RESEARCH ARTICLE OPEN ACCESS

Color Secret Image Encryption and Share Generation for Multiple-Secret Threshold Visual Cryptography

P. Kavipriya M.E[1], Dr. M. Sangeetha [2]

[1]Student, Department of Computer Science and Engineering, Coimbatore Institute of Technology, Coimbatore, Tamil Nadu -641014

[2] Assistant Professor (sr.gr),Department of Computer Science and Engineering, Coimbatore Institute of Technology, Coimbatore, Tamil Nadu -641014

ABSTRACT

Visual Cryptography Scheme (VCS) is a type of secret sharing scheme which allows the encoding of a secret image into n shares that distributed to n participants. Each share constitutes some information and when k shares out of n stack together the secret will reveal. However; less than k shares are not work. The advantage of the visual secret sharing scheme is its decryption process i.e. to decrypt the secret using Human Visual System without any computation. Traditional Visual Cryptography suffers from share identification problem. This problem can be solved by Multiple-Secret threshold visual cryptography (MVCS), which adds a meaningful cover image in each share. The proposed work presents threshold Visual cryptographic schemes in Color Images. This method uses half toning method to provide color image as a secret image. Then the secret image can be embedded in the original image by generating shares using Zigzags scanning method. Experimental result of proposed system provides robust security than conventional visual cryptographic schemes.

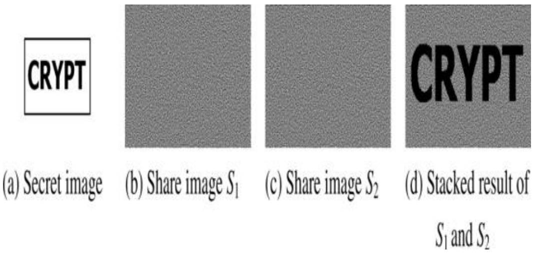
Keywords – Visual cryptography, Halftoning,Zig-Zag scanning.

I. INTRODUCTION

With the rapid evolution of communication technologies and computer networks, huge extents of digital data have been transmitted over the internet. However, transmission of secret data over an open channel can be easily forged, interfered or attacked by intruders. For security purpose, secret data is encrypted before transmission.

Thus, the design of secret sharing schemes allows the secret to be shared among a group of participants has become an important research topic in modern security.The concept of threshold secret sharing was first proposed by Shamir and Blakley independently in 1979.

Visual cryptography (VC) was first proposed by Naorand Shamir at Eurocrypt'94. A visual secret sharing (VSS) scheme deals with the visual version of secret sharing where the shared secret is in the form of an image, the encoded shares are stamped on shares also called as transparencies, and the decoding process becomes the human visual recognition to the superimposed transparencies. Any set of shares reveals the secret image to the user when they are stacked together whereas any set of less than original reveals no information of the secret.



(a) Secret image (b) Share image S_1 (c) Share image S_2 (d) Stacked result of S_1 and S_2

Figure 1: Threshold Visual cryptography

Fig. 1 shows a secret mage "CRYPT" creates a shares using (2,2)-threshold VSS scheme used to share the secret image ''As shown in figure 1, (b) and (c) gives meaningless shares. The secret image ''CRYPT" cannot be revealed by others with the obtained shares. Finally the secret image is revealed by the user by stacking the corresponding share which is shown in Fig1 (d).

II. RELATED WORK

Recently, various studies about visual cryptography are proposed. The following General access structures have been used for visual cryptographic schemes for generating shares.

In [1],(2,n)-Threshold VCS is used .This encrypts the secret image into n number of shares such that any two shares can be combined then reveals the secret image. In [2].(n,n)-Threshold VCS is used. In this the secret image can be encrypted into n shares such that when all n shares are combined together reveals the secret image. In [3],(k,n)-Threshold VCS is used. In this the secret image can be encrypted into n shares such that when any group of at least k shares are stacked which reveals the secret image.

All the above mentioned schemes focus on sharing only one secret image. In practical applications and complexity in theoretical interests, multiple secret images can be shared, in which different combinations of shares reconstruct different secrets, which is a challenging topic in the research.

The studies in this literature can be classified into two categories: direct superimposition and additional operation before superimposition. In that first one stacks are directly superimposed each other. In the second one [4] [5] before superimposition, at least one of the share is made to take any operation such as rotating, turning before stacking.

At present, the research on the first category is comparatively less than the second one. Mostly, the second category has achieved the sharing of any general secrets [5], [6], [7], whereas the first category has only involved the sharing of two secrets [8].

III. PROPOSED SYSTEM

The proposed framework uses half toning method for producing color secret image. This can be done by using Zig-Zag scanning methods in which it embeds the secret message in the original image by without expanding the pixels in the original image. In order to provide security for shares, cover images can be added on the shares by using watermarking technique.

3.1 Half toning

The proposed system uses color image as secret image by using Half toning method. So, before encryption of secret images to original image, half toning method can be applied. In this phase, the color secret image can be decomposed into three color planes Red(R), Green (G), Blue (B).In These planes were converted into C, M,Y planes. Then Halftone operation is carried out on each planes of C, M,Y separately. Then Halftoned C,M,Y planes is submitted to the encryptor.During Hlaftoning, greyscale images are converted into binary images. In color image, each color planes is a grayscale image.After halftone operation three binary images are obtained.

3.2 Encoding phase

The encoding process consists of two stages:

1. Zig-Zag scanning Algorithm
2. Share Generation Algorithm

3.2.1 Zig-Zag scanning Algorithm

Zig –Zag scanning algorithm takes 2-Dimensional secret image matrix A, of size mX n.The elements of Aare 0's and 1's. 0 represents the black pixels And 1 represents White pixels. Zig-Zag scanning is applied on secret image to convert 2-Dimentional image matrix of size mX n to 1-Dimensional vector of size 1 X m*n. By using this method original pixels adjacency connectivity of an image are demolished. The neighbouring pixels in the 2-Dimensional image are broadly separated in the 1-Dimensional data. By doing this partial pattern of an image gets prevented from creeping into the shares.

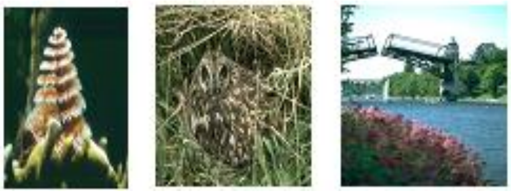
3.2.2 Share –Generation Algorithm

In this algorithm, the input is taken from the output of the zigzag method i.e., 1-D data. The output of this algorithm produces two or more non expandable shares. One of the on-expandable shares is stacked by performing rotation operation with other shares. The shares are then flipped and rotated 90 degree in clockwise direction. As a result the robust shares are generated with the encoded secret message.

IV. EXPERIMENTAL RESULT

To The proposed method can be evaluated by using MATLAB and tested with several images. The proposed system estimates the quality of the image with the pixel expansion and no pixel expansion. Compared with other visual cryptographic scheme, The proposed scheme lets the users to choose of color images with color levels in the reconstructed images based on the desired image quality. The following images show the generated output images.

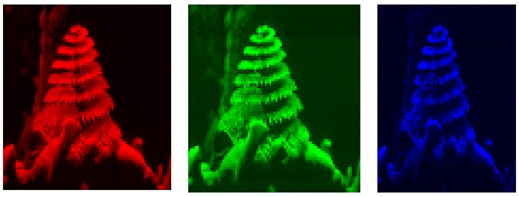
The three secret images (SI) are shown below:



SI 1 SI2 SI3

Figure 2: Secret images

The images in figure 2 show the secret images. Then three RGB planes of this above secret image is shown below.



Red-SI1 Green-SI1 Blue-SI1

Figure 3: RGB planes

The above figure 3shows the RGB planes of secret image 1.Similarly RGB planes of other secret image can be taken.

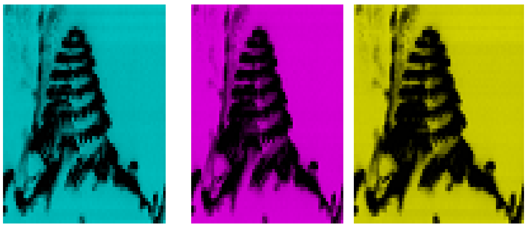


Figure 4: CMY planes

The above figure 4 shows the CMY planes of RGB Secret image 1.Similarly CMY of other three secret images is taken.

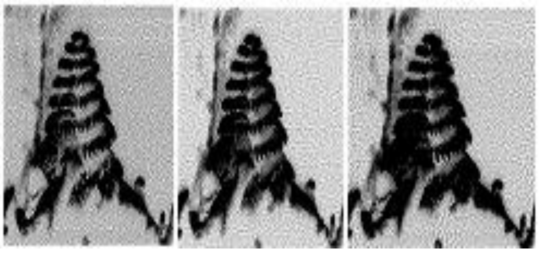


Figure 5: Halftoned secret image

The above figure 5 shows the half toned image of first secret image. Similarly the other two secret images can be generated.

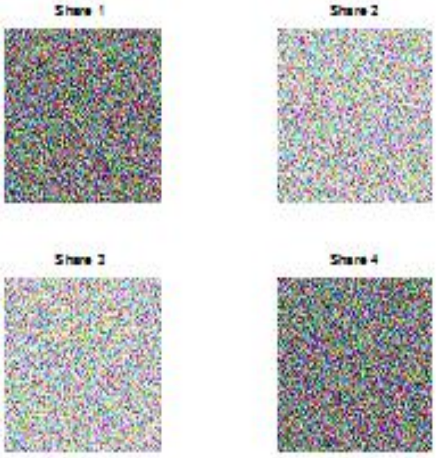


Figure 6: Shares of secret image

The above figure 6 shows the generated shares of secret image 1 by using Zigzag scanning method. Similarly corresponding shares of other secret image can be generated.

V. Conclusion

In this paper, an improved phase of threshold –visual cryptography is proposed. Half toning method used in this gives color secret message to be embedded in the original image. Then zigzag method is used provides non-expandable shares in which no –pixels are expanded during secret image embedding process. Thus the transmission of data needs only less storage spaces. Additional operation on shares such as flipping or rotation of shares can be done. By this the shares can be secured and prevented from attacks by the attackers. Thus the proposed method provides desired image quality after extraction of secret image and cover image.

References

[1] P. A. Eisen and D. R. Stinson, “Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels,”Designs, Codes and Cryptography, vol. 25, pp. 15–61, 2002.

[2] M. Naor and A. Shamir, “Visual cryptography,” Adv. Cryptography:Eurocrypt’94, Lecture Notes in Computer Sci., vol. 950, pp. 1–12,1995, Springer

[3] G. Ateniese, C. Blundo, A. De. Santis, and D. R. Stinson, “Extended capabilities for visual cryptography,” Theoretical Computer Sci., vol.250, pp. 143–161, 2001.

[4] S. J. Shyu and K. Chen, “Visual multiple secret sharing based upon turning and flipping,” Inf. Sci., vol. 181, pp. 3246–3266, 2011.

[5] S. J. Shyu and K. Chen, “Visual multiple secrets sharing by circle random grids,” SIAM J. Image. Sci., vol. 3, pp. 926–953, 2010.

[6] S. J. Shyu, S.-Y. Huang, Y.-K. Lee, R.-Z.Wang, and K. Chen, “Sharing multiple secrets in visual cryptography,” Pattern Recognit., vol. 40, pp.3633–3651, 2007

[7] C.-N. Yang and T.-H. Chung, “A general multi-secret visual cryptography scheme,” Opt. Commun., vol. 283, pp. 4949–4962, 2010.

[8] T. Katoh and H. Imai, “An extended construction method for visual secret sharing schemes,” Electron. Commun. Jpn. (Part III: Fundamental Electronic Science), vol. 81, pp. 55–63, 1998.