Research on Chaos Encryption Method in Image DCT Domain

Ying Chu [1], Xiaoman Wang *, Peng Liu [1], Shuchang Liu [1], Zhiqiang Han [2]

[1]Department of Electronic Information, Changchun University of Science and Technology, Changchun 130022, China

[2]Department of Foundation, Air Force Dalian Communication Sergeant Academy, Dalian 116600, China

Abstract. In this paper, we suggest one chaos image encryption method in DCT domain according to the characteristics of JPEG image compression. The chaotic models used in this algorithm are Logistic mapping and Chebyshev mapping. The one-dimensional Logistic mapping is used to generate a chaotic sequence which is considered as control matrix for scrambling DCT coefficient matrix. According to the JPEG image compression standard, scramble the DCT coefficient matrix by 8 8 pixels in blocks in order to remain low-frequency composition in the upper-left corner of the DCT matrix. When implement XOR operation between chaotic sequence and DCT coefficient matrix, only encrypt interested DCT coefficients. Using the above two methods, not only improve the encryption speed of the image but also avoid low image compression rates due to scrambling the image encryption method. At last, use the two chaotic models to generate sign matrix. The simulation results show that the algorithm has good encryption effects, fast encryption speed, and high security.

Keywords: Image compression, DCT, Logistic mapping, Compression rates.

1. Introduction

In order to solve the bandwidth of network for difficult to load the great image data transmission rate, people use the image compression technology to compress the image before image data processing, transmission and storage, and make the compressed digital image transmission and exchange by different forms on the network .At the same time, the secure and the security of digital image information is particularly important.

If encrypt the image information directly, it inevitably can't compress the image, which will be very difficult to reduce the workload for transmission and storage. Because the compressed image (such as JPEG image) or multimedia data, the data compression algorithm is generally performed in frequency domain, if combine the compression algorithm and the image frequency domain encryption algorithm, it will decrease the amount of calculation. The goal of image encryption algorithm in frequency domain is fast calculation speed, the higher encryption intensity, strong anti-interference ability, simple engineering application software and hardware. However, fast operation speed, the higher encryption intensity, the simple realization restrict each other, it cannot be achieved at the same time, only under one certain conditions, the suitable encryption scheme can be put forward. Due to large amount, high redundancy, strict security of image data, it makes traditional cryptography meets new challenges. As a new and a more secure image encryption technology, chaotic cryptography has emerged, and has caused the wide interest of domestic foreign scholars.

At present, the document about compression image encryption in DCT domain is not so much, and most of them reduce image compression ratio due to the encryption operation, which is not hope in actual engineering application. So in this paper propose one image DCT domain encryption method which Combine outstanding features of the chaos theory and JPEG image compression standard.

2. Algorithm Realization

2.1 JPEG compression algorithm feature

JPEG algorithm [2] [3] [4] as shown in Figure 1.assuming that the original image size is M*N. When compressed, the original image is divided into 8×8 data unit matrix.

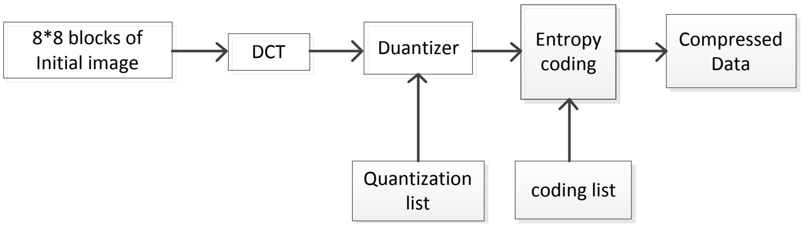
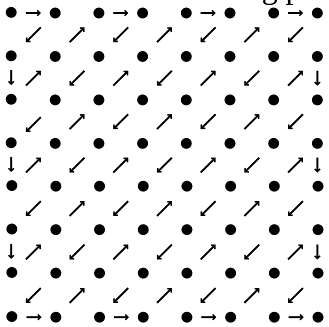


Fig.1 JPEG algorithm frame

The 8×8 image data after DCT transformation, the low-frequency components are concentrated in the upper left corner and the high frequency component distribution in the lower right corner, the F(0, 0) (the first row and first column elements) represents DC -coefficient, it is also the average value 8×8 sub block, we need code this 8×8 sub block. The other 63 elements are AC coefficient of 8×8 sub block, and using row coding which is called “Zig-Zag” Arrangement (as shown in Figure 2), it can increase continuous “0” numbers in row by this method. Because of low frequency component contains the main information of image, and the high frequency will be less important compared with low frequency, so remove high frequency components and maintain low frequency component by quantization operation. So, in the 8×8 image DCT matrix, only in the upper left corner has some nonzero element values, and the lower right corner is mostly zero elements, by this way make the row coding more effective.

The encryption algorithm should happen after the quantized DCT coefficients. If using position scrambling matrix generated by chaotic sequence directly encrypt the DCT coefficient matrix (M×N) after quantization, it inevitably will destroy the probability distribution of DCT coefficients, so that the subsequent code could not follow the optimal mode of operation, reduce the compression efficiency. Therefore, based on Article 5, the block unit scrambling technology in airspace is applied to the frequency domain. According to JPEG algorithm block principle, the DCT coefficient matrix is divided into 8×8 sub blocks, so that retains the characteristics of 8×8 image DCT coefficient matrixes when in image scrambling process, it will not affect the efficiency of the whole image compression. Block scrambling process as shown in figure 3.



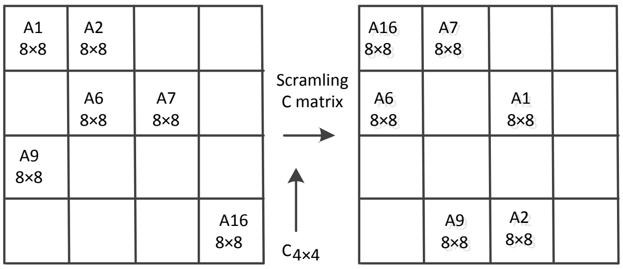


Fig.2 Zig-Zag arrangement Fig.3 Image block scrambling

In order to improve the security of the system, also need transform the coefficient value of DCT coefficient matrix by scrambling. In article 5 propose one XOR operation for chaotic matrix and absolute value of each element of DCT coefficient matrix. There is a certain problem in article 5, the compression efficiency will be higher only when DCT coefficient matrix has much more continuous “0” numbers and the "0" occupancy rate of every 8×8 DCT coefficient matrix is higher. If using XOR operation for chaotic sequence and "0", it will greatly increase the nonzero element values in DCT coefficients matrix and reduce the number of zero elements, thus affecting the compression ratio. Therefore, in this paper propose one encryption methods that only use XOR for the interesting DCT coefficient (also absolute value), and if the DCT values changed into "0" after encrypted, then use XOR again which means not encrypt this DCT coefficient. The reason is that: in the frequency domain the change in every point will have a certain impact on the whole data set, for image DCT transform coefficients, if there is a change in one element, it will embody in all pixel points by the

IDCT inverse. Each DCT coefficient is composed of two parts, the absolute value of DCT coefficient and the sign bit of the coefficient, it is obvious that it is very difficult to restore the original image if one not correctly. If one of the absolute value of the DCT coefficient change to "0" value when operate XOR operation with chaotic value, it will difficult to define the sign bit of the DCT coefficient before XOR operation during decryption process. So it is not suitable for encryption.

2.2 Chaotic encryption algorithm design

Scrambling matrix and transformation matrix generating. Logistic mapping [6] is a typical nonlinear chaos equation, which originated from a demographic dynamic system, although simple but reflects the basic characteristics of chaotic motion. The logistic mapping as following:

$$x_{n+1} = ux_n(1-x_n) \tag{1}$$

In the formula, $0 \le u \le 4, u$ identified as the control parameter, when u is fixed, by arbitrary initial value $x_0 \in (0,1)$, it can be iterated a definite sequence: x_1, $x_2, \dots, x_n, \dots$, for different u values, the system will show different characteristics. When the u reach ultimate value, steady-state solution of system is 2^{∞}, the system enters a chaotic state.

Using formula one iterative generate chaotic sequence, and extract former (M/8)×(N/8) of x_k ,by the method of row as the main sequence, is sequentially arranged in (M/8)×(N/8) matrix J. Sort the elements in J according to the max to min principle and generate G matrix using row highest priority method, form scrambling matrix H_{ij} (i≤M/8,j ≤N/8) by position coordinate in original J for each of the elements in G. Amplify, quantify and operate modular arithmetic (double (mod (round (x_k -*10^14) ,256) + 1) for each element in the sequence, and generate transformation matrix $P_{M\times N}$ by row highest priority method.

Symbol matrix generating. For the generation process of symbolic matrix, need to use another chaotic model. Equation as follows:

$$y_{n+1} = \cos[k \arccos(y_n)] \tag{2}$$

The definition interval is (-1, 1), when parameter k =6, the Lyapunov of Chebychev [7] system is 1.791733…, works in chaos state.

Using formula two iterative generate sequences $\{y_k, k = 1,2,3,,, M \times N\}$, by comparing the value of x_k and y_k generate symbolic transformation sequence and use this generate symbolic transformation matrix S as row highest priority method. In this paper no use initial value y_0 and parameter k of Chebychey as the key of the encryption system, but obtain the key through linear transformation of every two elements of x_k .Assume that only parameter y_0 and k not correct, other parameters are right in decryption, the decrypted image will reflect most information of original image. The reason is that a higher proportion of zero elements in quantized DCT coefficient matrix, the symbolic matrix only equivalent to the very few non-zero elements of encryption, that is simply using the symbolic matrix for encrypting will not good disturbing image information, it necessary to happen that error parameters decrypted image hide most information of original image, which makes the cracked easily decipher. So parameter y_0 and k belong to very weak keys, not suitable as the important key in system. Get the symbol matrix by the following equation.

$$S(k) = \begin{cases} -1, x_k < y_k \\ 1, x_k \le y_k \end{cases} k = 1,2,3,,, M \times N \tag{3}$$

2.3 Encryption algorithm realization

In this paper, use the initial parameters x_0 and control parameters u of the Logistic mapping as the initial key of the system.

The specific encryption process as follows: suppose that the encrypted image I, size M×N, gray level of 0-255.

Step 1: Logistic mapping in the key x_0 , u to generate a real value chaotic sequence x_k , Chebychev mapping in the key y_0 , k to generate chaotic sequence y_k .

Step 2: by chaotic sequence x_k according to the described in section 1.2.1 to generate position scrambling matrix H and transformation P matrix. According to 1.2.2, by x_k and y_k to generate the symbolic transformation matrix.

Step 3: transform image I by 8×8 DCT, and quantify it by the quantization table.

Step 4: block the DCT coefficient matrix according to the 8×8 standard in JPEG, and number the blocks according to the line sequential, use the scrambling matrix H scrambling DCT coefficient matrix.

Step 5: using P XOR with the absolute value of each element in the DCT coefficient, according to the method of encrypting image interesting coefficients (low frequency components of the image) and use another XOR for the DCT elements which after the first XOR value change into a "0" elements to maintain the original value.

Step 6: use the symbol matrix S point multiplication DCT coefficient matrix.

Step 7: save as JPEG image.

The decryption algorithm is the symmetric inverse process of encryption algorithm, in the decryption process must first point multiplication symbol matrix, then the XOR and position scrambling. Input the correct key, can decrypt the original DCT coefficient matrix, through the IDCT to restore the original image.

3. Simulation and analysis

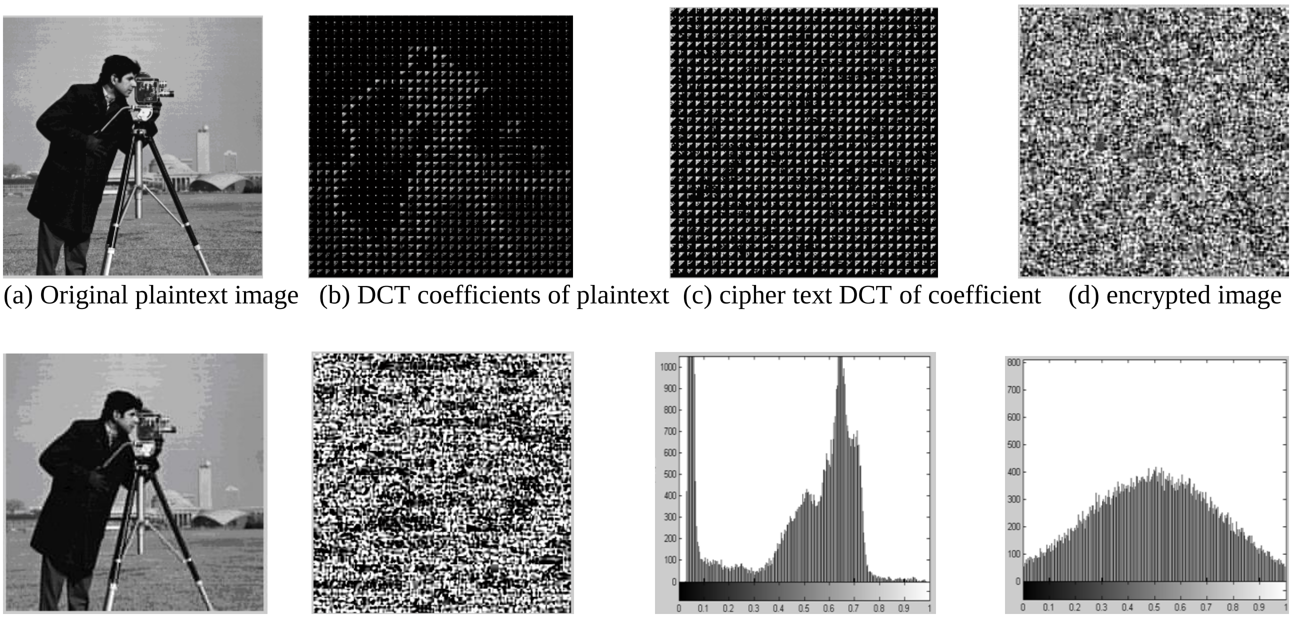
Below is the cameraman (256*256) images as an example, the simulation experiment is carried out by using Matlab. Because the quantization of JPEG image compression in is not emphasis in this paper, so the paper only the two value-mask showing in formula 4 to quantify each 8×8 image DCT coefficients matrix, here to retain 15 coefficients of DCT transform.

$$mask=\begin{bmatrix}1&1&1&1&1&0&0&0\\1&1&1&1&0&0&0&0\\1&1&1&0&0&0&0&0\\1&1&0&0&0&0&0&0\\1&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\end{bmatrix} \qquad (4)$$

The selected keys in encryption system are respectively x_0 =0.66, u =3.58, y_0 =0.25, k =5. In view of the number range of DCT conversion formula to be between -128 to +127 [8], need each pixel in the image to subtract the 128 and then transform cameraman by DCT. In this paper, by the following code to complete image DCT transform and quantization process.

```
(1) I = imread ('cameraman.tif'); I = im2double (I);
(2) I1 = 255*I -128; T = dctmtx (8);
(3) B = blkproc (I1, [8 8],'P1*x*P2', T, T');
(4) B1 = blkproc (B, [8 8],'P1.*x',mask);
(5) B2 = round (0.5*B1);
```

Among them, B is image DCT coefficients matrix, B2 is the coefficient matrix after quantized. Detailed simulation results as shown in Figure 4: (a) and (b) are the original plaintext image and the DCT coefficients of plaintext image, (c) and (d) the ciphertext DCT coefficient and encrypted image. (e) and (f) are decrypted images with correct parameters and the decrypted image with error parameters, (g) and (h) are the histogram of original image and histogram of encrypted image.



(a) Original plaintext image (b) DCT coefficients of plaintext (c) cipher text DCT of coefficient (d) encrypted image

(e) Correct parameters decrypted (f) error parameters decrypted (g) Histogram of original image (h) histogram of encrypted image

Fig.4 Image encryption/decryption simulate results

From the above simulation results we can be see that the distribution of original image pixels in gray level is not uniform, but after the chaotic encryption system, destroyed the original image of the statistical law, have good ciphertext diffusion. Just enter the correct key, the compressed image can well be decrypted, decrypted compressed image and the original image is consistent, cannot see the difference; when there are nuances of the decryption key and encryption key, can’t correctly decrypt the original image.

The sensitivity of the ciphertext counter to key refers to ciphertext image difference that for the same plaintext image using the, two slightly different key for decrypting .for the two times encryption, only x_0 not same, x_{01}=0.660222, x_{02}=0.660221,then the two encrypted compressed image contrast. Figure 5 is a map of the distribution of the difference from former 256 pixel of the two ciphertext. From the figure results, for the same plaintext, there will be a significant change in the ciphertext when only subtle changes in key, which also reflects the sensitivity of the ciphertext to key. Many experiments show that any key, small changes will make the ciphertext significantly change.

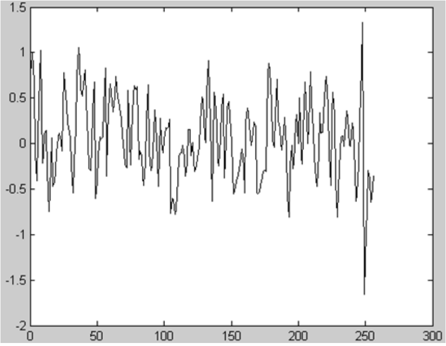


Fig. 5 Distribution of ciphertext pixel difference value

Analysis of the algorithm security include the correlation between adjacent pixels of the image, one purpose of encryption is to reduce the correlation between adjacent pixels of the image. Because the JPEG compression is loss compression, the original image by a handful of numerical quantization value through IDCT to restore, so the effect of encryption system object prime relevance in the frequency domain is not as well as the airspace, but the effect of the local random scrambling in spatial domain is bad than frequency domain. This paper from the original image and encrypted image compression randomly selected 16384 pairs of adjacent pixels. To calculate the correlation coefficient by following two formula: [9]

$$\operatorname{cov}(x,y)=E(x-E(x))E(y-E(y)) \tag{5}$$

$$r_{xy}=\operatorname{cov}(x,y)\Big/\sqrt{D(x)}\sqrt{D(y)} \tag{6}$$

Where x and y are gray value of the two adjacent pixel in image. In the numerical calculation, using the following discrete formula:

$$E(x)=1\big/N\sum_{i=1}^{N}x_i \tag{7}$$

$$D(x)=1\big/N\sum_{i=1}^{N}(x_i-E(x))^2 \tag{8}$$

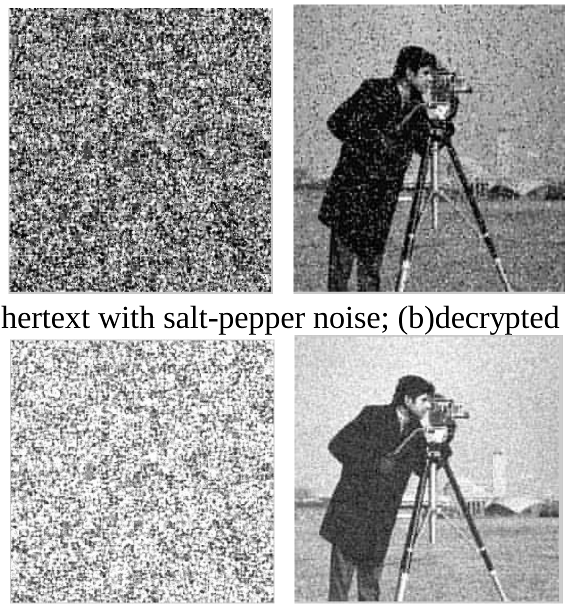
$$\operatorname{cov}(x,y)=1\big/N\sum_{i}^{N}(x_i-E(x))(y_i-E(y)) \tag{9}$$

Table 1 also calculated the correlation coefficient of 3 directions. We can see that the correlation coefficient of adjacent pixels of original image is concentrated in 0.95, while the correlation coefficient of the encrypted image in 0.5, which reduce the correlation.

Table 1 Coefficient of adjacent pixels of plaintext and ciphertext

pixel direction	plaintext	ciphertext
horizontal	0.9368	-0.5487
vertical	0.9584	0.4425
diagonal	0.9368	0.5487

The compressed image data transmission in the process will inevitably encounter all kinds of noise, so good algorithm should have strong anti-noise ability. Figure 6(a) is cipher image adding 10% salt-pepper noise [9], and decrypted it get figure 6(b). Figure 6(c) is cipher image adding 20% gauss noise [9], and decrypted it get figure 6(d). Through the decrypted results, it can see the general shape image. Obviously, the algorithm has good anti- noise ability.



(a) ciphertext with salt-pepper noise; (b)decrypted image of (a)

(c) ciphertext with guass; (d) decrypted image of (c)

Fig.6 Decrypted results of ciphertext with noise

In addition to the above analysis, algorithm running time and compression efficiency were also compared to l literature of 11 and 12. The algorithm time overhead also includes the generation time of chaotic key. From table 2 can see that the algorithm overhead time is very small, but with fast encryption speed.

Table 1The compare between operation and compress

literature	operation time(s)	compress ratio
literature 11	64.1713	4.28
literature12	19.0655	4.38
this paper	0.8372	8.25

4. Conclusion

In this paper proposed one chaotic encryption method in image DCT domain according to the characteristics of JPEG compression image. According to the characteristics of image DCT coefficient matrix by the quantized, in use of based on pixel block scrambling in airspace, put encryption only on the interest coefficients and run the again XOR scheme when element change to "0" value after first XOR in order to guarantee the high compression rate of image. Through the simulation experiment and performance analysis, validate that the algorithm is simple, fast, the characteristics of good encryption effect etc.

References

[1] Li yonghua, Wang bing. Image encryption algorithm base on chaos sequence. Computer Applications, 2009, 6 (29):p.1-2.

[2] Fan weiju, Jiang peigang, Zhan yong. A New Research of Still Image Encoding Compression Algorithm.Communication and Information Processing, 2010, 29(1):p.1-2.

[3] Chen Xuesong, Wang Haiwei. Research on Prosperity of J PEG Compressed Encoding Algorithm. Computer and Digital Engineering, 2009 (1):p.1-4.

[4] Lifford McLauchlan, Mehrübe Mehrübeoğlub. DWT and DCT embedded watermarking using Chaos theory. Proc of SPIE Vol, 2010: 7799 77990L-1.

[5] Sun xin, Yi kaixiang, Sun youxian.Image encryption algorithm base on chaose system.Journal of Computer Aided Design and Computer Graphics, 2002, 2(2):p.1-4.

[6] Huang hao, Huang ruisheng. “Chaos and Application” Wu Han university press.2007.

[7] YANG Fan, XUE Mo-gen. Research on digital image encryption algorithm based on compound chaotic image second-scrambling. Journal of HeFei University of Technology.2009, 32(8):p.4-5.

[8] Tang lei, Shi yongli. Reseach on static image coding.Journal of Wuhan Bioengineerimg Institute, 2006, 6(3):p.2-4.

[9] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah. An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption .Information. 2007:p.121-129.

[10] Rafael C. Gonzalez, Richard E. Woods. “Dital Image Processing”. Bei jing electronics industry press, 2003: p.176-179.

[11] Peng cheng, Liu ji.Compress image encryption algorithm application base on chaos sequence. Computer Engineering, 2008, 34(20):p.177- 179.

[12] Liu chunsheng. Compress image encryption method. Journal of Henan Education Institute, 2010, 18(4):p.3-5.