Integration of Elliptical Cryptography with RSA and Steganography using Biometric Authentication

Anjana Yadav
Department of
Electronics & Communication
Engineering
The Northcap University
Gurgaon, Haryana, 122017 India

Pankaj Rakheja
Department of
Electronics & Communication
Engineering
The Northcap University
Gurgaon, Haryana, 122017 India

ABSTRACT

Cryptography is a science of encrypting data to make it non readable and secure. But with time traditional cryptography is not that reliable because of multiple types of attacks on it. So, to make it effective it can be integrated with latest techniques available. Here in this paper a new mechanism has been proposed which integrates RSA and steganography with elliptical cryptographic technique along with biometric authentication as an addition security measure. This method provides good security with small key size too.

Keywords

Elliptic Curve Cryptography (ECC), Rivest Shamir Adleman (RSA), Biometric Encryption (BE).

1. INTRODUCTION

These days security has become a major issue in data communication. Existing modes for security are based on knowledge like Passwords, PIN and ID etc. These modes have many problems like someone can steal ID, can hack or crack passwords, and one may forget the PIN.

But by using biometric techniques these problems can be overcome because each person has his/her unique identification. Biometric based security system gives high degree of assurance.

The term cryptography defines a mathematical technique which is used to make a text or message in non-readable form. Cryptography presents a high degree of security in data communication. In most of the researches it is found that since biometric is more reliable and worldwide accepted, it is the most trustable technique for identification and authentication.

2. RELATED WORK

Elliptic curve cryptography has wide applications and has become an interesting topic to research in the field of providing a high level of security for data communication. Lot of research has done on this topic. Last year Nikita G. et al[5] proposed a method for ciphering of color images. They used NIST curves. Koblitz encoding was used to convert the matrix into points on the elliptic curve. It used two setups. First one was openCV with java and other was openCV with C++ for encryption and decryption of image using ECC. Cristian-Liviu-Leca et al[6] proposed an algorithm for point operations such as doubling, tripling, addition etc. Algorithm proposed by them gave much faster and efficient scalar multiplication. For image encryption El-din et al[9] discussed a method based on chaos as feedback stream cipher. Algorithm for symmetric key encryption based on chaos was discussed by M. Salleh et al[10] for security of images. I.A.Ismail[11]came up with a idea as chaos based stream cipher in which the key is altered after each pixel encryption of the plain image. Lifang.Wu et al[3] proposed a biometric based cryptographic key generation technique. He made use of face biometric, Principal Component Analysis (PCA), bio-key,Reed-Solomon Algorithm(RSA) and symmetric DES.

3. GENERAL TERMS

3.1 Biometric Encryption (BE)

Biometric encryption is a process of binding a digital key to a biometric or a digital key is generated from the biometric. With biometric encryption, it is not required to store any biometric image or template. It only requires to store a “biometrically encrypted key”. And this does not allow to retrieve any data i.e neither the digital key nor the biometric. By using biometric encryption, one can recreate digital key only if the right biometric sample is given on verification.

3.2 Elliptic Curves

Elliptic curves are defined by the given equation:

$$y^2 = x^3 + Ax + B \qquad (1)$$

Where x, y, A and B are defined for a specific field.

The above equation is known as Weierstrass equation for elliptic curves, and it is not for characteristic 2 or 3.

The generalised Weierstrass equation is given below and it is used for characteristic 2.

$$y^2 + d_1xy + d_3y = x^3 + d_2x^2 + d_4x + d_6 \qquad (2)$$

Group Law:

Suppose we have an elliptic curve ,E, and a point P(x_0 ,y_0) lies on this curve then the intersection between E and x=x_0 is

$$P' = (x_0 , -d_1x_0 - d_3 - y_0)$$

When characteristic is not 2 or 3 and when characteristic is 2

$$P' = (x_0 , -y_0)$$

3.2.1 Elliptic Curve Addition

We can find a third point, P_3 ,on elliptic curve if we are given two points on it say $P_1(x_1, y_1)$ and $P_2 = (x_2, y_2)$ which is given as

$$P_3 = P_1 + P_2$$

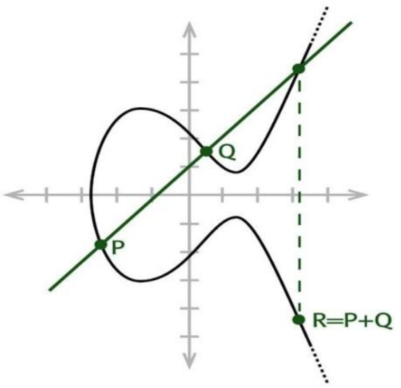


Fig 1: Elliptic Curve

A line passing through P_1 and P_2 intersects E at $P_3{}'$ and reflection of this in x-axis gives P_3 .

Now coordinates of this point P_3 can be found as follows:

Slope of line L, $y = m(x - x_1) + y_1$ is

$$m = \frac{y_2 - y_1}{x_2 - x_1} \qquad (3)$$

From Elliptic curve and line equations, we have

$$[m(x - x_1) + y_1]^2 = x^3 + Ax + B \qquad (4)$$

or

$$x^3 - m^2x^2 + \dots\dots\dots = 0 \qquad (5)$$

According to a theorem [14], negative of the coefficient of the x^2 is equal to the sum of the roots. Therefore,

$$x_3' = m^2 - x_1 - x_2$$

And $y_3' = m(x_3' - x_1) + y_1$

By reflecting $P_3{}'$ in the x-axis we will get

$$P_3 = (x_3, y_3)$$

Therefore,

$$x_3 = m^2 - x_1 - x_2$$

And

$$y_3 = m(x_1 - x_3) - y_1$$

By summarizing above ,we get three cases to find the point on Elliptic curve.

Case1: When $x_1 = x_2$ but $y_1 \neq y_2$, then the line through $P_1 and\ P_2$ is vertical, so

$$P_1 + P_2 = \infty$$

Case2: When$P_1 = P_2 = (x_1, y_1)$, then the line, L, is the tangent and slope of it is given by

$$\text{m} = \frac{3{x_1}^2 + A}{2y_1}$$

So, $P_3 = (x_3, y_3)$ is given as

$$x_3 = m^2 - 2x_1$$

$$y_3 = m(x_1 - x_3) - y_1$$

Case3: When $P_1 = P_2$ and also $y_1 = 0$ then

$$P_1 + P_2 = \infty$$

3.2.2 Prime Curve

Elliptic curves which are defined over Z_p are prime curves. In this we can reduce modulo 'p' at each stage.

We have Elliptic curve, E, equation as

$$y^2 = x^3 + Ax + B$$

We write E_p(A, B) for the set of integers (x, y) which satisfy the above equation along with a point at infinity, ∞.

3.2.3 Successive Doubling

For computing large integers, point addition technique will be not efficient, Therefore instead of point addition we use successive doubling to reduce this burden.

Algorithm for Successive Doubling

Suppose we need to calculate 'kP' , where 'P' is a point on Elliptic curve and 'k' is a positive integer. This can be done as follows

1. Set a=k ,B=∞ and C=P
2. If 'a' is even
   a = $\frac{a}{2}$, B=B and C=2C
3. If 'a' is odd
   a = a-1 , B =B+C ,C=C
4. If a ≠ 0 ,Go to step 2
5. When a = 0 ,give output B

This output, B, is 'kP'.

3.3 Elliptical Curve Cryptography (ECC)

Elliptic curve cryptography is based on elliptic curves and it is a public key cryptography. It generates smaller, faster and efficient cryptographic keys. Cryptographic keys are generated by using properties of the elliptic curve equation. A same level of security is achieved by using ECC with 164 bit key size as compared with other methods.

3.4 Fingerprint Biometric

The most well known metrics is fingerprint recognition. By comparison of two fingerprints, the identity of one can be derived. It is also accepted globally.

Fingerprint ridges have three basic patterns that are the arch, the loop and the whorl.

In arch pattern, ridge ridge enters one side of the finger then rises in the center and forms an arch and then from other side of the finger it exit.

In loop pattern, the ridge enters from one side of the finger, forms a curve and exits from the same side of the finger.

In whorl pattern, ridges form circularly around a central point.

3.5 RSA Algorithm

The Rivest-Shamir-Adleman (RSA) algorithm is the most popular asymmetric key cryptographic algorithm. According to a mathematical fact large prime numbers are easy to find and multiply but on the other hand to factor their product is very difficult. In RSA algorithm the encryption key is public and the decryption key is private.

1. Select two large prime numbers P and Q.
2. Calculate N=P×Q

3. Choose the encryption key E, as it is not a factor of (P-1)×(Q-1)
4. Decryption key D is selected in such a way that it satisfies the following equation i.e. (D×E)mod(P-1)×(Q-1)=1
5. Plaint text ,PT, is encrypted into cipher text ,CT, using encryption key E as follows: CT = PT^E mod N
6. Sender sends this cipher text ,CT, to the receiver.

By using decryption key D, receiver decrypts plain text PT, from the cipher text CT, as follows: PT =CT^D mod N.

3.6 Steganography

Do The process of hiding the message within another text or image so that the confidential data or message cannot be detectable to the casual eye.

3.6.1 Least significant bit, LSB, encoding:

It is the most popular method for encoding images. In LSB method to encode the message, least significant bit of every byte in an image is used to encode the message. This changes the value of each pixel slightly, but not as much to make major changes to the image. Human eye cannot identify these changes in the altered image even after comparing with the original image.

When steganography is combined with cryptography, it gives a high level of security.

4. PROPOSED METHODOLOGY

We proposed a method which is explained in steps as follows:

STEP 1: Sender Side

I. Sender, A, takes a 16×16 image.
II. Encrypts each pixel of the image using ECC.
III. Sends the encrypted image to the receiver B.
IV. Receiver decrypts the image.

STEP 2: Receiver Side

I. If the decrypted image is same to the original image then the receiver B sends the index of pixel intensity 1,5,9 and 13 back to A.
II. B sends the encoded image to A.

STEP 3: Sender Side

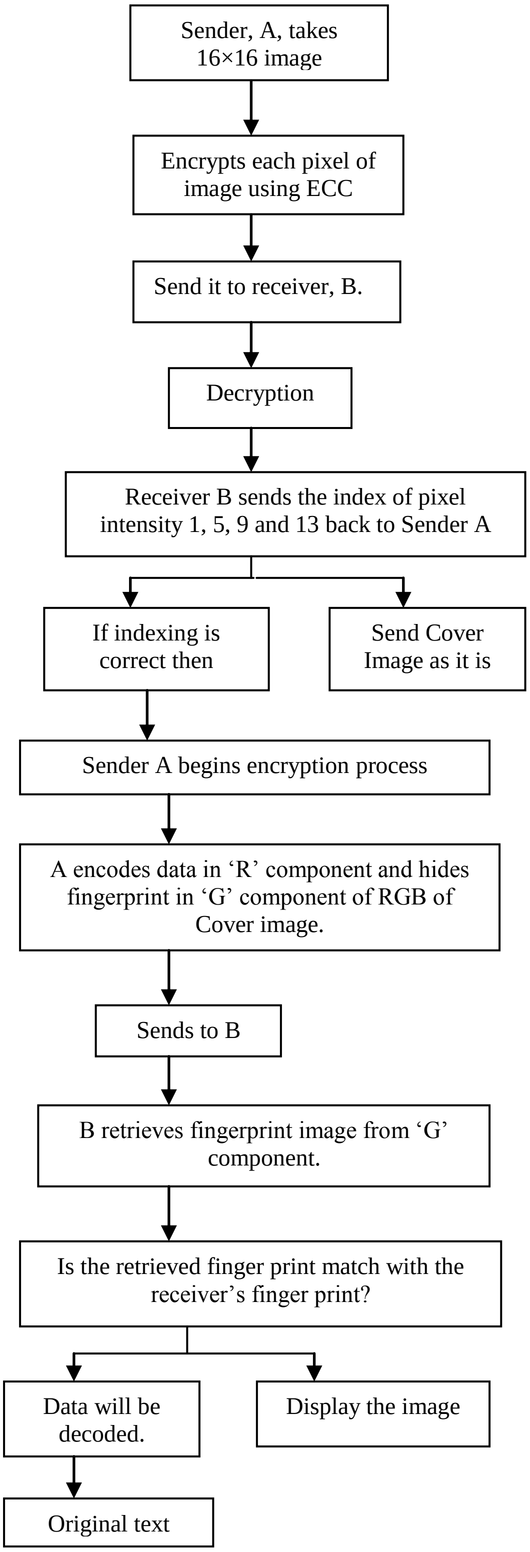
I. Now the sender A, encodes data in ‘R’ component of coloured image using RSA and hides fingerprint image of the receiver in ‘G’ component.
II. A sends the encoded image to B.

STEP 4: Receiver Side

I. B retrieves fingerprint image from ‘G’ component.
II. If the retrieved fingerprint matches with the receiver’s fingerprint, data will be decoded.

Result of decoding gives original text.

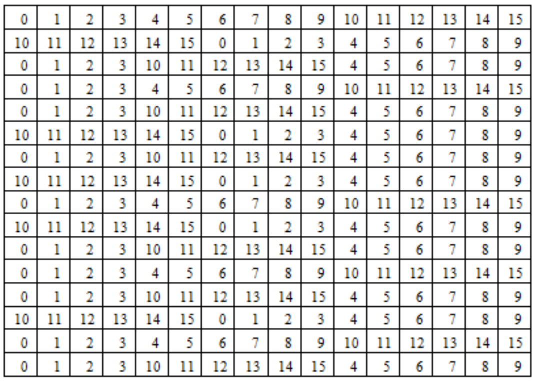
5. FLOWCHART


Sender, A, takes 16×16 image
Encrypts each pixel of image using ECC
Send it to receiver, B.
Decryption
Receiver B sends the index of pixel intensity 1, 5, 9 and 13 back to Sender A
If indexing is correct then
Send Cover Image as it is
Sender A begins encryption process
A encodes data in ‘R’ component and hides fingerprint in ‘G’ component of RGB of Cover image.
Sends to B
B retrieves fingerprint image from ‘G’ component.
Is the retrieved finger print match with the receiver’s finger print?
Data will be decoded.
Display the image
Original text

6. RESULTS

Table 1: Values of RSA Parameters

Value of p	17
Value of q	13
Value of N	221
Value of public key, e	5
Value of phi	192
Value of private key,d	77



0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
10	11	12	13	14	15	0	1	2	3	4	5	6	7	8	9
0	1	2	3	10	11	12	13	14	15	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	3	10	11	12	13	14	15	4	5	6	7	8	9
10	11	12	13	14	15	0	1	2	3	4	5	6	7	8	9
0	1	2	3	10	11	12	13	14	15	4	5	6	7	8	9
10	11	12	13	14	15	0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
10	11	12	13	14	15	0	1	2	3	4	5	6	7	8	9
0	1	2	3	10	11	12	13	14	15	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	3	10	11	12	13	14	15	4	5	6	7	8	9
10	11	12	13	14	15	0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	3	10	11	12	13	14	15	4	5	6	7	8	9

Fig 2: Randomly generated 16×16 image

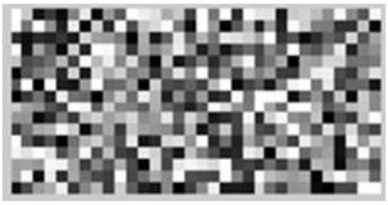
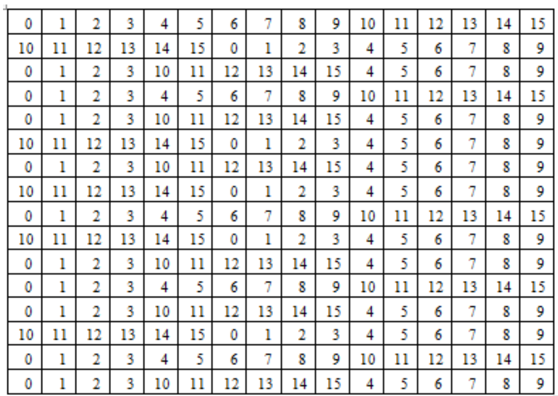


Fig 3: Encrypted image



0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
10	11	12	13	14	15	0	1	2	3	4	5	6	7	8	9
0	1	2	3	10	11	12	13	14	15	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	3	10	11	12	13	14	15	4	5	6	7	8	9
10	11	12	13	14	15	0	1	2	3	4	5	6	7	8	9
0	1	2	3	10	11	12	13	14	15	4	5	6	7	8	9
10	11	12	13	14	15	0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
10	11	12	13	14	15	0	1	2	3	4	5	6	7	8	9
0	1	2	3	10	11	12	13	14	15	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	3	10	11	12	13	14	15	4	5	6	7	8	9
10	11	12	13	14	15	0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	3	10	11	12	13	14	15	4	5	6	7	8	9

Fig 4: Decrypted 16×16 image

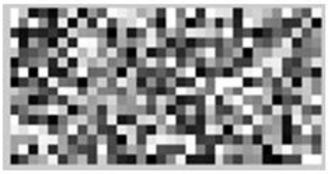


Fig 5: Image sent back to Sender

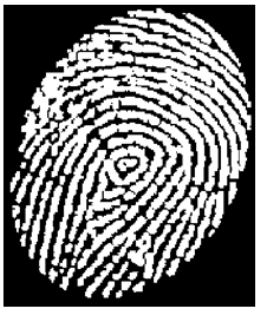


Fig 6: Fingerprint image to hide in leena image

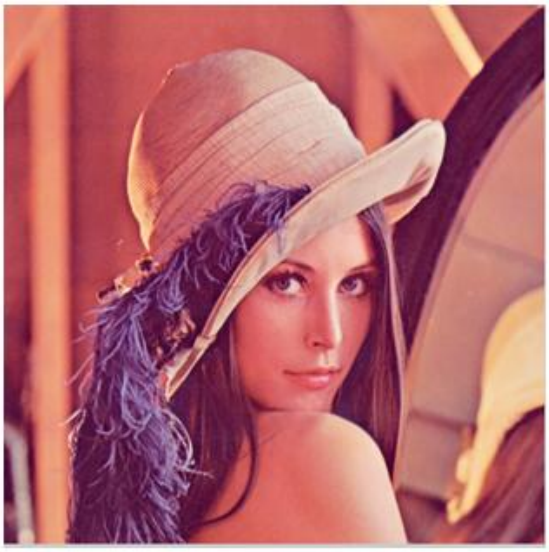


Fig 7: Fingerprint hidden in leena image

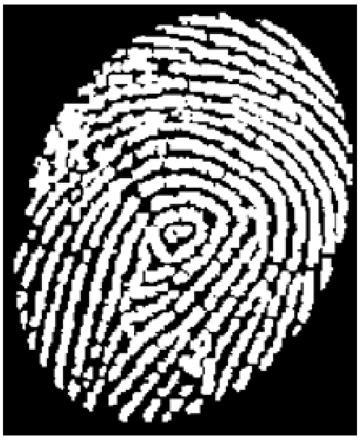


Fig 8: Decrypted fingerprint

Similarity between fingerprints = 1

Message to encode in 'R' component : 'this is a secret message'.

7. CONCLUSION

So from the above discussion we can conclude that the proposed methodology integrates elliptical cryptography with RSA and Biometric Steganography for high level authentication. The proposed method results in reduction in size of key needed in RSA encoding. Integration of Elliptical cryptography with RSA and Biometric Steganography can be implemented on small processors.

8. FUTURE SCOPE & CONCLUSION

New mechanism has been proposed which integrates RSA and steganography with elliptical cryptographic technique along with biometric authentication as an addition security measure. Steganographic image visually resembles Cover Image. This method provides good security with small key size too. The proposed method can be further improved by increasing the key size to upgrade the security level. More biometric features can be added along with finger print for high level of authentication and security.

9. REFERENCES

[1] V.Miller, "Uses of elliptic curves in cryptography", Advances in cryptology-crypto'85, pp.417-426, 1986.

[2] N.Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol.48, no.177, pp.203-208, 1987.

[3] Lifang Wu et al., "A novel key Generation Cryptosystem based on Face Features", Proc. of the IEEE on pp.1675-1678 on oct.2012.

[4] Fabian et al., "Cryptographic key Generation from Voice", 2001, IEEE, pp.202-213.

[5] Nikita Gupta et al., "Elliptic curve Cryptography for Ciphering Images", 2015, IEEE.

[6] Leca, Cristian-Liviu and Cristian-Iulian Rincu. "Combining Point Operations for Efficient Elliptic curve Cryptography Scalar Multiplication", Communications (COMM), 2014 10th International Conference on. IEEE, 2014.

[7] Ali Makki Sagheer, "Elliptic curves Cryptography Techniques", 2012, IEEE.

[8] Christina Thomas and Dr. K. Gnana Sheela, "Analysis of Elliptic curve Scalar Multiplication in Secure Communication" Proc. of the IEEE in Global conference on Communication Technologies, pp.623-627, 2015.

[9] H. El-din, H. Ahmed, H. M. Kalash, and O. S. F. Allah, "An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption", Informatica, vol. 31, pp. 121-129, 2007.

[10] M. Salleh, S. Ibrahim, and I. F. Isnin, "Image encryption algorithm based on chaotic mapping",Journal Technologies, vol. 39(D), pp. 1-12, 2003.

[11] I. A. Ismail, M. Amin, and H. Diab, "A digital image encryption algorithm based a composition of two chaotic logistic maps", International Journal of Network Security, vol. 11, no. 1, pp. 1-10, July 2010.

[12] Williams Stallings, Cryptography and Network Security, Prentice Hall, 4th Edition, 2006.

[13] Ali Soleymani, Md Jan Nordin, and Zulkarnain Md Ali, "A Novel Public key Image Encryption based on Elliptic curves over Prime Group Fields", Journal of Image and Graphics, vol. 1, no. 1, pp.43-49, March 2013, Engineering and Technology Publishing.

[14] Matthew England "Elliptic Curve Cryptography" dissertation MSc Applied Mathematical Sciences, Heriot-Watt University,2006.

[15] N. F. Johnson, S. Katzenbeisser. "A Survey of steganographic techniques." in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, 2000, pp. 43-78.

[16] M. Juneja and P.S. Sandhu. "Designing of robust image steganography technique based on LSB insertion and encryption." IEEE International Conference on Advances in Recent Technologies in Communication and Computing, 2009, pp. 302-305.

[17] Manoj Prabhakar, "Elliptic Curve Cryptography in securing networks by mobile authentication", International Journal on Cryptography and Information Security, ISSN 2013.3304, vol 3 no 3, September 2013.

[18] Ms. Manali Dubal, Ms. Aaradhana Deshmukh, "Achieving authentication and integrity using Elliptic Curve Cryptography architecture‖", International Journal of Computer Applications, ISSN 0975 – 8887, vol 69 no 24, May 2013.