Encryption and Decryption of data using Elliptical Curve Cryptography

V.Gnanalakshmi, N.Yogavarshini, A.Hemapriyadharshini, G.P.Mithra Pooja

Abstract: ***Aadhaar database is the world's largest biometric database system. The security of Aadhaar database plays a major role. In order to secure such huge database, an encryption and decryption algorithm has been proposed in this paper. Elliptic Curve Cryptography (ECC) is a public key cryptography which is used to provide high security to those databases. The Aadhaar database contains individual personal information as well as their biometric identities. ECC is widely used for providing security to all kinds of data. ECC has smaller key size, fast computation, high throughput compared to other cryptographic algorithms. The data's present in database are converted into their corresponding Pixel or ASCII values. After that the encryption process is done with the help of public key, private key, generation points and plain text. After the encryption process, the encrypted coordinates can be mapped with the generated points and from that corresponding ASCII value for text, pixel value for image can be retrieved. Then, the alphabet which is corresponding to ASCII will be displayed so that the cipher text can be viewed. This encrypted data is stored in the database. In order to retrieve the original data decryption process using ECC is carried out. In decryption process, receiver's private key and cipher coordinates which is retrieved from encryption process are used. Therefore, the personal details of an individual can be retrieved with the presence of that particular person who only knows that private key. So, the hackers will not be able to retrieve the database of any individual just by knowing their Aadhaar ID. The proposed work is implemented in the MATLAB software. The Performance metrics like PSNR, Similarity, Correlation Coefficient, NPCR and UACI has been done for analysis.***

Index Terms*: *Elliptic curve cryptography, Prime number, Points, Generation points, Cipher text

I. INTRODUCTION

Aadhaar card possession is one of the most sought after government needs today. It serves as an identity card as well as be used for proof whenever needed. The government has ensured that people from all walks of life, throughout the country is issued a card for their safety and guarantee. Most debates around the Unique Identification Authority of India and Aadhaar focus on privacy concerns, security of the database and on the legality of making Aadhaar mandatory. Data security is the most important parameter nowadays. The security in Aadhaar card database can be improved with the help of Elliptic Curve Cryptography (ECC) [1].

Revised Manuscript Received on July 01, 2019.

V.Gnanalakshmi, Department of Electronics and Communication, Mepco Schlenk Engineering College, Sivakasi, Tamilnadu, India.

N.Yogavarshini, Department of Electronics and Communication, Mepco Schlenk Engineering College, Sivakasi, Tamilnadu, India.

A.Hemapriyadharshini, Department of Electronics and Communication, Mepco Schlenk Engineering College, Sivakasi, Tamilnadu, India.

G.P.Mithra Pooja, Department of Electronics and Communication, Mepco Schlenk Engineering College, Sivakasi, Tamilnadu, India.

Elliptic curve cryptography (ECC) is the public-key cryptography based on the generation of elliptic curves over finite fields. The computation of encryption and decryption process requires only smaller key size. Further, this technique provides authentication and confidentiality. But the major drawback of this method is Elliptic Curve Discrete Logarithm Problem (ECDLP) [2]. By taking larger prime number (p), we can able to avoid this ECDLP. In text and image encryption, text is mapped with their corresponding ASCII values and images are mapped with their pixel values. The corresponding decimal values are mapped with the generated points [3-6], which are generated using the equation.

$$y^2 = (x^3 + ax + b) mod\ P, where\ (4a^3 + 27b^2) mod\ P \neq 0$$

Generation points are generated from the above equations by taking the values 0< x <P and 0<y<P [7-8].The corresponding coordinates of text and images are encrypted using ECC encryption formula and stored in the database. Later the data can be retrieved using decryption formula of ECC.

II. ELLIPTIC CURVE CRYPTOGRAPHY

The mathematical equation for elliptic curve cryptography is as follows

$$y^2 = (x^3 + ax + b) mod\ P, where\ (4a^3 + 27b^2) mod\ P \neq 0$$

where *a* and *b* are coordinates of the above equations and *P* is the prime number.There are several operations involved in elliptic curve cryptography [9].

A. Point Addition

Consider two coordinates P and Q which are not equal, then these two points can perform point addition using the formula below to produce third coordinate R.

$$\lambda = \frac{(y_2 - y_1)}{(x_2 - x_1)} mod p$$

where λ is mean value, (x_1, y_1) and (x_2, y_2) are coordinates of P and Q respectively. p is a prime number.Third coordinate R can be obtained using the below formula

$$x_3 = (\lambda^2 - x_1 - x_2) mod p$$
$$y_3 = (\lambda(x_1 - x_3) - y_1) mod p$$

where (x_3, y_3) are coordinates of R.

B. Point Doubling

Consider two coordinates P and Q which are equal, then these two points can perform point doubling using the formula below to produce third coordinate R.

$$\lambda = \frac{3x_1^2 + a}{2y_1} modp$$

where λ is mean value, (x_1, y_1) are coordinates of P . p is a prime number.

Third coordinate R can be obtained using the below formula

$$x_3 = (\lambda^2 - 2x_1) modp$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) modp$$

where (x_3, y_3) are coordinates of R.

C. Point Inverse

There is another case in which point subtraction can be done with the help of point inverse. The general representation of points can be done with the equation,

$$-J(x, y) = J(x, -y)$$

D. Scalar Multiplication

Scalar multiplication can be done only with the help of point addition and point doubling. Multiplication can be performed with repeated addition.

Q=k*P

Where k is a scalar and P is a coordinate.

III. PROPOSED METHOD

Fig.1 shows the block diagram of the process which had been implemented for the database security. The data's present in database are converted into their corresponding Pixel or ASCII values. After that the encryption process is done with the help of public key, private key, generation points and plain text. After the encryption process, the encrypted coordinates can be mapped with the generated points and from that corresponding ASCII value for text, pixel value for image can be retrieved. Then, the alphabet which is corresponding to ASCII will be displayed so that the cipher text can be viewed. This encrypted data is stored in the database. In order to retrieve the original data decryption process using ECC is carried out. In decryption process, receiver's private key and cipher coordinates which is retrieved from encryption process are used. Therefore, the personal details of an individual can be retrieved with the presence of that particular person who only knows that private key. So, the hackers will not be able to retrieve the database of any individual just by knowing their Aadhaar ID.

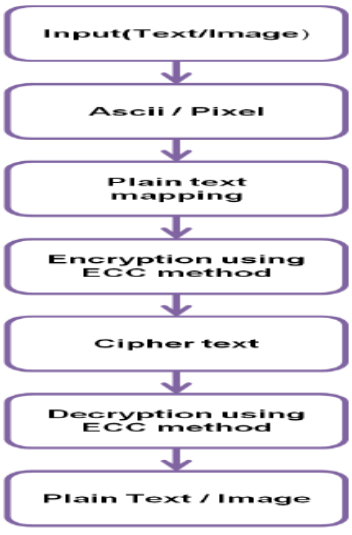

Fig.1 Block diagram

IV. IMPLEMENTATION

A. Point generation

The following steps are used to generate finite points for the taken prime number.

Here p = 271, a = 4, b = -1.

i) Determine the value of y from the equation

$$y^2 modp \text{ , } for y = 0 \text{ } top$$

ii) Determine the value of x from the equation

$$y^2 = (x^3 + ax + b) modp \text{ , } for x = 0 \text{ } top$$

iii) Match y^2 value in *i)* and *ii)*

iv) If the value matches, the corresponding values of x and y form the coordinates of elliptic curve.

Consider the minimum coordinate point (G) from the elliptic curve as the initial point and generate the coordinates up to the value of *p*.Fig.2 shows the generation of points.

	1	2
1	36	27
2	193	210
3	29	83
4	270	219
5	43	2
6	249	153
7	60	184
8	79	245
9	137	129
10	55	147

.....

261	116	226
262	90	130
263	61	111
264	148	117
265	170	146
266	186	220
267	260	122
268	248	217
269	5	259
270	59	14
271	163	33

Fig.2 Generation of points

B. Mapping ASCII value with generation points

The personal details of an individual will be entered as text only. These textcan be converted into its corresponding ASCII value.

Those ASCII values of each character are mapped with the corresponding generation points. The biometric images such as Fingerprint and Iris have the pixel value that ranges from range 0 to 255. These pixel valueswere mapped with the corresponding generation points. Thus plain text can be obtained.P_m is the plain text in the form of coordinates.

C. Encryption using ECC

The Private Key (*l*) and Public Key (*k*) were generated randomly. The mapped coordinates are encrypted using the formula

$$(c_1, c_2) = \{lG, P_m, + l(kG)\}$$

where P_m is the plain text, c_1, c_2 are cipher text.

D. Decryption using ECC

The plain text can be retrieved from the cipher text by decryption using the formula given below.

$$D = (c_2 - kc_1)$$

where *D* is the decrypted text.

E. Remapping

The decrypted coordinates can be mapped with the generated points and from that the corresponding ASCII value for text and pixel value for image can be obtained.

V. PERFORMANCE ANALYSIS

A. Peak Signal to Noise Ratio:

Peak signal to noise ratio is used to measure the quality of an image. The formula for PSNR is:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR (dB) is defined as

$$\text{PSNR} = 10\log_{10}\left(\frac{\text{MAX}_I^2}{\text{MSE}}\right)$$

$$\text{PSNR} = 20\log_{10}\left(\frac{\text{MAX}_I}{\sqrt{\text{MSE}}}\right)$$

$$\text{PSNR} = 20\log_{10}(\text{MAX}_I) - 10\log_{10}(\text{MSE})$$

B. Similarity ratio:

Similarity test is done to find similarity between two images. Here we have taken images of fingerprint and iris.

C. NPCR and UACI:

NPCR stands for Number of Changing Pixel Rate and UACI stands for Unified Averaged Changed Intensity.These two methods are applied to evaluate the strength of an encryption with respect to the differential attack.

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

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

where W and H are the width and height of C_1 and C_2.C_1 and C_2 are two ciphered images, whose corresponding original images have only one pixel difference and also have the same size. $C_1(i,j)$ and $C_2(i,j)$ are grey-scale values of the pixels.

D. Correlation Coefficient:

A Correlation Coefficient is the value that quantifies a type of correlation and dependence, meaning statistical relationship between two texts or two images.

$$r = \frac{n\sum xy - (\sum x)(\sum y)}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2]}}$$

VI. EXPERIMENTAL RESULTS

The proposed method is simulated in MATLAB Platform, in which the Aadhaar details of an individual person are taken as reference for doing encryption and decryption. The experimental results are shown below:

A. Input: Text

Text can be in the format of alphanumeric and special characters. Fig 3, Fig 4 and Fig 5 shows the input text, encrypted text and decrypted text respectively.

Fig.3 Input Text

Fig.4 Cipher Text

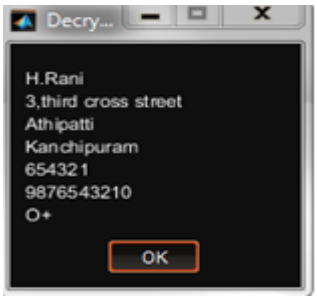

Fig.5 Decrypted Text

B. Input : Fingerprint

Fingerprint is given as input which is converted into grayscale image and process is being carried out. Fig 6, Fig 7 and Fig 8 shows the input, encrypted and decrypted images of fingerprint respectively.

Fig.6 Input Image

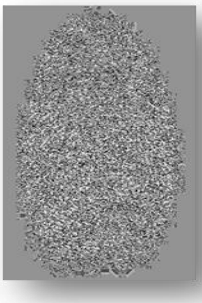

Fig.7 Encrypted Image

Fig.8 Decrypted Image

C. Input: Iris

Iris is given as input which is converted into grayscale image and process is being carried out. Fig 9, Fig 10, Fig 11 are input, encrypted and decrypted images of iris respectively.

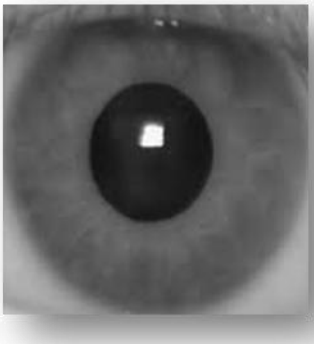

Fig.9 Input Image

Fig.10 Encrypted Image

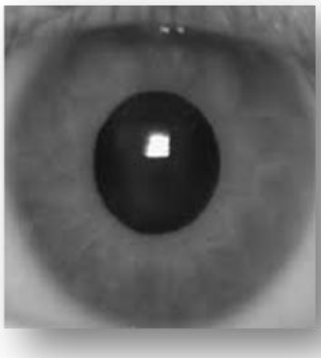

Fig.11 Decrypted Image

D. Performance Analysis:

The performance of this algorithm had been analyzed using various parameters to verify the strength of security level of encrypted and decrypted data. The results are shown in table 1

Table.1 Performance Analysis Results

Performance Analysis	Fingerprint		Iris	
	Input Vs Cipher	Input Vs Decrypted	Input Vs Cipher	Input Vs Decrypted
PSNR	6.9066	Inf	10.6816	Inf
Similarity	0.1942	1	0.0299	1
NPCR	0.9953	0	0.9898	0
UACI	0.4093	0	0.2488	0
Correlation Coefficient	-0.074	1	0.033	1

VII. CONCLUSION

Generally ECC has fast computation and smaller key size which makes the process quick. Security of data by this technique will make the hacking of data difficult by the intruder. Decryption is done to retrieve the data. The performance analysis of the encrypted and decrypted data is performed. It has proven that the data is stored in much secured manner. The time taken for encrypting the whole database is 55.1807 sec and the time taken for decrypting the whole database is 53.0415 sec. The time taken for processing complete database of an individual is comparatively less than any other technique.

REFERENCES

1. Neal Koblitz, Alfred Menezes and Scott Vanstone, "The State of Elliptic Curve Cryptography", Designs, Codes and Cryptography, 19, 173–193 (2000)
2. Moumita Roy, Nabamita Deb, Amar Jyoti Kumar, "Point Generation And Base Point Selection In ECC An Overview", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 5, May 2014.
3. Neal Koblitz, "Elliptic Curve Cryptosystems", Mathematics of Computation, Volume 4. Number 177. Pages 201-209.
4. F. Amounas and E.H. El Kinani, "Fast Mapping Method based on Matrix Approach for Elliptic Curve Cryptography", International Journal of Information & Network Security (IJINS), Vol.1, No.2, June 2012, pp. 54~59, ISSN: 20893299.
5. F. Amounas and E.H. El Kinani, "An Efficient Elliptic Curve Cryptography protocol based on Matrices", International Journal of Engineering Inventions, ISSN: 2278-7461, Volume 1, Issue 9 (November 2012) PP: 49-54.
6. Geetha G, Padmaja Jain, "Implementation of Matrix based Mapping Method Using Elliptic Curve Cryptography", International Journal of Computer Applications Technology and Research, Volume 3– Issue 5, 312 - 317, 2014, ISSN: 2319–8656.
7. Hitesh Kag, Ruchi Telang Gode, "Matrix Based Efficient ECC Technique For Text Encryption", International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-2, Issue-9, Sept.-2014.
8. V.Kamalakannan, S.Tamilselvan, "Security Enhancement of Text Message Based on Matrix Approach Using Elliptical Curve Cryptosystem", Procedia Materials Science 10(2015), 489 – 496, 2nd International Conference on Nanomaterials and Technologies (CNT 2014)
9. KefaRabah, "Elliptic curve ElGamal Encryption and Signature Schemes", Information Technology Journal 4(3):299-306,2005, ISSN1812-5638.
10. Dragan Vidakovic and Dusko Parezanovic," Generating Keys in Elliptic Curve Cryptosystems", International Journal of Computer Science and Business Informatics, ISSN: 1694-2108 | Vol. 4, No. 1. AUGUST 2013.