Advances in Intelligent Systems Research, volume 134
2nd International Conference on Control, Automation, and Artificial Intelligence (CAAI 2017)

A Novel Hybrid Algorithm Based on Fibonacci p-code and Gray DES

Guangming Yang[1], Jian Xiao[1], Zhenhua Tan[1] and Wei Cheng[1,2*]
[1]Software College Northeastern University, Shenyang, China
[2]National Model Experimental Teaching Center of Software Engineering Program, Shenyang, China
*Corresponding author

***Abstract*—In this paper, a novel hybrid algorithm is proposed to solve the security problem of image information, which is on the basis of gray DES algorithm and Fibonacci p-code algorithm. Then, using self-reverse matrix to improve the Fibonacci p-code encryption algorithm and combing it with Gray DES algorithm to proposes a new image encryption algorithm, in order to reduce image distortion. Finally, the paper evaluated the proposed hybrid algorithm's performance through statistical analysis and diffusion tests. As a result, the system is more robust against the JPEG compression method and can be compatible with the international universal compression method.**

Keywords-gray DES; fibonacci p-code; data encryption; frequency domain scrambling

I. INTRODUCTION

With the development of Internet, image, video and other multimedia information need to be transmitted on the network, so the security of image information becomes very important. The image encryption is the primary solution scheme,But the traditional encryption algorithm in the encryption speed is not only unacceptable, and a high security and high quality for encryption and decryption is also need to be solved.

Under such background, it is an urgent need for appropriate digital image encryption method to promote the security of network image. So the image encryption algorithm which integrates the gray level DES algorithm and the Fibonacci p-code algorithm is proposed, namely, the image through gray DES encryption, then Fibonacci p-code set chaos encryption. Finally, a complete system is formed.

In this paper, we use statistical analysis and diffusion testing to evaluate the algorithm. The result shows that our algorithm not only can resist the chaos and diffuse statistical attack, but also has good effect in dealing with differential attack. The remainder of the paper is organized as follows. Section 2 contains a review of related work and section 3 describes the proposed hybrid algorithm in detail. In section 4 we analyze the performance of the proposed hybrid algorithm. And finally, we conclude the paper in section 5.

II. RELATED WORK

In the field of image encryption, the image encryption technology based on pixel gray transform has become more and more popular among researchers. As compared with the simple pixel position scrambling, digital image pixel gray transform encryption scheme is more meaningful. However, the efficiency of using this encryption method is generally low.

Zhang Han and others proposed[1] a gray transform fast image encryption algorithm based on chaos system and Henon map. The method proposed in the literature[2] is also through the transformation of the digital image pixel gray to achieve encryption. However, the first image scrambling and then pixel gray transform algorithm seems to be more favored by researchers. Zhang et al. [3] used the AmoldCat map to iterate to change the psosition of each pixel of the image.Fei Gao, Li Xinghua in the literature[4] and Zhi-Hong Guan and so on in the literature[5] algorithm is also used the idea of first set random pixels and then gray scale transformation.

This hybrid encryption algorithm first gray the simple images, then the rearrange the pixel, and the hybrid encryption algorithm comes from two stable encryption algorithms:gray DES encryption algorithm and the encryption algorithm based on Fibonacci p-coding. The hybrid encryption algorithm is derived from two kinds of stable encryption algorithm, gray DES encryption algorithm[6] and Fibonacci p-code based encryption algorithm[7]. But the security is not strong enough,because of the DES algorithm is a kind of symmetrical encryption. Another kind of encryption algorithm is related to the DCT domain using Fibonacci p-code sequence image scrambling encryption method. The general idea of the method is using chaotic sequences to generate different chaotic pixels[8] .

III. PROPOSED HYBRID ALGORITHM

The idea of this hybrid encryption algorithm is the first using gray transform and then do the pixel scrambling. When the size of opened image is 265 x 265, using mixed encryption to encryption the image. Finally, the encrypted image will be displayed on the interface. The implementation process of the hybrid encryption algorithm will be described in detail below.

A. The Structure of Hybrid Encryption

We first dispose a 265×265 image with DES gray-scale processing method, use Fibonacci p-code scrambling for pixel scrambling, and complete the entire hybrid encryption. The framework flow chart of encryption system is shown in Figure 1. As the decryption algorithm is an inverse process of the encryption algorithm, the framework will not repeat decryption algorithm.

The following contents will focus on the details of the encryption algorithm logic.

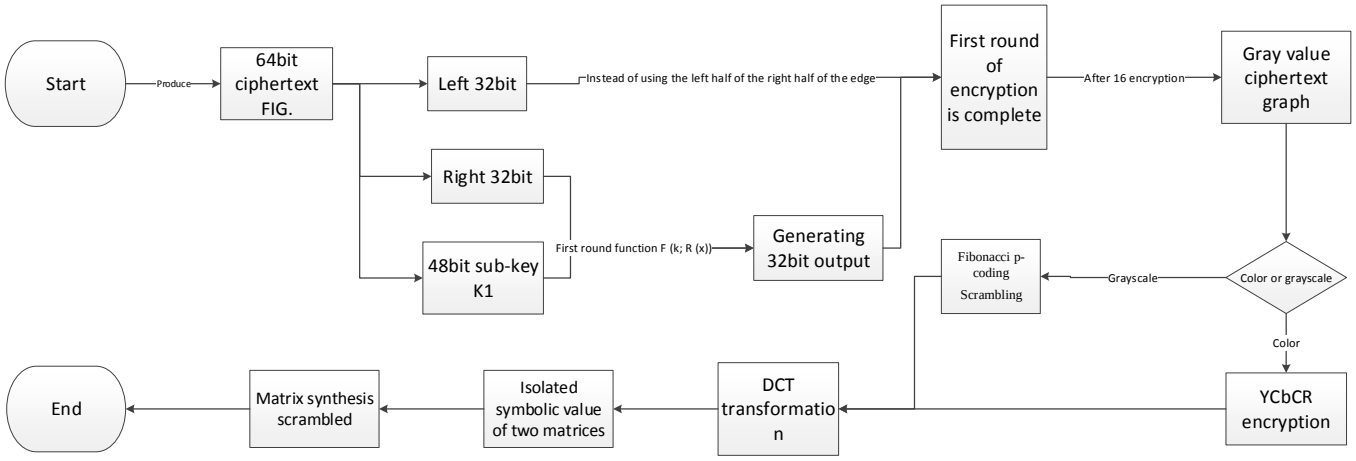

FIGURE I. ARCHITECTURE OF THE HYBRID ALGORITHM

B. DES Gray Level Encryption Processing

The gray scale DES image encryption is the data encryption in nature. The image file is considered as the gray value of a matrix of elements the matrix.The first step is to replace the input by the IP replacement table. The output will be divided into two parts, both the left and right part are 30 bits. The right part extends to 48 bits as the input of the S box with 48 bits key. Based on S-box operation principle, 6bit input get the 4 bit output, taking value of B2B3B4B5.The 32 bits result will be the input of the P box for replacement. Then does exclusive-or operation with the left side to get the new 32bit for left, thus the first round of encryption end. After 16 encryption to get a set of gray matrix scrambling completely, following is DES algorithm.

Step 1: According to the IP initialization replacement table, replace the 64bit of plain text.

Step 2: Divide into two parts, each 32bit, called the left part and right part.

Step 3: At the same time, generate the first 48bit sub key K1.

Step 4:Sub key of K1 which contact with the right part is applied to a function F (K; R (x)) to generate 32bit output. Here is a brief description of the function F.

①Application extension box, expand x from 32bit to 48bit.

②The E (x) and Y applied to the modulo-2 addition, the output is 48bit

③Input Bi into S-box for each length of 6bit, where the S-box is made by a linear function, take the 6bit as the input, get the 4bit output.

④the 32-bit output generated by ③ will be the input of the permutation function P.The result of the output of a round of function F is exclusive XOR of the left half of the plain text.

The formula for the process is:

$$F(\mathrm{k}, R(x)) = P(S(E(R(x)))) \oplus L(x)$$

The left part of the original plain text is replaced with the right part, and the original value is replaced by the XOR output.The function F_k is used to show this step.

The formula for the process is

$$f_k(x) = R(x) \| (L(x) \oplus F(k, R(x)))$$

At this point, a round of encryption DES algorithm completed. Repeat this process 15 rounds. The only difference is that the sub keys used for the input to the first function F are changed to K1, K2 and K15, respectively. When K16 is applied to the preoutput of the right and left halves, K16 is not converted.

C. Image Scrambling Encryption

After getting the gray value of the cipher text, the image need to be the secondary frequency domain encryption. The image need a time-frequency transform, transforming image matrix into the frequency domain data, and then the frequency domain data is encrypted. After DCT changes, the image will get the symbol matrix and numerical matrix. The scrambling operation is only processed on the symbol matrix. Fibonacci p-code chaotic sequence scrambling has two parameters, which can ensure the security of the algorithm. The step of scrambling algorithm based on Fibonacci p-code is as follows:

Input: scrambling the color (or gray scale) image needed.

Step 1: select the key parameter P, calculate Matrix row and column coefficient matrix which is transformed by two-dimensional Fibonacci p-code

Step 2: The color image is converted into YCbCr form, and divided into Y, Cb, Cr three components, each component is a two-dimensional matrix (gray scale image omitted this step).

Step 3: DCT transform is applied to each component to transform into the frequency domain (DCT transform gray scale image directly applied).

Step 4: The plus or minus symbols of each component of the DCT domain data and its numerical size separate into two matrices (gray scale image directly separated the plus or minus symbols and its numerical size into the two matrix).

Step 5:Through two-dimensional Fibonacci p-code transforming, scramble the plus or minus symbols of each color component of the DCT domain to scrambling symbol matrix (For gray scale images, the two-dimensional Fibonacci p-code transforming is applied to the symbol matrix of DCT domain directly.).

Step 6:Integrate the scrambling symbol matrix and its numerical size matrix into YCbCr image, and converts it into RGB scrambling color image (Gray scale images integrate scrambling DCT domain symbol matrix and its numerical size matrix into the scrambling image)

IV. ANALYSIS

In the test, there are two evaluation test methods, statistical analysis and diffusion tests, we use three indicators: histogram and variance, correlation of adjacent pixel, image information entropy. Detailed data on indicators will be presented below and the original test image as shown in Fig II.

FIGURE II. ORIGINAL TEST IMAGE

The following table I is original image, hybrid cryptography figure, gray DES image of a variety of indicators, and table II shows the correlation of the encrypted DES encryption, through the data we can see that the correlation is completely separated after DES encryption.

TABLE I. INDICATORS OF TEST RESULTS

index	Original image	Mixed encrypted	Gray DES encryption image
variance	S=5668.834	S=6751.203	S=193.9443
Information entropy	H=7.697436	H=6.874574	H=7.99703

TABLE II. CORRELATION COEFFICIENTS OF GRAY SCALE DES CIPHER

	Horizontal	vertical	diagonal
R	0.037187	-0.020074	-0.01774
G	0.037187	-0.020074	-0.01774
B	0.037187	-0.020074	-0.01774

Finally, table III is a correlation coefficient of hybrid encryption.By comparing the mixed encryption cipher text and the image correlation coefficient, we can see the correlation between the changes in the amount of encryption. The results of the experiments are as followed.

TABLE III. THE CORRELATION COEFFICIENT OF MIXED CIPHER TEXT GRAPH

	Horizontal	vertical	diagonal
R	0.943499	0.97029	0.931621
G	0.943499	0.97029	0.931621
B	0.943499	0.97029	0.931621

By comparing the correlation analysis of data, we can know that the distribution of mixed encryption is much more than that of the gray DES encryption, and the correlation analysis is the correlation between two adjacent pixels, which are vertical, horizontal and diagonal. Analysis of the above results, the correlation between hybrid encryption and encryption with the original gray are completely separate.

Information entropy means the amount of information contained in an image. The larger the value is, the more consistent the gray level distribution is[9], and the ideal information entropy of random image is close to eight.As shown in the data, the distribution of the encrypted result by the gray DES is more consistent, that is, the encryption effect is better

V. CONCLUSION

The main research direction of this paper is image encryption technique, for gray scale DES encryption and image scrambling based on Fibonacci p-code, designed to construct a more efficient image encryption system. Using the five indicators to image encryption system for test and evaluation in this paper, show that compare with the traditional encryption algorithm, the hybrid encryption algorithm is more efficient.

Next work mainly in the following aspects: First, key space in this article is not enough, further research needs to be done in the future. Second, the algorithm needs to be constantly revised and improved in order to reduce the loss of image information due to the image frequency encryption algorithm.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China under Grant No. 61402097, No. 61572123 and No. 61502092; the National Science Foundation for Distinguished Young Scholars of China under Grant No. 61225012 and No. 71325002; the Specialized Research Fund of the Doctoral Program of Higher Education for the Priority Development Areas under Grant No.

20120042130003; the Fundamental Research Funds for the Central Universities under Grant No. N151708005, and NO. N151604001.

REFERENCES

[1] Zhang Han.A fast image encryption algorithm based on chaos system and benon map[J].Journal of Computer Research and Development,2005,42(12):2137-2142

[2] Parcck N K,Vinod Patidar,Sud KK.Image encryption using chaotic logistic maps[J].Image and Vision Computing,2006,24:926-934.

[3] Zhang Jian.Image encryption scheme based on cat map and Lu chaotic map[J]Chinese Journal of Electron Devices. 2007,30(1):155-157.

[4] Fei Gao,Xinghua Li. Research-bit image encryption based on chaotic sequences[J]. Journal of Beijing Institute of Technology 2005,25(5):447-450.

[5] Guang Zhi-Hong,Huang Fangjun,Guang Wenjie.Chaos-based image encryption algorithm[J].Physics Letters A.2005,346:153-157

[6] Beckenbach E F, Bellman R. Inequalities[M]. Berlin:Springer-Verlag,1983.1.

[7] Shannon C E. Communication Theory of Secrecy Systems[J]. Bell system technical journal, 1949, 28(4): 656-715.

[8] C. K. Huang, H. H. Nien. Multi chaotic systems based pixel shuffle for image encryption[J]. Optics Communications, 2009, 282(11): 2123-2127.

[9] Guang-hui C A O, Kai H, He Y, et al. Algorithm of Image Encryption based on Permutation Information Entropy[C]//proceedings of 2010 3rd International Conference on Computer and Electrical Engineering (ICCEE 2010 no. 2). 2012.