Journal of Information Hiding and Multimedia Signal Processing ©2017 ISSN 2073-4212
Ubiquitous International Volume **8**, Number **5**, September **2017**

A Fast Image Encryption System based on AES and Chaos

Chuanfu Wang, Jia Liu, Xingyu Tian, Ziheng Yang*

Electronic Engineering College
Heilongjiang University,
Harbin, China
* yzh@hlju.edu.cn

Received July 2004; revised December 2004

Abstract. *Chaos, as a new discipline, has a broad application prospect in digital image encryption. A lot of digital image encryption schemes based on chaotic systems have been proposed. But in recent years, more and more scholars come to apply the traditional encryption algorithms into digital image encryption schemes, and have achieved good results. In this paper, a new digital image encryption scheme based on block cipher and chaotic system is proposed. The results indicate that the new encryption scheme in hardware is sufficiently safe and well behaved.*
Keywords: Image encryption, Cchaotic map, AES, FPGA

1. **Introduction.** With the advent of the information age, ordinary text data has been unable to meet the needs of people's daily lives. Digital image data is paid more and more attention and widely used in various types of electronics industry. So, it is very important to guarantee the safe transmission and storage of digital image. But now, the traditional encryption algorithms are not very suitable to encrypt digital image for encrypting the correlation between pixels. To overcome this shortcoming, three major schemes about digital image encryption are proposed by many scholars. Position permutation is one of the simplest schemes to encrypt digital image.The arrangement of each pixel location is a reordering of the positions to randomly eliminate the correlation between the pixels. Digital image can be represented by a matrix of pixels. There are two major algorithms to eliminate the correlation between pixels. One algorithm [1] is to exchange any two rows in the matrix randomly in the first step. In the second step, any two columns are also exchanged randomly. The other algorithm is to circularly shift each row and column randomly. A typical representative of position permutation is two-dimensional circular encryption algorithm (TDCEA) [2]. Just as the name implies, TDCEA encrypts digital image by shifting rows and columns circularly. However, the cryptanalysis of TDCEA are put forward quickly [3]. Facts proved that the security of those position permutation algorithms is not very well. The pixels' position is changed, but the value is unchanged. So, useful information can be obtained in encrypted digital image through histogram analysis. In recent years, some algorithms called substitution-permutation is proposed [4–7]. Unlike other position permutation algorithms, S-box is applied into substitution-permutation and get good results. It indicates that the theory of block cipher is still contributed to digital image encryption [8–13]. Therefore, a new position permutation algorithm based on the round function of block cipher is put forward. Among many aspects comparison

in a variety of block ciphers, AES (Advanced Encryption Standard) round function is selected as the new position permutation algorithm finally. Value transformation is the other major scheme to encrypt digital image, which transform the value of pixels into random number for hiding useful information. Stream cipher, as a traditional encryption method, is similar to the value transformation. In order to resist differential attacks in digital image encryption, the difference between value transformation and stream cipher is that value transformation is more complex [14–19] Chaotic systems have a lot of good properties, such as the sensitive dependence on initial condition, nonlinear, ergodicity, non-periodicity. Those good properties are related to some requirements such as confusion and diffusion in cryptography. Thus, chaotic systems are wildly used in value transformation algorithms. Compared with position permutation, the security of value transformation is higher but still not enough, because position permutation and value transformation has security of digital image encryption in different aspects. In order to get enough security, a desirable scheme for digital image encryption is combination of positon permutation and value transformation. The combination form is the third major scheme to encrypt digital image, and wildly recognized by many scholars. In order to avoid above shortcomings, a new digital image encryption is proposed. The new scheme is composed of position permutation algorithm and value transformation algorithm. The round function of AES is selected as position permutation algorithm. Compare with existing position permutation algorithms, the new position permutation algorithm changes not only the position but also the value of pixels Therefore, the statistic characteristics of the image pixels under new position permutation algorithm are effectively hidden. Chaos is a special form of nonlinear dynamics system For the latest decades, the research on chaos has been an important aspect in the study of cryptography. Logistic map is very simple to implement and has a strong dynamic characteristic. Thus, Logistic map is selected as value transformation algorithm. The rest of this paper is organized as follow. In section 2, a new position permutation is proposed. Compared with other position permutation algorithms, security and the complexity of hardware implementation is analyzed. In section 3, Logistic map is applied to value transformation algorithm to improve the security, and a complete digital image encryption system is proposed. Finally, conclusions are made in section 4.

2. **Position permutation algorithm.** Block cipher is one of the traditional encryption algorithms. The design method and cryptanalysis of block cipher are mature. AES is symmetric block cipher standard, and it is widely applied to government section and commerce organization. Therefore, it is determined that AES round function has good properties of diffusion and confusion for SP structure. Compared with Feistel structure, the spread of each bit in SP structure is better. The total spread of bits can be supported by two rounds encryption of AES round function, which means each bit in ciphertext depends on all bits in plaintext. In the theory of Feistel structure, the total spread of bits can be supported by three rounds encryption. But in practice, the total spread of bits can be supported by four or more rounds. In the consideration of resource consumption, encryption speed and diffusion performance, AES round function is selected to be a new position permutation algorithm.

2.1. **AES round function.** AES round function contains four modules: SubBytes, ShiftRows, MixColumns and AddRoundKey. The diagram of AES round function as shown in Figure 1.

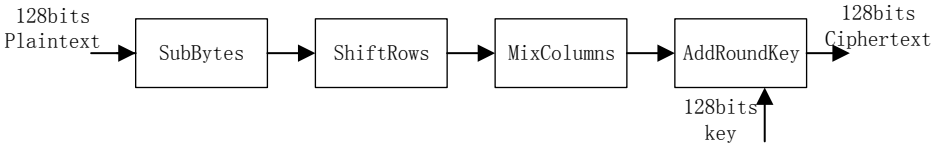


FIGURE 1. AES round function

Firstly, plaintext is divided into 4×4 matrix PT.

$$PT = \begin{bmatrix} P_{0,0} & P_{0,1} & P_{0,2} & P_{0,3} \\ P_{1,0} & P_{1,1} & P_{1,2} & P_{1,3} \\ P_{2,0} & P_{2,1} & P_{2,2} & P_{2,3} \\ P_{3,0} & P_{3,1} & P_{3,2} & P_{3,3} \end{bmatrix} \tag{1}$$

Element $P_{i,j}$ $(i, j \in (0, 1, 2, 3))$ in the matrix contains 8 bits. SubBtyes is a byte to byte map by S-box. S-box is a 16×16 matrix with each element containing 8 bits. The nonlinear transformation is represented by function symbol $S(x)$.

$$D = \begin{bmatrix} S(P_{0,0}) & S(P_{0,1}) & S(P_{0,2}) & S(P_{0,3}) \\ S(P_{1,0}) & S(P_{1,1}) & S(P_{1,2}) & S(P_{1,3}) \\ S(P_{2,0}) & S(P_{2,1}) & S(P_{2,2}) & S(P_{2,3}) \\ S(P_{3,0}) & S(P_{3,1}) & S(P_{3,2}) & S(P_{3,3}) \end{bmatrix} = \begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix} \tag{2}$$

ShiftRows is reversible linear transformation. The function symbol of ShiftRows is represented by $f(x)$

$$H = f(D) = \begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,1} & S_{1,2} & S_{1,3} & S_{1,0} \\ S_{2,2} & S_{2,3} & S_{2,0} & S_{2,1} \\ S_{3,3} & S_{3,0} & S_{3,1} & S_{3,2} \end{bmatrix} \tag{3}$$

MixColumns also is reversible linear transformation.

$$M = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} H \tag{4}$$

AddRoundKey is an exclusive or operation between key and M In order to make the key spread to each bit of the plaintext better, AddRoundKey is placed before SubBytes. The new round function is shown in Figure 2, and two rounds encryption is shown in Figure 3.

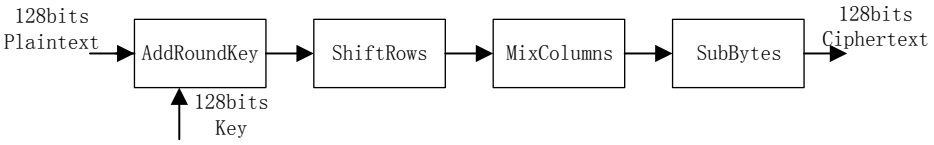


FIGURE 2. new round function

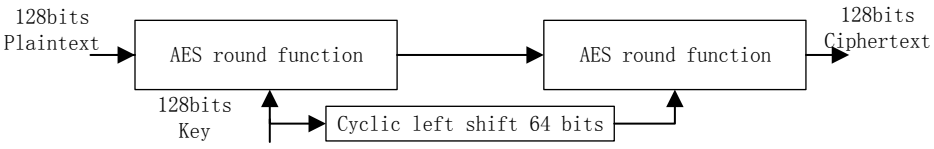


FIGURE 3. two rounds encryption

The top-level diagram of pipelined AES round function based on Field-Programmable Gate Array (FPGA) is shown in Figure 4.

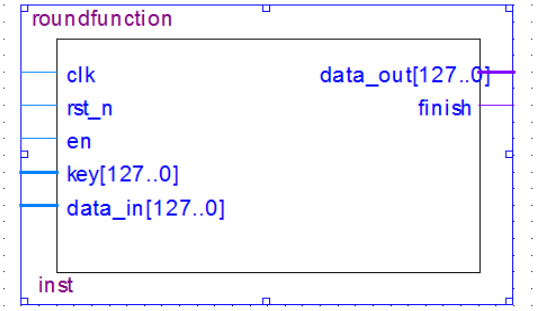


FIGURE 4. The top-level diagram of AES round function

Resource consumption and maximum frequency are shown in Table 1.

TABLE 1. Resource consumption and maximum frequency

Resource categories	One round encryption	two rounds encryption
Total logic elements	470	906
Total combination functions	468	901
Dedicated logic registers	275	421
Total logic registers	275	421
Total memory bits	32768	65536
Frequency max	155.59MHz	140M

The throughput of one round encryption and two rounds encryption can reach 2.431GB/s and 2.1875GB/s.

2.2. **Security analysis.** In this section, digital image of size 256×256 is used. Pixels of the digital image can be represented by 256×256 matrix with each element containing 8 bits. So, 16 elements in matrix are taken out to form the 128 bits input of new AES round function successively. Figure 5 show the AES round function encryption simulation results.

By comparing the (d) and (e) in Figure 5, we can see that the randomness of two rounds encryption is better. Differential cryptanalysis is a chosen plain text attack, which are wildly used in digital image encryption attack. NPCR (number of pixel change rate) and UACI (unified average change intensity) are the two major test indicators to show the strength of resistance to differential attack. The calculations of NPCR and UACI are given in section 3.2.2 in detail. Test of NPCR and UACI are shown in Table 2.

The standard value of NPCR and UACI is 99.6049% and 33.4635. So, it is obvious that the scheme has no resistance to differential attack. However, the encrypted digital image has good properties of confusion and shuffle. Compared with other position permutation

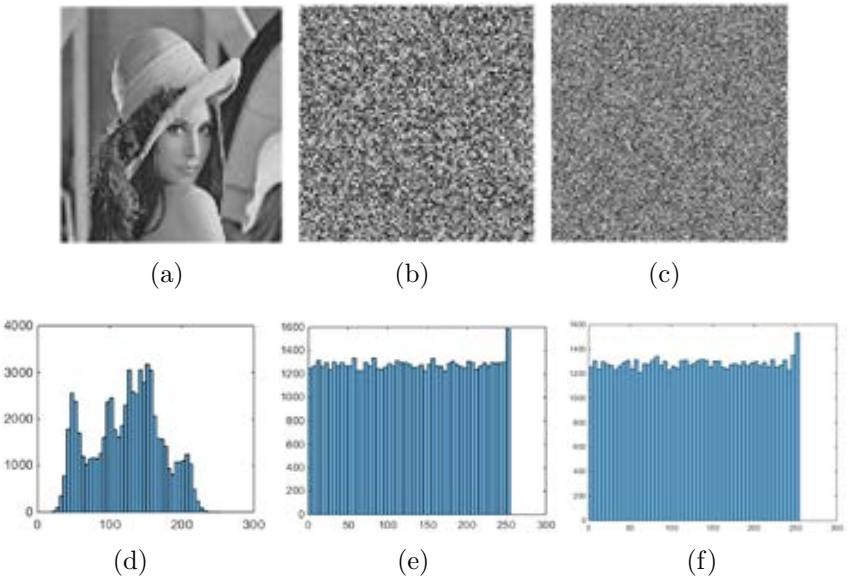


FIGURE 5. AES round function encryption. (a)original Lena image (b) cipher-image in one round encryption (c) cipher-image in two rounds encryption (d) histogram of original Lena image (e) histogram of cipher-image in one round encryption (f) histogram of cipher-image in two rounds encryption

TABLE 2. The test of NPCR and UACI

Encryption times	NPCR	UACI
One round encryption	0.061%	0.0022%
Two rounds encryption	0.024%	0.0055%

algorithms, the biggest difference is that the distribution of the pixel values becomes more and more uniform, which means the statistical properties of pixel values are hidden. Although the performance against differential attacks is very poor, but much better than others. Because the statistical of pixels in other position permutation algorithms are not hidden. The schemes called substitution-permutation just use s-box to shuffle pixels are proposed recently. However, the correlation between pixels remains unchanged Nevertheless, it is also insecure and dangerous to encrypt digital image by AES round function only. There are a lot of attack ways to the low rounds AES. It is proved by theory and practice that those methods are very effective, such as differential attack and Linear attack. Therefore, it is necessary to have a value transformation algorithm to overcome this shortcoming. Before the end of this section, the initial key sensitivity problem also must be paid attention to. Figure 6 shows encrypted digital images in different initial key.

Initial key sensitivity means the small change of initial key can cause the large change of pixels in encrypted digital image. The property of initial key sensitivity can be compared by Figure 6 and Figure 5. NPCR can be another way to test initial key sensitivity, because NPCR represents the number of pixel change rate. The test values are shown in Table 3.

The initial key sensitivity of two rounds encryption is better than one round encryption apparently. As shown in Table 3, a bit change in the initial key can change 99.9146% bits in the encrypted digital image.

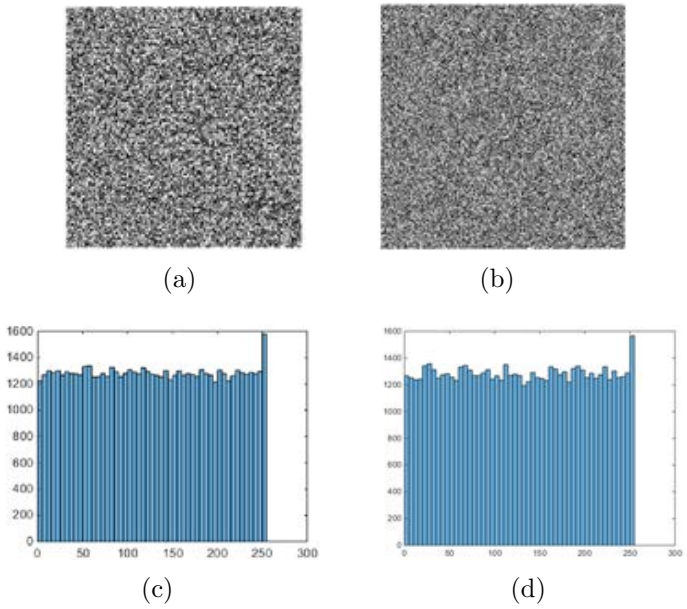


FIGURE 6. initial key sensitivity test. (a) cipher image of a bit change in initial key in one round encryption (b) cipher image of a bit change in initial key in two rounds encryption (c) histogram of a bit change in initial key in one round encryption(d) histogram of a bit change in initial key in two rounds encryption

TABLE 3. The test of NPCR

Encryption times	NPCR
One round encryption	25%
Two round encryption	99.9146%

2.3. **A new position permutation.** In this section, a new position permutation algorithm is proposed. Without loss of generality, we assume that the pixels in digital image are represented by a $M \times N$ matrix. Each pixel contains 8 bits. In general, $M \times N \times 8$ bits are multiple of 128. So, whole pixels in digital image can be divided into $\frac{M \times N \times 8}{128}$ groups. The new position permutation algorithm is made up with two steps.

Step1: The final 128 bits are obtained by making exclusive OR operation on $\frac{M \times N \times 8}{128}$ groups. The speed of exclusive OR operation is very fast in the hardware implementation, such as FPGA.

Step2: 128 bits obtained in Step 1 is used as initial key in AES round function encryption. $\frac{M \times N \times 8}{128}$ groups are fed into two rounds encryption orderly.

So, we can make a conclusion that one bit change in pixels can change almost whole bits in encrypted image by the new position permutation algorithm. Therefore, the new position algorithm has a strong defense against differential attacks.

3. **Value transformation.** In order to enhance the security of new position permutation algorithm, chaotic system is introduced into the value transformation algorithm. Compared with one-dimensional chaotic systems, multi-dimension and hyper chaotic systems have better properties in the sensitive dependence on initial condition, nonlinear, ergodicity and non-periodicity. But in the consideration of resource consumption and finite word length effect in FPGA implementation as well as better performance in new

position permutation algorithm, Logistic map is selected as digital chaos generator to generate pseudo-random sequence. In this section, pseudo-random sequence is used to make exclusive or with the output of two rounds encryption of AES round function.

3.1. **Logistic map.** Logistic map is one of the simplest and commonly used chaotic system. The Logistic map equation is as follows:

$$x_{n+1} = \mu x_n(1 - x_n) \tag{5}$$

where $\mu \in [0, 4] x_n \in [0, 1]$, $n \in (0, 1, 2, 3...)$. The influence of parameter μ in the Logistic map is very significant, which can be showed in Figure 7.

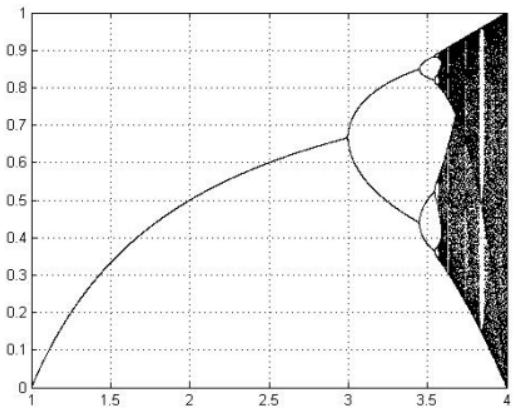


FIGURE 7. Bifurcation diagram of Logistic Map

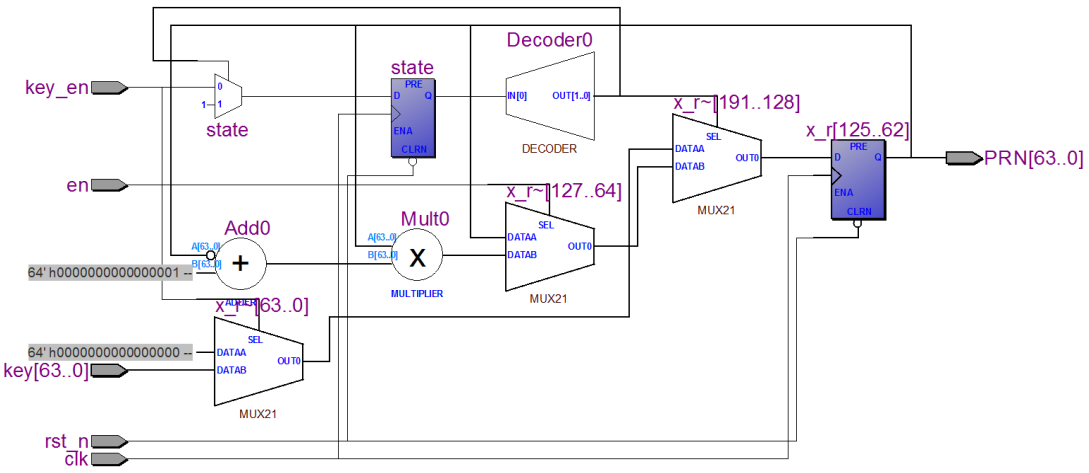


FIGURE 8. The diagram of Logistic map

When μ is equal to 4, the orbits of Logistic map have the properties of complete ergodic. The implementation diagram of Logistic map based on FPGA is shown in Figure 8. Resource consumption and maximum frequency are shown in Table 4.

If the precision of Logistic map is higher, the more logic elements will be consumed. Therefore, maximum frequency will be very low, and the throughput of encryption will be affected. In the Figure 8, the precision of Logistic map is selected as 64 bits.

NIST (United States National Institute of standards and Technology) standard testing package is given by the United States National Institute of standards and Technology, which is used to test the random numbers. There are many test methods in the NIST

Table 4. Resource consumption and maximum frequency

Resource categories	Logistic map
Total logic elements	2198
Total combination functions	2188
Dedicated logic registers	131
Total logic registers	131
Embedded Multiplier 9-bit elements	127
Frequency max	33.02MHz

standard testing package, such as frequency detection, block frequency test, runs test and so on. The NIST test is shown in Table 5.

Table 5. The test of NIST

Test categories	P value
Approximate Entropy	0.256575
Block Frequency	0.410774
Cumulative Sums	0.888683
	0.547525
FFT	0.966757
Frequency	0.630032
Linear Complexity	0.320360
Longest Run	0.075408
Nonoverlapping Template	0.360778
Overlapping Template	0.460403
Random Excursions	0.312270
Random Excursions Variant	0.387427
Rank	0.878337
Runs	0.134463
Serial	0.540732
	0.722744
Universal	0.418009

The standard value of P is 0.01. If P is greater than 0.01, it shows that the sequence has good randomness. In Table 5, P value shows that the pseudo-random numbers generated by Logistic map reach the NIST test standard..

3.2. **Digital images encryption and security analysis.** The pixel value encrypted by new position permutation are transformed by pseudo-random sequence generated by Logistic map. The cipher-image is shown in Figure 9.

As shown in Figure 9, useful information is well hidden. But some security test still should be carried out to prove the security of the new digital image encryption scheme in this paper.

3.2.1. *Histogram analysis.* The histogram reveals the distribution of pixel value. As Shannon pointed out, the uniform distribution of pixel value can resist statistical attack on the histogram analysis. Therefore, the uniform distribution of pixel value is one of the safety standards for digital image encryption. As shown in Figure 9, the distribution of pixel value is uniform.

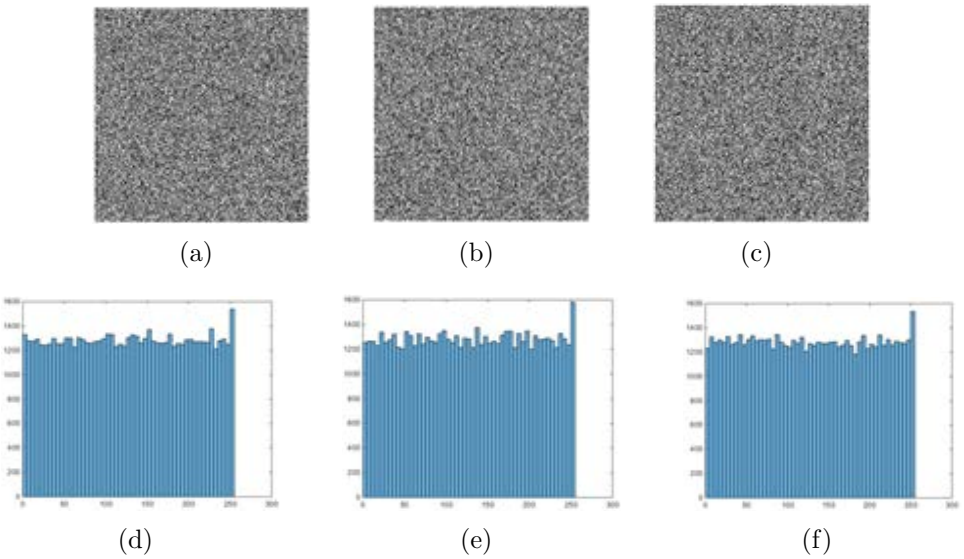


FIGURE 9. value transformation encryption (a) value transformation encryption for original digital image with original initial key (b) value transformation encryption for a bit change in digital image with original initial key (c) value transformation encryption for original digital image with a bit change in initial key (d) histogram of value transformation encryption for original digital image with original initial key (e) histogram of value transformation encryption for a bit change in digital image with original initial key (f) histogram of value transformation encryption for original digital image with a bit change in initial key

3.2.2. *Correlation analysis.* Correlation analysis is a special test method in image encryption scheme. The correlation analysis is calculated as follow:

$$r_{x,y} = \frac{E\{[x - E(x)][y - E(y)]\}}{\sqrt{D(x)}\sqrt{D(y)}} \tag{6}$$

Where $E(x) = \frac{1}{n}\sum_{i=1}^{n} x_i$, $D(x) = \frac{1}{n}\sum_{i=1}^{n} [x_i - E(x)]^2$.

In order to observe the correlation between pixels Intuitively the correlation analysis of Lena is shown by Figure 10 firstly.

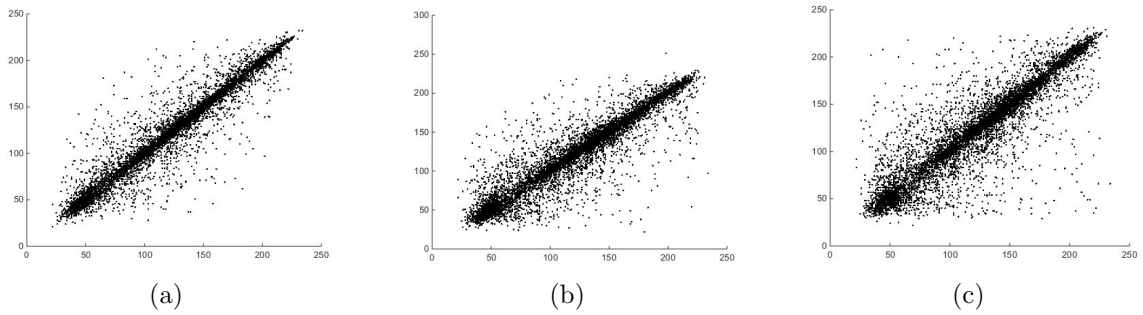
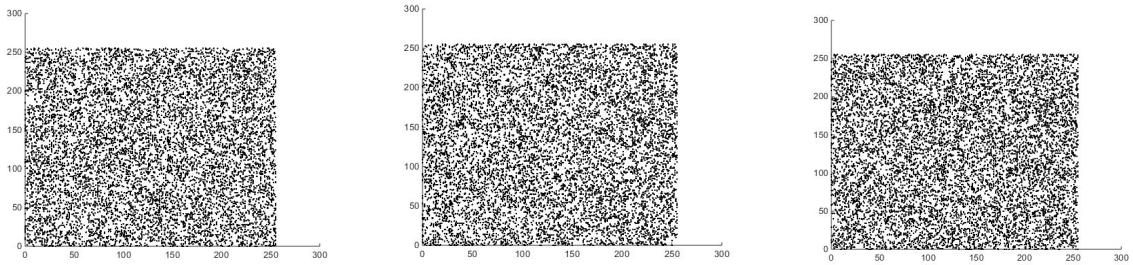


FIGURE 10. The correlation analysis of Lena (a)horizontally adjacent pixels (b) vertically adjacent pixels (c) diagonally adjacent pixels

As shown in figure 10, horizontally, vertically, diagonally adjacent pixels are concentrated in the middle of the coordinate plane. So, it is obvious that there is a very high

correlation between pixels. In order to compare the correlation of pixels between the Lena and the cipher image, the correlation analysis of cipher image is shown in Figure 11.



(a) (b) (c)

FIGURE 11. The correlation analysis of cipher image (a)horizontally adjacent pixels (b) vertically adjacent pixels (c) diagonally adjacent pixels

As shown in Figure 11 the correlation between the pixels of the encrypted image has a great change. The pixels are distributed in the coordinate plane uniformly. So we can make a conclusion that the information of correlation between pixels is well hidden.

In addition to the representation of coordinate plane, the correlation between pixels can also be represented by numerical value. The value of correlation analysis is shown in Table 6.

TABLE 6. The comparison of correlation analysis

	horizontally	vertically	diagonally
Lena	0.9709	0.9419	0.8996
Cipher image	0.080	0.00022285	-0.005

3.2.3. *Differential attack analysis.* NPCR and UACI are two major performance indices in the resistance of differential attack, which are wildly used in digital image encryption. NPCR test the number of pixels change rate. Without loss of generality, we assume that the digital image pixels are a $M \times N$ matrix. $C(i,j)$ and $C_1(i,j)$ is the value of pixel in encrypted digital image with just a bit difference in original digital image pixel. So, NPCR is calculated by

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{7}$$

Where $D(i,j) = \begin{cases} 1 \ when \ \mathrm{C}_1(i,j) \neq C(i,j) \\ 0 \ otherwise \end{cases}$.

UACI test the unified average changing intensity. So, UACI is calculated by

$$UACI = \frac{1}{M \times N} \left[\sum_{i,j} \frac{|C(i,j) - C_1(i,j)|}{255} \right] \times 100\% \tag{8}$$

NPCR and UACI are obtained by calculating the two pictures in Figure 9. The test of NPCR and UACI are shown in Table 6.

TABLE 7. The test of NPCR and UACI

NPCR	UACI
99.8764	33.6211

The standard value of NPCR and UACI is 99.6049% and 33.4635%. So, it is obvious that the digital image encryption scheme in this paper has a high resistance to differential attack.

3.2.4. *Key sensitivity analysis.* Similar to the test method in section 2.2, initial key sensitivity is tested by comparing the picture (a) and (c) in Figure 9. The NPCR test result is 99.6292%, which means that one bit changes in the initial key can change 99.6292% bits in the encrypted digital image.

3.2.5. *Information entropy analysis.* The concept of information entropy is also proposed by Shannon. Information entropy represent uncertainty of system or degree of disorder. So, it is often used as a test indices of encryption security. Information entropy is calculated by

$$H(m) = \sum_{i=0}^{m-1} (p(m_i) \log \frac{1}{p(m_i)}) \tag{9}$$

Where $p(m_i)$ represents the probability of occurrence of m_i, and log denotes based 2 logarithm. The ideal value of information entropy is 8. Information entropy test in Figure 9 is shown in Table 7.

Table 8. The test of information entropy

Picture in Figure 9	Information entropy
(a)	7.9893
(b)	7.9888
(c)	7.9892

3.2.6. *Key space.* In logistic map, μ and x_0 are selected as initial key. The μ and x_0 can be represented by 64 bits respectively. Therefore, the entire initial key reach 128 bits, which can against brute-force search attacks [24].

3.2.7. *Compared with other algorithms.* Image encryption scheme 2[1], scheme 3[4], scheme 4[6], scheme 5[7] , scheme 6[9] and scheme 7[12] are selected as contrast, and scheme 1 is the scheme proposed in this paper. Those image encryptions are all based on Lena. So, we can get the image encryption analysis comparison table 9 and 10.

Table 9. The analysis comparison table part one

scheme	Correlation			Differential attack		Information entropy	Key space
	horizontal	vertical	Diagonal	NPCR	UACI		
1	0.080	0.00022	-0.005	99.8764	33.6211	7.9893	$>2^{256}$
2	-0.0142	-0.0074	-0.0183	—	—	—	$>10^{70}$
3	0.0107	0.0141	0.0097	99.68	33.71	7.9972	—
4	0.000707	0.00216	0.01488	99.639	33.554	7.9994	2^{128}
5	-0.048	-0.0112	-0.0045	99.6228	33.7041	7.9963	$>2^{624}$
6	0.0020161	-000091	0.00165	9960517	33.399963	7.99930975	$>10^{42}$
7	0.0026	0.0034	-0.0019	99.6201	33.4757	7.9992	62^{32}

As shown in table 9, security analysis in scheme 1 has a good performance, especially in the differential attack analysis. Compared with other encryption schemes, the value of NPCR in scheme 1 is the highest, and UACI in scheme 1 is the closest to the ideal value. As shown in table 10, all the image encryption scheme pass the test of histogram analysis and key sensitivity analysis.

TABLE 10. The analysis comparison table part two

scheme	Histogram analysis	Key sensitivity analysis
1	passed	passed
2	passed	passed
3	passed	—
4	passed	passed
5	passed	passed
6	passed	passed
7	passed	passed

3.2.8. *Performances analysis.* Combined with the contents in section 2 and 3, a complete digital image encryption system is proposed. Based on using the experience of other subjects for reference [25–28], The diagram is shown in Figure 12.

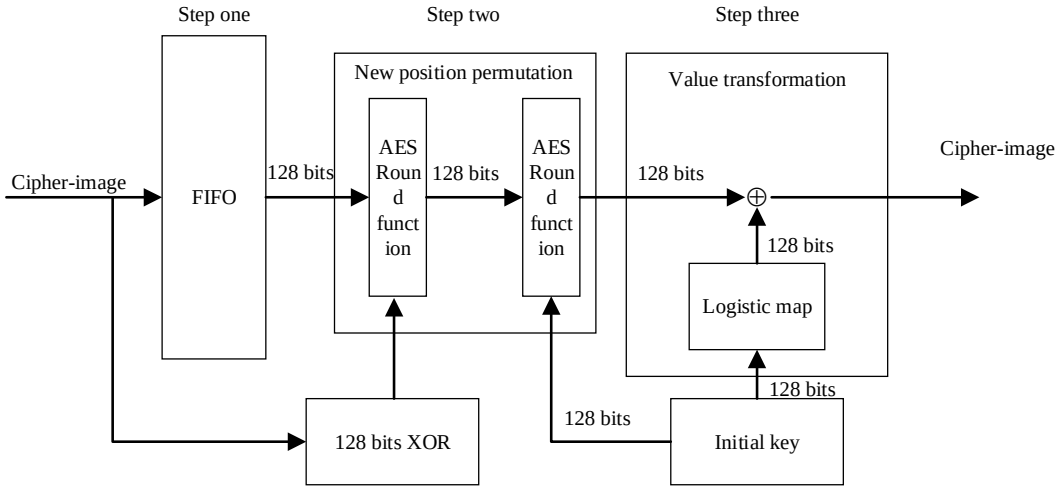


FIGURE 12. The diagram of complete digital image encryption system

As shown in Table 1 and Table 4, the throughput of the whole encryption system is limited by the maximum frequency of Logistic map. The maximum throughput of the whole encryption can reach 132.08MB/s by using a kind of chaotic digital quantization [25]. In the field of digital image processing, digital image is often divided into several small matrixes for processing. At present, the latest image compression standard H.265 also divide digital image into several small matrixes to process. Accordingly, digital image encryption in this paper can be closely applied to digital image storage and transmission.

4. **Conclusion.** In this paper, a complete new digital image encryption system is proposed. The new digital images encryption system contains two modules. In the position permutation module, two rounds of AES round function encryption are selected as position permutation algorithm. In the value transformation module, Logistic map is selected as value transformation algorithm. Through security analysis and hardware implementation, it is proved that the new digital image encryption system is feasible and efficiency.

Acknowledgment. Project supported by the National Natural Science Foundation of China (Grant Nos. 61471158), the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20132301110004) and College of Heilongjiang Province "Modern sensor technology" innovation team project(Grant No. 2012TD007).

REFERENCES

[1] T. Gao, Z. Chen, A new image encryption algorithm based on hyper-chaos, *Physics Letters A*, vol.372, no.4, pp.394-400, 2008.

[2] H. C. Chen, J. I. Guo, L. C. Huang, J. C. Yen, Design and realization of a new signal security system for multimedia data transmission, *EURASIP Journal on Advances in Signal Processing*, vol.2003, no.13, pp.1291-1305, 2003.

[3] C. De Cannière, J. Lano, B Preneel, Cryptanalysis of the Two-Dimensional Circulation Encryption Algorithm, *EURASIP Journal on Advances in Signal Processing*, vol.2005, no.12, pp.1-5, 2005.

[4] M. Khan, T. Shah, S. I. Batool, Construction of S-box based on chaotic Boolean functions and its application in image encryption, *Neural Computing and Applications*, vol.27, no.3, pp.677-685, 2016.

[5] V. Patidar, N. K. Pareek, K. K. Sud, A new substitutiondiffusion based image cipher using chaotic standard and logistic maps, *Communications in Nonlinear Science & Numerical Simulation*, vol.14, no.7, pp.3056-3075, 2009.

[6] Y. Wang, K. W. Wong, X. Liao, G. Chen, A new chaos-based fast image encryption algorithm, *Applied Soft Computing*, vol.11, no.1, pp.514-522, 2011.

[7] A. Belazi, A. A. A. El-Latif, S. Belghith, A novel image encryption scheme based on substitution-permutation network and chaos, *Signal Processing*, no.128, pp.155-170, 2016.

[8] K. W. Wong, A fast chaotic cryptographic scheme with dynamic look-up table, *Physics Letters A*, vol.298, no.4, pp.238-242, 2002.

[9] Z. L. Zhu, W. Zhang, K. W. Wong, H. Yu , A chaos-based symmetric image encryption scheme using a bit-level permutation, *Information Sciences An International Journal*, vol.181, no.6, pp.1171-1186, 2011.

[10] T. D. Nguyen, S. Arch-Int, N. Arch-Int, A novel secure block data-hiding algorithm using cellular automata to enhance the performance of JPEG steganography, *Multimedia Tools and Applications*, vol.74, no.15, pp.5661-5682, 2015.

[11] G. Ye, X. Huang, A novel block chaotic encryption scheme for remote sensing image, *Multimedia Tools and Applications*, no.18, pp.1-14, 2016.

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

[13] P. Ping, F. Xu, Z. J. Wang, Image encryption based on non-affine and balanced cellular automata, *Signal Processing*, vol.105, no.12, pp.419-429, 2014.

[14] N. K Pareek, V. Patidar, K. K. Sud, Image encryption using chaotic logistic map, *Image & Vision Computing*, vol.24, no.9, pp.926-934, 2006.

[15] C. Fu, J. J. Chen, H. Zou, W. H. Meng, Y. F. Zhan and Y. W. Yu, A chaos-based digital image encryption scheme with an improved diffusion strategy, *Optics Express*, vol.20, no.3, pp.2363-78, 2012.

[16] X. Y. Zhang, G. J. Zhang, X. Li, Y. Z. Ren, J. H. Wu, Image encryption using random sequence generated from generalized information domain, *Chinese Physics B*, vol.25, no.5, pp.176-185, 2016.

[17] H. Gao, Y. Zhang, S. Liang, D. Li, A new chaotic algorithm for image encryption, *Chaos Solitons & Fractals*, vol.29, no.2, pp.393-399, 2006.

[18] G. Zhang, Q. Liu, A novel image encryption method based on total shuffling scheme, *Optics Communications*, vol.284, no.12, pp.2775-2780, 2011.

[19] G. Chen, Y. Mao, C. K. Chui, G. Chen, Y. Mao, A symmetric image encryption scheme based on 3D chaotic cat maps, *Chaos Solitons & Fractals*, vol.21, no.3, pp.749-761, 2004.

[20] C. K. Huang, H. H. Nien, Multi chaotic systems based pixel shuffle for image encryption, *Optics Communications*, vol.282, no.11, pp.2123-2127, 2009.

[21] Z. H. Guan, F. Huang, W. Guan, Chaos-based image encryption algorithm, *Physics Letters A*, vol.346, no.1-3, pp.153-157, 2005.

[22] S. J. Xu, X. B. Chen, R. Zhang, Y. X. Yang,Y. C. Guo, An improved chaotic cryptosystem based on circular bit shift and XOR operations, *Physics Letters A*, vol.376, no.1011, pp.1003-1010, 2012.

[23] X. L. Chai, Z. H. Gan, Y. Lu, M. H. Zhang and Y. R. Chen, A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system, *Chinese Physics B*, vol.25, no.10,pp.100503.1-100503.13, 2016.

[24] S. J. LI, Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems, *International Journal of Bifurcation & Chaos*, vol.16, no.8, pp.2129-2151, 2011.

[25] W. K. Chen, H. P. Chen, H. K. Tso, A Friendly and Verifiable Image Sharing Method, *Journal of Network Intelligence*, Vol. 1, no.31, pp. 46-51, 2016.

[26] C. M. Chen, L. L. Xu, T. Y. Wu, C. R. Li, On the Security of a Chaotic Maps-based Three-party Authenticated Key Agreement Protocol, *Journal of Network Intelligence*, Vol. 1, no.32, pp.61-66, 2016.

[27] W. Shen, S. M. H., J. S. Qian, L. D. Li, Blind Quality Assessment of Dehazed Images by Analyzing Information, Contrast, and Luminance, *Journal of Network Intelligence*, Vol. 2, no.1, pp. 139-146, 2017.

[28] C.M. Chen, W. Fang, K.H. Wang, T.Y. Wu, Comments on "An improved secure and efficient password and chaos-based two-party key agreement protocol", *Nonlinear Dynamics*, Volume 87, no.3, pp 2073-2075, 2017.

[29] P. Li, Z. Li, S. Fettinger, Y. Mao, W. A. Halang, Application of Chaos-based Pseudo-Random-Bit Generators in Internet-based Online Payments, *Studies in Computational Intelligence*, no.37, pp.667-685, 2007.