Joint image compression and encryption method

Jiaojiao Xie[1*],Xiaojun Tong[1],Yimao Zhao[1]

[1]Harbin Institute of Technology,China

*xjj_edu@163.com

Keywords:chaos;sparse;Chinese remainder theorem;encryption;compression

Abstract. Joint encryption and compression method not only ensure the uniformity of the algorithm but also can enhance the security of algorithm, so it have very important practical significance.This paper studies the over complete dictionary of DCT and OMP algorithm,uses the two kinds of common chaos mapping and learns China remainder theorem. Then one joint image compression and encryption algorithms using chaos map, sparse decomposition and Chinese remainder theorem is proposed to realize image compression and encryption.The experimental results show that the algorithm realizes information transmission requirements in security and efficiency, and achieves the desired requirements.

1 Introduction

With the rapid development of network and multimedia technology, image as a carrier for the dissemination of information plays an important role. Today, secure and efficient transmission of image information has become a hot research direction.

The main method is image encryption to ensure the security of image transmission.While applied to the image, traditional encryption methods are not very good in terms of encryption effects and time .Meanwhile,with the improvement of decryption technology ,some traditional encryption methods become insecure.Because of the characteristics of massive and relevance , uncompressed images data hava brought tremendous pressure on the storage of information and network bandwidth. The conventional methods make compression and encryption as two separate steps, so the attackers can completely ignore the compression process and directly attack the encryption process.So it is the difficulty and deficiency of present study.

This paper aims to the research of combination of image compression and encryption technology,and makes the algorithm has not only good security but also high compression performance.Therefore, the study of this paper has a high value of practical application.

2 Preliminary work

2.1 Chaos theory

Chaos is a kind of similar to nonregular motion and produced similar random behavior in a deterministic nonlinear system.Because chaos has many basic features such as the randomness, sensitivity to initial conditions and these characteristics are accord with the basic requirements of cryptography. The method used in this paper are Logistic mapping and Arnold mapping which are both simple and safe.

2.2 Sparse decomposition

Sparse representation of images can be used to store and transfer images with less coefficients which is very important in image compression, denoising and so on.There are two common over complete dictionary:one is fixed dictionary (complete DCT, Contourlet, Wavelet dictionary),the other one is over complete dictionary which through the study of training set to produce.The DCT dictionary is producing simply and fast and easy for image compression and decompression.So now in this paper I choose the DCT dictionary to decompose the image[3].Due to the non-convexity of L0 norm,it is a typical NP hard problem when making the only solution.So many efficient algorithms have been proposed, such as MP, OMP, BP and so on. Among them, OMP is a kind of

improved MP algorithm and using Gram-Schmidt orthogonal algorithm which is introduced to improve the matching pursuit approach.

2.3 Chinese remainder theorem

The Chinese remainder theorem gives the linear congruent equation[4]:

$$(S):\begin{cases} x = a_1 (\bmod m_1) \\ x = a_2 (\bmod m_2) \\ \quad\vdots \\ x = a_n (\bmod m_n) \end{cases} \tag{1}$$

Assuming $m_1, m_2, \ldots, m_n$ are postitive integers which are mutually coprime, so the equations (S) are solved for arbitrary integer $a_1, a_2, \ldots, a_n$.

Setting $M = m_1 \times m_2 \times \cdots \times m_n$, $M_i = M / m_i$, $t_i M_i = 1(\bmod m_i)$, $\forall i \in \{1, 2, \ldots, n\}$, and the general form is as follows: $x = a_1 t_1 M_1 + a_2 t_2 M_2 + \cdots + a_n t_n M_n + kM$,$k \in Z$

4 The proposed image encryption-compression scheme

According to above content, the paper proposes a joint algorithm based on sparse decomposition, chaos and Chinese remainder theorem.The process is as follows:

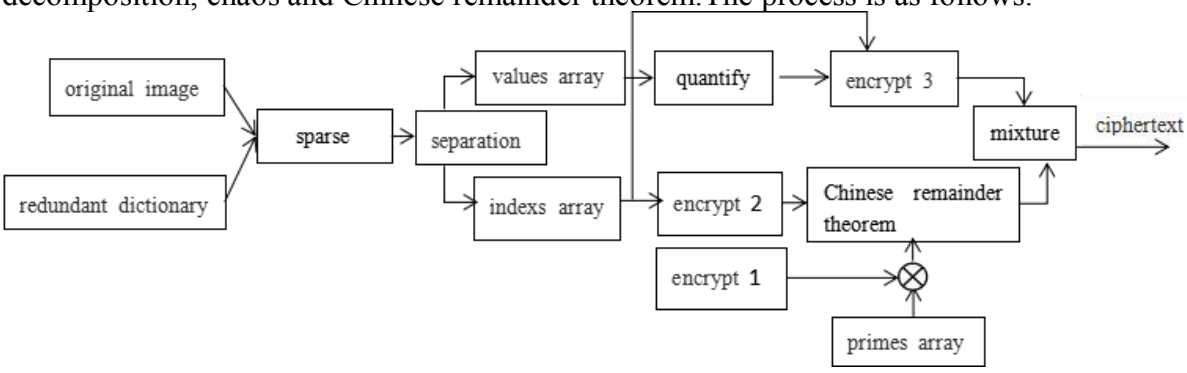

Figure 1.joint compression and encryption algorithm flow chart

Algorithm detailed steps are as follows:

(1)Sparsing decomposition:The original image is divided into N small pieces of 8x8. if the length of the image is not a multiple of 8,we can processing by adding 0.We use OMP algorithm to sparse for each small piece , then we get a column of the sparse coefficient vectors of $M \times 1$ which M is the size of the dictionary. So the sparse matrix is composed of the sparse coefficient vectors.

(2)Separation:we traverse sparse matrix by each column and record the abscissa of non-zero values,so we get the indexs array of . At the same time creating another the same size of the values array to record non-zero value.

(3)Encryption method 1:We create a size $K \times N$ of primes array.The first column of the primes array consist of K integers which are greater than 64 and different , and the rest columns' value is empty.We set the initial value x_0 and parameters μ and iterate the Logistic equation $1000 + K \times N$ times.In order to eliminate the chaotic transient effect, we get rid of the first 1000 values.So we get chaotic sequences A.The chaotic sequence A is divided into N blocks: $A_i = A_i^1, A_i^2, ..., A_i^K, i \in N$ .The sequence B obtain by ordering A from small to large.According to the change of the corresponding position in sequence A and B ,we set the i th columns of primes array by scrambling the $(i-1)$ th columns and repeatedly scramble N times.

(4)Encryption method 2:We set the initial value a, b and iterate Arnold mapping to shuffle the data of indexs array.

(5)Using Chinese remainder theorem:We use the i th column of the primes array as primes of the Chinese remainder theorem formula $m_n^i, 1 \le n \le K, 1 \le i \le N$ and the i th column of the indexs array as constants of the formula $a_n^i, 1 \le n \le K, 1 \le i \le N$ where i is the number of columns and n is the

number of values. So we get compression value $x^i, 1 \le i \le N$ by calculating m_n^i and a_n^i.

(6)Quantification:In order to improve the compression performance of the algorithm, we quantify the values array.The approximate value y is $y = round(x/Q)$ and $Q = (x_{\max} - x_{\min}) / \left(2^b - 1\right)$.

(7)Encryption method 3:We obtaine the average value and standard deviation by calculating all values of indexs array.Using them to disturb the initial value of Logistic mapping and Arnold mapping.Logistic mapping diffuse the data of indexs array and Arnold mapping scramble them.we get encrypted value for the array. Perturbation method is:

$$\begin{cases} x_0^{'} = (x_0 + \alpha / 64) \bmod 1 \\ u^{'} = (\mu + \beta) \bmod 1 \\ a^{'} = round(a + \alpha) \\ b^{'} = round(b + \beta) \end{cases} \tag{2}$$

(8)The processed values array and indexs array are combined into a cipher text array for transmission. In the receiving end, it is opposite to all the upper step when signal recovery and reconstruction.

5 Experimental results and analyses

We use Matlab 2012b to achieve the proposed algorithm. The results are analyzed and compared and the performance of algorithm is also analyzed.

(a) original image (b)The image after decompression

(c) compression and encryption

Figure 2. Effect contrast diagram

In safety, we analyse the gray level histogram and the correlation of adjacent pixels, the result is as follows:

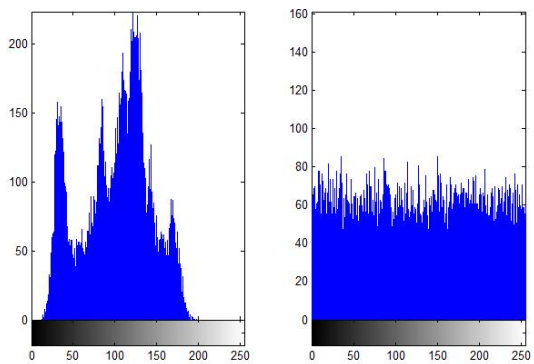

Figure 3. grey level histogram

As shown pixels of the encryption images can be evenly distributed in the [0,255], the distribution has nothing to do with the original image.The correlation of original image's adjacent pixels is that the horizontal direction is 0.99323, vertical direction to the 0.99383 and diagonal direction for 0.99125.And cipher image correlation is that level is 0.01162, vertical to the 0.14248, diagonal for 0.015665.Comparison shows that the encryption operations reduce the correlation and encryption effect is good.

On the basis of ensuring safety, judgment criteria for image compression algorithm has two: image compression ratio and PSNR between the original image and the restore image .Compared with the PSNR value and image compression ratio of the literature , which is shown in the table, and '-' said that this image was not to analyzed in reference .

Table1 The performance comparison of different compression and encryption of technology

	Lena		Pepper		Baboon		Barbara	
	CR	PSNR	CR	PSNR	CR	PSNR	CR	PSNR
Ref[5]	13.8	31.46	--	--	4.33	28.56	6.49	31.87
Proposed	15.0	33.27	7.64	29.34	4.44	28.79	7.21	31.03

The table shows that the proposed compression and encryption technology has good pe rformance in compression ratio and image quality.

6 Conclusion

The main research work of this paper is as the following: a brief review of chaotic map, sparse decomposition algorithm and the Chinese remainder theorem, propose a joint compression and encryption algorithm . According to the characteristics of the image, sparse decomposition and the Chinese remainder theorem are used to compression process, and chaos map is used to encryption process, so we achieve the joint compression and encryption effect. Meanwhile,this paper draws a flowchart of the algorithm, and makes detailed description of the algorithm and simulation experiment. The results of the experiment show that our algorithm has higher security and better compression.Due to the proposed joint compression and encryption technology involves many technologies, subject crossing and wide application fields,so considerable work remains to be done on this issue.

References

[1Ttheory and applications of chaotic cryptography,Beijing:science press, 2009: 2-4.

[2]Mairal J, Elad M,Sapiro G, Sparse representation for color image restoration, Image Processing, IEEE Transactions on, 2008, 17(1): 53-69.

[3]Yafang Mao,Study and implementation of the image compression and encryption technology based on chaotic system,Harbin:Harbin Institute of Technology,2014.

[4]Hegui Zhu,Cheng Zhao,Xiangde Zhang,A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem,Signal Processing:Image Communication,2013,28:670 -680.

[5]Yan Wu,Research on joint image compression and encryption method,Nanchang:Nanchang University,2013: 25-67.