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

Security Improvement of Image by Visual Cryptography Using Super Imposed Wavelet Transform in Image Processing

Nazimul Islam
Mtech Scholar
Department of ECE
PDM College of Engineering
MDU, Rohtak (Haryana), India

Shaloo Kikan
Assistant Professor
Department of ECE
PDM College of Engineering
MDU, Rohtak (Haryana), India

Abstract-In this paper the model of region incrementing in visual cryptography was introduced to encrypt an image into multiple secrecy levels. But, it suffers from the pixel enlargement increasing exponentially as the number of participant grows. In this paper, we propose a region 1-level discrete wavelet scheme based on visual cryptography. Wavelet technique is used to convert the Color Image to Gray Image. The important feature of the Visual Cryptography is that decryption doesn't need any computer and it requires less computational power. The proposed scheme is a general (J, m)-VCscheme, in which any t (j≤ t ≤ m) shares can be used to reconstruct the secret regions up to t − j + 1 levels. However, no information about the input image can be revealed by any j–1 or fewer shares. The experimental results show that this kind of new algorithm has high security. Using halftoned, we divide the image in two parts, i.e., share 1 & share 2. In this scheme, an intruder cannot hack the data easily which provides more security.

Keywords: Visual cryptography, wavelet, Halftone, etc.

I. INTRODUCTION

We proceed by first describing the (2,2) VCS model and after words the generalized model with its definitions and properties. In VCS the secret image which is to be shared secretly is divided into parts called shares. Dividing into parts exactly mean each and every pixel of the secret image is copied in to share images in a combination of m number of black and white pixel combinations.

This is done by dividing the image into parts to form share images and the process is called pixel expansion. Dividing/copying a pixel into share images as a combination of black and white pixels is called sharing a pixel.Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc.

Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text.[1]. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable.

II. LITRATURE REVIEW

A visual cryptography scheme is a broad spectrum method which is based upon general access structure. In k-out-of-n secret sharing scheme, any k shares will decode the secret image, which reduce the security level.

A new method of Extended Visual Cryptography for natural images is used to produce meaningful binary shares.

Nakajima[2] in the year 2002 presented a system which takes three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture is reconstructed by printing the two output images onto transparencies and stacking them together. Generally, visual cryptography suffers from the deterioration of the image quality. In this we also describe the method to improve the quality of the output image.

Hou[3] has proposed the binary visual cryptography scheme which is applied to gray level images, that a gray level image is converted into halftone images in the year 2004. The method that uses the density of the net dots to simulate the gray level is called "Halftone" and transforms an image with gray level into a binary image before processing.

In 2006 the Zhi Zhou, Gonzalo, R.Arce and Giovanni Dicrescenzo [4] have proposed halftone visual cryptography which produce good high quality and meaningful halftone shares, the generated halftone shares contain the visual information. In halftone visual cryptography a secret binary pixel „P‟ is encoded into an array of Q1 x Q2 („m‟ in basic model) sub pixels, referred to as halftone cell in each of the „n‟ shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained and also maintain contrast and security. Based on the blue noise dithering principles the proposed method utilizes the void and cluster algorithm.

In 2009 the Inkoo Kang,, Gonzo R. Arce,, and Heung-Kyu Lee [5]have proposed the Visual Cryptography for color image using visual information pixel (VIP) synchronization with error diffusion technique. They introduced a color Visual Cryptography encryption method which leads to significant shares and is free of the previously mentioned limitations.

III. PROBLEM STATEMENT

In existing visual cryptography scheme, the carriers (share-image holders) will bring their shares to the target place; the decoder will then stack the share images to find the original image. Here, there is no guarantee that carriers would not have changed or faked their images. This is the problem statement as known. To address these reliability problems, especially for large information content items such as secret images (satellite photos or medical images), an image secret sharing schemes (SSS) is a good alternative to remedy these types of vulnerabilities. In the proposed method, the decoder should be able to find whether the shared images brought to the target place are fake or not. Because of this, in our work, we proposed wavelet method to secure data.

IV. SYSTEM MODEL

Wavelet transform for image is obtained by as following procedure:-

1).first we apply the fractional random transform for an image. This is given below. The image can be defined by a symmetric random matrix Q. The matrix Q is generated by an N × N real random matrix P with a relation of

Q = (P + trans (P)) / 2

2.)We can also calculate N real orthogonal Eigen vectors of matrix Q. these eigen vectors are normalized using gram schmidt standard normalization procedure. Then we have N orthonormal vectors {v1,v2,v3…..vN}. from these column vectors form the matrix

V = [v1 v2 v3…vN]

The coefficient matrix, corresponds to the Eigen values of discrete fractional random transform can be defined as D=diag(1,exp(-2πα/M),exp(-4πα/M)…...exp(-2(N-1)πα/M)) In above equation there is no jump for odd and even integer N.

3.)We introduce here an integer number M in the coefficients. It indicates the periodicity of DFRNT with respect to the fractional order whose significance will be shown below. The kernel transform matrix of DFRNT can thus be expressed as

Rα=V*D*trans (V)

4.)Therefore the DFRNT of a one-dimensional discrete signal is written as

DFRNT(x) =Rα * x

The expansion of DFRNT for two dimensional signal is straightforward as

DFRNT(x) =Rα * x * trans(Rα)

5).then applying DWT for fractional random transformed image we can fractional random wavelet transform. 3). Reconstruction of image is obtained by applying IDWT and -α order fractional random transform.

V. PROPOSED IMPLEMENTATION

Initially we have two gray scale images: one input secret image and the other input visual image.

1. Using Error Diffusion halftoning method construct halftone image of secret image.
2. Using Error Diffusion halftoning method construct halftone image of visual image.
3.Constructs complement of halftone visual image.
4. Size of visual image is 3 times of input secret image (because every pixel of secret image is represented by 3*3 block of pixel in recovered image).

Algorithm 2 (For Constructing Initial Share).

1. For (i =1 to size of input secret image)
2. If (pixel value of halftone secret image(i) ==1) then
3. Sec1 = (1, 1, 0, 0) or (0, 0, 1, 1)
4. Sec0 = (1, 1, 0, 0) or (0, 0, 1, 1)
5. else
6. Sec1 = (1, 1, 0, 0) or (0, 0, 1, 1)
7. Sec0= (0, 0, 1, 1) or (1, 1, 0, 0)

VISUAL CRYPTOGRAPHY USING WAVELET ALGORITHM

In this section, the algorithm for extended color visual cryptography is described

Step I: Take a secret color image as input.

Step II: Encrypt it into ‘n’ number of shares using Encryption Algorithm.

Step III: Take ‘n’ other meaningful images.

Step IV: Embed individual secret image share into the Meaningful image using VIP synchronization and Error Diffusion Technique.

Step V: Distribute the meaningful images among ‘n’ participants.

Step VI: Take minimum of ‘k’ shares out of ‘n’.

Step VII: XOR them to get the original secret image. Then encryption, i.e. division of the image into n number of shares such that k numbers of shares are sufficient to reconstruct the image; is done using an algorithm.

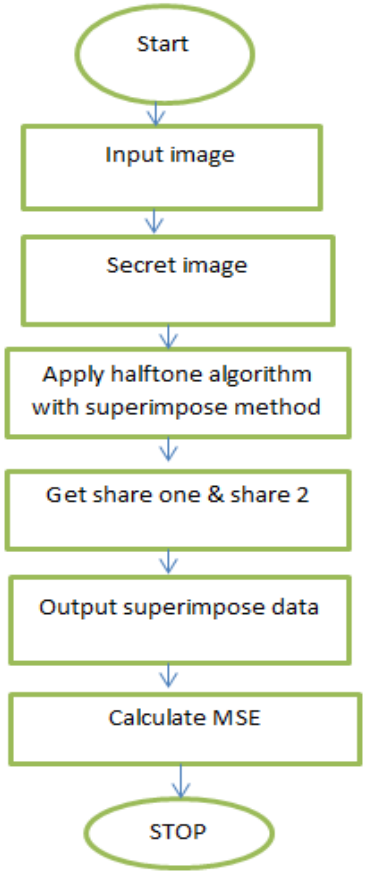

Figure 1: Flow chart of proposed concept

ENCRYPTION ALGORITHM

An image is taken as input. The number of shares the image would be divided (n) and number of shares to reconstruct the image (k) is also taken as input from user. The encryption, i.e. division of the image into n number of shares such that k numbers of shares are sufficient to reconstruct the image; is done by the following algorithm.

Step: I: Take an image as input and calculate its width (w) and height (h).

Step II: Take the number of shares (n) and minimum number of shares (k) to be taken to reconstruct the image. k must be less than or equal to n.

Step III: Calculate recons=(n-k)+1.

Step IV: Create a three dimensional array img_share[n][w*h][32] to store the pixels of n number of shares.

Step V:

for i=0 to (w*h-1)

{

Step VI: Scan each pixel value of the image and convert it into32 bit binary string let PIX.

for j=0 to 31

{

ifith position of PIX contains '1' call

Step VII: Random_Place(n, recons) for k=0 to (recons-1)

{

Set img_share[rand[k]][i][j] = 1

} } }

Step VIII: Create a one dimensional array img_cons[n] to store constructed pixels of each share.

Step IX:

for k1=0 to(n-1)

{ for k2=0 to (w*h-1)

{ String value= "" for k3=0 to 31

{ value=value+img_share[k1][k2][k3] }

construct alpha, red, green and blue part of each pixel by taking consecutive 8 bit substring starting from 0. Construct pixel from these part and store it into img_cons[k1].

}

generate image from img_cons[k1]. }

VI. RESULT ANAYLISIS

Simulation results for the proposed secret sharing scheme for color images are illustrated in this section. The experiment was conducted for different color images of size 512 x 512. The embedded secret image is of same size as the original image.

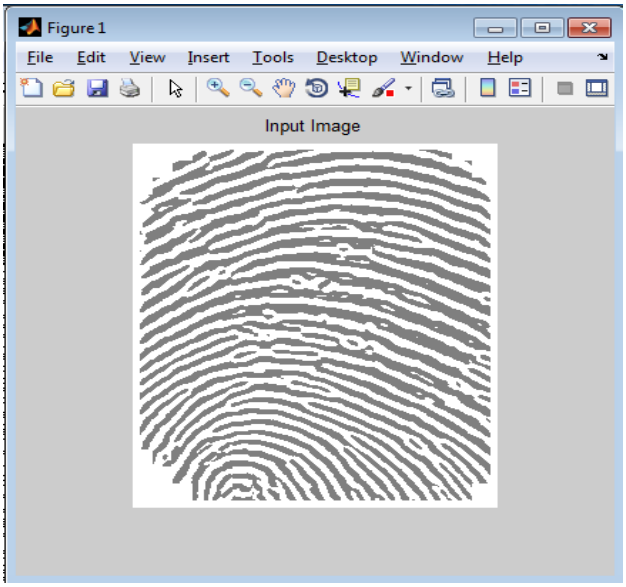

Figure 1: Input image for simulation

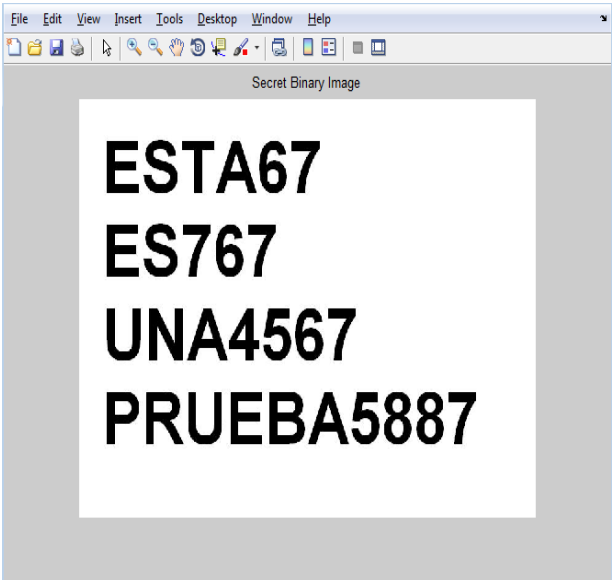

Figure 2: secrete image of is clearly revealed

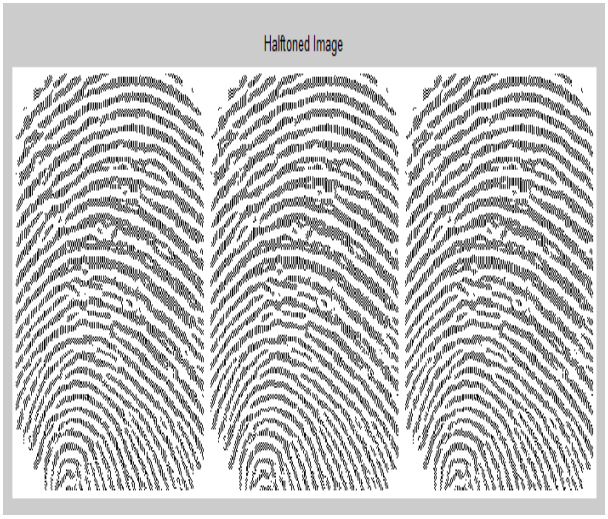

Figure 3: The Halftoned image

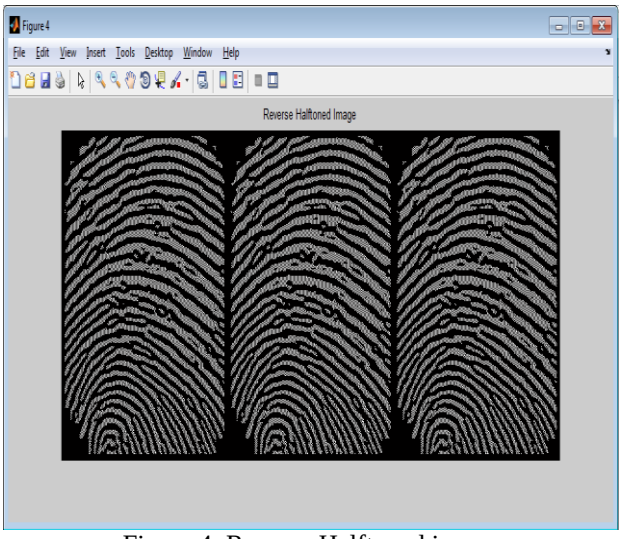

Figure 4: Reverse Halftoned image

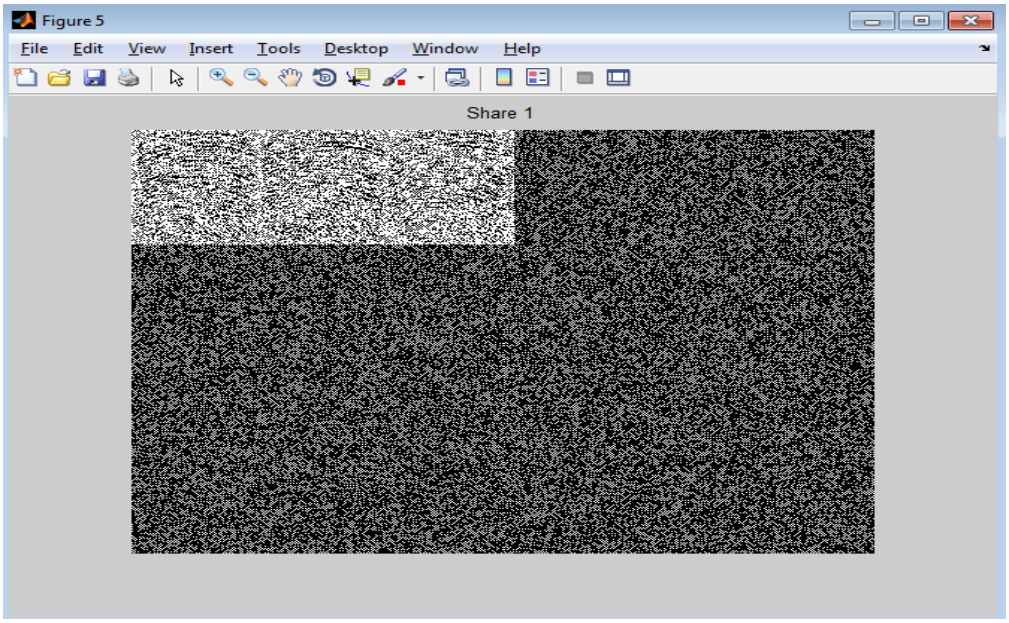

Figure 5: The share 1 image via Visual cryptography

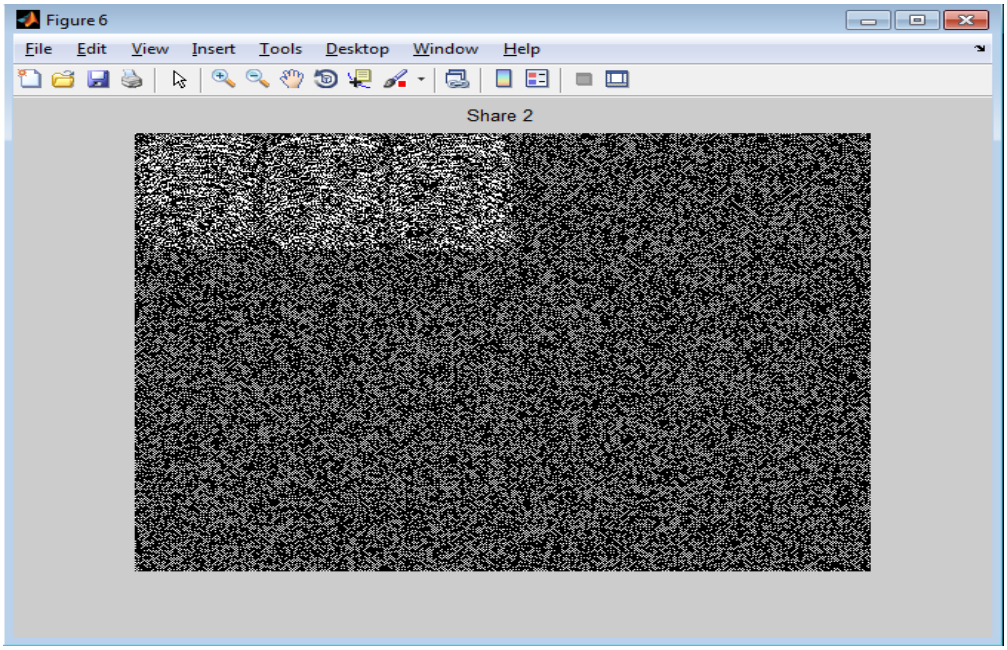

Figure 6: The share 2 image via VC

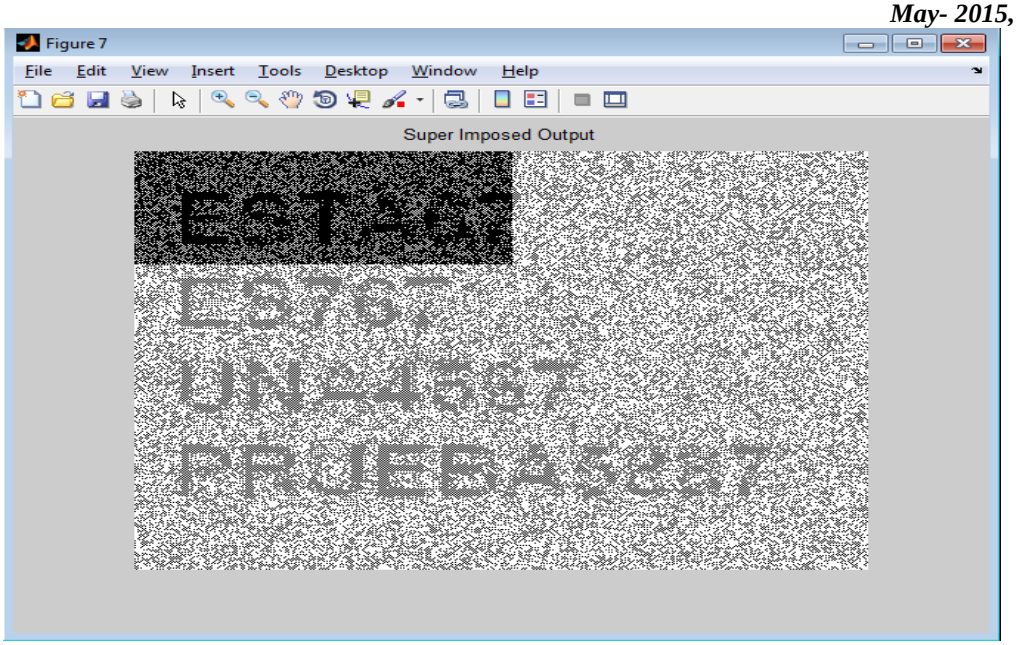

Figure 7: The output image superimposed in VC

VII. CONCLUSION

In this paper, Halftone visual cryptography is improved to achieve better halftone images by simultaneously encoding the secret image and producing the superimposed shares via visual cryptography&wavelet without expansion. We have shown that using an intelligent pre-processing of halftone images based on the characteristics of the original secret image, we are able to produce good quality images in the shares and the recovered image. The recovered secret image is not so clear but the shares are of better quality which means better secret hiding and hence the quality of the secret image can be traded off for better secrecy.

VIII. FUTURE WORK

This paper contains some details about Visual Cryptography Scheme. If lossless Image compression methodology is applied before encryption we can strengthen cryptographic security. Because compressed image has less redundancy than the original image, cryptanalysis will be difficult .The proposed system can be extended such that it can be applied to all types of image formats like JPEG, PNG, etc with other techniques.

REFERENCES

[1] A. Ross and A. A. Othman, "Visual Cryptography for Biometric Privacy", IEEE Transactions on Information Forensics and Security, vol. 6, no. 1, pp. 70-81, 2011.

[2] Mizuho Nakajima and Yasushi Yamaguchi, "Extended Visual Cryptography for Natural Images"

[3] Young-Chang Hou, "Visual cryptography for color images," Pattern Recognition, Vol. 36, No. 7, pp. 1619-1629, 2003.

[4] Z. Zhou, G.R. Arce and G. Crescenzo, "Halftone visual cryptography," IEEE Transactions on Image Processing, Vol. 15, No. 8, pp. 2441-2453, 2006.

[5] Inkookang, G.R. Arce, and H.K. Lee, "Color Extended Visual Cryptography using Error Diffusion," 2009.

