Digital Image Encryption using ECC and DES with Chaotic Key Generator

Bidyut Jyoti Saha[1], Kunal Kumar Kabi[2], Arun[3]
School of Computer Engineering, KIIT University, Bhubaneswar, India

Abstract

The modern world is experiencing multimedia and internet usage techniques. As, image data distribution is increasing, the security risks and threats are also coming into picture. To avoid the risks and to make the transmission of images secure, digital encryption techniques are evolved over recent years. In this paper, a digital image encryption technique has been proposed and simulated to enhance the security performance, efficiency and reliability. Original image is encrypted using DES (Digital Encryption Standard) with the help of a key sequence which is generated from a chaotic key generator with the help of Henon map and the encrypted image is mapped to the points of elliptic curve.

Keywords: ECC, DES, Henon map, Encryption, Decryption.

1. Introduction

In present, information security is very important in digital communication. As the internet and multimedia technology increasing, a need of secure algorithm is required to protect the authenticated and authorized multimedia contents such as, image, audio and video etc. Sensitive information like medical and legal records, credit ratings, Business transactions, Voice mail are also require to be protected from outsiders.

Cryptography is a technique to hide the information in digital communication which preserves integrity, confidentiality and authenticity of multimedia and text information.

Liu et. al. [1] had proposed a new method to enhance the algorithm of DES. In DES, logistic map is used to generate the random round keys which further enhance the complexity of the algorithm. The experiment in the paper shows that after image encryption, the original image becomes stochastic noise which is impossible for the attacker to attack.

Zhang et. al. [2] proposed a digital image encryption technique with the chaos and improving DES. The scheme uses a logistic chaos sequencer to make the pseudo-random sequence, carries on the RGB with this sequence to the image chaotically, then makes double time encryptions with improvement DES. The scheme has fast encryption speed, high security and key sensitivity. The algorithm shows improvements over traditional DES systems by including chaos mechanism. Kamlesh et. al. [3] proposed an encryption technique based on Elliptic Key Cryptography (ECC) with knapsack for image encryption in 2010. The analysis shows that the scheme had less encryption time, consumes low power and more reliable. Results also shows that ECC applications have high security.

Ling et. al. [4] proposed an encryption method based on S-DES and chaotic map. Through applying the sensitivity of initial value and randomness in chaotic map, the system has larger key quantities. It has effectively improved the security of image encryption. In the analysis it is shown that the secret key space of this algorithm is very wide, and it has strong sensibility, high security, and fairly good ability of resisting statistic attack.

2. Background

In this paper, we propose an encryption technique using ECC and DES. The key generation algorithm is used to generate the symmetric key for DES encryption using chaotic key generator. The different techniques used are:

A. Elliptic curve Cryptosystem (ECC)

Elliptic curves are cubic equations in two variables that are similar to the equations used to calculate the length of a curve in the circumference of an ellipse [5]. The general equation for an elliptic curve is:

$$E: y^2 + b_1xy + b_2y = x^3 + a_1x^2 + a_2x + a_3 \quad (1)$$

Elliptical curves over real numbers use a special class of elliptic curves of the form:

$$E: y^2 = x^3 + ax + b, \text{and denoted by } E_p(a, b) \quad (2)$$

Where, *a* and *b* are in rational numbers, complex numbers, integers mod n. In the above equation, if $4a^3 + 27\,b^2 \neq 0$,the equation represents a nonsingular elliptic curve; otherwise, the equation represented a **singular elliptic curve.** In a nonsingular elliptic curve, the equation $x^3 + ax + b = 0$ has three distinct roots (real or complex); in a singular curve the equation $x^3 + ax + b = 0$ does not have three distinct roots [5].

In eq. (3), *y* has a degree of 2 while *y* has a degree of 3. It means that a horizontal line can intersects the curve in three points if all the roots are real. However, a vertical line can intersects the curve at most in two points.

B. Data Encryption Standard (DES)

The Data Encryption Standard algorithm (DES) is the most widely used symmetric encryption algorithm in the world so far. DES was quickly adopted for non-digital media. The banking industry, adopted DES as a banking standard. Standards for the banking industry are set by the American National Standards Institute [6]. DES is a symmetric block cipher designed to encrypt and decrypt blocks of data consisting of 64 bits under control of a 56 bit key. Each 8^{th} bit of the 64-bit key is used for parity checking and otherwise ignored. Decrypting must be done by using the same key as for encryption.

For example, if the plaintext message is "12345678ABCDEF12" and the key to encrypt the plaintext be "1234123412341234", then the cipher text will be "E112BE1DEFC7A367". Decryption of the above cipher text using the same key results in the plain text message "12345678ABCDEF12" [5].

After an initial permutation (IP), the 64-bit plaintext is split into two 32 bit input (L_0 & R_0). DES consists of 16 rounds. In each round a function, '*f*' is performed in which the data is combined with a 48-bit permutation of the key. After the 16^{th} iteration, the right (R_{16}) and left (L_{16}) halves are concatenated and a inverse permutation (IP^{-1}) completes the encryption process [6]. The figure for the entire DES encryption is shown Figure 1 [7].

Function *f* of DES

The function of the DES algorithm is made up of four operations [5].

- The 32-bit right half of the plaintext R_0, is expanded to 48-bits with expansion box.
- 48 bit plaintext is XORed with a 48-bit sub-key, K_1.
- The result passes into 8 S-Boxes. Each S-Box transforms 6 bit input to 4 bit output.
- Finally, a permutation is performed; the output of the result is XORed with the initial left half L_0, to obtain the new right half R_1. The original right half, R_0, becomes the new left half L_1.

The whole process iterates for 16 times and operates with 16 different keys (K_1, K_2, K_3… K_{16}).

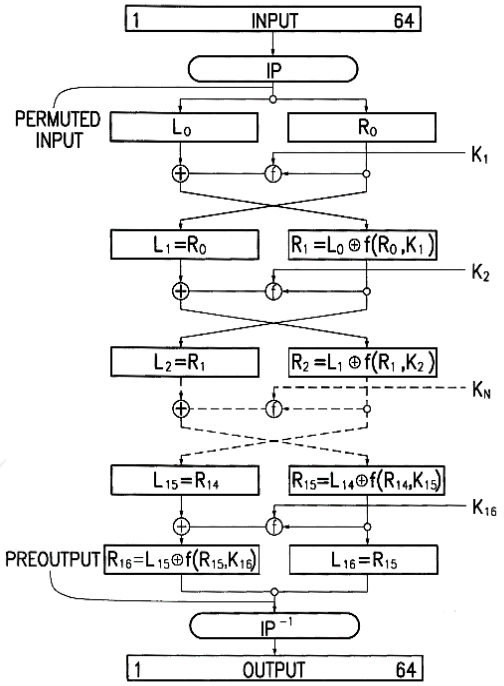


Figure 1: DES Encryption [7]

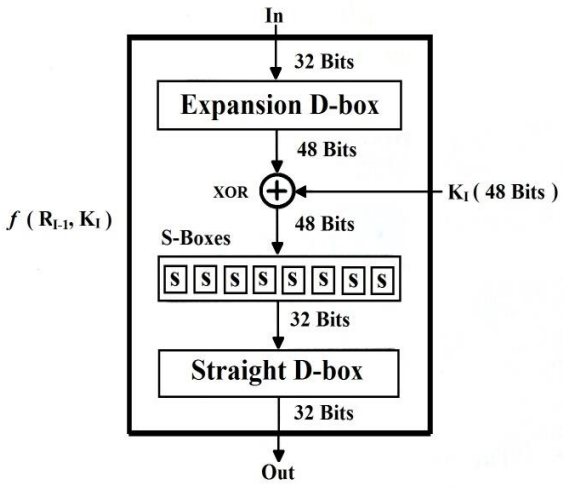


Figure 2: Function '*f*' of DES [5]

C. Henon map

The Henon map was proposed by M. Henon in 1976 which is 2D map represented with an attractor and also is a Lorenz equation of Poincare section. The Henon map generates cipher key which is random sequence and is used to encrypt the shuffled image or plain image. Chaotic behavior depends on initial system parameters and conditions. The Henon map equation which maps A_i, B_i to a new point A_{i+1}, B_{i+1} is represented as follows [8, 9]:

$$\begin{cases} A_{i+1} = B_i + 1 - uA_i^2 \\ B_{i+1} = vA_i \end{cases} \quad (3)$$

The initial value of A_0, B_0 is replaced by A_1, B_1 in next iteration of generation of sequence in Henon map. The Henon attractor is used to converge the sequence. The *u* and *v* are control parameters. For *u*=1.4 and *v*=0.3, the Henon map generates random sequence with chaotic behavior [9].

3. Proposed Algorithm

Let, M be the original image of size x*y.

Encryption

3.1 Round key generation

The 56 bit round key is generated using Henon map to produce random sequence of key bits with initial parameter using eq. (3). The same initial parameters are used to encrypt and decrypt the image in DES. Round key generated is chaotic in nature and passed to the DES encryption. A slight modification to Henon map equation is done by adding A and B components to another array called K as per eq. (4), after adding A and B components, the result is stored in K.

$$\boldsymbol{K = A + B} \quad (4)$$

The key generated becomes the round key for DES image encryption.

3.2 DES Encryption

The original image M is used as input to the DES algorithm. The whole image is divided into 64-bit blocks. The 64-bit is permuted according to predefined rule of initial permutation. Before the main rounds, each block is divided into two 32-bit halves and processed alternately. After 16 rounds of processing, a final permutation is applied to produce 64-bit cipher text. Similarly, all the resulting blocks are processed in the same manner and they together form a ciphered image M'.

3.3 Elliptic curve

The ciphered image M' produced from final rounds of DES are mapped to each point of elliptic curve. Each 8-bit of the cipher image is mapped to a unique point in the elliptic curve. In our algorithm, we map one to one plaintext with the points generated from the elliptic curve.

The corresponding point generated from the plaintext value is stored in 16-bit (8-bit for x-coordinate and 8-bit for y-coordinate) of the final encrypted image M". The image M' of size x*y produces an output of size (2x)*y of the final encrypted image M".

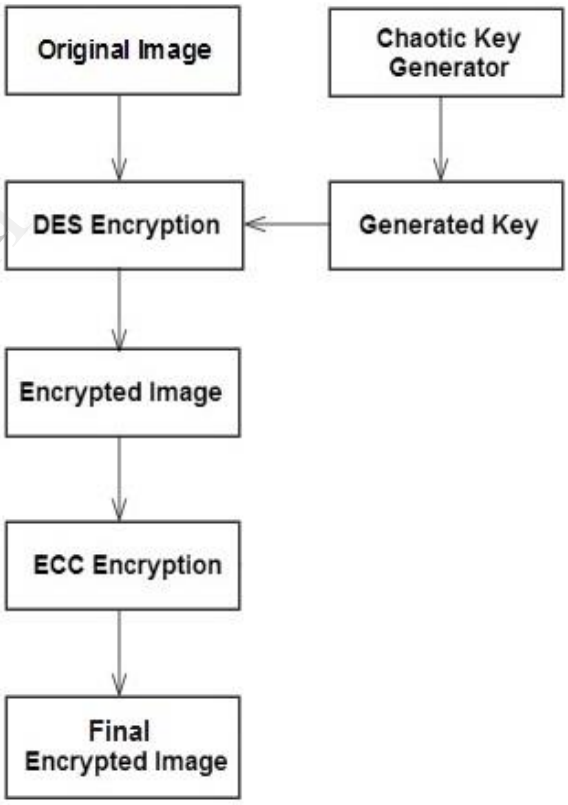


Figure 3: Image Encryption structure (DES and ECC)

Decryption

The points of the elliptical curve are recovered from the final Encrypted image M" of size (2x)*y. The plaintext is extracted from the corresponding recovered points and when stored will generate an image N' of size x*y. The resultant ciphered image is then applied to reverse DES with same

round key used in encryption process. Each block of 64-bit of ciphered image is the input for the DES. After 16 rounds of processing, the final output will be 64-bit plaintext. Similarly same process is repeated for all the remaining ciphered blocks. The original image is recovered after storing all the decrypted plaintexts of size x*y.

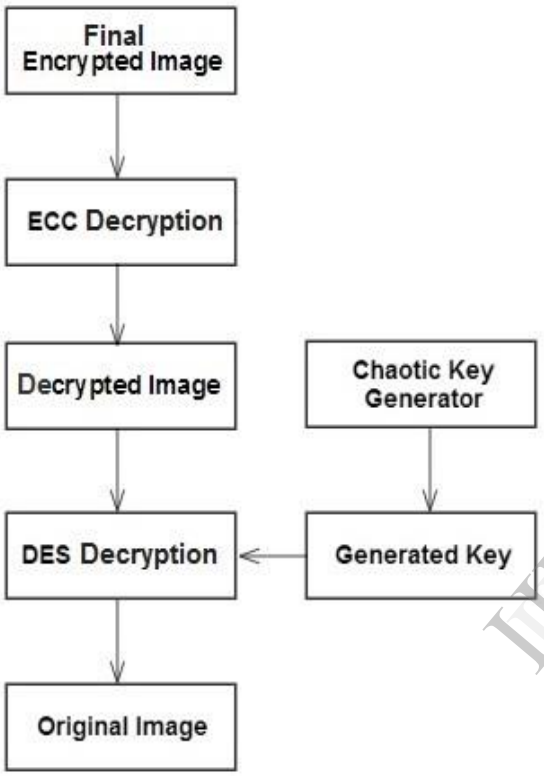
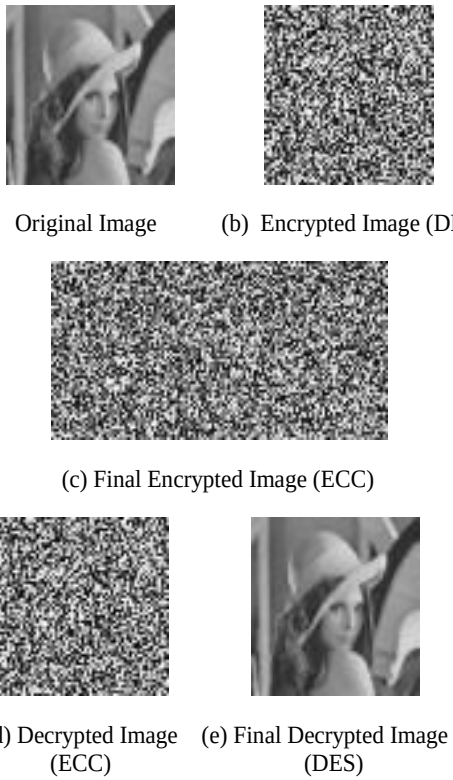


Figure 4: Image Decryption structure (DES and ECC)

4. Simulation Results

For experimental results, we have taken an image 'Lena64.bmp' of size 64*64. Henon map is used to generate the round key of size 56-bit. The key has been produced by taking initial parameters as A=0.54, B=0.34, u=1.4, and v=0.3 using eq. (3). The random key shows chaotic behavior in above parameters. *MATLAB* 2012a is chosen as simulation software. The simulation is shown in Figure (5). Picture (a) is original image. Picture (b) is encrypted image after applying DES. Picture (c) is final ECC encrypted image. Picture (d) is ECC decrypted image. Picture (e) is final decrypted image after applying reverse DES.

Here, we have chosen ***p*** (modulo) = 257 for ECC. The value of a and b of elliptical curve are 6 & 7 respectively.



(a) Original Image (b) Encrypted Image (DES)

(c) Final Encrypted Image (ECC)

(d) Decrypted Image (ECC) (e) Final Decrypted Image (DES)

Figure 5: Image Results

5. Conclusion

In past years, the algorithms of many cryptosystems are under development and enhancement. DES is still important, so improvements and accuracy is required. In this paper, we have taken a grayscale image and encrypted it with DES. The round key is generated from Henon chaotic map. The resulting image is further mapped using elliptic curve, which enhances the complexity of algorithm and impossible to attack without knowing the system parameters. In future, we will work with variations of DES along with 3D chaotic map.

6. References

[1] Ming-S. Liu, Yi Zhang, Jian-H. li, "Research on Improving Security of DES by Chaotic Mapping", *IEEE, Proceedings of the 8th International Conference on Machine Learning and Cybernetics, Baoding*, pp. 12-15, Jul 2009.

[2] Zhang Y. Peng, Zhai Z. Jun, Liu. Wei, Nie Xuan, Cao S. Ping, Dai W. di, "Digital Image Encryption Algorithm based

on Chaos and Improved DES", *IEEE, San Antonio TX, USA*, Oct. 2009.

[3] K. Gupta, S. Silakari, "Performance Analysis for Image Encryption using ECC", *First International Conference on Computational Intelligence, Communication Networks*, 2010.

[4] L. Bin, L. Lichen, Z. Jan, "Image Encryption algorithm based on chaotic map and S-DES", *IEEE*, pp. 41-44, 2010.

[5] Behrouzan A. Forouzan, "Cryptography & Network Security", *TMH Publisher*, 2010, ISBN. 9780070660465.

[6] Grabbe J.,"Data Encryption Standard: The DES algorithm illustrated", *Laissez faire City time*, vol. 2, no 28, 2003.

[7] M. McLoone, J. V. McCanny, "A High Performance FPGA Implementation of DES", *IEEE*, pp. 374-383, 2000.

[8] Ramesh Kumar Yadava, Dr. B. K.Singh, S. K. Sinha and K. K. Pandey, "A New Approach of Colour Image Encryption Based on Henon like Chaotic Map", *Journal of Information Engineering and Applications*, vol. 3, no. 6, , pp. 14-20, 2013.

[9] Alireza Jolfaei and Abdolrasoul Mirghadri,"An Image Encryption Approach using Chaos and Stream Cipher", *Journal of Theoretical and Applied Information Technology*, pp.117-125, 2010.