Color Image Fast Encryption Algorithm Based on JPEG Encoding

Ma Rong[1], Yao Gaohua[2(✉)], and Guo Hui[2]

[1] School of Electronics and Information Engineering, Wuzhou University, Wuzhou 543002, China

[2] Guangxi Key Laboratory of Machine Vision and Intelligent Control, Wuzhou University, Wuzhou 543002, China

12348906@qq.com

Abstract. In order to strengthen the security of standard JPEG format color images in network transmission, this paper proposes a kind of JPEG color image encryption algorithm which combines the efficient and stable compression encoding with encrypting selectively. First, it selects out mapping better chaotic characteristics as a pseudo-random number generator, and uses the generated chaotic sequence for the encryption algorithm. Then, it uses the edge detection algorithm to find the blocks with rich image contour information, which provides a basis for selection and encryption of later images. It Encrypts the quantized image coefficients and embeds in the important block information. The experimental results shows that the algorithm in this paper can hide the color information and contour information of the plaintext image effectively. At the same time, the key is more sensitive. Compared with the classic encryption algorithm AES, it has better performance in terms of time complexity and encryption quality.

Keywords: JPEG · Chaotic system · DC hiding · Encrypting selectively

1 Introduction

Image encryption algorithm is an important research issue in the fields of digital image processing, computer vision, and reliable video transmission [1]. With the increasing demand for image privacy in the context of the Internet, image encryption algorithms have been widely used in key areas such as politics, economy, military, and medical care [2]. Most mainstream image encryption algorithms are to hide data in the frequency domain and spatial domain. So, the mainstream image encryption can be divided into two categories: one is to select the larger part of the information in the image for the encryption algorithm, so as to reduce the amount of encrypted data; the other one is to use the encryption algorithm throughout the entire image compression coding process to reduce the generation of compressed data redundancy.

With the help of the idea of selective encryption, Xiao Ning et al. proposed an infrared image selection algorithm based on multi-feature difference detection and joint control

X. Jiang (Ed.): MLICOM 2021, LNICST 438, pp. 307–314, 2022.
https://doi.org/10.1007/978-3-031-04409-0_28

mapping [3]. Yu Ping et al. solved the problem of insufficient secure transmission on encryption algorithms, and proposed an infrared target selection encryption algorithm basing on geometric active contour mode and coupled mapping [4]. On the basis of selective encryption, Khan Naqash Azeem et al. proposed a new chaotic-based S-box to encrypt JPEG graphics selectively [5]. Yang Wei et al. proposed a three-dimensional image joint encryption and compression algorithm by optimizing the decryption accuracy and compression ratio [6]. Li Peiya et al. proposed JPEG joint graphic compression and encryption algorithm on JPEG graphics compression [7]. Liu Zhuo et al. proposed an image compression encryption algorithm based on the two-dimensional coupled image lattice model [8]. By encrypting images selectively, the amount of calculation can be greatly reduced, but the security cannot be guaranteed. The compression encryption algorithm is superior in encryption performance and security but time-consuming. Therefore, Considering the contradiction between efficiency and security, there are few reports on the combination of selective encryption and compression algorithms so far.

This paper analyzes the characteristics of two mainstream encryption algorithms systematically, and optimizes the whole image encryption process by the combination of image compression process encryption and selective encryption. First, it blocks scrambling and encrypting the original image, and then encrypts DCT coefficients and their rich symbols during JPEG encoding to realize hiding the image DCT coefficients. Simultaneously, it Chooses a map with better chaotic effects as a pseudo-random number generator to generate a chaotic sequence for the encryption algorithm, encrypting the edge detection image blocks with rich texture by the approach of edge detection, and then embeds the encrypted relevant information into the DCT coefficients. The final theoretical analysis and experimental results show that compared with the traditional encryption algorithms, the algorithm described in this paper is more advantageous, stable and robust in terms of timeliness, security, encryption quality, etc.

2 Color Image Encryption Algorithm Based on JPEG Encoding

Encryption algorithm of JPEG color image in this paper uses edge detection strategies to select regions with rich textures for image encryption and adopts chaotic coding strategy to realize spatial scrambling encryption of image. Then it completes the encryption operation in the frequency domain when the image data undergo DCT transformation, and at the same time it embeds the selected encrypted information into the image data. The overall flow chart of the algorithm is as follows (as shown in Fig. 1).

2.1 Image Edge Detection

If all DC coefficients and AC coefficients are encrypted, it is not only computationally expensive but also time-consuming. The selective encryption can effectively reduce various expenses in the encryption process and ensures the encryption effect. So, this paper focuses on selective encryption for areas with richer edge information.

First, the encrypted image is divided into 8×8 area, then it selects the Canny operator to detect the edge of the encrypted image, choosing a reasonable threshold T based on

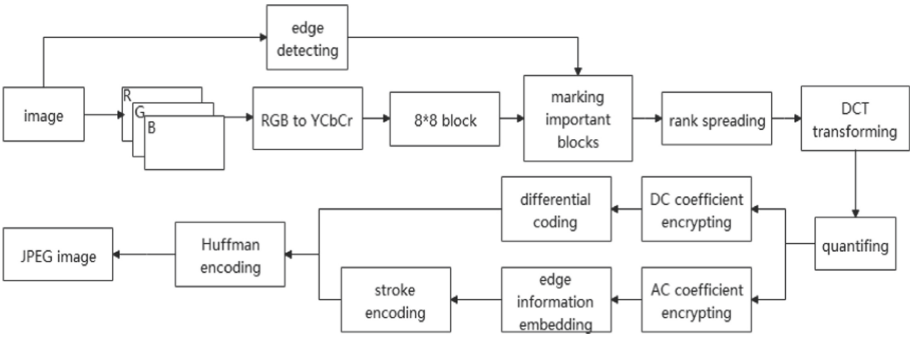


Fig. 1. Flow chart of color image encryption algorithm based on JPEG encoding

the amount of information at the edge of each block to complete the screening of whether there are key encrypted blocks in each block.

The images obtained after edge detection is shown below (as shown in Fig. 2).

Fig. 2. The result of House edge detection by canny operator

2.2 Key and Chaotic Sequence Generation

The characteristics of concealment, unpredictability, complexity and easy implementation of chaotic signals can completely match the relevant requirements of encryption algorithms for keys. Encryption algorithm in this paper uses the keys such as K1, K2, K3, K4, K5, etc., and adopts the Henon mapping and PWLCM mapping in the discrete chaotic sequence system to generate three sets of mixed sequences (H1, H2), P1 and P2. The Henon map is a two-dimensional discrete chaotic system.

The mapping equation is as follows:

$$\begin{cases} x_{n+1} = 1 - 1.4x_n^2 + y_n \\ y_{n+1} = 0.3x_n \end{cases} x \in (-1.5, 1.5), y \in (-0.4, 0.4) \quad (1)$$

PWLCM mapping is a piecewise linear chaotic map with good statistical characteristics and computer fixed-point realization ability. The mapping equation is as follows:

$$x(k+1) = C[x(k); \mu] = \begin{cases} \frac{x(k)}{\mu}, x(k) \in [0, \mu) \\ \frac{x(k)-\mu}{0.5-\mu}, x(k) \in [\mu, 0.5) \\ C[1 - x(k); \mu], x(k) \in [0.5, 1) \end{cases} \quad (2)$$

μ is a positive real number, the value range is $\mu \in (0, 0.5), x \in (0, 1)$.

In addition, the parameter disturbance function is defined to control the result in the corresponding parameter range. Among them, γ Adjust the factor for the range.

$$F(a, b, c) = \gamma \times \frac{a + b + c}{3} \quad (3)$$

The specific implementation steps are shown in the following figure (as shown in Fig. 3):

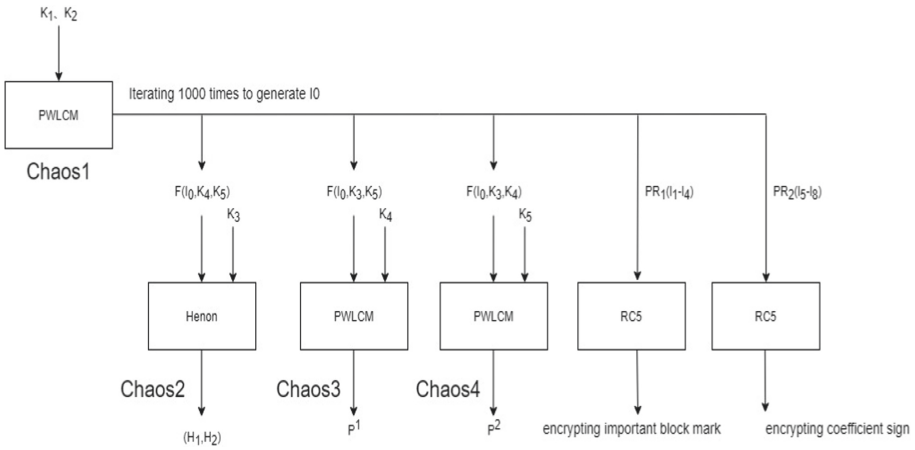


Fig. 3. The application of keys and the generation of chaotic sequences

2.3 Process of Image Spatial Space Block Scrambling Encryption

When the digital image is JPEG encoded, it is usually necessary to encrypt the image in the airspace first. Scrambling images is one of the commonly used airspace encryption methods. The parameters used in the scrambling process are inherently random, and the sequence generated by the discrete chaotic mapping system can be used as the image scrambling process.

The image scrambling method based on chaotic mapping can be summarized as follows:

1. Using Henon chaotic mapping to generate chaotic sequence (H_1, H_2).
2. Scrambling the lines of the image block map. Each row is cyclically shifted to the right, and the number of shifts is determined by the Henon chaotic mapping sequence H_1. In the same way, each column is shifted in blocks, and the number of shifts is determined by the *Henon* chaotic mapping sequence H_2.
3. Multiple rounds of block row and column cyclic shift operations can achieve encryption effects. The scrambling operation is realized by "modulo operation", and the result of the operation is controlled within the value range of the number of blocks. The formula is as follows:

$$\begin{cases} x_i = (x_i \times 1000000) \, mod \, L(x_i \in H_1) \\ y_i = (y_i \times 1000000) \, mod \, C(y_i \in H_2) \end{cases} \tag{4}$$

As shown in formula 3, L is the number of rows and C is columns in the block. Corresponding to the i-th row, the number of shifts in the i-th row is a x_i block, and the same is for columns.

2.4 Selective Encryption of Image DCT Domain Coefficients

After the image is transformed by DCT, the DC coefficient holds most of the information of the image, while the AC coefficient holds relatively little information. Therefore, the same strategy is adopted to realize the selective encryption of DC coefficients. Using the P^1 chaotic sequence generated by PWLCM mapping as the key stream of the sequence cipher to encrypt each coefficient, the process is shown in the following formula:

$$d_i = d_i xor((P_i^1 \times 1000000) \, mod \, (1023/Q_1)) \tag{5}$$

In formula (4), P_i^1 represents the i-th value in the chaotic sequence, and Q_1 is the same value in the quantization table as the coefficient position of each block. Since the DCT coefficient value range is -1024 to 1023, dividing 1023 by Q_1 and taking the remainder is to ensure that the DC coefficient is within the value range after XOR encryption.

The encryption of AC coefficients depends on the marking of image blocks, using Zig-zag method to select the first 16 AC coefficients from all marked blocks to encrypt. The calculation method is as follows:

$$a_i = a_i xor((P_i^1 \times 1000000) \, mod \, Q_i) \tag{6}$$

As shown in formula (5), it encrypts all 16 coefficients.P_i^1 is the i-th value in the chaotic sequence, and Q_i represents the same value in the quantization table as the position of the AC coefficient of each block.

In the algorithm for encrypting DCT coefficients, encrypting the absolute values of the DCT coefficients to be encrypted with serial ciphers, then it takes out the symbols of these coefficients to form a symbol bit sequence and encrypts them to achieve the effect of hiding the DCT coefficient information completely.

3 Analysis of the Results

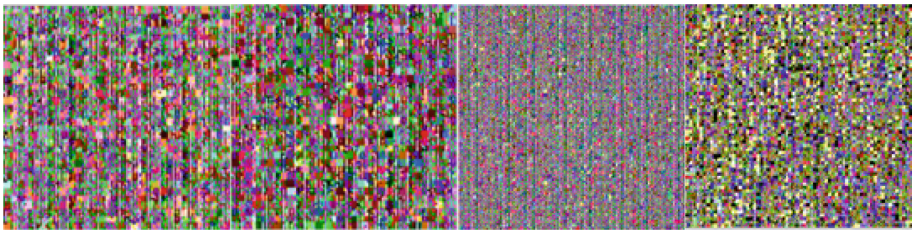
3.1 Experimental Platform and Standard Test Library

The relevant configuration of the machine in this experiment is: Intel(R) Core (TM) i5-4210U processor, 8G running memory, Win10 system, MatlabR2014a integrated development environment.

The experimental test image and the encryption result obtained by the algorithm in this paper are as follows (as shown in Fig. 4 and Fig. 5):

a. Lena b. Fruit c. Baboon d. Sailboat

Fig. 4. Experimental test image



a. Lena b. Fruit c. Baboon d. Sailboat

Fig. 5. Algorithm encryption effect

The experiment selects four representative color images in the USC-SIPI image library, and verifies and compares the classic AES encryption algorithm with the encryption algorithm described in this article. The experimental results show that the algorithm in this paper has better results in both the encryption effect and the encryption efficiency compared with the AES encryption algorithm. At the same time, it is verified that the algorithm described in this article is more superior, stable and robust in terms of timeliness, security, encryption quality, etc.

The algorithm encryption result evaluation table is as follows (as shown in Table 1).

PSNR and MSSIM and LSS in Table 1 respectively represent important parameters such as peak signal-to-noise ratio, average structure similarity index, and brightness similarity of the image. The algorithm in this paper has achieved better results in various

Table 1. Encryption algorithm and AES algorithm encryption results evaluation index data

Image	The algorithm in this paper			AES algorithm encryption		
	PSNR/dB	MSSIM	LSS	PSNR/dB	MSSIM	LSS
Lena	6.071	0.004	−20.348	7.906	0.008	−18.755
Fruit	6.170	0.002	−18.262	7.759	0.008	−18.010
Baboon	6.194	0.004	−15.369	8.776	0.008	−15.155
Sailboat	5.965	0.004	−21.013	8.114	0.010	−19.678

indicators. For images with rich textures, the peak signal-to-noise ratio and average structure similarity index are more convenient and effective.

The experimental situation of the algorithm when it is used in encryption is as follows (as shown in Table 2).

Table 2. Comparison of time-consuming algorithm encryption and AES algorithm encryption

Image	Size/px	Time consuming encryption algorithm/s	AES algorithm encryption time consuming/s
Lena	256 × 256	2.21	93.59
Fruit	256 × 256	2.31	91.00
Baboon	512 × 512	11.04	483.80
Sailboat	512 × 512	10.51	487.61

According to the data in Table 2, the algorithm in this paper has obvious advantages in terms of time over the AES algorithm, and the execution time of the encryption algorithm is more than tens of times faster than the AES algorithm.

4 Conclusion

This paper mainly studies image encryption technology, and designs the encryption algorithm fully according to the characteristics of the image data structure. Therefore, using color image compression encoding encryption and selective encryption, this paper proposes an encryption algorithm based on JPEG image compression coding. A certain amount of experimental results verify that the algorithm in this paper is more superior, stable and robust than traditional encryption algorithms in terms of timeliness, security, encryption quality, etc.

Acknowledgments. Supported by a project grant from National Natural Science Foundation (Grand No. 61961036 & 62162054), the University Young Teachers Basic Ability Improvement Project of Guangxi (Grand No. 2018KY0537 & 2017KY0629), Wuzhou Scientific Research and Technology Development Project (Grand No. 201501014), Guangxi Natural Science Foundation (Grand No. 2020GXNSFAA297259 & 2018GXNSFBA281173), Wuzhou Hightech Zone, Wuzhou University Industry-Education-Research Project (Grand No. 2020G001), the Guangxi Innovation-Driven Development Special Driven Develop Special Fund Project (Guike AA18118036), the Guangxi Science and Technology Base and Talent Special Project (Guike AD20297148).

References

1. Wade, M.I.: Distributed image encryption based on a homomorphic cryptographic approach. In: 2019 IEEE 10-th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UE-MCON), New York, USA, 2019, pp. 0686–0696, (2019). https://doi.org/10.1109/UEMCON47517.2019.8993025
2. Abdmouleh, M.K., Khalfallah, A., Bouhlel, M.S.: "A novel selective encryption dwt-based algorithm for medical images. In: 2017 14th International Conference on Computer Graphics, Imaging and Visualization, Marrakesh, Morocco, pp.79–84 (2017). https://doi.org/10.1109/CGiV.2017.10
3. Ning, X., Aijun, L.: Infrared image selection encryption algorithm based on multi-feature difference detection and joint control mapping. Appl. Opt. **38**(03), 406–414 (2017)
4. Ping, Y., Qiang, Y., Lijun, Z.: Infrared target selection encryption algorithm based on geometric active contour. Comput. Eng. Des. **39**(04), 1148–1154 (2018)
5. Khan, N.A., Altaf, M., Khan, F.A.: Selective encryption of JPEG images with chaotic based novel S-box. Multimedia Tools Appl. **80**(6), 9639–9656 (2020)
6. Wei, Y., Qingzhu, W., Renjie, S., Yuandong, Z.: Joint encryption and compression algorithm for three-dimensional images. Microelectron. Comput. **37**(07), 78–81 (2020)
7. Li, P., Lo, K.T.: Survey on JPEG compatible joint image compression and encryption algorithms. IET Signal Process. **14**(8), 475–488 (2020)
8. Zhuo, L., Yong, W.: Image compression and encryption scheme based on two-dimensional coupled image lattice model. J. Chongqing Univ. Posts Telecommun. (Nat. Sci. Edition) **32**(06), 1048–1057 (2020)