Improved Elliptic Curve Cryptography with Homomorphic Encryption for Medical Image Encryption

Shoulin Yin, Jie Liu, and Lin Teng
(Corresponding author: Jie Liu)

Software College, Shenyang Normal University[3]
Shenyang 110034, China
(Email: ljnan127@163.com)

(Received July 26, 2018; Revised and Accepted Dec. 20, 2018; First Online July 8, 2019)

Abstract

Medical image contains sensitive information of patients. In order to improve the efficiency and security of medical image encryption, we propose an improved elliptic curve cryptography by combining with homomorphic encryption in this paper. Traditional elliptic curve cryptography has some disadvantages, so we first make improvement for elliptic curve cryptography. Then the modified elliptic curve cryptography combining with homomorphic encryption is used in the process of medical image encryption. The experimental results show that compared with other algorithms, this new algorithm not only has good encryption effect, high security and large amount of key, but also has good sensitivity to initial value and anti-attack ability.

Keywords: Elliptic Curve Cryptography; Homomorphic Encryption; Medical Image Encryption

1 Introduction

With the rapid development of computer technology and multimedia technology, multimedia communication has gradually become an important way for people communicating with each other. At the same time, when people use computer communication to contact each other, a new request is put forward when confidential information transforming in network. Information security has gradually become the research focus. In the multimedia information, vivid image information has become one of the important means for human to express information, when it refers to confidential image information such as military, business and industry, information must be encrypted then it can transfer in the Internet [8, 10, 19].

Image encryption technology currently has the following three types:

1) Based on modern cryptography [20, 21]. Both commercially and militarily widely use the modern cryptography. In technically, image information as a data format is fully capable of being encrypted by modern cryptography including symmetric cryptography and asymmetric cryptography. In practical applications, symmetric cryptography is mainly used to encrypt commercial or military information, it is often used to encrypt short messages.

2) Based on image pixel scrambling [14, 16]. The represented approaches are Arnold transform and the magic square transform. These encryption algorithms directly act on the pixels of the image. According to some linear transformation, it changes the position of the pixel to achieve the purpose of image encryption.

3) Based on chaotic technique [2, 13]. due to the development of the chaotic dynamics in recent years, people gradually realize that the chaos can be used as a new password system, which can be used to encrypt text voice and image data. Chaos is used as a new cryptosystem which is determined by the properties of chaotic system itself.

For image encryption, there are some discoveries. Mccarthy [11] discussed that an identity-based encryption scheme enabled the efficient distribution of keys in a multi-user system. Such schemes were particularly attractive in resource constrained environments where critical resources such as processing power, memory and bandwidth were severely limited. This research examined the first pragmatic lattice-based IBE scheme and brought it into the realm of practicality for using on small devices. Assad [1] proposed a new fast, simple, and robust chaos-based cryptosystem structure and analyzed its performances. The cryptosystem used a diffusion layer followed by a bit-permutation layer, instead of byte-permutation, to shuffle the positions of the image pixels. Moreover, the

permutation layer was achieved by a new proposed formulation of the 2D cat map that allowed an efficient implementation, measured by the time complexity, in terms of arithmetic and logic operations, and also, in terms of clock cycles, of the key-dependent permutation process in comparison with the standard one. Hariyanto [4] presented arnold's cat map algorithm in digital image encryption. Su [15] proposed an image encryption scheme based on chaos system combining with DNA coding and information entropy, in which chaos system and DNA operation were used to perform substitution, and entropy driven chaos system was used to perform permutation. However, two vulnerabilities were found and presented in this paper, which made the encryption fail under chosen-plaintext attack. A complete chosen-plaintext attack algorithm was given to rebuild chaos systems' outputs and recover plain image, and its efficiency was demonstrated by analysis and experiments.

So this paper proposes an improved elliptic curve cryptography by combining with homomorphic encryption for medical image encryption. The rests of the paper are organized as follows. Section 2 introduces the improved elliptic curve cryptography. New medical image encryption is illustrated in Section 3. Section 4 outlines the experiments. Section 5 finally concludes the paper.

2 Improved Elliptic Curve Cryptography

2.1 Elliptic Curve Cryptography

Assuming that user A wants to send the encrypted plaintext m to B. A needs to execute the following operation [6]:

1) User A selects one elliptic curve E and one point in E as base point G.
2) User A selects private k and produces a public key $K = kG$.
3) User A sends E, G and public key K to user B.
4) User B receives this message, it codes the plaintext to one point M in E and randomly generates integer $r(r < n)$.
5) User B calculates $C1 = M + rK$ and $C2 = rG$.
6) User B sends $C1$ and $C2$ to user A.
7) User A receives this message, then it calculates $C1 - kC2$ and gets point M. Because $C1 - kC2 = M + rk - k(rG) = M + rK - r(kG) = M$, then M is decrypted to get plaintext.

2.2 Improved ECC

Traditional ECC [5, 7, 12, 17, 18] has a big computation burden due to inversion operation. Hence, we improve ECC by ignoring inversion which has a high efficiency.

1) Signer notarizes Hash function to generate information abstract.
2) Signer determines elliptic curve parameter $F = (P, a, h, g, n, h)$ or $(m, f(x), a, h, g, n, h)$.
3) Signer sends determined Hash function and elliptic curve parameter to verifier.
4) Signer chooses key x on the basis of finite field $G(P)$ and selected elliptic curve point group. Then it gets public key $y = xg$ and public y.
5) Signer selects random number $K, 1 \leq K \leq n-1$.
6) It computes $r = kg$, if $r = 0$ then return back step 5.
7) It computes $s = mrx - k$ and gets (s, r) as the signature of m. (s, r) and m are sent to verifier.
8) Verifier calculates $r' = sg + myr$.
9) Verifier judges whether $n' = r$, if they are equal, signature is properly. Otherwise, it rejects signature.

3 Proposed Scheme

3.1 Homomorphic Encryption

The ciphertext can be operated directly without decryption by Homomorphic encryption. Setting encryption function is E_{k1}, decryption function is D_{k2}, plaintext is $M = m_1, m_2, \cdots, m_n$. α and β denote operation. If encryption and decryption function satisfy Homomorphic encryption property, then the following formula is correct.

$$\begin{aligned} & \alpha(E_{k1}(m_1), E_{k2}(m_2), \cdots, E_{kn}(m_n)) \\ = \; & \beta(E_{k1}(m_1, m_2, \cdots, m_n)). \end{aligned} \tag{1}$$

When data $m_1, m_2, \cdots, m_n$ conducts β operation without leaking, we can encrypt it as $(E_{k1}(m_1), E_{k2}(m_2), \cdots, E_{kn}(m_n)$, then do α operation for it. The result is decrypted as $\beta m_1, m_2, \cdots, m_n$. The addition homomorphism and multiplication homomorphism can be expressed as:

$$\begin{aligned} & m_1 + m_2 + \cdots + m_n \\ = \; & D_k(E_k(m_1) + E_k(m_2) + \cdots + E_k(m_n)). \\ & m_1 \cdot m_2 \cdots m_n \\ = \; & D_k(E_k(m_1) \cdot E_k(m_2) \cdot \cdots \cdot E_k(m_n)). \end{aligned}$$

3.2 Improved ECC Homomorphic Encryption

We use the improved ECC to realize the addition homomorphism and multiplication homomorphism.

1) Homomorphic addition.

Plaintext m_i is coded on one point P_{m_i} in E. Randomly select a number r_i and get encrypted data (C_{1_i}, C_{2_i}). It makes additive operation for $(C_{1_l}, C_{2_l}) \cdots (C_{1_n}, C_{2_n})$ and obtains $(\sum_{i=1}^{n} C_{1_i}, \sum_{i=1}^{n} C_{2_i})$. Then calculate $C = k\sum_{i=1}^{n} C_{1_i}$. So we can prove:

$$\begin{aligned} k\sum_{i=1}^{n} C_{1_i} &= kG\sum_{i=1}^{n} r_i = k\sum_{i=1}^{n} r_i. \\ \sum_{i=1}^{n} C_{2_i} - C &= k\sum_{i=1}^{n} r_i + \sum_{i=1}^{n} P_{m_i} - k\sum_{i=1}^{n} r_i \\ &= \sum_{i=1}^{n} P_{m_i}. \end{aligned}$$

So we can get sum $\sum_{i=1}^{n} P_{m_i}$, and decrypt it to obtain $\sum_{i=1}^{n} m_i$.

2) Homomorphic multiplication. Plaintext m_i is calculated, then it gets $(C_{1_i}, C_{2_i}, C_{3_i})$. It makes multiplication operation for $(C_{1_l}, C_{3_l}) \cdots (C_{1_n}, C_{3_n})$ and obtains $(C_{1_l} \cdot C_{2_l} \cdots C_{1_n}, C_{3_l} \cdot C_{3_l} \cdots C_{3_n})$. Then calculate $k^n \cdot C_{1_l} \cdot C_{1_2} \cdot C_{1_n}$ through private key k. So we can prove:

$$\begin{aligned} k^n \cdot C_{1_l} \cdot C_{1_2} \cdot C_{1_n} &= k^n G^n r_1 \cdot r_2 \cdots r_n \\ &= C_{2_l} \cdot C_{2_2} \cdots C_{2_n}. \end{aligned}$$

So we can get $C_{3_l} \cdot C_{3_2} \cdots C_{3_n} \cdot C_{2_l}^{-1} \cdot C_{2_2}^{-1} \cdot C_{2_n}^{-1} = m_1 \cdot m_2 \cdots m_n$.

4 Experiments and Analysis

In order to verify the effectiveness of proposed medical image encryption, we select two medical images as input image conducted on MATLAB. Figures 1, 2 are the original images and histograms. Figures 3, 4 are the encrypted images and histograms. Figures 5, 6 are the decrypted images and histograms.

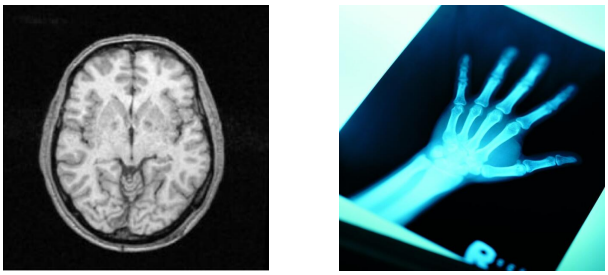

Figure 1: Original images

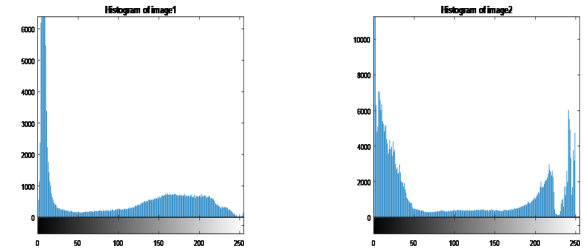

Figure 2: Histogram of original images

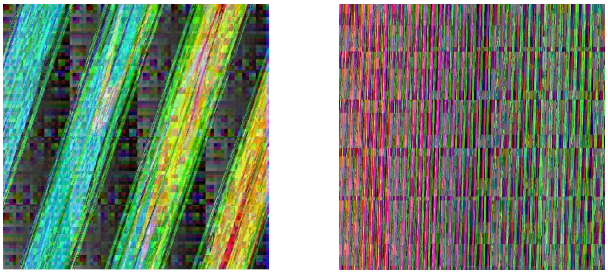

Figure 3: Encrypted images

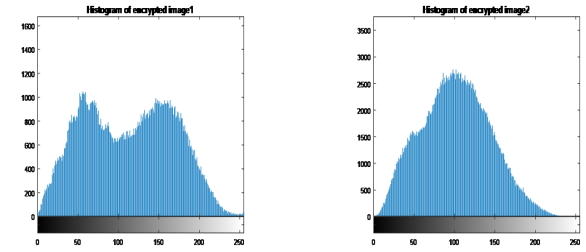

Figure 4: Histogram of encrypted images

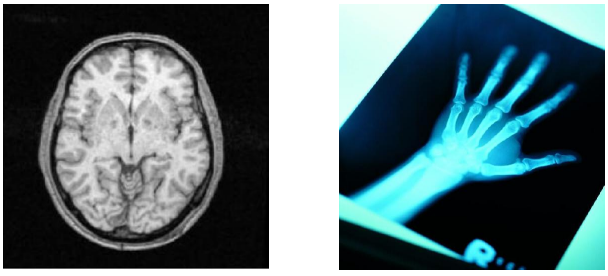

Figure 5: Decrypted images

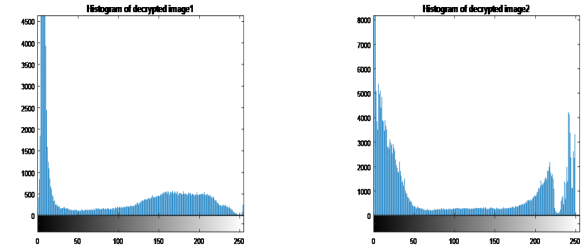

Figure 6: Histogram of decrypted images

Table 1: Correlation comparison between adjacent pixels

Correlation	vertical direction	Horizontal direction	Diagonal direction
Image1	0.9241	0.9235	0.9417
Encrypted image1	0.0015	0.0008	0.0021
Image2	0.9221	0.8719	0.9426
Encrypted image2	0.0041	0.0022	0.0018

4.1 Key Space Analysis

We adopt improved ECC to encrypt image, which has eight keys. If the computer accurates to 10^{-15}, the space size of the key is 10^{128}. The key space is large enough to resist the exhaustive attack.

4.2 Sensitivity Analysis

It is sensitive to system parameters and initial values, which means that if the initial value changes slightly, the decrypted image will not be associated with the original image. As shown in Figure 3, during the decryption process, key adds 0.1^8 to decrypt medical image. Based on the above theory, the algorithm is sensitive to key, which indicates that it has the ability to resist the exhaustive attack.

4.3 Correlation Analysis of Adjacent Pixels

We use the following formulas to calculate the correlation coefficients.

$$\begin{aligned} E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i. \\ D(x) &= \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)]^2. \\ Cov(x,y) &= \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)][y_i - E(y)]. \\ g_{xy} &= \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}. \end{aligned}$$

Where x and y denote two adjacent pixel values in the image and g_{xy} is correlation coefficient between adjacent pixels shown in Table 1.

4.4 Information Entropy

Information entropy denotes the degree of uncertainty system, and it is used to describe the uncertainty of image information. The information entropy can be used to analyze the distribution of gray value in the image. Let $P(m_i)$ be proportion of pixel with gray value m_i in image and $\sum_{i=0}^{255} P(m_i) = 1$. The information entropy of the pixel is defined as:

$$H(m) = -\sum_{i=0}^{255} P(m_i \log_2 P(m_i)).$$

We make comparison with HHC [12], CST [3] and CTM [9] as shown in Table 2.

Table 2: Information entropy comparison

Method	Encrypted image1	Encrypted image2
HHC	0.712	0.708
CST	0.687	0.693
CTM	0.667	0.689
Proposed	0.796	0.797

4.5 Plaintext Sensitivity Analysis

Differential attack: A small change in the original image can cause a huge change in the encrypted image. The attacker can obtain the connection between the original image and the encrypted image. We adopt number of pixel change rate (NPCR) and unified average changing intensity (UACI) to measure it. They are defined as:

$$\begin{aligned} NPCR &= \sum_{ij} D(i,j)/m \times n. \\ UACI &= \frac{1}{m \times n}[\sum_{ij} \frac{|C_1(i,j) - C_2(i,j)|}{255}]. \end{aligned}$$

Where m and n represent the row and column of the image respectively. C1 and C2 are obtained by changing only one pixel value of the original image. $C1(i,j)$ and $C2(i,j)$ represent the pixel values in the (i,j) coordinate.

NPCR and UACI values are shown in Table 3 and 4, the tiny change in the original image can make the encryption image close to 100% of NPCR changes, the encrypted image's average change is above 30% (UACI). At the same time, it also shows that image information spreads to the cipher image well, compared with the HHC, CST and CTM, the proposed algorithm has very good sensitivity, robustness for the differential attack.

Table 3: Encrypted image1

Method	NPCR%	UACI%
HHC	89.67	31.02
CST	91.42	37.62
CTM	92.14	38.54
Proposed	99.23	39.58

Table 4: Encrypted image2

Method	NPCR%	UACI%
HHC	90.76	32.01
CST	91.12	35.53
CTM	91.47	36.45
Proposed	99.18	38.59

5 Conclusion

In this paper, a new medical image encryption algorithm is proposed based on improved elliptic curve cryptography by combining with homomorphic encryption. We analyze the districts of traditional ECC, then we modify it. The experimental results show that the algorithm has better key space with better encryption effect and higher key sensitivity. In addition, the algorithm has strong robustness for resisting statistical attack and exhaustive attack. In the future, in terms of medical image encryption, we will adopt some deep learning models to study it.

References

[1] S. E. Assad, M. Farajallah, "A new chaos-based image encryption system," *Signal Processing Image Communication*, vol. 41, pp. 144-157, 2016.

[2] S. Farwa, T. Shah, N. Muhammad, *et al.* "An image encryption technique based on chaotic s-box and srnold transform," *International Journal of Advanced Computer Science & Applications*, vol. 8, no. 6, 2017.

[3] M. Ghebleh, A. Kanso, "A novel efficient image encryption scheme based on chained skew tent maps," *Neural Computing & Applications*, vol. 4, pp. 1-16 2017.

[4] E. Hariyanto, R. Rahim, "Arnold's cat map algorithm in digital image encryption," *International Journal of Science & Research*, vol. 5, no. 10, pp. 6-391, 2016.

[5] M. S. Hwang, C. C. Lee, J. Z. Lee, and C. C. Yang, "A secure protocol for bluetooth piconets using elliptic curve cryptography," *Telecommunication Systems*, vol. 29, no. 3, pp. 165-180, 2005.

[6] M. S. Hwang and I. C. Lin, *Introduction to Information and Network Security (6ed, in Chinese)*, Taiwan: Mc Graw Hill, 2017.

[7] M. S. Hwang, S. F. Tzeng, C. S. Tsai, "Generalization of proxy signature based on elliptic curves," *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 73-84, Mar. 2004.

[8] S. Khatoon, T. Thakur, B. Singh, "A provable secure and escrow-able authenticated group key agreement protocol without NAXOS trick," *International Journal of Computer Applications*, vol. 171, no. 3, pp. 1-8, 2017.

[9] C. Li, G. Luo, K. Qin, *et al.* "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127-133, 2017.

[10] J. Liu, S. L. Yin, H. Li and L. Teng, "A density-based clustering method for k-anonymity privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 1, pp. 12-18, Jan. 2017.

[11] S. Mccarthy, N. Smyth, E. O'Sullivan, "A practical implementation of identity-based encryption over NTRU lattices," *IMA International Conference on Cryptography and Coding*, pp. 227-246, 2017.

[12] A. Y. Niyat, M. H. Moattar, M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Optics & Lasers in Engineering*, vol. 90, pp. 225-237, 2017.

[13] S. Rajendran, M. Doraipandian, "Chaotic map based random image steganography using LSB technique," *International Journal of Network Security*, vol. 19, no. 4, pp. 593-598, 2017.

[14] H. Sharma, N. Khatri, "An image encryption scheme using chaotic sequence for pixel scrambling and DFrFT," *Proceedings of First International Conference on Smart System, Innovations and Computing*, pp. 487-493, 2018.

[15] X. Su, W. Li, H. Hu, "Cryptanalysis of a chaos-based image encryption scheme combining DNA coding and entropy," *Multimedia Tools & Applications*, vol. 76, no. 12, pp. 1-13, 2016.

[16] L. Teng, H. Li, S. Yin, "A multi-keyword search algorithm based on polynomial function and safety inner-product method in secure cloud environment," *International Journal of Network Security*, vol. 8, no. 2, pp. 413-422, 2017.

[17] L. Teng, H. Li, J. Liu and S. Yin, "An efficient and secure cipher-text retrieval scheme based on mixed homomorphic encryption and multi-attribute sorting method," *International Journal of Network Security*, vol. 20, no. 5, pp. 872-878, 2018.

[18] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem," *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61-71, Mar. 2004.

[19] S. L. Yin and J. Liu, "A k-means approach for map-reduce model and social network privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 6, pp. 1215-1221, Nov. 2016.

[20] S. Yin, L. Teng, J. Liu, "Distributed searchable asymmetric encryption," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 4, no. 3, pp. 684-694, 2016.

[21] Q. Zhang, L. T. Yang, X. Liu, Z. Chen, and P. Li, "A tucker deep computation model for mobile multimedia feature learning," *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 13, no. 3, pp. 1-39:18, 2017.

Biography

Shoulin Yin biography. He received the B.Eng. and M.Eng. degree from Shenyang Normal University, Shenyang, Liaoning province, China in 2016 and 2013 respectively. Now, he is a doctor in Harbin Institute of Technology. His research interests include Multimedia Security, Network Security, Filter Algorithm, image processing and Data Mining. Email:352720214@qq.com.

Jie Liu biography. Jie Liu is a full professor in Software College, Shenyang Normal University. He received his B.S. and M.S. degrees from Harbin Institute of Technology. He is also a master's supervisor. He has research interests in wireless networks, mobile computing, cloud computing,social networks, network security and quantum cryptography. Professor Liu had published more than 30 international journal papers (SCI or EI journals) on the above research fields. Email:ljnan127@163.com.

Lin Teng biography. She received the B.Eng. degree from Shenyang Normal University, Shenyang , Liaoning province, China in 2016. Now, she is a laboratory assistant in Software College, Shenyang Normal University. Her research interests include Multimedia Security, Network Security, Filter Algorithm and Data Mining. Email:910675024@qq.com.