IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 21, 2020, accepted February 10, 2020, date of publication February 13, 2020, date of current version February 25, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2973659

A Construction Method of (2, 3) Visual Cryptography Scheme

PENG LI[1], JIANFENG MA[1], LIPING YIN[1], AND QUAN MA[2]
[1]Department of Mathematics and Physics, North China Electric Power University, Baoding 071003, China
[2]Science and Technology on Reactor System Design Technology Laboratory, Nuclear Power Institute of China, Chengdu 610213, China

Corresponding authors: Peng Li (lphit@163.com) and Quan Ma (maquannpic@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61602173, in part by the Natural Science Foundation of Hebei Province under Grant F2019502173, and in part by the Fundamental Research Funds for Central Universities under Grant 2019MS116.

ABSTRACT Visual cryptography scheme (VCS) shares a binary secret image into multiple shadows, stacking qualified set of shadows will decode the secret image without computer resources. In this paper, we propose a (2, 3)-VCS, which can share one or two secret images into 3 shadows, stacking any two shadows will reveal the secret image. The shadow size is 3/2 times of the secret image. The contrasts of the revealed image are 1/3 and 1/2 when we share one and two secret images, respectively. We can also reveal the secret image by XOR decoding operation, and the visual quality of the revealed image can be further improved. By XOR decoding operation, the contrasts of the revealed image will be 2/3 and 1 when we share one or two secret images, respectively. In the case of sharing two secret images, the revealed two secret images have no distortion. Theoretic analysis and experimental results demonstrate the feasibility and advantages of the proposed (2, 3)-VCS.

INDEX TERMS Boolean operation, threshold scheme, secret image sharing, visual cryptography.

I. INTRODUCTION

Visual cryptography scheme (VCS) proposed by Naor and Shamir [1] encodes a binary secret image into multiple share images (also called shadows) and then distribute shadows to the corresponding participants. The decoding process is easy to be implemented. By printing shares on transparencies and then stacking them together, the secret information can be recognized by human visual system without any complex mathematical computation. Generally, for (k, n) threshold VCS, a secret image is first shared into n shadows. One secret pixel is expanded into m $(m > 1)$ pixels of each shadow. With any k or more shadows, the secret image can be revealed by stacking these shadows, while any k-1 or less shadows can get no information about the secret. Although VCS has the advantage of stacking-to-see decoding property, the visual quality of the revealed image is degraded. Following with Naor and Shamir's pioneer work, many VCSs were proposed with special properties, such as sharing gray and color images [2]–[4], progressive recovering VCS [5]–[7], sharing multiple images [8], [9], and VCS with meaningful shadows [10]–[12].

Pixel expansion of shadows and visual quality of the revealed image are the two most important indicators to measure the performance of VCS. Many VCSs were proposed to reduce shadow size and improve the visual quality of the revealed image. In Naor and Shamir's VCS, one secret pixel will be expanded into m $(m > 1)$ shadow pixels. Each shadow has m times size expansion. Probabilistic VCSs were proposed to reduce the size expansion [13], [14]. Yang [13] proposed probabilistic VCS, in which each shadow has the same size of the secret image. Cimato et al. [14] introduced probabilistic VCS that can achieve better visual quality at the price of larger size expansion. Researchers proposed random grid based visual secret sharing schemes [15], [16]. These schemes can achieve non-expansible shadows. However, the visual quality of revealed image is seriously degraded.

The visual quality of the revealed image is usually evaluated by contrast. Many researchers focused on improving visual quality by constructing VCS with optimal contrast [17], [18]. In traditional VCS, the stacking operation on shadows can be viewed as an implementation of Boolean OR operation. Actually, Boolean XOR operation can be realized by OR and inverse operations. With a copy machine that can copy and reverse transparences, we can implement XOR operation without computation. Obviously, XOR

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

operation can be also implemented by using light-weight computational devices, such as cell phone and smart devices. Therefore, many XOR-based VCS (XVCS) were proposed to improve contrast. Tuyls *et al.* [19] studied the threshold visual secret sharing schemes associated to XVCS systems. Wang *et al.* [20] proposed XVCS for $(2, n)$ and (n, n) thresholds. Liu *et al.* [21] proposed XVCS for general access structure by using (2, 2)-XVCS as the building block. Wu and Sun [22] proposed XVCS without size expansion and no code book required. Shen *et al.* [23] proposed the perfect contrast XVCS via linear algebra. The minimal qualified sets are partitioned into multiple parts. For each part of qualified sets, a sub-shadow is generated for each participant. The final shadow is a concatenation of multiple sub-shadows. Yang and Wang [24] analyzed the relationship between OR-based VCS and XVCS, and realized XVCS by using the basis matrices of OR-based VCS. Some researchers also tried to explore the application of VCS [25]. There are also come secret image sharing schemes with two decoding options [26]–[28]. A vague secret image can be decoded by stacking shadows, and a precise secret image can be decoded by computation.

In this paper, we focus on a special case of (k, n)-VCS, that is (2, 3)-VCS. Our main contribution is that we propose a novel construction method for (2,3)- VCS. The decoding process of our (2, 3)-VCS can be implemented by both OR and XOR operations. The proposed scheme can share one or two secret images. By OR decoding operation, the contrast of the proposed (2,3)- VCS is 1/3 when sharing one secret image, and 1/2 when sharing two secret images. By XOR operation, the contrast of the proposed scheme is 2/3 and 1 when sharing one and two secret images, respectively. The size expansion of each shadow is 1.5. When sharing two secret images, the secret images can be revealed without distortion and expansion.

The rest of the paper is organized as follows. In Section 2, we give the terminology and concepts used in the following sections, as well as OR based VCS and XVCS. The proposed scheme, and the theoretical analysis are included in Section 3. In Section 4, we show the experimental results and comparisons. Finally, we briefly conclude in Section 5.

II. RELATED WORKS

A. VISUAL CRYPTOGRAPHY SCHEME

Let $P = \{1, 2, \ldots, n\}$ is the set of all participants in a VCS and 2^P denotes the set of all subsets of P. Let $\Gamma_{Qual} \subseteq 2^P$, and $\Gamma_{Forb} \subseteq 2^P$, where $\Gamma_{Qual} \cap \Gamma_{Forb} = \emptyset$, and the elements in the Γ_{Qual} are referred to as qualified sets and the elements in the Γ_{Forb} are referred to as forbidden sets. The pair $(\Gamma_{Qual}, \Gamma_{Forb})$ is called the access structure.

Let Γ_0 denotes all the minimal qualified sets, which is defined as follows.

$\Gamma_0 = \{A \in \Gamma_{Qual} \,|A' \notin \Gamma_{Qual}$ for all $A' \subset A\}$

Let Γ_M denotes the set of all the maximal forbidden sets, which is

$\Gamma_{\mathrm{M}} = \{A \in \Gamma_{Forb} | A \cup \{i\} \in \Gamma_{Qual}$ for all $i \in P \backslash A\ \}$

The access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ on $P = \{1, 2, \ldots, n\}$ is called non-monotone if $\Gamma_{Qual} = \Gamma_0$. Otherwise, it is called monotone.

In particular, for a (k, n)-VCS, $\Gamma_{Qual} = \{A | A \subseteq P$, and $|A| \geq k\}$ and $\Gamma_{Forb} = \{A | A \subseteq P$, and $|A| < k\}$. We also have $\Gamma_0 = \{A | A \subseteq P$, and $|A| = k\}$ and $\Gamma_M = \{A | A \subseteq P$, and $|A| = k\text{-}1\}$.

Two participants i and j, which belong to the access structure $(\Gamma_0, \Gamma_{Forb})$, are referred to as equivalent participants on Γ_0 if they satisfy that, for $\forall A \in \Gamma_M$, $i \in A$ if and only if $j \in A$, denoted by $i \sim j$.

VCS is usually constructed by a pair of Boolean matrices sets. A formally definition of VCS is shown as follows.

Definition 1 [1]: Let $P = \{1, 2, \ldots, n\}$ be the set of all of participants in (k, n)-VCS. Let m, l and h be non-negative integers satisfying $0 \leq l < h \leq m$. Two sets of $n \times m$ Boolean matrices C_0 and C_1 constitute an effective (k, n)- VCS if the following conditions are satisfied:

(1) (**Contrast Condition**) Let $X = \{i_1, i_2, \ldots, i_k\} \subseteq P$. For any $M \in C_0$ (resp. $M \in C_1$), the OR-ed result on rows of M by restricting to the rows $i_1, i_2, \ldots, i_k$ is a vector v, that satisfies $\omega(v) \leq l$ (resp. $\omega(v) \geq h$), where $\omega(v)$ denotes the hamming weight of v.

(2) (**Security Condition**) For any $i_1, i_2, \ldots, i_k$ in P with $p < k$, two collections of F_1 and F_2, obtained by restricting each matrix in C_0 and C_1, respectively to the rows $i_1, i_2, \ldots, i_k$, are indistinguishable in the sense that they contain the same matrices with the same frequencies.

In the construction of VCS, the two collections of matrices C_0 and C_1 are usually generated by permuting the columns of two basis matrices B_0 and B_1, respectively. For a (k, n)-VCS constructed with two collections of matrices C_0 and C_1, to share a white (resp. black) secret pixel, a dealer randomly chooses a matrix from C_0 (resp. C_1), and distribute n rows of the chosen matrix to n shadows, respectively. Since each matrix has m columns, each shadow will receive m pixels when sharing one secret pixels. The shadow size is m times of the secret image. Usually, m is called size expansion of shadows. In order to reduce the cost in storage and transmission, the value of m should be as small as possible.

In decoding process, stacking shadows can visually perceive the content of the secret image. The underlined operation of stacking is Boolean OR operation. Actually, the OR-ed result of qualified shadows will not get the original secret image. Each secret pixel is represented by a block of pixels in the revealed image. By contrast condition in Definition 1, we know the number of black pixels in a block corresponding to black pixel is larger than that corresponding to white pixel. Let blackness refer to the proportion of black pixels in a block. For the black (resp. white) area of the revealed image, the blackness is h/m (resp. l/m). Then the difference between the blackness of black and white areas, denoted by contrast, can be perceived by our human visual system.

Formally, the contrast α is defined as follows.

$$\alpha = h/m - l/m = (h - l)/m$$

The definition of contrast is consistent with the definition in [1]. The value of α is between 0 and 1. When $\alpha = 1$, the visual quality of revealed secret image is the same as the secret image. In this case, VCS is called perfect. In practice, we need to construct VCS with the contrast as larger as possible

Example 1: (2, 3)-VCS [1]. Construct a (2,3)-VCS with basis matrices B_0 and B_1.

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

Permuting the columns of B_0 and B_1, we have two collections of share matrices C_0 and C_1, respectively.

$$C_0 = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

$$C_1 = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \right\}$$

In the sharing process, if a secret pixel is white (resp. black), randomly select a share matrix from C_0 (resp. C_1). The entries in the ith row of the share matrix are attributed to the ith shadow as the corresponding block of pixels. Until all secret pixels are processed, we have 3 generated shadows. Stacking any two of three shadows will visually decode the secret image. The size expansion of (2, 3)-VCS is 3 and the contrast is 1/3. Figure 1 shows the experimental result of Naor and Shamir's (2, 3)-VCS based on OR operation.

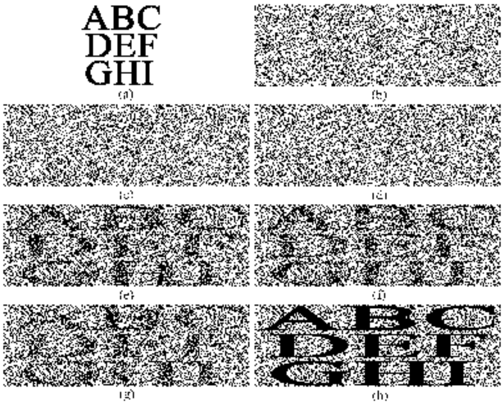

FIGURE 1. An experiment of Naor and Shamir's (2, 3)-VCS based on OR operation. (a) secret image; (b)-(d) three shadows; (e) revealed image by shadow 1 and shadow 2; (f) revealed image by shadow 1 and shadow 3; (g) revealed image by shadow 2 and shadow 3; (h) revealed image by three shadows.

B. *XOR-BASED VISUAL CRYPTOGRAPHY SCHEMES*

In Definition 1, the operation used in contrast condition is Boolean OR. VCS defined by Definition 1 is also called OR-based VCS. If we replace OR operation in Definition 1 by Boolean XOR operation, we have the definition of XOR-based VCS. Shen *et al.* [23] proposed a non-monotone XOR-based (k, n)-VCS. Specifically, for XOR-based (2, 3)-VCS, $\Gamma_{Qual} = \Gamma_0 =\{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$. Three qualified sets {1,2},{1,3} and {2,3} are represented by α, β, γ, respectively. For each qualified set, a pair of share matrices are generated by the basis matrix of (2, 2)-VCS. It should be noted that the row of basis matrix, corresponding to the uninvolved participant of the qualified set, is randomly generated with entries 0 or 1. The generated three pair of basis matrices are shown as follows.

$$B_0^{\alpha} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ * & * \end{pmatrix}, \quad B_1^{\alpha} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ * & * \end{pmatrix},$$

$$B_0^{\beta} = \begin{pmatrix} 0 & 1 \\ * & * \\ 0 & 1 \end{pmatrix}, \quad B_1^{\beta} = \begin{pmatrix} 1 & 0 \\ * & * \\ 0 & 1 \end{pmatrix},$$

$$B_0^{\gamma} = \begin{pmatrix} * & * \\ 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad B_0^{\gamma} = \begin{pmatrix} * & * \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

where * is assigned by 0 or 1 randomly.

Then partition the qualified sets Γ_0 into 2 parts $\Gamma 1\ 0 = \{\{1, 2\}, \{1, 3\}\}$ and $\Gamma 2\ 0 = \{\{2, 3\}\}$. For $\Gamma 1\ 0$, participant 2 and 3 are equivalent participants, which means they may have the same shadows. After combining the first two pair of basis matrices, we have the following two pair of basis matrices.

$$B_0^{\alpha\beta} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad B_1^{\alpha\beta} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}$$

$$B_0^{\gamma} = \begin{pmatrix} * & * \\ 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad B_1^{\gamma} = \begin{pmatrix} * & * \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

In the sharing process, a dealer first uses basis matrices $B_0^{\alpha\beta}$ and $B_1^{\alpha\beta}$ to share the secret image, and generate 3 sub-shadows as region 1 in the corresponding shadows. Then uses basis matrices B_0^{γ} and B_1^{γ} to share the secret image again, and generate another 3 sub-shadows as region 2 in the corresponding shadows. Note that only one column of basis matrix is randomly chosen to generate sub-shadows when sharing one secret pixel. Therefore, the size of each sub-shadow is the same as the secret image. The final shadow size is 2 times as the secret image. Region 1 and region 2 can be concatenated horizontally or vertically. In revealing process, the secret image can be decoded on a specific region when performing XOR operation on any two shadows. Figure 2 shows the experimental results of Shen et al.'s XOR-based (2, 3)-VCS.

III. THE PROPOSED (2,3)-VCS

A. *MOTIVATION*

Pixel expansion and contrast are two most concerns for VCS. To increase the contrast and decrease the pixel expansion,

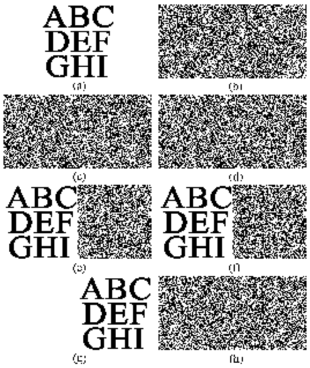

FIGURE 2. An experiment of Shen et al.'s (2, 3)-VCS based on XOR operation. (a) secret image; (b)-(d) three shadows; (e) revealed image by shadow 1 and shadow 2; (f) revealed image by shadow 1 and shadow 3; (g) revealed image by shadow 2 and shadow 3; (h) revealed image by three shadows.

we try to reduce the redundant pixels in shadows. Based on Shen et al.'s scheme [23], we proposed a (2, 3)-VCS with access structure partition. The randomly chosen pixels are eliminated by processing two secret pixels at one time. To process two pixels at one time, we need to construct basis matrices according to the different values of two pixels.

B. CONSTRUCTION OF THE BASIS MATRICES

In Shen et al.'s (2, 3)-VCS [23], two pairs of basis matrices $(B_0^{\alpha\beta}, B_1^{\alpha\beta})$ and $(B_0^{\gamma}, B_1^{\gamma})$ are constructed. However, there are randomly chosen pixels "$*$" in $(B_0^{\gamma}, B_1^{\gamma})$. We need to design new basis matrices, which can eliminate the random pixels "$*$". The main idea is that two share matrices can be merged if they have the same rows except for the rows that contain "$*$". We design the new basis matrices by processing two secret pixels at one time. For the first pixel a, the basis matrices are the same as those in Shen et al.'s scheme [23]. For convenience, we use a set of new notations here.

$$B_0^{a1} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad B_1^{a1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix},$$

$$B_0^{a2} = \begin{pmatrix} * & * \\ 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad B_1^{a2} = \begin{pmatrix} * & * \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Note that shadow 2 and shadow 3 decode the secret pixel a in region 2. Shadow 1 and shadow 2 decode the secret pixel a in region 1, so do shadow 1 and shadow 3.

For the second pixel b, the basis matrices are generated by switching the first two rows of above basis matrices. The third rows are unchanged. The new basis matrices are shown as follows.

$$B_0^{b1} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad B_1^{b1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$B_0^{b2} = \begin{pmatrix} 0 & 1 \\ * & * \\ 0 & 1 \end{pmatrix}, \quad B_1^{b2} = \begin{pmatrix} 1 & 0 \\ * & * \\ 0 & 1 \end{pmatrix}$$

Note that after switching rows of the basis matrices, the relation between the qualified set and region area may be changed. In this case, shadow 1 and shadow 3 will decode the secret pixel b in region 2. Shadow 1 and shadow 2 will decode the secret pixel b in region 1, so do shadow 2 and shadow 3. We also find that the random pixels in B_0^{a2} and B_1^{a2} are in the first row, while the random pixels in B_0^{b2} and B_1^{b2} are in the second row. And their third rows are the same. Since the qualified sets for decoding secret pixel in region 2 are different for secret pixels a and b, we can merge region 2 of secret pixel a and region 2 of secret pixel b as one region. In another word, both secret pixels a and b use the same region as their region 2. After combination, region 2 can be used to decode different secret information with different qualified sets. In the decoded image, region 2 may show the secret pixel a or secret pixel b. In the combined regions, the region 1 for secret pixel a is still region 1, and the region 1 for secret pixel b is represented as new region 3. Finally, secret pixel a will be decoded in region 1 or region 2, and secret pixel b will be decoded in region 2 or region 3. Figure 3 shows the relationship of the regions of two secret pixels.

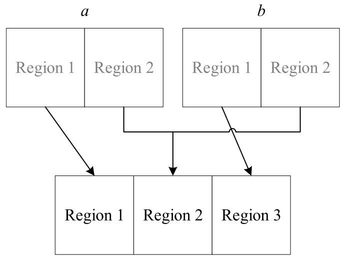

FIGURE 3. The relationship among regions of two secret pixels.

In addition, the basis matrix used for region 2 need to be reconstructed. Let p and q denote the value of secret pixels a and b, respectively. As we mentioned before, B_p^{a2} and B_q^{b2} have the same third rows, where p and q are in {0, 1}. We generate the basis matrix $B_{pq}^{Region2}$ for region 2, which has the same first row as B_q^{b2}, the same second row as B_p^{a2}, and the same third row as B_p^{a2} or B_q^{b2}.

For region 1, only secret pixel a will be decoded in region 1, then the basis matrix for region 1 $B_{pq}^{Region1}$ is the same as B_p^{a1}. For region 3, only secret pixel b will be decoded in region 3, then the basis matrix for region 3 $B_{pq}^{Region3}$ is the same as B_q^{b1}. For region 2, the first row of the basis matrix $B_{pq}^{Region2}$ is taken from the first row of B_q^{b2}, and the second and third rows of basis matrix $B_{pq}^{Region2}$ are taken from the second and third rows of B_p^{a2}.

For two binary secret pixels a and b with the values of p and q, there are four cases of permutation, i.e. 00, 01, 10 and 11. In convenience, we list out all the basis matrices for all cases as follows.

$$\text{Case1} : pq = 00$$

$$B_{00}^{Region1} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad B_{00}^{Region2} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix},$$

TABLE 1. The effective regions with different qualified set.

Qualified set	Region 1	Region 2	Region 3
(1, 2)	Effective	Non-effective	Effective
(1, 3)	Effective	Effective	Non-effective
(2, 3)	Non-effective	Effective	Effective

$$B_{00}^{Region3} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\text{Case2} : pq = 01$$

$$B_{01}^{Region1} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad B_{01}^{Region2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix},$$

$$B_{01}^{Region3} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\text{Case3} : pq = 10$$

$$B_{10}^{Region1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad B_{10}^{Region2} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$B_{10}^{Region3} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\text{Case4} : pq = 11$$

$$B_{11}^{Region1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad B_{11}^{Region2} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$B_{11}^{Region3} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

where $C_{pq}^{Regionr}$ denotes the basis matrix for region r with secret pixels' value p and q.

With above basis matrices, we can share a secret image into 3 shadows. Note that the secret pixels only shown in two out of three regions, called effective regions. The relationship between the qualified set and the effective regions is shown in the following table.

C. THE SHARING AND REVEALING PROCESSES

1) THE SHARING PROCESS FOR ONE SECRET IMAGE

For the case of one secret image, we share two continuous secret pixels at each time. According to the values p and q of these two secret pixels a and b, using basis matrices $B_{pq}^{Region1}$, $B_{pq}^{Region2}$ and $B_{pq}^{Region3}$ to generate shadows. First, randomly choose one column from basis matrix $B_{pq}^{Region1}$, and assign three entries of the chosen column to three shadows as their shadow pixels in region 1. In the same way, using basis matrices $B_{pq}^{Region2}$ and $B_{pq}^{Region3}$ to generate the shadow pixels in region 2 and region 3, respectively. By sharing two secret pixels, each shadow will receive three pixels. These three pixels are concatenated as a 3-pixel block. Figure 4 shows an example of the generation of shadow blocks. By sharing secret pixel a_1 and b_1, the first shadow receives three pixels S_{11}^1, S_{11}^2 and S_{11}^3 in region 1, region 2 and region 3, respectively. These pixels are concatenated as a 3-pixel shadow block in shadow 1. The shadow blocks of shadow 2 and shadow 3 are generated in the same way, where S_{ij}^k is the j-th shadow pixel of shadow i generated by sharing the k-th block of secret image, and a_k and b_k are the pixels in the k-th block of secret image.

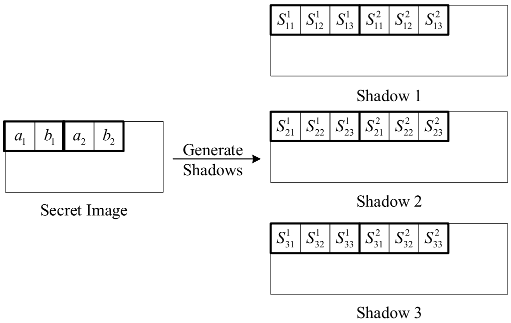

FIGURE 4. The generation process of shadows for sharing one image.

2) THE SHARING PROCESS FOR TWO SECRET IMAGES

Our scheme can also share two secret images simultaneously. As we introduced in Section 3.2, our scheme is designed by processing two secret pixels at one time. If these two secret pixels are coming from two secret image, respectively, our scheme can be used to sharing two secret images with the same sizes. Let A and B be the two secret images. First, we take the first pixel a_1 from A and the first pixel b_1 from B as a pair of secret pixels. Let p and q be the values of pixel a_1 and pixel b_1, respectively. Then, choose the basis matrices $B_{pq}^{Region1}$, $B_{pq}^{Region2}$ and $B_{pq}^{Region3}$ to generate shadows. By share a pair of secret pixels, one shadow will receive three pixels according to three regions. The shadow pixels are generated with the same method as that for sharing one secret image. The difference is the arrangement of the shadow pixels in three regions. Different from the method for sharing one secret image, all generated shadow pixels in the same region of each shadow are stored together. Hence each shadow is separated as three parts according to the pixels in three regions, respectively. Figure 5 shows the diagram of generating shadows with different regions. First, all pixels in the same region of each shadow are concatenated together. Then the three regions of each shadow are concatenated to generate the final shadow. Note that S_{ij}^k is the pixel of shadow i in region j generated by sharing the secret pixels a_k and b_k, where a_k and b_k are the k-th secret pixels of secret image A and B, respectively.

3) THE REVEALING PROCESS

In our proposed (2, 3)-VCS, we have two options to reveal the secret image. First, we can reveal the secret image by stacking any two out of three shadows. The stacking operation can be simulated by Boolean OR operation. The secret image can

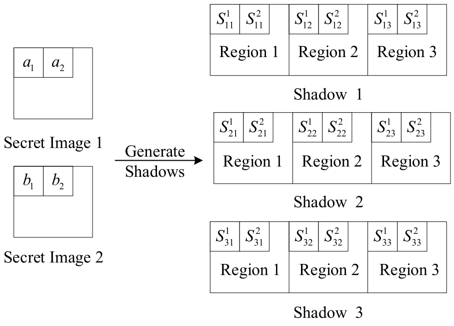
a_1 a_2
Secret Image 1
b_1 b_2
Secret Image 2
Generate Shadows
S^1_{11} S^2_{11} S^1_{12} S^2_{12} S^1_{13} S^2_{13}
Region 1 Region 2 Region 3
Shadow 1
S^1_{21} S^2_{21} S^1_{22} S^2_{22} S^1_{23} S^2_{23}
Region 1 Region 2 Region 3
Shadow 2
S^1_{31} S^2_{31} S^1_{32} S^2_{32} S^1_{33} S^2_{33}
Region 1 Region 2 Region 3
Shadow 3

FIGURE 5. The generation process of shadows for sharing two images.

be visually recognized with degreed visual quality. Second, the secret image can be decoded by XOR operation on any two shadows. By XOR operation, the revealed image will have better visual quality than that revealed by OR operation. Specifically, the secret images can be revealed perfectly as the original secret images when we share two secret images.

D. THEORETICAL ANALYSIS

In this subsection, we theoretically prove that the proposed (2, 3)-VCS satisfies the definition of VCS. For (2, 3)-VCS, any two out of three shadows consist of a qualified set, while each shadow is also a maximal forbidden set. To verify the proposed (2, 3)-VCS satisfies the security condition of VCS, we only need to prove that each shadow pixel is randomly selected in $\{0, 1\}$. To verify the contrast condition of (2, 3)-VCS, we only need to prove that the contrast value is larger than 0 by OR and XOR operations. In case of sharing two secret images, we only need to prove the contrast is larger than 0 in the effective regions.

First, we prove that the proposed (2, 3)-VCS satisfies the security condition.

Lemma 1: The proposed scheme satisfies the security condition of (2, 3)-VCS.

Proof: To prove that our scheme satisfies the security condition of (2, 3)-VCS, we need to prove any one shadow will not decode any information about the secret image. In the generation of shadows, each shadow pixel is generated by one entry of a randomly chosen column of a basis matrices. For each basis matrix, it is easy to verify that each row has two entries, 0 and 1. Therefore, the probabilities for each shadow pixel generated as 0 and 1 are the same. By one shadow, we cannot identify the secret pixels' values from the shadow values. Hence, the security condition of (2, 3)-VCS is satisfied. □

Next, we prove that our scheme satisfies the contrast condition, that is, the contrast of the revealed image is larger than 0. Since we have two decoding options with OR and XOR operations, we need to prove that the proposed (2, 3)-VCS satisfies the contrast condition by OR and XOR operations. In addition, we have two kinds of regions arrangements. For the first regions arrangement, any two-pixel secret block is shared into a three-pixel shadow block of each shadow. In another word, a secret pixel is shared into one and half shadow pixels. We need to verify that the average blackness in black area is larger than that in white area, and calculate the average contrast in three regions. For the second regions arrangement, three regions are concatenated region-by-region, and only two out of three regions of the revealed image are effective. We need the verify that the contrast in the effective regions is larger than 0. With the definition of contrast, we calculate the contrasts of the revealed images with different qualified sets of shadows and different regions arrangements. Table 2 and Table 3 show the contrasts of (2, 3)-VCS with different qualified sets using OR and XOR decoding operations, respectively.

TABLE 2. The contrasts of (2, 3)-VCS with different qualified sets using OR decoding operation.

Qualified set	The probabilities of the revealed pixels to be black in three regions with different values of p and q.				Effective regions	α_{Ave}	α_{Eff}
	pq=00	pq=01	pq=10	pq=11			
(1, 2)	0.5/0.5/0.5	0.5/1/1	1/1/0.5	1/0.5/1	1 and 3	1/3	1/2
(1, 3)	0.5/0.5/0.5	0.5/1/0.5	1/0.5/0.5	1/1/0.5	1 and 2	1/4	1/2
(2, 3)	0.5/0.5/0.5	0.5/0.5/1	0.5/1/0.5	0.5/1/1	2 and 3	1/4	1/2
(1, 2, 3)	0.5/0.5/0.5	0.5/1/1	1/1/0.5	1/1/1	1 and 3	5/12	1/2

TABLE 3. The contrasts of (2, 3)-VCS with different qualified sets using XOR decoding operation.

Qualified set	The probabilities of the revealed pixels to be black in three regions with different values of p and q.				Effective regions	α_{Ave}	α_{Eff}
	pq=00	pq=01	pq=10	pq=11			
(1, 2)	0/0/0	0/1/1	1/1/0	1/0/1	1 and 3	2/3	1
(1, 3)	0/0/0	0/1/0	1/0/0	1/1/0	1 and 2	1/2	1
(2, 3)	0/0/0	0/0/1	0/1/0	0/1/1	2 and 3	1/2	1

For the first regions arrangement, we need to calculate the average contrast in the revealed image. Suppose that the secret image has the two-pixel blocks of values (0, 0), (0, 1), (1, 0) and (1, 1) with the same proportions. The average contrast of the revealed image is calculated by the average difference of darkness between the white area and black area. As shown in Table 2, by OR decoding operation, the average contrasts of the revealed image with the first regions arrangement are 1/3, 1/4 and 1/4 with qualified sets (1, 2), (1, 3) and (2, 3), respectively. If all three shadows are stacked, the average contrast will be increased to 5/12.

For the second regions arrangement, the black secret pixels will be definitely decoded as black pixels, and white pixels will be decoded as white pixels with possibility1/2. Hence the contrasts in the effective regions are always 1/2 with qualified sets (1, 2), (1, 3) and (2, 3). For the case when three shadows are stacked together, white secret pixels of secret image *A* (resp *B*) will be decoded as white pixels with possibility1/2 in region 1 (region 3), while the black secret pixels of secret image *A* (resp. *B*) will be decoded as black pixels with possibility 1 in region 1 (region 3). Therefore, the effective regions with qualified set of (1, 2, 3) are region 1 and region 3, and the contrast in effective regions is 1/2.

When we decode the secret image by using XOR operation, the visual quality of the revealed image is better than that using OR operation. Table 3 lists the decoded pixels in three regions with different qualified sets. For the first regions arrangement, we calculate the average contrast in all regions, and we have contrasts 2/3, 1/2 and 1/2 with qualified sets (1, 2), (1, 3) and (2, 3), respectively. For the second regions arrangement, two secret images will be perfectly decoded in two effective regions, and the contrasts are all 1. Since we have two entries 1 and 0 when we perform XOR operation on three rows of each basis matrix, the contrast of the revealed image will be 0 when we use three shadows to decode the secret image by XOR operation. Therefore, (1, 2, 3) is not a qualified set of (2, 3)-VCS when using XOR decoding operation.

From above analysis and the contrasts listed in Table 2 and Table 3, we have the following Lemma.

Lemma 2: The proposed scheme satisfies the contrast condition of (2, 3)-VCS, that is the contrast is larger than 0.

With Lemma 1 and Lemma 2, we have that the proposed scheme satisfies both the security condition and the contrast condition of VCS. Finally, we have the following theorem.

Theorem 1: The proposed scheme is a (2, 3)-VCS under both OR and XOR operations.

For the first regions arrangement in our proposed (2, 3)-VCS, two secret pixels are shared into three shadow pixels of each shadow. Hence the size expansion of shadows is 1.5. For the second region arrangement, two secret images are shared into three regions of each shadow, and only two regions are effective to decode two secret images. The revealed secret images in effective regions have the same size of the secret images. Although the shadow size is three times of one secret image, with two secret images shared simultaneously, the total size expansion of shadows is still 1.5. We conclude the result about size expansion in following theorem.

Theorem 2: The size expansion of the proposed (2, 3)-VCS is 1.5.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

In this section, we conduct some experiments of the proposed (2, 3)-VCS. We show the experimental result for sharing one secret image and two secret images using OR and XOR decoding operations. We also compare the proposed scheme with literature schemes on performances.

A. THE EXPERIMENTAL RESULTS OF THE PROPOSED (2, 3)-VCS FOR SHARING ONE SECRET IMAGE

In this experiment, a binary secret image S with the size of 256 × 256 pixels as shown in Fig. 6(a) is shared into 3 shadows. Figure 6 (b)-(d) show the 3 generated shadows. Each shadow has the size as 3 times of the secret image. Stacking any two shadows can reveal the secret image. The stacking operation can be simulated by Boolean OR operation.

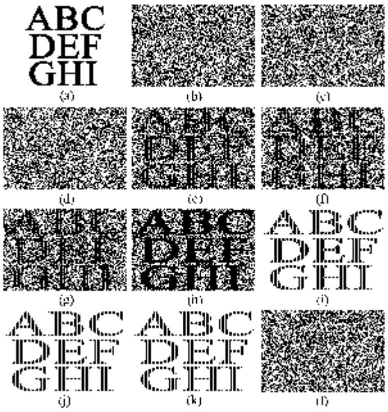

FIGURE 6. An experiment of the proposed (2, 3)-VCS sharing one secret image. (a) secret image; (b)-(d) three shadows; (e)-(g) revealed image by any two shadows with OR operation; (h) revealed image by three shadows with OR operation; (i)-(k) revealed image by any two shadows with XOR operation; (l) revealed image by three shadows with XOR operation.

Figure 6 (e)-(g) show the revealed image by staking shadows of qualified sets {1, 2}, {1, 3} and {2, 3}, respectively. The content of the secret image can be visual recognized by human visual system. By stacking three shadows, the revealed image has better visual quality as shown in Fig. 6 (h), and the contrast is 5/12. We can also reveal the secret image by Boolean XOR operation, and the revealed images are shown in Fig. 6 (i)-(k). Performing XOR operation on any two shadows, we have the revealed secret image. As we can see, the visual quality of the revealed image using XOR decoding operation is better than that using OR decoding operation. The contrast is increased to 2/3. Since {1, 2, 3} is not a qualified set of (2, 3)-VCS using XOR decoding operation, performing XOR operation on three shadows will not reveal the secret image. Figure 6. (l) shows the revealed image by three shadows using XOR operation, which is noise-like.

B. THE EXPERIMENTAL RESULTS OF THE PROPOSED (2, 3)-VCS FOR SHARING TWO SECRET IMAGES

In this experiment, two secret images are shared simultaneously. Figure 7 (a) and (b) shows two secret images with the same sizes 256 × 256. Successively select one secret pixel from each secret image, and then share them into three pixels of each shadow in three regions, respectively. Figure 7 (c)-(e) show three generated shadows. In the revealing process, we have two decoding operations to choose. First, we can reveal the secret image by OR operation, that is the secret image can be revealed by stacking any two shadows. Figure 7 (f)-(h) show the revealed image by the qualified sets of shadows {1, 2}, {1, 3} and {2, 3}, respectively. Since the shadow pixels are arranged region by region, two out of three regions are effective in the revealed image. The relation between the effective regions and the qualified set is shown in Table 1. By Table 2, we have that the contrasts of the revealed image in Fig. 7 (f)-(h) are all 1/2. When three shadows are stacked, the secret image is also revealed

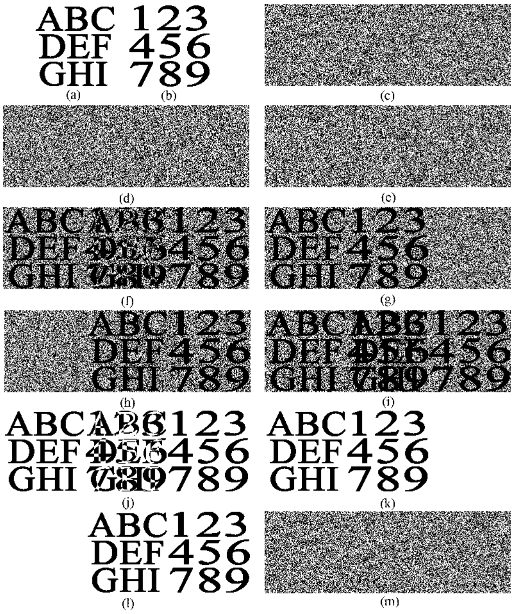

FIGURE 7. An experiment of the proposed (2, 3)-VCS sharing two secret images. (a) secret image A; (b) secret image B; (c)-(e) three shadows; (f)-(h) revealed image by any two shadows with OR operation; (i) revealed image by three shadows with OR operation; (j)-(l) revealed image by any two shadows with XOR operation; (m) revealed image by three shadows with XOR operation.

with the contrast 1/2 as shown in Fig. 7 (i). Second, we can reveal the secret image by XOR operation. Figure 7 (j)-(l) show the revealed images by performing XOR operation on the qualified sets of shadows {1, 2}, {1, 3} and {2, 3}, respectively. From the revealed images, we can see that two secret images are perfectly decoded in two effective regions. The contrasts of the revealed image in effective regions are all 1 by Table 3. The revealed image by performing XOR operation on three shadows is shown in Figure 7 (m), which shows that {1, 2, 3} is not a qualified set of the proposed (2, 3)-VCS using XOR decoding operation.

We also conduct an experiment using natural secret images. Since VCS only directly deals with binary images. We need process the secret image first to get a binary secret image. Two halftone dithered secret images "Lena" and "Baboon" with 512 × 512 pixels as shown in Fig. 8 (a) and (b) are first shared into three shadows as shown in Fig. 8 (c)-(e). Stacking any two out of three shadows can reveal two secret images in the corresponding regions. The revealed images are shown in Fig. 8 (f)-(h). We can also reveal the secret mage by stacking all shadows, and the revealed image is shown in Fig. 8(i). By Table 2, we have that the contrasts of the revealed images in the effective regions in Fig. 8 (f)-(h) are all 1/2. In addition, we can also reveal the secret image by XOR operation, and the revealed images are shown in Fig. 8 (j)-(m). As we can see, two secret images can be perfectly revealed in the effective regions. The contrasts in the effective regions are all 1 by Table 3.

To further measure the visual quality of the decoded secret images, we calculate the PSNR and SSIM values of the revealed images. Since the decoded secret images have the same sizes with the original secret images when sharing two secret images, we only calculate PSNR and SSIM values of the revealed images in Fig. 7 and Fig. 8 as shown in Table 4. Note that, the white pixel is represented as 255, and black pixel is represented as 0 when we calculate PSNR and SSIM values. As we can see, the revealed images by OR operation have poor visual quality, while the revealed images by XOR operation have perfect visual quality as original secret images.

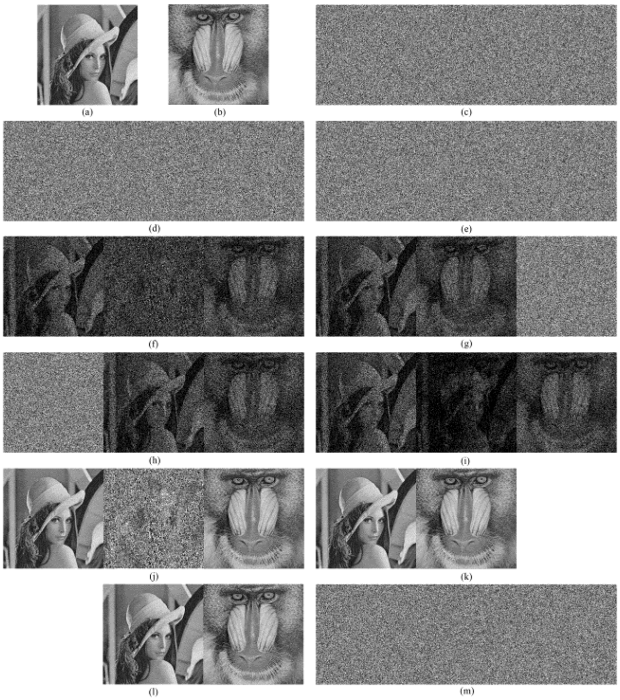

FIGURE 8. An experiment of the proposed (2, 3)-VCS using two natural secret images. (a) secret image A; (b) secret image B; (c)-(e) three shadows; (f)-(h) revealed image by any two shadows with OR operation; (i) revealed image by three shadows with OR operation; (j)-(l) revealed image by any two shadows with XOR operation; (m) revealed image by three shadows with XOR operation.

TABLE 4. The PSNR and SSIM values of the revealed images.

	PSNR		SSIM	
	Image A	Image B	Image A	Image B
Fig. 7(f)	4.7691	4.8794	0.27886	0.28033
Fig. 7(g)	4.7691	4.8026	0.27886	0.26571
Fig. 7(h)	4.7107	4.8794	0.26546	0.28033
Fig. 7(i)	4.7691	4.8794	0.27886	0.28033
Fig. 7(j)	Inf	Inf	1	1
Fig. 7(k)	Inf	Inf	1	1
Fig. 7(l)	Inf	Inf	1	1
Fig. 8(f)	6.2737	5.9893	0.45014	0.45076
Fig. 8(g)	6.2737	5.9825	0.45014	0.44962
Fig. 8(h)	6.2848	5.9893	0.45229	0.45076
Fig. 8(i)	6.2737	5.9893	0.45014	0.45076
Fig. 8(j)	Inf	Inf	1	1
Fig. 8(k)	Inf	Inf	1	1
Fig. 8(l)	Inf	Inf	1	1

TABLE 5. Comparison of the proposed scheme and some existing schemes.

Schemes	Type	Decoding Operation	Number of secret images	Contrast	Pixel Expansion
Ref. [1]	"D"	OR	one	1/3	3
Ref. [3]	"P"	OR	one	1/3	1
Ref. [9]	"D"	OR	two	1/6	6
Ref. [21]	"D"	XOR	one	1/2	10/3
Ref. [23]	"D"	XOR	one	1	2
Ref. [26]	"P"	OR	one	0.124	1
	"P"	XOR	one	0.25	1
Ref. [27]	"P"	OR	One	5/17	1
	"P"	XOR	One	2/5	1
	"D"	OR	One	1/3	3
Ref. [28]	"D"	Lagrange interpolation	One	1	$1/k$
Ours	"P"	OR	one	1/3	1.5
	"P"	OR	two	1/2	1.5
	"D"	XOR	one	2/3	1.5
	"D"	XOR	two	1	1.5

C. COMPARISON AND DISCUSSION

In this subsection, we compare our (2,3)- VCS with literature VCSs on performances and other property. First, we list out the sharing type of all schemes. There are two types, that are deterministic and probabilistic. For deterministic type, although the visual quality of the revealed image may be degraded, there is no information loss in the revealed image. For probabilistic type, the original secret image cannot be revealed perfectly even with computer resources. Second, we compared with decoding operations. For OR operation, we can easy implement it by stacking shadows without using computer. For XOR operation, we only need some light-weight devices. However, for Lagrange interpolation, we need complicated computation with computer. Finally, the contrast and pixel expansion under different decoding operations are compared. Since the definition of contrast in our scheme is consistent with that in the reference [1], the values can be directly compared. We also compare the proposed scheme with VCS sharing multiple secret images. The comparison results are shown in Table 5. The deterministic type is denoted by "D", and the probabilistic type is denoted by "P". For sharing one secret image, our scheme has the size expansion 1.5, which is small than the size expansion of Naor and Shamir's VCS 3. Although Yang's VCS has the size expansion 1, their scheme is probabilistic and the visual quality of the revealed image is very poor. We cannot reveal the original secret image even with computer resources. The contrast of the proposed scheme is 1/3 when stacking shadow 1 and shadow 2, and increased to 5/12 when stacking three shadows. If we reveal the secret image by XOR operation, the contrast is increased to 2/3. For sharing two secret images, the total shadow expansion is still 1.5. However, two secret images can be revealed in two effective regions without expansion and distortion. If we use OR decoding operation, the revealed secret images in effective regions have the contrast 1/2. If we use XOR decoding operation, the contrasts in effective regions are 1, and the secret images are perfectly revealed.

V. CONCLUSION

In this paper, we proposed a novel construction of (2,3)- VCS. The proposed scheme can share one or two secret images. Compared with size expansion 3 in Naor and Shamir's OR-based VCS and 2 in Shen et al.'s XOR-based VCS, the size expansion of the proposed scheme is 1.5. When sharing two secret images, the secret images can be revealed in two effective regions of the revealed image without expansion. In the decoding process, we have two choices of decoding operation. The secret image can be revealed by using both OR and XOR operations. When we share one secret image, the contrasts are 1/3 with OR operation, and 2/3 with XOR operation. When we share two secret images, the contrasts are increased to 1/2 and 1 with OR and XOR operations, respectively. To sum up, the proposed scheme has good performances on size expansion and visual quality of the revealed image. A future work might be constructing general (k, n)-VCS using proposed scheme as a building block to achieve better performances.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in *Cryptology-Eurocrypt'94* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1995, pp. 1–12.

[2] Y.-C. Hou, "Visual cryptography for color images," *Pattern Recognit.*, vol. 36, no. 7, pp. 1619–1629, Jul. 2003, doi: 10.1016/S0031-3203(02)00258-3.

[3] C.-N. Yang and T.-S. Chen, "Colored visual cryptography scheme based on additive color mixing," *Pattern Recognit.*, vol. 41, no. 10, pp. 3114–3129, Oct. 2008, doi: 10.1016/j.patcog.2008.03.031.

[4] S. J. Shyu, "Efficient visual secret sharing scheme for color images," *Pattern Recognit.*, vol. 39, no. 5, pp. 866–880, May 2006, doi: 10.1016/j.patcog.2005.06.010.

[5] Y.-C. Hou, Z.-Y. Quan, C.-F. Tsai, and A.-Y. Tseng, "Block-based progressive visual secret sharing," *Inf. Sci.*, vol. 233, pp. 290–304, Jun. 2013, doi: 10.1016/j.ins.2013.01.006.

[6] X. Yan, S. Wang, and X. Niu, "Threshold progressive visual cryptography construction with unexpanded shares," *Multimedia Tools Appl.*, vol. 75, no. 14, pp. 8657–8674, Jul. 2016, doi: 10.1007/s11042-015-2779-y.

[7] S. Shivani and S. Agarwal, "VPVC: Verifiable progressive visual cryptography," *Pattern Anal. Appl.*, vol. 21, no. 1, pp. 139–166, Feb. 2018, doi: 10.1007/s10044-016-0571-x.

[8] S. J. Shyu, S.-Y. Huang, Y.-K. Lee, R.-Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography," *Pattern Recognit.*, vol. 40, no. 12, pp. 3633–3651, Dec. 2007, doi: 10.1016/j.patcog.2007.03.012.

[9] J.-B. Feng, H.-C. Wu, C.-S. Tsai, Y.-F. Chang, and Y.-P. Chu, "Visual secret sharing for multiple secrets," *Pattern Recognit.*, vol. 41, no. 12, pp. 3572–3581, Dec. 2008, doi: 10.1016/j.patcog.2008.05.031.

[10] D. Wang, F. Yi, and X. Li, "On general construction for extended visual cryptography schemes," *Pattern Recognit.*, vol. 42, no. 11, pp. 3071–3082, Nov. 2009, doi: 10.1016/j.patcog.2009.02.015.

[11] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 307–322, Jun. 2011, doi: 10.1109/TIFS.2011. 2116782.

[12] C.-N. Yang and Y.-Y. Yang, "New extended visual cryptography schemes with clearer shadow images," *Inf. Sci.*, vol. 271, pp. 246–263, Jul. 2014, doi: 10.1016/j.ins.2014.02.099.

[13] C.-N. Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognit. Lett.*, vol. 25, no. 4, pp. 481–494, Mar. 2004, doi: 10.1016/j.patrec.2003.12.011.

[14] S. Cimato, R. De Prisco, and A. De Santis, "Probabilistic visual cryptography schemes," *The Comput. J.*, vol. 49, no. 1, pp. 97–107, Jan. 2006, doi: 10.1093/comjnl/bxh152.

[15] Y.-C. Hou, S.-C. Wei, and C.-Y. Lin, "Random-grid-based visual cryptography schemes," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 24, no. 5, pp. 733–744, May 2014, doi: 10.1109/TCSVT.2013.2280097.

[16] C.-N. Yang, C.-C. Wu, and D.-S. Wang, "A discussion on the relationship between probabilistic visual cryptography and random grid," *Inf. Sci.*, vol. 278, no. 10, pp. 141–173, Sep. 2014, doi: 10.1016/j.ins.2014.03.033.

[17] C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," *SIAM J. Discrete Math.*, vol. 16, no. 2, pp. 224–261, Jan. 2003, doi: 10.1137/S0895480198336683.

[18] M. Krause and H. U. Simon, "Determining the optimal contrast for secret sharing schemes in visual cryptography," *Combinator. Probab. Comp.*, vol. 12, no. 3, pp. 285–299, May 2003, doi: 10.1017/S096354830200559X.

[19] P. Tuyls, H. D. L. Hollmann, J. H. V. Lint, and L. Tolhuizen, "XOR-based visual cryptography schemes," *Des., Codes Cryptogr.*, vol. 37, no. 1, pp. 169–186, Oct. 2005, doi: 10.1007/s10623-004-3816-4.

[20] D. Wang, L. Zhang, N. Ma, and X. Li, "Two secret sharing schemes based on Boolean operations," *Pattern Recognit.*, vol. 40, no. 10, pp. 2776–2785, Oct. 2007, doi: 10.1016/j.patcog.2006.11.018.

[21] F. Liu, C. Wu, and X. Lin, "Step construction of visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 27–38, Mar. 2010, doi: 10.1109/TIFS.2009.2037660.

[22] X. Wu and W. Sun, "Extended capabilities for XOR-based visual cryptography," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1592–1605, Oct. 2014, doi: 10.1109/TIFS.2014.2346014.

[23] G. Shen, F. Liu, Z. Fu, and B. Yu, "Perfect contrast XOR-based visual cryptography schemes via linear algebra," *Des., Codes Cryptogr.*, vol. 85, no. 1, pp. 15–37, Oct. 2017, doi: 10.1007/s10623-016-0285-5.

[24] C.-N. Yang and D.-S. Wang, "Property analysis of XOR-based visual cryptography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 24, no. 2, pp. 189–197, Feb. 2014, doi: 10.1109/TCSVT.2013.2276708.

[25] M. E. Vizcarra Melgar and M. C. Q. Farias, "A (2,2) XOR-based visual cryptography scheme without pixel expansion," *J. Vis. Commun. Image Represent.*, vol. 63, Aug. 2019, Art. no. 102592, doi: 10.1016/j.jvcir.2019.102592.

[26] X. Yan, S. Wang, A. A. A. El-Latif, and X. Niu, "Visual secret sharing based on random grids with abilities of AND and XOR lossless recovery," *Multimedia Tools Appl.*, vol. 74, no. 9, pp. 3231–3252, May 2015, doi: 10.1007/s11042-013-1784-2.

[27] X. Wu and W. Sun, "Random grid-based visual secret sharing with abilities of OR and XOR decryptions," *J. Vis. Commun. Image Represent.*, vol. 24, no. 1, pp. 48–62, Jan. 2013, doi: 10.1016/j.jvcir.2012.11.001.

[28] C.-N. Yang and C.-B. Ciou, "Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability," *Image Vis. Comput.*, vol. 28, no. 12, pp. 1600–1610, Dec. 2010, doi: 10.1016/j.imavis.2010.04.003.

PENG LI received the B.S. degree in applied mathematics from North China Electric Power University, in 2004, and the M.S. degree in computational mathematics and the Ph.D. degree in computer application technology from the Harbin Institute of Technology, China, in 2006 and 2012, respectively. He is currently an Associate Professor with the Department of Mathematics and Physics, North China Electric Power University. His research interests include secret image sharing, visual cryptography, and information hiding.

JIANFENG MA received the B.S. degree from the Department of Mathematics and Physics, North China Electric Power University, China, in 2017, where he is currently pursuing the master's degree. His current research interests include visual cryptography and secret image sharing.

LIPING YIN received the B.S. degree from the Department of Mathematics and Physics, Qingdao University of Science and Technology, China, in 2018. She is currently pursuing the master's degree with the Department Mathematics and Physics, North China Electric Power University, China. Her current research interests include visual cryptography and secret image sharing.

QUAN MA was born in Nanchong, Sichuan, China, in 1981. He received the bachelor's degree in information and computing science from North China Electric Power University, in 2005, and the master's and Ph.D. degrees in nuclear energy science and engineering from the Nuclear Power Institute of China, in 2010 and 2018, respectively.

Since 2005, he has been a Senior Engineer with the Nuclear Power Institute of China. He is the author of 25 articles and more than 21 patents. Most of the articles were included in EI and SCI. His interests include the nuclear digital instrumentation control system equipment development, and manufacturing and dynamic reliability research. He is also a member of the editorial board of Electronic Instrumentation Customer and the Director of the Sichuan Science and Technology Youth Federation.