International Journal of Signal Processing, Image Processing and Pattern Recognition
Vol.9, No.8 (2016), pp.181-190
http://dx.doi.org/10.14257/ijsip.2016.9.8.16

Bit-Level Image Encryption Algorithm Based on Composite Chaotic Mapping

Cai Yang, Haiyu Zhang, Jinliang Guo, Songhao Jia and Fangfang Li

School of Computer and Information Technology, Nanyang Normal University, Nanyang 473061, Henan, China
nyyc@163.com

Abstract

Because the single chaotic mapping easily creates security weaknesses in the image encryption algorithm, the security needs to be improved. Aiming at this problem, a bit-level image encryption algorithm based on composite chaotic mapping (CCM-IEA) is proposed. First of all, the algorithm scrambles the plain image on bit level through the Cat mapping for the first time. And then the Henon mapping of two dimensional discrete is used to scramble for the second time. Finally, image diffusion is operated through the one dimensional Logistic mapping, and the data sensitivity is enhanced. The experimental results show that the performance of the CCM-IEA algorithm is better on the histogram, information entropy and correlation analysis. Compared with the single chaotic images encryption algorithm, the CCM-IEA algorithm has the ability to resist the information entropy analysis and correlation analysis. It can be seen that the CCM-IEA algorithm has high safety performance and good encryption effect.

Keywords: *Composite Chaotic Mapping, Cat Mapping, Henon Mapping, Image Diffusion, Logistic Mapping*

1. Introduction

With the rapid development of network technology, a variety of multimedia information such as images, sound communicate more and more on the Internet. In which, the image data has bigger comparison. Image transmission brings us convenience, but also produces serious security hidden danger. How to ensure the safety of image data is the current research focus.

Because the image has large amount data and high redundancy characteristics, the traditional encryption methods such as DES, RSA algorithm is not suitable for image encryption. Chaos is a unique phenomenon in a deterministic nonlinear system. Because of its initial conditions and control parameters of the extreme sensitivity and random behaviour, Chaos is widely used in the field of information security. Many scholars and experts have studied on the respect. K. Deergha Rao *et. al.*, proposed discrete wavelet transform and Modified Chaotic Key-Based Algorithm to enhance the security of CKBA. The enhanced security of the proposed algorithm was analyzed through cryptanalysis [1]. Akram Belazi *et. al.*, proposed a new image encryption method based on DNA encoding and chaotic systems. Equivalent mathematical model of the cryptosystem was designed and algebraic analysis was given [2]. A new method based on a hybrid model was proposed for image encryption. The hybrid model was composed of a genetic algorithm and a chaotic function [3]. Iqtadar Hussain et al. proposed a method for image encryption based on chaotic skew tent-map and substitution box transformation. This method provided confusion and diffusion at the same time [4]. Shahram Etemadi Borujeni et al. proposed an algorithm to encrypt an image in hybrid domain, frequency and time domains. The proposed method was a private key encryption system with two main

ISSN: 2005-4254 IJSIP
Copyright ⓒ 2016 SERSC

units, chaotic phase-magnitude transformation unit and chaotic pixel substitution unit [5]. An efficient image encryption algorithm using the generalized Arnold map was proposed. The algorithm was composed of two stages, *i.e.*, permutation and diffusion [6].

In summary, the chaotic mapping is widely used in image encryption algorithm. In image encryption process, single chaotic mapping only change the positions of the pixels. However, image pixel value is not changed. This can not resist the attack of the secret text. Because the image pixel permutation is limited, a certain number of iteration for single chaotic mapping is likely to decrypt the original image. The safety of single chaotic map encryption needs to be improved, and the effect of this algorithm is limited. This paper presents a composite chaos mapping image encryption algorithm to improve the security of image data. Composite chaotic mapping can increase the complexity of encryption algorithm, and reduce the risk of being cracked. Therefore, it can improve the security of image data. Firstly, the plaintext image has been done bit level scrambling by using Cat mapping and Henon mapping. Then, the scrambled image data are done diffusion operation by Logistic mapping. This operation makes the mutual influence between the pixels, even minor changes. Simulation results show that the composite chaos mapping image encryption algorithm can resist the aggressive behaviours such as the histogram analysis, key sensitivity analysis, and correlation analysis.

2. The Composite Chaos Mapping

2.1. Cat Mapping

Cat mapping is a transform in the study of ergodic theory. The general form of the kinetic equation is present as in Equation (1).

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod (N) \quad (1)$$

In this equation, (x_n, y_n) represents a coordinate in N*N images. The variables a and b are the parameters of the system, take positive integer. Cat mapping has typical chaotic characteristics [7].

2.2. Henon Mapping

Henon mapping is one of the most widely used two dimensional chaotic mappings. The mapping function is shown as Equation (2).

$$\begin{cases} x_{i+1} = 1 - ax_i^2 + y_i \\ y_{i+1} = bx_i \end{cases} \quad (2)$$

In the formula, the variables a and b are the parameters of the system. When the parameter is different, there is a periodic trajectory [10]. When a=1.4, b=0.3, the mapping is in chaotic state.

2.3. Logistic Mapping

In 1976, America mathematical ecologist R.May built the famous Logistic model in ecological research, its mapping function is shown as Equation (3).

$$x_{n+1} = \mu \cdot x_n \cdot (1 - x_n) \qquad n = 1, 2, 3\ldots \quad (3)$$

Among them, μ represents the control parameter, its range is $0 \le \mu \le 4$. X said the iteration interval, its range is $0 \le x \le 1$. When the value of μ is between 3.569946 and 4, the mapping is in chaotic state. The variable μ is closer to 4, the random

 Copyright ⓒ 2016 SERSC

performance is better. At the same time, the mapping shows similar white noise statistical characteristics of average distribution [11].

3. Design of the CCM-IEA Algorithm

According to the operated objects, image encryption algorithm can be divided into pixel level scrambling algorithm and bit level scrambling algorithm [12]. Pixel level scrambling image encryption algorithm uses pixels as the basic elements of operation, only exchanges position information between pixels [13]. However, the pixel value is unchanged. Bit level permutation algorithm converts the pixel integer sequence to a bits sequence, then the bit sequence are scrambled in whole. This algorithm has not only changed the bit position, also changed the pixel value. The CCM-IEA algorithm is a bit level image encryption algorithm. The algorithm consists of two process, image scrambling and image diffusion.

3.1. The Bit Level Image Scrambling

In the bit level image scrambling, each pixel of the image is no longer considered the minimum operating elements. And each pixel is seen as a bit set. For a high h, width w of a plain image, it can be said as a two-dimensional matrix M, which has h rows and w columns. M is shown as Equation (4).

$$M = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1w} \\ a_{21} & a_{22} & \cdots & a_{2w} \\ \cdots & \cdots & \cdots & \cdots \\ a_{h1} & a_{h2} & \cdots & a_{hw} \end{bmatrix} \tag{4}$$

Firstly, each pixel a_{ij} is converted to the 8 bit binary sequence $\{a_{ij1}, a_{ij2}\ldots a_{ij8}\}$. Among them, the value of a_{ijk} is 0 or 1, $k \in [1,8]$. A matrix M_1 can be got after the operation, which size is h×8w. According to the order from left to right and from top to bottom, the matrix M_1 is converted into a bit sequence P={P(1), P(2), …, P(8hw)}. Then, it is scrambled by using chaotic sequence. The bit sequence Q= {Q(1), Q(2), …,Q(8hw)} is obtained. Then, the one-dimensional sequence Q is converted to a bit matrix M_2, which size is h×8w. Finally, according to the order from left to right and from top to bottom, each 8 bits are converted to an integer [14-16]. In this way, the bit level image scrambling is completed.

3.2. Image Scrambling Process

The CCM-IEA algorithm scramble image by using the Cat mapping for the first time. Then, the image data is scrambled by Henon discrete mapping for the second time [17]. Specific steps are as follows.

Step 1: Each element of the plain image of the corresponding matrix is transformed into an 8 bit sequence, so as to obtain the bit sequence A. It contains elements of h rows and 8w columns. The variable h represents the rows number of the matrix. The variable w said the number of columns in the matrix.

Step 2: The parameters in Equation (1) are set to: x_0=10, y_0=20, a=3, b=4. Two groups of chaos random sequence are obtained: $x=\{x_1, x_2,\ldots x_h\}$, $y=\{y_1, y_2,\ldots y_{8\times w}\}$.

Step 3: The sequences of x and y is sorted in ascending order. Thus the index series are obtained. They are represented as $I_x=\{I_{x1}, I_{x2},\ldots I_{xh}\}$, $I_y=\{I_{y1}, I_{y2},\ldots I_{y8\times w}\}$.

Step 4: Through the index sequence I_x and I_y, the bit sequence A is scrambled. The scrambling principles are as follows. According to the index number in I_x, the elements in A are sorted. That is, the rows of A are replaced according to the value of I_x. Then, the columns of A are replaced according to the value of I_y. After the operation, a new bit sequence L is obtained. Then, the elements in the L are placed

Copyright ⓒ 2016 SERSC

in a row. Finally, a new sequence of LL is obtained, and expressed as LL= $\{L_1, L_2,\ldots L_{h\times 8w}\}$.

Step 5: The parameters in Equation (2) are set to: x_0=0.234567, y_0=0.123456, a=1.4, b=0.3. Two groups of chaos random sequence are obtained: x=$\{x_1, x_2,\ldots x_{h\times 8w}\}$, y=$\{y_1, y_2,\ldots y_{h\times 8w}\}$.

Step 6: The chaotic sequences of x and y are sorted in descending order, the index series are got. They are expressed as I_x=$\{I_{x1}, I_{x2},\ldots I_{xh\times 8w}\}$, I_y=$\{I_{y1}, I_{y2},\ldots I_{yh\times 8w}\}$.

Step 7: According to the index sequences of I_x and I_y, the bit sequence LL is performed the scrambling at second time. A bit sequence S is got. Scramble rules is shown as Equation (5).

$$\begin{cases} T_i = LL_{I_{xi}} & i = 1,2,\ldots,h\times 8w \\ S_j = T_{I_{yj}} & j = 1,2,\ldots,h\times 8w \end{cases} \quad (5)$$

Step 8: For the bit sequence S, each 8 bits are converted to an integer. One-dimensional bit matrix M_s is obtained, and its size is h×w.

3.3. Image Scrambling Process

The image diffusion is sufficiently sensitive with small change of plaintext, and can change the tiny diffusion to follow-up pixels. That is to say, the pixel value is associated with each other [18-19]. According to this idea, a new diffusion method is proposed. The operation is performed as Equation (6).

$$\begin{cases} c_0 = rand_1 \times 256 \mod 256 \\ c_{i+1} = rand_2(i) \times 256 \times \left\lceil c_i \times \left(1 - \frac{c_i}{256}\right) \oplus M_s(i+1) \right\rceil \mod 256 \end{cases} \quad (6)$$

Among them, $rand_1$ and $rand_2$ is a random sequence, which is generated by one-dimensional Logistic chaotic mapping. The length of $rand_1$ is 1. The value of parameter μ is 4, and the value of parameter x_0 is 0.99. The length of $rand_2$ is h×w, the other parameters are set as: μ=4, x_0=0.89. M_s(i+1) represents an integer after bit scrambling, the serial number of which is i+1. It can be seen from the Formula (6) that c_{i+1} and c_i have close association. There is a very strong correlation between pixels, so that the CCM-IEA algorithm has a good sensitivity to variations in pixel.

4. Experiment Results and Analysis

The effectiveness of CCM-IEA algorithm is verified by the simulation experiment. Matlab 2012 is used in experiment. The experiment used the image Lena (640*640).The hardware environment is set as follows.

OS: Window Server 2003

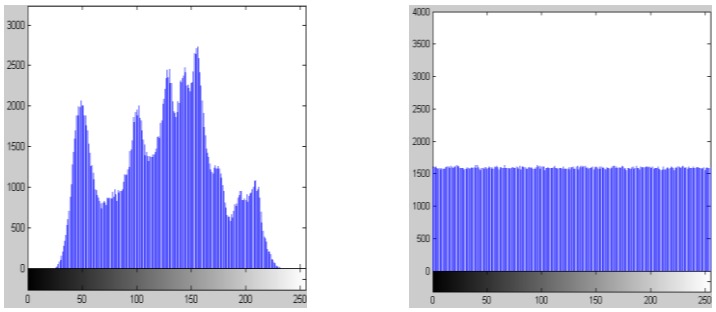
Hardware: Xeon E5620 2.4G, 8 nuclear CPU, 4GB RAM

4.1. Histogram Analysis

Histogram is called the image gray value distribution, which reflects the distribution of image pixel values [20]. Plaintext and ciphertext image histogram from experiment are shown as Figure 1.

It can be seen that the plain image histogram is non-uniform and the cipher image histogram is basically uniform distribution. That is to say, the cryptanalyst cannot get any information about the plaintext from the ciphertext image histogram. This shows that the encrypted image by the CCM-IEA algorithm can resist statistical attack.

 Copyright ⓒ 2016 SERSC

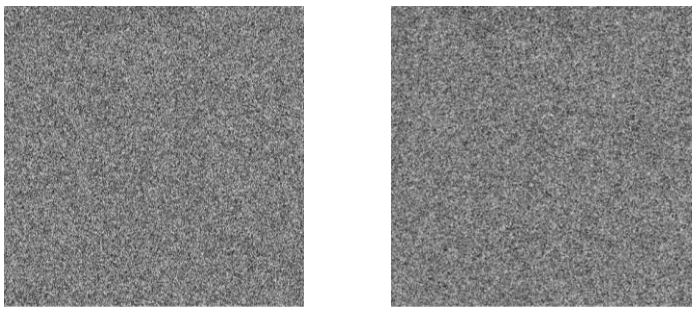


(a)The plain image histogram (b)The ciphered image histogram

Figure 1. Histogram Analysis

4.2. Key Sensitivity Analysis

When the CCM-IEA algorithm chooses the encryption key, Cat mapping and Logistic mapping parameters remain unchanged. The value of variable x_0 and y_0 in the Henon mapping are slight modified. The original value of x_0 is 0.234567, now is revised to 0.234568. The original value of y_0 is 0.123456, now is revised to 0.123455. The amplitude of variation is 10^{-6}. According to the different keys, Lena image is encrypted. The cipher image is shown as Figure 2. Through calculation, their difference value is 97.59%. It shows that the CCM-IEA algorithm is very sensitive to the encryption key.



(a) Encrypted image before key change (b) Encrypted image after key change slight

Figure 2. The Encryption Key Sensitivity Analysis

When the decryption key is chose, the parameters of Cat mapping and Henon mapping remain unchanged. At the same time, the parameters of the Logistic mapping are changed. In the image diffusion stage, the value of variable x_0 in function $rand_1$ is changed from 0.99 to 0.989999. The value of variable x_0 in function $rand_2$ is changed from 0.89 to 0.900001. The amplitude of variation is 10^{-6}. After this operation, the decryption image is shown as Figure 3. Through calculation, their difference value is 99.86%. It shows that the CCM-IEA algorithm is very sensitive to the decryption key.

Copyright ⓒ 2016 SERSC

(a) Decrypted image before key change

(b) Decrypted image after key change slight

Figure 3. The Decryption Key Sensitivity Analysis

4.3. Performance Comparison of Image Encryption Algorithm with Single Chaotic Mapping

Literature [8] and [9] used single chaotic mapping in image encryption algorithm. Through the comparison of the two algorithms and the CCM-IEA algorithm, the performance is verified.

4.3.1. Information Entropy Analysis: Information entropy is an important sign of determinacy of information source. If the uncertainty is stronger, the information entropy is greater. Therefore, it is used to judge the random of encryption scheme. The information entropy is expressed in Equation (7).

$$H(X) = -\sum_{i=0}^{n} p(x_i) \log_2 p(x_i) \tag{7}$$

Among them, $X=(x_0, x_1 \ldots x_n)$ said the information source. H(X) said the information entropy of X. $p(x_i)$ represents the appear probability in the sequence of x_i point.

According to the Formula (7), the information entropy is calculated. The calculation results are shown as Table 1.

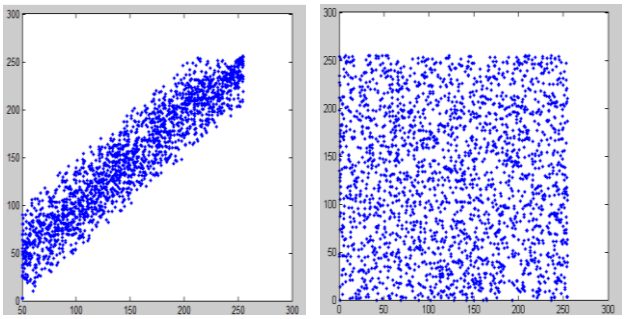
Table 1. Comparison of Information Entropy

	Information entropy
Plaintext image	7.45053
CCM-IEA	7.99967
Literature [8]	7.9963
Literature [9]	7.99926

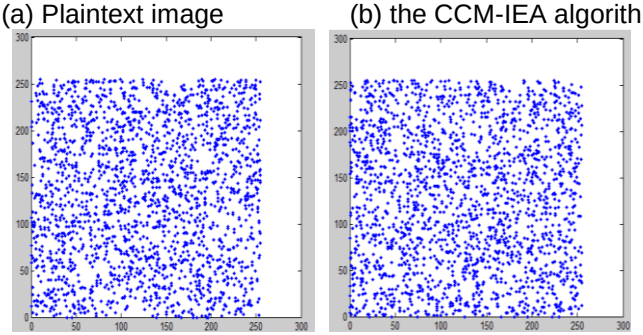
It can be seen from the Table 1, that the plain image information entropy is lowest. The information entropy in the CCM-IEA algorithm, literature [8] and literature [9] is higher. And the value is relatively close to the ideal value of 8. Moreover, the CCM-IEA algorithm has the maximum information entropy. This shows that the algorithm has more excellent performance, and can resist the attacks of using information entropy statistics.

4.3.2. Pixels Correlation Analysis: Pixels correlation shows the relationship between pixels. If the correlation is high, the attacker can predict other pixels value by a pixel value [21]. In the horizontal, vertical, diagonal directions, 2000 couple values of adjacent pixels are randomly selected from the plain image and the cipher image. The scattered point diagram is shown as Figure 4, Figure 5, and Figure 6.

 Copyright ⓒ 2016 SERSC

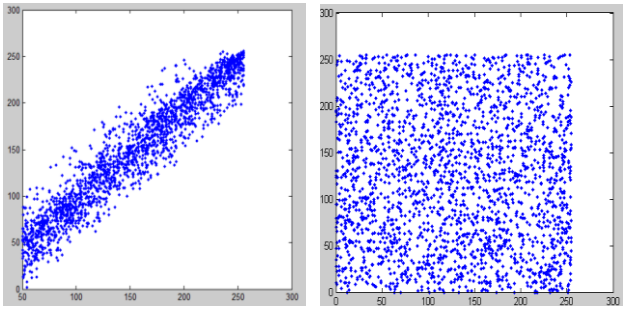


(a) Plaintext image (b) the CCM-IEA algorithm

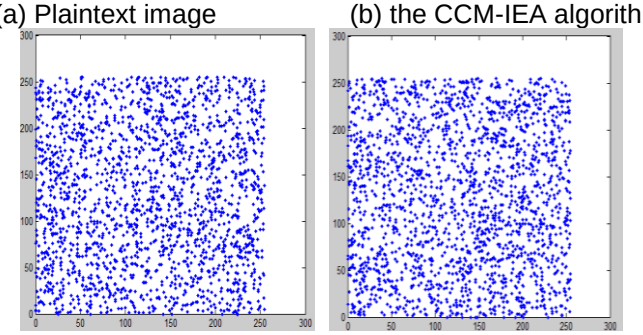


(c) Algorithm in literature [8] (d) Algorithm in literature [9]

Figure 4. The Horizontal Direction of the Scatter Diagram



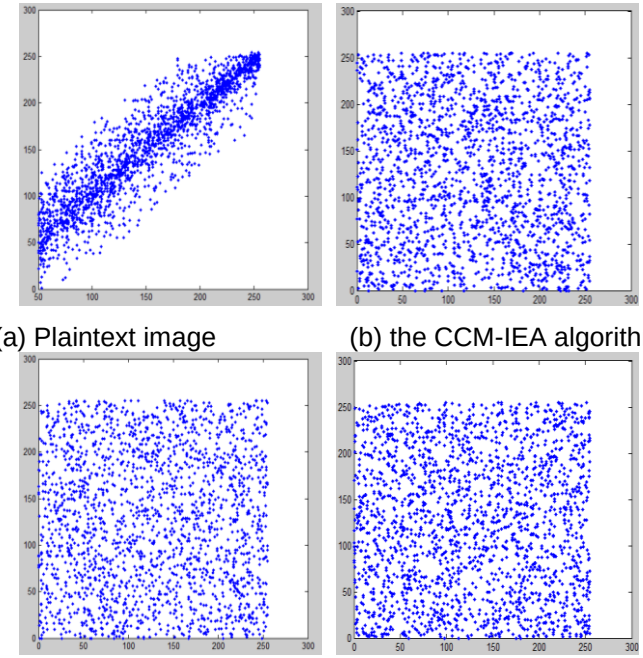
(a) Plaintext image (b) the CCM-IEA algorithm



(c) Algorithm in literature [8] (d) Algorithm in literature [9]

Figure 5. The Vertical Direction of the Scatter Diagram

Copyright ⓒ 2016 SERSC



(a) Plaintext image (b) the CCM-IEA algorithm

(c) Algorithm in literature [8] (d) Algorithm in literature [9]

Figure 6. The Diagonal Direction of the Scatter Diagram

It can be seen from Figure 4, Figure 5, and Figure 6, whether it is horizontal, vertical or diagonal direction, the cipher image scatter in CCM-IEA algorithm, literature [8] algorithm and literature [9] algorithm are disorganized. This indicates that their correlation is low. Because pixels in plaintext image have strong correlation, the scatter diagram of plaintext image has concentrated distribution.

Next, the coefficient of correlation between pixels is computed exactly through the formula. The calculation formula of coefficient correlation in scatter plots is shown as Equation (8).

$$r_{xy} = \frac{E((x - E(x))(y - E(y)))}{\sqrt{D(x)D(y)}} \tag{8}$$

Among them, x and y said two adjacent pixel gray value. r_{xy} said correlation coefficient. E(x) and D(x) express expectation and variance on variable x.

The value of correlation coefficient is shown as Table 2. It can be seen from the table that adjacent pixels correlation coefficients of the three cipher images are all close to 0. This shows that the correlation of adjacent pixels ciphertext between images is greatly reduced by encryption algorithm. In three encryption algorithms, the correlation coefficient of the CCM-IEA algorithm is lowest. It also verifies that the CCM-IEA algorithm is more able to resist the attack of adjacent pixels correlation analysis.

Table 2. Correlation Coefficients Comparison between the Plaintext Image and the Ciphered Image

Direction	Plaintext image	CCM-IEA	Literature [8]	Literature [9]
Horizontal	0.8253	0.0153	0.0172	0.0163
Vertical	0.6235	0.0102	0.0130	0.0125
Diagonal	0.5637	0.0086	0.0092	0.0090

Copyright ⓒ 2016 SERSC

5. Conclusion

Because the single chaotic mapping in image encryption algorithms has security hidden danger, a bit-level image encryption algorithm based on composite chaotic mapping encryption algorithm has been proposed to solve the problem. The algorithm consists of three main parts. First of all, the bit level image scrambling is performed by using Cat mapping and two-dimensional Henon mapping. Then, Logistic chaotic mapping is used to construct the method of image diffusion. Finally, the cipher image can be obtained. Using compound chaotic map, the security of the algorithm is improved. Simulation results show that the algorithm can resist statistical attack and is very sensitive to the decryption key. Compared with two kinds of single chaotic mapping algorithms, the CCM-IEA algorithm performance is more excellent in the information entropy and the pixel correlation statistical attack. This fully shows that the CCM-IEA algorithm is a relatively safe image encryption algorithm. It can be widely used in the image transmission.

Acknowledgment

This work was supported by the Research on Henan Province Natural Science Fund Project (142300410414, 142300410413) and the Education Department of Henan province science and technology research project (12A520033).

References

[1] K. D. Rao and Ch. Gangadhar, "Discrete Wavelet Transform and Modified Chaotic Key-based Algorithm for Image Encryption and its VLSI Realization", IETE Journal of Research, vol. 58, no. 2, **(2012)**, pp. 114-120.
[2] A. Belazi, H. Hermassi, R. Rhouma and S. Belghith, "Algebraic analysis of a RGB image encryption algorithm based on DNA encoding and chaotic map", Nonlinear Dynamics, vol. 76, no. 4, **(2014)**, pp. 1989-2004.
[3] A. H. Abdullah, R. Enayatifar and M. Lee, "A hybrid genetic algorithm and chaotic function model for image encryption", International Journal of Electronics and Communications, vol. 66, no. 10, **(2012)**, pp. 806-816.
[4] I. Hussain, T. Shah, M. A. Gondal, "Application of S -box and chaotic map for image encryption", Mathematical and Computer Modelling, vol. 57, no. 9, **(2013)**, pp. 2576-2579.
[5] S. E. Borujeni and M. Eshghi, "Chaotic image encryption system using phase-magnitude transformation and pixel substitution", Telecommunication Systems, vol. 52, no. 2, **(2013)**, pp. 525-537.
[6] G. Ye and K. W. Wong, "An efficient chaotic image encryption algorithm based on a generalized Arnold map", Nonlinear Dynamics, vol. 69, no. 4, **(2012)**, pp. 2079-2087.
[7] O. S. Faragallah, "An enhanced chaotic key - based RC5 block cipher adapted to image encryption", International Journal of Electronics, vol. 99, no. 7, **(2012)**, pp. 925-943.
[8] H. T. Panduranga, S. K. N. Kumar and Kiran, "Image encryption based on permutation-substitution using chaotic map and Latin Square Image Cipher", The European Physical Journal Special Topics, vol. 223, no. 8, **(2014)**, pp. 1663-1677.
[9] M. K. Mandal, G. D. Banik, D. Chattopadhyay and D. Nandi, "An Image Encryption Process based on Chaotic Logistic Map", IETE Technical Review, vol. 29, no. 5, **(2012)**, pp. 395-404.
[10] I. S. I. Abuhaiba, H. M. Abuthraya, H. B. Hubboub and R. A. Salamah, "Image Encryption Using Chaotic Map and Block Chaining", International Journal of Computer Network and Information Security, vol. 4, no. 7, **(2012)**, pp. 19-26.
[11] H. Hermassi, A. Belazi, R. Rhouma and S. M. Belghith, "Security analysis of an image encryption algorithm based on a DNA addition combining with chaotic maps", Multimedia Tools and Applications, vol. 72, no. 3, **(2014)**, pp. 2211-2224.
[12] M. SaberiKamarposhti, D. Mohammad, M. S. M. Rahim and M. Yaghobi, "Using 3-cell chaotic map for image encryption based on biological operations", Nonlinear Dynamics, vol. 75, no. 3, **(2014)**, pp. 407-416.
[13] F. Ahmed, A. Anees, V. U. Abbas and M. Y. Siyal, "A Noisy Channel Tolerant Image Encryption Scheme", Wireless Personal Communications, vol. 77, no. 4, **(2014)**, pp. 2771-2791.
[14] S. Saraireh, Y. Al-Sbou, J. Al-Saraireh and O. Alsmadi, , "Image Encryption Scheme Based on Filter Bank and Lifting", International Journal of Communications, Network and System Sciences, vol. 7, no. 1, **(2014)**, pp. 43-52.
[15] A. A. A. El-Latif, L. Li and X. Niu, "A new image encryption scheme based on cyclic elliptic curve and chaotic system", Multimedia Tools and Applications, vol. 70, no. 3, **(2014)**, pp. 1559-1584.

Copyright ⓒ 2016 SERSC

[16] S. Rakesh, "Image Encryption using Block Based Uniform Scrambling and Chaotic Logistic Mapping", International Journal on Cryptography and Information Security, vol. 2, no. 1, **(2012)**, pp. 49-57.
[17] H. T. Yau, T. H. Hung and C. C. Hsieh, "Bluetooth Based Chaos Synchronization Using Particle Swarm Optimization and Its Applications to Image Encryption", Sensors, vol. 12, no. 12, **(2012)**, pp. 7468-7484.
[18] K. D. Rao, K. P. Kumar and P. V. M. Krishna, "A New and Secure Cryptosystem for Image Encryption and Decryption", IETE Journal of Research, vol. 57, no. 2, **(2011)**, pp. 165-171.
[19] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh and M. R. Mosavi, "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process", Multimedia Tools and Applications, vol. 71, no. 3, **(2014)**, pp. 1469-1497.
[20] S. M. Wadi and N. Zainal, "High Definition Image Encryption Algorithm Based on AES Modification", Wireless Personal Communications, vol. 79, no. 2, **(2014)**, pp. 811-829.
[21] I. Hussain, T. Shah, M. A. Gondal and H. Mahmood, "A novel image encryption algorithm based on chaotic maps and GF(2 8) exponent transformation", Nonlinear Dynamics, vol. 72, no. 1, **(2013)**, pp. 399-406.

Authors

Cai Yang, female, lecturer. Her research interests include graphic image processing and pattern recognition.

Haiyu Zhang, female, lecturer. Her research interests include Intelligent algorithm and data mining.

Jinliang Guo, male, associate professor. His research interests include graphic image processing and algorithm design.

Songhao Jia, male, lecturer. His research interests include graphic image processing and network information processing.

Fangfang Li, female, lecturer. Her research interests include Data encryption and image processing.

 Copyright ⓒ 2016 SERSC