Medical Image Encryption Based on Stream Cipher Algorithm and Krill Group

Chu Zhao, Shoulin Yin, Hang Li, and Yang Sun
(Corresponding author: Shoulin Yin and Hang Li)

Software College, Shenyang Normal University
Shenyang 110034, China
(Email: 352720214@qq.com; lihangsoft@163.com)

(Received Oct. 13, 2018; Revised and Accepted Feb. 7, 2019; First Online June 15, 2019)

Abstract

The traditional image encryption algorithm is with low key sensitivity, low efficiency, low security, image scrambling and diffusion and high correlation. When using stream cipher to encrypt medical, the key sequence is too long and difficult to store and distribute. Therefore, this paper puts forward a new stream cipher method to encrypt medical image. First, medial image is coded as the text form. And then, we use the mutated character encoding table to encode text as the plaintext. Finally, we use krill group-based stream cipher algorithm to encrypt plaintext. By comparing the new method with the state-of-the-art encryption methods, experimental results show that the new method has greatly shortened the length of storing and distributing key sequence. The new algorithm has certain advantages in statistical performance, robust performance and key sensitivity, and also meets the requirements of image security and real-time performance.

Keywords: Character Encoding; Krill Group; Medical Image Encryption; Stream Cipher Algorithm

1 Introduction

Image encryption [12,20] is widely used in military reconnaissance and public security inspection. Medical image transmission in open network environment is vulnerable to eavesdropping attacks, so it is necessary to encrypt medical image before transmission [4–7,16,17]. However, how to balance the scrambling performance, security performance, robustness performance and the quality maintenance of decryption image is always difficult. Stream cipher [1,8] is a symmetric key encryption where the cryption key used to encrypt the binary image is randomly changed so that the cipher image produced is mathematically impossible to break. The advantage of using stream cipher is that the execution speed is higher when compared to block ciphers and have lower hardware complexity.

The stream cipher methods of medical image encryption include Martin image key system, rapid security sequence key, discrete cosine transform and stream cipher encryption methods, based on chaotic sequences and discrete wavelet transform partial encryption system, as well as classic RC4 stream cipher and Buddha sequence cipher system [2, 15]. These methods have a common disadvantage that the key sequence is too long.

Sudeepa [13] stated that maximum length sequence was applied for the RNS (Residue Number System) based additive stream cipher system. When the key sequence period was greater than the size of plain text, the system approaches secured one time pad cipher system. Imamura [9] analyzed the integrity of these schemes both in the standard INT-CTXT (integrity of ciphertext) notion and in the RUP (releasing unverified plaintext) setting called INT-RUP notion. Pu [14] presented a new algorithm by combining the true random sequences and the Tree Parity Machine (TPM), which was proven experimentally. Different from common method, true random sequences were proposed as dynamic inputs of TPM in this work compared to the pseudo-random sequences in the latest report. Xiao [19] proposed a new digital watermarking algorithm in encrypted image based on compressive sensing measurements and 2-D discrete wavelet transform (DWT). However, they cannot guarantee the privacy security.

In this paper, a stream cipher method similar to Vernam cipher employing an krill group [**?**] based approach to generate keys for encrypting medical images is proposed. This novel approach called stream cipher krill group image encryption (SCKGIE) algorithm is proposed to generate the keystream. The novelty in the approach is that an krill group approach is used to generate the keystream used for encryption based on the distribution of characters in the plain text denoting the image so that the keys in the keystream are encoded using a mutated character code table which would enable to increase the security of the system.

The advantage of the proposed stream cipher method

is that it would increase the security of the system by encoding the keys in the keystream and the characters in the plain text representing the encoded binary image using the mutated character code table. It reduces the number of keys to be stored and distributed when compared to that of Vernam cipher considered to be the perfect cipher. It overcomes the drawback of boolean cellular automaton method for image encryption and scan pattern method of image encryption in terms of the number of keys to be stored and distributed. The length of the key in SCKGIE algorithm is less when compared to DWT and chaos based image encryption method.

2 Algorithm Description

2.1 Encryption Process

First, the medical image is encoded as a text form using the characters in the ASCII code table (ASCII code values are from 32 to 126), and then it uses the mutated character code table to encode characters in the text, the result is as the plaintext. To encode the initial key sequence, the characters appearing in the plaintext use the mutated character encoding table to encode. Key sequences that do not appear in plaintext are encoded by using ASCII values. The same order of key sequences cannot be used to ensure security. The advantage of using a mutated character encoding table to encode characters in key sequences and text is that it can enhance the security of the system.

If the length of the plaintext sequence is greater than the length of the key sequence, the original key sequence is added with a predetermined value to generate the key sequence corresponding to the plaintext sequence to ensure the character length greater than the length of the key sequence.

The predetermined value is calculated by dividing the plaintext of the medical image into two parts as shown in Equation (1).

$$Indexvalue = int[length(P)/2]. \quad (1)$$

The plaintext sequence is partitioned into the size of the length of the key sequence, and the first corresponding key sequence is composed of the original key sequence. The key sequence corresponding to block i is obtained by adding the predetermined value to the key sequence corresponding to block $i-1$ as shown in Equation (2).

$$S_i = S_{i-1} + Indexvalue(i \geq 2). \quad (2)$$

Key value and plaintext value use XOR to obtain the ciphertext image.

2.2 Decryption Process

Decryption and encryption process use the same key sequence. The mutated character encoding table of contents and initial key sequence are sent to the receiver through the security channel, the receiver encodes the received initial key sequence through a simple table lookup operation. The character in key sequence that does not appear in character encode table is used ASCII to code. The receiver calculates the predetermined value based on the length of the ciphertext image. The corresponding key sequence is generated for the part of the ciphertext image exceeding the length of the key sequence. The key sequence and ciphertext image are subjected to XOR operation to obtain the plaintext, which is then decoded using the mutated character encoding table to get the text that represents the medical image, which is then decoded to obtain the original medical image.

2.3 Text Form for Medical Image

In order to encode the medical image as the text form represented by the characters in the ASCII table, each row of the 0,1 bit stream of the medical image is divided into several groups. There are only 95 characters in the ASCII table, so each group contains up to 94 bits. The grouping process continues until all the bit sequences are divided into one group and each group is coded separately. Characters from ! (ASCII code value is 33) to ∼ (ASCII code value is 126) are assigned a value of 1-94 respectively. To encode the 0, 1 bit stream of a medical image into text, the character value is established by an Equation (3).

$$Charactervalue = column(mod94). \quad (3)$$

If the value of the corresponding column position of the medical image is 0, replacing with character *space*. If the value of the corresponding column position of the medical image is 1, and the value of the column position mod94 is 0, replacing with character ∼. If the value of the corresponding column position of the medical image is 1, and the value of the column position mod94 is not 0, then replacing with the character value with corresponding character value. Strings are concatenated to form text to represent coded medical images.

2.4 Krill Swarm Algorithm

Krill swarm optimization algorithm is one of simulation swarm intelligence algorithms by simulating the action of krill, which was proposed by Alavi [3]. Each krill will be attracted or repelled by a certain range neighboring krill, so it can make local optimization. And the food center determined by fitness of krill would guide krill to make global optimization. In addition, the time interval needs to be adjusted, and the rest required parameters can be obtained from the research achievements of krill real ecological behavior. Meanwhile, krill swarm algorithm adopts Lagrangian model, therefore, the performance of krill swarm is superior to other optimization algorithms. The detailed processes of krill swarm algorithm are as follows:

1) Determine the Lagrangian model of krill swarm.
2) Motion induced by other krill individuals.
3) Foraging motion.
4) Stochastic diffusion process.
5) Updating krill positions.

3 Proposed Image Encryption

The objective function of the algorithm is to generate a key sequence, which satisfies the constraint that the energy value is greater than or equal to 80%. The energy value released by the krill is calculated by the counter, as Equation (4).

$$Energy(K_i) = \frac{count(C_j^i \in P)}{length(i)}. \quad (4)$$

Here K_i represents maximum number of krill, $i = 1, 2, \cdots$. C_j^i represents the key sequence length of $j-th$ character in the $i-th$ key sequence. P is the text of the medical image.

The krill path with the maximum energy value greater than or equal to the specified threshold is the solution of the problem. The key sequence is selected to encrypt the medical image. This allows the mutated character encoding table to encode most of the characters in the key sequence to increase the security of system.

Entropy coding has some properties related to cryptography. A character encoding tree is generated based on the statistical distribution of characters in text to encode characters in text and key sequences. The character encoding table is generated according to the character encoding tree. The purpose of establishing character encoding table is to encode the character appearing in text and key sequence through simple table lookup operation. Mutations in the character encoding tree can occur randomly at any node to enhance the security of the system. Research has shown that encryption should be combined with entropy coding using multiple statistical tables, and the benefit of using multiple statistical tables is that encryption can be done at a reasonably high security level.

The specific processes of the initial key sequence and text encoding are as follows:

1) Count the characters in the text and conduct Huffman encoding according to the possibility of character occurrence. The left branch of the tree is marked 0, and the right branch is marked 1.
2) The initial tree mutates in different non-leaf nodes by switching left and right branches. The character values in the character encoding tree are set up in decimal form.
3) For characters with the same value, the length of encoding is added to the character value to make the character value in the table correspond to the character value one to one.

4 Security of New Scheme

4.1 Key Space

The key sequence space that can be generated by 95 characters is given in Equation (5).

$$\sum_{i=1}^{95} \frac{95!}{(95-i)!} \approx 95!e. \quad (5)$$

In this size, it would take about 3×10^{125} years to decrypt the key, even though the world's fastest supercomputer, tianhe-1.

The character appeared in plaintext in key sequence will be replaced by the value in mutated character encoding table, which can increase the security of the system. Because character encoding table generation depends on the characters in plain text, the adversary needs to anticipate all possible sequences of character encoding trees. The Huffman tree encodes t characters, and the initial Huffman tree has $t-1$ non-leaf nodes, and the tree that may be different from the original tree through mutation has $2^{t-1}-1$. The key space generated by character encoding table is given by Theorem 1 and Theorem 2.

Theorem 1. *The number of possible character code tables is* 2.64×10^{176} *for images of size* $m \times n$ *where* $n \geq 94$.

Proof. Medical images are encoded as text. A character encoding tree is generated based on the occurrence probability of characters in text. The value of each character is generated by traversing the tree. The maximum possible number of characters is 95, the possible number of characters can be from 1 to 95, and the characters can appear in any order in the tree. Therefore, the possible number of initial character encoding trees is given in Equation (5). Each initial character encoding tree has $2t-1$ variants. Therefore, the maximum possible number of tables is:

$$\sum_{i=1}^{95} \frac{95!}{(95-i)!} \times 2^{i-1} \approx 2.64 \times 10^{176} \approx 2^{586}.$$

□

Theorem 2. *For images of size* $m \times n$, *where* $n < 94$ *the number of possible character code tables is:*

$$\sum_{i=1}^{n+1} \left(\frac{(n+1)!}{(n+1-i)!}\right) \times 2^{i-1}. \quad (6)$$

Proof. For images where the number of columns n is less than 94, the maximum number of characters will be $n+1$. Since the character code tree is generated based on the number of occurrence of the characters, the tree can have the characters of all possible orderings. That is out of the $n+1$ characters there can be all possible 1 or 2 or $\cdots$ or $n+1$ combination of all possible orderings without repetition. Thus the total number possible initial character

code tree is $\sum_{i=1}^{n+1}(\frac{(n+1)!}{(n+1-i)!})$. Each initial character code tree has 2^{t-1} tables as discussed above where $t-1$ are the number of inner nodes in a tree. Thus the total number of maximum possible tables is given in Equation (6). □

4.2 Histogram Analysis

Histogram describes the distribution of pixel points by drawing the number of pixels in each pixel level. In order to prevent information leakage, ciphertext image and plaintext image should have different statistical features. By analyzing the histogram of the ciphertext image and the original image, the number of pixels in each gray level is significantly different. The x-axis of the histogram represents the change in hue, and the y-axis represents the number of pixels in a particular hue. We chose two grayscale medical images with size 128×128. Figure 1,2 are the original images and histograms. Figures 3, 4 are the encrypted images and histograms. Figures 5, 6 are the decrypted images and histograms.

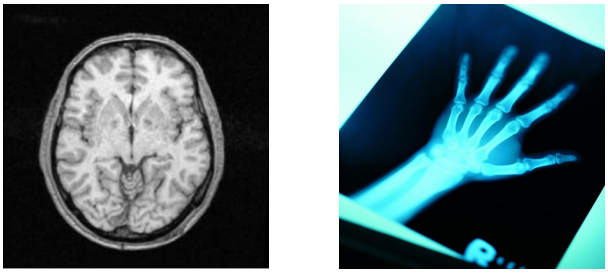

Figure 1: Original images

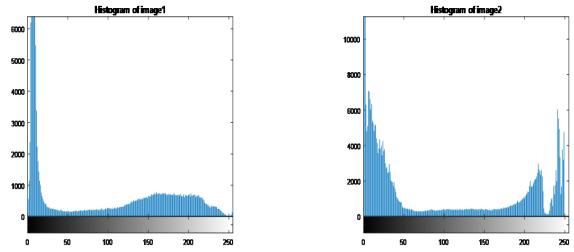

Figure 2: Histogram of original images

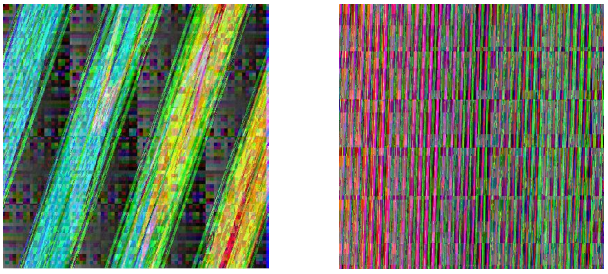

Figure 3: Encrypted images

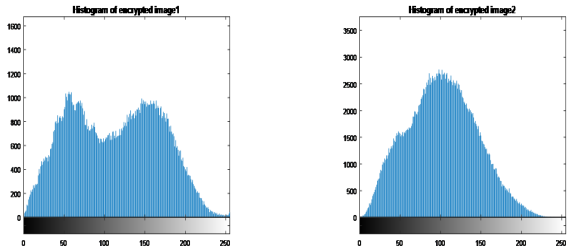

Figure 4: Histogram of encrypted images

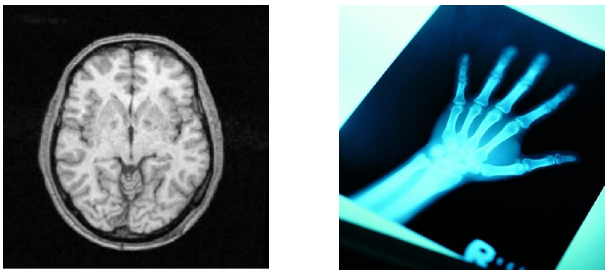

Figure 5: Decrypted images

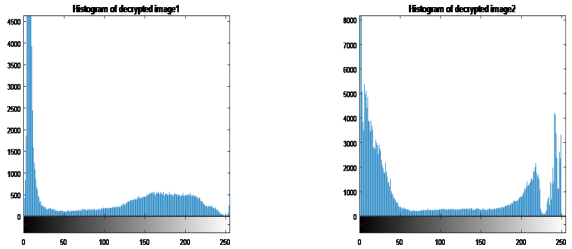

Figure 6: Histogram of decrypted images

It can be seen from the statistical histogram of ciphertext that all the peaks are almost uniformly scattered, and the plaintext does not have a statistical similarity with the plaintext. Therefore, using the new medical image encryption algorithm, ciphertext does not provide clues for the statistical attack.

4.3 Correlation Coefficient Analysis

The correlation coefficient between plaintext and ciphertext also shows their similarities. From the similarity between them, it can be inferred that the correlation coefficient between plaintext and ciphertext determines whether the algorithm has good diffusion and chaos characteristics, as well as resistance to statistical attacks.

If the correlation coefficient is between 0.5 and 1.0 or between -0.5 and -1.0, it means that there is a strong positive correlation or a strong negative correlation between them. If the correlation coefficient is between 0.0 and 0.5 or between -0.1 and -0.5, it means that there is a weak positive correlation or a weak negative correlation between them. Table 1 shows the correlation coefficients between plaintext and ciphertext, where key sequence lengths are 5 and 15, respectively.

Table 1: Correlation coefficient between plaintext and ciphertext

Image	Length=5	Length=15
Image1	0.0097	0.0074
Image2	0.0096	0.0073

It can be seen from Table 1 that there is a weak correlation between plaintext image and ciphertext image, which means that the medical image encryption algorithm based on SCKGIE encryption algorithm can resist statistical attacks.

5 Experiment Results and Analysis

In order to verify the effectiveness of proposed image encryption, We make comparison with RCM [10] and CCSC [11] conducted on MATLAB. We analyze differential attack, information entropy and robustness of new encryption method.

5.1 Differential Attack

Modifying the original plaintext image, high sensitivity is an important attribute in the image encryption algorithm. General experimental method is that it only modifies one pixel in the original image, and then observe the change of image to get quantitative relationship between ciphertext image and original image, if the original image has small changes that can cause larger cipher text image change, it argues that the encryption algorithm has good robustness for differential attack.

In order to test the effect of a pixel change on the entire ciphertext image, two famous measurement methods are adopted: UACI and NPCR. Setting two encrypted images, there is only one different pixel in the two images as I_1 and I_2, the corresponding gray values are $I_1(i,j)$ and $I_2(i,j)$. Define a bipolar array B, I_1 and I_2 have the same image size. $B(i,j)$ is determined by $I_1(i,j)$ and $I_2(i,j)$. If $I_1(i,j) = I_2(i,j)$, then $B(i,j) = 1$. Otherwise, $B(i,j) = 0$. So

$$NPCR = \frac{\sum_{i,j} B(i,j)}{W \times H} \times 100\%.$$

Where W and H represent the width and height of the encrypted image, and NPCR measures the ratio of the number of pixels with different pixel values between the two images to the total pixel values.

$$UACI = \frac{1}{W \times H}[\sum_{ij} \frac{I_1(i,j) - I_2(i,j)}{255}] \times 100\%.$$

UACI measures the average strength of the two images, and tests the medical images by modifying one pixel. The results are shown in Table 2. From the UACI and NPCR values in the table, it can be seen that the encryption algorithm in this paper has a great sensitivity to the small difference of the original image.

Table 2: NPCR, UACI comparison with different methods

Image	RCM	CCSC	Proposed algorithm
Image1(NPCR)	94.4	95.6	99.2
Image2(NPCR)	93.2	94.7	98.5
Image1(UACI)	33.7	32.1	27.6
Image2(UACI)	33.1	31.9	28.7

Table 3: Information entropy comparison

Method	Image1	Image2
RCM	0.715	0.726
CCSC	0.727	0.728
Proposed method	0.834	0.828

5.2 Information Entropy

Information entropy denotes the degree of uncertainty system, and it is used to describe the uncertainty of image information. The information entropy can be used to analyze the distribution of gray value in the image. Let $P(m_i)$ be proportion of pixel with gray value m_i in image and $\sum_{i=0}^{255} P(m_i) = 1$. The information entropy of the pixel is defined as:

$$H(m) = -\sum_{i=0}^{255} P(m_i \log_2 P(m_i)).$$

The comparison results are as shown in Table 3.

5.3 Robustness Analysis

Since noise is inevitably introduced in the encryption process, the robustness of the algorithm in this paper is tested, and PSNR value is used to judge the quality of the encrypted image as defined below:

$$PSNR = 10log\frac{WH255^2}{\sum_{i=0}^{H-1}\sum_{j=0}^{W-1}(f_1(i,j) - f_2(i,j))^2}$$

Where $f_1(i,j)$ is the pixel value of the original image pixel (i,j), and $f_2(i,j)$ represents the pixel value of the decryption terminal pixel (i,j). Obviously, the higher the PSNR value is, the better the performance of the encryption algorithm is. Table 4 is the PSNR value of Image1 and Image2. Obviously, the chaotic encryption algorithm in the transform domain has good robustness.

Table 4: PSNR comparison with different methods

Image	RCM	CCSC	Proposed method
Image1	52.18	53.75	59.76
Image2	52.38	54.55	58.59

6 Conclusion

This paper proposes a stream cipher based on krill group algorithm method, this new method is compared with both the sequence code method, which greatly reduces the need of storing and distributing the key sequence length, solves the key storage and distribution problem. At the same time, it uses the mutated character encoding table to encode the character in key and plaintext, which makes it hard for the adversary to break character coding table, this improves the security of system. And the experimental results show that the system has a high security degree by analyzing differential attack, information entropy and robustness.

7 Acknowledgments

This study was supported by the Natural Science Fund Project Guidance Plan in Liaoning Province of China (No. 20180520024).

References

[1] A. Belmeguenai, Z. Ahmida, S. Ouchtati, *et al.*, "A novel approach based on stream cipher for selective speech encryption," *International Journal of Speech Technology*, vol. 20, no. 9, pp. 1-14, 2017.

[2] X. Chai, Z. Gan, Y. Chen, *et al.*, "A visually secure image encryption scheme based on compressive sensing," *Signal Processing*, vol. 134, pp. 35-51, 2017.

[3] A. H. Gandomi, A. H. Alavi, "Krill herd: A new bio-inspired optimization algorithm," *Communications in Nonlinear Science & Numerical Simulations*, vol. 17, no. 12, pp. 4831-4845, 2012.

[4] L. C. Huang, M. S. Hwang, L. Y. Tseng, "Reversible and high-capacity data hiding in high quality medical images," *KSII Transactions on Internet and Information Systems*, vol. 7, no. 1, pp. 132–148, 2013.

[5] L. C. Huang, M. S. Hwang, and L. Y. Tseng, "Reversible data hiding for medical images in cloud computing environments based on chaotic Henon map," *Journal of Electronic Science and Technology*, vol. 11, no. 2, pp. 230–236, 2013.

[6] L. C. Huang, L. Y. Tseng, M. S. Hwang, "The study on data hiding in medical images", *International Journal of Network Security*, vol. 14, no. 6, pp. 301–309, 2012.

[7] L. C. Huang, L. Y. Tseng, M. S. Hwang, "A reversible data hiding method by histogram shifting in high quality medical images", *Journal of Systems and Software*, vol. 86, no. 3, pp. 716–727, Mar. 2013.

[8] T. Hwang, P. Gope, "Robust stream-cipher mode of authenticated encryption for secure communication in wireless sensor network," *Security & Communication Networks*, vol. 9, no. 7, pp. 667-679, 2016.

[9] K. Imamura, K. Minematsu, T. Iwata, "Integrity analysis of authenticated encryption based on stream ciphers," *International Journal of Information Security*, no. 3, pp. 1-19, 2016.

[10] M. Kumari, S. Gupta, "A novel image encryption scheme based on intertwining chaotic maps and RC4 stream cipher," *3d Research*, vol. 9, no. 1, pp. 10, 2018.

[11] Z. Lin, S. Yu, X. Feng, *et al.*, "Cryptanalysis of a chaotic stream cipher and its improved scheme," *International Journal of Bifurcation & Chaos*, vol. 28, no. 7, 2018.

[12] J. Liu, S. L. Yin, H. Li and L. Teng, "A density-based clustering method for K-anonymity privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 1, pp. 12-18, Jan. 2017.

[13] K. B. Sudeepa, G. Aithal, "Generation of maximum length non-binary key sequence and its application for stream cipher based on residue number system," *Journal of Computational Science*, vol. 21, pp. 379-386, 2016.

[14] X. Pu, X. J. Tian, J. Zhang, *et al.*, "Chaotic multimedia stream cipher scheme based on true random sequence combined with tree parity machine," *Multimedia Tools & Applications*, vol. 76, no. 19, pp. 1-15, 2016.

[15] L. Teng, H. Li, S. Yin, "A multi-keyword search algorithm based on polynomial function and safety inner-product method in secure cloud environment," *International Journal of Network Security*, vol. 8, no. 2, pp. 413-422, 2017.

[16] M. H. Tsai, S. F. Chiou, and M. S. Hwang, "A progressive image transmission method for 2D-GE image based on context feature with different thresholds", *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 2, pp. 379–386, Feb. 2009.

[17] M. H. Tsai, S. F. Chiou and M. S. Hwang, "A simple method for detecting protein spots in 2D-GE images using image contrast", *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 12, pp. 4617–4626, Dec. 2009.

[18] G. G. Wang, A. H. Gandomi, A. H. Alavi, "A chaotic particle-swarm krill herd algorithm for global numerical optimization," *Kybernetes*, vol. 42, no. 6, pp. 962-978, 2013.

[19] D. Xiao, Y. Chang, T. Xiang, *et al.*, "A watermarking algorithm in encrypted image based on compressive sensing with high quality image reconstruction and watermark performance," *Multimedia Tools & Applications*, vol. 76, no. 7, pp. 1-32, 2017.

[20] S. L. Yin and J. Liu, "A K-means approach for map-reduce model and social network privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 6, pp. 1215-1221, Nov. 2016.

Biography

Chu Zhao received the M.Eng. degree from Shenyang Normal University, Shenyang, Liaoning province, China in 2011. Her research interests include Network Security and Data Mining. Email:910675024@qq.com.

Shoulin Yin received the B.Eng. and M.Eng. degree from Shenyang Normal University, Shenyang, Liaoning province, China in 2016 and 2013 respectively. Now, he is a doctor in Harbin Institute of Technology. His research interests include Network Security, image processing. Email:ysl352720214@163.com.

Hang Li obtained his Ph.D. degree in Information Science and Engineering from Northeastern University. Hang Li is a full professor of the Kexin software college at Shenyang Normal University. He is also a master's supervisor. He has research interests in wireless networks, mobile computing, cloud computing, social networks, network security and quantum cryptography. Prof. Li had published more than 30 international journal and international conference papers on the above research fields. Email:lihangsoft@163.com.

Yang Sun obtained his master degree in Information Science and Engineering from Northeastern University. Yang Sun is a full associate professor of the Kexin software college at Shenyang Normal University. He is also a department head of network engineering. He has research interests in wireless networks, mobile computing, cloud computing, social networks and network security. Yang Sun had published more than 15 international journal and conference papers on the above research fields.