ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Survey on Embedded Extended Visual Cryptography Scheme

Navjot Kaur[*1], Dr. Rajiv Mahajan[2]
[*1]M.Tech Student (CSE), GIMET, Amritsar, India
[2]Professor (CSE), GIMET, Amritsar, India
navjot.632@gmail.com

Abstract

For the safeguard of digital contents from being intercepted by unauthorised parties is a very serious issue in information security.Visual cryptography is the art of securing information by concealing the secret image into number of shares and these shares are distributed to intended recipients. This paper defines how to implement the embedded extended visual cryptography scheme and the experiment results like PSNR, UQI , pixel expansion is smaller, better visual quality of shares and enhancement in security reveals that this EVCS scheme is competitive when compared with other EVCSs.

Keywords: Secret Sharing, random shares. Visual Cryptography Scheme.

Introduction

Whenever we transmit the data (image) over the network, any unauthenticated person can read our data (image). In order to provide security to our data (image) generally sender will encrypt the data and send it to the intended receiver and the receiver will decrypt the encrypted data and uses it. With the increase in popularity of internet, the security of digital content becomes a most significant demand.

Cryptography

Cryptography is an art of securing information. It is the technique which is employed in protecting the integrity or secrecy of electronic data by converting them into unreadable (cipher text) form. The plain text(original text) is converted into cipher text(disguised text) and the method of converting the plain text into cipher text is known as encryption and the method by which the cipher text is converted into plain text is called Decryption.

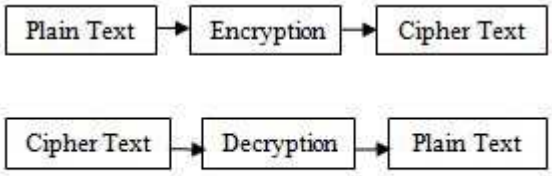


Figure 1. Process of Cryptography

Visual Cryptography

Visual Cryptography is a technique which allows visual information like pictures, text to be encrypted in such a way that decryption becomes a very easy operation that does not require any type of computation or computer. The main idea of Visual cryptography is to divide the original image (secret image) into number of images which are known as shares and then with the help of transparency sheets, these shares are printed out on these transparency sheets. The secret image is then revealed or reconstructed by stacking or overlapping these transparency sheets without any difficulty and that is why the decryption process in visual cryptography is considered as the easy one because the decryption is simply done by stacking the shares onto each other. For e.g. as given in the figure given below, the two share (a) and (b) are when stacked together the image revealed is the secret image.

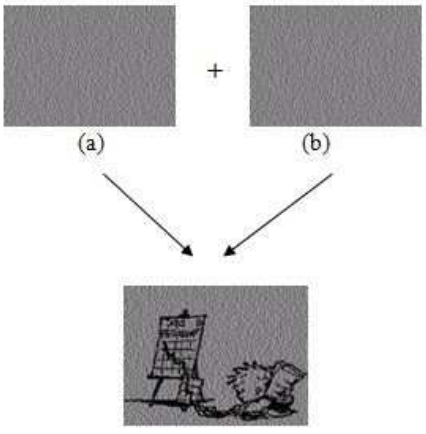


Figure 2. Visual Cryptography Scheme

ISSN: 2277-9655
Impact Factor: 1.852

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 overlaying some meaningful images together. Generally the 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.

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 and the process of embedding is as given below:

The embedding process:

Input: The covering shares constructed in Section IV, the corresponding VCS (C0,C1) with pixel expansion and the secret image I .

Output: The embedded shares e0, e1,..,en-1

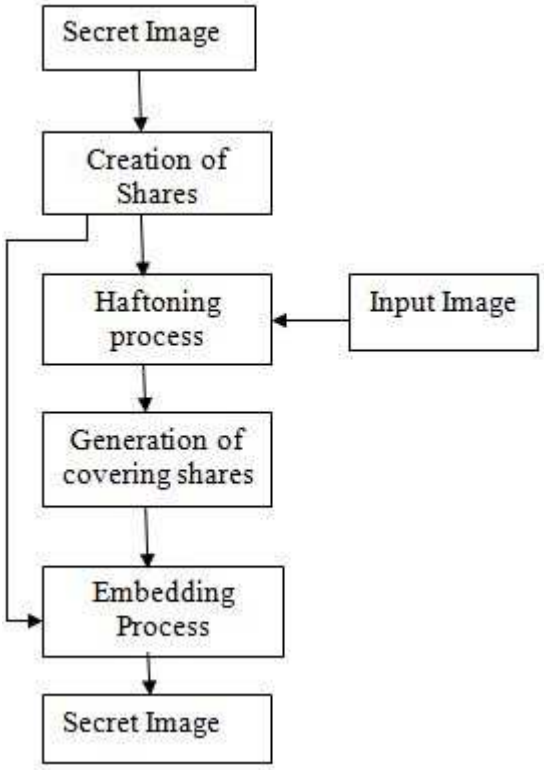
Step 1: Dividing the covering shares into blocks that contain (≥m) sub pixels each.

Step 2: Choose m embedding positions in each block in the n covering shares.

Step 3: For each black (respectively, white) pixel in I, randomly choose a share matrix M € C1 (respectively, M € C0).

Step 4: Embed the m sub pixels of each row of the share Matrix M into the m embedding positions chosen in Step 2.

The diagram shown below shows the complete process of Embedded Extended Visual Cryptography Scheme:



The Process of Embedded Extended Visual Cryptography Scheme is shown as below:

ISSN: 2277-9655
Impact Factor: 1.852

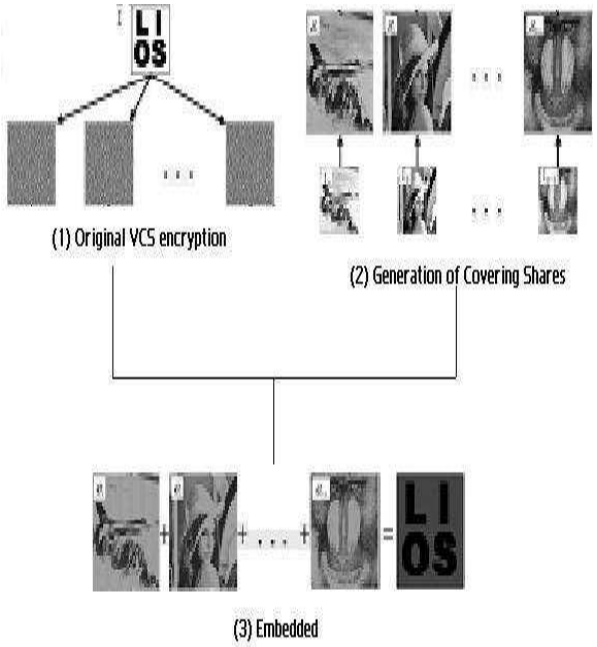


Figure 3. Process of EEVC Scheme

The visual Quality of Shares are measured by two numerical quantities:

a) PSNR

b) QUI

PSNR- Peak Signal to Noise Ratio. The PSNR is the Ration of Maximum possible power of signal and power of corrupting noise. The Peak signal to noise ratio is given by:

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

Conclusion

Nowadays there is a vital need to ensure the information safety in network environment. 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 the results are like expansion in image's pixel is smaller, no need of complementary shares, security increases and better visual quality of shares 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] 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 forn 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.

ISSN: 2277-9655
Impact Factor: 1.852

[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.