Secure Secret Image Sharing using Histogram Localization Based Block wise Methodology

D.R.Denslin Braja, V.S.Dharun, D.R.Denslin Brabin

Abstract**:** ***Various types of encryption techniques have been used for data security. Complex algorithms are followed for this purpose in most of the methods. Confidentiality is provided by a technique called visual cryptography excluding of any intricate computations and algorithms. In this paper, we put forward an innovative method called Histogram Localization based Blockwise (HLB) approach to solve pixel expansion problem at the same time it will increase the security and visual quality for highly confidential secret image which is in color. According to this method, the secret shares are generated based on the histogram and also the number of black pixels in the corresponding block. The image size of resultant shares is same as in the original secret image. These shares are distributed to participants, and human vision system is used for decryption purpose.***

Index Terms**:** ***Histogram, Blockwise approach, Visual Cryptography, Secret Sharing.***

I. INTRODUCTION

Visual Cryptography is used to solve the problem of encoding printed text, handwritten notes, images, drawings etc. Here encryption is the process of generation of shares and decryption is directly identified by the human vision. Moreover, it is perfectly secure. For instance, to encrypt the secret information into n transparencies, we need n participants, one transparency is dispersed to each participant, so that k or more participants can see the secret information by piling their transparencies at the same time k − 1 or less participants get no information. This is called k out of n Secret Sharing Scheme. These transparencies are the modified version of original pixel called shares. Each share is a compilation of black and white subpixels. A different kind of cryptographic scheme was proposed by Naor and Shamir [1] in the year of 1994 which can decode concealed images exclusive of any cryptographic computations. They proposed this scheme especially for black and white images. Each pixel in the original message is replaced by the set of subpixels to generate shares as shown in Fig. 1. Here shares are represented as transparencies and superimposing these shares can generate combined share and can decrypt by the Human Vision System (HVS). This method is secure and easy to implement.

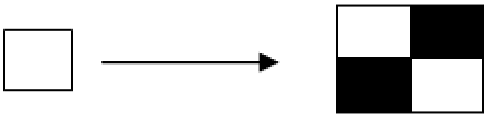

Fig.1. Example: Block of pixels substituted for single pixel

Here white represents 0 and black represents 1 and the resulting Boolean structure is n × m matrix. The Boolean matrix is represented as M = [m_{ij}], if the j^{th} subpixel in the i^{th} transparency is black then m_{ij} = 1 and if the j^{th} subpixel in the i^{th} transparency is white then m_{ij} = 0. When transparencies are piled together a collective share can be observed that is the secret image. The grey level of this collective share is proportional to the Hamming Weight H(V) of the OR-ed vector V. If H(V) >= d then grey level in the collective share is interpreted by the human vision as black and if H(V) <= d – α then it is interpreted as white. Some of the applications area of Visual cryptography are general access structures [2,3,4]in which the qualified set of shares are stacking together can expose the secret image but stacking the shares in forbidden set can't expose anything, Copyright protection [5] which provide shield to digital images from the manipulation and attacks, Visual authentication and identification [6] which can be utilized for communication over insecure network, etc.

Zhou et. al. and Wang et al. [7,8] proposed halftone visual cryptography. They used blue-noise dithering principles to achieve visual cryptography through halftoning. To encrypt a secret image into halftone shares two algorithms are proposed called void and cluster especially for black and white images. Visual quality that is obtained by this method is better than the methods that are available on that date. Conversely, the positions of secret information pixel in these algorithms are content based, it causes the appearance of the reconstructed image and also the pixel expansion leads to lower resolution.

Ito et. al. [9] initially proposed (k,n) visual secret sharing scheme for black and white image without pixel expansion. According to this scheme, each pixel in the secret image is replaced by a black or white pixel in the shared image. So that the size of the both share and the image are same. Moreover, the reconstructed image is also more visible than the previous schemes. Also, extend their work to generate color shared images. Chang et. al. [10] built a scheme for gray-level images using space filling curve ordered dithering algorithm.

Revised Manuscript Received on 30 July 2019.
* Correspondence Author

D. R. Denslin Braja*, Department of Information Technology, Noorul Islam University, Tamilnadu, India.

V. S. Dharun, Department of Electronics and Communication Engineering, Immanuel Arasar JJ College of Engineering, Tamilnadu, India.

D. R.Denslin Brabin, Department of Computer Science and Engineering, Madanapalle Institute of Technology & Science, Andhra Pradesh, India.

First, a gray level image is converted into an appropriate binary image using SFCOD (Space-Filling Curve Ordered Dithering) algorithm, then the visual cryptography technique is applied to generate shares. This method is feasible to apply only gray level images, can't apply to color images. Hou et. al. [11] developed a scheme for color images. They used halftone technology to convert continuous tone image into discrete tone image and color decomposition to separate color components from the secret color image namely cyan, magenta and yellow. Further, each pixel is substituted by a set of pixels, finally these blocks are combined to generate color shares. These methods are also expanding every pixel into 2x2 block leads to pixel expansion problem. Inkoo et. al. [12] proposed error diffusion technique especially for color images. They use visual information pixel synchronization to improve the visual contrast of the reconstructed image and error diffusion to halftone a secret color image. This technique also yields low visual contrast reconstructed image. Ross et al. [13] proposed visual cryptography technique to protect biometric data such as finger print, iris code and face images. Shares are stored into two separate database servers so that the biometric data can be exposed when both sheets are available concurrently. Chen [14] works to construct fully incrementing visual cryptography in non-monotonic structure. Some addition is also performing together with his work like widening, multi-atomic, and full-fledged methods. The forbidden subsets and qualified subsets are independent to accomplish non-monotonic structure. Moreover, he proposed throwing redundancy technique to reduce pixel expansion problem. Xingxing et. al. [15] developed collaborative visual cryptography scheme. It is used to embed multiple secrets for general access structure. Although it simplifies the process of combining more than one secrets on a single share and it overcome the security gap but still it required to work on contrast that affect the visual quality. Recently a visual cryptography based iris authentication scheme is proposed by Udayini et al.[16].

II. VISUAL CRYPTOGRAPHY MODEL

In visual cryptography model, encryption is the process of generation of shares and decryption is directly identified by the human vision. During the encryption process, each pixel in the original secret image, choose column permuted matrix of C0 or C1 based on the pixel value 0 or 1. When the pixel is white it chooses the matrix from C0 otherwise it chooses the matrix from C1. The chosen matrix defines the color of the m subpixels in each of the n transparencies.

A. *2 out of 2 Secret Sharing Scheme:*

In this method the original secret image is encrypted into two transparencies and for decryption it required these two transparencies stacking together to reveal the original secret image. The pictorial representation of pixel based visual cryptography is shown in Fig. 2. The matrices used in this scheme are given below:

$$C_0 := \left[\text{all permutations of columns of } \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \right]$$

$$C_1 := \left[\text{all permutations of columns of } \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \right]$$

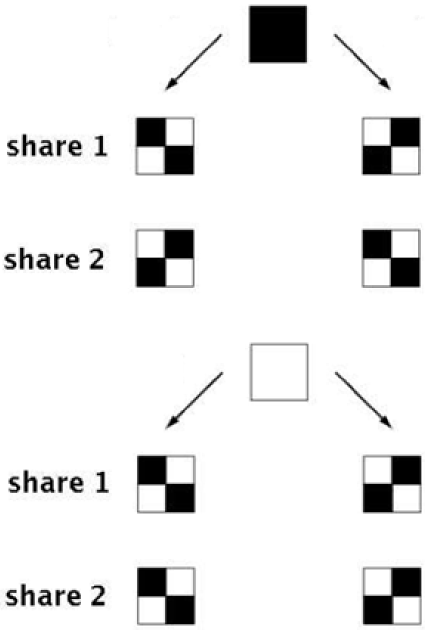

Fig. 2. Pixel based 2 out of 2 visual cryptography

B. *3 out of 3 Secret Sharing Scheme:*

The original secret image is encrypted into 3 transparencies. By stacking these three transparencies will reveal the original secret image. The matrices used in this scheme are given below:

$$C_0 := \left[\text{all permutations of columns of } \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \right]$$

$$C_1 := \left[\text{all permutations of columns of } \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \right]$$

C. *k out of n Secret Sharing Scheme:*

In this method the original secret image is encrypted into n number of transparencies and for decryption it required any k or more transparencies stacking together to reveal the secret image in its original form. The matrices used in this scheme are given below:

$$C_0 := \left[\text{all permutations of columns of} \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ \multicolumn{5}{c}{\dots\dots\dots\dots\dots} \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix} \right]$$

$$C_1 := \left[\text{all permutations of columns of} \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \multicolumn{5}{c}{\dots\dots\dots\dots\dots} \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \right]$$

III. PROPOSED WORK

In classical visual cryptography, encryption means generation of 'n' shares, these are the random noise shares. In our proposed work we introduce the new approach called Histogram localization based blockwise approach to generate shares then these shares are scattered to participants. The entire processing is shown in the Fig. 3. It includes the four modules: Color Decomposition, Halftone Generation, HLB Approach and Recovering of Secret Image.

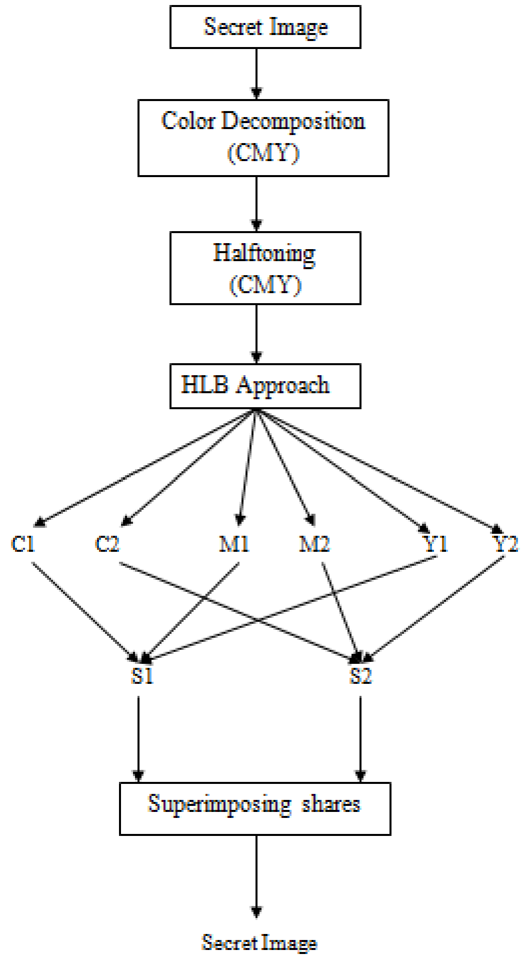

Fig. 3. Block diagram of the proposed work

A. *Color Decomposition*

This module is used to separate Cyan, Magenta and Yellow color from each pixel in the original secret color image. CMY is a subtractive color model, the relationship with RGB color model is C = 255 – R, M = 255 – G and Y = 255 – B. Therefore (0, 0, 0) is represented as white and (255, 255, 255) is represented as black in the CMY color model.

B. *Halftone Generation*

Each decomposed color image (C, M &Y) are halftoned by applying Floyd Steinberg Error Diffusion Method. This method is used to generate halftone image that is discrete tone image for the original continuous tone image. In this method the quantization error is scattered to upcoming adjacent pixels that are in right, right diagonal, left diagonal and bottom. Those pixels are processed that set remain unchanged. Fig. 4 shows how the quantization error of the particular pixel is scattered to the adjacent pixel and here the pixels are named in alphabetical order.

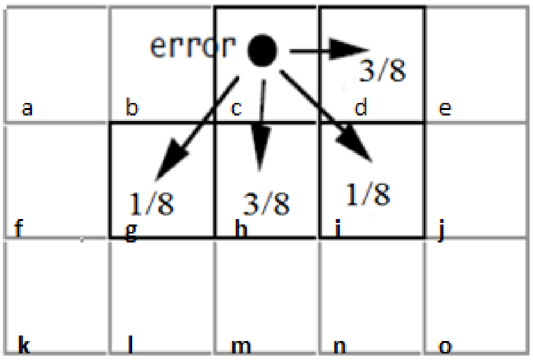

Fig. 4. Example of Floyd Steinberg Error Diffusion method

For example, consider the pixel c, the neighboring pixels are b, d, g, h, and i. Among these pixels b is already processed, so that it remains unchanged. The remaining pixels d, g, h and i will be changed based on the quantization error that has been generated by that pixel. Likewise, the process is continuing until all the pixels in the image are processed. When we process the pixel o, there is no other unprocessed pixel in the image, therefore it doesn't make any changes in the neighboring pixels. Then the secret color image is transformed into three halftone images (C, M, Y) using Floyd-Steinberg Error Diffusion Technique. Experimental results show that Floyd Steinberg method gives better PSNR and reduced error rate. The amount of error which is spread to right and bottom is 3/8 whereas diagonal is 1/8.

C. *Histogram Localization based Blockwise Approach*

This novel technique is used to produce shares of the highly confidential secret image without pixel expansion. The major negative aspect of visual cryptography scheme is the pixel expansion problem. In this, each pixel is replaced by block of subpixels. It leads to increasing storage and transmission cost. Also the existing techniques are not enough to regenerate secret image with good quality. Considering these limitations, we proposed the method Histogram Localization based Blockwise approach to generate shares According this approach, first the halftone image is divided into blocks.

Each blocks have m x n size, so that adjust the image size to get exact blocks. Each block is replaced by another block to generate shares, for that we consider histogram and localization of the original image. Our blockwise approach is shown in Fig. 5. According to this method, each halftone image is divided into 2 x 2 block and each block is substituted by two sets of same size block to generate shares. Each pixel component we are doing the same process for each color component, so that each component will create two shares. To get final shares we need to combine first shares of each color component to generate share-1 and second shares of each color to generate share-2.
To reconstruct simply it required to superimpose these shares. This method circumvents pixel expansion problem.

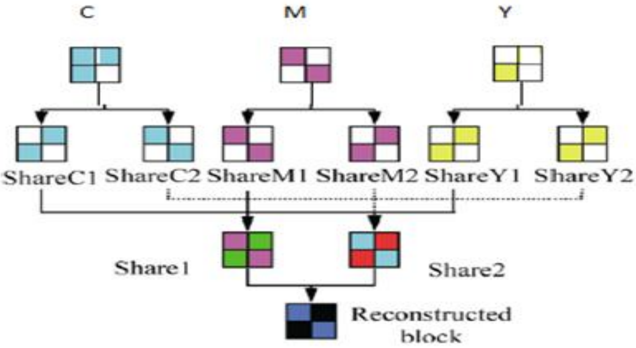

Fig. 5. Blockwise Approach

Histogram means graphical representation of an image and localization means number of black pixels in a particular block that is represented as one. Histogram is tested to identify whether it is left skewed or right skewed or normal distribution. If histogram of the original image is in normal distribution and the localization value of a particular block is less than 2, then randomly select the encoding combinations from Table 1, if the localization value is equal to 2 then randomly select an encoding combinations from Table 2 and if the localization value is greater than 2 then from Table 3. If histogram of the original secret image is left skewed and the localization value of a particular block is less than 1, then randomly select the encoding combinations from Table 1, if the localization value is equal to 1 then from Table 2 and if the localization value is greater than 1 then from Table 3. If histogram of the original secret image is right skewed and the localization value of that block is less than 3, then randomly select the encoding combinations from Table 1, if the localization value is equal to 3 then from Table 2 and if the localization value is greater than 3 then from Table 3. This process is repeated for the entire image to generate two shares C1 and C2.

Table 1. Encoding combinations for case 1

Basis Matrices		Possible Reconstructed Secret Blocks
Share 1	Share 2	
[0 0 1 1]	[0 0 1 1]	[0 0 1 1]
[0 1 0 1]	[0 1 0 1]	[0 1 0 1]
[0 1 1 0]	[0 1 1 0]	[0 1 1 0]

[1 0 0 1]	[1 0 0 1]	[1 0 0 1]
[1 0 1 0]	[1 0 1 0]	[1 0 1 0]
[1 1 0 0]	[1 1 0 0]	[1 1 0 0]

Similarly, the same process is repeated for Magenta halftone image to generate shares M1 and M2 and also Yellow halftone image to generate shares Y1 and Y2. Completion of this step will yield totally six shares named as C1, C2, M1, M2, Y1 and Y2. The shares C1, M1 and Y1 are combined to generate final share-1 (S1). The shares C2, M2 and Y2 are combined to generate the final share-2 (S2).

Table 2. Encoding combinations for case 2

Basis Matrices		Possible Reconstructed Secret Blocks
Share 1	Share 2	
[0 0 1 1]	[0 1 0 1]	[0 1 1 1]
[0 0 1 1]	[1 0 0 1]	
[0 0 1 1]	[0 1 1 0]	
[0 0 1 1]	[1 0 1 0]	
[1 1 0 0]	[0 1 0 1]	
[1 1 0 0]	[0 1 1 0]	
[1 1 0 0]	[1 0 0 1]	[1 0 1 1]
[1 1 0 0]	[1 0 1 0]	
[0 1 0 1]	[0 0 1 1]	
[0 1 0 1]	[1 0 0 1]	
[0 1 0 1]	[0 1 1 0]	
[0 1 0 1]	[1 1 0 0]	
[1 0 0 1]	[0 0 1 1]	[1 1 0 1]
[1 0 0 1]	[0 1 0 1]	
[1 0 0 1]	[1 0 1 0]	
[1 0 0 1]	[1 1 0 0]	
[0 1 1 0]	[0 0 1 1]	
[0 1 1 0]	[1 0 1 0]	
[0 1 1 0]	[0 1 0 1]	[1 1 1 0]
[0 1 1 0]	[1 1 0 0]	
[1 0 1 0]	[0 1 1 0]	
[1 0 1 0]	[0 0 1 1]	
[1 0 1 0]	[1 0 0 1]	
[1 0 1 0]	[1 1 0 0]	

Table 3. Encoding combinations for case 3

Basis Matrices		Possible Reconstructed Secret Blocks
Share 1	Share 2	
[1 0 0 1]	[0 1 1 0]	[1 1 1 1]
[1 0 1 0]	[0 1 0 1]	
[1 1 0 0]	[0 0 1 1]	
[0 1 1 0]	[1 0 0 1]	
[0 0 1 1]	[1 1 0 0]	
[0 1 0 1]	[1 0 1 0]	

D. *Recovering of Secret Image*

The shares S1 and S2 are collected first in order to renovate the secret image. Now these shares are printed on transparent sheets and stacked together, these sheets will recover the original secret image. In this approach the recovered image has good visual quality. Decryption is done by human vision to interpret the original secret image. This method provides more security and also it increases the visual quality of the renovated image. The algorithm of our proposed work is given below,

Step 1: Adjust the size of the original secret image so that the size will be multiple of 4. Every 2x2 pixel block is selected for encoding.

Step 2 : Decompose the secret image into Cyan, Magenta and Yellow color images.

Step 3: The decomposed images (C, M &Y) are halftoned by applying Floyd Steinberg error diffusion method.

Step 4: Select the halftone image C and divide into 2 x 2 blocks.

Step 5: Find the histogram and local ratio (n) of the original image.

i) If histogram is normal distribution then
- If n < 2 then, randomly choose the encoding combinations from Table 1.
- If n = 2 then, randomly choose the encoding combinations from Table 2.
- If n > 2 then, randomly choose the encoding combinations from Table 3.

ii) If histogram is right skewed then
- If n < 1 then, randomly choose the encoding combinations from Table 1.
- If n = 1 then, randomly choose the encoding combinations from Table 2.
- If n > 1 then, randomly choose the encoding combinations from Table 3.

iii) If histogram is left skewed then
- If n < 3 then, randomly choose the encoding combinations from Table 1.
- If n = 3 then, randomly choose the encoding combinations from Table 2.
- If n > 3 then, randomly choose the encoding combinations from Table 3.

iv) Repeat the steps (i) to (iii) until the entire block of the image is processed. This will generate shares C1 and C2.

Step 6: Repeat the steps 4 and 5 for M and Y halftone images and generate shares M1 and M2 & Y1 and Y2.

Step 7: Combine the shares C1, M1 and Y1 to generate share S1 and shares C2, M2 and Y2 to generate share S2.

Step 8: Now these shares S1 and S2 are dispersed to participants.

Step 9: To recover the secret image, the scattered shares are collected and printed on transparencies and stacking these transparencies renovate the original secret color image.

IV. EXPERIMENTAL RESULTS

The proposed approach is implemented using MATLAB and tested for several images. A sample secret image given as input to the proposed work is shown in Fig. 6. The first step in the proposed work is color decomposition of original image; the decomposed images are shown in Fig. 7. Then Floyd Steinberg error diffusion method is applied on the secret image, the output is shown in Fig. 8. The generated shares S1 and S2 after applying histogram localization based blockwise approach on the halftone images, are shown in Fig. 9. The reconstructed image of our proposed work is shown in Fig. 10. The simulation result shows that our proposed technique provides more security and also the visual quality of the renovated image is increased.

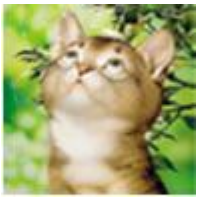

Fig. 6. Secret Image

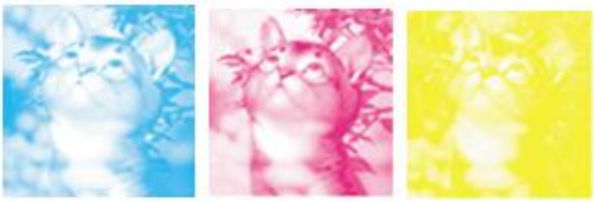

Fig. 7. Decomposed Images (Cyan, Magenta and Yellow)

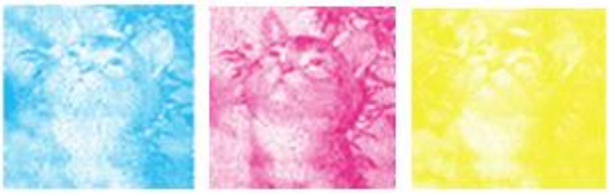

Fig. 8. Halftoned Images (Cyan, Magenta and Yellow)

Fig. 9. Generated shares S1 and S2

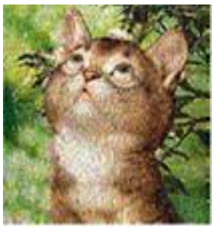

Fig.10. Reconstructed Image

The result of the proposed work is compared with the previous schemes like Ross et.al scheme, Ito et al. scheme and Chen et al. scheme. The comparison among these schemes is shown in Table 4. It shows the proposed work has the high visual quality than the other schemes and the PSNR value is also calculated to prove the same.

Table 4. Comparison of the proposed scheme with the other schemes

Features	**Ross et al. scheme [13]**	**Ito et al. scheme [9]**	**Chen et al. scheme [14]**	**Proposed scheme**
Pixel Expansion	Yes	No	No	No
Type of Shares	Meaning less	Meaning less	Meaning less	Meaning less
Histogram types	Normal	Normal	Normal, Right skewed and left skewed	Normal, Right skewed and left skewed
Visual Effect of Recovered Image	Medium	Medium	High but regionalization	High
PSNR	28.11	28.72	30.93	34.15

V. CONCLUSION

In this paper we have explored novel visual cryptography scheme using Histogram Localization based Blockwise approach. In this approach we are applying blockwise approach to evade pixel expansion problem and also to increase visual quality by considering two parameters histogram and localization value. It provides more security at the same time the visual quality of the renovated image is also increased. This work can be extended to compressed images like JPEG in future.

REFERENCES

1. M. Naor and A. Shamir, "Visual Cryptography," Advances in Cryptograhy: EUROCRYPT '94, LNCS, vol. 950, 1994, pp. 1-12.
2. G. Ateniese, C. Blundo, A. De Santis, D.R.Stinson, "Visual Cryptography for General Access Structures", Information and Computation, vol. 129, 1996, pp. 86-106.
3. Kai-Hui Lee and Pei-Ling Chiu, "An Extended Visual Cryptography Algorithm for General Access Structures," IEEE Transactions on Information Forensics and Security, vol. 7, no. 1, 2012, pp. 219-229.
4. Mitsugu Iwamoto, "A Weak Security Notion for Visual Secret Sharing Schemes", IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 372-382.
5. C.S. Hsu and Y.C.Hou, "Copyright Protection Scheme for Digital Images using Visual Cryptography and Sampling Methods," Optical Engineering, vol. 44, no. 7, 2005, 077003.
6. M.Naor, B.Pinkas, "Visual Authentication and Identification," Advances in Cryptology – CRYTO '97, LNCS, vol. 1294, 1997, pp. 322-336.
7. Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo, "Halftone Visual Cryptography," IEEE Transactions on Image Processing, vol. 15, no. 8, 2006, pp. 2441-2453.
8. Zhongmin Wang, Gonzalo R. Arce, and Giovanni Di Crescenzo, "Halftone Visual Cryptography Via Error Diffusion," IEEE Transactions on Information Forensics and Security, vol. 4, no. 3, 2009, pp. 383-396.
9. Ryo Ito, Hidenori Kuwakado and Hatsukazu Tanaka, "Image Size Invariant Visual Cryptography," IEICE Transactions on Fundamentals, vol. E82–A, no. 10, 1999, pp. 2172-2177.
10. Chang-Chou Lin, Wen-Hsiang T sai, "Visual Cryptography for Gray-level Images by Dithering Techniques," Pattern Recognition Letters, vol. 24, 2003, pp. 349-358.
11. Sudharsanan S, "Shared Key Encryption of JPEG Color Images," IEEE Transactions on Consumer Electronics, vol. 51, no. 4, 2005, pp. 1204-1211.
12. InKoo Kang, Gonzalo R. Arce, and Heung-Kyu Lee, "Color Extended Visual Cryptography Using Error Diffusion," IEEE Transactions on Image Processing, vol. 20, no. 1, 2011, pp. 132-145.
13. Arun Ross and Asem Othman, "Visual Cryptography for Biometric Privacy," IEEE Transactions on Information Forensics and Security, vol. 6, no. 1, 2011, pp. 70-81.
14. Yu-Chi Chen, "Fully Incrementing Visual Cryptography from a Succinct Non-Monotonic Structure," IEEE Transactions on Information Forensics and Security, vol. 12, no. 5, 2017, pp. 1082-1091.
15. Xingxing Jia, Daoshun Wang, Daxin Nie, and Chaoyang Zhang, "Collaborative Visual Cryptography Schemes," IEEE Transactions on Circuits and Systems for Video Technology, vol. 28, no. 5, 2018, pp. 1056-1070.
16. V. Udayini, Ch. Hima Bindu and P. Naga Malleswari, "Iris Image Authentication using Visual Cryptography," International Journal Recent Technology and Engineering, vol. 8, no. 1, 2019, pp. 288-291.

AUTHORS PROFILE

D. R. Denslin Braja, received the Bachelor of Engineering in Information Technoogy from Manonmaniam Sundaranar University and Master of Engineering in Computer Science and Engineering from Annamalai University, Tamilnadu, India in 2004 and 2006 respectively. Currently she is pursuing PhD in the Department of Computer Science and Engineering, Noorul Islam University, Tamilnadu, India. Her research interests include Cryptography, Network Security and Image Processing.

V. S. Dharun, received Ph.D. degree in Applied Electronics & Computer Science Engineering from the Manonmaniam Sundaranar University, India, in 2013. Currently he is serving as Professor at Immanuel Arasar JJ College of Engineering, Kanyakumari, India. His current research interests include Medical Image Processing, Speech Signal Processing, Wireless Networking.

D.R.Denslin Brabin received Ph.D. degree in Information and Communication Engineering from the Anna University, India in 2018. He has 16 years of teaching experience. He has published more than 10 research papers in International Journals. His current research interests include Image Processing and Cyber Security.