IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Secret Sharing Using Visual Cryptography Based on Reversed Images

Mrs.C.Banumathi[*1], Ms.A.AGNES PEARLY.[2]

[*1] Department of Electronics & Communication Engineering, Bharat University, Selaiyur, Chennai-600073, Tamilnadu, India

[2] Department of Electronics & Communication Engineering, IGCET, Chengalpattu, Athur Post 603101, Tamilnadu, India

vinusujana84@gmail.com

Abstract

Visual Cryptography is a new cryptographic technique which allows Visual information (e.g. printed text, picture) to be encrypted in such a way that their decryption can be performed by the human visual system, without any complex cryptographic algorithms. A novel secret sharing scheme using visual cryptography by reversing secret images is proposed in this paper. In generating the shares for the multiple images, the correlative matrices are designed to encode them into two ring shares. Different from conventional visual cryptography, the proposed scheme has no restriction on the number of secret images and has obviously improved the pixel expansion and the relative difference.

Keywords: Visual cryptography; reversing; correlative matrices; pixel expansion

Introduction

With the rapid development of computer and communication technology, more and more secret information are transmitted through the Internet. While using secret images, security issues should be taken into consideration because anyone may tend to intrude the system. One approach to have the essential information secure not retrieved by malicious users easily is making the essential information shared among several participants. Secret sharing schemes proposed by Shamir[1] and Blakley[2] in 1979, are to distribute secret information to participants. The secret can only be obtained by the cooperation of these participants. The ordinary concept of secret sharing is sharing the secret key, and secret sharing schemes are also widely used for secret transmission nowadays.

Using the basic theory of secret sharing, Naor and Shamir introduced the technology of visual cryptography (VC) in EUROCRYPT'94.[3] Visual cryptographic scheme (VCS), for a set P of n participants, is a cryptographic technique that enables us to divide a secret image into n shadow images called shares, where each participant in P receives one share. Certain qualified subsets of participants can “visually ” recover the secret image with some loss of contrast, but other forbidden subsets of participants have no information about the secret image. Neither computational devices nor cryptographic knowledge is required for the decryption process.

Since this pioneer research, many theoretical results on the construction or contrast (the relative difference between the reconstructed white and black pixels in the superimposed image) of VCS for general access structures have been proposed in the literature [4-6]. Yu and Fang[7-10] focused on the parameters optimizing of (2, n) VCS and gave two new schemes. The scheme based on combination makes its pixel expansion best and the scheme based on permutation can balance performance between pixel expansion and contrast. Hou[11] proposed a VCS for color images based on color-decomposing and half-toning.

In addition, Chen et al.[12] proposed a scheme to make the decryption result significant only at a desired stacking angle. But all of the above schemes aim to deal with only one secret image. This is very important in some applications where users want to share several images at the same time. In such a situation, the traditional visual cryptography scheme will not live up to the requirement because the number of secret images is restricted or the performance of recovered images is not good. In [13] and [14] the authors designed circular shares to overcome the angle’s constraint. Hsu et al.[15] proposed a scheme to encrypt two images into two ring shares with arbitrary angle. In order to increase the number of secret images, Feng et al.[16] present another scheme using four kinds of visual patterns. However, the pixel expansion of the scheme is $3n$,

which could be improved for better visual effects of the reconstructed images.

In this paper, the proposed multi-secret visual cryptography technique will apply area marks and reversed images to hide multiple secret images on the cylindrical surfaces of two shares. The secret images can be recovered easily by stacking rotated share *A* and share *B*.

The rest of this paper is organized as follows. In section 2 the basic model VCS and some basic definitions on our scheme are given. As the main part of this paper, Section 3 designs the multi-secret sharing and recovering procedures, and discusses the effectiveness of the scheme. Thereafter, the parameters analysis and experimental results would appear in Section 4. Finally, the Conclusions and future works are provided in the last section.

Preliminaries

The basic concept of visual cryptography is introduced in Section A and some basic definitions are given in Section B.

A. Basic (2,2) VC Scheme

In the (2, 2) VC scheme each secret image is divided into two shares such that no information can be reconstructed from any single share. The decryption process is performed by stacking the two shares and the secret image can be visualized by naked eye without any complex computations.

Here each pixel 'p' of the secret image is encrypted into a pair of sub pixels in each of the two shares. If 'p' is white, one of the two columns under the white pixel in Fig. 1 is selected. If p is black, one of the two columns under the black pixel is selected. In each case, the selection is performed randomly such that each column has 50% probability to be chosen. Then, the first two pairs of sub pixels in the selected column are assigned to share 1 and share 2, respectively. Since, in each share, p is encrypted into a black–white or white–black pair of sub pixels, an individual share gives no clue about the secret image. By stacking the two shares as shown in the last row of Fig. 1, if 'p' is white it always outputs one black and one white sub pixel, irrespective of which column of the sub pixel pairs is chosen during encryption. If 'p' is black, it outputs two black sub pixels. Hence there is a contrast loss in the reconstructed image.

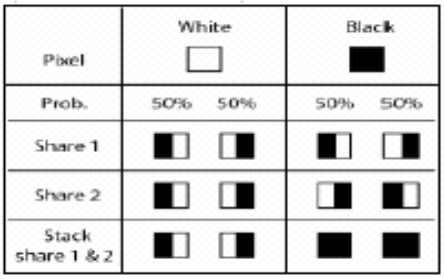


Fig.1 Construction of (2,2) VC Scheme

The important parameters of this scheme are

a) Pixel expansion 'm', which refers to the number of pixels in a share used to encrypt a pixel of the secret image. This implies loss of resolution in the reconstructed image.

b) Contrast '_', which is the relative difference between black and white pixels in the reconstructed image. This implies the quality of the reconstructed image.

B. Basic Definitions

Since the design of our scheme is different from the previous ones, some basic definitions related to the scheme are introduced. Suppose the dealer wants to share n secret images $S0, S1, \ldots, Sn\text{-}1$, with the size of $X \times Y$ ($Y \bmod 2n \equiv 0$).

Definition 1(Reversed Image): All the white pixels of the image are reversed into black pixels and all the black pixels are reversed into white pixels. $S_n = S0'$, $S_{n+1} = S1'$, …, $S_{2n-1} = S_{n-1}'$.

The basis unit of shares is sub-pixel block, denoted by a $2 \times n$ Boolean matrix. Each block corresponds to $2n$ secret image pixels, which consist of one pixel in every secret images and reversed images. Share A and B are both constituted of $X \times Y$ blocks of sub-pixels, hence the size of share $A(B)$ is $2X \times nY$. The index of sub-pixels in the block is shown in Fig 2.

Fig. 2 The index of a sub-pixel block

Definition 2(Marked Areas): Two shares and all secret images are divided into $2n$ areas averagely as Fig.3. A^k, B^k and $S^k{}_u$ denote the k-th areas respectively ($0 \le k \le 2n\text{-}1, 0 \le u \le 2n\text{-}1$). Therefore, $A = (A^0, A^1, \ldots, A^{2n-1})$, $B = (B^0, B^1, \ldots, B^{2n-1})$ and $S_u = (S^0{}_u, S^1{}_u, \ldots, S^{2n-1}{}_u)$.

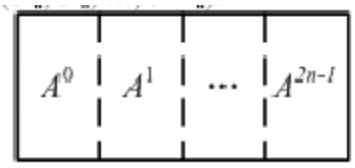


Fig.3 Share A is divide into $2n$ areas averagely

Definition 3 (Ring Shift Left Function): R (A,c) is a ring shift left function. It means that share A is ring shifted left c areas. $R(A,c) = (A^c, A^{(c+1) \bmod 2n}, \ldots, A^{(2n-1+c) \bmod 2n})$, $0 < c < 2n-1$.

Definition 4 (Correlative matrices): Suppose $A^k ij(B^k ij)$ is the i-th row j-th column block($2\times n$ boolean matrix) in the kth area of share $A(B)$ ($0 \le k \le 2n-1$, $0 \le i \le X-1$, $0 \le j \le Y/2n-1$). $RA_{ij}=\{A^k_{ij} \mid 0 \le k \le 2n-1\}$ and $RB_{ij}=\{B^k_{ij} \mid 0 \le k \le 2n-1\}$ are correlative matrices of share A and B.

Generally, "0" means white pixel in secret images and shares, while "1" means black pixel. In our scheme, there are "0" and 2n-1 "1" in each sub-pixel block of share A, and n "0" and n "1" in share B.

Definition 5 (Position Vector): Suppose RA_{ij} is correlative-matrices of share A. The positions of "0" in each matrix of RA_{ij} compose a vector $D = (d_0, d_1, \ldots, d_{2n-1})$ called Position Vector ($0 \le d_i \ne d_j \le 2n-1$, $0 \le i \ne j \le 2n-1$).

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 reversed image. The secret images can be recovered easily by stacking rotated share A and share B.

1. Sharing and recovering process of the proposed scheme

In this scheme, the secret images have to be preprocessed by extending the width of images to satisfy $Y \bmod 2n \equiv 0$. In the sharing process, a position vector is generated firstly, and then correlative-matrices RA_{ij} and RB_{ij} are constructed at the same time in one step. The specific multi-secret sharing algorithm is as follow.

Multi-secret Sharing Algorithm

Input: Secret images $S0, S1, \ldots, Sn-1$

Output: Two shares A and B

Step 1: Adjust the size of all secret images to $X \times Y$, $Y \bmod 2n \equiv 0$.

Step 2: Generate reserved secret images $S_n=S_0'$, $S_{n+1}=S_1'$,…, $S_{2n-1}=S_{n-1}'$.

Step 3: Divide share A and B into $2n$ areas averagely.$A=(A_0, A_1, \ldots, A_{2n-1})$, $B=(B_0, B_1, \ldots, B_{2n-1})$.

Step 4: Divide A^k and B^k into $X \times Y/2n$ blocks A^k_{ij} (B^k_{ij}), $0 \le k \le 2n-1$, $0 \le i \le X-1$, $0 \le j \le Y/2n-1$.

Step 5: Generate $(r_0, r_1, \ldots, r_{2n-1})$ as a random permutation of $(0, 1, \ldots, 2n-1)$ for Position Vector. Construct correlative matrices RA_{ij} and RB_{ij} with $i=0$ and $j=0$.

Step 5.1 Construct RA_{ij}.

$A^k_{ij}(q)=0$, if $q=r_k$, $0 \le k \le 2n-1$, $0 \le q \le 2n-1$.

$A^k_{ij}(q)=1$, if $q \ne r_k$, $0 \le k \le 2n-1$, $0 \le q \le 2n-1$.

Step 5.2 Construct RB_{ij}.

$B^k_{ij}(r_q) = S^k_{(q-k) \bmod 2n}(i, j)$, $0 \le k \le 2n-1$, $0 \le q \le 2n-1$.

Step 6: If $j < Y/2n$, return to Step 5 for the next pixel with $j=j+1$.

Step 7: If $i<X$, return to Step 4 for the next row with $i=i+1$.

Step 8: Out put the shares A and B.

For the recovering process, the two shares will be rolled up to become rings so that it is easy to rotate the share at any desired angle as shown in Fig.4. With share B in a stationary position, share A is rotated at angle u. $360°/(2\ n)$ to reveal secret image S_u.

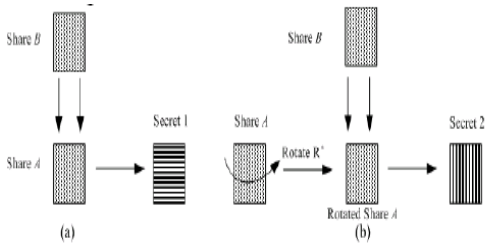


Fig.4 The Decryption Process

In order to understand the scheme, a simple example is shown in Fig. 5. $S_0=\{0,1,1,1\}$ and $S_1=\{1,0,1,1\}$ are two secret images. $S_2=\{1,0,0,0\}$ and $S_3=\{0,1,0,0\}$ are reserved of S_0 and S_1. Random permutation (1,0,3,2) for position vector.

Shares and recovered secret images are shown as follow.

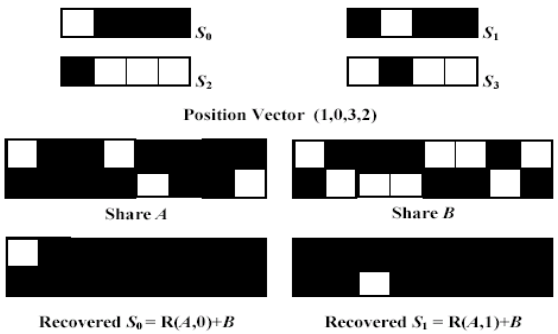


Fig.5 A simple example of the scheme

2. Effectiveness verification

The security and contrast are two aspects of the effectiveness of visual cryptography scheme. The first one means that a single share leaks nothing about secret information. And the second one means

the secret images can be recognized by stacking two shares. They will be discussed respectively.

Theorem 6 (Security). Any information cannot be taken from a single share.

Proof. Each block in share *A* is composed of a white subpixel and 2*n*-1 black ones, while each block in share *B* is composed of *n* white sub-pixels and *n* black ones. Furthermore, the order of the sub-pixels in area is decided by random permutation. If an adversary takes only one share, as well as knowing the size and the number (2*n* and *X*×*Y*) of the blocks and the interrelation of block's subpixels, nothing happened for the knowledge of the other share to get the whole picture of the original secret images. To see the security of our scheme, each share has a size of *X*×*Y* blocks; the block size is 2x*Y*, the num of secret images is *n*. Thus, the best guessed-work is $((2n)!/n!)^{-XY/n}$, which is telling a probability of hit rate better than nothing. Thus our scheme is very secure, and any information can not be taken from a single share.

Lemma 7. If share *A* is not rotated at correct angle, the expectation of the block's Hamming weight is equal to (4*n*-1)/2 after overlapping rotated *A* and *B*.

Proof. As a result of using of the reserved images, the block of share B is composed of *n* white sub-pixels and *n* black ones, and the probability of that the *i*th sub-pixel in the block is white is equal to the probability of it is black. If share *A*(a white sub-pixel and 2*n*-1 black sub-pixels) is not rotated at correct angle, the sub-pixel in share B at the position, where the sub-pixel in share A is white, is black or white with the same probability 1/2. So the Hamming weight of the block is 2n-1+1/2 = (4*n*-1)/2, after stacking rotated share *A* and share *B*. And any information can not be taken from the stacked shares.

Theorem 8 (Contrast). The secret image S_u can be decrypted by overlapping share *R*(*A*, *u*) and *B*.

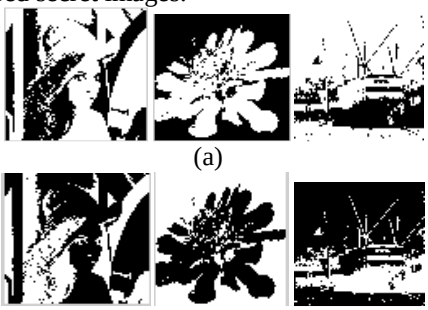
Proof. Let *w*(0, *k*) (*w*(1, *k*)) denotes the Hamming weight of the *k*-th block corresponding to the white (black) pixel of *Su* after stacking *R*(*A*, *u*) and *B*. For the block of share *A* is composed of a white sub-pixel and 2*n*-1 black ones, the key problem is the pixel of share *B* in the corresponding position where the pixel of share *A* is white. From the sharing process, when the pixel in S_u is white, the pixel of share *B* in the corresponding position is white, that is *w*(0, *k*) = 2*n*-1. And so on, we can get *w*(1, *k*) = 2*n*.

Since *w*(1, *k*) - *w*(0, *k*)=1, the blackness expectation of blocks corresponding to black pixels in S_u is bigger than the white ones after stacking shares. In conclusion, *Su* can be recovered by share *R*(*A*, *u*) and *B*.

Experimental Results and Analysis

In this subsection, we present some experimental results to illustrate the performance of our scheme. For simulation we have used Matlab 7.0 tool. In visual cryptography, the pixel expansion and the relative difference are two main parameters. The small pixel expansion means the small share size, while the big relative difference means the satisfied recovering effect. In our scheme, the size of sub-pixel block is 2*n*, and the Hamming weight difference between original white and black pixels is 1. Therefore, the pixel expansion is 2*n* and the relative difference is 1/(2*n*).

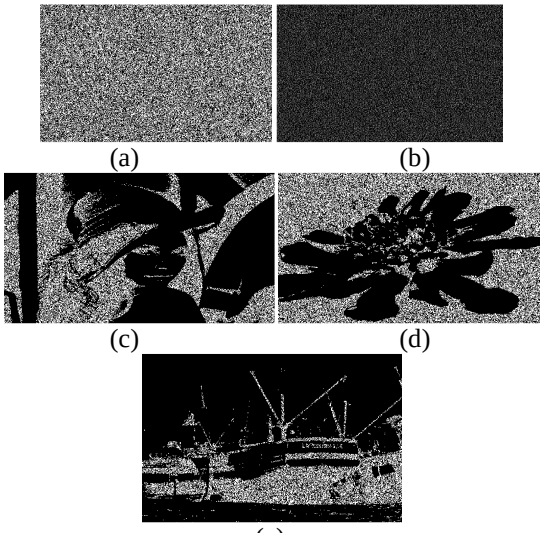
Take 3 secret images for an example. Fig. 6 gives the original secret images and the reversed secret images, while Fig. 7 shows 2 shares and 3 recovered secret images.



(a)

(b)

Fig. 6 Original secret images (a) and Reversed images (b)



(a) (b)

(c) (d)

(e)

Fig.7 (a) share A, (b) share B, (c)-(e) 3 recovered secret images

From this experiment, it is obvious that share *A* and *B* are both meaningless. Meanwhile, the recovered images can be seen by overlapping share *R*(*A*, *u*) and *B*. In the sharing process, reserved images are used to enhance security of the scheme. If revesed images are not used, share *B* will show

information about the secret images Therefore, the effectiveness of the scheme is demonstrated by the experimental results.

Conclusion

Visual cryptography is the current area of research where lots of scope exists. In this paper, a secret sharing visual cryptography scheme with reversed images has been proposed. The scheme is based on reversed secret images, correlative matrices and marked areas, which are different from previous ones. Since the novel design, the proposed scheme has the advantage of making the number of secret images unlimited and having obviously improved the pixel expansion and the relative difference. Future work is on the other area of visual cryptography where no satisfactory results yet achieved for color visual cryptography.

References

[1] Shamir. How to share a secret. Communications of the ACM, 1979, 22(11): 612-613.

[2] G. R. Blakley. Safeguarding cryptographic keys. Proceedings of the National Computer Conference, NJ, USA, 1979, 48: 242-268.

[3] M. Naor, A. Shamir. Visual cryptography. Advances in Cryptology-Eurocrypt'94, Berlin, 1995, LNCS 950: 1-12.

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

[5] Giuseppe Ateniese, CCarlo Blundo ,CAlfredo De Santis, CDouglas R. Stinson. Extended capabilities for visual cryptography. Theoretical Computer Science,143-161.2001.

[6] S. Droste. New results on visual cryptography. Advances in Cryptology-Eurocrypt'96, Lecture Notes in Computer Science. vol.1109, Springer-Verlag, Berlin, pp.401-415.1996.

[7] Fang Liguo. Research on optimizing parameters and aspect variant of visual cryptography. Institute of Electronic Technology Information Engineering University (In Chinese). Master's Thesis 2006.

[8] Fang Liguo, Yu Bin. A (2, n) visual threshold scheme based on permutation. Computer Engineering (In Chinese), 2007.33 (9): 157-159.

[9] Fang Liguo, Yu Bin. A (2, n) visual threshold scheme of best pixel expansion. Journal of Institute of Electronic Technology (In Chinese).2006.18 (7):11-15.

[10] Yu Bin, Fang Liguo. Research on aspect ratio invariant visual threshold schemes. Computer Engineering and Design (In Chinese). 2006, 27(11):1998-1999.

[11] Young-Chang Hou C Shu-Fen Tu. A visual cryptographic technique for chromatic images using multi-pixel encoding method. Journal of Research and Practice in Information Technology. 2005.

[12] L. H. Chen, C. C. Wu. A study on visual cryptography. [Master Thesis], National Chiao Tung University, Taiwan, 1998.

[13] H. C. Wu, C. C. Chang, Sharing visual multi-secrets using circle shares, Computer Standards & Interfaces, 28: 123–135, 2005.

[14] J. S. Shyong, S. Y. Huang, Y. K. Lee and R. Z. Wang. Sharing multiple secrets in visual cryptography, Pattern Recognition. 2007.

[15] 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. Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan, 2004: 996-1001.

[16] J. B. Feng, H. C. Wub, C. S. Tsaic, et al.. Visual secret sharing for multiple secrets. Pattern Recognition, 2008, 41(12): 3572-3581.