GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

IMAGE ENCRYPTION AND PERFORMANCE ANALYSIS USING ELLIPTICAL CURVE CRYPTOGRAPHY

P Santhosh Teja[*1] **& P S Maitrey**[2]

[*1]M.Tech (DE & CS), Department of ECE Vishnu Institute of Technology Bhimavaram, Andhra Pradesh, India

[2]Associate Professor, Department of ECE Vishnu Institute of Technology Bhimavaram, Andhra Pradesh, India

ABSTRACT

The growth of Data Communications and Internet in day -to-day life has led us to focus our attention on how this data (Text, Image, Video etc.,) can be transmitted securely over a network without being hacked. So, in order to protect the data from unauthorized access, encryption may be done. In this paper, Image Encryption and Performance analysis are done using Elliptical Curve Cryptography (ECC). ECC is based on public key cryptography for securing data that transmits over an unsecured public channel with relatively smaller key size. For encrypting an image using ECC, the pixel values of the particular image are directly mapped (encoded) to points over an elliptic curve and further encryption is done by adding the encoded point to a cipher point over an elliptic curve by using point multiplication, point addition and point doubling. Encrypted information received can be decrypted and decoded subsequently using a private key. Histogram analysis, Key sensitivity analysis, Correlation analysis and Entropy analysis are used to analyze the performance of the encryption technique.

Keywords: *cryptography, elliptic curve, image encryption, performance analysis, point multiplication.*

I. INTRODUCTION

The word “Cryptography” was derived from the Greek. Where the word ‘crypto’ means “secret” and ‘graphy’ means “writing” and literally ‘Cryptography’ means “secret writing”. In general, the science of keeping information secured is known as Cryptography. Depending on the key, cryptography will be classified into two types: Secret or Symmetric key cryptography and Public key cryptography. If both the receiver and the sender uses same key, then the system is called as Secret key cryptography. If receiver and sender uses altering keys, then the system is called as Public or asymmetric key cryptography.

Elliptical curve cryptography (ECC) uses private and public keys for encryption and also for decryption. It is a Public key cryptographic procedure, which was firstly introduced by Victor Miller and Neal Koblitz [1]. It. Each user will have a public key, It can be known publicly and a private key, which will be kept as a secret. By using the mathematical equations, private and public key [2] are generated. With the help of a public key, encryption will be performed and decryption can be performed by using a private key. Since the exchange of keys is not mandatory, ECC key administration reduces to a minimum level supports non-repudiation and considered to be highly secure.

II. LITERATURE SURVEY

Depending upon the properties of matrices, Amounas *et al*, explained a different mapping method for ECC. But this technique is limited only for numeric characters. An additional mapping process by Amounas [4] is correspondingly based on the matrices. Rao *et al*, [5] applied two mapping methods, where static mapping method is weak and dynamic mapping method is very difficult to decode. Fang *et al*, [6] and Padma *et al*, [7] suggested an algorithm for ECC to encrypt text messages. They completely explained and implemented the encryption of text messages, but they haven’t analyzed the performance of ECC encryption. Gupta *et al*, [8] doesn’t encrypted any images using ECC, but applied ECC to scramble only the key which is an important factor for encrypting the images. By using code computing, the image was encrypted. Garcia *et al*, [9] have evaluated the performance on Advanced

Encryption Standard (AES). But there are no performance measures for ECC in earlier works. In this paper, an ECC algorithm is implemented to encrypt a gray image and the novel performance measurement techniques for analyzing the performance of ECC encryption are proposed.

III. MATHEMATICS OF ECC

Elliptic curves are cubic curves (not in the form of ellipses) of the form **E**p (*a*, *b*): □= □+*ax*+ *b)* mod *p*, ECC involves mathematical operations [7] such as point multiplication, point doubling, point addition, and point subtraction for encrypting data.

A. ECC Point Doubling and Point Addition

Point doubling and Point addition are the important mathematical operations used in ECC. For two points A(,), B(□, □) which are mapped onto the elliptic curve, 'C(□, □)' can be calculated using the formula

□= □- - □ ,
□= (- □)-
Where = □-)/(□-), if A B
= (3 □+*a*)/2 , if A = B

Point Subtraction

Another mathematical operation which helps in the decryption process of ECC is point subtraction. It simply depends on point addition.

Here, subtraction [A-A] addition [A+(-A)]; Where, A = A(x, y); the negative point -A = A(x, -y) *C. Point Multiplication*

By performing a series of point doubling and addition operations, we can obtain Point multiplication . For the point A over the elliptic curve, elliptic scalar multiplication *j**A can be done by adding point A to itself *j* times, where *d* is an integer.

Q = *j**A = A+A+....+A. (*j* times addition)

Consider an example, 3A = A + A + A = 2A + A, where A + A can be done with the help of point double operation and the point P is added to the outcome of point doubling operation using point addition.

IV. ALGORITHM OF ECC

In this section, this paper explains how a gray image can be encrypted using elliptical curve cryptography. In general, an elliptic curve will be represented by the fixed points labeled by the equation:

A. Key Generation

ECC has a private key and a public key which provides securability to the next level. The elliptical curve equation ECC has a private key and a public key which provides securability to the next level. The elliptical curve equation used in this paper for encryption is □□*(-1, 0):* □________________________________=______________________________ □-*x* mod 89, where *a* = -1, *b* = 0, *p* = 89

which was taken from Fang *et al*, [7] Random integer □ is a private key chosen from {1,...,*l*-1}, To generate these keys, the following parameters are required for an elliptical curve cryptographic algorithm

□ Prime value *p*.
□ Elliptic curve's Order *l*.
□ Cofactor .
□ Generator *g*, which can be calculated using Particular pixel point and Cofactor.

B. Mapping Pixel values into Points over an Elliptical Curve

To encrypt the grayscale image using elliptical curve cryptography, each pixel value of the particular image are mapped onto elliptic curve point as‡□ A‡□ =(X‡□, Y‡□). The process of mapping pixel values into points of an elliptic curve is described below.

□ Choose an integer *d* from the interval [30, 50], now continuously work out *x = { *d)+v, v = 0,1,…,d-1}* when *(□+ax+b)* mod *p* will be the perfect square of the integer.

□ Attain the point P‡□ over an elliptical curve, equivalent to pixel value of the gray image as

‡□ A‡□ = (*x* mod *p*, (ξ ʻ *)* mod *p*)

Suppose the pixel value of an image is 26, taking *d* = 30, Where *v* equal to 9, we obtain *x* = 789. By substituting *x* value in the elliptical equation, □ = □-*x* = 491168280, □ mod *89* = 64, *y* = 8; we get A‡□ = (789 mod 89, 8) = (77, 8).

C. Encryption Using ECC

The purpose of encryption is to renovate a plain data into a cipher data, the encryption process of ECC will be described below.

□ Select an integer randomly from {1,...,*l*-1}, calculate the point = *g, where is kept as secret.

□ Now work out the point □ = * □*g), here □*g) is the receivers public key.

□ Obtain the point □ = (š , ›)+ □.

□ The encrypted data { , □} transmitted is the cipher data received by the receiver

D. Decryption Using ECC

The set of two points, {(, □)} is the encrypted data received by the receiver, where, = *g, □ = (š , ›)+

□.

○ The receiver computes

□-

□* ,

where □ is the private key of the receiver.

□-
□*

=

(š , ›
)+

□-
□*

=

(š , ›)+ * □*g) - □* *g)

=

(š , ›)

V. IMPLEMENTATION OF IMAGE ENCRYPTION

ECC Encryption can only encrypt points on the curve, not messages. In general, every image is a combination of pixels. In ECC, every pixel of an image should be taken as an individual message and plotted onto the point over a pre-defined elliptic curve for further encryption.

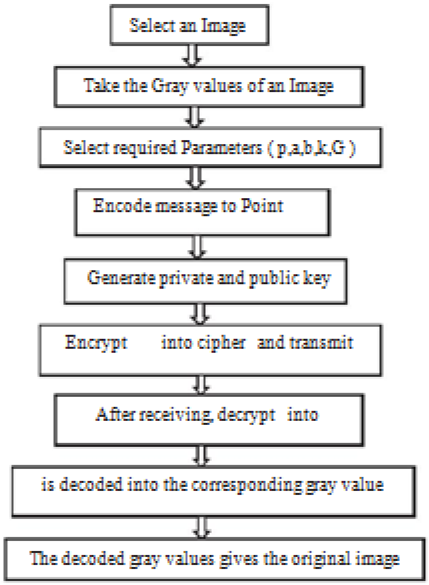

Select an Image
Take the Gray values of an Image
Select required Parameters (p,a,b,k,G)
Encode message to Point
Generate private and public key
Encrypt into cipher and transmit
After receiving, decrypt into
is decoded into the corresponding gray value
The decoded gray values gives the original image

Figure 1. Flowchart of ECC Algorithm

In this section, the pixel value of 26 is implemented using ECC. Mapping of pixel value onto the point over elliptic curve has been explained in section 3.2. For the pixel value of an image *e* = 26, the mapping point is = (77, 8). In order to encrypt this point, one should know the elliptical curve's order N by means of algorithm developed by Schoof [10]. The elliptic curve □□(-1, 0): □= □-*x* mod 89 which is used for encryption in this paper has order N = 80.

By selecting the order as a prime number over an elliptic curve, a point A(68, 4) is chosen, we calculate *l*P, for each divisor *l* of N, we get 1, 2, 4, 5, 8, 10, 16, 20, 40, 80.

Based on the point A(68, 4) the order will be the smallest *l* which satisfies *l*P = O(λ , λ), where 1A = (68, 4), 2A = (21, 42), 3A = (21, 47), 4A = (68, 85), 5A = O(λ , λ), we get order *l* = 5. Co-factor can be calculated by = N/*l* = 80/5 = 16. Point A(12,5) of an elliptical equation is taken randomly, which satisfies A O(λ , λ). We get the generator point *g* = *A = 16A = 16(12, 5) = (68, 85) by having values of order and cofactor as 5 and 16 respectively ,

Choose secret integer = 2 for encryption *and* □=3 as receivers private key from {1,…,*l*-1}, the receivers public key will be obtained as □*g = 3(68, 85) = (21, 42) as.

After mapping all the pixels onto the points over an elliptical curve, these points are to be encrypted using the receiver's public key. For encrypting a point on an elliptic curve results a set of two points {P1, P3}.

Where,

= *G = 2(68, 85) = (21, 47),

□ = * □*G) = 2(21, 42) = (68, 85)

□ =

+

□ =

+(68, 85)
(

□ can be calculated by using point addition operation between

□ and the message point

).

Therefore, the encrypted points for the message point

= (77, 8) is {(21, 47), (15, 45)}. Where the first point

is equivalent for all pixels, whereas the second point

□ varies for every pixel. Here, the encrypted points are calculated for pixel value 26. Likewise, all the pixels of the image should be encrypted. After encrypting all the pixels, the final step is releasing the encrypted points as an image.

VI. PERFORMANCE ANALYSIS OF IMAGE ENCRYPTION

To define whether the encryption system is secure or not, one should perform some analysis. There are different analysis techniques available for measuring the performance of the encrypted image. Some performance analyses on the proposed algorithm were implemented and analyzed using MATLAB [11] on a PC with Intel Core i3 processor, 4 GB of RAM and a 64-Bit Operating System. In this paper, Performance analysis was done on Lena - a common gray image in BMP format and Cameraman - a common gray image in TIF format.

A. Analysis of Histogram

Histogram is a graphical representation of pixels scattering at each grey level of an image. If the image is not completely changed after encryption, one can easily determine the nature (for example, whether it is a cartoon or not) of an image just by observing its histogram. If we observe Figure 2 and Figure 3, the histograms of Lena and Cameraman images, before and after encryption are strictly varied.

B. Correlation Analysis

In every image, two neighboring pixels are toughly correlated horizontally, diagonally and vertically. This is the property of an ordinary image. If there is no correlation between adjacent pixels for the encrypted image, one can easily ensure that the encryption technique is strong. Figure 5 and Figure 6 shows the Correlation distributions plotted for plain and encrypted images. The correlation values of diagonal, vertical, and horizontal adjacent pixels for original images are tabulated in Table I and Table III. There is no correlation between adjacent pixels for the encrypted images, which proves the strength of the encryption technique.

Correlation coefficient = $\frac{\sigma \quad \sigma \quad \sigma}{}$

σ□ σ □ σ□ σ □

C. Entropy Analysis

In performance analysis of an image encryption, entropy is an important parameter which measures the average information. The entropy value of an encrypted image which is lowest to ~0 has an arbitrary information. If the entropy is exactly zero for an encrypted image, then the encryption system is said to be extremely reliable. If we observe Table II, entropy values for both Cameraman and Moon images after encryption is exactly zero. This analysis also proves that the encryption algorithm is very strong.

Entropy = -σ □

Where P contains the normalized histogram counts returned from the histogram.

D. Key Sensitivity Analysis

The encryption algorithm which is completely sensitive to the secret key is called as the best secure encryption algorithm. This means that even the slight changes in the secret key cannot decrypt the encrypted image. The decryption results using a correct secret key and an incorrect key is illustrated in Figure 4. It proves that the encrypted technique is strong and resistant to brute-force attacks.

VII. RESULTS AND DISCUSSIONS

In this section, the performance Analysis done on both Lena and Cameraman images, before and after encryption are figured and tabulated below.

Table i. correlation values for plain and encrypted lena image

Correlation	**Lena Image**	**Encrypted Lena Image**
Horizontal correlation	TGↄ˛ TGTTT T TGↄ˛T TGTTT	TT TGT
Vertical correlation	TGↄ˛ TGTTT ↄↄ TGↄ˛ↄↄ TGTTT	TT TGT
Diagonal correlation	TGↄ TGTTT TИ TGↄ TИ TGTTT	TT TGT

By observing Table I and III, the correlation values for the Lena and cameraman (original) images is ~1. It shows the relationship between adjacent pixels is high. However, the correlation for the encrypted images is 0, meaning that there is no correlation between neighboring pixels. Therefore, it is hard to predict the values of adjacent pixels which makes the image is more secured.

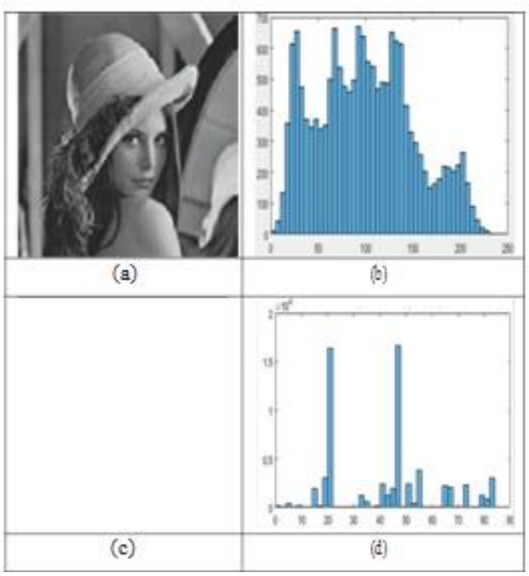


Figure 2. (a) Lena image (b) and its histogram (c) Encrypted Lena image (d) and its histogram.

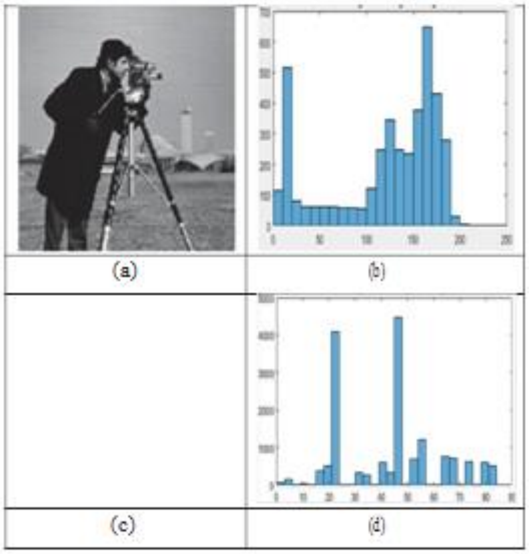


Figure 3. (a) Cameraman image (b) and its histogram (c) Encrypted Cameraman image (d) and its histogram.

Figures 2(c) and 3(c) are the images encrypted using ECC algorithm which are completely different from the original images. Likewise, the histograms of the original and the encrypted images are entirely different, So that no one can predict the image by observing histogram of an encrypted image.

In Table II, the entropy values for both Lena and cameraman (original) images is ~8, where it has a high rate of information For the encrypted images using ECC, there will be no information exists in it as its entropy is exactly ‘0’.

Table II. entropy values for plain image and encrypted images of cameraman and moon.

Image	Entropy

Cameraman Image	7.0097
Encrypted Cameraman Image	0.0000
Lena Image	7.6246
Encrypted Moon Image	0.0000

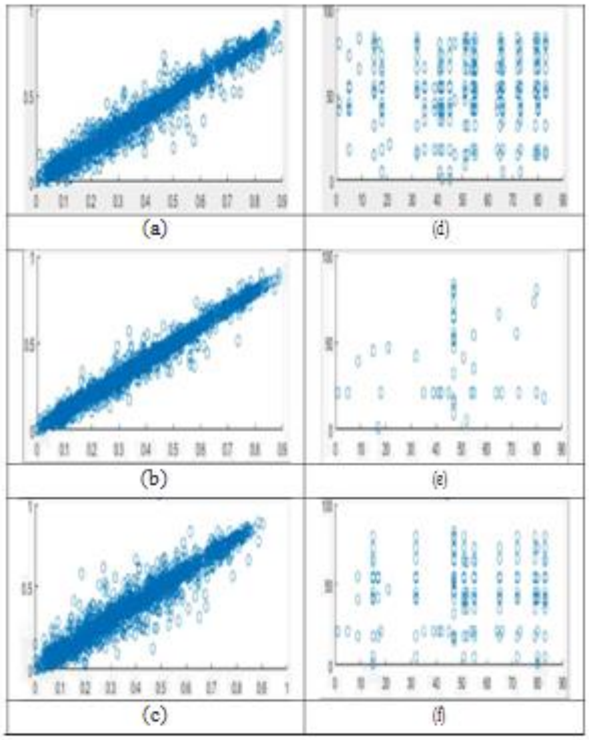


Figure 4. Correlation among the two neighboring pixels in the location of (a)Horizontal, (b) Vertical, (c) Diagonal in Lena image and (d) Horizontal, (e) Vertical, (f) Diagonal in Encrypted Lena image.

Table III. plain and encrypted cameraman image correlation values.

Correlation Type	Cameraman Image	Encrypted Cameraman Image
Horizontal correlation	TGɔˏ TGTTT ˏи TGTT TGɔˏˏи T	TT TGT
Vertical correlation	TGɔ TGTTT иɔˊ TGTT TGɔиɔˊ T	TT TGT
Diagonal	TGTTT TGɔ	TT

ISSN 2348 – 8034
Impact Factor- 5.070

correlation	TGɔT	T TGTT T	TGT

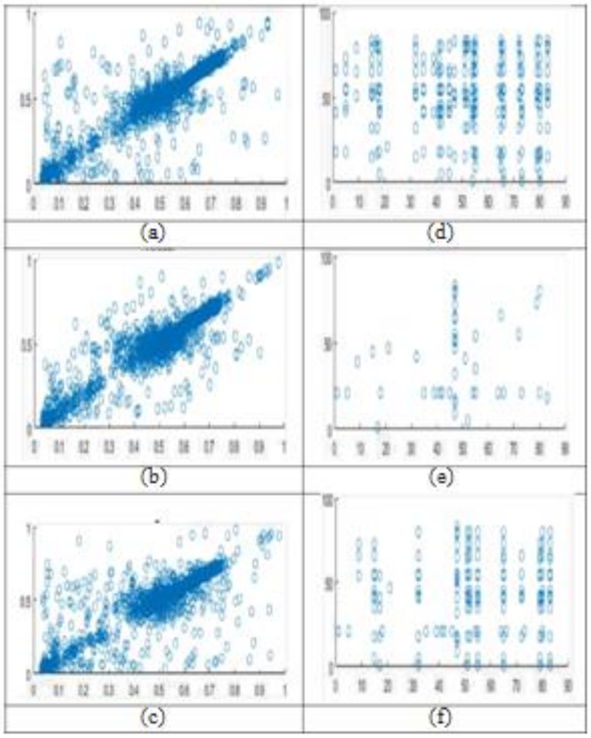
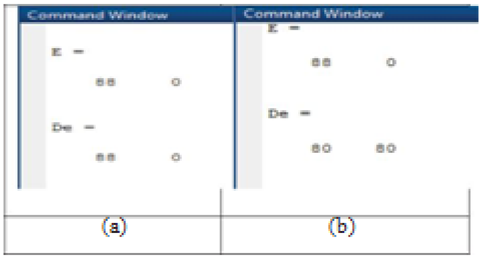


Figure 5. Correlation among the two neighboring pixels in the location of (a) Horizontal, (b) Vertical, (c) Diagonal in Cameraman image and (d) Horizontal, (e) Vertical, (f) Diagonal in Encrypted Cameraman image.

The correlation of horizontal, vertical and diagonal adjacent pixels for original images are allocated in Figure 5(a), 5(b), 5(c), 6(a), 6(b) and 6(c). Whereas the encrypted images are allocated in Figure 5(d), 5(e), 5(f), 6(d), 6(e) and 6(f) respectively. The correlation spotted in the above figures shows that the there is no related information between original and encrypted images.



```
E =

     88     0

De =

     88     0
```

```
E =

     88     0

De =

     80    80
```

Figure 6. (a) Decrypted result with correct secret key k=2, (b) Decrypted result with incorrect key k=3.

Changing the key value slightly results in different points which are spotted in Figure 4. By which the data cannot be decrypted and proves that the encryption technique is strong.

VIII. CONCLUSION

With respect to the smaller key size, Elliptical Curve Cryptography offers high-level security, which is exactly a new public or asymmetric key cryptographic method. This paper provides the elementary knowledge to recognize how the elliptic curve cryptography works, likewise, illustrates how the pixel values of a gray image are mapped onto the points over an elliptic curve. This is fast algorithm, has low complication and computation is easy to implement for numerous of points over an elliptic curve. The detailed illustration of ECC encryption algorithm is implemented with an example in this study and Performance analysis on encrypted images proved the strength of the encryption scheme and its robustness to statistical attacks

REFERENCES

1. *N. Koblitz, "Elliptic curve cryptosystems", Mathematics of Computation, AMS, vol. 48, no.177, pp. 203-208, 1987.*
2. *IEEE Standard Specifications for Public-Key Cryptography," in IEEE Std 1363-2000 , vol., no., pp.1-228, Aug. 29 2000.*
3. *F. Amounas and E.H.E. Kinani, "Fast mapping method based on matrix approach for elliptic curve cryptography", Int. J. Inform. Netw. Sec., vol.1, no.2, pp. 54-59, 2012.*
4. *F. Amounas and E.H.E. Kinani, "An efficient elliptic curve cryptography protocol based on matrices", Int. J. Eng. Invent., vol.1, no.9, pp. 49-54, 2012.*
5. *O.S. Rao and S.P. Setty, "Efficient mapping method for elliptic curve cryptosystems", Int. J. Eng. Sci. Tech., vol. 2, pp. 3651-3656, 2010.*
6. *X. Fang and Y. Wu, "Investigation into the elliptic curve cryptography," 2017 3rd International Conference on Information Management (ICIM), Chengdu, 2017, pp. 412-415.*
7. *B. Padma, D. Chandravathi and P. Roja, "Encoding and decoding of a message in the implementation of elliptic curve cryptography using koblitz's method", Int. J. Comput. Sci. Eng., vol. 2, no. 5, pp. 1904-1907, 2010.*
8. *Gupta, Kamlesh & Silakari, Sanjay & , Rjit & Academy, Bsf & , Tekanpur & P Gwalior, M & , India. (0002). EFFICIENT IMAGE ENCRYPTION USING MRF AND ECC. International Journal of Information Technology and Knowledge Management. 2. 245-248.*
9. *D. F. García, "Performance Evaluation of Advanced Encryption Standard Algorithm," 2015 Second International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), Sliema, 2015, pp. 247-252.*
10. *R. Schoof. Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p. Mathematics of Computation, Springer-Verlag Vol. 44, No.170, pp. 483-494, April 85.*
11. *MATLAB Summary and Tutorial, https://math.ufl.edu/help/matlab-tutorial/matlab-tutorial.html.*