2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)
Banff Center, Banff, Canada, October 5-8, 2017

An ACP-based Approach to Color Image Encryption Using DNA Sequence Operation and Hyper-chaotic System

Wenbo Zheng, Fei-Yue Wang* and Kunfeng Wang

***Abstract*—In order to achieve effective protection of digital image information and provide anti-attack capability for encrypted image, this paper proposed an ACP-based Approach to color image encryption using DNA sequence operation and hyper-chaotic system. By using the ACP method which is a way to solve the social computing problem, the influence of the chaotic data from the real world and the influence of the chaotic data from the simulation on the encryption were combined. First, obtaining chaotic data in reality, we made artificial random images by using cloud model; Then, chaotic data in reality were used to encrypt the artificial random image while chaotic data in simulation were used to encrypt the original image; Finally, using the method of parallel execution, combining with the influence of the chaotic data of the two groups, performing DNA-XOR operation on two groups encryption results and we get the final encrypted image. The simulation results show that the algorithm has a good encryption effect and a larger secret key space to the key. In addition, the algorithm can also resist the brute attack and differential attack, and achieve the hyper-chaotic image encryption in the disadvantages of low chaos.**

***Keywords*—Image encryption, The ACP method, Hyper-chaotic system.**

I. Introduction

Digital image encryption is a very important research direction of digital image information security. Digital image encryption based on chaos theory has been the hotspot of digital image encryption research in recent years, and has become the main research direction of digital image encryption technology. With the development of research, chaotic image encryption algorithm is combined with some others technologies such as artificial intelligence, signal processing and bioinformatics, so a number of robust image encryption algorithms were proposed [1]–[13].

Because the existing hyper-chaotic encryption technology is mostly based on four-dimensional chaotic system, it is easy to be attacked by phase space reconstruction method [14], [15], and the development and application of supercomputing ability put forward new challenges to chaos image encryption. It is necessary to introduce the idea of solving complex system.

Fei-Yue Wang proposed the ACP(Artificial societies, Computational experiments, Parallel execution) method [16]–[20], which is based on the complex system approach to the basic framework of the research about modeling and control of complex systems. This paper further explores the chaos of chaotic system in chaotic encryption algorithm based on the ACP method, and uses the ACP method to combine the chaotic data in reality with chaotic data in simulation.

Wenbo Zheng is with School of Software Engineering, Xi'an Jiaotong University, Xi'an 710049, China; he is also with the State Key Laboratory of Management and Control for Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China (email: zwb2017@stu.xjtu.edu.cn).

Fei-Yue Wang is the State Key Laboratory of Management and Control for Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China (email: feiyue.wang@ia.ac.cn).

Kunfeng Wang is with the State Key Laboratory of Management and Control for Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China (email: kunfeng.wang@ia.ac.cn).

*Fei-Yue Wang is corresponding author.

II. Related Work

A. Hyper-chaotic system

The dynamical equation of Chen's hyper-chaos is:

$$\begin{cases} x' = a(y - x) \\ y' = -xz + dx + cy - q \\ z' = xy - bz \\ q' = x + k \end{cases} \tag{1}$$

where, a, b, c, d, k are the system parameters. when $a = 36$, $b = 3$, $c = 28$, $d = 16$ and $k \in [-0.7, 0.7]$, the hyper-chaotic system have four chaotic sequences in the chaotic state. While k is set as 0.4, we got two positive Lyapunov exponents of the hyper-chaos.

B. DNA sequence operations

As we know that there are four nucleic acid bases A(adenine), C(cytosine), G(guanine) and T(thymine) in DNA sequence, where A and T are complementary, G and C are complementary. And the rules of the DNA code to encode the color image are shown in Table I.And corresponding to eight kinds of DNA encoding rules, we adopt one type of addition operation shown in Table II, the subtraction operation is shown in Table III and the XOR operation is shown in Table IV.

TABLE I
DNA encoding rules

	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

TABLE II
Addition operation for DNA sequences

+	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G
T	T	A	G	C

TABLE III
SUBTRACTION OPERATION FOR DNA SEQUENCES

-	A	G	C	T
A	A	T	C	G
G	G	A	T	C
C	C	G	A	T
T	T	C	G	A

TABLE IV
XOR OPERATION FOR DNA SEQUENCES

XOR	T	A	C	G
T	A	T	G	C
A	T	A	C	G
C	G	C	A	T
G	C	G	T	A

C. The cloud model

Let U be a quantitative universal set and C be the qualitative concept related to U. If $x \in U$, which is a random realization of the concept C, and x satisfies $x \sim N(Ex, En'^2)$, where $En' \sim N(En, He^2)$, and the certainty degree of x on C is

$$\mu = \exp[-\frac{(x-Ex)^2}{2(En')^2}]$$

then the distribution of x on U is a normal cloud, and every x is defined as a cloud drop.

The normal cloud model employs the expected value Ex, the entropy En, and the hyper-entropy He to represent the concept. Ex is the mathematical expectation of the cloud drops distributed in the universal set. En is the uncertainty measurement of the qualitative concept. Given the three parameters Ex, En, He, the normal cloud model can be generated.It was called the forward Gaussian cloud algorithm [21].

III. CHAOTIC DATA IN REALITY

Most studies show that China's stock market act obviously hyper-chaotic and nonlinear dynamic [22]–[24]. And chaotic system can be defined by Lyapunov coefficient. This paper uses the ex dividend data on "Pudong Development Bank","CITIC Securities" and "Hang Seng Electronics" since January 1st, 2014 to January 1st, 2017, so the Lyapunov coefficient can be calculated through small data method [25], [26], which results are 0.0930, 0.0868 and 0.0696.

Calculate the maximum Lyapunov coefficient through small data method [25], [26] of the seven chaotic data used in the encryption algorithm 1, and the number of the Lyapunov coefficients greater than 0, the coefficient is 2.117, and the number is 4. This is greater than the 6-dimensional hyper-chaotic system [27], [28]. That proves the algorithm improves the chaos.

IV. IMAGE ENCRYPTION ALGORITHM BASED ON THE ACP METHOD

A. Selection of secret key

x_1, y_1, z_1, q_1 are randomly initial values in Chen's hyper-chaotic system mentioned in II-A, it an be seen as the secret keys, in accordance to $x_1 = 0.3$, $y_1 = -0.4$, $z_1 = 1.2$, $q_1 = 1.0$ and the related system indexes are $a = 36$, $b = 3$, $c = 28$, $d = 16$ and $k = 0.2$. We build three one-dimensional cloud model, which was mentioned in II-C, the digital characteristics for the first cloud model is Ex_1, En_1, He_1 and N, the digital characteristics for the second cloud model Ex_2, En_2, He_2 and N, the digital characteristics for the third cloud model Ex_3, En_3, He_3 and N. We use $Ex_1 = 0$, $En_1 = 1$, $He_1 = 0.02$, $Ex_2 = 0$, $En_2 = 4$, $He_2 = 0.02$, $Ex_3 = 0$, $En_3 = 1$, $He_3 = 0.08$ and $N = 1000000$.

B. Algorithm description

As is well-known, there are inextricably links between chaos theory and simple cryptography, and chaotic dynamics shows some features that are desirable for the cipher system. Chaos was proposed by American meteorologist Lorenz in the 1960s. Since chaos system has good pseudo-random and uncertain, chaos system has great key space in image encryption. Yet the technology of attack is changing with the times. Many paper [14], [15] show that the images generated by a chaotic system are vulnerable to attacks. Therefore, in order to improve the security of the algorithm, it is necessary to combine the chaotic encryption algorithm with other methods. There are two facts, one is that the existing hyper-chaotic encryption technology is based on four dimensional chaotic system, which is easy to be attacked by the phase space attack method, the other is that the development and application of supercomputer computing power is a new challenge for chaos encryption. Because of the two facts, the idea of solving complex systems needs to be introduced. And the ACP method is the basic framework of the research about modeling and control of complex systems.

We propose an ACP-based approach to color image encryption using DNA sequence operation and hyper-chaotic system. Our encryption algorithm consists of three steps:

1) Step A, artificial encryption;
2) Step C, computational experiment;
3) Step P, parallel execution.

And our encryption steps were described in Algorithm.1, the flow chart is shown in Fig.1.The process of decryption is an inverse process of encryption. In the research of image encryption, this paper first introduces the ACP method and combines the thought with image encryption algorithm.

1) Artificial encryption: Generating artificial images, in a sense,we can be seen as a random "encrypted image". In many cases, researchers can only improve security through iterative encryption. And we use an artificial random image to replace the secret map that has been encrypted several times, improving the security of the encrypted image only once. During the generate process, the primary use of the cloud model with randomness is generated.

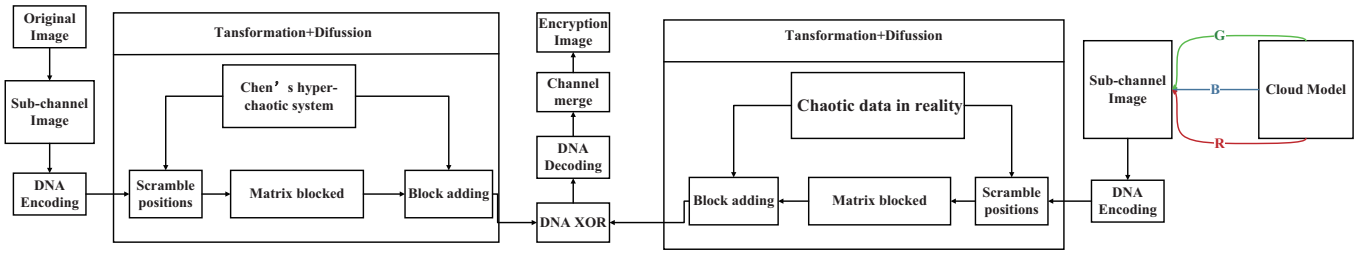


Fig. 1. The flow chart

Algorithm 1: Hyper-chaotic DNA Coding Digital Image Encryption Based on ACP Method

Input: Color image $I(m,n,3)$, Secret key x_1, y_1, z_1, q_1, k, Ex_1, En_1, He_1, Ex_2, En_2, He_2, Ex_3, En_3, He_3 and N

Output: Encrypted image E

Step A: 1: Execute artificial random image generation algorithm IV-B1 to generate artificial random image $I'(m,n,3)$

Step C and P: 2: Execute artificial random encryption algorithm IV-B2 to get encrypted artificial random image matrix R'', G'', B''

Step C and P: 3: Execute an blocking encryption algorithm based on DNA encodings and simulate chaos IV-B2 so that R', G', B' can be calculated

Step C and P: 4: Apply DNA XOR rule(2) shown in Table. IV to R', G', B' and R'', G'', B''.

$$\begin{cases} R_E(i,j) = R'(i,j) \oplus R''(i,j) \\ G_E(i,j) = G'(i,j) \oplus G''(i,j) \\ B_E(i,j) = B'(i,j) \oplus B''(i,j) \end{cases} \quad (2)$$
$$i = 1,2,3,.....,m;$$
$$j = 1,2,3,.....,n$$

5: Decode R_E, G_E, B_E according to the corresponding decoding method to get three binary matrix. Recombine them to write int color image E.

6: **return** Encrypted image E

We build three one-dimensional cloud model, which was mentioned in II-C, the digital characteristics for the first cloud model is Ex_1, En_1, He_1 and N, the digital characteristics for the second cloud model Ex_2, En_2, He_2 and N, the digital characteristics for the third cloud model Ex_3, En_3, He_3 and N.

Given three one-dimensional cloud model's parameters, the artificial random image can be generated. And this is given the artificial random image generation algorithm we call it.

We apply the forward Gaussian cloud algorithm [21] under the digital characteristics of Ex_1, En_1, He_1, Ex_2, En_2, He_2, Ex_3, En_3, He_3 and N to generate chaotic sequences $x' = \{x'_1, x'_2, x'_3, ..., x'_N\}$, $y' = \{y'_1, y'_2, y'_3, ..., y'_N\}$, $z' = \{z'_1, z'_2, z'_3, ..., z'_N\}$. For x', do the following transformation:

$$x'_i = [255 \times \frac{x'_i - x'_{\min}}{x'_{\max} - x'_{\min}}], i = 1,2,3,.....,N$$

In the above equation, x'_i is any element from sequence x', $x'_{\min}$ represents the minimum value in x', while $x'_{\max}$ is the maximum value of x', $[\cdot]$ represents the maximum integer that not exceeding $\cdot$. Apply the transformation mode of x' to y', z' to generate new sequence x', y', z' in interval $[0, 255]$.

Firstly, we generate 3 image matrix $R(m,n)$, $G(m,n)$, $B(m,n)$ by roles below

$$\begin{cases} R(i,j) = x'_{(j-1)\times m+i} \\ G(i,j) = y'_{(j-1)\times m+i} \\ B(i,j) = z'_{(j-1)\times m+i} \end{cases}$$
$$i = 1,2,3,.....,m;$$
$$j = 1,2,3,.....,n$$

Then, combine matrix $R(m,n)$, $G(m,n)$, $B(m,n)$ to write into original color image $I'(m,n,3)$. Finally, we get the artificial random image $I'(m,n,3)$.

2) Computational experiment: First of all, we use the chaotic data in reality to encrypt the artificial random images and get the matrix of artificial random encrypted image.In the algorithm, there are three chaotic sequences in reality x'', y'', z'' . And we use sequences x'', y'', z'' in position scrambling and use sequences x'', y'', z'' in block addition by the DNA addition operation. This is given the artificial random encryption algorithm we call it. We convert the color image $I'(m,n,3)$ to 3 image matrices $R'(m,n)$, $G'(m,n)$, $B'(m,n)$ and encode them by DNA coding in Table I.

First, we reorder stock-chaotic data sequence x'', y'', z'', which are $x'' = \{x''_1, x''_2, x''_3, ..., x''_{1095}\}$, $y'' = \{y''_1, y''_2, y''_3, ..., y''_{1095}\}$, $z'' = \{z''_1, z''_2, z''_3, ..., z''_{1095}\}$:

$$\begin{cases} [lx'', fx''] = sort(x'') \\ [ly'', fy''] = sort(y'') \\ [lz'', fz''] = sort(z'') \end{cases}$$

In the above equation, $[\cdot,\cdot] = sort(\cdot)$ is the sort function, fx'' is the new sequence after x'' ascending, lx'' is the location in original sequence of fx'' sequence. The relation between fy'' and ly'', also fz'' and lz'', is same as fx'' and lx''.

Second, make the following transformation:

$$\begin{cases} R'(i,j) \rightleftarrows R'(lx(i), ly(j)) \\ G'(i,j) \rightleftarrows G'(lx(i), lz(j)) \\ B'(i,j) \rightleftarrows B'(ly(i), lz(j)) \end{cases}$$

In the above equation scrambling R'', G'', B'' by choosing chaotic sequence combination (x'', y'', z''), among them, $i = 1, 2, \cdots, m$, $j = 1, 2, \cdots, n \times 4$, $R'(i,j)$, $G'(i,j)$, $B'(i,j)$ are respectively gray value of R, G, B channels in (i,j).

Third, we divide scrambling R, G, B into small blocks $Rb'(i,j)$, $Gb'(i,j)$, $Bb'(i,j)$, $i = 1, 2, \cdots, \frac{m}{4}$, $j = 1, 2, \cdots, n$, size of small block is 4×4. And according to the DNA addition rule in Table. II, add all blocks in Rb, Gb, Bb by the following equation.

$$\begin{cases} Rb'(i,j) \leftarrow Rb'(i,j) + Rb'(lx''(i), lz''(j)) \\ Gb'(i,j) \leftarrow Gb'(i,j) + Gb(ly''(i), lz''(j)) \\ Bb'(i,j) \leftarrow Bb'(i,j) + Bb(lx''(i), ly''(j)) \end{cases}$$

among them, $i = 1, 2, \cdots, m$, $j = 1, 2, \cdots, n \times 4$

So fourth, we regroup small blocks, $Rb'(i,j)$, $Gb'(i,j)$, $Bb'(i,j)$ are R'', G'', B'' and get the matrix of artificial random encrypted image R'', G'', B''.

Finally, we use a hyper-chaotic system to encrypt the original image.In the algorithm, there are four chaotic sequences x, y, z and q generated by Chen's hyper-chaotic system. We use sequences x, y, z in position scrambling and use sequences x, y, q in block addition by the DNA addition operation. We convert the color image $I(m,n,3)$ to 3 image matrices $R(m,n)$, $G(m,n)$, $B(m,n)$ and encode them by encoding method. We reorder Chen's hyper-chaotic system to generate 4 chaotic sequences , scramble the color image $I(m,n,3)$ and regroup the small blocks to get the encrypted three channel image by a similar approach to the artificial random image generation algorithm. And this is given the an blocking encryption algorithm based on DNA encodings and simulate chaos we call it.

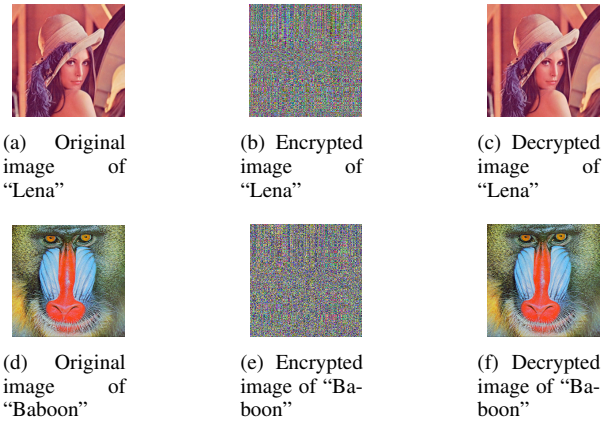
3) Parallel execution: We use hyper-chaotic encryption to encrypt the original image and image encryption using chaotic data in reality to encrypt artificial image, both parallel execution, in the end, perform DNA-XOR operation on two groups encryption results and we got the final encrypted image.In the process of encryption, the adoption of parallel technology increases the efficiency.Our algorithm make the influence of chaotic data in reality and hyper-chaotic system's data are combined.

Through the virtual interaction between actual chaotic data and artificial chaotic data, the chaos of the algorithm is improved III, and the security is improved V-B.

V. Experimental Results and Analysis

A. Simulated Results

In this paper, we use the standard $256 \times 256 \times 3$ color images "Lena" and "Baboon" shown in Fig.2 as the input images. Utilize Matlab 7.1 to simulate the encryption and decryption operations and set parameters $x_1 = 0.3$, $y_1 = -0.4$, $z_1 = 1.2$, $q_1 = 1.0$, $k = 0.2$ $Ex_1 = 0$, $En_1 = 1$, $He_1 = 0.02$, $Ex_2 = 0$, $En_2 = 4$, $He_2 = 0.02$, $Ex_3 = 0$, $En_3 = 1$, $He_3 = 0.08$ and $N = 1000000$. The encrypted images of "Lena" are shown in Fig.2(b), the decrypted images of "Lena" are shown in Fig.2(c).



(a) Original image of "Lena" (b) Encrypted image of "Lena" (c) Decrypted image of "Lena"

(d) Original image of "Baboon" (e) Encrypted image of "Baboon" (f) Decrypted image of "Baboon"

Fig. 2. Simulate Results

B. The Security Analysis

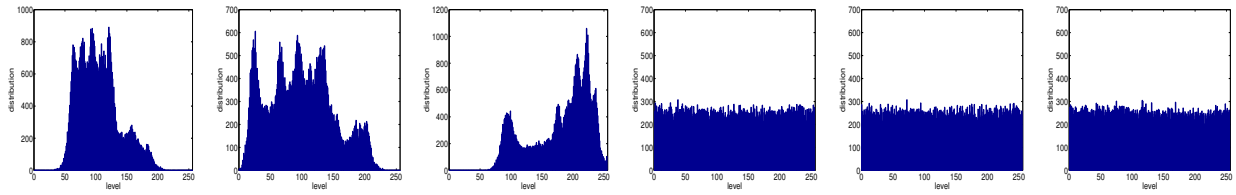
A good encryption algorithm should resist all kinds of known attacks, such as exhaustive attack, statistical attack and differential attack, etc [1]–[3], [29]. In this section, we will take the Lena picture as an example and discuss the security analysis of the proposed encryption scheme, and perform an encryption experiment

1) Ability of resisting exhaustive attack: In our algorithm, the initial value and the system parameter of the Chen's hyper-chaotic system which was mentioned in II-A and the cloud model which was mentioned in II-C can be seemed as secret key. Thus, there are fourteen secret keys in Algorithm. 1. If the precision is 10^{-15} , the secret key's space is $10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} = 10^{210} \approx 2^{700}$. Accordingly, the secret key's space is large enough to resist exhaustive attack.

2) Ability of resisting statistical attack:

a) Histogram analysis and information entropy: Comparing Fig. 3(a) and 3(d), 3(b) which shows the histograms of R, G and B channels from original image and 3(e), 3(c)and 3(f) which shows the histograms of R, G and B channels from encrypted image respectively, we find that pixel values of R, G and B channels from original image concentrate some values, but the corresponding histograms of R, G and B channels from encrypted image are nearly uniform. Hence, our algorithm can withstand statistical attack.

We can use the information entropy to express uncertainties of the image information.For an ideally random image, the value of the information entropy is 8. [29] The information entropies of three channel encryption images(R, G, B) are shown in Table V, all of which are very close to the theoretical value 8, which demonstrates that the cipher images are almost close to random sources and the information leakage in the encryption process is negligible.



(a) (b) (c) (d) (e) (f)

Fig. 3. Histograms of the original image and the encrypted image

TABLE V
THE INFORMATION ENTROPY OF ENCRYPTED IMAGE

	R	G	B
H	7.9987	7.9983	7.9987

b) Correlation coefficient analysis: We randomly select 5000 pairs in horizontal, vertical, and diagonal directions of adjacent pixels from the original image and the encrypted image to test the correlation between two adjacent pixels. From

TABLE VI
CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS IN ORIGINAL IMAGE AND ENCRYPTED IMAGE

	The original image			The encrypted image		
	R	G	B	R	G	B
Horizontal	0.98	0.959	0.9852	0.0681	0.0471	0.0044
Vertical	0.9804	0.9559	0.9347	0.0422	-0.0119	0.1271
Diagonal	0.9852	0.9856	0.9856	0.0497	0.0703	0.1043

Table VI, it can be seen that the correlation coefficient of the adjacent pixels in R, G and B channels from encrypted image is close to 0. It shows that the our image encryption algorithm has strong ability of resisting statistical attack.

3) Resistance to differential attack: NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) are generally devoted to evaluating the impact caused by one-pixel change on the plain-image.

Two images that are encrypted with one-pixel value difference in their original images are recorded as $C_1(i,j)$ and $C_2(i,j)$. NPCR is used to measure the percentage of different pixel numbers between $C_1(i,j)$ and $C_2(i,j)$, while UACI is used to measure the average intensity of the differences between $C_1(i,j)$ and $C_2(i,j)$. They are defined by Eqs.(3)(4)(5)

$$D(i,j) = \begin{cases} D(i,j) = 0 & C_1(i,j) = C_2(i,j) \\ D(i,j) = 1 & C_1(i,j) \neq C_2(i,j) \end{cases} \quad (3)$$

$$NPCR = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} D(i,j)}{M \times N} \times 100\% \quad (4)$$

$$UACI = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} |C_1(i,j) - C_2(i,j)|}{256 \times M \times N} \times 100\% \quad (5)$$

where M and N are the height and width of the image. We obtain the results by simulating experiment, which are shown in Table VII. The results can illuminate that our image encryption algorithm has strong ability of resisting differential attack.

TABLE VII
NPCR AND UACI OF THE ENCRYPTED IMAGES OF "LENA"

	NPCR/%	UACI/%
R	99.81	39.27
G	99.84	38.54
B	99.8	38.74

C. Speed analyses and performance comparison

Chaos-based image encryption scheme is mostly composed of permutation process and diffusion process. Thus, the round number of permutation, diffusion and image-scanning operations directly influence the running time. Table VIII is the performance comparison of different methods to meet a satisfactory security level. In this respect, our encryption algorithm has higher running efficiency than Refs. [3]–[5], [8], [9], [12] .

TABLE VIII
PERFORMANCE COMPARISON OF DIFFERENT METHODS TO ACHIEVE A SATISFACTORY SECURITY LEVEL

Method	NPCR	UACI	The round number of		
			Image-scanning	Permutation	Diffusion
Ours	> 0.996	> 0.333	1	2	2
Ref [3]	> 0.996	> 0.333	6	3	3
Ref [4]	> 0.996	> 0.333	3	4	4
Ref [5]	> 0.996	> 0.333	2	2	2
Ref [8]	> 0.996	> 0.333	4	2	2
Ref [9]	> 0.996	> 0.333	4	4	2
Ref [12]	> 0.996	> 0.333	6	3	3

Our algorithm is compared with those in [1]–[13] . The results are shown in Table IX. It is observed that the information entropy of ours is closest to 8 bits expect [2] and [12] . For key space analysis, the space of this scheme is large enough to resist the exhaustive attack. The value of NPCR and the value of UACI is greater than those of others. It is clear that the performance of our image encryption algorithm is nice as a whole.

VI. CONCLUSIONS

In this paper, an ACP-based approach to color image encryption using DNA sequence operation and hyper-chaotic

TABLE IX
PERFORMANCE OF THE PROPOSED SCHEME AND THIRTEEN COMPARABLE METHODS

Methods	Keyspace	Entropy	NPCR/%	UACI/%
Ours	2^{700}	7.9986	99.81	39.02
Ref [1]	2^{349}	7.997	99.5804	33.4782
Ref [2]	2^{212}	7.9998	99.122	33.1298
Ref [3]	2^{370}	7.9896	99.6521	33.3438
Ref [4]	2^{100}	7.9972	99.6175	33.4152
Ref [5]	2^{239}	7.998	99.6063	34.1951
Ref [6]	2^{233}	7.9968	99.5506	33.4055
Ref [7]	2^{299}	7.9897	99.6033	33.4655
Ref [8]	2^{186}	7.9989	0.0004	0.0005
Ref [9]	2^{66}	7.9975	99.6077	33.457
Ref [10]	2^{128}	7.997	99.57	33.42
Ref [11]	2^{269}	7.9974	99.59	33.42
Ref [12]	2^{505}	7.99881	99.60917	33.46566
Ref [13]	2^{327}	7.9007	99.58	33.43

system is proposed. There an ACP method is used to combine the influence of the chaotic data in reality on the encryption with the influence of the chaotic data in the simulation on the encryption. We can get the encrypted image through three steps which are artificial encryption, computational experiment and parallel execution. Through the experimental results and security analysis, we found that our algorithm achieves a good encryption effect and has a larger secret key space. In addition, the algorithm can also resist exhaustive attacks and statistical attacks. All above indicate that this paper overcomes the shortcomings of low chaos in hyper-chaotic image encryption, which is more suitable for image encryption than traditional chaotic image encryption algorithm.

ACKNOWLEDGMENT

This work was supported by National Natural Science Foundation of China (61533019, 71232006, 91520301).

REFERENCES

[1] S. Som, A. Kotal, A. Chatterjee, and S. Dey, "A colour image encryption based on dna coding and chaotic sequences," in *International Conference on Emerging Trends and Applications in Computer Science*, pp. 108–114, 2015.

[2] X. Huang and G. Ye, "An image encryption algorithm based on hyper-chaos and dna sequence," *Multimedia Tools and Applications*, vol. 72, no. 1, pp. 57–70, 2015.

[3] Y. Liu, J. Wang, J. Fan, and L. Gong, "Image encryption algorithm based on chaotic system and dynamic s-boxes composed of dna sequences," *Multimedia Tools and Applications*, vol. 75, no. 8, pp. 4363–4382, 2016.

[4] Q. Zhang, L. Guo, and X. Wei, "Image encryption using dna addition combining with chaotic maps," *Mathematical & Computer Modelling*, vol. 52, no. 1112, pp. 2028–2035, 2010.

[5] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on dna sequence operation and hyper-chaotic system," *Journal of Systems & Software*, vol. 85, no. 2, pp. 290–299, 2015.

[6] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on dna sequences and multiple improved 1d chaotic maps," *Applied Soft Computing*, vol. 37, no. C, pp. 24–39, 2015.

[7] L. Liu, Q. Zhang, and X. Wei, "A rgb image encryption algorithm based on dna encoding and chaos map ," *Computers & Electrical Engineering*, vol. 38, no. 5, pp. 1240–1248, 2015.

[8] X. Y. Wang, Y. Q. Zhang, and X. M. Bao, "A novel chaotic image encryption scheme using dna sequence operations," *Optics & Lasers in Engineering*, vol. 73, pp. 53–61, 2015.

[9] T. Hu, Y. Liu, L. H. Gong, and C. J. Ouyang, "An image encryption scheme combining chaos with cycle operation for dna sequences," *Nonlinear Dynamics*, pp. 1–16, 2016.

[10] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and dna sequence operations," *Signal Processing Image Communication*, vol. 52, pp. 6–19, 2017.

[11] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using dna sequence operations," *Optics & Lasers in Engineering*, vol. 88, pp. 197–213, 2017.

[12] M. J. Rostami, A. Shahba, S. Saryazdi, and H. Nezamabadi-Pour, "A novel parallel image encryption with chaotic windows based on logistic map ," *Computers & Electrical Engineering*, 2017.

[13] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A novel image encryption scheme based on dna sequence operations and chaotic systems," *Neural Computing and Applications*, pp. 1–19, 2017.

[14] T. V. Laptyeva, S. Flach, and K. Kladko, "The weak-password problem: Chaos, criticality, and encrypted p-captchas," *Epl*, vol. 95, no. 5, pp. 981–981, 2011.

[15] Q. N. Liao, "Color image encryption algorithm and its decryption method protecting from shearing attack," *Computer Engineering & Design*, vol. 32, no. 2, pp. 509–512, 2011.

[16] F. Y. Wang and P. K. Wong, "Intelligent systems and technology for integrative and predictive medicine: An acp approach," *Acm Transactions on Intelligent Systems & Technology*, vol. 4, no. 2, p. 32, 2013.

[17] K. F. Wang, C. Gou, and F. Y. Wang, "Parallel vision: An acp-based approach to intelligent vision computing," *Acta Automatica Sinica*, vol. 42, no. 10, p. 1490, 2016.

[18] K. F. Wang, C. Gou, N. N. Zheng, J. M. Rehg, and F. Y. Wang, "Parallel vision for perception and understanding of complex scenes: Methods, framework, and perspectives," *Artificial Intelligence Review*, to be published.

[19] K. F. Wang, C. Gou, Y. J. Duan, Y. L. Lin, X. H. Zheng, and F. Y. Wang, "Generative adversarial networks: The state of the art and beyond," *Acta Automatica Sinica*, vol. 43, no. 3, pp. 321–332, 2017.

[20] F. Y. Wang, "Parallel control: A method for data-driven and computational control," *Acta Automatica Sinica*, vol. 39, no. 4, pp. 293–302, 2013.

[21] D. Li, H. Meng, and X. Shi, "Membership clouds and membership cloud generators," *Journal of Computer Research & Development*, vol. 61, no. 6, pp. 15–20, 1995.

[22] H. Cao and Y. Li, "Unraveling chaotic attractors by complex networks and measurements of stock market complexity.," *Chaos*, vol. 24, no. 1, p. 013134, 2014.

[23] A. Serletis and M. Shintani, "No evidence of chaos but some evidence of dependence in the us stock market ," *Chaos Solitons & Fractals*, vol. 17, no. 23, pp. 449–454, 2003.

[24] S. Chun, K. Kim, and S. H. Kim, "Chaotic analysis of predictability versus knowledge discovery techniques: case study of the polish stock market," *Expert Systems*, vol. 19, no. 5, pp. 264–272, 2002.

[25] M. T. Rosenstein, J. J. Collins, and C. J. De Luca, "A practical method for calculating largest lyapunov exponents from small data sets," *Physica D-nonlinear Phenomena*, vol. 65, no. 1-2, pp. 117–134, 1993.

[26] L. Jin, Y. Zhan, and L. U. Jun, "The non-linear chaotic improved model of the electric power system short-term load forecasting," *Proceedings of the Csee*, vol. 32, no. 4, pp. 12–15, 2000.

[27] Y. Zhao, S. Li, H. Lian, and Z. Wu, "A six-dimensional hyperchaotic system selection and its application in ds-cdma system," *Journal of Communications*, vol. 9, pp. 859–866, 2014.

[28] F. Zhang and J. M. Liu, "A new six-dimensional hyperchaotic system and its circuit implementation," *Science Technology & Engineering*, 2013.

[29] Q. Zhang, L. Guo, X. Xue, and X. Wei, "An image encryption algorithm based on dna sequence addition operation," in *International Conference on Bio-Inspired Computing, 2009. Bic-Ta*, pp. 1–5, 2009.