Randomized Slice Based Image Cryptography Using With Rotational Encryption Framework

[1] SANJAPURI ESWAR RAJ, [2] Dr. O. SRINIVASA RAO

[1] M.TECH SCHOLAR, [2] PROFESSOR

Department of Computer Science & Engineering,

University College of Engineering (A), JNTUK-Kakinada, Andhra Pradesh, India

Abstract: (VC)Visual cryptography is an approach for pretending the image based secrets which has the technique of computational free decoding process. The secret image is first converted into threshold based parts with random prototypes with VC. There is a possibility to change the secret image apparently with superimposing a approved subset of transparencies. The main goal of this proposed work is to monitor the various different types of data hacking on the data/information and handle them with proper type named measures. Moreover the optimization of the countering method by proposed work. This is used to broadcast the original image from source to other end(receiver) with more confidentiality. In this work , three methods proposed for enhancement of the efficiency of the VC. With the first one RGB based share with multiple slots creation in the VC with respect to ECC techniques are suggested. The result outcomes that allowed certainly that Peak Signal Noise Ratio is 58.0028 , with Mean Squared Error(MSE) outcome is 0.1164 and CC(correlation coefficient) is near to 1. With the second approach sharing creation with security scheme in VC with respect to ECC with optimized scheme for the images with color is proposed. From the results of this approach, the outcome has revealed with PSNR is 65.7307 , MSE with -.-17367 and CC is 1, the optimized PSNR value is obtained in the CS(cuckoo Search) model. With the third approach, an innovative model of VSS(Visual secret share) used to improve the efficient of VC with ECC is the proposed one. The main outcome of this approach is PSNR is 69.568 , MSE is 0.013 and the CC is 0.992 and feasible PSNR value is obtained with GWO(grey wolf optimization. This work implemented with the performance evaluation and to compare the given mensioned secured shared created models.

***Index Terms* -** Shares, Encryption , ECC , visual cryptography, Image Cuckoo search model, Grey wolf optimization approach

I. INTRODUCTION

With increase the usage of the digital media, there must be the concreate mechanism such as information sharing with security is mandatory. There are main source of the media’s incremental extension can be linked up with the wealth of information revealed by the internet. VC process the technology of encrypting with time based and honored cryptography which are employed generally with extensive shelter data safety [1]. The employment of the cryptography approach is data integrating of a general methods. in this consideration, credit goes to Eshwar for developing as well as acclaimed method for special sharing which is known by the name cryptography approach [2]. The major role of the visual cryptography scheme is to encrypt the confidential (private) image by the help of threshold based splitting. The secrete message cannot be reveal by the help of some threshold and random split images. The original image needs all split images to be exposed. This is a popular flow in visual cryptography. The process of visual cryptography is to split an image into assigned mode or arranged number of parts and then without any mathematical flow or algorithm the secret image can reveal by aligning and align together [3].

Visual cryptography sharing (VCS) has various sectors in the academe and increasing the number of VCS approaches .they are image encryption, visual improved the authentication, image hiding and digital model of water marking visual cryptography in 1994. In visual cryptography is the main need to encrypt the image by using of model of encryption algorithm but for revealing the image, there does not need any approaches. The main challenge is to controll a number of un desired shares because all splits must need for various secrets to exploit. Therefore it is tedious to control and use [4]. ECC is a public/shared key cryptography, which is related to the mathematical model of elliptic curves with limited attributes. With the differentiation of ECC requires tiny keys than non-ECC cryptography to provide overall protection. Public key cryptosystem is the primary of all modern encryption or digital signal approaches where one key is decryption model key or signature generation key and the other one is cipher text makeup key or signature verification key [5].

The number factorization issue of RSA and (DLP) Digital Light Processing was resolved this approach in an aggressive manner, which have the predictable process of execution time. The Elliptic curve digital light processing (ECDLP) was resolved by a known fastest approach which have exponential predictable running time [6]. Basically,, the feasible theory and approaches are widely used in the field of applied mathematics The feasible method also includes finding the best accessed value of target model from a defined domain or variety of target methods from various and different type of domain [7].The main purpose of the feasibility/optimization is used to decrease the interval of a point multiplication depend on the number of required iteration. Moreover, the replicated arithmetic obstructs are used to increase the parallelism for basic process. Though most of the executions are take place on process optimization or improved arithmetic architectures or sometimes the processor dashboard also suitable for ECC point multiplication [8].

Another main advantage of elliptic curve cryptosystem is that to create ECC more attractive for the arithmetic methods in the basic applications [9]. Different type of feasible methods can be used in ECC and the private key feasibility. In ECC technique, for making the process of the cryptographic image several feasible approaches are used. Such as , Cuckoo search (CS) algorithm, genetic algorithm (GA), Differential evaluation (DE) algorithm, Particle Swarm Optimization (PSO) ,Ant Colony Optimization (ACO) and Gray Wolf Optimization (GWO) for the private key generation [10][11][12].

II. **RELATED WORK**

Related works about visual cryptography for grayscale images are seldom discussed. Verheul and van Tilborg (1997) described a basic and general method for(***k* - *n***)nÞ-threshold visual encryption of gray scale level images. We review their approach briefly mentioned here. For an image with c gray scale levels, expand first a pixel into b subpixels. Each subpixel may take one among gray levels of 0; 1, . . . ; c - 1. After all shares are done with stacked, gray level i is expells if relevant subpixels of all shares are of gray scale level i; else , the level of ‘‘black’’ (with the smallest gray scale level value) is exploited. As an illustration, our describes an example for the case of a (3,3)-threshold based scheme. If there are three level gray levels, we built three collections of matrices belonging to gray levels 0, 1, 2, respectively, in the following:

C0 = {all the matrices obtained by permuting the columns of A0},
C1 = {all the matrices obtained by permuting the columns of A1},
C2 = {all the matrices obtained by permuting the columns of A2},

where

$$A_0 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \end{pmatrix}$$

$$A_1 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 2 & 0 & 1 & 0 & 1 & 2 & 1 & 2 & 0 \end{pmatrix}$$

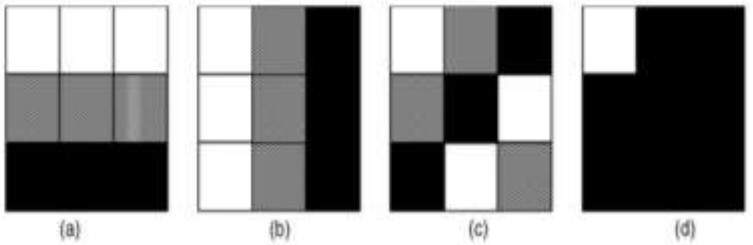

Figure0: The shared and decoded pixel with grayscale level0 of the example (3,3) visual cryptography
a) visual pattern of share1 b) visual pattern of share2 c) visual pattern of share3
d) decoding pixel result with gray scale 0.

And

$$A_2 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 1 & 2 & 0 & 2 & 0 & 1 & 0 & 1 & 2 \end{pmatrix}$$

To encrypt an image pixel of gray-level 0, we take input as share1to be the first row of a matrix R0 randomly chosen in C0 share2 the second row of R0 and share3 the third row of R0 The visual framed patterns of the shares and their stacking result are depicted in Fig. 0. We can see in the subsequent result that the subpixel of all these three shares at the top left corner is of gray scale level 0 that is the original graylevel value of the encoded pixel, while the graylevel ‘‘black’’ viusals in the other parts. The encryption results of the other two gray levels can be acheieved with similarly It is easy to see that this scheme yields decoded images with expanded sizes. More precisely, after encrypting an image with c gray levels using the (***k***-***n***)-threshold visual cryptography scheme proposed in (Verheul and van Tilborg, 1997), the size increase as derived in (Verheul and van Tilborg, 1997) is with a factor c power k-1 at least when c >= n.

III. Proposed approaches:

1. A Secure multi share creation model in VCC with assistance :

In this apporach, the pixel values (Pv) of the colored image (RGB image) are extracted from the main/original image and indicated as matrix (P*Q). The extracted pixels values as matrix representation are used to make the more shares (share1, share2…share n) and the shares are divided into multiple blocks. The blocks of the shares/splits are encrypted by using the ECC approach and the encrypted image is decrypted by using the decryption of the ECC approach. Figure 1 shows the main block diagram of the worked out visual cryptography scheme I.

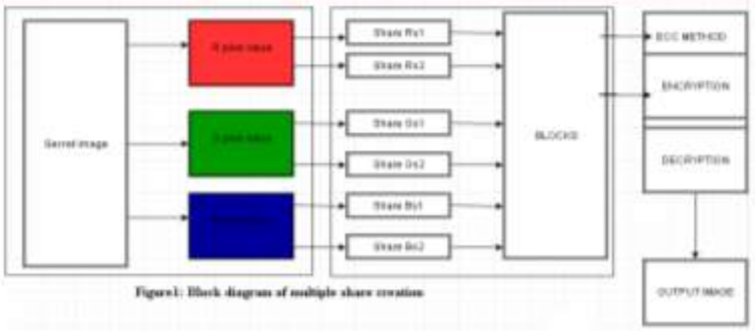

Figure1: Block diagram of multiple share creation

Finally the outcome image is compared with the main image for evaluation their performance by using the PSNR, MSE and CC outcomes. It is clear that the PSNR values are 58.0025, 57.4297, 56.684 and 58.1438 the image smartens is stored in spite of adhoc made on the secret image. The (CC)correlation coefficient value is the nearly all the images are mostly 1 and the MSE is the 0.103, 0.1176, 0.1454 and 0.0997. From that, the main image quality is not evaluated and it is back to normal position by using the proposed approach. The CC estimations have made it fair that the encryption approach is performed on the secret image so as to store the secretly of the image. Thus the confidentiality of the image is upheld with the more runs and the retained image is offered the variant image without in any way adversely influencing the main quality of the image.

2. A Secure/secret Multiple Share Creation model in Visual Cryptography using Elliptic Curve cryptography with feasible Technique

The proposed approach is utilized to broadcast an original image from the source to the destinations with confidential and secret. From the main/original image, the pixel values (Pv) are extracted and they will be created with an RGB pixel matrix. The proposed approach is used to create the shares from their pixel values(in the form of matrix). The extracted pixel values are used to make the multiple shares (share1, share2…share n) and the splits/shares. The multiple shares/splits created for the secure image broadcast and to maintain the image information with confidentiality, and then the image shares are divided into blocks/splits. The blocks of the each split 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 main block diagram of the proposed visual cryptography scheme 2.

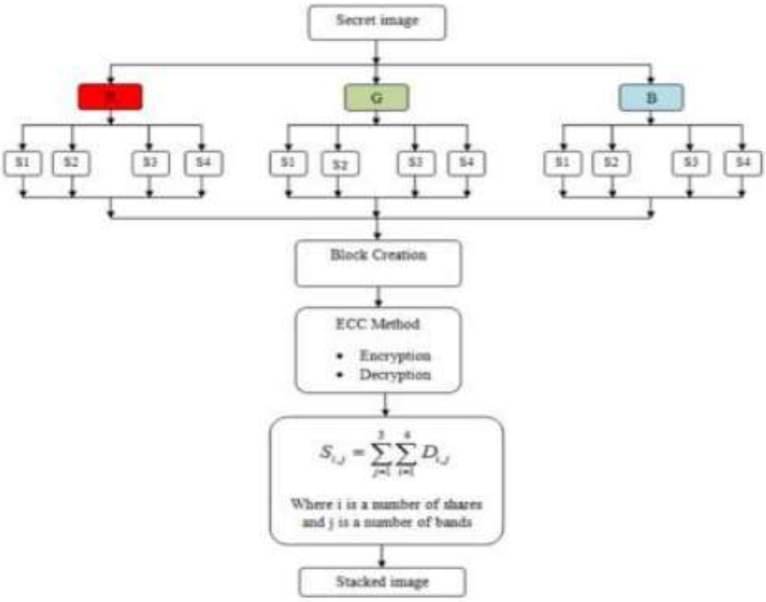
Secret image
R
G
B
S1
S2
S3
S4
S1
S2
S3
S4
S1
S2
S3
S4
Block Creation
ECC Method
• Encryption
• Decryption
$S_{i,j} = \sum_{j=1}^{3}\sum_{i=1}^{4} D_{i,j}$
Where i is a number of shares and j is a number of bands
Stacked image

Figure2: Block diagram of multiple share creation

In encryption approach, the public key randomly created and the decryption approach employs the optimization approach for the private key generated of the ECC application. For enhancing the performance of the cryptographic image in ECC approach, different feasible technique is used such as Genetic Algorithm (GA), Cuckoo search (CS) algorithm, and Differential Evaluation (DE) algorithm. The improvement of the image is taken as a fitness value for the feasible process such as PSNR value which is shown the difference between the original image and CC value. It is crystal and clear that the PSNR values of the secret different images are 65.73057, 65.7167, 64.9333, and 65.7563. The MSE value is reduced in all images is 0.0107, 0.0107, 0.0209 and 0.0172 then the inter relation/ correlation coefficient value is the almost all the images are nearly1.

3. A Secure Visual Secret Share (VSS) Creation approach in Visual Cryptography using Elliptic Curve cryptography with feasible Techniques.

This final approach is used to block the image based secrets that has a mathematical computaion-free decoding process. In this approach, a number of shares/splits have been made from secret image. From the secret image the with individual matrix is created for the RGB by using their relevant pixel values (Pv). From those matrix based pixel values, shares are created by using the sharing approach of the visual cryptography. In the share/split creation process each share is individually created by utilizing the new Visual Secret Share (VSS) making procedure to increase the performance of the images. Various Shares are splits into blocks for the security purpose of the images utilized the ECC approach. The key making for the encryption process includes the ECC multiplication process addition of and doubling of point utilized to generate the public key. Decryption process

employs the feasible technique for the private key generation of the ECC approach. For increasing the performance of the cryptographic image in the ECC method, various optimization approaches are used such as the Ant Colony Optimization (ACO), Particle Swarm Optimization (PSO) ,Cuckoo Search (CS) and Grey Wolf Optimization (GWO) for the private key generation by the ECC method.

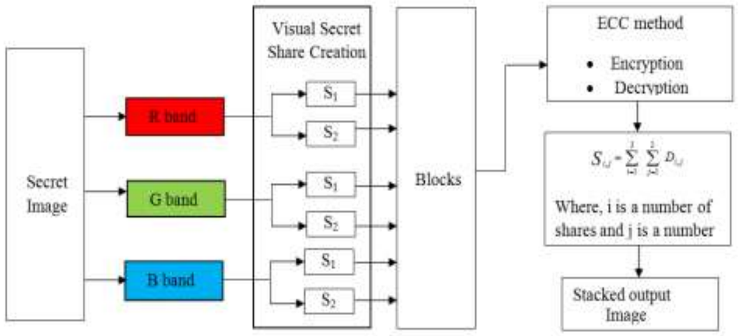

Figure 3: shows the block diagram of the proposed visual cryptography approach 3

The performance of the image is taken as the fitness value for the feasible process such as the PSNR and correlation coefficient CC value. Post process of the decryption process, finally the output image is compared with the main/original image for performance evaluation by using the PSNR value; Mean by the feasible technique and for evaluation of the performance of the optimization the PSNR, MSE and CC. The private key (H) is generated CC are utilized . From the test results, it is exposed that the PSNR is 69.568, the MSE is 0.013 and the CC is 0.992 for the decrypted image without any distorted of the original image and the optimal PSNR value is attained in the (GWO)Grey Wolf Optimization approach. By using this approach, the original image is shared securely and its information is maintained with confidentiality.

IV. Performance analysis:

Process1:

1. **PSNR(Peak signal noise ratio):** 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 = 1/N(RPSNR + GPSNR + BPSNR) (1)
Where N is the band count;
$R_{PSNR} = 1/S\sum^{S}_{I=0} 20\times\log_{10}(255^2 / MSE_i)$ (2)
$G_{PSNR} = 1/S\sum^{S}_{I=0} 20\times\log_{10}(255^2 / MSE_i)$ (3)
$B_{PSNR} = 1/S\sum^{S}_{i=0} 20\times\log_{10}(255^2 / MSE_i)$ (4)

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

2. **MSE(Mean Square Error)**

The means square error is the average error in specific images and following equation is

$MSE = 1/N(R_{MSE} + G_{MSE} + B_{MSE})$
$R_{MSE} = 1/S\sum^{S}_{i=l} (1/w*L(\sum^{x}_{kml} \sum^{y}_{jml}(A_{KJ} - E_{KJ})^2))$
$G_{MSE} = 1/S\sum^{S}_{I=1}(1/W*L(\sum^{X}_{K=0} \sum^{y}_{J=0}(A_{KJ} - E_{KJ})^2)$
$B_{MSE} = 1/S\sum^{S}_{I=1}(1/W*L(\sum^{X}_{K=0} \sum^{y}_{J=0}(A_{KJ} - E_{KJ})^2)$

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

3. **(CC)Correlation factor:**

To analyze the correlation involving two neighboring pixels throughout plain mage as well as ciphered image, this process has been executed. Mathematical process the correlation coefficient of each one set through the preceding equations,

$W(x,y) = con(x, Y)\sqrt{m(x) * m(y)}$

Where

$con(x, Y) = 1/F_X \sum_{lm1}((X_1 = M(x))*(Y_1 - M(y)))$
$M(x) = 1/F_x \sum^{fx}_{i=1} X_1$
$M(y)=1/F_y \sum^{fy}_{l=1}(y_1-m(x))^2$

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

Process2: Performance analysis

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

Table 1: 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 this work's strategy is connected with the image and output images are represented by their PSNR values. The PSNR value denotes the nature of the image to the output image after the proposed method 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 partition.

Process 3 : Performance analysis

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

Table 2: 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 denotes the nature of the image to the output image after the improved 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 variations 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 partition.

Process4 : Performance analysis

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

Table 3: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 partition.

V. **Conclusion**:

Different feasible 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.

VI. 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#Computation al_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.