International Journal For Technological Research In Engineering
Volume 2, Issue 10, June-2015 *ISSN (Online): 2347 - 4718*

RANDOMIZED SECRET SHARING ON COLOR IMAGES

Yashaswini A R[1], Manju N[2]
[1]Student, Dept of IS&E, [2]Assistant Professor
SJCE, Mysuru, India

Abstract: Visual secret sharing is a method of encrypting the secret image by dividing secret image into multiple shares. Each share provides some information and multiple shares are stacked together to decrypt the original secret image. However, less number of shares will not work. Decryption process does not require additional knowledge about visual cryptography, it uses Human Visual System to decrypt secret image and this is the key advantage of visual secret sharing. The resultant secret recovered through this scheme is double in size of the original secret image. The algorithms, Randomized (2, 2) visual secret sharing scheme and (3, 3) visual secret sharing are proposed for gray scale images and color images, stacks the shares and results with an image of same size as original secret image and its shadow image. Randomization and pixel reversal approaches are used in all methods.
Keywords: Pixel Reversaal, Visual Secret Sharing.

I. INTRODUCTION

Cryptography is an approach of protecting secret information. It uses mathematical calculations to encrypt the content of information and then the decryption is done to revert back onto the original image and it requires the use of a secret key. Conventional cryptography methods are used to encrypt the images but it is limited because of two main reasons:

1. As image size is greater than that of text, the conventional systems requires a lot of time to directly encrypt the image data.
2. Also, the decrypted data must be equal to the original data , but due to the nature of human views the decrypted image should not necessarily be equal to the original image as small distortion in image is acceptable as far as human is able to perceive that distortion [7].

Even with peculiar advances in computer technology, using a computer to decrypt secret image is impracticable in some situations. During these circumstances, users use visual system to decrypt the secret. Hence human visual system is most comfortable and reliable technique. Moni Noar and Adi Shamir developed a new concept called visual cryptography in 1994. Their ideas are used to develop new scheme of secret sharing. Hence it becomes the stepping stone in visual cryptography and visual secret sharing to innovate new methodologies. If user wants to send some visual information secretly, the confidential data is divided into 'n' number of transparencies. If the user stacks all 'n' transparencies, the secret image is obtained. If less number of 'n' transparencies will not provide original data. The area of this problem moved from gray scale images to color images. By doing more number of transparencies, visual information secrecy level is increased. Hence visual cryptography and visual secret sharing becomes more popular to protect the confidential data .Visual cryptography consumes less power and does not require any additional work or knowledge to decrypt the original data.

The whole Visual cryptographic process is shown in the following Figure 1.

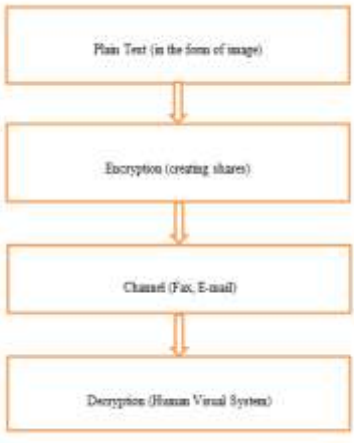


Figure 1.Visual Cryptography Process

II. PREVIOUS WORK

Visual cryptography is a technique used to encrypt visual data (image, text, pictures etc.) before it is transferred to the user. Encryption of the visual data like images is done by dividing the secret image into different shares. Once all the shares are superimposed original image is decrypted. Human visual system is used to decrypt the original image. However less number of shares will not gain any information about it [1]. Steganography techniques are used to hiding the existence of data in other cover media. The main idea is to superimpose multiple invisible instances over each other [2]. Halftone Visual cryptography (HVC) uses error diffusion methods. Here the input secret images embedded concurrently into binary valued shares while these shares are halftone by error diffusion. Halftoning algorithms are used halftoning the images [3]. Binary image is partitioned into different shares of meaningful halftone images. The pixel values of input images are encoded. Direct binary search (DBS) halftoning methods are used to encode the secret pixels [4]. The secret images may be natural images, gray scale images or color images. Visual cryptography (VC) features are extended for natural images. Three images are given as input to the extended VC. It generates two images which are related to two of three input images. The final

image is reconstructed by printing two output images on to shares and stacking them together [5]. The quality of output images is improved using extended VC. Visual cryptography method uses chaotic pseudo-random number generation, zigzag scan pattern method to encrypt secret image. The secret images are encrypted into shares by using above method [6].The incipient alg rithms are used in (2, 2) visual cryptography, visual secret sharing and steganography process which includes LSB (Least Significant Bit) is essential for data hiding. The approach is used for gray scale image and by putting one on top another shares [8].
Limitations:

- The recovered secret image is double in size.
- The recovered secret image is darker and contains visual impairments.
- Some of the shares unhides the confidential data.
- Pixel expansion in the decrypted image.
- Reduces the resolution of the decrypted original secret image.

III. PROPOSED ALGORITHM

Pixel reversal and randomization methods are used to overcome the drawbacks of the existing system. The proposed methods are used for both gray scale images and color images. The resultant secret image is achieved in same size as original input image. After seeing several experiments results and came up few new approaches of (2, 2) and (3, 3) visual secret sharing schemes. In (2, 2) visual cryptography scheme or (3, 3) scheme one secret gray scale image or color image (CI) is given as input to the algorithm. Input image is encrypted in form of creating two or three different shares using Randomization and Pixel Reversal methods. Once all the shares are superimposed original secret image is decrypted. The approach for the (3, 3) visual cryptography scheme is explained.In this scheme we have one secret color image or gray scale image (CI) as input to the algorithm. Where CI is consider as a matrix Cij where i and j shows pixel positions and i, j= 1, 2, 3,.., n.

Algorithm (3, 3) visual cryptography scheme
Input: Secret Gray scale or color image (CI)
Output: Valid shares Share1, Share2, Shares3
Step 1- Extract the color components from input image.
Step 2- Convert input image to gray scale image.
Step 3- Pixel C_{ij} with position i and j is the input called original pixel.
Step 4- Apply pixel reversal method i.e $C_{ij}' = 255 - C_{ij}$.
Step 5- Use randomization method to reduce C_{ij}' randomly.
Step 6- Take the difference of C_{ij}' with original pixel C_{ij}.
Step 7- Use randomization method to reduce reversed value of Cij' randomly.
Step 8- Apply pixel reversal method i.e $C_{ij}'' = 255 - C_{ij}'$.
Step 9- Store in matrix as image called share 1.
Step 10- Take the difference of two random numbers generated from randomization method with original pixel C_{ij}.
Step 11- Apply pixel reversal method i.e $C_{ij}''' = 255 - C_{ij}'$.
Step 12- Store C_{ij}''' in matrix as image called share 2.
Step 13- Take the difference of two pixel reversal values generated from C_{ij}'' and C_{ij}''' with original pixel C_{ij}.
Step 14- Apply pixel reversal method i.e $C_{ij}'''' = 255 - C_{ij}'$
Step 15- Store C_{ij}'''' in matrix as image called share 3.
Step 16- Repeat point 1 to 15 for all pixel value from original image.

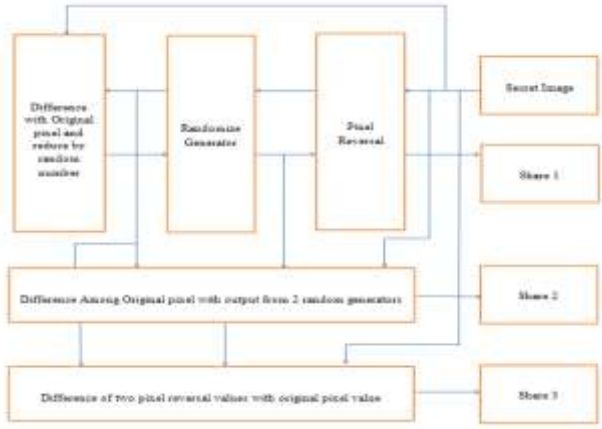


Figure 2. Randomized (3, 3) visual secret sharing scheme

IV. RESULTS

Results shows that the after giving the true color picture as secret image has better results in comparison of algorithm without preprocessing. The algorithm is implemented in MATLAB. Three shares are created using randomized (3, 3) visual secret sharing scheme. Figure 3 shows the experiment results for gray scale images and Figure 4 shows the results for color images.

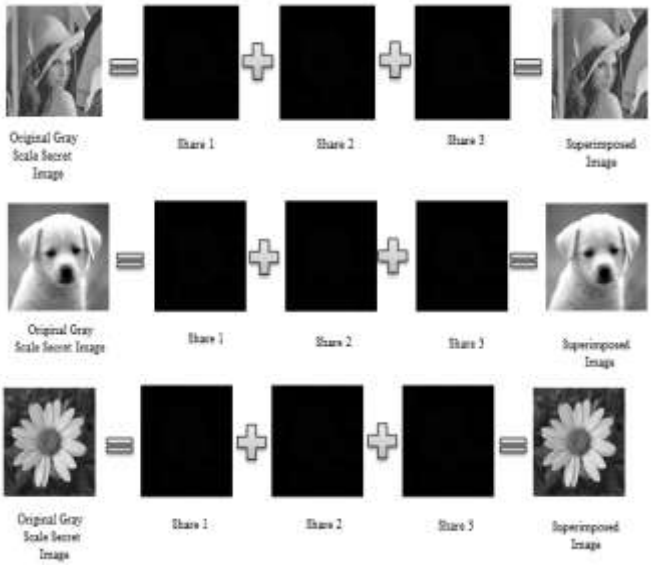
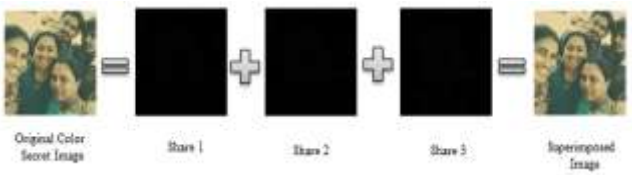


Figure 3. Results for gray scale images as input



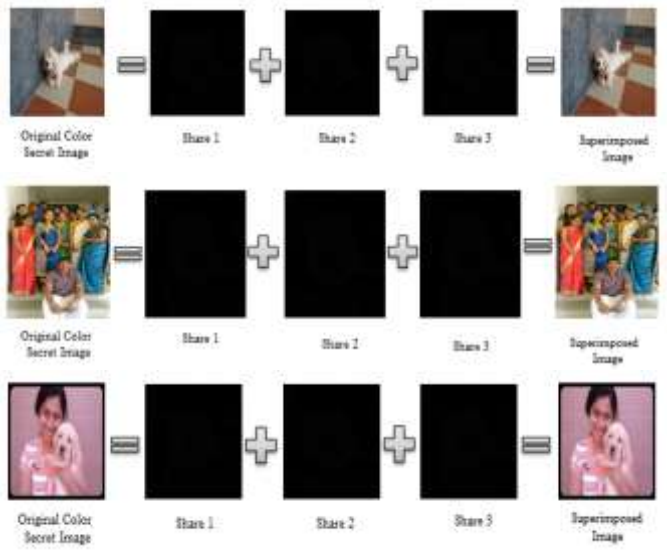


Figure 4. Results for Color images as input

Table.1 Comparisons of Algorithms

Algorithm	**Pixel**	**Security**	**Quality**
Noar, Shamir	Double	Increase	Poor
(k,n) VC scheme	Double	Increase	Poor
Existing Method	No Expansion	Increase	Increase (Grayscale Image)
Proposed Method	No Expansion	Increase	Increase(Color Image)

The above table shows the comparison of the existing and proposed techniques of randomized visual secret sharing.

V. CONCLUSION

Randomized (2, 2) visual cryptography is shown in practice where the shares are generated based on pixel reversal, random reduction in original pixel and subtractions of the original pixel with previous shares pixel. The original secret image is divided in such a way that after OR operation of qualified shares we reveals the secret image. In the (3,3) visual secret sharing scheme shares are generated based on pixel reversal, random reduction in original pixel and subtractions of the original pixel with previous shares pixel and storing the final value of the share pixel after reversal into the shares in round robin fashion. The result of the three shares and after OR operation using stacking of all these qualified shares the original secret reveal. The improvement of the algorithm regarding the acceptance of the true real gray scale image and color images is successful. Our schemes have shown less pixel expansion which is desirable and good for the final retrieval of the secret image. Some contrast is change and impairments are still visible in the results of these schemes. However by dividing the pixels into two or more sub pixel retrieve the secret picture with more impairments and bad resolutions. In our scheme the results are better then and the size of the retrieve image is the same as the original. However size of pixel increases provides more easiness for alignment of the shares. This is the still researchable area to reduce this effect. Also our proposed schemes have shown high level of security because of randomness.

VI. FUTURE WORK

This technique can be further extended with 3D images for creating the shares that have partial secret and reveal that secret by overlapping multiple shares. Quality analysis and Performance analysis to be done. Based on these two, can decide number of shares.

REFERENCES

[1] Naor, M. and Shamir, A., ”Visual cryptography”, In Proc. Eurocrypt 94, Perugia, Italy, May 912, LNCS 950, pp. 112. Springer Verlag., 2010.
[2] Dmitri V., ”Digital Security and Privacy for Human Human Rights Defenders”, The International Foundation for Human Right Defenders, Manual, Feb. 2007
[3] Zhongmin Wang and Gonzalo R. Arce, ”Halftone Visual Cryptography Through Error Diffusion”, Department of Electrical and Computer Engineering, University of Delaware, Newark, IEEE, 2006.
[4] Zhongmin Wang, Gonzalo R. Arce and Giovanni Di Crescenzo ”Halftone Visual Cryptography via Direct Binary search” , Department of Electrical and Computer Engineering University of Delaware, Newark, DE, USA, 2010.
[5] Nakajima, M. and Yamaguchi, Y., Extended Visual Cryptography for Natural Images, WSCG02,2002, 303.
[6] Akshatha M M, Lokesh B, Nuthan A C “Visual Cryptographic Technique for Enhancing the Security of Image Transaction” , Dept. of ECE, SIT, Mangalore, India. 2014.
[7] Dimple Kapoor, Swati Keshari, Saurabh Kumar Gaur “ An Overview of Visual Cryptography “ International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, February 2014.
[8] Pradeep S, Somashekar B “ Private Data Distribution Using Visual Secret Sharing Scheme”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, 2015.

