Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 70 (2015) 462 – 468

Procedia Computer Science

4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS 2015

Sharing a Secret Image with Encapsulated Shares in Visual Cryptography

Shankar K*, Eswaran P

Department of Computer Science and Engineering, Alagappa University, Karaikudi-630 003,India

Abstract

Due to advances in digital world, security has become an inseparable issue while transmitting the image. Visual cryptography (VC) is a modern cryptographic technique which is used to the secret image is shared securely and also its information is maintained with utmost confidentiality. A sender transmits the secret image which is divided into shares and it holds hidden information. When all of these shares are aligned and stacked together, they tend to expose the secret image information to the receiver. Earlier VC scheme, the secrecy of the share is not maintained due to any other fake shares can easily insert or modified remain to be continuing challenges. To solve this security issues, a secure share creation scheme constructed by a (2, 2) XOR based VC scheme is proposed. Once the shares are created, it is encrypted separately by using Advanced Encryption Standard (AES) algorithm. In this process, shares and AES algorithm bind together to give the resultant shares are called the encapsulated shares. Consequently, the secret image information cannot be retrieved from any one transparency via human visual perception. The Proposed scheme offers better security for shares and also reduces the fraudulent shares of the secret image. Further, the experimental results and analyses have demonstrated that the proposed scheme can effectively encrypt the image with the fast execution speed and minimized PSNR value.

Peer-review under responsibility of the Organizing Committee of ICECCS 2015

Keywords: Visual cryptography; Shares; AES; XOR; Encryption; PSNR.

1. Introduction

With the emergence of multimedia application, there is a huge demand for transmission and secured storage of information. So security is indispensable to discover proper protection.

*Corresponding author. Tel.: +919942725200 ;
E-mail address:shankarcrypto@gmail.com

Peer-review under responsibility of the Organizing Committee of ICECCS 2015
doi:10.1016/j.procs.2015.10.080

If the information is protected, the intruders may not be distorted the data. The way to proper and secure transmission of the data becomes a challenging issue. Cryptographic techniques afford the confidentiality and security by reducing the prospect of adversaries [1]. It deals with the technique which is used to renovate the data among understandable and incomprehensible forms by using encryption and decryption method under the power of the keys. It provides the content security and access control. One of the most widely used type of information sharing or secret sharing is the visual secret sharing. Without involving any complex computations, decode the secret image visually by superimposing a qualified subset of shares through the visual secret sharing method. In the context, there exist Boolean operation of the secret image sharing that overcomes the drawback of low visual quality and pixel expansion created by the VSS [2]. Visual cryptography is a special secret sharing technique that means it is dissimilar from usual cryptography, for the reason that it does not require complex computation to decrypt. Color Visual Cryptography, emerging field, encrypts the color secret messages into multiple numbers of color halftone image shares. A visual Information Pixel synchronization and error diffusion technique enables the encryption of visual data with high quality. Synchronization decoding the spot of pixels along with the secret images during error diffusion produces shares agreeable to human visual system. The noise created by the preset pixels was diffused by the neighbor pixels whenever the encryption on share taken place [3]. The data hiding is the embedding technique which the secret shares are hidden using some kind of methods. The combination of the visual cryptography with the watermarking technique is to increase the image efficiency and security [4]. In the modern public key cryptography, factors decomposition hassles dependent on huge numbers are habitually employed, the classic example being the RSA cryptography. In visual cryptographically the generated image shares are encrypted by using RSA algorithm. The combination of visual cryptography with the public key encryption ends in high security while transmitting the image [5]. The solution of the innovative technique for keeping dishonesty at bay is the acceptance of several secret images in such a way that each qualified subsets will expose the relative secret image only, leaving the other secret images unfamiliar to the prospective hawkers[6].

2. Related works

Srinivasan nagaraj et al [7].The enlarged size of the internet and vast communication across it and also medical needs digital images require of security plays vital role. New encryption technique Using elliptic curve cryptography with magic matrix operations for securing images that transmits over a public unsecured channel. There are two most important groups of image encryption algorithms: some are non chaos-based selective methods and chaos-based selective methods.

Xuehu Yan et al [8] have proposed three general threshold construction methods from specific cases. The constructed threshold VCSs are also progressive VCS without the pixel expansion. The shadow images (Shares) are random noise-like, hence the authors proposed CVCS has no cross interference of secret image in the shadow images. From the progressive visual quality of the authors, covered secret image can be gained for the CVCS. When the shadow images are collected, cannot retrieve any information of the secret image could be recognized, which shows the security of the CVCS.

Paulius Palevicius et al [9] presented the integration of dynamic visual cryptography technique based on the inter play of visual cryptography and time averaging geometric with Gerchberg–Saxton algorithm. The authors made study on the stochastic grating, which is used to embed the secret into a single cover image. The hidden information can be visually decoded by a naked eye if only the amplitude of harmonic oscillations corresponds to an accurately preselected value. The visual image encryption scheme is based on computer generated holography, optical time-averaging and principles of dynamic visual cryptography were provided by the authors.

3. The Proposed Scheme

The proposed visual cryptography technique is used to send an original image from the sender to the receiver with supreme confidentiality and secrecy. From the secret image the RGB color band of the pixel values are taken and create the separate matrix (R_i, G_i, B_i) [13]. The basic matrices R_1, R_2, G_1,G_2 and B_1,B_2 are obtained by dividing each and every value in R_i, G_i and B_i by 2. Generate globalized key matrix randomly (K_m , where m=0, 1, 2...255) based on size of the basic matrices. Then, the XOR(K_m, R_1) and XOR(K_m ,R_2) performs an XOR function on the

elements of R_1 and R_2 matrices with key matrix K_m separately and get the resultant matrices as R_{S1} and R_{S2} in R_i matrix. This process is repeated for creating G_{S1}, G_{S2} and B_{S1}, B_{S2} in G_i and B_i matrices also. According to Hou's well-acclaimed Secret Sharing Scheme [11], combine the R_{S1}, G_{S1} and B_{S1} matrices to create share 1 and R_{S2}, G_{S2} and B_{S2} matrices to create share 2. When the share creation process is done, each share is encrypted by using AES algorithm to keep its information securely. In this process, shares and AES algorithm binds together to give the resultant shares are called the encapsulated shares. It is used to secure the shares from adversaries or attackers. The whole proposed encryption processes described above are simply states as the block diagram is shown in Figure 1.

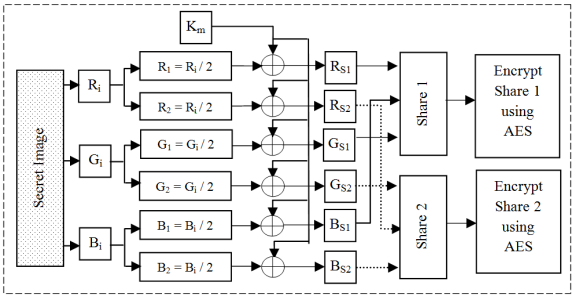

Fig. 1. Block diagram of proposed Encryption method.

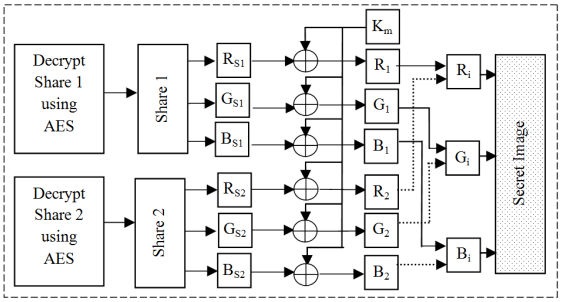

Fig. 2. Block diagram of proposed Decryption method

During the decryption process, the encapsulated shares are extracted by decryption process of AES algorithm to retrieve the share1 and share2. Then, the shares reconstruction process, each shares individually extract the color band and create matrices as R_{S1}, G_{S1}, B_{S1} and R_{S2}, G_{S2}, B_{S2}. Then, the XOR (K_m, R_{S1}), XOR (K_m, G_{S1}) and XOR (K_m , B_{S1}) and XOR (K_m , B_{S1}) performs XOR function on the elements of R_{S1}, $G_{S1}$and B_{S1} matrices with key matrix Km separately and retrieve the basic matrices as R_1,$G_1$and B_1. This process is repeated to retrieve other basic matrices such as R_2, G_2 and B_2 also. Finally, all decrypted shares are stacked (Combine these (R_1, R_2) (G_1, G_2) and (B_1, B_2) matrices) together to retrieve the secret image. Only if all the numbers of secret shared images are stacked together, it is possible to reveal the secrets. If any one of the shares of the original image is missing, it is impossible to retrieve the original image. The whole proposed Decryption processes described above are simply states as the block diagram is shown in Figure 2. When the decryption process is completed, the encrypted image is compared with the original image for evaluating their performance by using the peak signal to noise ratio value. By using this scheme, the original image is shared securely and the original image information is maintained confidentially.

3.1. Shares Creation Scheme

The RGB pixel values are taken from the original image and the separate matrix (Original Matrix) (R_i, G_i, B_i). Generate globalized key matrix K_m , Where m= 0, 1, 2…255. For example,

$$R_i = \begin{bmatrix} 127 & 127 & 128 & 125 \\ 127 & 126 & 127 & 123 \\ 126 & 125 & 127 & 125 \\ 126 & 126 & 126 & 127 \end{bmatrix} \quad G_i = \begin{bmatrix} 234 & 234 & 236 & 233 \\ 233 & 233 & 234 & 230 \\ 230 & 229 & 232 & 230 \\ 230 & 230 & 230 & 231 \end{bmatrix} \quad B_i = \begin{bmatrix} 125 & 123 & 122 & 116 \\ 121 & 118 & 117 & 112 \\ 113 & 111 & 111 & 107 \\ 110 & 107 & 106 & 105 \end{bmatrix} \quad K_m = \begin{bmatrix} 100 & 120 & 154 & 80 \\ 161 & 234 & 180 & 120 \\ 121 & 185 & 148 & 59 \\ 108 & 132 & 220 & 170 \end{bmatrix}$$

The basic matrices R_1, R_2, G_1,G_2 and B_1,B_2 are obtained by dividing each and every value in R_i, G_i and B_i by 2. For example, let the R_i Matrix value is 127, 127/ 2= 63.5. So consider the Floor value as R_1 = 63 and Ceiling value as R_2 = 64, hence 63+64 = 127. For example,

$$R_1 = \begin{bmatrix} 63 & 63 & 64 & 62 \\ 63 & 63 & 63 & 61 \\ 63 & 62 & 63 & 62 \\ 63 & 63 & 63 & 63 \end{bmatrix} \qquad R_2 = \begin{bmatrix} 64 & 64 & 64 & 63 \\ 64 & 63 & 64 & 62 \\ 63 & 63 & 64 & 63 \\ 63 & 63 & 63 & 64 \end{bmatrix}$$

Then, the XOR(K_m, R_1) and XOR(K_m ,R_2) performs an XOR function on the elements of R_1 and R_2 matrices with key matrix Km separately and get the resultant matrices named as R_{S1} and R_{S2} in R_i matrix.

$$R_{S1} = \begin{bmatrix} 91 & 71 & 218 & 110 \\ 158 & 213 & 139 & 69 \\ 70 & 135 & 171 & 5 \\ 83 & 187 & 227 & 149 \end{bmatrix} \qquad R_{S2} = \begin{bmatrix} 36 & 56 & 218 & 111 \\ 225 & 213 & 244 & 71 \\ 70 & 134 & 212 & 4 \\ 83 & 187 & 227 & 234 \end{bmatrix}$$

This process is repeated for creating G_{S1}, G_{S2} and B_{S1}, B_{S2} in G_i and B_i matrices also. According to Hou's well-acclaimed Secret Sharing Scheme, combine the R_{S1}, G_{S1} and B_{S1} matrices to create share 1, R_{S2}, G_{S2} and B_{S2} matrices to create share 2.

3.2. AES Algorithm based Shares Encryption and Decryption

AES (Advanced Encryption Standard), the standard algorithm used for the encryption is considered as one of the strongest algorithm. Its block size and lengthy key size make it most effective scheme for the encryption. It falls under the category of the symmetric key encryption in which both the communicating parties uses same key. It encrypts and decrypts a data block of 128 bits. The key size, in which can be 128, 192 or 256 bits. It uses 10,12or 14 rounds depending on the key size.

3.2.1. Shares Encryption

Basically AES algorithm consists of the flowing four base procedures. SubBytes Transformation: The SubBytes () transformation is a non linear byte substitution that operates independently on each byte of the state using a substitution table. ShiftRows Transformation: In the ShiftRows ( ) transformation, the bytes in the last three rows of the state are cyclically shifted over different number of bytes. The first row will not get shifted. MixColumn Transformation: In MixColumn ( ), the columns of the state are considered as polynomial and then multiplied by modulo with fixed polynomial, individually. AddRoundKey Transformation: In the AddRoundKey () transformation, a round key is added to a state by a simple bitwise XOR operation. Each round key consists of N_b words from the key schedule; those N_b words are each added into the columns of the state. To encrypt the shares the input is considered as a shares. Hence, the shares are taken that is converted into block matrices. During the encryption process, the shares are undergone to the basic procedure of AES algorithm and the output is encrypted share. In this process, shares and AES algorithm binds together to give the resultant shares are called the encapsulated shares.

3.2.2. Shares Decryption

The rounds of the decryption algorithm are governed by the following four stages namely the Inverse Shift rows, Inverse Substitute Bytes, Add round key and Inverse Mix columns steps. The inverse AddRoundKey step was eliminated. AES decryption occurs simply as the reverse order of encryption. The encrypted shares are now fed as the input blocks, in which the inverse shifting of the rows value is taken place. It is then followed by the inverse substitution of the pixel positions along with the Key value. Finally, the inverse mix column step was taken place. The resultant image thus produced was the original image at the time of share creation. During the decryption process, the encapsulated shares are extracted by decryption process of AES Algorithm to retrieve the share 1 and share2.

3.3. Shares Reconstruction Scheme

Finally, all decrypted shares are stacked (Combine these (R_1, R_2) (G_1, G_2) and (B_1, B_2) matrices) together to retrieve the secret image. Only if all the numbers of secret shared images are stacked together, it is possible to reveal the secrets. If any one of the shares of the original image is missing, it is impossible to retrieve the original image.

4. Result and Discussion

The proposed method is implemented with Visual Studio 2010, C# language under the configuration of windows 7 operating system with Core-i3 and 3 GB RAM. The performance evaluation factors Peak Signal to Noise Ratio and time requirement for share creation and stack reconstruction is acquired from different sample images.

4.1. Experimental analysis

The experimental result from the implementation of the proposed scheme, the original image, shares, encrypted share and decrypted share of the Lena and Baboon image is represents in the Figure 3 and 4.

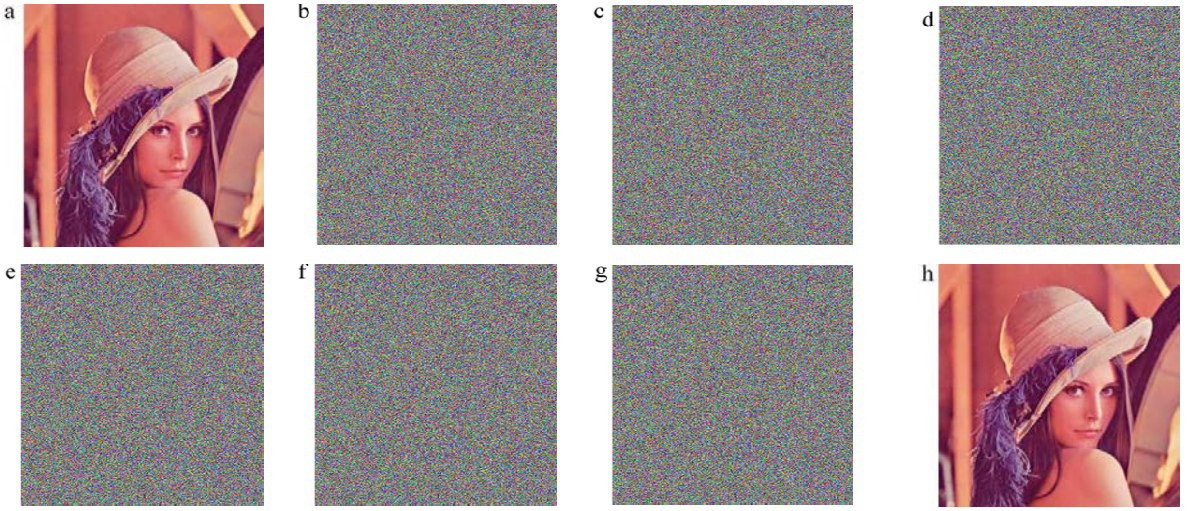

Fig. 3. (a) Secret image; (b, c) Shares; (d, e) Encrypted Shares; (f, g) Decrypted Shares; (h) Stacked Image;

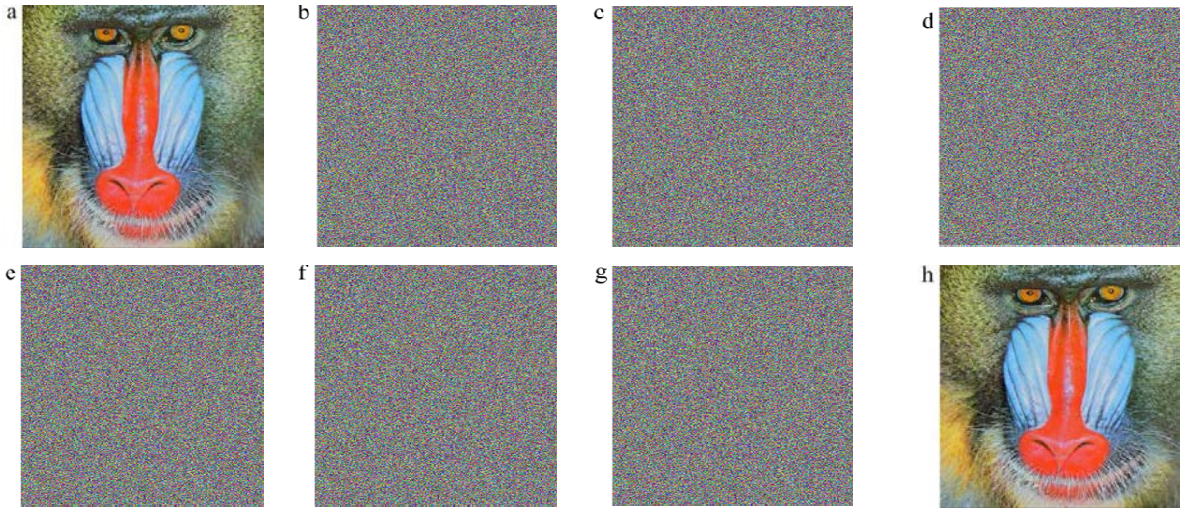

Fig. 4. (a) Secret image; (b, c) Shares; (d, e) Encrypted Shares; (f, g) Decrypted Shares; (h) Stacked Image;

4.2. Performance Analysis

4.2.1. Peak Signal to Noise Ratio:

Image encryption is a conversion of secret image into scrambled image. The image quality may be differing from secret image to encrypted image depending on the encryption algorithm. High PSNR (Peak Signal to Noise Ratio) indicate a lower variation between the original (without noise) and reconstructed image. The major benefit of this measure is simplicity of computation, but it does not reflect perceptual quality of the image [10].

Table 1.PSNR (in db) values for Different sample images.

Image Name	Shares Generation		Shares are Encrypted using AES	
	Share 1	Share 2	Share 1 Encryption	Share 2 Encryption
Lena	8.78	8.78	8.77	8.77
Baboon	8.81	8.81	8.80	8.81

In table 1, the proposed scheme with their PSNR is employed for various sample test images. As per PSNR understanding with original image and decrypted image, the value should be higher. It shows the better for its superiority. When the PSNR value is compared for the original image with encrypted image, the PSNR is low which yields better encryption quality. It is clear that the PSNR values are 8.78 and 8.81, which shows low PSNR value, it represents better encryption quality with high security of the secret image.

4.2.2. Measurement of Share Generation and Reconstruction Time:

Distant from quality measures considerations, execution time is the measurement of Shares Generation and reconstruction of proposed scheme is summarized in table 2.

Table 2.Shares Generation and reconstruction Time (in seconds) for Different sample images.

Image Name	Shares Generation	Shares Reconstruction
Lena	0.095	0.011
Baboon	0.098	0.013

The time taken to generate the share is nearly 0.095 seconds and shares reconstruction is 0.011 seconds respectively. Thus, by implementing the proposed scheme time taken for shares generation and reconstruction is very fast and also image quality is maintained.

4.3. Comparative Analysis

Table 3 show a comparison between time required for the shares Generation and reconstruction of proposed scheme with the different methods (reference number.12).

Table 3.Comparison of different methods on the Basis of Shares Generation and Reconstruction Time.

Methods	Shares Generation (sec)	Shares Reconstruction (sec)
Basic VC	1.343	0.046
Hilbert Curve	4.157	0.016
Zigzag Scan approach	1.297	0.016
Proposed method	0.095	0.011

The graphical representation of Figure 5 and 6 reveals the proposed scheme is less time required for share generation and share reconstruction compare between earlier methods.

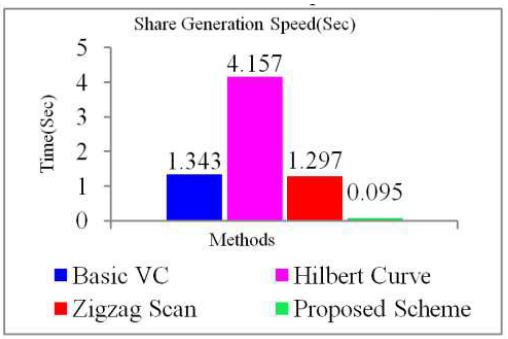

Fig. 5. Shares Generation time of Different techniques

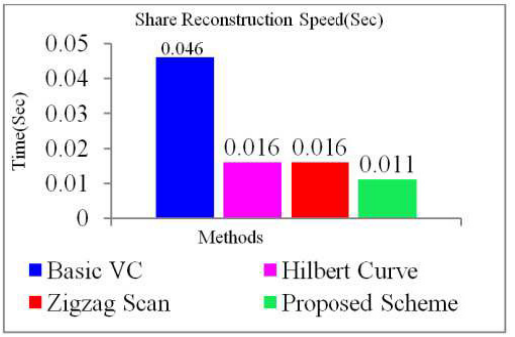

Fig. 6. Shares Reconstruction time of Different techniques.

5. Conclusion

Most of the existing VC schemes, to maintain the shares information is highly complex. This predominant issue is considered in this paper, a novel secure share creation scheme is proposed. It constructs an encapsulated share mechanism that leftovers a useful scheme to protect the shares. The result gives that how to create an encapsulated share in VC scheme and difficulty in exposing the identity of the secret image under different real time applications. In this proposed scheme provides the combination of VC scheme and shares encryption to increase the computation complexity to some extent, but it provides high security to share. For further research, it is extended that the visual cryptography would be used for different share creation procedure as well as minimization in its PSNR value.

References

1. Shamir. A. How t o Share a Secret. Communications of the ACM 1979; 22: 612-613.
2. A Nag, S Biswas, D Sarkar, PP Sarkar. Secret Image Sharing Scheme Based on Boolean Operation. Cybernetics and Information Technologies 2014;14:98-113.
3. I. Kang, G. R. Arce, H. K. Lee. Color extended visual cryptography using error diffusion. IEEE Trans. Image Process 2011; 20:132–145.
4. Debasish Jena, Sanjay Kumar Jena. A Novel Visual Cryptography Scheme. International Conference on Advanced Computer Control 2008.
5. Kulvinder Kaur,Vineeta Khemchandani. Securing Visual Cryptographic shares using Public Key Encryption. Advance Computing Conference (IACC).IEEE 3rd International 2013; 1108, 1113.
6. Du-Shiau Tsai, Tzung-Her Chen and Gwoboa Horng: A cheating prevention scheme for binary visual cryptography with homogeneous secret images. Journal of Pattern Recognition 2007.40: 2356-2366.
7. Srinivasan nagaraj, Raju and Koteswara rao: Image Encryption Using Elliptic Curve Cryptography and Matrix. In proceedings of Intelligent Computing, Communication & Convergence 2015; 48: 276-281.
8. Yan, X., Wang, S., Niu, X. Threshold construction from specific cases in visual cryptography without the pixel expansion. Signal Processing 2014;105:389–398.16/j.sigpro.2014.06.011.
9. Paulius Palevicius, Minvydas Ragulskis. Image communication scheme based on dynamic visual cryptography and computer generated holography. Optics Communications 2015; 335:161-167.
10. K. Shankar, K. Mahesh,K, Kuppusamy.K. Analyzing Image Quality via Color Spaces. International Journal of Image Processing and Data Visualization 2014.
11. Young-Chang Hou. Visual cryptography for color images. Journal of Pattern Recognition 2003; 36:1619-1629.
12. Soumyahegde, BhaskaraRao. Visual Cryptography (VC) using Zigzag Scan Approach. Journal of computer science engineering and technology 2011;1:456-461.
13. 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.