

A Modified Multi-secret Visual Cryptography with Ring Shares

Zheng-xin Fu^{1, a}, Bin Yu^{1, b}

¹ Zhengzhou Information Science and Technology Institute, P. R. China, 450004

^afzx2515@163.com, ^bbyu2009@163.com

Keywords: Visual cryptography, Multiple secret sharing, Ring share, Marked area.

Abstract. A visual cryptography scheme encoding multiple secret images into two ring shares is proposed in this paper. In the secret sharing process, two shares are produced by the marked areas and the basis matrices of $(2, 2)$ -VCS. Using ring shift right function, the secret images are recovered by stacking two shares. The security and contrast properties of the scheme have been proved. Compared with the previous ones, the scheme makes the number of secret images unlimited. Furthermore, the pixel expansion and the relative difference are improved greatly.

Introduction

Secret sharing, proposed independently by Shamir [1] and Blakley [2] in 1979, is an effective method for a group to protect the confidential information. The principle is encoding the secret into some shares to be distributed to a set of participants. Only the qualified sets of these participants can recover the secret, whereas the unqualified sets learn nothing about the secret. Most secret sharing schemes are based on the finite field arithmetic, which are mainly realized by the computer.

As a new secret sharing technology, visual cryptography scheme (VCS) was introduced by Naor and Shamir [3] in Eurocrypt'94. The dealer encodes a secret image into shares to be distributed to n participants. These shares, when printed on transparencies, can be reconstructed simply by overlapping them. Since the security of VCS is equal to "one time pad" [3] and the reconstruction is performed without any machine, many researchers pay much attention to this domain. In recent years, the main results of VCS include the general access structure [4], the optimization of pixel expansion and relative difference [5-8], grey and chromatic images [9-12], etc. However, the schemes above can only share one secret image. The participants have to manage many shares when encoding several images, reducing the work efficiency.

In order to share multiple images effectively, Yu et al. [13] present a multi-secret visual cryptography scheme (MVCS) based on the general access structure, in which the different secret images are shared by different qualified sets of participants. Another research interest to recover different images is by overlapping two shares with different positions. Chen et al. [14] have designed $(2,2,2)$ -MVCS to share images S_1 and S_2 into shares T_1 and T_2 . S_1 can be recovered by overlapping T_1 and T_2 directly. S_2 is decrypted also by stacking T_1 and T_2 while T_2 is rotated with angle 90° , 180° or 270° . In order to overcome the angle restriction, Wu et al. [15] and Shyong et al. [16] devise the shares to be circles and encode secrets without the angle's constraint. However, the decrypted images are distorted from square to circular and have less contrast.

Different from the square and circle shares, Hsu et al. [17] propose a scheme to hide two images in two ring shares with arbitrary rotating angles and undistorted shapes. Though Hsu's scheme has no restriction of angle, only two secret images can be encrypted. Based on the ring shares, Feng et al. [18] present another scheme to share much more images using four different visual patterns. Nevertheless, the pixel expansion of Feng's scheme is $3n$ and the relative difference is $1/(3n)$, which imply the large share size and the indistinct effect of the decrypted image respectively.

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 functions and statuses of two shares are dissimilar, which can influence the parameters of MVCS. Different from the above-mentioned idea, this paper proposes















a *MVCS* based on the regional contrast and the basis properties of $(2, 2)$ -*VCS*. The secret sharing and recovering procedures are designed with the premise that two ring shares are divided into some marked areas. The effectiveness of the scheme can be also guaranteed, which contains security and contrast properties. Furthermore, the two shares have the same statuses, and the pixel expansion and relative difference are improved obviously.

The rest of this paper is organized as follows. Section II briefly reviews $(2, 2)$ -*VCS* and the region contrast. In Section III, some basic definitions on our scheme are given. As the main part of this paper, Section IV 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 V. Section VI concludes the paper.

Related Studies

As the earliest visual cryptography scheme, $(2, 2)$ -*VCS* is used as the basic unit in our scheme. The encoding principle is easy to understand (Table 1).

Table 1. Encryption rules of $(2, 2)$ -*VCS*

Secret pixel color	Methods	Share 1	Share 2	Overlay share 1 and 2
	1			
	2			
	1			
	2			

A white pixel is shared into two identical blocks of a white sub-pixel and a black one. A black pixel is shared into two complementary blocks. Any single share is a random set of blocks. When two shares are stacked together, the Hamming weight of block is either 1 (corresponding to an original white pixel) or 2 (corresponding to an original black pixel). Therefore, the reconstructed image can be recognized.

The traditional scheme requires every pixel to satisfy the contrast condition. Actually, the secret can be successfully reconstructed as long as human eyes system can distinguish the difference between black and white regions, not every pixel. Therefore, if the blackness expectation of blocks corresponding to black pixels in secret images is bigger than the white ones, a visual cryptography scheme can also be realized [5]. The idea is also utilized in this paper, which would be discussed in detail in Section IV.

Basic Definitions

Since the scheme design is different from the previous ones, some basic definitions related to the scheme are introduced first.

Assume that the secret images S_1, S_2, \dots, S_n are sized $X \times Y$, where $Y \bmod n \equiv 0$. In the scheme, share A and share B are both constituted of $X \times Y$ sub-pixel blocks. Each sub-pixel block corresponds to n pixels of secret images, consisting of one pixel in every secret image at the same position.

Definition 1 (Marked Areas). Each sub-pixel block is denoted by a $2 \times n$ Boolean matrix. Every column in matrix is called an area, which can be marked from 1 to Y (Fig. 1(a)).

As like Feng et al.'s scheme, the secret images are encrypted by row in this paper. Therefore, the pixels of each secret image are marked by column (Fig. 1(b)).

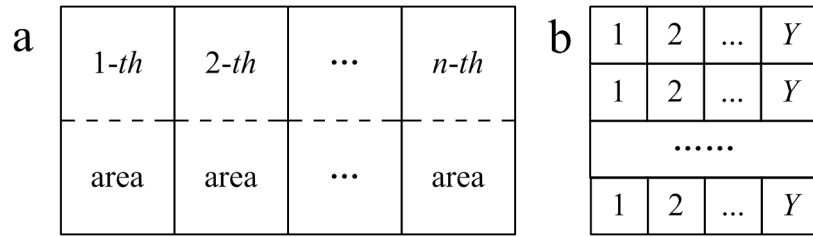


Fig. 1. (a) the areas in the sub-pixel block, (b) the pixel marks of the secret image

The areas in A and B have different marks. And each i -th area is related to one pixel of S_i according to the same mark. In share A , the order of marks in all i -th areas is same as S_i . In share B , the marks of all i -th areas are shown in Fig. 2(a). If $i=1$, the mark orders of all i -th areas and S_i are uniform.

The marks in different areas are independent, which are decided by different secret images. Two shares with complete marks are given in Fig. 2(b) and Fig. 2(c).

Definition 2 (Ring Shift Right Function). Let $R(B, i-1)$ be a function, which means share B ring shifts right $i-1$ sub-pixel areas ($1 \leq i \leq n$).

Evidently, only the marks of i -th areas are identical in share A and $R(B, i-1)$.

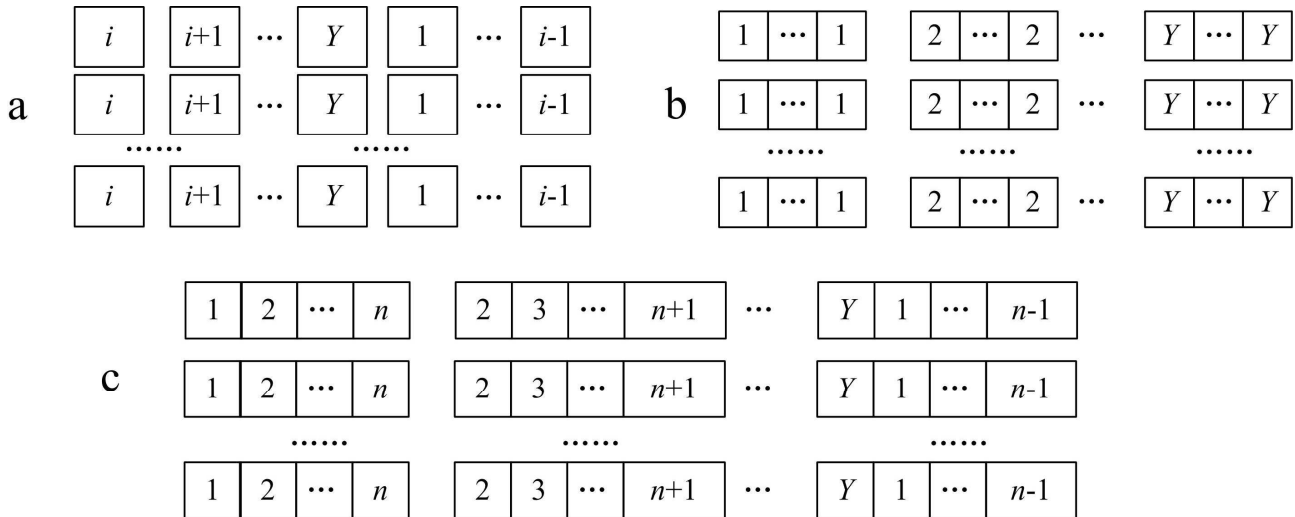


Fig. 2. (a) the marks of all i -th areas in share B , (b) share A with complete marks, (c) share B with complete marks

The Proposed Scheme

This section proposes the multi-secret sharing and recovering processes of the scheme. In the sharing process, the shares are generated by area marks and the basis matrices of $(2, 2)$ -VCS. Different from the multi-secret sharing, the secret images can be recovered easily by stacking share A and rotated share B . Meanwhile, the effectiveness of the scheme is proved in this section.

The secret images have to be preprocessed by extending the width of images to satisfy $Y \bmod n \equiv 0$. $B_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$ and $B_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ are basis matrices of $(2, 2)$ -VCS. B_0 (B_1) is selected to encode the white (black) pixels of secret images. In the sharing process, choose a pixel of the secret image and confirm the basis matrix M first. The areas of two shares, corresponding to the selected pixel, are evaluated by $P(M)$. $P(M)$ denotes the random permutation of matrix B by column. The specific multi-secret sharing algorithm is as follow.

Multi-secret Sharing Algorithm

Input: Secret images S_1, S_2, \dots, S_n

Output: Two shares A and B

Step 1: Adjust the size of all secret images to $Y \bmod n \equiv 0$.

Step 2: Select the secret image S_i , where $i=1$.

Step 3: Initialize the process row $r=1$ of S_i .

Step 4: Choose the k -th pixel in row r with $k=1$.

Step 5: If the color of the selected pixel is black, $C = P(B_1)$. Otherwise, $C = P(B_0)$.

Step 6: Fill the i -th area marked k in row r of share A (B) with the first (second) column of C^T .

Step 7: If $k < Y$, return to Step 5 for the next pixel with $k=k+1$.

Step 8: If $r < X$, return to Step 4 for the next row with $r=r+1$.

Step 9: If $i < n$, return to Step 3 for the next secret image with $i=i+1$.

Step 10: Out put the shares A and B .

In contrast with the sharing procedure, the recovering of the secret image is very simple. S_i can be recovered when the marks of the i -th areas in shares A and B are same. In light of Definition 2, the participants can identify S_i by stacking share A and $R(B, i-1)$, which is shown in Fig. 3.

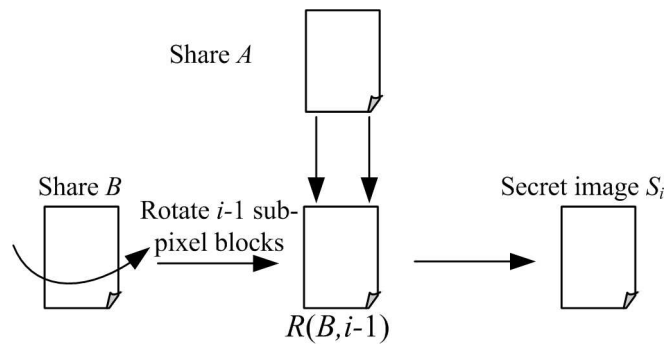


Fig. 3. The procedure of secret recovering

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. They would be discussed respectively.

Theorem 3 (Security). Any information can not be taken from a single share.

Proof. Each area in share is composed of a white sub-pixel and a black one, no matter the color of the corresponding secret pixel. Furthermore, the order of the sub-pixels in area is decided by random permutation. The probability for adversary to get the secret image by a single share is equal to guessing the secret images directly. In other words, $H(S_i | A) = H(S_i | B) = H(S_i)$, where H denotes the entropy and $i \in [1, n]$. Therefore, the security of the scheme is perfect. \square

Lemma 4. If share A and rotated B have different marks orders in the i -th areas, the expectation of i -th area's Hamming weight is equal to $3/2$ after overlapping A and B .

Proof. Since marks orders of all i -th areas in two shares are dissimilar, the corresponding pixels in S_i of two shares are at different positions. Assume an i -th area in share A is $[0, 1]^T$. On the basis of the sharing process, the i -th area in share B with the same position is $[0, 1]^T$ or $[1, 0]^T$ with the same probability $1/2$, no matter whether the corresponding secret pixels' colors are same. The reason is the two areas are generated by twice random column permutation of the basis matrices.

To sum up, the expectation of the i -th area's Hamming weight is $(1+2) \times 1/2 = 3/2$, after stacking share A and rotated B . \square

Theorem 5 (Contrast). The secret image S_i can be recovered by stacking share A and $R(B, i-1)$.

Proof. Let $w(0, i, j)$ ($w(1, i, j)$) denotes the Hamming weight of the j -th area corresponding to the white (black) pixel of S_i after stacking A and $R(B, i-1)$. $E[w(0, i, j)]$ ($E[w(1, i, j)]$) is the expectation of $w(0, i, j)$ ($w(1, i, j)$). $E[w(0, i, \Sigma)]$ ($E[w(1, i, \Sigma)]$) denotes the Hamming weight expectation of the sub-pixel block related to the white (black) pixel of S_i .

Therefore, $E[w(0, i, \Sigma)] = \sum_{j=1}^n E[w(0, i, j)]$, and $E[w(1, i, \Sigma)] = \sum_{j=1}^n E[w(1, i, j)]$, where $1 \leq i, j \leq n$. In terms of the marking statement, the marks of share A and $R(B, i-1)$ are same only in the i -th areas. In accordance with Lemma 4, $E[w(0, i, \Sigma)] = E[w(0, i, i)] + \sum_{j=1, j \neq i}^n E[w(0, i, j)] = 3(n-1)/2 + 1$, and $E[w(1, i, \Sigma)] = E[w(1, i, i)] + \sum_{j=1, j \neq i}^n E[w(1, i, j)] = 3(n-1)/2 + 2$.

Since $E[w(1, i, \Sigma)] - E[w(0, i, \Sigma)] = 1$, the blackness expectation of blocks corresponding to black pixels in S_i is bigger than the white ones after stacking shares. In conclusion, S_i can be taken by share A and $R(B, i-1)$. \square

Experiments and Analyses

As the fundamental parameters in visual cryptography, the pixel expansion and the relative difference are always used for measuring schemes. 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 sub-pixel block is $2n$, and the Hamming weight expectation difference between original white and black pixels is 1. Therefore, the pixel expansion is $2n$ and the relative difference is $1/(2n)$. The comparison between our scheme and others is shown in Table 2.

Table 2. The parameters comparison

Number of secret images	The scheme in [17]		The scheme in [18]		The proposed scheme	
	Pixel expansion	Relative difference	Pixel expansion	Relative difference	Pixel expansion	Relative difference
2	4	1/2	6	1/6	4	1/4
3	N/A	N/A	9	1/9	6	1/6
n	N/A	N/A	$3n$	$1/(3n)$	$2n$	$1/(2n)$

Take 4 secret images for an example. Fig. 4 gives the original secret images, 2 shares and 4 recovered secret images. '+' means the overlaying operation. From this experiment, it is obvious that any information about secret images can not be taken by share A and B separately. The recovered images can be seen clearly by overlapping share A and $R(B, i-1)$ ($1 \leq i \leq 4$). Therefore, the experimental results demonstrate that the scheme is feasible.

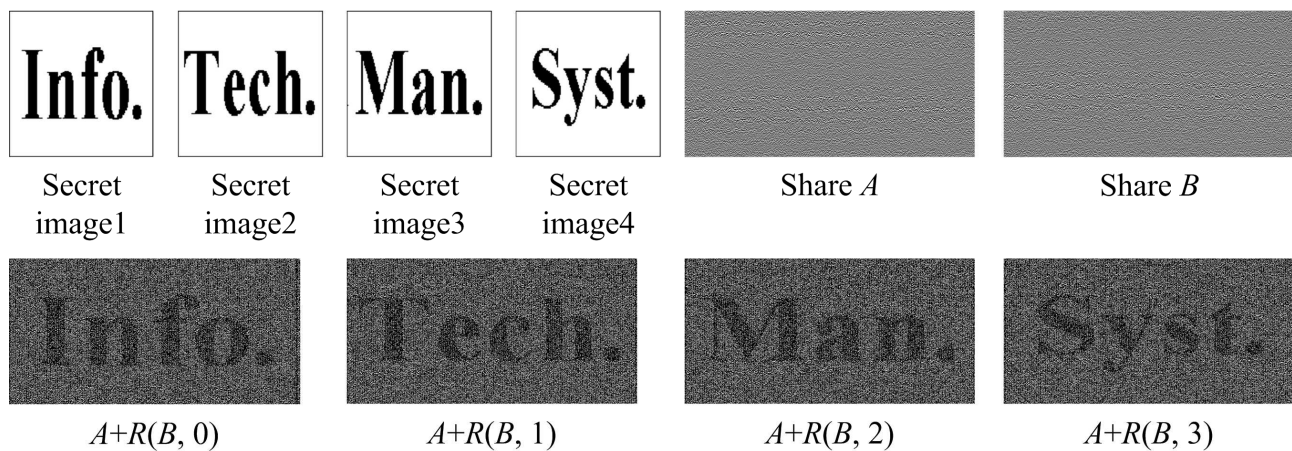


Fig. 4. The secret images, shares, and recovered secret images

Conclusion

A modified multi-secret visual cryptography scheme has been proposed in this paper, in which any amount of secret images is encoded into two ring shares. The scheme is based on $(2, 2)$ -VCS and marked areas, which are different from previous schemes. The novel design makes better visual effects, as well as perfect security. The scheme is only suit to two shares too, thus how to extend to (k, n) threshold scheme is our future work.

Acknowledgment

This work was supported in part by NSFC under Grant Nos. 61070086. The authors would like to thank the anonymous reviewers for their valuable comments.

References

- [1] A. Shamir, How to share a secret, Communications of the ACM, 22 (1979) 612-613.
- [2] G. R. Blakley, Safeguarding cryptographic keys, in: Proceedings of the National Computer Conference, NJ, USA, 1979, pp. 242-268.
- [3] M. Naor, A. Shamir, Visual cryptography, in: Advances in Cryptology-Eurocrypt'94, Berlin, 1995, pp. 1-12.
- [4] G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, Visual cryptography for general access structures, Information and Computation, 129 (1996) 86-106.
- [5] C. S. Hsu, S. F. Tu, Y. C. Hou, An optimization model for visual cryptography schemes with unexpanded shares, in: ISMIS2006, LNAI, Berlin, 2006, pp. 58-67.
- [6] L. G. Fang, B. Yu, Research on pixel expansion of $(2, n)$ visual threshold scheme, in: 1st International Symposium on Pervasive Computing and Applications Proceedings (SPCA06), Ningbo, 2006, pp. 856-860.
- [7] S. Lin, S. Chen, J. Lin, Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion, Journal of Visual Communication & Image Representation, 21 (2010) 900-916.
- [8] S. J. Shyu, M. C. Chen, Optimum Pixel Expansions for Threshold Visual Secret Sharing Schemes, IEEE Transactions on information forensics and security, 6 (2011) 960-969.
- [9] C. C. Lin, W. H. Tai, Visual cryptography for gray-level images by dithering techniques, Pattern Recognition Letters, 24 (2003) 349-358.
- [10] S. Cimato, R. De Prisco, A. De Santis, Optimal colored threshold visual cryptography schemes, Designs, Codes and Cryptography, 35 (2005) 311-335.
- [11] C. N. Yang, T. S. Chen, Colored visual cryptography scheme based on additive color mixing, Pattern Recognition, 41 (2008) 3114-3129.
- [12] F. Y. Ng, D. S. Wong, On the security of a visual cryptography scheme for color images, Pattern Recognition, 42 (2009) 929-940.
- [13] B. Yu, X. H. Xu, L. G. Fang, Multi-secret sharing threshold visual cryptography scheme, in: 2007 International Conference on Computational Intelligence and Security (CIS 2007), Harbin, 2007, pp. 815-818.
- [14] L. H. Chen, C. C. Wu, A study on visual cryptography, Master Thesis, National Chiao Tung University, Taiwan, 1998.

-
- [15]H. C. Wu, C. C. Chang, Sharing visual multi-secrets using circle shares, *Computer Standards & Interfaces*, 28 (2005) 123-135.
 - [16]J. S. Shyong, S. Y. Huang, Y. K. Lee and R. Z. Wang, Sharing multiple secrets in visual cryptography, *Pattern Recognition*, 40 (2007) 3633-3651.
 - [17]H. C. Hsu, T. S. Chen, Y. H. Lin, 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*, Taipei, Taiwan, 2004, pp. 996-1001.
 - [18]J. B. Feng, H. C. Wub, C. S. Tsaic, Visual secret sharing for multiple secrets, *Pattern Recognition*, 41 (2008) 3572-3581.