Multimedia Tools and Applications (2019) 78: 8207–8223
https://doi.org/10.1007/s11042-018-6779-6

An efficient XOR-based verifiable visual cryptographic scheme

Xingxing Jia[1] · Daoshun Wang[2] · Qimeng Chu[1] · Zhenhua Chen[3]

Received: 26 July 2018 / Revised: 3 October 2018 / Accepted: 12 October 2018 /
Published online: 23 October 2018

Abstract

Visual cryptographic (VC) schemes have been widely used in secure multimedia systems for data transmission and data storage. It divides a secret image into n random-seemingly share images printed on the transparencies. Superimposing the designed shares will display the recovered secret image which can be recognized by human visual system. It is very convenient to decode the secret since it requires no cryptographic knowledge and computation. However, there is a high chance for dishonest shareholders to present faked shares in the secret reconstruction phase, which would result in a huge damage to the honest shareholders. In this article, a secure approach to verify the cheating shares has been proposed to achieve fair reconstruction of the image secret. It is designed to share a verification image among the original shares of the XOR based VC scheme. It only increases pixel expansion by one to achieve the verification function. Cheating detection ability is attained by pairwise superimposing the shares so that any cheating behavior can be detected by the honest participant. The secret image is recovered and its recovered contrast becomes $\frac{m}{m+1}$ times of the original contrast where m denotes the pixel expansion of the original scheme. The verification image is probabilistically recovered and its recovered contrast is $\frac{1}{2(m+1)}$. Compared with traditional verifiable (k, n)-VC schemes against cheating, it overcomes the drawbacks such as requiring additional shares, additional large pixel expansion, or lower contrast. The experimental results show that the visual quality of the recovered secret image is as good as expected. The security analysis and comparative results based on various aspects of VC schemes demonstrate the better efficiency of the proposed approach over existing schemes.

Keywords Visual cryptography · Verifiable visual cryptographic scheme · Pixel expansion

✉ Xingxing Jia
jiaxx@lzu.edu.cn

[1] School of Mathematics and Statistics, Lanzhou University, Lanzhou, Gansu, China

[2] School of Computing, Tsinghua University, Beijing, China

[3] School of Computer Science and Technology, Xi'an University of Science and Technology, Xi'an, Shaanxi, China

1 Introduction

The widespread use of the network has brought explosive growth of multimedia contents. Cloud-based media hosting facilitates and accelerates the development of multimedia contents. However, multimedia faces various potential attacks and is vulnerable when it takes advantages of high end computational resources, storage capacity, accessibility from the network and cloud media hosting. Encrypting the multimedia content before being transmitted over the network or hosting on the cloud is obviously a good solution. VC provides a good encoding strategy for the multimedia content. VC is initially designed to manage important keys in order to ensure a group cooperation. Hereafter, it shows powerful ability in image encryption without computational overhead in decryption because it decodes the encrypted image only by human visual system. In this paper, an efficient XOR-based verifiable visual cryptographic scheme is proposed to solve the security problem for multimedia content to be transmitted over the network and to be stored in public cloud.

The human visual system was firstly suggested to be used for security purposes by Arazi et al. [2]. The basic principle and detailed construction were first studied by Noar et al. [19], named as Visual Cryptography (VC). A (k, n) VC scheme divides a secret image into n random-seemingly share images printed on the transparencies among a set of n shareholders. At least k shares will be superimposed to reveal the secret image, and fewer than k shares cannot know any information about the secret. It is shown that this system is equivalent to a One Time Pad encryption scheme based on the boolean OR function and therefore unconditionally secure [18, 19]. The stacking-to-see property requires neither knowledge of cryptography nor complex computation, which makes visual cryptography attractive in steganography [32] and steganalysis [15, 17, 33], visual authentication and identification in an electric payments [14, 16, 18] and secure two-party computation [7] for distributed network communication. VC scheme is not only an encryption method for image in insecure network communication [18, 19], but also an key management in distributed cryptography used in social network [11].

VC is designed to establish a fair cooperation relation in a group of n mutually suspicious participants with conflicting interests. However, some malicious participants may deliberately cheat other honest participants by providing faked shares. Then the cheaters will obtain the authentic secret image but the honest participants will only obtain the forged image. It will result in unpredictable damage to the honest participants. The authentication and identification in VC schemes were firstly introduced in [18] to resist cheating behavior. Horng et al. first analyzed the case of collusive cheating among the participants and proposed two methods to resist cheating in visual cryptography [8]. The first one is realized by using an additional verification share for each participant; and the second one makes use of the basis matrices of $(2, n + l)-$VCS ($l \geq 1$) for $(2, n)-$VCS to resist $n - 1$ participants' collusion. The two constructions require additional shares or increase the share size. De prisco and De Santis considered the malicious collusion case in which $n - 1$ participants become cheaters [20]. They proposed a method which adds $2^n + 1$ columns to the basis matrices of $(2, n)-$VC scheme to prevent the cheaters from the accurate speculation for the only honest participant's share by using their $n - 1$ shares. It significantly increases the share size by exponential times. Tsai et al. proposed to encrypt homogeneous secret images for the aid of cheating prevention, which is equivalent to repeating $\frac{n(n-1)}{2}$ times of $(2, 2)-$VC schemes in distinct regions on the shares [26]. Its large pixel expansion reduces the efficiency of this scheme. Afterwards, Hu and Tzeng [9] first proposed two attack models and then proposed a $(\Gamma, m+2)-$CPVC scheme, which needs an additional verification share with pixel expansion $m + 2$. The additional shares make the scheme more complex.

An almost perfect recovery of secret image was shown in [3], but it is only suitable to $(2, 2)$ scheme and requires complex decoding computation for the recovery of the secret image. Liu et al. [13] and Chen et al. [4] pointed that the $(\Gamma, m + 2)-$CPVC scheme in [9] is not cheating immune. Liu et al. proposed a new authentication method by using t additional share matrices for some randomly chosen black (resp. white) secret pixels [13]. However, it is not practical to recognize a single pixel in a VC scheme since a pixel takes very small space in the recovered image. Lin et al. proposed to use an authentication pattern stamping process to encode the n base-shares to get n verifiable shares [12] but it will seriously degrade the visual quality of recovered secret images by $\frac{1}{2^k}$ times. Ren et al. proposed to use Latin square to choose authentication regions [21] but an additional share for each participant is needed to check other shares by counting the number of solid black regions on the stacked results. The verification process is troublesome for human visual system to see confused square and each participant needs to take an additional verification share.

The previous methods face several disadvantages: 1) unacceptable large pixel expansion [8, 20, 26], 2) extra verification shares with the same size as the original shares [8, 9, 21], 3) complex encoding computation [21] or a special threshold with $k = 2$ [5, 8, 20], and 4) lower visual quality for the secret image caused by boolean OR operation [8, 9, 20, 21, 26]. It is desirable to carefully design an VC scheme to overcome the above problem existing in the traditional VC schemes against cheating.

VC scheme has poor visual quality for a reconstructed secret image. The operation built beneath the stacking results is the boolean OR operation. Many conventional VC schemes are based on OR operation, which are referred to as OR-based VC (OVC) scheme. OVC schemes suffer from huge pixel expansion and lower contrast of the reconstructed secret images. Integral linear programming [11, 24], probabilistic method [6, 30] and linear algebraic techniques [1] have been proposed to optimize the pixel expansion. To further enhance the visual quality, XOR-based VC (XVC) schemes were proposed [23, 27, 28] to improve contrast. The optimal constructions of XVC scheme with threshold access structure or general access structure were shown in [22, 23]. XVC schemes were proved to have much higher contrast than OVC schemes by 2^{k-1} times if the shares are encoded using the same basis matrices of OVC scheme [31].

From the above analysis, we propose a new scheme that addresses the aforementioned challenges existing in the state-of-the-art schemes by using XOR operation. In order to preserve the visual quality of the secret image, we using a special probabilistic $(2, n)$-XVC scheme to encode the verification image which uses only one pixel [28]. Each verification pixel encoding is mixed among the corresponding pixel encoding of the secret image. Cheating detection ability is attained by pairwise superimposing the shares so that any participant can detect the cheaters. We theoretically prove that the proposed scheme is suitable to authenticate the shares' genuineness. The requirement for the verification image is illustrated by a formula. The proposed verifiable (k, n)-XVC ((k, n)-VXVC) scheme can be used on any XVC scheme, including those with general access structure. The secret image is primarily recovered and its recovered contrast becomes $\frac{m}{m+1}$ times of its original contrast if the pixel expansion of the original scheme is assumed as m. The verification image is probabilistically recovered and its recovered contrast is $\frac{1}{2(m+1)}$. Detailed construction has been presented for the generation of basis matrices. Compared with traditional (k, n) VC schemes, it overcomes the drawbacks of previous verification methods such as requiring additional shares, lower visual quality and special threshold constraint. It ensures the secret image being securely transmitted and prevents the collusion attack from the malicious participants. The visual quality of the recovered secret image is quite

good as evaluated. The security analysis and comparative results based on various aspects of VC schemes demonstrate the higher efficiency of the proposed approach over existing schemes.

The rest of this paper is organized as follows. Section 2 provides the basic concepts and detailed scheme of visual cryptography. Section 3 gives the scheme construction and related properties analysis. Section 4 demonstrates the construction procedure with an detailed example and presents the experiment results to show the correctness and the effectiveness of the XVC scheme. Comparison with other VC schemes against cheating is also presented. Conclusions are drawn in Section 5.

2 Preliminaries

This section briefly reviews the background of VC scheme. The definition of (k, n)-XVC scheme is formally presented and a traditional (2, 3)-XVC scheme is presented to show its construction process in Section 2.1. The probabilistic $(2, n)-$XVC scheme is presented in Section 2.2 [28] and the recognition area in the recovered image is discussed in the same section.

2.1 $(k, n)-$XVC scheme

Visual cryptography scheme is the visual version of secret sharing scheme. $(k, n)-$XVC scheme is proved to have advanced properties, such as better contrast and lower pixel expansion than $(k, n)-$OVC scheme [31]. Decryption of the secret from the shares in a $(k, n)-$XVC scheme can be done by a small, cheap and light-weight computational devices which can be flexibly connected to network or open cloud. Based on the above advantages, $(k, n)-$XVC schemes are widely adopted to improve the $(k, n)-$OVC scheme. Many sophisticated approaches were presented to decrease the construction complexity [22, 23, 25, 28, 29]. The notations and its formal definition are presented as follows.

Consider threshold access structure on a set $\mathcal{P} = \{1, 2, \ldots, n\}$ of n participants. Let $2^{\mathcal{P}}$ denote the set of all subsets of $\mathcal{P}$. A $(k, n)-$VC scheme has qualified set family $\Gamma_{Qual} = \{U \subseteq \mathcal{P} : |U| \geq k\}$ and forbidden set family $\Gamma_{Forb} = \{U \subseteq \mathcal{P} : |U| < k\}$. Members of Γ_{Qual} and Γ_{Forb} are referred to as qualified sets and forbidden sets. The pair $(\Gamma_{Qual}, \Gamma_{Forb})$ is called the access structure of a $(k, n)-$VC scheme. Apparently, $\Gamma_{Qual} \subseteq 2^{\mathcal{P}}$, $\Gamma_{Forb} \subseteq 2^{\mathcal{P}}$, and $\Gamma_{Qual} \cap \Gamma_{Forb} = \emptyset$.

Let $H(v)$ denote the Hamming weights (the number of $1s$ in the vector v) of vector v. Let $\otimes$ denote the Boolean XOR operation. $\otimes(B_i|U)$ denotes the Boolean XOR-ing of the row j, $j \in U$ of B_i, $i = 0, 1$. Let $|U|$ denote the cardinality of participant set U. The formal definition of the $(k, n)-$XVC scheme was presented by Yang et al. in a simplified form as follows [31].

Definition 2.1 [31] With a set of two $n \times m$ Boolean basis matrices B_0 and B_1, the result of a column permutation of B_i defines the color of the m subpixels in each one of the n shares when sharing a pixel $i \in \{0, 1\}$. Such basis matrices constitute a $(k, n)-$XVC scheme if the following conditions are met:

1) **Contrast Condition:** $H(\otimes(B_1|U)) \geq h$ and $H(\otimes(B_0|U)) \leq l$ for $|U| = k$, where $0 \leq l < h \leq m$.
2) **Security Condition:** $H(\otimes(B_1|U)) = H(\otimes(B_0|U))$ for $|U| \leq k - 1$.

The condition 1) assures that secret image can be visually revealed due to their different Hamming weights of black and white colors. The contrast, $\alpha = (H(\otimes(B_1|U)) - H(\otimes(B_0|U)))/m$, denotes the relative difference of the grey levels of the two pixel types. It provides a measurement for the quality of the reconstructed secret image. The condition 2) shows the perfect secrecy of the $(k, n)-$XVC scheme. The parameter m is called the pixel expansion, i.e., the number of pixels, on the share image used to encode one pixel of the secret image. We give an example to illustrate the above definition.

Example 1 Basis matrices of a $(2, 3)-$XVC scheme

$$B_0 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad B_1 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

The participant set is $\mathcal{P} = \{1, 2, 3\}$. The pixel expansion m is 3. B_0 and B_1 satisfy security conditions

$$H(\otimes(B_1|U)) = H(\otimes(B_0|U)) \text{ for } |U| = 1,$$

and contrast conditions

$$H(\otimes(B_0|U)) = 0 = l, \ H(\otimes(B_1|U)) = 2 = h, \ \text{ for } |U| = 2.$$

The contrast is

$$\alpha = \frac{H(\otimes(B_1|U)) - H(\otimes(B_1|U))}{m} = \frac{h - l}{3} = \frac{2}{3}, \text{ for } |U| = 2.$$

To share a secret pixel $i \in \{0, 1\}$, the basis matrix B_i is chosen and randomly permutated in columns. The resulting matrix is used to encode the secret pixel i and its n rows are distributed to the n shares. Therefore, the basis matrices are fundamental to constructing a $(k, n)-$XVC scheme. The established efficient constructions for a $(k, n)-$XVC scheme are based on integer linear programming [23] or linear algebra [22]. Instead of discussing its construction technique, we focus on its function of cheating prevention.

2.2 Probabilistic $(2, n)-$XVC scheme

To solve the pixel expansion problem of VC schemes, Ito et al. [10], Yang [30] and Cimato [6] proposed probabilistic VC models. The frequency of black pixels in a white (resp., black) area is used to display the contrast of the recovered image. They define p_0 (resp., p_1) as the appearance probability of black pixel in a white (resp., black) area of the recovered image. For a fixed threshold probability $0 < p_{TH} \leq 1$ and relative contrast $\alpha > 0$, if $p_1 \geq p_{TH}$ and $p_0 \leq p_{TH} - \alpha$, the frequency of black pixels in a black area of the recovered image should be higher than that in a white area.

Wang et al. [28] proposed a $(2, n)-$XVC scheme with no pixel expansion. Its contrast α is $\frac{1}{2}$ when two shares are used to recover the image. This scheme is much more efficient than popular schemes in [23, 27] but it is just considered as a normal $(2, n)-$XVC scheme. Its extensive property and more applications are not further explored. Here we first show its construction in the pseudo-code style in terms of its input, output, the construction procedure and the revealing procedure from [28]. Then we analyze its characteristics and show its possibility used as verification for $(k, n)-$XVC scheme. The detailed construction is shown as the following Construction 1.

Construction 1 A probabilistic $(2, n)-$XVC scheme
Input: an integer n with $n \geq 2$, and the secret pixel p being 0 or 1.
Output: Basis matrices V_0 and V_1.
Construction: 1. Generate $n+1$ random pixels $b_1, \ldots, b_{n+1}$.
2. Compute n intermediate pixels $c_1, \ldots, c_n$, with $c_i = b_i \& p$ for $i = 1, \ldots, n$.
3. Compute n share pixels $v_1, \ldots, v_n$, with $v_i = b_{n+1} \otimes c_i$ for $i = 1, \ldots, n$.
4. We have $V_p = [v_1, \ldots, v_n]'$, $'$ denotes the transposition of matrix.

In the above probabilistic $(2, n)-$XVC ($(2, n)-$PXVC) scheme, boolean operations XOR ($\otimes$) and AND ($\&$) are used to construct the shares. It can be verified that $p_0 = 0$, $p_1 = \frac{1}{2}$, $\alpha = \frac{1}{2}$ and $m = 1$ when two share images are XOR-ed to recover the secret image. We find that $\alpha = \frac{1}{2}$ when even shares are XOR-ed to recover the secret, while $\alpha = 0$ when odd shares are XOR-ed to recover the secret. We show it in Theorem 2.1.

Theorem 2.1 *The $(2, n)-$PXVC scheme shown in Construction 1 satisfies that*

1. $\alpha = \frac{1}{2}$ *when even shares are XOR-ed to recover the secret;*
2. $\alpha = 0$ *when odd shares are XOR-ed to recover the secret.*

Proof With the above construction procedure, for a "0" pixel in the secret image, we have $c_i = b_i \& 0 = 0$ and $v_i = b_{n+1} \otimes c_i = b_{n+1}$. Thus,

$$v' = v_{i_1} \otimes v_{i_2} \otimes \cdots \otimes v_{i_{|U|}} = \overbrace{b_{n+1} \otimes b_{n+1} \otimes \cdots \otimes b_{n+1}}^{|U|}$$
$$= \begin{cases} 0, & |U| \text{ equals to an even number;} \\ b_{n+1}, & |U| \text{ equals to an odd number.} \end{cases}$$

It is obtained that

$$p_0 = \begin{cases} 0, & |U| \text{ equals to an even number;} \\ \frac{1}{2}, & |U| \text{ equals to an odd number.} \end{cases}$$

For a "1" pixel in the secret image, we have $c_i = b_i \& 1 = b_i$ and $v_i = b_{n+1} \otimes c_i = b_{n+1} \otimes b_i$. Thus

$$v' = v_{i_1} \otimes v_{i_2} \otimes \cdots \otimes v_{i_{|U|}} = b_{n+1} \otimes b_{i_1} \otimes b_{n+1} \otimes b_{i_2} \otimes \cdots \otimes b_{n+1} \otimes b_{i_{|U|}}$$
$$= \begin{cases} b_{i_1} \otimes b_{i_2} \otimes \cdots \otimes b_{i_{|U|}}, & |U| \text{ equals to an even number;} \\ b_{n+1} \otimes b_{i_1} \otimes b_{i_2} \otimes \cdots \otimes b_{i_{|U|}}, & |U| \text{ equals to an odd number.} \end{cases}$$

Since $b_{n+1}, b_{i_1}, b_{i_2}, \cdots, b_{i_{|U|}}$ are random pixels being 0 or 1, $b_{i_1} \otimes b_{i_2} \otimes \cdots \otimes b_{i_{|U|}}$ is random being 0 or 1 with same probability $\frac{1}{2}$. The same conclusion is obtained for $b_{n+1} \otimes b_{i_1} \otimes b_{i_2} \otimes \cdots \otimes b_{i_{|U|}}$. Therefore, $p_1 = \frac{1}{2}$ no matter $|U|$ takes odd number or even number.
Since $\alpha = p_1 - p_0$, the conclusions are obvious. The theorem is proved. □

Therefore, we will use the $(2, n)-$PXVC scheme to detect and authenticate the cheaters by pairwise XOR-ed the shares. Because the verification image will appear when even number of share images are XOR-ed and disappear when odd number of share images are XOR-ed. It is suitable to combine a $(k, n)-$XVC scheme with odd k to attain the verification function. Later we will prove that it is also suitable to a $(k, n)-$XVC scheme with even k ($k \neq 2$). The special case for $k = 2$ is processed independently.

As pointed out in [30], in a probabilistic VC scheme, small areas, not single pixels, will be reconstructed. It is important to know how many pixels are needed to recognize black and white area correctly in the verification image. Let N be the total number of pixels in an area. By using Empirical Rule, an area can be correctly recognized with about 99% probability if N satisfies the following condition:

$$N > 9\left(\frac{\sqrt{p_0(1-p_0)}+\sqrt{p_1(1-p_1)}}{p_1-p_0-d}\right)^2, \tag{2.1}$$

where d is a "separation factor" and $0 \le d < p_1 - p_0$. In the $(2,n)-$PXVC scheme, it is detailed as

$$N > 9\left(\frac{\sqrt{0.5\cdot 0.5}}{0.5-d}\right)^2 = 9\left(\frac{0.5}{0.5-d}\right)^2.$$

When the $(2,n)-$PXVC scheme is used to identify the verification images in a verifiable scheme, the p_0 and p_1 are given new values. The recognized area N is needed to be recomputed. We will demonstrate it in Section 3.2.

3 Construction of the verifiable (*k*, *n*) XOR-based visual cryptographic scheme

The section proposes a new verifiable $(k,n)-$XVC ($(k,n)-$VXVC) scheme by combing any established $(k,n)-$XVC scheme and the $(2,n)-$PXVC scheme. The $(k,n)-$VXVC scheme encrypts the secret image and the verification image in one noise-like share. In the reconstruction phase, the verification image will be recognized by XOR-ing any two shares with contrast $\frac{1}{2(m+1)}$. The secret image will be recovered by XOR-ing any k shares with contrast $\frac{m}{m+1}\alpha$. m and α are pixel expansion and contrast of the established $(k,n)-$XVC scheme. Before the participants prepare to recover the secret image, any cheating behavior can be detected and authenticated by pairwise XOR-ing their shares. Section 3.1 gives the formal definition of the $(k,n)-$VXVC scheme and describes the share construction process. The performance analysis including contrast analysis, share analysis, and theoretical proof as well as the requirement for the verification images is shown in the remaindering subsection.

3.1 Construction of the shares

Suppose the secret image S and a verifiable image V have the same size $w \times h$. The $(k,n)-$VXVC scheme is actually a two secret sharing scheme. We now give a formal definition of the $(k,n)-$VXVC scheme with $\mathcal{P}$ as follows.

Definition 3.1 With a set of 4 $n \times m$ basis matrices $B_{0,0}$, $B_{0,1}$, $B_{1,0}$ and $B_{1,1}$, the result of a column permutation of $B_{p,q}$ defines the color of the m sub-pixels in each of the n shares when sharing two pixels $p \in S$ and $q \in V$, $p, q \in \{0, 1\}$. Such basis matrices constitute the $(k,n)-$VXVC ($k \ge 3$) scheme if the following conditions are met:

1) **Contrast condition** $H(\otimes(B_{1,q}|U)) \ge h_s$ and $H(\otimes(B_{0,q'}|U)) \le l_s$ for $|U| = k$, $q' \in \{0, 1\}$, where $h_s > l_s$; $H(\otimes(B_{p,1}|U)) \ge h_v$ and $H(\otimes(B_{p',0}|U)) \le l_v$ for $|U| = 2$, where $h_v > l_v$, $p' \in \{0, 1\}$,;

2) **Security condition** $H(\otimes(B_{1,q}|U)) = H(\otimes(B_{0,q'}|U))$ for $|U| \leq k-1$; $H(\otimes(B_{p,1}|U)) = H(\otimes(B_{p',0}|U))$ for $|U| = 1$;

Then we present our new construction. Our scheme is described in a pseudo-code style below in terms of its input, output, the construction procedure (how to compute the share images) and the revealing procedure (how to reconstruct the secret images from the shadows). Let B_0 and B_1 be the basis matrices for a $(k, n)-$XVC scheme with pixel expansion m and contrast α. Next we will give the construction of $(k, n)-$VXVC scheme.

Construction 2 A new $(k, n)-$VXVC scheme with odd k ($k \geq 3$)

Input: a secret image S and a verifiable image V. The basis matrices B_0 and B_1 for a $(k, n)-$XVC scheme.

Output: The share images $S_1, \ldots, S_n$.

Construction:
1. Take one pixel $S(x, y)$ and $V(x, y)$ from the secret image S and the verifiable image V, respectively, $1 \leq x \leq w$, $1 \leq y \leq h$.
2. Generate a column vector $V_{V(x,y)}$ for $V(x, y)$ by calling Construction 1.
3. Generate the basis matrices $B_{S(x,y),V(x,y)} = [B_{S(x,y)}||V_{V(x,y)}]$, here $||$ denotes the matrix concatenation.
4. Randomly permutate $B_{S(x,y),V(x,y)}$ among its columns and distribute its ith row to S_i, $i \in \{1, 2, \ldots, n\}$.

Revealing:
1. The verifiable image V can be revealed when two shares are XOR-ed.
2. The secret image S can be revealed when k shares are XOR-ed.

3.2 Contrast analysis

The $(k, n)-$VXVC scheme is a multi-secret sharing scheme. It encrypts the secret image and the verification image from two different schemes. Its basic properties in terms of contrast, pixel expansion, and basis matrices have been changed and are different from its two component schemes. In the following we give the related analysis.

Apparently, the pixel expansion of the proposed $(k, n)-$VXVC scheme is $m + 1$. It is a combination of a probabilistic XVC scheme and a deterministic XVC scheme. Their contrasts are defined in a different manner, that is, $\alpha = (h-l)/m$ for a deterministic scheme [31] and $\alpha = p_1 - p_0$ for a probabilistic XVC scheme [28, 30]. In order to express the contrast in the proposed $(k, n)-$VXVC scheme in a unified form, we define the contrast as the following form

$$\alpha = \frac{\bar{h} - \bar{l}}{m}, \tag{3.1}$$

where $\bar{h}$ and $\bar{l}$ are the average appearance times of black pixel for the recovered black and white secret pixel, respectively.

It can be deduced that $\alpha = \frac{\bar{h}-\bar{l}}{m} = p_1 - p_0$ for the probabilistic XVC scheme since $p_1 = \frac{\bar{h}}{m}$ and $p_0 = \frac{\bar{l}}{m}$ according to their definition in [30]. The new definition of contrast in (3.1) is coincident with contrast definition of probabilistic XVC scheme. It is obviously consistent with contrast definition of deterministic XVC scheme because $\bar{h} = h$ and $\bar{l} = l$.

Due to the definition of $\bar{h}$ and $\bar{l}$, we need to modify the contrast condition and security condition in Definition 3.1 to suit our Construction 2 as follows:

1′) **Contrast condition** $H(\otimes(B_{1,q}|U)) \geq \bar{h}_s$ and $H(\otimes(B_{0,q'}|U)) \leq \bar{l}_s$ for $|U| = k$, where $\bar{h}_s > \bar{l}_s$, $q' \in \{0, 1\}$; $H(\otimes(B_{p,1}|U)) \geq \bar{h}_v$ and $H(\otimes(B_{p',0}|U)) \leq \bar{l}_v$ for $|U| = 2$, where $\bar{h}_v > \bar{l}_v$, $p' \in \{0, 1\}$;

2′) Security condition $H(\otimes(B_{1,q}|U)) = H(\otimes(B_{0,q'}|U))$ for $|U| \leq k-1$; $H(\otimes(B_{p,1}|U)) = H(\otimes(B_{p',0}|U))$ for $|U| = 1$;

Assume a $(k,n)-$XVC scheme used in Construction 2 has h and l as the black pixel numbers of the recovered black and white pixel. Let its pixel expansion be m and contrast be α. Then we have $\bar{h}_s = h$ and $\bar{l}_s = l$. We will prove it in the following contrast proof and security proof.

According to the contrast formula (3.1), now we give the contrast representations of the recovered images in the proposed $(k,n)-$VXVC scheme as follows

$$\alpha_s = \frac{\bar{h}_s - \bar{l}_s}{m'} \tag{3.2}$$

$$\alpha_v = \frac{\bar{h}_v - \bar{l}_v}{m'} \tag{3.3}$$

where $m' = m+1$, denoting the total pixel expansion of the proposed $(k,n)-$VXVC scheme. The contrast of the recovered secret image α_s is $\frac{m}{m+1}\alpha$, since $\alpha_s = \frac{\bar{h}_s - \bar{l}_s}{m'} = \frac{h-l}{m+1} = \frac{h-l}{m}\frac{m}{m+1} = \frac{m}{m+1}\alpha$. The contrast of the recovered verification image α_v is $\frac{1}{2(m+1)}$. Generally speaking, the $(k,n)-$XVC scheme is deterministic scheme and has contrast α no less than $\frac{1}{m}$. Therefore, we always have $\alpha_s \geq 2\alpha_v$. The secret image is primarily recovered, which keeps almost the same contrast with its original $(k,n)-$XVC scheme. The verification image is recovered with no more than half of the contrast of the secret image. This conforms to the aim of secret sharing to protect the secret primarily.

3.3 Share analysis

In Construction 2, the basis matrices V_0 and V_1 for the verification image are $V_0 = [0,0,0,0,0]'$ or $V_0 = [1,1,1,1,1]'$, as well as $V_1 = [b_1,b_2,b_3,b_4,b_5]'$ or $V_1 = [1-b_1, 1-b_2, 1-b_3, 1-b_4, 1-b_5]'$. Thus, each execution of Construction 2 yields completely different and unpredictable basis matrices $B_{p,q}$, $p,q \in \{0,1\}$. In fact, there are $2^n(m+1)!$ possible $B_{p,1}$ and $2(m+1)!$ possible $B_{p,0}$ when all possible column permutations and combinations of B_p and V_q are considered. This property ensures completely different, unpredictable and non-repetitive shares, which results in high security. Especially, when $n-1$ cheaters are colluded to cheat the only honest participant, it is still hard to predict the black verification pixels. This scheme partially solves the malicious collusion problem addressed in [8, 20].

3.4 Theoretical analysis of the $(k,n)-$VXVC scheme with odd k ($k \geq 3$)

Now we present the contrast and security proofs for the $(k,n)-$VXVC scheme.

Theorem 3.1 *The proposed $(k,n)-$VXVC scheme in Construction 2 with odd k, $3 \leq k \leq n$, is a secure $(k,n)-$VXVC scheme.*

Proof We verify its contrast condition and security condition.

To show contrast, Let $U = \{r_1, r_2, \ldots, r_t\} \subset \mathcal{P}$. According to Construction 2, when a secret pixel p and a verification pixel q with the same position are chosen, the basis matrix $B_{p,q}$ is determined without considering the random column permutation, which equals to $[B_p||V_q]$. Let $B_p|U$ be the $t \times m$ matrix with B_p's rows in U. B_p and V_q are the basis

matrices of $(k, n)-$XVC scheme and $(2, n)-$PXVC scheme defined in Section 2. When $|U| = k$, B_p satisfies the following relation,

$$H(\otimes(B_0|U)) \leq l, \quad H(\otimes(B_1|U)) \geq h$$

with $l < h$. When $|U| = t$, B_p satisfies the following relation,

$$H(\otimes(V_0|U)) = l', \quad H(\otimes(V_1|U)) = h'.$$

Since l' and h' are both 1 with $\frac{1}{2}$ probability for an odd t shown in Theorem 2.1, l' and h' can be expressed using average Hamming weight $\bar{l}'$ and $\bar{h}'$ for a unified form. They both have value $\frac{1}{2}$.

Therefore we have that, when $|U| = k$,

$$H(\otimes(B_{0,q}|U)) = H(\otimes(B_0|U)) + H(\otimes(V_q|U)) \leq l + \frac{1}{2} = \bar{l}_s,$$

and

$$H(\otimes(B_{1,q'}|U)) = H(\otimes(B_1|U)) + H(\otimes(V_{q'}|U)) \geq h + \frac{1}{2} = \bar{h}_s.$$

Since $l < h$, we have $\bar{l}_s < \bar{h}_s$. The contrast condition for the secret image is attained.

When $|U| = 2$, we have

$$H(\otimes(B_{p,0}|U)) = H(\otimes(B_p|U)) + H(\otimes(V_0|U)) \leq H(\otimes(B_p|U)) + l' = \bar{l}_v,$$

and

$$H(\otimes(B_{p',1}|U)) = H(\otimes(B_{p'}|U)) + H(\otimes(V_0|U)) \geq H(\otimes(B_{p'}|U)) + h' = \bar{h}_v.$$

We have $H(\otimes(B_p|U)) = H(\otimes(B'_p|U))$ for $|U| = 2 < k$ from Definition 2.1. We have $l' = 0$ and $h' = \bar{h}' = \frac{1}{2}$ for $|U| = 2$ from Theorem 2.1. $\bar{l}_v < \bar{h}_v$ is obtained. The contrast condition for verification image is obtained.

To show security: We will prove the fact that $H(\otimes(B_{1,q}|U)) = H(\otimes(B_{0,q'}|U))$ for odd t with $2 < t \leq k - 1$. It is obvious from

$$H(\otimes(B_{0,q}|U)) = H(\otimes(B_0|U)) + H(\otimes(V_q|U)),$$

$$H(\otimes(B_{1,q'}|U)) = H(\otimes(B_1|U)) + H(\otimes(V_{q'}|U)),$$

$H(\otimes(B_0|U)) = H(\otimes(B_1|U))$ for $|U| \leq k - 1$ according to Definition 2.1, and $H(\otimes(V_q|U)) = H(\otimes(V_{q'}|U))$ for odd $|U|$ according to Theorem 2.1.

For an even $|U|$ with $2 < |U| \leq k - 1$, $H(\otimes(B_0|U)) = H(\otimes(B_1|U))$ still holds, but $H(\otimes(V_0|U)) = 0$ and $H(\otimes(V_1|U)) = \frac{1}{2}$. Since verification image is independent of the secret image, the pixels q and q' are independent of the secret pixel. Thus, we have

$$H(\otimes(V_q|U)) = H(\otimes(V_{q'}|U)) = \frac{1}{2}H(\otimes(V_0|U)) + \frac{1}{2}H(\otimes(V_1|U)) = 1/4,$$

$H(\otimes(B_{1,q}|U)) = H(\otimes(B_{0,q'}|U))$ is obtained for even $|U|$. The security of secret image is obtained. $H(\otimes(B_{p,0}|U)) = H(\otimes(B_{p',1}|U))$ is obvious since $H(\otimes(V_0|U)) = H(\otimes(V_1|U))$ for $|U| = 1$ is derived from 2.1. The security of verification image is achieved. □

3.5 Verification and cheater authentication

Any honest participant can verify the possible cheaters by XOR-ing his share with other's shares. If the correct verification image appears, these shares can be seen correct. Other-

wise the cheating share is authenticated. In fact, the proposed scheme has another property as $H(\otimes(B_{p,0}|U)) < H(\otimes(B_{p',1}|U))$ for even $|U| < k$. The verification image will show when even participants XOR their shares. This can be used to detect the cheating behaviors by using the participant set with biggest even cardinality less than k before recovering the secret. It will have less verification overhead than pairwise XOR-ing verifications. If the correct verification image appears, these shares can be seen correct. The pairwise verifications can be omitted. If the verification image is random looking, there must be cheating behavior. The cheater identification can be done within such participant set by using pairwise verification.

3.6 $(k, n)-$VXVC scheme with even k ($k \geq 2$)

In the Construction 2, we present the $(k, n)-$VXVC scheme with an odd k. When the Construction 2 is used for the $(k, n)-$XVC scheme with even $k \geq 4$, the secret image and verification image will appear simultaneously when k shares are XOR-ed. We have inferred $\alpha_s \geq 2\alpha_v$. The recovered secret image will be clearly shown with heavy grey-scale and the verification image will be shown with light grey-scale. The secret image may be affected by the verification image. We can use image processing software to erase the verification image from the recovered image. $(k, n)-$VXVC scheme with even $k \geq 4$ can be solved directly by using integer linear programming not via the established $(k, n)-$XVC scheme [11].

For $k = 2$, the Construction 2 cannot be used. The idea of [12] can be used to add verification ability to the $(2, n)-$XVC scheme by using the $(2, 2)-$XVC scheme. We divide the secret image into $n - 1$ equal-sized, non-overlapping partitions, and numbered from partition 1 to partition $n - 1$ sequentially from top to bottom. The secret image can be normally encoded by the $(2, n)-$XVC scheme with pixel expansion m. The resulting shares M_1, M_2, ..., M_n contain similar $n - 1$ divisions as the secret image. The partitions of n shares form n matches such that share M_i matches its $j-1$th division to the ith division of M_j. The size of the verification image is equal to a division of the secret image. The two matched divisions are used to encode the corresponding verification image by the $(2, 2)-$XVC scheme. It produces a $(2, n)-$VXVC scheme with the pixel expansion $m+1$. The verification image is encrypted and recovered deterministically with contrast $\frac{1}{m+1}$. The secret image has contrast $\frac{m}{m+1}\alpha$ where α is the contrast of the $(2, n)-$XVC scheme. The n verification images can be same or different.

3.7 Recognition of small areas in the verification image for the $(k, n)-$VXVC scheme

Now we present the requirement for the suitable verification image. Since the verification image is encoded by the $(2, n)-$PXVC, the verification image is probabilistically recovered. Now we present the least recognized area size.

Assume the established $(k, n)-$XVC scheme have pixel expansion m. In the proposed $(k, n)-$VXVC scheme, the recovered verification image has $p_0(\geq 0)$ and $p_1(= p_0 + \frac{1}{2(m+1)})$ as the recovered black pixel ratios for their original white and black pixels. The contrast α_v equals to $\frac{1}{2(m+1)}$ for the verification image which decreases as m increases. By using (2.1), we can derive the least recognizable area size N satisfying the following condition,

$$N > 9\left(\frac{\sqrt{p_0(1-p_0)} + \sqrt{p_1(1-p_1)}}{\frac{1}{2(m+1)} - d}\right)^2. \tag{3.4}$$

Since $p_0 < p_1 \leq 1$, $\left(\sqrt{p_0(1-p_0)} + \sqrt{p_1(1-p_1)}\right)^2$ is upper bounded by 1. Thus, we can present a tighter estimation for N as

$$N > 9/\left(\frac{1}{2(m+1)} - d\right)^2, \tag{3.5}$$

where d is a separation factor and satisfies $0 \leq d < \frac{1}{2(m+1)}$. Because the verification image has same size with the secret image, we can always choose the verification image with a large N. Such an N can always be obtained for m that is not so big. Thus, if we select the secret image more carefully and satisfy the lower bound of N, we can get the clear recovered verification image. The verification image with a large scale of solid pattern is considered in [12]. This idea can be also used in our scheme. Then the verification images can be shown conspicuously and can be easily detected by the human eye.

4 Experiment results and comparison

4.1 Experimental results

Here we present one experiment to illustrate the construction procedure of our proposed $(k, n)-$VXVC scheme in Construction 2.

Example 2 Constructing a $(3, 5)-$VXVC scheme from a $(3, 5)-$XVC scheme shown in Example 2 of [31].

This experiment is to show $(3, 5)-$VXVC scheme and its construction procedure. The basis matrices for a $(3, 5)-$XVC scheme are taken from the Example 2 in [31] being

$$B_0 = \begin{pmatrix} 1&0&0&0&0&1&1&1 \\ 0&1&0&0&0&1&1&1 \\ 0&0&1&0&0&1&1&1 \\ 0&0&0&1&0&1&1&1 \\ 0&0&0&0&1&1&1&1 \end{pmatrix}, \quad B_1 = \begin{pmatrix} 0&1&1&1&1&0&0&0 \\ 1&0&1&1&1&0&0&0 \\ 1&1&0&1&1&0&0&0 \\ 1&1&1&0&1&0&0&0 \\ 1&1&1&1&0&0&0&0 \end{pmatrix}.$$

The basis matrices for the verification image are $V_0 = [0, 0, 0, 0, 0]'$ or $V_0 = [1, 1, 1, 1, 1]'$, as well as $V_1 = [b_1, b_2, b_3, b_4, b_5]'$ or $V_1 = [1 - b_1, 1 - b_2, 1 - b_3, 1 - b_4, 1 - b_5]'$. The resulting pixel expansion m' is 9. We can get the four basis matrices $B_{p,q}$ of $(3, 5)-$VXVC scheme, $p, q \in \{0, 1\}$. The contrasts for the secret image are $\alpha_s = \frac{4}{9}$ when 3 shares are XOR-ed. The contrast for the verification image is $\alpha_v = \frac{1}{18}$ when even number of shares are XOR-ed. The verification image requires $N > 9/(\frac{1}{18} - d)^2 \geq 54^2$. The secret image and verification image are given in Fig. 1a and b with size 180×180. The share images and reconstructed images are shown in Fig. 1c–r. The secret image is revealed when three shares are XOR-ed. The verification image is revealed when two shares are XOR-ed. The security and contrast conditions are satisfied. We find that when 5 shares are XOR-ed, the secret image also appears. This is determined by the properties of the $(3, 5)-$XVC scheme. When 4 shares are XOR-ed, the verification image appears but the secret image does not. A special characteristic of the $(3, 5)-$VXVC scheme is $H(\otimes(B_1|U)) = H(\otimes(B_0|U))$ for $|U| = 4$.

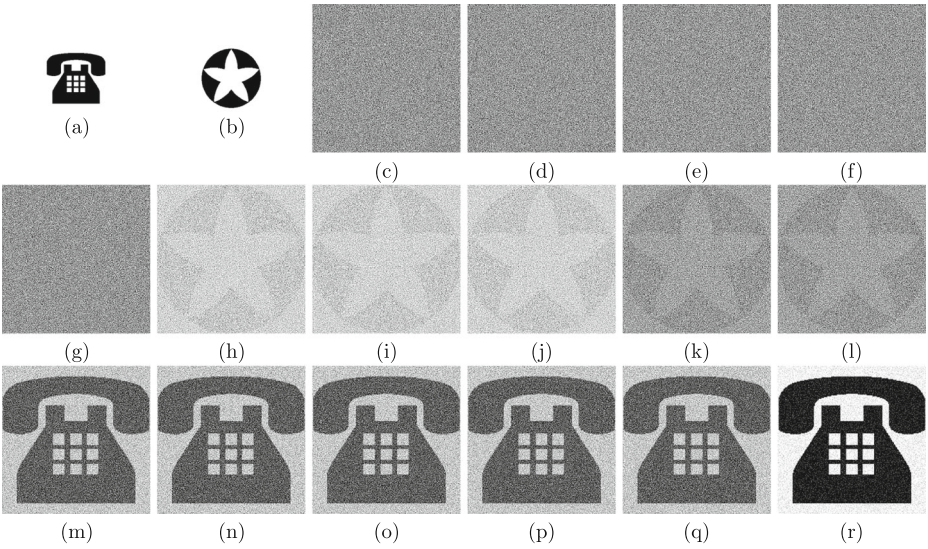

Fig. 1 The share images and reconstructed images for (2,5)-VXVC scheme, **a** secret image, **b** verification image, **c** share S_1, **d** share S_2, **e** share S_3, **f** share S_4, **g** share S_5, **h** $S_1 \otimes S_3$, **i** $S_2 \otimes S_4$, **k** $S_1 \otimes S_2 \otimes S_3 \otimes S_4$, **l** $S_2 \otimes S_3 \otimes S_4 \otimes S_5$, **m** $S_1 \otimes S_2 \otimes S_3$, **n** $S_2 \otimes S_3 \otimes S_4$, **o** $S_3 \otimes S_4 \otimes S_5$, **p** $S_1 \otimes S_3 \otimes S_5$, **q** $S_2 \otimes S_4 \otimes S_5$, **r** $S_1 \otimes S_2 \otimes S_3 \otimes S_4 \otimes S_5$

In our scheme, we emphasize on the recovery of the secret image, not the verification image. Thus, recovered secret image has high contrast but the recovered verification image has lower contrast. In fact, we can adjust their visual quality. The $(2, n)-$PXVC scheme can be replaced with a deterministic $(2, n)-$XVC scheme [6]. Then we can do a probabilistic combination of $(k, n)-$XVC scheme and $(2, n)-$XVC scheme to adjust their visual quality. This scheme can be seen in some previous work [12].

4.2 Comparison with the state-of-the-art approaches

The efficiency of the proposed scheme is compared with other verifiable VC schemes in terms of pixel expansion, contrast for the secret image, contrast for the verification image, applicable range of threshold k, operation and additional verification shares shown in Table 1. Here we assume that the established $(k, n)-$VC scheme has pixel expansion m and contrast α.

From Table 1, we can see that scheme I in [8] and schemes in [12, 21] have the same share size as the original threshold scheme but schemes in [8, 21] require additional verification shares. They doubly increase storage complexity of the participants. Scheme in [12] decreases the contrast exponentially. Schemes in [20, 26] and Scheme II in [8] have large extra pixel expansion in order to achieve the verification function. Scheme [9] has slight larger share size than that of the original scheme, but it also requires the additional shares to authenticate other participants. Our proposed scheme can be used to achieve verification function based on either a $(k, n)-$VC scheme or a $(k, n)-$XVC scheme. It improves the contrast almost 2^{k-1} times, compared with that of the original $(k, n)-$VC scheme. It just increases one pixel expansion if it is constructed based on a established $(k, n)-$XVC scheme but it can maintain similar contrast of the original scheme.

Table 1 The performance comparison

Scheme	Pixel expansion	Contrast (secret image)	Contrast (verification image)	k	Operation	Additional (share)
Scheme I in [8]	m	α	m	$k(\geq 2)$	OR	Yes
Scheme II in [8]	$m \cdot \frac{2(n+l)^2}{n}$	$\frac{m}{m+l}\alpha$	m	2	OR	No
Scheme [20]	$m+n+1$	$\frac{m}{m+n+1}\alpha$	$\frac{1}{m+n+1}$	2	OR	No
Scheme [26]	$m \cdot \frac{n(n-1)}{2}$	$\frac{1}{2}$		2	OR	No
Scheme [9]	$m+2$	$\frac{\alpha \cdot m+1}{m+2}$	$\frac{1}{m+2}$	$k(\geq 2)$	OR	Yes
Scheme [21]	m	α	$\frac{1}{2}$	$k(\geq 2)$	OR	Yes
Scheme [12]	m	$\frac{1}{2}\alpha$	$\frac{1}{4}$	$k(\geq 2)$	OR	No
our VXCS	$m+1$	$\frac{2^{k-1}\dot{m}}{m+1}\alpha$	$\frac{1}{2(m+1)}$	$k(\geq 2)$	XOR	No

5 Conclusions

In this paper, we present a novel $(k, n)-$VXVC scheme for an established $(k, n)-$XVC scheme without resorting to any complex algorithms. Based on our construction, any VC scheme or XVC scheme for sharing a single secret can be transformed into a verifiable secret scheme easily by increasing one pixel expansion. Compared with previous verifiable VC schemes, the proposed scheme can improve the contrast by $\frac{m}{m+1}2^{k-1}$ times and almost keeps the same pixel expansion. The proposed scheme is more optimal in both visual quality and pixel expansion than previous schemes. The proposed scheme is applicable for an odd threshold and had lower visual effect for an even threshold. An interesting open problem is to further improve the construction for even threshold. The VC schemes have both encryption and key management properties and can recover the secret visually. They are proposed to be used in steganography and electric wallet. The proposed scheme provides a secure methodology for multimedia covert communication forensics. It also presents a new strategy for secure storage of multimedia content on cloud-based hosting and for secure confidential information transmission over the network.

Acknowledgments This work was supported in part by 2017 Teaching and Research Program of Lanzhou University under Grant No. 2017114, in part by the National Natural Science Foundation of China under Grant Nos. U1536102, U1536116, U1636219, and 61872289, in part by Plan for Scientific Innovation Talent of Henan Province (No. 2018JR0018) and the Science and Technology Program of Guangxi (No. 16380076), in part by China Mobile Research Fund Project (MCM20170407), and Key Laboratory of Digital Content Anti-Counterfeiting and Security Forensics of the state Administration of Press, Publication, Radio, Film and Television of the People's Republic of China.

References

1. Adhikari A (2014) Linear algebraic techniques to construct monochrome visual cryptographic schemes for general access structure and its applications to color images. Des Codes Crypt 73(3):865–895
2. Arazi B, Dinstein I, Kafri O (1989) Intuition, perception, and secure communication. IEEE Trans Syst Man Cybern 19(5):1016–1020

3. Chang CC, Lin CC, Le THN, Le HB (2009) Sharing a verifiable secret image using two shadows. Pattern Recogn 42(11):3097–3114
4. Chen YC, Horng G, Tsai DS (2012) Comment on "cheating prevention in visual cryptography". IEEE Trans Image Process: A Publication of the IEEE Signal Processing Society 21(7):3319
5. Chen YC, Tsai DS, Horng G (2012) A new authentication based cheating prevention scheme in Naor–Shamir's visual cryptography. J Vis Commun Image Represent 22(1):55–63
6. Cimato S, De Prisco R, De Santis A (2006) Probabilistic visual cryptography schemes. Comp J 49:97–107
7. D'Arco P, De Prisco R (2014) Secure two-party computation a visual way. In: Padró C (ed) Information theoretic security. Springer International Publishing, Cham, pp 18–38
8. Horng G, Chen T, Tsai DS (2006) Cheating in visual cryptography. Des Codes Crypt 38(2):219–236
9. Hu CM, Tzeng WG (2007) Cheating prevention in visual cryptography. IEEE Trans Image Process A Publication of the IEEE Signal Processing Society 16(1):36–45
10. Ito R (1999) Image size in variant visual cryptography. IEICE Trans Fundam 82(10):2172–2177
11. Jia X, Wang D, Nie D, Zhang C (2018) Collaborative visual cryptography schemes. IEEE Trans Circ Syst Video Technol 28(5):1056–1070
12. Lin PY, Wang RZ, Chang YJ, Fang WP (2015) Prevention of cheating in visual cryptography by using coherent patterns. Inf Sci 301(C):61–74
13. Liu F, Wu C, Lin X (2011) Cheating immune visual cryptography scheme. IET Inf Secur 5(1):51–59
14. Liu Y, Guo W, Fan C, Chang L, Cheng C (2018) A practical privacy-preserving data aggregation (3pda) scheme for smart grid. IEEE Trans Ind Inf 1–1. https://doi.org/10.1109/TII.2018.2809672
15. Luo X, Song X, Li X, Zhang W, Lu J, Yang C, Liu F (2016) Steganalysis of hugo steganography based on parameter recognition of syndrome-trellis-codes. Multimed Tools Appl 75(21):13557–13583
16. Liu Y, Zhong Q, Chang L, Xia Z, He D, Cheng C (2017) A secure data backup scheme using multi-factor authentication. IET Inf Secur 11(5):250–255
17. Ma Y, Luo X, Li X, Bao Z, Zhang Y (2018) Selection of rich model steganalysis features based on decision rough set -positive region reduction. IEEE Trans Circuits Syst Video Technol PP(99). https://doi.org/10.1109/TCSVT.2018.2799243
18. Naor M, Pinkas B (1997) Visual authentication and identification. In: Beth T (ed) Cryptography: proceedings of the workshop on cryptography advances in cryptology - Crypto'97, vol 1997. Springer, Berlin, pp 322–336
19. Naor M, Shamir A (1994) Visual cryptography. In: Beth T (ed) Cryptography: proceedings of the workshop on cryptography advances in cryptology - EUROCRYPT '94, vol 1994. Springer, De Santis, Berlin, pp 1–12
20. Prisco RD, Santis AD (2010) Cheating immune threshold visual secret sharing. Comput J 53(9):1485–1496
21. Ren Y, Liu F, Guo T, Feng R, Lin D (2017) Cheating prevention visual cryptography scheme using latin square. IET Inf Secur 11(4):211–219
22. Shen G, Liu F, Fu Z, Yu B (2016) Perfect contrast xor-based visual cryptography schemes via linear algebra. Des Codes Crypt 85(1):1–23
23. Shyu SJ (2017) XOR-based visual cryptographic schemes with monotonously increasing and flawless reconstruction properties. IEEE Trans Circuits Syst Video Technol PP(99):1–1
24. Shyu SJ, Chen MC (2011) Optimum pixel expansions for threshold visual secret sharing schemes. IEEE Trans Inf Forensics Secur 6(3):960–969
25. Singh P, Raman B, Misra M (2018) A (n, n) threshold non-expansible xor based visual cryptography with unique meaningful shares. Signal Process 142:301–319
26. Tsai DS, Chen TH, Horng G (2007) A cheating prevention scheme for binary visual cryptography with homogeneous secret images. Pattern Recogn 40(8):2356–2366
27. Tuyls P, Hollmann HDL, Lint JHV, Tolhuizen L (2005) XOR-based visual cryptography schemes. Des Codes Cryptogr 37(1):169–186
28. Wang D, Zhang L, Ma N, Li X (2007) Two secret sharing schemes based on boolean operations. Pattern Recogn 40(10):2776–2785
29. Wu X, Sun W (2014) Extended capabilities for XOR-based visual cryptography. IEEE Trans Inf Forensics Secur 9(10):1592–1605
30. Yang CN (2004) New visual secret sharing schemes using probabilistic method. Pattern Recogn Lett 25(4):481–494
31. Yang CN, Wang DS (2014) Property analysis of XOR-based visual cryptography. IEEE Trans Circ Syst Video Technol 24(2):189–197
32. Yuan HD (2014) Secret sharing with multi-cover adaptive steganography. Inf Sci 254:197–212
33. Zhang Y, Qin C, Zhang W, Liu F, Luo X (2018) On the fault-tolerant performance for a class of robust image steganography. Signal Process 146:99–111

Xingxing Jia received the B.S. and Ph.D. degrees from the School of Mathematics and Statistics, Lanzhou University, Lanzhou, China, in 2004 and 2010, respectively. She is currently a lecturer with the School of Mathematics and Statistics, Lanzhou University. Her research interests include secret sharing and visual cryptography.

Daoshun Wang received the B.S. degree from the Department of Mathematics, Lan Zhou University, China, in 1987, and the Ph.D. degree from the Department of Mathematics, Sichuan University, China, in 2001. He is currently an associate professor with the Department of Computer Science and Technology, Tsinghua University. His research interests include visual cryptography, digital watermarking, and label anti-counterfeit.

Qimeng Chu was born in Henan Province, China, in 1997. He received the B.S. degree from the School of Mathematics and Statistics, Lanzhou University, Lanzhou, China, in 2018. His research majors in visual cryptography.

Zhenhua Chen received her Ph. D. degree from Shaanxi Normal University in 2014. She is currently a associate professor with School of Computer Science and Technology, Xi'an University of Science and Technology. Her research interests include public-key cryptography, secure multi-party computation, and secret sharing.