A Homomorphic Encryption Algorithm for Chaotic Image Coding Data in Cloud Computing

Bin-bin Jiang(✉)

School of Software, Nanyang Institute of Technology, Nanyang, China
gongzuo8788@163.com

Abstract. The traditional image data encryption methods tend to ignore the classification of encryption attack types, resulting in poor security and accuracy of encryption results. In order to better guarantee the performance of chaotic image coding, a homomorphic encryption algorithm for chaotic image coding data in cloud computing environment is proposed. First, the homomorphic encryption matrix of coded data is normalized, and the homomorphic encryption parameters are calculated according to the results of the specification. According to the encryption parameters, the image encoding instructions are set, the common encryption attack types are divided, the encryption instructions are selected according to the partition results, and the accurate encryption of chaotic image coding data is finally realized. Finally, the experimental results show that the homomorphic encryption algorithm of chaotic image coding data in cloud computing environment has higher security and accuracy than the traditional encryption algorithm. It is indicated that the proposed encryption algorithm has a certain feasibility.

Keywords: Cloud computing · Chaotic image · Coded data · Homomorphic encryption

1 Introduction

The characteristic of the image data information is that the information amount is large, the correlation is strong and the redundancy is large, and these characteristics determine that the encrypted digital image data information cannot be encrypted directly using the text encryption algorithm [1]. For this reason, a new field of password research is created, which is image encryption. The feature of the image data information causes the information security researchers to design a better image encryption algorithm to better protect the digital image data information. In the image data information, the operation of the spatial domain is a technique based on the direct operation of the pixels [2]. In cryptography, image encryption in spatial domain is the process of encrypting image pixel value directly. This method only allows the authorized party to retrieve the original information and read it. In the practical application of image encryption, symmetric key encryption system is more widely used than asymmetric key encryption system. With the development of chaos theory, chaos technology has also been applied to the field of digital image data encryption [3]. Compared with the traditional image

G. Gui and L. Yun (Eds.): ADHIP 2019, LNICST 301, pp. 448–457, 2019.
https://doi.org/10.1007/978-3-030-36402-1_48

encryption algorithm, the key space is generally small, the key space generated by the hybrid system is large, and the distribution of the key space is more random. In addition, chaotic system has three basic characteristics: high sensitivity of initial value and control parameters, pseudo-randomicity of motion trajectory and simple realization of software and hardware. Based on these three characteristics, chaos technology is applied to digital image data encryption, and a chaotic-based digital image data encryption method is proposed.

2 A Homomorphic Encryption Algorithm for Chaotic Image Coding Data in Cloud Computing

2.1 Coded Data Homomorphic Encryption Algorithm

Compared with text data, digital image data has the characteristics of large amount of data, strong correlation of adjacent pixel data and high redundancy of whole pixel data. These characteristics make the traditional cryptosystem based on text information no longer suitable for digital image data encryption system [4]. According to the different characteristics of the two stages of image acquisition and processing, there are two main branches in the research of image encryption system: One is the encryption and decryption processing system based on digital image data acquisition/display, which is called digital image data information encryption/decryption system; The second is an encryption and decryption system based on digital image data information stored and transmitted in digital signal form, called a digital image cryptographic system. The digital image encryption and decryption system based on chaotic system belongs to the digital image cryptosystem, which is referred to as chaotic digital image cryptosystem. Chaotic encryption is one of the best alternatives to ensure security [5]. Due to the extreme sensitivity of chaotic mapping to initial conditions, unpredictability and random behavior, an image encryption scheme based on chaotic mapping is proposed based on these properties.

Chaotic mapping image encryption is the combination of word key, number or expression to encrypt the original image data. Because of the basic role of chaotic image data in various applications, the security protection of chaotic image data information has become an important topic for most image and data processing researchers [6]. Chaotic image coded data homomorphism encryption algorithm is a mathematical function used in encryption and decryption process. By using different combinations of keywords, numbers or expressions to encrypt the original data, the key strength is improved. Therefore, it is necessary to set the key privacy strength attribute matrix first in the coding area, if the key confidentiality intensity attribute matrix is R_{ij}, and:

$$R_{\mathrm{ij}} - \begin{bmatrix} 1.104 & 0.942 & 1.241 & 1.547 & 1.648 \\ 0.942 & 0.122 & 0.411 & 0.347 & 0.694 \\ 1.012 & 1.042 & 0.924 & 1.044 & 1.651 \\ 1.640 & 1.648 & 0.812 & 0.794 & 1.408 \\ 0.841 & 1.105 & 1.351 & 1.054 & 1.918 \\ 0.945 & 1.641 & 1.034 & 1.841 & 1.648 \end{bmatrix} \tag{1}$$

If R_{ij} is data feature extraction symbol type attribute. In the process of data encryption and filtering, the data exchange and contrast algorithm is carried out.

Setting m_i to be a different data characteristic symbol type attribute, wherein the selection range is (x, y), and N is the corresponding bad data characteristic attribute discrimination parameter, and the D_{zir} is a thermal encryption information extraction range reference function, the image coding carrying symbol is s, and the mixed image data constraint range is (i, j), so as to complete the primary filtering processing calculation on the bad information vocabulary, and the algorithm is as follows:

$$T_n = \log \frac{N}{Rm_i} [s(D_{zir}^2 + R_{ij}) - b] \tag{2}$$

If T_n is the weight factor of data encryption feature lookup, fron is the primary agreement condition of information filtering [7].

In order to ensure the accuracy of information filtering, it is necessary to retrieve the threshold range of information filtering. In the course of secondary processing, the maximum detection threshold range should be selected first, and the information filtering should be processed twice within the effective detection range. The selected algorithms are as follows:

$$\delta = \frac{1}{2} fron \sum_{j=1}^{i} T_{\mathrm{n}} s(R_{ij} a_n - 1) f(x, y) \tag{3}$$

In order to further encrypt the data, let $K(x_i, y_i)$ be the symbol attribute range of the data encoded by the information; e is the key word feature pre-processing screening parameter, the encryption parameters of chaotic image can be calculated effectively. The algorithm is as follows:

$$\mathrm{v} = \sum K(x_i, y_i) - \frac{1 + f(x, y)}{2\Delta\delta[\ln T_n - \ln R_{ij} - \delta] + \log(\ln e - 1)} \tag{4}$$

Combined with the above algorithm, the security parameters of homomorphic encryption of chaotic image coded data can be accurately calculated, thus the massive intrusion data in cloud computing environment can be effectively prevented and filtered.

2.2 Chaotic Image Encoding Encryption Instruction Setting

The image encoding and encryption technology of hull usually adopts pixel replacement on image or video, which makes the data difficult to decipher. This technique ensures the security of image data to a certain extent, but also changes the relationship between adjacent pixel values, so that the subsequent compression operation to be less suitable [8]. Homomorphic data encryption technology is a new method to encrypt sensitive digital image data, which is important in human perception. It improves encryption efficiency, satisfies real-time requirements better, and keeps file format unchanged. According to the requirement of bandwidth during transmission, chaotic image is encoded by homomorphic encryption technology. The principle of chaotic image coding is shown in the following Fig. 1:

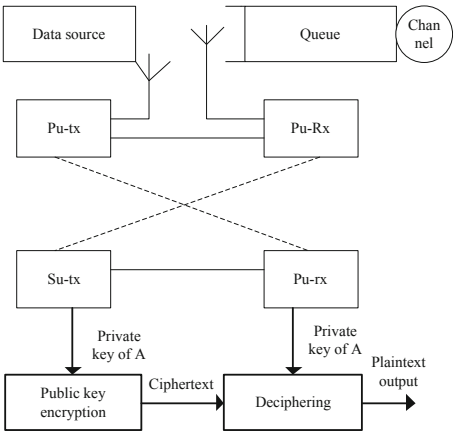


Fig. 1. Chaotic image coding principle

The chaotic image coding is optimized by homomorphic encryption algorithm. In the process of encryption and coding, the plaintext image is transcoded by encryption key, and the encrypted ciphertext image is obtained. Then the encrypted ciphertext image and encryption key are sent to the receiver [9]. The cipher text image encrypted by the receiving end uses the same key to decrypt, and the decrypted image is the plain text image, and the process completes the encrypted transmission of the digital image data information. Encryption on the spatial domain is the operation of each pixel value in plaintext image data, that is, the operation is done directly in pixels. Full and partial encryption can be performed on a spatial domain [10]. In complete encryption, consider the entire image value and encrypt each pixel. In the process of encryption, the main instructions of chaotic image encoding and encryption should be designed. Because the encryption password is relatively private, the imitating instruction proposed in this paper is used as a substitute. In order to describe the chaotic image symbols and their meanings, a password convention is carried out. The initial SP authentication convention instruction is constructed as follows:

(a) Suppose the server-side SP is identified as IDs, SP sending instructions to IDA:

$$\mathrm{SP} \rightarrow \mathrm{IDA} : \{(\mathrm{hash2}(\mathrm{hash2}(\mathrm{IDs}) \| \mathrm{N})\}$$

(b) IDA authenticates SP with the following authentication instructions:

$$\begin{aligned} \mathrm{forIDA} \ + \ \{&\mathrm{Received}(\mathrm{hash2}(\mathrm{hash2}(\mathrm{IDs}) \| \mathrm{N}) \\ &= (\mathrm{hash2}(\mathrm{hash2}(\mathrm{IDs}) \| \mathrm{x}); \mathrm{x} = \mathrm{x} + 1; \} \end{aligned}$$

When the IDA again requests the SP to provide the transcoding encryption service, the saved image information list L can be used for verification, and the one-time public key is not needed to be constructed, and the IDA does not change the authentication method of the SP. The following is an example of an SP-to-IDA authentication:

(a) IDA sends instructions to the SP:

$$\mathrm{IDA} \rightarrow \mathrm{SP} : \{\mathrm{hash2}(\mathrm{ID_i}), \mathrm{hash2}(\mathrm{hash2}(\mathrm{ID_i}) \| \mathrm{x})\}$$

(b) SP authenticates IDA with the following authentication instructions:

$$\mathrm{ForallH} \in \mathrm{L} \left\{ \begin{array}{c} \mathrm{Receivedhash2}(\mathrm{hash2}(\mathrm{ID_i}) \| \mathrm{x}) \\ \mathrm{hash2}(\mathrm{H} \| \mathrm{N} + 1)\mathrm{N} + 1\mathrm{SaveNinL}. \end{array} \right\}$$

the encryption protocol can realize the two-way authentication between the terminal IDA and the server SP. When IDA visits the service for the first time, SP authenticates the IDA by verifying the one-time public key, that is, by judging whether the equation $\mathrm{e}(\mathrm{P_i}, \mathrm{P}) = \mathrm{e}(\mathrm{U_i}, \mathrm{P})$ is valid or not. Only legitimate users registered in the TC can pass the authentication. If $\mathrm{e}(\mathrm{P_i}, \mathrm{P}) = \mathrm{e}(\mathrm{U_i}, \mathrm{P})$, the Pi contains the system master key, as a result, the sender has registered. After IDA access, the x cannot be calculated even if the attacker intercepts, only the real SP owns the private key SP, through the calculate the random number x to provide the correct hash value $\mathrm{hash2}(\mathrm{hash2}(\mathrm{IDs}), \mathrm{N})$. According to the security condition of hash function, it is difficult for the attacker to obtain the correct hash value under the condition of N unknown, thus realizing the validity of the current verification. In the post-IDA access, only legitimate terminals can authenticate IDA, through hash table lookup.

2.3 Realization of Homomorphic Encryption of Chaotic Image Coded Data

Because the digital image data information is different from the text data information, it has the characteristics of large amount of data, strong correlation of adjacent pixel data and high redundancy of the whole pixel data. For some reasons, traditional text data encryption algorithms such as RSA, DES can not be directly used in digital image data encryption. One of the reasons is that the size of the image is much larger than the text, so the traditional cryptosystem needs a lot of time to process the image data by direct public key cryptosystem. The public key cryptosystem is based on the mathematical

one-way function. It uses two keys to separate the encryption and decryption functions, one key as the encryption key and one key as the decryption key. Through the conversion of encryption and decryption key, secure socket layer protocol for secure communication and digital signature can be realized by the same technology. Secure Sockets layer (SSL) is a secure data transmission technology developed by the company. It can prevent the communication between client and server applications from being eavesdropped by attackers, and can always authenticate the server and choose to authenticate the client. The advantage of the protocol is its independence from the application layer protocol. It ensures that the encryption algorithm is completed before the communication of the application layer protocol, the negotiation of the communication key and the authentication of the server. After that, the data transmitted by the application layer protocol will be encrypted. At the same time, because the transmitted message includes the integrity check of the message, the protocol provides a higher security channel is the confidentiality, integrity and reliability of the secure transaction protocol, complete the encoding and encryption of the image data. The detailed chaotic image coding data homomorphism encryption steps are shown in Fig. 2:

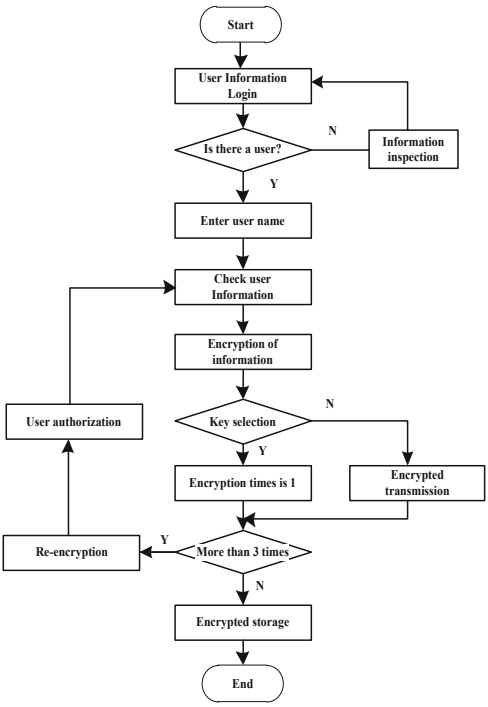


Fig. 2. Steps of homomorphic encryption of chaotic image coded data

In the process of homomorphic encryption of chaotic image coded data, the decrypted image with small distortion is acceptable. In addition, the security analysis of image encryption is a technique to decrypt all or part of the ciphertext without knowing

the decryption key. Therefore, in the process of decryption, we need to rely on the information and control system, through encryption analysis to obtain the key or part of the key, decrypt the image or part of the decryption image. In the decryption process, the type of the image encryption attack is divided according to the difficulty degree of the attack, and the method comprises the following steps of:

(1) Ciphertext attack only: Also known as violent attacks, The cipher text image attacker can only master the cipher text data information, analyze the cipher text data by using the poor lifting method, and try to find out the key. This kind of attack is impossible to design and perfect the encryption system. Ability to prevent known ciphertext attacks is a minimum requirement for an encryption scheme
(2) Known plaintext attack: The encryption analyst has a string of clear text P and its corresponding ciphertext C, which will help the encryption analyst to determine the key or part of the key, thereby attacking the ciphertext image.
(3) Select clear text attack: The encryption analyst can choose to input the plaintext image data into a closed system containing encryption algorithm and encryption key. The closed system will output the corresponding ciphertext image data information, and after analysis, According to the relationship between the plaintext image data information and the ciphertext image data information, the encryption analyst finds out some or even all of the keys.
(4) Select a ciphertext attack: The encryption analyst can choose to input the information of ciphertext image data into a closed system containing encryption algorithm and encryption key, and the closed system will output the corresponding plaintext image data information, and after analysis, According to the relationship between the plaintext image data information and the ciphertext image data information, the encryption analyst finds out some or even all of the keys.

In order to ensure the security and stability of chaotic image data homomorphic encryption security and stability can be ensured by dividing the characteristics of the above attack types and selecting the coded encryption key and the transcode password in order to ensure the security and stability of chaotic image data homomorphism encryption.

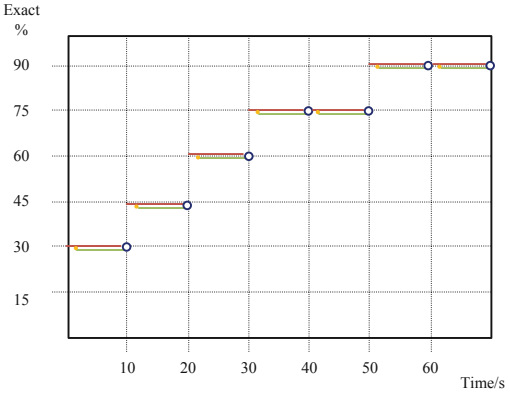
3 Experimental Results and Analysis

The experiments of encryption and decryption of digital images of different sizes are carried out, and the time consuming of encryption and decryption process is recorded, and the statistics of encryption and decryption speed are analyzed. Experimental environment information for CPU Core dual-core 2.26 Ghz, memory 4 GB notebook computer, system for Debian7.5, simulation software for Matlab7.0. Because the quality of chaotic picture is relatively low and the definition is not enough, in order to get the characteristics of the image and encrypt it accurately, it is necessary to collect the bitmap and pixel of the image in the process of encrypting the transcode, and so on, in order to get the character of the image better and carry on the accurate transcoding encryption processing. The average encryption/decryption time of digital images with different pixel sizes is obtained, and the data is shown in the following Table 1.

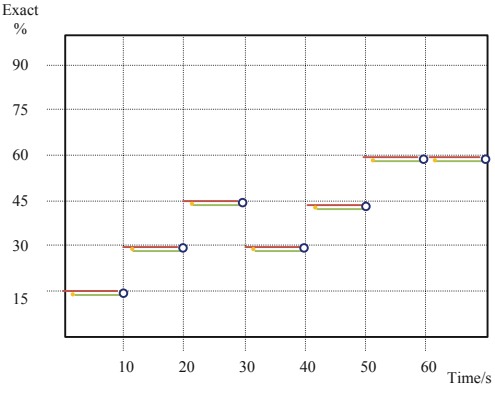
Table 1. Parameters affecting chaotic Image encryption

Image size (pixels)	Bitmap (bit)	Average encryption time (s)
256 * 256 * 3	24	0.90
512 * 512 * 3	24	1.24
876 * 876 * 3	24	1.64
1024 * 1024 * 3	24	2.03
2063 * 2063 * 3	24	2.64

In the above parameter environment, the traditional encryption method and the homomorphic encryption method proposed in this paper are used to encrypt the image data respectively, and the accurate values of the authentication encryption method are



(a)Experimental group



(b)Control group

Fig. 3. Comparison of experimental results

recorded and compared. In the process of detection, the higher the coding accuracy value is, the more accurate the image data is. The better the encryption, the better the security and stability. The test results are as shown in Fig. 3:

As shown in Fig. 3, the accuracy of traditional methods for encoding and encrypting chaotic images is relatively low. However, the encryption accuracy of the homomorphic addition algorithm for chaotic image coding data based on cloud computing environment is obviously better than that of traditional methods under the same experimental environment and parameters, which fully satisfies the research requirements.

4 Conclusion

In order to study the encryption technology of chaotic image data, a homomorphic encryption algorithm for chaotic image coded data in cloud computing environment is proposed. The design flow and main steps of the scheme are given, and the experimental results and safety are analyzed. The experimental results show that the homomorphic encryption algorithm for chaotic image coded data in cloud computing environment can produce one-dimensional chaotic sequences with better chaotic performance and larger chaotic range. It is proved that the encryption algorithm is effective and has good performance in digital image data encryption and various attacks.

In this paper, through the homomorphism encryption algorithm of encoded data, the encoded homomorphic encryption matrix is constructed, the common types of encryption attacks are analyzed, and the image coding instructions are segmented. On the basis of this, the encryption of chaotic image encoded data is realized. This method can effectively encrypt the image data according to the attack type, and provide a new idea for chaotic image encryption.

References

1. Xiang, S., Yang, L.: Robust reversible watermarking algorithm for images based on homomorphic encryption system. J. Softw. **29**(4), 957–972 (2018)
2. Shi, J., Yang, G., Sun, Y., et al.: Efficient parallel homomorphic encryption algorithm supporting floating point operations. Comput. Sci. **45**(5), 123–129 + 137 (2018)
3. Yang, X., Chen, Z., Han, T.: Improvement and application of homomorphic encryption algorithm in application scope and efficiency. Comput. Eng. Des. **38**(2), 318–322 (2017)
4. Qin, J., Wang, X., Wang, G.: Identity-based homomorphic encryption and its application in cloud computing. Comput. Program. Ski. Maint. **46**(6), 93–95 (2017)
5. Zhu, S., Li, J., Wang, W.: Security analysis of improved image encryption algorithm based on DNA coding and chaos. Comput. Appl. Res. **34**(10), 3090–3093 (2017)
6. Zhang, W., Wang, D., Meisheng, Yu.: Image encryption algorithm based on two independent chaotic functions. J. Chongqing Univ. Posts Telecommun. (Nat. Sci. Ed.) **29**(2), 232–239 (2017)
7. Xiong, J., Deng, Z.: An image stream encryption algorithm based on nonlinear chaos and data sharing. Electron. Technol. Softw. Eng. **53**(4), 194 (2017)

8. Niu, Y., Zhang, X.: Chaotic image encryption algorithm based on bit permutation and nucleic acid sequence library. Comput. Eng. Appl. **53**(17), 130–136 (2017)
9. Lei, J., Xiao, L.: Design of digital image chaotic encryption system based on SOC technology. Inn. Mong. Sci. Technol. Econ. **35**(19), 95–96 (2017)
10. Lin, Z., Hu, Q., Li, J., et al.: Image encryption algorithm based on hyperchaotic sequence and bit plane scrambling. J. Nanchang Univ. (Eng. Ed.) **39**(2), 169–174 (2017)