Secret color images sharing schemes based on XOR operation

Wang Dao-Shun*, Zhang Lei, Ma Ning and Huang Lian-Sheng

Department of Computer Science and Technology, Tsinghua University, Beijing, 100084, China

Abstract

This paper presents two new constructions for the secret color images sharing schemes .One is a (n, n) threshold scheme, which can be constructed based on XOR operation. The other is a (2, n) threshold scheme, which can be constructed by using AND and XOR operations. The two schemes have no pixel expansion, and the time complexity for constructing shared images is $O(k_1 n)$, excluding the time needed for generating n distinct random matrices (here k_1 is the size of the shared image). The reconstructed images can be obtained in the two schemes by using the XOR operation alone. The relative differences of the two schemes are 1 and 1/2, respectively. The time complexity of the recovered images is $O(k_1 n)$ and $O(2k_1)$, respectively. The two schemes also provide perfect secrecy.

Keywords: Secret sharing scheme; Visual cryptography; Visual secret sharing scheme; XOR operation; Perfect secrecy

1. Introduction

After Blakely and Shamir independently proposed the (k, n) threshold scheme [1-2], hundreds of papers were published reporting research about this topic. However, these schemes are only suitable for digital data such as text files, passwords, and encryption /

* Corresponding author. Tel.: +86-10-62782930

E-mail address: daoshun@mail.tsinghua.edu.cn

decryption keys [3]. Compared with digital data such as passwords and text files, digital images have a large amount of datum, and the difference between two neighboring datum is very small. Because of the features of digital images, it is impractical to apply the traditional threshold scheme to share a secret digital image directly, so it is very important and necessary to investigate (k, n) threshold schemes of digital images. In [3], the Chang and Hwang proposed the first specific (k, n) threshold scheme based on vector quantization for secret digital images by using modular arithmetic instead of real arithmetic according to Shamir's ideas. Thien and Lin [4] presented a (k, n) threshold scheme proposed by Shamir's (k, n) threshold scheme directly. In [5], Wu, Thien and Lin presented a method to implement sharing and hiding secret images into ordinary images by slightly modifying [4]'s scheme. The advantage of the schemes proposed to date for sharing a secret digital image by modifying Shamir's method is that there is no data expansion and the relative difference is approximately 1. The algorithmic complexity of the recovery image in [3-5] is equal to the one in Shamir's scheme. Generally, the security of information transfer is obtained by processing the data with encryptions and decryptions using modern cryptography technology. The problem is, however, that the computation needed to recover the data is complex and takes much time causing low efficiency. Under this situation, researchers have focused on developing a security system that can recover the original data with a comparatively low computation complexity and without any special tools.

In 1994, Naor and Shamir [6] firstly introduced their theory of visual cryptography to solve this problem. Visual cryptography conceals the original data in a shared image; the original data can be recovered from the overlap of several modified images using the contrast abilities of human vision. In a (k, n) visual cryptography scheme, the shared secret image becomes visible by overlaying and aligning any k of the n transparencies on an overhead projector. However, if there are less than k shares, none of the information of

the shared secret image can be revealed. The reconstruction can be performed by the human visual system without any knowledge of cryptography or cryptographic computations. After Naor and Shamir's proposal in [6], some results can be found based on the (n, n) visual threshold schemes in [6-10,11]. The different construction methods have been proposed for (2, n) visual cryptography schemes in [6-8,11-13].

The color visual cryptography scheme is another interesting research topic, through which the user can share a color secret image. Many studies have researched the (n, n) color visual cryptography schemes [10,14-26]. Some results of the (2, n) visual cryptography schemes for color images can be obtained in [14-19, 21,22,26,27].

The reconstructed secret image in visual cryptography only requires the very simple OR computation, while the conventional cryptographic system requires more complex computation. The cost of the recovering the image by using the human visual system in visual cryptography is pixel expansion and loss of contrast. In (k, n) colored visual cryptography schemes, it is impractical to use transparency stacking and aligning by using human vision to reconstruct secret digital images directly when $k, n \geq 3$. In practical application, tools such as projectors and imaging software are used to reconstruct secret images. In this case, we sought to design a new technique for image cryptography with easy encryption and decryption, lower computation complexity, smaller or even no pixel expansion and better contrast. Most importantly, the recovery of the original data must be easy and convenient to accomplish with common tools, such as Photoshop software. The XOR operation is an elemental computer operation. It is swift, simple, and very adaptive to apply to an image cryptography system. The image sharing schemes presented in this paper are based on this operation, and have the benefits of simple arithmetic operation, better contrast than the current schemes and, most importantly, no pixel expansion.

The paper is organized as follows. In section 2, we give a brief review of visual cryptography. In section 3, we present the construction of a new colored (n, n) threshold

scheme. In section 4, we give a colored (2, n) threshold scheme. We discuss the computation complexity and security analysis in section 5. In section 6, we compare the results between our schemes and previous visual cryptography schemes for (n, n) threshold schemes and (2, n) threshold schemes. Finally, the experimental results and conclusion are given in section 7.

2. Review of visual cryptography scheme

Here, we briefly review Naor and Shamir's visual cryptograph scheme [6]. In this scheme, the secret image consists of a collection of black and white pixels and each pixel is subdivided into a collection of m black and white sub-pixels in each of the n shares. Each share is a collection of m black and white sub-pixels, which are printed in close proximity to each other so that the human visual system averages their individual black and white contributions. The collection of sub-pixels can be represented by a $n \times m$ Boolean matrix $S=[s_{ij}]$, where element s_{ij} represents the j-th sub-pixel in the i-th share. A white sub-pixel is represented as a 0, and a black sub-pixel is represented as a 1. $s_{ij}=1$ IFF the j-th sub-pixel in the i-th share is black. The gray level of this combined share is proportional to the Hamming weight $H(V)$ of the "or" for the m-vector V. This gray level is interpreted as black by the user's visual system if $H(V) \geq d$, and as white if $H(V) < d - \alpha.m$ for some fixed threshold $1 \leq d \leq m$ and relative difference $\alpha > 0$. The following definition is the formal definition for black and white visual cryptography schemes given in [6].

Definition 1 [6]: A solution to the k out of n visual secret sharing scheme consists of two collections of $n \times m$ Boolean matrices C_0 and C_1. To share a white pixel, the dealer randomly chooses one of the matrices in C_0, and to share a black pixel, the dealer randomly chooses one of the matrices in C_1. The chosen matrix defines the color of the m

sub-pixels in each one of the n transparencies. The solution is considered valid if the following three conditions are met.

1. For any $S \in C_0$, the OR m-vector V of any k of the n rows in S satisfies $H(V) < d - \alpha.m$.

2. For any $S \in C_1$, the OR m-vector V of any k of the n rows in S satisfies $H(V) \geq d$.

3. For any subset $\{i_1, ..., i_q\}$ of $\{1,\ldots,n\}$ with $q<k$, the two collections of $q \times m$ matrices D_t for $t \in \{0,1\}$ obtained by restricting each $n \times m$ matrix in C_t (where t=0,1) to rows $i_1,...,i_q$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

For a visual secret sharing scheme to be valid, these three conditions must be met. The first two conditions of this definition ensure that some contrast is kept and the third condition ensures that security is maintained.

In this definition parameter m is called the pixel expansion, which refers to the number of sub-pixels in a share required to represent a single pixel in the original image. The pixel expansion represents the loss in resolution from the original image to the shared one and can make the share transparencies difficult to align. Therefore, it is desirable to minimize pixel expansion as much as possible.

The difference between the gray levels of black and white pixels is called the contrast. The relative contrast difference α refers to the difference in contrast between the original image and the recovered image. This represents the loss in contrast. It is desirable to have a relative contrast difference as large as possible to minimize the loss of contrast in the recovered image. So the contrast can be measured by the relative difference.

For an intuitive justification, consider the contrast of two adjacent buildings A and B at night, formed by the number of illuminated windows. The contrast formed by 100 illuminated windows in A and 99 in B, is much less than with 1 illuminated window in A and 0 in B. Because of this fact, Verheul and Van Tilborg point out in [10] that this

concept of contrast is not really suitable. The general relative contrast for black and white visual cryptography scehme is also defined in [10]. According to the definition in [10], we consider the relative contrast difference in [6] as the maximal relative contrast difference in [10]. We also note that the contrast in [11] is equal to the relative difference.

In color visual cryptography schemes, the brightness of the reproduced image can be evaluated by the color ratio, which was first defined in [22]. Adhikari and Sikdar in [27] gave a simple definition of this color ratio:

The color ratio =

$$number\ of\ subpixels\ that\ possess\ the\ true\ color \Big/ the\ total\ number\ of\ subpixels$$

We use the symbol α^* to represent the color ratio.

The two factors that determine the quality of the recovered image are the pixel expansion and the relative contrast difference. We shall now consider a scheme in which the recovered image has no loss of contrast, while the relative contrast difference or color ratio is equal to 1, as described below.

3. The construction method for our (*n*, *n*) color secret sharing scheme

Our scheme supports the RGB model. Red, green and blue are the primary color components of the RGB color space. All the other desired colors can be obtained by using additive color mixing of different RGB components. CRT and LCD displays are examples of the RGB color mixing generation. An RGB color is equal to a set of three intensity values, one for each primary color. This RGB color may be reproduced by mixing the red, green and blue components set to these intensity values. We defined an RGB color palette as a set of RGB colors. The intensity of a primary color can be defined as the gray level in the gray-scale palette. A primary color will have an intensity range between 0 and 1, with 0 representing black and 1 representing the maximum possible intensity of that color. The RGB color palette is created from three gray-scale palettes,

which represent the intensity palettes for red, green and blue. Combining the members in the gray- scale palettes in all possible ways creates the color palette.

In a real color system, R, G, and B are each represented by 8 bits, and therefore each single color based on R, G, and B can represent 0-255 variations of scale. When RGB is used to represent a color pixel, (0,0,0) represents full black and (255,255,255) represents the maximum possible intensity of that color viz. full white.

We use the symbols "$\oplus$" and "&" to represent the XOR and AND operations of two number bits with 0 and 1, respectively. It is well known that associative law and commutative law hold with respect to $\oplus$ and &.

The $\oplus$ and & operations are defined as follows:

$0 \oplus 0=0, 1 \oplus 0 = 0 \oplus 1 = 1$ and $1 \oplus 1=0$.

$0 \,\&\, 0=0, 1 \,\&\, 0 = 0 \,\&\, 1 = 0$ and $1 \,\&\, 1 =1$.

Special symbols are used in this paper for convenience, and we provide the definitions as needed. Now assume that 0,1…,*c* are the set of all colors appearing in an original image; here $c \geq 2$ is the maximum color value of a color images.

$$A = [a_{ij}]_{m\times n}, \text{ where } a_{ij} \in \{0,\cdots,c-1\},\ (i = 1,2,\cdots,m; j = 1,\cdots,n) \quad (1)$$

The definitions are specified as followings:

Definition 2.Performing the XOR and AND operation on matrix *A* and matrix *B* is to perform the XOR operation and AND operation entries of matrix *A* and matrix *B* in the same position.

Namely, the XOR operation and AND operation of matrices can be described by the formula:

$\forall\ a_{ij} \in A,\ b_{ij} \in B,$

$$C = A \oplus B = [a_{ij} \oplus b_{ij}]\ (i = 1,2,\cdots,m; j = 1,\cdots,n)$$

$$D = A \,\&\, B = [a_{ij} \,\&\, b_{ij}]\ (i = 1,2,\cdots,m; j = 1,\cdots,n).$$

The expression $C = A \oplus B$ means that the *ij*-th element c_{ij} of matrix C is equal to $a_{ij} \oplus b_{ij}$, where a_{ij} and b_{ij} are the *ij*-th elements of matrix A and matrix B, respectively. The expression $D = A \& B$ means that the *ij*-th element d_{ij} of matrix D is equal to $a_{ij} \& b_{ij}$, where a_{ij} and b_{ij} are the *ij*-th elements of matrix A and matrix B, respectively.

To express the model conveniently, several assumptions were made, as follows:

Assumption 1. The pixel matrix of secret image A is equal to secret image A.

Assumption 2. The matrix of a secret image is $m \times n$, $A_{i1}, \cdots, A_{in}$ are used to denote *n* distinct matrices of $A_1, \cdots, A_n$ ($n \geq 2$) for convenience.

Theorem 1. If $n \geq 2$, then there must be *n* distinct matrices $A_1, \cdots, A_n$ satisfying the following conditions:

1. $\bigcup_{j=1}^{n-1} \left(\oplus A_{ij} \right) \neq A$, it means the XOR of any *n*-1 matrices cannot be used to obtain any information of matrix *A*.
2. $\bigcup_{j=1}^{n} \left(\oplus A_{ij} \right) = A$, it indicates that only the XOR of *n* matrices can be used to recover information form matrix *A*.

Proof. Using the following method of constructing we can get *n* different special matrices $A_1, \cdots, A_n$

$$A_1 = B_1$$

$$A_2 = B_1 \oplus B_2$$

……

$$A_{n-1} = B_{n-2} \oplus B_{n-1}$$

$$A_n = B_{n-1} \oplus A$$

$$B_j = [b_{ij}]_{m \times n}, b_{ij} \in \{0, \cdots, c-1\}, (j = 1, \cdots n-1)$$

This algorithm indicates that B_j (j=1,…,n-1) is the random matrix, which satisfies the above conditions.

It also shows that the n matrices above satisfy the following conditions:

a. $A_i \neq A_j (i \neq j)$

Proof. $B_i \oplus B_j$ is a random matrix, while B_j (i, j=1,…,n-1) is a random matrix.

$B_j \oplus A$ (constant matrix) is also a random matrix

A_i (i=1,…,n-1) is obviously a random matrix, from which we can get $A_i \neq A_j$

b. This algorithm satisfies condition case 1 of theorem 1.

That is, no information of matrix A could be obtained by the XOR operation for any n-1 matrices.

Proof. (in the two cases):

Case 1. excluding A_n

$A_1 \oplus A_2 \oplus \cdots \oplus A_{n-1} = B_{n-1}$, it *is a* random matrix.

Case 2. including A_n:

Suppose A_{im} excludes ($im \in \{1, \cdots, n-1\}$)

$$A_n \oplus \sum_{ij=1}^{n-2} (\oplus A_{ij}) = B_{im-1} \oplus B_{im} \oplus A = A_k ; k \in \{1, \cdots, n-1\}$$

It is then not difficult to prove that A_k is also a random matrix.

c. This algorithm satisfies the condition for case 2 of theorem 1.

Obviously, $\sum_{i=1}^{n-1} (A_n \oplus A_i) = A$.

The theorem therefore is proved.

From the proof of the theorem above, we have:

Corollary 1. If $m \times n$ matrices $A_1, \cdots, A_n$ satisfy theorem 1, the *n* distinct matrices can be used to construct a (*n*, *n*) threshold scheme, the relative contrast difference is 1, and the pixel expansion is 0.

4. (2, *n*) threshold scheme for color images

We shall now give the method for constructing the 2 out of n threshold scheme.

Using $B_1, B_2, \cdots, B_{n+1}$ to denote $n+1$ distinct random matrices ($n \geq 1$), for convenience, suppose that matrix $A_i \ (i = 1, \cdots, n)$ has *n* matrices.

We give two special operations using $B_1, B_2, \cdots, B_{n+1}$ and the original matrix A.

$$C_i = B_i \,\&\, A, \ A_i = B_{n+1} \oplus C_i \quad (i = 1, \cdots, n) \qquad (2)$$

We shall obtain the next theorem by using formula (2)

Theorem 2. The *n* matrices above $A_1, A_2, \cdots, A_n$ can be used to construct a (2, *n*) color threshold scheme, in which the relative difference is ½, and there is no pixel expansion.

Proof. It is easy to verify that the *n* matrices $A_1, A_2, \cdots, A_n$ are *n* distinct random matrices from formula (2); each $A_i \ (i = 1, \cdots, n)$ does not contain any information of the original matrix A.

Two matrices A_i and A_j are randomly chosen from *n* matrices $A_1, A_2, \cdots, A_n$; then we have:

$$A_i \oplus A_j = B_{n+1} \oplus C_i \oplus B_{n+1} \oplus C_j = C_i \oplus C_j, i \neq j \qquad (3)$$

We can then reconstruct the original matrix A by using formula (3).

Suppose R_i is a random number. Here $R_i \in [0,1]$, i=0,1,2…

Let $F_A(i, j)$ denote the *ij*-th entry of matrix A. We define:

$$F_{A_i}(i, j) = F_{B_i}(i, j) \,\&\, F_A(i, j) \qquad (4)$$

Formula (4) represents that the *ij*-th element of matrix A_i is equal to the *ij*-th element of matrix B_i 'AND' the *ij*-th element of matrix A at the same position.

Now we discuss formula (4) according to the color value of the original image A.

Case 1. c=2, namely a binary image,

If $F_A(i,j)=0$, thus:

$$F_{Ai}(i,j)=F_{Bi}(i,j)\ \&\ 0=0,$$

$$F_{Ai}(i,j)\oplus F_{Aj}(i,j)=0\oplus 0=0;$$

If $F_A(i,j)=1$, thus:

$$F_{Ai}(i,j)=F_{Bi}(i,j)\ \&\ 1=R_i,$$

$$F_{Ai}(i,j)\oplus F_{Aj}(i,j)=R_i\oplus R_j.$$

From the above:

If $a_{ij}=0\in A$, thus:

$$b_{ij}\oplus c_{ij}=0,\forall\ b_{ij}\in A_i,\ c_{ij}\in A_j;$$

If $a_{ij}=1\in A$, thus:

$$b_{ij}\oplus c_{ij}=R_i,\ \forall\ b_{ij}\in A_i,\ c_{ij}\in A_j.$$

It is clear that the relative contrast is equal to1/2, namely α=1/2.

Case 2. c>2,

Suppose $F_A(i,j)=(\mathrm{a_n a_{n-1}\ldots a_1})_2$, $a_i\in[0,1]$, and $F_{C_i}(i,j)=(\mathrm{b_n b_{n-1}\ldots b_1})_2$, $b_i\in[0,1]$.

From formula（2），we have:

$$b_i=\begin{cases}0 & a_i=0\\ R_0 & a_i=1\end{cases}$$

$$F_{Ai}(i,j)\oplus F_{Aj}(i,j)=F_{Ci}(i,j)\oplus F_{Cj}(i,j)$$

Since the relative contrast of any bit of the reconstructed image is 1/2 from case 1, then the relative contrast of the recovered image can be obtained by the following:

Because $(a_n a_{n-1} \ldots a_1)_2 = \sum (a_i * 2^i)$, $\alpha(\sum (1/2(a_i * 2^i)) = (1/2)\alpha(\sum (a_i * 2^i)$.

The relative contrast of the reconstructed image is 1/2, namely, α =1/2.

Without loss of generality, if the color value of the original image is C_1, the color value of the shared images must be C_2. In this case, we can construct a (2, *n*) threshold scheme for the color images according to the method above. In this scheme the relative contrast is $C_2/2C_1$.

5. Computation complexity and security analysis comparison with results of reported secret image sharing schemes

5.1 Computation complexity

The algorithmic complexity in [1] is $O(n \log^2 n)$ for polynomial evaluation and interpolation. The algorithmic complexity of the setup phase is equal to $m \times n \lfloor (k-1)/2 \rfloor + 2$ module multiplications plus $m \times n(k-1)$ module additions, where $m \times n$ is the size of the codebook, excluding the time needed for generating the codebook. One recovery phase is equal to $O(k \log^2 k)$ in [3]. Thien et al. use Shamir's (*k*, *n*) threshold scheme directly in [4-5]. The algorithmic complexity in [4-5] is the same as one of Shamir's.

We shall now discuss the algorithmic complexity of our two schemes. We used two steps to construct our two schemes.

First, we determined the time needed to obtain *n* different matrices according to random matrix generation.

Secondly, we spent $O(k_1 n)$ to construct our (*n*, *n*) threshold scheme and (*2*, *n*) threshold scheme, where k_1 is equal to $m \times n$.

Now we shall show the algorithmic complexity of reconstructing the secret image in our two schemes.

Reconstructing the image takes $O(k_1 n)$ in the (n, n) threshold scheme and $O(2k_1)$ in the (2, n) threshold scheme.

Thus, compared with other reported secret image sharing schemes with (n, n) threshold scheme, the algorithmic complexity of our schemes is more efficient.

5.2 Security analysis

In the proposed secret sharing image schemes, visual cryptography schemes have perfect security. The scheme in [3] has perfect security. In [4], the (k, n) threshold scheme can generate the k-1 degree polynomial by using the k coefficients as the gray value of k pixels. Therefore, shares are often only $1/k$ of the secret image in size. The major difference between this scheme and Shamir's is that no random coefficient is used. Although the scheme does not guarantee perfect secrecy, the property that the size of each shared image is smaller than the secret image gives the benefit of the possibility of further processing of the shared images, such as storage, transmission, or image hiding. The scheme in [4-5] has weak security.

From corollary 1 and theorem 2, we know that the security in our two schemes consists of two factors: one is the security of the random matrices, and the other is the security of the two schemes themselves. We shall now discuss the security of random matrices.

Since we won't be generating a truly random number, we will refer to pseudo- random number generators, or pRNG. In contrast to linear congruential generators, linear feedback shift registers, and other related non-secure pRNGs, the BBS generator is provably secure, assuming that it is hard to factor large number into prime number (see [28]: pp337, [29]). The Naor – Reingold pseudo-random number generator in [30] (also see [28]: pp338), is relatively new. As with the BBS algorithm, of which it is something of a descendant, it is demonstrably secure assuming the infeasibility of factoring integers $n = p.q$, while p and q are sufficiently large primes (both probably congruent to 3 mod 4).

From the pseudo-random number generators above, the n distinct random matrices are secure when the BBS generator or Naor-Reingold pseudo-random number generator are used.

In our (n, n) threshold scheme, by performing XOR operations on n of the shares, the secret image can be recovered, but performing XOR operations on less than n of them will not reveal any information about the secret image from theorem 1 in section 2.

In our (2, n) threshold scheme, through any 2 of n shares we can obtain the original secret image by performing the XOR operation, but any one of them will not reveal any information.

6. The pixel expansion and relative contrast difference results compared with the visual cryptography scheme

6.1 (n, n) visual cryptography scheme for black and white images

In the visual cryptography scheme for black and white images, Naor and Shamir first introduced an optimal (n, n) threshold scheme for black and white images in [6]. The same result for a (n, n) visual cryptography scheme can be found in [7-8,10,11]:

$m = 2^{n-1}$, $\alpha = 1/2^{n-1}$.

Alteniese et al. in [9] proposed a (n, n) threshold extended visual cryptography scheme that is optimal with respect to the pixel expansion.

$$m \geq 2^{n-1} + 2$$

6.2 (n, n) visual cryptography scheme for color images

We reviewed the (n, n) color visual cryptography schemes in [16-20,23]. The results in [18,19] are optimal in regard to pixel expansion.

The minimum pixel expansion (see [19]):

$$m \geq \begin{cases} c.2^{n-1} - 1, & if\ n\ is\ even \\ c.2^{n-1} - c + 1, & if\ n\ is\ odd \end{cases}$$

The optimal contrast of a c-color (n, n) threshold scheme (see [19]):

$$\alpha_{opt} = \begin{cases} 1/(c.2^{n-1} - 1), & if\ n\ is\ even \\ 1/(c.2^{n-1} - c + 1), & if\ n\ is\ odd \end{cases}$$

The minimum difference is obtained for any (n, n) gray level image visual cryptography in [20,24].

The minimum pixel expansion m is given by

$m \geq (g-1).2^{n-1}$, where the image has g gray levels ranging from 0 (representing a white pixel) to g -1 (representing a black pixel).

The minimum relative difference:

$$\alpha \leq 1/((g-1).2^{n-1})$$

The results in [18-20,24] have the same pixel expansion and relative difference although different construction methods are used, if we ignore the difference of color value between color images and gray level images.

According to corollary 1 in our schemes, the relative difference is 1, and there is no pixel expansion in our scheme. Our scheme has relative difference α =1 and pixel expansion m =0, which is the best possibility compared to the schemes proposed in [16-20,23], ignoring the processing operation of the reconstructed image.

6.3 (2, n) visual cryptography scheme for black and white images

Many studies have researched the (*2*, *n*) visual cryptography; for example, different results can be found in [6,7,8, 10-13]. We shall now list some typical results with regard to pixel expansion and relative difference.

The construction of the 2 out of n visual cryptography scheme for a general access structure has the best result with respect to pixel expansion and relative difference in [7,8,12,13].

The minimum pixel expansion:

$$m = \binom{n}{\lfloor n/2 \rfloor}$$

The optimal contrast[7,8,11-13]:

$$\alpha \le (\lfloor n/2 \rfloor \lceil n/2 \rceil)/((n-1)n)$$

In [11], if a balanced (*2*, *n*) visual cryptography scheme had $\alpha \ge 1/4$, the pixel expansion was at least $\lfloor (n+1)/2 \rfloor$. For any fixed α <1/4, there is a balanced (*2*, *n*) scheme with $m = O(\log n)$ sub-pixels and a contrast of at least α .

6.4 (*2*, *n*) *visual cryptography schemes for color images*

In [14], Rijmen and Preneel gave the optimal (2,2)–visual cryptography scheme for color images. The optimal relative difference is 1 in [14,15], and the pixel expansion is 4.

Adhikari and Sikdar presented a new scheme for (*2*, *n*) visual cryptography for color images in which the secret image has colors such that no two colors can be combined to produce a third color [27].

Comparing the (*2*, *n*) visual cryptography schemes proposed for color images in [10,16,17, 21,22,26,27], the result in [27] has a better color ratio than the schemes proposed in [21,22].

The color ratio in [27]:

$$1/(2c) + (\lfloor n/2 \rfloor \lceil n/2 \rceil)/(n(n-1).c)$$

The pixel expansion:

$$2.\binom{n}{\lfloor n/2 \rfloor}.c$$

In our $(2, n)$ threshold scheme, the relative difference is 1/2, and there is no pixel expansion.

Table 1 and Table 2, see the appendix, show optimal results of (*2*, *n*) and (*n*, *n*) visual cryptography with pixel expansion and relative difference. Table 3, see the appendix,

illustrates that our proposed (*2*, *n*) and (*n*, *n*) secret color image sharing scheme have optimal contrast difference and no pixel expansion in comparison to the previous results, if we do not consider whether the processing operation of reconstructed image is OR operation or XOR operation.

7. Experimental results and conclusion

In this section, we present some experimental results to illustrate our two threshold schemes and conclude our paper.

7.1 Experimental result

We used two examples to test our schemes: a (3,3)–threshold scheme was used for the (*n*, *n*)–threshold scheme, and a (2,3)–threshold scheme was used for the (*2*, *n*) threshold scheme. Example 1, see the appendix, is the (3,3)–threshold scheme based on the XOR operation (Fig.1).

Fig.1 (a) displays the secret image Lena, and Figs.1 (b)-(d) display the three-shared images. Notably, the size of the secret image and shared images are 128×128 pixels with 256 colors. The secret image can be reconstructed by collecting the three-shared images and using on XOR operation at the same position. Fig. (e) shows the recovered secret image, which has no loss of contrast.

Example 2, see the appendix, is shown in Fig.2. Based on the (2,3)-threshold scheme: (a) is the secret image with a color value of 128×128 size with 256 colors; (b)-(d) are the three shadow images shared by using the above proposed scheme, while *n*=3. Each of the three shares has the same size as image a. The image can be recovered from any two of these images with a relative contrast of 1/2. The results can be seen in Fig. e, Fig. f and Fig. g.

7.2 Conclusion

This paper presented methods for constructing a (n, n) threshold scheme and a (2, n) threshold scheme. The constructing and reconstructing of the (n, n) threshold scheme adopt only the XOR operation, and the quality of the recovered image is equal to that of the original image. We used the AND and the XOR operations to construct a (2, n) threshold scheme, in which the recovered secret image can be performed only by using the XOR operation. Compared with the results from (2, n) visual cryptography schemes, the advantages of our schemes are: There is no pixel expansion; the contrast of the recovered image is 1/2; common tools, such as Photoshop software, can easily be used to reconstruct the secret image. The algorithmic complexity of our schemes is lower than that of the previously proposed secret image sharing schemes. Moreover, our schemes also provide perfect security. Problems to be addressed in further study include: extending this scheme to the (k, n) threshold scheme based on XOR operations with no pixel expansion and no loss of quality.

Acknowledgements

This research was supported by the National Science Fund of the People's Republic of China under Grant No. 90304014.

References

[1] G.R.Blakley, Safeguarding cryptography keys, Proceedings AFIPS 1979 National Computer Conference, Vol.48, New York, USA,1979, pp.313-317.

[2] A.Shamir, How to share a secret, Communication of the Association for Computing Machinery 22(11) (1979) 612-613.

[3] C.C.Chang, R.J. Hwang, Sharing secret images using shadow codebooks, Information Sciences 111 (1998) 335-345.

[4] C.C.Thien, J.C.Lin, Secret image sharing, Computer & Graphics 26 (2002) 765-770.

[5] Y.S.Wu, C.C. Thien, J.C.Lin, sharing and hiding secret images with size constraint, Pattern Recognition 37 (2004) 1377-1385.

[6] M.Naor, A.Shamir, in. A.De Santis (Ed.), Visual cryptography, Advances in Cryptology-EUROCRYPT'94, Lecture Notes in Computer Science,Vol. 950, Springer-Verlag, Berlin, 1995, pp. 1-12.

[7] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, in.F.M. auf der Heide and B. Monien (Eds.), Constructions and bounds for visual cryptography, 23rd International Colloquium on Automata, Languages and Programming (ICALP'96), Vol. 1099, Springer-Verlag, Berlin, Lecture Notes in Computer Science, 1996, pp.416-428.

[8] G.Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for general access structures, Information and Computation 129(2)(1996) 86-106.

[9] G. Alteniese, C.Blundo, A. De Santis, and D.R. Stinson, Extended capabilities for visual cryptography, Theoretical Computer Science 250(2001)143-161.

[10] E. R. Verheul, H. C. A. Van Tilborg, Constructions and properties of k out of n visual secret sharing schemes, Designs, Codes and Cryptography 11 (1997) 179-196.

[11] T. Hofmeister, M.Krause, H.U.Simon, Contrast-optimal k out of n secret sharing schemes in visual cryptography, Theoretical Computer Science 240 (2000)471-485.

[12] C.Blundo, A. De Santis, D.R.Stinson, On the contrast in visual cryptography schemes. Journal of Cryptology 12 (4) (1999) 261-289.

[13] A. Adhikari, M. Bose, A new visual cryptographic scheme using latin squares, IEICE Trans. Fundamentals E87-A(5) (2004) 1198- 1202.

[14] V. Rijmen,B. Preneel, Efficient colour visual encryption or 'Shared Colors of Benetton', Eurocrypto'96,Rump Session ,Berlin,1996. Available at http://www.iacr.org/conferences/ec96/rump/preneel.ps.

[15] C.N. Yang, A note on efficient color visual encryption, Journal of Information Sc ence and Engineering 18 (2002) 367-372.

[16] M.Naor, A.Shamir, Visual Cryptography II: Improving the contrast via the cover base, Security Protocols, Lecture Notes in Computer Science, Vol. 1189, Springer-Verlag, Berlin,1997, pp. 197-202.

[17] C.Blundo, A. De Bonis, and A.De Santis, Improved schemes for visual cryptography, Designs,Codes and Cryptography 24(2001) 255-278.

[18] C.N.Yang, C.S. Laih, New colored visual secret sharing schemes, Designs, Codes, and Cryptography 20 (2000) 325-335.

[19] S.Cimato, E.De Prisco, A.De Santis, Contrast optimal colored visual cryptography schemes, Information Theory Workshop, Proceedings 2003, 2003 IEEE, 2003, pp.139–142.

[20] C.Blundo, A.De Santis, M. Naor, Visual cryptography for grey level images, Information Processing Letters 75 (2000)255-259.

[21] H.Koga, H.Yamamoto, Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images, IEICE Trans. Fundamentals E81-A(6)1998 1262-1269.

[22] H.Koga, M.Iwamoto, H.Yamamoto, An analytic construction of the visual secret sharing scheme for color images, IEICE Trans. Fundamentals E84-A(1) (2001) 262-272.

[23] T.Ishihara, H.Koga, New constructions of the lattice-based visual secret sharing scheme using mixture of colors, IEICE Trans. Fundamentals E85-A(1)(2002)158-166.

[24] M.Iwamoto, H.Yamamoto, The optimal n -out of- n visual secret sharing scheme for gray-scale images, IEICE Trans. Fundamentals E85-A (10) (2002) 2238-2247.

[25]T. Ishihara, H. Koga, A visual secret sharing scheme for color images based on meanvalue-color mixing, IEICE Trans. Fundamentals E86-A(1)(2003)194-197.

[26] Y.C.Hou, Visual cryptography for color images, Pattern Recognition 36(7) (2003) 1619-1629.

[27] A. Adhikari, S. Sikdar, In. T. Johansson and S.Maitra (Eds.), A new (2, *n*)-visual threshold scheme for color images, INDOCRYPT 2003, Lecture Notes in Computer Science, Vol.2904, Springer-Verlag, Berlin, 2003, pp.148-161.

[28] Paul Garrett, Making, Breaking codes: An introduction to cryptology, Prentice-Hall, Inc., 2001.

[29] L.Blum, M.Blum, and M. Shub, A simple unpredictable random number generator, SIAM Journal on Computing 15(2) (1986) 364-383.

[30] M. Naor, O.Reingold, Synthesizers and their application to the parallel construction of pseudo-random functions, Proceedings of the IEEE 36th Annual Symposium on Foundations of Computer Science (1995), pp.170-181.

Appendix

Table 1. The optimal pixel expansion and optimal relative difference of (*2*, *n*) and (*n*, *n*) visual cryptography schemes for black-white images

	n	3	4	5	6	7	8	9
$(2,n)$	m	3	6	10	20	35	70	126
	α^*	1/3	1/3	3/10	3/10	2/7	2/7	5/18
(n,n)	m	4	8	16	32	64	128	256
	α	1/4	1/8	1/16	1/32	1/64	1/128	1/256

Table 2. The optimal pixel expansion and optimal color ratio or optimal relative difference of (*2*, *n*) and (*n*, *n*) visual cryptography schemes with 256 colors:

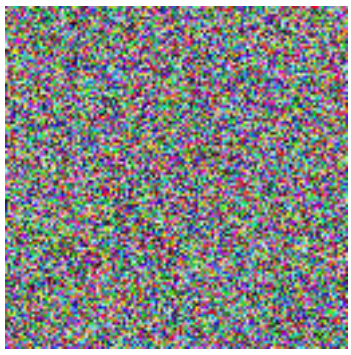
	n	3	4	5	6	7	8	9
$(2,n)$	m	1536	3072	5120	10240	17920	35840	64512
	α^*	5/1536	5/1536	1/320	1/320	11/3584	11/3584	7/2304
(n,n)	m	769	2047	3841	8191	16129	32767	65281
	α	1/769	1/2047	1/3841	1/8191	1/16129	1/32767	1/65281

Table 3. The pixel expansion and relative difference in our schemes with any color in our schemes:

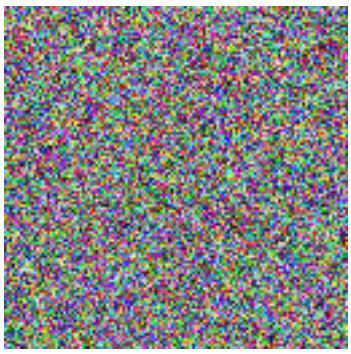
	n	with any n
$(2,n)$	m	0
	α^*	1/2
(n,n)	m	0
	α	1

Example 1:

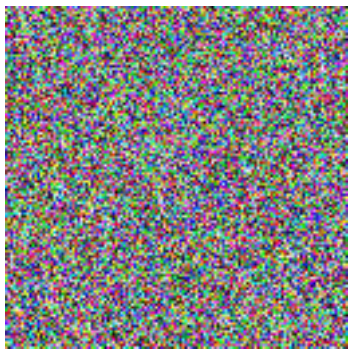
(a)



(b)



(c)



(d)

(e)

Fig.1 Experimental results:

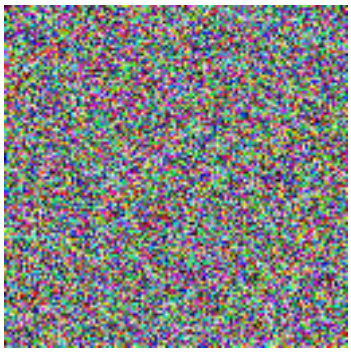
(a): A 128×128 secret image with 256 colors;

(b) - (d): Three shadow images with sizes the same as image a.

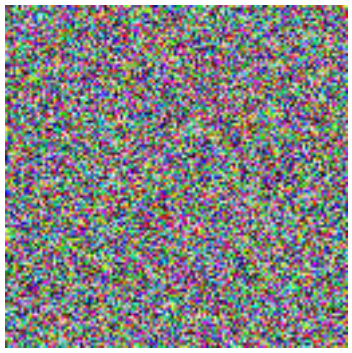
(e): Image recovered from the three shadow images.

Example 2:

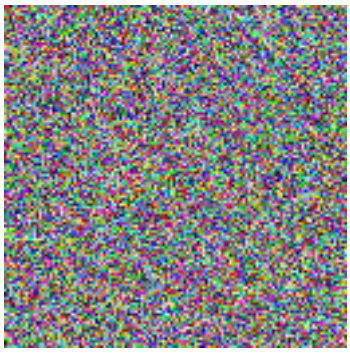
(a)



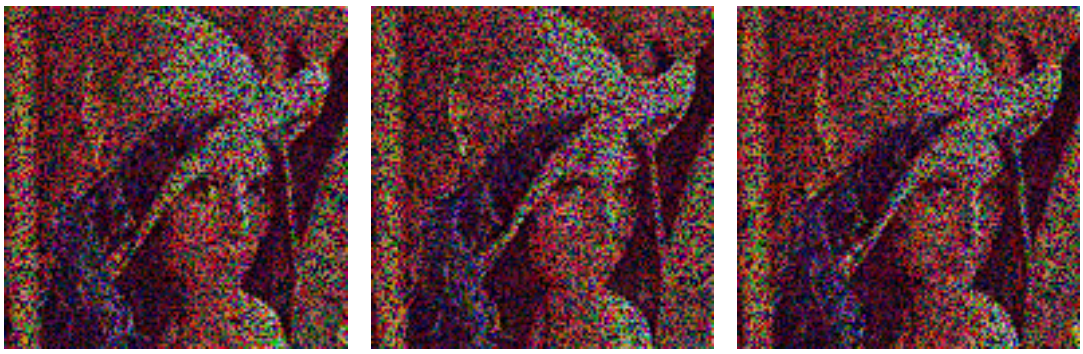
(b)



(c)



(d)



(e) (f) (g)

Fig.2 Experimental results:

(a): A 128×128 secret image with 256 colors;

(b)-(d): Three shadow images with sizes the same as image a.

(e)-(g): Image recovered from any two of the three shadow images.