3-Out-of-n Cheating Prevention Visual Cryptographic Schemes

Ching-Nung Yang[1], Stelvio Cimato[2], Jihi-Han Wu[1] and Song-Ruei Cai[1]
[1]*Department of Computer Science and Information Engineering, National Dong Hwa University, Hualien, Taiwan*
[2]*Dipartimento di Informatica, Università degli studi di Milano, Crema, Italy*

Keywords: Visual Cryptography, Cheating, Deterministic Cheating, Cheating Prevention.

Abstract: In literature, (2, n) cheating prevention visual cryptographic schemes (CPVCSs) have been proposed, dealing with the case of dishonest participants, called cheaters, who can collude together to force honest participants to reconstruct a wrong secret. While (2, n)-CPVCSs resistant to deterministic cheating have been presented, the problem of defining (k, n)-CPVCS for any k has not been solved. In this paper, we discuss (3, n)-CPVCS, and propose three (3, n)-CPVCSs with different cheating prevention capabilities. To show the effectiveness of the presented (3, n)-CPVCS, some experimental results are discussed as well.

1 INTRODUCTION

The cryptographic technique for the visual sharing of secret images, denoted Visual Cryptography (VC) or Visual Secret Sharing (VSS) was firstly proposed in (Naor and Shamir, 1994). A VC scheme (VCS) is usually implemented as a threshold (k, n) scheme, where a secret image is decomposed into n shadow images (called "*shadows*") which are then distributed to the n participants. Any set of k participants is enabled to reconstruct the secret image by simply stacking together the shadows they own, while (k–1) or fewer participants cannot obtain any secret information. In a (k, n)-VCS, each pixel of the secret image is "expanded" into m subpixels in each shadow, where the value m is called the pixel expansion. Following Naor and Shamir's work, most studies dealt with the pixel expansion of VCS (Cimato et al., 2006; Ito et al., 1999; Kuwakado and Tanaka, 2007; Wang et al., 2011; Yan et al., 2015; Yang, 2004).

A (k, n)-VCS usually consider honest participants, who can provide correct shadows during the reconstruction phase. However, cheating behaviour occurs in VCS, when some dishonest participants, called cheaters, collude together to forge shadows and force honest participants to reconstruct a wrong secret. Several methods (Horng et al., 2006; Hu and Tzeng, 2007; De Prisco and De Santis, 2009; Hu and Tzeng, 2007; Liu et al, 2011; Tsai et al., 2007) have been proposed to face the cheating problem. In (Horng et al., 2006), the problem of (n–1)-colluder cheating has been defined and a (2, n) cheating prevention VCS (CPVCS) has been proposed by using (2, n+l)-VCS instead of (2, n)-VCS. Horng's (2, n)-CPVCS makes (n–1) collusive cheaters harder to predict the structure of the honest participant's shadow, and is immune to deterministic cheating. However, Horng's (2, n)-CPVCS only prevents deterministic cheating for the black secret pixel. De Prisco and De Santis in (De Prisco and De Santis, 2009) extend Horng et al.'s work and propose a new (2, n)-CPVCS, which does not allow deterministic cheating for both black and white colors. A (k, n)-CPVCS for any k still remains unsolved.

In this paper, we study the (n–1)-colluder cheating problem in (k, n)-CPVCS for k=3. Our (3, n)-CPVCS can prevent deterministic cheating for both black color and white color. The rest of the paper is organized as follows. Section 2 introduces (k,n)-VCS and reviews the previous (2, n)-CPVCSs. In Section 3, we propose three (3, n)-CPVCSs with different cheating prevention capabilities. Examples in Section 4 are given to demonstrate the effectiveness of our scheme. Conclusions are drawn in Section 5.

Yang, C-N., Cimato, S., Wu, J-H. and Cai, S-R.
3-Out-of-n Cheating Prevention Visual Cryptographic Schemes.
DOI: 10.5220/0005740504000406
In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, pages 400-406
ISBN: 978-989-758-167-0

2 RELATED WORKS

2.1 (K, *n*)-VCS

In a black-and-white VCS, each pixel is subdivided into *m* subpixels in each of *n* shadows. A *(k, n)*-VCS uses h_1 black subpixels and (m-h_1) white subpixels (denoted as h_1b(m-h_1)w) to represent black and white secret pixels, respectively, where $0 \le h_0 < h_1 \le m$. The values of h_1 and h_0 are the blackness of black color and white color. Let X be a set of involved participants, and $w(v)$ be the Hamming weight of v. Suppose that M is an nxm matrix. The notation $(M|X)$ defines a $|X|xm$ matrix, which selects the rows of the corresponding participants in X from M. With $add(M|X)$ we denote the OR-ed vector of all rows in $(M|X)$, and with $D(M|X)$ we denote a set including all distribution matrices obtained by permuting all the columns in $(M|X)$. The formal definition of a VCS is then given as follows:

Definition 1. A (k, n)-VCS is given by (nxm) black and white base matrices B_1 and B_0 satisfying the following two conditions.

(i) (Contrast condition): Given any qualified set X, where $\|X\|=k$, we have that $w(B_1 \mid X) \ge h_1$ (respectively, $w(B_0 \mid X) \le h_0$), where $0 \le h_0 < h_1 \le m$.
(ii) (Security condition): Given any forbidden set X, where $\|X\|<k$, we have $D(B_1 \mid X)$ and $D(B_0 \mid X)$.

The collection C_1 (respectively, C_0) is obtained by permuting the columns of the corresponding matrix B_1 (respectively, B_0) in all possible ways. When sharing a black (respectively, white) secret pixel, the dealer randomly selects one matrix from C_1 (respectively, C_0) and chooses each row of the matrix to a relative shadow.

To easily describe base matrices of VCS, some notations are introduced. The notation $\mu_{n,i}$ represents a matrix composed of all n-bit columns with Hamming weight i. Obviously, $\mu_{n,i}$ is a matrix, e.g., $\mu_{3,0} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, $\mu_{3,1} = \begin{bmatrix} 100 \\ 010 \\ 001 \end{bmatrix}$, $\mu_{3,2} = \begin{bmatrix} 011 \\ 101 \\ 110 \end{bmatrix}$, and $\mu_{3,3} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$. Let $l\mu_{n,i}$ denote the concatenation of l matrices, i.e., $l\mu_{n,i} = \overbrace{(\mu_{n,i} \| \cdots \| \mu_{n,i})}^{l}$, where $\|$ is the concatenation operation. Also, let $\mu_{n,all} = \mu_{n,0} \| \mu_{n,1} \| \ldots \| \mu_{n,n}$, e.g., $\mu_{3,all} = \mu_{3,0} \| \mu_{3,2} \| \mu_{3,3}$.

2.2 (2, *n*)-CPVCS

In (Horng et al., 2006), authors introduced the problem of (n–1)-colluder cheating in (2, n)-VCS, where (n–1) cheaters collude together to force the honest participant to reconstruct a wrong secret. Consider as an example, the case of (2, 3)-VCS: If two cheaters (say participants P_1 and P_2) collude together, they have S_1 and S_2 and can exactly know the structure of S_3. Then, they can provide fake shadows $\hat{S}_1$ and $\hat{S}_2$, and let P_3 obtain a wrong secret image $\hat{S}$ (i.e., $\hat{S}_1 + S_3 = \hat{S}$ or $\hat{S}_2 + S_3 = \hat{S}$). Horng et al. proposed a (2, n)-CPVCS to make it harder for (n–1) cheaters to predict the structure of the other shadow. They adopted (2, n+l)-VCS, where $l \ge 1$, instead of (2, n)-VCS. Afterwards, the dealer randomly takes only n out of (n+l) shadows and delivers them to n participants. Horng et al.'s approach consists in adding l all-0 columns into the base matrices of (2, n)-VCS (see Construction 5.5 in (De Prisco and De Santis, 2009)). By the notation, the base matrices of Horng et al.'s (2, n)-CPVCS are $B_0 = \mu_{n,n} \| (n+l-1)\mu_{n,0}$ and $B_1 = \mu_{n,1} \| l\mu_{n,0}$.

$$B_0 = \mu_{3,3} \| 2\mu_{3,0} = \begin{bmatrix} 100 \\ 100 \\ 100 \end{bmatrix} \quad (1\text{-}1)$$

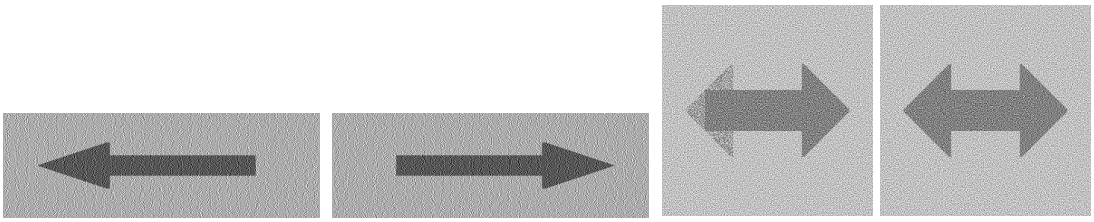
$$B_1 = \mu_{3,1} = \begin{bmatrix} 100 \\ 010 \\ 001 \end{bmatrix} \quad (1\text{-}2)$$

For n=3, base matrices of Naor and Shamir's (2, 3)-VCS and Horng et al.'s (2, 3)-CPVCS are shown in Eq. (1) and Eq. (2), respectively.

$$B_0 = \mu_{3,3} \| 3\mu_{3,0} = \begin{bmatrix} 1000 \\ 1000 \\ 1000 \end{bmatrix} \quad (2\text{-}1)$$

$$B_1 = \mu_{3,1} \| 3\mu_{3,0} = \begin{bmatrix} 1000 \\ 0100 \\ 0010 \end{bmatrix} \quad (2\text{-}2)$$

Suppose that blocks B and W are black and white m-subpixel blocks in shadows. Let $P_{C_1 \to C_2}$ be the probability that cheaters can change the C_1 color block to C_2 color block, where C_1 and $C_2 \in \{B, W\}$. Obviously, from Eq. (1-1), cheaters exactly know the structure of B and W, so that they can apply deterministic cheating on Naor and Shamir's (2, 3)-



(a) $S = S_1 + S_3$ (b) $\hat{S} = \hat{S}_1 + S_3$ (c) $\hat{S} = \hat{S}_1 + S_3$ (d) $\hat{S} = \hat{S}_1 + S_3$

Figure 1: The 2-colluder cheating: (a) no cheating on (2, 3)-VCS (b) cheating on (2, 3)-VCS (c) cheating on (2, 3)-CPVCS (d) cheating on (2, 3)-CPVCS by a left-right arrow faked image.

VCS (i.e., $P_{W\to B} = P_{W\to B} = P_{B\to W} = P_{B\to W} = 1$). For the white secret pixel, from the matrix B_0 in Eq. (1-2), two cheaters P_1 and P_2 can exactly know the structure of W in S_3. Thus, they can change the white block W to be any color block, i.e., $P_{W\to B} = 1$ and $P_{W\to W} = 1$. However, for the black pixel, from the matrix B_1 in Eq. (1-2), cheaters can only identify the location of "1" of B in the shadow S_3 with 50% probability. Therefore, cheaters only have $P_{B\to W} = 0.5$ to modify 2B2W (denotes 2 black subpixels and 2 white subpixels in a block) to 1B3W. In general, for (2, n)-CPVCS, (n–1) cheaters have $P_{B\to W} = 1/(l+1)$.

It is evident that cheaters have the probability $P_{B\to B} = 1$ since they just do not change their subpixels in shadow. The following example shows that 2-colluder cheating can perform deterministic cheating on (2, 3)-VCS, but is not completely effective for 100% in Horng et al.'s (2, 3)-CPVCS.

Example 2 Apply 2-colluder cheating on Naor and Shamir's (2, 3)-VCS and Horng et al.'s (2, 3)-CPVCS.

Consider the case of 2-colluder cheating, where the two cheaters P_1 and P_2 want to fool the honest participant P_3 to get a wrong secret. Suppose that the secret image is a left arrow $\boxed{\leftarrow}$. Fig. 2(a) shows the stacked result of (2, 3)-VCS (say S_1+S_3) without cheating, where a left arrow $\boxed{\leftarrow}$ is correctly recovered. Suppose that two cheaters produce a forged shadow $\hat{S}_1$, and intentionally tamper the secret image from a left arrow $\boxed{\leftarrow}$ to a right arrow $\boxed{\rightarrow}$. Cheating results $\hat{S} = \hat{S}_1 + S_3$ (a right arrow) on (2, 3)-VCS and (2, 3)-CPVCS are shown in Figs. 2(b) and (c). As shown in Fig. 2(b), cheaters can perform deterministic cheating successfully. However, in Fig. 2(c), although cheaters can fake a right arrowhead they cannot remove the left arrowhead completely (note: cheaters can only correctly identify the location of "1" of B in the shadow S_3 with 50% probability). If we adopt a left-right arrow $\boxed{\leftrightarrow}$ as the faked secret image, where the black areas include all black areas of the left arrow, then the cheating is still successful for (2, 3)-CPVCS (see Fig. 2(d)).

In (De Prisco and De Santis, 2009), authors proposed a new (2, n)-CPVCS with base matrices $B_0 = \mu_{n,all} \,||\, \mu_{n,n} \,||\, n\mu_{n,0}$ and $B_1 = \mu_{n,all} \,||\, \mu_{n,1} \,||\, \mu_{n,0}$,which can prevent deterministic cheating for both black and white colors. However, this scheme has a large pixel expansion m=(2^n+n+1). For n=3, De Prisco and De Santis's (2, 3)-CPVCS has the base matrices with m=12, reported in Eqs. (3).

$$B_0 = \mu_{n,all} \left|\left|\mu_{n,n}\right|\right| n\mu_{n,0} = \\ = \begin{bmatrix} 010011011000 \\ 001010111000 \\ 000101111000 \end{bmatrix} \quad (3\text{-}1)$$

$$B_1 = \mu_{n,all} || \mu_{n,1} || n\mu_{n,0} = \begin{bmatrix} 010011011000 \\ 001010110100 \\ 000101110010 \end{bmatrix} \quad (3\text{-}2)$$

The cheating prevention approach proposed by De Prisco and De Santis's (2, 3)-CPVCS is briefly described below. Two cheaters P_1 and P_2 have different ways of performing a cheating attack. In the following we show the most effective cheating attack with the maximum $P_{W\to B}$ and $P_{B\to W}$. By modifying $\begin{bmatrix}1\\1\\1\end{bmatrix}$ and $\begin{bmatrix}0\\0\\0\end{bmatrix}$ in B_0 to $\begin{bmatrix}0\\1\\1\end{bmatrix}$ and $\begin{bmatrix}1\\0\\0\end{bmatrix}$, respectively, the white block 7B5W is changed to the black block 8B4W in $\hat{S}_1 + S_3$. As shown in Eq. (3), from S_1 and S_2, cheaters have the probability 2/3 (see Eq. (4-1)) and 4/5 (see Eq. (4-2)) to correctly select the column $\begin{bmatrix}1\\1\\1\end{bmatrix}$ and $\begin{bmatrix}0\\0\\0\end{bmatrix}$, respectively, where

boldface denotes wrong choices. Finally, the probability $P_{W\to B}$ is 2/3×4/5=8/15.

$$B_0 = \begin{bmatrix}0100\\0010\\0001\end{bmatrix}\begin{bmatrix}\mathbf{1}\\\mathbf{1}\\\mathbf{0}\end{bmatrix}\begin{matrix}10\\01\\11\end{matrix}\begin{bmatrix}1\\1\\1\end{bmatrix}\begin{bmatrix}1\\1\\1\end{bmatrix}\begin{matrix}000\\000\\000\end{matrix} \quad (4\text{-}1)$$

$$B_0 = \left[\begin{bmatrix}0\\0\\0\end{bmatrix}\begin{matrix}10\\01\\00\end{matrix}\begin{bmatrix}\mathbf{0}\\\mathbf{0}\\\mathbf{1}\end{bmatrix}\begin{matrix}11011\\10111\\01111\end{matrix}\begin{bmatrix}0\\0\\0\end{bmatrix}\begin{bmatrix}0\\0\\0\end{bmatrix}\begin{bmatrix}0\\0\\0\end{bmatrix}\right] \quad (4\text{-}2)$$

By the same argument, the most effective cheating way of changing *B* to *W* is modifying $\begin{bmatrix}1\\0\\0\end{bmatrix}$ and $\begin{bmatrix}0\\0\\1\end{bmatrix}$ in B_1 to $\begin{bmatrix}0\\0\\0\end{bmatrix}$ and $\begin{bmatrix}1\\0\\1\end{bmatrix}$, respectively, so that the black. Block 8B4W is changed to the white block 7B5W in $\hat{S}_1 + S_3$.

As shown in Eq. (5), from S_1 and S_2, cheaters have the probability 2/3 (see Eq. (5-1)) and 2/4 (see Eq. (5-2)) to correctly select the column $\begin{bmatrix}1\\0\\0\end{bmatrix}$ and $\begin{bmatrix}0\\0\\1\end{bmatrix}$, respectively, where boldface denotes the wrong choices. Finally, the probability $P_{B\to W}$ is 2/3×2/4=1/3.

$$B_1 = \begin{bmatrix}0\\0\\0\end{bmatrix}\begin{bmatrix}1\\0\\0\end{bmatrix}\begin{matrix}001\\101\\010\end{matrix}\begin{bmatrix}\mathbf{1}\\\mathbf{0}\\\mathbf{1}\end{bmatrix}\begin{matrix}01\\11\\11\end{matrix}\begin{bmatrix}1\\0\\0\end{bmatrix}\begin{matrix}000\\100\\010\end{matrix} \quad (5\text{-}1)$$

$$B_1 = \left[\begin{bmatrix}\mathbf{0}\\\mathbf{0}\\\mathbf{0}\end{bmatrix}\begin{matrix}10\\01\\00\end{matrix}\begin{bmatrix}0\\0\\1\end{bmatrix}\begin{matrix}110110\\101101\\011100\end{matrix}\begin{bmatrix}0\\0\\1\end{bmatrix}\begin{bmatrix}\mathbf{0}\\\mathbf{0}\\\mathbf{0}\end{bmatrix}\right] \quad (5\text{-}2)$$

Readers can found a detailed analysis of the successful probabilities to change the color in (De Prisco and De Santis, 2010). However, the examples above are two cheating ways having maximum $P_{W\to B}$ and $P_{B\to W}$.

Although Horng's (2, 3)-CPVCS does not have the cheating prevention capability for white color, Horng's (2, 3)-CPVCS with *m*=12 (adding 9 all-0 columns) has $P_{B\to W} = 1/9$, that is much lesser than $P_{B\to W} = 1/3$ of De Prisco and De Santis's (2, 3)-CPVCS.

3 THE PROPOSED (3, *n*)-CPVCS

Horng's (2, *n*)-CPVCS adopts a very simple approach by adding *l* all-0 columns, but its cheating prevention capability is only effective for the black secret pixel. And, this will be a problem if the secret image allows meaningful forging by only changing *W* to *B*. De Prisco and De Santis's (2, 3)-CPVCS solves the weakness of Horng's (2, *n*)-CPVCS by using a larger pixel expansion, so that cheaters cannot figure out the shadow of honest participant.

In this paper, we use a well-known Naor and Shamir's (3, *n*) to construct the proposed (3, *n*)-CPVCS. Our scheme has the same cheating prevention capability like De Prisco and De Santis's (2, *n*)-CPVCS that is effective for both black and white colors (i.e., $P_{B\to W} < 1$ and $P_{W\to B} < 1$), and we only adopt the simple approach (adding all-0 columns and all-1 like Horng's (2, *n*)-CPVCS. Naor and Shamir's (3, *n*)-VCS has base matrices $B_0 = \mu_{n,n-1} \| (n-2)\mu_{n,0}$ and $B_1 = \overline{B_0} = \mu_{n,1} \| (n-2)\mu_{n,n}$ For *n*=4, Naor and Shamir's (3, 4)-VCS has the base matrices reported as Eq. (6).

$$B_0 = \mu_{4,3} \| 2\mu_{4,0} = \begin{bmatrix}011100\\101100\\110100\\111000\end{bmatrix} \quad (6\text{-}1)$$

$$B_1 = \mu_{4,1} \| 2\mu_{4,4} = \begin{bmatrix}100011\\010011\\001011\\000111\end{bmatrix} \quad (6\text{-}2)$$

Construction 1. By adding *l* all-0 columns, where *l*≥2, into Naor and Shamir's (3, *n*)-VCS with base matrices B_0 and B_1, we have a (3, *n*)-CPVCS with white and black base matrices $B_0' = (B_0 \| l\mu_{n,0})$ and $B_1' = (B_1 \| l\mu_{n,0})$

Theorem 1. Under the (*n*−1)-colluder cheating, the proposed (3, *n*)-CPVCS from Construction 1 has the probabilities $P_{B\to W} = 2/(l+1)$, and $P_{B\to B} = P_{W\to B} = P_{W\to W} = 1$ *Proof.* Suppose that (*n*−1) cheaters (say participants P_1, P_2, …, and P_{n-1}) collude together to force the honest participant (P_n) to reconstruct a wrong secret. From Construction 1, the base matrices of (3, *n*)-CPVCS are given in Eq. (7).The black and white blocks *B* and *W* in the reconstructed image are (*n*+1)B(*n*+*l* −3)W and *n*B(*n*+*l*−2)W, respectively. For the white secret pixel (see B_0' in Eq. (6)), (*n*−1) cheaters exactly know the locations of "1" and "0" in the other shadow. Thus, cheaters can change the white block *W* to any color block, i.e., $P_{W\to B} = P_{W\to W} = 1$. For the black secret pixel, we obviously have probability $P_{B\to B} = 1$ since cheaters just do not change their subpixels in shadows.

$$B_0' = B_0 \,||\, l\mu_{n,0} = (\mu_{n,n-1} \,||\, (n-2)\mu_{n,0}) \,||\, l\mu_{n,0} = \mu_{n,n-1} \,||\, (n+l-2)\mu_{n,0} = \left[\begin{array}{c|c} \overbrace{01\cdots11}^{n} & \overbrace{0\cdots0}^{n+l-2} \\ 10\cdots11 & 0\cdots0 \\ \vdots\ \ddots\ \vdots & \vdots\ddots\vdots \\ 11\cdots01 & 0\cdots0 \\ 11\cdots10 & 0\cdots0 \end{array}\right] \tag{7-1}$$

$$B_1' = B_1 \,||\, l\mu_{n,0} = (\mu_{n,1} \,||\, (n-2)\mu_{n,n}) \,||\, l\mu_{n,0} = \left[\begin{array}{c|c|c} \overbrace{10\cdots00}^{n} & \overbrace{1\cdots1}^{n-2} & \overbrace{0\cdots0}^{l} \\ 01\cdots00 & 1\cdots1 & 0\cdots0 \\ \vdots\ \ddots\ \vdots & \vdots\ddots\vdots & \vdots\ddots\vdots \\ 00\cdots10 & 1\cdots0 & 0\cdots0 \\ 00\cdots01 & 1\cdots1 & 0\cdots0 \end{array}\right]. \tag{7-2}$$

Cheaters do not exactly know all the locations of "1" and "0", but they do know (n–2) locations of "1" and (n–1) locations of "0" (see B_1' in Eq. (7)). By this observation, cheaters can produce two forged shadows (say $\hat{S}_1$ and $\hat{S}_2$), from the matrix in Eq. (8), where the underlined "0" and "1" denote the known locations to cheaters (the locations of (n-2) "1" and (n-1) "0"). Every one row and every two rows of the matrix in Eq. (7) are indistinguishable in the sense that they contain the same matrices with the same frequency.

$$\begin{bmatrix} \hat{S}_1 \\ \hat{S}_2 \\ S_n \end{bmatrix} = \left[\begin{array}{c|c|c} \overbrace{0\cdots01}^{n-1}\overbrace{\cdots110}^{n-2} & \overbrace{110\cdots0}^{l-1} \\ 0\cdots01\cdots101 & 110\cdots0 \\ \underline{0\cdots01\cdots111} & 100\cdots0 \end{array}\right]. \tag{8}$$

Thus, the honest participant does not know that the shadows $\hat{S}_1$ and $\hat{S}_2$ are fake. In the last (l+1) columns, cheaters do not know the exact location of the single "1" in S_n, and they can only achieve the probabilistic cheating. In the last (l+1) columns, there are C_2^{l+1} possible cheating combinations, and C_1^l of them have nB(n+l–2)W. Cheaters can successfully modify the black block (n+1)B(n–3+l)W to the white block nB(n–2+l)W with the probability $P_{B\to W} = C_1^l / C_2^{l+1} = 2/(l+1)$. This probability is $P_{B\to W}$ =1 for l=1. So, Construction 1 should have the value l≥2. □

Construction 2. By adding l all-1 columns, where l≥2, into Naor and Shamir's (3, n)-VCS with base matrices B_0 and B_1, we have a (3, n)-CPVCS with white and black base matrices $B_0' = (B_0 \,||\, l\mu_{n,n})$ and $B_1' = (B_1 \,||\, l\mu_{n,n})$.

Theorem 2. Under the (n–1)-colluder cheating, the proposed (k, n)-CPVCS from Construction 2 has the probabilities $P_{W\to B} = 2/(l+1)$, and $P_{W\to W} = P_{B\to B} = P_{B\to W} = 1$.

Proof. Naor and Shamir's (3, n)-VCS has base matrix $B_1 = \overline{B}_0$. By the same argument in the proof of Theorem 1, we can prove that cheaters can modify the white block (n+l)B(n–2)W to the black block (n+l+1)B(n–3)W with the probability $P_{W\to B} = 2/(l+1)$, and $P_{W\to W} = P_{B\to B} = P_{B\to W} = 1$.

Construction 3. By adding l_1 all-0 columns and l_2 all-1 columns, where l_1≥2 and l_1≥2, into Naor and Shamir's (3, n)-VCS with base matrices B_0 and B_1, we have a (3, n)-CPVCS with white and black base matrices $B_0' = (B_0 \,||\, l_1\mu_{n,0} \,||\, l_2\mu_{n,n})$ and $B_1' = (B_1 \,||\, l_1\mu_{n,0} \,||\, l_2\mu_{n,n})$.

$$\begin{bmatrix} \hat{S}_1 \\ \hat{S}_2 \\ S_n \end{bmatrix} = \left[\begin{array}{c|c|c} \overbrace{0\cdots01}^{n-1}\overbrace{\cdots110}^{n+l_2-2} & \overbrace{110\cdots0}^{l_1-1} \\ 0\cdots01\cdots101 & 110\cdots0 \\ \underline{0\cdots01\cdots111} & 100\cdots0 \end{array}\right] \tag{9-1}$$

$$\begin{bmatrix} \hat{S}_1 \\ \hat{S}_2 \\ S_n \end{bmatrix} = \left[\begin{array}{c|c|c} \overbrace{1\cdots10}^{n-1}\overbrace{\cdots001}^{n+l_2-2} & \overbrace{001\cdots1}^{l_1-1} \\ 1\cdots10\cdots010 & 001\cdots1 \\ \underline{1\cdots10\cdots000} & 011\cdots1 \end{array}\right]. \tag{9-2}$$

Theorem 3. Under the (n–1)-colluder cheating, the proposed (3, n)-CPVCS from Construction 3 has the probabilities $P_{B\to W} = 2/(l_1+1)$, $P_{W\to B} = 2/(l_2+1)$, and $P_{B\to B} = P_{W\to W} = 1$.

Proof. From the matrix in Eq. (9-1), by the same argument in the proof of Theorem 1, cheaters can modify the black block (n+l_2+1)B(n–3+l_1)W to the white block (n+l_2)B(n–2+l_1)W with $P_{B\to W} = 2/(l_1+1)$, and $P_{B\to B} = 1$. Also, from the matrix in Eq. (9-2), we can prove that cheaters can modify the white block (n+l_2)B(n–2+l_1)W to the

black block $(n+l_2+1)$B$(n-3+l_1)$W with $P_{W\to B}=2/(l_2+1)$, and $P_{W\to W}=1$.

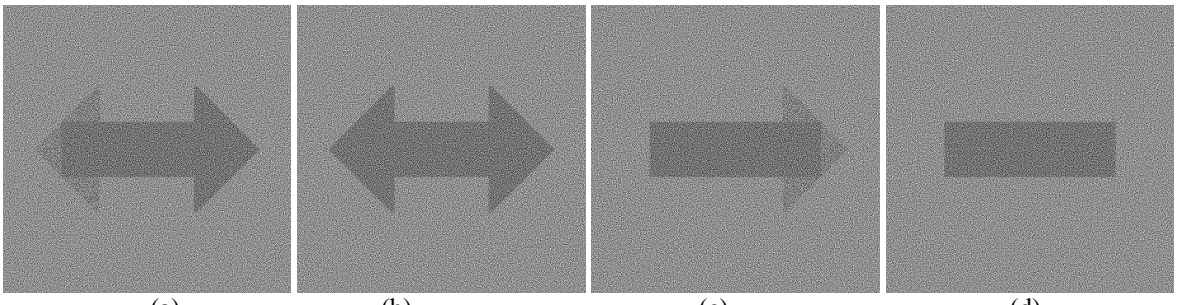
4 EXAMPLES

Construction 1 has the cheating prevention capability against the modifications of the black color to the white color, while Construction 2 has the cheating prevention capability against the modifications of the white color to the black color. Construction 3 has both prevention capabilities of Construction 1 and Construction 2. Two examples are given to test the effectiveness of Constructions 1, 2, and 3. Both examples adopt a left arrow $\boxed{\leftarrow}$ as the secret image. To test different cheating prevention capabilities, we use three fake secret images, a right arrow $\boxed{\rightarrow}$, a left-right arrow $\boxed{\leftrightarrow}$, and a rectangle without arrow $\boxed{-}$. In the right arrow $\boxed{\rightarrow}$, the black (respectively, white) areas do not contain all black (respectively, white) areas in the secret image (the left arrow). The black areas in the left-right arrow $\boxed{\leftrightarrow}$ contain all black areas in the secret image, and the white areas in the rectangle without arrow $\boxed{-}$ contain all white areas in the secret image.

Example 2. Construct the (3, 4)-CPVCSs Construction 1 and Construction 2, respectively.

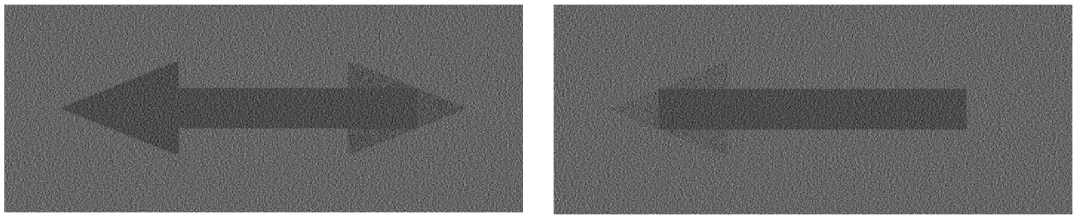
To achieve the invariant aspect ratio, we add 3 (≥2) all-0 columns into Naor and Shamir's (3, 4)-CPVCS to form the (3, 4)-CPVCS with m=9 by Construction 1.

Base matrices are $B_0=\mu_{4,3}\,\|\,5\mu_{4,0}$ and $B_1=\mu_{4,1}\,\|\,2\mu_{4,4}\,\|\,3\mu_{4,0}$. The three colluders (say participants P_1, P_2, and P_3) get their shared pixels from the first three rows in base matrices. Cheaters can produce two forged shadows $\hat{S}_1$ and $\hat{S}_2$ to maliciously modify the black block (5B4W) to the white block (4B5W) by using the matrix $\begin{bmatrix}\hat{S}_1\\ \hat{S}_2\\ S_4\end{bmatrix}=\begin{bmatrix}00010|1100\\ 00001|1100\\ \underline{00011}|1000\end{bmatrix}$, where the underlined positions denote the known locations to cheaters. In the last four columns, cheaters do not know the exact location of the single "1" in S_4, and thus they can only achieve the probabilistic cheating. There are six possible cheating combinations $\begin{bmatrix}1100\\1100\\1000\end{bmatrix}$, $\begin{bmatrix}0011\\0011\\1000\end{bmatrix}$, $\begin{bmatrix}1001\\1001\\1000\end{bmatrix}$, $\begin{bmatrix}0110\\0110\\1000\end{bmatrix}$, $\begin{bmatrix}1010\\1010\\1000\end{bmatrix}$, and $\begin{bmatrix}0101\\0101\\1000\end{bmatrix}$. Cheaters can change the black color (5B3W) to the white color (4B4W) with 3/6=1/2 probability. Fig. 2 shows the cheating results by applying 3-colluder cheating on this scheme. The stacked results $\hat{S}=\hat{S}_1+\hat{S}_2+S_4$ using the right arrow $\boxed{\rightarrow}$ and the left-right arrow $\boxed{\leftrightarrow}$ as secret image, respectively, are shown in Figs. 2(a) and (b). Because Construction 1 only provides the cheating prevention capability against the modification from B to W, it has similar result to Horng et al.'s (2, n)-CPVCS. As shown in Fig. 2(a), we have a lighter residual of the left arrowhead. . However, Fig. 2(b) shows that cheaters can completely fool the honest participant to get the wrong secret, that is a left-right arrow $\boxed{\leftrightarrow}$ (since the black areas in $\boxed{\leftrightarrow}$ contain all black areas in $\boxed{\leftarrow}$). Analyses of (3, 4)-CPVCS with $B_0=\mu_{4,3}\,\|\,2\mu_{4,0}\,\|\,3\mu_{4,4}$ and $B_1=\mu_{4,1}\,\|\,5\mu_{4,4}$ from Construction 2, are the same as the above. Figs. 2 (c) and (d) show the cheating results for using the right



(a) (b) (c) (d)

Figure 2: The 3-colluder cheating on (3, 4)-CPVCS by using the secret image: (a, b) Construction 1 (c, d) Construction 2.



(a) (b)

Figure 3: The 3-colluder cheating on the (3, 4)-CPVCS by using the secret image: (a) Construction 3 using the left-right arrow (b) Construction 3 using the rectangle without arrow.

arrow and the rectangle without arrow as secret images, respectively. As shown in Fig. 2(c), some parts of the right arrowhead still remain. Fig. 2(d) shows that cheaters can fool the honest participant to get the wrong secret $\boxed{—}$, where the white areas contain all the white areas in $\boxed{\leftarrow}$.

Example 3. Construct a (3, 4)-CPVCS by Construction 3.

To achieve the minimum pixel expansion, we add 2 (l_1=2) all-0 columns and 2 (l_2=2) all-1 columns into Naor and Shamir's (3, 4)-CPVCS to form the (3, 4)-CPVCS with m=10. Base matrices are $B_0 = \mu_{4,3} \| 4\mu_{4,0} \| 2\mu_{4,4}$ and $B_1 = \mu_{4,1} \| 4\mu_{4,4} \| 2\mu_{4,0}$. Cheaters can fake two forged shadows $\hat{S}_1$ and $\hat{S}_2$ to maliciously modify the black block (7B3W) to the white block (6B4W) with the probability $P_{B\to W}$=2/3 by using the matrix $\begin{bmatrix} \hat{S}_1 \\ \hat{S}_2 \\ S_4 \end{bmatrix} = \left[\begin{array}{c|c} 0001110 & 110 \\ 0001101 & 110 \\ \underline{0001111} & 100 \end{array}\right]$. Also, this scheme can produce two forged shadows $\hat{S}_1$ and $\hat{S}_2$ to modify the white color (6B4W) to the black color (7B3W) with probability $P_{W\to B}$=2/3 by using the matrix $\begin{bmatrix} \hat{S}_1 \\ \hat{S}_2 \\ S_4 \end{bmatrix} = \left[\begin{array}{c|c} 1110001 & 001 \\ 1110010 & 001 \\ \underline{1110000} & 011 \end{array}\right]$. We use $\boxed{\leftrightarrow}$ and $\boxed{—}$ as secret images, so that the cheating attack in Construction 1 and Construction 2 is successful. Fig. 3 shows that Construction 3 can detect both cheatings.

ACKNOWLEDGEMENT

This work was supported in part by Ministry of Science and Technology, Taiwan, under Grant 104-2918-I-259-001 and 104-2221-E-259-013.

REFERENCES

Cimato, S., De Prisco, R., & De Santis, A. (2006). Probabilistic Visual Cryptography Schemes. *The Computer Journal, 49*(1), 97-107.

De Prisco, R., & De Santis, A. (2009). Cheating Immune Threshold Visual Secret Sharing. *The Computer Journal, 53*(9), 1485-1496.

Horng, G., Chen, T., & Tsai, D. (2006). Cheating in Visual Cryptography. *Design Codes and Cryptography, 38*(2), 219-236.

Hu, C., & Tzeng, W. (2007). Cheating Prevention in Visual Cryptography. *IEEE Transactions on Image Processing, 16*(1), 36-45.

Ito, I., Kuwakado, H., & Tanaka, H. (1999). Image size invariant visual cryptography. *IEICE Transaction on Fundamentals of Electronic communications and Computation Sciences, E82-A*, 2172-2177.

Kuwakado, H., & Tanaka, H. (2007). Size reduced visual secret sharing scheme. *IEICE Transaction on Fundamentals of Electronic communications and Computation Sciences, E87-A*, 1193-1197.

Liu, F., Wu, C., & Lin, X. (2011). Cheating immune visual cryptography scheme. *IET Information Security, 5*, 51-59.

Naor, M., & Shamir, A. (1994). Visual cryptography. *Advances in Cryptology "EUROCRYPT'94". Lecture Notes in Computer Science vol.950*, p. 1-12. Perugia: Springer.

Tsai, D., Chen, T., & Horng. (2007). A cheating prevention scheme for binary visual cryptography with homogeneous secret images. *Pattern Recognition, 40*(8), 2356-2366.

Wang, D., Yi, F., & Li, X. (2011). Probabilistic visual secret sharing schemes for grey-scale images and color images. *Information Sciences, 181*(11), 2189-2208.

Yan, X., Wang, S., Niu, X., & Yang, C. (2015). Generalized random grids-based threshold visual cryptography with meaningful shares. *Signal Processing, 109*, 317-333.

Yang, C. (2004). New visual secret sharing schemes using probabilistic method. *Pattern Recognition Letters, 25*(4), 481-494.