Halftone Visual Cryptography with Complementary Cover Images

Gang Shen[1(✉)], Feng Liu[2,3], Zhengxin Fu[1], Bin Yu[1], and Wen Wang[2]

[1] Zhengzhou Information Science and Technology Institute, Zhengzhou 450001, China
shengang_zisti@163.com
[2] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[3] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100093, China

Abstract. By the addition of halftone techniques, halftone visual cryptography scheme (HVCS) embeds a secret image into halftone shares taking meaningful visual information. In this paper, we propose a (k, n)-HVCS using complementary cover images. Before the halftone processing of the cover images by error diffusion, secret information pixels (SIPs) are prefixed based on the underlying (k, n)-VCS. In the halftone processing, several pairs of complementary cover images are adopted and two halftone methods on the cover images are designed for different (k, n) threshold access structures. The proposed scheme removes the share's cross interference from other shares and obtains better visual quality. Furthermore, the proposed scheme eliminates the burden that each participant may carry multiple shares.

Keywords: Visual cryptography · Visual secret sharing · Extended visual cryptography · Halftone visual cryptography · Meaningful shares

1 Introduction

Naor and Shamir [5] introduced a variant form of secret sharing, called visual cryptography scheme (VCS) that is usually referred to as visual secret sharing. Particularly in a (k, n)-VCS, each pixel of the black-and-white secret image is encoded into m subpixels, referred to as pixel expansion, for each of the n shares (distributed to n participants respectively) by designing two collections of $n \times m$ Boolean matrices C^0 and C^1. To encode a white pixel, the dealer randomly chooses one of the matrices in C^0, and to encode a black pixel, the dealer randomly chooses one of the matrices in C^1. The chosen matrix defines the color of the m subpixels in each of the shares. If any k or more shares are stacked together, our eyes can perceive the secret information due to the darkness difference, referred to as contrast, between black pixels and white pixels in the

Y.Q. Shi et al. (Eds.): IWDW 2016, LNCS 10082, pp. 223–237, 2017.
DOI: 10.1007/978-3-319-53465-7_17

stacked result, while if fewer than k shares are superimposed it is impossible to perceive the secret information.

In a VCS, all shares consisting of random pixel patterns do not take any visual information and may lead to suspicion of secret information encryption. Moreover, managing an increasing number of meaningless shares is challenging since the shares are difficult to manage or use and require careful labeling and storage. Shares showing meaningful images are more desirable in terms of the steganography aspects.

To cater for this need, several extended VCSs (EVCSs), where the shares contain both visual information of the cover images and the secret information, were presented by manipulating the basis matrices [1,2,8]. Then, Nakajima et al. [4] extended the $(2, 2)$-EVCS to natural grayscale images. Tsai et al. [6] proposed a transformation method that can transfer any basis matrices of VCSs to generate meaningful shares, where its shares are simply generated by replacing the white and black subpixels in a traditional VCS share with transparent pixels and pixels from natural colourful images, respectively. Yang and Yang [11] developed an EVCS by using the range distribution instead of the fixed pattern. The major shortcomings with these methods are poor visual quality of the shares, no (k, n) threshold, unsatisfied security or contrast conditions, or cross interference from the shares on the reconstructed secret image.

To avoid the above drawbacks, halftone VCS (HVCS) is proposed, where the secret image is embedded into meaningful shares obtained by the halftone processing of the grayscale cover images. Generally, a share in an HVCS is made up of two parts: secret information pixels (SIPs) carrying the secret information and non-SIPs carrying the visual information of cover images. First, Zhou et al. [12] used complementary cover images to avoid the cross interference from the shares on the reconstructed secret image, however, for general access structures multiple shares may be hold by each participant, which is a burden on the share management. Then, three HVCSs were developed by Wang et al. [9] based on error diffusion. Just as the way proposed in [12], Wang et al.'s first method also faces the same drawback. Wang et al.'s second method introduces auxiliary black pixels (ABPs), a part of the non-SIPs, to avoid the cross interference from the shares on the reconstructed secret image, but more ABPs are imported so that the visual quality of shares is degraded. In Wang et al.'s third method, less ABPs are imported, whereas the share's cross interference from other shares is introduced due to the ABPs' selection relying on the image content of the shares. Liu et al. [3] proposed an HVCS by using the special design of dithering matrix to avoid the cross interference from the shares on the reconstructed secret image, however, the cover images are darkened before the halftone processing, which inevitably affects the visual quality of the shares. Recently, Yan et al. [10] generalized Wang et al.'s third method [9], but decreasing the share's cross interference from other shares still remains to be solved.

In this paper, to avoid the share's cross interference from other shares and improve the visual quality of shares, we propose an HVCS with complementary cover images through error diffusion. Before the halftone processing, the location

of SIPs is prefixed. In the halftone processing, complementary cover images are adopted to avoid the cross interference from the shares on the reconstructed secret image. Moreover, two halftone methods on the cover images for different (k, n) cases are put forward to ensure each participant receive only one share. Finally, the additional quantization errors introduced by SIPs and non-SIPs are diffused away by error diffusion to the neighboring grayscale pixels, and hence better visual quality of the halftone shares is achieved.

The rest of this paper is organized as follows. Section 2 introduces some preliminaries for the proposed scheme. In Sect. 3, the proposed scheme is presented in detail. Section 4 proves the validity of the proposed scheme and analyzes the visual quality of the halftone shares theoretically. To show the effectiveness and advantages of our scheme, experimental results and comparisons are given in Sect. 5. Finally, this paper is concluded in Sect. 6.

2 Preliminaries

This section provides the model of VCS where some terms and concepts will be referenced in subsequent sections. An introduction of error diffusion is also provided.

2.1 The Model of VCS

The secret image of this paper consists of a collection of black and white pixels. A white pixel is identified as 0 while a black pixel is identified as 1. Each pixel is shared separately. To understand the sharing process consider the case where the secret image consists of just a single black or white pixel. On sharing, this pixel appears in the n shares distributed to the participants. Generally, a secret pixel is encrypted into m subpixels in each share and thus the size of each share is m times the size of the secret image. This m is called the pixel expansion. We further assume that the subpixels are sufficiently small and close enough so that human visual system averages them to some shade of gray. In order that the recovered image is clearly discernible, it is important that the gray level of a black pixel be darker than that of a white pixel. Actually, to construct a VCS, it is sufficient to construct the basis matrices corresponding to the black and white pixel. The collections of matrices C^0 and C^1 are obtained by giving all possible column permutations to the basis matrices S^0 and S^1 respectively. As a result, the dealer has to store only the two basis matrices S^0 and S^1, making the scheme efficient space-wise. In the following, we formally define what is meant by basis matrices.

Notations: Suppose $P = \{1, 2, \ldots, n\}$ be a set of participants. Let M be an $n \times m$ Boolean matrix and $X = \{i_1, i_2, \ldots, i_p\} \subseteq P$. Then M_X denotes the $|X| \times m$ submatrix obtained from M by considering its restriction to rows corresponding to the elements in X. $\otimes(M_X)$ denotes the stacking (Boolean OR) operation to the rows of M_X. $\omega(\otimes(M_X))$ denotes the Hamming weight of the row vector $\otimes(M_X)$, which denotes the number of 1's in the vector $\otimes(M_X)$.

Definition 1. *Two $n \times m$ basis matrices S^0 and S^1 constitute a (k, n)-VCS if the following conditions are satisfied:*

1. *Any k or more participants can recover the secret image. Formally, for $|X| \geq k$, we have $\omega(\otimes(S_X^1)) > \omega(\otimes(S_X^0))$.*
2. *Any less than k participants have no information on the shared image. Formally, for $|X| < k$, S_X^1 and S_X^0 are identical up to a column permutation.*

The first property is related to the contrast of the reconstructed secret image. It states that when a qualified set of participants stack their shares they can perceive the secret information due to the darkness difference. Usually, the contrast is defined as follows:

$$\alpha = \frac{\omega(\otimes(S_X^1)) - \omega(\otimes(S_X^0))}{m}, \tag{1}$$

where α $(0 \leq \alpha \leq 1)$. It is lucid that for a valid VCS, $\alpha = 0$ if $|X| < k$ and $\alpha > 0$ when $|X| \geq k$. From the point of view of participants, the contrast α is expected to be as large as possible.

The second property is called security, since it implies that, even by inspecting all their shares, a forbidden set of participants cannot gain any information in deciding whether the shared pixel was white or black.

2.2 Error Diffusion

Error diffusion is a simple, yet efficient algorithm to realize the halftone processing of a grayscale image. The error means the difference between the original grayscale pixel value and its final halftone pixel value. The quantization error at each pixel is diffused away to the neighboring grayscale pixels. Figure 1 shows the flow chart of error diffusion where $C(i, j)$ represents the (i, j)th pixel of the input grayscale image, $D(i, j)$ is the sum of the input pixel value and the diffused past errors, and $HS(i, j)$ is the output quantized pixel value. Error diffusion consists of two main components. The first component is the thresholding block where the output $HS(i, j)$ is given by

$$HS(i,j) = \begin{cases} 1, & if\ D(i,j) \geq T(i,j) \\ 0, & otherwise. \end{cases} \tag{2}$$

The threshold $T(i, j)$ can be position-dependent and the threshold modulation shown in Eq. (3), which tries to adjust the current threshold by using the information of three preceding halftone pixels, is adopted in this paper,

$$T(i,j) = 0.25 + 0.33 \times 0.25 \times [HS(i,j-1) + HS(i,j-2) + HS(i,j-3)]. \tag{3}$$

The second component is the error diffusion matrix $H(k, l)$ whose input $E(i, j)$ is the difference between $D(i, j)$ and $H(i, j)$. Herein, the widely used Floyd-Steinberg error diffusion matrix in Eq. (4) is applied in this paper,

$$H(k,l) = \begin{bmatrix} 0 & (i,j) & \frac{7}{16} \\ \frac{3}{16} & \frac{5}{16} & \frac{1}{16} \end{bmatrix}. \tag{4}$$

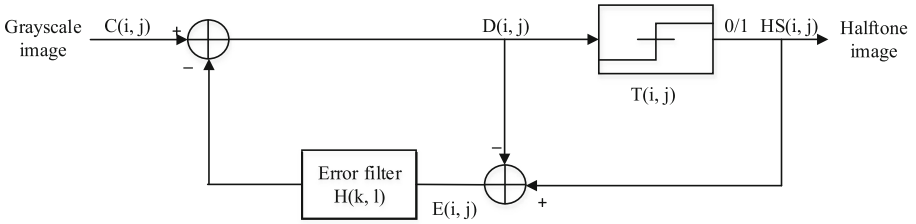

Fig. 1. The flowchart of error diffusion.

Finally, we can compute $D(i,j)$ as

$$D(i,j) = C(i,j) - \sum_{k,l} H(k,l)E(i-k, j-l). \tag{5}$$

The recursive structure of error diffusion indicates that the quantization error $E(i,j)$ depends not only on the current input and out but also on the entire past history. The errors introduced by SIPs and non-SIPs of Sect. 3 in this paper are high frequency or blue noise in nature, and they are diffused away by the error diffusion matrix $H(k,l)$, leading to visually pleasing halftone shares.

3 The Proposed Scheme

The proposed HVCS with complementary cover images is built upon the fundamental principles of VCS. Given a binary secret image and multiple grayscale cover images including some complementary pairs, n halftone shares are generated such that the resultant shares are no longer random patterns, but take meaningful visual images. Stacking at least k shares will reconstruct the secret, while stacking less than k shares gives no clue about the secret.

3.1 Problem Description

In a (k,n)-HVCS, each halftone share is divided into non-overlapping halftone cells of size $q = v_1 \times v_2$, where $q > m$. For a secret pixel, the encoded m pixels by a (k,n)-VCS is embedded into one halftone cell in each share. Within the q pixels in a halftone cell, only the m pixels are called secret information pixels (SIPs), which really carry the secret information. The remaining $q-m$ pixels, called non-SIPs, carry the visual information of the cover images. From the point of view of information coding theory, $q \geq 2m$ is suggested to obtain good visual quality of shares.

In general, it is required that when all qualified shares are stacked together, only the secret visual information is revealed. Thus, to prevent the cross interference from shares on the reconstructed secret image, it should be satisfied for non-SIPs to be all black in the reconstructed halftone cell. To the best of our knowledge, there are four methods to achieve this goal, which are analyzed as follows:

1. With the aid of auxiliary black pixels [9]. Over the non-SIPs, There are some pixels that are forced to be black (value 1) called auxiliary black pixels (ABPs), while the remaining pixels are responsible for carrying the information of halftone shares. ABPs are deliberately introduced into the shares so that the visual information of one share is completely blocked by the ABPs on the other shares. But, a sufficient number of ABPs are usually needed and hence less pixels carry the information of halftone shares, leading to a poor visual quality of the shares.
2. Exploiting parallel halftone processing [9,10]. This method is based on the fact that the halftone processing of grayscale images alone may generate a sufficient number of black pixels to block the share visual information from showing on the reconstructed image. Within the halftone processing, all the shares are checked at each non-SIP position to see if a sufficient number of black pixels have been produced. If a sufficient number of black pixels have not yet been generated, black pixels are deliberately inserted at that position. Obviously, the decision to insert a black pixel or not depends on the image content of the shares. Thus, there exists the share's cross interference from other shares.
3. Designing dithering matrix [3]. By the special design of dithering matrix, the grayscale cover images are converted into halftone shares, where the stacking results of the qualified shares are all black images. This method requires that the gray-levels of all the pixels in each grayscale cover image have to be not too large. Images that do not satisfy this requirement need to be darkened before the halftone processing, which will inevitably cause the loss in the visual quality of the shares.
4. Using complementary pairs of halftone shares [9,12]. A pair of complementary shares can be employed to block all the share's visual information from showing on the reconstructed image. The generated halftone shares in the general scheme must satisfy that any qualified set of shares contains at least one pair of complementary halftone shares. This requirement, however, may not be satisfiable for all access structures unless each participant is distributed more than one share.

According to the above analysis, there is a natural question we can ask: can we put forward such a method that the cross interference from shares on the reconstructed secret image, the share's cross interference from other shares, poor visual quality of shares and multiple shares per participant will be avoid in all?

3.2 SIP Assignment

In the embedding process of SIPs, for security purposes, the distribution of SIPs should be independent of their values. Moreover, to achieve good quality of shares, it is also desirable to distribute the SIPs homogeneously so that one SIP is maximally separated from its neighboring SIPs. Since the SIPs are maximally separated, the quantization error caused by an SIP will be diffused away before

the next SIP is encountered leading to visually pleasing halftone shares. To the best of our knowledge, we adopt the void and cluster algorithm (please refer to [7] for details) to distribute the SIPs in this paper.

After the distribution of SIPs is generated, the next step is to assign the values to all the SIPs. This procedure only depends on the underlying VCS. Under the (k, n)-VCS, the basis matrices S^0 and S^1 are constructed first. Then construct a pair of collections of matrices (C^0, C^1) from the basis matrices. For each m SIPs of a halftone cell, a matrix M is randomly selected from C^0 and C^1 according to the value of the corresponding secret image pixel. The values of SIPs in the uth share are then replaced with the uth row of M.

In summary, the distribution and values of the SIPs can be fixed prior to the generation of halftone shares.

3.3 Non-SIP Assignment

To answer the question raised in the first subsection, in this subsection we use the complementary cover images and propose two non-SIP assignments for different (k, n) thresholds to block all the share's visual information from showing on the reconstructed image.

Suppose there are n grayscale cover images $C_1, C_2, \ldots, C_n$ including λ, $1 \leq \lambda \leq \lfloor \frac{n}{2} \rfloor$, pairs of complementary grayscale images and $n-2\lambda$ arbitrary grayscale images. Let c_u $(0 \leq c_u \leq 1)$ denote a pixel value in the grayscale cover image C_u, $1 \leq u \leq n$. Without loss of generality, the pixels of n grayscale cover images are listed in sequence as $\{c_1, \overline{c_1}, c_3, \overline{c_3}, \ldots, c_{2\lambda-1}, \overline{c_{2\lambda-1}}, \ldots, c_n\}$, where $(c_{2v-1}, \overline{c_{2v-1}})$, $1 \leq v \leq \lambda$, is the vth complementary pair of grayscale cover pixels. We call $A = [a_1, a_2, \ldots, a_n]^T$, where $a_u \in \{c_1, \overline{c_1}, c_3, \overline{c_3}, \ldots, c_{2\lambda-1}, \overline{c_{2\lambda-1}}, \ldots, c_n, 1\}$, an assignment column vector for the n halftone shares. The non-SIP assignments of the proposed (k, n)-HVCS are described according to various k and n as follows.

Assignment 1: For (k, n)-HVCS, $k > \lceil \frac{n}{2} \rceil$, on sharing a secret pixel, we input $\lambda = n - k + 1$ pairs of complementary grayscale pixels and $n - 2\lambda$ arbitrary grayscale pixels and set

$$A = [c_1, \overline{c_1}, \ldots, c_{2\lambda-1}, \overline{c_{2\lambda-1}}, c_{2\lambda+1}, \ldots, c_n]^T. \tag{6}$$

Assignment 2: For (k, n)-HVCS, $k \leq \lceil \frac{n}{2} \rceil$, on sharing a secret pixel, we input $\lambda = \lfloor \frac{n}{2} \rfloor$ pairs of complementary grayscale pixels and $n - 2\lambda$ arbitrary grayscale pixels and randomly select one of $t = \lceil \frac{n}{2(k-1)} \rceil$ assignment column vectors $A_1, \ldots, A_t$ set as follows:

$$\begin{cases} A_l = [\underbrace{1, \ldots, 1}_{n_1}, \underbrace{c_{2(l-1)(k-1)+1}, \overline{c_{2(l-1)(k-1)+1}}, \ldots, c_{2l(k-1)-1}, \overline{c_{2l(k-1)-1}}}_{n_2}, \underbrace{1, \ldots, 1}_{n_3}]^T, \\ A_t = [\underbrace{1, \ldots, 1}_{n_4}, \underbrace{c_{2(t-1)(k-1)+1}, \overline{c_{2(t-1)(k-1)+1}}, \ldots, c_{2\lambda-1}, \overline{c_{2\lambda-1}}}_{n_5}, \underbrace{c_{2\lambda+1}, \ldots, c_n}_{n_6}]^T, \end{cases} \tag{7}$$

where $l = 1, \ldots, t-1$, $n_1 = 2(l-1)(k-1)$, $n_2 = 2(k-1)$, $n_3 = n - 2l(k-1)$, $n_4 = 2(t-1)(k-1)$, $n_5 = 2(\lambda - (t-1)(k-1))$ and $n_6 = n - 2\lambda$.

3.4 Generation of Halftone Shares via Error Diffusion

Once the assignments of SIPs and non-SIPs are determined, a halftoning algorithm can be applied to generate the halftone shares from grayscale cover images. Error diffusion is used in this paper as it is a computationally efficient way to generate halftone shares.

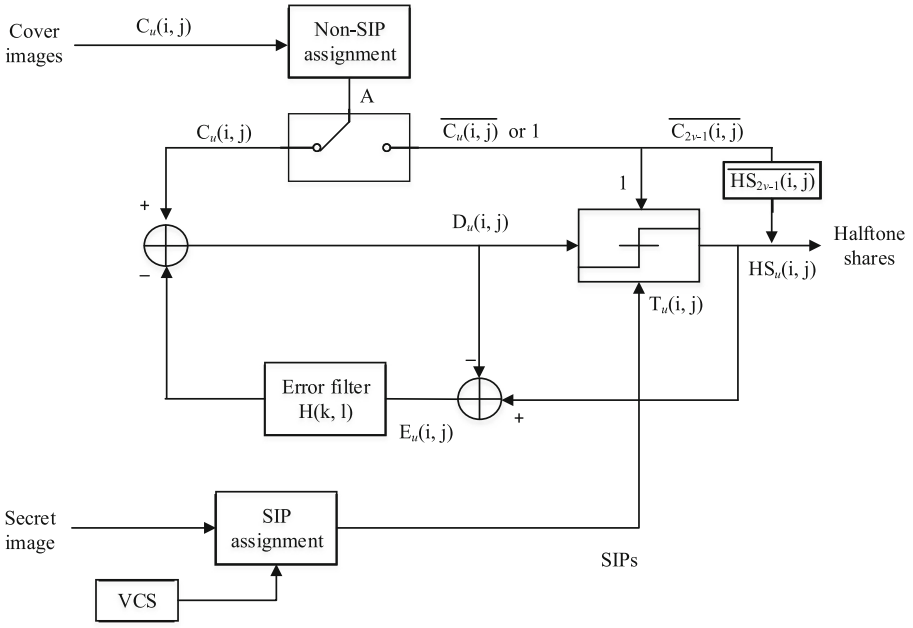

Fig. 2. The flowchart of the proposed HVCS.

In the proposed (k, n)-HVCS, the generation of halftone shares based on error diffusion is shown in Fig. 2, where the SIPs are prefixed in the halftone shares. By the non-SIP assignment, we are first able to know the grayscale cover images to be input. Suppose we need to input λ pairs of complementary grayscale images and $n - 2\lambda$ arbitrary grayscale images $\{C_1, \overline{C_1}, C_3, \overline{C_3}, \ldots, C_{2\lambda-1}, \overline{C_{2\lambda-1}}, \ldots, C_n\}$. To produce the halftone share pixel $HS_u(i, j)$, a grayscale cover image pixel $c_u = C_u(i, j)$ is provided. Then we can get the input and output to the threshold block as follows:

$$D_u(i, j) = C_u(i, j) - \sum_{k,l} H(k, l) E_u(i - k, j - l), \tag{8}$$

$$HS_u(i, j) = \begin{cases} 1, & if\ D_u(i, j) \geq T_u(i, j) \\ 0, & otherwise, \end{cases} \tag{9}$$

where $E_u(i, j) = HS_u(i, j) - D_u(i, j)$.

Given a non-SIP assignment column vector $A = [a_1, a_2, \ldots, a_n]^T$ where $a_u \in \{c_1, \overline{c_1}, c_3, \overline{c_3}, \ldots, c_{2\lambda-1}, \overline{c_{2\lambda-1}}, \ldots, c_n, 1\}$, the above procedure is applied only when $HS_u(i,j)$ is a non-SIP and $a_u \in \{c_1, c_3, \ldots, c_{2\lambda-1}, \ldots, c_n\}$. Otherwise, if $HS_u(i,j)$ is a SIP, the value of $HS_u(i,j)$ is set equal to the value of the corresponding predetermined SIP. If $HS_u(i,j)$ is a non-SIP and $a_u = 1$, the value of $HS_u(i,j)$ is set to be 1. For the above two cases, the error $E_u(i,j)$ is calculated as the difference between the input to the thresholding block and the SIP value or the value 1. The quantization error caused by the introduction of the SIPs and black pixels is diffused away to the neighboring grayscale pixels, as illustrated in Fig. 2, and will lead to visually pleasing halftone shares. If $HS_u(i,j)$ is a non-SIP and $a_u \in \{\overline{c_1}, \overline{c_3}, \ldots, \overline{c_{2\lambda-1}}\}$, the value of $HS_u(i,j)$ is just set equal to the value obtained by reversing the corresponding $HS_{2v-1}(i,j)$, $1 \le v \le \lambda$. In summary, the SIPs are seamlessly embedded into the generated halftone shares and the halftone share is structured taking meaningful visual information.

4 Discussions

In this section, we first prove that the proposed HVCS is a valid construction of VCS by Theorem 1. Then visual quality of meaningful shares generated by the proposed HVCS is discussed.

4.1 Proof of Validity

In general, a valid construction of VCS means that the contrast and security conditions of Definition 1 should be satisfied. To prove the proposed HVCS is a valid VCS, we first give the following lemmas.

Lemma 1. *For* Assignment 1*, any k halftone shares include at least one pair of complementary grayscale cover pixels.*

Proof. When selecting all the arbitrary grayscale cover pixels and all single pixels of each pair of complementary grayscale cover pixels, only $n-k+1+n-2(n-k+1) = k-1$ pixels are included. Therefore, any k halftone shares include at least one pair of complementary grayscale cover pixels. □

Lemma 2. *For* Assignment 2*, any k halftone shares include at least one pair of complementary grayscale cover pixels or at least one black pixel.*

Proof. For $k \le \lceil \frac{n}{2} \rceil$, there are $t = \lceil \frac{n}{2(k-1)} \rceil$ assignment column vectors $A_1, \ldots, A_t$. For A_l, $l = 1, \ldots, t-1$, each includes only as many as $k-1$ different pairs of complementary grayscale cover pixels and $n-2(k-1)$ black pixels. Therefore, any k halftone shares include at least one pair of complementary grayscale cover pixels or at least one black pixel. For A_t, if n is even, $n_6 = 0$, and hence there is $\frac{n_5}{2} \le (k-1)$ different pairs of complementary grayscale cover pixels and $n-n_5$ black pixels; else $n_6 = 1$, and hence there is $\frac{n_5}{2} \le (k-2)$ different pairs of complementary grayscale cover pixels and $n-n_5-1$ black pixels. Therefore, any k halftone shares also include at least one pair of complementary grayscale cover pixels or at least one black pixel. □

Theorem 1. *The proposed HVCS is a valid VCS.*

Proof. For each halftone cell, since the distribution of SIPs is independent of the values of SIPs, no secret can be inferred from the locations of SIPs which can be detected by comparing the original halftone image and the corresponding halftone share. In addition, since the values of SIPs are only determined by the underlying (k, n)-VCS, no secret information can be obtained by looking at the values of SIPs of fewer than k halftone shares. Therefore, the security condition of Definition 1 is satisfied.

Now consider the stacking result of any k or more halftone shares. Note that, in our generation of halftone shares, one of the complementary grayscale cover pixels is processed by error diffusion and the other is processed by reversing the former one. Hence, by Lemmas 1 and 2, when stacking together shares of any k participants, the non-SIPs in each reconstructed halftone cell are always black as a result of the OR operation. If a secret pixel is white (resp. black), let the reconstructed halftone cell be denoted as Q_0 (resp. Q_1). Then we have

$$\omega(Q_0) = q - m + \omega(\otimes(S^0_{X_k})), \tag{10}$$

$$\omega(Q_1) = q - m + \omega(\otimes(S^1_{X_k})), \tag{11}$$

where X_k is a set of any k or more participants for the underlying (k, n)-VCS. Thus, we have

$$\alpha^h = \frac{\omega(Q_1) - \omega(Q_0)}{q} = \frac{\omega(\otimes(S^1_{X_k})) - \omega(\otimes(S^0_{X_k}))}{q} = \frac{\alpha m}{q} > 0, \tag{12}$$

where the contrast α^h is for the proposed (k, n)-HVCS and the contrast α is for the underlying (k, n)-VCS. Therefore, the contrast condition of Definition 1 is satisfied. □

4.2 Visual Quality of Halftone Shares

In our HVCS, the non-SIPs are responsible for carrying the visual information of the cover images and preventing all the share's visual information from showing on the reconstructed image. Specifically, in an assignment column vector A, with the exception of 1's, all pixels are assigned to carry the share visual information. The proportion of these pixels governs the image quality of the resultant halftone shares. The quantity β is called the quality index of the halftone share and is represented as

$$\beta = \frac{q - m - e}{q}, \tag{13}$$

where e is the number of 1's assigned in each halftone cell. A large β leads to good image quality of the halftone share. However, β cannot be arbitrarily large for all non-SIP assignments. For Assignment 1, $e = 0$ and hence $\beta = \frac{q-m}{q} < 1$, where $k > \lceil \frac{n}{2} \rceil$. For Assignment 2, $e = \frac{q-m}{t}$ and hence $\frac{1}{2}\frac{q-m}{q} \leq \beta = \frac{q-m}{q}(1 - \frac{1}{t}) < \frac{q-m}{q} < 1$, where $t = \lceil \frac{n}{2(k-1)} \rceil$ and $k \leq \lceil \frac{n}{2} \rceil$; moreover, if $n \gg k$, the quality index β achieves the optimal value $\frac{q-m}{q}$ approximately.

(a) (b) (c)

Fig. 3. Original images used in this paper. (a) The binary secret image with size of 170×170; (b)–(c) two grayscale cover images with size of 510×510, which will be zoomed to their proper size if necessary.

Remark: Note that the pixel expansion m and contrast α of the underlying VCS is predetermined by k and n. Thus, if we fix k and n, then better visual quality of halftone shares can be obtained in larger halftone cells according to Eq. (13). On the contrary, larger halftone cell sizes lead to lower contrast of the reconstructed secret image by Eq. (12). Therefore, a tradeoff exists between the visual quality of the halftone shares and the contrast of the reconstructed secret image. It should be also noted that we use complementary cover pixels or black pixels to block all the share's visual information from showing on the reconstructed image. Besides allowing complementary halftone shares, we remove the share's cross interference from other shares, since the decision to insert the black pixels, according to Assignment 2, is independent of the content of cover images.

5 Experiment and Comparison

In this section, experiments and comparisons are given to demonstrate the effectiveness and advantages of the proposed HVCS. In addition, the original images that will be used in this paper are shown in Fig. 3.

5.1 Experiment

To demonstrate the effectiveness of our HVCS, we design three experiments, involving the two non-SIP assignments, for answering the following questions.

1. Whether or not the proposed HVCS is a valid VCS?
2. Whether or not the proposed HVCS generates meaningful shares? If so, is there a tradeoff between the visual quality of the halftone shares and the contrast of the reconstructed secret image.
3. Whether or not the cross interference from the share images on the reconstructed secret image is avoided?
4. Whether or not the share's cross interference from other shares is avoided?

Experimental results by the proposed HVCSs for $(2, 3)$ and $(3, 4)$ threshold cases are shown in Figs. 4, 5 and 6, respectively, where the basis matrices of

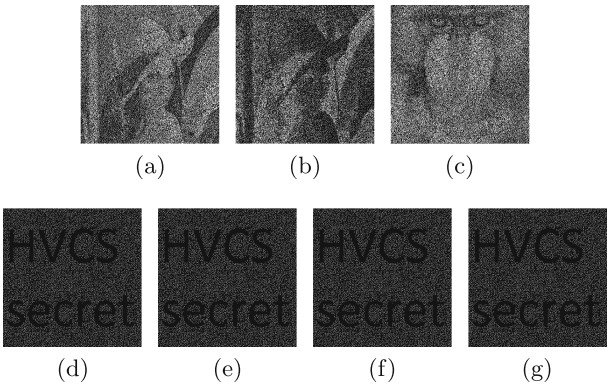

Fig. 4. Experimental results of the proposed $(2,3)$-HVCS, where $m = 3$, $q = 9$. (a)–(c) Three meaningful shares, where $\beta = \frac{3}{9}$; (d)–(f) stacking results by any two of the three shares, where $\alpha^h = \frac{1}{9}$; (g) stacking result by three shares, where $\alpha^h = \frac{1}{9}$.

$(2,3)$-VCS are $S^0 = \begin{pmatrix} 1\,1\,0 \\ 1\,1\,0 \\ 1\,1\,0 \end{pmatrix}$ and $S^1 = \begin{pmatrix} 1\,1\,0 \\ 1\,0\,1 \\ 0\,1\,1 \end{pmatrix}$, and the basis matrices of $(3,4)$-VCS are $S^0 = \begin{pmatrix} 0\,0\,1\,1\,1\,0 \\ 0\,0\,1\,1\,0\,1 \\ 0\,0\,1\,0\,1\,1 \\ 0\,0\,0\,1\,1\,1 \end{pmatrix}$ and $S^1 = \begin{pmatrix} 1\,0\,0\,0\,1\,1 \\ 0\,1\,0\,0\,1\,1 \\ 0\,0\,1\,0\,1\,1 \\ 0\,0\,0\,1\,1\,1 \end{pmatrix}$.

All of Figs. 4(a)–(c), 5(a)–(c) and 6(a)–(d) show visually pleasing halftone cover images, where the shares cross interference from other shares does not happen with the exception of some complementary shares. From Figs. 4(a)–(c),

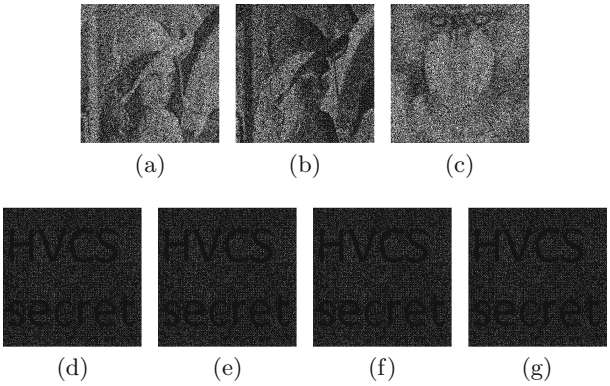

Fig. 5. Experimental results of the proposed $(2,3)$-HVCS, where $m = 3$, $q = 16$. (a)–(c) Three meaningful shares, where $\beta = \frac{13}{32}$; (d)–(f) stacking results by any two of the three shares, where $\alpha^h = \frac{1}{16}$; (g) stacking result by three shares, where $\alpha^h = \frac{1}{16}$.

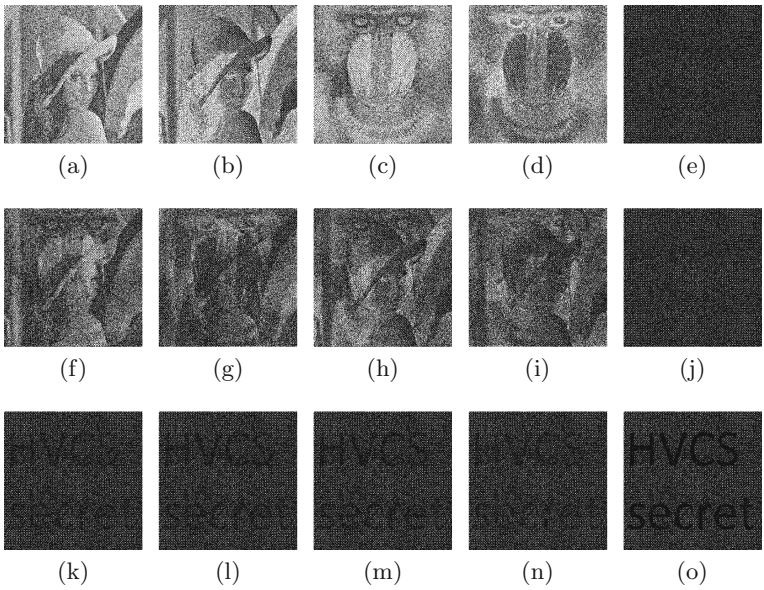

Fig. 6. Experimental results of the proposed $(3, 4)$-HVCS, where $m = 6$, $q = 16$. (a)–(d) Four meaningful shares, where $\beta = \frac{10}{16}$; (e)–(j) stacking results by any two of the four shares; (k)–(n) stacking results by any three of the four shares, where $\alpha^h = \frac{1}{16}$; (o) stacking result by four shares, where $\alpha^h = \frac{2}{16}$.

5(a)–(c) and 6(a)–(j), we see that any less than k shares give no clue about the secret image, however, from Figs. 4(d)–(g), 5(d)–(g) and 6(k)–(o), we see that any k or more shares can reconstruct the secret image, where the cross interference from the shares on the reconstructed secret image is removed. In addition, comparing Fig. 4 with Fig. 5, we conclude that the content of each meaningful share in Fig. 5 is recognized more clearly with a quality index $\beta = \frac{13}{32}$ while the content of the reconstructed secret image in Fig. 4 is perceived more easily with a contrast $\alpha^h = \frac{1}{9}$. The above result illustrates the tradeoff between the visual quality of the halftone shares and the contrast of the reconstructed secret image.

5.2 Comparison

To show the advantages of our HVCS, we compare our scheme with related EVCSs or HVCSs [1–4,6,8–12] as follows:

1. The EVCSs proposed in [1,2,11] can only deal with binary input share images, while our proposed scheme can deal with grayscale input images.
2. The pixel expansion of the proposed scheme is less than that of [1,2,8], which is clearly discussed in [3].
3. The EVCS proposed in [4] is only for the $(2, 2)$ threshold access structure, and the scheme may have security issues when relaxing the constraint of the

dynamic range as already noted in [4]. Our proposed scheme can be applied to (k, n) access structure for all k and n, and is always unconditionally secure which is inherited from the corresponding VCS.

4. For the HVCS proposed in [12] and the first HVCS proposed in [9], the participants are required to take more than one share for some access structure, while our proposed scheme does not have such a requirement and each participant only needs to take one share.
5. Compared with the EVCSs [6,11], the third HVCS [9] and the HVCS [10], the cross interference from the share images on the reconstructed secret image and the share's interference from other shares, which may increase the suspicion of secret image encryption and decrease the visual quality, are both avoided in our proposed scheme.
6. Compared with the HVCS [3], our proposed scheme does not require the dealer to choose carefully or darken the input grayscale images, which will inevitably cause the loss in the visual quality of the shares.
7. The second HVCS [9] achieves the quality of halftone shares $\beta^* \leq \frac{k-1}{n}\frac{q-m}{q}$, while our proposed scheme achieves better quality of halftone shares, where $\beta = \frac{q-m}{q} \geq \frac{k-1}{n}\frac{q-m}{q} \geq \beta^*$ for $k > \lceil \frac{n}{2} \rceil$ and $\beta = \frac{q-m}{q}(1 - \frac{1}{\lceil \frac{n}{2(k-1)} \rceil}) > \frac{k-1}{n}\frac{q-m}{q} \geq \beta^*$ for $k \leq \lceil \frac{n}{2} \rceil$.
8. The proposed scheme is flexible in the sense that there exists a trade-off between the visual quality of the halftone shares and the contrast of the reconstructed secret image. This flexibility allows the dealer to choose the proper parameters, k, n, q and β, for different applications.

6 Conclusion

In this paper, we have proposed an HVCS with complementary cover images by error diffusion. The main questions existing in previous EVCSs and HVCSs, including the cross interference from shares on the reconstructed secret image, the share's cross interference from other shares, poor visual quality of shares and multiple shares per participant, are solved in all. Extending the proposed scheme from (k, n) to general access structures will be our future work.

Acknowledgments. We would like to thank the anonymous reviewers for their important and helpful comments. This work was supported by the National Natural Science Foundation of China with No. 61602513 and No. 61671448, the Strategic Priority Research Program of the Chinese Academy of Sciences with No. XDA06010701, and the National Key R&D Program of China with No. 2016YFB0800100.

References

1. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Extended capabilities for visual cryptography. ACM Theor. Comput. Sci. **250**, 143–161 (2001)
2. Droste, S.: New results on visual cryptography. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 401–415. Springer, Heidelberg (1996). doi:10.1007/3-540-68697-5_30

3. Liu, F., Wu, C.K.: Embedded extended visual cryptography schemes. IEEE Trans. Inf. Forensics Secur. **6**, 307–322 (2011)
4. Nakajima, M., Yamaguchi, Y.: Extended visual cryptography for natural images. In: WSCG 2002, pp. 303–412. CSRN, Plzen (2002)
5. Naor, M., Shamir, A.: Visual cryptography. In: Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995). doi:10.1007/BFb0053419
6. Tsai, D.S., Chen, T., Horng, G.: On generating meaningful shares in visual secret sharing scheme. Imaging Sci. J. **56**, 49–55 (2008)
7. Ulichney, R.A.: The void-and-cluster method for dither array generation. In: Human Vision, Visual Processing, and Digital Display IV, San Jose, CA, vol. 1913, pp. 332–343. SPIE (1993)
8. Wang, D.S., Yi, F., Li, X.: On general construction for extended visual cryptography schemes. Pattern Recogn. **42**, 3071–3082 (2009)
9. Wang, Z., Arce, G.R., Di Crescenzo, G.: Halftone visual cryptography via error diffusion. IEEE Trans. Inf. Forensics Secur. **4**, 383–396 (2009)
10. Yan, X.H., Shen, W., Niu, X.M., Yang, C.N.: Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality. Digital Sig. Process. **38**, 53–65 (2015)
11. Yang, C.N., Yang, Y.Y.: New extended visual cryptography schemes with clearer shadow images. Inf. Sci. **271**, 246–263 (2014)
12. Zhou, Z., Arce, G.R., Di Crescenzo, G.: Halftone visual cryptography. IEEE Trans. Image Process. **15**, 2441–2453 (2006)