Image encryption algorithm based on chaotic mapping and Chinese remainder theorem

Cai Yang

School of Computer and Information Technology,
Nanyang Normal University,
Nanyang 473061, Henan, China

Min Hua

Department of Computer Science,
Xinyang College of Agriculture and Forestry,
Xinyang 464000, Henan, China

Songhao Jia

School of Computer and Information Technology,
Nanyang Normal University,
Nanyang 473061, Henan, China

Abstract
When the image data are regularly changed, existing image encryption algorithm is easy to be decrypted. In order to improve the security of encryption algorithm, this paper proposes an image encryption algorithm based on chaotic mapping and Chinese remainder theorem. The encryption algorithm is divided into pixel scrambling and image diffusion. Firstly, the Chebyshev mapping is used to generate a chaotic sequence, which is used to scramble the image pixel bit value. Then, the pixel position is scrambled by formula. Finally, the scrambled image is substantially changed by the application of the Chinese Remainder Theorem and Fibonacci series. Simulation results show that, compared with other typical encryption algorithm, the proposed encryption algorithm has better effect on the key sensitivity, histogram statistics, information entropy analysis and correlation analysis.

Key words: CHEBYSHEV CHAOTIC MAPPING, CHINESE REMAINDER THEOREM, FIBONACCI SERIES, PIXEL SCRAMBLING, IMAGE DIFFUSION

Introduction

With the development of Internet, more multimedia information have been stored and transmitted. Having the characteristics of intuition and vividness, image transmissions hold a high proportion. In the case of convenience to the people, the security problem of image information transmission is more and more outstanding. Because the image has a large amount of data and higher characteristic correlation, traditional encryption methods such as DES, RSA has low efficiency on image encryption. How to ensure the safety of the transmission of image data is the current research hotspot.

Many scholars and experts have studied on image encryption, and presented a lot of encryption algorithms. K. Deergha Rao et al proposed a new secure cryptosystem based on the BB equation and chaos for image encryption and decryption. Cryptanalysis of the proposed cryptosystem was also provided [1]. Amnesh Goel and Nidhi Chandra introduced a new image encryption method which first rearranges the pixels within image on basis of RGB values and then forward intervening image for encryption [2]. Mrinal Kanti Mandal et al proposed a high security image encryption technique using logistic map. The proposed image encryption algorithm was described in detail along with its security analysis such as key space analysis, statistical analysis and differential analysis [3]. Discrete wavelet transform and Modified Chaotic Key-Based Algorithm were proposed to enhance the security of CKBA. The enhanced security of the proposed algorithm was analyzed through cryptanalysis [4]. A permutation technique based on the resolution of the system of three independent Diophantine equations was presented. From this permutation algorithm, an efficient chaos-based block cipher using a chaotic logistic map was proposed [5]. Himan Khanzadi et al proposed an algorithm for image encryption using the random bit sequence generator and based on chaotic maps. Chaotic Logistic and Tent maps were used to generate required random bit sequences [6].

Through the change of pixel data or position, the image encryption algorithm has obtained the certain effect. However, the image is changed too regularly. So the encrypted data is decrypted easily, which is not conducive to the safety of image transmission. This paper presents a kind of image encryption algorithm based on chaotic mapping and Chinese remainder theorem (CMCRT-IEA). The Chebyshev chaos mapping is used to scramble pixel bit value. So the pixel value is changed. At the same time, the pixel position is changed by a certain rule, which completely disrupted the original distribution. Finally, the image data is encrypted by Chinese Remainder Theorem and Fibonacci series, which further change the value of the image data and position. Through the CMCRT-IEA algorithm, bit values of image are completely changed. Because the algorithm does not use fixed rules to change image, the security of image data transmission has been greatly improved.

2. Basic Knowledge

2.1. Chebyshev chaos mapping

Chebyshev sequence is a one-dimensional chaotic mapping and the iterative equation is simple and easy to realize [7]. The k order Chebyshev mapping expression is present as in Eq. (1).

$$x_{n+1} = \cos(\mathrm{k} \times \arccos(\mathrm{x}_n)) \qquad (1)$$

In this equation, the valid value of x_n is between -1 and 1. When k>=2, the system enters chaotic state.

2.2. Chinese remainder theorem

The Chinese remainder theorem is a kind of method to solve a set of linear congruences, and it is an important theorem in number theory. The main contents are as follows.

Assume that $m_1, m_2, \cdots m_n$ are n mutual prime number integers, for any given n integers: $a_1, a_2, \cdots a_n$ (n>=2), Eq. (2) has unique solution.

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad\vdots \\ x \equiv a_n \pmod{m_n} \end{cases} \qquad (2)$$

The unique solution is shown as in Eq. (3).

$$x \equiv M_1 M_1^{-1} a_1 + M_2 M_2^{-1} a_2 + \cdots + M_n M_n^{-1} a_n \pmod{m} \quad (3)$$

In the formula, M_i^{-1} is the number of M_i inverse modulo m_i. At the same time, the formula meets $M_i\ M_i^{-1} \equiv 1$ (mod m_i), i=1, 2…n. The m value meets $m=m_1 \times m_2 \times \ldots \times m_k$, $m=M_i m_i$, i=1, 2… n.

2.3. Fibonacci sequence

Fibonacci sequence is a group of regular integer values. The rule is shown as in Eq. (4).

$$F(n) = \begin{cases} 1 & n \le 2 \\ F(n-1) + F(n-2) & n > 2 \end{cases} \qquad (4)$$

In the formula, F(n) represents the Fibonacci Series value when the parameter is n.

3. The Idea of the CMCRT-IEA Algorithm

The CMCRT-IEA algorithm is consists of two processes, image scrambling and image diffusion. Image scrambling includes bit value scrambling and pixel position scrambling. In the image diffusion stage, the Chinese remainder theorem and Fibonacci sequence are used to completely change the image pixel values [8-10].

3.1. Bit value scrambling

A plain image can be used to indicate by a matrix M, which has h rows and w columns. The height of the plain image is h, and the width is w. Each element in the M is represented by an integer between 0 and 255. Each pixel consists of 8 bit bytes, and pixel scrambling refers to change the 8 bit value. Detailed steps are as follows.

Step 1: The plain image is converted to a one-dimensional sequence $A=\{A_1,A_2,\cdots A_{8\text{h}\times\text{w}}\}$. Each pixel A_i is represented as an 8 bit binary sequence $b_i=\{b_{i1},b_{i2},\cdots b_{i8}\}$.

Step 2: Through the Chebyshev chaos mapping, a length $(\text{t}+8\text{h}\times\text{w})$ of chaotic sequence is generated. In order to ensure the chaos sequence, the first t number is discarded. So a new chaotic sequence is obtained, which is expressed as $X=\{X_1,X_2,\cdots X_{8\text{h}\times\text{w}}\}$. Among them, t is a constant, h and w said the plain image width and height.

Step 3: The 8 numbers are randomly selected from the chaotic sequences X. The 8 numbers are expressed as $Y_i=\{Y_{i1},Y_{i2},\cdots Y_{i8}\}$. The choice of Y_i is not the same each time.

Step 4: Y_i is sorted in ascending order and a new sequence $Y_i^{'}$ is obtained. At the same time, an index sequence T_i can be got, which is expressed as $T_i=\{t_1,\text{t}_2,\cdots t_8\}$. Among them, t_i said the position in Y_i of first i number in $Y_i^{'}$. For example, if t_1=3, which says the $Y_i^{'}$ first number is the third number in Y_i.

Step 5: According to the T_i value, the b_i is converted to a bit sequence $c_i=\{c_{i1},c_{i2},\cdots c_{i8}\}$. Transformation rule is shown as in Eq. (5).

$$c_{ij}=b_{i\,t_j} \qquad (5)$$

Step 6: All element in sequence A are executed step 3, step 4 and step 5. So, the bit sequence C can be obtained, which length is $8h\times w$. C is expressed as $C=\{c_1,c_2,\cdots c_{\text{h}\times\text{w}}\}$.

Step 7: Each 8 bit value in sequence C is converted to an integer. A size of $h\times w$ pixel matrix M_2 is got.

In step 2, the initial value of Chebyshev mapping is set to k=4, x_0=0.123456.

3.2. Pixel position scrambling

Through the above algorithm, pixel scrambling changes pixel values. However, pixel location information has not been changed, which brings hidden trouble to the safety of image data. It is necessary to change the position information of pixel, so as to improve the effect of image data encryption. Specific steps are as follows.

Step 1: First, the element in M_2 matrix is expressed as M_2 (i, j). Among them, the variable i represents the row, and the variable j represents the column. 1<=i<=h, 1<=j<=w.

Step 2: The position of i row elements are changed, and the rule is shown as in Eq. (6).

$$j^{'}=(\text{i}+\text{j}) \bmod w \qquad (6)$$

The transformed column is expressed as $j^{'}$

Step 3: The variable i takes all values between 1 and h. Then, step 2 is executed.

Step 4: The position of j column elements are changed and the rule is shown as in Eq. (7).

$$i^{'}=(\text{h}-\text{i}+\text{j}) \bmod h \qquad (7)$$

The transformed row is expressed as $i^{'}$.

Step 5: The variable j takes all values between 1 and w. Then, step 4 is executed.

After the above steps are executed, the scrambling matrix M_s is got.

3.3. Image diffusion

Through change the value and location of each pixel, a certain effect of encryption has obtained. However, a considerable part of the plaintext information has not been hidden, and the encryption effect is not ideal [11-13]. In the CMCRT-IEA algorithm, scrambling image is diffused by Chinese remainder theorem and Fibonacci sequence. In this stage, the steps are as follows.

Step 1 : k integers are randomly selected, which are expressed as m_1,m_2… m_k. Among them, the following equation must meet the conditions: $\gcd(\text{m}_i,\text{m}_j)=1$, $i\in[1,\text{k}]$, $j\in[1,\text{k}]$. Scrambling of gray value is converted to a one-dimensional sequence $D=\{D_1,D_2,\cdots D_{\text{h}\times\text{w}}\}$.

Step 2: The k elements are taken from Fibonacci sequence, which form an index sequence $I=\{F(2),\text{F}(3),\cdots F(\text{k}+1)\}$. According to the values in the sequence I, k elements are taken from D, which form a new sequence $B_i=\{D_{F(2)},D_{F(3)},\cdots D_{F(\text{k}+1)}\}$. The next element $D_{h\times w}$ is assumed D_1, that is to say that D is cyclic. In this way, the $(h\times w)/k$ sequences can be got and the number of each sequence element is k.

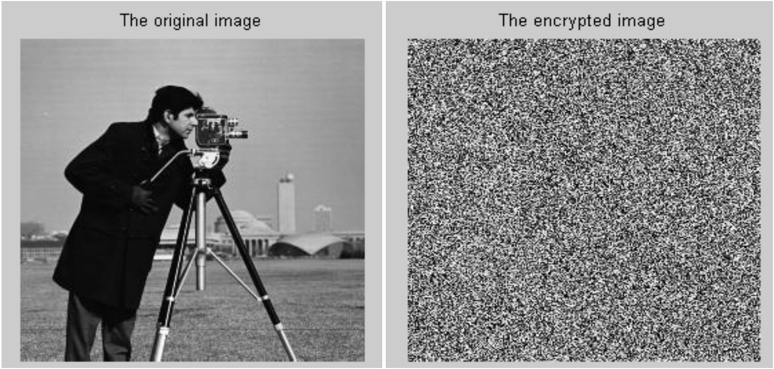
Step 3: Sequence B_i is encrypted into an integer T_i through Chinese remainder theorem. Among them, the range of variable i is between 1 and $(h\times w)/k$. The temporary sequence T is got, which is expressed as $T=\{T_1,T_2,\cdots T_{(\text{h}\times\text{w})/\text{k}}\}$.

Step 4: For each element T_i in sequence T, the final encryption sequence $E=\left\{E_1,E_2,\cdots E_{(h\times w)/k}\right\}$ are got by the formula $E_i=T_i \bmod 256$.

The sequence E can be transformed into a two-dimensional image matrix. Thus the final encrypted image is got.

4. Experimental results and analysis

In the simulation process, Cameraman is chose to evaluate the algorithm performance. The experiment platform is shown as follows [14-16]. The Simulation software is Matlab 2010.

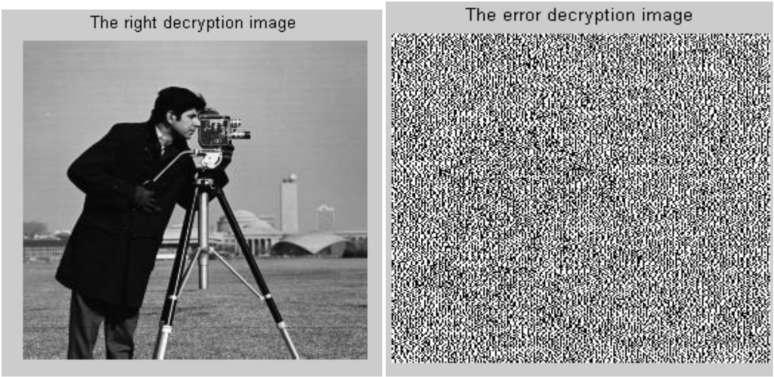


(a) The original image (b) The encrypted image

Figure 1. The encrypted image contrast

4.1. Sensitivity analysis of the key

Decryption is the inverse of the encryption process. In the internal pixel image scrambling, the key is set to k=4, x_0=0.123456. The original image and encrypted image by the CMCRT-IEA algorithm are contrasted as shown in Figure 1. When the decryption key and encryption key is the same, the right decryption image is got. When the decryption key is set to k=4.000001, x_0=0.1234561, decryption image is obtained as shown in Figure 2(b).



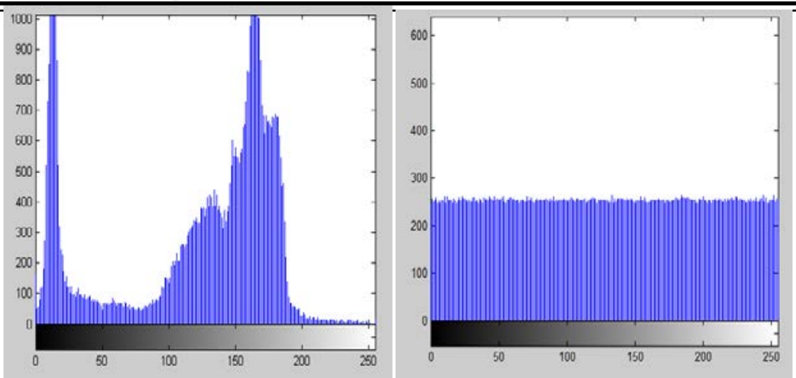
(a) The right decryption image (b) The error decryption image

Figure 2. Decryption result comparison

It can be seen from Figure 2, in the process of decryption, the decryption image and original image are different when key slightly changes. This shows that the CMCRT-IEA algorithm is highly sensitive to the key.

4.2. Statistical characteristic analysis

The image gray histogram is a distribution map, which can reflect the distribution of pixel values [17-19]. X-axis parameters are the gray values. And y-axis parameters are the number of the gray value. Plaintext and ciphertext image histogram are shown as Figure 3. It can be seen that the uneven pixel values distribution of original image is become uniform distribution by the CMCRT-IEA algorithm.



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

Figure 3. Histogram analysis

Figure 3 (b) shows that pixel value of the cipher image in the range of [0, 255] basically present uniform distribution, the correlation of ciphertext is greatly reduced. The cryptanalyst cannot get any information about plaintext from the encrypted image histogram. Therefore, the encrypted image can resist the attack of statistical characteristic analysis.

4.3. Information entropy analysis

Information entropy is one of the important indexes of sequence random properties. If the information entropy is bigger, the random sequence has better performance [20]. The information entropy is expressed in Eq. (8).

$$H(S) = -\sum_{i=0}^{n} p(s_i)\log_2 p(s_i) \qquad (8)$$

In the formula, S = (s_0, s_1… s_n) said the source of information. H (S) said the information entropy of S. p(s_i) represents the appear probability in the sequence of s_i point.

The ciphertext information entropy of some images is shown in Table 1. And these images are encrypted by the CMCRT-IEA algorithm. The ciphertext information entropy of Cameraman image is shown in Table 2, which is encrypted by different encryption algorithms. It can be seen from the table that ciphertext information entropy of the CMCRT-IEA algorithm is closer to the ideal value 8 than literature [1] and literature [3]. This shows that the CMCRT-IEA algorithm can resist information entropy statistical attack, and has better performance of encryption.

Table 1. Information entropy of ciphered images

Image	Information entropy
Lena	7.99972
Couple	7.99966
Boat	7.99983
Cameraman	7.99978

Table 2. Information entropy of ciphered Cameraman image

Encryption algorithm	Information entropy
Literature [1]	7.9932
Literature [3]	7.9946

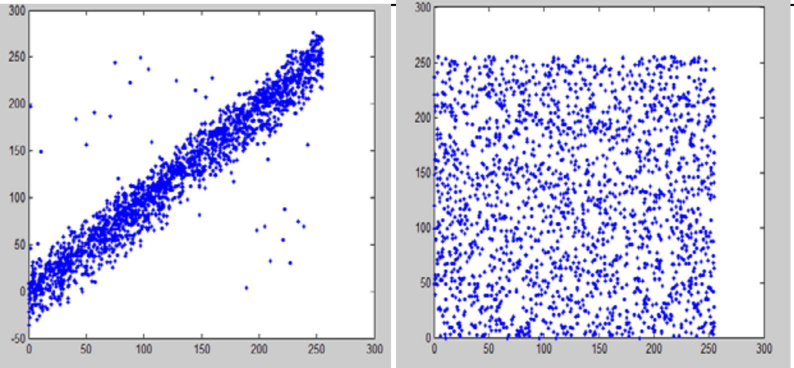
4.4. Analysis of the correlation between adjacent pixels

Because the plain image gray value is generally continuous, the correlation between adjacent pixels is high. For good encryption algorithm, the correlation between the adjacent pixels of cipher image should be lower [21]. Correlation of adjacent pixels is done quantitative analysis with the Eq. (9).

$$r_{xy} = \frac{E((x-E(x))(y-E(y)))}{\sqrt{D(x)D(y)}} \qquad (9)$$

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.

In the horizontal, vertical and diagonal directions, the 2000 gray values are randomly selected to compare the correlation between pixels. In the diagonal direction, the correlation between adjacent pixels plaintext and ciphertext is shown as Figure 4.



(a)The plain image scatter diagram (b) The ciphered image scatter diagram

Figure 4. The diagonal direction of the scatter diagram

Compared with the literature [1] and [3], the results of operations are shown as Table 3. It can be seen that correlation between adjacent pixels of the original image is high, and the value is close to 1. The correlation coefficient of the encrypted image is close to 0. This suggests that the correlation of the encrypted image is greatly reduced. Compared with encryption algorithms in Literature [1] and Literature [3], the correlation coefficient of the CMCRT-IEA algorithm is the least. This shows that the CMCRT-IEA algorithm has the better performance in the aspect of resist the correlation.

Table 3. The correlation coefficient between the plaintext and ciphertext image

Direction	Plaintext image	CMCRT-IEA	Literature [1]	Literature [3]
Horizontal	0.9215	0.0129	0.0168	0.0150
Vertical	0.9538	0.0135	0.0153	0.0167
Diagonal	0.9032	0.0092	0.0129	0.0124

Conclusions

In order to improve the effect of image encryption algorithm, this paper has proposed an encryption algorithm of pixel level image based on chaotic mapping and Chinese remainder theorem. The image scrambling and diffusion image are combined in the algorithm. The Chebyshev chaotic mapping is introduced in the process of scrambling, and Chinese remainder theorem is introduced to diffuse image. The CMCRT-IEA algorithm not only retains the merits of the "scrambling-diffusion" algorithm, but also overcomes the shortcomings of the plaintext attack in the existing algorithms. Simulation experiment is carried out in the key sensitivity, statistical characteristics, information entropy and pixel correlation. The experiment results show that the proposed algorithm is stability and can resist correlation attack. Therefore, the algorithm is a secure image encryption algorithm and is worthy to be popularized.

Acknowledgements

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. Deergha Rao, K. Praveen Kumar, P. V. Murali Krishna (2011) A New and Secure Cryptosystem for Image Encryption and Decryption. *IETE Journal of Research*, 57(2), p.p. 165-171.
2. Amnesh Goel, Nidhi Chandra (2012) A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group-Wise Of RGB Values and Explosive Inter-Pixel Displacement. *International Journal of Image, Graphics and Signal Processing*, 4(2), p.p.16-22.
3. Mrinal Kanti Mandal, Gourab Dutta Banik, Debasish Chattopadhyay, et al. (2012) An Image Encryption Process based on Chaotic Logistic Map. *IETE Technical Review*, 29(5), p.p.395-404.

4. K. Deergha Rao, Ch. Gangadhar (2012) Discrete Wavelet Transform and Modified Chaotic Key-based Algorithm for Image Encryption and its VLSI Realization. *IETE Journal of Research*, 58(2), p.p.114-120.
5. J. S. Armand Eyebe Fouda, J. Yves Effa, Bertrand Bodo, et al. (2013) Diophantine Solutions Based Permutation for Image Encryption. *Journal of Algorithms & Computational Technology*, 7(1), p.p.65-86.
6. Himan Khanzadi, Mohammad Eshghi, Shahram Etemadi Borujeni (2014) Image Encryption Using Random Bit Sequence Based on Chaotic Maps. *Arabian Journal for Science and Engineering*, 39(2), p.p.1039-1047.
7. Daniel Caragata, Ion Tutanescu (2014) On the security of a new image encryption scheme based on a chaotic function. *Signal, Image and Video Processing*, 8(4), p.p. 641-646.
8. Ahmed A. Abd El-Latif, Li Li, Xiamu Niu. (2014) A new image encryption scheme based on cyclic elliptic curve and chaotic system. *Multimedia Tools and Applications*, 70(3), p.p. 1559-1584.
9. OsamaS. Faragallah (2012) An enhanced chaotic key‐based RC5 block cipher adapted to image encryption. *International Journal of Electronics*, 99(7), p.p. 925-943.
10. Benyamin Norouzi, Sattar Mirzakuchaki, Seyed Mohammad Seyedzadeh, et al. (2014) A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. *Multimedia Tools and Applications*, 71(3), p.p. 1469-1497.
11. Abir Awad, Abdelhakim Saadane (2010) New Chaotic Permutation Methods for Image Encryption. *IAENG International Journal of Computer Science*, 37(4), p.p. 402-410.
12. Fawad Ahmed, Amir Anees, Vali Uddin Abbas, et al. (2014) A Noisy Channel Tolerant Image Encryption Scheme. *Wireless Personal Communications*, 77(4), p.p. 2771-2791.
13. R. Huang, K. H. Rhee, S. Uchida (2014) A parallel image encryption method based on compressive sensing. *Multimedia Tools and Applications*, 72(1), p.p. 71-93.
14. Salim Muhsin Wadi, Nasharuddin Zainal (2014) High Definition Image Encryption Algorithm Based on AES Modification. *Wireless Personal Communications*, 79(2), p.p. 811-829.
15. B.K.ShreyamshaKumar, Chidamber R.Patil (2010) JPEG image encryption using fuzzy PN sequences. *Signal, Image and Video Processing*, 4(4), p.p. 419-427.
16. Morteza SaberiKamarposhti, Dzulkifli Mohammad, Mohd Shafry Mohd Rahim, et al. (2014) Using 3-cell chaotic map for image encryption based on biological operations. *Nonlinear Dynamics*, 75(3), p.p. 407-416.
17. Benyamin Norouzi, Seyed Mohammad Seyedzadeh, Sattar Mirzakuchaki, et al. (2014) A novel image encryption based on hash function with only two-round diffusion process. *Multimedia Systems*, 20(1), p.p. 45-64.
18. H.T. Panduranga, S.K. Naveen Kumar, Kiran (2014) Image encryption based on permutation-substitution using chaotic map and Latin Square Image Cipher. *The European Physical Journal Special Topics*, 223(8), p.p. 1663-1677.
19. Ibrahim S.I.Abuhaiba, Hanan M. Abuthraya, Huda B. Hubboub, et al. (2012) Image Encryption Using Chaotic Map and Block Chaining. *International Journal of Computer Network and Information Security*, 4(7), p.p. 19-26.
20. Her-Terng Yau, Tzu-Hsiang Hung, Chia-Chun Hsieh (2012) Bluetooth Based Chaos Synchronization Using Particle Swarm Optimization and Its Applications to Image Encryption. *Sensors*, 12(12), p.p. 7468-7484.
21. Saraireh, Saleh, Al-Sbou, et al. (2014) Image Encryption Scheme Based on Filter Bank and Lifting. *International Journal of Communications, Network and System Sciences*, 7(1), p.p. 43-52.