International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Colour Extended Visual Cryptography based on MKGED

T. Anuradha[1], Dr. K. Usha Rani[2]

[1]Research Scholar, Department of CS, Sri Padmavathi Mahila Viswavidyalayam, Tirupati, India

[2]Professor, Department of CS, Sri Padmavathi Mahila Viswavidyalayam, Tirupati, India

Abstract: ***Visual Cryptography is a technique used to protect image based secrets. In this work, encryption method based on Modified Kernel based Gaussian Error Diffusion (MKGED) for colour extended visual cryptography, for visual quality improvement. This work depends on two important parameters and they are cluster centre points m_k and pseudo covariance matrix Q_k. On analysis, it is found that the performance of our proposed system is much better than existing methodologies and is proved by Peak-to-Signal-Noise Ratio (PSNR) value, Normalized Correlation Coefficient (NCC) and Mean Square Error (MSE).***

Keywords: Color Extended Visual Cryptography, Error diffusion, PSNR, NCC, MSE.

1. Introduction

Due to the advent of internet, people tend to exchange multimedia information through network, which is vulnerable to security threats. It is an essential need to protect the privacy and security of the data being exchanged via network. For this sake, several techniques were proposed to provide security. Due to the extensive usage of images, there is a strong need for image security.

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 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 [5-7].

The nature of error diffusion techniques is to spread up the pixels as homogeneous as it can, for quality improvement. In this technique, a secret pattern is embedded into the cover images and when the cover images are overlaid the secret pattern can be retrieved. This can be called as halftone visual cryptography techniques.

The simple construction of (2, 2) visual cryptography scheme is presented in Fig 1. Each pixel of the secret image is embedded into a 2×2 block of the cover image. The figure depicts the possibility of share 1&2 selection. The base of this system is when black is laid over black, the result is black, same way, white and black is black and white and white is white. On superimposing both cover images, the blocks that corresponds to black pixel in secret image, will appear complete black and white pixels resemble half black and half white.

In this work, we propose an algorithm based on modified kernel based Gaussian error diffusion, as an enhancement over [8]. This work depends on two important parameters and they are cluster centre points m_k and pseudo covariance matrixQ_k. The threshold value is selected with utmost care. This work shows good result than the work proposed in [8], with good security and share quality. The results are compared in terms of Peak-to-Signal-Noise Ratio (PSNR), Normalized Correlation Coefficient (NCC) and Mean Square Error (MSE).

The remainder of this work is organized as follows. Review of literature is presented in section 2. Section 3 presents the proposed algorithm and the experimental results and performance analysis are carried out in section 4. Finally, concluding remarks are presented.

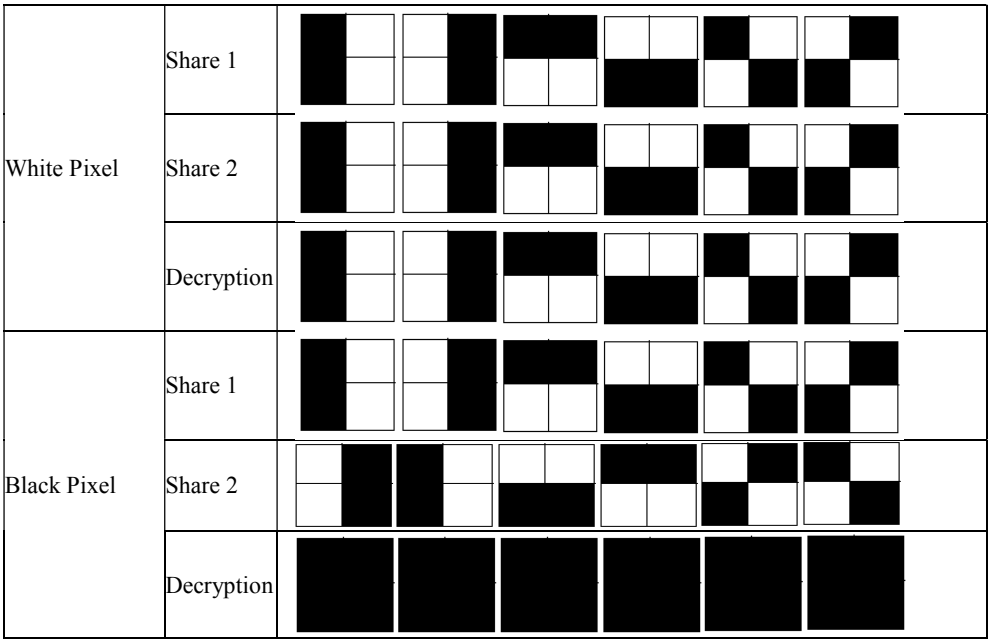

Figure 1: (2, 2) VC Scheme

2. 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.

In [9], Extended Visual Cryptography (EVC) is presented with meaningful share images, by exploiting hypergraph colourings. The share images produced by this system are prone to severe white noise and the share quality is very poor, because of random pixel distribution.

A visual cryptographic scheme based on additive colouring is proposed in [10], and it involves pixel expansion by degree of three, which increases the size of encrypted shares. The work proposed in [11] utilized halftoning methods, in order to have good quality shares. The works presented in [12, 13] involves in creating meaningful shares, however the share quality is not up to the mark.

Data hiding in halftone images by stochastic error diffusion [14] is the first work that produced halftone images based on error diffusion. The enhancement of [14] is presented in [15]. In [16], colour halftone images are used as a carrier for binary secrets. In [17], a system based on colour conjugate error diffusion is presented, however the system lack in visual quality of extracted image.

In [8], a system that is based on Gaussian error diffusion is presented with reasonable share quality. Gaussian distribution is known for its smoothening ability and efficiency. This resulted in a system with appealing share quality.

Motivated by all these works, we propose to introduce a system based on Modified Kernel based Gaussian Error Diffusion (MKGED). Error diffusion is an efficient algorithm to produce halftone images. The quantization error at every pixel is filtered and is passed to process further. The difference of low frequency between the input and the output images are minimized as much as possible, so as to improve the quality of the halftone images [18]. The efficiency of the proposed work can be observed in experimental results.

3. Proposed System based on MKGED

In this work, we propose a system based on modified kernel based Gaussian error diffusion, which is the refined version of [8]. The obtained share quality is more impressive than the share quality of [8]. This system relies on two main parameters cluster centre points m_k and pseudo covariance matrixQ_k. The threshold value is selected with utmost care. The algorithm is presented in this section.

3.1 Error Diffusion

Error diffusion is an efficient algorithm to produce halftone images. Every pixel is quantized by carrying out neighbourhood operation. It is based on scan line operation and scanning is done through every pixel of each row. Each pixel is compared with the threshold. The resultant pixel will be white, if the value of the pixel is greater than the threshold. Else, the resultant pixel is black.

All the colour channels are passed and let $f_{ij}(m,n)$ be the input, where (m,n) is the pixel on the input channel j($1 \leq i \leq n, 1 \leq j \leq 3$) of the i^{th} share. $d_{ij}(m,n)$ is the input that is passed and is given by

$$d_{ij}(m,n)= f_{ij}(m,n)-\sum_{k,l} h(k,l)\ e_{ij}(m-k,n-l) \qquad (1)$$

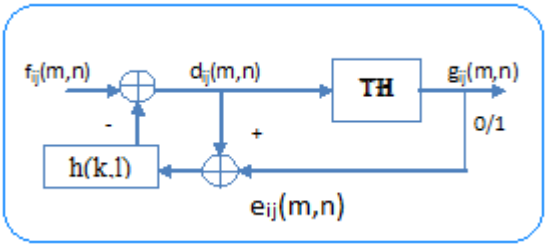

Figure 2: Standard Error Diffusion

$gij(m,n)$ is determined by the threshold (TH) and it can be represented as

$$\text{gij}(\text{m},\text{n}) = \begin{cases} 1 \text{ if}(\text{d}_{\text{ij}}(\text{m},\text{n}) > \text{T}(\text{m},\text{n}) \\ 0 \text{ otherwise} \end{cases} \quad (2)$$

The steps for threshold determination are presented below.

3.2 Proposed Algorithm

1. Select the cover images in colour.
2. Choose an enumeration of the pixels.
3. At each pixel location, add the input I(i), a weighted average of the previous errors in neighbourhood pixels, in order to obtain the modified input M(i).
4. Choose O(i) as an element of V which is closer to M(i).
5. Define the error e(i) as M(i)-O(i). (The simplest case is: v(M(i))=O(i), e(i)=M(i)-v(M(i)), M(i)=I(i)+e(i-1)).
6. Function Modified Kernel based Gaussian Error Diffusion
   a. Let C be cluster count.
   b. Select C entities randomly and let m_k be the cluster
   c. Allocate partition matrix S by Euclidean distance with m_k.
      $S_{ik} = 1, if\ D_{Euc}(x_i, m_k) < D_{Euc}(x_i, m_j),$
      $j = 1,2,\dots,C\ and\ j \neq k.$
      $S_{ik} = 0, else$
   d. Calculate cluster_centre, and the entity located in clusters
      $m_k = \frac{\sum iS_{ik}x_i}{\sum iS_{ik}}, n_k = \sum kS_{ik}$
   e. Calculate the false covariance matrix Q_k, using the matix based genetic algorithm
   f. Calculate partition matrix S by MGA measure with m_k and Q_k.
      $S_{ik} = 1, if\ D_{MGA}(x_i, m_k; Q_k) < D_{MGA}(x_i, m_j; Q_k),$
      $j = 1,2,\dots,C\ and\ j \neq k.$
      $S_{ik} = 0, else$
   g. If S remains the same, end the process. Otherwise, repeat step c through step f.
7. Embed the secret pattern, after the calculation of threshold. Extraction of the secret image is done by the application of XOR operation.

This algorithm renders appealing visual quality of shares and can be seen in Figure 3.

Figure 3: Shares Created by MKGED

The decrypted image of the proposed system is presented in Fig 4.

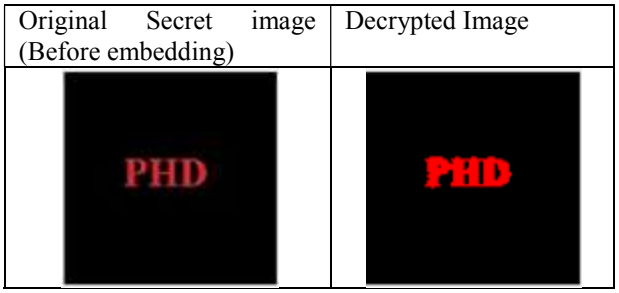

Figure 4: Secret Image before and after decryption

From figures 3 and 4, it is evident that the visual quality of the shares is considerably improved, by means of Modified Kernel based Gaussian Error Diffusion method. This system is compared with existing systems such as Halftone Error Diffusion (HED) proposed in [19], Edge Directed Error Diffusion (EDED) proposed in [20], Optimized Error Diffusion (OED) proposed in [21], Gaussian Error Diffusion (GED) proposed in [8], in terms of PSNR, NCC and MSE. The proposed system outperforms all the other systems and the results shown in graphs.

4. Experimental Analysis

The proposed system is compared with existing systems such as Halftone Error Diffusion (HED) proposed in [19], Edge Directed Error Diffusion (EDED) proposed in [20], Optimized Error Diffusion (OED) proposed in [21], Gaussian Error Diffusion (GED) proposed in [8]. 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 the other methodologies and is proved by PSNR ratio, Normalized Correlation Coefficient (NCC) and MSE. The results of analysis are presented from Table 1 to Table 3. The analysis is carried out by employing Matlab.

Peak Signal to Noise Ratio (PSNR)

This performance metric evaluates the image quality between original and the cryptographic image and is calculated by (3) and the results are shown in Fig 5.

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

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.

Table 1: PSNR Analysis (dB)

Image Name	Half Tone Error Diffusion	Edge Directed Error Diffusion	Optimized Error Diffusion	Gaussian Error Diffusion	Modified Gaussian Error Diffusion
Lena	15.4528	19.3562	25.4856	43.8627	54.6282
Boat	14.5268	20.2612	25.4856	41.5264	53.1246
Pepper	15.2364	22.5632	26.5945	44.8562	54.8569
Sail Boat	14.8567	21.5231	24.5621	42.5214	52.1284
Barbara	14.8523	20.5845	25.8569	42.8547	52.4965

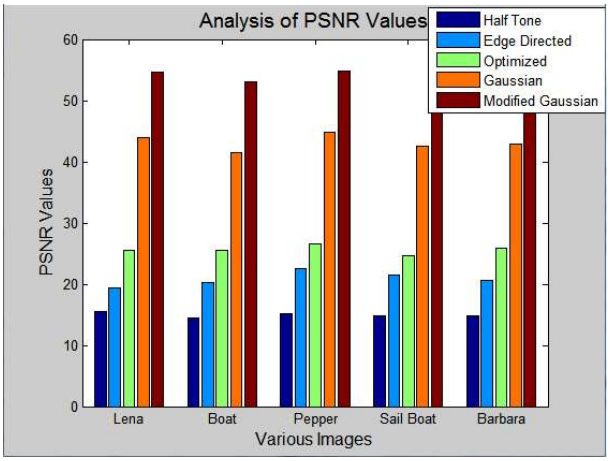

Figure 5: PSNR Analysis

Normalized Correlation Coefficient (NCC)

This metric measures the quality of key image. The quality of extracted and the original key image is evaluated by (4).

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

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. The experimental results of NCC analysis are presented in fig 6.

Table 2: NCC Analysis

Image Name	Half Tone Error Diffusion	Edge Directed Error Diffusion	Optimized Error Diffusion	Gaussian Error Diffusion	Modified Gaussian Error Diffusion
Lena	1	1	1	1	1
Boat	1	1	1	1	1
Pepper	1	1	1	1	1
Sail Boat	1	1	1	1	1
Barbara	1	1	1	1	1

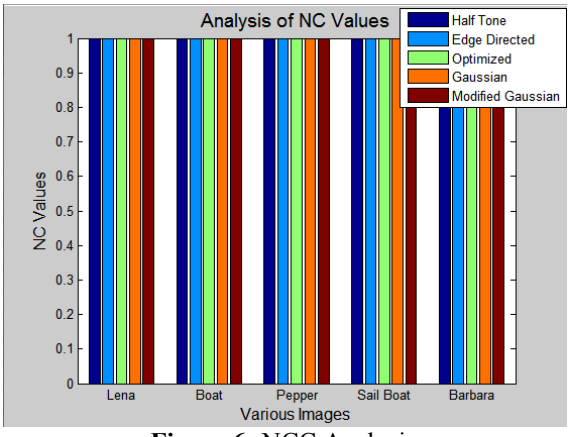

Figure 6: NCC Analysis

Mean Square Error (MSE)

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 (5). MSE analysis is presented in fig 7.

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

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 3: MSE Analysis (dB)

Image Name	Half Tone Error Diffusion	Edge Directed Error Diffusion	Optimized Error Diffusion	Gaussian Error Diffusion	Modified Gaussian Error Diffusion
Lena	17.8214	15.2634	10.2346	5.3338	1.9535
Boat	16.7421	15.2846	10.8546	4.1254	2.0125
Pepper	17.1547	14.5238	9.2365	4.9658	1.5264
Sail Boat	16.7317	15.8547	10.2546	4.0325	1.8569
Barbara	17.1536	14.9654	10.8546	4.8591	2.1254

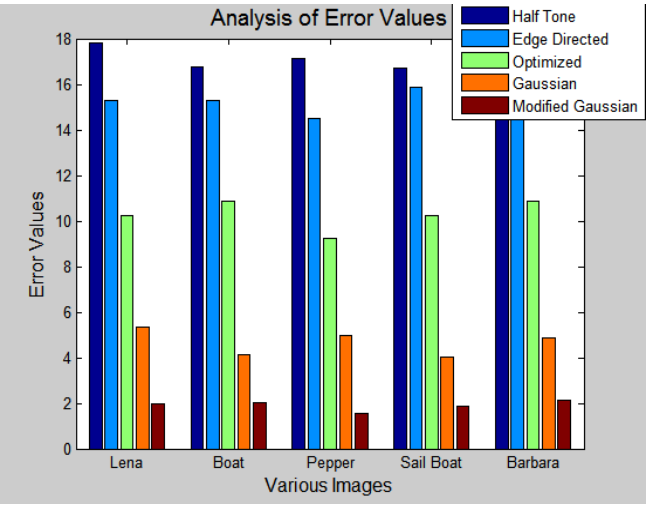

Figure 7: MSE Analysis

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

5. Conclusion

This work proposes an encryption method based on Modified Kernel based Gaussian Error Diffusion (MKGED) for colour extended visual cryptography, for visual quality improvement. This system relies on two main parameters cluster centre points m_k and pseudo covariance matrix Q_k. The threshold value is selected with utmost care. On analysis, it is found that the performance of our proposed system is much better than all other methodologies and is proved by PSNR value, normalized correlation coefficient and MSE.

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] Emi Myodo, Shigeyuki Sakazawa and Yasuhiro Takishma, "Visual Cryptography based on void and cluster halftoning technique", ICIP, pp.97-100, 2006.
[6] 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.
[7] Zhongmin Wang and Gonzalo R. Arce, "Halftone visual cryptography through error diffusion", ICIP, 109-112, 2006.
[8] T. Anuradha, Dr. K. Usha Rani, "A Novel Gaussian Error Diffusion based Colour extended Visual Cryptography", International Journal of Computer Science and Information Technologies, Vol. 5 (5), 2014, 6528-6531.
[9] 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.
[10] C. N. Yang and T. S. Chen, "Visual cryptography scheme based on additive color mixing," Pattern Recognit.,vol. 41, pp. 3114–3129, 2008.
[11] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography," *IEEE Transaction on Image Processing*, vol. 15, no. 8, pp. 2441–2453, 2006.
[12] Stefan Droste, "New results on visual cryptography," *CRYPTO '96 Springer-Verlag LNCS*, vol. 1109, pp. 401–415, 1996.
[13] R. Lukac and K. N. Plataniotis, "Colour image secret sharing," *IEE Electronic Letters*, no. 9, pp. 529–530, 2004.
[14] M.S. Fu and O.C. Au, "Data hiding in halftone images by stochastic error diffusion," *in Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*. IEEE, 2001, vol. 3, pp. 1965-1968.
[15] M.S. Fu and O.C. Au, "Steganography in halftone images: conjugate error diffusion," *Signal Processing,* vol. 83, pp. 2171-2178, January 2003.
[16] S.C. Pei and J.M. Guo, "Hybrid pixel-based data hiding and block-based watermarking for error-diffused halftone images," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol.13, no.8, pp. 867- 884, Aug. 2003.
[17] M.S. Fu and O.C. Au, "Watermarking technique for color halftone images," *in Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*. IEEE, 2004, vol. 3, pp. 381-384.
[18] *InKoo Kang, Gonzalo R. Arce, Heung-Kyu Lee, "*COLOR EXTENDED VISUAL CRYPTOGRAPHY USING ERROR DIFFUSION*", ICASSP 2009, pp 1473-1476, 2009.*
[19] Zhi Zhou, Gonzalo R. Arce, Giovanni Di Crescenzo, "Halftone Visual Cryptography", IEEE Transactions on Image Processing, Vol.15, pp.2441-2453,2006.
[20] Xin Li, "Edge-Directed Error Diffusion Halftoning", IEEE Signal Processing Letters, Vol.13, pp.688-690, 2006.
[21] Mortada Mehyar Demetri Spanos Steven H. Low, "Optimization Flow Control with Estimation Error", INFOCOM 2004, Mar 7-11, Vol.2, pp. 984-992, 2004.