Secret Multiple Share Creation with Color Images using Visual Cryptography

Conference Paper · April 2019

DOI: 10.1109/ICCSP.2019.8698013

2 authors:

Karolin M.
Alagappa University
6 PUBLICATIONS **23** CITATIONS
SEE PROFILE

Meyyappan Thirunavukkarasu
Alagappa University
20 PUBLICATIONS **75** CITATIONS
SEE PROFILE

Secret Multiple Share Creation with Color Images using Visual Cryptography

M. Karolin and T. Meyyappan

***Abstract*—Visual cryptography technique which allows the visual information to be confidential. Visual Cryptographic technique can be applied over those visual information or images before transmission. In presented method is plant for the share created, it is encrypted individually by using AES algorithms. The input image is improved to the RGB color code forms. The proposed method is also used to generate the share creation techniques. The proposed method is created to RGB images and then share1, share2 created using blowfish algorithm. The proposed method is RGB image, shares Encrypted and Decrypted to stacked image and then same as the original image. The testing results of the proposed system are compared to the share generation technique. The planned algorithm is designed and implemented with Matlab coding.**

***Index Terms*—Visual cryptography XOR Share creation Share Encryption Decryption Blowfish algorithm RGB color images**.

I. Introduction

NOWADAYS, due to enormous developments in digital world make it hard to maintain the in sequence to be secret. The secret letter should be quiet both at the sender's storage space as well as in the communication medium. The group services are now open to approximately each one. Several methods such as the cryptography, Steganography were occupied for the reason of secure data. Visual cryptography, in sequence finally changed to meaningless design, so that the impostor cannot achieve them. Visual Cryptography method for encrypting, user-defined into several technique of shares. The method was planned by Naor and Shamir in 1994. It plant on the standard of transforming underground picture provided by the dispersed to clients during communiqué media. The receiver can restore the new image by stacking all understandable shares on each other. The most important feature of the visual Cryptography is that, it recovers the secret image not including any computation [1-13]. The visual cryptography paper is prepared as fallows. Section II and Section III describes the Related works and Proposed Method. Section IV discuss about the Result. Section V concludes the paper with conclusion.

II. Related Method

Image secret share creation for rgb images was introduced by Naor and Shamir based on features semigroups [1], Young-Chang Hou[12] presenteda 2 out of 2 visual cryptography schemes by applying the design of color assortment.

M. Karolin and Dr. T. Meyyappan are with the Department of Computer Science, Alagappa University, Karaikudi (email: karolinmsc@gmail.com)

L. N. Pandey and NeerajShukla [2], Stacking two transparencies with multiple flag given the new third color combination proposed method improves the drawbacks of using limited color in shares.

TingyuanNie and TengZhang [8], shows that blowfish algorithm paper is regarding encryption and decryption of images with a secret key block cipher called 64-bits.

M.Karolin Dr.T. Meyyappan [11] says that the images are transmitted after applying the visual cryptographic technique. It exploits the individual Visual scheme to translate the secret communication from some overlapped shares. This technique overcomes the disadvantage of complex computations required in traditional cryptography. Visual cryptography can also be applied to color images by converting them into black and white binary images.

III. Proposed Method

In this Research work is implemented with visual cryptography method is used to throw the unique image from dispatcher to recipient with utmost confidentiality and secrecy. In the proposed method RGB color image is full for the information distribution. In the proposed system RED, GREEN, BLUE color system is divided in 16 standard color code forms lacking any decrease and declaration. RGB share1, share2 creation the share1encrypted and decrypted share2 encrypted decrypted to stacked images. The proposed algorithm is original image share1and share2 to transparent the stacked image. The dithering algorithm is used to instead the halftoning techniques. The proposed algorithm is original image distribution and followed by stacking the decryption occupied. The Blowfish algorithm is secure next to illegal attacks and run quicker than the accepted presented algorithms. The research work is new method for shares encryption, decryption is designed and implemented with Matlab coding.

The proposed method share encryption technique is used to throw on new image from the dispatcher to the recipient absolute privacy and secrecy. 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_i, G_i, and B_i by 2. This method is continual for creating 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 Blowfish algorithm to keep its in order strongly.

978-1-5386-7595-3/19/$31.00 ©2019 IEEE

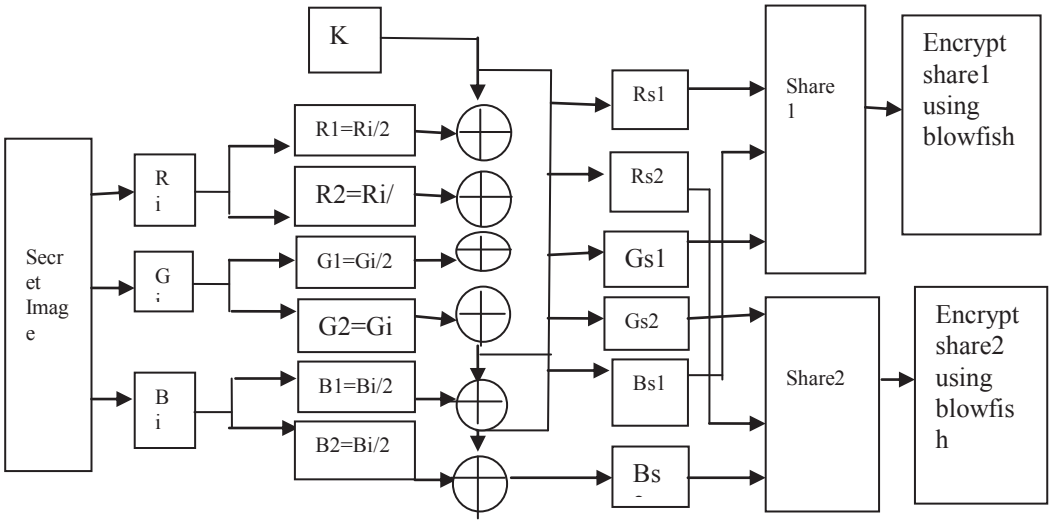


Fig. 1. Proposed Method of Share Encryption

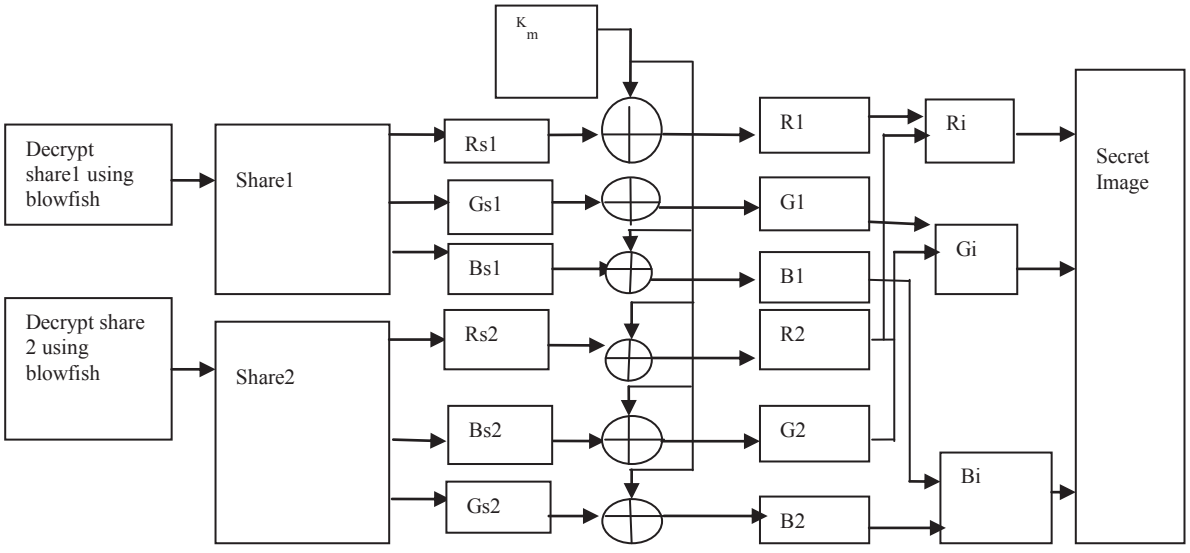


Fig. 2. Proposed Method of Share Decryption

A. Share Creation Method

The Red, Green, Blue pixel values are taken from the novel image and the separate matrix (original matrix) (Ri, Gi, Bi) create globalized key matrix K Where m=0, 1,2,3,….255. For Example,

$$Ri = \begin{pmatrix} 127\ 127\ 127\ 125 \\ 127\ 126\ 127\ 123 \\ 126\ 125\ 126\ 127 \\ 126\ 126\ 126\ 127 \end{pmatrix} \quad Gi = \begin{pmatrix} 234\ 234\ 236\ 233 \\ 233\ 233\ 234\ 230 \\ 230\ 229\ 232\ 230 \\ 230\ 230\ 230\ 231 \end{pmatrix}$$

$$Bi \begin{pmatrix} 125123\ 122\ 116 \\ 121\ 118\ 117\ 112 \\ 113\ 111\ 111\ 107 \\ 110\ 107\ 106\ 105 \end{pmatrix} \quad Km = \begin{pmatrix} 100\ 120\ 154\ 180 \\ 161\ 234\ 180\ 120 \\ 121\ 185\ 148\ 59 \\ 108\ 132\ 220\ 170 \end{pmatrix}$$

Ri matrix value is 127,127/2=63.5. So regard as the bottom value R1=63 and R2=64, hence 63=64=127 for example.

$$R1 = \begin{pmatrix} 63\ 63\ 64\ 62 \\ 63\ 63\ 63\ 61 \\ 63\ 63\ 63\ 63 \\ 63\ 63\ 63\ 63 \end{pmatrix} \quad R2 = \begin{pmatrix} 64\ 64\ 63\ 63 \\ 64\ 63\ 64\ 62 \\ 63\ 63\ 64\ 62 \\ 63\ 63\ 63\ 64 \end{pmatrix}$$

This method is repetitive for creating Gs1, Gs2, and Bs1, Bs2 in Gi and Bi matrices to share 1 and share2.

B. Secret share Encryption/Decryption steps

Step1: Input the Secret Ri Gi Bi images
Step2: Share creation include the R1=Ri/2, R2=Ri/2 create the Red color share creation.
Step3: This is process is repeated to retrieve the other basic Color G1, G2, and B1, B2 share creation.
Step4: Key matrix K_m individually and catch the resulting as RS1, Rs2 and GS1, GS2 and then BS1, BS2 share creation furthermore.
Step5: share1 created to Rs1, Gs1, Bs1, and share2 created the Rs2, Gs2, and Bs2.
Step6: Share1 share2 Encrypted using Blowfish algorithm.
Step7: End the Output secret images.
Step8: This process is opposite to the share decryption Method.
Step9: Share1 share2 Decrypted using Blowfish algorithm.
Step10: End the secret image.

TABLE I
SHARE CREATION AND ENCRYPTED USING BLOWFISH

Image Name	Share Generation		Share Encrypted using blowfish	
	Share1	Share2	Share1 Encrypted	Share2 Encrypted
Lena	7.78	7.78	7.87	7.87
Jet	7.71	7.71	7.70	7.71

C. Blowfish Algorithm

Bruce Schneier planned blowfish in 1993 as a high-speed, free special to existing encryption algorithms. Blowfish is a cipher based on the Feistel rounds, and the plan of the F-function used amounts to an indication of the values used in Data encryption Standard to present the equal protection with better speed and efficiency in software. Blowfish is a 64-bit block cipher and is possible as an alternate for the Data encryption standard. So in this paper, to be implementing the blowfish algorithm this is strongest and highest in data processing store estimate to other algorithms. Blowfish algorithm is really protected since it has a longer key length 32 to 448 bit (more no of key size).

TABLE II
ALGORITHM COMPARISON

	Algorithm	Created By	Key size(Bits)	Block size(Bits)
Existing algorithm	AES	Rijndael	128	128
Proposed algorithm	Blowfish	Bruce Schneier	32 to 448	64

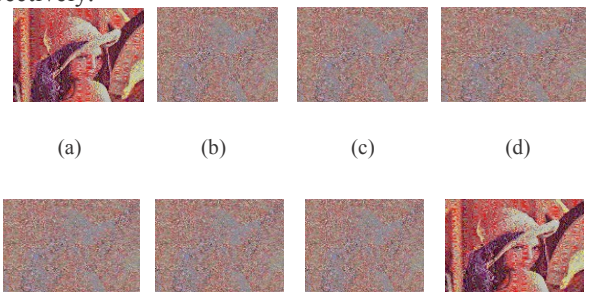
a) Algorithm Steps

Blowfish Algorithm Encryption and Decryption 64 bit plaintext and 64 bit cipher text and then 32 to 448 bit key value to16 round festal network.
Step 2: Input the value to encryption image for i=0 to 16
Blowfish Encryption Method
Encrypt (L, R)
For int (i=0; i<16; i++)
L^=P[i];
R^=F (L);
R^=P [i+1];
L^=F(R);
L^=P [16];
R^=P [17];
Step3: input the Key value for 32 to 448
Key generation
Step4: Decryption of p1, p2….p18 reverses in Encryption algorithm.
Step5: Blowfish algorithm is Original image sahre1Encrypted and share2Encrypted and then stacked image.
Step6: Blowfish algorithm used to Lena and Jet images.
Step7: End the Algorithm.

IV. Result And Discussion

A. Experimental Analysis

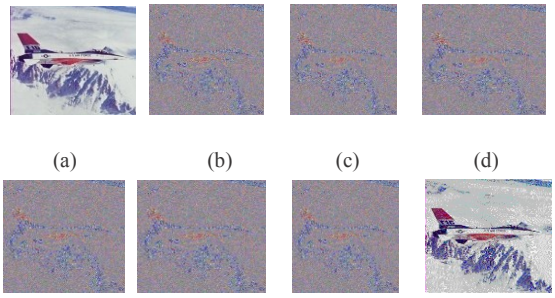
This division presents the reproduction outcome illustrating the presentation of the proposed technique. The proposed method of share encryption and decryption shown in Fig. 1 and Fig. 2 respectively occupation is implemented with Visual cryptography and language user Matlab R2013a Consequently the proposed scheme is a strong one. Shown in Fig. 3 and Fig. 4, "Lena" and "Jet" served as the tested image respectively.



(a) (b) (c) (d)

(e) (f) (g) (h)

Fig 3. (a) secret image,(b,c) share1&share2 (d,e) encrypted share (f,g) Decrypted share (h) stacked image.



(a) (b) (c) (d)

(e) (f) (g) (h)

Fig 4. (a)secret image,(b,c) share1&share2 (d,e) encrypted share (f,g) Decrypted share (h) stacked image.

B. Performance Analysis

The next division shows the special presentation metrics measured to display the value of generated shares. The Peak signal to noise ratio computes the ratio of highest potential signals to the sound that affects the image reliability depiction. The Peak signal to noise ratio in sound unit. Mean square error is the calculate which represents the collective squared error between the novel image and secondary image.

$$MSE = \frac{1}{MXN} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [C1(i,j) - C2(i,j)]^2$$

$$PSNR = 10\log_{10} \frac{(M \times N \times 255^2)}{MSE}$$

TABLE III
LENA AND JET PSNR AND MSE VALUE

Images	PSNR	MSE
Lena	61.34	113
Jet	59.11	110

C. Comparative Analysis

The Table I and Table II shows the share creation and encrypted using blowfish and algorithm comparison calculation respectively. The values in Table III give the value estimate by using the production metrics Peak signal to noise ratio and Mean square error as the results. Comparative Analysis of the AES algorithm and Blowfish algorithm to compare the PSNR and MSE value calculation shown in Table IV and Fig. 5. Proposed method is many techniques used to compare the Floyd Steinberg dithering algorithm XOR operation, and then color error division methods.

TABLE IV
PROPOSED METHOD FOR PSNR AND MSE VALUE

Methods	PSNR	MSE
Floyd dithering algorithm	24	180.90
Adaptive order dithering Algorithm	25.25	190
CED using XOR	27.17	125
Proposed Method	61.34	113

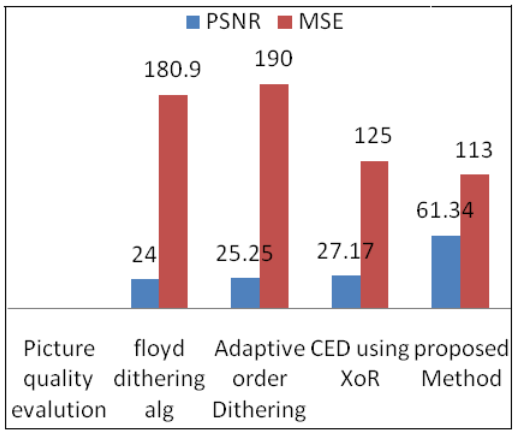


Fig. 5. Comparative of PSNR and MSE

V. Conclusion

Visual cryptography paper, is a original visual cryptography algorithm is proposed to secure the transmitted images. The process divides the image into multiple numbers of printable shares which exploit the human visual system. In this paper presentation of dithering knowledge and color breakdown to construct R,G,B color code models from usual red, green, and blue. The proposed method constructs an R, G, B color code method which is

more fitting to defend the shares. The proposed algorithm generating more number of colors to produce the shares. Blowfish method is 64-bit block cipher and key price in the range to 448 is adapted for securing the image. The proposed algorithm is best result to share encrypted and decrypted image. The existing work better then image quality and then image encryption and decryption to proposed work

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Proceedings of Advances in Cryptology: Eurocrypt94, Lecture Notes in Computer Science, Vol. 950, pp. 1 - 12, 1995.

[2] C. Yang and C. Laih, "New Colored Visual Secret Sharing Schemes", Designs, Codes and cryptography, 20, pp. 325–335, 2000.

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

[4] R. Lukac, K.N. Plataniotis, "Bit-Level Based Secret Sharing For Image Encryption", Pattern Recognition 38 (5), pp. 767–772, 2005.

[5] TingyuanNie and Teng Zhang," A Study of DES and Blowfish Encryption Algorithm", IEEE, 2009.

[6] 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, September- October 2012, pp.1090.

[7] Yuanfeng Liu, Zhongmin Wang; "Halftone Visual Cryptography with Color Shares", International Conference on Granular Computing (GrC), pp. 746-749, IEEE, 2012.

[8] 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, pp:62 – 66.

[9] 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, pp: 733 – 743, 2013.

[10] 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, July 2015.

[11] 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 2015:10:5:1841-1845.

[12] AshaBhadran R,"An Improved Visual Cryptography Scheme for Color Images" International Research Journal of Engineering and Technology (IRJET), Volume.0.2, Issue: 05, August 2015.

[13] 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, No. 8, 2018, 277-281.