ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Performance Evaluation of Secure Share Creation Schemes in Visual Cryptography

K.Shankar[1], Dr.P.Eswaran[2]

[1]Ph.D Research Scholar, [2]Assistant Professor
Department of Computer Science and Engineering, Alagappa University,
Karaikudi-600 003, Tamilnadu, India.
[1]shankarcrypto@gmail.com,[2]eswaranperumal@gmail.com

***Abstract*— The Visual Cryptography (VC) is a method for protecting the image-based secrets that has a computation-free decoding process. A secret image is converted into n transparencies of random prototypes in VC. It is possible to convert the secret image outwardly by superimposing a qualified subset of transparencies. The Main objective of the proposed research work is to observe the different type of attacks on the information and tackle them with the right type of counter measures. Moreover, optimize the countering process by the proposed schemes. It is used to send an original image from the transmitter to the receivers with confidentiality. In this research work, three schemes are proposed to enhance the efficiency of VC. In the first scheme, RGB based multiple share creation in VC with aid of ECC techniques is proposed. The test outcomes have revealed the fact that the Peak Signal to Noise Ratio is 58.0025, Mean Square Error (MSE) value is 0.1164 and the Correlation Coefficient (CC) is 1. In the second scheme, secure share creation in VC using ECC with aid of optimization technique for color images are proposed. From the test results of this scheme, the outcome has exposed the PSNR is 65.73057, then MSE is 0.017367 and the CC is 1 and this optimal PSNR value is attained in the Cuckoo search (CS) algorithm. In the third scheme, new Visual Secret Share (VSS) creation technique to enhance the efficiency of VC with ECC is proposed. The result of this scheme, it is revealed that the PSNR is 69.568, the MSE is 0.013 and the CC is 0.992 and this optimal PSNR value is attained in the Grey Wolf Optimization (GWO) algorithm. This paper presents the performance evaluation and comparison of the above mentioned three secure share creation schemes.**

***Keywords*— Visual Cryptography, Elliptic Curve Cryptography, Image, Visual Secret Share, Shares, Encryption, Cuckoo search algorithm, Grey Wolf Optimization algorithm.**

I. INTRODUCTION

With the increase in digital media, there is need to protect such information is becoming more necessary. The source of digital media's growth can be linked to the wealth of information provided by the Internet. Visual cryptography process the encrypting technologies of time-honored cryptography are generally employed extensively to shelter data safety [1]. The employment of the cryptography technique is data concealing of a universal method. And in this regard, credit goes to Shamir for launching a well-acclaimed method for secret sharing which is known by the name cryptography technique [2]. The vital role of the visual cryptography scheme is to encrypt the private image by the help of splitting. The private message cannot be reveal by the help of some split images. The original image requires all split images to reveal. This is a popular study in visual cryptography. The process of visual cryptography is to divide an image into prearranged number of parts and then without any computation or algorithm the secret image can reveal by aligning and stacking together [3].

Visual secret sharing (VSS) has impressed in academia and increasing a number of VSS applications such as image encryption, visual authentication, image hiding and digital watermarking visual cryptography (VC) in 1994. In visual cryptography is mainly need to encrypt the image by using of encryption algorithm but for exposing the image, there does not need any algorithms. The challenge is controlling a number of meaningless shares because all shares must need for various secrets to expose. Therefore it is difficult to control and use [4].

ECC is a public key cryptography which is related on the arithmetic model of elliptic curve with limited fields. By the differentiation of ECC requires smaller keys than non-ECC cryptography to provide equivalent protection. Public key cryptosystem is the basic of all modern encryption or digital signal methods where one key is decryption key or signature generation key and the other one is cipher text generation key or signature verification key [5].

The integer factorization difficulty of RSA and Digital Light Processing (DLP) was solved this algorithm in a fast manner, which have the predictable execution time. The Elliptic curve digital light processing (ECDLP) was solved by a known fastest algorithm which have exponential predictable running time [6]. Generally, the optimization theory and methods are mostly used in the field of applied mathematics.

The optimization method also includes finding the best accessible value of target function from a defined domain or variety of target functions from different type of domain [7].

The main purpose of the optimization is used to reduce the interval of a point multiplication depend on the number of required cycles. Especially, the replicated arithmetic obstructs are used to improve the parallelism for fundamental process. Though most of the executions are take place on algorithm optimization or improved arithmetic architectures or sometimes the processor architecture also suitable for ECC point multiplication [8].

Another important advantage of elliptic curve cryptosystem is that create ECC more impressive for the arithmetic functions in the basic areas [9]. Different type of optimization methods can be used in ECC and the private key optimization. In ECC technique, for developing the process of the cryptographic image several optimization method is used. Such as genetic algorithm (GA), Cuckoo search (CS) algorithm, Differential evaluation (DE) algorithm, Ant Colony Optimization (ACO), Particle Swarm Optimization (PSO) and Grey Wolf Optimization (GWO) for the private key generation [10][11][12].

II. PROPOSED SCHEMES

A. *Scheme I : A Secure Multiple Share Creation Scheme in Visual Cryptography with assist of Elliptic Curve Cryptography*

In this scheme, the pixel values (P_v) of the color image (RGB image) are extracted from the original image and represent as matrix (P*Q). The extracted pixels values are used to create the multiple shares (share1, share2…share n) and the shares are divided into blocks. The blocks of the shares are encrypted by using the ECC method and the encrypted image is decrypted by using the decryption of the ECC method. Figure 1 shows the block diagram of the proposed visual cryptography scheme I.

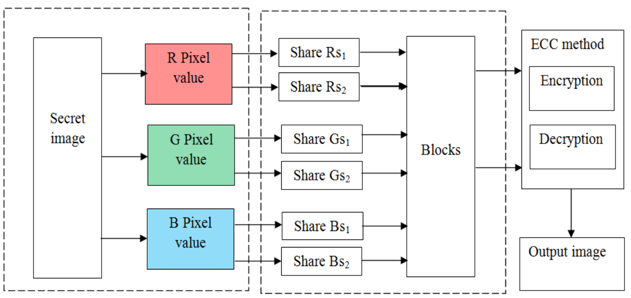

Fig. 1 Scheme I: Block diagram of Multiple Share Creation

Finally the output image is compared with the original image for evaluating their performance by using the PSNR, MSE and CC values. It is clear that the PSNR values are 58.0025, 57.4297, 56.684 and 58.1438 the image excellence is preserved in spite of ambushes made on the secret image. The correlation coefficient value is the almost all the images are nearly 1 and the MSE is the 0.103, 0.1176, 0.1454 and 0.0997. From that, the original image quality is not assorted and it is retained by using the proposed method. The CC estimations have made it crystal clear that the encryption technique is performed on the secret image so as to preserve the confidentiality of the image. Thus the confidentiality of the image is upheld in the long run and the reclaimed image is offered the unique image without in any way adversely influencing the quality of the image.

B. *Scheme II : A Secure Multiple Share Creation Scheme in Visual Cryptography using Elliptic Curve Cryptography with Optimization Technique*

The proposed scheme II is used to send an original image from the transmitter to the receivers with confidential and secret. From the original image, the pixel values (P_v) are extracted and separately create an RGB pixel matrix. The proposed method is used to create the shares from their pixel values. The extracted pixel values are used to create the multiple shares (share1, share2…share n) and the shares. The multiple shares created for the secure image transmission and maintain the image information confidentiality, and then the image shares are divided into blocks. The blocks of the each share are encrypted by using the ECC method and the encrypted image is decrypted by using the decryption of the ECC method. Figure 2 shows the block diagram of the proposed visual cryptography scheme II.

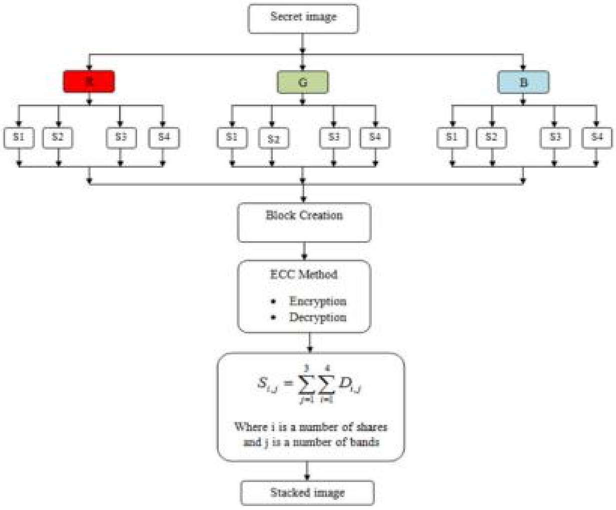
Secret image
R
G
B
S1
S2
S3
S4
Block Creation
ECC Method
Encryption
Decryption
$S_{i,j} = \sum_{j=1}^{3} \sum_{i=1}^{4} D_{i,j}$
Where i is a number of shares and j is a number of bands
Stacked image

Fig. 2 Scheme II: Block diagram of Multiple Share Creation

In encryption process, the public key randomly generated and the decryption process employs the optimization technique for the private key generation of the ECC method. For improving the performance of the cryptographic image in

ECC method, different optimization technique is used such as Genetic Algorithm (GA), Cuckoo search (CS) algorithm, and Differential Evaluation (DE) algorithm. The performance of the image is taken as a fitness value for the optimization process such as PSNR value which is shown the difference between the original image and CC value. It is clear that the PSNR values of the secret different images are 65.73057, 65.7167, 64.9333, and 65.7563. The MSE value is minimized in all images is 0.0107, 0.0107, 0.0209 and 0.0172 then the correlation coefficient value is the almost all the images are nearly1.

C. *Scheme III: A Secure Visual Secret Share (VSS) Creation Scheme in Visual Cryptography using Elliptic Curve cryptography with Optimization Techniques.*

This final scheme is used to protecting the image-based secrets that has a computation-free decoding process. In this method, a number of shares have been generated from secret image. From the secret image the separate matrix is created for the RGB by using their pixel values (P_v). From those pixel values, shares are created by using the sharing process of the visual cryptography.

In the share creation process each share is separately created by utilizing the new Visual Secret Share (VSS) creation procedure to improve the performance of the images. Multiple Shares are divided into blocks for the security purpose of the images utilized the ECC method.

The key generation for the encryption process includes the ECC multiplication process Point addition and Point doubling utilized to generate the public key. Decryption process employs the optimization technique for the private key generation of the ECC method. For improving the performance of the cryptographic image in the ECC method, different optimization techniques are used such as the Cuckoo Search (CS), Ant Colony Optimization (ACO), Particle Swarm Optimization (PSO) and Grey Wolf Optimization (GWO) for the private key generation by the ECC method. Figure 3 shows the block diagram of the proposed visual cryptography scheme III.

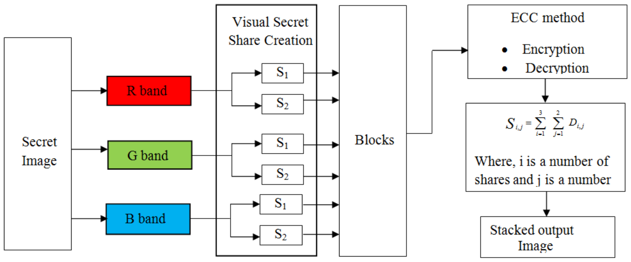
Secret Image
R band
G band
B band
Visual Secret Share Creation
S1
S2
S1
S2
S1
S2
Blocks
ECC method
• Encryption
• Decryption
$S_{i,j}=\sum_{i=1}^{3}\sum_{j=1}^{2}D_{i,j}$
Where, i is a number of shares and j is a number
Stacked output Image

Fig. 3 Scheme III: Block diagram of Visual Secrets Share Creation

The performance of the image is taken as the fitness value for the optimization process such as the PSNR and correlation coefficient CC value. After the decryption process, finally the output image is compared with the original image for evaluating their performance by using the PSNR value; Mean by the optimization technique and for evaluating the performance of the optimization the PSNR, MSE and CC. The private key (H) is generated CC are used.

From the test results, it is revealed that the PSNR is 69.568, the MSE is 0.013 and the CC is 0.992 for the decrypted image without any distortion of the original image and the optimal PSNR value is attained in the Grey Wolf Optimization (GWO) algorithm. By using this scheme, the original image is shared securely and its information is maintained with confidentiality.

III. PERFORMANCE ANALYSIS

A. *Performance metrics*

1) Peak Signal to Noise Ratio (PSNR): The peak signal to noise ratio is defined as the ratio between the maximum possible power of the signal and the power of corrupted noise.

$$PSNR=\frac{1}{N}(R_{PSNR}+G_{PSNR}+B_{PSNR}) \quad (1)$$

Where N is the number of bands

$$R_{PSNR}=\frac{1}{s}\sum_{i=1}^{s}20\times\log_{10}\left(\frac{255^2}{MSE_i}\right) \quad (2)$$

$$G_{PSNR}=\frac{1}{s}\sum_{i=1}^{s}20\times\log_{10}\left(\frac{255^2}{MSE_i}\right) \quad (3)$$

$$B_{PSNR}=\frac{1}{s}\sum_{i=1}^{s}20\times\log_{10}\left(\frac{255^2}{MSE_i}\right) \quad (4)$$

Where S is the number of shares (i=1,2,..4) and MSE is the mean square error.

2) Mean Square Error (MSE): The Mean Square Error is the average square of the error in particular images and the following equation is

$$MSE=\frac{1}{N}(R_{MSE}+G_{MSE}+B_{MSE}) \quad (5)$$

$$R_{MSE}=\frac{1}{s}\sum_{i=1}^{s}\left(\frac{1}{w*l}(\sum_{k=1}^{x}\sum_{j=1}^{y}(A_{kj}-E_{kj})^2)\right) \quad (6)$$

$$G_{MSE}=\frac{1}{s}\sum_{i=1}^{s}\left(\frac{1}{w*l}(\sum_{k=1}^{x}\sum_{j=1}^{y}(A_{kj}-E_{kj})^2)\right) \quad (7)$$

$$B_{MSE}=\frac{1}{s}\sum_{i=1}^{s}\left(\frac{1}{w*l}(\sum_{k=1}^{x}\sum_{j=1}^{y}(A_{kj}-E_{kj})^2)\right) \quad (8)$$

where, w and l is the width and length of the original image, x and y is the row and column value of the pixel, A is the original image pixel and E is the decrypted image pixel value. This equation is depending upon obtained MSE value for each shares of each band.

3) Correlation Coefficient (CC) Factor : To analyse the correlation involving two adjacent pixels throughout plain-image as well as ciphered image, this process has been executed. Compute the correlation coefficient of each one set through the subsequent equations,

$$W(x,y) = \frac{CON(x,y)}{\sqrt{M(x) * M(y)}} \qquad (9)$$

Where

$$CON(x,y) = \frac{1}{F_x} \sum_{l=1}^{F_x} ((x_l - M(x)) * (y_l - M(y))) \qquad (10)$$

$$M(x) = \frac{1}{F_x} \sum_{l=1}^{F_x} x_l \qquad (11)$$

$$M(y) = \frac{1}{F_y} \sum_{l=1}^{F_y} (y_l - M(x))^2 \qquad (12)$$

where, W(p, q) is the correlation coefficient, M(x) and M (y) are the mean value of the x_l and y_l are the two adjacent pixel values; F_x is the number of pairs (x, y). This equation is based obtained CC in each share.

B. *Scheme I : Performance Evaluation*

The proposed scheme I with their PSNR, MSE and CC values are shown in Table 1.

TABLE I
SCHEME I: VALUES OF PSNR, MSE AND CC TESTS OF VARIOUS IMAGES

Original image	PSNR	MSE	CC
Lena	58.00	0.103	1
House	57.42	0.117	1
Peppers	56.68	0.145	1
Baboon	58.14	0.099	1

Through images, the proposed strategy is connected with the image and output images are indicated by their PSNR values. The PSNR value indicates the nature of the image to the output image after the proposed technique connected with it. Here, the PSNR qualities are 58.0025, 57.4297, 56.684 and 58.1438. Also the MSE values and CC values are shown in Table 2. From the MSE values, it gives the original image and decrypted image differences and it should be minimum for any images. Here, the MSE values are nearly 0.1 and it gives the original image is retained in decrypted image after the proposed part.

C. *Scheme II : Performance Evaluation*

The proposed scheme II with their PSNR, MSE and CC values are shown in table 2.

TABLE II
SCHEME II: VALUES OF PSNR, MSE AND CC TESTS OF VARIOUS IMAGES

Original image	PSNR	MSE	CC
Lena	65.73	0.017	1
House	64.93	0.020	1
Peppers	65.75	0.017	1
Baboon	65.71	0.017	1

The PSNR value indicates the nature of the image to the output image after the proposed technique connected with it. Here, the PSNR qualities are 65.73, 64.93, 65.75 and 65.71. Also the MSE values and CC values are shown in table 2. From the MSE values, it gives the original image and decrypted image differences and it should be minimum for any images. Here, the MSE values are nearly 1 and it gives the original image is retained in decrypted image after the proposed part.

D. *Scheme III : Performance Evaluation*

The proposed scheme III with their PSNR, MSE and CC values are shown in table 3.

TABLE III
SCHEME III: VALUES OF PSNR, MSE AND CC TESTS OF VARIOUS IMAGES

Original image	PSNR	MSE	CC
Lena	68.957	0.010	1
House	69.917	0.006	1
Peppers	67.194	0.031	1
Baboon	71.599	0.005	1

Table 3 explains that the different images with the presentation assessment parameters such as PSNR, MSE and CC for the suggested work. For the ECC strategy the intended system encloses the many share creation, encryption, and decoding technique. Through images, by their PSNR values the suggested approach is linked with the image and output images are pointed out. Here, the PSNR qualities are 68.957, 69.917, 67.194 and 71.599. Also the MSE values and CC values are shown in table 2. From the MSE values, it gives the original image and decrypted image differences and it should be minimum for any images. Here, the MSE values are nearly 1 and it gives the original image is retained in decrypted image after the proposed part.

IV. COMPARATIVE ANALYSIS

Different optimization techniques such as Grey Wolf Optimization (GWO), Ant Colony Optimization (ACO), Particle Swarm Optimization (PSO) and Cuckoo Search (CS) are used to the find the private key in scheme II and III. The fitness estimation of this process is maximum values of PSNR and CC attained in GWO algorithm. The average PSNR value of the all images in GWO algorithm is 69.56. It is contrasted to the PSNR value of the other optimization technique is 9.238% minimized. When comparing MSE value of GWO with ACO the error variation is 5.4% for all images. Therefore, GWO is better than other optimization techniques based on performance study factor.

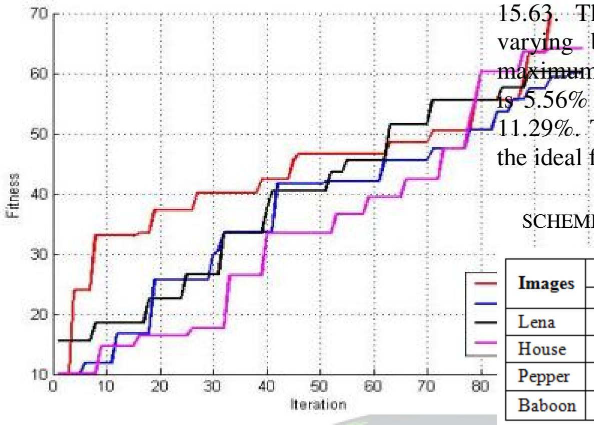

Fig. 4 Convergence Graph

Figure 4 shows that the convergence graph is plotted between the iteration and fitness estimations of the various strategies for GWO, PSO, ACO and CS. This graph basically resolves that the GWO procedure is given the greatest fitness using least possible iteration. Through the graph, the GWO strategy takes the minimum iteration for providing the ideal result. Subsequently, it is maximized to 69.45 and it's attained in 94 iterations. Initial iteration the fitness value of GWO is 22.36 and other techniques also the initial fitness value is 15.63. Then the iteration is varied the performance also varying based on the procedure of the techniques. The maximum fitness of GWO compared to the CS the difference is 5.56% similarly the other algorithm also the difference is 11.29%. Through the graph, the GWO strategy just specifies the ideal fitness value with the efficient results.

TABLE IV

SCHEME III: VALUES OF PSNR, MSE AND CC TESTS OF VARIOUS IMAGES

Images	**VC-ECC-GWO**			**VC-ECC-CS**			**VC-ECC**		
	PSNR	**MSE**	**CC**	**PSNR**	**MSE**	**CC**	**PSNR**	**MSE**	**CC**
Lena	68.957	0.010	1	65.73	0.017	1	58.00	0.103	1
House	69.917	0.006	1	64.93	0.020	1	57.42	0.117	1
Pepper	67.194	0.031	1	65.75	0.017	1	56.68	0.145	1
Baboon	71.599	0.005	1	65.71	0.017	1	58.14	0.099	1

Table 4 shows that the comparison of all the three proposed schemes based on PSNR, MSE and CC. It describes PSNR value is maximum for the proposed visual secret share with GWO process comparing the existing process. All the four images of the PSNR value 11.85% of Scheme I and 6.541% of Scheme II increased with scheme III. Graph in Figure 5 shows that the performance comparison of the all the proposed schemes.

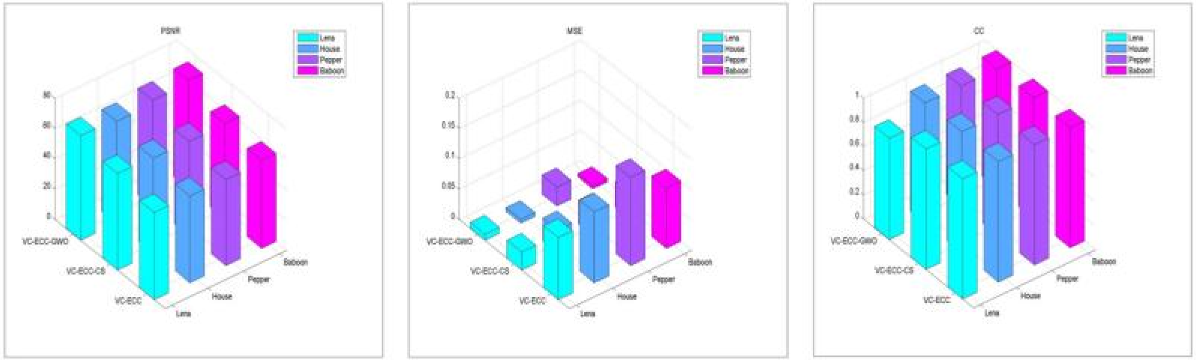

Fig. 5 Comparison between optimization techniques in different images for proposed Schemes

V. CONCLUSIONS

In the ground-breaking technique, the multiple shares with the elliptical cryptography for visual cryptography have been found to usher in superlative performance. A plethora of illogical-shares are generated which are effectively encrypted and decrypted by means of the encryption and decryption technique in line with the ECC. The proposed secure share creation schemes are clearly show that the PSNR values of the secret different images are 68.95, 69.917, 67.174 and 71.599. , MSE value is minimized in all images is 0.010, 0.006, 0.03 and 0.005 and then the correlation coefficient value is the almost in all the images are nearly 0.999 is attained in the Scheme III (VC_ECC_GWO). The proposed schemes have made it clear that the encryption technique was performed on the secret image so as to preserve the confidentiality of the image. In Future, the performance of the secret image will increase with help of other method instead of ECC and also PSNR value will be improved as well as minimizing its MSE value.

REFERENCES

[1] Young-Chang Hou, "Visual cryptography for color images", Journal of Pattern Recognition, Vol.36, pp.1619 – 1629, 2003.

[2] Naor, Moni, and Adi Shamir. "Visual cryptography." Advances in Cryptology—EUROCRYPT'94. Springer Berlin/Heidelberg, 1995.

[3] Abhishek Parakh and Subhash Kak, "A Recursive Threshold Visual Cryptography Scheme", arXiv preprint arXiv,pp.1-8,2009.

[4] Chih-Hung Lin, Yao-Sheng Lee and Tzung-Her Chen, “Friendly progressive random-grid-based visual secret sharing with adaptive contrast”, Journal of Visual Communication and Image Representation, Vol.33, pp.31-41,2015.

[5] Woei-Jiunn Tsaur, “Several security schemes constructed using ECC-based self-certified public key cryptosystems”, Journal of Applied Mathematics and Computation, Vol.168, pp.447–464,2005.

[6] HankMenVan, Darrel Hankerson, Alfred Menezes, Scott Vanstone, “Guide to Elliptic Curve Cryptography”, Springer ISBN 0- 387-95273-X, 2004.

[7] https://en.wikipedia.org/wiki/Mathematical_optimization#Computational_optimization_techniques.

[8] Durga Bhavani and Soundarya Mala, “Optimized Elliptic Curve Cryptography”, Journal of Engineering Research and Applications,Vol.2, No.5, pp.412-419,2012.

[9] Al-Daoud, R, mahmod, Md. Rushdan, A. Kilicman , “A new addition formula for Elliptic curve over GF (2n)”, IEEE Transactions on Computers, vol. 51, no. 8, pp. 972-975,2002.

[10] K.Shankar and P.Eswaran. “An Efficient Image Encryption Technique Based on Optimized Key Generation in ECC Using Genetic Algorithm”, Advances in Intelligent Systems and Computing, Springer, Vol. 394, pp.705-714, 2016.

[11] K.Shankar and P.Eswaran. “A Secure Visual Secret Share (VSS) Creation Scheme in Visual Cryptography using Elliptic Curve Cryptography with Optimization Technique”. Australian Journal of Basic and Applied Sciences. 9(36): 150-163, 2015.

[12] K.Shankar and P.Eswaran. “ECC Based Image Encryption Scheme with aid of Optimization Technique using Differential Evolution Algorithm”, International Journal of Applied Engineering Research, Vol.10, No.5, pp. 1841–184, 2015.