Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (3): 435-441, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.435.441

Seeing and Believing is a Threat: A Visual Cryptography Schemes

Rengarajan Amirtharajan, Sumaiya Sulthana and J.B.B. Rayappan
Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613 401, India

Corresponding Author: Rengarajan Amirtharajan, Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613 401, India

ABSTRACT

Visual cryptography is the latest means of cryptography modes that takes in the human's natural vision to decrypt the image without any tedious processes involved. This technique has the methods of setting information in a haphazard manner which get properly distinguishable to the human eye only when they are superimposed. In this study, three such visual cryptographic schemes are analysed with proper illustrations, advantages and disadvantages. So, the banalities of various secret sharing are (k, n) scheme, pixel rotation, share rotations are analysed and the results are presented. These methods improvise information as well a security than the regular schemes.

Key words: Visual cryptography, (k,n) shamir VC, share rotations, pixel rotations

INTRODUCTION

Pace of development of network technology has helped the man in sending and receiving any digital data over the Internet and on the GO. The Information security places a very vital role in providing the safer path for the data between two users without the third's intervention and a one of the ways is by image secret sharing. Even though Cryptography (Schneier, 2007) and image steganography is the good candidates, where, the former needs special decryption device and the latter never reveals its presence.

In the conventional cryptography techniques, the problems being the image been seen by the intruders is solved by many effective algorithms. However, still the decryption of the encrypted cipher text need strict computations making it a costly and lesser effective of the hardware/software for the decoding has direct proportions to the security algorithm, hence making the relation of security and cost/efficiency directly proportional.

To tackle the above problems, Noar and Shamir (1995) found visual cryptography, which deals the humans vision ability in the decryption process (Wu and Chen, 1998). The secret is differentiated (broken into parts called shares) and when seen individually reveals nothing (Lukac and Plataniotis, 2005) but when the transparencies, i.e., shares are integrated; the original secret message is visible to human visual system.

The Visual cryptography which merely makes use of human insight is much useful in scenarios where neither computational devices, nor cryptographic knowledge is not available or usage is impossible. This particular attribute of Visual Cryptography, rules over all other cryptographic techniques for sharing secret images securely.

There are many works available in the literature for binary image (Noar and Shamir, 1995) secret sharing, gray image (Lin and Tsai, 2003) as secret or even to colour images (Hou, 2003; Leung *et al*., 2009). Visual cryptography is available for different purposes like secret image sharing (Shyu *et al*., 2007), authentication (Chen *et al*., 2012), visual digital signature scheme (Jaafar and Samsudin, 2013), Cheat immune and traceable visual cryptography scheme (Yuan *et al*., 2012) and copyright protection (Chen *et al*., 2009) like watermarking (Jin and Kim, 2012).

After carefully reviewing the available literature, this study has been suggested to know about Visual cryptography and its variants for sharing single secret to multiple users and multiple secret to multiple users in binary and gray level images.

LITERATURE REVIEW

(k, n)-Threshold scheme: For the n receivers the secret image is divided to n shares by the famous k,n-threshold procedure. The shares contain only an nth portion of the complete image and when combined, the complete picture i.e., secret image appears. A simple schematic diagram has been illustrated in Fig. 1, its the method from Lukac and Plataniotis (2005), Firstly, by the process of half toning (dithering), the, input image gets converted as binary form having spatial coordinates x and y whose range is from 1, 2, up to K1 and 1, 2, up to K2, respectively. Then the image is shared. The original pixel r(x, y) (1 for white, 0 for black) is expanded to a set of smaller pixels (m1×m2) through a function for encryption to yield shares of the n receivers. As the spatial arrangement deviates for each block useful data is not unveiled until and unless an access to the predefined number of shares has been obtained.

A reference pixel r (i, j) sited at (i, j) (of original image) is mapped into blocks of size m1×m2 by an encrypting function, say, fe(.). For illustration, let us consider a block of 2×2 for 2, 2 routine:

$$S1 = [S'_{(2i,\,1,\,2j-1)},\ S'_{(2i,\,1,\,2j)},S'_{(2i,\,2j-1)}\ S'_{(2i,\,2j)}] \text{ in share S1 and}$$

$$S2 = [S''_{(2i,\,1,\,2j-1)},\ S''_{(2i,\,1,\,2j)},S''_{(2i,\,2j-1)}\ S''_{(2i,\,2j)}] \text{ in share S2}$$

The encryption procedure is as follows:

$$f_e\,(r(i,j)) = \begin{cases} [s1,s2]^T \in C0 \text{for } r(i,j) = 0 \\ [s1,s2]^T \in C1 \text{ for } r(i,j) = 1 \end{cases}$$

The sets:

$$C_0 = \left\{ \begin{bmatrix} 0,1,0,1 \\ 1,0,1,0 \end{bmatrix}, \begin{bmatrix} 1,0,1,0 \\ 0,1,0,1 \end{bmatrix}, \begin{bmatrix} 0,0,1,1 \\ 1,1,0,0 \end{bmatrix} \right.$$
$$\left. \begin{bmatrix} 1,1,0,0 \\ 0,0,1,1 \end{bmatrix}, \begin{bmatrix} 1,0,0,1 \\ 0,1,1,0 \end{bmatrix}, \begin{bmatrix} 0,1,1,0 \\ 1,0,0,1 \end{bmatrix} \right\}$$

and

$$C_1 = \left\{ \begin{bmatrix} 0,1,0,1 \\ 0,1,0,1 \end{bmatrix}, \begin{bmatrix} 1,0,1,0 \\ 1,0,1,0 \end{bmatrix}, \begin{bmatrix} 0,0,1,1 \\ 0,0,1,1 \end{bmatrix} \right.$$
$$\left. \begin{bmatrix} 1,1,0,0 \\ 1,1,0,0 \end{bmatrix}, \begin{bmatrix} 1,0,0,1 \\ 1,0,0,1 \end{bmatrix}, \begin{bmatrix} 0,1,1,0 \\ 0,1,1,0 \end{bmatrix} \right\}$$

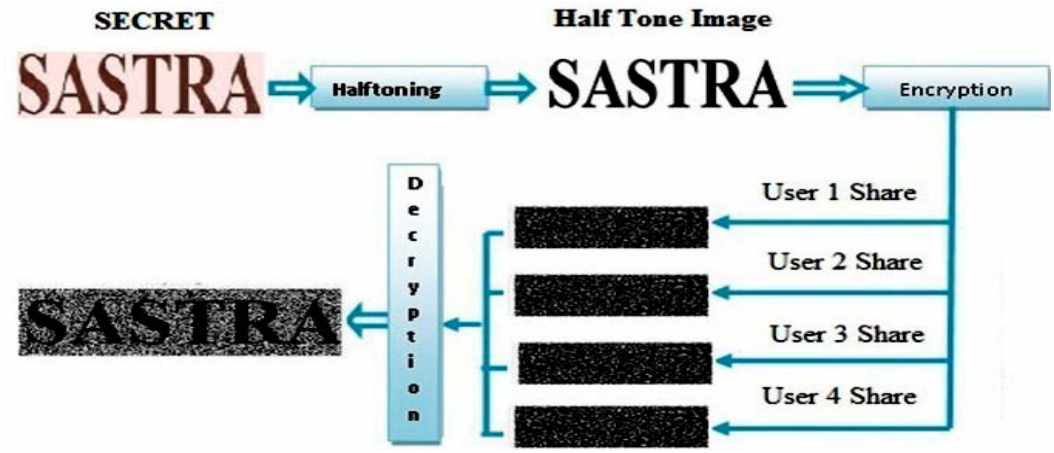

Fig. 1: Visual cryptography schema

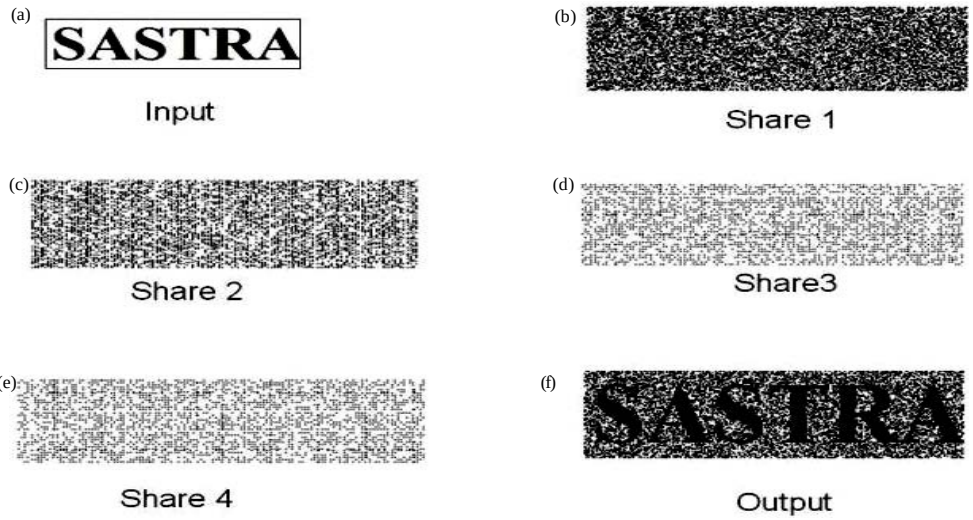

Fig. 2(a-f): A sample result-modified (k, n) threshold scheme for 4 users, (a) Input, (b) Share 1, (c)Share 2, (d) Share 3, (e) Share 4 and (f) Output

The entire matrices from the column permutation of basis matrices $n \times m_1 m_2$ are taken into account:

$$A_0 = \begin{bmatrix} 0101 \\ 1010 \end{bmatrix} \text{ and } A_1 = \begin{bmatrix} 0101 \\ 0101 \end{bmatrix}$$

Some sample results are presented in Fig. 2 for 4 such users.

Spreading factor m1, m2 decides the matrices' dimension in addition to n ($n \times m_1 m_2$) gives the participants' number. How much a share is big when compared to the (original) image is also based on this spreading factor. Hence, m1, m2 must be as small as possible for optimum functioning. If the secret pixel is white it may belong to set C1 and else if it is black then the S1, S2 must be chosen

from set C0. Random number generator is employed for the choice. Intended for this 2, 2 plots, all pixels in both S1 and S2 are tantamount if secret pixel is white and S1 should be complement of that in S2 if the pixel is black.

Decryption is done by a simple process of stacking these shares. The original secret image can be viewed by human visual ability, without the need of any complex computations. This study reveals four steps: half toning, encrypting and decrypting.

Advantages:

- The (N, N) visual cryptography scheme encrypts a digital data or image into number of shares, that is, if there are N participants, then the secret can be revealed only when all the N participants stack their shares. Non-availability of even one share does not reveal the secret image or data. Hence, maintains a very high degree of security
- The computation process at the receiver is almost absent except for the stacking of the shares, which immediately reveals the secret input. Hence, is more computational efficient than other cryptographic techniques

Drawback:

- The main limitation of (k, n) cryptography is that only one message or data is split into n shares, which is not economical than other cryptographic techniques. Hence, developed sharing multiple secrets in visual cryptography by Shyu *et al.* (2007)

MATERIALS AND METHODS

Method 1- Pixel rotation: Wu and Chen took up the problem of two image sharing using visual cryptography and concealed the binary images which are secretive into two stochastic shares, S1 and S2, respectively where if the two shares are stacked, designated as, S1*S2, secret 1 is revealed and secret 2 is got by $S1^{\theta}$*S2 (Here*signifies superimposition function and $^{\theta}$ is nothing but anti clockwise rotation).

Here, both S1 plus S2 are of same size and are of square shape. For the alignment of the post encoding, pixels ought to be on S1*S2 and $S1^{\theta}$*S2 as well; $^{\theta}$can take any value of 90, 180 or 270. Consider two M×M secret (square) binary images, say, P1 and P2, the above connive outputs shares (S1, S2)and they don't convey anything with reference to P1 or P2 on an individual basis. But if they are placed one over the other, P1 becomes visual and when stacking $S1^{\theta}$ and S2, P2 ($S1^{\theta}$ is got by rotating $S1^{90^{\circ}}$ in the Anti-clock direction) is viewed.

Methodology

Encryption:

- **Step 1:** Consider two (square) binary secluded images P1, P2 of size N×N
- **Step 2:** Compare every pixel of the secret images P1 and P2
- **Step 3:** By traditional means, make the blocks s1 and s2
- **Step 4:** For replication of the pixels, generate s1' by rotating s1 to 90 degree in anti-clock direction
- **Step 5:** Outline the shares S1, S2, $S1^{90^{\circ}}$ using s1, s2, s1, blocks, respectively

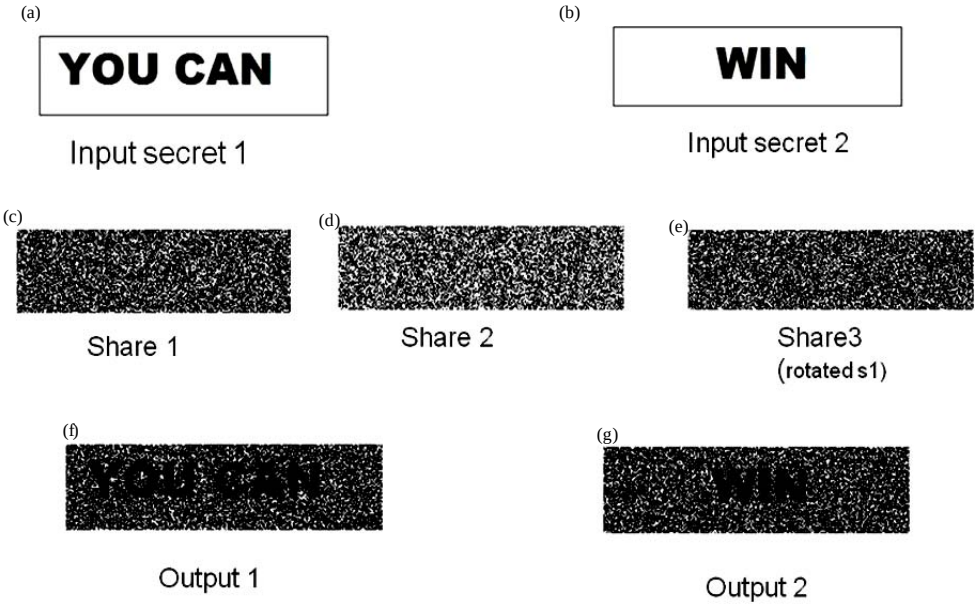

Fig. 3(a-g): Sample results two secret and three shares (a) Input secret 1, (b) Input secret 2, (c)Share 1, (d) Share 2, (e) Share 3, (f) Output 1 and (g) Output 2

Decryption:

- **Step 1:** Stack S1 and S2 for the first P1 secret image
- **Step 2:** Stack $S1^{90^\circ}$ and S2 for the P2

Some of the sample results are given in Fig. 3 is given below:

Advantages:

- Both the images can be sent securely to the receiver through only 3 parts (S1, S2, $S1^{\theta}$)
- Further enhanced security, as the exact combinations must have to known for the revealing part
- Can be extended for Multi secret transmission

Drawback:

- The rotated share (which is just formed by the pixel rotation of a pre formed share) must also be transmitted
- This can be overcome by the following method where the number of shares, for multiple secrets is reduced hence increasing the efficiency

Method 2-share rotation: In this method, the transmitted share is rotated at different angles for the revealing process. Taken three images needs to be transmitted, during the first step of encoding process the share A and a temporary share (i.e., temp share) are created out of secret images and as the second step shares B and C are generated from the temp share. Therefore, shares A, B and C are transmitted. For the process of decoding, once the three shares are received, the shares B and

C are ORed to create the temp share, while the first secret image can be viewed by stacking the share A and temp share. Here the second can be obtained by stacking, the clockwise 90° rotation of the share A and share temp. The third is got anticlockwise 90° of the share A and temp share.

Methodology:

- **Step 1:** Take three (N×N) square binary secret images P1, P2, P3
- **Step 2:** Compare all of the covert images' corresponding pixels
- **Step 3:** By the traditional method, generate the blocks SA and Stemp
- **Step 4:** Create share A such that each of its block is selected randomly from the patterns having only one black and three white pixels
- **Step 5:** From the created share temp, generate shares B and C randomly such that the logical OR operation of B and C produces share temp
- **Step 6:** Transmit shares A, B and C

Decryption:

- **Step 1:** Choose the correct shares, B and C from the transmitted three shares
- **Step 2:** To decrypt the share temp, perform logical OR operation between the shares B and C
- **Step 3:** To obtain the first secret image P1, stack share A and share temp
- **Step 4:** To obtain the second secret image P2, rotate share A clockwise 90° and stack with share temp
- **Step 5:** To obtain the third secret image P3, rotate share A counter clockwise 90° and stack with share temp

Advantages:

- Receiver must know the logic operation for the intermediate share
- The angle of rotation must also be known
- Knowledge of key share is vital
- Reduction in the number of shares makes this method as an efficient one

Some sample results are given in Fig. 4.

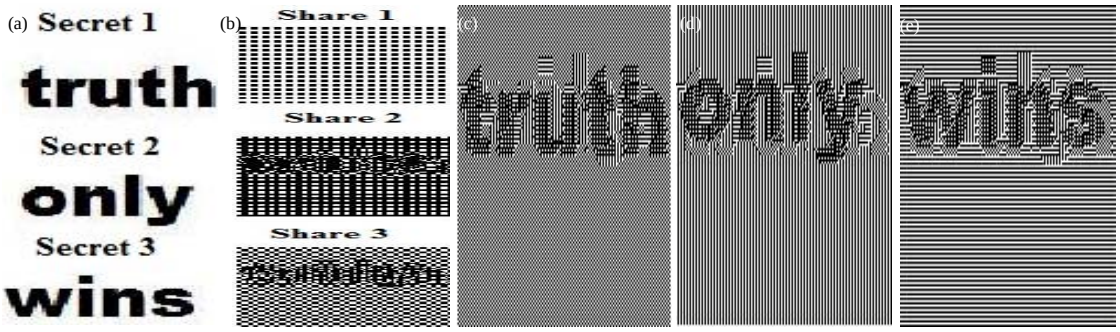

Fig. 4(a-e): (a) Three individual user secret inputs, (b) Three individual user shares (c) User 1 output (d) User 2 output and (e) User 3 output

Applications: Multiple secret sharing schemes can have plethora of applications. For example, three shareholders of the World Bank contain separate key containing random information. When the prime member of the groups combines his shares with one of the member, the secret image is known. But this is nothing for Second and third, which is actually the original password for the member 1. Hence, all the transactions/ processing must happen only with the Prime Member of the World Bank.

CONCLUSION

When compared to the conventional method which is used for only single secret image transmission, this provides a much better way of transmission as it supports multiple secrets. Here, though the channel is insecure the internal security fights every threat on it. The multiple secret image sharing has applications for which the world is still to explore and get the full benefit of it.

REFERENCES

Chen, T. H., C.C. Chang, C.S. Wu and D.C. Lou, 2009. On the security of a copyright protection scheme based on visual cryptography. Comput. Standards Interfaces, 31: 1-5.

Chen, Y.C., D.S. Tsai and G. Horng, 2012. A new authentication based cheating prevention scheme in Naor-Shamir's visual cryptography. J. Visual Commun. Image Representation, 23: 1225-1233.

Hou, Y.C., 2003. Visual cryptography for color images. Pattern Recognit., 36: 1619-1629.

Jaafar, A. and A. Samsudin, 2013. An improved version of the visual digital signature scheme. Int. Arab J. Inform. Technol., Vol. 10.

Jin, X. and J. Kim, 2012. A Secure Image Watermarking Using Visual Cryptography. In: Computer Science and its Applications, Yeo, S.S., Y. Pan, Y.S. Lee and H.B. Chang (Eds.). Springer, Netherlands, pp: 179-187.

Leung, B.W., F.Y. Ng and D.S. Wong, 2009. On the security of a visual cryptography scheme for color images. Pattern Recognit., 42: 929-940.

Lin, C.C. and W.H. Tsai, 2003. Visual cryptography for gray-level images by dithering techniques. Pattern Recognit. Lett., 24: 349-358.

Lukac, R. and K.N. Plataniotis, 2005. Bit-level based secret sharing for image encryption. Pattern Recognit., 38: 767-772.

Noar, M. and A. Shamir, 1995. Visual Cryptography. In: Advance in Cryptography, DeSantis, A. (Ed.). Springer, Netherlands, pp: 1-12.

Schneier, B., 2007. Applied Cryptography: Protocols, Algorithm and Source Code in C. 2nd Edn., Wiley, India.

Shyu, S.J., S.Y. Huang, Y.K. Lee, R.Z. Wang and K. Chen, 2007. Sharing multiple secrets in visual cryptography Pattern Recognit., 40: 3633-3651.

Wu, C.C. and L.H. Chen, 1998. A study on visual cryptography. Master Thesis, National Chiao Tung University, Taiwan, R.O.C.,

Yuan, Z.L., G.S. Xia, J.Q. Liu and Z. Han, 2012. Cheat immune and traceable visual cryptography scheme. Int. J. Digital Content Technol. Appl., 6: 226-237.