Ideal Secure Multi-Secret Visual Cryptography Scheme with Ring Shares

Zheng-xin Fu and Bin Yu

Zhengzhou Information Science and Technology Institute, P.R. China, 450004
{fzx2515,byu2009}@163.com

Abstract. With visual cryptography in mind, the security property of a new scheme is always one of main concerns. However, the ideal security is not taken into account in some visual cryptography schemes sharing multiple secrets. In this paper, the security of a multi-secret visual cryptography scheme proposed by Feng et al. is analyzed. We show that the security of their scheme is not ideal. Precisely, it is insecure since some information of the secret images can be inferred by block attacking the second share alone. In order to realize the ideal security, we redesign the visual patterns and the rule of random permutation. Moreover, the proposed ideal secure scheme has better pixel expansion and relative difference. Finally, we give some experimental results and comparisons to show the effectiveness of the proposed scheme.

Keywords: Visual cryptography, Security, Multiple secret sharing, Ring share.

1 Introduction

Visual cryptography scheme (VCS) was introduced by Naor and Shamir in Eurocrypt'94 [1]. The difference between visual cryptography and the traditional secret sharing schemes [2,3] is the decryption process. Most secret sharing schemes are mainly realized by the computer, while visual cryptography schemes can decrypt secrets only with human eyes. Due to the ease of decoding, VCS provides some new and secure imaging applications, e.g., visual authentication, steganography, and image encryption. In recent years, the studies of VCS focus on the general access structure [4], the optimization of the pixel expansion and the relative difference [5-8], and the grey and color images [9-12], etc.

Most VCSs can only encrypt one secret image, which reduces the work efficiency and limits its possible applications. A so-called multi-secret VCS (MVCS) was then proposed to encrypt multiple secret images simultaneously. Chen et al. [13] designed (2, 2, 2)-MVCS to encode two secret images S_1 and S_2 into two square shares A and B. S_1 was decoded by stacking share A and B directly. S_2 could be decrypted by overlapping shares A and the rotated share B with 90°, 180°or 270°. In order to overcome the angle restriction, the shares were devised to be circles in literatures [14,15]. Although the rotation angles were unlimited, the shapes of decrypted images were distorted from square to circular and the recovery images had less contrast.

Y.Q. Shi (Ed.): Transactions on DHMS IX, LNCS 8363, pp. 42–56, 2014.

Different from the square and circle shares, Hsu et al. [16] proposed a scheme to hide two images in two ring shares with arbitrary rotating angles and undistorted shapes. Although there was no restriction of angles in Hsu's scheme, only two secret images could be encrypted. In order to share more secret images, Feng et al. [17] designed a new (2, 2, m)-MVCS with ring shares based on four different visual patterns. The scheme could share Y secret images at most, where Y was the width of the secret images. The pixel expansion of Feng's scheme was $3m$, where m denoted the number of secret images.

In the above schemes, one share is always used as a mask, while the other one is decided by the secret images and the mask. Therefore, the security of the secret images relies on the second share. Taking Feng's scheme for example, we analyze the relationship between the visual patterns which are the basic units of the shares. It is discovered that some information about the secret images can be inferred by computing the second share alone. This method is called block attacking. The weaknesses of (2, 2, 3)-MVCS and (2, 2, m)-MVCS are computed and discussed in detail, which threaten the schemes' security.

In order to realize the ideal security, two new visual patterns are designed instead of the previous four visual patterns. Based on the new visual patterns and the new rule of random permutations, the secret sharing algorithm is proposed with ideal security. Theoretical analysis and experimental results show the effectiveness of the proposed scheme.

The rest of this paper is organized as follows. Section 2 briefly reviews the scheme in literature [17]. Section 3 analyzes the security of the multi-secret visual cryptography scheme with ring shares. As the main part of this paper, Section 4 designs the multi-secret sharing and recovering procedures, and discusses the effectiveness of the scheme. The parameters analysis and experimental results would appear in Section 5. Section 6 concludes the paper.

2 Related Studies

To overcome the number restriction of secret images and the shape distortions, Feng et al. proposed a scheme to hide multiple secret images into two ring shares. Assume that the secret images S_1, S_2, $\cdots$, S_m are all sized $X \times Y$, where X is the height and Y is the width of images. Their scheme rolls up the shares to rings so that it is possible to recover many secrets at some setting angles as shown in Figure 1.

Since each row of the secret images is independent with others, the scheme encrypts one row at a time. The basic unit in shares is block, corresponding to one pixel of every secret image. Collect m blocks with interval $360°/m$ to form a set. Therefore, all shares blocks on a row can be separated to Y/m sets. $a_i^P(b_i^P)$ denotes the i-th block in the p-th set of a certain row in the share A (B), where $1 \leq i \leq m$ and $1 \leq p \leq Y/m$. The relationship between the blocks and the secret images is illustrated in Figure 2.

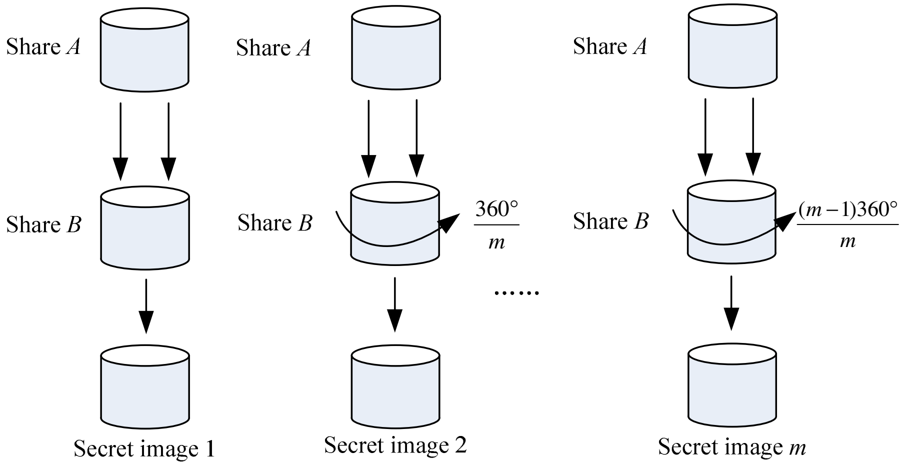

Fig. 1. The decryption model of Feng et al.'s scheme

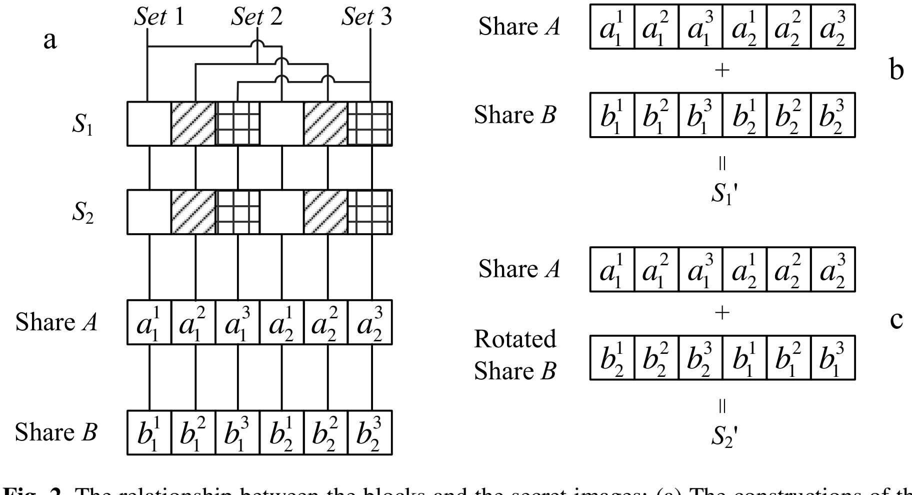
a
Set 1
Set 2
Set 3
S_1
S_2
Share A
a_1^1 a_1^2 a_1^3 a_2^1 a_2^2 a_2^3
Share B
b_1^1 b_1^2 b_1^3 b_2^1 b_2^2 b_2^3
b
Share A
a_1^1 a_1^2 a_1^3 a_2^1 a_2^2 a_2^3
+
Share B
b_1^1 b_1^2 b_1^3 b_2^1 b_2^2 b_2^3
||
S_1'
c
Share A
a_1^1 a_1^2 a_1^3 a_2^1 a_2^2 a_2^3
+
Rotated Share B
b_2^1 b_2^2 b_2^3 b_1^1 b_1^2 b_1^3
||
S_2'

Fig. 2. The relationship between the blocks and the secret images: (a) The constructions of the shares. (b) The recovery of S_1. (c) The recovery of S_2.

In the scheme, each share block is filled with m visual patterns. $a_{i,j}^{P}(b_{i,j}^{P})$ denotes the j-th pattern of $a_i^P(b_i^P)$. There are four visual patterns P_E={1,0,1}, P_I={1,1,0}, P_W={1,0,1}, and P_B={0,1,1}, which are used to produce some special features. The effective visual pattern P_E will reveal meaningful stacking results patterns P_W and P_B, while the ineffective pattern P_I will always cause black blocks. Table 1 shows the relations between the visual patterns.

Table 1. Necessary relations between visual patterns

Stacking operations	Block of results
$P_E + P_W = \{1,0,1\}$	White
$P_E + P_B = \{1,1,1\}$	Black
$P_I + P_W = \{1,1,1\}$	Black
$P_I + P_B = \{1,1,1\}$	Black

For the p-th process on the r-th row, $a_i^P(b_i^P)$ are generated according to the following equations, where $1 \le j \le m$.

$$a_{i,j}^{p} = \begin{cases} P_E & i = j \\ P_I & i \ne j \end{cases} \tag{1}$$

$$b_{i,j}^{p} = \begin{cases} P_W & S_{1+(i-j)\bmod m}\left(r, p+(j-1)Y/m\right) = 0 \\ P_B & else \end{cases} \tag{2}$$

The last part is using random permutation for every block to break up the regular pixel distribution. Then the pixel positions in a single share image are no longer related to the secrets. In other words, the security of the scheme is relied on the random permutation. Meanwhile, a_1^P, a_2^P, …, a_m^P and b_1^P, b_2^P, …, b_m^P are applied with the same random permutation, and therefore the secrets can still be decrypted by stacking the share images.

The complete encryption algorithm for (2, 2, m)-MVCS is as follows [16].

Input: Secret images S_1, S_2, … , S_m

Output: Two share A, B

Step1: Adjust the size of all secret images to $X \times Y$ that the X must be a multiple of m.

Step 2: Initialize the processing row $r = 1$ of the images.

Step 3: Start the p-th process of the proposed scheme with $p = 1$.

Step 4: Select the 1, m+1, 2m+1, $\cdots$, X–m+1 secret pixels to generate the blocks a_1^P, a_2^P, …, a_m^P and b_1^P, b_2^P, …, b_m^P according to Eqs. (1) and (2).

Step 5: Perform permutation on the generated blocks a_1^P, a_2^P, …, a_m^P and b_1^P, b_2^P, …, b_m^P.

Step 6: Fill the blocks in the share images. a_i^P is the block on the r-th row and $(p + X(i - 1)/m)$-th column of share A, and b_i^P is the block on the r-th row and $(p + X(i - 1)/m)$-th column of share B.

Step 7: If $p<X/m$, return to Step 4 for the next process $p := p+1$.

Step 8: If $r <Y$, return to Step 3 for the next row $r:=r+1$.

Step 9: Out put the two shares A and B.

3 Security Analysis of MVCS

The security of visual cryptography schemes is as same as “one time pad” [1]. The attackers can’t get any information on secret images from the forbidden set of participants. For the (2, 2, m)-MVCS, a single share should not leak any information on the m secret images. However, the scheme proposed by Feng et al. doesn’t satisfy the ideal security. The main reason is that share B leaks the correlation of the secret pixels.

3.1 Block Attacking

The basic units of share A are P_E and P_I, which are independent with the secret images. Therefore, Share A is just like a mask used for effecting and ineffecting the blocks of share B. The attackers can’t get anything information of secret images from share A. On the contrary, the basic units of share B are P_B and P_W, which are decided by the secret images. The weakness of share B will threaten the security of the visual cryptography scheme.

Firstly, the characteristics of P_B and P_W are analyzed. Since $P_W = \{1,0,1\}$ and $P_B = \{0,1,1\}$, we can get $P_W \oplus P_W = \{0,0,0\}$, $P_W \oplus P_B = \{1,1,0\}$, $P_B \oplus P_B = \{0,0,0\}$, where $\oplus$ is XOR operator. Obviously, the XOR result reflects whether the two blocks are same.

Next taking the random permutation into consideration, let P_i and P_j ($i, j \in \{B, W\}$) denote two patterns. P_i’ and P_j’ denote the same random permutation of P_i and P_j. $W(P)$ denotes the ‘1’s number of the pattern P. It is obvious that $W(P_i' \oplus P_j') = W(P_i \oplus P_j) = 0$ or 2.

Although we can not guess the color of the secret pixel encoded by P_i (P_j), the equality relation between P_i and P_j can be deduced. If $W(P_i' \oplus P_j')=0$, we can get $P_i \oplus P_j = \{0,0,0\}$, that means the secret pixels encoded by P_i and P_j are the same. Otherwise, if $W(P_i' \oplus P_j')=2$, we can get $P_i \oplus P_j = \{1,1,0\}$ or $\{1,0,1\}$ or $\{0,1,1\}$, that means the secret pixels are different.

Based on the relation between P_B and P_W, we can compute the different number in the m pixels encoded by b_i^P and b_j^P, which are consist of P_B and P_W.

The procedure of Block Attacking is as follows.

Input: $b_i'^p$ and $b_j'^p$, the i-th and j-th blocks in the p-set of the share B

Output: The correlation between the m secret pixels encoded in b_i^P and the m secret pixels encoded in b_j^P

Step1: Compute $b_i'^p \oplus b_j'^p$. $b_i'^p$ ($b_j'^p$) means the random permutation of block b_i^P (b_j^P), and the random permutations for b_i^P and b_j^P are the same.

Step2: Let d denotes the number of ‘1’ in $b_i^P \oplus b_j^P$. d is equal to the number of ‘1’ in $b_i'^p \oplus b_j'^p$.

Step3: According to characteristics of P_B and P_W, we can make sure that there are $d/2$ different pixels between the m secret pixels encoded in b_i^P and b_j^P.

Step4: Output $d/2$.

Although the attackers known nothing about the random permutation, they can get the correlations between the secret pixels. The results of the Block Attacking leak the information about the secret images.

3.2 Attacking to (2, 2, 3)-MVCS

In the section, a simple (2, 2, 3)-MVCS is analyzed firstly. Based on the Block Attacking, the security of general (2, 2, 3)-MVCS is discuss in detail.

Let S_1 = [0 1 1], S_2 = [1 0 0], and S_3 = [0 1 0], which are three secret images with X=1 and Y=3. There is only one process needed with r=X=1 and p=Y/3=1. According to Eqs. (1) and (2), $a_1^1=[P_E\ P_I\ P_I]^T$, $a_2^1=[P_I\ P_E\ P_I]^T$, $a_3^1=[P_I\ P_I\ P_E]^T$, $b_1^1=[P_W\ P_B\ P_W]^T$, $b_2^1=[P_B\ P_B\ P_W]^T$, $b_3^1=[P_W\ P_W\ P_B]^T$. The secret images can be recovered by overlaying share A and B at three angles. The shares without random permutation are shown in Figure 3.

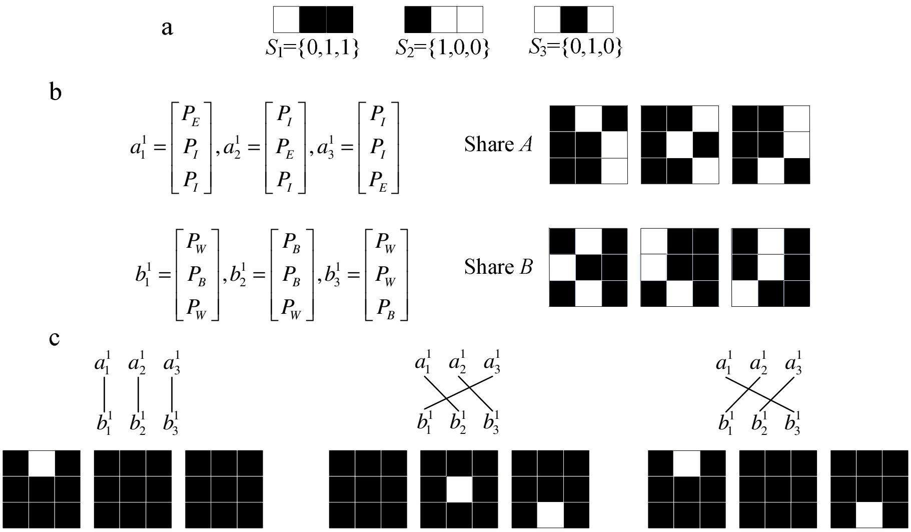
a
S_1={0,1,1}
S_2={1,0,0}
S_3={0,1,0}
b
$a_1^1=\begin{bmatrix}P_E\\P_I\\P_I\end{bmatrix}, a_2^1=\begin{bmatrix}P_I\\P_E\\P_I\end{bmatrix}, a_3^1=\begin{bmatrix}P_I\\P_I\\P_E\end{bmatrix}$
Share A
$b_1^1=\begin{bmatrix}P_W\\P_B\\P_W\end{bmatrix}, b_2^1=\begin{bmatrix}P_B\\P_B\\P_W\end{bmatrix}, b_3^1=\begin{bmatrix}P_W\\P_W\\P_B\end{bmatrix}$
Share B
c
a_1^1 a_2^1 a_3^1
b_1^1 b_2^1 b_3^1
a_1^1 a_2^1 a_3^1
b_1^1 b_2^1 b_3^1
a_1^1 a_2^1 a_3^1
b_1^1 b_2^1 b_3^1

Fig. 3. An example of the (2, 2, 3)-MVCS: (a) Three secret images. (b) The generated share images. (c) The stacking secret image at 0°, 120°, 240°.

In order to break up the regular pixel distribution, let a random permutation *Permu* =(2,5,1,7,3,0,6,4,8) be applied to the blocks a_1^1, a_2^1, a_3^1, b_1^1, b_2^1, b_3^1. The attackers can't guess the secret pixels from the permutated blocks $a_1'^1, a_2'^1, a_3'^1, b_1'^1, b_2'^1, b_3'^1$. Meanwhile, the secret images can also be recovered by overlaying the share A' and B' at 0°, 120°, 240°. The permutated shares and the recovery images are illustrated in Figure 4.

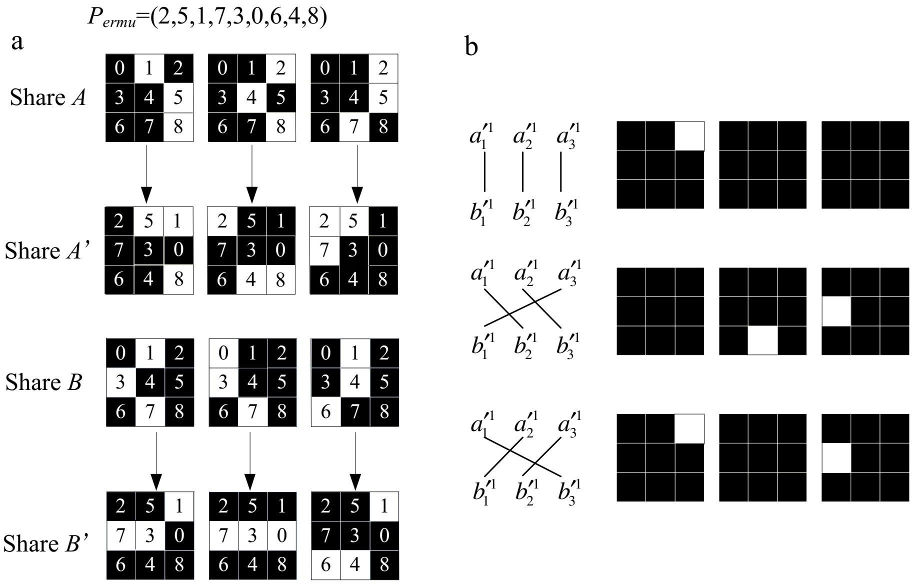
P_{ermu}=(2,5,1,7,3,0,6,4,8)
a
b
Share A
Share A'
Share B
Share B'
$a_1'^1$ $a_2'^1$ $a_3'^1$
$b_1'^1$ $b_2'^1$ $b_3'^1$

Fig. 4. The (2, 2, 3)-MVCS with permutation: (a) Permutation on share blocks. (b) The stacking secret image at 0°, 120°, 240°.

According to Figure 3 and Figure 4, the correlations between b_1^1 and b_2^1 are analyzed using the Block Attacking.

Step1: $b_1'^1 \oplus b_2'^1$ =[110001111] ⊕ [111000111] = [001001000].

Step2: There are 2 ‘1’ in $b_1'^1 \oplus b_2'^1$. We can get the number of ‘1’ in $b_1^1 \oplus b_2^1$, which is d=2. (Figure 5 shows that the numbers of ‘1’ in $b_1^1 \oplus b_2^1$ and $b_1'^1 \oplus b_2'^1$ are equal as expectation.)

Step3: There are d/2=1 different pixels between the 3 secret pixels encoded into b_1^1 and b_2^1.

Step4: Output d/2=1.

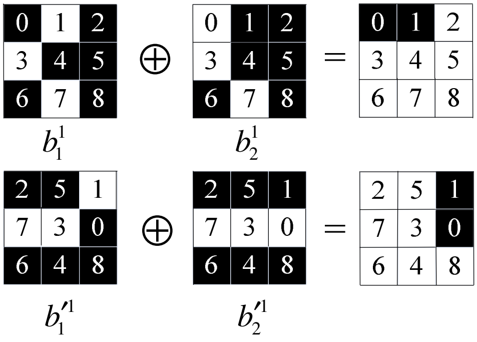

Fig. 5. b11⊕b21and $b_1'^1 \oplus b_2'^1$

According to the conclusion of the Block Attacking, the all combinations of secret pixels encrypted into $b_1{}^1$ and $b_2{}^1$ are enumerated in the Table 2.

Table 2. The combinations of secret pixels encrypted into $b_1{}^1$ and $b_2{}^1$

The possible combinations of 3 secret pixels encrypted into $b_1{}^1$	000	001	010	011	100	101	110	111
The corresponding combinations of 3 secret pixels encrypted into $b_2{}^1$	100	101	110	111	000	001	010	011
	010	011	000	001	110	111	100	101
	001	000	011	010	101	100	111	110

From Table 2, there are only 8×3=24 possible combinations for 6 secret pixels. However, if the (2, 2, 3)-MVCS is ideal secure, there should be 2^6=64 combinations for 6 secret pixels. Although the attackers can't guess the exact secret pixels encoded into $b_1{}^1$ and $b_2{}^1$, the 6 secret pixels' space is reduced from 64 to 24. Actually, the secret pixels in $b_1{}^1$ are [010], and the secret pixels in $b_2{}^1$ are [110]. [010] and [110] are exist in Table 2. Therefore, the Block Attacking is effective.

The correlations between $b_2{}^1$ and $b_3{}^1$ can also be analyzed by the Block Attacking.

Step1: $b_2'^1 \oplus b_3'^1$ =[111000111] ⊕ [110111001] = [001111110].

Step2: There are 6 '1' in $b_2'^1 \oplus b_3'^1$, and d=6.

Step3: There are d/2=3 different pixels between the 3 secret pixels encoded into $b_2{}^1$ and $b_3{}^1$.

Step4: Output d/2=3.

The result means that the 3 secret pixels encoded into $b_2{}^1$ are all different from $b_3{}^1$. Taking the relation between $b_1{}^1$, $b_2{}^1$ and $b_3{}^1$ into consideration, there are only 8×3×1=24 possible combinations for all 9 secret pixels. The 9 secret pixels' space is reduced from ideal 2^9=512 to 24 by analyzing the share B alone. The weakness threatens the example of (2, 2, 3)-MVCS severely, which is ignored in Feng et al.'s scheme.

Table 3. The statuses of '1's in $b_i'^p \oplus b_j'^p$

d, the number of '1' in $\hat{b}_i^p \oplus \hat{b}_j^p$	The number of the different secret pixels	The possible combinations of the secret pixels encoded into b_i^P and b_j^P
0	0	2^3×C(3, 0)= 8
2	1	2^3×C(3, 1)= 24
4	2	2^3×C(3, 2)= 24
6	3	2^3×C(3, 3)= 8

Using the Block Attacking to the general (2, 2, 3)-MVCS, let the sizes of the secret images are all X×Y. There are Y/3 sets in every row, so the share B has XY/3 sets totally. The p-set contains 3 blocks $b_1'^p, b_2'^p$ and $b_3'^p$, and every 3 secret pixels are encoded into one block. There are 4 statuses of d, the number of '1' in $b_i'^p \oplus b_j'^p$ $(1 \leq i \neq j \leq 3$, $1 \leq p \leq XY/3)$, which are shown in Table 3.

The best situation for attackers is d=0 or 6 for every pair of the 3 blocks in every set. Then, the attacking difficulty of one set declines from 2^9 to 2^3. Furthermore, the attacking difficulty of the secret images decreases from 2^{3XY} to 2^{XY}.

The worst situation for attackers is d=2 or 4 for the blocks in every set. Then, the attacking difficulty of one set declines from 2^9 to $2^3 \times 3 \times 3 = 9 \times 2^3$. Furthermore, the attacking difficulty of the secret images decreases from 2^{3XY} to $2^{XY} \times 3 \times 3 \approx 2^{XY+3.2}$.

3.3 Attacking to (2, 2, *m*)-MVCS

Using the Block Attacking to the (2, 2, m)-MVCS, let the sizes of the secret images are all $X \times Y$. There are Y/m sets in every row, so the share B has XY/m sets totally. p-set contains m blocks $b_1'^p, b_2'^p, \ldots, b_m'^p$, and every m secret pixels are encoded into one block. There are m +1 statuses of d, the number of '1' in $b_i'^p \oplus b_j'^p$ $(1 \leq i \neq j \leq m$, $1 \leq p \leq XY/m)$, which are shown in Table 4.

Table 4. m +1 statuses of '1's in $b_i'^p \oplus b_j'^p$

d, the number of '1' in $\hat{b}_i^p \oplus \hat{b}_j^p$	The number of the different secret pixels	The possible combinations of the secret pixels encoded into b_i^P and b_j^P
0	0	$2^m \times C(m, 0)$
2	1	$2^m \times C(m, 1)$
……	……	……
$2i$	i	$2^m \times C(m, i)$
……	……	……
$2m$	m	$2^m \times C(m, m)$

The best situation for attackers is d=0 or $2m$ for every pair of the m blocks in every set. Then, the attacking difficulty of one set declines from 2^{mm} to 2^m. Furthermore, the attacking difficulty of the secret images decreases from 2^{mXY} to 2^{XY}.

The worst situation for attackers is $d = \lceil m/2 \rceil$ or $\lfloor m/2 \rfloor$ for every pair of the m blocks in every set. Then, the attacking difficulty of one set declines from 2^{mm} to $2^m \times C(m, \lfloor m/2 \rfloor)^{m-1}$. Furthermore, the attacking difficulty of the secret images decreases from 2^{mXY} to $2^{XY} \times C(m, \lfloor m/2 \rfloor)^{m-1}$.

It is difficult to modify the scheme directly. If we use different random permutations for the m blocks in one set, the ideal security can be guaranteed, but the secret images can't be decrypted.

4 Proposed Scheme

In this section, an ideal secure MVCS is proposed by using two new visual patterns. The multi-secret sharing algorithm is redesigned, and the security and contrast properties of the scheme are analyzed.

4.1 Multi-secret Sharing Algorithm

In order to realize the ideal secure MVCS, we design two visual patterns P_0={1,0} and P_1={0,1} instead of the previous four patterns. P_0 and P_1 have the same Hamming weight "1". Meanwhile, if P_0 is permuted randomly, the result may be P_0 and P_1 with the same probability 50%. Table 5 shows the relations between the visual patterns.

Table 5. Relations between visual patterns P_0 and P_1

Stacking operations	Block of re-sults
$P_0 + P_0$ ={1,0}	White
$P_1 + P_1$ ={0,1}	White
$P_0 + P_1$ ={1,1}	Black

For the p-th process on the r-th row, a_i^P and b_i^P are generated according to the following equations, where $1 \le j \le m$.

$$a_{i,j}^p = P_0 \tag{3}$$

$$b_{1+(i+j-2)\bmod m,j}^p = \begin{cases} P_0 & S_j\left(r, p+(i-1)Y/m\right) = 0 \\ P_1 & S_j\left(r, p+(i-1)Y/m\right) = 1 \end{cases} \tag{4}$$

The last part is using random permutation for $a_{i,j}^p$ and $b_{1+(i+j-2)\bmod m,j}^p$ to break up the regular pixel distribution. Meanwhile, $a_{i,j}^p$ and $b_{1+(i+j-2)\bmod m,j}^p$ are applied with the same random permutation, and therefore the secret $S_j(r, p+(i\text{-}1)Y/m)$ can still be decrypted by stacking $a_{i,j}^p$ and $b_{1+(i+j-2)\bmod m,j}^p$. The rule of random permutation is different from Feng et al.'s. In [17], the random permutation is performed on a_1^P, a_2^P, …, a_m^P and b_1^P, b_2^P, …, b_m^P simultaneously.

The complete encryption algorithm for the proposed scheme is as follows.

Input: Secret images S_1, S_2, … , S_m

Output: Two share A, B

Step1: Adjust the size of all secret images to $X \times Y$ that the X must be a multiple of m.
Step 2: Initialize the processing row r = 1 of the images.
Step 3: Start the p-th process of the proposed scheme with p = 1.

Step 4: Select the 1, m+1, 2m+1, $\cdots$, X–m+1 secret pixels to generate the blocks $a_1{}^P$, $a_2{}^P$, …, $a_m{}^P$ and $b_1{}^P$, $b_2{}^P$, …, $b_m{}^P$ according to Eqs. (3) and (4).
Step 5: Let $(a^p_{i,j}, b^p_{1+(i+j-2)\bmod m,j})$ denotes a pair of patterns. Perform independent random permutations on all pairs of $a_1{}^P$, $a_2{}^P$, …, $a_m{}^P$ and $b_1{}^P$, $b_2{}^P$, …, $b_m{}^P$.
Step 6: Fill the blocks in the share images. $a_i'^p$ is the permutated block on the r-th row and (p + X(i – 1)/m)-th column of share A, and $b_i'^p$ is the permutated block on the r-th row and (p + X(i – 1)/m)-th column of share B.
Step 7: If $p<X/m$, return to Step 4 for the next process $p := p+1$.
Step 8: If $r <Y$, return to Step 3 for the next row $r:=r+1$.
Step 9: Out put the two shares A and B.

4.2 Effectiveness Formal Proof

The effectiveness of visual cryptography scheme contains two aspects: security and contrast. The security means a single share can not leak the secret information, while the contrast means human visual system can recognize the secret images after overlapping two shares.

Theorem 1 (Security). Any information can not be taken from a single share.

Proof. For share A, every block is composed of m permuted visual patterns. According to the sharing algorithm, $a^p_{i,j} = P_0$. But for the permuted $a'^p_{i,j}$, $P(a'^p_{i,j} = P_0)$ $= P(a'^p_{i,j} = P_1) = 0.5$, which is independent of the secret pixel $S_j(r, p+(i\text{-}1)Y/m)$. So, $H(S_i \mid A)= H(S_i)$, where H denotes the entropy.

For share B, every block is composed of m permuted visual patterns too. According to the sharing algorithm, $b^p_{1+(i+j-2)\bmod m,j}$ relies on $S_j(r, p+(i\text{-}1)Y/m)$. But after random permutation, $P(b'^p_{1+(i+j-2)\bmod m,j} = P_0) = P(b'^p_{1+(i+j-2)\bmod m,j} = P_1) = 0.5$, which is independent of the secret pixel $S_j(r, p+(i\text{-}1)Y/m)$. Hence, $H(S_i \mid B)=H(S_i)$.

In conclusion, any information can not be taken from a single share, which means the security of the scheme is ideal.

The block attacking is inefficient for the proposed scheme, because the visual patterns in blocks are permutated by different random series.

Lemma 1. For $a'^p_{i,j}$ and $b'^p_{k,j}$ ($k \neq 1+(i+j\text{-}2) \bmod m$), the expectation of Hamming weight of $a'^p_{i,j} + b'^p_{k,j}$ is equal to 3/2.

Proof. Since $k \neq 1+(i+j\text{-}2) \bmod m$, $a'^p_{i,j}$ and $b'^p_{k,j}$ are generated by different random permutations. Without generality, suppose $a'^p_{i,j} = P_0$. Then $b'^p_{k,j}$ is equal to P_0 or P_1 with the same probability 50%.

We can get $P(a'^{p}_{i,j}+b'^{p}_{k,j}=\{1,0\})=P(a'^{p}_{i,j}+b'^{p}_{k,j}=\{1,1\})=0.5$. Therefore, the expectation of Hamming weight of $a'^{p}_{i,j}+b'^{p}_{k,j}$ is (1+2)× 1/2=3/2.

Theorem 2 (Contrast). The secret image S_j can be recovered by stacking share A and share B at $(j\text{-}1)360°/m$.

Proof. By rotating share B at $(j\text{-}1)360°/m$, the p-th set in the r-th row of share B $b'^{p}_{1},b'^{p}_{2},\cdots,b'^{p}_{m}$ have been changed into $b'^{p}_{j},\cdots b'^{p}_{m},b'^{p}_{1},\cdots,b'^{p}_{j-1}$. Stacking share A and the rotated share B means that $a'^{p}_{1}+b'^{p}_{j},a'^{p}_{2}+b'^{p}_{j+1},\cdots,a'^{p}_{m}+b'^{p}_{j-1}$. Let $E(\cdot)$ denotes the expectation of Hamming weight.

Since $a'^{p}_{1}+b'^{p}_{j}=\sum_{k=1}^{k=m}(a'^{p}_{1,k}+b'^{p}_{j,k})$, we have $E(a'^{p}_{1}+b'^{p}_{j})=\sum_{k=1}^{k=m}E(a'^{p}_{1,k}+b'^{p}_{j,k})$. According to Lemma 1, $E(a'^{p}_{1,k}+b'^{p}_{j,k})$ =3/2 where $k\neq j$.

If $S_j(r, p) = 0$, we have

$$E(a'^{p}_{1,j}+b'^{p}_{j,j})=1$$

$$E(a'^{p}_{1}+b'^{p}_{j})=E(a'^{p}_{1,j}+b'^{p}_{j,j})+\sum_{k=1}^{k\neq j}E(a'^{p}_{1,k}+b'^{p}_{j,k})=3(m\text{-}1)/2+1 \qquad (5)$$

If $S_j(r, p) = 1$, we have

$$E(a'^{p}_{1,j}+b'^{p}_{j,j})=2$$

$$E(a'^{p}_{1}+b'^{p}_{j})=E(a'^{p}_{1,j}+b'^{p}_{j,j})+\sum_{k=1}^{k\neq j}E(a'^{p}_{1,k}+b'^{p}_{j,k})=3(m\text{-}1)/2+2 \qquad (6)$$

Comparing Eq.(5) with Eq.(6), the secret pixel $S_j(r, p)$ can be recovered by the stacking blocks $a'^{p}_{1}+b'^{p}_{j}$. The rest secret pixels may be deduced by analogy.

In conclusion, S_j can be recovered by stacking share A and share B at $(j\text{-}1)360°/m$.

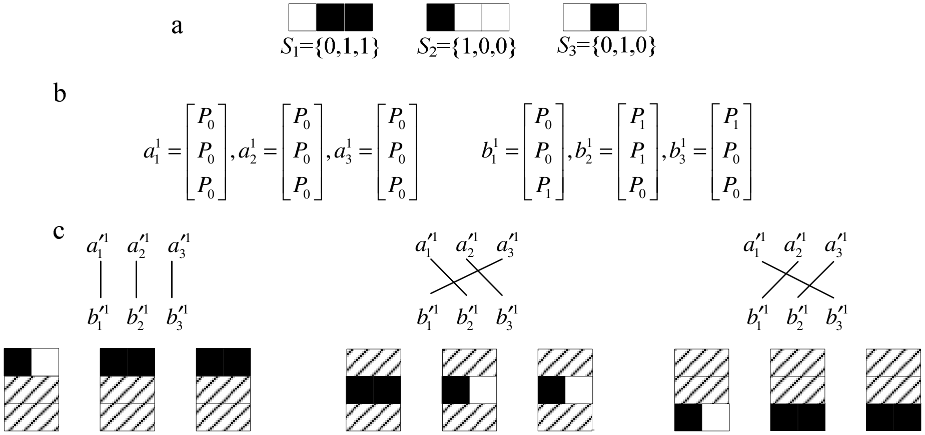
a
S1={0,1,1}
S2={1,0,0}
S3={0,1,0}
b
$a_1^1=\begin{bmatrix}P_0\\P_0\\P_0\end{bmatrix},a_2^1=\begin{bmatrix}P_0\\P_0\\P_0\end{bmatrix},a_3^1=\begin{bmatrix}P_0\\P_0\\P_0\end{bmatrix}$
$b_1^1=\begin{bmatrix}P_0\\P_0\\P_1\end{bmatrix},b_2^1=\begin{bmatrix}P_1\\P_1\\P_0\end{bmatrix},b_3^1=\begin{bmatrix}P_1\\P_0\\P_0\end{bmatrix}$
c
a'^1_1 a'^1_2 a'^1_3
b'^1_1 b'^1_2 b'^1_3
a'^1_1 a'^1_2 a'^1_3
b'^1_1 b'^1_2 b'^1_3
a'^1_1 a'^1_2 a'^1_3
b'^1_1 b'^1_2 b'^1_3

Fig. 6. The (2, 2, 3)-MVCS of our scheme: (a) Three secret images. (b) The generated share images. (c) The stacking secret image at 0°, 120°, 240°.

Figure 6 shows the (2, 2, 3)-MVCS of our scheme. There are 9 pairs of visual patterns: $(a^1_{1,1}, b^1_{1,1})$, $(a^1_{2,1}, b^1_{2,1})$, $(a^1_{3,1}, b^1_{3,1})$, $(a^1_{1,2}, b^1_{2,2})$, $(a^1_{2,2}, b^1_{3,2})$, $(a^1_{3,2}, b^1_{1,2})$, $(a^1_{1,3}, b^1_{3,3})$, $(a^1_{2,3}, b^1_{1,3})$ and $(a^1_{3,3}, b^1_{2,3})$. After performing 9 different random permutations on the 9 pairs, we can get the final blocks $a_1'^1, a_2'^1, a_3'^1, b_1'^1, b_2'^1, b_3'^1$. The shadow zone in the recovered image means that the expectation of the visual pattern's Hamming weight is 3/2.

5 Experimental Results and Discussions

To demonstrate the feasibility of the present multi-secret sharing scheme, the experiments are conducted by adopting (2, 2, 4)-MVCS for example. Four secret images S_1, S_2, S_3 and S_4, as shown in Fig.7 (a), will be encoded into two share images A and B, as shown in Fig.7 (b). In the decoding phase, Fig.7(c) shows the stacking secret image at 0°, 90°, 180° and 270°.

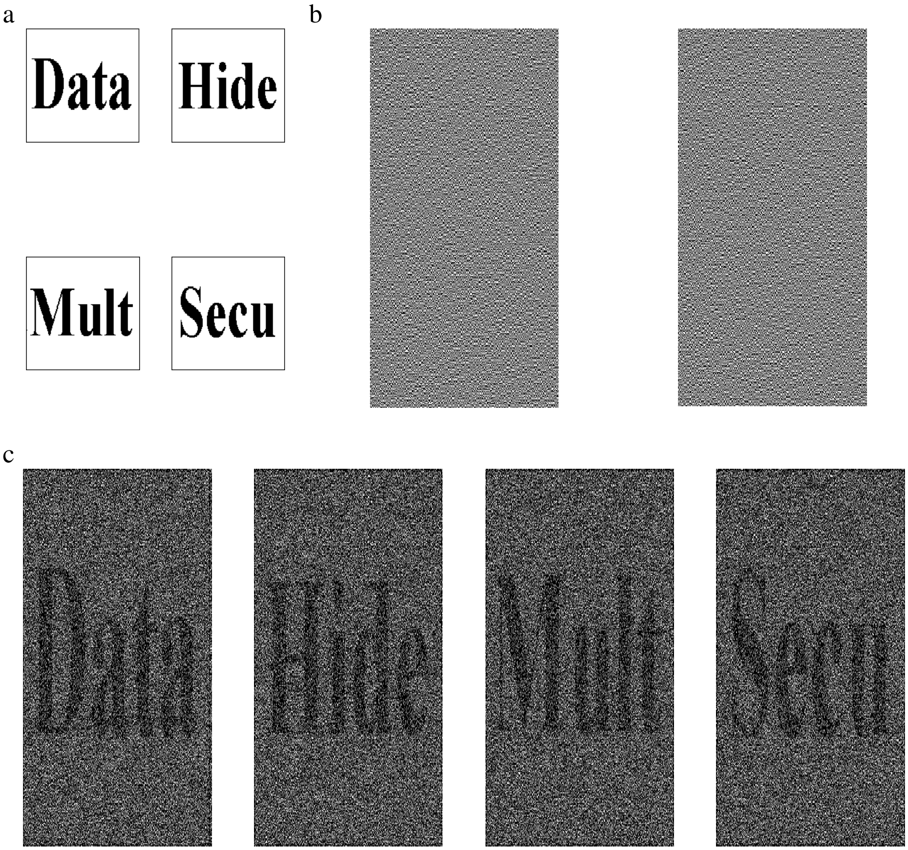

Fig. 7. (a) Four secret images. (b) Two share images. (c) The stacking secret image at 0°, 90°, 180°, 270°.

For visual cryptography scheme, the pixel expansion and the relative difference are two important parameters. The smaller pixel expansion and the bigger relative difference mean the smaller share size and the better recovering effect, respectively. In our scheme, the size of block is 2×m, and the Hamming weight difference between the recovered white and black pixel is 1. Therefore, the pixel expansion is 2m and the relative difference is 1/(2m). The comparison between our scheme and Feng et al.'s is shown in Table 6.

Table 6. The comparison between Feng et al.'s and the proposed scheme

	Feng et al.'s scheme	The proposed scheme
Pixel expansion	3m	2m
Relative difference	1/(3m)	1/(2m)
Ideal secure	N	Y

6 Conclusion

An ideal secure multi-secret visual cryptography scheme has been proposed in this paper, in which any amount of secret images can be encoded into two ring shares. The scheme is based on two new visual patterns and random permutations, which are different from previous schemes. The novel design makes better visual effects, as well as perfect security. Theoretical analysis and experimental results show the effectiveness of the proposed scheme. The scheme is only suit to two shares, thus how to extend to general access structure is our future work.

Acknowledgment. This work was supported by the National Natural Science Foundation of the People's Republic of China under Grant No. 61070086. The authors would like to thank the anonymous reviewers for their valuable comments.

References

1. Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995)
2. Shamir, A.: How to share a secret. Communications of the ACM 22, 612–613 (1979)
3. Blakley, G.R.: Safeguarding cryptographic keys. In: Merwin, R.E., Zanca, J.T., Smith, M. (eds.) National Computer Conference, vol. 48, pp. 242–268. IEEE Press, New York (1979)
4. Ateniese, G., Blundo, C., Santis, A., De, S.D.R.: Visual cryptography for general access structures. Information and Computation 129, 86–106 (1996)
5. Hsu, C.S., Tu, S.F., Hou, Y.C.: An optimization model for visual cryptography schemes with unexpanded shares. In: Esposito, F., Raś, Z.W., Malerba, D., Semeraro, G. (eds.) ISMIS 2006. LNCS (LNAI), vol. 4203, pp. 58–67. Springer, Heidelberg (2006)

6. Liu, F., Wu, C., Lin, X.: Step construction of visual cryptography schemes. IEEE T. Inf. Foren. Sec. 5, 27–38 (2010)
7. Shyu, S.J., Chen, M.C.: Optimum pixel expansions for threshold visual secret sharing schemes. IEEE T. Inf. Foren. Sec. 6, 960–969 (2011)
8. Yang, C.N., Wang, C.C., Chen, T.S.: Visual cryptography schemes with reversing. The Computer Journal. Bxm 118, 1–13 (2008)
9. Lin, C.C., Tai, W.H.: Visual cryptography for gray-level images by dithering techniques. Pattern Recognition Letters 24, 349–358 (2003)
10. Cimato, S., Prisco, R.D., Santis, A.D.: Optimal colored threshold visual cryptography schemes. Designs, Codes and Cryptography 35, 311–335 (2005)
11. Yang, C.N., Chen, T.S.: Colored visual cryptography scheme based on additive color mixing. Pattern Recognition 41, 3114–3129 (2008)
12. Ng, F.Y., Wong, D.S.: On the security of a visual cryptography scheme for color images. Pattern Recognition 42, 929–940 (2009)
13. Chen, L.H., Wu, C.C.: A study on visual cryptography. Master Thesis, National Chiao Tung University, Taiwan (1998)
14. Wu, H.C., Chang, C.C.: Sharing visual multi-secrets using circle shares. Computer Standards & Interfaces 28, 123–135 (2005)
15. Shyong, J.S., Huang, S.Y., Lee, Y.K., Wang, R.Z.: Sharing multiple secrets in visual cryptography. Pattern Recognition 40, 3633–3651 (2007)
16. Hsu, H.C., Chen, T.S., Lin, Y.H.: The ring shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing. In: Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, pp. 996–1001. IEEE Press, New York (2004)
17. Feng, J.B., Wub, H.C., Tsaic, C.S., Chud, Y.P.: Visual secret sharing for multiple secrets. Pattern Recognition 41, 3572–3581 (2008)