# Image compression and encryption based on wavelet transform and chaos

*H. Gao [1], W. Zeng [1]*
[1] *College of Information Science & Engineering, Hunan International Economics University, Changsha 410205, China*

***Abstract***

With the rapid development of network technology, more and more digital images are transmitted on the network, and gradually become one important means for people to access the information. The security problem of the image information data increasingly highlights and has become one problem to be attended. The current image encryption algorithm basically focuses on the simple encryption in the frequency domain or airspace domain, and related methods also have some shortcomings. Based on the characteristics of wavelet transform, this paper puts forward the image compression and encryption based on the wavelet transform and chaos by combining the advantages of chaotic mapping. This method introduces the chaos and wavelet transform into the digital image encryption algorithm, and transforms the image from the spatial domain to the frequency domain of wavelet transform, and adds the hybrid noise to the high frequency part of the wavelet transform, thus achieving the purpose of the image degradation and improving the encryption security by combining the encryption approaches in the spatial domain and frequency domain based on the chaotic sequence and the excellent characteristics of wavelet transform. Testing experiments show that such algorithm reduces the memory consumption and implements the complexity, not only can decrease the key spending and compress the time spending, but also can improve the quality of decoded and reconstructed image, thus showing good encryption features with better encryption effect.

*Keywords*: image encryption, wavelet coefficient, chaotic system.

*Citation*: Gao H, Zeng W. Image compression and encryption based on wavelet transform and chaos. Computer Optics 2019; 43(2): 258-263. DOI: 10.18287/2412-6179-2019-43-2-258-263.

*Acknowledgments*: This work was supported in part by Hunan Provincial Education Science five-year plan funded project (No:XJK014BGD046) and 2017 Hunan Education Department Scientific Research Project (NO:17B151,17C0900,17C0899).

## *Introduction*

Image encryption is widely applied in such fields as the secure communication, information hiding and digital watermarking etc. The study on the image encryption has a high theoretical and practical significance. With the development of the digital age, the number of information to be stored, transmitted and processed increases exponentially. And the biggest characteristic and difficulty of image is the representation and transmission of huge amounts of data, with the guarantee of the safety of image data [1], [2]. How to safely and effectively store and transmit the image data becomes the urgent need in the modern information society. The original image data are highly correlated, and there is a lot of redundancy. Eliminating these redundancies can save code word and achieve the purpose of data compression. In most images, there is a large correlation between adjacent pixels, which is spatial redundancy. There is a large correlation between the adjacent frames before and after the sequence image, which is time redundancy. The purpose of compression is to eliminate these redundancies as much as possible, to increase the compression ratio of image encryption, to increase the encryption efficiency of the image, and to facilitate the transmission and storage of the cipher text information. At present, almost all the image encryption algorithms are single image encryption systems, the efficiency of image encryption is low, and the image compression encryption algorithm with high resolution wavelet analysis is less. The wavelet transform coding provides multi-scale and multi-resolution image transformation, and can effectively remove the statistical redundancy and visual redundancy. The field of image compression coding occupies an important position. The application of wavelet transform to the image compression and encryption can obtain compressed images with any compression ratio in theory, and it is also relatively simple to implement such an aim in practice, of course any method has the advantages that are different from other methods, and has certain defects at the same time. Therefore, in order to well achieve the image compression and encryption, a variety of technologies are utilized comprehensively. Such image compression and encryption based on wavelet analysis is not an exception, and in most cases, the dynamic combination of the wavelet analysis and other related technologies is also needed to achieve a more perfect result [3]. In view of this, the research of the image compression and encryption based on the wavelet analysis and chaotic theory not only has an important theoretical value, but also with certain application value. This paper proves that traditional encryption algorithms are not suitable for the image encryption according to the characteristics of large amount of image data and high redundancy. Besides, the schemes exclusively used in image selection encryption that are raised by researchers are still not enough. This paper analyses the deficiency of the common image selection encryption technologies and puts forward the improvement plan based on the wavelet analysis and chaos theory.

Image coding technology began in the late 1940s, and all early classical coding theories such as the entropy cod-

ing, prediction coding and transform coding derive from Shannon's information theory, and the starting point of these coding theories is to eliminate the statistic redundant information in the image. In the 1980s, some new kind of image coding methods such as the sub-band coding, fractal coding and model-based coding arise at the historic moment, and these methods focus on eliminating the visual redundancy, structural redundancy and knowledge redundancy in the image data [4]. After 1990s, because the wavelet transform coding provides a multi-scale and multi-resolution image transform way, and also can effectively remove the statistical redundancy and visual redundancy, the wavelet transform begins to occupy the important position in the image compression coding field, and the still image coding standard JPEG2000 of new generation adopts the wavelet transform. Since Cambridge in England held the first symposium in the information hiding field in 1996, the research of digital image encryption technology has achieved great development [5]. The second and the third international symposiums on information hiding held in the United States and Germany in 1998 and 1999 make more and more scholars devote to the research field of image encryption. The 4th international symposium on information hiding was held in Pittsburgh in the United States in April 2001, and the fifth and the sixth international conferences on information hiding were respectively held in October, 2002 and May, 2004 in Netherlands and Canada [6]. In the study of image encryption, the wavelet theory and chaos theory will be a hot research topic, at the same time, the image encryption is achieved in the frequency domain and the image compression and image encryption is combined, and the compressed encrypted image can also be used as the pretreatment before the digital watermark is embedded. All these will become research hotspots now and later.

This paper firstly introduces the image compression of the discrete cosine transform, the wavelet transform and vector quantization, focuses on how to implement the image compression and encryption with the wavelet transform and chaos theory, and also focuses on realizing the image encryption and the image compression at the same time. However, the image is encrypted with the compression perception alone, and methods are too simple and the encryption process belongs to a linear operation, thus the algorithm has certain security problems. If the wavelet transform and chaos theory are combined, the complexity of the encryption algorithm can be increased, and thus enhancing the security of encryption algorithm. The experimental simulation proves that this algorithm has good diffusion and disturbing feature, conforms to the characteristics of modern cryptography, and also can resist some attacks. This paper shows that with quite high encryption strength, big key space and good practicability, such simple algorithm is simple, easy to implement and not easy to crack.

## *1. Image compression*

### *1.1. Digital image compression method*

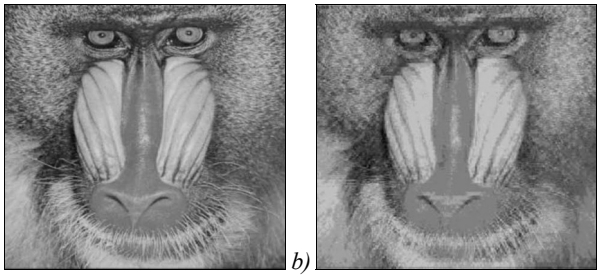
A typical encoder of the transform coding system performs four steps: image block, transform, quantization and coding. Here are some common digital image compression methods [7].

1) Run length encoding, this method is a kind of statistical coding. The main technology is to test repeated bits or characters of sequence, and more suitable for the binary image coding, and the continuous repetitive numerical value is sought in a given data image, and their occurrences are replaced. For images with very large area of the same color, the run length encoding method is very effective. The run length principle derives many concrete run length compression methods, such as PCX run length compression, BI RLE8 compression, BI_RLE compression and Packbits, etc.
2) Huffman coding is to scan image data first and calculate the occurrence probability of all pixels, specify the only codon of different lengths according to the size of the probability, thus getting a Hoffman table of such image. The image data encoded records the codon of each pixel, and the corresponding relations between the codon and the actual pixel values are recorded in the table. Huffman coding adopts the variable length code table to process the source symbols, and the variable length code table is obtained through evaluating the occurrence probability of source symbols. Shorter code is used for letters with high occurrence probability, whereas longer code is used for letters with low occurrence probability, thus the average length and expectation value of encoded character strings is reduced, so as to achieve the goal of lossless data.
3) LZW compression, LZW compression is to achieve the compression by establishing a string table and representing long strings with shorter codes, extract different characters of the original text file data and create a compiling table on the basis of these characters and then use the index of the characters in the compiling table to replace the corresponding characters of the original text file data to reduce the original data size. Compiling table is not created beforehand, but dynamically created according to the original file data, and the original compiling table is restored from the encoded data when decoding. LZW is reversible and all information is retained.
4) Arithmetic compression coding, arithmetic compression coding is a kind of lossless data compression method, and also a kind of entropy coding method. Its basic principle is to express the coded message into an interval between real number 0 and 1. The longer the message is, the smaller the interval expressed by the coding is, and the more binary digits required by such interval are. Arithmetic coding uses two basic parameters: the probability of symbol and its encoding interval. Source symbol probability decides the compression encoding efficiency and also decides

the interval of the source symbol during the coding process, and these intervals are included between 0 and 1. The interval during the encoding determines the output of compressed symbols.

### *1.2. Image compression based on discrete cosine transformation (DCT)*

Discrete cosine transform has been widely applied in the image compression. During the image compression processing, each component image is segmented into 8×8 or 16×6 non-overlapping pixel blocks, and each 8×8 pixel block is called a data unit (DU). When sampling the image, different sampling frequencies can be adopted by the double sampling method, then, two-dimensional DCT transform is processed on each image block, and finally the transformed DCT coefficients are quantified and encoded to form compressed image formats. When displaying images, DCT coefficients quantified and encoded are firstly decoded, and two-dimensional DCT inverse transform is processed on each 8×8 or 16×16 block, and finally all processed blocks are reconstructed into a complete image. After DCT is completed on each 8×8 data block DU, 64 coefficients obtained represent the frequency components of such image block, and the low frequency component concentrates in the upper left corner, and the high frequency component distributes in the lower right corner. The top left corner of the coefficient matrix is called direct current (DC) coefficient, which represents the average of such data block, and the remaining 63 coefficients are called alternating current (AC) coefficients [8]. For a typical image, after DCT, most DCT coefficient values are very close to zero, if these DCT coefficients close to zero are abandoned, the image quality will not significantly drop therefore during the image reconstruction. Divide the following original image shown in Fig. 1(a) into 8×8 sub-images, and process DCT on each image, so that each sub-image has 64 coefficients. 50 % small transform coefficients are abandoned and the 2:1 compression is processed to show the decoded image, as is shown in following Fig. 1*b*.



*a)* *b)*

*Fig. 1. Computational results after discrete cosine transform experiment: Original Image (a), DCT Computational results (b)*

## *2. Wavelet transform and logistic chaotic mapping*

### *2.1. Orthogonal wavelet packet*

Regard the wavelet as a window function and use the time-frequency window to understand the time-frequency localization ability of wavelet transform. Orthogonal wavelet packet is generally explained as

$$\{g_n\}_{n\in Z}\ \{h_n\}_{n\in Z}\ g_n=(-1)^n h_{1-n},$$
$$\begin{cases}\phi(t)=\sqrt{2}\sum_{k\in Z}h_k\phi(2t-k)\\ \psi(t)=\sqrt{2}\sum_{k\in Z}g_k\phi(2t-k).\end{cases} \quad (1)$$

The coefficient filter is only considered.

For convenience to represent the wavelet packet function, the following notations are introduced.

$$\begin{cases}\mu_0(t):=\phi(t)\\ \mu_1(t):=\phi(t)\end{cases},\qquad \begin{cases}\mu_0(t)=\sqrt{2}\sum_{k\in Z}h_k\mu_0(2t-k)\\ \mu_1(t)=\sqrt{2}\sum_{k\in Z}g_k\mu_0(2t-k)\end{cases}. \quad (2)$$

By $\mu_0$, $\mu_1$, $h$, $g$, a group of these can be defined in a fixed scale to be the function of wavelet packet.

From

$$\begin{cases}\mu_{2n}(t)=\sqrt{2}\sum_k h_k\mu_n(2t-k)\\ \mu_{2n+1}(t)=\sqrt{2}\sum_k g_k\mu_n(2t-k)\end{cases}. \quad (3)$$

The function of recursive definition $\mu_n$, $n=0,1,2\ldots$ is called the wavelet packet determined by the orthogonal scaling function $\mu_0=\varnothing$.

Wavelet packet transform can provide a finer decomposition for the high frequency part, and such decomposition has no redundancy and no omission, therefore it can better realize time-frequency localization analysis towards signals including a large number of intermediate frequency and high frequency. Wavelet packet decomposition algorithm is as follows.

$$\begin{cases}d_j^{2n}[k]=\sum_{l\in Z}h_{l-2k}d_{j+1}^n[l]\\ d_j^{2n+1}[k]=\sum_{l\in Z}g_{l-2k}d_{j+1}^n[l]\end{cases}. \quad (4)$$

Wavelet package reconstruction,

$$d_{j+1}^n[k]=\sum_{l\in Z}h_{k-2l}d_j^{2n}[l]+\sum_{l\in Z}g_{k-2l}d_j^{2n+1}[l]. \quad (5)$$

Wavelet packet transform is achieved towards given signals to obtain the wavelet packet coefficient of treelike structure, select the information cost function, use the best wavelet packet basis to select the algorithm and the best basis, process corresponding wavelet packet coefficients of the best orthogonal wavelet packet basis, thus reconstructed signals are obtained by the wavelet packet reconstruction algorithm towards processed wavelet packet coefficients [9].

### *2.2. Chaotic sequence based on logistic mapping*

Logistic mapping is a one-dimensional discrete chaotic system with fast computing speed. The equation repeated iteration can produce good chaotic sequence. The chaotic sequence is extremely sensitive to the initial state and the system parameter. Logistic mapping is defined as:

$$X(n)=F\left[x(n-1)\right]=u*x(n-1)*\left(1-x(n-1)\right). \quad (6)$$

In which, the control parameter u is between (0, 4), and $x(n)$ is between (0,1). A large number of studies on logistic mapping have shown that, when $u$ reaches the limit value, namely $u = 3.5699456$, the steady state solution cycle of the system is $\propto$. When $3.5699456 < u \le 4$ or less, the Logistic map presents the chaotic state, so in order to realize chaos in practical application, the scope of $u$ should be set to: $3.5699456 < u \le 4$ or less.

Define XML string length as $|X|$ and the system interaction time as $N$. $S$ stands for the product of $|X|$ and $N$ after turning into decimals. For example, if $|X| = 35$ and $N = 8$, so $S = 0.352*0.8$, $u = 3.569946 + S/2$ ($u < 4$ is guaranteed); and $X_0 = S$.

After multiple iteration formula $F[x(n-1)]$, a sequence value $X_i (i = 0, 1, 2, 3, 4 \ldots n)$ is obtained. Take the places from number $j$ to number $j+k$ after the decimal point to obtain an encryption key with $n*(k+1)$ place.

A good pseudo-random sequence should have average distribution, that is, the probability of each number should be equal. The iterative sequence distribution of logistic mapping is not uniform, and the other $X_0$ values also have the similar structure. Its distribution is such a situation that the middle is small and both ends are big. Although the distribution is not very average, but for the general case, logistic mapping sequence can meet our requirements [10, 11].

## *3. Implementation of algorithm*

### *3.1. Image compression and encryption based on wavelet transform and chaos*

The image compression and encryption algorithm based on wavelet transform and chaos has such core idea: first, achieve the image wavelet decomposition, and then use the chaotic sequence to rearrange the wavelet coefficients to realize the image encryption. The specific steps are as follows.

1) First determine an expression formula providing chaos, for the given function $f(x) = \mu x(1-x)$, when $\mu = 4.5$, and the initial value $x_0$ is between 0 and 1, the iterative computation is realized. Iterative computation has a strong sensitivity to the initial value, even if the initial value difference is very small, but, after several iterations, both trajectories will vary a lot, for each trajectory of the initial value, the point of the trajectory will not be repeated.
2) Wavelet decomposing the image, the one-dimensional array $C$ after decomposition is the wavelet coefficient set.
3) Take initial value as $x_0 = 0.2$ to make the expression formula $f(x) = 4.5x(1-x)$ iterate, and store the obtained $x(i)$ value in the array $Y$.
4) Establish corresponding relationship between elements in the $C$ and elements in the array $Y$. During transmission, it is difficult to decipher the meaning of such information even if the information leakage. After the transmission, take initial value as $x_0 = 0.2$, and use the expression formula $f(x) = 4.5x(1-x)$ to iterate.

## *4. Experimental test*

Then use a standard Plane image as the test image, adopt the above solution to process the wavelet decomposition and encryption towards the original images. Such solution selects Haar wavelet to realize the original image wavelet decomposition, and chooses two-dimensional logistic mapping to adjust low frequency coefficients. The computational results of the image encryption, compression, decryption and reconstruction based on wavelet transform and chaotic sequence are shown in Fig. 2 – 4. The statistical properties of proposed image encryption and compression algorithm are analyzed by comparing the image histogram.

From the Fig. 2 and Fig. 3, we can see that in the process of compression, encryption, decryption and decompression, the encrypted image compression and encryption quality change little, but still the most information of the original image can be recognized, this indicates that such algorithm show a good compression performance without affecting encryption quality.

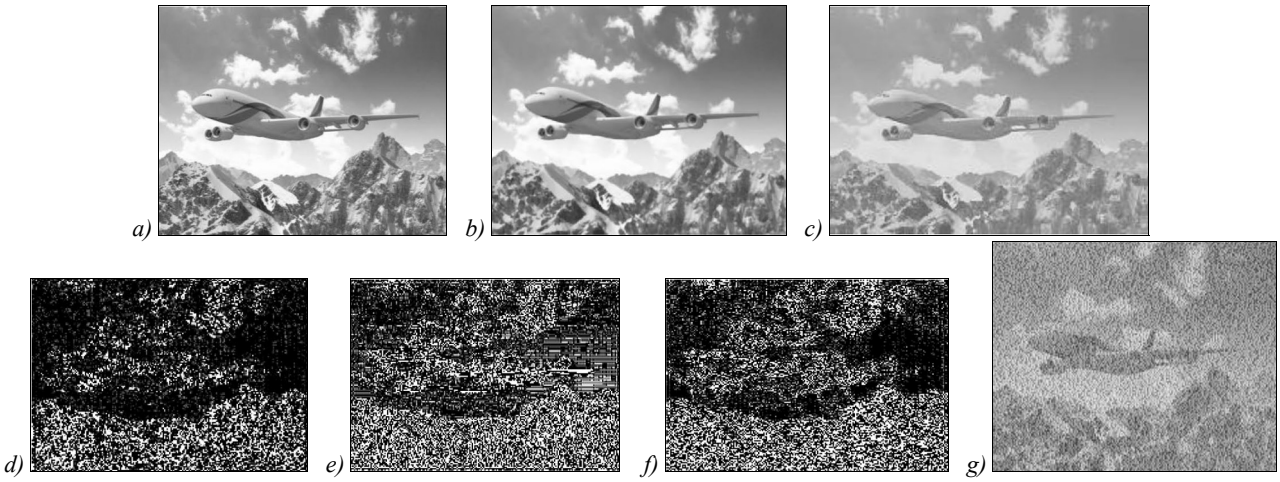



*Fig. 2. Decomposition and encryption: Original image (a), Gray scale image (b), Image approximation (c), Low-frequency horizontal component (d), Low-frequency vertical component (e), High-frequency component (f), Encryption (g)*

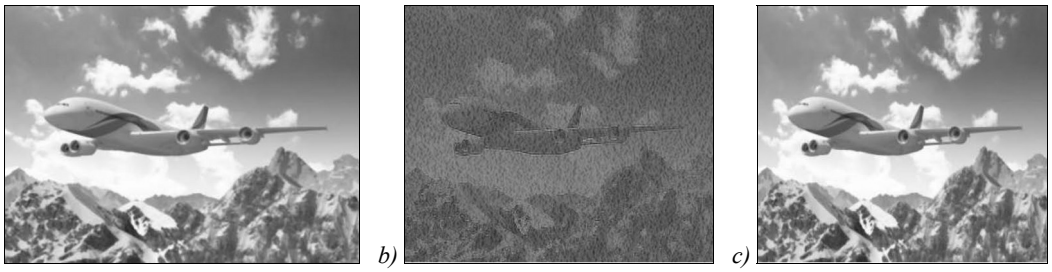


*Fig. 3. Computational results of wavelet reconstruction: Gray scale image wavelet reconstruction (a), Result of encrypted wavelet reconstruction (b), Result of decrypted wavelet reconstruction (c)*

Histogram is a kind of common analysis method in the image encryption algorithm. Fig. 4(b) is histogram after ca1 coefficient encryption and Fig. 4(c) and (d) are respectively the histograms after encryption and decryption. From the test results, encrypted image gray scale histogram is a kind of Gaussian distribution, so from the encrypted image gray scale histogram, the attacker is difficult to get the useful information of the original image. In addition, such algorithm adopts compression sensing to compress images to reduce the ciphertext data amount, thus facilitating the ciphertext transfer and storage.

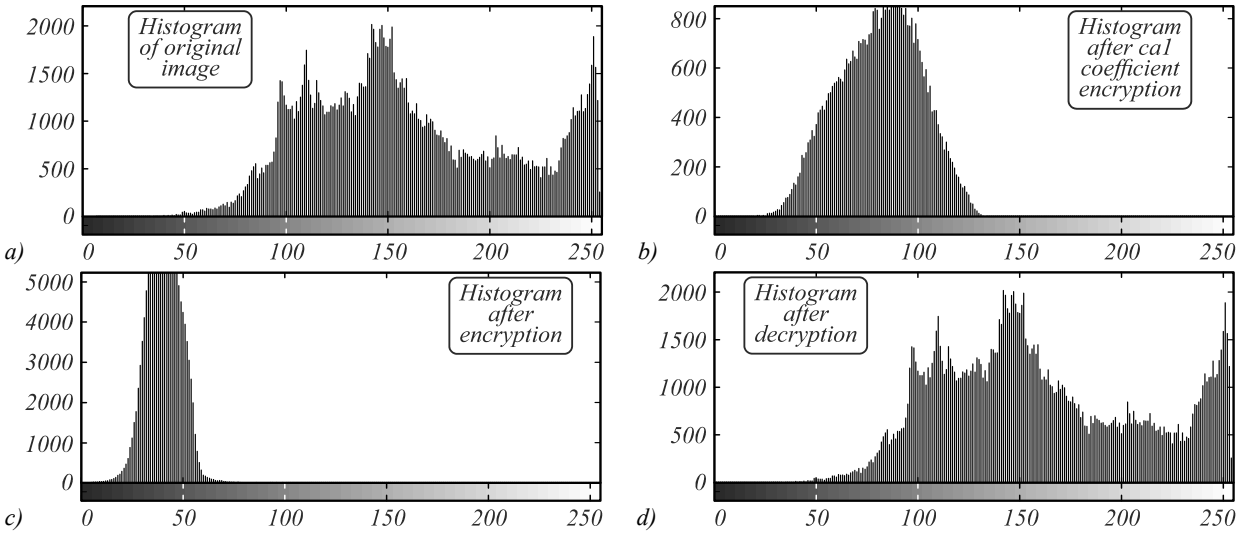



*Fig. 4. Histogram change of whole process: Histogram of original image (a), Histogram after ca1 coefficient encryption (b), Histogram after encryption (c), Histogram after decryption (d)*

The computational formula of MSE is defined as follows.

$$MSE = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}(W(i,j)-M(i,j))}{N^2} \quad (7)$$

The computational formula of PSNR is defined as follows.

$$PSNR = 10\lg(\frac{f_{\max}^2}{MSE}) \quad (8)$$

Here, $N$ is the image size, $(i,j)$ refers to the coordinate of spatial domain; the image to be encrypted is the 256-level gray image $M$, the encrypted image is W, $f_{max}$ is the maximum gray level and its value is 255 in the 8-digit gray image we use. MSE has a poor correlation with subjective assessment and its result frequently differs from the subjective feeling of humans. So, PSNR is mostly adopted as an assessment index. The smaller PSNR means greater difference between the images and the bigger PSNR indicates better image restoration. The PSNR is 28.37 dB and 30.81 dB in Tab.1 and in Tab.2 respectively. This paper has conducted the impact testing on compression efficiency on the algorithm of this paper. The testing contents involve compression time cost, key cost and PSNR of the decrypted reconstructed image. The testing results can be found in Tab. 1 and Tab. 2 below.

Given the uncertainties existing in subjective assessment, it is required to evaluate the restoration performance of the image more objectively. The measurements adopted in this paper include compression time cost, key cost, mean square error (MSE) and peak signal-to-noise ratio (PSNR). Compression time cost is the percentage of the coding and decoding process in the entire operation process of the algorithm. Key cost is the percentage of the size of the key in the size of the original image.

Different encryption methods have different impact on compression efficiency. It can be seen from Tab. 1 and Tab. 2 that when the coding compression ratio is 0.25bpp and 0.5bpp, the compression time cost, i.e. the percentage of the time the compression takes in the entire time the algorithm takes, is smaller and it means that this encryption algorithm has little impact on the compression process. So, the algorithm of this paper has little impact on compression. The key cost refers to the ratio of the size of the key in the size of the original image. It is clear that the key cost falls in the algorithm of this paper. PSNR of the reconstructed image shows the restoration quality after the image is de-

crypted. The bigger PSNR, the better the restoration result. Therefore, the algorithm of this paper can restore a better imaged with a small key cost.

*Table 1. The testing results of this method on compression efficiency in 0.25 bpp*

| Category / Algorithm | Compression time cost | Key cost | PSNR of reconstructed image |
|---|---|---|---|
| This algorithm | 84.38 | 0.037 | 28.37 |

*Table 2. The testing results of this method on compression efficiency in 0.5 bpp*

| Category / Algorithm | Compression time cost | Key cost | PSNR of reconstructed image |
|---|---|---|---|
| This algorithm | 95.43 | 0.037 | 30.81 |

## *Conclusion*

In the process of image compression transmission, sometimes for the sake of security, images are often encrypted, compressed. The image data confidentiality encryption mode makes the encrypted image information present a pseudo random state to prevent illegal users steal. According to the excellent characteristics of wavelet transform and chaotic sequence, this paper introduces the wavelet transform and chaos into the compressed digital image encryption algorithm, which uses the characteristics of wavelet transform and chaotic mapping to overcome the former insufficiencies, and combines the encryption approaches in the airspace and frequency domain to encrypt images, thus improving the encryption security. Experimental tests show that the compressed encrypted method in this paper shows good encryption features and better encryption effect.

## *References*

[1] Tong X, Chen P, Zhang M. A joint image lossless compression and encryption method based on chaotic map. Multimedia Tools and Applications 2017; 76(12): 13995-14020.

[2] Zhu H, Zhao Ch, Zhang X. A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem. Signal Processing: Image Communication 2013; 28(6): 670-680.

[3] Alfalou A, Brosseau C, Abdallah N. Assessing the performance of a method of simultaneous compression and encryption of multiple images and its resistance against various attacks. Opt Express 2013; 21(7): 8025-8043.

[4] Kong Y, Lu H-j. Time-varying neural networks for dynamical systems modeling with application to image compression. International Journal of Security and Its Applications 2016; 10(12): 323-334.

[5] Tang J. Critical algorithm for graph and image compression and transmission research. International Journal of Future Generation Communication and Networking 2016; 9(12): 387-394.

[6] Jaferzadeh K, Gholami S, Moon I. Lossless and lossy compression of quantitative phase images of red blood cells obtained by digital holographic imaging. Appl Opt 2016; 55(36): 10409-10416.

[7] Alfalou A, Brosseau C, Abdallah N, Jridi M. Assessing the performance of a method of simultaneous compression and encryption of multiple images and its resistance against various attacks. Optics Express 2013; 21(7): 8025-8043.

[8] Zhou J, Liu X, Au OC, Tang YY. Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation. IEEE Transactions on Information Forensics and Security 2014; 9(1): 39-50.

[9] Babu RN, Arulmozhivarman P. Improving forecast accuracy of wind speed using wavelet transform and neural networks. Journal of Electrical Engineering and Technology 2013; 8(3): 559-564.

[10] Khalili M, Asatryan D. Colour spaces effects on improved discrete wavelet transform-based digital image watermarking using Arnold transform map. IET Signal Processing 2013; 7(3): 177-187.

[11] Mikherskii RM. Application of an artificial immune system for visual pattern recognition. Computer Optics 2018; 42(1): 113-117. DOI: 10.18287/2412-6179-2018-42-1-113-117.

## *Authors' information*

**Haibo Gao** (b. 1979) graduated from Central South University in 2007, majoring in Computer Application Technology. Currently, he is an associate professor of Hunan International Economics University, China. His research interests include computer graphics processing, information security and algorithm research and analysis.

**Wenjuan Zeng** (b. 1979) received the Master's degree in Computer and Communication, Hunan University, China in 2009. Currently, she is an assistant researcher of Hunan International Economics University, China. His research interests include information security, image processing and algorithm research and analysis.

*Received May 25, 2018. The final version – March 25, 2019.*