ISSN:0975-9646

A Novel Gaussian Error Diffusion based Colour Extended Visual Cryptography

T. Anuradha [#], Dr. K. Usha Rani [*]

[#] *Research Scholar, Department of CS,*
Sri Padmavathi Mahila Viswavidyalayam, Tirupati, India
[*] *Professor, Department of CS,*
Sri Padmavathi Mahila Viswavidyalayam, Tirupati, India

***Abstract*— Visual Cryptography is a technique used to protect image based secrets. This paper presents a colour extended visual cryptographic system based on Gaussian error diffusion, which results in good quality of shares and improved security. Gaussian error diffusion is applied by choosing an enumeration of pixels and the quantization error is computed. Other computations are made on the basis of threshold. Finally, XOR operation is applied for extracting the secret image. The performance of our proposed system is measured in terms of Peak Signal to Noise Ratio (PSNR), Normalized Correlation Coefficient (NCC) and Mean Square Error (MSE) and is shown in experimental results.**

***Keywords*— Visual Cryptography, Gaussian error diffusion.**

I. INTRODUCTION

The present era can be called as an era of data, as everyone deals with the multimedia data. Obviously, the multimedia data is transferred through the networks, which are prone to several security breaches. Proper care has to be rendered while transferring important secret images, as the adversaries may hack the data. Visual cryptography is composed with several techniques that deal with providing security to the multimedia data.

Visual Cryptography is a technique used to protect image based secrets. The main concept behind this is, to encrypt a secret image into some shares. The secret can be revealed only when all the shares are combined. Thus, this scheme is very effective. Visual cryptography hides secrets within images. These images are encoded into multiple shares and decoded afterwards without any computation [1].

Visual Cryptography requires no knowledge of cryptography, which makes sense that decryption is carried out by human visual system and there is no need for any cryptographic computation [2, 3]. Visual cryptography is an emergent cryptographic methodology, which is proposed by Naor and Shamir [4].

The image based secret is encrypted by a simple algorithm, so as to produce shares depending on the access structure of the system. Mostly preferred access structure is (2, 2). Such system produces two shares and both of these shares are needed to be decrypted, in order to access the secret. If the quality of shares is not good, then it results in suspicion. In order to have visually appealing shares, halftone shares are generated. Halftone images can be produced by several techniques such as error diffusion and dithering. Halftone shares reduce the degree of suspicion of any man-in-the-middle, as the quality of the shares is good. Thus, the security of the system is improved.

The most useful type of visual cryptography is Colour visual cryptography. The main reason behind this is that the usage of colour images is more and also, natural coloured images are the best covers to hide a secret without any suspicions. It is claimed that the quality of shares can be improved by error diffusion [17-19]. The nature of error diffusion techniques is to spread up the pixels as homogeneous as it can, for quality improvement.

Main requirements cited by [18] for improving image quality with error diffusion techniques are as follows. 1. Natural image is preferred for cover image 2. The cover image should be of high quality and finally 3. Low computational cost must be incurred.

In this work, the halftone image is produced by Gaussian error diffusion, so as to improve security and quality of the shares.

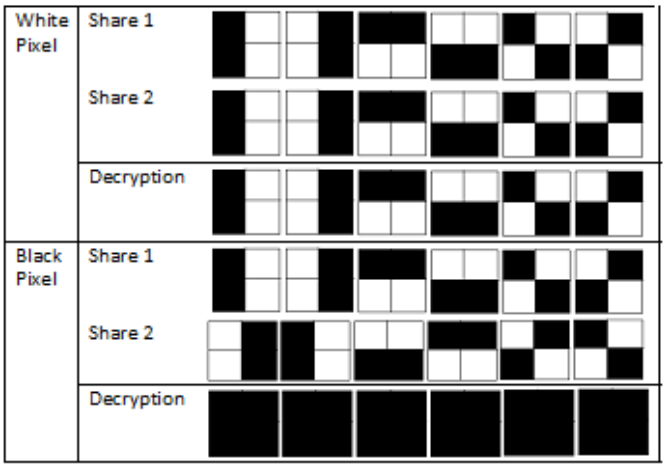

Fig 1: (2,2) VC Scheme

This paper presents a colour extended visual cryptographic system based on Gaussian error diffusion, which results in good quality of shares and improved security. The performance of our proposed system is measured in terms of Peak Signal to Noise Ratio (PSNR), Normalized Correlation Coefficient (NCC) and Mean Square Error (MSE) and is shown in experimental results.

The remainder of this paper is organized as follows. Section 2 is presented with literature review and section 3 carries the proposed methodology. The experimental results are presented in section 4 and the concluding remarks are presented in section 5.

II. Review of Literature

Several related works were studied in order to arrive at a system with enhanced quality. Images with good quality reduce the degree of suspicion of the man-in-the-middle or the hacker. Several systems were proposed for enhancing the image quality and are listed below.

The work proposed in [5] comes up with the (k, n) scheme that gets rid of contrast issue of share images. The visual cryptography scheme focuses on greyscale share images instead of binary images [6-9]. A visual cryptographic scheme is proposed in [7] for greyscale share images along with access structures. The work proposed in [10] presented a scheme that converts greyscale image into a halftone image and greyscale shares are produced by employing binary visual cryptographic scheme. However, this system is not so secure.

Extended visual cryptography is proposed in [11] and the shares here are meaningful. However, this system exploited hypergraph colourings and thus the shares are formed with heavy white noise and thus the image quality is not up to the mark. The image quality is enhanced in [12] by utilizing natural greyscale images.

Halftoning methods were employed in [13], in order to yield high quality shares. Halftone shares were created in [14] by making use of visual cryptography and watermarking techniques. Halftone shares were produced in [15] by using threshold arrays. In [16], halftone shares were produced by error diffusion techniques, which resulted in good quality shares.

RGB is the additive colour model and CMY is the subtractive colour model. Halftoning and reverse halftoning plays a vital role in colour images. A colour image is separated into three different colour channels (RGB) and manipulated.

Motivated by the previous works, we propose to develop a secure system with improved quality of shares by employing Gaussian error diffusion.

III. Proposed Algorithm

The overall idea of halftoning is to distribute more white dots over brighter areas and lesser dots over darker regions of an image. Error diffusion was introduced by Floyd and Steinberg in the year 1976 [20, 21]. The halftones produced by this technique are of high quality.

Error diffusion requires the computation on neighbourhood pixels and threshold based operation. Quantization error is circulated to all the neighbours of the considered pixel that are not halftoned, based on a threshold. The quantization error is diffused along the path of the image scan.

The idea of this system is to use colour extended visual cryptography along with Gaussian error diffusion to produce high quality shares. A colour image of size w x h is chosen. The image is separated into RGB colour channels.

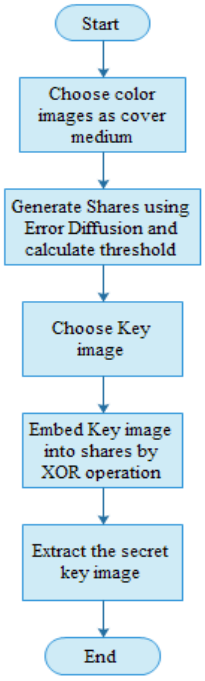

Fig 2: Overall Flow of the System

A. Algorithm for Share Generation

The algorithm to generate shares is presented below. Our algorithm relies on neighbourhood pixel manipulation along with thresholding operation.

Step 1: Select the image.
Step 2: Choose an enumeration of pixels
Step 3: At each location of pixel, add to the input in(i) a weighted average of the previous errors in certain neighbourhood to attain the modified input mo_in(i).
Step 4: Select o(i) from v, closer to mo_in(i).
Step 5: Define err(i) as mo_in(i)-o(i).
Step 6: Gaussian error diffusion(f[.],t)

```
Create output image g[.];
  Create error image e[.];
For each pixel Pix of image f[.] on a scanline path
  do
   If f[Pix]>threshold then
     g[Pix]=white;
   Else
   g[Pix]=black;
end;
return output image g[.];
```

Step 7: Embed secret image and decrypt by XOR operation.

The Gaussian error diffusion of input image is computed by considering the left, centre, right, left bottom and bottom centred regions of an image. Initially, the image is converted to double and the size of the image is obtained. The Gaussian error diffusion is applied to all the three colour channels and the halftone images are generated for all the three channels and are combined.

Images	
Cover images in colour	
Shares	
Secret Key Image	
After embedding key image	
After extraction	

Figure 3: Proposed Scheme

The proposed system shows good security and quality of share images, which is the main goal of the system.

IV. Performance Analysis

In this work, the comparison is carried out by creating shares with Halftone Error Diffusion (HED) proposed in [22], Edge Directed Error Diffusion (EDED) proposed in [23], Optimized Error Diffusion (OED) proposed in [24] and our proposed Gaussian Error Diffusion (GED). The performance is measured by PSNR, MSE and NCC. On analysis, it is found that the performance of our proposed system is much better than all other methodologies and is proved by PSNR ratio, normalized correlation coefficient and MSE. The results of analysis are presented in Table 1. The analysis is carried out by employing Matlab.

A. Peak Signal to Noise Ratio

This performance metric evaluates the image quality between original and the cryptographic image and is calculated by (1).

$$PSNR = 10 \times log_{10} \frac{255 \times 255}{\frac{1}{H \times W} \sum_{x=0}^{H-1} \sum_{y=0}^{W-1} [f(x,y) - g(x,y)]^2} \quad (1)$$

where H and W are the height and width of the image, respectively; and f(x,y) and g(x,y) are the grey levels located at coordinate (x,y) of the original image and cryptography image, respectively.

B. Normalized Correlation Coefficient

This metric measures the quality of key image. The quality of extracted and the original key image is evaluated by (2).

$$NCC = \frac{1}{M \times N} \sum_{1}^{M} \sum_{1}^{N} E(x,y) \times O(x,y) \quad (2)$$

where M and N are the height and width of the image and E(x,y) and O(x,y) are the grey levels located at coordinate (x,y) of the extracted key image and original key image, respectively.

C. Mean Square Error

This metric represents the cumulative squared error between the original and cryptographic image. The lower the MSE, the higher the accuracy rate and is calculated by (3).

$$MSE = \frac{1}{H \times W} \sum_{x=0}^{H-1} \sum_{y=0}^{W-1} [f(x,y) - g(x,y)]^2 \quad (3)$$

where H and W are the height and width of the image, respectively; and f(x,y) and g(x,y) are the grey levels located at coordinate (x,y) of the original image and cryptography image, respectively.

TABLE I

Performance Analysis

Image	PSNR Analysis				NCC Analysis				MSE Analysis			
	HED	EDED	OED	GED	HED	EDED	OED	GED	HED	EDED	OED	GED
Lena	15.4528	19.3562	25.4856	43.8627	1	1	1	1	17.8214	15.2634	10.2346	5.3338
Boat	14.5268	20.2612	25.4856	41.5264	1	1	1	1	16.7421	15.2846	10.8546	4.1254
Pepper	15.2364	22.5632	26.5945	44.8562	1	1	1	1	17.1547	14.5238	9.2365	4.9658
Sail Boat	14.8567	21.5231	24.5621	42.5214	1	1	1	1	16.7317	15.8547	10.2546	4.0325
Barbara	14.8523	20.5845	25.8569	42.8547	1	1	1	1	17.1536	14.9654	10.8546	4.8591

Corresponding graph for Table 1 is provided in figures 4-6. The PSNR analysis is presented in Fig 4. Fig 5 and Fig 6 depicts NCC and MSE analysis respectively.

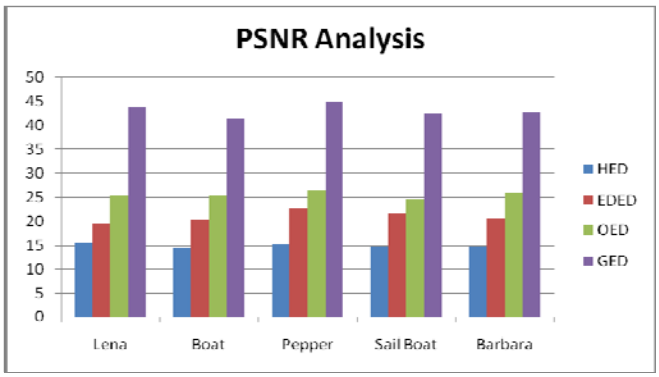

Fig 4: PSNR Analysis

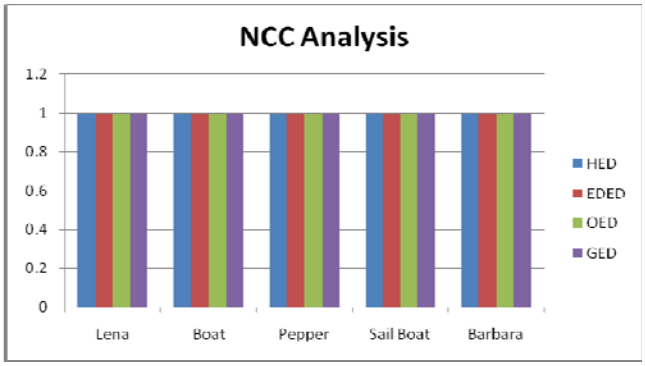

Fig 5: NCC Analysis

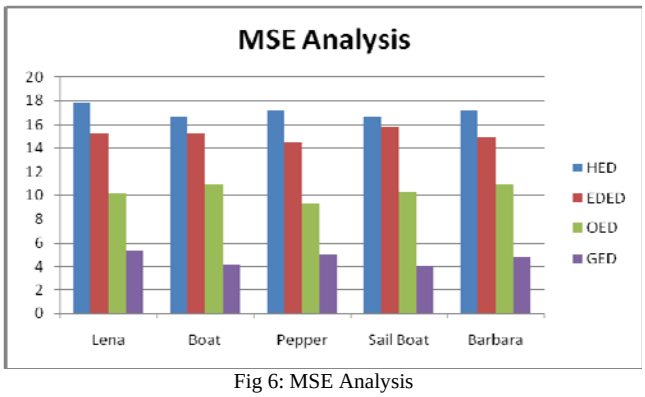

Fig 6: MSE Analysis

From the above presented results, the performance of the proposed system based on GED can be observed with maximum PSNR value and the least MSE value.

V. Conclusion

This paper presents a colour extended visual cryptographic system based on Gaussian error diffusion, which results in good quality of shares and improved security. Error diffusion requires the computation on neighbourhood pixels and threshold based operation. Quantization error is circulated to all the neighbours of the considered pixel that are not halftoned, based on a threshold. The quantization error is diffused along the path of the image scan. The performance of our proposed system is measured in terms of Peak Signal to Noise Ratio (PSNR), Normalized Correlation Coefficient (NCC) and Mean Square Error (MSE) and is shown in experimental results.

References

[1] T. Anuradha, K. Usha Rani, “Comparative Analysis on Visual Cryptographic Schemes” International Journal of Computer Science and Mobile Computing, Vol.3, pp. 134-140, 2014.

[2] W. Hawkes, A. Yasinsac, C. Cline, An Application of Visual Cryptography to Financial Documents, technical report TR001001, Florida State University (2000)

[3] F. van der Heijden, Image Based measurement Systems, John Wiley & Sons, Chichester (1994).

[4] Moni Naor and Adi Shamir, “Visual Cryptography”, advances in cryptology– Eurocrypt, pp 1-12,1995.

[5] C. Blundo, P. D’Arco, A. D. S. , and D. R. Stinson, “Contrast optimal threshold visual cryptography schemes,” SIAM J. Discrete Math., vol.16, no. 2, pp. 224–261, 2003.

[6] L. A. MacPherson, “Gray level visual cryptography for general access structrue,” M. Eng. thesis, Univ. Waterloo, Ontario, Canada, 2000.

[7] C. Blundo, A. D. Santis, and M. Naor, “Visual cryptography for grey level images,” Inf. Process. Lett., vol. 75, no. 6, pp. 255–259, 2000.

[8] Y. T. Hsu and L. W. Chang, “A new construction algorithm of visual cryptography for gray level images,” in Proc. IEEE Int. Symp. Circuits Syst., 2006, pp. 1430–1433.

[9] C. C. Lin and W. H. Tsai, “Visual cryptography for gray-level images by dithering techniques,” Pattern Recognit. Lett., vol. 24, pp. 349–358, 2003.

[10] Y. C. Hou, “Visual cryptography for color images,” Pattern Recognit., vol. 36, pp. 1619–1629, 2003.

[11] G. Ateniese, C. Blundo, A. Santis, and D. R. Stinson, “Extended capabilities for visual cryptography,” ACM Theor. Comput. Sci., vol. 250, pp. 143–161, 2001.

[12] M. Nakajima and Y. Yamaguchi, “Extended visual cryptography for natural images,” J. WSCG, vol. 10, no. 2, 2002.

[13] Z. Zhou, G. R. Arce, and G. D. Crescenzo, “Halftone visual cryptography,” IEEE Trans. Image Process., vol. 18, no. 8, pp. 2441–2453, Aug. 2006.

[14] M. S. Fu and O. C. Au, “Joint visual cryptography and watermarking,” in Proc. IEEE Int. Conf. Multimedia Expo, 2004, pp. 975–978.

[15] E. Myodo, S. Sakazawa, and Y. Takishima, “Visual cryptography based on void-and-cluster halftoning technique,” in Proc. IEEE Int. Conf. Image Process., 2006, pp. 97–100.

[16] Z. M. Wang, G. R. Arce, and G. Di Crescenzo, “Halftone visual cryptography via error diffusion,” IEEE Trans. Inf. Forensics Security, vol.4, no. 3, pp. 383–396, Sep. 2009.

[17] Emi Myodo, Shigeyuki Sakazawa and Yasuhiro Takishma, "Visual Cryptography based on void and cluster halftoning technique", ICIP, pp.97-100, 2006.

[18] Emi Myodo, Koichi Takagi, Satoshi Miyaji and Yasuhiro Takishma, "Halftone visual cryptography embedding a natural grayscale image based on error diffusion technique", ICME, pp.2114-2117, 2007.

[19] Zhongmin Wang and Gonzalo R. Arce, "Halftone visual cryptography through error diffusion", ICIP, 109-112, 2006.

[20] R. Floyd and L. Steinberg, “An adaptive algorithm for spatial greyscale”. Journal of the Society for Information Display. pp. 36-37, 1976.

[21] R. Floyd and L. Steinberg, “An adaptive algorithm for spatial greyscale”. Journal of the Society for Information Display. pp. 36-37 , 1976.

[22] Zhi Zhou, Gonzalo R. Arce, Giovanni Di Crescenzo, "Halftone Visual Cryptography", IEEE Transactions on Image Processing, Vol.15, pp.2441-2453,2006.

[23] Xin Li, "Edge-Directed Error Diffusion Halftoning", IEEE Signal Processing Letters, Vol.13, pp.688-690, 2006.

[24] Mortada Mehyar Demetri Spanos Steven H. Low, "Optimization Flow Control with Estimation Error", INFOCOM 2004, Mar 7-11, Vol.2, pp. 984-992, 2004.