Embedded Extended Visual Cryptography Schemes

Feng Liu[1] and ChuanKun Wu[1]

[1]The State Key Laboratory of Information Security

Institute of Software, Chinese Academy of Sciences, Beijing 100190 China

Email: {liufeng, ckwu}@is.iscas.ac.cn

Homepage: http://iscas.ac.cn/ liufeng

Abstract

Visual cryptography scheme (VCS) is a kind of secret sharing scheme which allows the encoding of a secret image into n shares that distributed to n participants. The beauty of such scheme is that a set of qualified participants is able to recover the secret image without any cryptographic knowledge and computation devices. Extended visual cryptography scheme (EVCS) is a kind of VCS which consists of meaningful shares (compared to the random shares of traditional VCS). In this paper, we propose a construction of EVCS which is realized by embedding random shares into meaningful covering shares, and we call it the embedded extended visual cryptography scheme (embedded EVCS). Experimental results compare some of the well-known EVCS's proposed in recent years systematically, and show that the proposed embedded EVCS has competitive visual quality compared with many of the well-known EVCS's in the literature. Besides, it has many specific advantages against these well-known EVCS's respectively.

Keywords: Secret sharing, Embedded extended visual cryptography scheme

1 Introduction

The basic principle of visual cryptography scheme (VCS) was first introduced by Naor and Shamir. VCS is a kind of secret sharing scheme [1, 2] that focuses on sharing secret images. The idea of the visual cryptography model proposed in [3] is to split a secret image into two random shares (printed on transparencies) which separately reveals no information about the secret image other than the size of the secret image. The secret image can be reconstructed by stacking the two shares. The underlying operation of this scheme is logical operation *OR*. In this paper, we call a VCS with random shares the traditional VCS or simply the VCS. In general, a traditional VCS takes a secret image as input, and outputs n shares that satisfy two conditions: (1) Any qualified subset of shares can recover the secret image; (2) Any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image. An example of traditional $(2, 2)$-VCS can be found in the following Figure 1, where, generally speaking, a (k, n)-VCS means any k out of n shares could recover the secret image. In the scheme of Figure 1, shares (a) and (b) are distributed to two participants secretly, and each participant cannot get any information about the secret image, but after stacking shares (a) and (b), the secret image can be observed visually by the participants. VCS has many special applications, for example, transmitting military orders to soldiers who may have no cryptographic knowledge or computation devices in the battle field.

Many other applications of VCS, other than its original objective (i.e. sharing secret image), have been found, for example, authentication and identification [4], watermarking [5] and transmitting passwords [6] etc..

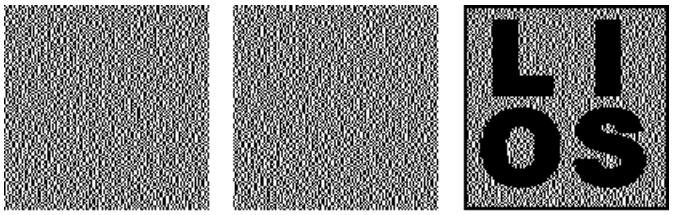

Figure 1: An example of traditional $(2, 2)$-VCS with image size 128×128.

The associated secret sharing problem and its physical properties such as contrast, pixel expansion and color were extensively studied by researchers worldwide. For example, Naor et al. [3] and Blundo et al. [7] showed constructions of threshold VCS with perfect reconstruction of the black pixels. Ateniese et al. [8] gave constructions of VCS for the general access structure. Krishna et al., Luo et al., Hou et al. and Liu et al. considered color visual cryptography schemes [9–12]. Shyu et al. proposed a scheme which can share multiple secret images [13]. Furthermore, Eisen et al. proposed a construction of threshold VCS for specified whiteness levels of the recovered pixels [14].

The term of extended visual cryptography scheme (EVCS) was first introduced by Naor et al. in [3], where a simple example of $(2, 2)$-EVCS was presented. In this paper, when we refer to a corresponding VCS of an EVCS, we mean a traditional VCS that have the same access structure with the EVCS. Generally, an EVCS takes a secret image and n original share images as inputs, and outputs n shares that satisfy the following three conditions: (1) Any qualified subset of shares can recover the secret image; (2) Any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image; (3) All the shares are meaningful images. Examples of EVCS can be found in the experimental results of this paper, such as Figure 4, 5 and 6.

EVCS can also be treated as a technique of steganography. One scenario of the applications of EVCS is to avoid the custom inspections, because the shares of EVCS are meaningful images, hence there are fewer chances for the shares to be suspected and detected.

There have been many EVCS's proposed in the literature. Droste [15], Ateniese et al. [16] and Wang et al. [17] proposed three EVCS's, respectively, by manipulating the share matrices. Nakajima et al. [18] proposed a $(2, 2)$-EVCS for natural images. Tsai et al. [19] proposed a simple EVCS, where its shares were simply generated by replacing the white and black sub-pixels in a traditional VCS share with transparent pixels and pixels from the cover images respectively. Furthermore, Zhou et al. and Wang et al. [20–22] presented an EVCS by using halftoning techniques. Their methods made use of the complementary images to cover the visual information of

the share images. Recently, Wang et al. proposed three EVCS's by using error diffusion halftoning technique [23] to obtain nice looking shares. Their first EVCS also made use of complementary shares to cover the visual information of the shares as the way proposed in [20]. Their second EVCS imported auxiliary black pixels to cover the visual information of the shares. In such a way, each qualified participants did not necessarily require a pair of complementary share images. Their third EVCS modified the halftoned share images and imported extra black pixels to cover the visual information of the shares.

However, the limitations of these EVCS's mentioned above are obvious. The first limitation is that the pixel expansion is large (Formal definitions of pixel expansion will be given in Definition 1 of Section 2.1). For example, the pixel expansion of the EVCS in [16] is $m+q$, where m is the pixel expansion of the secret image and q is the chromatic number of a hyper-graph, in any case the value of q satisfies $q \geq 2$. The construction in [15] has the pixel expansion $\sum_{q=1}^{n} 2^{q-1} b_q$, where b_q is the number of elements of S which contains exactly q elements, and S is the set of the qualified subsets. For example, for a $(3,3)$-EVCS, the pixel expansion will be 13 (see the last example of Section 7 in [15]). The pixel expansion of the (k,n)-EVCS in [17] is $m + m_0$ where $m_0 \geq \lceil n/(k-1) \rceil$. The second limitation is the bad visual quality of both the shares and the recovered secret images; this is confirmed by the comparisons in [20]. Unfortunately, the EVCS in [20] has other limitations, first it is computation expensive, second, the void and cluster algorithm makes the positions of the secret pixels dependent on the content of the share images and hence decrease the visual quality of the recovered secret image, third and most importantly, a pair of complementary images are required for each qualified subset and the participants are required to take more than one shares for some access structures, which will inevitably cause the attentions of the watchdogs at the custom and increase the participants' burden. The same problems also exist in the first method proposed by Wang et al. [23]. For Wang et al.'s second method, each qualified subset does not require complementary images anymore; however, this method is only for threshold access structure, and the auxiliary black pixels of their EVCS also darkened the shares. In fact, the way of generating auxiliary black pixels of this method can be viewed as a special case of our approach in Section 4 of this paper. For Wang et al.'s third method, the halftoned share images are modified and extra black pixels are imported to cover the visual information of the shares. The limitation of this method is that, the visual effect of each share will be affected by the content of other shares, and the content of the input original share images should be chosen in a selected way.

Tsai et al.'s EVCS [19] is simple, but it may not satisfy the contrast condition of anymore. And the recovered secret image contains the mixture of the visual information of share images. Consider the essence of mixing grey-level pixels; the secret information may be hard to be recognized by human eyes.

At last, the EVCS proposed in [18] is only for $(2,2)$ access structure, besides their limitations on the access structure, the scheme may have security issues when relaxing the constraint of the

dynamic range. (Explicit discussions on the security of the EVCS in [18] can be found in Section 4.2 of [18]).

The rest of this paper is organized as follows: Section 2 gives some preliminary results about VCS and the halftoning technique. In Section 3, we introduce the formal definition of embedded EVCS, and give the main idea about our construction. In Section 4, we give two methods to generate the covering shares. In Section 5, we embed the traditional VCS into the covering shares and discuss the bounds of our scheme. In Section 6, we propose a method to further reduce the black ratio, which enhances the visual quality of the shares. In Section 7, we give some experimental results and comparisons. At last, in Section 8, we conclude the paper.

2 Preliminaries

In this section, we give some definitions about VCS and some preliminary results about the halftoning technique by using the dithering matrix.

2.1 Definitions of traditional VCS

Suppose all the participants of a secret sharing scheme is $\mathcal{V} = \{0, 1, \ldots, n-1\}$. The specifications of all qualified and forbidden subsets of participants constitute an access structure $(\Gamma_{Qual}, \Gamma_{Forb})$, where Γ_{Qual} is the superset of qualified subsets, and Γ_{Forb} is the superset of forbidden subsets, and $\Gamma_{Qual} \cap \Gamma_{Forb} = \varnothing$. In this paper we only consider the access structure with $\Gamma_{Qual} \cup \Gamma_{Forb} = 2^{\mathcal{V}}$. The superset Γ_{Qual} is monotone because if part of the participants in a set $B(\in \Gamma_{Qual})$ can recover the shared secret, then it is obvious that all the participants in B can recover the shared secret as well. Let

$$\Gamma_m = \{A \in \Gamma_{Qual} : \forall B \subsetneq A \Rightarrow B \notin \Gamma_{Qual}\} \text{ and } \Gamma_M = \{A \in \Gamma_{Forb} : \forall B \supsetneq A \Rightarrow B \notin \Gamma_{Forb}\}$$

Then Γ_m is called *the minimal qualified access structure*, Γ_M is called *the maximal forbidden access structure*. For the superset of subsets $\mathcal{C} \subseteq 2^{\mathcal{V}}$, define $cl(\mathcal{C}) = \{B \subseteq \mathcal{V} : \exists A \in \mathcal{C} \ st.\ B \supseteq A\}$. We call $cl(\mathcal{C})$ the closure of $\mathcal{C}$. Since Γ_{Qual} is monotone, then $cl(\Gamma_m) = \Gamma_{Qual}$. From the above discussion it is known that the qualified access structure Γ_{Qual} and the minimal qualified access structure Γ_m are determined by each other, so when we discuss the qualified access structure, we only need to give discussions on the minimal qualified access structure in the rest of this paper.

The threshold access structure is a special case of the general access structure. More specifically, a threshold (k, n) access structure is a general access structure satisfies the following

$$\Gamma_{Qual} = \{B \subseteq \mathcal{V} : |B| \geq k\} \text{ and } \Gamma_{Forb} = \{B \subseteq \mathcal{V} : |B| \leq k-1\}$$

and

$$\Gamma_m = \{B \subseteq \mathcal{V} : |B| = k\} \text{ and } \Gamma_M = \{B \subseteq \mathcal{V} : |B| = k-1\}$$

Take a $(2,3)$ access structure as an example. We have $\Gamma_{Qual} = \{\{1,2\},\{2,3\},\{1,3\},\{1,2,3\}\}$, $\Gamma_{Forb} = \{\{\},\{1\},\{2\},\{3\}\}$, $\Gamma_m = \{\{1,2\},\{2,3\},\{1,3\}\}$ and $\Gamma_M = \{\{1\},\{2\},\{3\}\}$.

In this paper, we will focus on black and white secret image only, where the white pixel is denoted by 0 and the black pixel is denoted by 1. Generally, a VCS consists of a pair of collections of matrices (C_0, C_1). The matrices in the collections (C_0, C_1) are called share matrices, where each share matrix consists of $n \times m$ sub-pixels. However, many studies make use of basis matrices to simplify their discussions (see examples in [7, 8, 14, 16, 17, 24]). Now we give the formal definition of the basis matrix VCS as follows.

Definition 1 (Basis Matrix VCS [8]) *Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure on a set of n participants. The boolean $n \times m$ matrices M^0 and M^1 are the basis matrices of a visual cryptography scheme if there exist values $\{h_X : \ for\ X \in \Gamma_{Qual}\}$ and $\alpha(>0)$ satisfying:*

1. *(Contrast) If $X = \{i_1, i_2, \cdots, i_p\} \in \Gamma_{Qual}$, then the* OR *of rows $i_1, i_2, \cdots, i_p$ of M^0 is a vector v that satisfies $w(v) \leq (h_X - \alpha m)$, whereas, for M^1, we have that $w(v) \geq h_X$.*
2. *(Security) If $F = \{i_1, i_2, \cdots, i_p\} \in \Gamma_{Forb}$, then the $p \times m$ matrices obtained by restricting M^0 and M^1 to rows $i_1, i_2, \cdots, i_p$ are equal up to a column permutation.*

In the above definition,

- $w(v)$ is the hamming weight of a vector v.
- m is called the pixel expansion of the traditional VCS. Besides, in this paper, we also define the secret image pixel expansion as the pixel expansion of the recovered secret image over the original secret image, and we define the share pixel expansion as the pixel expansion of the final output shares over the original share images.
- α is called the contrast of the recovered secret image.
- h_X is called the threshold of a qualified subset X.

When the dealer encodes a secret pixel he just needs to randomly choose a share matrix in C_0 (resp. C_1) for a white (resp. black) pixel and distributes the $i-th$ row, containing m sub-pixels, to the $i-th$ participant. In another word, a share matrix in C_0 (resp. C_1) can be seemed as a random column permutation of the basis matrix M^0 (resp. M^1). When decoding the secret pixel, the participants only need to stack their shares, i.e. they print their shares on the transparencies and stack the transparencies. Then the secret pixel can be observed visually by human eyes. This approach of construction of VCS will have small memory requirements (it keeps only the basis matrices) and it is efficient (to choose a matrix in C_0 (*resp.* C_1) as it only needs to generate a permutation of the basis matrices randomly).

2.2 Halftoning technique by using dithering matrix

One of the main drawbacks of the VCS's proposed in [3, 7, 8, 16] is that, they cannot deal with the grey-scale image. MacPherson [24] proposed a VCS to deal with the grey-scale image, however, it has large pixel expansion $c \times m$, where c is the number of the grey-levels and m is the pixel expansion of the corresponding black and white VCS. In order to deal with the grey-scale image, the halftoning technique was introduced into the visual cryptography [11, 18, 25–27]. The halftoning technique (or dithering technique) is used to convert the grey-scale image into the binary image. This technique has been extensively used in printing applications which has been proved to be very effective. Once we have the binary image, the VCS proposed in [3, 7, 8, 16] can be applied directly. However, the concomitant loss in quality is unavoidable in this case.

Many kinds of halftone algorithms have been proposed in the literature. In this paper, we make use of the patterning dithering [28]. The patterning dithering makes use of a certain percentage of black and white pixels, often called patterns, to achieve a sense of grey scale in the overall point of view. The pattern consists of black and white pixels, where different percentage of the black pixels stands for the different greynesses. The halftoning process is to map the grey scale pixels from the original image into the patterns with certain percentage of black pixels. The halftoned image is a binary image. However, in order to store the binary images one needs a large amount of memory. A more efficient way is by using the dithering matrix. The dithering matrix is a $c \times d$ integer matrix, denoted as D. The entries, denoted as $D_{i,j}$ for $0 \leq i \leq c-1$ and $0 \leq j \leq d-1$, of the dithering matrix are integers between 0 and $cd-1$, which stand for the grey-levels in the dithering matrix. Denote $g \in \{0, \cdots, cd\}$ as the grey-levels of a pixel in the original image. The halftoning process is formally described in Algorithm 1.

Generally, for an input image I of size $p \times q$, the halftoning process runs on each pixel in I as follows.

Algorithm 1 *The halftoning process for each pixel in I:*
***Input**: The $c \times d$ dithering matrix D and a pixel x with grey-level g in input image I*
***Output**: The halftoned pattern at the position of the pixel x*

For $i = 0$ to $c-1$ do
  For $j = 0$ to $d-1$ do
    If $g \leq D_{ij}$ then print a black pixel at position (i,j);
    Else print a white pixel at position (i,j);

To describe the halftoning process clearer, take the dithering matrix with 10 $(= 3 \times 3 + 1)$ grey-levels as an example, where the grey-levels of the original image range from 0 to 9.

Example 1 *Dithering matrix with 10 grey-levels D_0 is shown in Matrix 1.*

$$D_0 = \begin{array}{|c|c|c|}\hline 7 & 0 & 5 \\ \hline 2 & 4 & 6 \\ \hline 3 & 8 & 1 \\ \hline \end{array}$$

Matrix 1: Dithering matrix with 10 grey-levels D_0.

In Algorithm 1, the halftoning process causes the cd pixel expansion on the input image. We call it the *halftone pixel expansion*. In the rest of the paper, we denote s as the halftone pixel expansion, i.e. $s = cd$. Take the above dithering matrix D_0 as an example, the halftoned patterns of the grey-levels $0, \cdots, 9$ are shown in Figure 2.

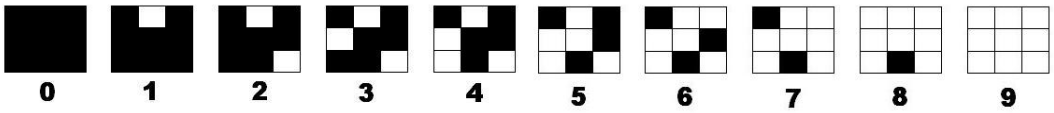

Figure 2: The halftoned patterns of the dithering matrix D_0 of the grey-levels $0, \cdots, 9$.

3 A sketch and the main idea of the proposed embedded EVCS

In this section, we will give an overview of our construction. First we introduce the formal definition of embedded EVCS.

Definition 2 (embedded EVCS) *Denote M^0 and M^1 as the basis matrices of a traditional VCS with access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ and pixel expansion m. In order to encode a secret image I, the dealer takes n grey-scale original share images as inputs, and converts them into n covering shares which are divided into blocks of t sub-pixels ($t \geq m$). By embedding the rows of M^0 and M^1 (after randomly permuting their columns) into the blocks, the embedded EVCS outputs n shares $e_0, \cdots, e_{n-1}$, and there exist values $\{h_X : \ for\ X \in \Gamma_{Qual}\}$, α and ρ satisfying:*

1. *The stacking result of each block of a qualified subset of shares can recover a secret pixel. More precisely, if $X = \{i_1, \cdots, i_p\} \in \Gamma_{Qual}$, denote $B_{i_1}, \cdots, B_{i_p}$ as the blocks at the same position of the shares $e_{i_1}, \cdots, e_{i_p}$, then for a white secret pixel, the* OR *of $B_{i_1}, \cdots, B_{i_p}$ is a vector v that satisfies $w(v) \leq h_X - \alpha t$, and that for a black secret pixel, it satisfies $w(v) \geq h_X$.*

2. *Part of the information of the original share images is preserved in the shares. Define $\rho = (t - m)/t$ be the ratio of the information of the original share images that preserved in the shares, and it satisfies $\rho > 0$.*

In Definition 2, the first condition ensures that the secret image can be visually observed by stacking a qualified subset of shares. The second condition ensures that the shares are all

meaningful in the sense that parts of the information of the original share images are preserved. The value ρ reflects the ratio of the information of the original share images that preserved in the shares. Explicitly, the value of ρ is between 0 and 1, where $\rho = 0$ means that no information of the original share images can be observed, and $\rho = 1$ means that all the information of the original share images can be observed. Generally, when $\rho > 0$, the shares can be considered as meaningful. The larger the value of ρ is the better visual quality the shares will have. At last, Definition 2 does not have the security condition. The secret image is, in fact, encrypted by the corresponding VCS, and then we embed its shares into the covering shares. Hence, the security of the embedded EVCS is guaranteed by the security of the corresponding VCS, i.e. the security condition of Definition 1.

Furthermore, we need to point out that, in [16], Ateniese et al. proved the optimality of their scheme under their definition of EVCS. Under the definition of Ateniese et al., all the information of the original share images is preserved in the shares. However, as the second condition of the above Definition 2 indicates, only parts of the information of the original share images are preserved in the shares, i.e. Definition 2 is a relaxed model of the EVCS model proposed in [16]. Hence our scheme can have smaller pixel expansion by sacrificing part of the information of the original share images. We claim that our definition is reasonable, because the information of the original share images is not as important as that of the secret image for the participants. Besides, experimental results of this paper show that preserving all the information of original share images does not imply better visual quality of the final output shares.

The idea of our embedded EVCS contains two main steps: (1) Generate n covering shares, denoted as $s_0, s_1, \cdots, s_{n-1}$; (2) Generate the embedded shares by embedding the corresponding VCS into the n covering shares, denoted as $e_0, e_1, \cdots, e_{n-1}$.

In step 1, we generate the covering shares for an access structure Γ_m. We take n grey-scale original share images, denoted as $I_0, I_1, \cdots, I_{n-1}$, as the inputs, and output n binary meaningful shares $s_0, s_1, \cdots, s_{n-1}$, where the stacking results of the qualified shares are all black images, i.e. the information of the original share images are all covered. We call the n output meaningful shares the *covering shares* in the rest of this paper. (In fact, the stacking results are not necessarily to be all black images, we will discuss this case in Section 6, and before Section 6, we assume that the stacking results are all black images). The covering shares have the advantage that, when the qualified subsets are stacked, all the information of the patterns in the original share images is covered. Hence the visual quality of the recovered secret image is not affected. Otherwise, the information of the original share images may appear in the recovered secret image, and hence results in bad visual quality. A method to generate covering shares will be introduced in Section 4.

In step 2, we first make use of the corresponding VCS to encode a secret image, and then embed the shares of the corresponding VCS into the covering shares that generated in step 1; we call the output shares of step 2 the *embedded shares*. In such a way, when we stack a qualified subset of embedded shares the secret image will appear, because the stacking result of covering

shares covers all the information of the original share images. The detailed information about the embedding process will be introduced in Section 5.

4 Generating the covering shares by using the dithering matrices

In this section, we propose a method to construct the covering shares $s_0, s_1, \cdots, s_{n-1}$ by using the n input original share images $I_0, I_1, \cdots, I_{n-1}$.

Let D_0 be the dithering matrix in Example 1. Suppose the grey-levels of all the pixels in the image I_0 are smaller than 4, then the positions corresponding to D^0_{00}, D^0_{02}, D^0_{11}, D^0_{12} and D^0_{21} of all the pixels in the image $I_0^{'}$ are always black after being halftoned by D_0, where D^0_{ij} is the entry in the i-th row and j-th column of D_0. We now give another dithering matrix D_1:

$$D_1 = \begin{array}{|c|c|c|}\hline 1 & 8 & 3 \\ \hline 6 & 4 & 2 \\ \hline 5 & 0 & 7 \\ \hline \end{array}$$

Matrix 2: Dithering matrix D_1 for 10 grey-levels.

If an image I_1 has all its pixels with grey-levels smaller than 5, after running Algorithm 1, we get that, the positions correspond to D^1_{01}, D^1_{10}, D^1_{20} and D^1_{22} of all the pixels in the image $I_1^{'}$ are always black. Hence, when we stack the images $I_0^{'}$ and $I_1^{'}$, the resulting image will be an all black image and $I_0^{'}$ and $I_1^{'}$ are covering shares. At this point, we can embed the share matrices of the $(2,2)$-VCS into the images $I_0^{'}$ and $I_1^{'}$.

Generally, in order to construct the covering shares $s_0, s_1, \cdots, s_{n-1}$ for the general access structure Γ_m, we need to construct n dithering matrices $D_0, D_1, \cdots, D_{n-1}$. By halftoning the input original share images $I_0, I_1, \cdots, I_{n-1}$ (after being properly darkened where the darkening method is proposed in Section 4.2 Equation 1), we get the covering shares $s_0, s_1, \cdots, s_{n-1}$ satisfying that the stacking results of the qualified covering shares are all black images.

Define the positions of the dithering matrix as the elements in the universal set $\mathcal{G} = \{g_0, g_1, g_2, \cdots, g_{s-1}\}$, i.e. the universal set contains all the grey-levels in the dithering matrix, where s is the halftone pixel expansion. We denote the sets $A_0, A_1, \cdots, A_{n-1}$ as n subsets of $\mathcal{G}$, each subset A_i corresponds to a participant $i \in \mathcal{V}$ and a covering share s_i. For any qualified subset $Q \in \Gamma_m$, the union of the corresponding subsets of $A_0, A_1, \cdots, A_{n-1}$ covers $\mathcal{G}$, i.e. $\bigcup_{j \in Q} A_j = \mathcal{G}$. In the rest of this paper, we call the subsets $A_0, A_1, \cdots, A_{n-1}$ the *covering subsets* as they correspond to the covering shares respectively.

Here, we introduce two new concepts: the black ratio for a subset A_i and the average black ratio (Section 4.2 explains the reason for the necessity of these two concepts). Define the *black ratio* of the covering subset A_i for the universal set $\mathcal{G}$ to be $R(A_i, \mathcal{G}) = |A_i|/|\mathcal{G}|$, and define the *average black ratio* to be $\bar{R}(\mathcal{G}) = (\sum_{i=0}^{n-1} |A_i|)/(n|\mathcal{G}|)$. The black ratio of the covering subsets

and the average black ratio are expected to be as small as possible (we will explain the reason in Section 4.2 as well).

At this point, it is clear that in order to generate the covering shares, we need three steps: (1) Generate the covering subsets $A_0, A_1, \cdots, A_{n-1}$ given a Γ_m; (2) Convert the subsets into the dithering matrices $D_0, D_1, \cdots, D_{n-1}$; (3) Halftone the original share images $I_0, I_1, \cdots, I_{n-1}$ to generate the covering shares $s_0, s_1, \cdots, s_{n-1}$ by using D_0, D_1, $\cdots$, D_{n-1}.

The rest parts of this section are organized as follows: In Section 4.1 we show a method to generate the covering subsets and in Section 4.2 we show a method to convert the covering subsets into the dithering matrices and show how to halftone the original share images.

4.1 Generating the covering subsets with minimum average black ratio

Our approach is to construct the covering subsets first for the case of threshold access structure and then extend to the general access structure. In this paper, the covering subsets for threshold access structure are called *threshold covering subsets* and the covering subsets for the general access structure are called *general covering subsets*.

Recall that s is the halftone pixel expansion, and n is the number of shares. Because s is independent of the value of n, we have the following three cases: 1. $s = n$, 2. $s < n$ and 3. $s > n$. First we consider the case $s = n$.

Construction 1 *(The construction of (k, n) threshold covering subsets)*

Let $s = n$. Denote the universal set as $\mathcal{G} = \{g_0, \cdots, g_{n-1}\}$. Define the covering subsets $A_i = \{g_{(0+i) \bmod n}, g_{(1+i) \bmod n}, \cdots, g_{(n-k+i) \bmod n}\}$.

We have the following theorem:

Theorem 1 *For the universal set $\mathcal{G} = \{g_0, \cdots, g_{n-1}\}$, Construction 1 generates n covering subsets $A_0, A_1, \cdots, A_{n-1}$, satisfying that the union of any k out of n subsets is the universal set $\mathcal{G}$. The black ratio of each covering subset is $R(A_i, \mathcal{G}) = (n-k+1)/n$ for $i = 0, \cdots, n-1$. Furthermore these covering subsets have the minimum average black ratio $\bar{R}(\mathcal{G}) = (n-k+1)/n$.*

Proof: First, we prove that the subsets $A_0, A_1, \cdots, A_{n-1}$ are covering subsets. Let the $n \times n$ matrix T be the incidence matrix of A_i, $i = 0, \cdots, n-1$, whose entries are defined as $T_{ij} = \begin{cases} 1 & if\ g_i \in A_j, \\ 0 & otherwise. \end{cases}$. Then we have

$$T = \begin{array}{c} \\ g_0 \\ g_1 \\ \vdots \\ \vdots \\ g_{n-k-1} \\ g_{n-k} \\ g_{n-k+1} \\ \vdots \\ \vdots \\ g_{n-1} \end{array} \begin{array}{c} \begin{array}{ccccc} A_0 & A_1 & \cdots & \cdots & A_{n-1} \end{array} \\ \left[\begin{array}{ccccc} 1 & 0 & \cdots & \cdots & 1 \\ 1 & 1 & \cdots & \cdots & 1 \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ 1 & 1 & \cdots & \cdots & 1 \\ 1 & 1 & \cdots & \cdots & 0 \\ 0 & 1 & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & \cdots & 1 \end{array}\right] \end{array}$$

Because there are $k-1$ 0's in each row, so the union of any k out of n subsets must contain at least one 1 for each row, which implies that the union of any k out of n subsets is the universal set. Since there are $n-k+1$ 1's in each column, so the black ratio of each covering subset equals to $(n-k+1)/n$, and the average black ratio equals to $(n-k+1)/n$.

Then we prove that the average black ratio for $A_0, A_1, \cdots, A_{n-1}$ is minimum: Suppose n subsets $A_0^{'}, A_1^{'}, \cdots, A_{n-1}^{'}$ are the covering subsets for the (k,n) threshold access structure with universal set being $\mathcal{G} = \{g_0, \cdots, g_{n-1}\}$. By constructing the incidence matrix for $A_0^{'}, A_1^{'}, \cdots, A_{n-1}^{'}$, denote it as T, then we have that the number of the 0's in each row of T should be less than k, otherwise, there always exists a collection of subsets that the union of these subsets is not the universal set (i.e. the subsets correspond to the k 0's in the row). This means that the minimum number of the 1's in each row must be at least $n-k+1$. So, the total number of the 1's in the matrix T is at least $n(n-k+1)$, and the average black ratio is at least $(n-k+1)/n$. □

In the above construction, all the subsets $A_0, A_1, \cdots, A_{n-1}$ have the same cardinality, i.e. have the same black ratio. However, it is not necessary. The following corollary gives a way to change the black ratio of the covering subsets, while the average black ratio remains the same as the original covering subsets. This change will result in that some covering subsets will have their black ratio decreased by sacrificing the black ratio increase of other covering subsets. This makes sense because in practical applications, different covering subsets may have different importance and hence have different sensitivity on their black ratios.

Corollary 1 *Denote the universal set as $\mathcal{G} = \{g_0, \cdots, g_{n-1}\}$, and denote the (k,n) threshold covering subsets generated by Construction 1 as $A_0, A_1, \cdots, A_{n-1}$. For any two covering subsets A_i and A_j, where $i \neq j$, for any element $x \in A_i$ and $x \notin A_j$, we remove x from A_i and put x into A_j, denote the new constructed subsets as $A_0^{'}, A_1^{'}, \cdots, A_{n-1}^{'}$, then the subsets $A_0^{'}, A_1^{'}, \cdots, A_{n-1}^{'}$ are still (k,n) threshold covering subsets. Furthermore, the average black ratio of $A_0^{'}, A_1^{'}, \cdots, A_{n-1}^{'}$ remains the same as that of $A_0, A_1, \cdots, A_{n-1}$.*

Proof: Let T be the incidence matrix of $A_0, A_1, \cdots, A_{n-1}$, and suppose the element x belongs to row r for $r \in \{0, \cdots, n-1\}$. Then after x being transferred from A_i to A_j, the number of 0's in the row r remains the same. So the union of any k out of n subsets of $A_0^{'}, A_1^{'}, \cdots, A_{n-1}^{'}$ will

cover the universal set, as what the original covering subsets $A_0, A_1, \cdots, A_{n-1}$ do. Furthermore, because the total number of 1's in the incidence matrix T is not changed, so the average black ratio remains the same. Hence the corollary follows. □

The following example demonstrates how Corollary 1 works.

Example 2 *For the* $(3,4)$ *threshold covering subsets* $A_0 = \{g_0, g_1\}$, $A_1 = \{g_1, g_2\}$, $A_2 = \{g_2, g_3\}$ *and* $A_3 = \{g_0, g_3\}$, *we get to know that the black ratio of the four covering subsets are* $R(A_i, \mathcal{G}) = |A_i|/|\mathcal{G}| = 1/2$ *for* $i = 0, 1, 2, 3$, *and the average black ratio is* $\bar{R}(\mathcal{G}) = 1/2$.

By moving the element g_0 *from the covering subset* A_0 *to* A_1, *and by moving the element* g_1 *from the covering subset* A_0 *to* A_2, *then the four covering subsets are converted into* $A_0^{'} = \emptyset$, $A_1^{'} = \{g_0, g_1, g_2\}$, $A_2^{'} = \{g_1, g_2, g_3\}$ *and* $A_3^{'} = \{g_0, g_3\}$, *and the black ratio of the four covering subsets are:* $R(A_0^{'}, \mathcal{G}) = |A_0^{'}|/|\mathcal{G}| = 0$, $R(A_1^{'}, \mathcal{G}) = |A_1^{'}|/|\mathcal{G}| = 3/4$, $R(A_2^{'}, \mathcal{G}) = |A_2^{'}|/|\mathcal{G}| = 3/4$ *and* $R(A_3^{'}, \mathcal{G}) = |A_3^{'}|/|\mathcal{G}| = 1/2$, *and the average black ratio is still* $\bar{R}(\mathcal{G}) = 1/2$.

At this point, if the input images $I_0, I_1, \cdots, I_{n-1}$ have different requirements on the black ratio of the shares, this can be made feasible according to Corollary 1.

We then construct the covering subsets for the cases $s < n$ and $s > n$ for the universal set $\mathcal{G} = \{g_0, \cdots, g_{s-1}\}$ in Construction 2 and 3 respectively:

Construction 2 *We consider the case* $s < n$: *We make use of the covering subsets* $A_0, \cdots, A_{n-1}$ *of Construction 1. Let* $A_0^{'}, \cdots, A_{n-1}^{'}$ *be generated by removing the elements* $g_s, g_{s+1}, \cdots, g_{n-1}$ *from the covering subsets* $A_0, \cdots, A_{n-1}$. *i.e.* $A_i^{'} = A_i - \{g_s, g_{s+1}, \cdots, g_{n-1}\}$, $i = 0, \cdots, n-1$. *The subsets* $A_0^{'}, A_1^{'}, \cdots, A_{n-1}^{'}$ *will satisfy that the union of any* k *out of* n *shares will cover the new universal set* $\mathcal{G} = \{g_0, g_1, g_2, \cdots, g_{s-1}\}$ *of* s *elements, i.e.* $A_0^{'}, \cdots, A_{n-1}^{'}$ *are the covering subsets for the case* $s < n$.

Construction 3 *We consider the case* $s > n$. *We make use of the covering subsets* A_0, A_1, $\cdots$, A_{n-1} *of Construction 1. First, we add* $n - (s \mod n)$ *elements into the universal set* $\mathcal{G} = \{g_0, g_1, g_2, \cdots, g_{s-1}\}$, *denote the* $n-(s \mod n)$ *elements as* $a_0, \cdots, a_{n-(s \mod n)-1}$. *Let* $s^{'} = s+n-(s \mod n)$, *then we divide the* $s^{'}$ *elements of the new universal set* $\mathcal{G}^{'} = \{g_0, g_1, g_2, \cdots, g_{s^{'}-1}\}$ *into* $s^{'}/n$ *groups, where each of the* $s^{'}/n$ *groups has* n *elements, denote the* $s^{'}/n$ *groups as* $G_1, \cdots, G_{s^{'}/n}$. *For each* G_i, *we treat it as a universal set, and call Construction 1 to construct the covering subsets. Then we will have the following subsets:* $A_0^1, A_1^1, \cdots, A_{n-1}^1$, $A_0^2, A_1^2, \cdots, A_{n-1}^2$, $\cdots\cdots$, $A_0^{s^{'}/n}, A_1^{s^{'}/n}, \cdots, A_{n-1}^{s^{'}/n}$, *where denote* A_i^j *as the* i*-th covering subset belongs to the group* G_j. *Then let the* n *covering subsets for the universal set* $\mathcal{G}^{'}$, *denoted as* $A_0^{'}, A_1^{'}, \cdots, A_{n-1}^{'}$, *be* $A_0^{'} = A_0^1 \cup A_0^2 \cup \cdots \cup A_0^{s^{'}/n}$, $A_1^{'} = A_1^1 \cup A_1^2 \cup \cdots \cup A_1^{s^{'}/n}$, $\cdots\cdots$, $A_{n-1}^{'} = A_{n-1}^1 \cup A_{n-1}^2 \cup \cdots \cup A_{n-1}^{s^{'}/n}$, *and they satisfy that the union of any* k *out of the* n *subset will cover the universal set* $\mathcal{G}^{'} = \{g_0, g_1, g_2, \cdots, g_{s^{'}-1}\}$. *At this point, by removing the elements* $a_0, \cdots, a_{n-(s \mod n)-1}$ *from the subsets* $A_0^{'}, A_1^{'}, \cdots, A_{n-1}^{'}$, *and denote the new subsets as* $A_0^{''}, A_1^{''}, \cdots, A_{n-1}^{''}$. *Then the* n *covering subsets* $A_0^{''}, A_1^{''}, \cdots, A_{n-1}^{''}$ *satisfy*

that the union of any k out of n subsets will cover the universal set $\mathcal{G} = \{g_0, g_1, g_2, \cdots, g_{s-1}\}$, *i.e.* $A_0^{''}, \cdots, A_{n-1}^{''}$ *are the covering subsets for the case* $s > n$.

An example of Construction 2 and 3 can be found in Example 3 which will be introduced later to cover more cases. Furthermore, we have the following corollary about the average black ratio for the cases $s < n$ and $s > n$:

Corollary 2 *For the universal set* $\mathcal{G} = \{g_0, \cdots, g_{s-1}\}$ *and the threshold access structure* (k, n), *the covering subsets constructed by Construction 2 and 3 for the case* $s < n$ *and* $s > n$, *respectively, have the minimum average black ratio.*

Proof: Because the number of the 0's in each row of the incidence matrix remains unchanged during Construction 2 and 3, and according to Theorem 1, the corollary follows immediately. □

We now construct the covering subsets for the general access structure Γ_m. A simple construction for the general covering subsets can be: Denote $B \in \Gamma_m$ as a qualified subset and $min\{|B| : B \in \Gamma_m\}$ be the minimum number of the cardinality of all the qualified subsets B in Γ_m. Then the construction of the general covering subsets $A_0, A_1, \cdots, A_{n-1}$ can be converted into the construction of the $(min\{|B| : B \in \Gamma_m\}, n)$ threshold covering subsets. The constructions of the general covering subsets for the cases $s < n$ and $s > n$ can be the same as the construction of the $(min\{|B| : B \in \Gamma_m\}, n)$ threshold covering subsets. This construction is simple, however, the disadvantage of this construction is that it has high black ratio for each covering subset (i.e. $(n - min\{|B| : B \in \Gamma_m\} + 1)/n$). Take the general access structure $\Gamma_m = \{\{0, 1\}, \{1, 2\}, \{2, 3\}\}$ as an example: the black ratio for each covering subset will be $(4 - 2 + 1)/4 = 3/4$.

In order to reduce the black ratio of covering subsets, we then propose a construction for general covering subsets by using the technique of cumulative array that introduced in [29].

Construction 4 *Denote* Γ_M *as the maximal forbidden access structure for the general access structure* $(\Gamma_{Qual}, \Gamma_{Forb})$. *A cumulative map* $(A, \mathcal{G})$ *for the* Γ_{Qual} *is a finite set* $\mathcal{G}$ *along with a mapping* $A : \mathcal{V} \to 2^{\mathcal{G}}$ *such that for* $Q \subseteq \mathcal{V}$ *implies that,* $\bigcup_{a \in Q} A_a = \mathcal{G} \Leftrightarrow Q \in \Gamma_{Qual}$, *where* A_a *is the subset mapped from* $a \in \mathcal{V}$.

We can construct a cumulative map $(A, \mathcal{G})$ *for* Γ_{Qual} *by using* Γ_M *as follows: Assume* $\Gamma_M = \{F_0, \cdots, F_{t-1}\}$. *Let the universal set be* $\mathcal{G} = \{g_0, \cdots, g_{t-1}\}$ *and for any* $i \in \mathcal{V}$, *let* $A_i = \{g_j \mid i \notin F_j,\ 0 \le j \le t-1\}$. *For any* $X \in \Gamma_{Qual}$ *we have* $\bigcup_{i \in X} A_i = \mathcal{G}$. *Note that for any set* $X \in \Gamma_{Forb}$, *we have* $\bigcup_{i \in X} A_i \neq \mathcal{G}$.

Construction 4 produces the general covering subsets with $s = t$ elements. The constructions of the covering subsets of the cases $s < t$ and $s > t$ for general access structure can be the same as the threshold ones, i.e. Construction 2 and 3. The following example shows how the above constructions work.

Example 3 *We make use of the general access structure:* $\Gamma_m = \{\{0,1\}, \{1,2\}, \{2,3\}\}$. *We have the maximal forbidden access structure be* $\Gamma_M = \{\{0,2\}, \{0,3\}, \{1,3\}\}$. *So, we get to know that* $t = 3$ *and we have* $A_0 = \{g_2\}$, $A_1 = \{g_0, g_1\}$, $A_2 = \{g_1, g_2\}$ *and* $A_3 = \{g_0\}$. *The incidence matrix, denoted as* K, *of the subsets* A_0, A_1, A_2 *and* A_3 *is: (Where* K_{ij} *is the entry of* K *at the* i*-th row and* j*-th column, and is defined as* $K_{ij} = \begin{cases} 1 & if\ g_i \in A_j \\ 0 & otherwise \end{cases}$ *.)*

$$K = \begin{array}{c} \\ g_0 \\ g_1 \\ g_2 \end{array} \begin{array}{c} \begin{array}{cccc} A_0 & A_1 & A_2 & A_3 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

According to Construction 3, we assume $s = 4$, *and since* $t = 3$, *we add two elements* a_0 *and* a_1, *then we have* $s^{'} = 6$, *hence the incidence matrix, denoted as* $K^{'}$, *for the subsets* $A_0^{'}$, $A_1^{'}$, $A_2^{'}$ *and* $A_3^{'}$ *becomes: (Where* $K_{ij}^{'}$ *is the entry of* K' *at the* i*-th row and* j*-th column, and is defined as* $K_{ij}^{'} = \begin{cases} 1 & if\ g_i \in A_j \\ 0 & otherwise \end{cases}$ *)*

$$K^{'} = \begin{array}{c} \\ g_0 \\ g_1 \\ g_2 \\ g_3 \\ a_0 \\ a_1 \end{array} \begin{array}{c} \begin{array}{cccc} A_0^{'} & A_1^{'} & A_2^{'} & A_3^{'} \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

By removing the elements a_0 *and* a_1, *we get the general covering subsets* $A_0^{''} = \{g_2\}$, $A_1^{''} = \{g_0, g_1, g_3\}$, $A_2^{''} = \{g_1, g_2\}$ *and* $A_3^{''} = \{g_0, g_3\}$. *The black ratios for the four covering subsets are:* $R(A_0^{''}, \mathcal{G}) = |A_0^{''}|/|\mathcal{G}| = 1/4$, $R(A_1^{''}, \mathcal{G}) = |A_1^{''}|/|\mathcal{G}| = 3/4$, $R(A_2^{''}, \mathcal{G}) = |A_2^{''}|/|\mathcal{G}| = 1/2$ *and* $R(A_3^{''}, \mathcal{G}) = |A_3^{''}|/|\mathcal{G}| = 1/2$ *and the average black ratio is* $\bar{R}(\mathcal{G}) = 1/2$.

4.2 Converting the covering subsets into dithering matrices

In this part, we will construct the dithering matrices D_i by using the covering subsets A_i, $i = 0, 1, \cdots, n-1$. The dithering matrix D_i should satisfy that, the grey-levels at the positions in A_i of D_i are larger than $s - |A_i|$. As we previously defined, the dithering matrix is an $s(= c \times d)$ integer matrix.

Construction 5 *We define the starting dithering matrix, denoted as* D, *as described in Matrix 3. (The starting dithering matrix is a random matrix with* s *entries, where each entry of* D *contains a grey-level, and each grey-level of* $\{0, \cdots, s-1\}$ *appears in* D *once. Particularly, if* s *is a square number, we can choose a magic square as the starting dithering matrix* D. *For example* D_0 *and* D_1 *in Matrix 1 and 2 respectively.)*

We construct the dithering matrix D_i *by using the starting dithering matrix* D *and the covering subset* A_i, $i = 0, \cdots, n-1$. *Suppose* $A_i = \{g_{i_0}, g_{i_1}, \cdots, g_{i_{t-1}}\}$. *We swap the grey-levels in* A_i

$$D = \begin{array}{|c|c|c|c|} \hline g_0 & g_1 & \cdots \quad \cdots & g_{c-1} \\ \hline g_c & g_{c+1} & \cdots \quad \cdots & g_{2c-2} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \quad\ddots & \vdots \\ \hline g_{(d-1)c} & g_{(d-1)c+1} & \cdots \quad \cdots & g_{s-1} \\ \hline \end{array}$$

Matrix 3: The starting dithering matrix D.

with the grey-levels $\{s-1, s-2, \cdots, s-t\}$. *Particularly, one can swap the grey-level* g_{i_j} *with the grey-level* $s-1-j$ *in* D *for* A_i, *where* $j = 0, \cdots, t-1$.

Repeat the above process for all the covering subsets A_i, $i = 0, \cdots, n-1$, *we get* n *dithering matrixes* $D_0, \cdots, D_{n-1}$ *respectively.*

An example of Construction 5 can be found in Example 4.

At this point, we halftone the input original share images $I_0, I_1, \cdots, I_{n-1}$ by using the dithering matrices $D_0, D_1, \cdots, D_{n-1}$, and hence get the covering shares $s_0, s_1, \cdots, s_{n-1}$. The stacking result of the qualified covering shares will be an all black image. However, we have to point out that, this construction requires that the grey-levels of all the pixels in each image have to be no larger than $s - |A_i|$ respectively, where s is the halftone pixel expansion, i.e. $s = |\mathcal{G}|$. This constraint requires the dealer to choose the input images carefully. Images that do not satisfy this requirement need to be darkened before being halftoned. A simple method to darken an image I_i satisfying that the grey-levels of all the pixels in I_i are no larger than $s - |A_i|$ is as follows,

$$I_i(x, y) \leftarrow I_i(x, y) \cdot \frac{s - |A_i|}{max(I_i)} \tag{1}$$

where $I_i(x, y)$ is the grey-level of the pixel at the position (x, y) in I_i and $max(I_i)$ is the largest grey-level of the pixels in I_i.

The darkening process will inevitably cause the loss in the visual quality of the shares. So the value of $s - |A_i|$ is expected to be as large as possible, and hence the value of $|A_i|/s$ is expected to be as small as possible, i.e. the black ratio of A_i is expected to be as small as possible. Hence the black ratio $R(A_i, \mathcal{G}) = |A_i|/s$ reflects the requirements on a single input image I_i. Furthermore, we introduced the notion *average black ratio* which reflects the requirements on darkness of all the input images $I_0, I_1, \cdots, I_{n-1}$ from an overall point of view. Another reason we introduce the concept of the average black ratio is that: One cannot design the threshold covering subsets with all of them having minimum black ratio simultaneously (Corollary 1), but one can design the threshold covering subset with minimum average black ratio (Theorem 1, Corollary 1 and Corollary 2), so the average black ratio provides a more appropriate criterion about the effectiveness of the covering subsets. We will propose further methods to decrease the average black ratio in Section 6 under different conditions.

Note that, after halftoning I_i by using D_i of Construction 5, the pixels corresponding to the covering subset A_i in dithering matrix D_i will be black pixels. If those pixels are regularly arranged in D_i. Some grid patterns are likely to appear in the halftoned shares from an overall point of view. According to our experiments, using random matrix or magic square as the starting dithering matrix D can mitigate this phenomenon. That is the reason for choosing random matrix or magic square as the starting dithering matrix in Construction 5.

5 Embedding the corresponding VCS into the covering shares

After generating the covering shares, the embedding process can be realized by the following algorithm.

Algorithm 2 *The embedding process:*

Input: *The n covering shares constructed in Section 4, the corresponding VCS (C_0, C_1) with pixel expansion m and the secret image I.*

Output: *The n embedded shares $e_0, e_1, \cdots, e_{n-1}$.*

Step 1: *Dividing the covering shares into blocks that contain $t(\geq m)$ sub-pixels each.*

Step 2: *Choose m embedding positions in each block in the n covering shares.*

Step 3: *For each black (resp. white) pixel in I, randomly choose a share matrix $M \in C_1$ (resp. $M \in C_0$).*

Step 4: *Embed the m sub-pixels of each row of the share matrix M into the m embedding positions chosen in Step 2.*

In the above Algorithm 2, suppose the size of each covering shares is $p \times q$. We first divide each covering shares into $(pq)/t$ blocks with each block contains t sub-pixels, where $t \geq m$. In case pq is not a multiple of t, then some simple padding can be applied, for which the detail is skipped here. We choose m positions in each t sub-pixels to embed the m sub-pixels of M. In this paper, we call the chosen m positions that are used to embed the secret information the *embedding positions*. In order to correctly decode the secret image only by stacking the shares, the embedding positions of all the n covering shares should be the same. At this point, by stacking the embedded shares, the $t - m$ sub-pixels that have not been embedded by secret sub-pixels are always black, and the m sub-pixels that are embedded by the secret sub-pixels recover the secret image as the corresponding VCS does. Hence the secret image appears.

Because $t \geq m$, we have the following two cases: When $t = m$, the embedded EVCS degenerates to a VCS, because all the information of the covering shares is covered by the secret sub-pixels of the share matrices of the corresponding VCS. When $t > m$, we have $\rho = (t - m)/t > 0$, which

implies that the scheme is an embedded EVCS. In this embedded EVCS, there are $t-m$ sub-pixels in the covering shares $s_0, s_1, \cdots, s_{n-1}$ that preserve the information of the original share images $I_0, I_1, \cdots, I_{n-1}$ and the remaining m sub-pixels carry the secret information of the secret image. Hence, we get to know that the smallest secret image pixel expansion is $m+1$ when we use the above algorithm.

To summarize the above discussion we have the following theorem.

Theorem 2 *When embedding m sub-pixels of the basis matrix into the m embedding positions of each block of t sub-pixels in the covering shares, if $t = m$, then the scheme is a VCS, and if $t > m$ the scheme is an embedded EVCS.* □

Because the m sub-pixels in the share matrix correspond to one secret pixel in the secret image, and the m sub-pixels in the share matrix are embedded into t positions in the n covering shares, we get to know that, one pixel in the secret image corresponds to t sub-pixels of the embedded shares in our construction. Hence, the secret image pixel expansion is t in our construction.

By examining Algorithm 2, it is easy to note that the share pixel expansion can be different from the secret image pixel expansion. The secret image pixel expansion is independent of the share pixel expansion. Because we can choose the block size t to be arbitrarily large (we assume the covering shares can be arbitrarily large), the secret image pixel expansion can be arbitrarily large. In our scheme, because the original share images are only expanded when they are halftoned, the share pixel expansion equals to the halftone pixel expansion. In the rest of the paper, we denote s as the share pixel expansion or equivalently the halftone pixel expansion. To avoid the image distortion during the halftoning process, we usually let s be a square number. For example: 4, 9, 16, etc..

When the secret image is much smaller than the covering shares, we may have a number of choices of the values of t. For a bigger t, there are more sub-pixels (say $t-m$) preserving the information of the covering shares, and hence we have better visual quality for the shares. So there exists a trade-off between the secret image pixel expansion and visual quality of the shares. Furthermore, for bigger halftone pixel expansion, the dithering matrix can simulate more grey-levels; hence have better visual quality for the shares. So another trade-off lies between the share pixel expansion and the visual quality of the shares. (Recall that the share pixel expansion equals to the halftone pixel expansion.)

The above discussions show that our scheme is flexible with regard to the share pixel expansion, secret image pixel expansion and the visual quality of the shares.

6 Further improvements on the visual quality of the shares

In this section, we propose a method to reduce the black ratio, which will enhance the visual quality of the shares. We first describe the method for the case $s = t$ in Section 6.1, then consider the case $s \neq t$ in Section 6.2, where s is the share pixel expansion (halftone pixel expansion) and t is the secret image pixel expansion.

6.1 Reducing the black ratio of the covering subsets for $s = t$

The black ratio of A_i requires the grey-levels of all the pixels in the original input images I_i to be no larger than $s - |A_i|$. So, for an input image, the dealer needs firstly to darken the input image to satisfy the requirement. If the black ratio is high, the darkening process will decrease the visual quality of the covering shares, so the black ratio is expected to be as small as possible. Recall that in the embedding process, the m out of every t sub-pixels in the covering shares are replaced by the sub-pixels of the basis matrix of the corresponding VCS. Hence, there is no difference whether these m sub-pixels are all black or not in the stacking result of the qualified covering shares. Our method of reducing the black ratio is realized by reducing the number of the elements in the universal set. The universal set can be modified as follows: Let the new universal set be $\mathcal{G}' = \{g_0, g_1, g_2, \cdots, g_{s-m-1}\}$, which contains $s - m$ elements, recall that the universal set before was $\mathcal{G} = \{g_0, g_1, g_2, \cdots, g_{s-1}\}$, which contains s elements, we have $\mathcal{G}' \subset \mathcal{G}$. The stacking result of the qualified covering shares only needs to satisfy that the positions corresponding to the universal set $\mathcal{G}'$ are all black.

A modified version of the methods proposed in Section 4 to generate the dithering matrix is as follows.

Construction 6 *The construction of the dithering matrix with reduced black ratio:*

Step 1: *Choose the $m(< s)$ embedding positions in the starting dithering matrix, and denote the grey-levels in the embedding positions as $\{g_0, \cdots, g_{m-1}\}$. Remove these positions from the universal set $\mathcal{G}$, and denote the new universal set as $\mathcal{G}' = \{g'_0, g'_1, g'_2, \cdots, g'_{s-m-1}\}$, i.e. the rest grey-levels other than that in the embedding positions.*

Step 2: *Generate the covering subsets A'_i for the universal set $\mathcal{G}'$, by using the methods proposed in Section 4.1, where $i = 0, \cdots, n-1$.*

Step 3: *Convert the covering subsets A'_i into the dithering matrix D'_i, by using the method proposed in Section 4.2, where $i = 0, \cdots, n-1$.*

Step 4: *For each dithering matrix D'_i, swap the grey-levels $\{g_0, \cdots, g_{m-1}\}$ in the embedding positions with grey-levels $\{s-|A_i|-1, \cdots, s-|A_i|-m\}$ in a similar way as that of Construction 5. Denote the final dithering matrix as D_i, where $i = 0, \cdots, n-1$.*

Note that, in Construction 6, the reason for Step 4 is as follows: In Step 3, we get the dithering matrix D'_i, and after halftoning a share image I_i by D'_i, the pixels correspond to grey-levels $\{s-1, \cdots, s-|A_i|\}$ will be halftoned into black pixels with certainty. Beside these pixels, the pixels correspond to grey-levels $\{s-|A_i|-1, \cdots, s-|A_i|-m\}$ will be halftoned into black pixels with the largest possibility, compared to that of the rest grey-levels. Hence, if these pixels (correspond to grey-levels $\{s-|A_i|-1, \cdots, s-|A_i|-m\}$) are replaced by the secret sub-pixels of the corresponding VCS. The halftoned shares will look brighter than other pixels are replaced.

To demonstrate how Construction 6 works, we give the following example.

Example 4 *We construct the dithering matrices of an embedded $(2,2)$-EVCS. Suppose the basis matrices of the corresponding VCS are: $M^0 = \begin{bmatrix} 01 \\ 01 \end{bmatrix}$ and $M^1 = \begin{bmatrix} 10 \\ 01 \end{bmatrix}$. Let the halftone pixel expansion be $s = 9$, and let the starting dithering matrix D be as follows.*

$$D = \begin{array}{|c|c|c|} \hline 7 & 0 & 5 \\ \hline 2 & 4 & 6 \\ \hline 3 & 8 & 1 \\ \hline \end{array}$$

In this example, we choose the positions with grey-levels 3 and 4 as the embedding positions. Then the new universal set will be $\mathcal{G} = \{g'_0, g'_1, g'_2, \cdots, g'_6\} = \{8,7,6,5,2,1,0\}$. Then the covering subsets can be $A_0 = \{8,7,6,5\}$ and $A_1 = \{2,1,0\}$. The black ratio of each A_i will be $R(A_0, \mathcal{G}) = |A_0|/s = 4/9$ and $R(A_1, \mathcal{G}) = |A_1|/s = 1/3$, which require the grey-levels of the input images to be smaller than 5 and 6 respectively. It should be noted that these grey-levels are bigger than the ones in the beginning of Section 4.

According to Construction 6, the dithering matrices, D_0 and D_1 corresponding to the covering subsets A_0 and A_1 are as follows (identical to the Matrix 1 and Matrix 2 respectively).

$$D_0 = \begin{array}{|c|c|c|} \hline 7 & 0 & 5 \\ \hline 2 & \mathbf{4} & 6 \\ \hline \mathbf{3} & 8 & 1 \\ \hline \end{array} \qquad D_1 = \begin{array}{|c|c|c|} \hline 1 & 8 & 3 \\ \hline 6 & \mathbf{4} & 2 \\ \hline \mathbf{5} & 0 & 7 \\ \hline \end{array}$$

Matrix 4: The dithering matrices D_0 and D_1.

It is easy to verify that, when the grey-levels of the pixels in the input image I_0 (resp. I_1) are smaller than 5 (resp. 6), the stacking result of the above dithering matrices will result that the positions correspond to grey-levels $\{8,7,6,5,2,1,0\}$ are all black.

The experimental results of Example 4 are shown in Figure 6 in Section 7, where the dithering matrices are from Matrix 4.

Another experimental results of an embedded $(3,3)$-EVCS is given in Figure 4 (in Section 7), where the stacking result of the shares (a), (b) and (c) is the secret image (d). The basis matrices

of the corresponding VCS are: $M^0 = \begin{bmatrix} 0110 \\ 0101 \\ 0011 \end{bmatrix}$ and $M^1 = \begin{bmatrix} 1001 \\ 0101 \\ 0011 \end{bmatrix}$. Let the halftone pixel expansion be $s = 16$, the starting dithering matrix be magic square as follows.

$$D = \begin{array}{|c|c|c|c|} \hline 0 & 14 & 13 & 3 \\ \hline 11 & 5 & 6 & 8 \\ \hline 7 & 9 & 10 & 4 \\ \hline 12 & 2 & 1 & 15 \\ \hline \end{array}$$

Then the dithering matrices D_0, D_1 and D_2 for the three covering shares are given in Matrix 5, where the entries with grey-levels $\{8, 9, 10, 11\}$ are the embedding positions.

$$D_0 = \begin{array}{|c|c|c|c|} \hline 15 & \mathbf{10} & \mathbf{9} & 12 \\ \hline 0 & 5 & 6 & 3 \\ \hline 7 & 2 & 1 & 4 \\ \hline \mathbf{8} & 13 & 14 & \mathbf{11} \\ \hline \end{array} \quad D_1 = \begin{array}{|c|c|c|c|} \hline 0 & \mathbf{10} & \mathbf{9} & 3 \\ \hline 4 & 14 & 13 & 7 \\ \hline 12 & 6 & 5 & 15 \\ \hline \mathbf{8} & 2 & 1 & \mathbf{11} \\ \hline \end{array} \quad D_2 = \begin{array}{|c|c|c|c|} \hline 0 & \mathbf{9} & \mathbf{10} & 3 \\ \hline 12 & 5 & 6 & 15 \\ \hline 7 & 14 & 13 & 4 \\ \hline \mathbf{11} & 2 & 1 & \mathbf{8} \\ \hline \end{array}$$

Matrix 5: The dithering matrices D_0, D_1 and D_2 for an embedded $(3, 3)$-EVCS.

6.2 Reducing the black ratio of the covering subsets for $s \neq t$

Denote $lcm(a, b)$ as the least common multiple of the two integers a and b. Our method is to construct $lcm(s, t)/s$ dithering matrices for the i-th input original share image, denoted as $D_{i,0}, \cdots, D_{i,lcm(s,t)/s-1}$. The $lcm(s, t)/s$ dithering matrices are used to halftone $lcm(s, t)/s$ adjacent pixels of the input original share images at a time. The $lcm(s, t)/s$ dithering matrices can be divided into $lcm(s, t)/t$ blocks with t sub-pixels for each block, we embed m secret sub-pixels into each block. Hence each dithering matrix has a different universal set. For each universal set, we construct the dithering matrix by using the method that is similar to Construction 6 respectively. Hence we get the $lcm(s, t)/s$ dithering matrices for each input original share image. The whole process of generating the dithering matrices can be formally described as follows.

Construction 7 *The construction of the $lcm(s, t)/s$ dithering matrices for each input original share image for $s \neq t$:*

Step 1: *Concatenate $lcm(s, t)/s$ starting dithering matrices with s entries, and divide these starting dithering matrices into $lcm(s, t)/t$ blocks.*

Step 2: *Choose the m embedding positions in each block.*

Step 3: *Concatenate the $lcm(s, t)/t$ blocks, and divide them into $lcm(s, t)/s$ dithering matrices.*

Step 4: *For each dithering matrix, remove the embedding positions, and the rest positions in each dithering matrix constitute the universal set for this dithering matrix.*

Step 5: *Generate the dithering matrixes according to Construction 6.*

To demonstrate how the above steps can be executed, we give the following example for an embedded $(2, 2)$-EVCS.

Example 5 *We take the embedded* $(2, 2)$*-EVCS as an example, i.e. the pixel expansion of the corresponding VCS is* $m = 2$*. Suppose the halftone pixel expansion is 9, i.e.* $s = 9$*. Suppose that we embed the secret information into every 6 sub-pixels, i.e.* $t = 6$*. Then we need to construct* $lcm(9, 6)/9 = 2$ *dithering matrices for each input original share image. Let the starting dithering matrices* D *of the two dithering matrices that have the same pattern as shown in Matrix 6.*

We first concatenate s *starting matrices and divide them into 3 blocks as shown in Matrix 7.*

$$D = \begin{array}{|c|c|c|}\hline 7 & 0 & 5 \\ \hline 2 & 4 & 6 \\ \hline 3 & 8 & 1 \\ \hline \end{array}$$

Matrix 6

$$\begin{array}{|c|c||c|c||c|c|}\hline 7 & 0 & 5 & 7 & 0 & 5 \\ \hline 2 & 4 & 6 & 2 & 4 & 6 \\ \hline 3 & 8 & 1 & 3 & 8 & 1 \\ \hline \end{array}$$

Matrix 7

We choose the positions 7 and 0 in the first block, and the positions 6 and 2 in the second block, and the positions 8 and 1 in the third block. By removing these positions, we get the universal set for each dithering matrix as follows: For the first dithering matrix, the universal set is $\mathcal{G} = \{1, 2, 3, 4, 5, 8\}$ *and for the second dithering matrix, the universal set is* $\mathcal{G}' = \{0, 3, 4, 5, 6, 7\}$*. According to Construction 3, we have the covering subsets for* $\mathcal{G}$ *as* $A_0 = \{2, 3, 4\}$*,* $A_1 = \{6, 7, 8\}$*, and for* $\mathcal{G}'$ *as* $A'_0 = \{0, 3, 4\}$*,* $A'_1 = \{5, 6, 7\}$*. Then according to Construction 6, we can construct the 2 dithering matrices* $D_{i,0}$ *and* $D_{i,1}$ *for the* i*-th share, where* $i = 0, 1$*, as shown in Matrix 8.*

$$D_{0,0}||D_{0,1} = \begin{array}{|c|c|c||c|c|c|}\hline 4 & 5 & 0 & 2 & 8 & 0 \\ \hline 7 & 2 & 3 & 3 & 6 & 1 \\ \hline 6 & 1 & 8 & 7 & 5 & 4 \\ \hline \end{array} \qquad D_{1,0}||D_{1,1} = \begin{array}{|c|c|c||c|c|c|}\hline 4 & 3 & 6 & 7 & 0 & 8 \\ \hline 2 & 7 & 5 & 3 & 1 & 6 \\ \hline 0 & 8 & 1 & 2 & 5 & 4 \\ \hline \end{array}$$

Matrix 8

At this point, we can halftone 2 pixels of the input original share images at a time, and embed 3 pixels of the secret image at a time.

7 Experimental results and comparisons

In this section, we give the experimental results for the algorithms and constructions in this paper. We also compare the proposed embedded EVCS with many of the well-known EVCS's in the literature.

First, we give the original images that will be used in the paper (Figure 3): Lena, airplane, baboon and the secret image. The size of the four images is 256×256; they will be scaled to their proper size when necessary.

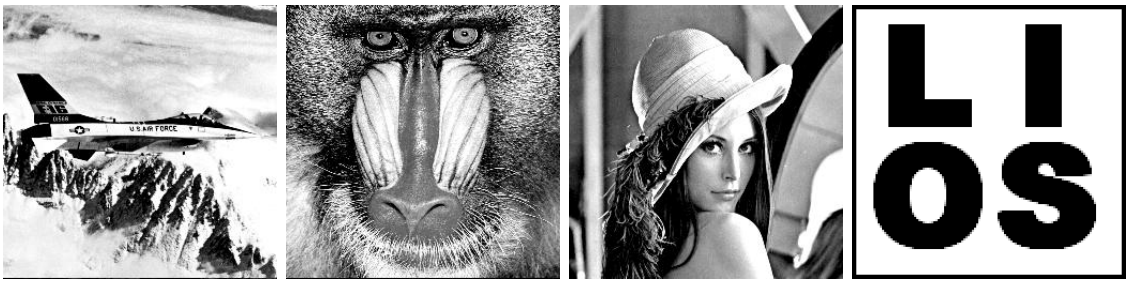

Figure 3: The original share images (airplane, baboon and lena) and the secret image.

We provide two well-known objective numerical measurements for the visual quality, the peak signal-to-noise ratio (PSNR) and the universal quality index (UQI) [30]. In this paper, the PSNR is adopted to assess the distortion of each share image with its original halftoned share image (i.e. without the darkening process). In such a way, the PSNR values in Table 9 and 10 can reflect the effects of a combination of the following possible processes in EVCS's: Darkening, embedding and modification. The PSNR is defined as follows,

$$PSNR = 10 \log \frac{255^2}{MSE} \tag{2}$$

where MSE is the mean squared error (MSE). The UQI is adopted to assess the distortion of each share image with its original grey-scale share image (after being scaled to the size of shares). Hence, the UQI value can reflect the effect of the halftoning process besides that of the darkening, embedding and modification processes in EVCS's. The formal definition of UQI can be found in [30]. In this paper, the block size of UQI is set to be 8 for all the experiments.

The original halftoned share images of the proposed schemes, here, are generated by applying Algorithm 1 on the original share images in Figure 3 directly, and the dithering matrix that is used during the halftoning process of each original share image, after being halftoned, is the same as that is used in the proposed scheme respectively. The original halftoned share images of the Zhou et al. and Wang et al.'s schemes in Figure 5 are generated by the blue noise halftoning technique and error diffusion halftoning technique on the original share images in Figure 3 directly.

We give two experimental results for the Construction 6, where the black ratio is reduced. The three images of Figure 6 are the experimental results of an embedded $(2, 2)$-EVCS, where the stacking of the two shares on the left will be the recovered image on the right. The share pixel expansion and secret image pixel expansion are 9 and 9 respectively. The contrast of the recovered secret image is 1/9. The PSNR and UQI values can be found in Table 10. Figure 4 show the experimental results of an embedded $(3, 3)$-EVCS [1], where the stacking of the shares airplane,

[1] One may observe grid patterns in the shares of Figure 4 and 6. In fact when the shares are in their original size

baboon and lena is the recovered secret text "LOIS". The share pixel expansion and secret image pixel expansion are 16 and 16 respectively. The contrast of the recovered secret image is 1/16. The PSNR and UQI values can be found in Table 9.

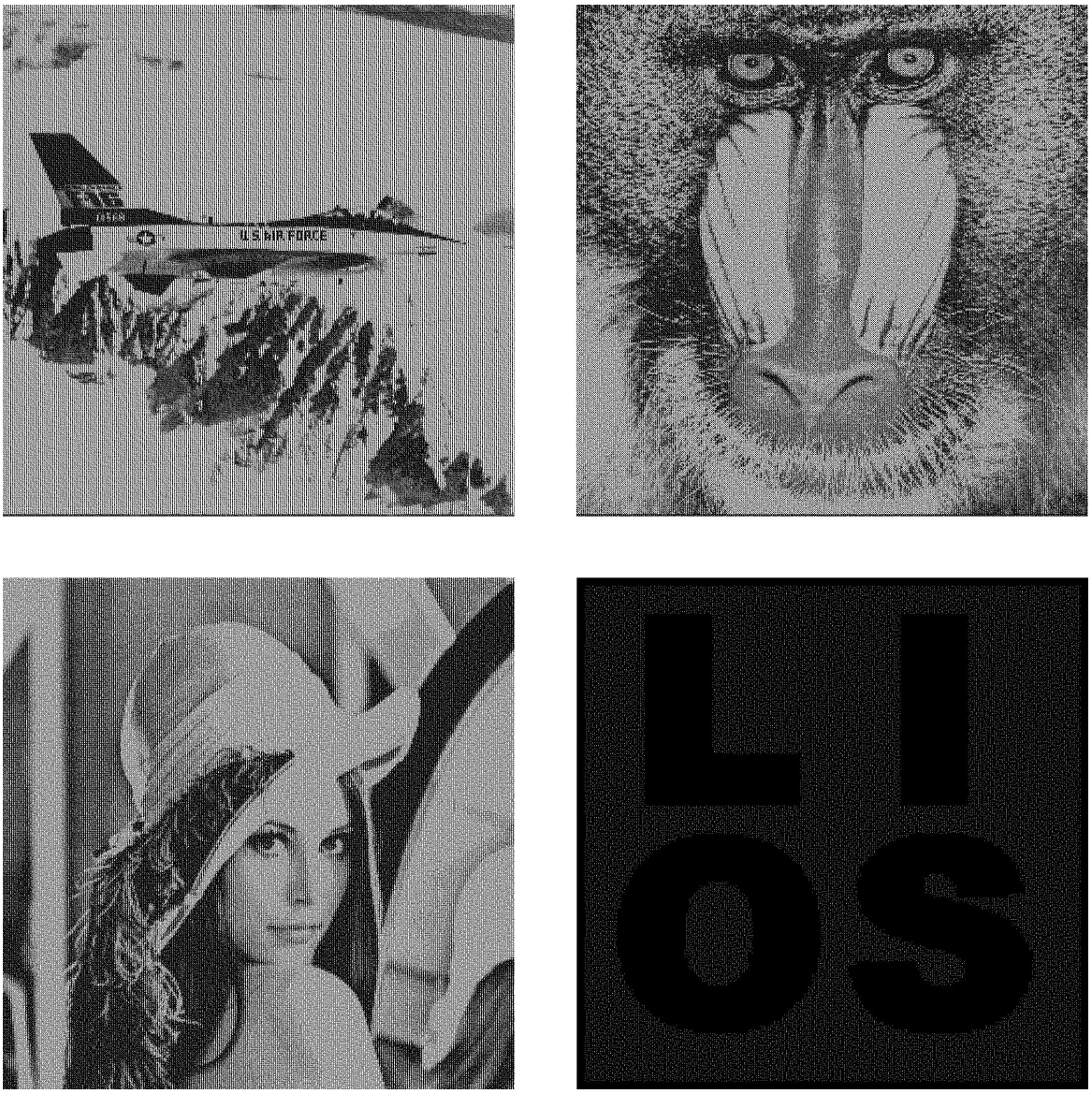

Figure 4: The shares and the recovered secret image of an embedded $(3, 3)$-EVCS after reducing the black ratios, the image size is 1024×1024.

Then we give the experimental results (Figure 5 and 6) to compare the visual quality of the shares between the proposed scheme and several well-known schemes proposed in [15–17, 23, 25], where, for each scheme, the stacking of the two shares on the left will be the recovered image on the right. The corresponding pixel expansions, contrast, PSNR and UQI values of each scheme can be found in Table 10.

The three images in the first line are the experimental results of the schemes proposed in [16],

the grid patterns are not obvious, and the grid patterns are exaggerated when we use latex to scale the image to a smaller size.

[15] and [17] with pixel expansion 9. Note that, the schemes proposed in [16], [15] and [17] have the same basis matrices for the case of $(2, 2)$-EVCS, hence they have the same experimental results. Because they do not support grey scale input share images, we first halftone the original share images into black and white images, then apply the schemes proposed in [16], [15] and [17], the PSNR values, in Table 9, are obtained by comparing the shares with the original halftoned share images. According to Figure 5, Figure 6 and Table 10, it is clear that, the visual quality of the share images of EVCS's proposed in [16], [15] and [17] is not as good as that of the proposed scheme.

The three images in the second line are the experimental results of the schemes proposed in [25] with share pixel expansion 9. Note that, the PSNR of first share image is larger than that of our scheme because it does not need the darkening process; however, the PSNR of the second share image is smaller than that of our scheme because it needs to be converted to its complementary image. According to the UQI values for the same original share image, the visual quality of the first share image is better than that of ours (0.0445 vs. 0.0293); the main reason is that, it does not need the darkening process. However, the visual quality of the second share image is worse than that of ours (-0.0315 vs. 0.0281). The main disadvantage of this EVCS is that, two complementary share images are needed; hence, it is much more likely to incur the watchdog's attention.

The three images in the third line are the experimental results of the second EVCS proposed in [23] with share pixel expansion 9. Note that the PSNR values are not as good as that of ours, and the UQI values are about the same to that of ours. The reason is the existence of ABPs (Auxiliary black pixels) in their scheme. The ABPs can be viewed as noises, and are diffused to other parts of the share images during the error diffusion halftoning process. And this is the very reason that their shares are vaguer than that of ours, e.g. in the share "Airplane", the word "FORCE" on the body of the airplane is not recognizable in their first share, while in our share the word "FORCE" can be recognized visually. Note that, the shares in the third line look smoother than that of ours. In fact, this is the most advantage of the second EVCS in [23].

The three images in the fourth line are the experimental results of the third EVCS proposed in [23] with share pixel expansion 9. Note that, the PSNR values of their scheme are smaller than that of ours, because it requires modifications to the halftone shares. However, the UQI values of their scheme are larger than that of ours, because it does not require darkening the images. According to the Figure 5, it can be observed that the main disadvantage of this EVCS is that, the visual content of each share image appears in each other. Actually, the third EVCS of [23] requires choosing approximately complementary share images. However, we choose the most popular images in the digital image processing society for simulation. The reasons are as follows: First, for a $(2, 2)$-EVCS, if we choose complementary share images, the third EVCS of [23] will be the same as the EVCS of [25]; Second, different share images affect the visual quality of the output shares significantly. It will be unfair if we choose different share images for the third EVCS

of [23]; At last, if we choose approximately complementary share images, the experimental results will conceal the disadvantage of the third EVCS of [23], i.e. the content of the share images affects each other. That is unfair for other schemes either.

At this point, from a subjective point of view, we can conclude that, the proposed EVCS, Zhou et al.'s EVCS and Wang et al.'s second EVCS all have their own advantages respectively. Among the five EVCS's in Figure 5 and 6, we can observe that proposed EVCS preserves the most details of the share images. For example, in the share "Airplane", only in our scheme one can recognizes the word "FORCE" on the body of the airplane. Zhou et al.'s EVCS generates the brightest shares. Wang et al.'s second EVCS generates the smoothest shares.

In order to get a clear insight of the visual quality of the experimental images in this section, we also give the objective numerical measurements as follows (Table 9 and 10), where PE' and PE" stand for share pixel expansion and secret image pixel expansion respectively.

	Content	PSNR			UQI					
	interaction	share 1	share 2	share 3	share 1	share 2	share 3	Contrast	PE'	PE"
Figure 4	No	8.69db	8.62db	8.93db	0.0311	0.0699	0.0215	1/16	16	16

Table 9: Objective numerical measurements of Figure 4.

	Content	PSNR		UQI				
	interaction	share 1	share 2	share 1	share 2	Contrast	PE'	PE"
[15–17]	No	3.19db	3.77db	0.0008	0.0032	2/9	9	9
[25]	Yes	9.54db	0.51db	0.0445	-0.0315	1/9*	9	9
Method 2 of [23]	No	3.16db	4.08db	0.0254	0.0304	1/9	9	9
Method 3 of [23]	Yes	4.62db	4.11db	0.0578	0.0332	1/9	9	9
Proposed scheme	No	5.67db	6.01db	0.0293	0.0281	1/9	9	9

Table 10: Objective numerical measurements of Figure 5 and 6.

In Table 10, the mark $*$ in the second line means that, the recovered secret image is disturbed by the visual contents of the share images. Note that, the void-and-cluster algorithm, applied in Zhou et al.'s scheme for choosing the secret pixel positions, is the very reason of this phenomenon.

Note that, the second column of Table 9 and 10 indicates whether the contents of the shares interact on each other, i.e. the contents of the shares relate to the contents of other shares. If the contents of the shares interact on each other, two drawbacks are obvious: First, the visual quality of the shares will be decreased; Second, it is much more likely to incur the watchdog's attention. Consider the content interaction between shares in EVCS of [25] and third EVCS of [23], it is unfair to compare the visual quality of a single share. In such a case, the second EVCS of [23] is most competitive to our EVCS for that is has similar UQI values for both shares to that of our

Figure 5: Comparing the experimental results of the proposed scheme and the scheme proposed in [15, 16, 23, 25] for the case of $(2, 2)$-EVCS. The size of all the images is 768×768.

Figure 6: Proposed $(2, 2)$-EVCS. The size of all the images is 768×768.

scheme. However, the PSNR values of the second EVCS of [23] are inferior to that of ours. It also reflects the fact that their EVCS preserves fewer details of share images than that of ours.

Besides the visual quality, compared with the known EVCS's in the literature [15, 16, 18, 20], the proposed scheme also has the following advantages:

- First, the EVCS's proposed in [15, 16] can only deal with binary input share images, while our proposed embedded EVCS can deal with grey-scale input images.

- Second, the minimum secret image pixel expansion of the proposed embedded EVCS is $m+1$, however, the secret image pixel expansion of the EVCS in [16] is $m + q$ $(q \geq 2)$, and the secret image pixel expansion of the EVCS in [15] is $\sum_{q=1}^{n} 2^{q-1} b_q$, which is much larger than that of the proposed embedded EVCS, and the secret image pixel expansion of the EVCS in [17] is $m + m_0$ where $m_0 \geq \lceil n/(k-1) \rceil$.

- Third, the EVCS proposed in [18] is only for the (2,2) access structure, and the scheme may have security issues when relaxing the constraint of the dynamic range as already noted in [18]. Besides, Wang et al.'s [23] second EVCS is also only for threshold access structure. Our proposed embedded EVCS can be applied on general access structure and is always unconditionally secure which is inherited from the corresponding VCS. In fact, the way of generating auxiliary black pixels of Wang et al. can be viewed as a special case of the proposed method in Section 4.

- Fourth, the EVCS schemes proposed in [20–22] and the first EVCS proposed in [23] require a pair of complementary input share images for each qualified subset, and the participants are required to take more than one shares for some access structure, while our proposed embedded EVCS does not have such requirement for the input share images, and each participant only needs to take one share.

- Fifth, compared with the third EVCS proposed in [23], the shares of our scheme do not affect each other and the original share image can be chosen arbitrarily.

- At last, the proposed embedded EVCS is flexible in the sense that there exist two trade-offs between the share pixel expansion and the visual quality of the shares and between the secret image pixel expansion and the visual quality of the shares. This flexibility allows the dealer to choose the proper parameters for different applications.

8 Conclusions

In this paper, we proposed a construction of EVCS which was realized by embedding the random shares into the meaningful covering shares. The shares of the proposed scheme are meaningful images, and the stacking of a qualified subset of shares will recover the secret image visually. We show two methods to generate the covering shares, and proved the optimality on the black ratio of the threshold covering subsets. We also proposed a method to improve the visual quality of the share images. According to the comparisons with many of the well-known EVCS in the literature [15, 16, 18, 20, 21, 23], the proposed embedded EVCS has many specific advantages against different well-known schemes, such as can deal with grey-scale input images, has smaller pixel expansion, always unconditionally secure, does not require complementary share images, one participant only needs to carry one share and can be applied for general access structure. Furthermore, our construction is flexible in the sense that there exist two trade-offs between the share pixel expansion and the visual quality of the shares and between the secret image pixel expansion and the visual quality of the shares.

Comparisons on the experimental results show that, the visual quality of the share of the proposed embedded EVCS is competitive with that of many of the well-known EVCS's in the literature.

9 Acknowledgements

The paper was first submitted in 2006, and has been reviewed for several times. During the reviewing procedure, many anonymous reviewers' comments are very valuable. We thank a lot to these anonymous reviewers. This work was supported by China national 973 project No. 2007CB311202, NSFC grants No. 60903210 and China national 863 project No.2009AA01Z414.

References

[1] A. Shamir. How to share a secret. In *Communications of the ACM*, volume 22 (11), page 612C613, 1979.

[2] G. R. Blakley. Safeguarding cryptographic keys. In *Proceedings of the National Computer Conference*, volume 48, page 313C317, 1979.

[3] M. Naor and A. Shamir. Visual cryptography. In *EUROCRYPT '94, Springer-Verlag Berlin*, volume LNCS 950, pages 1–12, 1995.

[4] M. Naor and B. Pinkas. Visual authentication and identification. In *Crypto '97, Springer-Verlag LNCS*, volume 1294, pages 322–336, 1997.

[5] T.H. Chen and D.S. Tsai. Owner-customer right protection mechanism using a watermarking scheme and a watermarking protocol. In *Pattern Recognition*, volume 39, pages 1530–1541, 2006.

[6] P. Tuyls, T. Kevenaar, G.J. Schrijen, T. Staring, and M.V. Dijk. Security displays enabling secure communications. In *First International Conference on Pervasive Computing, Boppard Germany, Berlin Springer LNCS*, volume 2802, pages 271–284, 2004.

[7] C. Blundo, A. De Bonis, and A. De Santis. Improved schemes for visual cryptography. In *Designs, Codes and Cryptography*, volume 24, pages 255–278, 2001.

[8] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson. Visual cryptography for general access structures. In *Information and Computation*, volume 129, pages 86–106, 1996.

[9] N. Krishna Prakash and S. Govindaraju. Visual secret sharing schemes for color images using halftoning. In *Proceedings of the International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007)*, volume 3, pages 174–178, 2007.

[10] H. Luo, F.X. Yu, J.S. Pan, and Z.M. Lu. Robust and progressive color image visual secret sharing cooperated with data hiding. In *Proceedings of the 2008 Eighth International Conference on Intelligent Systems Design and Applications*, volume 3, pages 431–436, 2008.

[11] Y.C. Hou. Visual cryptography for color images. In *Pattern Recognition*, volume 1773, pages 1–11, 2003.

[12] F. Liu, C.K. Wu, and X.J. Lin. Color visual cryptography schemes. In *IET Information Security*, volume 2, Issue 4, pages 151–165, 2008.

[13] S.J. Shyu, S.Y. Huang, Y.K. Lee, R.Z. Wang, and K. Chen. Sharing multiple secrets in visual cryptography. In *Pattern Recognition*, volume 40, Issue 12, pages 3633–3651, 2007.

[14] P.A. Eisen and D.R. Stinson. Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels. In *Designs, Codes and Cryptography*, volume 25, pages 15–61, 2002.

[15] S. Droste. New results on visual cryptography. In *CRYPTO '96, Springer-Verlag LNCS*, volume 1109, pages 401–415, 1996.

[16] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson. Extended capabilities for visual cryptography. In *ACM Theoretical Computer Science*, volume 250 Issue 1-2, pages 143–161, 2001.

[17] D.S. Wang, F. Yi, and X.B. Li. On general construction for extended visual cryptography schemes. In *Pattern Recognition*, volume 42, pages 3071–3082, 2008.

[18] M. Nakajima and Y. Yamaguchi. Extended visual cryptography for natural images. In *WSCG Conference 2002*, pages 303–412, 2002.

[19] D. S. Tsai, T. Chenc, and G. Horng. On generating meaningful shares in visual secret sharing scheme. In *The Imaging Science Journal*, volume 56, pages 49–55, 2008.

[20] Z. Zhou, G.R. Arce, and G. Di Crescenzo. Halftone visual cryptography. In *IEEE Transactions on Image Processing*, volume 15, NO.8, pages 2441–2453, 2006.

[21] Z.M. Wang and G.R. Arce. Halftone visual cryptography through error diffusion. In *IEEE International Conference on Image Processing*, pages 109–112, 2006.

[22] Z.M. Wang, G.R. Arce, and G. Di Crescenzo. Halftone visual cryptography via direct binary search. In *EUSIPCO '06*, 2006.

[23] Z.M. Wang, G.R. Arce, and G. Di Crescenzo. Halftone visual cryptography via error diffusion. In *IEEE Transactions on Information Forensics and Security*, volume 4 No.3, pages 383–396, 2009.

[24] L.A. MacPherson. Grey level visual cryptography for general access structures. In *Master Thesis, University of Waterloo*, 2002.

[25] Z. Zhou, G.R. Arce, and G. Di Crescenzo. Halftone visual cryptography. In *Proceedings of 2003 International Conference on Image Processing*, volume 1, pages I–521–524, 2003.

[26] D. Jin, W.Q. Yan, and M.S. Kankanhalli. Progressive color visual cryptography. In *Journal of Electronic Imaging*, volume 14, Issue 3, page 033019, 2005.

[27] C.C. Lin and W.H. Tsai. Visual cryptography for gray-level images by dithering techniques. In *Pattern Recognition Letters*, volume 24, Issue 1-3, pages 349 – 358, 2003.

[28] J.O. Limb. Design of dither waveforms for quantized visual signals. In *Bell System Technology Journal*, volume 48,7, pages 2555–2582, 1969.

[29] G.J. Simmons, W.Jackson, and K. Martin. The geometry of shared secret schemes. In *Bulletin of the ICA*, pages 71–88, 1991.

[30] Zhou W. and A.C. Bovik. A universal image quality index. In *IEEE Signal Processing Letters*, volume 9(3), pages 81–84, 2002.