International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 3, Issue 11 (June 2014) PP: 8-16

Security Enhancement of Image Encryption Based on Matrix Approach using Elliptic Curve

F. Amounas[1] and E.H. El Kinani[2],
[1, 2] *(R.O.I Group, Computer Sciences Department, A.A Group, Mathematical Department, Moulay Ismaïl University, Faculty of Sciences and Technics, Errachidia, Morocco)*

Abstract: *Encryption is used to securely transmit data in open networks. Each type of data has its own features. With the rapid growth of internet, security of digital images has become more and more important. Therefore different techniques should be used to protect confidential image data from unauthorized access. In this paper an encryption technique based on elliptic curves for securing images to transmit over public channels will be proposed. Encryption and decryption process are given in details with an example. The comparative study of the proposed scheme and the existing scheme is made. Our proposed algorithm is aimed at better encryption of all types of images even ones with uniform background and makes the image encryption scheme more secure. The output encrypted images reveal that the proposed method is robust.*

Keywords: *Image Encryption, Elliptic Curve Cryptography, Involutory Matrix, Elliptic Curve Discrete Logarithm Problem, Mapping technique.*

I. INTRODUCTION

With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various networks. And therefore, with rapid evolution of internet, confidentiality of digital images has become prime concern.

Multimedia data including video, audio, images, etc form large files, thus making their transmission difficult. But, with rapid growth of internet large multimedia files are easily transmitted over networks. Research work on image encryption methods has become prime concern and has attracted attention recently. But, the problem identified in this route is, that most of the available encryption algorithms are used for text data. Though, the multimedia storage and transmission also needs to be protected against unauthorised duplication and consumption, and, unauthorized disclosure and misuse. There by, posing a need of good encryption technique ensuring users privacy and copyright ownership. Many different image encryption methods have been proposed to enhance digital image security. Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one.

In the literature, there are two major groups of image encryption algorithms: (a) non-chaos selective methods and (b) chaos-based selective or non-selective methods. Most of these algorithms are designed for a specific image format compressed or uncompressed, and some of them are even format compliant. In [1], the authors have studied the encryption and decryption of the text with simple example and the work is extended to the image applications. In [2], Megha Kolhekar and al. have studied application of elliptic curves over finite fields for traditional key exchange and encryption of text. It has implemented the proposed scheme for encryption of images. In [3], G. Zhu et al. have tried to encrypt an image by scrambling pixels and then adding a watermark to scrambled image. Then, they encrypted scrambling parameters using ECC. In our previous works [4], [5] and [6], we have proposed cryptographic algorithm for text encryption using elliptic curve. We also described how to combine steganography with cryptography using Amazigh alphabet [7].

The main motivation of this work is to propose a novel encryption algorithm to encrypt an image based elliptic curve. The most important phase in encryption based ECC is transformation algorithm using mapping technique. The paper is organized as follows: the basic concept of elliptic curve is outlined in section 2. Section 3 discusses about the involutory matrix. In section 4, the proposed method is explained in detail. Section 5 presents the implementation with an example. Experimental results are discussed in section 6. Finally, section 7 describes the concluding remarks.

II. MATHEMATICAL BACKGROUND OF ELLIPTIC CURVE

The elliptic curves are not the same as an ellipse. They are named so because they are described by cubic equations. An elliptic curve may be defined as a set of points on the coordinate planes, satisfying the equation of the form,

$$E: y^2 = x^3 + ax + b \mod p, \tag{1}$$

(where $p \neq 2, 3$ is a prime number).

2.1. Curve Operations

The crucial property of an elliptic curve is that, the resultant point obtained by adding two points on the curve is also on the curve. The addition rule satisfies the normal properties of addition. If $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are points on the elliptic curve, the addition rule has the form:

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3) \tag{2}$$

where

$$x_3 = t^2 - x_1 - x_2 \mod (p) \tag{3}$$

$$y_3 = t(x_1 - x_3) - y_1 \mod (p) \tag{4}$$

with

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

It is know that rational points form an additive group in the addition over the elliptic curve shown in the following figure:

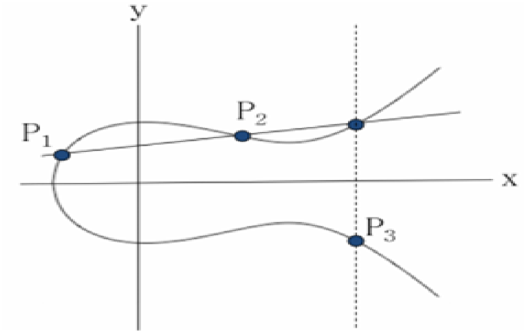


Figure 1. Addition of points on elliptic curve

Multiplication λP over an elliptic group is computed by repeating the addition operation λ times by (3) and (4). The strength of an ECC cryptosystem is depends on difficulty of finding the number of times that P is added to itself to get λP. Reverse operation known as Elliptic Curve Discrete Logarithm Problem (ECDLP).

2.2. Discrete Logarithm Problem on Elliptic Curve (ECDLP)

ECC is based on the discrete logarithm problem applied to elliptic curves over a finite field [8]. More precisely, for an elliptic curve E, it relies on the fact that it is easy to compute $Q = \lambda P$, for λ in F_p and P, Q in E. However there is currently no known sub exponential algorithm to compute λ given P and Q. In fact the discrete logarithm problem can be used to build cryptosystems with finite Abelian group. Indeed multiplicative groups in a finite field were originally proposed. In fact, the difficulty of the problem depends on the group, and at present, the problem in elliptic curve groups is orders of magnitude harder than the same problem in a multiplicative group of a finite field. This feature is a main strength of elliptic curve cryptosystems.

III. INVOLUTORY KEY MATRIX

In the literature, the various proposed methods can be found, some of them in [9, 10]. One of the methods is explained below. A is called involutory matrix if $A = A^{-1}$. In our case, we generate the involutory key matrix with elements are integers values that are the residus of modulo arithmetic of a number. This algorithm can generate involutory matrices of order (n×n) where n is even. Let A be an (n×n) involutory matrix partitioned to four sub-matrix noted A_{11}, A_{12}, A_{21} and A_{22}.

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ & \dots & & \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{pmatrix}$$

where A_{ij} is a matrix of $(\frac{n}{2} \times \frac{n}{2})$ order.

So that, $A_{12}A_{21} = I - A_{11}^2 = (I - A_{11})(I + A_{11})$.

If A_{12} is one of the factors of $(I - A_{11}^2)$, then A_{21} is the other. Solving the second matrix equation results $A_{11}+A_{22} = 0$, then form the matrix.

The algorithm is given below:

1. Select any arbitrary matrix A_{22} of $(\frac{n}{2} \times \frac{n}{2})$ order.
2. Obtain $A_{11} = -A_{22}$.
3. Take $A_{12} = \alpha (I - A_{11})$ or $\alpha (I + A_{11})$ where α is a non-vanishing number ($\alpha \neq 0$).
4. Then $A_{21} = \frac{1}{\alpha} (I + A_{11})$ or $\frac{1}{\alpha} (I - A_{11})$.
5. Form the matrix completely.

The proposed method uses an involutory key matrix for encryption process.

IV. MAIN RESULTS

4.1. Proposed Method

The common feature of our previous works [11, 12], is the use of ECC mechanism for text encryption based matrix approach. Here, we extend this approach to encrypt image using transformation Algorithm.

Every image consists of pixels. In gray scale images each pixel has an 8-bit value between 0 and 255. In color images each pixel defined by three 8-bit values separately demonstrate the Red, Green and Blue intensity. To encrypt an image using ECC, each pixel is considered as a point on elliptic curve.

4.1.1. Transformation Algorithm

In this paper, proposed mapping technique is based on transformation process that works as follows:

To define the map matrix, the elliptic group E_p (a, b) which is all possible points on the finite field are generated first and then the original image is divided into data matrices of 8×8. The row indexes are start from 0 and end with 63 for the first matrix, from 64 to 127 for the second, … Each row stands for a pixel intensity value. Starting from the first pixel in plain image, the corresponded point with the intensity value in the matrix is mapped to this pixel and continue to the last pixel. For any matrix, 64 points are selected in such directory by following spiral technique with the first point is a secure key generated.

The generated (or transformed) image is then fed to the encryption algorithm. The main idea is that an image can be viewed as an arrangement of matrices with its elements are points on elliptic curve.

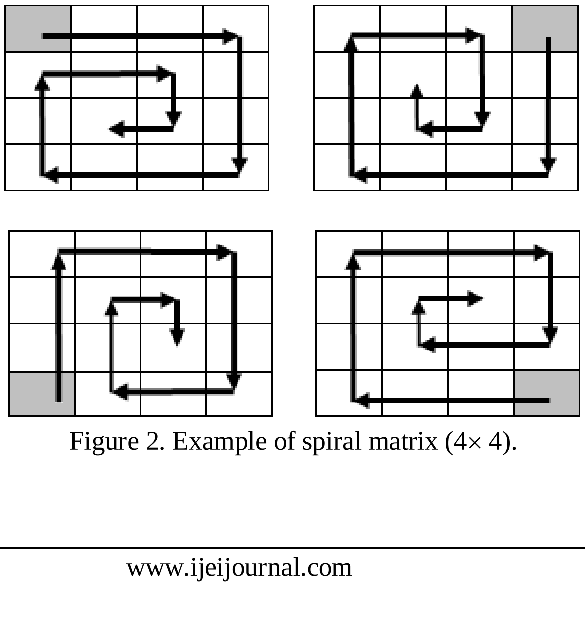


Figure 2. Example of spiral matrix (4× 4).

The overview model of the proposed method using elliptic curve based Transformation Algorithm is shown in Figure 3.

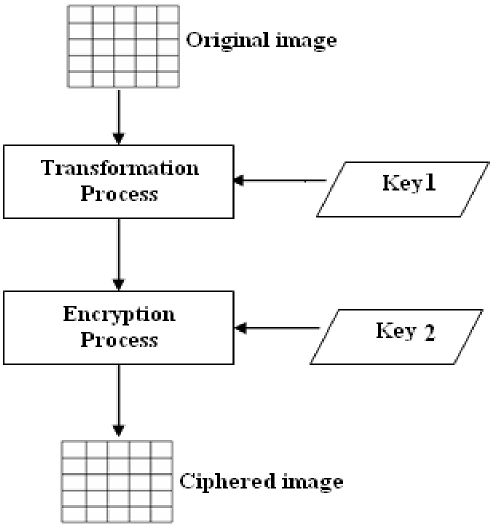


Figure 3.An overview diagram of the proposed method.

4.1.2. Encryption Algorithm

The output of the transformation process is served as input to the encryption algorithm. Image encryption procedure is discussed below.

Suppose that we have some elliptic curve E defined over a finite field F_p and a point P on E (F_p) that P has prime order N. The curve E and P are publicly known, as is the embedding system $m \rightarrow P_m$ which imbed intensity values on an elliptic curve E. Bob chooses a random integer n_B, and publishes the point $P_B = n_BP$ (while n_B remains secret).

Then when Alice wishes to encrypt an image and send it to Bob, she proceeds thus:

Step 1. Chooses a random integer k with $1 \leq k \leq N$ and compute $R = kP_B$.

Step 2. Imbed the original image into points on elliptic curve using the transformation algorithm.

Then, the plain image is divided into data matrices of n × n, noted M_i, i = 1, 2, …

$$M_i = \begin{pmatrix} P_{1,1} & P_{1,2} & \dots & P_{1,n} \\ P_{2,1} & P_{2,2} & \dots & P_{2,n} \\ & & \dots & \\ P_{n,1} & P_{n,2} & \dots & P_{n,n} \end{pmatrix}$$

where P_m is the mapping point of intensity value m.

Step 3. A involutory matrix A of n × n is constructed.

Step 4. Perform the product: $C_i = M_iA$, (i=1, 2, …) using addition and doubling points on elliptic curve.

Now, continue the same process until all pixels are crypted. The result can be represented as an image.

Step 5. The cipher text is represented by (kP, C_i) where the second part is the encrypted image.

Therefore, the cipher text is transmitted to Bob through an insecure channel.

To decrypt the received image, Bob does the following:

Step 1. Extract the first block from the received cipher text. It is mapped to find its equivalent point noted $P_1 = kP$. Then, applies his secret key and Compute $R = n_BP_1$.

Step 2. Extract the remaining blocks and stored into square matrices of (n × n).

Step 3. Generate the involutory matrix and compute M_i.

To view the encrypted points as an image, we refer to the data matrix (section 4.1.1) and find the current index according to each point.

V. ILLUSTRATION AND RESULTS

In this section, we consider the elliptic curve E_{73} (70, 57) given by the Weierstrass equation:

$$E: y^2 \bmod 73 = x^3 + 70x + 57 \bmod 73 \qquad (5)$$

The elliptic curve contains 74 points. The base point P is selected as (3, 41).
To create the data matrix, the secure key will place in the row 0 which is corresponded to pixel with intensity value of 0, and then continue next point with next value. After placing first 64 points in first matrix, next we choose another point in the first row 0, then 64 points will place in second matrix and hereafter will do the same for next points to the last. In this example, there are 74 points on the curve. These points completely fill 64 cellule of each matrix.
Hence we shall assume that $n_B = 13$, $k = 29$, $P_B = (19; 56)$, $R = (41, 69)$, for instance,
The data matrices generated is shown in Table 1.

(41, 69)	(53, 72)	…	(19,56)	(63, 67)		(44, 31)	(22, 28)	…	(58, 31)	(41, 69)
(11, 48)	(13, 5)	…	(4, 67)	(12, 17)		(23, 16)	(1, 36)	…	(6, 6)	(53, 72)
…	…	…	…	…		…	…	…	…	…
(52, 38)	(26, 20)	…	(19, 17)	(35, 7)		(12, 17)	(22, 45)	…	(58, 42)	(19,56)
(42, 17)	(64, 42)	…	(47, 15)	(60, 69)		(4, 67)	(50, 2)	…	(11, 48)	(63, 67)
(63, 67)	(11, 48)	…	(50,2)	(4, 67)		(6, 67)	(12, 17)	…	(23,16)	(44, 65)
(19, 56)	(58, 42)	…	(22, 45)	(12, 17)		(50, 2)	(22, 45)	…	(1, 36)	(22, 28)
…	…	…	…	…		…	…	…	…	…
(53, 72)	(6, 6)	…	(1, 36)	(23, 16)		(11, 48)	(58, 42)	…	(6, 6)	(58, 31)
(41, 69)	(58, 31)	…	(22, 28)	(44, 65)		(63, 67)	(19, 56)	…	(53, 72)	(41, 69)

Table 1. Data Grid generated.

To encrypt an image using this method, all pixels are mapped into points on elliptic curve using data Grid generated (Table 1). The Table 2 demonstrate some pixels intensity value of the image chosen ("Lena"), the result of mapping transformation of pixel to point on elliptic curve and the corresponding encrypted points. After encrypting all the points using involutory matrix, in order to show the encrypted points as an image, first create a matrix the same size of image, find each point in the data grid and then place the rang index in equivalent element of created matrix.

To view the encrypted points as an image, we refer to the mapping data grid and find the current Number according to each point and replace with the related value.

In our case, we use the involutory matrix given as follow:

$$A = \begin{pmatrix} 3 & 11 & 9 & 4 \\ 10 & 9 & 6 & 10 \\ 2 & 12 & 10 & 2 \\ 5 & 5 & 3 & 4 \end{pmatrix}$$

Table 2. Result of Mapping technique of pixels to points and the corresponding encrypted points.

Intensity value	130	129	193	192	194	157	158	159
Mapping point	(57, 30)	(12, 17)	(11, 48)	(63, 67)	(13, 5)	(42, 17)	(12, 56)	(55, 22)
Encrypted point	(52, 35)	(6, 6)	(19, 56)	(44, 65)	(47, 15)	(60, 69)	(62, 0)	(50, 71)

VI. EXPRIMENTAL RESULTS

This section represents the simulation results illustrating the performance of the proposed encryption algorithm. Netbeans is chosen as simulation software. Our algorithm has been validated using grayscale and color images. The results of application of our algorithm on Lena image are given in Figures (Figure 4, Figure 5, Figure 6, Figure 7).

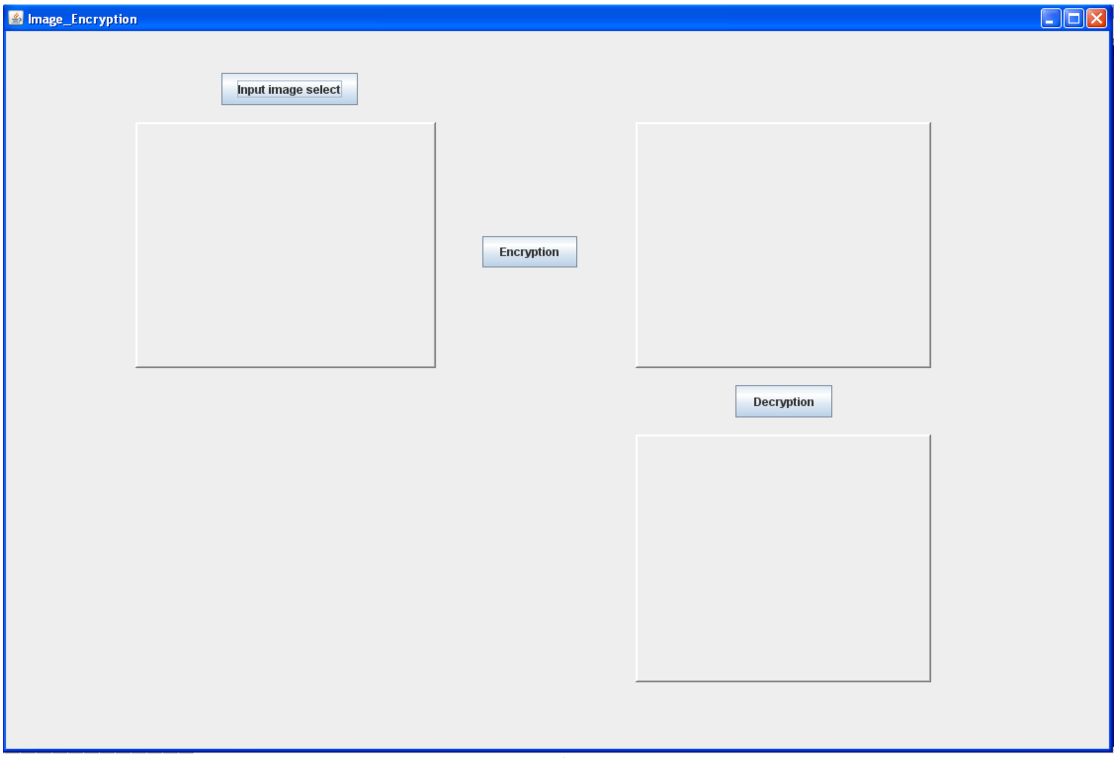
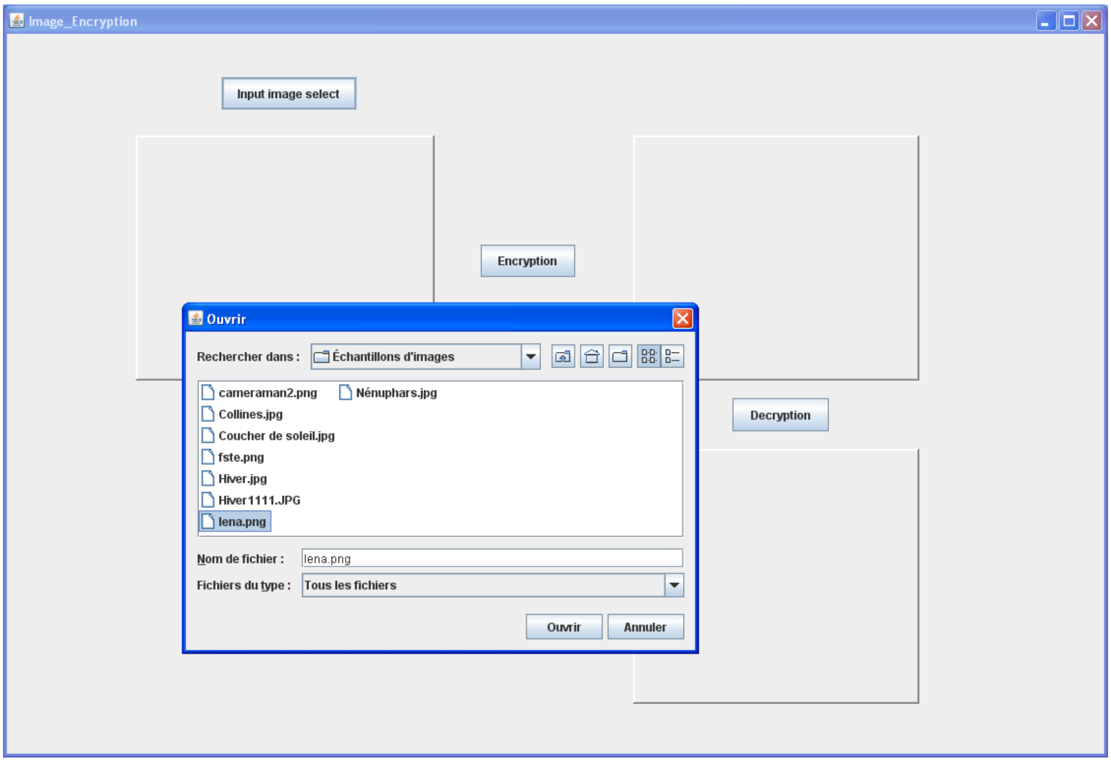


Figure 4. Layout of Proposed System



Rechercher dans : Échantillons d'images

Nom de fichier : lena.png

Fichiers du type : Tous les fichiers

Figure 5. Select Input Image

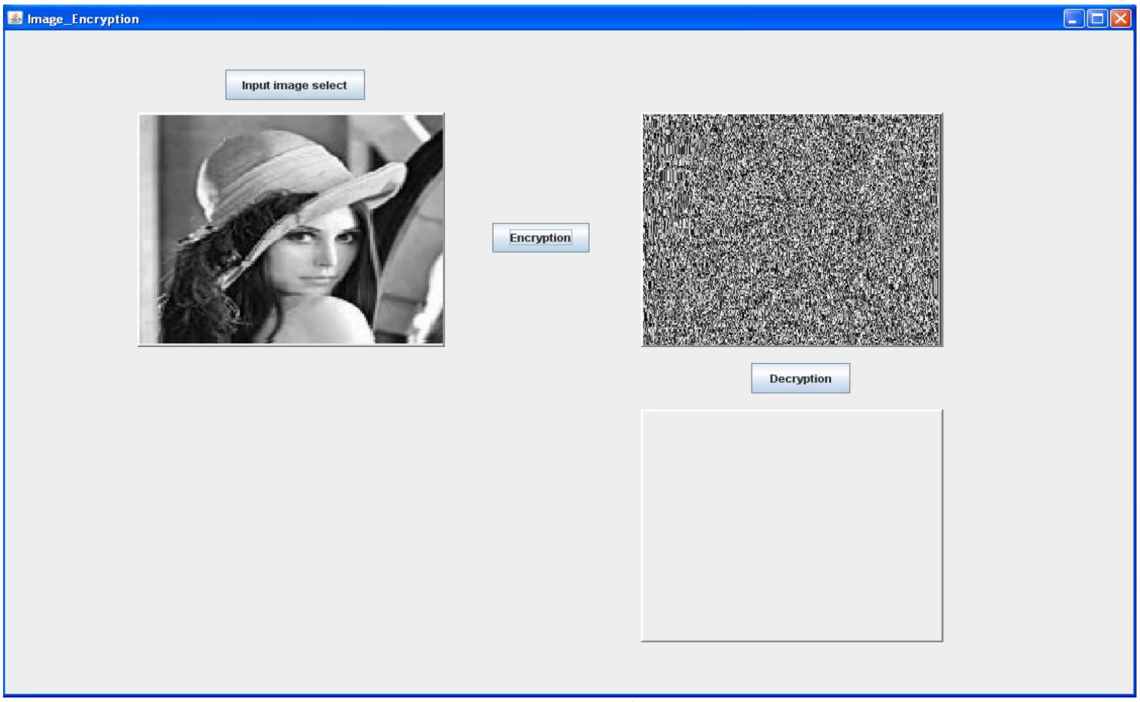


Figure 6. Encrypted Image of "Lena image".

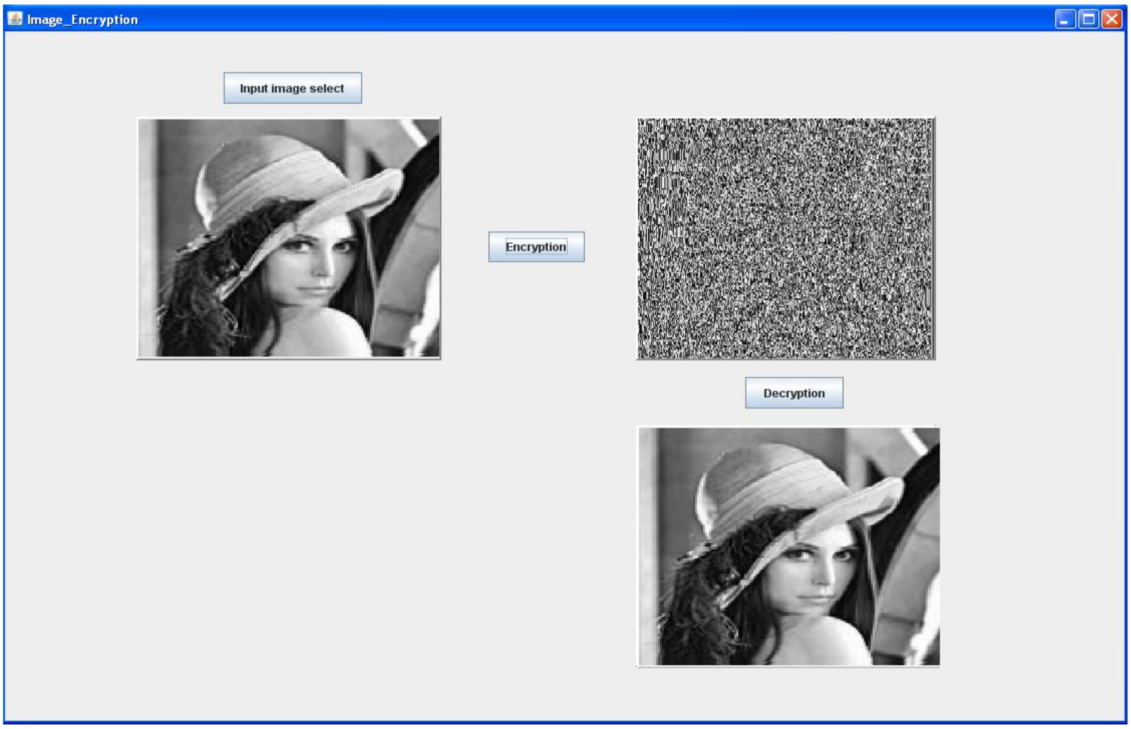


Figure 7. Decrypted Image of "Lena image".

In [13], the authors demonstrate that Hill cipher can't encrypt the image properly if the image consists of large area covered with same color and gray level. In our case, we have taken Lena image and encrypted it using the proposed algorithm. The proposed method works for any images with different gray scale as well as color images. The result in Figure 7 shows that the proposed method encrypt image properly as compared to the original Hill cipher algorithm. Moreover, this total process of image-encryption has highly time efficient, and secure, and gives a very simple and flexible approach.

The above algorithm is tested on the color image "FSTE". Figure 8 and Figure 9 show result of application of our algorithm on color image to obtain encrypted and decrypted images. Encrypted images visually appear secure enough and decryption leads to successful retrieval of original image.

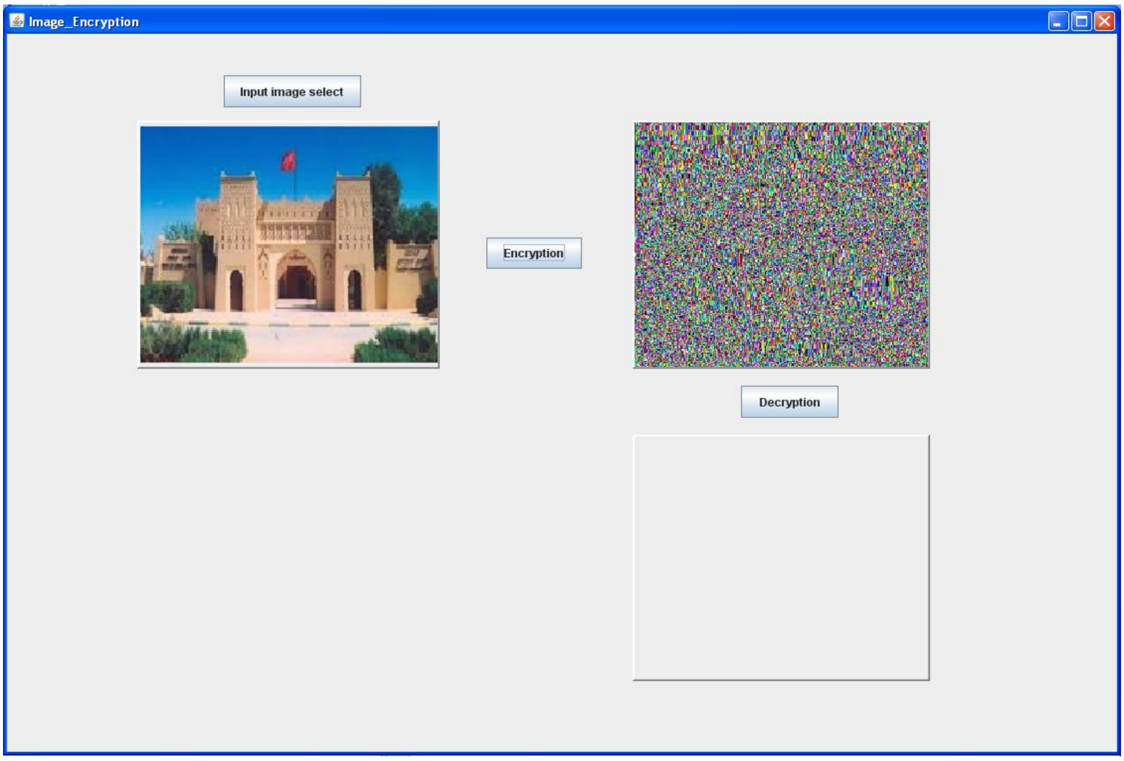


Figure 8. Encrypted Image of “FSTE image”.

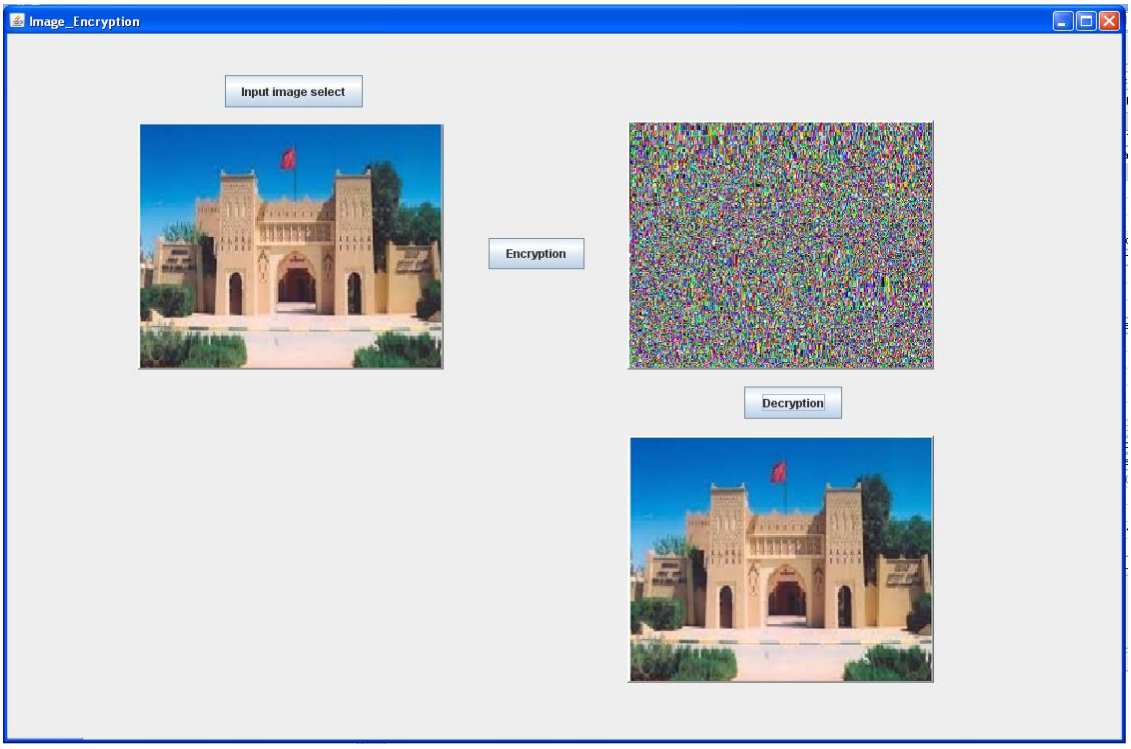


Figure 9. Decrypted Image of “FSTE image”.

VII. CONCLUSION

This paper introduced a new approach for image encryption using elliptic curve. In fact, the plain image is divided into blocks: data matrix. The proposed cryptosystem uses a different key for mapping and encryption process and the possibility of known plaintext attack is highly reduced as the key used changes with every block and it is generated randomly using transformation algorithm based ECC. In this paper a new mapping method introduced to convert an image pixel value to a point on a predefined elliptic curve over finite field F_p using transformation algorithm. This mapping technique is very fast with low complexity and computation. This technique will results a high distribution of different points for repetitive intensity values. The result shows that the proposed method is more secure to force attacks as compared to the original Hill cipher algorithm. As a future work, the proposed cryptosystem can be extended for encrypting the video messages as well as sound encryption process.

REFERENCES

[1] S.Maria Celestin Vigila1and K. Muneeswaran2,"Nonce Based Elliptic Curve Cryptosystem for Text and Image Applications," International Journal of Network Security, 2012, vol.14, No.4, PP.240-246.

[2] Megha Kolhekar and Anita Jadhav "implementation of elliptic curve cryptography on text and image", International Journal of Enterprise Computing and Business Systems, ISSN (Online): 2230-8849, 2011, vol. 1, Issue 2.

[3] G. Zhu, W. Wang, X. Zhang, and M. Wang, "Digital image encryption algorithm based on pixels," IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS), 2010, pp.769-772.

[4] F.Amounas, E.H. El Kinani and A.Chillali, "An application of discrete algorithms in asymmetric cryptography, " International Mathematical Forum, 2011, vol. 6, no. 49, pp. 2409-2418.

[5] F.Amounas and E.H. El Kinani, "Elliptic Curve Digital Signature Algorithm Using Boolean Permutation based ECC", International Journal of Information & Network Security, 2012, vol.1, No.3, pp. 216-222.

[6] F.Amounas and E.H. El Kinani, "Proposed Developments of Blind Signature Scheme based on The Elliptic Curve Discrete Logarithm Problem", Computer Engineering and Applications Journal, 2013, vol 2, No 1.

[7] H.Sadki, F.Amounas and E.H. El Kinani, "A Novel Approach of Amazigh Text Steganography based Elliptic Curve", International Journal of Information & Network Security, 2014, vol 3, No 2, pp. 83-91.

[8] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography", Designs, Codes, Cryptography, 2000, vol. 19, pp. 173-193.

[9] Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, Saroj Kumar Panigrahy. "Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm", International Journal of Security, 2007, vol 1, Issue 1, pp. 14-21.

[10] Bibhudendra Acharya, Debasish Jena, Sarat Kumar Patra and Ganapati Panda,"Invertible, Involutory and Permutation Matrix Generation Methods for Hill Cipher System", Proceedings of the 2009 International Conference on Advanced Computer Control, ICACC '09, 2009, pp. 410-414.

[11] F.Amounas and E.H. El Kinani, "An Efficient Elliptic Curve Cryptography protocol Based on Matrices", International Journal of Engineering Inventions, 2012, vol 1, Issue 9, pp. 49-54.

[12] F.Amounas and E.H. El Kinani, "Fast mapping method based on matrix approach for elliptic curve cryptography", International Journal of Information & Network Security, 2012, vol.1, No.2, pp. 54-59.

[13] Shahrokh Saeednia, " How to make the Hill cipher secure". Cryptologia, 2000, 24 (4), pp. 353-360.