Error Filtering Schemes for Color Images in Visual Cryptography

Shiny Malar F.R
Dept. of Computer Science & Engineering
Noorul Islam University, Kumaracoil
Kanyakumari district, India

Jeya Kumar M.K
Professor, Dept. of Computer Applications
Noorul Islam University, Kumaracoil
Kanyakumari District, India

Abstract - **The color visual cryptography methods are free from the limitations of randomness on color images. The two basic ideas used are error diffusion and pixel synchronization. Error diffusion is a simple method, in which the quantization error at each pixel level is filtered and fed as the input to the next pixel. In this way low frequency that is obtained between the input and output image is minimized which in turn give quality images. Degradation of colors are avoided with the help of pixel synchronization. The proposal of this work presents an efficient color image visual cryptic filtering scheme to improve the image quality on restored original image from visual cryptic shares. The proposed color image visual cryptic filtering scheme presents a deblurring effect on the non-uniform distribution of visual cryptic share pixels. After eliminating blurring effects on the pixels, Fourier transformation is applied to normalize the unevenly transformed share pixels on the original restored image. This in turn improves the quality of restored visual cryptographic image to its optimality. In addition the overlapping portions of the two or multiple visual cryptic shares are filtered out with homogeneity of pixel texture property on the restored original image. Experimentation are conducted with standard synthetic and real data set images, which shows better performance of proposed color image visual cryptic filtering scheme measured in terms of PSNR value (improved to 3 times) and share pixel error rate (reduced to nearly 11%) with existing grey visual cryptic filters. The results showed that the noise effects such as blurring on the restoration of original image are removed completely.**

Keywords - Error Diffusion; Visual Cryptography; Fourier Filtering; Context Overlapping; Color Extended Visual Cryptography.

I. INTRODUCTION

Visual Cryptography, an encryption technique allows cryptic to be possible only if the proper key is supplied by the user and decryption can be performed without the intervention of the computer. It works on the principle that when an image is splited into k shares only the user who has all the k shares can decrypt the message, any k-1 shares held by the user do not contain any useful information[1].

Naor and Shamir [2], in 1994 proposed a new security technique named visual cryptography scheme. In this technique, a secret image of type binary is encoded in a cryptographical manner into random binary patterns which contains n shares in a k-out-of-n scheme. The n shares are distributed among n participants in such a way the each participant's share is not known to another participant. The secret image can be visually revealed by k or more participants by joining all the shares available. Even if computational power decoding is available, cannot be done on the secret image by k-1 or fewer participants.

As the shares in the layers occur as random noise, the attackers cannot identify any useful information about the individual shares. Even with the availability of computer, it is not possible to decrypt the message or information with the limited availability of the share. The limitation of the above method is its randomness without any visual information. Extended Visual Cryptography have been suggested which also suffers from the same drawbacks of randomness. This paper is well thought-out as follows, Section II deals with the review of literature. Section III described about the error filtering schemes for color images. Section IV and V offered to Experimental result and discussion .Finally the conclusion of this paper in Section VI.

II. RELATED WORKS

Recently in the literature, many new methods have been implemented for visual cryptography. In 1995 Naor and Shamir [3], have predicted an optimal dissimilarity in k-out-of-n scheme to alleviate the contrast loss problem in the reconstructed image. 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. To overcome this problem the basic secret sharing scheme is extended to general access structure. The concept of general access structure method was introduced in the year 1996 and 1997, by Ateniese, C.Blundo, A.Desantis and D.R.Stinson [4 , 5,6,7].In 1999,[8,9] Image size invariant visual cryptography was introduced by R. Ito, H. Kuwakado, and H. Tanaka and also in the same year the C.-N. Yang and C.-S. Laih have proposed some new types of visual secret sharing schemes.

In previous works of visual cryptography, binary images were concentrated which is not enough in real time applications. This general access structure method is applied to the gray level images are introduced by L. A. MacPherson,Chang Choulin[10,11,12],in the year 2000. In 2001 the G. Ateniese, C. Blundo, A. Santis, and D. R. Stinson have predicted the extended capabilities for visual cryptography in the natural images [13-16]. Ateniese has projected the hypergraph coloring method for Visual cryptography , which is used to construct meaningful binary shares. Since hypergraph colorings are constructed by random distributed pixels, this method produce insufficient results. A new method of Extended visual cryptography for natural images is used to produce meaningful binary shares which is predicted by Nakajima[17,18] in the year 2002.Wen-Hsiang Tsai[19-23] have estimated the dithering technique which is applied to gray level images in visual cryptography. This technique is used for transformation of gray level images into binary images in the year 2003 . Again, Hou[24,25] 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.

In 2006 the Zhi Zhou, Gonzalo, R.Arce and Giovanni Dicrescenzo [29-33] have proposed halftone visual cryptography which produce good 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 maintained contrast and security. Abhishek parakh and Subhash Kak have proposed recursive threshold visual cryptography which is used in network applications and also reduce the network load. In 2007 the C.M. Hu and W.G. Tzeng [34, 35] have proposed a cheating method in Visual Cryptography schemes. In their cheating method, the cheater needs to know the exact distribution of black and white sub pixels of the shares of honest participants. In the same year, a Cheating Prevention Scheme for Binary Visual Cryptography with Homogeneous Secret Images was introduced by D.S. Tsai, T.H. Chen, G. Horng, Which is used to prevent the cheater from obtaining the distribution [26, 27, 28].

However, the knowledge of distribution is not a necessary condition for a successful cheats. They also proposed another cheat-preventing method in which the stacking of the genuine share and verification share reveals the verification image in some small region that it is possible to attack the method. Niranjan Damera-Venkata, and Brian L. Evans have predicted the design and analysis of vector color error diffusion halftoning systems. And also quantization of accumulate diffused errors in error diffusion method was introduced by Ti-Chiun Chang and Jan P. Allebach in the year 2005 [26, 27, 28].

In 2009 the Zhongmin Wang, Gonzalo R. Arce,, and Giovanni Di Crescenzo [36,37] have proposed the Visual Cryptography for color image using visual information pixel (VIP) synchronization with error diffusion technique. They are introduced a color Visual Cryptography encryption method which leads to significant shares and is free of the previously mentioned limitations. This method is used to filtering the error in an image and produces the meaningful shares. The error filtering schemes for color images is very simple and efficient method.

III. ERROR FILTERING SCHEMES FOR COLOR IMAES

A. Fourier filtering for color visual cryptographic images

The Fourier Transform of an image can be carried out using the Discrete Fourier Transform (DFT) method. Fig.1 shows the DFT also allows spectral data (i.e. a transformed image) to be inverse transformed, producing an image once again. If we compute the DFT of an image, then immediately inverse transform the result, we expect to regain the same image. If we multiply each element of the DFT of an image by a suitably chosen weighting function we can accentuate certain frequency components and attenuate others. The corresponding changes in the spatial form can be seen after the inverse DFT has been computed.

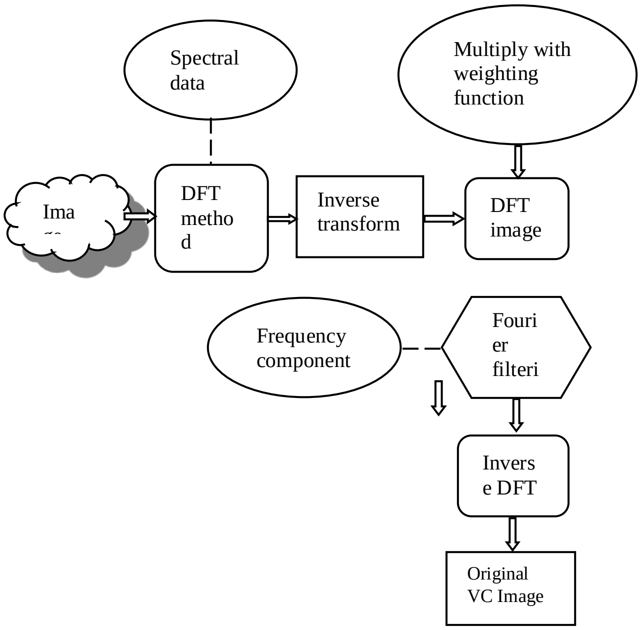

Figure 1. Fourier filtering for color visual cryptographic images.

The selective enhancement/suppression of frequency components is known as Fourier Filtering. The fourier filtering is used for convolution with large masks (Convolution Theorem), compensate for known image defects (restoration), reduction of image noise, suppression of 'hum' or other periodic interference and reconstruction of original restored visual cryptographic image.

1) Fourier Filtering

The DFT is the sampled Fourier Transform and does not have all frequencies to form an image, but only a set of forms which is large enough to fully define the spatial domain image. The total number of frequencies correspond to the total number of pixels in the spatial domain image, ***i.e.*** the image in the spatial and Fourier domain is of the equal size.

For a square image of size $N \times N$, the two-dimensional DFT is shown in the equation 1.

$$F (x,y) = \sum_{p=0}^{N-1} \sum_{q=o}^{N-1} f (p,q)\, e^{-y2\Pi (xp/N + yq/N)} \qquad (1)$$

where f(p,q) is the image in the spatial domain . The exponential term is the basic function corresponding to each point F(x,y)in the Fourier space. The value of each point F(x,y) is calculated by multiplying the spatial image with the corresponding base function and adding the result.

Similarly, the Fourier image can be re-transformed to the spatial domain. The inverse Fourier transform is exposed in the equation 2.

$$f (i,j) = 1/ N^2 \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} F (x,y)\, e^{y2\Pi (xi / N + yj / N)} \qquad (2)$$

Here, $\frac{1}{N^2}$ normalization term in the inverse transformation. Sometimes, this normalization is carried out for the forward transformation instead of the inverse transformation. To access the result for the above equations, a double sum has to be obtained for each image point. However, the Fourier Transform is given by equation 3.

$$F(x,y) = 1/N \sum_{j=0}^{N-1} K (x, j)\, e^{-y2\Pi pj / N} \qquad (3)$$

where

$$K (x, j) = 1 / N \sum_{i = 0}^{N-1} f (i, j)\, e^{-y2\Pi xi / N}$$

By using these two equations, initially the spatial domain image is transformed into an intermediate image using ***N*** one-dimensional Fourier Transforms. This intermediate image is then transformed into the final image, again use ***N*** one-dimensional Fourier Transforms. Expressing the two-dimensional Fourier Transform in terms of a series of ***2N*** one-dimensional transform reduces the number of needed computationsB. *Texture overlapping*

Texture overlapping filters decide which parts of the input image to be patched into the output texture. After finding a good patch offset between two inputs, the computer is the best patch seam (the seam yielding the highest possible MRF likelihood among all possible seams for that offset). The two overlapped visual cryptic shares images are copied to the output, cut by max-flow/min-cut algorithm and then stitched together along optimal seams to generate a new output that is shown in fig.2. When filtering an overlapped texture, we want the generated texture to be perceptually similar to the original image. In this approach, the concept of perceptual similarity has been formalized by a Markov Random Field (MRF). It brings an accurate estimation of perceptual effect according to human's vision.

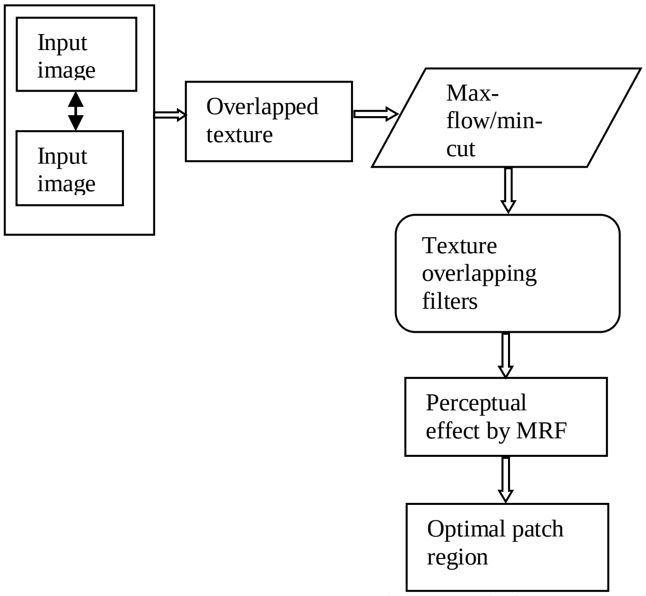

Figure 2. Texture overlapping method

In most of other techniques, the size of the patch is chosen a-prior. But this texture overlap filtering technique determine the optimal patch region for any given offset between the input and output texture. Finally the performance measure checks this flexibility for different offsets.

Let us assume a secret image *A* of N_R *X* N_M. Each pixel of *A* can take any one of M different colors or gray-levels. Image *A* is represented by an integer matrix A given by equation 4.

$$A = [a_{pq}]\, N_R \text{ X } N_M \qquad (4)$$

Now *M =2* for a binary image, and *M =256* for a grayscale image with one byte per pixel. In a color image, the pixel value will be an index to a color table, thus *M = 256*. In a color image using an RGB model, each pixel has three integers: R (red), G (green) and B (blue). If each R, G or B takes value between 0 and 255, we have *M = 2563.*

The VCS requires taking pseudo-random numbers as input to guide the choice of the share matrices. Denote the share matrices in M_p *as* S_0^p *,....* $S^q{}_{|Mp|-1}$, and denote $P\,(S^p{}_q\,)$ *for p = 0, 1 and q = 0, 1,.....* $|Mp|$*-1* as the probability that choosing the share matrix $S^p{}_q$ .Hence the input of the pseudo-random numbers should guarantee ,that is represented as shown in the equation 5.

$$P\,(S^p{}_0) = P\,(S^p{}_1) = ... = P\,({}^{Sp}{}_{|Mp|-1}) \qquad (5)$$

In order to choose a share matrix pseudo-randomly in *Mp* , the dealer needs at least $log_2\,|Mp|$ bits pseudo-random numbers (we will consider the case that $log_2\,|Mp|$ is not an integer in a later time). Denote *B(q)* as the binary representation of integer q with length $log_2\,|Mp|$, i.e. *B(q)* is the binary string that represents q. Without loss of generality, we assume that when the input pseudo-random number is *B(q)*, the dealer chooses the share matrix $S^p{}_q$ to encrypt the secret pixel p,and denote *P(B(q))* as the probability of generating the binary string B(q) by the pseudo-random generator. According to the equation 6,

$$P(B(0))=P(B(1))= ….. =P(B(|Mp|-1)) \qquad (6)$$

In fact the cipher texts of the AES and Twofish have satisfied the above equation, because they have passed the serial test. Hence, take the AES and Twofish as the pseudo-random generator.

IV. Experimental Results

In this paper, the experimental simulation is conducted by using the image processing software package (MATLAB). The color image (RGB image) is stored in MATLAB as an M-by- N-by-3 data array that defines red, green, and blue color components for every individual pixel. The color of each and every pixel is defined by the combination of the red, green, and blue intensities stored in each color plane at the pixel's location

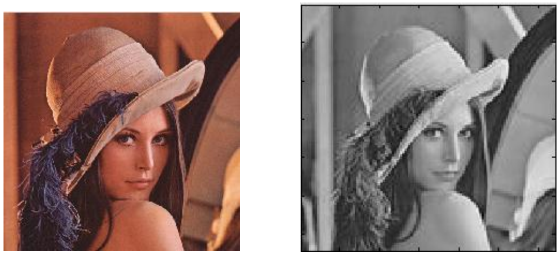
a)Input image b) DFT image

Figure. 3 The experimental result of original input image with out Using error diffusion and DFT image using Fourier Filtering.

During the experiment, uncompressed image is taken as input image. Here used (2, 2) VCS scheme and consider the Lena color image of size 256 X 256 for experimental results shown in fig. 3(a). This input image is multiplied with the filter function in a pixel-by-pixel model. To have the resulting image in the spatial domain, filtered image has to be re-transformed using the inverse Fourier Transform. The most simple low pass filter is used to suppress all frequencies greater than the cut-off frequency and it leaves smaller frequencies unchanged. In most implementations, cut-off frequency is taken as a fraction of the highest frequency represented in the Fourier domain image shown in fig. 3(b).

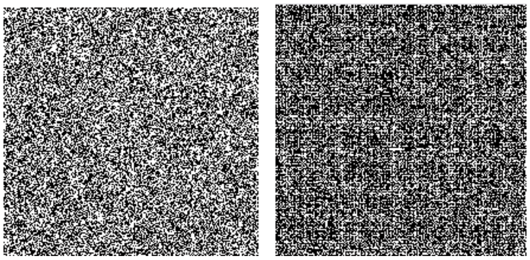
(a)Share1 image (b) Share2 image

Figure. 4 Experimental result of (2,2) Visual cryptography Shares using error diffusion with the fourier Filtering method.

The (2, 2) VCS scheme is illustrated to introduce the basic concepts of texture overlapping schemes. In the encryption process every secret pixel is splitted into two shares. Each share belongs to the corresponding share image. In the decryption process the two corresponding shares are joined together by using OR operation to retrieve the secret pixel. Two share of a white secret pixel are of the equal while those of a black secret pixel are complementary as shown in Figure 4(a) and (b).

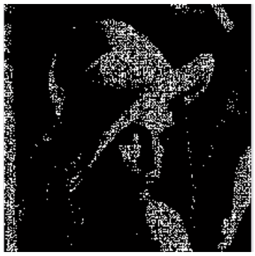
Figure 5. Decoded image from shares
Error diffusion with texture Overlapping

Consequently a white secret pixel is retrieved by a share with the combined result of half white sub-pixels and a black secret pixel is retrieved by all black. Using this basic VCS Scheme we can’t completely retrieve the white Secrete pixel which generates loss in contrast. In XOR based VCS scheme where the share images are superimposed using XOR operation which results in perfect reconstruction of both Black and white pixels as shown in Figure 5 and sub sampling a 2 X 2 share into a single pixel we get decrypted image of the same size as original secret image.

The essential parameter indicates the superiority of the renovation is the Peak Signal-To-Noise Ratio(PSNR). PSNR is the ratio between the maximum possible power of the signal and the power of corrupted noise that is articulated in decibels.

Mean Square Error = Error/Size of the image (7)

The Mean Square Error is the average square of the error in particular images. The calculation of MSE & PSNR is given by the equation 8and equation 9.

$$MSE = 1/MN \left[\sum_{i=1}^{M} \sum_{j=1}^{N} (I_{ij} - I'_{ij})_2 \right] \qquad (8)$$

$$PSNR = 20 * \log10\,(255 / \mathrm{sqrt}(MSE)) \qquad (9)$$

Where, 255 is the maximum possible value of the image. In general the Peak signal -to-noise ratio for the two shares are increased and the perceived error for that two shares are decreased [38]. The imitation result also shows that the proposed scheme is compared to the existing scheme that is shown in table 1.

TABLE I. COMPARE THE EXISTING ERROR FILTERING METHOD AND PROPOSED ERROR FILTERING METHOD.

Error filtering Method	VC Scheme	Size of the Image	Test image - Lena	
			PSNR in dB	Error Ratio
Floyd & Steinberg Error Filtering (Existing)	2-out-Of-2	256 X 256	11.91	4.74
Discrete Fourier Filtering (Proposed)	2-out-Of-2	256 X 256	36.5826	0.0290

These works are some examples that prove the improvements and high performance of the color images in visual cryptography and also reduce the perceived errors.

V. Results and Discussion

This section provides some experimental results to exemplify the effectiveness of the proposed method. The scheme proposed generates meaningful color shares with high quality as well as the colorful decrypted share by using Filtering scheme. The performance of the proposed method is evaluated and exposed in table.1 (that is, our proposed method is compared with the previous methods). VC can be treated as a special case in our proposed methods, which means no visual information is carried by the share. In existing method, shares carry visual information and there is a tradeoff between the contrast of the reconstructed image and the contrast of the share image. This tradeoff is similar to the tradeoff between the contrast of the reconstructed image and the image quality of the halftone shares in the proposed methods. Compared with the existing methods, our method achieves better image quality, which is given in table2.

Table 2. Reducing the error ratio of the images and Meaningful color shares with high visual Quality.

Existing Method				Proposed Method			
No.of Pixels	Error Rate	Color Shares	Error Rate	No. of Pixels	Error Rate	Color Shares	Error Rate
1000	11	500	22	1000	8	500	18
2000	19	750	29	2000	9	750	19
3000	28	1000	32	3000	13	1000	20
4000	38	1250	50	4000	19	1250	21
5000	48	1500	60	5000	23	1500	22

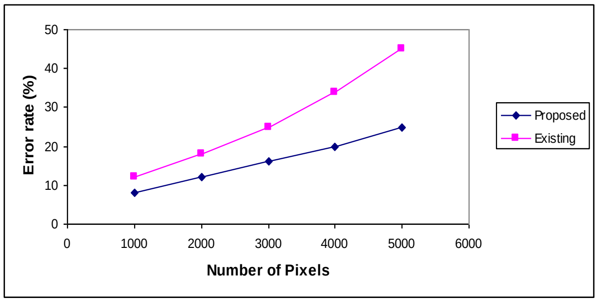

Figure 6. Number of pixels Vs Error rate

The results of experiments in which figure 6 and figure 7 indicate that the reducing the error ratio of the images and meaningful color shares with high visual quality that can improve the overall performance of the visual cryptography using texture overlapping and fourier filtering. The error rate is reduced to 11% compared with the existing scheme.

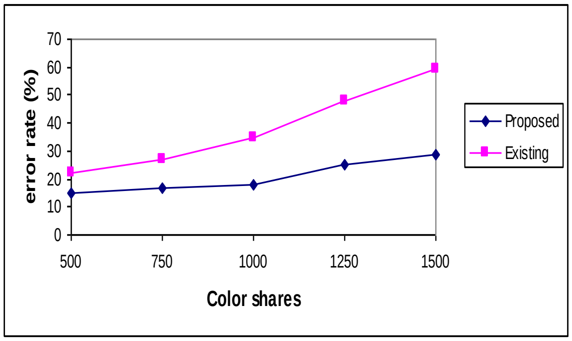

Fig 7. Color Shares Vs Error rate

VI. Conclusion

Some methods for color visual cryptography are not satisfactory in terms of producing either meaningless shares or meaningful shares with low visual quality, leading to suspicion of encryption. In the existing work of color VC the quality of images being restored depends on error diffusion, other image degradations due to blurring, transformation and overlapping were not handled in it.

The color VC focuses on the encryption method, to produce color Extended Visual Cryptographic System deploying VIP (Visual Information Pixel) Synchronization and Error Diffusion for improvement of quality. Error Diffusion results in the shares with good quality images and VIP Synchronization regains the actual values before and after encryption. This paper enhances the image quality on color visual cryptography using texture overlapping and Fourier filtering. The proposal in our work improves the image quality on restored original image from visual cryptic shares by presenting an efficient color image visual cryptic filtering scheme. The color image visual cryptic filtering method is presented here for deblurring effect on the non-uniform distribution of visual cryptic share pixels.

In the future, color image visual cryptic filtering scheme proposed in this paper, can be used to maintain digital document trade marking and licensing with ownership security schemes. Various multi-party security models used recently can be adapted in the future for the ownership security. Privacy preservation techniques (i.e., data transformation and perturbation) can also be considered for future direction in providing ownership confidentiality of digital documents.

Acknowledgement

The authors would like to thank the anonymous reviewers for their valuable advice and suggestions that have contributed to the improvement in the quality and presentation of this paper. In particular, we thank the reviewer who pointed us to error filtering method in this paper.

REFERENCES

[1] InKoo Kang, Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Heung-Kyu Lee, Member, IEEE," Color Extended Visual Cryptography Using Error Diffusion," IEEE Transactions on image processing, vol. 20, no. 1, pp. 132-145, January 2011.

[2] M.Naor and A.Shamir, "Visual Cryptography ", in pro. EUROCRYPT, 1994,pp. 1-12.

[3] M.Naor and A. Shamir, Visual Cryptography, in "Advanced in Cryptology – EUROCRYPT'94", A. De. Santis, Ed., Vol. 950 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, PP. 1-12,1995.

[4] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual cryptographyfor general access structures," Inf. Comput., vol. 129, no. 2, pp. 86–106, 1996.

[5] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, Extended Schemes for Visual Cryptography, submitted to Discrete Mathematics, 1996.

[6] M. Naor and B. Pinkas, "Visual authentication and identification," in Proc. Advances in Cryptology, 1997, vol. 1294, LNCS, pp. 322–336.

[7] E. R. Verheul and H. C. A. Van Tilborg, "Constructions and properties of k out of n visual secret sharing schemes," Designs, Codes, Cryptog,,vol. 11, no. 2, pp. 179–196, 1997.

[8] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," IEICE Trans. Fund. Electron. Commun. Comput. Sci., vol.E82-A, no. 10, pp. 2172–2177, 1999.

[9] C.-N. Yang and C.-S. Laih, "Some new types of visual secret sharing schemes," in Proc. Nat. Computer Symp., 1999, vol. 3, pp. 260–268.

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

[11] T. Hofmeister, M. Krause, and H. U. Simon, "Contrast-optimal k out of n secret sharing schemes in visual cryptography," heoreti. Comput.Sci., vol. 240, pp. 471–485, 2000.

[12] C. N. Yang and C. S. Laih, "New colored visual secret sharing schemes," Designs, Codes Crypt., vol. 20, no. 3, pp. 325–336, 2000.

[13] 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.

[14] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended Schemes for Visual Cryptography". Theoretical Computer Science, No. 250, pp. 143-161, 2001.

[15] C. Blundo, A. De Bonis and A. De Santis, ' Improved Schemes for Visual Cryptography". Designs, Codes, and Cryptography, No. 24, pp. 255–278, 2001.

[16] Niranjan Damera-Venkata, and Brian L. Evans, "Design and Analysis of Vector Color Error Diffusion Halftoning Systems"IEEE transactions on image processing, vol. 10, no. 10, pp. 1552 - 1565 October 2001.

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

[18] W.-G. Tzeng and C.-M. Hu, "Anewapproach for visual cryptography," Designs, Codes, Cryptog., vol. 27, no. 3, pp. 207–227, 2002.

[19] 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.

[20] C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson, "Contrast Optimal Threshold Visual Cryptography Schemes' , SIAM J. on Discrete Math. 16, pp. 224-261, 2003.

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

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

[23] C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images" Pattern Recognit. Lett., vol. 25, pp. 349–358,2003.

[24] M. Krause and H.-U. Simon, "Determining the optimal contrast for secret sharing schemes in visual cryptography," Combin., Probab. Comput., vol. 12, no. 3, pp. 285–299, 2003.

[25] C.-N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognit. Lett., vol. 25, no. 4, pp. 481–494, 2004.

[26] D. Jin, W. Q. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," J. Electron. Imag., vol. 14, no. 3, p. 033019, 2005.

[27] Ti-Chiun Chang and Jan P. Allebach, "Quantization of Accumulated Diffused Errors in Error Diffusion", IEEE Transactions on image processing, vol. 14, no. 12, pp. 1960 – 1975 , December 2005.

[28] C. N. Yang and T. S. Chen, "Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion," Pattern Recogniti. Lett., vol.26, pp. 193–206, 2005.

[29] W. P. Fang and J. C. Lin, "Progressive viewing and sharing of sensitive images," Pattern Recogniti. Image Anal., vol. 16, no. 4, pp. 632–636,2006.

[30] 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.

[31] 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.

[32] G. Horng, T.H. Chen, D.S. Tsai, "Cheating in Visual Cryptography," Designs, Codes and Cryptography, Vol. 38, No.2, pp. 219-236, 2006.

[33] S. J. Shyu, "Efficient visual secret image sharing for color images," Pattern Recognit., vol. 39, no. 5, pp. 866–880, 2006.

[34] C.M. Hu and W.G. Tzeng, "Cheating Prevention in Visual Cryptography," IEEE Transactions on Image Processing,Vol. 16, No. 1, pp. 36-45, 2007.

[35] D.S. Tsai, T.H. Chen, G. Horng, "A Cheating Prevention Scheme for Binary Visual Cryptography with Homogeneous Secret Images," Pattern Recognition, Vol. 40, No. 8, pp. 2356-2366, 2007.

[36] Zhen He ,'Hierarchical Error Diffusion", IEEE Transactions on image processing, Vol. 18, No. 7, pp. 1524-1534, July 2009

[37] 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, 383-395, September 2009.

[38] 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.

AUTHORS PROFILE

F.R. Shiny malar was born in Nagercoil,Tamil Nadu State,India in 1986. She studied Information Technology in theSt.Xavier's Catholic college of Engineering, Chunkankadai, Kanyakumari District, Tamilnadu State,India fom 2003 to 2007. She received Bachelor‟ sdegree from Anna University, chennai 2007. And received the Master degree from Manonmaniam Sundaranar University Tirunelveli. currently, she is a research scholar at the Department of Computer Science and Engineering, in Noorul Islam Center for Higher Education, Noorul Islam University, Kumarakoil, Tamilnadu, India; working in the area of image processing under the supervision of Dr. M. K. Jeya Kumar. She has presented a number of papers in national conferences and their research interest include image security , networking and image processing.

M. K. Jeya Kumar received his PhD degree in Mobile Adhoc Networks from Dr. MGR University,Chennai, India, in 2010. He is Assistant Professor at the Department of Computer Application, Noorul Islam University, Kanyakumari District, Tamilnadu,India. His research interests include networks andnetwork security, image processing and softcomputing techniques.