International Journal of Security and Its Applications
Vol. 9, No. 6 (2015), pp. 157-166
http://dx.doi.org/10.14257/ijsia.2015.9.6.16

Image Encryption Research based on Key Extracted from Iris Feature

RuiYun Xie[1], MingFei Wang[1] and BenZhai Hai[2]

[1]*Computer Science and Technology Department, Henan Mechanical and Electrical Engineering College, Henan Xinxiang 453000, China*
[2]*Information Engineering College, Wuhan University Of Technology, Hubei Wuhan 430070, China*
271932557@qq.com

Abstract

The encryption algorithm has disadvantages like the long key making memory difficult and uneasy safekeeping, which causes a potential threat to the information security. Therefore, a new direction of the encryption method research is to combine the biometric information with the traditional encryption algorithm. The key extracted from the iris and AES encryption algorithm are used in the image encryption algorithm. The db2 wavelet decomposition to the iris region is performed, and the third level high frequency coefficient is extracted as the iris feature codes, from which a 192 bit key is generated by using the stochastic mapping function. The randomness of the key extraction is analyzed. The proposed algorithm is employed to do the encryption test to the image. The encryption effect is compared with the scrambling encryption effect of the classic Arnold method. The experiment results show that security of the encryption image gained by using the proposed algorithm is higher, achieving the purpose of protecting image information.

Keywords: *iris feature, encryption key, AES, image encryption*

1. Introduction

The security of encryption algorithm is determined by the key. However, the long key has the disadvantages for uneasy memory and difficult storage. Besides, the key is from the outside, which leads to the hidden security trouble to the encryption algorithm. The key is extracted from biometric of the human body, with the sole, life-long and portability advantages so that the security of the encrypted information can greatly improve. The key based on the biometric features was applied earliest in online trading for the IBM transaction security system in 1989, by using signature pen and handwriting signal processor [1]. MONROSE *et al.*, extract the key successfully from the sound [2] and keystroke behavior [3]. Clancy *et al.*, combine the fingerprint characteristics with the intelligent equipment to improve the security of the encrypted information [4]. CHANG *et al.*, are mapped into the encryption key according to the distribution of biological characteristics in the position of the whole feature space [5]. However, these algorithms have certain distances from the practical application. Furthermore, there are few key generation methods based on iris features and how exact effect the generated key is used in the encryption to, which are worthy of further study.

The algorithm is proposed based on iris feature for the use of the image encryption. After completing iris preprocessing, iris features are extracted by using db2 wavelet. The stochastic mapping function is used to extract 192 bit random key from the encoding of iris features using, combining with the AES algorithm for image encryption experiment. The experiment results show that the encrypted image could reach the purpose of protecting the image information with higher security, compared with the classical Arnold

ISSN: 1738-9976 IJSIA

image scrambling encryption algorithm.

2. Iris Feature Keys Extraction based on Wavelet Transform

2.1. The Basic Principle of Wavelet Transform

Since 1986, Wavelet Analysis has rapidly developed an emerging discipline due to the foundation work of Y. Meyer, S. Mallat and I. Daubechies, as the revolutionary evolution result of Fourier analysis. Its history could be traced to Haar's work in 1909. From the perspective of the modern wavelet transform, many new directions associating with wavelet appeared in the 1930s, such as the work of Lévy, Littlewood and Paley, Franklin and Lusin. Since then, because of the impact of the Second World War, there have not been performances. The wavelet analysis is mainly related to the work of Calderón in 1960 and the research of Grossmann and Morlet in 1980, later known as the "atomic decomposition". Especially work after 1986 has rapid developed due to the widespread application [6].

Wavelet analysis has deep and wide dual meanings of the theory and application. It is the local transformation between the time and the frequency, which can effectively extract information from the signal. At the same time, multi-scale analysis is done to functions or signals through the extension and translation, so that the wavelet transform is known as "mathematical microscope". It has achieved important results with scientific significance and application value in many disciplines of the mathematics field itself, signal analysis, image processing, computer recognition, data compression, feature extraction and other fields.

The short-time Fourier transform(STFT) window function is shown as:

$$\varphi_a(t,\omega) = \varphi(t-a)e^{-it\omega} \tag{1}$$

The window function is obtained through translation and frequency limitation of the function in time axis, and the time-frequency analysis window has a fixed size. However, the non-stationary signal needs multiresolution time-frequency window, namely the request has high time resolution in the high-frequency range, while the request has high frequency resolution in the low frequency range. There are the ability of localization in time domain and frequency domain. Therefore, the window function family $\{\psi_{a,b}(t)\}$ is introduced as follows:

$$\psi_{a,b}(t) = |a|^{-\frac{1}{2}} \psi(\frac{t-b}{a}) \tag{2}$$

$\psi_{a,b}(t)$ is the analysis wavelet or continuous wavelet, as shown in Figure 1.

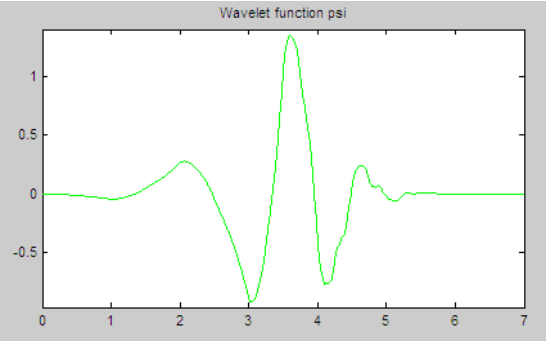


Figure 1. Wavelet Function

Continuous wavelet transform (CWT) of signal *f* is defined as:

$$(W_\psi f)(a,b) = \left\langle f, \psi_{a,b} \right\rangle = |a|^{-\frac{1}{2}} \int_{-\infty}^{+\infty} f(t) \bar{\psi}(\frac{t-b}{a}) dt \qquad (3)$$

$(W_\psi f)(a,b)$is the wavelet coefficient, which is function of scale a and position b. Among them, "< >" presents inner product; $\bar{\psi}$ represents the complex conjugate of ψ. a is the scale parameter; $a \in$ R and $a \neq 0$ represents the stretching related to the frequency. b is the parameter of the time location. By expanding and contracting the scale and moving parameter b, the band-pass characteristic of wavelet is used to decompose signals in different rates. The result of translation can take this group of signal as the window, to observe the interesting part. As shown in Figure 2, a Daubechies wavelet (db3) is taken as an example, showing changes in different scale parameter a and location parameter b.

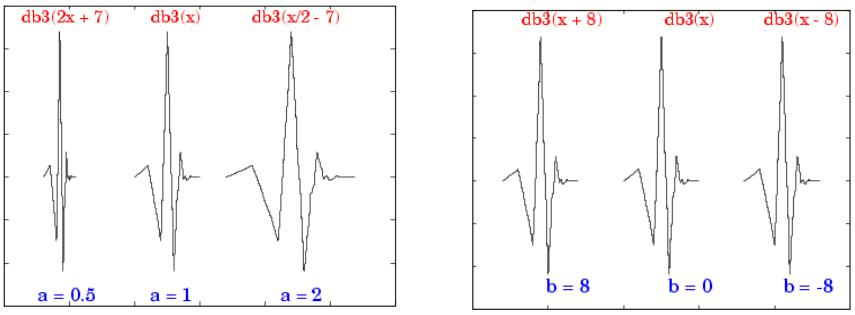


Figure 2. Example of Wavelet Function Changes caused by Parameters

Because the wavelet expression in the function graph should mainly exist in the "wave" of the limited range, so the requirements of permit conditions can be met:

$$C_\psi = \int_R \frac{|\hat{\psi}(\omega)|^2}{|\omega|} d\omega < +\infty \qquad (4)$$

Meeting the conditions of the type (5.15) is called a basic wavelet or maternal wavelet, and $\hat{\psi}$ is regarded as Fourier transform of ψ.

For formula (3), when the scale parameter a changes, the bandwidth and center frequency of band-pass filter change. When a is small, the center frequency becomes larger, while the bandwidth becomes wide; when a becomes large, the center frequency becomes small, and the bandwidth is narrow. The characteristics of wavelet transform have important application value for the local characteristics analysis of signal f. For example, the place where the signal changes slowly is mainly the low frequency component, and frequency range is narrow. At this time, the band-pass filter of the wavelet transform is equivalent to the situation of large a; conversely, the place where signal changes suddenly is mainly the high frequency component, and frequency range is wide. The band-pass filter of the wavelet transform is equivalent to the situation of small a. When the scale parameter a changes from small to large, the filter range changes from high to low frequency. Therefore, the wavelet transform has a zoom feature. Wavelet transform has the following properties:

(1) Linear transformation. Wavelet transform is linear, and linear transformation has overlapped character;

(2) Time transformation characteristic. If CWT of f is $(W_\psi f)(a,b)$, then CWT of $f(x\text{-}x_0)$ is $(W_\psi f)(a,b-x_0)$;

(3)Scale transformation. If CWT of f is $(W_\psi f)(a,b)$, CWT of $f(\frac{x}{\lambda})$ is $\sqrt{\lambda}(W_\psi f)(\frac{a}{\lambda},b)$.

In addition to meet the permit conditions, wavelet need meet the following properties: function $\psi(t)$ has compact support characteristics, namely the function value outside a finite interval is zero. At the same time, the function has a fast decay character to obtain the spatial localization. For a natural number *N*, function $\psi(t)$ has *N*-order vanishing moment.

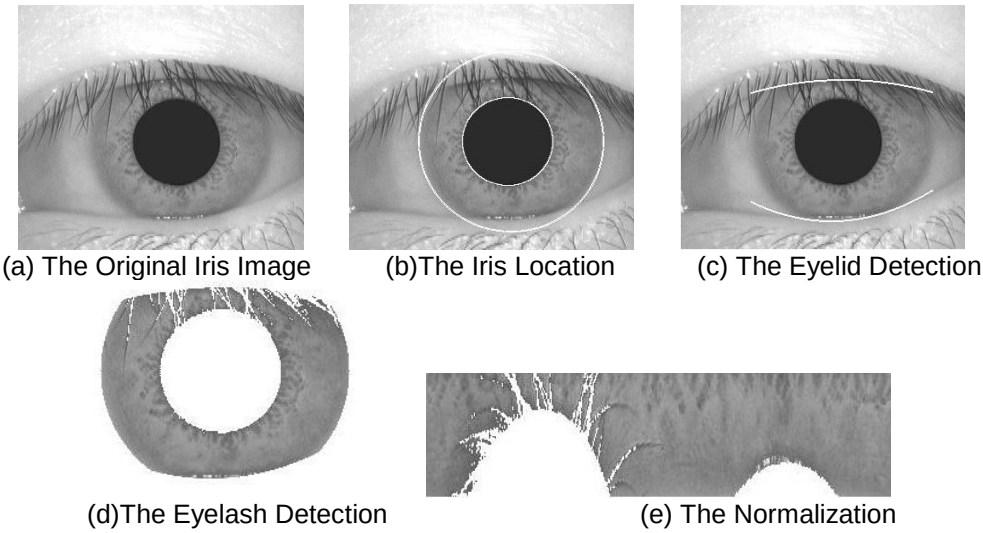
$$\int_{-\infty}^{+\infty} t^k \psi(t)dt = 0, k = 0,1,\cdots,N-1 \tag{5}$$

When vanishing moment N increases, the wavelet function $\psi(t)$ will shock increasingly fiercely.

2.2. Iris Feature Extraction

Before extracting the feature, it is necessary to do iris preprocessing, including the iris image acquisition, iris localization, and iris image normalization [7]. Iris image includes iris, and interference from the eyelids, eyelashes and light spot. Therefore, the iris needs to be localized to eliminate interferences. It is necessary to normalize the shape of th iris image into a rectangle of fixed size to compare different shape iris as shown in Figure 3.

Iris structure is shown in Figure 4. The distance of iris region to the inner edge is about 1.5mm. The jagged region of ring shape is called the iris collarette. Based on the collarette, the iris is broadly divided into two parts: the part near the inner edge is called the iris pupil; the part near the outer edge is called the iris ciliary body [8]. Because Pupil part contains rich texture details and therefore this region can contribute more iris texture features for the identification.



(a) The Original Iris Image (b)The Iris Location (c) The Eyelid Detection

(d)The Eyelash Detection (e) The Normalization

Figure 3. Iris Preprocessing

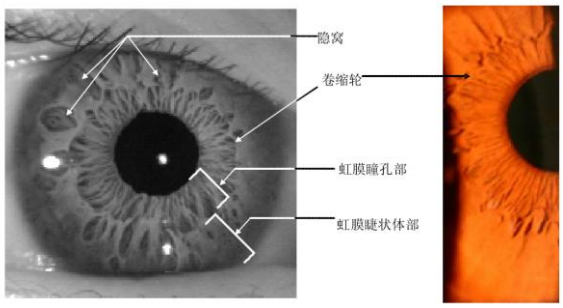
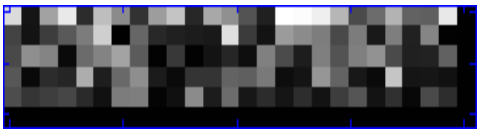


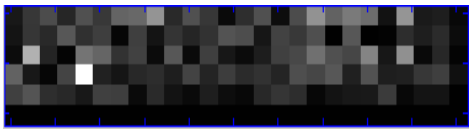
Figure 4. Iris Texture Features

The normalized extraction region of the iris feature is obtained through the iris image preprocessing, as shown in Figure 5. The normalized image resolution is set as 100×400, and the feature extraction region is generally not less than 1/6 of the normalized image. Here it is set as 80×200. The existing algorithms of the iris feature extraction are mostly based on the classical Gabor wavelet transform. The db2 wavelet is used to iris feature extraction, because db2 wavelet has orthogonal, compactness and generalized linear phase features [9]. The db2 wavelet is used to do the three-layer transform of the two-dimensional wavelet transform on extraction region and get low frequency coefficients, horizontal high frequency coefficient, vertical high frequency coefficients and the diagonal high frequency coefficients, as shown in Figure 6. Because the details of the iris texture feature are rich, which is mainly shown by the high frequency coefficients, the number of high frequency coefficients of the first or second levels are large. If they are extracted as the iris feature to cause longer encoding, the recognition efficiency will be affected. The high frequency coefficient of the third layer is moderate, which is suitable as the iris feature.

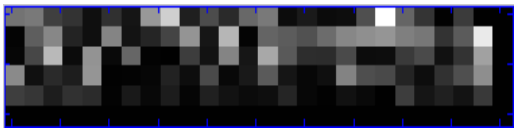
Figure 5. The Feature Extraction Region



(a) The Vertical High Frequency Coefficients



(b) The Horizontal High Frequency Coefficients



(c) The Diagonal High Frequency Coefficients

Figure 6. The Third Layer High Frequency Coefficients

The capacity of each high frequency coefficient of the third layer is $(80 \times 200)/(2^3 \times 2^3)=250$ and the capacity of high frequency coefficient in the three directions is $250 \times 3=750$, as shown in the following figure. The extracted 750 high frequency coefficients are used by random mapping function to generate 192 bit key of the cryptographic algorithm.

3. Image Encryption Algorithm based on AES

3.1. AES Encryption Algorithm

With the development of cryptanalysis technology and the improvement of the computer operation performance, the National Institute of standards (NIST) promulgated Data Encryption Standard (DES) with the length of key is 64 in 1977, which becomes unsafe. In 1997, NIST launched a collection of Advanced Encryption Standard (AES) activity, and chose Rijndael proposed by Joan Daemen and Vincent Rijment as AES from many algorithms. Because of its uniqueness, AES became a pronoun of Rijndael. AES has strong flexibility, and variable size of its encryption plaintext blocks are 128,192 or 256, and variable key lengths are 128,192 or 256, and the number of iterations and the plaintext block size are closely linked with the key length, which has higher safety achieve software and hardware faster, compared with DES. Since the advent of AES, with its strong anti cracking ability, no cryptanalysis attack method can break AES. In 2001, it became the advanced encryption standard promulgated by NIST [10].

AES algorithm is a kind of grouping encryption algorithm with changeable block plaintext length and key length. Meanwhile, it is the symmetric encryption algorithm, whose encryption and decryption use the same key. Its grouping length and the key length are respectively 128 bit, l92 bit or 256 bit. Let N_b be equal to the length of the plaintext grouping words (1 word =4 bytes =32 bit). N_k is the word of the key length. The relationship between the number of encryption rounds N_r, N_b and N_k is shown in Table 1.

Table 1. The Relation between N_r ,N_b and N_k

N_r \ N_k / N_b	4	6	8
4	10	12	14
6	12	12	14
8	14	14	14

Each round transformation of encryption and decryption of AES includes substitute, line shift, mix column and key plus operations, and the decryption process is composed of the corresponding inverse operation.

3.2. The Image Encryption Principle

The color image mostly uses RGB model, which can be regarded as the formation of R, G, and B superposition. RGB can use from 0 (black) to 255 (white) values, being consistent with the range of the grayscale image value, and therefore the encryption method for the grayscale image can also be applied to the color image.

A grayscale digital image is expressed by matrix $f(i, j)$, and the image size is $M \times N$, of which: $0 \leq i \leq M\text{-}1$, $0 \leq j \leq N\text{-}1$. $f(i,j)$ represents grayscale value of the image row i column j, and there are 2^8=256 grades; the range is [0 ~ 255], which is consistent with pixel gray value range of the gray image [11]. Because the AES algorithm in the plaintext input is in bytes, 16 bytes as the matrix elements, range is also [0 ~ 255]. Therefore, the key XOR operation, displacement, line shift and column confusion are applied to the grayscale digital image encryption. After encryption, the following functions are exerted:

(1) The key XOR is used to realize pixel grayscale value transformation;

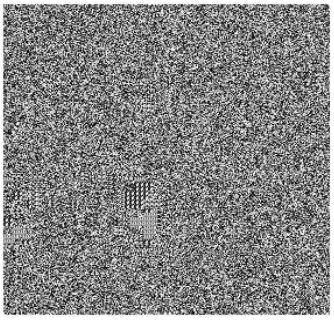
(2) The replace operation is used to complete the displacement of the image pixel grayscale value to control the scrambling;

(3) The line shift and column confusion are used to complete the image pixel position transformation for high diffusion over scrambling.

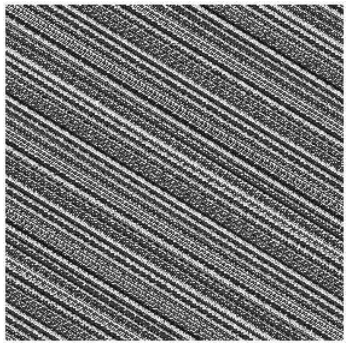
4. Analysis of Image Encryption Experiment

The classical Arnold transform [12] is used to do scrambling encryption to the lena image in Figure 7(a). In Figure 7 (b), the proposed algorithm encryption results are shown. Figure 7 (c) is the encryption results of the Arnold transform and its number of iterations are 10 times. Figure 7 (d) is the histogram of Figure 7 (b). Figure 7 (e) is the histogram of Figure 7 (c).

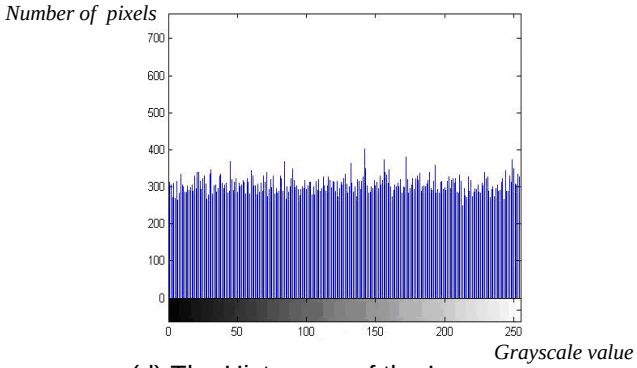
(a) The Lena Ima



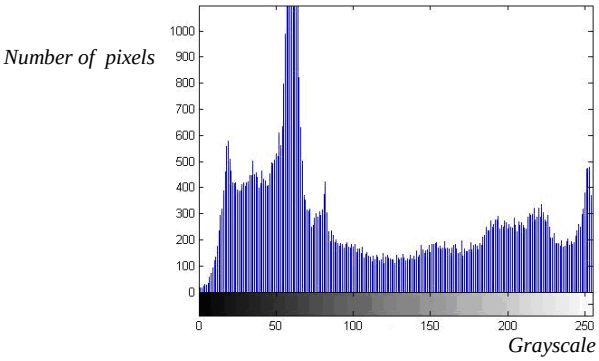
(b) The Encryption Image of the Proposed



(c) The Encryption Image of Arnold Transform



(d) The Histogram of the Image Encryption by the Proposed



(e) The Histogram of the Image Encryption by the Arnold Transform

Figure 7. Encryption Effect Comparison between the Proposed Algorithm and Arnold Transformation

According to the definition of scrambling degree [], the definition is given to calculate the scrambling degree for image encryption through the above two algorithms.

$$\mu_{iris} = \frac{\sigma^2_{new}}{\sigma^2_{org}} = \frac{5437.1}{977.4} = 5.56 \quad (6)$$

$$\mu_{Arnold} = \frac{\sigma^2_{new}}{\sigma^2_{org}} = \frac{5070.4}{977.4} = 5.18 \quad (7)$$

μ_{iris} is the scrambling degree of the image encryption by the proposed algorithm, while μ_{Arnold} is the scrambling degree of the encryption image by Arnold transform. μ_{iris} is larger than μ_{Arnold} ; at the same time, the encrypted image histogram is analyzed, the histogram of the image encryption by the proposed algorithm is flatter than that of Arnold transform, while the image signal is random. The worse the readability of the encrypted images is, the smaller reductive possibility is and the safer the image after the encryption is. According to the above analysis, image encryption security of the encryption algorithm proposed is higher than that of Arnold transform.

5. Conclusion

An image encryption algorithm is proposed based on key extracted from iris feature. The randomness of the key is analyzed. The proposed algorithm is used for the encryption test to the image. The encryption effect by the proposed algorithm is compared with that of the classic Arnold algorithm. The experiment results show that the security of image encryption of the proposed algorithm is higher, reaching the purpose to protect the image information.

Acknowledgements

The study was supported by following Funds.
(1) Scientific research fund of henan provincial education department [14A520085].
(2)Teacher education curriculum reform of Henan Province [2014-JSJYYB-026].
(3) Youth Science Fund of Henan Normal University.

References

[1] D. G. Abraham, G. M. Dolan, G. P. Double and J. V. Stevens, “Transaction Security System”, IBM Systems Journal, vol. 30, no. 2, **(2011)**, pp. 206-229.
[2] F. Monrose, M. K. Reiter, Q. Li and S. Wetzel, “Cryptographic key generation from voice”, IEEE Symposium on Security and Privacy, **(2011)**, pp. 202-213.
[3] F. Monrose, M. K. Reiter and R. Wetzel, “Password hardening based on keystroke dynamics”, Proc of Sixth ACM Conference of Computer and Communication Security, USA, ACM Press, **(1999)** May 1-3, pp. 73-82.
[4] C. Charles, K. Negar and J. Dermis, “Secure Smartcard-Based Fingerprint Authentication”, ACM Workshop on Biometrics Methods and Application, Berkeley, California, **(2009)**,pp. 45-52.
[5] G. Davida, Y. Frankel and B. Matt, “On enabling secure applications through offline biometric identification”, Proceedings of IEEE Symposium on Security and Privacy, Oakland, California, **(2011)**, pp. 148-157.
[6] S. Lim, K. Lee and D. Byeon, “Efficient iris recognition through improvement of feature vector and classifier”, ETRI Journal, vol. 23, no. 2, **(2001)**, pp. 233-235.
[7] Q. C. Tian, Q. Pan, Y. M. Cheng and H. C. Zhang, “The experimental research on incomplete iris patterns and uniqueness”, Application Research of computers, vol. 20, no. 1, **(2006)**, pp. 237-239.
[8] Q. C. Tian and R. S. Zhang, “The overview of biological feature identification technology”, Research of computer application, vol. 26, no. 12, **(2009)**, pp. 4401-4410.
[9] K. Gyundo, B. Yungcheol and L. Kwanyong, “Improved Techniques for an Iris Recognition System with High Performance”, Australian Joint Conference on Artificial Intelligence, Adelaide, Australia, **(2001)**, pp. 177-188.
[10] L. H. Liu and C. J. Wen, “AES differential-algebraic attacks”, Computer engineering and application, vol. 46, no. 5, pp. 111-113.

[11] Z. Gang, T. Zhen and L. Jianping, "Encryption scheme of image key generation and Rijndael algorithm based on biometric characteristics", Computer engineering and science, vol. 31, no. 12, **(2009)**, pp. 11-12.
[12] H. X. Zhang and P. L. Qiu, "The applications of scrambling technology in digital watermarking", Journal of circuits and systems, vol. 6 ,no. 3, **(2001)**, pp. 33-36.

Authors

RuiYun Xie, received her Master Degree from Wuhan University of Technology in 2009. She is now an Lecturer of Henan Mechanical and Electrical Engineering College in China. His research interests include computer application, Computer Network. He has published more than 7 papers in journals and conferences.

MingFei Wang, received his Master Degree from Henan Normal University in 2007. He is now an Lecturer of Henan Mechanical and Electrical Engineering College in China. His research interests include computer application; Computer Network. He has published more than 10 papers in journals and conferences.

BenZhai Hai, received her Master Degree from Wuhan University of Technology in 2009. She is now an Lecturer of Henan Mechanical and Electrical Engineering College in **China**. His research interests include computer application, Computer Network. He has published more than 7 papers in journals and conferences.