K out of *K* Extended Visual Cryptography Scheme Based on "*XOR*"

Wanli Dang[1]*, Mingxing He[1], Daoshun Wang[2], Xiao Li[1]
[1]Department of Mathematics and Computer Engineering, Xihua University, Chengdu 610039, China.
[2]Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China.

*Corresponding author. Tel.: 18781961187; email: dangwanli417@sina.com
Manuscript submitted October 23, 2014, accepted April 10, 2015.
doi: 10.17706/ijcce.2015.4.6.439-453

Abstract: Visual cryptography schemes (*VCS*) is an encryption technique that utilizes human visual system in recovering secret image and it does not require any complex calculation. Many *VCS*s without pixel expansion have been proposed. But they recover secret image with low contrast due to the stacking operation. To improve the quality of recovered image, XOR-based *VCS* has been proposed. However, shares constructed from XOR-based *VCS* are random-looking. It suffers a management problem which dealers cannot visually identify each share. In this paper, we propose an (*k*, *k*) extended visual cryptography scheme (*EVCS*) by "XOR" operation to solve above mentioned problem. This is implemented by diving the share image into two parts using a parameter and operating the secret pixels and cover pixels respectively. Comparing with previous schemes, the qualities of share images and recovered image are improved, and our scheme also suit the "OR" operation.

Key words: Contrast, pixel expansion, probability, visual secret share, XOR.

1. Introduction

A (*k, n*) Visual cryptography scheme (*VCS*) firstly proposed by Naor and Shamir [1] encodes a secret image into *n* random-looking shares that appears distinctly different from an "innocent-looking" meaningful image. The secret can be visually recovered by stacking *k* or more shares. But such random-looking images would attract the attention of attackers. One solution to this problem is encoding the secret in meaningful share images. An important advantage of using meaningful share images is that one can clearly identify each share by vision [2]. Ateniese *et al*. [3] have proposed an extended visual cryptographic scheme (*EVCS*) to encode a secret image into *n* meaningful images. This scheme was implemented by concatenating an extended matrix to each basis matrix. Zhou *et al*. [4] improved upon Ateniese's method for dealing with halftone images designed to make the recovered image less unclear. Chang *et al.* [5] found a way to hide a color secret image in two color cover images, but pixel expansion made the share images nine times large than the original image. Wang *et al*. [6] presented a general construction method for the extended matrix and proved the minimum bound of the size of the extended matrix. Their method is simple and easy to operate. These schemes are realized based on a larger pixel expansion.

Because the visual quality of a recovered image is degraded by a large pixel expansion, most studies try to reduce the pixel expansion [7]-[10]. For example, Yang *et al.* [7] proposed a scheme to construct *VCS* with no pixel expansion using probabilistic method (*PVCS*). But these schemes generate shares are random-looking.

Chen *et al*. [11] extended Random Grids-*VCS* to a user-friendly (2, 2)-*VCS*, which resolves the pixel expansion problem and the share meaningless problems by complementary cover images. Ref. [12], [13] continues Chen's work proposed (*k*, *k*)-*EVCS* schemes which resolve the pixel expansion and the share meaningless problems. However, the visual qualities of share images and recovered image of their schemes [11]-[13] should be further improved.

In order to improve the contrast of recovered image, another model of *VCS* was proposed by Tuyls [14]. This model constructs an efficient (*k*, *k*)-*VCS* based on "*XOR*". A number of *XOR*-based *VCS*s were proposed in [15], [16]. The share images of these schemes are still meaningless. Liu *et al.* [17] proposed an *EVCS* for the even *k* which based on the "*XOR*" operation, this can make the share images show the meaningful content, but there exists extra pixel expansion. So far the study of *VCS* has been mainly on the *OR* and *XOR* operations [18]-[20]. By a comparison of these two operation, we can find that *XOR* operation –based *VCS* have better parameters in the sense of large contrast and smaller pixel expansion, but the used hardware devices are a bit more complex than the *OR* operation-based *VCS*. Hence, a *XOR* operation-based *VCS* which also works under the *OR* operation should be a better choice.

To solve the above problems, in this paper, we will propose a (*k*, *k*)-*EVCS* with no pixel expansion by the "*XOR*" operation which use the probability method. This scheme improves the qualities of recovered image and share images and also works under the *OR* operation. Further, we will give a (*k*, *n*) *XOR*-based meaningful *VCS*.

This paper is organized as follows: In Section 2, we introduce some related works and motivation. In Section 3, we show our scheme and give some theorems about the proposed scheme. In Section 4, we give some experimental results and compare our scheme with the previous schemes. In Section 5, we conclude this paper.

2. Related Works and Motivation

In order to better illustrate our scheme, we introduce some notations as Table 1.

Table 1. Introduction of Notations

Notation Used	
B_0 and B_1	basis matrices of *VCS*
$H(.)$	the Hamming weight
m	pixel expansion for *VCS*
$\lvert A \rvert$	the size of the matrix *A*
$P_{0,OR}$ ($P_{1,OR}$)	the probability of white pixels in the white and black areas when operated by "*OR*" operation
$P_{0,XOR}$ ($P_{1,XOR}$)	the probability of white pixels in the white and black areas when operated by "*XOR*" operation
$P_{0,XOR,s}(P_{0,XOR,c})$	the probability of white pixels in the white and black areas of S_f^s when operated by "*XOR*" operation
$P_{1,XOR,s}(P_{1,XOR,c})$	the probability of white pixels in the white and black areas of S_f^c when operated by "*XOR*" operation
$P_{0,OR,s}(P_{0,OR,c})$	the probability of white pixels in the white and black areas of S_f^s when operated by "*OR*" operation
$P_{1,OR,s}(P_{1,OR,c})$	the probability of white pixels in the white and black areas of S_f^c when operated by "*OR*" operation

2.1. VCS-Based "*XOR*"

Tuyls *et al.* [14] gave the contrast and security conditions for *XOR*-based *VCS*. And they showed some

construction methods for *XOR*-based *VCS.* Then Yang and Wang [10] give a formal definition of conditions for *XOR*-based *VCS* based on the *OR*-based *VCS* [1].

Definition 1[10]: The (*k*, *n*)-*VCS* proposed by Shamir which based on "*OR*" operation is still valid under the "*XOR*" operation. And let l' and h' represent the whiteness of black and white area in the recovered image when we stack the shares by "*XOR*". Let the notation $XOR(B_i \mid r)$, *i*=0, 1, denote the *XOR*-ed vector of any *r* rows in B_i .The *VCS* scheme based on "*XOR*" operation is considered valid if the following two conditions are met.

1) **[Security]:** $H(XOR(B_1 \mid r)) = H(XOR(B_0 \mid r))$ for $r \le (k-1)$.
2) **[Contrast]:** $H(XOR(B_1 \mid r)) \ge (m - l')$ and $H(XOR(B_0 \mid r)) \le (m - h')$ where $0 \le l' \le h' \le m$, i.e. $H(XOR(B_1 \mid r)) - H(XOR(B_0 \mid r)) \ge (h'-l')$ for $r = k$.

The first condition (1) assures the perfect secrecy of the scheme. The second condition (2) shows that the secret image can be visually revealed through their different contrasts of black and white colors. The contrast $\alpha_{XOR} = [H(XOR(B_1|r) - H(XOR(B_0|r)]/m = (h'-l')/m$ is then defined as the difference in weight between a white pixel and a black pixel in the reconstructed image [10].

Example 2.1: Consider a (3, 3)-*VCS* with basic matrices: $B_0 = \begin{bmatrix} 0110 \\ 0101 \\ 0011 \end{bmatrix}$, $B_1 = \begin{bmatrix} 1001 \\ 0101 \\ 0011 \end{bmatrix}$.

Since $H(XOR(B_0 \mid 2)) = 2$, $H(XOR(B_1 \mid 2)) = 2$, this satisfies condition (1). Also, $H(XOR(B_0 \mid 3)) = 0$ and $H(XOR(B_1 \mid 3)) = 4$, this satisfies condition (2). The contrast is: $\alpha_{XOR} = [H(XOR(B_1 \mid 3)) - H(XOR(B_0 \mid 3)] / m = 1$.

We know, in ref. [1], the *VCS* can be implemented based on "*OR*" operation, let l, h represent the whiteness of black and white area in the recovered image when we stack the shares by "*OR*" operation, and the contrast of this scheme is represented by $\alpha_{OR} = (h-l)/m$. So the following theorem can be obtained.

Theorem 1[10]: The *VCS* proposed by Shamir [1] which was based on "*OR*" operation is still a valid under the "*XOR*" operation. The difference of white whiteness and black whiteness is $h'-l' = 2^{(k-1)} \times (h-l)$. And $\alpha_{XOR} = 2^{(k-1)} \cdot \alpha_{OR}$.

Example 2.2 (continuation of Example 2.1): In a (3, 3)-*VCS* which have been given in example 2.1 with $h = 1, l = 0, m = 4$ and $h' = 4, l' = 0$ by "*OR*" and "*XOR*" operation, we can obtain $\alpha_{OR} = (h-l)/m = 1/4$, then $\alpha_{XOR} = 2^{(k-1)} \cdot \alpha_{OR} = 2^{(3-1)} \cdot (1/4) = 1$.

2.2. *PVCS*-Based "*OR*"

The *PVCS* can solve the problem of pixel expansion for *VCS*. In *PVCS*, the probability of white pixels in the white area is higher than it in the black area of recovered image. Naor and Shamir's *VCS* [1] was implemented by using two basis matrices B_1 and B_0 . A secret pixel is expanded to m sub-pixels and the number of black pixels for a white and black secret pixel is l and h, they also give the security and contrast conditions. Yang *et al.* [7] proposed (*PVCS*) for binary images with no pixel expansion. The basis matrices can use all the columns of B_1 and B_0 . Then we will give the following definition.

Definition 2[7] : Based on the basic matrix, we can obtain that the probabilities of white sub-pixels in the white and black areas of recovered image are $p_{0,OR} = h/m, p_{1,OR} = l/m$. The average contrast is defined as $\bar{\alpha}_{OR} = p_{0,OR} - p_{1,OR} = (h-l)/m$.

In real situation, when two images have the same contrasts, but visual qualities of them are different, because of the black areas in the recovered image are not reconstructed as 100% black. So they need to modify the contrast to consist with the real situation.

Definition 3[7]: A new average contrast is defined by their observation of the actual situation, $\bar{\alpha}_{OR} = (p_{0,OR} - p_{1,OR}) / (1 + p_{1,OR})$.

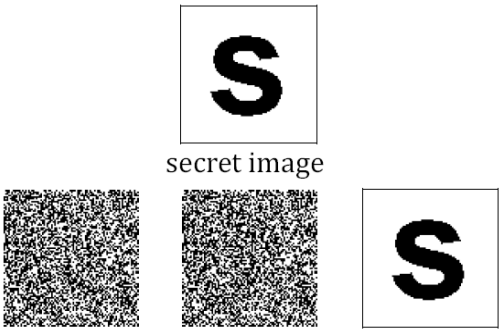
2.3. Motivation

In order to improve the contrast of recovered image, "*XOR*" operation of *VCS* was proposed. The VCS proposed by Shamir which based on "*OR*" operation is still valid under the "*XOR*" operation. When we operate secret image by probabilistic method based on "*XOR*" in $(k,k)-VCS$, we will find that every pixel of secret image can be correctly reconstructed.

Example 2.3: Construct basis matrices for (2, 2)-*VCS*, the basis matrices B_0 and B_1 are shown below.

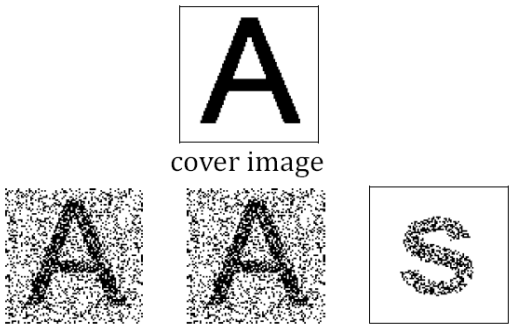
$$B_0 = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}, \quad B_1 = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}.$$

We operate secret image by probabilistic method based on "*XOR*", the experimental result is shown below. Our all experiments use secret image is following, where "$\otimes$" represents the "*XOR*" operation (See Fig. 1 and Fig. 2).



share 1 share 2 share 1 $\otimes$ share 2

Fig. 1. The experiments for "$\otimes$"operation.



share 1 share 2 share 1 $\otimes$ share 2

Fig. 2. The experiment for our method.

This can correctly reconstruct secret image and with no pixel expansion, however share images are looking-random, these suffer from a management problem-dealers cannot identify shares. Conventional *EVCS*s designed basis matrices to encode each secret pixel as a block of sub-pixels, which leads to a pixel expansion problem. Chen and Tsao [11] extended Random Grids (*RG*)-based *VCS* to a user-friendly (2, 2)-*VCS*, which resolves the pixel expansion problem and the share images are meaningful by complementary cover images. The contrast of the recovered image and meaningful shares is a tradeoff made by adjusting parameters during construction of the method. If we use their method to divide share images into two parts, a part is used to operate secret pixel, another is used to embed cover pixels, when we stack the shares by "*XOR*", we can implement the result as follows (The operation method will be presented in Section 3).

The visual quality of shares and recovered images can be improved compared with Chen and Tsao's method. More details discuss in Section 4. We know *XOR*-based *VCS* can improved the qualities of images, but have a bit more complex than the *OR* operation-based *VCS*. *So* an *EVCS* that can work both under the *OR* and *XOR* operation will be a better choice. In this work, we guess whether our method can be extended to a

general (*k*, *k*)-scheme for sharing binary secret images by "*XOR*" operation. And the proposed scheme also suit the "*OR*" operation. The objectives of the study include solving the pixel expansion, providing an adjustable contrast for recovered image and meaningful shares to satisfy dealers' requirements, and improving the qualities of the recovered images and share images.

3. The Proposed Scheme

In this section, we propose a (*k*, *k*)-*EVCS* scheme for binary images by the "*XOR*" operation. In Section 3.1, we describe the construction procedure for the shares. Next we analyze the proposed scheme with the help of the previous results which are presented in Section 2.

3.1. The Process of Encryption

The proposed extended visual cryptographic scheme based on "*XOR*" extends from user friendly RG-based *VCS* proposed by Chen and Tsao [11]. The proposed (*k*, *k*)-*EVCS* based on "*XOR*" operation can implement the meaningful shares and generate the share images and recovered image with no pixel expansion. In the encoding phase, a secret image *S* and a cover image *C*, both with the size of $p \times q$ are encoded in *k* meaningful shares S_f (*f*=1,...,*k*) with the same size of *S*.

The process of encoding a pixel is demonstrated in Fig. 3. One should select a parameter β, where β is used to make a trade-off visual qualities between share images and recovered image and choose an operation between a secret pixel *S* (*i*, *j*) and a cover pixel *C* (*i*, *j*) $(1 \le i \le p, 1 \le j \le q)$. While the results of stacking all share images $S_1 \otimes S_2 \otimes \cdots \otimes S_k$ will reveal the content of the secret image *S*.

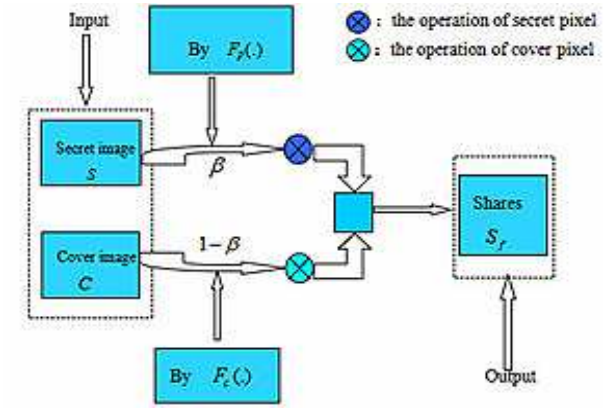


Fig. 3. The process of encryption.

In Fig. 3, the equation of $F_p(.)$ will be designed as follows: when $S(i, j) = 0$, we will randomly select column from B_0; when $S(i, j) = 1$, we will randomly select column from B_1. This is the probability method, the basic matrices are B_0 and B_1. And the Equation of $F_C(.)$ will be designed as follows:

$$F_C(\cdot) = \begin{cases} S_f(i, j) = 1, \text{if } C(i, j) = 1 \\ S_f(i, j) = 0, \text{if } C(i, j) = 0 \end{cases} \quad \text{(a)}$$

In the design of the equation $F_C(.)$, $S_f(i, j)$ denotes the each share image pixel $(1 \le i \le p, 1 \le j \le q)$. This can implement the meaningful share images. In our scheme, the designs of the encoding process and the cover image embedding process for (*k*, *k*)-*EVCS* are separated. With the parameter β, the proposed

scheme provides an adjustable contrast for meaningful shares and recovered image to satisfy dealers' requirements.

3.2. Construction of Shares

For easily illustrating the proposed scheme, a definition and notations are given first.

In the following Algorithm 1, the function $X \leftarrow F(M)$ randomly selects an unrepeatable pixel position (i, j) from the input image *M* and stores (i, j) into the sequence *X*, where $1 \le i \le p, 1 \le j \le q$. S_f represents share image which shows the content of cover image. S_f^c represents the area of S_f when we operate the pixels of cover image and store them in the corresponding positions of the share image S_f. Similarly, S_f^s represents the area of S_f when we operate the pixels of secret image and store them in the corresponding positions of the share image S_f. Thus S_f, S_f^c, S_f^s satisfy: $S_f = S_f^c \cup S_f^s$ and $S_f^c \cap S_f^s = \varnothing$. When we stack the shares, $S_1 \otimes S_2 \otimes \cdots \otimes S_k$, the secret information will be revealed. Next we will give the construction of (*k*, *k*)-*EVCS* by "*XOR*" operation.

Let B_0 and B_1 be the basis matrices for a binary *VCS* with pixel expansion m and contrast α, Boolean *XOR* operation. Our proposed (*k*, *k*)-*EVCS* takes two input images: one is the secret image S, the other is cover image C.

Next, we will give an example which can help us to understand the Algorithm 1.

Algorithm 1:

Input: A secret image $S = \{S(i,j) \mid 1 \le i \le p, 1 \le j \le q\}$, a cover image $C = \{C(i,j) \mid 1 \le i \le p, 1 \le j \le q\}$. And a parameter β, $0 \le \beta \le 1$.

Output: ***k*** shares with meaningful $S_f (f = 1, \cdots, k)$ $S_f = \{S_f(i, j) \mid 1 \le i \le p, 1 \le j \le q\}$.

Step1: Generate a random bit α which satisfies: $p(\alpha = 0) = \beta, p(\alpha = 1) = 1 - \beta$

Step2: If $\alpha = 0$, we operate the pixels of secret image $S(i, j)$, and store it in $S_f^s(i, j)$ of the shares. Namely, $S_f^s(i, j) \leftarrow F(F_p(S(i, j)))$.

Step3: If $\alpha = 1$, we operate the pixels of cover image $C(i, j)$, and store it in $S_f^c(i, j)$ of the shares. Namely, $S_f^c(i, j) \leftarrow F(F_C(C(i, j)))$.

Step4: If *k* is even, Output S_f $(f = 1, \cdots, k)$

Step5: If *k* is odd, when the generated k pixels ($S_f(i, j) = 0$, $f = 1, \cdots, k$) for the areas of S_f^c are all white, we randomly choose a $S_f^c(i, j)$ and set it to 1.

Step6: Output ($S_1, S_2, \cdots, S_k$)

Example 3.1: A (3, 3)-*EVCS* scheme, the main codebook B_0 and B_1 are $B_0 = \begin{bmatrix} 0110 \\ 0101 \\ 0011 \end{bmatrix}$ and $B_1 = \begin{bmatrix} 1001 \\ 0101 \\ 0011 \end{bmatrix}$ and

$\beta = 0.5$. Fig. 2 illustrates the encryption process in the scheme.

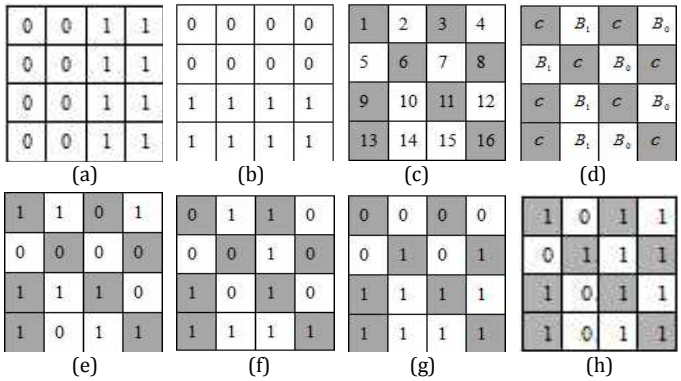


Fig. 4. An example of (3, 3)-*EVCS* with β=0.5: (a) Secret image; (b) Cover image; (c) Coordinates; (d) Encryption decision, B_i(i=0, 1): the selected encoding for secret image, C: for cover image; (e) Share 1; (f) Share 2; (g) Share 3; (h) Share1⊗Share2⊗Share3.

Fig. 4 presents the process of encoding secret image and embedding cover image. And "1" represents the black pixel, "0" represents the white pixel. The black blocks represent the area of S_f^c, the white blocks represent the area of S_f^s. Fig. 4(e)-Fig. 4(g) illustrate share1-share3. We randomly select column from B_0 to encrypt pixels for secret image at coordinates 2, 5, 10, 14. Similarly, we randomly select column from B_1 to encrypt pixels for secret image at coordinates 4, 7, 12, 15. Then we embed pixels for cover image at coordinates 1, 3, 6, 8, 9, 11, 13, 16 based on the step 3 of algorithm 1. Observation of the (h), the black blocks are black, so the cover image does not leave any trace in the recovered image. And obviously, the white pixels in the white area more than in the black area of recovered image, so the secret image can be revealed.

3.3. Analysis of Images' Contrasts

In this section, we will analyze the contrasts of recovered image and share images with the help of the previous results which are presented in Section 2.

3.3.1. Contrast of recovered image

We use the probabilistic *VCS* method for $S(i, j)$. Before proving the theorem of the contrast of recovered image, we need to present three lemmas.

Lemma 1 [1]: For a probabilistic (k, k)-*VCS*, when we stack the shares by "*OR*" operation. We can obtain $P_{0,OR} = 1/2^{k-1}$, $P_{1,OR} = 0$ and $\alpha_{OR} = 1/2^{k-1}$.

Lemma 2: For a probabilistic (k, k)-*VCS* scheme, when we stack the shares underlying "*XOR*" or "*OR*" operation. We can obtain $\alpha_{XOR} = 2^{(k-1)} \cdot \alpha_{OR}$.

Proof: Because of the probabilistic (k, k)-*VCS*'s implementation can use all the column of B_0 and B_1. So the result of the theorem 1 also suit for the Lemma 2.

Lemma 3: For a probabilistic (k, k)-*VCS* scheme, when we stack the shares underlying "*XOR*" or "*OR*" operation. We can obtain: $p_{0,XOR} = 2^{(k-1)} \cdot p_{0,OR}$, $p_{1,XOR} = p_{1,OR} = 0$.

Proof: Form ref. [6], we know the property of the basis matrices of the (k, k)-*VCS*: the number of "1" is even for every column of B_0 and the number of "1" is odd for every column of B_1 and $|B_0| = |B_1| = 2^{k-1}$. By the property of *XOR* operation (0 for even "1" and 1 for odd "1"), when any k rows of $B_0(B_1)$ under the "*XOR*" operation, we can obtain: $P_{0,XOR} = 1$ and $P_{1,XOR} = 0$. From Lemma 2, we have: $P_{0,OR} = 1/2^{k-1}$ and

$P_{1,OR}=0$. Thus $p_{0,XOR}=2^{(k-1)}\cdot p_{0,OR}$ and $p_{1,XOR}=p_{1,OR}=0$.

Now we state the Theorem 2 as follows.

Theorem 2: The average contrast of the stacking result $S_1\otimes S_2\otimes\cdots\otimes S_k$ of Algorithm 1 is: $\overline{\alpha_F(m)}=\beta(0\le\beta\le 1)$.

Proof: From the encoding process of Algorithm 1, we know that $S_f(i,j)$ is from $S(i,j)$ with probability β and from $C(i,j)$ with probability $(1-\beta)$. Thus we have the following two cases:

1) $S_f(i,j)$ is from $S(i,j)$ with probability β. We consider the area of S_f^s. When we stack share images underlying "*OR*" operation, from Lemma 1, we can obtain:

$$p_{0,OR,s}=\beta/2^{k-1},\ p_{1,OR,s}=0. \tag{1}$$

From lemma 4, we can obtain:

$$p_{0,XOR,s}=\beta,\ p_{1,XOR,s}=0 \tag{2}$$

2) $S_f(i,j)$ is from $C(i,j)$ with probability $1-\beta$. We consider the area of S_f^c. By the property of *XOR* operation (0 for even "1" and 1 for odd "1") and the step 3, 4 of Algorithm1, we can obtain:

When *k* is even:

$$P_{0,XOR,c}=1\cdot(1-\beta),\ P_{1,XOR,c}=1\cdot(1-\beta) \tag{3}$$

When *k* is odd:

$$P_{0,XOR,c}=0\cdot(1-\beta),\ P_{1,XOR,c}=0\cdot(1-\beta) \tag{4}$$

Thus the average contrast of recovered image is:

$$\overline{\alpha_F(m)}=P_{0,XOR}-P_{1,XOR}=(P_{0,XOR,s}+P_{0,XOR,c})-(P_{1,XOR,s}+P_{1,XOR,c})=\beta$$

3.3.2. Contrast of share images

Property 1: Given a (*k*, *k*)-*VCS*, let its basic matrices be $B_i(i=0,1)$, we have:

1) $H(B_0\mid i)=H(B_1\mid i)$, *i* represents every row of B_i.

2) $H(B_0\mid i)=H(B_0\mid j), H(B_1\mid i)=H(B_1\mid j), i\ne j$.

3) The number of "1" is equal to the number of "0" for every row of $B_i(i=0,1)$.

Theorem 3: For any f satisfy $1\le f\le k$, the average contrast of share images S_f is: (1) when *k* is even, $\overline{\alpha_S(m)}=2(1-\beta)/(2+\beta)$; when *k* is odd, $\overline{\alpha_S(m)}=[2\cdot(k-1)\cdot(1-\beta)]/[k\cdot(2+\beta)]$.

Proof: From the Algorithm 1, we know that the proposed scheme procedure is designed differently with the different *k* (odd or even).

1) when *k* is even

- $S_f(i,j)$ is from $S(i,j)$ with probability β. We consider the area of S_f^s. From the property 1, the probabilities of white pixel in the white and black areas of S_f^s are:

$$p_{0,s} = (1/2)\cdot\beta, p_{1,s} = (1/2)\cdot\beta \tag{5}$$

where $p_{i,s}(i=0,1)$ represents the probability of white pixels in the white and black areas of S_f^s.

- $S_f(i,j)$ is from $C(i,j)$ with probability $1-\beta$. We consider the area of S_f^c. From the step 3 of Algorithm1, the probabilities of white pixels in the white and black areas of S_f^c are:

$$p_{0,c} = 1-\beta, p_{1,c} = 0 \tag{6}$$

where $p_{i,c}(i=0,1)$ represents the probability of white pixels in the white and black areas of S_f^c, thus we can obtain the probability of white pixels in the white area and black area of S_f are:

$$p_0 = p_{0,s} + p_{0,c} = (1/2)\cdot\beta + (1-\beta) \tag{7}$$

$$p_1 = p_{1,s} + p_{1,c} = (1/2)\cdot\beta + 0 = (1/2)\cdot\beta \tag{8}$$

From Equations (7), (8) and definition 3, we can obtain the average contrasts of share images are:

$$\overline{\alpha_S(m)} = (p_0 - p_1)/(1+p_1) = 2(1-\beta)/(2+\beta)$$

2) when k is odd

- $S_f(i,j)$ is from $S(i,j)$ with probability β. We can obtain that $p_{0,s} = (1/2)\cdot\beta, p_{1,s} = (1/2)\cdot\beta$.
- $S_f(i,j)$ is from $C(i,j)$ with probability $1-\beta$.

The share pixels are generated by Step 4 of Algorithm 1. When $C(i,j)=0$, the probability of generating white pixel of $S_f(i,j)$ is $(k-1)/k$. We can obtain, the probability of white pixels in the white (resp. black) area of X^C is:

$$p_{0,c} = [(k-1)/k]\cdot(1-\beta), p_{1,c} = 0. \tag{9}$$

Thus we can obtain that the probabilities of white pixels in the white and black area of S_f are:

$$p_0 = p_{0,s} + p_{0,c} = (1/2)\cdot\beta + [(k-1)/k]\cdot(1-\beta);$$
$$p_1 = p_{1,s} + p_{1,c} = (1/2)\cdot\beta + 0 = (1/2)\cdot\beta \tag{10}$$

From Equation (10) and definition 3, we can obtain that the average contrasts of share images are:

$$\overline{\alpha_S(m)} = (p_0 - p_1)/(1+p_1) = [2\cdot(k-1)\cdot(1-\beta)]/[k\cdot(2+\beta)]$$

3.4. Analysis of Algorithm1's Security

Theorem 4(security): For the proposed scheme, when we stack the share images, $S_1 \otimes S_2 \otimes \cdots \otimes S_k$, we can obtain $H(XOR(B_1 \mid r)) = H(XOR(B_0 \mid r)), (r < k)$. In other words, the probabilities of white sub-pixels in the white and black areas of recovered image are equal.

Proof: From the encoding process of Algorithm 1, the designs of the encoding secret image and embedding cover images are separated.

1) When $S_f(i, j)$ is from $S(i, j)$, from definition 1, we know the fact that the Hamming weight of the *XOR* of any *t, t<k,* rows are the same in the basic matrices $B_i (i = 0,1)$. So the probability of white sub pixels in the white and black areas of S_f^s is equal.
2) When $S_f(i, j)$ is from $C(i, j)$, since the $S_f(i, j)$ dose not depend on the secret pixel which is from $C(i, j)$. So the shares of S_f^c will not leak the secret information.

Therefore, the security condition is ensured.

3.5. Recognition of Small Areas in Secret Image

In a deterministic (*k*, *k*)-*VCS* scheme, there exists a difference between a recovered black pixel and a recovered white pixel. But in probabilistic *VCS* scheme, the difference is not maintained. In ref. [14], we know that the RG-based *VCS* is a special case of the probability *VCS*. So Chen's scheme also exists the recognition of small areas in the recovered image. In this section, we will discuss the recognition of small areas for our proposed scheme.

In ref. [7], let *N* be the total number of pixels in an area of secret image, S_N be the number of white pixels in that area of the recovered image. The probability of each pixel being white is $p_{0,OR}$ (resp. $p_{1,OR}$) in a white (Black) area of secret image. In ref. [6], the S_N obey the normal distribution. So it gets the lower bound of *N* that one can distinguish the black for the *Prob-VCS* scheme as the following:

$$N > 9[(\sqrt{p_{0,OR}(1-p_{0,OR})} + \sqrt{p_{1,OR}(1-p_{1,OR})}) / (p_{0,OR} - p_{1,OR} - d)]^2 \ (0 \le d \le (p_{0,OR} - p_{1,OR})) \tag{10}$$

For the proposed scheme, our recognition of small areas in the secret image is similar to Yang. So we can obtain:

$$N > 9[(\sqrt{p_{0,XOR}(1-p_{0,XOR})} + \sqrt{p_{1,XOR}(1-p_{1,XOR})}) / (p_{0,XOR} - p_{1,XOR} - d)]^2 \ (0 \le d \le (p_{0,XOR} - p_{1,XOR})) \tag{11}$$

From Lemma 3 and Algorithm 1, we can obtain:

$$p_{0,XOR} = 2^{k-1} \cdot \beta \cdot p_{0,OR}, \ \ p_{1,XOR} = 2^{k-1} \cdot \beta \cdot p_{1,OR} \tag{12}$$

In a (*k*, *k*)-*VCS* scheme, $p_{1,OR} = 0$, $p_{0,OR} = 1/2^{k-1}$,

From Equation (11), (12), the *N* satisfies the following equation:

$$N > 9[\sqrt{\beta(1-\beta)} / (\beta - d)]^2 (0 \le d \le \beta)$$

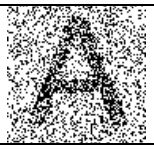
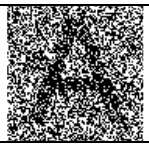
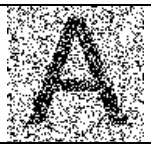
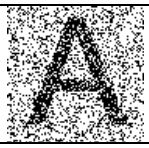
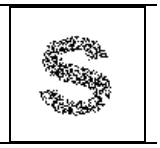
That is, the β determine the lower bound of *N*, the recognition of small areas in secret image do not rely on the basis matrices, the reason that is a white secret pixel must be decoded a white pixel and a black secret

pixel must be decoded a black pixel when we operate the shares by "*XOR*" in (*k*, *k*)-*VCS*. Many times, the share information is not more important than the secret information, so that we have $0.5 \le \beta < 1$.

4. Experiment and Comparison

This section, we first present the experimental results for our scheme and the previous schemes. The comparison experimental result is summarized as Table 2. Second, we compare the proposed scheme with some related schemes in two aspects: (1) The contrasts of share images and recovered image; (2) Comparing the proposed scheme with the previous in some typical aspects. Comparison results respectively by Tables 3 and 4.

Table 2. The Experimental Results for Some Schemes

Schemes with $\beta=0.5$	Share 1	Share 2	Recovered image
Chen and Tsao [7]			
	$\alpha_s = 3/11$	$\alpha_s = 3/11$	$\alpha_F = 1/9$
Guo [8]			
	$\alpha_s = 1/5$	$\alpha_s = 1/5$	$\alpha_F = 1/4$
Our scheme			
	$\alpha_S = 2/5$	$\alpha_S = 2/5$	$\alpha_F = 1/2$

In the Table 2, we choose the parameter $\beta = 0.5$. We can see, In Chen and Tsao [11]'s scheme, the visual qualities of their share images and recovered image are so far worse than the ones obtained with our scheme and Guo [12]'s scheme. The main reason is that in their scheme, the black areas in the recovered are not reconstructed as all black. And obviously, our scheme outperforms Guo's scheme in terms of the qualities of share images and recovered image.

From Table 3, we observed that as β increases for our scheme, the contrast of recovered image increase while the contrasts of share images decrease (the experimental results present in Appendix A). By observing Table 2 from left to right, we observed that when the value of β is certain, the proposed scheme outperforms the schemes proposed by Chen [11] and Guo [12] in terms of the contrasts of share images and recovered image.

Table 4 presents the results of comparison between our scheme and the previous schemes. From Table 4, we can see that comparing with the previous scheme, the quality of the share images and the recovered image are improved. And the proposed scheme has no pixel expansion with meaningful share images. But our scheme have a bit more complex than the *OR* operation-based Schemes. So sometimes, a scheme that can work both under the *OR* and *XOR* operation will be a better choice. When we consider (*k*, *k*)-*EVCS* with even *k*, we can use a pair of complementary cover images, when *k* is odd, and our input is not change (the experimental results present in Appendix B). The proposed scheme was based on "*XOR*" operation is still a valid under the "*OR*" operation.

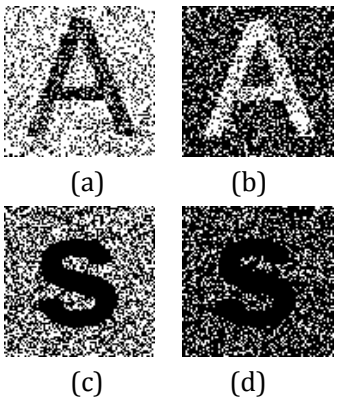
Table 3. The Contrasts of Share Images and Recovered Image That Are Generated by (2, 2)-*EVCS* with $\beta = 0$, 1/4, 1/2, 3/4, 1

β	Ref.[7](model 1) $\rho =$		Ref.[8]		Our scheme	
	$\alpha_S = \frac{1-\beta}{3}$	$\alpha_F = \frac{\beta}{3-\beta}$	$\alpha_S = \frac{1-\beta}{2+\beta}$	$\alpha_F = \frac{1}{2}\beta$	$\alpha_S = \frac{2(1-\beta)}{2+\beta}$	$\alpha_F = \beta$
0	1/3	0	1/2	0	1	0
1/4	1/4	1/11	3/9	1/8	2/3	1/4
1/2	1/6	1/5	1/5	1/4	2/5	1/2
3/4	1/12	1/3	1/11	3/8	2/9	3/4
1	0	1/2	0	1/2	0	1

Table 4. Comparison with Previous Results

Schemes	Pixel Expansion	Meaningful Share	Decryption	Complexity decryption	Visual Quality	Type of VSS
Ref.[3],[4]	Yes	Yes	*OR*	$O(1)$	Mediur	(k, n)
Ref.[11]	Yes	No	*XOR*	$O(k)$	High	(k, n)
Ref.[6]	No	No	*OR*	$O(1)$	Mediu	(k, n)
Ref.[5]	Yes	Yes	*XOR*	$O(k)$	High	(k, n)
Ref.[7]	No	Yes	*OR*	$O(1)$	Low	(k, k)
Ref.[8]	No	Yes	*OR*	$O(1)$	Mediu	(k, k)
Our	No	Yes	*XOR*	$O(k)$	High	(k, k)

For example: The proposed (2, 2)-*EVCS* with $\beta = 0.5$, our experimental results are shown in Fig. 5:



(a) (b) (c) (d)

Fig. 5. The experiments with (2, 2)-*EVCS*: (a) share1, (b) share2, (c) share1⊗share2, (d) share1⊗share2.

where the "$\oplus$"represent the "*OR*" operation, we can see, our proposed scheme not only suit the "*XOR*" operation, but also suit the "*OR*" operation.

5. Conclusion

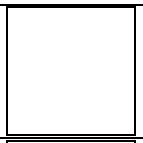
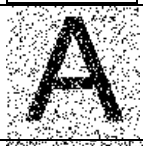
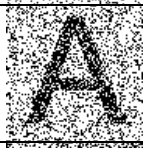
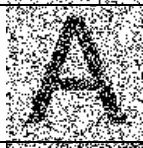
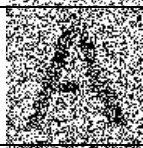
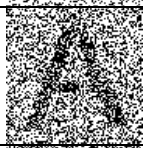
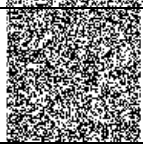
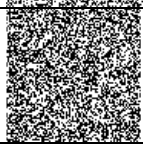
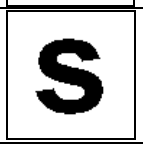
This paper proposed a (k, k)-*EVCS* scheme based on "*XOR*" operation. When we use a pair of complementary cover images for the even k, our scheme is still valid under the "*OR*" operation. The visual quality between share images and recovered image can be adjusted to be more friendly for the dealer by different β. Comparing with the previous scheme, the quality of the shadow images and the recovered image are improved.

Appendix

Appendix A

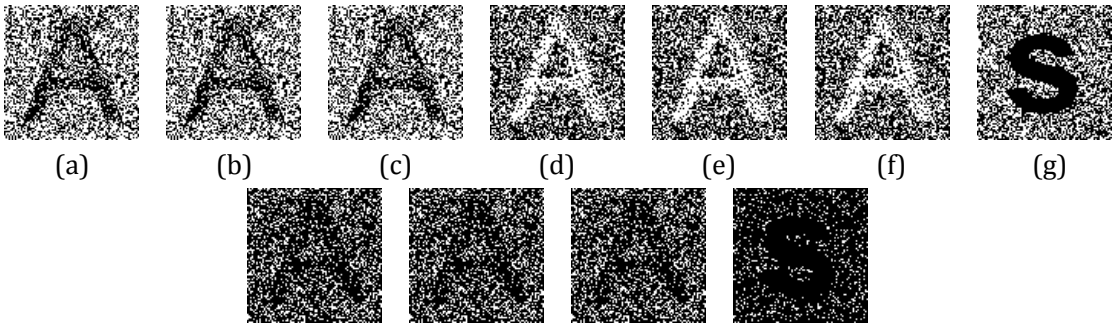
This section gives the experimental results for Algorithm 1 of (2, 2)-*EVCS* with β=0, 0.25, 0.5, 0.75 and 1. By observing Table 5 from top to bottom, it is convenient to see that as β increases, the quality of recovered image increase while the qualities of share images decrease, consistent with the above inference from Table 3.

Table 5. The Experimental Results for (2, 2)-*EVCS* with Different β

β	Share 1	Share 2	Recovered image
0			
1/4			
1/2			
3/4			
1			

Appendix B

This section gives the experiments of (3, 3)-*EVCS* with β = 0.5, we can see that when k is odd, the proposed scheme was based on "*XOR*" operation is still a valid under the "*OR*" operation. (See Fig. 6).



(a) (b) (c) (d) (e) (f) (g)

(h) (i) (j) (k)

Fig. 6. The experiments with (3, 3)-*EVCS*: (a) share 1, (b) share 2, (c) share 3, (d) share1⊗share2, (e) share1⊗share3, (f) share2⊗share3, (g) share1⊗share2⊗share3, (h) share1⊗share2, (i) share1⊗share3, (j) share2⊗share3, (k) share1⊗share2⊗share3.

Acknowledgments

This research was supported in part by the National Key Technology R.D Program of the Ministry of Science and Technology, (No.2011BAH26B00), International Cooperation Project of Sichuan Province (2009HH0009), Chunhui project of the Ministry of China (Z2014045), and Sichuan Province Key Discipline

Construction Project (ZD0802-09-1), and the Graduate Innovation foundation ycjj2014040.

References

[1] Naor, M., & Shamir, A. (1995). Visual cryptography. *Proceedings of Advances in Cryptology-EUROCRYPT'94*: *Vol. 950* (pp. 1-12).

[2] Droste, S. (1996). New results on visual cryptography. *Proceedings of Advances in Cryptology—CRYPTO'96* (pp. 401-415).

[3] Ateniese, G., Blundo, C., Santis, A. D., *et al.* (2001). Extended capabilities for visual cryptography. *Theoretical Computer Science*, *250(1)*, 143-161.

[4] Wang, Z., Arce, G. R., & Crescenzo, G. D. (2009). Halftone visual cryptography via error diffusion. *IEEE Transactions on Information Forensics and Security*, *4(3)*, 383-396.

[5] Chang, C. C., Tai, W. L., & Lin, C. C. (2005). Hiding a secret color image in two color images. *Image Science Journal*, *53(4)*, 229-240.

[6] Wang, D. S., Yi, F., & Li, X. B. (2009). On general construction for extended visual cryptography schemes. *Pattern Recognition, 42(11)*, 3071-3082.

[7] Yang, C. N. (2004). New visual secret sharing schemes using probabilistic method. *Pattern Recognition Letters*, *25(4)*, 481-494.

[8] Wang, D. S., Yi, F., & Li, X. B. (2011). Probabilistic visual secret sharing schemes for grey-scale images and color images. *Information Sciences*, *181(11)*, 2189-2208.

[9] Ito, R., Kuwakado, H., & Tanaka, H. (1999). Image size invariant visual cryptography. *IEICE Trans. Fundam*, *E82-A(10)*, 2172–2177.

[10] Cimato, S., Prisco, R. D., & Santis, A. D. (2006). Probabilistic visual cryptography schemes. *The Computer Journal*, *49(1)*, 97-107.

[11] Chen, T. H., & Tsao, K. H. (2011). User-friendly random-grid-based visual secret sharing. *IEEE Transactions on Circuits and Systems for Video logy*, *21(11)*, 1693-1703.

[12] Guo, T., Liu, F., & Wu. C. K. (2014). *k* out of *k* extended visual cryptography scheme by random grids. *Signal Processing*, *94*, 90-101.

[13] Chiu, P. L., Lee, K. H., Peng, K. W., *et al.* (2013). User-friendly visual cryptography with complementary cover images. *Proceedings of 2013 IEEE China Summit& International Conference on Signal and Information Processing* (pp. 641-644).

[14] Tuyls, P., Hollmann, H. D. L., & Van Lint, J. H. (2005). XOR-based visual cryptography schemes. *Designs, Codes and Cryptography*, *37(1)*, 169-186.

[15] Wang, D. S., Zhang, L., Ma, N., *et al.* (2007). Two secret sharing schemes based on Boolean operations. *Pattern Recognition*, *40(10)*, 2776-2785.

[16] Wang D. S., & Yi, F. (2010). On converting secret sharing scheme to visual secret sharing scheme. *EURASIP Journal on Advances in Signal Processing*, 1-11.

[17] Liu, F., Wu, C. K., & Lin, X. J. (2010). Some extensions on threshold visual cryptography schemes. *The Computer Journal*, *53(1)*, 107-119.

[18] Yang, C. N., & Wang, D. S. (2014). Property analysis of *XOR* based visual cryptography. *IEEE Transactions on Circuits and Systems for Video Technology*, *24(2)*.

[19] Viet, D. Q., & Kurosawa, K. (2004). Almost ideal contrast visual cryptography with reversing. *Topics in Cryptology–CT-RSA 2004* (pp. 353-365).

[20] Cimato, S., Santis, D. A., Ferrara, A. L., *et al.* (2005). Ideal contrast visual cryptography schemes with reversing. *Information Processing Letters*, *93(4)*, 199-206.

Wanli Dang was born in Shanxi Province, China, in 1990. She received the B.S. degree from the Department of Mathematics at Xianyang Normal University, China, in 2012. She is currently a M.S. candidate at the School of Mathematics and Computer Engineering, Xihua University, China. Her current research interests conclude cryptography and applied mathematics.

Mingxing He received the M.S. degree from Chongqing University and the Ph.D. degree from Southwest Jiaotong University, China, in 1990 and 2003, respectively. He is a member of the IEEE and ACM, a senior member of CAAC. He is currently a professor and the director of the Key Lab of Cyberspace Security Insurance of Sichuan, Xihua University. He has published over 80 research papers in refereed journals and conferences. He has been a reviewer for several international academic journals. His research interests include information security and cryptography.

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

Xiao Li was born in Sichuan province, China, in 1972. He received the M.S. degree from Xihua University in 2005. He is an associate professor and a graduate students supervisor of Xihua University. He has published over 10 research papers in refereed journals and conferences. His current research interests include information security and cryptography.