A Secure Visual Secret Sharing Scheme Using Color Visual Cryptography and Multiple Encryption

Megha Mohan[1], Rajkumar K K[2]

[1]Research Scholar, Department Of Information Science and Technology, Kannur University, Kannur, Kerala, India
[2]Associate Professor, Department Of Information Science and Technology, Kannur University, Kannur, Kerala, India

---***---

Abstract - *Visual cryptography is a secret sharing technique for securing visual contexts like images or texts by encoding into multiple number of shares. In decryption process, one can decrypt the secret image (SI) by stacking the shares without any additional computations. Color visual cryptography (CVC) encodes a color secret image (SI) into several shares in which each color pixels are separately handled using RGB or CMY models. In this paper we proposed CVC technique for secret color images encoding schemes with multiple encryption algorithm to make the secret image highly secured. In this method, a color secret image is encrypted by extracting R, G, B component from the original secret image and halves of each of them into two separate matrices. Each of these matrices are then XORed with a randomly generated key matrices (Ki) to generate six different shares for each of the three color planes. By using Hou's scheme, share 1 and share 2 are then constructed by stacking the three first level shares and three second level shares of each color components respectively. The generated two shares are further encrypted by hybrid security algorithm called AES and Blowfish. On the recipient side, color SI is retrieved form these shares with the equivalent quality as that of original image by performing all the operations that we accomplished in the encryption processes in reverse order. The proposed method is then evaluated by using performance measures such as PSNR and SSIM. The result obtained by these two evaluation parameters show that the reconstructed image retain the quality of the original image. Therefore the proposed method is excellent for hiding secrets in the form color images confidently compared to the existing VCS schemes.*

Key Words: **Color Visual Cryptography; Shares; Multiple Encryption; Information Srcurity; Secret Sharing; Image Quality**

1.INTRODUCTION

Use of online services for transmission of data is very common in nowadays with the rise of Internet. To accomplish safe and secure data transmission, one need to conceal the confidential data using symmetric and asymmetric key cryptography before the transmission over the Internet. In general, Cryptographic techniques involves a series of complex computation process so that it become impossible for an intruder to break the system easily. Visual cryptography (VC) is an extension of cryptographic technique addressed by Naor and Shamir in 1994. VC introduced secure transferring of digital images without using a series of complex computation as in cryptography [1]. VC is the technique for encrypting images, text, etc... in which the decoding process can be carried out by a human visual system rather than complex decoding algorithms. Digital image encryption works on the principle that a user-defined secret images (SI) is divided into different shares (transparencies), and these transparencies are distributed among different participants. On the decoding side, the decoder may retrieve the secret image (SI) by stacking sufficient number of shares collected from different participants.Visual cryptography scheme (VCS) employs a way of encrypting and decrypting the binary image containing a set of black and white pixels. Every black and white pixel of the binary image is transformed into m subpixels. The decoding process can be carried out by overlaying or stacking the encrypted shares which works similar to Boolean OR operation [2] [3].

Color plays an important role in human visual communication for object identification or removal from a scene. In human visual system, millions of cone cells in our eyes are responsible for color sensation, and are more sensitive towards Red(R), Green (G), and Blue (B) colors. Thus, many color scheme systems use R, G, B as primary colors whereas Cyan (C), Magenta (M), and Yellow (Y) as secondary colors by adding any two primary colors [4]. Color Visual Cryptography (CVC) is used for encrypting colored secret images (SI) into different transparencies called shares and the original SI can be reconstructed by superimposing all the transparencies together. Each share by itself does not reveal any data of the SI. A color VCS is generally useful to a color image containing a set of color pixels which are handled separately using RGB or CMY color models. The rest of the paper is organized as follows. In section II Standard Color visual cryptographic schemes and multiple encryption schemes such as AES and blowfish algorithm are explained. In section III discusses about the related study conducted in this area. Section IV explains the proposed method for multiple encryptions and decryption of RGB images. Section V discusses the results and performance evaluation about the outcome of the proposed method and followed by the conclusion in section VI.

2. Standard color visual cryptography schemes(VC schemes)

VC is an encoding scheme that encrypts user-defined images into various shares without using any encryption or decryption keys .Color VC deals with color images rather than binary or monochromatic images. There are different types of color VC schemes existing in literature. Verheul and Van Tilborg, Rijmen and Preneel's, and Hou's color VC schemes are the most commonly used color visual cryptographic scheme in general.

2.1 Verheul and Van Tilborg schemes for color images

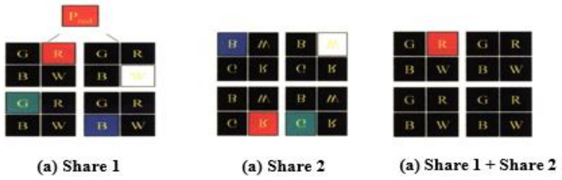
Verheul and Van Tilborg [6] introduced a simple color VCS in 1997 using 2 x 2 secret sharing scheme for four subpixels. In this method, every pixel of the color secret image (SI) is transformed into any number of subpixels for creating shares, and every subpixel in each block is further divided into C color regions with one original color block and the remaining black block placed randomly. When two such shares are superimposed, i.e., two color pixels overlap, the resultant pixels will be completely black, except when both pixels are the identical color. The entire Verhuel van Tilborg scheme for color image are shown in the figure 1[7].

2.2 Rijmen and Preneel's Scheme

Rijmen and Preneel [8] introduced a new color scheme with relatively less number of subpixels. In this method, every pixel of the original color image is divided into four subpixels filled with Red (R), Green (G), and Blue (B) and transparent colors randomly. Thus, in this scheme 24 combination are possible for different shares of each pixel. To encode a pixel of color secret image (SI), each single pixel is divided into two shares of four subpixels. The first share is created randomly by arranging four subpixels. In the second share, subpixels are arranged in such a way to generate the required colors by combining two transparencies [7]. Rijmen and Preneel's encoding scheme is summarized in figure 2. The pattern of share 1 remains the same and share 2 varies, these two shares are stacked to generate original image back.

2.3 Hou's Scheme

Young-Chang Hou [9] proposed three new color VC schemes for color images using additive and subtractive color models. In the additive color model, a combination of primary colors Red (R), Green (G), and Blue (B) are used to get the preferred color. In subtractive model, uses Cyan (C), Magenta (M), and Yellow (Y) as primary components, and each color is represented by a combination of color light reflected from the surface of a body. Hou's color VC scheme makes use of two techniques, namely, halftoning and color decomposition. Halfton**ing** is a printing technique that makes use of series of dots rather than continuous tone in images. These dots can be



(a) Share 1 (a) Share 2 (a) Share 1 + Share 2

FIGURE 1. Construction of Verheul and Van Tilborg color VC Scheme.

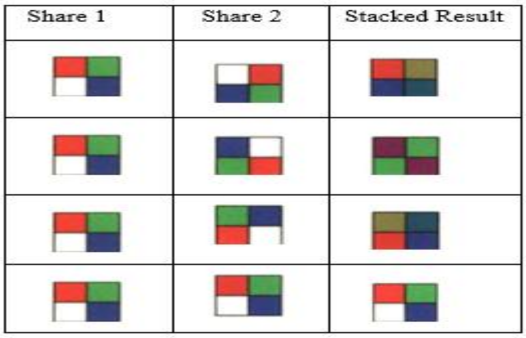


FIGURE 2. Construction of Rijmen and Preneel's color VC scheme.

of various sizes, colors, and shapes. Larger dots portray darker and denser regions of the image whereas smaller dots represent lighter regions.[10] In the color decomposition technique, color images are split into three-primitive colors based on additive or subtractive color models. In this scheme, a colored secret image (SI) is decomposed into three primary-color images under the subtractive model, viz, C, M, and Y images. Each primary-color image is halftoned to generate C, M, Y halftoned images. Finally, these three C, M, Y halftoned images are combined to generate a halftoned color image [7].

Among the three-color VC scheme proposed by Y.C Hou, the third algorithm gives a minimum contrast reduction up to 25 % comparing to the other [11]. According to traditional visual cryptography, shares are constructed by splitting every pixel of the originally halftoned color image into 2 x 2 subpixels contains two transparent and two same color pixels. If the pixel in the color secret image (SI) is transparent, share 1 and share 2 are constructed with same subpixel pattern, and if a pixel in color secret image (SI) is color, share 2 have the complement of share 1 [3].The entire process of share construction can be done for each color component C, M, Y and thus we construct six different shares for each three colors called Cyan, Magenta, and Yellow. From these shares new two share are constructed by combining share 1 components of C, M, and Y., and share 2 component of C, M, Y. Original color image can be retrieved by stacking these two new shares [9]. The entire construction of Hou color creation scheme is illustrated in figure 3.

2.4 Multiple encryption and decryption of shares

The work proposed in this paper uses multiple encryption and decryption of shares. This is achieved through AES and Blowfish algorithm. Thus, multiple encryptions of shares provide better and reliable data transmission through the network. In the decryption process the doubly encrypted shares are decrypted in the reverse order as we have encrypted the message using AES and Blowfish algorithm.[12]

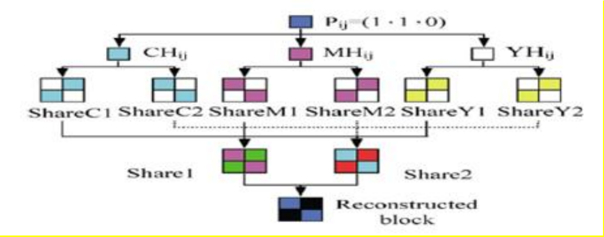


FIGURE 3. Construction of Hou's color VC scheme

2.4.1 AES Algorithm

Advances Encryption Standard (AES) is the most popular and one of the strongest encryption algorithms in cryptography. It is designed as a symmetric block cipher in which the dispatcher and recipient uses the same key. It encodes 128 bits (16 bytes) of data blocks represented in 4 x 4 matrix and uses key of size either 128 bits, 192 bits, or 256 bits and number of rounds is relied to these key lengths. It uses 10, 12, or 14 rounds for 128 bits, 192 bits and 256 bits respectively. [13] In encryption, each round consists of four basic sub processes: Byte Substitution, Shifting of Rows, Mixing of Columns, and Add Round Key. Initially, *SubBytes () transformation* operates separately on each byte of input data. Each of the 16 bytes in the state is substituted to another byte using nonlinear S-box (Substitution table). Secondly, *ShiftRows () transformation* cylindrically shifts the byte of the state matrix in each row to left except row number zero. In this process, the zeroth row remains the same and first row is shifted one byte circular to the left [21]. The second row and third row are shifted left of order two and three respectively [21]. The third phase is the *MixColumn*, mix each column of the state array with a predefined polynomial by multiplying each row of matrix transformation with each column of the state array. Finally, in *AddRoundKey () method* bytes of state array matrix is XORed with a round key. Each round key represented by *nb* words of the columns of the state array. Decryption of AES uses the opposite procedure of encryption that compromise four procedure: Inverse Shift Rows, Inverse Substitution Bytes, Add Round Key and Inverse Mix Column. [14][15]

2.4.2 Blowfish Algorithm

Blowfish algorithm was designed by Bruce Schneir in 1993. It uses a symmetric block cipher in which both the collaborating parties use the same key for encryption and decryption of the messages. It is proposed as a substitute algorithm for DES. Blowfish follows a Feistel structure consisting of 16 rounds. It encrypts and decrypts 64 bits block of data at a time using a key of variable length 32 to 448 bits and subordinate S-boxes. It is the fastest encryption algorithm.[1][16]. In the encryption schedule, there exist 16 subkeys which are stored in a P-array with each array element of 32-bit entry[22].. Initially, the 64 bits input data is halved 32 bit-left and 32-bit right. In every round, the left 32 bits are XORed with P-array, then, right-32 bits are XORed with Blowfish function of left- 32 bits that make use of four S-boxes and finally, swap the left and right half. The decryption of Blowfish is similar to encoding process except the p-arrays are used in opposite order. [23][26]

2.4.3 PEAK SIGNAL-TO-NOISE RATIO (PSNR)

PSNR is the computation of the highest possible value of the image to the power of distorting sound that disturbs the image quality. It is computed in Decibel (dB) Scale. Higher PSNR value indicate high quality of reconstructed image, ie, low difference between the reference and rebuilt image. The value of PSNR lies between 0 dB for completely different image and 100 dB for same images. MSE (Mean Square Error) is used to compute cumulative square error between the reconstructed and original image, the low MSE value indicates lower error.[24] MSE and PSNR can be calculated as follows,

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\|I(i,j) - K(i.j)\|^2 \qquad (1)$$

$$PSNR = 10.log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

$$= 20.log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \qquad (2)$$

2.4.4 Structural Index Similarity (Ssim)

It is an alternate method for calculating the image quality degradation caused in transmission of data or compression of data. In SSIM, image quality is assesed based on three factors, that is, luminance, contrast and structure of the image. SSIM is used for finding similarity between the original reference(x) and reconstructed image (y). It can be calculated using the following way, [25]

$$\boldsymbol{S(x,y)} = \frac{2(\mu_X\,\mu_X+C_1)(2\,\sigma_{XY}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \qquad (3)$$

Where μ_x and μ_y is the average pixels in x and y, σ_X^2 and σ_Y^2 is variance of pixels in x and y. The variables c_1 and c_2 are constants, $c_1= (k_1L)^2$ and $c_2 = (k_2L)^2$ where k1 and k2 are constants and L is the maximum pixel value which is 255. The value of SSIM lies between 0.0 for completely different images and 1.0 for same images. [25]

3. LITERATURE REVIEW

Naor and Shamir proposed a cryptographic technique called visual cryptography in 1994 [2]. In visual cryptography, visual information can be encrypted into several shares and decrypted by human eyes. Main advantage of visual cryptographic scheme is that, there is no need of a computational device or any complex algorithm for decryption. Naor and Shamir proposed visual cryptography which includes implementation of (2, 2) visual cryptography schemes. In this scheme, the confidential image is splitted into shares namely, share 1 and share 2. For retrieving the original secret image back, stack these two shares together. Secret information is visualized only when both the shares are superimposed together. In 2002, Young Chang Hou [9] has proposed "Visual cryptography for color images". In this scheme, two techniques namely, color decomposition and halftoning method are used to construct the shares that when superimposed together gives a reconstructed image. The third algorithm introduced by him, with the two shares give a minimum contrast reduction up to 25 % than the other two methods.

Q. Zhang and Q.Ding [14] proposed "Digital Image Encryption Based on Advanced Encryption Standard (AES)" providing high security. AES is a symmetric block cipher which encrypts 128 bit block of data using key size of either 128 bits, 192 bits, or 256 bits [26]. T. Nie, T. Zhang [16], presents a blowfish algorithm paper for encrypting and decrypting images. This symmetric algorithm follows Fiestel structure consisting of 16 rounds and encrypts 64 bit block of data with a secret key of variable length. Sougata Mandal, Sankar Das, Asoke Nath [17], introduced an approach for hiding data based on visual cryptography. The authors made a study on hiding color image /message in two or more shares. This method uses halftone technology for share generation. It is impossible to extract hidden information from one share without having other shares. In order to retrieve a better decoded image, different share creation procedure can be applied.

M krolin, T. Meyappan [18] has proposed a secret sharing scheme for color images in which 256 color code format are converted to sixteen RGB format. The shares are constructed using (2,2) XOR based visual cryptography scheme. By using their scheme, image is retrieved by stacking the shares using XOR operation. The performance of the proposed method is evaluated using parameters, namely, PSNR and MSE, to show the visual quality of the reconstructed image which seems good.Asha Bhadran R [10] presents a secure data communication model using color visual cryptography and traditional cryptography. The referred paper discusses technique for encoding visual cryptographically constructed shares again using RSA algorithm providing double security. For this, a 2,2 visual cryptography scheme is used for share generation. The proposed scheme uses halftoning concept which produces color halftoned decoded image. In this approach, the size of the secret and retrieved image is not equivalent which can be observed as further enhancements. Anantha Kumar Kondra, Snt, U. V Ratna Kumara [19] uses visual information pixel (VIP) synchronization and error diffusion for color VC. The intent of this work is to provide a solution to identify errors in the shares and to verify the authentication. Their method is that, cyclic redundancy check [CRC] algorithm, color VC scheme are used to generate shares with better quality and provides higher security. Cryptanalysis is also done to evaluate the security level of the proposed scheme.Jinu Mohan, Rajesh Ramachandran [7] review papers on color visual cryptography schemes. The paper presents various existing color visual cryptography schemes and their features. A comparative study of various methods evolved in color visual cryptography is done to evaluate their performance. Comparative analysis is done based on the shares creation method, number of shares constructed, types of shares and decoding methods. *"Sharing a secret image with encapsulated shares in visual cryptography*" introduced by Shankar K and Eswaran P [20] presents a method for encoding visual cryptographically generated shares using symmetric encryption. Advanced Encryption Standard (AES) is used for encrypting the shares, thus providing security to the confidential document. The secret visual information is divided into two shares using Hou's third method. The shares created are encapsulated by encrypting it again using AES algorithm [13]. Thus, shares are not in their real form, so any attempt to create fake shares by the third-parties fails.

In general, all the above works discussed in the literature review possess certain advantages as well as disadvantages in the way of transmitting secret images through the communication channel. Most of the methods discussed in the literature make use of halftone concept and color decomposition techniques for creating shares. The results of all these methods are contrast reduction in the final reconstructed images. This is due to the use of halftoning concept of the color image. Further the reviews also revealed that standard encryption techniques such as AES and Blowfish algorithms provide higher level security for the transmission of shares through the channel. So, making use of these advantages and retaining the contrast of the retrieved image as that of the original image is one of the best challenges in Color Visual Cryptographic encoding scheme. In this paper, we are going to propose a color visual cryptographic scheme with multiple level encryption techniques of the shares using both AES and Blowfish algorithm as an alternative color encryption technique which expect to overcome all the demerits that we identified during the literature review. We demand that the proposed method will reconstruct the secret as such as the original image without losing any type of contrast reduction or information. One important advantage of this method is that it does not use halftone concept in the formation of shares.

4. Proposed Method

In this proposed method, visual cryptography encryption/decryption scheme is used to dispatch confidential images from sender to recipient with the higher level of security and confidentiality. Initially the RGB component of color secret image (SI) is extracted to create three distinct Red (R_i), Green (G_i), and Blue (B_i) matrices, each matrix represents the color components of SI. The individual color component of secret image (SI) is extracted by using the following equation:

$$\left.\begin{array}{l} R = SI\,[:,:,0] \\ G = SI\,[:,:,1] \\ B = SI\,[:,:,2] \end{array}\right\} \qquad (4)$$

The basis matrices, namely, R_1, R_2, G_1, G_2, B_1 and B_2 are constructed by splitting each pixel of R, G, and B into equally halved by each of the color component using equation [20](5).

$$\left.\begin{array}{r} R_1 = \frac{R}{2}, R_2 = R - R_1 \\ G_1 = \frac{G}{2},\ G_2 = G - G_1 \\ B_1 = \frac{B}{2},\ B_2 = B - B_1 \end{array}\right\} \qquad (5)$$

Then, a key matrix Ki with a size equivalent to Ri, Gi, and Bi matrices are generated randomly. This key matrix is XORed with the basic matrices of each color components to produce further matrices, namely, R_k1, R_k2, and G_k1, G_k2 and B_k1, B_k2 matrices respectively using equation (6).

$$\left.\begin{aligned} R_{K1} &= R_1 \oplus K_i,\ R_{K2} = R_2 \oplus K_i \\ G_{K1} &= G_1 \oplus K_i,\ G_{K2} = G_2 \oplus K_i \\ B_{K1} &= B_1 \oplus K_i,\ B_{K2} = B_2 \oplus K_i \end{aligned}\right\} \qquad (6)$$

Shares are constructed according to Hou's secret sharing scheme [9] by stacking R_k1, G_k1, B_k1 matrices into share 1 and R_k2, G_k2, B_k2 matrices into share 2 using equation (7).

$$\left.\begin{aligned} Share\ 1 &= Stack\ (R_{K1}, G_{K1}, B_{K1})\ \} \\ Share\ 2 &= Stack\ (R_{K2}, G_{K2}, B_{K2})\} \end{aligned}\right\} \qquad (7)$$

Once the shares construction process is over, both the shares constructed earlier are further encoded using the hybrid security algorithm such as AES followed by Blowfish for providing better security[11][13]. This is achieved by transforming each shares into matrix block and then performed basic encryption process of AES algorithm These encrypted shares are further encoded using blowfish algorithm by applying Blowfish algorithm to the AES encrypted shares to generate doubly encrypted shares.

In the share reconstruction phase, shares that doubly encrypted by Blowfish and AES algorithms are decrypted by basic decryption process of Blowfish algorithm and followed by basic decryption process of AES .Once the decryption process is over using above two algorithm, RGB values are extracted from those shares to construct the matrices R_k1, R_k2, and G_k2, G_k2, and B_k1, B_k2 using equation (8).

$$\left.\begin{aligned} R_{K1} &= Share1\ [:,:,0] \\ G_{K1} &= Share1\ [:,:,1] \\ B_{K1} &= Share1\ [:,:,2] \\ R_{K2} &= Share2\ [:,:,0] \\ G_{K2} &= Share2\ [:,:,1] \\ B_{K2} &= Share2\ [:,:,2] \end{aligned}\right\} \qquad (8)$$

The resultant matrices are XORed with the key matrix Ki which is generated earlier in the share construction phase to produce basis matrices, namely, R_1, G_1, B_1 and R_2, G_2, B_2 using following equation (9).

$$\left.\begin{aligned} R_1 &= R_{K1} \oplus K_i,\ R_2 = R_{K2} \oplus K_i \\ G_1 &= G_{K1} \oplus K_i,\ G_2 = G_{K2} \oplus K_i \\ B_1 &= B_{K1} \oplus K_i, B_2 = B_{K2} \oplus K_i \end{aligned}\right\} \qquad (9)$$

Finally, the R, G, B components of the secret image are constructed by combining, (R_1, R_2), (G_1, G_2) and (B_1, B_2) matrices using equation (10).

$$\left.\begin{aligned} R &= R_1 + R_2 \\ G &= G_1 + G_2 \\ B &= B_1 + B_2 \end{aligned}\right\} \qquad (10)$$

The original color secret image (SI) can be reconstructed by stacking all the R, G, B matrices together as in equation (11).

$$Reconstructed\ Image = Stack(R, G, B)\} \qquad (11)$$

Original color images can be reconstructed by stacking all shares of the secret image together.[20] The entire process in proposed method is as shown in figure 4.

5. Experiment Results

The above proposed method is implemented in Python 3.0 by using a dataset which comprises five real images captured using standard camera and mobile phone and five standard images as shown in figure 5. Initially RGB components of each image in the dataset is constructed followed by basis matrices for each color component are constructed by halving each color component extracted by 2. Then the random key matrix is generated with the size as that of basis matrices. The basis matrices constructed from each color component is XORed with the K_i for obtaining key matrices R_k1, G_k1, B_k1, R_k2, G_k2, B_k2 respectively. Share 1 and share 2 are then constructed by stacking each color component R_k1, G_k1, B_k1 and R_k2, G_k2, B_k2

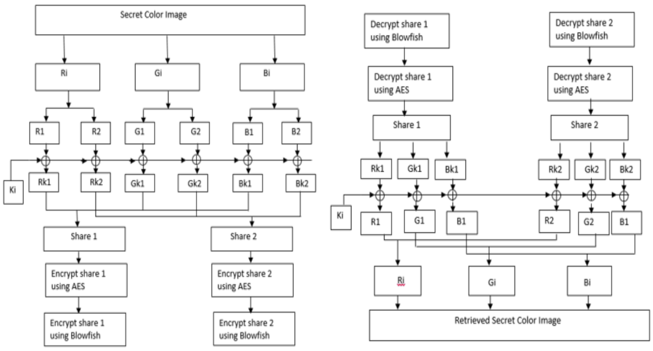

Secret Color Image
Ri
Gi
Bi
R1
R2
G1
G2
B1
B2
Ki
Rk1
Rk2
Gk1
Gk2
Bk1
Bk2
Share 1
Share 2
Encrypt share 1 using AES
Encrypt share 2 using AES
Encrypt share 1 using Blowfish
Encrypt share 2 using Blowfish
Decrypt share 1 using Blowfish
Decrypt share 2 using Blowfish
Decrypt share 1 using AES
Decrypt share 2 using AES
Share 1
Share 2
Rk1
Gk1
Bk1
Rk2
Gk2
Bk2
Ki
R1
G1
B1
R2
G2
B1
Ri
Gi
Bi
Retrieved Secret Color Image

FIGURE 4. Block diagram of proposed encryption and decryption method

Image Name	Original Image		Share Generation				Shares are Encrypted using AES				Shares are Multiply Encrypted using Blowfish				Reconstruct-ed Image	
			Share 1		Share 2		Share 1		Share 2		Share 1		Share 2			
	PSNR	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR
Parrots	1.00	100	0.01	27.82	0.01	27.81	0.00	27.81	0.00	27.80	0.00	27.80	0.00	27.80	1.00	100
Jet	1.00	100	0.00	27.90	0.00	27.90	0.00	27.89	0.00	27.89	0.00	27.87	0.00	27.87	0.99	100
Penguin	1.00	100	0.00	27.88	0.00	27.88	0.00	27.87	0.00	27.87	0.00	27.87	0.00	27.86	0.99	100
Flower	1.00	100	0.00	27.91	0.00	27.91	0.00	27.90	0.00	27.90	0.00	27.89	0.00	27.81	1.00	100
Pepper	1.00	100	0.00	27.89	0.00	27.89	0.00	27.88	0.00	27.88	0.00	27.87	0.00	27.87	1.00	100
Lena	1.00	100	0.01	27.90	0.01	27.90	0.00	27.89	0.00	27.90	0.00	27.80	0.00	27.80	0.99	100
Baboon	1.00	100	0.00	28.80	0.00	28.80	0.00	28.77	0.00	28.77	0.00	28.70	0.00	28.70	1.00	100
Rose	1.00	100	0.01	27.89	0.00	27.86	0.00	27.80	0.00	27.86	0.00	27.69	0.00	27.77	0.99	100
Pot	1.00	100	0.00	27.90	0.00	27.99	0.00	27.83	0.00	28.83	0.00	27.83	0.00	27.83	1.00	100
Garden	1.00	100	0.00	27.89	0.00	27.86	0.00	27.80	0.00	27.86	0.00	27.71	0.0	27.71	1.00	100

Table 1 PSNR and SSIM calculation of different Samples

respectively. Once these shares are formed, AES and Blowfish algorithm are used to encrypt the share 1 and share 2 respectively. In the reconstruction phase, the original secret image is retrieved by applying all the above steps in the reverse order. The output that obtained by the above method as shown in figure. The performance of the proposed scheme is evaluated by using two parameters such as PSNR and SSIM as shown in table 1 and corresponding output is given in figure 5.

On evaluating the SSIM and PSNR value of the ten images in the dataset as shown in the tabel 1, we can see that the value of these two parameters are very much close in both the reconstructed image after going through the multilevel encryptions techniques discussed in this paper. The SSIM and PSNR vlaue of all the original image in the dataset as well as the reconstructed image have almost same value. This reveals that almost all the reconstructed images by the proposed method original image before the construction of shares and the produces exactly same image as that of the original images in the dataset. Further we evaluated SSIM and PSNR value of all the intermediate levels of the share construction and it shows wide variations in all these levels. Therefore, we can coclude that the proposed color visual cryptographic encryption schemes with multiple level of encryption techniques all together produce better and good output compared to all other methods that we discussed.

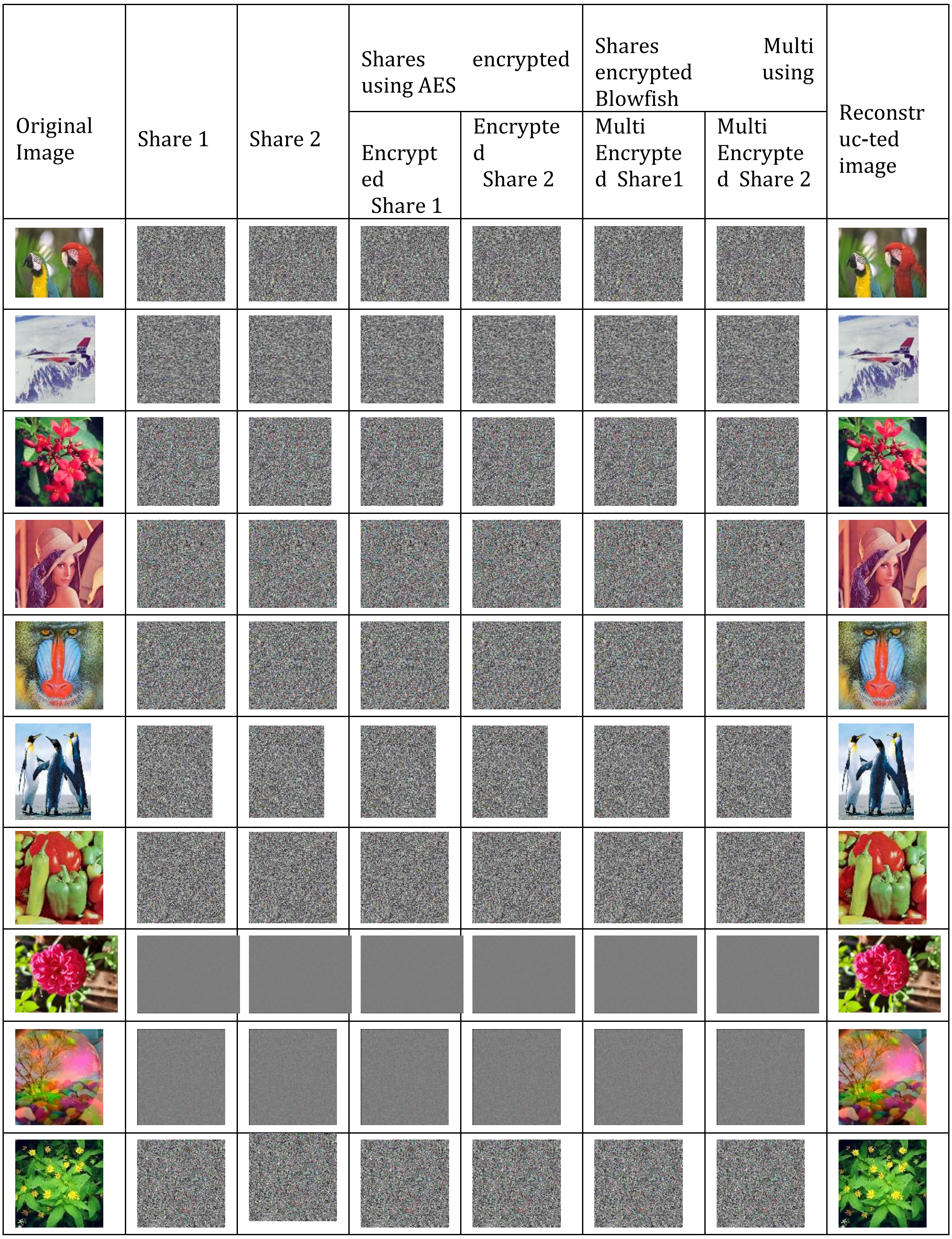


Figure 5 Examples of the Proposed Scheme

6. CONCLUSION

In this paper, we presented a secure transferring of the secret color images with the highest level of security. Separate R, G, B matrices are extracted from secret color images. Each of these matrices is then equally halved to generate, R_1, R_2, G_1, G_2, B_1, B_2 matrices. These matrices were XORed with key matrix Ki to produce basis matrices: R_k1, G_k1, B_k1, R_k2, G_k2, B_k2. Using well-known Hou's third method in color visual cryptography, combine R_k1, G_k1, B_k1 into share 1 and R_k2, G_k2, B_k2

into share 2. These shares were further encode using the AES and Blowfish algorithm for providing better security. All the images that are constructed from the dataset retains the same quality of the original image by using this proposed method. Thus, the proposed method is very good method for hiding secrets confidently compared to already established work. Even though the proposed method preserves the quality of the retrieved image as that of the original image, the algorithm used here contains complicated computation steps and it took too much time for execution. By reducing the complex step in algorithm and increase the performance of this algorithm that fruitfully hiding color image securely is the further enhanced work that has to be in cooperated in future.

7. REFERENCES

[1] William Stallings, “Cryptography and Network Security Principles Practices”, Prentice Hall of India Pvt. Ltd,2008 M.

[2] Naor, A. ShamirVisual Cryptography. In: Advances in Cryptography-Eurocrypt’94 vis Lecture Notes in Computer Science, 950 (1994), pp. 1-12

[3] Sankrithidevaki K P, Rajkumar K K, "A study on hiding confidential data in images using different Visual Cryptographic threshold schemes", IPASJ INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY

[4] Kour, Haneet.(2015). IJARCCE Analysis on Image Color Model. 4. 233-235. 10.17148/IJARCCE.2015.41253

[5] "Control, Computation and Information Systems", Springer Science and Business Media LLC, 2011

[6] Eric R. Verheul and Henk C. A. Van Tilborg, Constructions and Properties of k out of n Visual Secret Sharing Schemes, Designs, Codes, and Cryptography, 11:179-196, 1997.

[7] Jinu Mohan, Dr. Rajesh.R, "Exploration of Color Visual Cryptography Schemes", International Journal of Science andResearch(IJSR), https://www.ijsr.net/search_index_results_paperid.php?id=SUB156559,Volume 4 Issue 7, July 2015, 1033 – 1038

[8] V. Rijmen, B. Preneel, Efficient colorvisual encryption forshared colors of Benetton, Eurocrypto’96, Rum Session,Berlin, 1996.

[9] Young-Chang Hou. Visual cryptography for color images, Journal of Pattern Recognition 2003; 36:16191629

[10] AshaBhadran R, “An Improved Visual Cryptography Scheme for Colour images”, International Research Journal of Engineering and Technology, Volume 02, Issue:05, Aug-2015

[11] Bhatia, Shradha & Khatri, Sunil Kumar & Singh, Ajay. (2018). Digital Image Security Using Hybrid Visual Cryptography. 570-576.10.1109/ICRITO.2018.8748622.

[12] PURWINARKO, Aji; HARDYANTO, Wahyu. A

Hybrid Security Algorithm AES and Blowfish for Authentication in Mobile Applications. **Scientific Journal of Informatics**, [S.l.], v. 5, n. 1, p. 80, may 2018. ISSN 2460-0040.

[13] Specification for the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, Nov. 2001

[14] Q. Zhang and Q. Ding, "Digital Image Encryption Based on Advanced Encryption Standard (AES)", 2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC),Qinhuangdao,2015,pp.12181221,doi:10.1109/IMCCC.2015.261.

[15] Luhaniwal, Chandani. (2019). Data Security by Encryption-Decryption using AES Algorithm of Cryptography. International Journal for Research in Applied Science and Engineering Technology.7.1260-1265. 10.22214 / ijraset.2019.7205.

[16] T. Nie and T. Zhang, "A study of DES and Blowfish encryption algorithm," TENCON 2009 - 2009 IEEE.

[17] Sougata Mandal, Sankar Das and Asoke Nath, “Data Hiding and Retrieval using Visual Cryptography”,in International Journal of Innovative Research in Advanced Engineering(IJIRAE),Volume1,Issue1,April 2014,pp:102 – 110.

[18] RGB Based Secret Sharing Scheme in Color Visual Cryptography, M.Karolin , Dr.T.Meyyapan, International Journal of

Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2015.

[19] Anantha Kumar Kondra, Smt. U. V. Ratna Kumari, "An Improved (8, 8) Colour Visual Cryptography Scheme Using Floyd Error Diffusion", in International Journal of Engineering Research and Applications, Vol. 2, Issue 5, September-October 2012, pp.1090- 1096.

[20] Shankar K. Eswaran.Sharing a Secret Image with Encapsulated Shares in Visual CryptographyIn: Procedia Computer Science, 70 (2015),pp. 462-468

[21] M.Nazm-Bojnordi, N. Sedaghati-Mokhtari, S.Mehdi Fakhraie."ASelf-Testing FullyPipelined Implementation for the Advanced EncryptionStandard",2005 International Conference on Microelectronics, 2005

[22] Anindita Sarkar, Swagata Roy Chatterjee, Mohuya Chakraborty. "Chapter 5 Role of Cryptography in Network Security", Springer Science and Business Media LLC, 2021

[23] Mahmoud Rajallah Asassfeh, Mohammad Qatawneh, & Feras Mohamed ALAzzeh.(2018).Performance Evaluation of Blowfish Algorithm on Supercomputer IMAN1. International Journal of Computer Networks Communications (IJCNC), 10(2), 43–53.

[24] P. Kashyap and A. Renuka, "Visual Cryptography for colour images using multilevel thresholding," 2019 Third International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2019, pp. 567-572, doi: 10.1109/ICISC44355.2019.9036432.Region 10 Conference, Singapore, 2009, pp. 1-4,doi: 10.1109 / TENCON.2009.5396115

[25] .MohammedAbdulameer Aljanabi, Zahir M. Hussain, Noor Abd Alrazak Shnain & Song Feng Lu (2019) Design of a hybrid measure for image similarity:a statistical,algebraic,and information-theoretic approach,European Journal of Remote Sensing,52:sup4,215, DOI: 10.1080/22797254.2019.1628617

[26] Muhammad Faheem, Sapiee Jamel,Abdulkadir Hassan, Zahraddeen A., NurShafinaz, Mustafa Mat. "A Survey on the Cryptographic Encryption Algorithms",International Journal of Advanced ComputerScience and Applications, 2017