The Research and Implementation of 3DES Encryption Algorithm Based on Chaos System

Heyuan WANG[1, a], Jian-nan XU[2,b]
[1]*College of Sciences , Liaoning University of Technology, Jinzhou 121001, China*
[2]*Liaoning Petro-chemical Vocational Technology College, Jinzhou 121001, China*
[a]*wangheyuan6400@sina.com,* [b]*693196257@qq.com*

Abstract

This paper introduces the DES encryption algorithm and the characteristics of chaotic encryption algorithm, and propose a kind of hybrid encryption algorithm based on Rossler chaos equations and 3DES. The algorithm generate 3DES cryptographic key by Rossler chaos equations, and expand the 3DES encryption algorithm cryptographic key space. Simultaneously we realize this algorithm by using C++ procedure , the numerical simulation results show that the algorithm is feasible.

Keywords: chaos; DES algorithm ; cryptographic key; Rossler systems; numerical simulation.

1 Introduction

Recently, encryption technology has been developed quickly and many image encrypt methods have been put forwarded(as discussed elsewhere [1, 2]).The chaotic encryption is applied in image encryption due to its randomness and sensitivity. The technologies of chaotic encryption are widely used in information security fields, such as network communication and image encryption.Chaos is produced by deterministic nonlinear systems, which has noise-like, broadband frequency spectrum character, it is pseudorandom, reproducible phenomena, and chaotic system is extremely sensitive to initial condition, so chaos can be novel

nature cryptosystem. If we make use of chaos in image encryption techniques, the image encryption algorithm will have a good efficiency and be safer.In the early 70 s video image encryption algorithm was proposed, and widely used in the late 90 s;1999 Romeo present the RPK encryption algorithm(as discussed by Romeo A.Romdolti G,Nattavelli N [3])； In 2002 Bao Guanjun designed the image encryption algorithm (as discussed by BAO Guanjun，JI Shiming [4]). In 2006 ShangYanhong put forward the method of scrambling image position (as discussed by SHANG Yanhong，LI Nan，ZOU Jiancheng [5]). In 2003 WuMin present the chaos masking encryption methods(as discussed by WU Min，QIU Shuisheng [6]); In 2004 FanLei put forward the language encryption algorithm(as discussed by FAN Lei，MAOYaobin，SUN Jinsheng. [7]); In 2006 DingWenxia put forward the chaotic system independent key DES digital image encryption algorithm(as discussed by DING Wenxia，LU Huanzhang，XIE Jianbin [8]); In 2007, the Hossam E1-din H.Ahmed put forward a kind of chaotic feedback password concept(as discussed by Hossam E1-din H,Ahmed,Hamdy [9]).

2 Encryption scheme of chaos system

Rossler system is typical three dimensional chaotic system，generated the chaotic sequences mainly has the following advantages： First, chaotic system is extremely sensitive to initial condition； Second, chaos is produced by deterministic nonlinear systems, which has noise-like, broadband frequency spectrum character, it is pseudorandom, reproducible phenomena; Third, uniform distribution of the chaotic system state；Fourth, nonlinear.

The original chaotic floating-point sequence is a single chaotic variables through the Rossler system and high dimensional system to produce sequence password, it also can be the combination of multiple variables，so the design and application of the sequence password are more flexible and convenient，it has more space and enhanced security, improved accuracy of limited by short cycle effect.

The dynamics equation of three-dimensional Rossler chaotic system：

$$\begin{cases} \dot{x} = -y - z \\ \dot{y} = x + ay \\ \dot{z} = b + z(x - c) \end{cases} \quad (1)$$

Where a=0.2,b=0.2,c=5, a,b,c is system parameters， Rossler system presents chaos.

3 Composite encryption algorithm combined with DES algorithm and chaotic systems

DES(Data Encryption Standard) is a kind of use of the key encryption password. It was determined for the federal data processing standard (FIPS) by United States the federal government's national bureau of standards in 1976, then spread widely in the international (as discussed by Qian L,Nahrstered K [10]). It used a key of 56 symmetric algorithms, because the algorithm contained some confidential design element, it was suspected of containing the back door of the national security archive and the relatively short key length , so in the beginning it is controversial, DES are under the intense academic type review, and promote the modern piece of code and the development of the password analysis. DES is a symmetric encryption method, it was published by the U.S. National Bureau of Standards in 1997, According to Shannon proposed the diffusion and confusion of password design system, two basic technical design of the algorithm make full use of the replacement, substitution, iteration, a variety of commonly used computing methods. With the development process of cryptography, it has played a very important role.

DES is the typical iteration cryptographic algorithm. It generates 56-bit sub key, and encrypts 64-bit data block. The DES encryption algorithm is the 64-bit plaintext input block into 64-bit ciphertext input block through a series of replacement, iterations, and grouping.

3DES（Triple DES）is a encryption algorithm of DES transition to the AES. 3DES algorithm is more secure than the DES. Specific encryption process and decryption process are shown in figure 1:

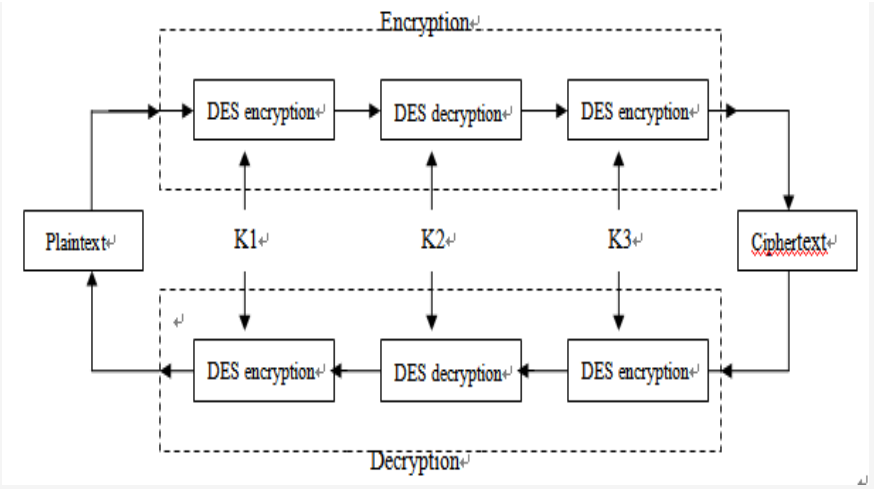

Fig. 1 3DES algorithm structure chart

The image is encrypted by chaotic sequence combined with DES algorithm at the transmitter. The initial replacement for the first time, iteration and grouping, then the chaotic sequence generated by the Rossler equations as a sub key embedded in the 16 iterations, the final inverse initial permutation will be encrypted ciphertext. The DES algorithm to encrypt and decrypt using the same set of algorithms, but the use of sub-key in reverse order, the decryption process is simply contrary to the order of sub-key, one can get the original image.

A new chaotic encryption algorithm is presented, which overcomes the limitation of Logistic map and Henon map. The scheme will use chaotic numbers as encryption keys based on the analysis of the principium of DES encryption and the weak relativity between the generation of sub-key and the critical arithmetic. The new algorithm is perfectly emanative, real-time and security.

4 Simulation

Using C + + programming, debugging and running in the VS2008 environment applications, the numerical simulation, the results are as follows:

Fig. 2: Original image

Fig. 3: Gray scale image after processing

Fig. 4: similar image

Fig. 5: Encrypted image

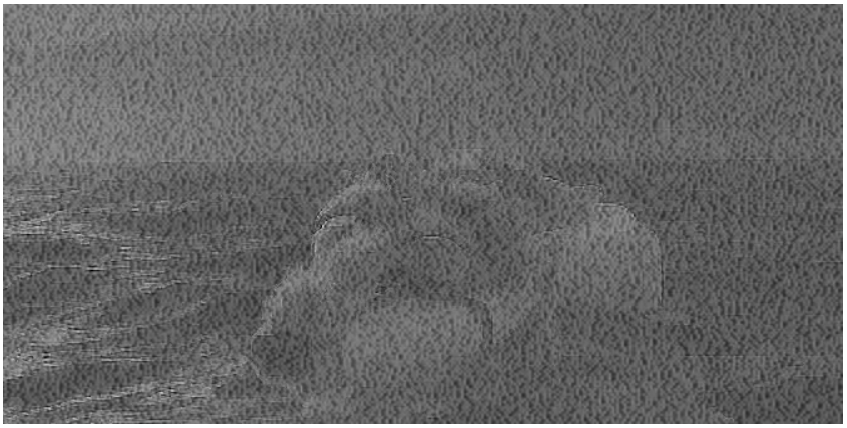

Fig. 6: Being decrypted image

Fig. 7: Decrypted image

5 Safety analysis

Encryption algorithm in this article uses the combining method of traditional encryption algorithms and chaotic encryption algorithm. It greatly improves the safety performance of the system. Key generated by the chaotic system, which makes each packet key is dynamically changed, each packet of the key space is huge. The other hand, the security of the encryption algorithm in this article do not depend on the confidentiality of the algorithm, even if the decryption master chaotic systems, mere speculation is almost impossible to get these critical values, which ensure that this encryption algorithm can effectively resistance to brute-force attack.

Simulation results and security analyses show that the proposed cryptosystem has large key space and high sensitivity to key and plaintext, and can resist the brute attack and statistical attack.

6 Conclusion

A scheme of image secure communication is presented. The image is encrypted by chaotic sequence combined with DES algorithm at the transmitter. Accordingly, the received signal is decrypted. Taking advantages of chaotic sequence and DES algorithm, the communication system is securer than that using any encryption technique lonely. The computer simulation results show that the proposed image secure communication scheme is effective.

Acknowledgements

This work was financially supported by the science and research foundation of Liaoning education committee (L2013248) and technology funds of Jinzhou city (13A1D32).

References

[1] Natlas Y，Shamir A. A video scrambling technique base on space filling surves 76(5) (1987), 550-559

[2] W.Diffie，M.Hellman. Access control system for the MAC/packet family: Eurocrpt.European standard EN 50094.(1992).

[3] Romeo A.Romdolti G,Nattavelli N. et al.Cryptosystem architectures for very high through put multimedia encryption:the RPK solution.(1999), 261-264.

[4] BAO Guanjun，JI Shiming. Cube transform and its applications in digital image encryption. Computer Applications, 22(11) (2002), 25-27.

[5] SHANG Yanhong，LI Nan，ZOU Jiancheng. Fibonacci transformation in the application of digital watermarking. Journal of sun yat-sen university (natural science edition).43（A2）(2004) 148-155.

[6] WU Min，QIU Shuisheng. A chaotic image encryption method. Journal of communication, 24（8）(2003), 31-36.

[7] FAN Lei，MAOYaobin，SUN Jinsheng. A voice encryption algorithm combined with the cat mapping and Loglstic mapping. Control and decision,19(10) (2004), 1167-1170.

[8] DING Wenxia，LU Huanzhang，XIE Jianbin. Digital image encryption algorithm Based on chaos system independent key DES. Computer Applications, 23(2)(2006), 35-37.

[9] Hossam E1-din H,Ahmed,Hamdy. An Effielent Chaos-Based Feedback Stream Cipher（ECBFSC）for mage Encryption and Decryption. Information 31.(2007), 121-129.

[10] Qian L,Nahrstered K.A new algorithm for mpeg video encryption.(1997), 27-29.