An Improved Image Encryption Algorithm Based on Chaotic Mapping and Discrete Wavelet Transform Domain

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

Software College, Shenyang Normal University
Shenyang 110034, China
(Email: ysl352720214@163.com)

(Received Aug. 28, 2018; Revised and Accepted Nov. 22, 2018; First Online Mar. 9, 2019)

Abstract

The traditional chaotic image encryption algorithm has some problems, such as low security, image scrambling and diffusion (cannot resist the Chosen-plaintext attack), low efficiency and low key sensitivity and high correlation. Therefore, an improved image encryption algorithm based on chaotic mapping and discrete wavelet transform domain is proposed in this paper. First of all, the image scrambling only changes the position of each pixel, but cannot change the pixel value. Its statistical features do not change. Therefore, image encryption algorithm widely adopts the combination of scrambling and grayscale diffusion, through multiple rounds of encryption, to enhance the image confusion and diffusion characteristics. Then, the image is processed by wavelet transform. Finally, the image is mapped by chaos. Experimental results show that the 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: Chaotic Mapping; Discrete Wavelet Transform; Grayscale Diffusion; Image Encryption

1 Introduction

Image encryption is widely used in military reconnaissance and public security inspection. The security and efficiency of image encryption have been studied widely. In many special application scenarios such as confidential video meetings and military, the image's security requirements are very high. So it is very important for the image encryption [3, 10]. However, how to balance the scrambling performance, security performance, robustness performance and the quality maintenance of decryption image is always difficult. In recent years, many researchers had applied chaotic systems to cryptosystems which has obtained the better encryption effect. The chaos system is very sensitive to the initial conditions. As long as the initial conditions are slightly changed, the results will be greatly different, which is very suitable for plaintext scrambling. The chaotic system is characterized by randomness, sensitivity to initial values and broadband power spectral density of similar noise. The traditional encryption algorithm (such as AES, DES, *etc.*) is inefficient and difficult to meet the real-time requirements [4,9,20]. The chaotic system has the characteristics of ergodicity, pseudo-randomness and initial value sensitivity and the chaotic cipher has natural advantages in the large data volume processing. Therefore, the chaotic cipher is adopted, which becomes the hot spots for fast image encryption algorithm.

Image encryption technology currently has the following three types:

1) Based on image pixel scrambling [13, 15]. The represented approaches are Arnold transform and the magic square transform. These encryption algorithms directly act on the pixels of the image. According to some linear transformation, it changes the position of the pixel to achieve the purpose of image encryption.

2) Based on modern cryptography [18, 21]. Both commercially and militarily widely use the modern cryptography. In technically, image information as a data format is fully capable of being encrypted by modern cryptography including symmetric cryptography and asymmetric cryptography. In practical applications, symmetric cryptography is mainly used to encrypt commercial or military information, it is often used to encrypt short messages.

3) Based on chaotic technique [5, 12]. due to the development of the chaotic dynamics in recent years, people gradually realize that the chaos can be used as a new password system, which can be used to encrypt text voice and image data. Chaos is used as a new

cryptosystem which is determined by the properties of chaotic system itself.

For image encryption, there are some discoveries. Mccarthy [11] discussed that an identity-based encryption scheme enables the efficient distribution of keys in a multi-user system. Such schemes are particularly attractive in resource constrained environments where critical resources such as processing power, memory and bandwidth are severely limited. This research examines the first pragmatic lattice-based IBE scheme and brings it into the realm of practicality for use on small devices. Assad [2] proposed a new fast, simple and robust chaos-based cryptosystem structure and analyzed its performances. The cryptosystem used a diffusion layer followed by a bit-permutation layer, instead of byte-permutation, to shuffle the positions of the image pixels. Moreover, the permutation layer was achieved by a new proposed formulation of the 2D cat map that allowed an efficient implementation, measured by the time complexity, in terms of arithmetic and logic operations and also, in terms of clock cycles, of the key-dependent permutation process in comparison with the standard one. Hariyanto [7] presented arnold's cat map algorithm in digital image encryption. Su [14] proposed an image encryption scheme based on chaos system combining with DNA coding and information entropy, in which chaos system and DNA operation were used to perform substitution and entropy driven chaos system was used to perform permutation. However, two vulnerabilities were found and presented in this paper, which made the encryption fail under chosen-plaintext attack. A complete chosen-plaintext attack algorithm was given to rebuild chaos systems' outputs and recover plain image and its efficiency was demonstrated by analysis and experiments. Ye [19] proposed an efficient symmetric image encryption algorithm based on an intertwining logistic map.

So this paper propose an improved image encryption algorithm based on chaotic mapping and discrete wavelet transform domain. The rest of the paper is organized as follows. Section 2 introduces the improved elliptic curve cryptography. New medical image encryption is illustrated in Section 3. Section 4 outlines the experiments. Section 5 finally concludes the paper.

2 Chaotic Encryption Algorithm

Baker mapping [6, 8, 16] is one of chaotic mapping processing two-dimensional mapping for unit plane. When returning the spatial domain, the Baker mapping can obtain a large degree of randomness. Baker mapping is defined as follows.

$$Baker(x,y) = \begin{cases} (2x, y/2) & 0 \le x \le 0.5 \\ (2x-1, y/2+0.5) & 0.5 \le x \le 10. \end{cases}$$

Discrete Baker mapping can be denoted as $Baker(n_1, n_2, \cdots, n_k)$. Where $(n_1, n_2, \cdots, n_k)$ is integer sequence. Each integer divides N, $N_i = n_1 + \cdots + n_i$. For the pixel in position of (r, s), $N_i \le r \le N_i + n_i$, $0 \le s < N$, so the Baker mapping of this position is:

$$\begin{aligned} Baker_{(n_1,n_2,\cdots,n_k)}(r,s) = & [\frac{N}{n_i}(r - N_i) + s \bmod (\frac{N}{n_i}) \\ & + \frac{n_i}{N}(s - s \bmod (\frac{N}{n_i})) + N_i]. \end{aligned}$$

First, one square matrix $N \times N$ is divided into k vertical rectangle (height is N, width is n_i). Then each vertical rectangle is segmented as n_i sub-patches with N points. Map each sub-block to a row of pixels through the column-column.

3 Proposed Image Encryption

Digital image can be described in the spatial domain by pixel location and grey value information. The digital image encryptions are based on the combination of the two factors. Conventional image encryption algorithm is divided into pixel scrambling and gray diffusion. Image scrambling only changes the position of each pixel, cannot change the pixel values, its statistical characteristics do not change. If only using gray diffusion, the tiny change of ciphertext pixel is difficult to influence all ciphertext pixels, therefore, we combine scrambling and gray diffusion in image encryption algorithm, through several rounds of encryption, it enhances the image confusion and diffusion properties.

3.1 Image Pixel Scrambling

The scrambling of digital images is a commonly used algorithm for dealing with image security problems. Image scrambling is to change the order of pixels of the original image, so that the third party cannot distinguish image information. Using chaotic system to achieve image scrambling, the methods can be divided into two categories: a) Using chaotic transformation as a scrambling transformation matrix, this method is simple and fast, but the scrambled image has strong texture features; b) Using the chaotic system to generate sequences row-by-row of the images. The texture features are not obvious and the randomness is good. However, the multi-round iteration of chaotic systems is expensive and slow. Since Arnold is the most widely used chaotic transform, this paper uses Logistic map to generate image scrambling method by combining control parameters and Arnold mapping, which improves the scrambling algorithm.

The Arnold mapping expression is shown in following equation.

$$[x_{i+1}\ y_{i+1}]^T = [(1,q)(p,pq+1)]^T [x_i\ y_i]^T (\mathrm{mod} N).$$

Where p and q are the control parameters of the chaotic equation. (x, y) is the image pixel position; N is the side length of the image. The control parameters in the equation are generated by the Logistic map and the Logistic

map is as shown:

$$x_1(n+1) = \lambda x_1(n)[1 - x_1(n)].$$

To achieve chaotic state, let $3 \leq \lambda \leq 3.2$ (the encrypter can select floating-point type data within this range). The specific process of generating control parameter is as follows:

- Iterate the Logistic map 200 times to eliminate the impact of the initial value.
- Generate a scrambling control parameter by above equation, where $\lfloor x \rfloor$ represents the largest integer not greater than x.

$$p = \lfloor x_1(k_1) \times 2^{12} \rfloor \bmod N$$
$$q = \lfloor x_1(k_1) \times 2^{10} \rfloor \bmod N.$$

  Where $x_1(k_1)$ is the state value after the equation iterates k_1 times and N is the edge length of the image.

The position of the $(0, 0)$ pixel in the image remains unchanged regardless of the number of rounds of scrambling. In order to prevent the cracker from analyzing the ciphertext with $(0, 0)$ as the breakthrough point, it chooses to exchange $(0, 0)$ with the scrambled (m, n) point to reduce the risk of ciphertext being cracked.

3.2 Image Gray Diffusion

The using of pixel scrambling alone cannot prevent the decipher from analyzing through plaintext attacks. Decipherers often choose specific points and study their position changes during the scrambling process to find the law of transformation. The security is not high only using scrambling method. The gray-scale diffusion algorithm changes the gray value of each pixel, which avoids the above-mentioned plaintext attack and further improves the confidentiality.

The diffusion algorithm is generally performed by using a modulo operation and an addition operation. The modulo algorithm can make the calculation result within a normal value interval and the addition operation can correlate the gray values of different pixels with each other to increase the mutual influence between the pixels. On the other hand, the distribution of the gray value of each pixel is made more uniform and the texture features of the scrambled image are eliminated. In order to enhance the diffusion effect, referring to the pseudo-randomness and ergodicity of chaotic phenomena, this paper introduces the Kent chaotic factor into the algorithm. The following equation is a diffusion formula based on modulo operations, addition operations and chaotic sequences.

$$c(k) = S(k) \oplus |[P(k) + S(k)] \bmod M| \oplus C(k-1).$$

Where $P(k)$ and $C(k)$ are the current plaintext value and ciphertext value, respectively. $C(k-1)$ is the previous ciphertext value, where $C(0)$ is defined as a constant (here set to 100). $M = 256$ is the gray level. $S(k)$ is the control parameter. It is different from the control parameter generation method of pixel scrambling, $S(k)$ is obtained by Kent mapping, which is also a commonly used chaotic map. The Kent mapping definition is as shown in:

$$x_2(n+1) = \begin{cases} x_2(n)/\mu & \text{if } 0 < x \leq \mu \\ (1 - x_2(n))/(1 - \mu) & \text{if } \mu < x \leq 1. \end{cases}$$

In the above equation, taking $0 < \mu < 1$ (the encrypter can select the floating point type data within this range). The specific process of controlling parameter generation is as follows:

- Iterate the Kent mapping 200 times to eliminate the impact of the initial value.
- The scramble control parameter is generated by above equation.

$$S(k) = \lfloor x_2(k_2) 2^{16} \rfloor \bmod M.$$

Where $x_2(k_2)$ is the state value after iterating k_2 in Kent mapping.

3.3 Discrete Wavelet Transform

For a $N \times N$ image, we define the discrete wavelet transform(DCT) as:

$$C(u,v) = \frac{2}{N}\alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y) \cos[u\pi\frac{x}{N} + \frac{u\pi}{2N}]\cos[v\pi\frac{y}{N} + \frac{v\pi}{2N}].$$

In here, $f(x, y)$ is the pixel density of position (x, y), $C(u, v)$ denotes the DCT coefficient. In this paper, we define $\alpha(u) = \alpha(v) = 1$.

The DCT decomposes the original signal into a set of integral coefficients. The lifting method is an effective method for DCT operation and the lifting scheme generally uses roundoff function, defined as rof.

$$d_i^{l+1} = s_{2i+1}^l - rof(0.5625(s_{2i}^l + s_{2i+2}^l) - 0.0625(s_{2i-2}^l + s_{2i+4}^l)).$$
$$s_i^{l+1} = s_{2i}^l + rof(0.25(d_{i-1}^{l+1} + d_i^{l+1})).$$

Decomposed signal in $l + 1$th is s_i^l. When the time is i, the input is d_i^{l+1} along with high frequency output. First, the image is processed by DWT. After wavelet decomposition, image is divided into four blocks, that is, a low-frequency block and three high-frequency blocks, they are encrypted by four different keys to improve security than other methods.

4 Experiment Results and Analysis

In order to verify the effectiveness of proposed image encryption, we select two images (512×512 size) as input

Table 1: PSNR comparison with different methods

Image	DCC	DNAE	C-ECE	New
Lena	51.28	55.37	55.86	56.97
Pepper	51.18	52.17	53.84	57.41

image conducted on MATLAB. Figures 1 and 2 are the original images. We also make comparison with DCC [1], DNAE [22] and C-ECE (Chaotic Systems and Elliptic Curve ElGamal Scheme) [17].


Figure 1: Original images

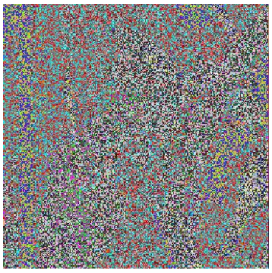
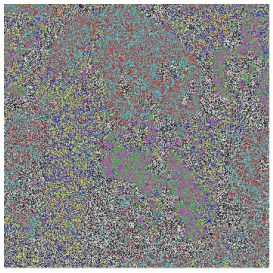

Figure 2: Encryption result with proposed method

4.1 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 1 is the PSNR value of Lena and Pepper. Obviously, the chaotic encryption algorithm in the transform domain has good robustness.

4.2 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 the Lena, Pepper image 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	DCC	DNAE	C-ECE	New
Lena(NPCR)	93.2	95.4	96.7	98.1
Pepper(NPCR)	95.8	96.1	97.1	97.9
Lena(UACI)	32.5	31.6	30.9	28.7
Pepper(UACI)	31.9	30.7	30.1	29.2

4.3 Performance of Proposed Scheme

The algorithm has strong ability of resisting differential attack, encrypting 512×512 image only needs 0.041s for Lena. And we make comparison with other two methods obtaining Table 3. The comparison result shows that the method introduced in this paper guarantees the security of encryption, while the encryption speed is fast and the real-time performance is strong.

4.4 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

Table 3: Performance comparison with different methods

Image	DCC	DNAE	C-ECE	New
Lena	0.081	0.078	0.069	0.041
Pepper	0.084	0.067	0.062	0.052

Table 4: Information entropy comparison

Method	Lena	Pepper
DCC	0.675	0.712
DNAE	0.708	0.721
C-ECE	0.735	0.784
New	0.957	0.926

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 4.

4.5 Key Sensitivity Analysis

Since the precision of floating point data can reach 10^{15}, the key space of the algorithm is $2 \times N^2 \times 10^{59}$, so it can be seen that the algorithm has sufficient key space. In the decryption part, we change the key, the decryption of image is fail. So the experiment shows that the algorithm has good confidentiality and the slight difference of the key will lead to the failure of image decryption as shown figure 3 in terms of Lena.

Figure 3: Left: Correct decryption result; Right: Wrong decryption result

Figure 4 is the histogram of original Lena and encrypted Lena. Figure 5 is the histogram of original Pepper and encrypted Pepper. It can be seen from the comparison of the two gray histogram images that the encrypted image pixels are uniformly distributed in the gray range of 0 255, which well covers the statistical properties of the original image and meets the expected requirements.

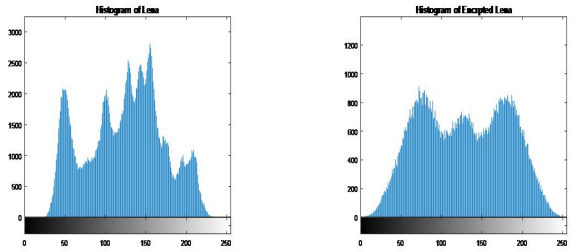

Figure 4: Left: Histogram of original Lena; Right: Histogram of encrypted Lena

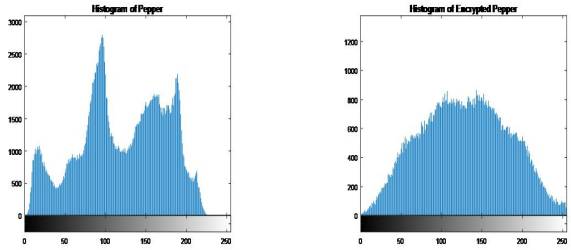

Figure 5: Left: Histogram of original Pepper; Right: Histogram of encrypted Pepper

5 Conclusion

In this paper, aiming to solve the weak performance of chaotic encryption algorithm in space domain, we propose an improved image encryption algorithm based on chaotic mapping and discrete wavelet transform domain. First, image encryption algorithm widely adopts the combination of scrambling and grayscale diffusion, through multiple rounds of encryption, to enhance the image confusion and diffusion characteristics. Then, the image is processed by wavelet transform. Finally, the image is mapped by chaos. The experimental analysis shows that the algorithm has sufficient key space and strong key sensitivity and can effectively resist the exhaustive analysis attack. After encryption, the pixel gray distribution is uniform and the correlation between adjacent pixel points is weak, which can well resist the difference attack; In the current size of the image, encryption time is short, real-time performance is strong, which can meet the need of real-time encryption and decryption.

6 Acknowledgments

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

References

[1] S. E. Assad, M. Farajallah, "A new chaos-based image encryption system," *Signal Processing Image Communication*, vol. 41, pp. 144-157, 2016.

[2] S. E. Assad, M. Farajallah, "A new chaos-based image encryption system," *Signal Processing Image Communication*, vol. 41, pp. 144-157, 2016.
[3] C. C. Chang, M. S. Hwang, T. S. Chen, "A new encryption algorithm for image cryptosystems", *Journal of Systems and Software*, vol. 58, no. 2, pp. 83–91, Sep. 2001.
[4] S. Dey and R. Ghosh, "A review of cryptographic properties of S-Boxes with generation and analysis of Crypto secure S-Boxes," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 49-73, 2018.
[5] S. Farwa, T. Shah, N. Muhammad, *et al.*, "An image encryption technique based on chaotic s-box and arnold transform," *International Journal of Advanced Computer Science & Applications*, vol. 8, no. 6, 2017.
[6] C. Fu, Z. K. Wen, Z. L. Zhu, *et al.*, "A security improved image encryption scheme based on chaotic Baker map and hyperchaotic Lorenz system," *International Journal of Computational Science & Engineering*, vol. 12, no. 2, 2016.
[7] E. Hariyanto, R. Rahim, "Arnold's cat map algorithm in digital image encryption," *International Journal of Science & Research*, vol. 5, no. 10, pp. 6-391, 2016.
[8] 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.
[9] 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.
[10] L. Liu, Z. Cao, "Analysis of two confidentiality-preserving image search schemes based on additive homomorphic encryption," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 1–5, 2016.
[11] S. Mccarthy, N. Smyth, E. O. Sullivan, "A practical implementation of identity-based encryption over NTRU lattices," in *IMA International Conference on Cryptography and Coding*, pp. 227-246, 2017.
[12] S. Rajendran, M. Doraipandian, "Chaotic map based random image steganography using LSB technique," *International Journal of Network Security*, vol. 19, no. 4, pp. 593-598, 2017.
[13] H. Sharma, N. Khatri, "An image encryption scheme using chaotic sequence for pixel scrambling and DFrFT," in *Proceedings of First International Conference on Smart System, Innovations and Computing*, pp. 487-493, 2018.
[14] X. Su, W. Li, H. Hu, "Cryptanalysis of a chaos-based image encryption scheme combining DNA coding and entropy," *Multimedia Tools & Applications*, vol. 76, no. 12, pp. 1-13, 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] L. Teng, H. Li, J. Liu and S. Yin, "An efficient and secure cipher-text retrieval scheme based on mixed homomorphic encryption and multi-attribute sorting method," *International Journal of Network Security*, vol. 20, no. 5, pp. 872-878, 2018.
[17] J. Wu, X. Liao, B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," *Signal Processing*, vol. 141, 2017.
[18] S. Yin, L. Teng, J. Liu, "Distributed searchable asymmetric encryption," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 4, no. 3, pp. 684-694, 2016.
[19] G. Ye, X. Huang, "An efficient symmetric image encryption algorithm based on an intertwining logistic map," *Neurocomputing*, vol. 251, pp. 45-53, 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.
[21] Q. Zhang, L. T. Yang, X. Liu, Z. Chen and P. Li, "A tucker deep computation model for mobile multimedia feature learning," *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 13, no. 3, pp. 1-39:18, 2017.
[22] P. Zhen, G. Zhao, L. Min, *et al.*, "Chaos-based image encryption scheme combining DNA coding and entropy," *Multimedia Tools & Applications*, vol. 75, no. 11, pp. 6303-6319, 2016.

Biography

Lei Meng biography. He is a full associate professor of the Kexin software college at Shenyang Normal University. He has research interests in wireless networks, cloud computing and network security. Email:8871346@qq.com

Shoulin Yin biography. He 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 multimedia security, network security and image processing.

Chu Zhao biography. She 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.