Advanced Share Creation by Random Matrix Using OFB in Visual Cryptography

DEBASHIS SANKI[1] DR. NISARG GANDHEWAR[2]

[1,2]Department of Computer Science & Engineering, Dr. A. P. J. Abdul Kalam University, Indore 452010, India
Correspond Author Email: Debashis.sanki @gmail.com

Abstract— In Cryptography Visual Cryptography is one of the important area for security of information. It can be applied for both image and test. This method is presenting a new approach of share creation with random values followed by OFB for individual share. The suggested method first creates RGB photos before applying the blowfish algorithm to build share1, share2. The updated technique works with RGB images, and shares are both encrypted and decrypted and flow slandered practice for staking and retrieving the image or message. The suggested system's testing outcomes are examined and contrasted with those of industry norms. The approach is created and put into action using Matlab code.

Key Terms—Visual cryptography, OFB, XOR, Share creation, Encryption Decryption, AES, RGB

I. INTRODUCTION

In today world information exchange is completely depend on internet or electronics commination. The amount of data exchanges also huge so it is very much important to protect the data. Visual cryptography is one of the important aspect towards the data security. The encryption and decryption process of visual cryptography is different. Decryption process of VC is based on stacking share one upon another and it include human visual system for retrieving information. The important area of VC is secret share creation. The meaning full shares are created and distributed among different parties. Later during retrieval of information are staked one upon another with proper sequence and the information is retrieved. The (k,n) share technique are also important innovation in the field of VC, where n share are created and distributed among n parties. Out of n minimum K share is required to retrieve the information, but if it is less than k then information should not be retrieved. The VC method was planned by Naor and Shamir in 1994 , and later more advancement and modification has been done by many researcher and Several techniques.By extending the original technique in this way, VC offers a safe means to transport and store data. Different section of the suggested paper are

II. RELATED WORK

C. Yang et al. have unveiled fresh designs for color VC schemes. The techniques explore expansion ,change of VC white-and-black method. It has been demonstrated that color VSS schemes can increase block length, and the sub pixel infrastructure for our suggested construction can be deployed right away in picture editing software.

TingyuanNie et al. [10], proposed that blowfish algorithm for encryption and decryption of images with a secret key block cipher.

L. N. Pandey et al. [13], recommended stacking of two transparent picture shares with additional flags given the new colour scheme, which mitigates the drawbacks of shares utilising a limited palette of colours.

Shyong Jian Shyu et.al [14] proposed the use of integer linear programmes for-MVCSs in order to minimise pixel expansions. VCS constructions are cutting-edge, adaptable, and capable of handling multiple MVCS types.

M.Karolin et al. [15] presented visual cryptography method which interprets the secret message from some overlapped shares by taking use of each Visual scheme. This paper does a good job of addressing the problem with the difficult computations needed for classical cryptography. By transforming colour photos into binary black and white images, visual cryptography may also be used with colour images.

II. PROPOSED METHOD

The suggested study focuses on a VC method for sending images from the sender to the recipient with greater secrecy and confidentiality. RGB image is divided in RED, GREEN, BLUE color. RGB share1 & share2 creation and both the shares encrypted and decrypted to stacked images. The dithering method is used for the half toning techniques. The AES algorithm is secure next to illegal attacks and also fast in nature for image computation. The confidential image the Red, Green, Blue color group of the pixel values are taken and produce the divide matrix (R, G, B).The basic matrices R1, R2, G1, G2 and B1, B2 are obtained by separating each and all value in R, G, and B by 2.for producing RS1, RS2, and GS1, GS2, and then BS1, BS2 in R, G and B matrices also.Rs1,Gs1 and Bs1matrices to create the share1and combine the Rs2, Gs2and Bs2 matrices to create the share2

.When the share creation process is done, each share is encrypted and decrypted by using AES algorithm to keep its in order strongly. During this process another important factor is worked here, the Key generation which itself a complex and secure method. The Key generation is mainly focused on outcome base method.

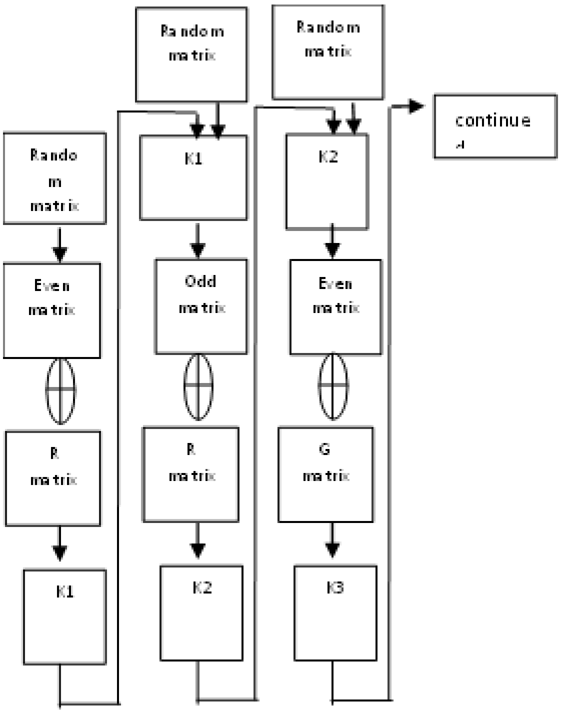


Figure 1: Key generation by OFB model

Step1:A random matrix is generated as per the size requirement base on the (R1 to B2).
Step2:The matrix is converted to even matrix. The Even matrix is XOR with R matrix and produces K1 key.
Step3:K1is XOR with the random matrix and converted to odd matrix.
Step4: The odd matrix is XOR with R matrix and produces K2 key.
Step5:K2is XOR with the random matrix and converted to even matrix.
Step6: The even matrix is XOR with G matrix and produces K3 key.
Step7:K3is XOR with the random matrix and converted to odd matrix .
Step8: The odd matrix is XOR with G matrix and produces K4 key.
Step9:K4is XOR with the random matrix and converted to even matrix .
Step10:The even matrix is XOR with B matrix and produces K5 key.
Step11:K5is XOR with the random matrix and converted to odd matrix .
Step12:The odd matrix is XOR with B matrix and produces K6 key
Using of original picture Red, Green, and Blue (R, G, B) matrixes are created using all color pixel values. The key matrixes K1,K2,….K255 are created through key generation process with OFB technique. R1,R2 matrixes are generated by R/2 , if one of the value of R matrix is odd then small part goes to 1st matrix and big one goes to 2nd matrix, otherwise if the value is even then it is distributed equally to both the matrix.For example :

Table1: R matrix, R1 matrix and R2 matrix

	112	234	151	120
R	258	261	149	325
	110	107	106	105
	108	132	220	170

	56	117	75	60
	129	130	74	162
R1	55	53.5	53	53
	54	66	110	85

	56	117	76	60
R2	129	131	75	163
	55	54	53	53
	54	66	110	85

The same procedure is applied on Green and Blue color share also and created G1 ,G2 from G and B1,B2 from B.
Step1: Input the Secret Red, Green, Blue images
Step2: Share creation involved in division by 2, to create the share R1,R2,G1,G2,B1,B2.
Step3: This process is same to the other basic Color G1, G2, and B1, B2 share creation.
Step4: Key generated through Outcome feedback method (OFB) for each share K1 to Km as per the requirement.
Step5: R1 XOR K1 ,R2 XOR with K2 and so on for all the remaining share and produce the RS1to BS2 shares.
Step6: Final share1 formed by RS1, GS1, BS1, and share2 by RS2, GS2, and BS2.
Step7: Final shares are Encrypted using AES algorithm.
Step8: This process is opposite to the share decryption Method.

After creation of final shares any encryption method can be used for the next level of encryption and the same algorithm will be used in decryption. In this case we have used AES algorithm for encryption and decryption. This algorithm is widely used in visual cryptography mainly for ensuring the security of information.

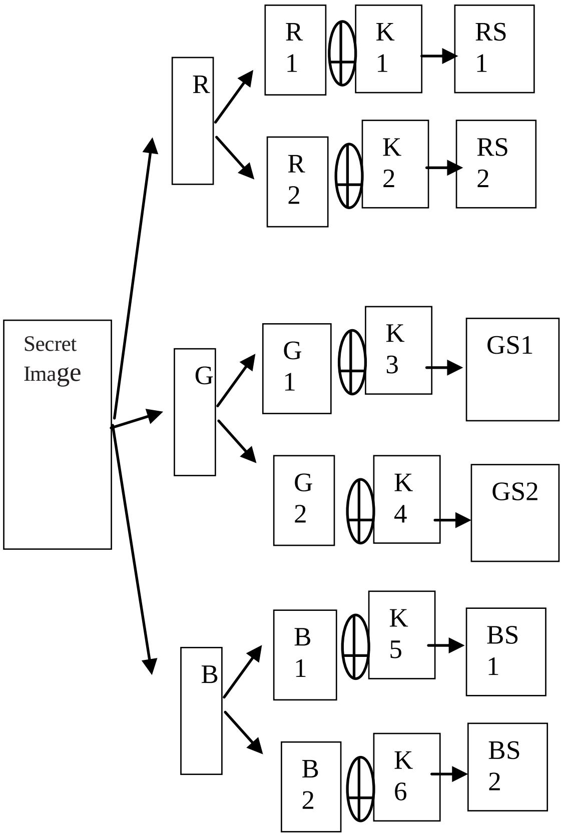


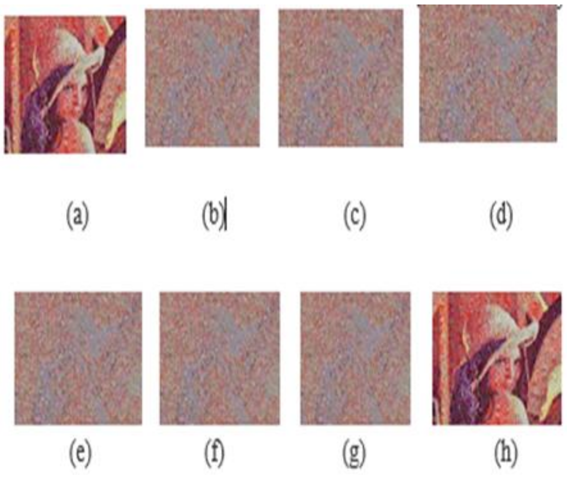
Figure 2: Operation procedure to produce R,G,B shares.

III. RESULTS & DISCUSSION

Visual Cryptography mainly deal with image processing , which deal with pixel reading segrigation and all other mechanisam. The evaluation of image quality done using pick to signal ratio (PSNR). In the proposed method image procession g techniques and tools are used in share creation and encryption purpose and PSNR is calculated for quality cheaking of shares and reconstructed images.

Img:1: Original image

Img:2: R,G,B images



Img 3: secret image-a, share1&share2-b,c encrypted share-d,e Decrypted share-f,g stacked image-h.

Visual cryptography and the language employed here are utilised to implement the suggested way of share encryption and decryption as demonstrated in Img. 3. Matlab. Original secret image Lena (a) , then two share is created (b,c). After encryption the proposed method produced encrypted share(d,e). During the reconstruction encrypted shares (d,e) decrypted and produced shares(f,g). Finally share f and g are stacked and produced image h.

Table: 2 Comparison of the PSNR values of various image sharing.

	PSNR			
	Existing System[19,20]		Proposed system	
Image	S1	S 2	S 1	S2
Lena	8.74	8.32	8.76	8.35
Pepper	8.32	8.12	8.3	8.08
Bird	7.85	7.64	7.9	7.71

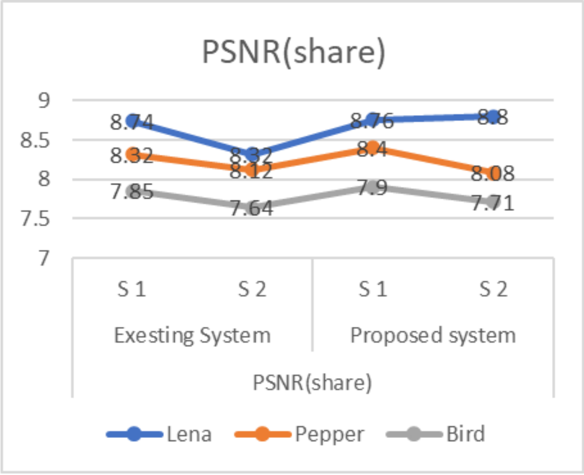


Figure: 3 Graphical representation of table 2.

We have study the PSNR for the different share created in existing methods as an average value and compared with the share created through proposed method and the observation indicate the share 1 are more and less same but the share two is in better side in terms of PSNR.

Table 3: PSNR comparisons between different methods based on the reconstructed images.

Image	PSNR(Reconstructed image)		
	Existing System		Proposed Method
	Shankar and Eswaran[19]	Javvaji Ratnam [20]	
Lena	59.632	49.657	61.005
Pepper	57.365	55.127	59.896
Bird	60.702	51.002	62.668

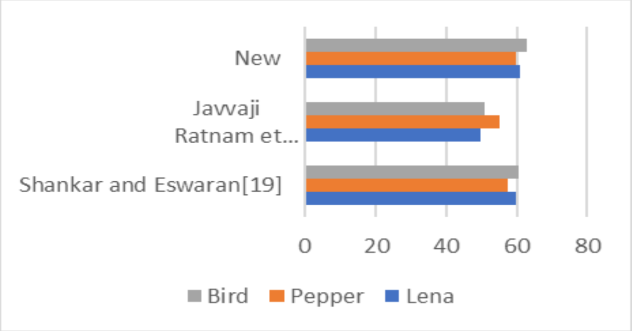


Figure 4: Graphical representation of table 3.

The proposed method also tested on with comparison to the existing method for reconstructed image through stacking the images. One of the crucial factors in comparing photographs is the PSNR. The results of the experiments demonstrate that the suggested strategy provided PSNR on the higher side.

IV. CONCLUSION

Visual Cryptography is an important aspect of security. This paper's suggested algorithm is highly focused on security means secure the transmitted imagesThe proposed method employs the dithering technique and colour breakdown to create the standard red, green, and blue colour codes. The suggested approach builds an R, G, and B colors coding system that is better appropriate to defend the shares. The proposed OFB based key generation with random matrix and XOR operation provide encrypted key which itself secure and produce enough security in share creation. Lastly the AES

REFERENCES

[1] M. Naor and A. Shamir, “Visual cryptography,” Proceedings of Advances in Cryptology: Eurocrypt94, Lecture Notes in Computer Science, Vol. 950, 1995.

[2] Luiz Velho and Jonas de Miranda Gomes “Digital halftoning with space lling curves” Computer Graphics, July 1991.

[3] Chang-Chou Lin andWen-Hsiang Tsai “Visual cryptography for gray-level images by dithering techniques” Pattern Recognition Letters, 2003..

[4] Young-Chang Hou “Visual cryptography for color images” Pattern Recognition, 2002.

[5] Der-Chyuan Lou, Hong-Hao Chen, Hsien-Chu Wu, and Chwei- Shyong Tsai “A novel authenticable color visual secret sharing scheme using non-expanded meaningful shares” Displays, 2011.

[6] C-C Chang, W-L Tai, and C-C Lin. Hiding a secret colour image in two colour images. The Imaging Science Journal, 2005.

[7] C. Yang and C. Laih, “New Colored Visual Secret Sharing Schemes”, Designs, Codes and cryptography, 2000.

[8] I.Ozturk, I.Sogukpinar, "Analysis and comparison of image encryption algorithm," Journal of transactions on engineering, computing and technology, vol. 3, 2004.

[9] R. Lukac, K.N. Plataniotis, “Bit-Level Based Secret Sharing For Image Encryption”, Pattern Recognition 38 (5), 2005.

[10] TingyuanNie and Teng Zhang,“ A Study of DES and Blowfish Encryption Algorithm”, IEEE, 2009.

[11] Anantha Kumar Kondra, Smt. U. V. RatnaKumari, “An Improved (8, 8) Color Visual Cryptography Scheme Using Floyd Error Diffusion”,in International Journal of Engineering Research and Applications, Vol. 2, Issue 5.

[12] Yuanfeng Liu, Zhongmin Wang; “Halftone Visual Cryptography with Color Shares”, International Conference on Granular Computing (GrC), IEEE, 2012.

[13] L. N. Pandey and NeerajShukla, “Visual Cryptography Schemes using Compressed Random Shares”, in International Journal of Advanced Research in Computer Science and Management Studies, Volume 1, Issue 4, September 2013.

[14] Shyong Jian Shyu, Hung-Wei Jiang; “General Constructions for Threshold Multiple-Secret Visual Cryptographic Schemes” IEEE Transactions on Information Forensics and Security, Volume: 8 , Issue: 5, 2013.

[15] M.Karolin Dr.T.Meyyappan,”RGB Based Secret Sharing Scheme in Color visual cryptography”, in International Journal of Advanced Research in Computer and Communication Engineering,Vol. 4, Issue 7, 2015.

[16] K.Shankar, Dr.P. Eswaran: ECC Based Image Encryption scheme with aid of optimization Technique using Differential Evolution algorithm. International Journal of Applied Engineering Research 2015.

[17] AshaBhadran R,”An Improved Visual Cryptography Scheme for Color Images” International Research Journal of Engineering and Technology (IRJET), Volume.0.2, Issue: 2015.

[18] M.Karolin Dr.T. Meyyappan .SM. Thamarai: “Image encryption and decryption of color images using visual cryptography” International Journal of Pure and Applied Mathematics, Volume. 118, 2018.

[19] Shankar K, Eswaran P ―Sharing a Secret Image with Encapsulated Shares in Visual Cryptography‖ 4th International Conference on Eco-friendly Computing and Communication Systems, Procedia Computer Science 70 , 2015

[20] Rafel C. Gonzalez and Richard E. Woods, ―Digital Image Processing‖, Pearson Education.