Advances in Engineering Research (AER), volume 82
2016 International Conference on Engineering and Advanced Technology (ICEAT-16)

Research on medical image encryption based on DES algorithm

Rui Wang[1,a], Jinguo Wang[2,b*], Na Wang[3,c]
[1]Department of Information Engineering,Jilin Business and Technology College China
[2]Department of Urology, the First Hospital of Jilin University,China
[3]Department of Anaesthesiology, the First Hospital of Jilin University, China
[a]Xiaoben6666@126.com,[b]wangjinguolily@163.com,[c]lilyly12345@163.com
*corresponding author

Keywords: Medical image. DES algorithm.

Abstract. The 3D chaotic system, the algorithm is very complex, the operation speed is slower than one dimension mapping, but it has a large key space and high security. The improved DES algorithm proposed in this paper can take into account the security of the algorithm, the operation speed and the realization of the algorithm. In order to achieve the highest level of security, we must be able to make the complexity of time and space is relatively small, the key space is relatively large, and can overcome the inherent shortcomings of DES algorithm.

1. Introduction

In order to simplify the exchange of medical image information, the standard of storage format and transmission mode of medical image is introduced. Medical image visits because medical image standards and remote medical treatment has become very easy, but the data is changed as well as the risk of being attacked also increased accordingly. According to the law, the patient's case data must be encrypted to spread online, which requires a feasible method to protect the security of these data, which is also the target of medical image data encryption to achieve.

Cryptography research began in 1970s. Shannon in 1949 published a "communication theory of secrecy system"[1]. Since then, the development of mathematics theory and computer science has made more scholars pay attention to the field of cryptography. Diffie and Hellman proposed the idea of the public key cryptography in the papers published in 1976, which is suitable for the network secure communication, so the scholars began to study the public key cryptography in cryptography field[2]. In 1978, Rivest and other proposed RSA code system is an important milestone in the development of cryptography. Robert and Matthews for the first time to be mixed with pure technology applied to cryptography, in 1989, they proposed a hybrid Logistic mapping based on the mixed flow cipher scheme[3]. Since then, many domestic and foreign scholars have started to design encryption method based on the theory of mixed theory and discuss its security. As a result, it is

gradually as a branch of research. Because of the close relationship between pure mixed theory and modern cryptography and communication theory, it is a new method to study the mixed cipher in the ninety's. Using pure mixed system to design a password, only a very short period of more than 20 years, the scholars have only a relatively junior understanding of mixed password. So, the present study mixed pure password system only in the exploratory stage in the field there are many issues that need further research[4].

2. Chaotic block cipher

The relationship between chaotic maps and Cryptography**.** Block cipher is a kind of mapping, it satisfies the conditions,Same points of chaos map and password transformation[5]:

1、Two transformations are all determined, and all have similar characteristics.

2、There is a consistent performance of the hybrid characteristics of the chaotic map with the existence of the topological transport and the password.

3、Both sensitive to initial values and parameters.

The biggest difference between the chaotic map and the cipher transformation is that it can be defined on a continuous closed set, but the operation of the cipher is only in the finite field. So, it is a need to design a hybrid mapping application to the password system.

The relationship between design block cipher and chaotic map. The design of block cipher is to search for an algorithm, which can be used to find a replacement in the key of the key. If you use a good mix of Jing principles and principles can be spread, it will transform encryption safe enough. The chaos principle design of cryptographic algorithms can let the secret key and the cipher text and plaintext and cipher text have quite complex relations, so the cryptanalyst cannot take advantage of this relationship to decipher the password. Diffusion principle one design of cryptographic algorithm can make every key can affect the number of bits of the digital, so the code cannot be decoded by the secret pin, and each of the clear number can also affect a number of cipher numbers, so that the statistics can be hidden.

Chaos: the typical performance of the mapping is to fold and stretch in a limited area. Due to the mixed Pei with aliasing properties, indicating that in the mapping and the role of, any non-zero measure sets, through evolution will spread to the whole phase space. Another useful property of chaotic systems is that any initial distribution is not uniform in the dynamic system. Because the system has the characteristics of mixing, and the last of these sets tend to be uniform. In view of this, the application of chaotic mapping in block cipher, the data can be quickly spread and mixed jing. In order to be able to achieve the confusion and diffusion of data, many block cipher systems are used to "set" and "replace" method.

3. DES algorithm based on two dimensional chaotic maps

DES algorithm. DES algorithm is obtained by the development of Lucifer password; it is a traditional packet encryption method. The theory of DES algorithm and the

accumulation of hardware and software have been thirty years of history, although the advanced data encryption standard AES has been replaced by the algorithm, but scholars are still keen to improve the DES algorithm, to further improve its security.

Since DES algorithm is made, it caused the academic and business circles of considerable importance. The DES algorithm, which has been studied deeply, has greatly promoted the theoretical research of the cryptography. Moreover, the security of DES algorithm has been suspected by many scholars, the criticism of it mainly focuses on three aspects: the length of the key, the number of iterations and the design of the S box.

DES algorithm is a Feistel type of password, fully embodies the principle of confusion and diffusion. DES algorithm is a group of encryption algorithm, which is based on the 64 bit text as a packet encryption. At beginning of the algorithm, inputting 64 bits proclaimed in writing, and then it will output 64 bits cipher text. DES algorithm is a symmetric algorithm, that is, the encryption and decryption shared the same password. Key length is 56 bits. Keys should be 64, but each eighth bit is used for parity check. The key is an arbitrary 56 digit, and can be changed at any time. There are very few weak keys, which need to be avoided, because the secrecy is dependent on the key.

4. Improved DES algorithm

The DES algorithm of the dense pin dynamics is achieved by means of two-dimensional Logistic mapping and Henon mapping. The realization of the dynamic change of the DES algorithm is the key to design the algorithm. That is to say, the key in the original algorithm is invariable, and now, after each encryption, the next round of the key is to be changed, and the new key and the last round of the key is not any linear relationship, which is the need of the chaos sequence.

The algorithm can also be used to design the two-dimensional Henon mapping, and the two-dimensional Logistic mapping is the second. The two-dimensional Logistic map is used in this paper as following:

(1)

The encryption step of the improved DES algorithm is:

1. The chaotic system is carried out by N_0 iteration, which makes it into the state of chaos.
2. After a N_{0+i} (i=1,2,……)iteration, a set of keys is generated K_i.
3. Number the points in the image from the top to bottom and left to right.
4. In the image, select a point P_i, converted it value to binary B_i, at the same time the value K_i converted to binary . It has

(2)

In which, is the value of the pixel points after the encryption. Finally, the value of the point is converted to a decimal value, which is placed in the original position of the image.

5. Repeat step (2) and step (3), until all the points in the image are encrypted, and the encrypted image is obtained.

5. Security analysis of improved DES algorithm

The important symbol of the information age is that the Internet has been rapidly spread, so that a large amount of information can be shared, but the data is also very easy to leak, tampering and counterfeiting, so to ensure the safety of information is a key issue. Medical image encryption is needed to encrypt and hide information. On the other hand, it is a lossless image in the process of encryption. Analysis of the encryption algorithm of the image is to be able to secure storage and transmission of images, which is very important for the safety of medical image data.

Because of the logistic mixed with pure systems have very complex dynamic performance, the statistical relationship between the plain text and the cipher text is very complex. That is, if the crack is obtained from the statistical relationship between the text and the text, it is difficult to predict the key.

The improved DES algorithm is applied to medical image encryption. The simulation results show that the encrypted image has the kind of noise, and the information is very difficult to identify the key. Thus, it can effectively protect the image data. Finally, the security of the algorithm is demonstrated by several attack methods.

References

[1] Pay-Chin Leow,Priti Bahety,Choon Pei Boon,Chong Yew Lee,Kheng Lin Tan,Tianming Yang,Pui-Lai Rachel Ee. Functionalized curcumin analogs as potent modulators of the Wnt/β-catenin signaling pathway[J]. European Journal of Medicinal Chemistry . 2014.

[2] V. Tomar,G. Bhattacharjee,Kamaluddin,Ashok Kumar. Synthesis and antimicrobial evaluation of new chalcones containing piperazine or 2,5-dichlorothiophene moiety[J]. Bioorganic & Medicinal Chemistry Letters . 2007 (19).

[3] Sylvie Ducki,David Rennison,Meiko Woo,Alexander Kendall,Jérémie Fournier Dit Chabert,Alan T. McGown,Nicholas J. Lawrence. Combretastatin-like chalcones as inhibitors of microtubule polymerization. Part 1: Synthesis and biological evaluation of antivascular activity[J]. Bioorganic & Medicinal Chemistry . 2009 (22).

[4] Babasaheb P. Bandgar,Sachin A. Patil,Rajesh N. Gacche,Balaji L. Korbad,Balwant S. Hote,Santosh N. Kinkar,Shivkumar S. Jalde. Synthesis and biological evaluation of nitrogen-containing chalcones as possible anti-inflammatory and antioxidant agents[J]. Bioorganic & Medicinal Chemistry Letters . 2009 (2).

[5] K.L. Lahtchev,D.I. Batovska,St.P. Parushev,V.M. Ubiyvovk,A.A. Sibirny. Antifungal activity of chalcones: A mechanistic study using various yeast strains[J]. European Journal of Medicinal Chemistry . 2008 (10).