Hindawi Publishing Corporation
Journal of Sensors
Volume 2016, Article ID 2646205, 7 pages
http://dx.doi.org/10.1155/2016/2646205

*Research Article*

# A Novel Encryption Algorithm Based on DWT and Multichaos Mapping

**Wei Wang,[1] Haiyan Tan,[1] Yu Pang,[1] Zhangyong Li,[1] Peng Ran,[1] and Jun Wu[2]**

[1]*Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
[2]*Chongqing Kaize Technology Co. Ltd., Chongqing 400042, China*

Correspondence should be addressed to Yu Pang; pangyu@cqupt.edu.cn

Received 21 December 2015; Revised 17 March 2016; Accepted 28 March 2016

Academic Editor: Valerio Bellandi



Encryption of a digital image is very important especially in applications of body area networks (BANs) since the image may include a number of privacy. Past encryption methods have disadvantages of the small key space and low ability of resistance to attack. In this paper, we propose a new encryption algorithm based on discrete wavelet transform (DWT) and multichaos which has characteristics of the deterministic, pseudorandomness, and sensitivity of initial values. The image is first decomposed and spatial reconstructed by two-dimensional DWT and then is performed by multichaos matrices for space encryption. The experimental results indicate that the proposed algorithm has a large key space, high key sensitivity, and excellent ability of resistance to attack.

## 1. Introduction

In recent years with the rapid development of Internet and wireless sensor networks, data such as images and texts generally require encryption. For example, BANs play a significant role in remote medical monitoring which use many sensors surrounded with a human body [1]. The information is private and only utilized by authorized agencies, so encryption of the information is necessary. How to guarantee the safety of the multimedia information becomes a new direction of computer cryptography. Image network interaction is applied in many fields such as military cooperation, finance, and scene monitoring. Since images have some characteristics of large data, redundancy, correlation, and format consistency, image encryption has become a concerned topic [2].

Traditional image encryption techniques have caused concern. For instance, the methods of one-dimensional, two-dimensional, frequency domain, and hybrid encryption obtain abundant achievements. The technology of one-dimensional image encryption includes DES and AES as the representative of the modern cryptography system, S-box encryption, and SCAN language encryption, matrix transformation encryption, and DNA computation system [3–8]. These above spatial methods have advantages of fast calculation and easy implementation.

Chaos is a kind of unpredictable and similar random motion sensitive to initial values in a deterministic dynamical system. The pseudorandom sequence generated by chaotic map has good randomness, correlation, and complexity, which includes unique cryptography characteristics, so its derivative of the super chaotic map is widely used in the field of image encryption. The paper [9] is of significance in the literature to introduce a chaotic encryption algorithm with a diffusion sequence for applications of nonlinear functions. The contribution of the paper [10] is to implement the Baker chaotic map and sequence encryption. In past chaotic image encryption algorithms, the problem of subkey security exists in the papers [11–13] in the key analysis scheme of the paper [14] and the paper [15] adopts logistics chaotic encryption scheme with higher security than that of the papers.

The transform domain image encryption technology uses Fourier transform (FT), discrete cosine transform (DCT), and discrete wavelet transform (DWT) to perform conversion from spatial domain to transform domain and safely encrypt obtained coefficients; that is, the image is encrypted by changing the values or positions of the coefficients [16–20]. The paper [21] performs multilayer wavelet decomposition for the image and implements frequency domain scrambling in each block of every layer. This technique leads to the decrypted lossless image which becomes the key to be applied

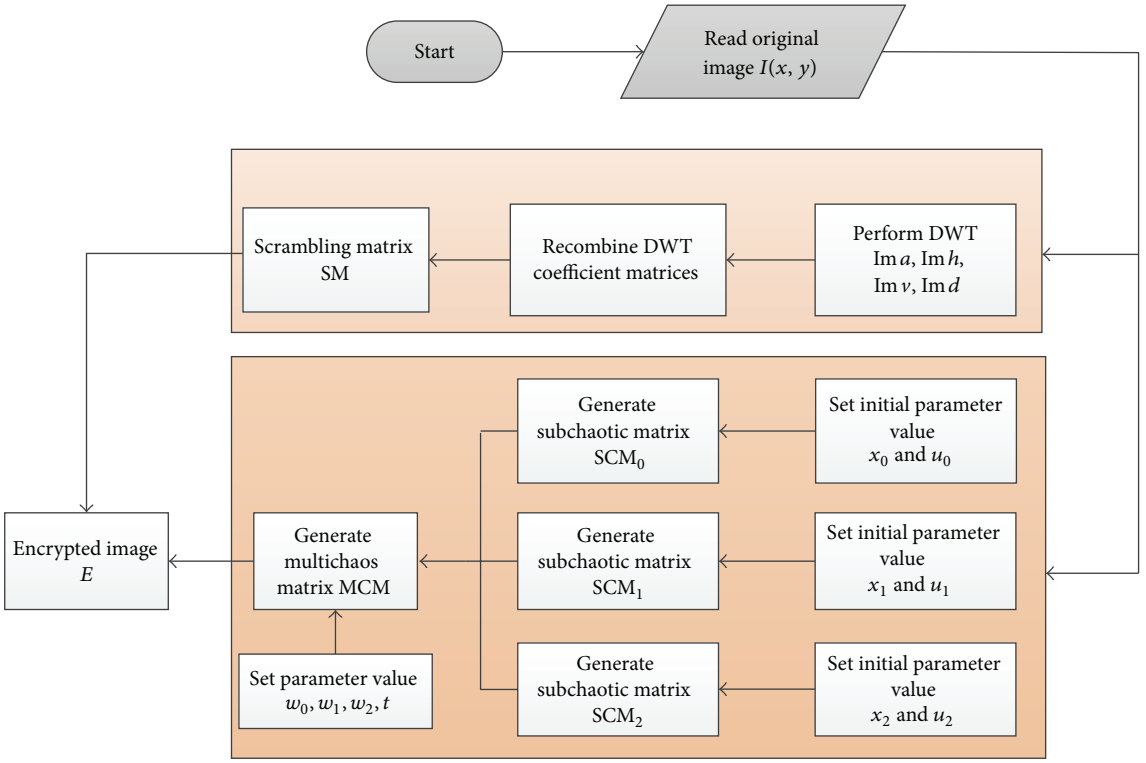



Figure 1: The flow of the proposed algorithm.

in frequency domain image encryption. The unique characteristics of chaos usually combine with the transform domain encryption mode to form mixed encryption algorithms with more advantages. Liu et al. [22] present a novel confusion and diffusion method, which generates a new key according to the original image and key and then uses piecewise linear chaotic map and Chebyshev chaotic map for DNA coding. Zhang et al. [7] code the original image to obtain a DNA sequence matrix, divide the matrix into several blocks, and finally use DNA computation combined with two logistic chaotic maps to achieve the goal of encryption.

In this paper, we take advantages of chaotic mapping and combine Haar wavelet to design the algorithm structure by a composite form of coefficient transform and multichaos. The proposed algorithm is sensitive to the initial state and system parameters with large key space and has low calculation complexity and high capability against attacks.

## 2. Theoretical Analysis of the Encryption Algorithm

*2.1. The Algorithm Flow of Image Encryption.* The steps of the algorithm are described as follows (as illustrated in Figure 1):

(i) Read the original image.

(ii) Perform DWT to obtain coefficient matrices Im $a$, Im $h$, Im $v$, and Im $d$.

(iii) Recombine the four matrices to obtain the scrambling matrix SM.

(iv) Set initial parameter values of $x_0$, $x_1$, $x_2$, $u_0$, $u_1$, $u_2$ to generate three subchaotic matrices $SCM_0$, $SCM_1$, and $SCM_2$.

(v) Set parameter values of $w_0$, $w_1$, $w_2$, and $t$ combining the above three subchaotic matrices to generate the multichaos matrix MCM.

(vi) Perform BitXOR operation of the scrambling image SM and multichaos matrix MCM to obtain the final encrypted image $E$.

*2.2. Multiscale Wavelet Decomposition in Two-Dimensional Images.* First, we transform the original image from time domain to wavelet domain using multiscale wavelet analysis, which is founded by the theory of function space. The multiscale decomposition of a two-dimensional gray image $I(x, y)$ is shown as follows:

$$\begin{aligned} \operatorname{Im} a &= \langle I(x, y), \phi(x - 2m, y - 2n) \rangle \\ \operatorname{Im} h &= \left\langle I(x, y), \Psi^1(x - 2m, y - 2n) \right\rangle \\ \operatorname{Im} v &= \left\langle I(x, y), \Psi^2(x - 2m, y - 2n) \right\rangle \\ \operatorname{Im} d &= \left\langle I(x, y), \Psi^3(x - 2m, y - 2n) \right\rangle. \end{aligned} \tag{1}$$

Here the Haar wavelet is used by one layer of decomposition to process the picture because the reconstruction has lossless feature. Different frequency coefficient matrices Im $a$, Im $h$, Im $v$, and Im $d$ are obtained by the decomposition. The image size is $M \times N$, $\phi(x, y)$ is the two-dimensional

scale function, and $\Psi(x, y)$ is the wavelet functions for corresponding positions. The initial encryption image $E$ is obtained by recombining each layer coefficient matrix:

$$\mathrm{SM} = \begin{bmatrix} \mathrm{Im}\, a & \mathrm{Im}\, h \\ \mathrm{Im}\, v & \mathrm{Im}\, d \end{bmatrix}. \tag{2}$$

Then we perform the multichaos operation for the initial encryption matrix $E$. The multichaos encryption matrix comes from subchaos matrices. The chaos mapping is the key of generating the subchaos matrices, which is a one-dimensional logistics mapping with characteristics of initial value sensitivity, parameter sensitivity, state ergodic property, and hybrid similarity stochastic:

$$l_n = \mu * l_{n-1}\left(1 - l_{n-1}\right). \tag{3}$$

$l_n$ represents the logistics chaotic mapping value in the pixel $(i, j)$ by iteration. When the parameter $\mu = [3.5699456, 4]$, $l_0 \in (0, 1)$, and $n \in N$, $l_n$ is in chaotic state. Given different initial values of $l_0$ and $\mu$, we can obtain three chaotic matrices $\mathrm{SCM}_0$, $\mathrm{SCM}_1$, and $\mathrm{SCM}_2$ generated by traversing each pixel to calculate the three different chaotic sequences $\{l_n\}$. Please note that the number of subchaotic matrices determines the time complexity of the algorithm. Using more subchaotic matrices may lead to higher encryption performance but the improvement is very limited by evaluation, so here only choosing three subchaotic matrices to form the multichaotic matrix is a good balance considering complexity and performance.

The multichaos encryption matrix MCM is calculated by the regulation parameters and three chaotic matrices:

$$\begin{aligned} \mathrm{MCM}(i, j) = {} & W_0 (1 - t)^2 \mathrm{SCM}_0(i, j) \\ & + 2W_1 (1 - t) \mathrm{SCM}_1(i, j) \\ & + W_2 t^2 \mathrm{SCM}_2(i, j). \end{aligned} \tag{4}$$

Here $W_0$, $W_1$, $W_2$, $t$ are matrix regulation parameters and all belong to the range $(0, 1)$. It is worth noting that they only participate in the generation of the multichaos matrix and so have little effect on the key space. Finally, the encrypted image $E$ is obtained by

$$E = \mathrm{MCM}\#\mathrm{SM}. \tag{5}$$

Here the symbol "#" means the BitXOR operation.

The wavelet decomposition and reconstruction can effectively scramble the original image and largely cause pixel change compared to the Fourier transform and discrete cosine transform, while keeping the advantage of fast calculation because of only one layer performed. Here we use three logistic chaotic mapping with different initial conditions to generate three independent pseudorandom sequences leading to subchaotic matrices, so the created multichaotic matrix can resist the iterative attack from chaotic systems and have obvious advantages compared to classical chaos. Combining multiple chaotic systems can obtain more complex dynamic characteristics and become difficult to predict since the application of the multichaotic matrices enhances the average changing intensity and sensitivity of initial parameter values. By mixing the wavelet transform and multichaos, the proposed method more excellently resists various attacks which can satisfy safety requirements of digital images and also the time complexity is acceptable.

## 3. Experimental Results and Analysis

To help investigate the security performance of the proposed algorithm, a program is developed and run on a 4 G memory, 3.2 GHz Intel(R) Core(TM) i5-4570 machine under Windows 8. The experimental data comes from the authoritative image database and we choose the image Lenna.jpg which can test each processing algorithm because it mixes detail, smooth area, shadow, and texture.

*3.1. Visual Results Display.* We compare the original image and encrypted image according to evaluation criteria [26]. The display results and the pixel histograms are shown, respectively, in Figures 2 and 3. The encrypted image in Figure 2(b) is completely different with the original and cannot be distinguished. The histogram of the original image exists in a narrow area (40–220) shown in Figure 3(a) and obviously has several maximum values in 50, 100, and 150. The histogram of the encrypted image in Figure 3(b) has wider distributed area and smooth values which means the characteristics of the image are covered up well.

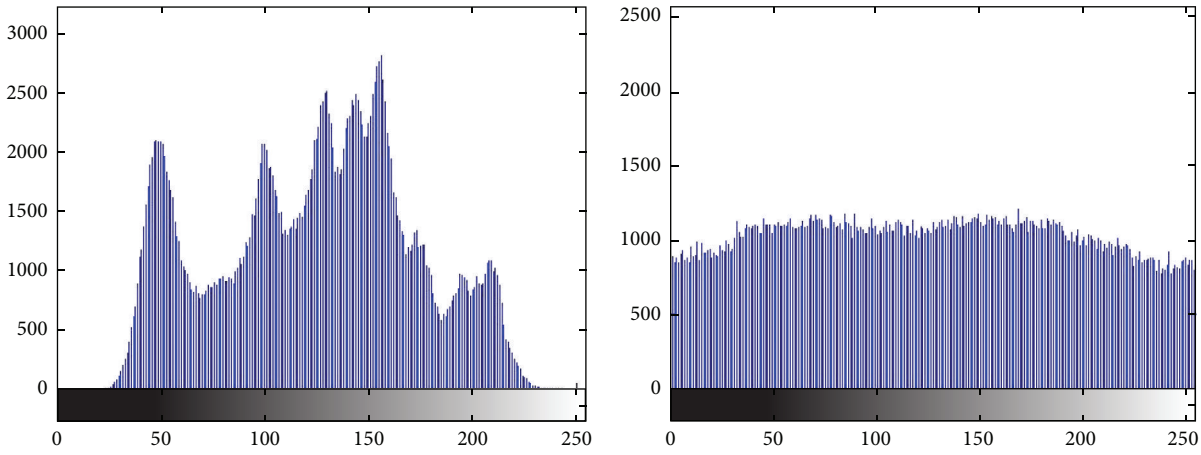
*3.2. Analysis of Quantitative Results.* The most difference between image data and text data is that image data has strong correlation and a number of adjacent pixels have the same gray values or very small difference. If a data point and its adjacent data point still keep adjacent positions after scrambling, they are easy to be attacked by area analysis leading to low security. Adjacent elements include pixel in horizontal and vertical direction as well as diagonal direction. The correlation of adjacent elements is calculated as

$$\begin{aligned} \gamma &= \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \\ \mathrm{cov}(x, y) &= \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right), \\ D(x) &= \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2, \\ E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i. \end{aligned} \tag{6}$$

Here $x_i$ and $y_i$ represent gray values of two adjacent pixels and $N$ is the pixel number. In Table 1, the correlations in three directions are all beyond 0.9 that denotes that adjacent pixels have very similar gray values before encryption, while they decrease to under 0.01 after encryption, which means the much smaller correlation can make better resistance attack.

(a) The original image (b) The encrypted image

Figure 2: The encryption effect of the proposed algorithm.




(a) The histogram of the original image (b) The histogram of the encrypted image

Figure 3: The original and encrypted statistical histograms.

Table 1: The correlation comparison before and after encryption of the image Lenna.jpg.

| Correlation | Horizontal | Vertical | Diagonal |
|---|---|---|---|
| Before encryption | 0.9388 | 0.9633 | 0.9417 |
| After encryption | 0.0005 | −0.0003 | 0.0085 |

The goal of image encryption makes the encrypted image and original image as different as possible and hard to recognize. Obviously, the less fixed point ratio between two images represents more difference of the two images and better scrambling effect. The number of pixels change rate (NPCR) is defined as follows:

$$\text{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{MN} \times 100\%. \quad (7)$$

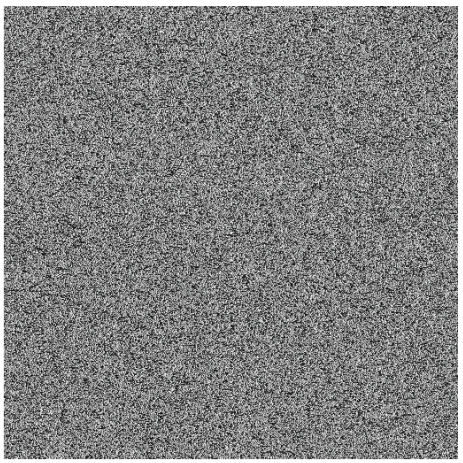
$D(i, j)$ is the gray value difference of the original and encrypted images in the pixel $(i, j)$.

Gray values of many pixels may change after encryption, so NPCR plays a good indicator to reflect the gray value change in number but noneffective to express the degree of gray value change. The average gray value change is necessary for evaluation. We give the definition of the unified average changing intensity (UACI):

$$\text{UACI} = \frac{1}{M \times N}\left[\sum_{i,j}\frac{|I(i,j) - E(i,j)|}{255}\right] \times 100\%. \quad (8)$$

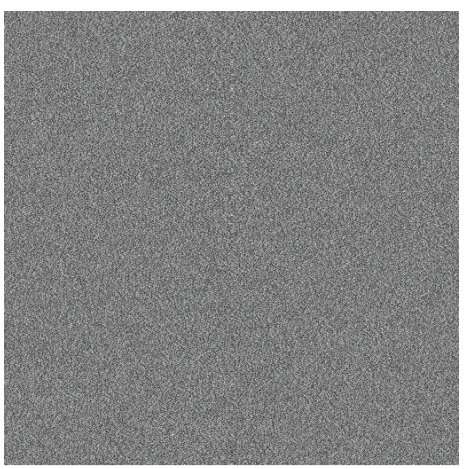
Here $I(i, j)$ and $E(i, j)$ represent the gray values of the original and encrypted images in the pixel $(i, j)$.

Furthermore, we use information entropy of the encrypted image to evaluate the degree of the average uncertainty. When the cipher has equal probability distribution leading to the maximum entropy value "8", the ideal random feature is achieved so the encrypted image has strong average

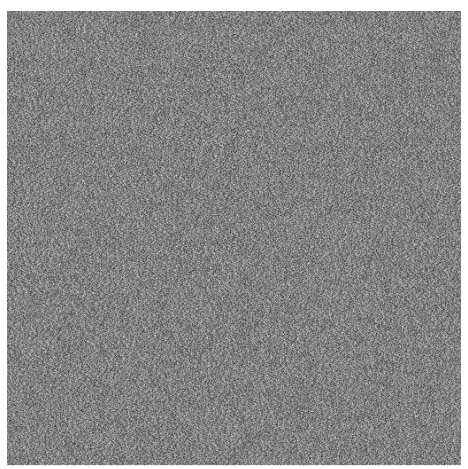


(a) The encrypted image

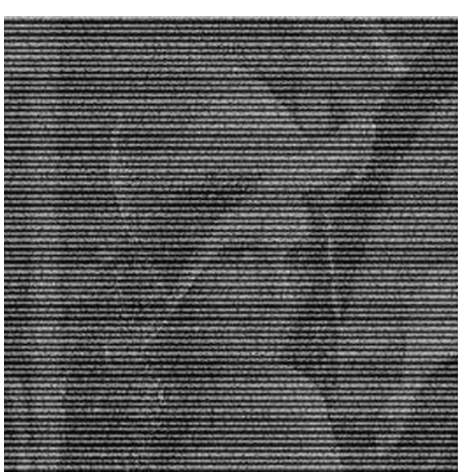
(b) The correct decrypted image



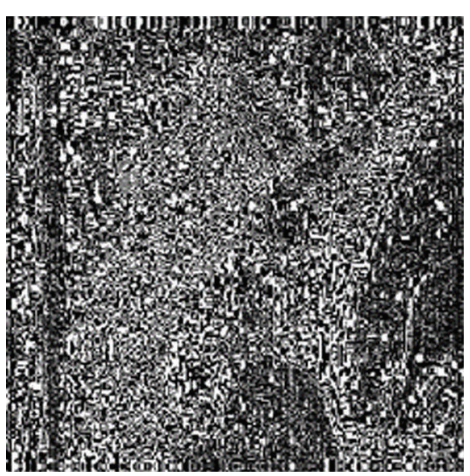
(c) The decrypted image with minor change of the parameter $\mu$



(d) The decrypted image with minor change of key initial value $x_0$



(e) The decrypted image with minor change of the parameter $w$



(f) The decrypted image with minor change of the parameter $t$

Figure 4: Test results of key sensitivity.

Table 2: The performance comparison of several algorithms.

| Indicator | NPCR | UACI | $H$ |
|---|---|---|---|
| Our algorithm | 0.9987 | 0.3338 | 7.9989 |
| The paper [23] | 0.9962 | 0.3340 | 7.9992 |
| The paper [24] | 0.9985 | 0.3301 | 7.9904 |
| The paper [25] | — | — | 7.9822 |

uncertainty and high resistance to statistical attacks and entropy attacks. The entropy of each pixel is calculated as

$$H(M) = -\sum_{i=1}^{256} P(m(i)) \log_2 P(m(i)) = 7.9889 \approx 8. \quad (9)$$

Here $P(m(i))$ represents the probability that each gray value shows.

We compare the proposed algorithm to other papers in Table 2 which all use methods of chaotic encryption. The paper [25] does not provide indicators of NPCR and UACI. Our algorithm can obtain the maximum NPCR value and the paper [23] plays best in UACI and $H$, so each of the two algorithms has its own advantages and both have better performance than the others.

*3.3. Analysis of Security Key.* The composition and size of the key space determine the security of encryption algorithms [26–28]. The proposed algorithm consists of two stages: the first stage combines two-dimensional DWT to scramble the image pixels and the second finishes pixels diffusion using multichaos. Therefore, the algorithm has various key combination forms with the parts of wavelet parameters and multichaos parameters.

We test the correct key and approximate key in the experiment of key sensitivity. The results are shown in Figure 4.

Figure 4(a) is the encrypted image and Figure 4(b) is the correct decryption image. We change parameters in the key with a very minor value ($10^{-8}$) to test sensitivity of initial values. The results in Figures 4(c) and 4(d) denote that the decrypted images cannot be distinguished and have no relation with the original image when the parameters have slight alternations. Figures 4(e) and 4(f) show the decrypted images when the parameters $w$ and $t$ are changed slightly. Obviously, these two images still maintain some features of the original image and the performance of resistance to attack is much worse than that of Figures 4(c) and 4(d). The reason is that the parameters of $\mu$ and $x_0$ need multiple iterations to form the subchaotic matrices SCM according to (3), so the slight alternation may be propagated and enlarged leading to totally confused and unpredictable results. On the contrary, the parameters $w$ and $t$ only occur in (4) to form the final multichaotic matrix, so the small change has relatively minor effect.

According to Figure 4, very small change of parameters $\mu$ and $x_0$ cause completely different results. Because of almost unlimited number of $\mu$ and $x_0$ in their ranges and considering that each subchaotic matrix has its own parameters, the key space beyond $10^{80}$ is much larger than that of classical chaos algorithms, so the proposed algorithm has stronger capability to resist exhaustive attack.

## 4. Conclusions

The proposed algorithm in this paper encrypts image pixel values and pixel locations according to basic idea of image encryption. Pixel gray change is processed by multichaos and pixel scrambling uses DWT for pixel encryption, which changes the traditional encryption idea of image resolution invariability.

The algorithm effectively hides the image size and improves the safety with advantages of large key space, sensitive to key and clear text, and easy to fast implementation. The compound chaotic system makes attackers difficult to analyze and estimate leading to high system complexity and safety. Furthermore, the algorithm has strong expansibility. Using other chaotic systems or external generators to create a key can enhance more safety of the algorithm. Dynamically setting the length of the key and packet according to the parameter adjustment is helpful to broaden serviceability of the algorithm and suitable to applications of secure communications and network security.

## Competing Interests

The authors declare that they have no competing interests.

## Acknowledgments

This project is supported by the National Science Foundation of China (Grant nos. 61471075 and 61301124), Chongqing Integrated Demonstration Project (CSTC2013jcsf10029), Chongqing Talented Youth Development Plan (cstc2013kjrc-qnrc10001), Wenfeng Innovation Foundation of CQUPT, 2013 University Innovation Team Construction Plan Funding Project of Chongqing (Smart Medical System and Key Techniques), and Chongqing Key Laboratory Improvement Plan (Chongqing Key Laboratory of Photoelectronic Information Sensing and Transmitting Technology).

## References

[1] M. Patel and J. Wang, "Applications, challenges, and prospective in emerging body area networking technologies," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 80–88, 2010.

[2] M. Xiang-Feng, C. Lu-Zhong, and Y. Xiu-Lun, "Information security system by iterative multiple-phase retrieval and pixel random permutation," *Applied Optics*, vol. 45, no. 14, pp. 3289–3297, 2006.

[3] V. M. El-Zoghdy, Y. A. Nada, and A. A. Abdo, "How good is the DES algorithm in image ciphering," *International Journal of Advanced Networking and Applications*, vol. 2, no. 5, pp. 796–803, 2011.

[4] B. Subramanyan, V. M. Chhabria, and T. G. S. Babu, "Image encryption based on AES key expansion," in *Proceedings of the 2nd International Conference on Emerging Applications of Information Technology (EAIT '11)*, pp. 217–220, Kolkata, India, February 2011.

[5] R.-J. Chen and S.-J. Horng, "Novel SCAN-CA-based image security system using SCAN and 2-D *von Neumann* cellular automata," *Signal Processing: Image Communication*, vol. 25, no. 6, pp. 413–426, 2010.

[6] V. P. Singh, R. Beg, and B. Mishra, "Practical approach on image encryption and decryption technique using matrix transformation," *MIT International Journal of Computer Science & Information Technology*, vol. 3, no. 1, pp. 38–41, 2013.

[7] Q. Zhang, L. Guo, and X. P. Wei, "Image encryption using DNA addition combining with chaotic maps," *Mathematical and Computer Modelling*, vol. 52, no. 11-12, pp. 2028–2035, 2010.

[8] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Applied Soft Computing Journal*, vol. 12, no. 5, pp. 1457–1466, 2012.

[9] J. S. A. E. Fouda, J. Y. Effa, S. L. Sabat, and M. Ali, "A fast chaotic block cipher for image encryption," *Communications in Nonlinear Science & Numerical Simulation*, vol. 19, no. 3, pp. 578–588, 2014.

[10] E. Solak, C. Cokal, O. T. Yildiz, and T. Biyikoğlu, "Cryptanalysis of Fridrich's chaotic image encryption," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 20, no. 5, pp. 1405–1413, 2010.

[11] Y. Y. Sun, R. O. Kong et al., "An image encryption algorithm utilizingMandel bot set," in *Proceedings of the International Workshop on Chaos-Fractal Theroy and Its Applications*, pp. 170–173, 2010.

[12] C.-C. Chang and T.-X. Yu, "Cryptanalysis of an encryption scheme for binary images," *Pattern Recognition Letters*, vol. 23, no. 14, pp. 1847–1852, 2002.

[13] X. J. Tong and M. R. Cui, "Image encryption with compound chaotic sequence cipher shifting dynamically," *Image and Vision Computing*, vol. 26, no. 6, pp. 843–850, 2008.

[14] C. Q. Li, S. J. Li, M. Asim, J. Nunez, G. Alvarez, and G. Chen, "On the security defects of an image encryption scheme," *Image and Vision Computing*, vol. 27, no. 9, pp. 1371–1381, 2009.

[15] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926–934, 2006.

[16] M. Mishra and P. Mishra, "Image encryption using fibonacci-lucas transformation," *International Journal on Cryptography and Information Security*, vol. 2, no. 3, pp. 131–141, 2012.

[17] A. A. Abd El-Latif, X. Niu, and M. Amin, "A new image cipher in time and frequency domains," *Optics Communications*, vol. 285, no. 21-22, pp. 4241–4251, 2012.

[18] S. Sasidharan and D. S. Philip, "A fast partial image encryption scheme with wavelet transform and RC4," *International Journal of Advances in Engineering & Technology*, vol. 1, no. 4, pp. 322–331, 2011.

[19] A. Nikolaids, "Asymptotically optimal detection for additive watermarking in the DCT and DCT Domian," *IEEE Transactions on Image Processing*, vol. 12, no. 5, pp. 563–571, 2003.

[20] Y. Liang, G. Liu, N. Zhou, and J. Wu, "Image encryption combining multiple generating sequences controlled fractional DCT with dependent scrambling and diffusion," *Journal of Modern Optics*, vol. 62, no. 4, pp. 251–264, 2015.

[21] G. Ye, "A block image encryption algorithm based on wave transmission and chaotic systems," *Nonlinear Dynamics*, vol. 75, no. 3, pp. 417–427, 2014.

[22] H. J. Liu, X. Y. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Applied Soft Computing*, vol. 12, no. 5, pp. 1457–1466, 2012.

[23] J. S. Armand Eyebe Fouda, J. Y. Effa, S. L. Sabat, and M. Ali, "A fast chaotic block cipher for image encryption," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 3, pp. 578–588, 2014.

[24] A. Jolfaei and A. Mirghadri, "An image encryption approach using chaos and stream cipher," *Journal of Theoretical and Applied Information Technology*, vol. 19, no. 2, pp. 117–125, 2010.

[25] A. H. Abdullah, R. Enayatifar, and M. Lee, "A hybrid genetic algorithm and chaotic function model for image encryption," *AEU-International Journal of Electronics and Communications*, vol. 66, no. 10, pp. 806–816, 2012.

[26] J. Ahmad and F. Ahmed, "Efficiency analysis and security evaluation of image encryption schemes," *International Journal of Video & Image Processing and Network Security*, vol. 12, no. 4, pp. 18–31, 2012.

[27] M. Su, W. Wen, and Y. Zhang, "Security evaluation of bilateral-diffusion based image encryption algorithm," *Nonlinear Dynamics*, vol. 77, no. 1-2, pp. 243–246, 2014.

[28] A. K. Selvi and D. M. M. Sathik, "Efficiency analysis and security evaluation of block based image encryption schemes," *Digital Image Processing*, vol. 7, no. 1, 2015.