AN IMPROVED SCHEME OF EMBEDDED EXTENDED VISUAL CRYPTOGRAPHY

[1]Navjot Kaur, [2]Rajiv Mahajan
[1]M.Tech Student (CSE), [2]Professor in Dept. of CSE
GIMET, Amritsar, Punjab, India

ABSTRACT
To prevent the misuse of adversaries the encryption and decryption method ids normally used. Visual cryptography is a method where the secret image is divided into two or more images which are known as shares and the secret image is revealed by overlaying the shares without any complex computation involved. This paper defines how to implement the embedded extended visual cryptography scheme by taking more than one input as well secret image. The image visual quality metrics like PSNR,MSE and MAXERROR are defined here.

KEYWORDS: *Secret Sharing, random shares. Visual Cryptography Scheme.*

1. INTRODUCTION

With the speedy advancement in various communication technologies, the transmission as well instant access to digital data is a common and most popular example. So to prevent this digital data to be interfered and forged by unauthorized parties is one of the most critical demand in computer' era. Various cryptographic techniques are recommended for the sake of security purpose.

2. VISUAL CRYPTOGRAPHY

Cryptography is a technique where the plain text is converted into cipher text on sender side and this process is known as encryption and the cipher text is converted into plain text on receiver side which is known as decryption process. In order to protect the data Visual Cryptography is a technique which was invented by Moni Naor and Adi Shamir in 1994 which allows visual information like pictures, text, data to be encrypted in such a way that decryption becomes a very easy operation that does not require any type of computation or computer. Visual Cryptography Scheme (VCS) is a kind of secret sharing scheme which allows the encryption of a secret image into n shares that are distributed to n participants. The most important property of visual cryptography scheme is that, the decryption of the secret images requires neither the knowledge of cryptography nor complex computation. The decoder is a human visual system and we can easily recover the secret by using the eyes of human being without the help of any computing devices. VCS is a kind of secret sharing scheme that focuses on sharing secret images. For e.g. as given in the figure given below, shares (a) and share (b) are distributed to two participants secretly, and each participant cannot get any information about the secret image, but after overlaying these shares (a) and (b), the secret image can be observed visually by the participants.

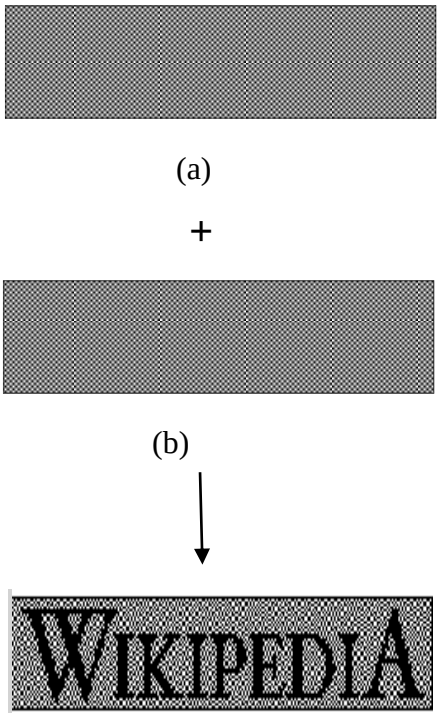


Figure 1. Visual Cryptography Scheme

3. EXTENDED VISUAL CRYPTOGRAPHY(EVCS)

Extended Visual Cryptography is a type of Visual Cryptography which is capable of generating meaningful shares and which reconstructs the image by stacking some meaningful images together. Generally the Extended Visual Cryptography Scheme (EVCS) takes a secret image and n original shares images as input and output n shares which satisfy three conditions as follows:
(a) Any qualified subset of shares can recover the secret image.
(b) Any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image
(c) All the shares are meaningful images.

4. EMBEDDED EXTENDED VISUAL CRYPTOGRAPHY (EVCS)

The Embedded Extended Visual cryptography scheme consists of two phases:
(a) Generation of covering Shares.
(b) Embedding VCS into covering shares

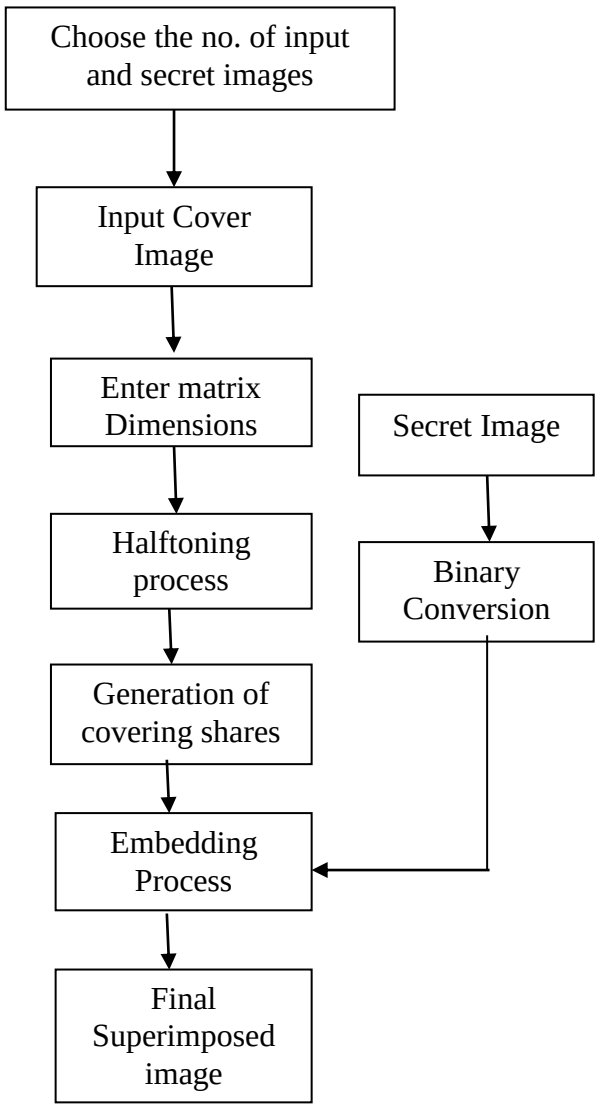
(a) Generation of covering Shares

The generation of covering shares are carried out with the help of half toning technique using dithering matrix.
The **dithering** is a technique to simulate the display of colors that are not in the current color palette of an image. Full colors are usually represented with reduced number of colors. It is accomplished by arranging the adjacent pixels of different colors into a pattern which simulate colors that are not available.
The **Halftoning** is a method which is used to convert the gray level images into binary images. The halftoning method uses the density of net dots to simulate the grey level and transforms an image with grey level into binary image before processing. The basic idea of halftoning is that the binary patterns of shares have no visual meaning and hamper the objective of visual cryptography.
The halftoning process is given below:
The halftoning process for each pixel in :
Input: The dithering matrix and a pixel with

Gray-level in input image
Output: The halftoned pattern at the position of the pixel
For I = 0 to c -1 do
For j = 0 to d - 1 do
If g≤ Dij then print a black pixel at position (i, j);
Else print a white pixel at position (i, j);

(b) Embedding VCS into covering shares

When the generation of meaningful shares have been completed, the embedding process is carried out. This paper represents the improved Embedded Extended Visual Cryptography Scheme in which we took multiple input images and secret images. Firstly we may choose the number of input image and secret binary image i.e. may be 1,2 3,….Then dimensions of matrix are set by using dithering matrix technique. Then the input image is converted into halftoned image, then to reverse halftoned image, then the corresponding shares are produced i.e the final Extended Visual Halftoned (EVC) image and Reverse Final Extended halftoned image. Then the Embedding process starts. The Shares and the secret binary image are embedded and it becomes the final superimposed image.



The visual Quality of Shares are measured by three numerical quantities:
a) PSNR
b) MSE
(c) MAXERROR

PSNR- Peak Signal to Noise Ratio. The PSNR is the Ration of Maximum possible power of signal and power of corrupting noise. PSNR is usually expressed in terms of the logarithmic decibel scale. The Peak signal to noise ratio is given by:

$$PSNR=10 \log \frac{255}{MSE}$$

MSE-. The mean squared error (MSE) allows us to compare the "true" pixel values of our original image to our degraded image. The higher the PSNR, the better degraded image has been reconstructed to match the original image and the better the reconstructive algorithm:

MSE=

$$\frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}||f(i,j)-g(i,j)||\dot{2}$$

f rep the matrix data of our original image
g rep the matrix data of our degraded image
m represents the numbers of rows of pixels of the images
i represents the index of that row
n represents the number of columns of pixels of the image
j represents the index of that column

5. CONCLUSION

In todays' computer era to ensure the safely transmission of is of vital importance. The Embedded Extended Visual Cryptography scheme is a secret sharing scheme which shows better results in terms of peak to signal ratio as compared to other Extended Visual Cryptography Schemes and if we took multiple input and secret images the security issues automatically increase as the degree of randomness increases and the results like expansion in image's pixel is smaller, no need of complementary shares and better visual quality of shares. also here we calculate the PSNR,MSE,MAXERROR between each segment and also the experiment results revels that the proposed scheme has the ability of providing better visual quality of shares which is considered and competitive as compared with other embedded extended cryptography schemes.

REFERENCES

[1] A. Shamir, "*How to share a secret*," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.
[2] M. Naor and A. Shamir, "*Visual cryptography,*" in Proc. EUROCRYPT' 94, Berlin, Germany, 1995, vol. 950, pp. 1 –12, Springer-Verlag, LNCS.
[3] M. Naor and B. Pinkas, "*Visual authentication and identification*," in Proc. CRYPTO'97, 1997, vol. 1294, pp. 322 –336, Springer-Verlag LNCS.
[4] C. Blundo, A. De Bonis, and A. De Santis, "*Improved schemes for visual cryptography*," Designs, Codes and Cryptography, vol. 24, pp. 255–278, 2001.
[5] D. S. Wang, F. Yi, and X. B. Li, "*On general construction for extendedvisual cryptography schemes,*" Pattern Recognit., vol. 42, pp*3071–3082, 2009*.
[6] Asha S.N, Dr.Shreedhara,"*Performance Evaluation Of Extended Visual Cryptography Schemes With Embedded*
Extended Visual Cryptographic Scheme," International Journal of Scientific & Engineering Research Volume 3, Issue 4, April-2012.
[7]Young-Chang Hou,"*Viusal Cryptography for color images"* Pattern Recognition 36 (2003) 1619 – 1629.
[8] Rezvan Dastanian and Hadi Shahriar Shahhoseini," *Multi Secret Sharing Scheme for Encrypting Two Secret Images into*
Two Shares", 2011 International Conference on Information and Electronics Engineering
IPCSIT vol.6 (2011).
[9] Sandeep Katta," *Visual Secret Sharing Scheme using Grayscale Images",* Information Processing Letters, Vol. 27, pp. 255-259.
[10] Shyong Jian Shyu,, Shih-Yu Huanga,Yeuan-Kuen Lee," *Sharing multiple secrets in visual cryptography",* Pattern Recognition 40 (2007) 3633 – 3651

[11] Mizuho nakajima ,Yasushi yamaguchi," *extended visual cryptography for natural images*", Theory of Cryptography Library,(96-07), 1996.
[12] Anandhi1 and S.Satthiyaraj2," *Embedded Visual Cryptography Schemes for Secret Images",* IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.12, December 2012.
[13 D. S. Tsai, T. Chenc, and G. Horng, "On generating meaningful shares in visual secret sharing scheme," *Imag. Sci. J.*, vol. 56, pp. 49–55, 2008.
[14] C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recognit. Lett.*, vol. 24, no. 1-3, pp.349–358, 2003.
[15] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography,"*IEEE Trans. Image Process.*, vol. 15, no. 8, pp. 2441– 2453, Aug. 2006.
16] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography,"*IEEE Trans. Image Process.*, vol. 15, no. 8, pp. 2441– 2453, Aug. 2006.