevention VSS will be reviewed. Conventional cheat-prevention VSS schemes [16–18] are introduced in Section 3. The improved scheme is proposed in Section 4. Experimental results are shown in Section 5 and conclusions and future works are given in Section 6.

2 Preliminaries

This section briefly describes secret sharing (SS), visual SS (VSS), and cheat-prevention VSS.

2.1 Secret Sharing

Here, a (k, n)-threshold SS method [1] in which k of n shares should be gathered to recover the secret information is described with introducing terms and notations.

Let $\mathbf{P} = \{P_1, P_2, \ldots, P_n\}$ be the set of n participants, and each participant P_i holds share S_i where $i = 1, 2, \ldots, n$. Let $2^{\mathbf{P}}$ be the set of all subsets of $\mathbf{P}$.

Let Γ_{Q} and Γ_{F} be the qualified sets and forbidden sets, respectively. Assume Γ_{Q} is monotone increasing and Γ_{F} is monotone decreasing. Denote Γ_{Q}^{*} and Γ_{F}^{*} as the minimum qualified sets and the maximum forbidden sets.

Here, $(\mathbf{P}, \Gamma_{\mathrm{Q}}, \Gamma_{\mathrm{F}})$ is an access structure if $\Gamma_{\mathrm{Q}} \cap \Gamma_{\mathrm{F}} = \emptyset$ and $\Gamma_{\mathrm{Q}} \cup \Gamma_{\mathrm{F}} = 2^{\mathbf{P}}$. Access structure $(\mathbf{P}, \Gamma_{\mathrm{Q}}, \Gamma_{\mathrm{F}})$ for a (k, n)-threshold SS method is that $X \in \Gamma_{\mathrm{Q}}$ if and only if $|X| \geq k$, where $|X|$ is the number of participants in X.

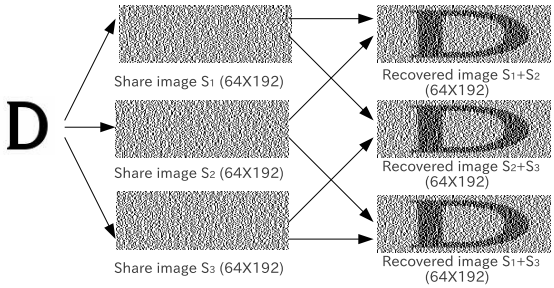


Fig. 1: An example of the $(2, 3)$-threshold visual secret sharing method for binary images [2]. A pixel in the secret image is expanded to three subpixels in a share image, i.e., $m = 3$.

2.2 Visual Secret Sharing

VSS is a kind of secret sharing [2], so the access structure of VSS is the same as SS. There are two differences between VSS and SS; 1) images are used as shares in VSS and 2) decryption needs no computations, it is done by human eyes of watching stacked share images.

Let $\mathbf{S}^0$ and $\mathbf{S}^1$ be the $n \times m$-sized basic matrices for the share image generation in a black-and-white VSS method where $\mathbf{S}^0$ and $\mathbf{S}^1$ are for white and black pixels, respectively. For example, in the original (k, n)-threshold VSS method [2] in which a pixel in a secret image is expanded to m subpixels in share image S_i, $\mathbf{S}^0$ and $\mathbf{S}^1$ are given as

$$\mathbf{S}^0 = \begin{bmatrix} 1\,0\,0 \\ 1\,0\,0 \\ 1\,0\,0 \end{bmatrix} \quad \text{and} \quad \mathbf{S}^1 = \begin{bmatrix} 1\,0\,0 \\ 0\,1\,0 \\ 0\,0\,1 \end{bmatrix} \tag{1}$$

under the condition that $n = m = 3$ and $k = 2$. Each participant P_i holds share image S_i where $i = 1, 2, \ldots, n$. This $(2, 3)$-threshold VSS method generates share image S_i as

Step 1. For each white pixel in the secret image, put the i-th row of $\mathbf{S}^0$ to S_i as m-length subpixels.
Step 2. For each black pixel in the secret image, put the i-th row of $\mathbf{S}^1$ to S_i as m-length subpixels.

Figure 1 shows an example for this $(2, 3)$-threshold VSS method [2].

In general, a VSS method is expected to meet the following requirements.

Req. 1. The increase in pixel expansion should be as small as possible.
Req. 2. The contrast of the secret image in the stacking of shares is not significantly reduced.
Req. 3. It does not rely on the help of an on-line trusted authority.

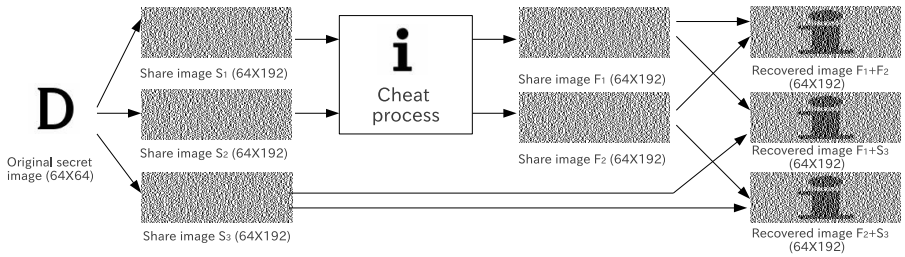


Fig. 2: Two malicious participants collude to deceive the other honest participant in the $(2, 3)$-threshold VSS scheme with $m = 3$.

2.3 Cheat-Prevention Visual Secret Sharing

In normal VSS methods, two or more participants can collude to generate fake shares. For example, as shown in Eq. (1), subpixels corresponding to a white pixel are $[1\ \ 0\ \ 0]$ regardless of participant P_i in the $(2, 3)$-threshold VSS scheme with $m = 3$. In addition, when two participants collude, $\mathbf{S}^1$ can be easily estimated from subpixels in their shares which subpixels correspond to black pixels. Now, colluded two participants know $\mathbf{S}^0$ and $\mathbf{S}^1$, they can generate a fake share to deceive the other participant. In this scenario, the fake secret image is revealed by stacking the fake shares and share (shares) from honest participant (participants) as shown in Fig. 2. In order to overcome this situation, cheat-prevention VSS have been proposed [16, 17].

It is noted that the above cheat is successful when Req. 1 is satisfied. The more the pixel is expanded in the VSS method, the harder the cheat becomes. For example, in the $(2, 3)$-threshold VSS scheme with $m = 4$, $\mathbf{S}^0$ and $\mathbf{S}^1$ are given as

$$\mathbf{S}^0 = \begin{bmatrix} 1\,0\,0\,0 \\ 1\,0\,0\,0 \\ 1\,0\,0\,0 \end{bmatrix} \quad \text{and} \quad \mathbf{S}^1 = \begin{bmatrix} 1\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,1\,0 \end{bmatrix}. \tag{2}$$

When two participants are collusive to cheat, $\mathbf{S}^0$ can be estimated, but $\mathbf{S}^1$ can't be revealed, i.e., the cheat becomes harder. However, the contrast of revealed secret image becomes quite low by increasing the number of subpixels; being uncompliant with Req. 1 becomes uncompliant with Req. 2. Both conventional and proposed cheat-prevention VSS described in this paper meet Req. 1.

A successful cheat-prevention VSS prevents any participant from deceiving an honest participant, and it is summarized [16] that an efficient and robust cheat-prevention scheme should has the following properties in addition to Reqs. 1, 2, and 3:

Req. 4. Each participant verifies shares presented by other participants.
Req. 5. The verification image of each participant is different and confidential.
Req. 6. A cheat-prevention scheme should be applicable to any VSS method.

3 Conventional Cheat-Prevention VSS Schemes

This section reviews two conventional schemes [16, 17] for cheat-prevention VSS. In a cheat-prevention VSS, each of all n participants $\mathbf{P}$ holds two images for satisfying Req. 4; one (share image S_i) is for secret recovery and the other (verification image share V_i) is for verification.

Before revealing the secret image, participant P_i can check others' share image S_j by stacking V_i and S_j, i.e., $V_i + S_j$ where $j = 1, 2, \ldots, n$ and $j \neq i$. If this stacked image $(V_i + S_j)$ reveals verification image O_i of P_i, which is set in advance, share image S_j is judged to be authentic, if not, S_j is forged. It is noted that verification image O_i of P_i should whole be known by P_i only.

3.1 Conventional Scheme 1

Based on given $\mathbf{S}^0$ and $\mathbf{S}^1$ which are the $n \times m$-sized basic matrices for share image generation in a black-and-white VSS method, this scheme [16] firstly creates four $n \times (m+2)$-sized basic matrices $\mathbf{T}^0$, $\mathbf{T}^1$, $\mathbf{R}^0$, and $\mathbf{R}^1$ as

$$\mathbf{T}^0 = \left[\begin{array}{c|c} 10 & \\ \vdots & \mathbf{S}^0 \\ 10 & \end{array}\right], \mathbf{T}^1 = \left[\begin{array}{c|c} 10 & \\ \vdots & \mathbf{S}^1 \\ 10 & \end{array}\right], \tag{3}$$

$$\mathbf{R}^0 = \left[\begin{array}{c|c} 10 & \\ \vdots & 0 \\ 10 & \end{array}\right], \mathbf{R}^1 = \left[\begin{array}{c|c} 01 & \\ \vdots & 0 \\ 01 & \end{array}\right], \tag{4}$$

where $\mathbf{T}^0$ and $\mathbf{T}^1$ are used for generating share S_i and $\mathbf{R}^0$ and $\mathbf{R}^1$ are used for generating verification image share V_i, respectively.

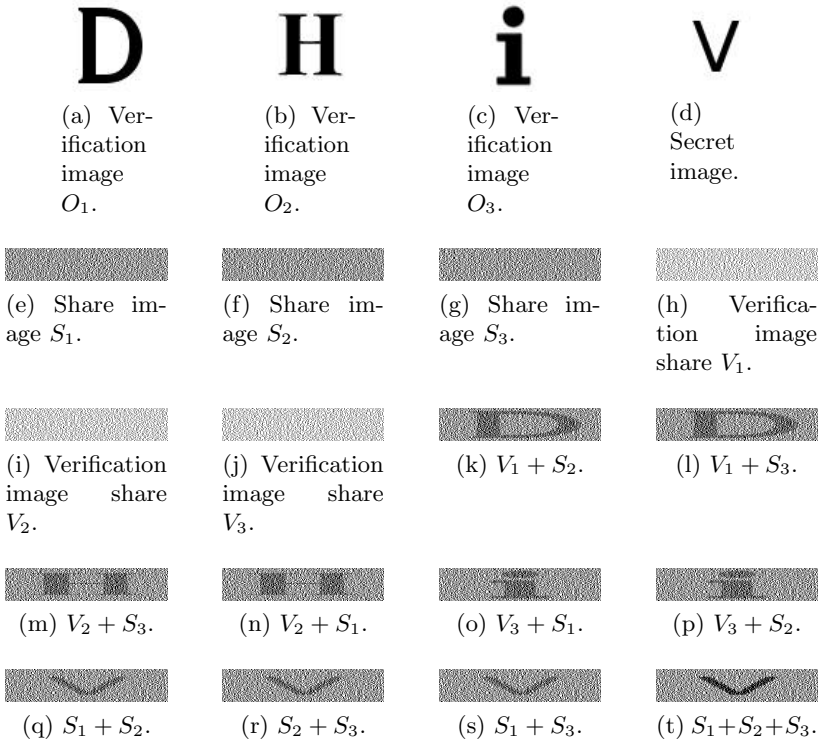
This scheme generates share image S_i as follows:

Step 1. For each white pixel in the secret image, put the i-th row of $\mathbf{T}^0$ to S_i as $(m+2)$-length subpixels.
Step 2. For each black pixel in the secret image, put the i-th row of $\mathbf{T}^1$ to S_i as $(m+2)$-length subpixels.

According to verification image O_i of participant P_i, this scheme generates verification image share V_i as follows:

Step 1. For each white pixel in O_i, put the i-th row of $\mathbf{R}^0$ to V_i as $(m+2)$-length subpixels.
Step 2. For each black pixel in O_i, put the i-th row of $\mathbf{R}^1$ to V_i as $(m+2)$-length subpixles.

By adding two columns consisting of one 0 and one 1 to $\mathbf{S}^0$ and $\mathbf{S}^1$, stacking shares by colluded participants cannot disclose $\mathbf{S}^0$ or $\mathbf{S}^1$. In addition, a generation of fake shares with taking account into the verification image share of the honest participant (participants) becomes much harder. It is noted that columns in $\mathbf{T}^0$,



(a) Verification image O_1. (b) Verification image O_2. (c) Verification image O_3. (d) Secret image.

(e) Share image S_1. (f) Share image S_2. (g) Share image S_3. (h) Verification image share V_1.

(i) Verification image share V_2. (j) Verification image share V_3. (k) $V_1 + S_2$. (l) $V_1 + S_3$.

(m) $V_2 + S_3$. (n) $V_2 + S_1$. (o) $V_3 + S_1$. (p) $V_3 + S_2$.

(q) $S_1 + S_2$. (r) $S_2 + S_3$. (s) $S_1 + S_3$. (t) $S_1 + S_2 + S_3$.

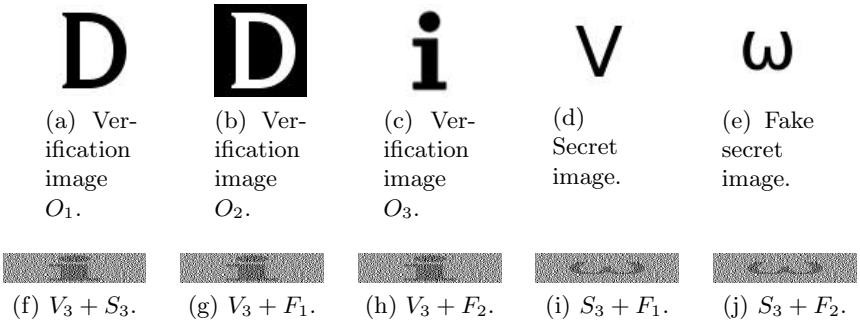
Fig. 3: An example of conventional cheat-prevention VSS scheme 1 [16] on $(2, 3)$-threshold VSS [2]. Image shares and verification image shares are five times larger in width to verification and secret images, i.e., $m + 2 = 5$. The contrast of recovered secret images are $\frac{1}{m+2} = \frac{1}{5}$ (two shares stacked).

$\mathbf{T}^1$, $\mathbf{R}^0$, and $\mathbf{R}^1$ are differently permuted at each pixel of the secret image before generating share images to be more secure.

Figure 3 shows an example of this cheat-prevention VSS scheme [16] when it is applied to $(2, 3)$-threshold VSS [2]. It is shown that participant P_i can see his/her own verification image O_i by stacking V_i and S_j where S_j is the image share from participant P_j. It is also shown that stacking shares shows the secret image.

3.2 Conventional Scheme 2

It was found that cheat-prevention in conventional scheme 1 [16] described in the previous section is breakable when adversaries use complementary verification images [17]. As shown in Eq. (4), verification image share V_i has subpixels in which the first column is '1' for white pixels and subpixels in which the second



(a) Verification image O_1. (b) Verification image O_2. (c) Verification image O_3. (d) Secret image. (e) Fake secret image.

(f) $V_3 + S_3$. (g) $V_3 + F_1$. (h) $V_3 + F_2$. (i) $S_3 + F_1$. (j) $S_3 + F_2$.

Fig. 4: Attack [17] to conventional scheme 1 [16].

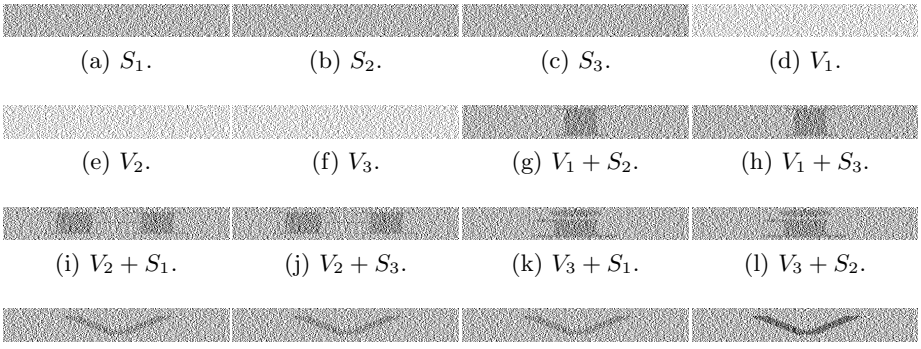
column is '1' for black pixels. All other $(m+1)$ columns are zeros. From this fact, if two complementary verification images are used by two malicious participants, they can fool conventional scheme 1.

A tangible example is given here with three participants P_1, P_2, and P_3 in the conventional scheme 1 on $(2, 3)$-threshold VSS with Eq. (1). It is assumed that P_1 and P_2 are collusive cheaters and P_3 is the victim. Column permutation of $\mathbf{T}^0$, $\mathbf{T}^1$, $\mathbf{R}^0$, and $\mathbf{R}^1$ are omitted here for simplicity, and the permutation does not prevent P_1 and P_2 from deceiving P_3. The attack is illustrated as follow:

Step 1. P_1 and P_2 choose complimentary verification images O_1 and O_2 as shown in Fig. 4 (a) and (b), respectively.
Step 2. Each participant receives the share and verification image shares.
Step 3. P_1 and P_2 stack their verification image shares V_1 and V_2 to determine the positions of the added columns in $\mathbf{R}^0$ and $\mathbf{R}^1$ by focusing the position of '1.' It is easily determined that the first and second columns are added to zero matrices to form $\mathbf{R}^0$ and $\mathbf{R}^1$ as shown in Eq. (4).
Step 4. The basic matrices $\mathbf{T}^0$ and $\mathbf{T}^1$ can be uniquely determined because the first and second rows of $\mathbf{T}^0$ and $\mathbf{T}^1$ which for S_1 and S_2 are known and the positions of the added columns in $\mathbf{T}^0$ and $\mathbf{T}^1$ which are the same as those in $\mathbf{R}^0$ and $\mathbf{R}^1$ are known.
Step 5. Subpixels in S_3 are now determined from the third row of $\mathbf{T}^0$ and $\mathbf{T}^1$.
Step 6. According to the third row of $\mathbf{T}^0$ and $\mathbf{T}^1$ and the positions of added columns, fake share images F_1 and F_2 which for P_1 and P_2, respectively, can be forged.

As shown in Figs. 4 (g) and (h), P_3 confirms own verification image O_3 (shown in Fig. 4 (c)) from $V_3 + F_1$ and $V_3 + F_2$ as from $V_3 + S_3$ shown in Fig. 4 (f). However, $S_3 + F_1$ and $S_3 + F_2$ reveal the fake secret image (shown in Fig. 4 (e)) instead of the secret image (shown in Fig. 4 (d)) as shown in Figs. 4 (i) and (j).

From the fact clarified in the literature [17], another requirement is further introduced to cheat-prevention scheme:



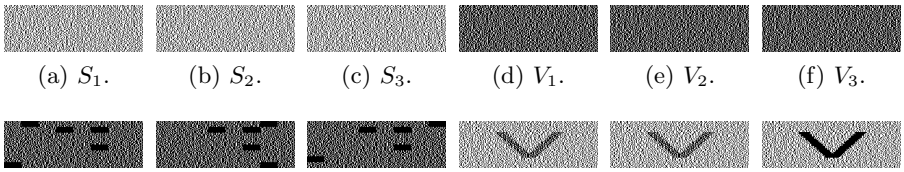
(a) S_1. (b) S_2. (c) S_3. (d) V_1.

(e) V_2. (f) V_3. (g) $V_1 + S_2$. (h) $V_1 + S_3$.

(i) $V_2 + S_1$. (j) $V_2 + S_3$. (k) $V_3 + S_1$. (l) $V_3 + S_2$.

(m) $S_1 + S_2$. (n) $S_2 + S_3$. (o) $S_3 + S_1$. (p) $S_1 + S_2 + S_3$.

Fig. 5: An example of conventional scheme 2 [17] on $(2, 3)$-threshold VSS method [2] with Eq. (1). Pixels in the secret image are expanded to seven subpixles under the condition that foiling up two collusive participants, i.e., $m + (u + 1) + 1 = 3 + 3 + 1 = 7$. The contrast of the recovered secret images are low ($\frac{1}{m + (u + 1) + 1} = \frac{1}{7}$)(two shares stacked).



(a) S_1. (b) S_2. (c) S_3. (d) V_1. (e) V_2. (f) V_3.

(g) $V_1 + S_2$. (h) $V_1 + S_3$. (i) $V_3 + S_2$. (j) $S_1 + S_2$. (k) $S_2 + S_3$. (l) $S_1 + S_2 + S_3$.

Fig. 6: An example of conventional scheme [18] on $(2, 3)$-threshold VSS [18].

Req. 7. Added columns cannot be estimated even collusive cheaters use complimentary verification images.

The literature [17] has proposed a scheme to meet Req.7 where the scheme is referred to as conventional scheme 2 in this paper. In order to foil up u collusive cheaters, $(u + 1)$ of zero columns and one of 1 column, i.e., $(u + 2)$ columns are added to the basic matrices with m-columns. This remedy is considered as increasing the columns of basic matrices, and it is achieved at the cost of higher pixel expansion which is against Reqs. 1 and 2 as shown in Fig. 5, and the literature also points out this problem by itself [17].

3.3 Conventional Scheme 3

A new visual structure called 'black pattern' is introduced to the conventional scheme [18] to prevent cheating between participants. A black pattern is a rectangle filled with black pixels and some black patterns appear by stacking verification image share V_i and share image S_j as shown in Figs. 6 (g), (h), and (i). It is noted that the dealer instead of participants decides the number and positions of black patterns for each participant.

This conventional scheme 3 [18] has two disadvantages: The scheme is only applicable to $(2, n)$-threshold VSS and participants are not allowed to choose their verification images freely. The former does not satisfy Req.6, whereas conventional schemes 1 [16] and 2 [17] meet Req.6. On the latter, this kind of limitation can prevent collusive cheaters from estimating added columns even in conventional scheme 1 [16]; Cheaters cannot choose complimentary verification images freely under such limitation.

The next section proposes a new cheat-prevention VSS scheme which overcomes the problems: Req. 7 is not satisfied (in conventional scheme [16]) and Req. 1 is not satisfied (in conventional scheme 2 [17]). In addition, the proposed scheme is applicable to (k, n)-threshold VSS.

4 Proposed Scheme

This section gives details of the proposed scheme in which randomness is introduced to share generation instead of increasing the number of columns of basic matrices for meeting Req. 7; preventing cheaters with complimentary verification images from estimating added columns. Let $\mathbf{S}^0$ and $\mathbf{S}^1$ be the $n \times m$-sized basic matrices for share generation in a black-and-white VSS method in which each participant P_i holds share image S_i where $i = 1, 2, \ldots, n$ and a pixel in a secret image is expanded to m subpixels in a share image.

4.1 Algorithm

Firstly, the proposed scheme creates four $n \times (m + 2)$-sized basic matrices $\mathbf{T}^0$, $\mathbf{T}^1$, $\mathbf{R}^0$, and $\mathbf{R}^1$ as the same as conventional scheme 1 [16], i.e., as Eqs. (3) and (4). In addition, participant-dependent $(m+2)$-length row vector $\mathbf{r}_i^0$ is obtained from $\mathbf{t}_i^0$ which is the i-th row of $\mathbf{T}^0$ where $i = \{1, 2, \ldots, n\}$;

$$\mathbf{t}_i^0 = \left[\, 1\ 0 \middle| \mathbf{s}_i^0 \,\right], \tag{5}$$

where $\mathbf{s}_i^0$ is the i-th row of $\mathbf{S}^0$. With the assumption that the number of 1's in $\mathbf{s}_i^0$ is l where $0 < l < m$, the number of 1's in $\mathbf{t}_i^0$ is $(l + 1)$. One 1 is randomly chosen from $(l + 1)$ of 1's, and l of 1's are set to zero to obtain new $(m + 2)$-length row vector $\mathbf{r}_i^0$ which contains exact one 1 at each pixel of the verification image.

Then, $\mathbf{T}^0$ and $\mathbf{T}^1$ are used for generating share images S_i as in the conventional schemes [16, 17]. In contrast, according to the pixel value of secret and

verification images, verification image share generation can be divided into 4 cases as,

Case 1. The focal pixel in the secret and verification images are black.
Case 2. The focal pixel in the secret and verification images are black and white, respectively.
Case 3. The focal pixel in the secret and verification images are white and black, respectively.
Case 4. The focal pixel in the secret and verification images are white.

Each $(m+2)$-length subpixels in verification image share V_i are generated as follows:

Cases 1, 2, or 3 Use $\mathbf{R}^0$ and $\mathbf{R}^1$ as in the conventional scheme 1 [16]. That is, put the i-th row of $\mathbf{R}^0$ and $\mathbf{R}^1$ to V_i as $(m+2)$-length subpixels, for white and black pixels in verification image O_i, respectively.
Case 4 Put participant-dependent row vector $\mathbf{r}_i^0$ to V_i as $(m+2)$-length subpixels.

4.2 Example

A tangible example of the proposed scheme is given by using $(2,3)$-threshold VSS method with Eq. (1). Then, from Eqs. (1) and (3), $\mathbf{T}^0$ is given as

$$\mathbf{T}^0 = \left[\begin{array}{c|c} 10 & \\ \vdots & \mathbf{S}^0 \\ 10 & \end{array}\right] = \begin{bmatrix} 1\,0\,1\,0\,0 \\ 1\,0\,1\,0\,0 \\ 1\,0\,1\,0\,0 \end{bmatrix}, \tag{6}$$

and $\mathbf{t}_i^0 = [1\ \ 0\ \ 1\ \ 0\ \ 0]$ regardless of i. The proposed scheme randomly replaces 1's in $\mathbf{t}_i^0$ with 0 to generate participant-dependent row vector $\mathbf{r}_i^0$:

$$\mathbf{r}_i^0 = \begin{bmatrix} 1\,0\,0\,0\,0 \end{bmatrix} \quad \text{or} \quad \mathbf{r}_i^0 = \begin{bmatrix} 0\,0\,1\,0\,0 \end{bmatrix}. \tag{7}$$

When malicious participants try to attack the proposed scheme based on the description in Section 3.2, i.e., with complementary verification images, expanded subpixels in stacked verification image shares of malicious participants are either $[1\ \ 1\ \ 0\ \ 0\ \ 0]$ or $[0\ \ 1\ \ 1\ \ 0\ \ 0]$. So, it is impossible to identify the position of added columns exactly in the proposed scheme.

4.3 Discussion

This section discusses the pixel expansion efficiency and decrypt-able randomness of the proposed scheme.

Minimum Pixel Expansion Assume that w columns are added to $n \times m$-sized base matrices of VSS method to create two $n \times (m + w)$-sized base matrices in a cheat-prevention VSS scheme where $w \geq 1$.

To meet Req. 1, it is desired that $w = 1$, and the size of pixel expansion is $m+w = m+1$. Then, the added column must be a zero vector, because stacking verification image share V_i and share image S_j ($V_i + S_j$) should become either black or white where $1 \leq i, j \leq n$ and $i \neq j$. On the other hand, if the added column consists of one, a white pixel of verification image O_i becomes black when V_i and S_j are stacked.

When $w = 1$, a black pixel of O_i is expanded to $(m + 1)$-length subpixels consisting of one of 1 and m of zeros in verification image share V_i and a white pixel of O_i is expanded to subpixels compounded of $(m+1)$ of zeros in V_i. That is, V_i leaks O_i without stacking with S_j. It goes against Req. 5. So, the number of added columns are at least two, i.e., $w \geq 2$.

From this perspective, the proposed scheme which adds two columns to $n \times m$-sized basic matrices achieves the minimum pixel expansion, i.e., the proposed scheme satisfies Req. 1. So, the proposed scheme overcomes the problem in conventional scheme 2 [17] (Note that the minimum pixel expansion is achieved in the field where participants can choose their verification images freely).

Decrypt-Able Randomness As discussed in Section 4.3, the most efficient pixel expansion is to add 2 columns to $n \times m$-sized basic matrices. It is assumed again that Eq. (1) is used, then, from Eqs. (3) and (4), $\mathbf{T}^0$, $\mathbf{T}^1$, $\mathbf{R}^0$, and $\mathbf{R}^1$ are as follows:

$$\mathbf{T}^0 = \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{array}\right], \qquad \mathbf{T}^1 = \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{array}\right], \tag{8}$$

$$\mathbf{R}^0 = \left[\begin{array}{cc|ccc} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{array}\right], \qquad \mathbf{R}^1 = \left[\begin{array}{cc|ccc} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{array}\right]. \tag{9}$$

In conventional scheme 1 [16], it is easy to tell that the proportion of white pixels to black pixels is 3/2 in each 5-length subpixels in $V_i + S_j$, if the corresponding pixel in O_i is white. In contrast, the proportion is 2/3, if the corresponding pixel in O_i is black. Note that the proportion doesn't change even a column permutation is applied to matrices.

In case 4 which is defined in Section 4.1, 5-length subpixels in V_i are [1 0 | 0 0 0], those in S_j [1 0 | 1 0 0], and thus $V_i + S_j$ becomes [1 0 | 1 0 0] in conventional scheme 1 [16] where $i \neq j$. Meanwhile, $\mathbf{r}_i^0$ could be either [1 0 | 0 0 0] or [0 0 | 1 0 0] in the proposed scheme by introducing randomness, even the promotion of white pixels to black pixels in 5-length subpixels in $V_i + S_j$ is 2/3, i.e., it is decrypt-able even randomness is introduced. For other cases, randomness could change the proportion, and it is the reason that randomness is introduced only to case 4.

As the key point of the attack to conventional scheme 1 [16] is to determine the position of added columns [17], the proposed scheme introduces randomness in generating verification image shares to make the accurate estimation of the added columns impossible, i.e., the proposed scheme meets Req. 7. Thus, the proposed scheme overcomes the problem in conventional scheme 1 [16].

Accidental Unveiling of Added Columns Though it is quite difficult, there is a possibility that random guessing gives the correct estimation of the positions of added columns in the proposed scheme and even in conventional scheme 2 [17]. It is assumed here that verification and secret images randomly consist of equiprobable white and black pixels. The proposed scheme introduces randomness to Case 4, and in Case 4 in $(2,3)$-threshold VSS, which was discussed in Section 4.2, the possibility of correct guessing of added columns becomes $1/2$. So, for a $X \times Y$-sized image, the possibility of correctly guessing all positions of added pixels is $\left(\frac{1}{2}\right)^{\frac{XY}{4}}$. Similarly, that in conventional scheme 2 [17] is $\left(\frac{1}{18}\right)^{\frac{XY}{2}}$.

Based on this possibility, the proposed scheme is inferior to conventional scheme 2 [17]. The proposed scheme, however, is superior in the contrast of decrypted images to conventional scheme 2. This situation is the same as that slightly weakening the security could be a choice to improve the visual contrast in VSS [11, 12].

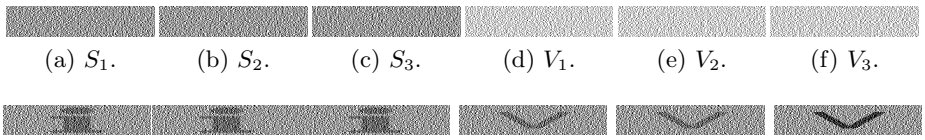
4.4 Features

The features of the proposed scheme are summarized here.

Cheat-Prevention Functionality Improvement The problem of conventional scheme 1 [16] is due to all rows in $\mathbf{R}^0$ are the same and simultaneously all rows in $\mathbf{R}^1$ are the same. That is, all participants receive verification image share V_i's in which subpixels corresponding to black pixels in verification image O_i are the same regardless of participant and simultaneously subpixels corresponding to white pixels in O_i are the same regardless of participant. This fact allows malicious participants to collude for deceiving an honest participant by using complementary verification images [17]. Conventional scheme 2 [17] expands pixels much more, whereas the proposed scheme introduces participant-dependent subpixels to V_i's. Both strategies prevent malicious participants from estimating $\mathbf{R}^0$ and $\mathbf{R}^1$, i.e., from deceiving an honest participant as well.

Consequently, the proposed scheme is superior in the cheat-prevention functionality to conventional scheme 1 [16].

Improvement in Pixel Expansion and Contrast of Recovered Images The problem of conventional scheme 2 [17] is due to increasing zero columns to prevent malicious participants from deceiving an honest participant, c.f., Figs. 3 and 5. On the other hand, the proposed scheme simply introduces randomness to the share generation process. The proposed scheme, thus, keeps the subpixel



(a) S_1. (b) S_2. (c) S_3. (d) V_1. (e) V_2. (f) V_3.

(g) $V_3 + S_1$. (h) $V_3 + S_2$. (i) $V_3 + S_3$. (j) $S_1 + S_2$. (k) $S_2 + S_3$. (l) $S_1 + S_2 + S_3$.

Fig. 7: An example of the proposed scheme on $(2, 3)$-threshold VSS method [2]. The contrast of recovered secret images are $\frac{1}{5}$ (two shares stacked), the same as conventional 1 [16].

size as small as possible and it results in keeping the contrast of the recovered secret image as that in conventional scheme 1 [16]. Although the security is weakened in the proposed scheme than that in the conventional scheme [17], the pixel expansion efficiency and contrast of decrypted images are improved. Other literatures [11, 12] also show that it is a reasonable choice to improve contrast in VSS.

Consequently, the proposed scheme is superior in pixel expansion efficiency to conventional scheme 2 [17].

5 Experimental Results

The proposed scheme is implemented on $(2, 3)$-threshold VSS method in this experiment. Verification images are those shown in Figs. 4 (a), (b), and (c), respectively. The secret and fake secret images are those shown in Figs. 4 (d) and (e), respectively.

Figures 7 (a), (b), and (c) show secret image shares S_1, S_2, and S_3, respectively, and Figs. 7 (d), (e), and (f) are verification image shares V_1, V_2, and V_3, respectively. Figs.7 (g), (h), and (i) are revealed verification images. Figs.7 (j), (k), and (l) are revealed secret images. As added pixels can't be accurately estimated, so it is impossible to generate fake secret share.

6 Conclusions

This paper has improved the visual secret sharing schemes with cheat-prevention. The proposed scheme has better performance than conventional scheme 1 [16] in cheat-prevention functionality and less pixel expansion than conventional scheme 2 [17]. The proposed scheme can be applied to (k, n)-threshold VSS different from a latest scheme [18] which is only suitable for $(2, n)$-threshold VSS. The effectiveness of the proposed scheme has been confirmed through experimental results.

References

1. A. Shamir, "How to share a secret," Commun. ACM, vol.22, pp.612–613, Nov. 1979.
2. M. Naor and A. Shamir, "Visual cryptography," Proc. IACR EUROCRYPT, LNCS, vol.950, pp.1–12, 1994.
3. I. Biehl and S. Wetzel, "Traceable visual cryptography," Proc. Int. Conf. Information Communication Security, LNCS, vol.1334, pp.61–71, 1997.
4. T. Hofmeister, M. Krause, and H.-U. Simon, "Contrast-optimal k out of n secret sharing schemes in visual cryptography," Theoret. Comput. Sci., vol.240, no.2, pp. 471–485, 2000.
5. S. Cimato, R.D. Prisco, and A.D. Santis, "Optimal colored visual cryptography schemes," Designs, Codes and Cryptography, vol.35, pp.311–335, 2005.
6. T. Ishihara and H. Koga, "A visual secret sharing scheme for color images based on meanvalue-color mixing," IEICE Trans. Fundamentals, E86-A, no.1, pp.194–197, 2003.
7. H. Koga and T. Ishihara, "A general method for construction of (t, n)- threshold visual secret sharing schemes for color images," Designs, Codes and Cryptography, vol.61, no.2, pp.223–249, 2011.
8. G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, "Extended capabilities for visual cryptography," Theor. Comput. Sci., vol.250, pp.143–161, Jan. 2001.
9. C.-C. Chang and T.-X. Yu, "Sharing a secret gray image in multiple secret," Proc. International Symposium on Cyber Worlds, pp.1–8, 2002.
10. M. Iwamoto, L. Wang, K. Yoneyama, N. Kunihiro, and K. Ohta, "Visual secret sharing schemes for multiple secret images allowing the rotation of shares," IEICE Trans. Fundamentals, vol.E89, no.5, pp.1382–1395, 2006.
11. M. Iwamoto, "A weak security notion for visual secret sharing schemes," IEEE Trans. Information Forensics and Security, vol.7, no.2, pp.372–382, 2012.
12. M. Iwamoto, "Security notions of visual secret sharing schemes," Proc. IWAIT, pp.95–100, 2013.
13. S. Cimato, A. De Santis, A.L. Ferrara, and B. Masucci, "Ideal contrast visual cryptography schemes with reversing," Inf. Process. Lett., vol.93, no.4, pp.199–206, 2005.
14. P.A. Eisen and D.R. Stinson, "Threshold visual cryptography with specified whiteness levels of reconstructed pixels," Designs, Codes, and Cryptography, vol.25, no.1, pp.15–61, 2002.
15. D.S. Tsai, T.H. Chen, and G. Horng, "A cheating prevention scheme for binary visual cryptography with homogeneous secret images," Pattern Recog., vol.40, no.8, pp. 2356–2366, Aug. 2007.
16. C.M. Hu and W.G. Tzeng, "Cheating prevention in visual cryptography," IEEE Trans. Image Process., vol.16, no.1, pp. 36–45, Jan. 2007.
17. Y.C. Chen, G. Horng, and D.S Tsai, "Comment on 'Cheating Prevention in Visual Cryptography' " IEEE Trans. Image Process., vol.21, no.7, pp.3319–3323, July 2012.
18. Y.C. Chen, D.S Tsai, and G. Horng "A new authentication based cheating prevention scheme in Naor-Shamir's visual cryptography" J. Vis. Commu. Image R., vol.23, pp.1225-1233, Nov. 2012.