Available online at www.ijpe-online.com

International Journal of Performability Engineering

vol. 15, no. 8, August 2019, pp. 2277-2284
DOI: 10.23940/ijpe.19.08.p28.22772284

Image Pixel Value Unification Digital Watermarking Embedding Method based on Quantum Key

Jianan Wu[a,b], Di Zhang[a,b], Huan Wang[a,b], Dexin Zhu[a,b], and Lijun Song[b,c,*]

[a]*College of Computer Science and Technology, Changchun University, Changchun, 130022, China*
[b]*Institute for Interdisciplinary Quantum Information Technology, Jilin Engineering Normal University, Changchun, 130052, China*
[c]*Jilin Engineering Laboratory for Quantum Information Technology, Jilin Engineering Normal University, Changchun, 130052, China*

Abstract

At present, most watermarking algorithms use pseudo-random number sequences as watermarks, and the design of the algorithm is more focused on improving the concealment and robustness. The common problem is poor security of the watermark itself. At the same time, the frequency domain algorithm also has poor concealment. Based on quantum secure communication technology, this paper proposes a new frequency domain watermark embedding and extraction algorithm for secure communication. The algorithm, based on the principle of the BB84 protocol, uses the quantum key with true randomness generated by the mechanism for distributing the quantum key as the data source for preparing watermarks. Simultaneously, the quantum key is combined with the frequency domain wavelet transform watermarking algorithm to embed and extract the watermark. The results indicate that the proposed algorithm has high security, the same robustness as the classical frequency domain watermarking algorithm, and higher concealment than the frequency domain watermarking algorithm.

Keywords: wavelet transform; quantum key; digital watermarking; frequency domain algorithms

(Submitted on June 11, 2019; Revised on July 15, 2019; Accepted on August 10, 2019)

© 2019 Totem Publisher, Inc. All rights reserved.

1. Introduction

It is simple and fast to transmit multimedia digital information by computer networks. However, in the process of digital file transmission, there are certain security risks including malicious attacks and illegal copying of information, mainly due to the factors of network channel security and information self-security. By embedding invisible information in protected digital objects, digital watermarking technology proves the attribution of copyright and ensure the security of the information itself [1]. In addition, image processing technology is also widely used in medicine [2-3].

Based on domain differences, digital watermarking algorithms can be divided into spatial domain algorithms and frequency domain algorithms. The most typical spatial domain algorithm is the least significant bit algorithm LSB (least significant bits), which was proposed by L. F. Turner [4] in 1994. It implements watermarking embedding by modifying the least significant bits in the original data. It is simple to operate and conceal, but its resistance to attacks is poor. The frequency domain algorithm embeds a watermark by changing transform coefficients (such as color, texture, and frequency domain). For example, Cox et al. [5-6] proposed in 1995 to embed the watermark into the DCT (discrete cosine transform) domain of the original image, which has better resistance to compression and geometric attacks. However, the algorithm replaces the DCT coefficients in the original image with a pseudo-random sequence, which makes the algorithm have certain hidden dangers in security. In 1999, Ruanaida et al. [7] used discrete Fourier transform to control the amount of embedded watermarks and proposed a new algorithm for embedding digital watermarks into the DFT (discrete wavelet transform) domain of original images. It was proven that phase modulation is more suitable for robust watermarking from the perspective of communication theory, but Fourier transform cannot complete the time domain analysis of the signal, and the processing efficiency is low. Subsequently, Kunder et al. [8] proposed a method of embedding watermarks into the DWT (discrete wavelet transform) domain and solved many bottleneck problems of the Fourier algorithm by means of

* Corresponding author.
E-mail address: ccdxslj@126.com

translation, scaling, and other methods. Frequency domain algorithms generally have higher robustness [9].

At present, most methods have solved the robustness and concealment of the digital watermarking algorithm, but there are relatively few studies on how to ensure the security and correctness of communication information [10]. Many methods usually use pseudo-random number sequences as watermarks and try to ensure their security and robustness [10-11]. However, most digital watermarking algorithms, combined with spatial and frequency domains, use visual masks to select the embedding position. Due to the low complexity of the watermark and the unfavorable security communication, the pseudo-random number is used to control the embedding position of the watermark to enhance the confidentiality of the watermark [12]. In addition, there are also digital watermarking algorithms combined with quantum key in the airspace. Although the concealment is greatly improved compared to other spatial algorithms, the robustness is not improved and the airspace algorithm is basically the same [13].

Through the above analysis, this paper proposes a new watermark embedding and extraction algorithm based on wavelet transform fusion quantum key combined with quantum secure communication technology. Based on the principle of BB84 protocol, the algorithm is generated by a truly random quantum key through the mechanism of quantum key distribution as the information source for watermarking, which makes the watermark information extremely uncertain. At the same time, the quantum key is combined with the frequency domain wavelet transform watermarking algorithm to embed and extract the watermark. While having the self-security of quantum key and high robustness of the classical frequency domain watermarking algorithm, the proposed algorithm is also more concealed than other frequency domain watermarking algorithms.

2. Basic Concept

2.1. Preparation of Quantum Key

Based on the principle of the BB84 [14] protocol proposed by Bennett and Brassard, the quantum key with real randomness and security is generated through the mechanism for QKD.

The BB84 protocol consists of two links: Alice randomly generates and transmits a single photon sequence, and Bob randomly selects two different measurement bases $(\times, +)$ to receive a single photon and sends the randomly selected measurement base to Alice through the classical channel. Alice compares the base vectors to determine which bits of Bob are using the correct measurement base. Discarding the results of different measurement bases, both parties obtain the same common key [15].

2.2. Discrete Wavelet Transform

Wavelet analysis is a method of signal analysis that is becoming widely used. It has important applications in signal analysis, video image analysis, data, and compression [16].

A mathematical model for analyzing digital images using discrete wavelet transforms [17] is the following: given a digital image $A_{m\times n}$, form a data set for pixels in the image as shown in Equation (1):

$$A = \{a_{i,j}^0, 0 \le i \le m, 0 \le j \le n\} \tag{1}$$

There must be a function $f(x, y) \in L^2(R^2)$ to make $f(x, y) = \sum_{i,j} a_{i,j}^0 \phi_{i,j}(x, y)$. L-layer wavelet decomposition is obtained by discrete wavelet transform as shown in Equation (2):

$$f(x, y) = \sum_{i,j} a_{i,j}^0 \phi_{i,j}(x, y) = \sum_{i,j} a_{i,j}^L \phi_{i,j}^L(x, y) + \sum_{k,d} \sum_{i,j} c_{i,j}^{k,d} \varphi_{i,j}^{k,d}(x, y) \tag{2}$$

This is recorded as Equation (3) [16]:

$$\mathrm{DWT}\{a_{i,j}^0, 0 \le i \le m, 0 \le j \le n\} \Rightarrow \{\mathrm{a}_{i,j}^L, \mathrm{c}_{i,j}^{k,d}, 0 \le \mathrm{i} \le 2^{-k}m, 0 \le j \le 2^{-k}n, k = 1, 2, \cdots, L, d = 1, 2, 3\} \tag{3}$$

Where $a_{i,j}^L$ is the low frequency coefficient, $c_{i,j}^{k,d}$ is the high frequency coefficient in the different direction, and m and n are the number of rows and columns of the original host image, respectively.

2.3. Quantum-Key Matrix

The watermark image used in this paper is a quantum-key matrix QMatrix generated with quantum key as a data source. Each element in the quantum-key matrix QMatrix is a quantum key with a value of "1" or "0". As a watermark, the quantum-key matrix QMatrix is treated as a binary image output, as shown in Figure 1. The size of the quantum-key matrix QMatrix is determined by the size of the *HL* band coefficients after a single-level 2-D discrete wavelet transform of the original host image.

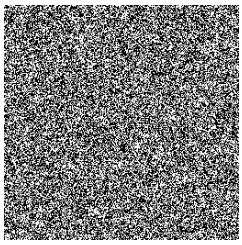


Figure 1. Quantum-key matrix QMatrix binary graph

There is a similar concept in reference [13], but compared with the key matrix in reference [13], the quantum key in the quantum-key matrix QMatrix proposed in this paper has higher utilization as watermark embedding.

2.4. Arnold Transformation

1) A method of $Arnold$ transformation: $Arnold$ transformation is proposed in the study on the traversal theory of $Arnold$. It is commonly known as cat face transformation, since it was originally used for cat mapping [18-19]. Imagine drawing a cat face image in the plane unit square, and transform it as shown in Equation (4):

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod\ 1 \tag{4}$$

In fact, for the position transformation on a 2-D plane, a type of transformation can be promoted by the $Arnold$ transformation to satisfy this "positional movement" requirement. Qi et al. [20] proved the following 2×2 matrix in Equation (5):

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \tag{5}$$

When its element satisfies $ad - bc = 1$, its transformation to the plane coordinates can be used as a scrambling transformation.

2) A generalized method of $Arnold$ transformation: In order to improve the flexibility and security of discrete $Arnold$ transformation for image scrambling, when the elements of the transform matrix are parameterized and satisfy certain constraints, the following generalized $Arnold$ transformation is obtained [21]:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod\ N \tag{6}$$

Where $a, b, c, d \in G$ and $gcd(ad - bc, N) = 1$.

With regard to Equation (6) for the generalized $Arnold$ transformation, if $a = 1, d = 1 + bc$, or $a = 1 + bc, d = 1$, $a = 1 + bc, d = 1$, or $b = 1, c = ad - 1$, or $b = ad - 1, c = 1$, a typical generalized transformation can be obtained [22].

Convert Equation (6) into a system of equations as shown in Equation (7):

$$\begin{aligned} x_{n+1} &= (ax_n + by_n)\ mod\ N \\ y_{n+1} &= (cx_n + dy_n)\ mod\ N \end{aligned} \tag{7}$$

3) An image encryption algorithm using generalized *Arnold* transformation: The discrete 2-D *Arnold* transform is mainly used to scramble image pixel positions, scramble adjacent pixels of an image, and make the pixel spatial distribution as uniform as possible. Qi [23] discussed the algorithm of high-dimensional transform for encrypting the pixel value of the image, which is given as Equation (8):

$$\begin{bmatrix} x_1' \\ x_2' \\ \vdots \\ x_n' \end{bmatrix} = \begin{bmatrix} a_{11} & a_{11} & \cdots & a_{11} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} mod\ 256 \tag{8}$$

Where $x_i(i = 1, 2, \cdots, n)$ is the pixel value of a row or column of the image before encryption. $x_i(i = 1, 2, \cdots, n)$ is the pixel value of a row or column of the image after encryption. The transform coefficient matrix $\mathbf{A} = (a_{ij})_{n\times n}$ satisfies the constraint condition $\gcd(\det \boldsymbol{A}, 256)$.

2.5. Image Gray Value Homogenization

The so-called image gray value is uninformative, that is, the pixel values of the original host image are distributed approximately in each region of the image uniformly, and the semantic sequence is transformed into a non-semantic sequence. An image scrambling algorithm, which is often used as an *Arnold* transform for the pretreatment of watermark images, is an operation that homogenizes the gray value of an image. The method of the image gray value homogenization in this paper is a high dimensional transformation.

3. Details of The Watermarking Algorithm

3.1. Watermark Embedding Algorithm

Input The original host image I and the quantum-key matrix QMatrix

Output The host image embedded with watermark I'

Step 1 Make the original host image I of the pixel value well-distributed once. Obtain the host image G.

Step 2 Transform G through single-level 2-D discrete wavelet transformation. Obtain LL, LH, HL, and HH, which are the frequency band coefficients of G.

Step 3 Insert each binary pixel of the quantum-key matrix QMatrix into HL, a frequency band coefficient of G, in order. Obtain HL_W, the frequency band coefficient of HL that embedded the watermark.

Step 4 Reconstruct LL, LH, HL_W, and HH through inverse discrete wavelet transform. Obtain the watermark host image G_W with the well-distributed pixel value.

Step 5 Inversely make the original host image G_W of the pixel value well-distributed once. Obtain the watermarked host image I'.

3.2. Watermark Extraction Algorithm

Input The watermarked host image I′ and the quantum-key matrix QMatrix

Output The extracted quantum-key matrix $QMatrix$

Step 1 Make the watermark host image I' of the pixel value well-distributed once. Obtain the image G' with the well-distributed pixel value.

Step 2 Transform G' through single-level 2-D discrete wavelet transformation. Obtain LL, LH, HL, and HH, which are the frequency band coefficients of G'.

Step 3 Collect the corresponding binary pixels sequentially from HL, a frequency band coefficient of G'. Form the

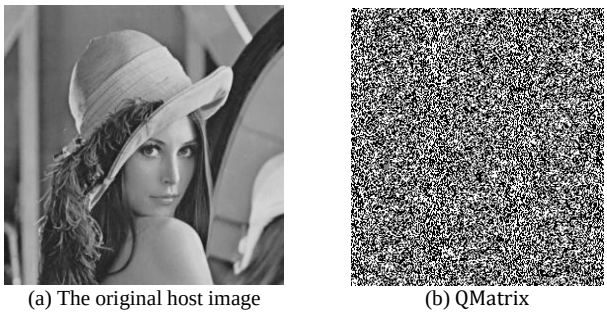
extracted quantum-key matrix QMatrix.

4. Analysis of Experiments and Results

4.1. Simulation Environment and Experimental Image

The algorithm program running software in this paper is $MATLAB2018b$.

The original host image is a 512×512 Lena grayscale image, as shown in Figure 2(a). The watermark image used in the simulation experiment is a quantum-key matrix QMatrix generated with a quantum key as a data source, as shown in Figure 2(b).



(a) The original host image (b) QMatrix

Figure 2. The original host image and the quantum-key matrix QMatrix

4.2. Algorithm Evaluation Index

The peak signal-to-noise ratio (PSNR) can be used to measure the concealment of watermarks [24].

The larger the PSNR, the better the image quality is kept. The smaller the impact of the watermark information on the carrier image, the better the concealment. Given an original image $f(x, y)$ of size $M \times N$ as a pixel and a processed image $g(x, y)$, the *PSNR* of the image $g(x, y)$ is defined as Equation (9):

$$PSNR = 10 \times \log_{10}(\frac{2^n - 1}{\sqrt{MSE}}) \tag{9}$$

The *MSE* is given by Equation (10):

$$MSE = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [g(x, y) - f(x, y)]^2 \tag{10}$$

The similarity coefficient (normal correlation, NC) is generally used to measure the robustness of the watermark.

Given an original carrier image $f(i, j)$ of size $M \times N$ and an image $g(x, y)$ embedded in the watermark, the similarity coefficient of the watermark is shown as Equation (11):

$$NC = \frac{\sum_{i=1}^{N-1} \sum_{j=1}^{M-1} f(i, j) g(x, y)}{\sqrt{\sum_{i=1}^{N-1} \sum_{j=1}^{M-1} f(i, j)} \sqrt{\sum_{i=1}^{N-1} \sum_{j=1}^{M-1} f(i, j) g(x, y)}} \tag{11}$$

As can be seen from the above formula, when the host image embedded in the watermark is attacked, the NC value of the original watermark and the extracted watermark is calculated. The closer the NC value is to 1, the more similar the extracted watermark is to the original watermark, and the stronger the robustness of the watermark.

4.3. Analysis of Results

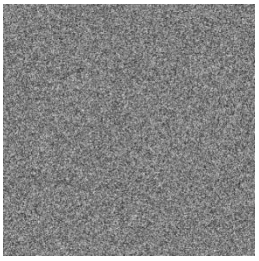
1) The watermark security: In this paper, the quantum key is embedded as a watermark into the frequency domain

coefficients of the host image, which makes the watermark information highly variable. Unless the correct key sequence is obtained, there is almost no possibility of forging watermark information, which greatly improves the security of the watermark.

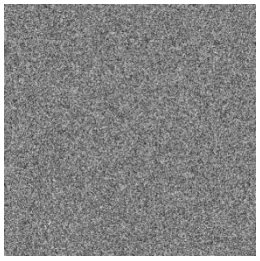
2) Results of the image pixel value homogenization: The uniformization of image pixel values involves making the watermark more uniformly distributed in the host image and improving the robustness of the algorithm to an extent.

As can be seen from the above Figure 3, when the pixel value is not homogenized, the gray value of the Lena image is concentrated between 25 and 225, and there are 5 peak regions. However, after the pixel value is homogenized, the gray value of the Lena image is almost uniformly distributed between 0 and 255.

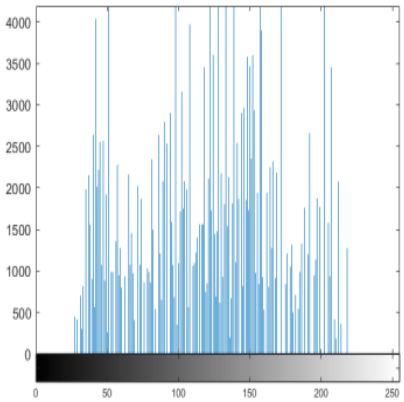
(a) The original Lena grayscale image



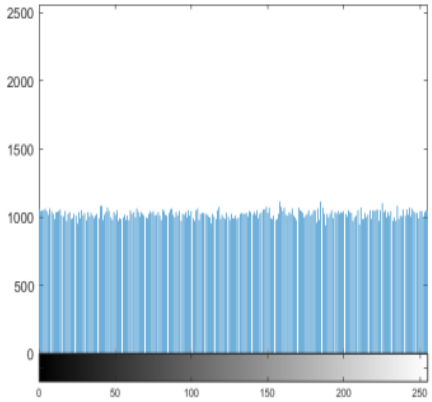
(b) Results of pixel value row-by-row homogenization



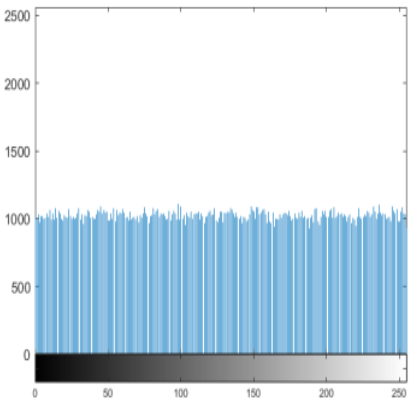
(c) Results of pixel value row-by-row and column-by-column homogenization



(d) Lena grayscale original image 1-D histogram



(e) 1-D histogram of the result of pixel value row by row homogenization

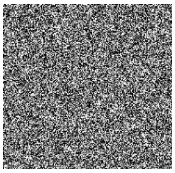


(f) 1-D histogram of the result of pixel value row by row and column-by-column homogenization

Figure 3. Results of the image pixel value homogenization

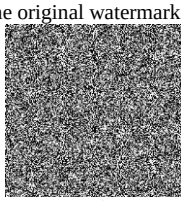
3) The concealment and robustness of algorithm: In addition to the Lena image, the Barbara, Peppers, and Baboon images were used as original host images for watermark concealment and robustness testing when performing algorithm concealment testing, as shown in Figure 4.

(a) Original host image, in order: Baboon, Barbara, Lena, and Peppers



(b) The original watermark image

(c) The host image after embedding watermark



(d) The extraction of watermark image

Figure 4. Results of the algorithm

When the PSNR of the watermark host image is greater than 30 dB, the human eye cannot perceive the watermark

information embedded in the image [25]. It can be seen from Table 1 that although the PSNR values of the algorithm are lower than those of the algorithm in reference [13], the algorithm has higher PSNR values than the frequency domain watermarking algorithm in reference [25].

At the same time, the algorithm of this paper, as a frequency domain watermarking algorithm, is as robust as the classical frequency domain watermarking algorithm.

Table 1. PSNR values after embedding watermarks in different host images in the algorithm

PSNR/dB	Baboon	Barbara	Lena	Peppers
The Algorithm	52.46	52.44	52.46	51.16
Reference [25]	-	42.02	42.55	42.17
Reference [13]	60.50	60.65	60.46	-

5. Conclusions

In view of the current poor security of most watermarking algorithms and the poor concealment of frequency domain watermarking algorithms, a new watermark embedding and extraction algorithm based on wavelet transform and quantum key is proposed. The algorithm, based on the principle of BB84 protocol, uses quantum key with true randomness generated by the mechanism of distributing quantum key as the data source for preparing watermarks. Simultaneously, the algorithm implements the first combination of quantum key and the frequency domain watermark algorithm. While having the high self-security of quantum key and the high robustness of the classical frequency domain watermark algorithm, the quantum key watermarking based on wavelet transform is also more concealed than other frequency domain watermark algorithms.

In addition, the pre-processing of the image gray value homogenization of the original host image, compared to the scrambling process adopted by most watermarking algorithms in the past, better enables the watermark information to be distributed uniformly in the host image.

Acknowledgements

This work is supported by the Science and Technology of Jilin Province Development Plan Project (No. 20170204023GX) and the Education Department of Jilin Province (No. JJKH20191201K, JJKH20191202KJ, and JJKH20170496KJ).

References

1. R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual Watermarks for Digital Images and Video," *Proceedings of the IEEE*, Vol. 87, No. 7, pp. 1108-1126, 1999
2. W. B. Li, H. W. Pan, P. Y. Li, X. Q. Xie, and Z. Q. Zhang, "A Medical Image Retrieval Method based on Texture Block Coding Tree," *Signal Processing*: *Image Communication*, Vol. 59, pp. 131-139, 2017
3. L. L. Gao, H. W. Pan, Q. Li, X. Q. Xie, Z. Q. Zhang, J. M. Han, et al., "Brain Medical Image Diagnosis based on Corners with Importance-Values," *BMC Bioinformatics*, Vol. 18, No. 1, pp. 505, 2017
4. R. G. Van-Schydel, A. Z. Tirkel, and C. F. Osborne, "A Digital Watermark," in *Proceedings of IEEE International Conference on Image Processing*, No. 2, pp. 86-90, 1994
5. I. Cox and J. Kilian, "Secure Spread Spectrum Watermarking for Images, Audio and Video," in *Proceedings of IEEE International Conference on Image Processing*, 1996
6. I. Cox, J. Kilian, and T. Leighton, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transaction on Image Processing*, Vol. 6, No. 12, pp. 1673-1687, 1997
7. J. Ruanaidh, W. Dowling, and F. Boland, "Phase Watermarking of Digital Image," in *Proceedings of IEEE International Conference on Image Processing*, 1999
8. D. Kudur and D. Hatzinakos, "A Robust Digital Image Watermarking Method using Wave Let-based Fusion," in *Proceedings of International Conference on Image Processing*, pp. 544-547, 1997
9. B. Zhao and G. H. Qing, "High Robustness Image Watermarking Algorithm," *Journal of Jilin University Engineering and Technology Edition*, Vol. 47, No. 1, pp. 249-254, 2017
10. Q. M. Zheng, X. Jin, G. M. Gu, and F. H. Wang, "A Digital Watermarking Algorithm based on Data Matrix," *Journal of China University of Petroleum*, Vol. 39, No. 1, pp. 188-193, 2015
11. P. Wang, H. Yao, and L. Li, "An Adaptive Digital Watermarking Algorithm Combining Spatial and DWT Domain," *Optics Precision Engineering*, Vol. 14, No. 6, pp. 1057-1062, 2006
12. K. Loukhaoukha, M. Nabti, and K. Zebbiche, "A Robust SVD-based Image Watermarking using a Multi-Objective Particle Swarm Optimization," *Opto Electronics Review*, Vol. 22, No. 1, pp. 45-54, 2014
13. J. N. Wu, S. G. Wang, D. Zhang, G. X. Liu, and Y. Zhou, "Binary Image Watermarking with True Randomness of Quantum Key," *Optical Precision Engineering*, Vol. 25, No. 11, pp. 2968-2974, 2017
14. C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proceedings of the*

IEEE International Conference on Computers, Systems, and Signal Processing, 1984
15. J. N. Wu, G. X. Liu, S. G. Wang, R. K. Wei, J. W. Han, and L. J. Song, "Quantum Cryptography Network Flow Control Strategy based on BB84 Protocol," *Journal of Jilin University: Science Edition*, Vol. 52, No. 1, pp. 76-80, 2014
16. H. J. He and J. S. Zhang, "Self-Embedding Watermarking Algorithm with Robustness Against Watermark Information Alterations," *Journal of Software*, Vol. 20, No. 2, pp. 437-450, 2009
17. X. D. Zhang, G. D. Lu, and J. Feng, "Fundamentals of Image Coding and Wavelet Compressing: Principles, Algorithms and Standards," Tsinghua University Press, pp. 235-270, Beijing, 2004
18. V. I. Arnold and A. Avez, "Ergodic Problems of Classical Mechanics," *Mathematical Physics Monograph Series*, W. A. Benjamin, New York Inc., 1968
19. D. X. Qi, "Fractal and its Application," Science Press, pp. 143- 145, Beijing, 1994
20. D. X. Qi, J. C. Zou, and X. Y. Han, "A New Class of Scrambling Transformation and Its Application in the Image Information Covering," *Science in China* (*Series E*), Vol. 43, No. 3, pp. 304- 312, 2000
21. C. M. Wu, "Improvement of Discrete Arnold Transform and Its Application in Image Scrambling Encryption," *Acta Physica Sinica*, Vol. 63, No. 9, 2014
22. Z. G. Ma and Y. S. Qiu, "An Image Cryptosystem based on General Cat Map," *Journal of China Institute of Communications*, Vol. 24, No. 2, pp. 51-57, 2003
23. D. X. Qi, "Matrix Transformation and its Applications to Image Hiding," *Journal of North China University of Technology*, Vol. 11, No. 1, pp. 24-28, 1999
24. Y. H. Wang, C. Q. Zhu, S. B. Su, and K. M. Ding, "An Authentication Method based on Perceptual Hashing and Watermarking for Remote Sensing Image," *Optics Precision Engineering*, Vol. 24, No. 10, pp. 640-648, 2016
25. Y. X. Gu and X. H. Ma, "Digital Watermarking Algorithm using Sparse Transform and Laplacian Pyramid," *Journal of Computer-Aided Design & Computer Graphics*, Vol. 30, No. 5, pp. 901-910, 2018

Jianan Wu is an associate professor in the School of College of Computer Science and Technology at Changchun and studies computer networking technology. Email address: 2962475@qq.com

Di Zhang is an undergraduate student in the School of College of Computer Science and Technology at Changchun University.

Huan Wang is an undergraduate student in the School of College of Computer Science and Technology at Changchun University.

Dexin Zhu is a lecturer in the School of College of Computer Science and Technology at Changchun University and studies computer applications and quantum communication.

Lijun Song is a professor in the School of Institute for Interdisciplinary Quantum Information Technology at Jilin Engineering Normal University and studies quantum information.