International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Elliptic Curve Blended Cross Chaos Based Secure Image Communication

Sujarani Rajendran, S Abilashaa, Manivannan Doraipandian

Abstract:-Image encryption has proven a successful method to communicate the confidential information. Some of the images may or may not be confidential. So there is a need to secure the confidential images. Initially, symmetric encryption is used for security purpose. But it has the problem that if the key is revealed the interceptors can immediately decode it. To make the key transformation more secure, asymmetric encryption is introduced. In this two different keys are used for encoding and decoding. So even the interceptors hacked the key it cannot be possible to decode. In this project Elliptic Curve Cryptography (ECC) is utilized for generating the keys and the cross chaotic map used for generating the chaotic sequence. These chaotic sequences are utilized to encode the image for secure communication.

Keywords— Chaotic , ECC, Encryption, image security.

I. INTRODUCTION

With the rapid evolution of social media and transmission technology, transferring images across internet become popular. These transferred images can be used for personal or official use without antecedent authorization. Image encryption is one efficient strategy to protect images from interceptors. Cryptography provides us a secure communication. Asymmetric key cryptosystem provides secure key sharing compared to symmetric cryptosystem. ECC is healthier, because it is able to provide a very high degree of security with a relatively smaller key size than other cryptographic systems.By using the technique of Diffie-Hellman, both the sender as well as the receiver can exchange their public keys[1].ECC operates with a petite key volume and also witha diminutive quantity of memory as compared with RSA.Thereby, lot of ECC based image cryptosystem has been developed. Later an effective public key cryptography technique called Elliptic Curve Cryptography (ECC) was proposed. Later a powerful cryptosystem scheme using two rounds of encryption techniques was introduced. A strong key is used as an input for every image to develop the confusion as well as the diffusion processes. Confusion technique is achieved using non linear S-box. Here, the diffusion technique is achieved using matrix multiplication on the sub-matrix of image. The proposed system has a good ciphering speed that can repel various types of attacks which are known. Then, a scheme of encryption based on DNA encoding and ECC (Elliptic Curve Cryptography) was developed. Generally a good scheme of encryption should produce an indecipherable cipher text.

Later [2]suggested an encryption system based on chaos and substitution permutation network. This scheme is composed of four stages. 1) A diffusion stage using bitwise operation XOR and proposed a new chaotic map. 2) Then, generates a substitution phase which is based on well-built S-boxes. 3) For enhancing the performance of encryption a diffusion phase based on chaotic map is introduced. 4) Finally, block permutation operation is applied. The proposed system has got better working in term of security, speed and sensitivity when compared with some schemes of chaos-based encryption. Based on heterogeneous bit-permutation and correlated chaos, in [3]Puneet et al. proposed an encryption algorithm. By dividing the bits plane in to high and low bits plane, the heterogeneous bit-permutation is performed. High plane - 5^{th} to 8^{th}bit planes. Low plane - 1^{st} to 4^{th}- bit planes. Combination of all the planes produces a permuted image. The heterogeneous permutation of bit provides better permutation efficiency and decreases the computation cost. For increasing the security and execution speed, [4] proposed a data encryption algorithm using modified AES with increasing the number of rounds. By using feistel network and special properties of quaternion, [5] proposed an

(DICOM) Digital Imaging and Communications in Medicineencryption. The speed of this encryption is compared with (AES-ECB) Advanced Encryption Standard-Electronic Code Book. DICOM is faster than AES-ECB. One of the promising techniques of public key cryptography is ECC (Elliptic Curve Cryptography) [6].As compared to other encryption schemes, it has the capacity to provide better security with lesser key size.

Afterward, Hill cipher is introduced, Which is one of the asymmetric techniques. It is simply ordered and high speed. But feeble in security, because both the sender as well as the receiver shares private key (identical key) via unsecured channels. By using hill cipher algorithm [7] proposed a new method for encryption. It first produces the numerical values of cipher text, and then converts it in to points on ECC using the scalar product.

Manuscript published on 30 September 2019
* Correspondence Author
Sujarani Rajendran*, Department of Computer Science and Engineering, Srinivasa Ramanujan Centre, SASTRA Deemed University, Kumbakonam ,Tamilnadu,India.
S. Abilashaa, Department of Computer Science and Engineering, Srinivasa Ramanujan Centre, SASTRA Deemed University, Kumbakonam. Tamilnadu,India.
(Email::sabilashaa@gmail.com)
Manivannan Doraipandian, School of Computing, SASTRA Deemed University, Thanjavur , Tamilnadu, India.

This technique increases the safety and its computation time, because usually scalar multiplication takes long time for computation. The key matrix should be invertible in hill cipher algorithm for decryption process.

Later, [8]proposed a new technique called self invertible key matrix (k=k^{-1}) that avoids the above problem. It uses single matrix for encrypting the pixels inside the image but it takes more time. In this paper, ECC is used for generating the seed key and cross chaotic map is used for generating chaotic series.The article is structured as follows Section II elaborates the preliminaries of the work and section III defines the whole procedure of the system and trial results are discussed in section V. Conclusion is given in section VI.

II. PRELIMINARIES

A. Ecc equation

ECC is an asymmetric public key encryption technique used for creating faster, smaller and more efficient keys. Here, ECC is used to generate initial key points. An elliptic curve E over a prime field F_p is defined in Eq.(1)

$$E: y^2 \bmod p = x^3 + ax + b(\bmod p)$$
$$\text{where} a, b \in F_p \text{and} p \in \text{prime} \quad (1)$$

Also, ECC satisfies the equation

$4a^3 + 27b^2$ congruent to 0(mod p) and $p \neq 2,3$

1) Point addition

Suppose $m_1 = (a_1,b_1)$ and $m_2 = (a_2,b_2)$,$m_1 \neq m_2$. These m_1 and m_2 lies on the elliptic curve E. Adding these produces the output C represents in Eq.(2)

$$C = (a_3, b_3) = m_1 + m_2$$
$$S = \frac{(b_2 - b_1)}{(a_2 - a_1)} \quad (2)$$
$$\text{where} \begin{cases} a_3 \equiv (S^2 - a_1 - a_2)(\text{modp}) \\ b_3 \equiv (Sa_1 - Sa_3 - b_1)(\text{modp}) \end{cases}$$

2) Point multiplication

Summing up the point P= $(\mathbf{a_1},\mathbf{b_1})$ which lies on the elliptic curve E to itself, named point doubling. The point C results from the doubling of the point $\mathbf{m_1}$, the resulting C ∈ E.

$$C = 2P = P + P = (a_3, b_3)$$
$$S = \frac{3a_1^2 + a}{2b_1} \quad (3)$$
$$\text{where} \begin{cases} a_3 \equiv (S^2 - 2a_1)\ (\text{modP}) \\ b_3 \equiv (Sa_1 - Sa_3 - b_1)\ (\text{modP}) \end{cases}$$

B. Cross chaotic map

Cross chaotic map is used to generate chaotic series. It takes two key points as input and produces two chaotic series as output say, cx_i and cy_i which is depicted in Eq. (4)

$$cx_i = \sin^2 3\ (\arcsin\sqrt[2]{|cy_{i-1}|}) \quad (4)$$
$$cy_i = 4cx_{i-1}^3 - 3cx_{i-1}$$

where x_i, y_i , i = 1,2,…,rows

C. ECC Diffie – Hellman key exchange

Let n1 and n2 be the private keys of both sender and the receiver. Let m_a and m_b be the public keys of both sender and receiver. Public keys are calculated by point multiplication of private keys with generator point G. Shared key is computed as $n1m_b$ for the sender and $n2m_a$ for the receiver as specified in Eq.(5)

$$n1m_b = n1n2G = n2n1G = n2m_a \quad (5)$$

III. PROPOSED ENCRYPTION SCHEME

Step 1: Import the plain image I for encryption and the Key KG Points (x,y) of ECC.

Step 2: Convert points to initial key of x and y by applying the following Eq.(6)

$$cx_0 = {}^{x}/_{10^n} \quad cy_0 = {}^{y}/_{10^n} \quad (6)$$
$$n = number of digits of x/y$$

Step 3: The values of x_0 and y_0 are applied to the cross chaotic map which is defined in Eq. (6)for generating two chaotic series

$$CX = \left\{cx_1, cx_2, cx_3 \dots \dots cx_{\frac{NxM}{2}}\right\} \text{and} \quad (7)$$
$$CY = \{cy_1, cy_2, cy_3 \dots \dots cy_{(NxM)/2}\}$$

where M and N specifies the width and height of the image.

Step 4: The input image I is partitioned into 16 x 16 non overlapping blocks.

Step 5: The first stage of the encryption process is confusion, each blocks are scrambled using three folding technique depends on the binary value of the ECC key points. Suppose the key point is 95 the concerned binary value is 01011111. The first two bits are taken for choosing option of folding. The possibilities of the 2 bits are 00, 01, 10, 11. After folding the blocks each pixels in the folded blocks are shuffled by using Diagonal, horizontal and vertical folding.

Case 00: Take next two bits

Case01:Diagonal, Vertical, Horizontal

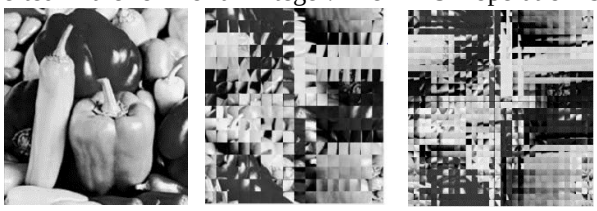
Case 10: Vertical, Horizontal, Diagonal

Case 11:Horizontal, Diagonal, Vertical

$$I' = folding(I)$$

The following Fig.1 illustrate the results of block folding and pixel folding inside each block by taking the first two bit (01) in ECC point.

Step 6: The second stage in encryption process is diffusion, which is done by XORing the chaotic series with confused image. For diffusion, the chaotic series need to be converted in the form of an integer. Then XOR operation is



(a) (b) (c)

Fig.1 Confusion result: a) original image b)block folding c) pixel folding on each block

implemented between the integer series and pixels of the confused image which is demonstrated in Eq.(5)

$$key_{i,j} = (cx_k \times 10^{14})\ mod\ 256\ \ if\ (jmod\ 2 == 0)$$
$$key_{i,j} = (cy_k \times 10^{14}) mod\ 256\ \ if (jmod\ 2! = 0)$$
$$where i, j = 1,2, \dots . \frac{M}{N} \quad (8)$$
$$where k = 1,2, \dots \dots \frac{M \times N}{2}$$
$$E_{i,j} = I'_{i,j} \oplus key_{i,j}$$

The final encrypted image E is corresponded between sender and receiver. For getting original image, the receiver has to do the reverse of the encryption procedure by using concerned keys. The block diagram of the entire logic is given in the following Fig .2

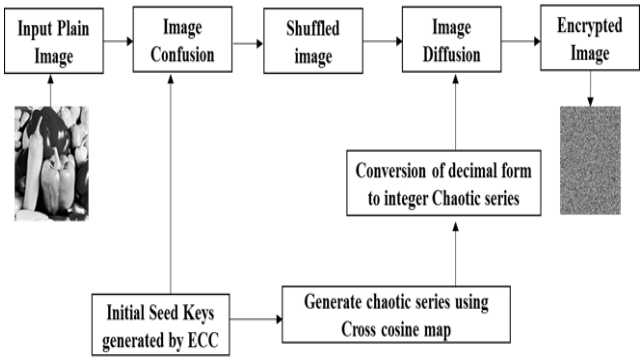


Fig.2 Block diagram

IV. EXPERIMENTAL RESULT

Matlab R2016b is used for implementing the planned scheme. Distinct images are taken for the trial purpose of the size (256×256). An ECC equation and plain image is given as input. Both the plain image and ECC equation is shared between the sender and receiver in secure manner. Firstly the sender generates public and private key using ECC equation. These two keys are passed to the cross chaotic map for generating the chaotic series. On the other hand, the input image is confused using folding concept and diffusion is done by XORing the chaotic series with pixel position of the image. Fig .3 shows the results of each phases.

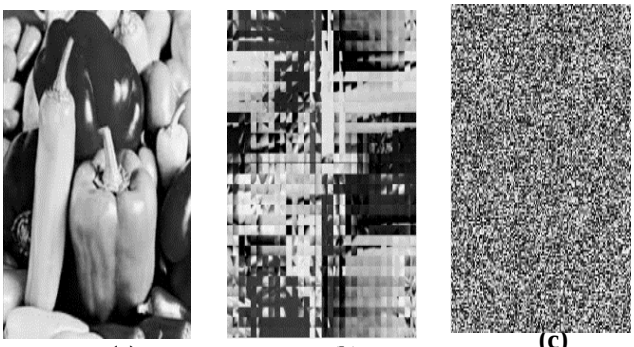


Fig.3 trial result: a) Original image b) Confused image c) Cipher image

V. EFFICIENCY AND SECURITY ANALYSIS

A well-organized image cipher opposes various types of attacks such as linear attack and differential attack. The level of defense of the proposed system has proved histogram, correlation, entropy analysis and the cipher image attack analysis.

A. Histogram study

The pixel of encrypted image is randomly distributed using histogram analysis [9]. It reveals the graphical depiction of pixel allocation in cipher image. Fig.4 shows the histogram of plain image and the cipher image. Based on the histogram study, the pixel of the cipher image is ultimately allocated so it is very tricky for the interceptors to apply statistical analysis for gettingthe original image.

B. Correlation coefficient analysis

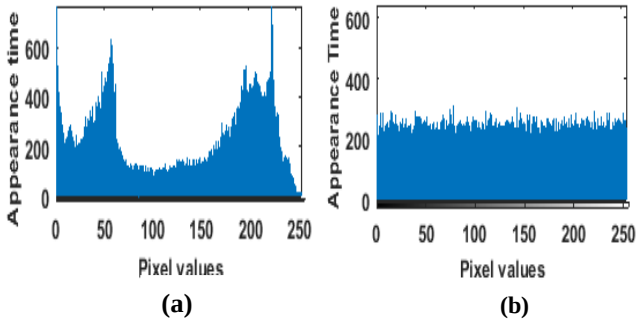


Fig.4 Histogram analysis a)Plain image b)Cipher image

The pixels of the plain image are extremely connected with each other in all paths. A good image encryption should produce the cipher image with less correspondence between the values of the pixel. The best way of finding efficiency in the proposed system is to find the correlation among the pixels using correlation coefficient analysis [10]. We have chosen 1000 pairs of pixel from each and every direction of the cipher image and the encrypted image to check the correlation. (6) represents the computation of correlation coefficient. A less correlation values of cipher image among the pixel can only be achieved by a good cryptosystem.

$$\mathrm{Exp}(a) = \frac{1}{N}\sum_{i=0}^{n} a_i$$

$$\mathrm{Var}(a) = \frac{1}{N}\sum_{i=0}^{n}(a_i - \mathrm{Exp}(a))^2$$

$$\mathrm{Covar}(a,b)\frac{1}{N}\sum_{i=0}^{n}(a_i\,\mathrm{Exp}(a))(b_i\mathrm{Exp}(b))^2$$

$$r_{ab} = \frac{\mathrm{Covar}(a,b)}{\sqrt{D(a)}\times\sqrt{D(b)}} \quad (8)$$

Where, a and b are values refers two ne ixels, Covar(x,y) refers to the covariance, Var(x) refers to variance and E(x) refers to the mean value of the pixels. The correlation coefficient of diagonal direction of the plain image and the cipher image is given in fig .5.

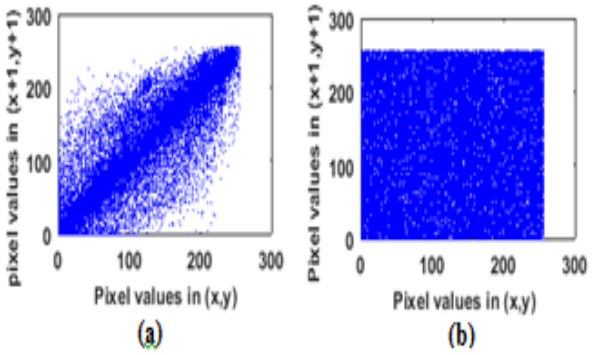


Fig.5 Correlation results a)plain image b)cipher image

C. Entropy analysis

Unreliability of pixel values in the cipher image can be calculated using information entropy. The exact value of arbitrary image entropy is 8. In this proposed system, the cipher image is considered as uniformly distributed if the information value of entropy for the cipher image is nearer to 8 and also it has capacities to struggle against statistical entropy. The entropy value is calculated by applying the following Eq. (9)

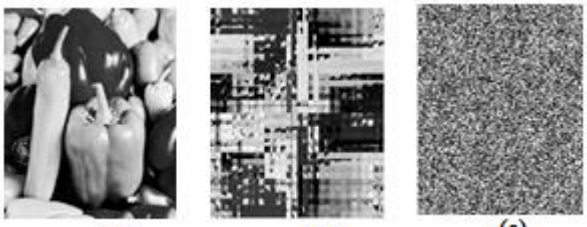
$$E(A) = \sum_{i=0}^{n} P(A_i) \log_2 \frac{1}{P(A_i)} \qquad (9)$$

Where, A_i is the i^{th} pixel value of image and $P(A_i)$ is the probability of A_i. The entropy significance of cipher image is (7.9967) which are nearer to 8. It implies that it can struggle against statistical attack.

D. Cipher image attack analysis

The hackers can smash up the cipher image by using noise attacks and cropping during the conduction of cipher image between the sender and the receiver. It is not possible for them to decrypt it using the correct key even if the cipher image is received by the appropriate receiver. A slight change in the cipher image can disintegrate the entire outcome of decryption. Thus the good image cryptography must oppose cipher assaults[11]. In this proposed system it is examined by applying the attack of crop and noise.

1) Cropped attack analysis



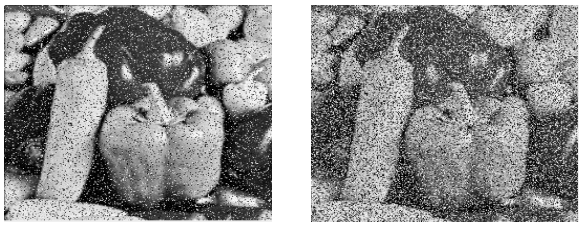
(a) (b) (c)

Fig.3 trial result: a) Original image b) Confused image c) Cipher image

Heftiness can be easily recognized by applying crop attack to encrypted image. It is possible to apply the cropping in two different approaches. In first approach, the cipher image is cropped randomly with small size in different regions and in the second approach; the cipher image is cropped as a single region with a large size. Fig. 6demonstrates that the proposed system haseffectiveness to struggle against cropped attack.

2) Noise attack analysis

At the time of broadcast different noises demean the cipher image. A minor change in the encrypted image might possibly lead a high collapse in decoded image. So that a validated receiver possibly will not envision the plain image even if it is decrypted in a correct way. A superior cipher should oppose against the noisy attacks. The heftiness of the proposed system can be checked by applying the noise of salt and pepper to the encrypted image in various concentrations and check the design attribute of the decoded image demonstrated in Fig.7



(a) (b)

Fig. 7 Noise attack analysis: Decrypted image with a) 0.02 intensity b) 0.05 intensity

VI. CONCLUSION

A new image cryptosystem has successfully proposed by joining the ECC and cross-chaotic map which produces the chaotic series. The proposed system has been built by the combination of two phases. In confusion, image is scrambled by differentfolding methods. Firstly, it does block folding followed by cell folding. In diffusion phase, a pixel value of the scrambled image is double XORed with the key series of cross chaotic map. To prove the efficiency and security, the encrypted image is undergone through several attack analyses. The result of the analyses proves that the proposed technique has adequate scope of security. Hence, the proposed scheme is applicable for real-time image communication.

REFERENCES

1 W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 2004.

2 A. U. Rehman and X. Liao, "A novel robust dual diffusion/confusion encryption technique for color image based on Chaos, DNA and SHA-2," *Multimed. Tools Appl.*, pp. 1–29, 2018.

3 P. Kumar and S. B. Rana, "Development of modified AES algorithm for data security," *Optik (Stuttg).*, vol. 127, no. 4, pp. 2341–2345, 2016.

4 M. García-Martínez and E. Campos-Cantón, "Pseudo-random bit generator based on multi-modal maps," *Nonlinear Dyn.*, vol. 82, no. 4, pp. 2119–2131, 2015.

5 M. Dzwonkowski, M. Papaj, and R. Rykaczewski, "A New Quaternion-Based Encryption Method for DICOM Images," *IEEE Trans. Image Process.*, vol. 24, no. 11, pp. 4614–4622, 2015.

6 B. Alese, E. Philemon, and S. Falaki, "Comparative Analysis of Public-Key Encryption Schemes," *Int. J. Eng. Technol.*, vol. 2, no. 9, pp. 1552–1568, 2012.

7 K. Madhusudhan Reddy, A. Itagi, S. Dabas, and B. Kamala Prakash, "Image Encryption Using Orthogonal Hill Cipher Algorithm," *Int. J. Eng. Technol.*, vol. 7, no. 4.10, pp. 59–63, 2018.

8 Z. E. Dawahdeh, S. N. Yaakob, and R. Razif bin Othman, "A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 30, no. 3, pp. 349–355, 2018.

9 S. Rajendran and M. Doraipandian, "Biometric template security triggered by two dimensional logistic sine map," *Procedia Comput. Sci.*, vol. 143, pp. 794–803, 2018.

10 A. Yaghouti Niyat, M. H. Moattar, and M. Niazi Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Opt. Lasers Eng.*, vol. 90, no. October 2016, pp. 225–237, 2017.

11 A. Girdhar and V. Kumar, "A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences," *Multimed. Tools Appl.*, vol. 77, no. 20, pp. 27017–27039, 2018.