Research on Medical Image Encryption Method Based on Uniform Scrambling and Chaotic Mapping Based on Swarm Intelligence

Kun Li, Jing Liu, Chunfeng Song

Faculty of Network Science, Haikou University of Economics, Haikou, Hainan, 571127, China

Keywords: Swarm intelligence algorithm; uniform scrambling; chaotic mapping medicine; image encryption

Abstract: Medical images need to be encrypted in the process of storage and transmission because of the important issues such as privacy, in order to improve the quality of medical image encryption and ensure the speed of encryption. Based on swarm intelligence (swarm intelligence) algorithm, the medical image encryption methods of uniform scrambling and chaotic mapping are studied. A uniform scrambling method based on Arnold mapping is used, and a pseudo-random number is generated in combination with the logistic map to control the scrambling parameters, and the values of the pixel points are XORed to further encrypt the image. The experimental results show that the image encryption algorithm has a large key space, is sensitive to the initial conditions of the key, has a high degree of grayscale scrambling, and has fast encryption and decryption speed. It is suiTable for real-time encryption protection of digital image information on the Internet.

1. Introduction

The image is two-dimensional information, and the amount of information is large. Many traditional encryption functions designed for one-dimensional information cannot ensure good coverage of image information. Therefore, chaotic systems are introduced into image encryption algorithms [1]. However, while the Internet provides us with powerful functional advantages, it also leaves an opportunity for unauthorized individuals to intercept information. They often maliciously copy, spread or destroy them after interception [2]. In order to remain invincible in the competition, many companies often need to invest a lot of manpower and resources to carry out preliminary research work on cutting-edge technology, as the company's technical reserves [3]. Chaotic systems have many excellent properties, such as sensitive dependence on initial conditions and system parameters, ergodicity of States and mixed diffusion (stretching and folding) characteristics. When the information contained in the image is personal privacy, company's confidential information and the national situation is confidential, the security and importance of image transmission is more prominent [4]. Therefore, as an important data encryption technology and an effective means of security enhancement, the research of digital image scrambling technology in the pre-processing of message and carrier image is of great significance to improve the security of information camouflage system [5]. Therefore, information security and information protection have become a hot research topic.

The use of the Internet to transmit information is a mainstream way, the main reasons include: geographical independence, no time constraints, and low cost [6]. Chaotic systems are sensitive to initial values and have self-similarity. Research results, such as electronic design and mechanical design, are largely preserved in the form of technical drawings. Their security and confidentiality issues are of great importance to companies [7]. But it is also a very difficult problem. How to ensure the convenience of use and the security of these data has become an urgent problem for major companies. Therefore, it is necessary to encrypt the image data [8]. These characteristics meet the requirements of the cryptosystem for chaos and scatter characteristics, so chaotic systems are ideal for constructing cryptosystems. Therefore, when the ever-changing network and communication technologies bring us convenience, there are also many security risks [9]. With the gradual emergence of problems, some scholars began to explore the security of digital images in the field of digital imaging [10]. The former can be further divided into a scrambling method based on

  DOI: 10.25236/mmmce.2019.007

two-dimensional affine transformation and a scrambling method based on pixel position migration. The latter can be further divided into a scrambling method based on single pixel gradation and a scrambling method based on multi-pixel gradation. Given the statistical nature of the original image and the encrypted image, the encryption strength of these algorithms is still not ideal.

2. Uniform scrambling and logistic mapping

2.1 Evenly scrambled

The chaotic encryption algorithm has the characteristics of sensitivity to initial conditions, aperiodicity, non-convergence and control parameters. However, using the formula alone to scramble the image, the iteration will have a certain periodicity, that is, the iteration will lose the encryption after a certain number of iterations. However, almost all algorithms are based on pixel scrambling and encryption, especially pixel-based scrambling encryption algorithms, and their security needs to be improved. However, most of these discrete chaotic cryptosystems use only one chaotic map, which has the following disadvantages: one is that the key space is small, so that the function of anti-exhaustive attacks is weak; the other is that it is vulnerable to phase space identification. And by combining digital images with cryptography, a new type of image encryption technology, namely image scrambling technology, is further proposed. Making full use of the chaotic mapping's characteristics of disorder, randomness and sensitivity to initial values, the Logistic chaotic mapping is applied to the principle of sequence crossover, and a double combination algorithm is proposed. Through analysis, the partitioned blocks can be restored, and the Arnold scrambling parameters used in the algorithm are fixed. However, these algorithms only consider location scrambling encryption, and the size of the pixel value has not changed. Then, the chaotic sequences generated by the three-dimensional Chen system are used to encrypt the red, green and blue primary colors of the scrambled image respectively. In addition, a new ciphertext output feedback mechanism is introduced in the encryption process, which improves the sensitivity of ciphertext to plaintext.

Table 1 lists the results of correlation coefficients calculated in three directions. The results show that the adjacent pixels of the original plaintext image are highly correlated, and the correlation coefficients are close to 1. The correlation coefficient of adjacent pixels of encrypted image is close to 0, and the adjacent pixels are basically uncorrelated, which indicates that the statistical features of plaintext have been well spread to random ciphertext.

Table 1 Coefficient of correlation between adjacent pixels in plaintext and ciphertext

Direction	Plaintext	Ciphertext
Horizontal direction	0.9394	-0.0004
Vertical direction	0.9754	-0.0035
Diagonal direction	0.9154	0.0017

2.2 Application of Logistic Mapping in Image Encryption

In order to hide the information further, the random number is generated by logistic mapping, and the bitwise exclusive or operation is performed with the image pixel value. Considering the simplicity and high security, many researchers use one-dimensional chaotic system to improve the algorithm. Researchers have organically combined multiple chaotic systems and used DES-like algorithms to scramble images. These algorithms have achieved good results. The design of the algorithm should consider not only the sensitivity of the final key to the subtle changes of the initial key, but also the sensitivity of the ciphertext to the subtle changes of the plaintext, and the uniformity of the ciphertext diffusion distribution, as well as the breadth of the initial key space. This important encryption method has been valued by scientific researchers, and many valuable encryption methods have been proposed one after another. Through continuous improvement and overthrowing, more and more mature scrambling encryption technology has been proposed and has been well applied. . The quantized value of the Logistic chaotic sequence is used to determine which combination needs to be inserted, which is called “combination one”. Logistic mapping is

also used to generate Arnold mapping parameters to better mask information. A good encryption method should be extremely sensitive to the key, the key space is large enough, and it must have the ability to withstand the statistical analysis of external attacks, ie grayscale distribution. It makes the image every row and every column have the opportunity to scramble, and at the same time makes the algorithm one time and one dense, which improves the image scrambling efficiency and makes the sequence crossover algorithm generalized.

3. Analysis of several image scrambling algorithms

3.1 Analysis of Image Encryption Methods Based on Two Chaotic Sequences

A scrambling method combining Logistic mapping and tent mapping is used to encrypt an original image. Here, in order to make the encrypted ciphertext sensitive dependent on the encrypted object, a mechanism for generating a point of encryption key after the previous ciphertext output control is introduced. To this end, the algorithm takes a bit plane based scrambling. Two rounds of encryption are performed on the entire image, and C0 used for the first point of the first round is pre-specified, and the first point of the second round is encrypted using the ciphertext outputted by the last point of the previous round. This makes it possible to cause a change in all pixels of the entire image regardless of whether the change in the plaintext occurs anywhere. The generated key sequence IntKey is sensitively dependent on the change of any plaintext point. The pixel values of the image after being scrambled by the bit plane have been completely destroyed, and the encrypted image is almost the same from the visual visual effect, and can realize complete undistorted decryption and restoration. However, increasing the parameters will affect the implementation and increase the computational complexity. For example, using more than one encryption algorithm will also reduce the efficiency of image encryption. The decryption algorithm is the inverse operation of the above operation, that is to say, the scrambling strategy and the pseudo-random sequence used to modify the pixel value can be obtained by the same key, and the pixel value can be restored by XOR again, and the whole process can be completed by putting the pixels in place.

Fig. 1 is the histogram of the plaintext Lena image used in this experiment. Fig. 2 is the two histogram validation data of the corresponding ciphertext image encrypted by this algorithm.

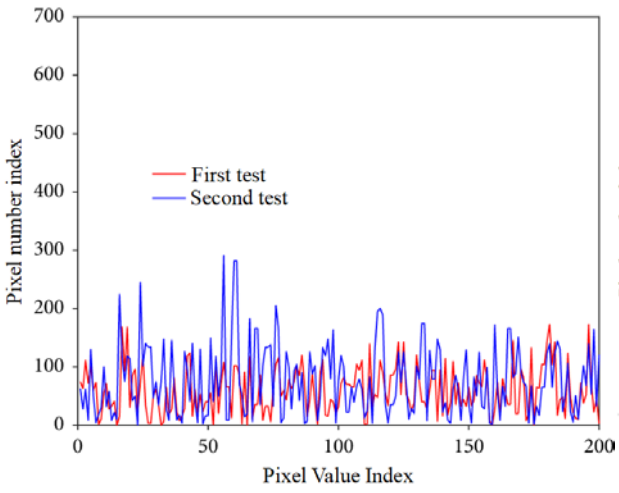

Fig.1. Histogram of plaintext image

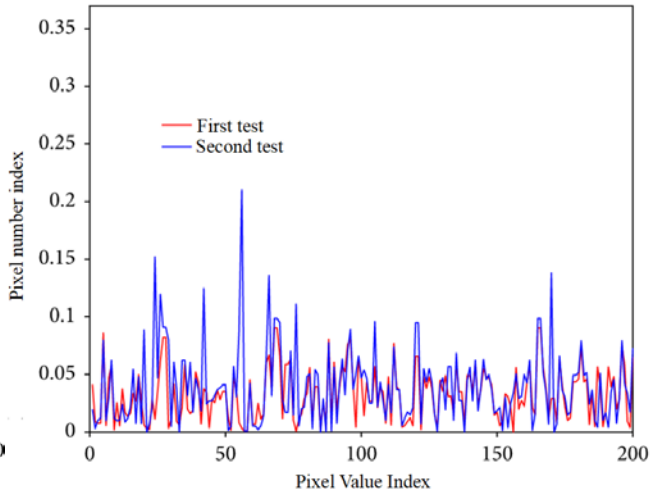

Fig.2. Histogram of ciphertext image

3.2 Analysis of New Two-Dimensional Mapping Image Scrambling Algorithms Based on Image Segmentation

Based on the image segmentation algorithm, each pixel of the image is connected into a straight line according to some mapping, and then folded according to the original size of the image. In this way, the image position is scrambled, and then the generated chaotic sequence is used to form a diffusion function to change the pixel value of the image, and finally the image encryption is

realized. Because in the double combination algorithm, if the initial value of the chaotic map is different, the correlation coefficients of the scrambled image will be different. For this reason, 30 groups of different initial values can be selected to scramble the image separately, and the correlation coefficients obtained under different initial values can be averaged. In order to improve the sensitivity of the ciphertext to the key, the chaotic map is first pre-iterativeed N times, and the sequence generated by the iterative process is used as the sequence for generating the intermediate key. Another way to encrypt an image is to perform histogram analysis on the image. At the same time, gray distribution encryption is implemented according to pixel bits, and the algorithm can further enhance the encryption strength and improve the security of encryption. There are two total key parameters, and the two parameters have a large range of values, which is in line with the large key space, which increases the difficulty of deciphering. The biggest advantage of this algorithm is that the processing of non-square images is the same, there is no limitation on the selection of images, and redundant information is not added. However, the grayscale scrambling factor is small, which will affect the scrambling effect.

4. Conclusion

The encryption algorithm that combines uniform scrambling with logistic mapping makes up for the shortcomings of these two encryption methods when used alone. Further research on the algorithm can be extended to high-dimensional chaotic maps to achieve higher security image encryption. The algorithm is simple and easy to implement in hardware, and the encryption/decryption efficiency is high; the security of the encryption algorithm depends only on the key and has a large enough key space. It can completely resist various attacks such as exhaustion and has been applied to the encryption/decryption of a company's technical drawings. The pixel substitution is based on the combined encryption of the two-dimensional chaotic system, which overcomes the shortcomings of the single one-dimensional chaotic system and the inability to resist the phase space reconstruction attack. In this paper, a position scrambling method combining layered rotation and cyclic shift is proposed to encrypt the image. The diffusion function is used to scramble its gray value, and the plaintext control key is used to generate the key, which makes the chaotic parameters or plaintext change slightly, and the ciphertext will be greatly affected. A large number of experiments show that this method successfully solves the limitation that the direct sequence crossover algorithm only applies to even element images, and improves the accuracy of a single key to 10-9 orders of magnitude. After image encryption, the pixels change dramatically, which can cover up all the original information and protect the patient's privacy.

Acknowledgement

Funding: This work is supported by Hainan Provincial Natural Science Foundation of China(No. 619QN246).

References

[1] Sanchez V M, Chavez-Ramirez A U, Duron-Torres S M, et al. Techno-economical optimization based on swarm intelligence algorithm for a stand-alone wind-photovoltaic-hydrogen power system at south-east region of Mexico[J]. International Journal of Hydrogen Energy, 2014, 39(29):16646-16655.

[2] Ntouni G D, Paschos A E, Kapinas V M, et al. Optimal detector design for molecular communication systems using an improved swarm intelligence algorithm[J]. Micro & Nano Letters, 2018, 13(3):383-388.

[3] Gao P, Wang S, Lv J, et al. A database assisted protein structure prediction method via a swarm intelligence algorithm[J]. RSC Adv. 2017, 7(63):39869-39876.

[4] Zhang X, Yu J. Power Load Forecasting Based on Swarm Intelligence Algorithm[J]. Journal of

Computational and Theoretical Nanoscience, 2015, 12(12):5323-5332.

[5] Sobecki, Janusz. Comparison of Selected Swarm Intelligence Algorithms in Student Courses Recommendation Application[J]. International Journal of Software Engineering and Knowledge Engineering, 2014, 24(01):91-109.

[6] Nurhanim K, Elamvazuthi I, Vasant P, et al. Joint Torque Estimation Model of Surface Electromyography(sEMG) Based on Swarm Intelligence Algorithm for Robotic Assistive Device[J]. Procedia Computer Science, 2014, 42:175-182.

[7] Fouda J S A E, Effa J Y, Sabat S L, et al. A fast chaotic block cipher for image encryption[J]. Communications in Nonlinear Science & Numerical Simulation, 2014, 19(3):578-588.

[8] Wei X, Guo L, Zhang Q, et al. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system[J]. Journal of Systems and Software, 2012, 85(2):290-299.

[9] Bai S, Zhu G B, Ji X Y. Comments on “A Novel Image Encryption-Compression Scheme Using Hyper-Chaos and Chinese Remainder Theorem”[J]. Applied Mechanics and Materials, 2015, 743:333-337.

[10] Zhang Y Q, Wang X Y. Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation[J]. Nonlinear Dynamics, 2014, 77(3):687-698.