Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Multiple Image Sharing Scheme using Visual Cryptography

[1]Dr. Ch. Samson, [2]Masabattula N S S Durgamba
[1]Associate Head, Dept. of Information Technology, SNIST, Hyderabad, Telangana, India
[2]M.Tech (CNIS) Student, SNIST, Hyderabad, India

***Abstract — In this paper we propose Multiple Image Sharing Scheme (MISS) to generate numerous share images for multiple secret images. In the first level, a secret image and key image are used to generate a compound image. The first share is generated with the help of the input image and the compound image. The secret image and the first share are used to generate the second share. These two shares are concatenated to generate the second image which is supplied as an input to the second level. These steps are repeated for n levels and two shares are sent to communication partners and multiple secret images and input reference images can be extracted/decrypted from share images at different levels. The proposed scheme enhances the ability of the conventional visual secret sharing scheme for multiple images without losing image quality.***

***Keywords — Visual cryptography, Image Encryption, Image Decryption, secret sharing, and share image***

## I. INTRODUCTION

With the advancement of the Internet technology, security has become a major issue in information storage and transmission. Cryptography [1] plays a vital role in the field of information security. Usually, the encrypting methods of traditional cryptography are used to protect information. With such methods, the data become disordered after being encrypted and can then be recovered by using a correct key. Without the correct key, the encrypted source content can hardly be detected even though unauthorized persons steal the data.

Visual Cryptography [2] is an emerging area of research in computer science. It is a secret-sharing technique that encrypts a secret image into several shares but requires neither computer nor complex calculations to decrypt the secret image. Instead, the secret image is reconstructed simply by overlaying the encrypted shares. The technique was proposed by Naor and Shamir [3] in 1994. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images and layers are required to reveal the information.

In 2-out-of-2 Visual Cryptography, every secret pixel of the original binary image is converted into four sub pixel of two share images and recovered by simple stacking process. This is equivalent to using the logical OR operation between the shares. Four sub pixels are generated from a pixel of the secret image in a way that two sub pixels are white and two sub pixels are black.

In the present paper our objective is to share multiple secret images and input reference images without any loss of image quality. Here our interest is to increase the capacity of the conventional visual cryptography schemes.

The rest of the paper is organised as follows. In Section II, the related work is presented. Section III describes the proposed scheme. Section IV deals with the implementation results obtained in our analysis. Finally in Section V, we draw conclusions from the results obtained.

## II. RELATED WORK

Visual cryptography has attracted the attention of many researchers in the recent past. Many authors focussed their attention on different Visual Cryptography Schemes for different applications. Each scheme has its own advantages and disadvantages. Noar and Shamir [3] have worked on basic Visual Cryptography Scheme. Without complex calculations, it can restore encrypted messages by stacking two shares via human visual system. The first visual cryptography scheme is used for the black-and-white image. Each pixel is sub divided into 4 sub pixels into two shares. Share 1 is a key and share 2 is assumed to be cipher. The sub pixels of the share are aligned using XOR to get half black pixel and full black pixels. Visual Cryptography starts with selecting random cells in 6 choices shown below.

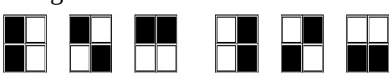

Figure1: Random secrete key for Visual Cryptography

The selected random cell is a key. Share 1 does not provide any information. The cipher share2 is generated by choosing complementary cell for black sub pixel and same cell for white sub pixel. Then two shares are stacked to extract the original information.

Some researchers proposed visual secret sharing schemes for binary images in the literature [4–7]. Some studies [8–10] focused on the visual cryptographic schemes for gray-level or color images.

 

Wu and Chen [11] were the first researchers to propose the visual cryptography schemes to share two secret images in two shares. They have hidden two secret binary images into two random shares, that is A and B, such that the first secret can be seen by stacking the two shares, denoted by A⊗ B, and the second secret can be obtained by first rotating AΘ anti-clockwise. They designed the rotation angle Θ to be 90◦. However, it is easy to obtain that Θ can be 180◦ or 270◦. To overcome the angle restriction of Wu and Chen's scheme, they have refined the idea of Wu and Chen [11] by encoding shares to be circles so that the restrictions to the rotating angles (Θ = 90◦, 180◦ or 270◦) can be removed. Some researchers [12-13] made effort to hide more secret images into two share images. Unfortunately, the existing visual secret sharing schemes restrict the number of secret images.

## III. PROPOSED SCHEME

In this paper, we have proposed an efficient scheme for multiple image sharing called MISS using visual cryptography. Multiple images are combined and encrypted into two share images. The encryption of images can be done at different levels. At every level, a compound image is generated with the help of secret image and key image. Two share images are generated with the help of compound image and input image. The two shares at every level are combined and given as an input image to the next level. The two share images at the last level and the key are sent to communication partners at the receiving end. At the receiver end, all the encrypted images are decrypted at different levels using the key and two share images.

The system architecture of encryption process for three levels is shown in Figure 2. Note that it can be extended to n levels.

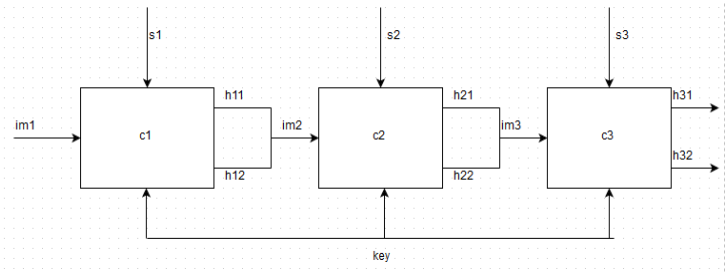


Figure 2: System architecture of encryption process

The encryption algorithm for MISS is given below.

**Algorithm for Encryption**

Step 1: Read the input images(im1, im2… imn), multiple secret images(s1,s2,…sn) and a key image(k) for n levels

Step 2: Generate the first compound image c1 by using s1and k in level 1,

$c1 = s1 \oplus k$

Step 3: Generate share images h11 and h12 as follows:

$h11 = c1 \oplus im1$, and

$h12 = h11 \oplus s1$

Step 4: Concatenate the two share images h11 and h12 to form im2 which is supplied as the input image to level 2.

Step 5: Resize s2 and k such that their size is equal to the second input image im2 in level 2 and generate the second compound image c2.

Step 6: Generate share images h21 and h22 as done in Step 3.

Step 7: Repeat the steps from Step 4 to Step 6 for n levels and send final two share images to communication participants at the receiving end.

The system architecture for decryption process is shown in Figure 3. The process of decryption starts from the last level.

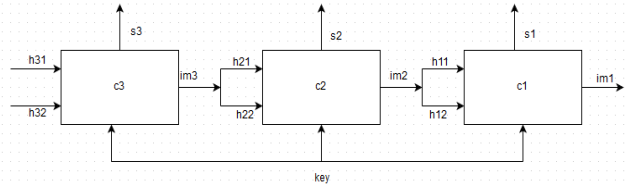


Figure 3: System architecture of decryption process

The decryption algorithm for MISS is given below.

**Algorithm for Decryption**

Step 1: Read the key image(k) and share images of the final level (say h31 and h32 if n=3)

Step 2: Extract/decrypt the secret image s3 of level 3 by using the relation

$s3 = h31 \oplus h32$,

and resize s3 suitable for the next(second) level

Step 3: Decrypt the compound image c3 from s3 and resized k,

$c3 = s3 \oplus k$

Step 4: Decrypt the input image im3 from c3 and h31,

$im3 = c3 \oplus h31$

 

Step 5: Obtain the shares h21 and h22 by splitting im3
Step 6: Repeat from Step 2 to Step 5 according to the level till the first level is reached
Step 7: Display secret images, compound images and the input image

## IV. EXPERIMENTAL RESULTS

We have developed an efficient scheme for sharing multiple secret images. All the programs for encryption and decryption of the scheme are implemented by using MATLAB [14]. Experiments are performed on gray level images and results for three levels are given below.

The first input image im1 for level 1 is selected from the list of images we have collected, as shown below in Figure 4.

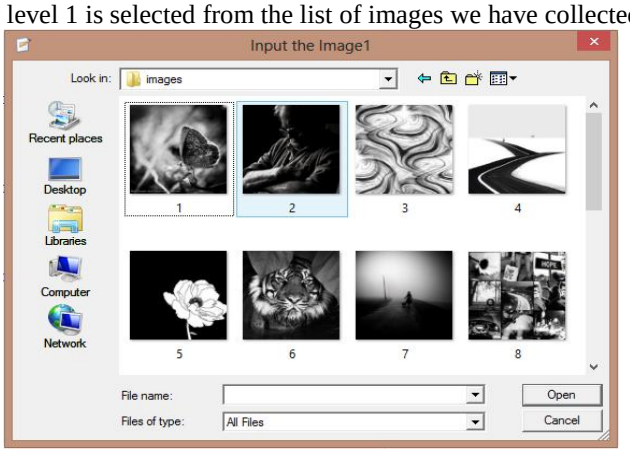


Figure 4: Browsing for input image im1

After that a reference image called key is chosen from the list of images as shown in Figure 5.

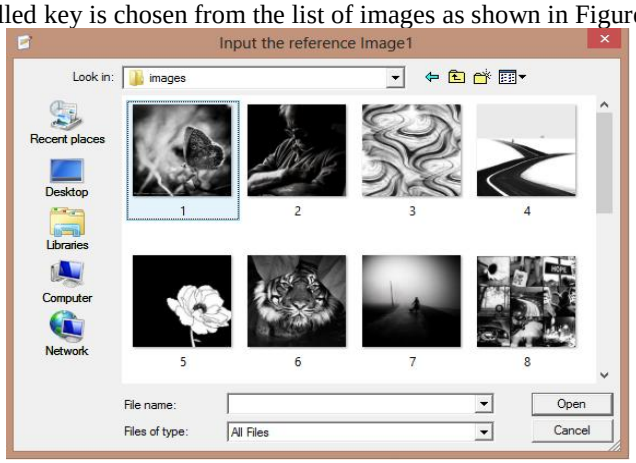


Figure 5: Browsing for reference(key) image k

Then the first secret image is selected and by adopting the encryption process, a compound image c1, and shares h11 and h12 are generated. The input image im2 for the second level is formed by concatenating h11 and h12. The secret image s2 and key image are resized according to the size of im2 and the compound image c2 and share images h21 and h22 are generated at level 2. The same steps are repeated for level 3 also and share images h31 and h32 so produced, as given in Figure 6, are sent to the communication participants at the receiving end.

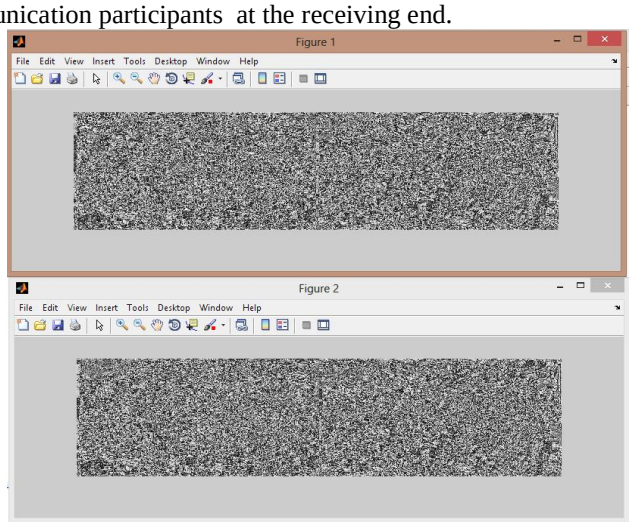


Figure 6: Share images at level 3

 

On using the final share images, key image and adopting the decryption process, input image im1 and secret images s1,s2,s3 are decrypted/extracted successfully, which are shown in Figure 7. It may be noted here that the secret images and key image are resized according to the size of the input image from second level to last level.

Figure 7: Decrypted images

## V. CONCLUSIONS

In this paper we have implemented a scheme for multiple image sharing using visual cryptography. The proposed scheme is able to encrypt multiple number of secret images and decrypt them successfully without degrading the quality of the images. From the results obtained in this analysis, we conclude that the proposed scheme not only achieves the desired goals but also improves the efficiency of visual cryptography for numerous secret images. As the scheme is more secure, it can be used in defense, military and commercial applications. The proposed visual cryptography scheme can be applied to color images.

## REFERENCES

[1] William Stallings, Cryptography and Network Security, Principles and Practice, Third edition, Pearson, 2003.
[2] Shamir, .How to Share a Secret,. Communication ACM, vol. 22, 1979, pp. 612-613.
[3] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT,1994, pp. 1–12.
[4] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for general access structures, Inf. Comput. 129 (1996) 86–106.
[5] D.R. Stinson, An introduction to visual cryptography, Presented at Public Key Solutions '97, Toronto, Canada, April 28–30, 1997.
[6] E.R. Verheul, H.C.A. Van Tilborg, Constructions and properties of *k* out of *n* visual secret sharing schemes, Des. Codes Cryptogr. 11 (1997) 179–196.
[7] C. Blundo, A. De Santis, D.R. Stinson, On the contrast in visual cryptography schemes. J. Cryptology 12 (1999) 261–289.
[8] Y.-C. Hou, Visual cryptography for color images, Pattern Recognition36 (2003) 1619–1629.
[9] C.-C. Lin, W.-H. Tsai, Visual cryptography for grey-level images by dithering techniques, Pattern Recognition Lett. 24 (2003) 349–358.
[10] S.J. Shyu, Efficient visual secret sharing scheme for color images, Pattern Recognition 39 (2006) 866–880.
[11] Verheuland H. V. Tilborg, "Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes. "Designs, Codes and Cryptography, 11(2), pp.179–196, 1997.
[12] L.-H. Chen, C.-C. Wu, A Study on Visual Cryptography, Master Thesis, National Chiao Tung University, Taiwan, ROC, 1998.
[13] 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, March 2004, pp. 996–1001.
[14] Alasdair Mcandrew, ―Digital Image processing with MatLab, Cengage learning 2004.

## AUTHORS PROFILE

**Dr. Ch. Samson** obtained his Diploma from Govt. Polytechnic, Hyderabad in 1994, B. E. from Osmania University in 1998, M. E from SRTM University in 2000 and Ph.D from JNT University Hyderabad in 2015. He published 20 research papers in various international journals and two papers in conferences. He is currently working as Associate Head in the Dept. of Information Technology, SNIST, and Hyderabad. His research interests are Image Processing, Image Cryptography and Network Security.

 