© 2019 IJSRSET | Volume 6 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology
DOI : https://doi.org/10.32628/IJSRSET196430

An Enhanced Image Encryption Scheme Based on ECC and PWLCM

Salma Bendaoud[1], Fatima Amounas[1], El Hassan El Kinani[2]

[1]R.O.I Group, Computer Sciences Department, Faculty of Sciences and Technics, Moulay Ismail University, Errachidia, Morocco

[2]M.M.S.C Group, ENSAM, Moulay Ismail University, Meknes, Morocco

ABSTRACT

Elliptic curve cryptography (ECC) is an effective approach to protect privacy and security of information. Digital Image encryption is an important issue widely used to protect the data and to ensure the security. Several encryption and decryption cryptosystems are available to keep image secure from unauthorized user. Elliptic Curve Cryptography (ECC) has proven to be the best solution for public key encryption. It provides a good level of security with smaller key size. In this paper we attempt to develop an enhanced Image Encryption Scheme based on ECC and PWLCM (Piecewise Linear Chaotic Map). Here, we generate a key image to enhance data security using ECC and PWLCM. From the experiment results and security analysis, we prove that our scheme cannot only achieve good encryption, but also resist the exhaustive, statistical and differential attacks.

Keywords : Image Encryption, Prime Group Field, Elliptic Curve, Piecewise Linear Chaotic Map

I. INTRODUCTION

In recent years, Elliptic curve cryptography has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. Various encryption algorithms are available to protect the image from unauthorized user. In the literature, several image encryption methods have been proposed to secure multimedia information before transmission over unsecure channels [3-5]. ECC is a better method to transmit the image securely Several Image encryption algorithms have been proposed [1-10]. For instance, Li Li et al [6] had proposed in 2012 an encryption scheme using elliptic curve ElGamal based homomorphic image for sharing secret images. They selected the parameter of the elliptic curve to resist Pollard's rho, isomorphic and Pohlig Hellman attack. The experimental result indicates that this algorithm has high security than encryption using RSA and ElGamal. Moreover, Bidyut Jyoti Saha and. al [8] proposed a digital Image Encryption using ECC and DES with Chaotic Key Generator in 2013. The scheme encrypts the original image using DES with the help of key sequence which is generated from a chaotic key generator with the help of heron map and then mapped the encrypted image in the points of elliptic curve. Next, Laiphrakpam Dolendro Singh et al [3] proposed an image encryption using elliptic curve cryptography in 2015. In this work, they have presented the implementation of image encryption process. They combine the digital signature to the cipher image to provide authenticity and integrity to the received image. In 2018 Umar Haya et al [9] proposed a novel image encryption scheme based on elliptic curve. This algorithm presents a new methods for the construction of substitution boxes (S-boxes), and the generation of pseudo random numbers (PRN)

with high entropy, and security of confidential images based on elliptic curves over a prime field.

In this paper, we attempt to develop an enhanced approach to secure digital images using ECC and PWLCM. This approach will boost the security of the cryptosystem using scrambling process based on PWLCM . The rest of this paper is organized as follows: preliminary works are presented in section 2. The proposed image encryption algorithm is described in detail in section 3. Section 4 is devoted to the experimental results. The security analysis of the proposed scheme is examined in section 5. Finally, conclusions are made in section 6.

II. METHODS AND MATERIAL

A. Elliptic Curve Cryptography

Elliptic curves are algebraic curves which have been studied by many mathematicians for a long time. In 1985, Neal Koblitz (Koblitz 1987) and Victor Miller (Miller 1986) independently proposed the public key cryptosystems using elliptic curve. Since then, many researchers have spent years studying the strength of ECC and improving techniques for its implementation. The Elliptic curve cryptosystem provides a smaller and faster public key cryptosystem. In the present paper, for encryption and decryption using elliptic curves, so consider the equation of the form

$$y^2 = x^3 + ax + b \ (mod\ p) \qquad (1)$$

Where $a, b \in F_p$, $p \neq 2, 3$ and satisfy $\Delta = 4a^3 + 27b^2 \neq 0 \ (mod\ p)$. The set $E(F_p)$ consist of all point (x, y) that satisfy the elliptic curve E along with a point at the infinity O [11]. The set of points on $E(F_p)$ also include point, which is the point at infinity and which is the identity element under addition. The addition operator is defined over $E(F_p)$ and it can be seen that $E(F_p)$ forms an abelian group. The basic operations on elliptic curves are addition and doubling.

The addition of points follows specific rules indicated below:

a) Identity law: P + O = O + P = P for every P ∈ E

b) Inverse law: P + (– P) = O for every P ∈ E

c) Associative law: (P + Q) + R = P + (Q + R) for all P, Q, R ∈ E

d) Commutative law: P + Q = Q + P for all P, Q ∈ E

The Rules for Addition

Let $E: y^2 = x^3 + ax + b$ be an elliptic curve and let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E, where $P_1 \neq P_2$, and k is an integer. Adding the two points P_1 and P_2 giving a point R that should lie on the same curve E.

$$R = P_1 + P_2 = (x_3, y_3)$$

where

$$x_3 = \lambda^2 - x_1 - x_2 \text{ and } y_3 = \lambda(x_1 - x_3) - y_1$$

With λ define by:

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & if\ P_1 \neq P_2 \\ \dfrac{3x_1^2 + a}{2y_1} & if\ P_1 = P_2 \end{cases}$$

B. Piecewise Linear Chaotic Map

Piecewise linear chaotic map (PWLCM) has gained more and more attention in chaos research recently for its simplicity in representation, efficiency in implementation, as well as good dynamical behavior [12]. The simplest PWLCM is defined by:

$$x_{n+1} = F_P(x_n) = \begin{cases} x_n/p, & 0 < x_n < p \\ \frac{(x_n - p)}{(0.5-p)}, & p \leq x_n < 0.5 \\ F_P(1-x_n), & 0.5 \leq x < 1 \end{cases} \qquad (2)$$

Where $x_n \in (0, 1)$ and $p \in (0, 0.5)$. In our experiment we assign $p = 0.25678900$

C. Proposed Method

In this section, we present our main result. First consider the elliptic curve given by the Weierstrass equation Eq 1. Suppose here that we have some elliptic curve E defined over a finite field F_p and that E and a point P ∈ E are publicly known. The proposed method is based on ECC and PWLCM.

The overall architecture of our cryptosystem is divided into three stages: key generation, encryption process and decryption process.

Then, when Alice wants to communicate secretly with Bob, they proceed thus:

a. Key generation

Step 1. Bob chooses a random integer k_B, and publishes the point $P_B = k_B P$ (while k_B remains secret).
Step 2. Alice chooses a random integer k and computes
$Q = k P_B$
Step 3. Alice generates the pixel value of key image using Eq. (2) and Eq. (3).

$$pixel = [x \times 256] \quad (3)$$

where $x \in (0,1)$ is iteration value of PWLCM.
Step 4. Alice repeat step 3 to obtain the key image.

b. Encryption process

The algorithm of encryption is given as follows:
Step 1. Choose randomly one row and one column in the key image and apply the scrambling process on the plain image.
Step 2. Imbed each pixel m of the plain image and key image into point on the elliptic curve, where m → Pm is the embedding system which imbeds intensity values on points of an elliptic curve E [2].
Step 3. Encrypt the mapping points using ECC technique.
Step 4. Send the encrypted image to the receiver.

c. Decryption process

The process is done by reversing the operations done in the encryption process. The algorithm of decryption is given as follows:
Step 1. Choose a random integer k_B and compute

$$Q = k_B P_A$$

where k_A is private key of Alice and $P_A = k_A P$ is his public key.
Step 2. generate the key image using Eq. (2) and Eq. (3).
Step 3. Imbed each pixel of the cipher image and key image into point on the elliptic curve E.
Step 4. Decrypt the mapping points using reverse ECC technique.
Step 5. Apply a reversal of scrambling to unscramble the decrypted image.
The results of encryption and decryption processes are presented in Figure 1.

III. RESULTS AND DISCUSSION

A. Statistics Analysis

In theory, a good image encryption algorithm should have a strong immunity against any kinds of statistical attacks. Statistical analysis methods such as: Histograms and correlation analysis of two adjacent pixels on cipher images can help us to validate the uniformity property of the encrypted image and to check the independence property.

The histogram shows how the pixels are distributed by plotting on a graph the value intensity. In this work, we have analyzed the histograms of Peppers and its corresponding cipher image. The plots of the original and the encrypted images histograms are shown in Figure 2. The result shows that the histogram of the encrypted image is uniformly distributed with respect to the histogram of the original image. The proposed encryption algorithm makes the dependence of the statistical properties of the encrypted image and the original image almost random. This makes cryptanalysis increasingly

difficult because the encrypted image does not provide any element which relies on the exploitation of the histogram and which makes it possible to design a statistical attack on the proposed image encryption process.

Furthermore, we checked the correlations of adjacent horizontal, vertical and diagonal adjacent pixels of the plain image and cipher images respectively. Figure 3a, c, e shows the correlation distributions of adjacent pixels of plain image "Peppers" along horizontal, vertical and diagonal directions, Figure 3b, d, f gives the corresponding distributions of the cipher image. Experiments using the proposed method resulted that there is a very good correlation among the horizontal adjacent pixels in the digital image. From Figure 3, it is obvious that the adjacent horizontal of cipher image is uniform from of the original image. Hence it does not provide any statistical attacks to the algorithm.

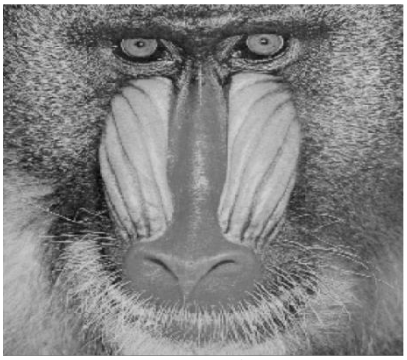
More precisely, we calculate the correlation coefficients $r_{x,\ y}$ of adjacent pixels along different directions by using Eq. (4) and Eq. (5) [5]. The results of the correlation coefficients for horizontal, vertical and diagonal adjacent pixels for the plain image and its cipher image are given in Table 1.

$$cov(x, y) = E\{(x - E(x))(y - E(y))\} \quad (4)$$

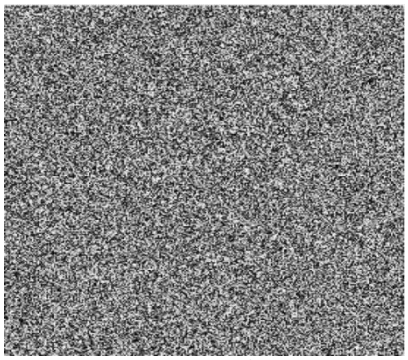
$$r_{x,y} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (5)$$

where x and y are values of two adjacent pixels in the plain image or cipher image and N denotes the number of selected pixel pairs.

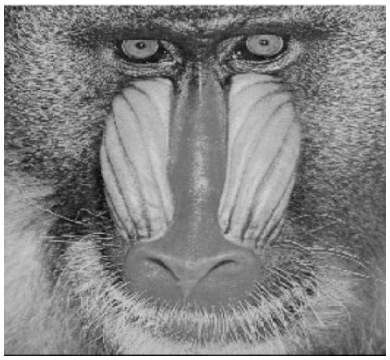
$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i,\ D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2$$



(a) Plain image of Baboon

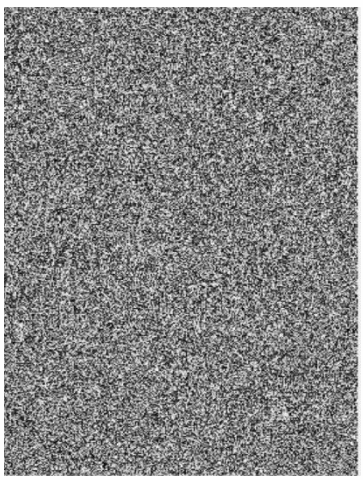


(b) Cipher image of Baboon



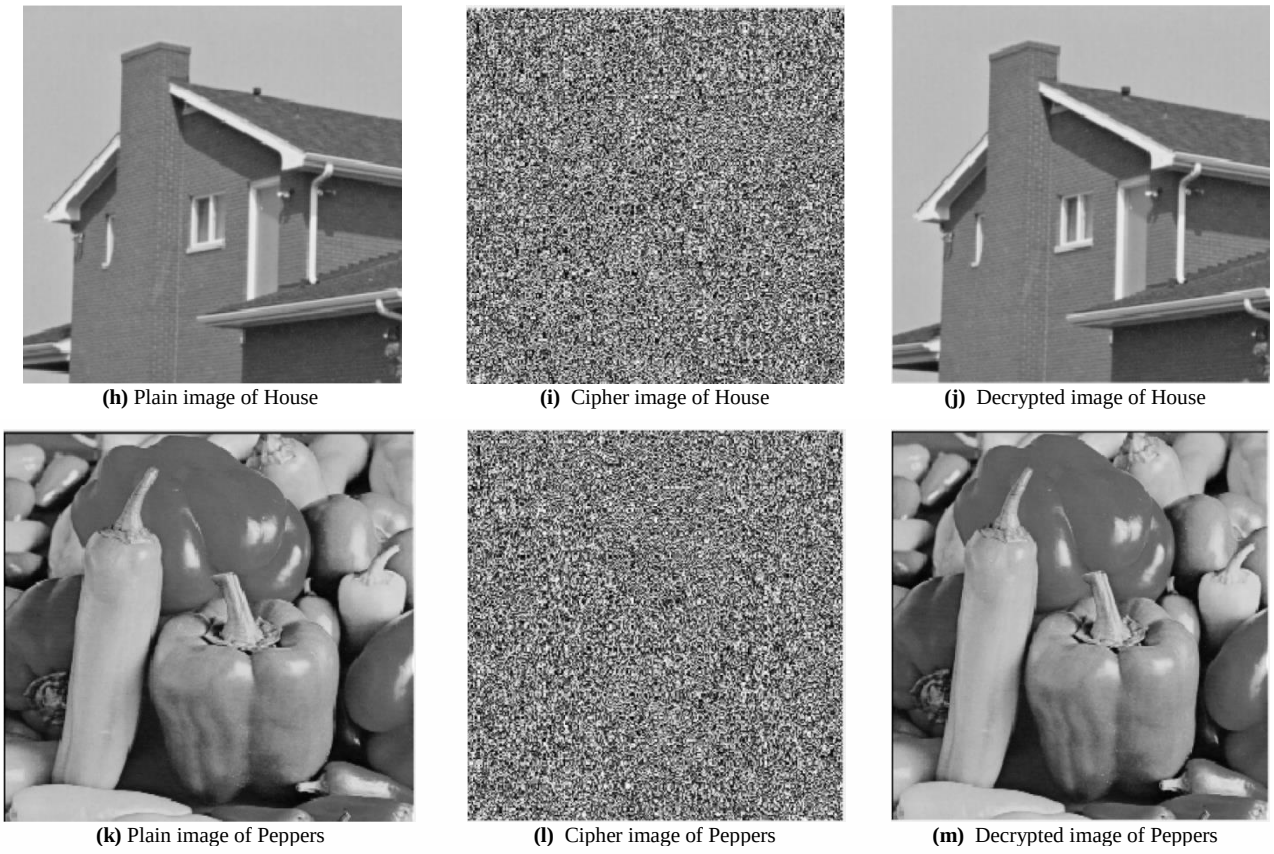
(c) Decrypted image of Baboon

(e) Plain image of Barbara



(f) Cipher image of Barbara

(g) Decrypted image of Barbara



(h) Plain image of House **(i)** Cipher image of House **(j)** Decrypted image of House

(k) Plain image of Peppers **(l)** Cipher image of Peppers **(m)** Decrypted image of Peppers

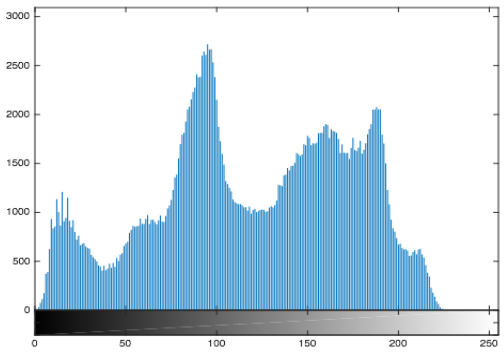
Figure 1: Results of encryption and decryption

TABLE I

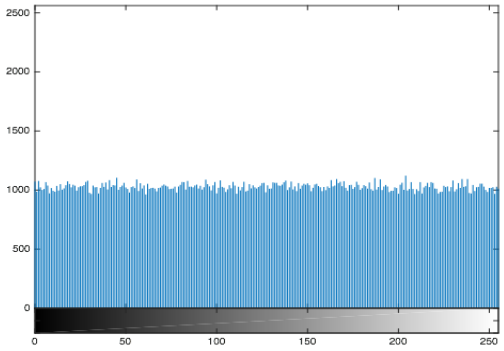
CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS IN THE PLAIN AND CIPHER IMAGES

Image	Plain image			Cipher image		
	Horizontal	Diagonal	Vertical	Horizontal	Diagonal	Vertical
Baboon	0.9322	0.8647	0.9100	-0.0031	-0.0018	0.0041
Barbara	0.8271	0.8310	0.9501	-0.0019	-0.0004	-0.0125
Boat	0.9368	0.9240	0.9709	-0.0027	-0.0013	0.0540
House	0.9735	0.9481	0.9586	0.0029	0.0035	-0.0070
Lena	0.9691	0.9639	0.9841	-0.0007	0.0016	-0.0037
Peppers	0.9299	0.9072	0.9309	-0.0032	-0.0031	-0.0093

It is clear from Figure 3 and Table 1 that the strong correlation between adjacent pixels in plain image is greatly reduced in the cipher image produced by the proposed scheme.



(a) Plain Image



(b) Cipher Image

B. Information Entropy

The Information entropy is a parameter that measures the level of the complexity of a system. It is used by researchers to weigh the performance of encryption algorithm. Let m be the information source, and the formula for calculating information entropy is:

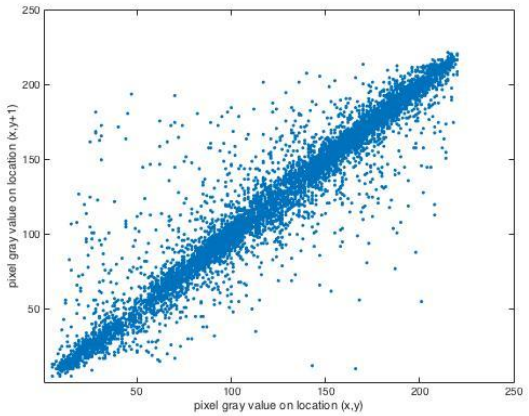
$$H(m) = -\sum_{i=0}^{2^N-1} p(m_i) \log_2 p(m_i) \qquad (6)$$

where $p(m_i)$ represents the probability of symbol m, and N is the total number of symbols. We know the closer it gets to 8, the less possible for the cryptosystem to divulge information. We use Eq. (6) to calculate the information entropy of the ciphered images of Figure 1. Table 2 shows the assessing results entropy of different cipher images, which are all close to the ideal value 8. So, the proposed algorithm is secure against the entropy attack.

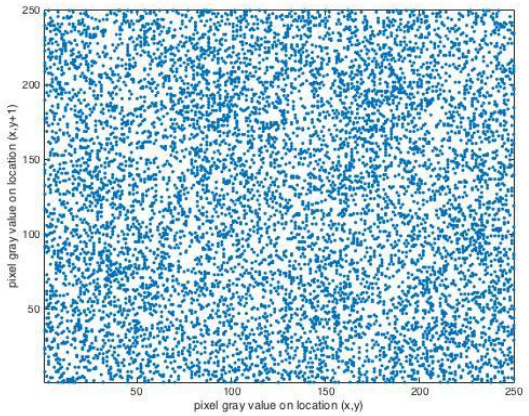
TABLE II

INFORMATION ENTROPY OF PLAIN AND CIPHER IMAGES

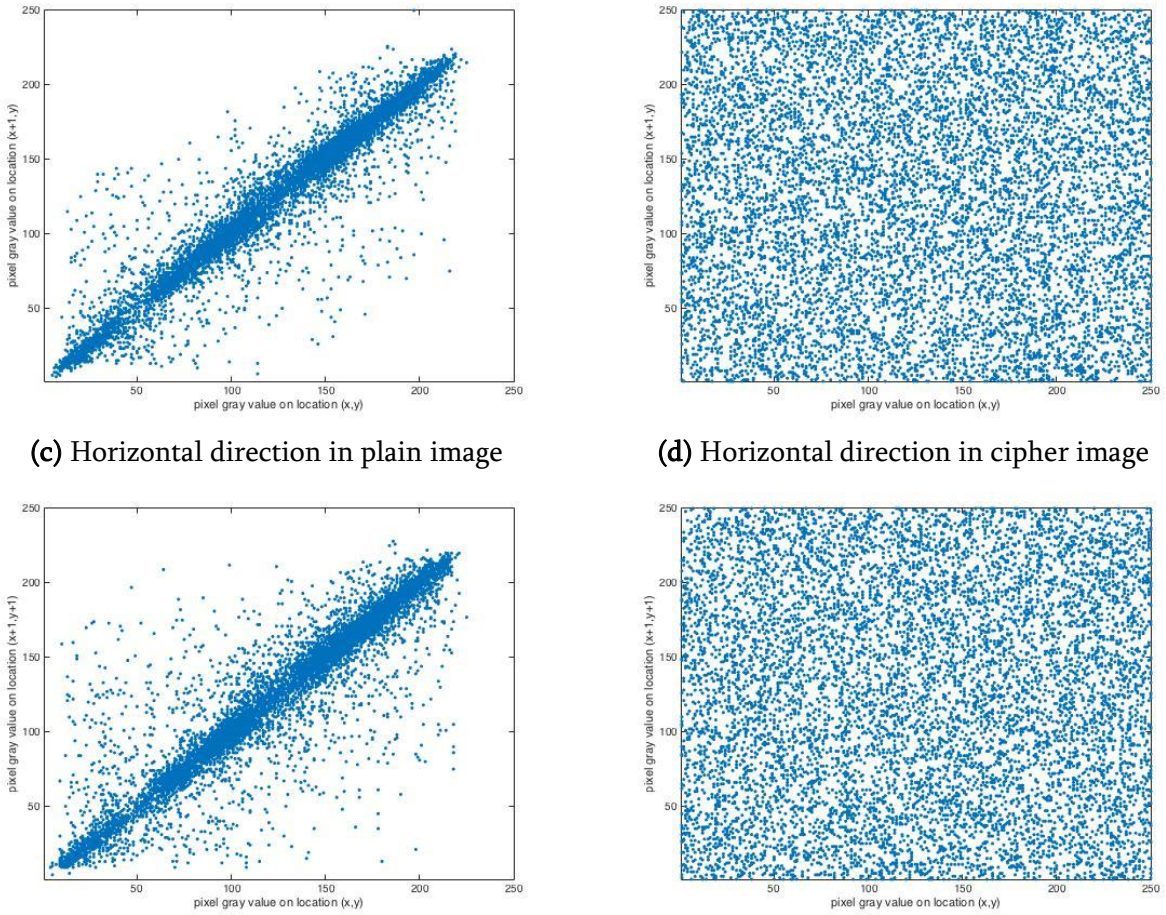
Image	Plain image	Cipher image
Baboon	7.2925	7.9994
Barbara	7.1674	7.9994
Boat	7.1914	7.9993
House	6.4971	7.9973
Lena	7.4455	7.9993
Peppers	7.5327	7.9973



(a) Vertical direction in plain image



(b) Vertical direction in cipher image



(c) Horizontal direction in plain image

(d) Horizontal direction in cipher image

(e) Diagonal direction in plain image

(f) Diagonal direction in cipher image

Figure 3. Correlation of two adjacent pixel of peppers image

C. Analysis of Resisting Differential Attack

The diffusion performance is commonly measured by means of two criteria, namely, the number of pixel change rate (NPCR: number of pixels change rate) and the unified average changing intensity (UACI: unified average changing intensity) [13].

The NPCR and the UACI values are given by:

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (7)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \quad (8)$$

where C_1 and C_2 are the cipher images before and after one pixel of the plain image is modified, and W and H are the width and height of the image, respectively. *D(i,j)* is defined as:

$$D(i,j) = \begin{cases} 1, & C_1(i,j) \neq C_2(i,j) \\ 0, & otherwise \end{cases}$$

Table 3 shows the results according to the proposed algorithm of NPCR and UACI. We have found that the NPCR is over 99% and the UACI is over 33%. While using the proposed method, a fairly good result can be obtained, thus the efficiency of the image cryptosystem is significantly improved.

TABLE III
NPCRS AND UACIS

Image	NPCR	UACI
Baboon	0.9961	0.2752
Barbara	0.9961	0.3003
Boat	0.9961	0.2838
House	0.9779	0.2761
Lena	0.9961	0.2860
Peppers	0.9936	0.3045

IV. CONCLUSION

This paper proposed an enhanced symmetric cryptographic system based elliptic curve and PWLCM chaotic system to encrypt image. The performance of the proposed algorithm is good security and it was implemented in MATLAB R2015a as the simulation software. The results of experiments and security analysis show that the proposed image encryption scheme can achieve a good encryption result with excellent image quality and can resist against common attacks. In the future, it can be enhanced by making this method compatible to encrypt multimedia data which have to be transmitted securely over unsecured channels.

V. REFERENCES

[1] Loai Tawalbeh, Moad Mowafi and Walid Aljoby. 2012. "Use of Elliptic Curve Cryptography for Multimedia Encryption". IET Information Security. vol 7, issue 2, pp. 67–74(2012).

[2] Amounas F and El Kinani E.H. 2014. "Security Enhancement of Image Encryption Based on Matrix Approach using Elliptic Curve". International Journal of Engineering Inventions, vol 3, issue 11, pp 8-16 (2014).

[3] Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh. 2015. "Encryption using Elliptic Curve Cryptography". International Multi-Conference on Information Processing-2015 (IMCIP-2015).

[4] Salma Bendaoud, Fatima Amounas and El Hassan El Kinani. 2017. "A Novel Image Encryption Scheme based on Elliptic Curve and Rubik's Cube". International Research Journal of Advanced Engineering and Science, vol 2, issue 2, pp 144-147(2017).

[5] Jiahui Wu, Xiaofeng Liao and Bo Yang .2017. "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme". Signal Processing, vol 141, pp 109–124 (2017).

[6] Li Li, Ahmed A. Abd El-Latif and Xiamu Niu.2012. "Elliptic Curve ElGamal Based Homomorphic Image Encryption Scheme for Sharing Secret Images". Signal Processing, Elsevier, vol 92, pp 1069–1078, (2012).

[7] K. Shankar and P. Eswaran.2016. "An efficient image encryption technique based on optimized key generation in ECC using genetic algorithm". Artificial Intelligence and Evolutionary Computations in Engineering Systems, Springer, pp. 705–714(2016).

[8] Bidyut Jyoti Saha and Kunal Kumar Kabi. 2013. "Digital Image Encryption using ECC and DES with Chaotic Key Generator". International Journal of Engineering Research & Technology (IJERT), vol 2, issue 11, pp 2593-2597 (2013).

[9] Umar Hayat and Naveed Ahmed Azam. 2018. "A novel image encryption scheme based on an elliptic curve". In: Signal Processing, Elsevier, vol 155, pp 391–402, (2018)

[10] K. Gupta and S. Silakari.2010. "Performance Analysis for Image Encryption using ECC". First International Conference on Computational Intelligence, Communication Networks, pp 79-82 (2010).

[11] J.H. Silverman, J. Pipher and J. Hoffstein. 2008. "An Introduction to Mathematical Cryptography". Springer (2008).

[12] Alexander Baranovski and D.Daems. 1995. "Design of one-dimensional chaotic maps with prescribed statistical properties". International Journal of Bifurcation and Chaos, vol 5, issue 6, pp 1585–1598 (1995).

[13] Wu Y. 2011. "NPCR and UACI Randomness Tests for Image Encryption", Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), p 31-38 (2011).

Cite this article as :

Salma Bendaoud, Fatima Amounas, El Hassan El Kinani, "An Enhanced Image Encryption Scheme Based on ECC and PWLCM", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 6 Issue 4, pp. 285-293, July-August 2019. Available at doi : https://doi.org/10.32628/IJSRSET196430
Journal URL : http://ijsrset.com/IJSRSET196430