Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics
San Antonio, TX, USA - October 2009

Digital Image Encryption Algorithm Based on Chaos and Improved DES

ZHANG Yun-peng
College of Software and Microelectronics
Northwestern Polytechnical University
Xi'an, China
poweryp@163.com

ZHAI Zheng-jun
College of Computer science
Northwestern Polytechnical University
Xi'an, China
Zhaizjun@nwpu.edu.cn

LIU Wei
College of Software and Microelectronics
Northwestern Polytechnical University
Xi'an, China

NIE Xuan
College of Software and Microelectronics
Northwestern Polytechnical University
Xi'an, China

CAO Shui-ping
College of Software and Microelectronics
Northwestern Polytechnical University
Xi'an, China

DAI Wei-di*
School of Computer Science and Technology
Tianjin University
Tianjin, China
davidy@126.com

***Abstract*—In recent years, encryption technology has been developed quickly and many image encryption methods have been put forward. Chaos based image encryption technique is a new encryption technique for images. It utilizes chaos random sequence to encrypt image, which is an efficient way to deal with the intractable problem of fast and highly secure image encryption. However, the Chaos based image encryption technique has some deficiencies, such as the limited accuracy problem. This paper researches on the chaotic encryption, DES encryption and a combination of image encryption algorithm, and simulate these algorithms, through analysis of the algorithm to find the gaps. And on this basis, the algorithm has been improved. The new encryption scheme realizes the digital image encryption through the chaos and improving DES. Firstly, new encryption scheme uses the Logistic chaos sequencer to make the pseudo-random sequence, carries on the RGB with this sequence to the image chaotically, then makes double time encryptions with improvement DES, displays they respective merit. Theoretical analysis and the simulation indicate that this plan has the high starting value sensitivity, and enjoys high security and the encryption speed. In addition it also keeps the neighboring RGB relevance close to zero. The algorithm can be used in the actual image encryption.**

***Keywords*—Cryptography, Chaos theory, DES, Digital image**

I. INTRODUCTION

Digital images, accounting for 70% [1] of the information transmission on the internet, is an important parts of network exchanges. However, the image information, which is different from text message, has larger scale of data, higher redundancy and stronger correlation between pixels[2]. Traditional encryption algorithms such as DES, IDES, are against the text messages to be proposed, which are not suitable for digital image encryption[3], therefore, an reliable digital image with characteristics is in urgent need of the encryption scheme.

Chaos is suitable for image encryption, with is closely related to some dynamics of its own characteristics. Chaotic, having kind of randomness, is affirmed in the academic community unanimously[4-5], the nature of encryption system is a necessty . In addition, the chaos, which also has characteristics of categories of noise-sensitive initial long-term unpredictability, ergodicity, mixed and the the divergence index, is very suitable for encryption. It is a natural encryption tools, especially in two-dimensional plane of the irregular, it has created favorable conditions for the two-dimensional images of encryption[3].

In 1997, fridrich applied chaos to encryption of digital images for the first time[4]. After that, many scholars committed to the research of the chaotic image encryption methods[1,3,5,8,10,13]. Compared with the traditional method, chaotic image key encryption algorithm has a large space, simple implement, robustness, and the advantages of faster encryption.

However, the new chaotic encryption technology, compared to the mature traditional encryption technology, is very immature. Chaos image encryption technology still have problems such as remain limited precision, short-cycle and other issues, and the actual formation of the password and

978-1-4244-2794-9/09/$25.00 ©2009 IEEE

cycle are difficult to measure[6]. It is required that further study and improvement be carried out.

The literature[7] proposed a scheme which combine chaotic encryption technology with traditional DES encryption technology to encryption digital image. In this paper, the advantages and disadvantages of this method are analyzed and improvements are made to its shortcomings. It makes chaotic and applications of improvement DES encryption in the image complement it each other, and inhibits their shortcomings by effect.

II. ANALYSIS OF ALGORITHMS

The thought of image encryption which combining the chaos with conventions is not only innovative but also feasible. However, only combining the chaotic sequence with DES simply will inevitably lead to some deficiencies of the algorithm, as follows:

1) The speed of using chaotic and DES level two to encrypt digital images is unsatisfactory. Because of the characteristics of image information, DES algorithm is not the ideal choice for digital image encryption, otherwise, there will be a negative impact on the algorithm. The first level encryption uses the chaos, and the high degree of redundancy issues have a very good solution. However, the large amount of information has highlighted the issue. DES, to be 16 iterations, will cause encryption very slow. For example, in the same environment, chaotic algorithms need 14 seconds to encrypt 500 K of the image data, while the DES needs 467 seconds[8]. Therefore, the problem of low speed encryption can not be ignored.

2) The inherent shortcomings of DES – lacks space key [9]. DES, in a 56 initial key control, transforms 64 expressly division of the text into 64 groups. The whole encryption process need to go through 16 transforms. Each round uses a key associated with the initial round of the 48 keys, through repeating substitution and replacement to increase its strength. This has created a DES inherent weakness: lack of space key. Allowing an attacker to take advantage, the current method of the attack on the DES more or less uses the shortcoming of DES . In order to solve the problem, scholars have made a triple DES and AES to replace the DES (Advanced Encryption Standard). However, the approaches will make algorithm more complicate and less efficiency. Therefore, a new method in the circumstances of retaining complexity needs to be found out to expand the DES key space.

In general, the approach of simply adding two kinds of algorithm is debatable, but more feasible approach is to combine the characteristics of digital image information, in-depth understanding of encryption thinking on the premise of the design image encryption algorithm. Ultimately they complement each other, and inhibit their shortcomings by effect.

Therefore, this organic combination of chaos and improvement of DES makes the final algorithm more secure, faster and more suitable for digital image encryption.

III. IMPROVEMENT AND PRINCIPLE

A. Improvement

1) Reduce the time of DES iteration to four speed. To do so, first of all the problems encountered on the security of encryption algorithm whether the negative impacts. The literature shows that[9]16 iterations can not effectively resist the difference of DES today and the attack of password linear analysis, therefore, the effectiveness of several iteration only reflected in the explicit information in the text of the confusion and Proliferation effects, can reduce the statistical properties of the text and resist directly to the attack of the text. In the original algorithm, the first-class chaos on the encryption algorithm has reached a purpose of confusion and the proliferation[7], making of the statistics of the text low, therefore, it was unnecessary for 16 iterations. Through massive test, it shows that four iterations can effectively balance the security and speed, of course, the security of 16 iterations is higher than four times iteration. However, the negative impacts on the security of the whole algorithm were only a little compared to the promotion of the efficiency. After calculations, there is about 70 percent improvements on efficiency and the decrease of the security is almost negligible.

2) The expansion of the DES E box was been improved. The realization of f function (Figure 1) is the most critical part of DES algorithm. Through analyzing the transform rules of some components of f function, it shows: in each round of iterative process, the realization of the function f focused on the expansion of E replacement, S-Box replacement and P replacement. If we can reduce the calculation workload of these replacements operation, the algorithm will certainly enhance the operating speed. The literature[9] has done a detailed analysis on E boxes to find its transformation rules and the method in improving the efficiency of calculation.

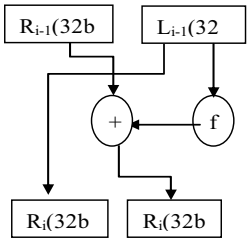


Figure 1. DES summary of the process

TABLE I. EXPANSION OF REPLACEMENT E TABLE

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	21	32	1

In the implement action of DES algorithm, it is necessary to achieve E expansion. From Table I, the data is expanded into 48 bits one by one , so the calculation is larger. Extended

replacement E data in the table clearly reflects the replacement of the rule: the first bit of Ri- 1 is assigned to the second bit of R'i-1,and the second bit of Ri-1 is assigned to the third bit of R'i-1 and so on. Find this rule, it is not necessary to take data one by one from the tablet to find the rule, and the program can be improved and the calculation speed can be increased. The realization of this expansion 48, where calculation replaces look-up table, can improve speed in accordance with the procedures of the following.

```
for (i = 0; i < 8; i ++)
        for (j = 0; j < 6; j ++)
                a = i * 4 + j;
```

Now only the first and last special treatment, and other Members in accordance with a value of the replacement, can effectively reduce the amount of computation, improve the speed, meanwhile, reducing the storage requirements.

3) Use a chaotic map to expand DES key space. As the initial encryption key of DES algorithm keep constant in the whole process, if you want to continue to transform the initial key to enhance the strength of passwords, encryption and decryption-of-sync key have new problems. At the same time, through continually changing the initial key, although the DES algorithm can enhance the strength of your password, it did not change the algorithm in the initial round of key and the key inter-linear relationship.

Using Logistic mapping to randomly generate round keys independent of each other can properly solve this problem. The end of encryption and decryption structure Logistic mapping with the same parameters is used as the initial value of Logistic map as encryption / decryption of the initial key and generated by the Logistic map of the round of 48 on each round of key data encryption. Each dealt with a set of explicit; it continues to produce the next round of key groups. As long as the original keys are the same, encryption / decryption at both ends of the chaos will be on the same sequence. Thus, both the end of encryption and decryption key reach the round of sync[10]. Therefore, the DES key space is further expanded.

B. Encryption framework of principles

According to the idea of the literature[7], combining conventional encryption technology to the principles of encryption algorithm.

Algorithm at the following five steps:

1) Logistic chaotic map produced chaotic sequence, with an interception 50, and 255 die from generation key k;
2) Key k and each pixel (8) of original image p or vary according to place, using chaotic encryption to generate the first of text-c;
3) Grouping The first class of the division with each 64 bits as two express c ';
4) Logistic chaotic map produce the chaotic sequence, generating 48 a group of the two encryption keys k ';
5) Two key k ' make use of improvement of DES to encrypt the two express c', encryption of a final text, generating encryption images p '.

IV. SIMULATIONS

This test is done on the computer with the Celeron M Processor 370,512 M memory using Visual C + + 6.0, encrypted image is 256 × 256 Lena image.

A. Deciphering test

Chaos initial value level encryption keys were 0.60000001, 4; DES encryption-key initial value for 0.6,4, D algorithm in the initial value for 0.60000001,4 key results as shown in Figure 2:

a) Relevant

b) After the encryption algorithm of plans

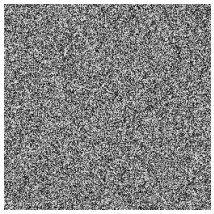
c) Figure correct decryption

Figure 2. Deciphering test

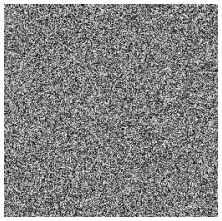
From the effect of encryption and decryption of the Images, the improved encryption algorithm is not weaker than the results of the original encryption algorithm. Two algorithms declassified has the same clear picture, compared to the original image ,there are no major differences.

B. Defaults sensitivity tests

In order to verify the performance of this encryption scheme, the system uses keys with small differences to decrypt the image map 3 - b, d encrypted, as a means of inspection systems for the initial sensitivity. Figure 3 in the same circumstances of 4 parameters, are the results of using initial 0.60000002 to decrypt.



a) This article decryption key algorithm using the wrong results

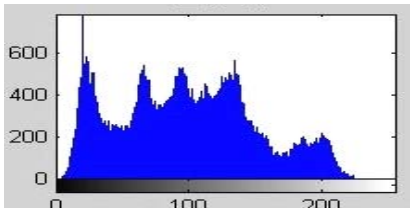


b) The decryption key algorithm using the wrong results

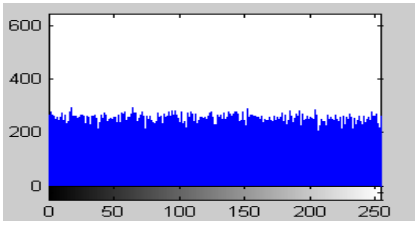
Figure 3. initial value sensitivity test plans

From Figure 3 it can be seen that , sensitivity of the initial results are very high in the two encryption, even if the initial value is increased by only 0.00000001, After decrypting ,explicit information can not be seen from the picture.

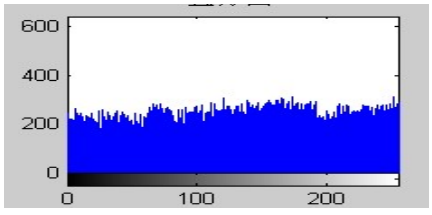
C. Statistical Analysis



a) Expressly image histogram



b) This article encryption algorithm image histogram



c) The original image histogram encryption algorithm

Figure 4. comparing image histogram

In figure 4, encryption process expresses image pixel value of the uneven distribution of pixels into a uniform distribution of the text of pixels in the [0,255] the entire space within the values of equal probability. The statistical properties of expresses have been completely broken, so that the relevance of the text is much lower. And this method is superior to the original algorithm.

D. The relevance of adjacent pixels

To test the relevance of adjacent pixels of explicit images and text images, 1,000 pairs of adjacent pixels (horizontal, vertical or diagonal) will selected randomly from images, and then the following formula was used to calculate the relevance of adjacent pixels quantitatively[11]:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2$$

$$Con(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))$$

$$\gamma_{xy} = \frac{Conv(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

Thereinto, x and y partly respect the gray value of two adjacent pixels in the image, and γ_{xy} is the correlation coefficient of the two adjacent pixels. Figure 5 explicitly describes the correlation of adjacent pixels of Horizontal direction expressly and Ciphertext.

TABLE II. EXPANSION OF REPLACEMENT E TABLE

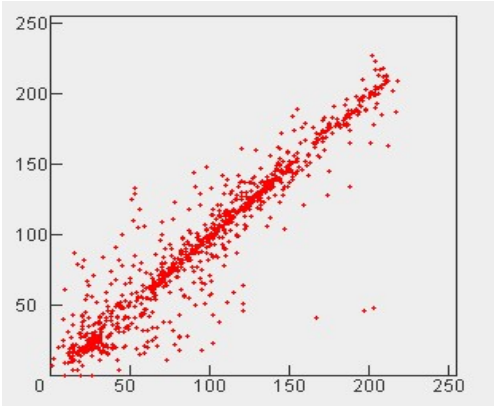
	Expressly	**This paper algorithm of the text**	**Algorithm of the original text**
Level	0.9403	0.0019	0.0082
Vertical	0.9437	0.0158	0.0373

Table II lists the relevance results calculated according to two directions. Adjacent pixels of explicit images are highly relevant, with the correlation coefficient close to 1. Coefficient adjacent pixels of the encrypted image are close to 0.Adjacent pixels are basically not relevant, which clearly shows that demographic characteristics spread into random text, and the adjacent pixels relevance of improved algorithm is superior to the original algorithm.

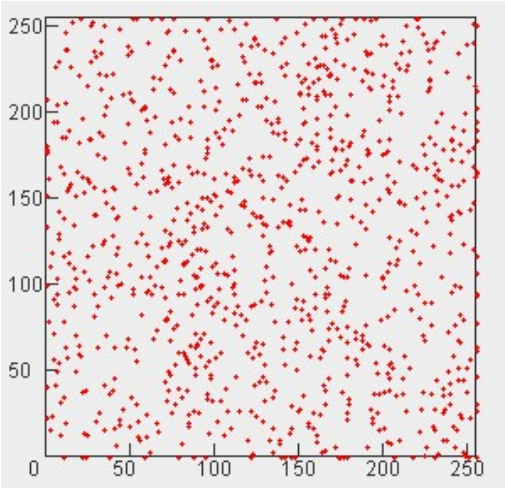
V. SECURITY AND COMPLEXITY ANALYSIS

A. Security Analysis

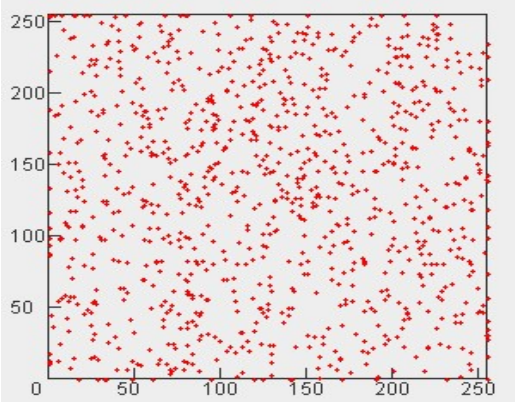
Conventional encryption method used for encryption can be broken[4,12,13], in addition to exhaustive attacks, all the known conventional encryption algorithm method of attack is the basic condition for the corresponding express only some of the text[14]. And the use of encryption can conceal the two DES encryption-class express information informations, therefore the existing password for the DES algorithm analysis methods such as linear analysis, password analysis will expire. From this we can draw the conclusion that is safer.The analysis is as follows:



1) Explicit images related to the horizontal direction of adjacent pixels



2) This algorithm, the level of correlation between the horizontal direction of adjacent pixels



3) Algorithm of the original text of the horizontal direction correlation between adjacent pixels

Figure 5. in the horizontal direction of adjacent pixels, the relevance of the

On the one hand, is the chaotic encryption technology and the security. The signal used in the chaotic encrypted signals, is the mapping of the chaotic sequence under a certain initial value, and 50 by the interception of a pseudo-random sequence. The process involves encryption product, interception, and such as model for computing. Chaos is different from the original sequence, thus confidentiality has been strengthened; Secondly in the channel of transmission of the text was obtained after two encryption. A combination of both, can confront the literature [5] raised in the chaotic system of identification and the initial value determined by decipher ways to enhance confidentiality.

On the other hand is the DES encryption system of security and confidentiality. The use of the Signal chaotic signal of the extreme sensitivity of the initial and long-term unpredictability, causes chaos to be encrypted signal as DES encryption level of input. In doing so, we will find the corresponding explicit does not exist between the DES algorithm makes the input and output - of The text [7] has overcomes the DES key and weak in the semi-weak key weaknesses, thus it can resist the current attacks on the most effective DES password linear analysis [9] and improve the confidentiality. DES encryption algorithm used in the round of 48 key, is generated through the chaotic map. In simulation tests the initial setting value of X0, μ, can be admitted to the decimal point after 10, 10 +10 = 20 values, and Uncertain, which may be a combination of 1020, the final key space is about 264, much larger than the 256 DES. The space of the key is great enough to resist the exhaustive attacks.

B. Complex analysis

This paper algorithm adopted the used of chaotic sequence with different values or pixels, called the Operation 1. Then use the results are improved by DES encryption, known as Operation 2.

VI. CONCLUSION

Confidentiality of technology ,based on the combination of the chaotic encryption technology and the traditional encryption technology, is better than any one of encryption technology when used on their own[12], and The two have complementary advantages and disadvantages have been contained. Results of computer simulation show that good results in our project the programme using the nature of Chaos mechanism to achieve the improvements of the traditional encryption techniques,have been obtained.

ACKNOWLEDGMENT

This work is supported by Innovation Project of Northwestern Polytechnical University (W016141).

REFERENCES

[1] Dang P P, Chan P M. Image encryption for secure Internet multimedia applications [J]. IEEE Transactions on Consumer Electronics, 2000, 46(3): 395～443.

[2] Guodeng Feng. Principle and network security technology[M].Beijing: Science Press, 2003.

[3] Hua Zhong. Based on the chaotic image encryption technology research [D]. Changsha Polytechnic University master's thesis,hunan, Changsha,5～6。

[4] Fridrich J.Image Encryption Based on Chaotic Maps.IEEE,1997,1105～1110

[5] Sobhy M I, Shehata A-E R. Methods of Attacking Chaotic Encryption and Countermeasures. In:IEEE International Conference on Acoustics, Speech, and Signal Processing, 2001, 2: 1001～1004

[6] XiangSheng-Wang, Junren-Gan. A Chaotic Sequence Encryption Method. Chinese Journal of Computers，2002，25（4），351～356

[7] Shuisheng-Qiu, Yangfeng-Chen, WuMin. Discussion on Chaotic Secure Communication and New Schemes of Chaotic Encryption[J]. Journal of South China University of Technology(Natural Science Edition), 2002, 30 (11): 75～80

[8] Lina Wang. Multimedia network information security technology[M]. Wuhan Hubei：Wuhan Publishing House，2003，27-33

[9] Li Lv, jia Zhao. Analysis and Research of DES Encryption Algorithm[J]. Journal of Nanchang Institute of Technology, 2006,12(5): 28～31

[10] Chen Guanrong, Mao Yaobin, Charles K. A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps[J]. Chaos,Solitons and Fractals, 2004, 3(21): 749～761.

[11] Yaoqun Xu, jian Liu, honglei Qin. Plane tent map chaotic sequence analysis of binary [J]. Harbin University Business Journal (Natural Science), 2003.2, 19(1): 47～51.

[12] M Naor,A Shamir.Visual cryptography. In Proc of Europcrypt＇94,1994,1～12

[13] Chen Guanrong, Mao Yaobin, Charles K. A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps[J]. Chaos, Solitons and Fractals, 2004, 3(21): 749～761.

[14] Stallings W.Cryptography and Network Security Principles and Practices, Fourth Edition [M]. Prentice Hall

[15] dengguo Feng. Analysis of password [M]. beijing: Tsinghua University Press, 2000:54~83