International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2015)

Conference Organized by Interscience Institute of Management and Technology,
Bhubaneswar, Odisha, India

Image Encryption Using Elliptic Curve Cryptography and Matrix

*Srinivasan nagaraj                             Dr.G.S.V.P.RAJU          *K.Koteswara rao

*Asst.Professor Dept.of CSE, GMRIT, Rajam. AP.   Professor , Dept, Of CS&ST Andhra Universit, Vizag-03.

Abstract

The enlarged size of the internet and vast communication across it and also medical needs digital images require of security plays vital role. So different techniques are used to protect confidential image data from unauthorized access. In this paper, we propose a New encryption technique Using elliptic curve cryptography with a magic matrix operations for securing images that transmits over a public unsecured channel. There are two most important groups of image encryption algorithms: some are non chaos-based selective methods and chaos-based selective methods. The majority of these algorithms is planned for a specific image format, compressed or uncompressed.

© 2014 The Authors. Published by Elsevier B.V.
Selection and peer-review under responsibility of scientific committee of Missouri University of Science and Technology.

Keywords: ECC, magic Matrix, encryption , decryption
1. INTRODUCTION

Cryptography Goals: The following six goals are used in cryptography:

- **Authentication**: That provides the authenticity of one entity towards permit them or not to permit accesses of resources.
- **Confidentiality**: It can be defined that the message cannot be modified by others except the authorized receiver.
- **Integrity and Non-repudiation**.
- **Availability**: Computer system assets are available to authorized parties when needed.

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

\[ Y^2 = x^3 + ax + b \]

To increase the security and make use of the magic matrix features of generating private keys and producing Elliptic Curves. This proposed system combined the elliptic curve and matrix values to seed that will be used to generate the curve against the cryptanalysis.

The generated parameters will be used in the cryptographic process such as Elliptic Curve Cryptography.

**Elliptic Curve Domain Parameters are** \( D = (q, FR, a, b, G, n) \)

- **\( q \)**: prime power, that is \( q = p \) or \( q = 2^m \), where \( p \) is a prime
- **\( FR \)**: field representation of the method used for representing field elements \( (F_q) \)
- **\( a, b \)**: field elements, they specify the equation of the elliptic curve \( E \) over \( F_q \),
  \[ y^2 = x^3 + ax + b \]
- **\( G \)**: A base point represented by \( G = (x_g, y_g) \) on \( E \) \( (F_q) \)
- **\( n \)**: Generated Prime number.

Take the secret key as the \( x \) value and calculate the \( y \) value using the ECC equation.

\[ Y^2 = x^3 + ax + b \]

From this, we get point \( x, y \) on the curve.

**Magic matrix notation:**

First circle the any number in the matrix example, 5. Then draw the line through which all the squares that lie in the same row and column for the selected number:

```
  1 3 2 1
  3 5 2 1
  1 3 2 1
  2 4 3 2
```

2. Proposed algorithm:

**Transformation Algorithm**: To define the mapping 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 x 8. The row indexes are starting from 0 and end with 63 for the first matrix, from 64 to 127 for the second and so on. 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. From that you have to choose a random pixel in plain image, that corresponded to some intensity value in the matrix and the image is then fed into the encryption algorithm.

2.1 CONSTRUCTION OF MAGIC MATRIX:
Start in the bottom right corner of the grid, and count along, but only put the numbers you count on the diagonal lines. i.e. follow the path marked out below, putting numbers on the diagonals

Next, starting at the bottom left, count backwards from 16, putting the numbers in the blank spaces.

If the image size is large we should make the images into parts and then we should represent each part as a matrix.

2.2 Encryption at A:-
Then when A wishes to encrypt an image and send it to B, the procedure thus:
Step 1. Chooses a random integer k with 1 < k ≤ N and compute S = KPb.
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 X n, noted PMj, j = 1, 2, . . . , n
Where \( P_m \) is the mapping point of intensity value \( m \).

**Step 3:** We used 4X4 magic matrix for representing the image pixels.
In case of larger image also we need to divide it into 4X4 MATRIX size in which its pixel values can be stored in magic matrix form.

**Step 4:**

\[
P_{m1} = aP_m
\]

// \( P_m \): Is random point on EC

\[
P_b = n_b \ast G
\]

// \( G \) is the base point of EC

// \( n_b \) is the private key

**Cipher Text** = \{KG; \( P_{m1} + K \ast P_b \)}

Continue the same process until all pixels are encrypted. The result can be represented as image.

**Step 5:**
The cipher text is transmitted to Bob through an insecure channel.

Let us consider the equation of the elliptic curve:

\[
y^2 \mod p = (x^3 + ax + b) \mod p
\]

Where, \( p \) is a prime number.

Algorithm:
Inputs: \( p, a, b \)

a. Enter the input data.

b. \( x = [0: p-1] \)

c. For each value of \( x \), check which values of \( y \) from 0 to \( p-1 \) satisfies the equation.

d. Display the required point.

**For example:** \( p=231, a=1, b=3 \)

**Table a: Elliptic curve points:**

| Database | \( X \) | \( Y \) |
|----------|--------|--------|
| 1        | 18     | 78     |
| 2        | 12     | 84     |
| 3        | 11     | 50     |
| 4        | 26     | 7      |
| 5        | 5      | 56     |
| 6        | 6      | 15     |
| 7        | 27     | 78     |
| 8        | 32     | 1      |
| 9        | 33     | 105    |
| 10       | 39     | 15     |
| 11       | 47     | 77     |

**2.3 Decryption at B:**

Let \( KG \) be the first point and \( P_{m1} + K \ast P_b \) be the second point

\( n_b \ast KG = n_b \ast \) first point;

Compute the \( P_{m1} = P_{m1} + KP_b - n_b \ast KG \); Calculate the \( P_m \) value from \( P_{m1} \) using discrete Logarithm.
3 EXPERIMENTAL RESULTS:

Fig.1: Encryption of the image

Fig.2: Decryption of the image

CONCLUSION: The performance of the proposed algorithm is good security and it was implemented in DOTNET as the simulation software. In future, it can be enhanced by making this method compatible to encrypt multimedia data which have to be transmitted securely over unsecured channels. In the future, security provided by Biometric Encryption will be merged with this approach which undoubtedly help to promote more widespread use of cryptographic systems. This proposed algorithm has been implemented grayscale images.

REFERENCES

[1] S. Maria Celestin Vigila1 and 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 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.
[10] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography", Designs, Codes, Cryptography, 2000, vol. 19, pp. 173-193