A CHEAT PREVENTING METHOD WITH EFFICIENT PIXEL EXPANSION FOR NAOR-SHAMIR'S VISUAL CRYPTOGRAPHY

Shenchuan LIU[*]*, Masaaki FUJIYOSHI, and Hitoshi KIYA*

Department of Information and Communication Systems, Tokyo Metropolitan University
6–6 Asahigaoka, Hino-shi, Tokyo 191–0065, Japan

ABSTRACT

This paper proposes a cheat-prevention method of visual cryptography (VC) for binary images. A VC technique encrypts a secret image into images referred to as shares so that stacking sufficient shares recovers the secret image, where shares are kept by different parties. The proposed method prevents malicious parties from deceiving an honest party, i.e., from cheating the honest party. To fight cheating, no further pixel expansion is introduced to the proposed method, so this method improves the contrast of recovered secret image and cheat-prevention functionality.

Index Terms**—** Visual Secret Sharing, Authentication, Cheating prevention

1. INTRODUCTION

A secret share (SS) technique [1] splits a secret into n shares. n shares are held by different parties and the secret can be recovered if and only if k or more shares are gathered. This technique is called the (k,n)-threshold SS technique, and it is useful for secure cloud storage [2–4]. Though computer technology is highly developed, computers are not available in anytime at anywhere. Visual SS or visual cryptography (VC) was proposed to overcome this situation where decryption can be done by the human visual system [5]. The first VC scheme has been proposed for binary images [5].

As decryption can be done visually, the contrast of the revealed secret image is very important in VC [6–9], and minimum pixel expansion is usually applied in most VC schemes to enhance the contrast. This leads to a scenario that malicious parties deceive an honest party, and cheat-prevention VC methods have been proposed to fight it [10–15]. This paper focuses on the cheat-prevention VC.

A literature [12] found that the original cheat preventing VC method [11] fails for some attacks. The literature [12] also proposed a new method to fight those attacks, but pixel expansion is sacrificed significantly. Later, another method with less expansion was proposed by the same authors [13], but it introduces a further restriction and it also has a security problem. The latest method [14, 15] introduces randomness into generating image shares to achieve better cheat-prevention results, however, further columns addition is still needed.

Table 1. Notations in this paper.

Symbol	Meaning	Symbol	Meaning
S	secret image	P_i	i-th party
F	fake secret image	S_i	secret image share for P_i
F_i	fake secret image share for P_i	V^i	verification image of P_i
V_i	verification image share of P_i	m	pixel expansion
α	contrast of revealed S	β	contrast of revealed V^i
$\mathbf{S}^0$	basic matrix for a white pixel	$+$	stacking two images
$\mathbf{S}^1$	basic matrix for a black pixel	i	$\{1,2,\ldots,n\}$

This paper proposes a new $(3,n)$-threshold cheat-prevention VC method which solves the problem in the original cheat preventing VC method [11]. It simultaneously improves the contrast of recovered images in comparison with the conventional methods [11, 12, 14, 15]. In addition, the proposed method finds a problem in the conventional method [13] which leads to a new requirement for cheat preventing VC.

2. PRELIMINARIES

2.1. Visual Cryptography

Table 1 shows some notations in this paper. VC is achieved by generating n shares as n images. In general, a VC scheme is expected to meet the following requirements.

Req. 1. Pixel expansion m should be as small as possible.

Req. 2. Contrast α is not significantly reduced.

For example, in the original (k,n)-threshold VC scheme [5] where a pixel in S 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 $k = 2$, where 0 and 1 in Eq. (1) are white and black, respectively. Let $\mathbf{s}_i^p$ be the i-th row of $\mathbf{S}^p$ where $p \in \{0,1\}$, then one pixel in S is expanded as $\mathbf{s}_i^p$ in S_i. Contrast of the recovered image is $\alpha = 1/3$ [1]. Here,

[*] The author is currently with HiSilicon Technologies Co., Ltd.

[1] When the pixel in S is p, let N_p^0 and N_p^1 be the number of white and black subpixels in m subpixels, respectively, then stacking the corresponding

978-1-4799-5751-4/14/$31.00 ©2014 IEEE

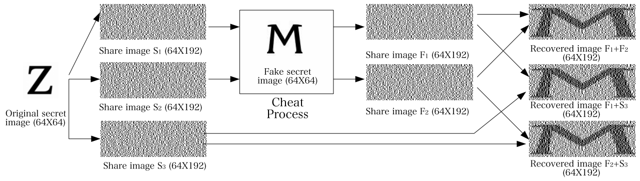

Z
Original secret image (64X64)
Share image S1 (64X192)
Share image S2 (64X192)
Share image S3 (64X192)
M
Fake secret image (64X64)
Cheat Process
Share image F1 (64X192)
Share image F2 (64X192)
Recovered image F1+F2 (64X192)
Recovered image F1+S3 (64X192)
Recovered image F2+S3 (64X192)

Fig. 1. Two malicious parties collude to deceive the other honest party in the $(2,3)$-threshold VC scheme with $m = 3$.

two parties collude, matrices $\mathbf{S}^0$ and $\mathbf{S}^1$ can be easily estimated [11]. Now, colluded two parties know $\mathbf{S}^0$ and $\mathbf{S}^1$, and they can generate fake shares F_i's to deceive the other party. In this cheating scenario, fake secret image F is revealed by stacking the fake shares and the share (shares) from honest party (parties) as shown in Fig. 1.

The more subpixels are expanded in the VC scheme, the harder the cheat becomes. For example, in the $(2,3)$-threshold VC scheme with $m = 4$, $\mathbf{S}^0$ and $\mathbf{S}^1$ are given as

$$\mathbf{S}^0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \text{and} \quad \mathbf{S}^1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \qquad (2)$$

When two parties are collusive to cheat, $\mathbf{S}^0$ can be revealed, but $\mathbf{S}^1$ cannot be exactly estimated, i.e., the cheat becomes harder. However, increasing m usually makes α lower.

It is summarized [11] that an efficient and robust cheat-prevention method should have the following properties in addition to Reqs. 1 and 2.

Req. 3. P_i verifies S_j $(i \neq j)$ by confirming $V_i + S_j$ reveals V^i.

Req. 4. V^i is different and confidential.

Req. 5. Contrast β is not significantly reduced.

3. CONVENTIONAL CHEAT-PREVENTION VISUAL CRYPTOGRAPHY

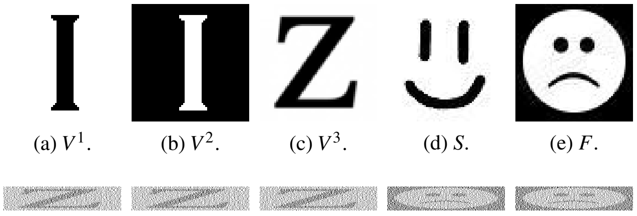
3.1. Conventional Method 1

This method [11] firstly creates two $n \times (m+2)$-sized basic matrices $\mathbf{T}^0$, $\mathbf{T}^1$ and two $1 \times (m+2)$-sized basic matrices $\mathbf{R}^0$, $\mathbf{R}^1$ by adding two columns as

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

$$\mathbf{R}^0 = \left[\, 10 \mid 0\ldots0 \,\right], \mathbf{R}^1 = \left[\, 01 \mid 0\ldots0 \,\right]. \qquad (4)$$

This method generates S_i and V_i as follows:


(a) V^1. (b) V^2. (c) V^3. (d) S. (e) F.

(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. 2. Attack [12] to conventional method 1 [11] ((a)-(e): 64×64 pixels and (f)-(j): 64×320 pixels, i.e., $m + 2 = 5$).

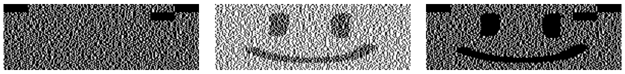

(a) $V_2 + S_1$. (b) $S_1 + S_2$. (c) $V_2 + S_2$.

Fig. 3. An example of conventional method 3 [13] on $(2,3)$-threshold VC (64×192 pixels, i.e., $m = 3$).

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

All columns in $\mathbf{T}^0$, $\mathbf{T}^1$, $\mathbf{R}^0$, and $\mathbf{R}^1$ are differently permuted at each pixel of S before generating S_i and V_i.

3.2. Conventional Method 2

Conventional method 1 [11] is breakable by estimation of added two columns when adversaries use complementary verification images [12]. In Figs. 2 (g) and (h), P_3 confirms V^3 (shown in Fig. 2 (c)) in $V_3 + F_1$ and $V_3 + F_2$ as from $V_3 + S_3$ shown in Fig. 2 (f). However, as shown in Figs. 2 (i) and (j), $S_3 + F_1$ and $S_3 + F_2$ reveal the fake secret image shown in Fig. 2 (e) instead of the secret image shown in Fig. 2 (d).

The literature [12] has proposed a method to overcome the above problem. 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, and the literature also points out this problem by itself [12].

3.3. Conventional Method 3

A new visual structure called 'black pattern' is introduced to conventional method 3 [13] to prevent cheating between parties. A black pattern is a rectangle consisting of black subpixels as shown in Fig. 3 (a). It is noted that the dealer instead of parties decides the number and positions of black patterns for each party.

subpixels in S_i and S_j $(i \neq j)$ gives $N_0^0 = 2$, $N_0^1 = 1$, $N_1^0 = 1$, and $N_1^1 = 2$. Contrast α is defined as

$$\alpha = \frac{N_0^0 - N_1^0}{m} = \frac{N_1^1 - N_0^1}{m}.$$

978-1-4799-5751-4/14/$31.00 ©2014 IEEE

This method has some questionable points. First, if parties cannot choose their own V^i freely, then conventional method 1 [11] will not have secure risk at all. Because the attack [12] is successful based on the fact that parties can choose their own verification images freely. Secondly, as white pixels and black pixels in V^i are applied to different V_i generating mechanisms, the 'black pattern' cannot cross white regions and black regions. This results in undesired information leakage of S to P_i that the edge of S will be perceived when $S_i + V_i$ as shown in Fig. 3 (c). So, a cheating prevention should also meet the following requirement,

Req. 6. $S_i + V_i$ will reflect no information about S.

3.4. Conventional Method 4

In conventional method 4 [14,15], four basic matrices $\mathbf{T}^0$, $\mathbf{T}^1$, $\mathbf{R}^0$, and $\mathbf{R}^1$ are created as in conventional method 1 [11]. In addition, party-dependent $(m+2)$-length row vector $\mathbf{r}_i^0$ is obtained from $\mathbf{t}_i^0$ which is the i-th row of $\mathbf{T}^0$; $\mathbf{t}_i^0 = \begin{bmatrix} 1 & 0 \mid \mathbf{s}_i^0 \end{bmatrix}$, 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 $N_0^1 = l$ 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.

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

- When the focal pixels in S and V^i are both white, put party-dependent row vector $\mathbf{r}_i^0$ to V_i.
- Otherwise, put the i-th row of $\mathbf{R}^0$ and $\mathbf{R}^1$ to V_i, for white and black pixels in verification image V^i, respectively, as well as conventional method 1 [11].

Even this method is attractive, there is room to reduce the pixel expansion and to improve α and β.

4. PROPOSED METHOD

As the same as Noar-Shamir's $(3,n)$-threshold VC [5], $\mathbf{S}^0$ and $\mathbf{S}^1$ in the proposed method are as follows,

$$\mathbf{S}^0 = \left[\underbrace{\begin{matrix} 0 & \cdots & 0 \\ 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{matrix}}_{n-2} \middle| \underbrace{\begin{matrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{matrix}}_{n} \right], \tag{5}$$

$$\mathbf{S}^1 = \left[\underbrace{\begin{matrix} 1 & \cdots & 1 \\ 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{matrix}}_{n-2} \middle| \underbrace{\begin{matrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{matrix}}_{n} \right]. \tag{6}$$

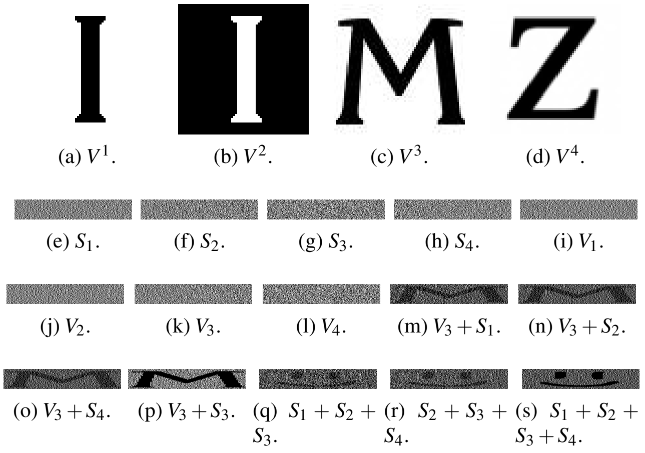

(a) V^1. (b) V^2. (c) V^3. (d) V^4.
(e) S_1. (f) S_2. (g) S_3. (h) S_4. (i) V_1.
(j) V_2. (k) V_3. (l) V_4. (m) $V_3 + S_1$. (n) $V_3 + S_2$.
(o) $V_3 + S_4$. (p) $V_3 + S_3$. (q) $S_1 + S_2 + S_3$. (r) $S_2 + S_3 + S_4$. (s) $S_1 + S_2 + S_3 + S_4$.

Fig. 4. An example of the proposed method on $(3,4)$-threshold VC scheme [5] ((a)-(d): 64×64 pixels and (e)-(s): 64×384 pixels, i.e., $n = 4$ and $m = 2n - 2 = 6$).

So, one pixel in S is expanded as $\mathbf{s}_i^p$ in the proposed method as well as the ordinary $(3,n)$-threshold VC.

In addition, in the proposed method, $(2n-2)$-length subpixels in V_i are generated as follows:

- When the focal pixel in V^i is black, put party-dependent row vector $(1 \oplus \mathbf{s}_i^p)$ to V_i as $(2n-2)$-length subpixels.
- When the focal pixel in V^i is white, put party-dependent row vector $\mathbf{s}_i^p$ to V_i as $(2n-2)$-length subpixels.

It is noted that $\oplus$ is the element-wise exclusive-or operator.

Features of the proposed method are discussed in the next section with experimental results.

5. EXPERIMENTAL RESULTS AND DISCUSSIONS

5.1. Experimental Results

The proposed method is implemented on the $(3,4)$-threshold VC. Verification images V^i are those shown in Figs. 4 (a), (b), (c), and (d). Secret image S is the same as shown in Fig. 2 (d). Figures 4 (e), (f), (g), and (h) show secret image shares S_1, S_2, S_3, and S_4, respectively, and Figs. 4 (i), (j), (k), and (l) are verification image shares V_1, V_2, V_3, and V_4, respectively. No information is given from these image shares or verification image shares. Figures 4 (m), (n), and (o) are revealed verification images. Verification image V^3 for party P_3 can be recognized in these images. Figures 4 (q), (r), and (s) are revealed secret images. Secret image S shown in Fig. 2 (d) appears in these images. In contrast, it is shown in Fig. 4 (p) that no information about S is reflected, that is, Req. 6 is also satisfied in the proposed method.

As no added pixels are introduced in the proposed method, attack based on estimating added pixels [12] will all fail.

Table 2. Characteristics summarization of proposed and conventional methods (applicable VC type, pixel expansion, contrasts (α & β), and security). Contrast α here shows the contrast of stacking three shares of $(3,n)$-threshold scheme.

	Type	Pixel Expansion	Contrast α	Contrast β	Security
Conventional Method 1 [11]	(k,n)	$m+2$	$\frac{1}{m+2}$	$\frac{1}{m+2}$	X
Conventional Method 2 [12]	(k,n)	$\geq (m+2)$	$\leq \frac{1}{m+2}$	$\leq \frac{1}{m+2}$	O
Conventional Method 3 [13]	$(2,n)$	m	$\frac{2}{m}$	$\frac{1}{m}$	X
Conventional Method 4 [14, 15]	(k,n)	$m+2$	$\frac{1}{m+2}$	$\frac{1}{m+2}$	O
Proposed Method	$(3,n)$	m	$\frac{1}{m}$	$\frac{m-4}{2m}$	O

5.2. Discussion

Table 2 summarizes the characteristics of the proposed and conventional [11–15] methods. Applicable VC type, pixel expansion m, contrast of revealed secret image α, contrast of revealed verification image β, and security are discussed in the following subsections.

5.2.1. Applicable VC Type

Conventional methods 1 [11], 2 [12], and 4 [14, 15] can be applied to (k,n)-threshold VC. Conventional method 3 [13] can be applied to $(2,n)$-threshold VC. The proposed scheme can be applied to $(3,n)$-threshold VC. Cheat prevention VC method without further pixel expansion which is applicable to (k,n)-threshold VC is currently unavailable to the best of authors' knowledge.

5.2.2. Pixel Expansion

In conventional methods 1 [11], 2 [12], and 4 [14, 15], added columns are needed. So, pixel expansions are larger than m which is required by VC [5]. But in conventional method 3 [13] and the proposed method, no added columns are introduced, so the pixel expansion remain as the same as m. It is noted that for $(3,n)$-threshold scheme ($n \geq 4$), the minimum pixel expansion is $m = 2n-2$.

5.2.3. Contrasts α and β

Because no columns are added to the basic matrices in the proposed method, the contrast of revealed secret image, α, is the same as Naor-Shamir's original VC. As shown in Table 2, α in the proposed method is larger than that in conventional methods 1 [11], 2 [12], and 4 [14, 15].

The i-th row of $\mathbf{S}^p$ represented by $\mathbf{s}_i^p$ contains $(n-1)$ black subpixels and $(n-1)$ white subpixels as shown in Eqs. (5) and (6). If the pixel in V^i is white, the pixel is expanded as $\mathbf{s}_i^p$ in V_i as described in Section 4. Thus, stacking the corresponding subpixels in V_i and S_j equals to stacking two different rows i and j in $\mathbf{S}^0$ or $\mathbf{S}^1$, which are $\mathbf{s}_i^p$ and $\mathbf{s}_j^p$ $(i \neq j)$, because a pixel in S is expanded as $\mathbf{s}_j^p$ as described in Section 4. So it is obvious that the result will be n black subpixels and $(n-2)$ white subpixels, c.f., Eqs. (5) and (6). Similarly, if the pixel in V^i is black, stacking the corresponding subpixels in V_i and S_j equals to stacking $\left(1 \oplus \mathbf{s}_i^p\right)$ and $\mathbf{s}_j^p$ $(i \neq j)$, so the result always will be $(2n-3)$ black pixels and 1 white pixel. Thus, the contrast of revealed verification image, β, is $\dfrac{(n-2)-1}{m} = \dfrac{(2n-3)-n}{m} = \dfrac{m-4}{2m}$, since $m = 2n-2$ as mentioned in Section 5.2.2.

For the $(3,n)$-threshold scheme, the largest contrast in conventional methods 1, 2, and 4 are all 1/10, however in the proposed method, the minimum contrast α is 1/6 which is always larger than $1/10$. Furthermore, $m \to \infty$, $\beta \to 0$ in conventional methods 1, 2, and 4, but in the proposed method, $m \to \infty$, $\beta \to \frac{1}{2}$. It is trivial that the contrast of stacking S_i and V_i is 1/2 in the proposed method. Consequently, the contrast of revealed verification image, β, in the proposed method is better than that in conventional methods 1, 2, and 4.

5.2.4. Security

As it is discussed in conventional method 4 [14,15], for a $X \times Y$-sized image, the possibility of accidental correctly guessing all positions of added pixels in conventional methods 2 [12] and 4 [14,15] are $\left(\frac{1}{18}\right)^{\frac{XY}{2}}$ and $\left(\frac{1}{2}\right)^{\frac{XY}{4}}$, respectively. In conventional method 1 [11], estimation of added subpixels will always be 100% successful [12] as demonstrated in Section 3.2. As shown in Fig. 3 (c), stacking one's own V_i and S_i will reflect S, so conventional method 3 [13] is not secure.

In the proposed method, accidental guessing all positions of V_i is $\left(\frac{1}{2}\right)^{XY}$, this possibility is higher than that in conventional method 2 [12], but less than that in conventional method 4 [14,15]. As discussed in [6,7], in order to enhance α, it is a considerable way to weaken the security.

Our contributions include:

- Exploration of the problem of conventional method 3 [13] which leads to a new requirement when cheat-prevention VC is constructed.
- Proposal of $(3,n)$-threshold cheating prevention VC method without further pixel expansion.

6. CONCLUSIONS

This paper has proposed a novel VC method with cheat-prevention. The proposed method introduces no added pixels and improves the contrast of revealed verification image dramatically. The proposed method is the first cheat-prevention without extra pixel expansion while satisfying Reqs. 1–6.

Further works include detailed analysis of the proposed method and developing a cheat-preventing method without extra pixel expansion for (k,n)-threshold VC schemes.

REFERENCES

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

[2] T. Ermakova and B. Fabian, "Secret sharing for health data in multi-provider clouds," in *Proc. IEEE CBI*, 2013, pp.93–100.

[3] S. Takahashi and K. Iwamura, "Secret sharing scheme suitable for cloud computing," in *Proc. IEEE AINA*, 2013, pp.530–537.

[4] M. Nojoumian and D.R. Stinson, "Social secret sharing in cloud computing using a new trust function," in *Proc. IEEE PST*, 2012, pp.161–167.

[5] M. Naor and A. Shamir, "Visual cryptography," in *Proc. IACR EUROCRYPT*, LNCS, vol.950, 1994, pp.1–12.

[6] M. Iwamoto, "A weak security notion for visual secret sharing schemes," *IEEE Trans. Info. Forensics and Security,* vol.7, pp.372–382, Apr. 2012.

[7] M. Iwamoto, "Security notions of visual secret sharing schemes," in *Proc. IEICE/ITE/KSBE IWAIT*, 2013, pp.95–100.

[8] S. Cimato, A. De Santis, A.L. Ferrara, and B. Masucci, "Ideal contrast visual cryptography schemes with reversing," *Inf. Process. Lett.*, vol.93, pp.199–206, Feb. 2005.

[9] P.A. Eisen and D.R. Stinson, "Threshold visual cryptography with specified whiteness levels of reconstructed pixels," *Designs, Codes, and Cryptography*, vol.25, pp.15–61, Jan. 2002.

[10] 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, pp. 2356–2366, Aug. 2007.

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

[12] Y.C. Chen, G. Horng, and D.S Tsai, "Comment on 'Cheating Prevention in Visual Cryptography' " *IEEE Trans. Image Process.*, vol.21, pp.3319–3323, Jul. 2012.

[13] 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.

[14] S. Liu, M. Fujiyoshi, and H. Kiya, "A cheat-prevention visual secret sharing scheme with efficient pixel expansion" *IEICE Trans. Fundamentals*, vol.E96-A, pp.2134–2141, Nov. 2013.

[15] S. Liu, M. Fujiyoshi, and H. Kiya, "A cheat-prevention visual secret sharing scheme with minimum pixel expansion," in *Proc. IWDW*, 2013.