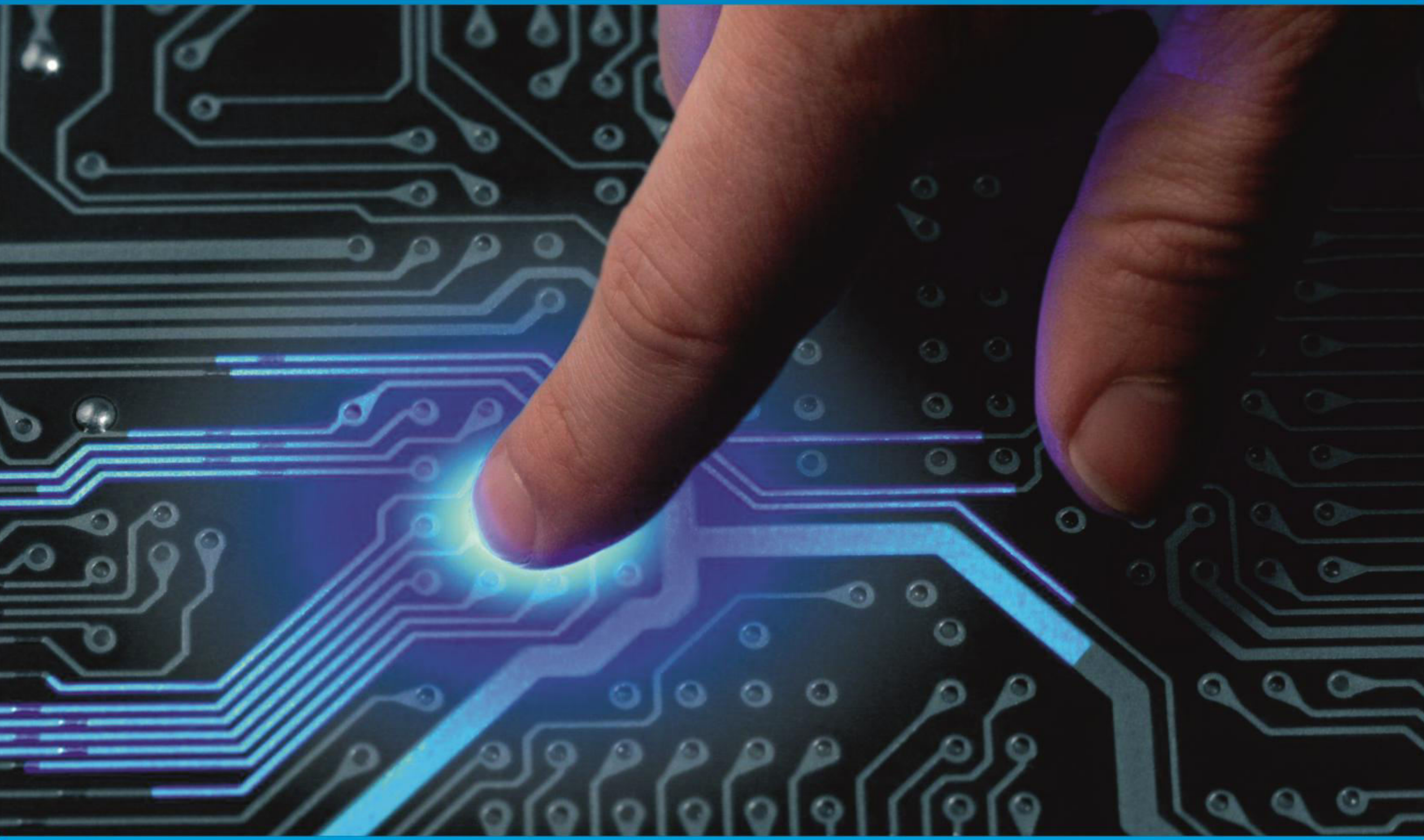
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 4, April 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904129 |

Modified Image Encryption System Using Elliptic Curve Cryptography

M.Thangavel [1], Sanjay Raj M[2], Vigneshkumar D[3], Siddharth A[4]

Assistant Professor, Department of Electronics and Communication Engineering, VSB Engineering College, Tamilnadu, India[1]

U.G Student, Department of Electronics and Communication Engineering, VSB Engineering College, Tamilnadu, India[2,3,4,],

ABSTRACT: Picture encryption is quickly expanded as of late by the expanding utilize of the web and communication media. Sharing imperative pictures over unsecured channels is obligated for assaulting and stealing. Encryption methods are the appropriate strategies to ensure pictures from assaults. Slope cipher algorithm is one of the symmetric methods, it features a basic structure and fast computations, but weak security since sender and collector have to be utilize and share the same private key inside a non-secure channels. A unused picture encryption procedure that combines Elliptic Curve Cryptosystem with Slope Cipher (ECCHC) has been proposed in this paper to change over Slope Cipher from symmetric strategy to asymmetric one and increment its security and proficiency and resist the programmers. Self-invertible key framework is used to generate encryption and unscrambling mystery key. So, no have to be discover the converse key framework within the decryption process. A mystery key network with measurements 4 × 4 will be utilized as an case in this study.Entropy, PSNR, and MSEare analyzed to survey the grayscale picture encryption proficiency and compare the scrambled picture with the first picture to evaluate the execution of the proposed encryption procedure.

KEYWORDS: ECC, Entropy, PSNR,MSE, ECCHC

I. INTRODUCTION

Cryptography is one of the scientific procedures that are utilized to ensure pictures from foes and increase the security of communications. Encryption is done by the sender to change over the first grayscale image to scrambled picture some time recently sending it through the web to the other client (beneficiary). Decoding is done by the recipient to return the ciphered picture back to the first picture. Symmetric (private key) and asymmetric (open key) encryption procedures are two bunches of cryptography. In symmetric encryption, the same key (private key) is utilized for both encryption and decoding forms, though in asymmetric encryption the sender employments a private key diverse than the receiver's private key and each party generates the open and mystery key independently after concurring on the elliptic bend space parameters [1] [2]. Both sender and recipient are trading their open keys, which are not mystery by utilizing Elliptic Bend DiffieHellman technique (1976).

Elliptic bend cryptography (ECC) is one of the compelling open key cryptography procedures, it proposed independently by Mill operator [4] and Koblitz [5]. The hardness of fathoming the Elliptic Bend Discrete Logarithm Issue (ECDLP) from the foes is one of the ECC advantages. ECC works on a little key estimate with a small sum of memory and moo control compared to other systems like RSA [6][7][8][9]. Slope cipher calculation is one of the symmetric methods; it has tall throughput, high speed, and straightforward structure, but frail security since both sender and collector ought to utilize and share the same key (private key) through unsecured channels [10][11].

A part of analysts attempted to create Slope Cipher strategy and make strides its security. Ismail, et al. (2006) proposed a modern Slope cipher (HillMRIV) that altering the encryption key and employing a distinctive key for each plaintext piece rather than utilizing one key network for all squares and increasing the security of Slope algorithm, but it contains a downside when the plaintext piece contains as it were zeroes [12]. Bibhudendra, et al. (2009) solved the unscrambling issue in case the converse key network that does not exist by proposing a novel progressed Hill algorithm (AdvHill) that employments the same involutory key framework for encryption and unscrambling and eliminates the computations required by the beneficiary to discover the converse key matrix, additionally expanded the cipher randomization which expanded the effectiveness of the calculation compared with the initial Slope cipher [11]. Hamissa, et al.

(2011) upgraded the first Slope cipher calculation security by utilizing calculated outline chaotic functions and proposing a unused encoder-decoder procedure (ChaoEncoDeco) for pictures encryption [13]. Panduranga, et al. (2012) presented an approach that comprises of three stages counting Slope cipher to improve the entropy of the scrambled picture. Firstly, each pixel esteem in two input pictures is changed over to eight double bits and k bits are pivoted and switched. Following, the lower snack of the pixels of the pictures are exchanged. At long last, Slope cipher calculation is executed on the pixel values [14]. Nordin, et al. (2013) proposed a modern Slope calculation (Slope++) that computed a arbitrary framework key based on the past blocks as an additional key for encryption and stood up to all zeroes plaintext squares, it combined Slope cipher with the affine cipher and delivered an calculation that expanded assault resistance [15].

Agrawal& Gera (2014) produced a modern strategy for encryption by utilizing Slope cipher calculation to begin with to deliver the ciphertext numerical values, and after that change over it to focuses on the ECC by utilizing scalar increase. This method increased the security but too expanded the time of computations since scalar duplication devoured a long time [16]. Sharma &Chirgaiya (2014) proposed a strategy to fathom the Slope cipher decryption problem if the key framework isn't invertible, they recommended utilizing setting balanced esteem one in case the determinant of a matrix is zero and counterbalanced esteem -1 in case the determinant is negative [17].

Mahmoud &Chefranov (2014) proposed an viable alteration for the Slope cipher (HCM-PRE) that stands up to known plaintext-ciphertext attack by utilizing pseudo-random eigenvalues and changing key lattice for each square powerfully to make the proposed method quicker than other alterations [18]. Rajput &Gulve (2014) proposed a framework that consists of three stages; the primary organize partitions the picture into n squares, at that point performs XOR between blocks, the pixel esteem of the picture is converted into 8-bit twofold within the moment organize, and within the final arrange the image is scrambled by utilizing the expanded slope cipher [19].

A unused encryption strategy has been proposed in this paper to combine Elliptic Bend Cryptosystem (ECC) with Slope Cipher (HC) method to reinforce the security and create a modern approach (ECCHC) comparable in rule to the work proposed in [20]. The modern approach employments ECC to create the private and public keys, and after that both sender and recipient have the capacity to create the mystery key with no require to share it through the web or unsecured communication channel. One of the most downsides in Hill cipher calculation is that the converse of the key network does not continuously exist.So, on the off chance that the key lattice is not invertible, the decoding prepare cannot be done, and the recipient cannot get the first information. This paper avoids this issue by utilizing the self-invertible key lattice (the key framework is self-invertible on the off chance that =) which decreases the computational handle needs amid the unscrambling prepare to compute key matrix inverse [21]. Both sender and recipient build the self-invertible key lattice and utilize it for encryption and decryption with no have to be create the converse of the key lattice. The modern strategy will be implemented and tried on the grayscale pictures.

The effectiveness and execution of the modern strategy will be assessed by utilizing a few security measures like Entropy, PSNR, and MSE. It is simulated in MatLab 2013a with core i3 processor.The rest of this paper is organized as takes after. A presentation to elliptic bend work is displayed in Section 2. Segment 3 depicts the first Slope Cipher calculation. Area 4 clarifies the proposed hybrid encryption approach. An execution case of the proposed approach is given in Segment 5. Security Analysis for a few measures is clarified in Area 6. At last, the conclusion and the focal points of the proposed approach are appeared in Section 7.

1. ELLIPTIC CURVE FUNCTION AND HILL CIPHER

We use Elliptic curve function to generate key using public key cryptography. A finite field is defined and private key, generator point is randomly chosen in that finite field. Generation of key is given in proposed system. After key generation, Encryption and Decryption are done using Hill Cipher. Mathematically expression for encryption and decryption for Hill Cipher technique is given below.

$C=MK \bmod 256$

$M=CK^{-1} \bmod 256$

Where,

C is the cipher image

M is the original image

K, and K^{-1} are Key and inverse of Key respectively.

2. PROPOSED SYSTEM

We have taken color image of size 256x256 and our proposed system is implemented in MatLab. For this color image is represented in matrix format of size 256x256x3. It consists of three components called R, G, B and each are represented with dimensions 256x256. In our proposed system each components are individually encrypted and fused to produce cipher image. In receiver, RGB components are separated again and decrypted individually. Finally all three decrypted RGB components are fused to produce the decrypted image.

The proposed system consists of the following set of procedures.

a. Initializing key parameters
b. Key generation and exchange between sender and receiver
c. Encryption by sender
d. Decryption by receiver

a. Initializing key parameters

We decided to use Elliptic curve cryptography as it has more security and cryptanalysis by attacker is practically impossible. Elliptic curve over a finite field F_z

is considered for key generation. The generator point over the finite field G is shared between sender and receiver.

Mathematical expression of Elliptic curve is as follows.

$$y^2 \equiv x^3 + ax + b \bmod z$$

In order to use the above cryptographic curve for our system, it must satisfy the following condition.

$$4a^3 + 27b^2 \not\equiv 0 \bmod z$$

b. Generating key from sender side

1. Sender selects a private key Pr_s over the field F_z
2. Sender computes public key $Pu_s=Pr_s$. G
3. The public key of sender Pu_s is shared with receiver
4. Computes the primary keyKp= Pr_s. Pu_r= (x,y)
5. Computes the values for matrix. $K_1 = x.G = (k_{11}, k_{12})$ and $K_2 = y.G = (k_{21}, k_{22})$
6. Generates the key matrix $K = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}$

2.1.2 Key generation at receiver

1. Receiver selects a private key Pr_r over the field F_z
2. Sender computes public keyPu$_r$=Pr_r . G
3. The public key of receiverPu$_r$ is shared with sender
4. Computes the primary keyKp= Pr_r. Pu_s= (x,y)
5. Computes the values for matrix. $K_1 = x.G = (k_{11}, k_{12})$ and $K_2 = y.G = (k_{21}, k_{22})$
6. Generates the key matrix $K = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}$

c. Encryption by sender

Once the key is generated, that key is used by sender for encryption. We use Hill cipher to encrypt our color image with the generated key 'K'. Let us assume, M is the matrix which is taken from image pixel values. The pixel values in the matrix M is multiplied with the generated key 'K' to produce cipher. It is explained as follows.

$$[C] = [M][K] \bmod 256$$

Where, [C]is the pixel values of the cipher image. For color image, cipher matrix is obtained for all R, G, B components and it is integrated to produce the cipher image,

d. Decryption by sender

The pixel values in the matrix C is multiplied with the inverse of the key 'K' to produce cipher. It is explained as follows.

$$[D] = [C][K^{-1}] \bmod 256$$

Where,[D]is the pixel values of the decrypted image. For color image, cipher matrix is obtained for all R, G, B components and it is integrated to produce the final decrypted image,

IV. RESULTS AND DISCUSSION

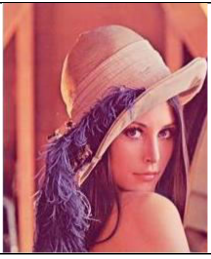
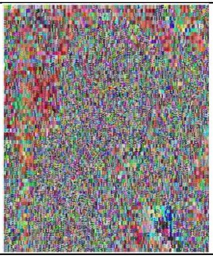
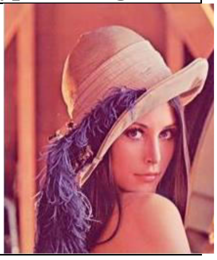
Original Lena Image	Encrypted Image	Decrypted Image
		

Figure 4.1: Original Image, encrypted image, and decrypted image

4.1 Histogram

Histogram of an image is the graphical representation of the tonal distribution of the image which is to be analyzed. The number of pixels for each tonal value is represented in the histogram by plotting the tonal variations versus the number of pixels in that particular tone. It is also used to check the correctness of the image details after image processing.

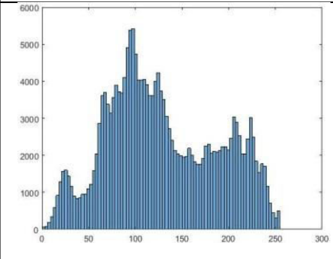
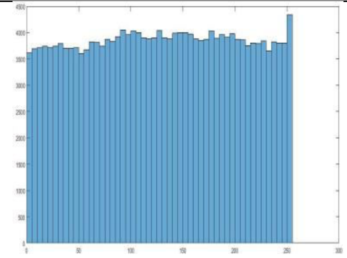
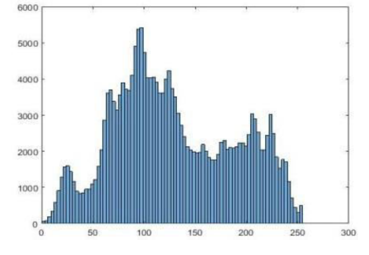
Original Lena Image	Encrypted Image	Decrypted Image
		

Figure3: Histogram of original, encrypted, and decrypted image

4.2 Entropy

Entropy of a cipherimage is defined as the mean amount of information generated at the time of encryption. Theoretically it is proved that entropy value near to 8 achieves a better encryption.Mathematically, entropy of a cipher image is calculated as

$$E = \sum P_i \text{ x } \log_2 P_i$$

Where, $Pi = \frac{Frequency\ of\ the\ pixel\ i}{Total\ number\ of\ image\ pixels}$

Our obtained entropy forcipher image is 7.9986

Entropy	Red channel	Green channel	Blue channel
Proposed	7.9894	7.9924	7.9904
Ref. [1]	7.9886	7.9896	7.9892
Ref. [8]	7.98710	7.98810	7.98780
Ref. [9]	7.98970	7.98770	7.98960

Table2: Entropy for proposed system and comparison

4.3 MSE

MSE stands forMean Square Errorand it is used to measure the difference between the original and cipher image. Mean Square Error of original and cipher images are calculated as

$$\text{MSE}=\frac{1}{n \times n}\sum_{i=1}^{n}\sum_{j=1}^{n}(M_{i,j}-C_{i,j})^2$$

Where, $m \times m$represents the dimension of the image

$M_{i,j}$is the original image

$C_{i,j}$isthe cipher image

The MSE obtained for our system and other comparison is shown in Table 3.

Component	**Red**	**Green**	**Blue**
MSE	10197	8400.2	6518.6

Table3: MSE of proposed system

4.4 Peak Signal to Noise Ratio (PSNR)

PSNR is the parameter related to error and it is evaluated as follows.

$$PSNR = 10\log_{10}\frac{(Max)^2}{MSE}$$

Where, **Max** is the maximum pixel value

MSE is Mean Square Error value obtained in the above section..

PSNR obtained in our system is shown in Table 4.

Component	Red	Green	Blue
PSNR	8.0461	8.8879	9.9892

Table4: PSNR of proposed system

V. CONCLUSION

The proposed system is implemented in three phases namely key generation, encryption, and decryption. Our key is generated using ECC over a finite field. Encryption and decryption are implemented with Hill Cipher. Our proposed work is simulated using Matlab and various parameters are studied. We achieved entropy of 7.9894 for Red channel, 7.9924, and 7.9904 for Green, and Blue channel. It indicates that better result is achieved for the color image. Other parameters are also analyzed like MSE and PSNR. As it is implemented in ECC with Hill cipher, our system is more secured from different attacks.

REFERENCES

[1] Khan, M.K., Zhang, J., and Alghathbar, K., Challengeresponse-basedbiometric image scrambling for secure personalidentification. Futur.Gener.Comput. Syst. 27(4):411–418,2011

[2] Tan, Z., An efficient biometrics-based authentication schemefor telecare medicine information systems. Network 2(3):200–204,2013

[3] Lumini, A., and Nanni, L., An improved biohashing for humanauthentication. Pattern Recogn. 40(3):1057–1065, 2007

[4] Kocher, P., Jaffe, J., and Jun, B., Differential power analysis.In: Advances in CryptologyCRYPTO99: Springer, 388–397,1999

[5] Yang, C.C., Yang, H.W., and Wang, R.C., Cryptanalysis of securityenhancement for the timestamp-based password authenticationscheme using smart cards. IEEE Trans. Consum. Electron.50(2):578–579, 2004

[6] M. Maas, “Pairing-based cryptography.” Master’s thesis,TechnischeUniversiteit Eindhoven, januari 2004. BIBLIOGRAFIEBIBLIOGRAFIE, 2004.

[7] J. M. Steele and J. Michael, The Cauchy-Schwarz master class: anintroduction to the art of mathematical inequalities. CambridgeUniversity Press, 2004.

[8] Fan Zhang, “Charm-crypto Benchmark.” [Online]. Available:http://student.seas.gwu.edu/~zfwise/crypto/report 1 4 1.pdf.for Digital Image Encryption. Opt. Commun. 2011, 284, 5415–5423.

[9] B. Tiwari and A. Kumar, “Physiological Value Based PrivacyPreservation of Patient’s Data Using Elliptic Curve Cryptography,”Heal. Informatics - An Int. J., vol. 2, no. 1, pp. 1–14, 2013. map. Comput.Electr. Eng. 2012, 38, 1240–1248.

[10] Zhang, J., Hou, D., Ren, H., 2016. Image Encryption Algorithm Based on Dynamic
DNA Coding and Chen’s Hyperchaotic System, Mathematical Problems in
Engineering, Article ID 6408741, 11pages.

[11] S. Peter, D. Westhoff, and C. Castelluccia, “A Survey on theEncryption of Convergecast Traffic with In-Network Processing,”IEEE Transactions on Dependable and Secure Computing, vol. 7,no. 1. pp. 20–34, 2010.

| DOI: 10.15680/IJIRCCE.2021.0904129 |

[12] Zhang Y, Xiao D. Self-adaptive permutation and combined global diffusion for chaotic color image encryption. AEU-International Journal of Electronics and Communications, 2014, 68(4): 361-368.
[13] Chen JX, Zhu ZL, Fu C, Yu H, Zhang LB. An efficient image encryption schemeusing gray code based permutation approach. Opt Laser Eng 2015;67:191–204.
[14] Xu L, Li Z, Li J, Hua W. A novel bit-level image encryption algorithm based onchaotic maps. Opt Laser Eng 2016;78:17–25.
[15] Wang XY, Teng L, Qin X. A novel color image encryption algorithm based onchaos. Signal Process 2012;92:1101–8.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details