IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 31, 2019, accepted June 4, 2019, date of publication June 12, 2019, date of current version June 27, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2922376

A Color Image Encryption Using Dynamic DNA and 4-D Memristive Hyper-Chaos

ZHENTAO LIU[1,*], CHUNXIAO WU[1,*], JUN WANG[1], AND YUHEN HU[2], (Fellow, IEEE)
[1]School of Electronics and Information Engineering, Sichuan University, Chengdu 610065, China
[2]Department of Electrical and Computer Engineering, University of Wisconsin - Madison, Madison, WI 53706, USA

[*]*ZHENTAO LIU and CHUNXIAO WU contributed equally to this work.* Corresponding author: Jun Wang (jwang@scu.edu.cn)

This work was supported by the Sichuan Science and Technology Program under Grant 2018GZ0533.

ABSTRACT In this paper, a color image encryption is proposed based on the dynamic DNA and the 4-D memristive hyper-chaos. First, chaotic matrices are generated from the 4-D memristive hyper-chaos by using the plain image, the salt key, and control parameters. Second, the dynamic encoding process is performed on three components of the plain image to obtain three DNA matrices. Third, to enhance both the security and robustness of encrypted image, dynamic confusion and diffusion are applied to the encoded DNA matrices. Finally, the encrypted image is generated by DNA decoding and components combining. The main feature of our proposed algorithm is that dynamic DNA mechanism based on hyper-chaos is performed on the processes of encoding, confusion, and diffusion. Simulation results and security analysis further demonstrate that it has a strong resistance against various attacks and outperforms other methods in the literature.

INDEX TERMS Dynamic DNA, color image, encryption, memristive hyper-chaos.

I. INTRODUCTION

Currently, we are in a brilliant era of digital communication, where millions of digital images are transmitted and stored on the internet. It is imperative that the security of digital images with tremendous quantities of information should be guaranteed by reliable algorithms. The intrinsic features of digital images such as bulky data capacity, strong correlation among adjacent pixels and high redundancy make traditional encryption methods ineffective [1]. Moreover, there are many new issues in image encryption such as fast encryption in real-time system [2], [3], secure mechanism to generate one-time key [4], [5] and strong ability to resist various attacks [6], [7], etc. In image encryptions, the chaotic system is known as an ideal pseudo-random generator due to its various features such as high sensitivity to initial states, pseudo-randomness, ergodicity and non-periodicity [8]–[10]. Meanwhile, the DNA-based encryption method has aroused increasing attention owing to its excellent performance on confusion and diffusion [11]–[14]. The combination of DNA and chaos has aroused wide interest among scholars in image encryption [2], [15], [16].

However, the attacks against image encryption turn out to be various, including attacks based on statistical analysis, attacks based on cryptography analysis, attacks based on brute-force, attacks based on noise, occlusion or compression, etc. Few encryption methods can simultaneously satisfy the security and robustness to resist various attacks [17]–[20]. Designing an encryption algorithm with excellent security and robustness performance is a rewarding work nowadays.

Recently, many researchers proposed various image encryption algorithms based on chaos. Y. C. Zhou *et al.* proposed an effective chaotic system using a combination of two existing 1-D chaotic maps [21]. X. J. Wu *et al.* used three improved 1-D chaotic systems(LTS, LSS and TSS) in image encryption [14]. T. F. Zhang *et al.* proposed an encryption scheme based on three different 1-D chaotic maps in parallel-then-cascade fashion [22]. Moreover, Logistic map [23]–[25], Lorenz Chaos [23], [26], [27] and NCA map [28], [29] as three typical chaos are also widely used in image encryption. Since a color image encryption is our target, the high-dimensional chaos is concerned because it can provide us with complex and effective chaotic sequences for components, confusion and diffusion operations. Chen's system [24], [26], [30] is a classic hype-chaos wildly used in image encryption. According to its generation, chaotic

The associate editor coordinating the review of this manuscript and approving it for publication was Abdullah Iliyasu.

system can be divided into aerodynamic chaos [23], [27], spatiotemporal chaos [31]–[33], optical chaos [5], [34], [35] and memristive chaos [36]–[39]. Due to the characteristic of the memristor including non-volatility, nano-size and low power consumption, it is appropriate for designing chaotic circuits as a nonlinear circuit element. In 2015, J. Ma. *et al.* proposed a new 4-D memristive hyper-chaos based on a three-dimensional autonomous chaotic system by adding a smooth flux-controlled memristor and a cross-product item [40]. X. L. Chai *et al*. combined the 4-D memristive hyper-chaos with gene recombination [37] in an image encryption algorithm. The 4-D memristive hyper-chaos is quite appropriate for color image encryption due to its sensitivity to the initial key and complex dynamical behavior.

Nevertheless, the chaotic system is just an excellent pseudo-random number generator that establishes foundations for subsequent encryption steps. The combination of chaos and DNA operation for image encryption aroused widespread interest among scholars [12], [15], [16], [41]–[43] since DNA has massive parallelism, huge storage and ultra-low power consumption [11]. DNA encoding is the initial step that transforms a pixel matrix into a DNA encoded matrix for the subsequent DNA operation. The traditional DNA encoding is static since the mapping between '00','01','11','10' and 'AGCT' is fixed and linear [11], [13],[45]–[48], which is vulnerable to chosen-plaintext attack [17], [18]. One significant feature of such static encoding is that the distribution of encoded 'AGCT' is not uniform. Some researchers put forward some improvements based on pseudo dynamic encoding. X. J. Wu. *et al.* presented an encryption method where random numbers are used to choose the DNA encoding rules for three components [14]. In X. Q. Fu. *et al.*'s encryption scheme [34], the plain image was divided into 12 DNA planes where different encoding rules were adopted. X. Zhang. *et al.* proposed a DNA encoding method that the encoding rule of each pixel relies on the pixel's position [49]. However, such improvements are not really dynamic encoding method because the DNA encoding rule is still regular and static for different plain images. A really dynamic encoding method is a challenging and valuable work.

DNA operation involves DNA confusion and diffusion. DNA confusion will only change the value of every DNA unit, the position of which remains stable. Typical DNA confusion operation includes DNA Exclusive-OR [30], [50], addition [51], [52], subtraction [53] and complementary [50], [54], [55]. The security is not guaranteed if only using DNA confusion. Therefore, DNA confusion is usually combined with DNA diffusion. DNA diffusion will change the position of DNA units, which can easily lead to proliferation. It is proliferation that decreases the robustness though the diffusion is necessary and can enhance the security. Therefore, it is necessary and a challenge to develop an appropriate algorithm to simultaneously meet the security and robustness of the system based on dynamic DNA.

In this paper, a novel and efficient algorithm is proposed to realize secure and robust encryption. The proposed encryption algorithm is made of three parts: generation of the initial key and chaotic matrix, dynamic DNA encoding and dynamic DNA operation. Firstly, in order to guarantee the security of key communication, the idea of salt key is introduced, which is used to generate and process the chaotic matrix by the 4-D memristive hype-chaos. Secondly, considering the uneven AGCT distribution of traditional encoding method, the original RGB image is encoded to the DNA matrix using the dynamic DNA encoding rule. Thirdly, the dynamic DNA operation including DNA confusion and DNA diffusion is performed on the encoded DNA matrix. During the process of DNA operation, DNA confusion based on DNA XOR rule enhances the security, and DNA diffusion based on dynamic blocking method intensifies the robustness. Eventually, the encrypted images are obtained after DNA decoding and components combining. It is verified by simulation results and security analysis that the proposed encryption scheme has both high security and strong robustness, which can resist different kinds of attacks.

The sections of the paper are as follows. Some preliminary work and mathematical model are given in Section 2. In Section 3, the process of our encryption methods is presented. In Section 4, simulations and security analysis are made. Finally, the conclusion is given in Section 5.

II. PRELIMINARY WORKS

A. 4-D MEMRISTIVE HYPE-CHAOS

Employing a flux-controlled memristor, a 4-D memristive hype-chaos was proposed by J. Ma [40], which can be described as follow:

$$\begin{cases} \dot{x} = ax + byz \\ \dot{y} = cy + dxz - kyW(u) \\ \dot{z} = ez + fxy + gxu \\ \dot{u} = -y \end{cases} \tag{1}$$

where $a = 0.35, b = -10, c = -0.6, d = 0.3, e = -1.6, f = 2$, $W(u) = m + 3nu^2$, and k, m, n, g are positive control parameters. The simulation results of the 4-D memristive hype-chaos are shown in Fig. 1.

Bifurcations and Lyapunov exponents are two important factors to measure the dynamic behaviors of a chaotic system [56]. The simulation results are shown in Fig. 2, which indicates that the 4-D memristive chaotic system is ergodicity for encryptions.

B. DYNAMIC DNA ENCODING

The DNA molecule is two twisted strands which are composed of four bases, including adenine (A), guanine (G), cytosine(C), and thymine (T). As the Watson-Crick base pairing principle, A and T are complementary, and C and G are complementary. Essentially, the nucleotides sequence is a symbolic representation of biomolecular. Inspired by this,

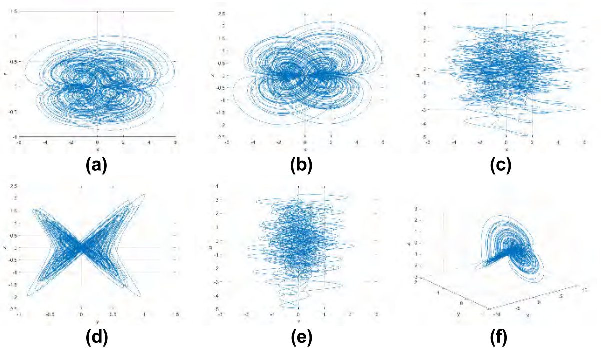


FIGURE 1. Simulation results. Projection on (a) x-y plane, (b) x-z plane, (c) x-u plane, (d) y-z plane, (e) z-u plane, and (f) x-y-z plane.

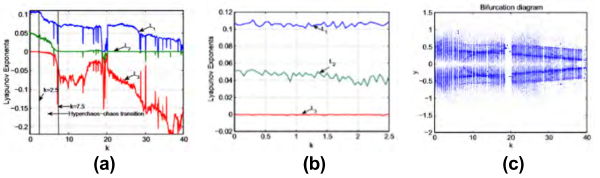


FIGURE 2. Bifurcations and Lyapunov exponents analysis. Two methods (a) QR decomposition-based method (when $g = 0.8$ and k increases from 0 to 40) and (b) Wolf method (when $g = 0.8$ and k increases from 0 to 2.5) are used to calculate Lyapunov exponents versus parameter k of the chaotic system. (c) Bifurcation diagram for increasing parameter k (from 0 to 40 with a step size 0.2).

we can represent A, T, C, and G as two binary numbers such as 00, 01, 10, 11. Basically, there are 24 DNA encoding rules. Nevertheless, due to the Watson-Crick base pairing principle, only 8 rules have been maintained. These 8 encoding rules are listed in Table. 1.

For a color image, the value of each pixel in one component can be represented by an 8-bit binary number which is encoded into four bases. After DNA encoding, the method of DNA confusion and DNA diffusion will be used in encryption steps. With the characteristics of massive parallelism, huge storage and ultra-low power consumption, DNA method has excellent performance in image encryption.

Traditionally, the DNA encoding scheme is fixed, which means that the same encoding rule is applied to all pixels in one image. Although some improvements have been made [14], [34], [49], these algorithms fail to show high security. Hence, a real dynamic encoding algorithm, in which the encoding rules depends on the chaotic matrix, could be a promising solution. We will discuss the algorithm in details in section 3.

III. PROPOSED ENCRYPTION ALGORITHM

The proposed encryption algorithm is made of three parts: A. generation of the initial key and the chaotic matrix, B. dynamic DNA encoding and decoding, C. DNA confusion and diffusion. The flow chart of the encryption algorithm is shown in Fig. 3. Similarly, the decryption algorithm is exactly the inverse of the encryption algorithm, which leads to a lossless recovery of the original color image. We will discuss the specific encryption parts as follows

TABLE 1. The DNA encoding rule.

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

A. GENERATION OF THE INITIAL KEY AND THE CHAOTIC MATRIX

The 4-D memristive hype-chaos is used to generate the DNA confusion and diffusion matrix. The security of the 4-D memristive hype-chaos relies on the key space of the initial key, hence the generation of the initial key is considered to be very important. The steps are as follows:

*Step*1: We use the hash algorithm of SHA-512 to generate the original key. M_o represents the pixel matrix of the original image. Hashing by SHA-512, we can get K_o. What needs to be emphasized is that K_o is a one-time key because K_o varies with different images

$$K_o = f_{Sha-512}(M_o) \tag{2}$$

*Step*2: Then the salt key K_s *is* added, and the value range of K_s is (0, 2^{512}-1). We combine K_o and K_s to hash by SHA-512 again. The output is the initial key K_i to generate the chaotic sequence. To be more intuitive, an example of the initial key generation is shown in Fig. 4.

$$K_i = f_{Sha-512}(K_o || K_s) \tag{3}$$

*Step*3: With the generation of the initial key, we can use it to obtain get the initial parameters for the chaotic system. Firstly, every 8 bits of the 512-bit K_i are combined into one block and we can get 64 blocks $b_1, b_2, \ldots, b_{64}$. Then every 4 blocks are grouped together, hence there will be 16 groups $g_1, g_2, \ldots, g_{16}$. The process will be shown in Fig. 5.

$$g_j = \{b_{4j-3}, b_{4j-2}, b_{4j-1}, b_{4j}\} \quad (1 \leq j \leq 16) \tag{4}$$

*Step*4: Random seeds $s_1, s_2, \ldots, s_{16}$ for our chaotic system are calculated as follows:

$$s_j = \prod_{m=0}^{3} \frac{b_{4j-m}}{2^7} (1 \leq j \leq 16) \tag{5}$$

*Step*5: Now we can use the random seeds to generate the initial parameters x_0, y_0, z_0 and u_0 for our chaotic system as follows:

$$x_0 = s_1 + s_2 + s_3 + s_4 \tag{6}$$
$$y_0 = s_5 + s_6 + s_7 + s_8 \tag{7}$$
$$z_0 = s_9 + s_{10} + s_{11} + s_{12} \tag{8}$$
$$u_0 = s_{13} + s_{14} + s_{15} + s_{16} \tag{9}$$

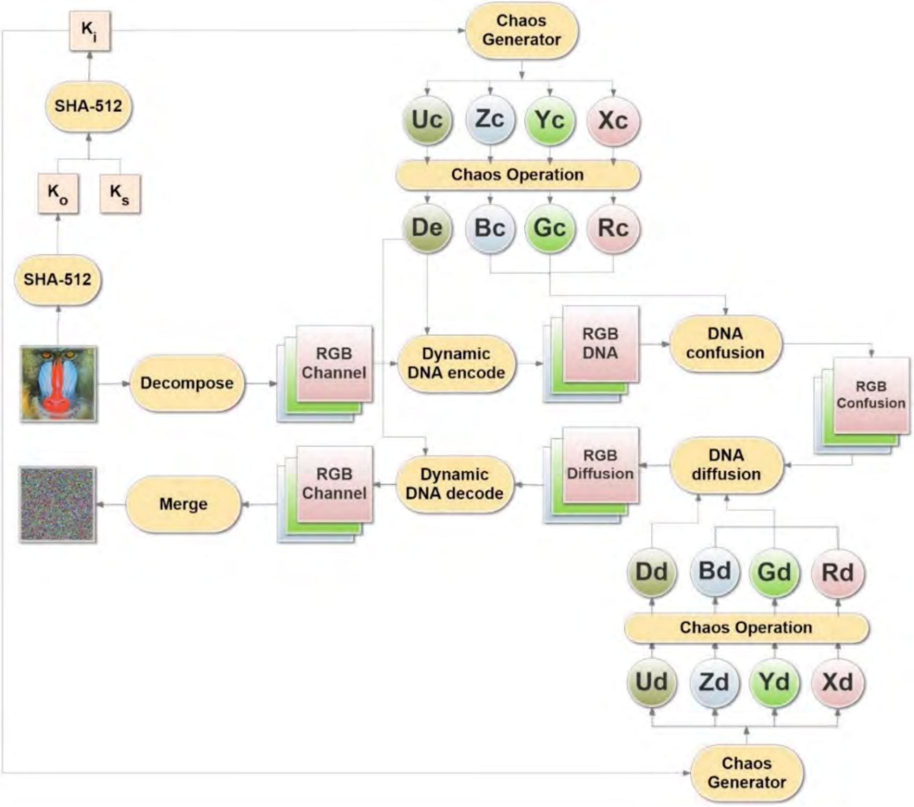


FIGURE 3. The flow chart of the proposed algorithm.

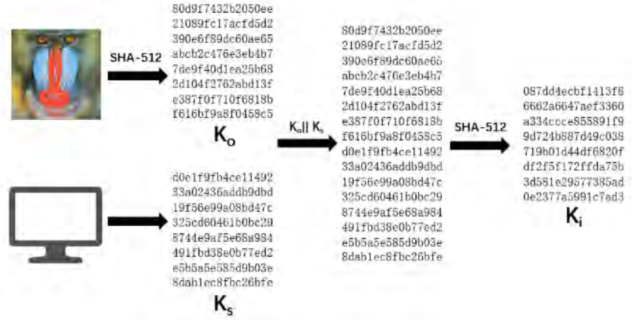


FIGURE 4. An example of the initial key generation.

*Step*6: When the initial parameters are generated, we can use them to generate the chaotic matrix. We need two types of chaotic matrix in our encryption algorithm. One is confusion chaotic matrix (X_c, Y_c, Z_c, U_c) used for DNA confusion operation and the other is diffusion chaotic matrix (X_d, Y_d, Z_d, U_d) used for DNA diffusion operation. If there is an image matrix of m rows and n columns, the size of confusion chaotic the matrix is m*n and the size of the diffusion chaotic matrix is $1 * n$.

*Step*7: We sort the chaotic matrices X_c, Y_c, Z_c, U_c, X_d, Y_d, Z_d, U_d and get the index of each element. Subsequently, based on the sorting and indexing, we get two groups of indexing matrices X_{ci}, Y_{ci}, Z_{ci}, U_{ci} and R_d, G_d, B_d, U_{di}.

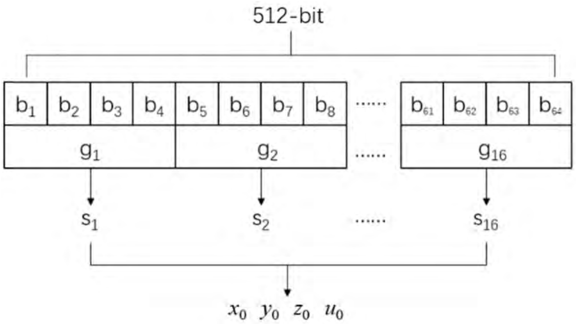


FIGURE 5. The generation of initial parameters.

Step 8: For each element $(x_{ci}, y_{ci}, z_{ci}, u_{ci},, u_{di})$ in X_{ci}, Y_{ci}, Z_{ci}, U_{ci}, U_{di}, we calculate by the following formula to get X'_{ci}, Y'_{ci}, Z'_{ci}, D_e, D_d.

$$x'_{ci} = \mathrm{mod}(x_{ci}, 4) \tag{10}$$

$$y'_{ci} = \mathrm{mod}(y_{ci}, 4) \tag{11}$$

$$z'_{ci} = \mathrm{mod}(z_{ci}, 4) \tag{12}$$

$$d_e = \mathrm{mod}(u_{ci}, 8) + 1 \tag{13}$$

$$d_d = \mathrm{mod}(u_{di}, 3) \tag{14}$$

Subsequently, we use DNA encoding rule (1) in Table 1 to encode each element in X'_{ci}, Y'_{ci}, Z'_{ci}. so that we can get R_c, G_c, B_c.

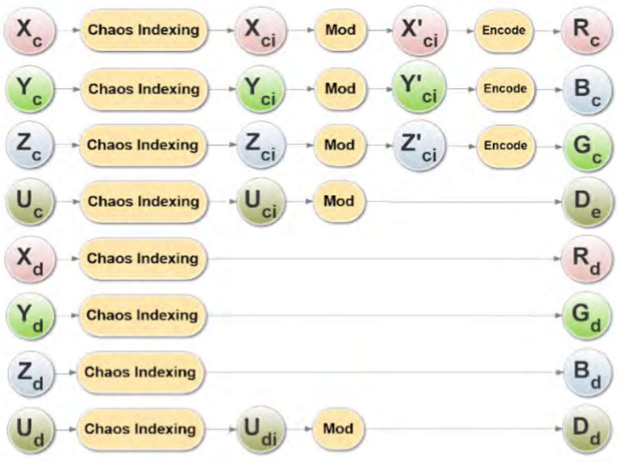
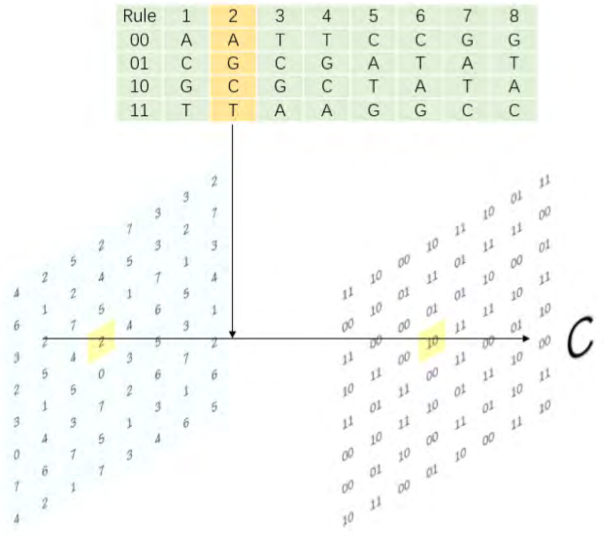


FIGURE 6. The flow chart of chaos operation.



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

FIGURE 7. An example of dynamic DNA encoding.

*Step*9: By *Step* 7∼8, eventually, we get the ultimate R_c, G_c, B_c, D_e and R_d, G_d, B_d, D_d. In the following steps, D_e will be used in the dynamic DNA encoding, R_c, G_c, B_c will be used in the DNA confusion and R_d, G_d, B_d, D_d will be used in the DNA diffusion. Fig.6 is the flow chart of chaos operation.

B. THE DYNAMIC DNA ENCODING

*Step*1: We decompose the original image (m×n) into three components *R*, *G* and *B*.

*Step*2: Every pixel of the RGB matrix is transformed into 8-bit binary number and hence we can get three different matrices R_B G_B and B_B, the size of which is m×8n.

*Step*3: Every binary number of the R_B, G_B, B_B is encoded dynamically according to Table 1 and the results are R_D, G_D, B_D. The dynamic encoding rule matrix is D_e generated in Section III. A. Step 7∼8. An Example of dynamic encoding is shown in Fig. 7.

TABLE 2. DNA XOR rule.

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

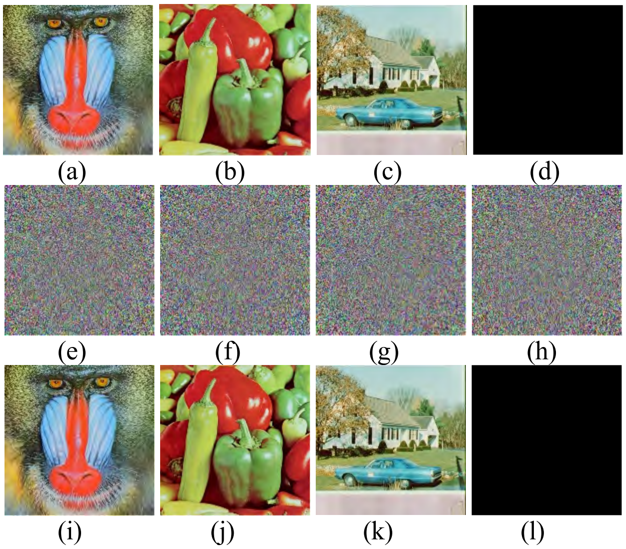


FIGURE 8. Results of (a) Baboon, (b) Pepper, (c) House, and (d) Black. (e)-(h) and (i)-(l) are encrypted and decrypted images, respectively.

C. DYNAMIC DNA CONFUSION AND DIFFUSION

*Step*1: We use the DNA XOR rule to realize DNA confusion according to Table 2.

*Step*2: To intensify the robustness of our encryption system, the process of DNA diffusion is performed in groups. However, if the DNA diffusion rule is definite, the complexity of encryption can't be guaranteed. Therefore, we use another kind of chaotic matrices to make the DNA diffusion process complicated. According to Fig. 6, the diffusion chaotic matrices are X_d, Y_d, Z_d, U_d, R_d, G_d, B_d represents three different DNA diffusion rules. Which rule we use to diffuse each row is determined by D_d. Assume that *i* represents the *i*-th row of the DNA matrix, the rules are as follows:

if $D_d[i]=0$, then use rule R_d;
if $D_d[i]=1$, then use rule G_d;
if $D_d[i]=2$, then use rule B_d.

*Step*3: Use the dynamic DNA decoding rule to get the binary matrix. Then transform the binary matrix into the pixel matrix of *R*, *G*, *B* components.

*Step*4: Eventually, we combine the three components into the encrypted image.

IV. EXPERIMENT AND SECURITY ANALYSIS

A. RESULTS OF ENCRYPTION AND DECRYPTION

We use four RGB color images of size 256 × 256 to simulate the encryption and decryption: Baboon, Pepper, Lake and

TABLE 3. Parameters of our simulation.

Item	Value
Salt Key	d0e1f9fb4ce1149233a02436addb9dbd19f56e99a0 8bd47c325cd60461b0bc298744e9af5e68a984491fbd 38e0b77ed2e5b5a5e585d9b03e8dab1ec8fbc26bfe

Initial Parameter	a = 0.35, b = -10, c = -0.6,
	d = 0.3, e = -1.6, f = 2

Control Parameter	r = 0.1, s = 0.01, k = 0.2, g = 0.1

Black. Some initial parameters and control parameters are shown in Table 3.

The simulation environment is Windows 10, 8.00GB RAM, i7-7500U CPU and the development tool is Python 3.6. The simulation results are shown in Fig. 8.

B. KEY ANALYSIS

1) KEY SPACE ANALYSIS

The key space of an encrypted algorithm is the size of the encryption key. The ability of an encryption system to resist the brute force attack relies on the size of key space. The key space of the proposed algorithms depends on the initial parameters and the control parameters of the 4-D memristive hype-chaos, which are x_0, y_0, z_0, u_0, etc. If the accuracy of the computer is 10^{-14}, the key space of our system will be 10^{112}, which indicates that the proposed algorithm has a strong ability to resist the brute force attack. The secret key's space in this paper is much larger than that in [28], [37], [44], [47], [57]. Additionally, the generation of keys depends on the combination of the one-time pad and the salt key, which makes it rather difficult for attackers to predict the encryption key.

2) KEY SENSITIVITY ANALYSIS

Key sensitivity is another important feature for an encryption system to defend against brute force attack. For an ideal encryption system, a slight change in the initial key will lead to a totally different decryption image. In our experiment, we make a tiny difference (only change the least-significant bit of the initial key's 512-bit hash value) in four RGB color images respectively.The decryption results and the significant differences between the original images (256 × 256) and the decrypted images are shown in Fig. 9.

C. STATISTICAL ANALYSIS

We use various statistical analysis to test the complexity of our encryption algorithm, including the analysis of information entropy, histogram, and correlation coefficient.

1) INFORMATION ENTROPY

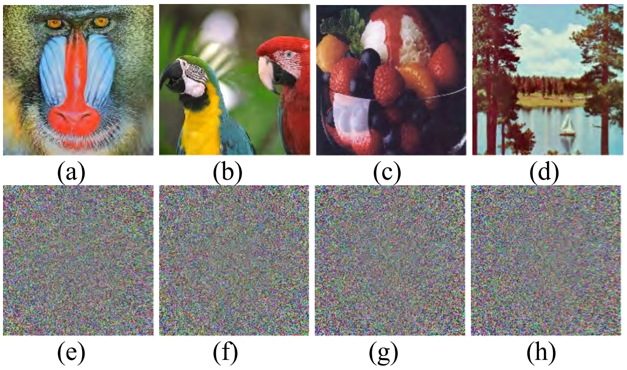


FIGURE 9. The key sensitivity test results of (a) Baboon, (b) Birds, (c) Fruits and (d) Lake. (e)-(h) are corresponding decrypted images.

TABLE 4. The results of entropy analysis.

	Original Image			Encrypted Image		
	R	G	B	R	G	B
Lena	7.2531	6.9686	7.5952	7.9992	7.9993	7.9994
Peppers	7.3282	7.0912	7.5415	7.9992	7.9993	7.9991
Baboon	7.7326	7.7591	7.4557	7.9993	7.9993	7.9993
Birds	7.4711	7.2205	7.6080	7.9992	7.9992	7.9993
House	7.4156	7.4354	7.2295	7.9992	7.9992	7.9992
Lake	7.3074	7.2747	7.6369	7.9992	7.9989	7.9990
Fruits	4.7681	4.3149	3.8754	7.9991	7.9985	7.9988
Black	0	0	0	7.9965	7.9948	7.9955
White	0	0	0	7.9914	7.9942	7.9856

Information entropy is a very useful statistical indicator to measure how stochastic a system is, which was firstly introduced by Claude Shannon in 1948. It can be described in Eq. (15), where $p(m_i)$ denotes the probability that the symbol m_i appears, and K is the total number of image pixels. In image encryption, it can effectively measure the complexity of encryption algorithms. For an ordinary image, its information entropy ranges from 0 to 8. For an encrypted image, its information entropy is always above 7.9. The closer the information entropy of an encrypted image is, the more brilliant the entropy algorithm is.

$$H(m) = -\sum_{i=0}^{K} p(m_i) \log_2 p(m_i) \tag{15}$$

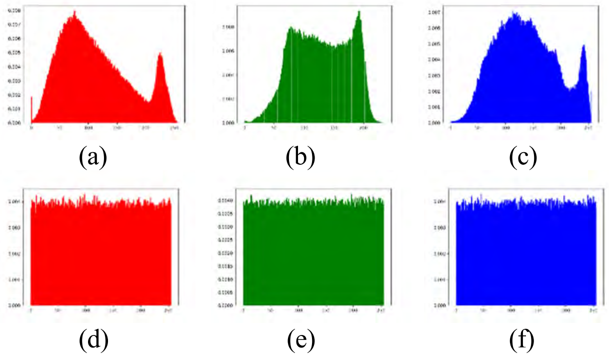
We choose 7 typical color images and all white/black images to measure the information entropy of original and encrypted images in three components. The size of these images are all 256 × 256. the entropy results are shown in Table 4. Table 5 shows that the proposed encryption algorithm outperforms the others in the literature.

2) THE HISTOGRAM ANALYSIS

The histogram analysis is a very useful tool to measure the distribution of an image. Ordinary images usually have uneven distributions, while encrypted images have uniform distributions. A more uniform histogram can resist statistic attacks better. Mathematically, the variances of histograms can be used to quantitatively measure how uniform the

TABLE 5. Comparison with other algorithms in entropy analysis.

	R	G	B
Lena	7.2531	6.9686	7.5952
Proposed	7.9992	7.9993	7.9994
Ref. [14]	7.9893	7.9896	7.9903
Ref. [28]	7.9892	7.9898	7.9899
Ref. [47]	7.9903	7.9890	7.9893
Ref. [58]	7.9973	7.9969	7.9971
Ref. [59]	7.9874	7.9872	7.9866
Ref. [60]	7.9896	7.9893	7.9896
Ref. [61]	7.9901	7.9912	7.9921


(a) (b) (c)

(d) (e) (f)

FIGURE 10. Histograms of Baboon in red, green, and blue. Histograms of original and corresponding encrypted images in row 1 and 2, respectively.

TABLE 6. The Histogram variances analysis of original images (256 x 256) and encrypted images (256 x 256).

	Original Image			Encrypted Image		
	R	**G**	**B**	**R**	**G**	**B**
Baboon	3.07×10^5	5.85×10^5	3.11×10^5	1.08×10^3	9.54×10^2	1.04×10^3
Bird	1.03×10^6	5.27×10^5	1.61×10^6	1.18×10^3	1.00×10^3	1.20×10^3
Fruits	1.77×10^7	2.27×10^7	3.13×10^7	1.31×10^3	1.70×10^3	2.21×10^3
House	7.68×10^5	1.33×10^6	9.92×10^5	1.22×10^3	1.23×10^3	1.15×10^3
Lake	8.00×10^5	5.37×10^5	1.22×10^6	1.14×10^3	1.46×10^3	1.53×10^3
Lena	1.02×10^6	4.54×10^5	1.38×10^6	1.11×10^3	9.18×10^2	1.05×10^3
Peppers	8.69×10^5	9.33×10^5	1.69×10^6	1.13×10^3	1.27×10^3	1.06×10^3
White	2.67×10^8	2.67×10^8	2.67×10^8	1.29×10^4	2.17×10^4	8.53×10^3
Black	2.67×10^8	2.67×10^8	2.67×10^8	5.17×10^3	1.10×10^4	7.78×10^3

TABLE 7. The results of correlation analysis.

		Original Image			Encrypted Image		
		R	**G**	**B**	**R**	**G**	**B**
Baboon	H	0.9225	0.8810	0.9283	0.0012	-0.0018	-0.0042
	V	0.8497	0.7860	0.8799	-0.0036	0.0038	0.0022
	D	0.8377	0.7609	0.8535	0.0002	0.0053	0.0011
Birds	H	0.9651	0.9567	0.9653	0.0015	-0.0009	0.0012
	V	0.9680	0.9474	0.9570	0.0026	-0.0047	-0.0011
	D	0.9542	0.9300	0.9414	-0.0014	-0.0006	-0.0033
Black	H	NA	NA	NA	0.0013	-0.0008	-0.0014
	V	NA	NA	NA	-0.0003	0.0005	0.0023
	D	NA	NA	NA	-0.0031	-0.0015	-0.0008
Fruits	H	0.9739	0.9604	0.9667	-0.0007	-0.0019	0.0023
	V	0.9775	0.9697	0.9758	0.0015	-0.0021	-0.0022
	D	0.9710	0.9602	0.9649	0.0031	0.0020	-0.0023
House	H	0.9534	0.9429	0.9707	0.0006	0.0031	0.0031
	V	0.9571	0.9154	0.9672	-0.0020	-0.0014	0.0009
	D	0.9169	0.8699	0.9424	0.0045	-0.0039	0.0004
Lake	H	0.9549	0.9745	0.9785	0.0009	0.0067	0.0017
	V	0.9435	0.9745	0.9767	-0.0021	-0.0024	0.0020
	D	0.9246	0.9585	0.9618	0.0001	0.0001	0.0003
Lena	H	0.9758	0.9657	0.9330	0.0008	0.0031	0.0018
	V	0.9876	0.9829	0.9573	0.0009	-0.0018	-0.0039
	D	0.9632	0.9538	0.9173	-0.0036	-0.0033	-0.0058
Peppers	H	0.9754	0.9847	0.9745	0.0045	-0.0005	0.0017
	V	0.9769	0.9853	0.9752	-0.0022	0.0003	-0.0004
	D	0.9663	0.9735	0.9599	0.0010	-0.0002	-0.0022
White	H	NA	NA	NA	-0.0017	-0.0015	0.0003
	V	NA	NA	NA	0.0000	0.0005	-0.0013
	D	NA	NA	NA	-0.0036	0.0028	-0.0013

histogram is, which is defined as follows:

$$var(X) = \frac{1}{2n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}(x_i - x_j)^2 \tag{16}$$

where $x_1, x_2, \ldots, x_{255}$ are 255 different histogram values and x_i and x_j are the numbers of pixels whose values equal to i and j.

The histogram results of the original and encrypted images of Baboon (256 × 256) in three components are shown in Fig. 10 and the histogram variance analysis results are shown in Table 6. Significant differences are shown between original and encrypted images.

3) CORRELATION COEFFICIENT ANALYSIS

For digital images, the correlation between adjacent pixels tends to be very large. Attackers can take advantage of such a feature to achieve decipher. Therefore, algorithm design should make the correlation of adjacent as negligible as possible. We can calculate the correlation coefficient by

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)D(y)}} \tag{17}$$

$$E(x) = \frac{1}{K}\sum_{i=1}^{K} x_i \tag{18}$$

$$D(x) = \frac{1}{K}\sum_{i=1}^{K}(x_i - E(x))^2 \tag{19}$$

$$cov(x, y) = \frac{1}{K}\sum_{i=1}^{K}(x_i - E(x))(y_i - E(y)) \tag{20}$$

where x, y refer to the grayscale values of two adjacent pixels in the image, and K is the total number of pixels randomly selected from the image. In our experiment, we randomly select 100000 pairs of adjacent pixels to test the correlation coefficient of 9 original images (256 × 256) and their corresponding encrypted images horizontally, vertically and diagonally. The results are shown in Table 7.

We also make correlation analysis with the grayscale image of Lena (256 × 256) to make comparisons with other algorithms, and the results are shown in Table 8. Moreover, the distribution of adjacent pixels of Peppers and its encrypted image is shown in Fig. 11. It is clear that most points in the plain image have strong correlation while points in the encrypted image are in random distribution.

TABLE 8. Comparison with other algorithms in correlation analysis.

	Horizontal	Vertical	Diagonal
Lena	0.9770	0.9874	0.9686
Proposed	0.0011	−0.0013	−0.0019
Ref. [7]	0.0024	−0.0006	0.0012
Ref. [15]	0.0020	−0.0007	−0.0014
Ref. [14]	−0.0082	−0.0128	−0.0012
Ref. [24]	0.0022	0.0001	−0.0017
Ref. [42]	0.0058	0.0022	0.0031
Ref. [58]	−0.0027	0.0033	−0.0035
Ref. [62]	0.0080	0.0035	0.0024
Ref. [63]	0.0214	0.0465	−0.0090
Ref. [64]	0.0373	0.0228	−0.0221
Ref. [65]	−0.0001	0.0089	0.0091
Ref. [66]	0.0017	0.0016	0.0014
Ref. [67]	−0.0152	0.0014	0.0218

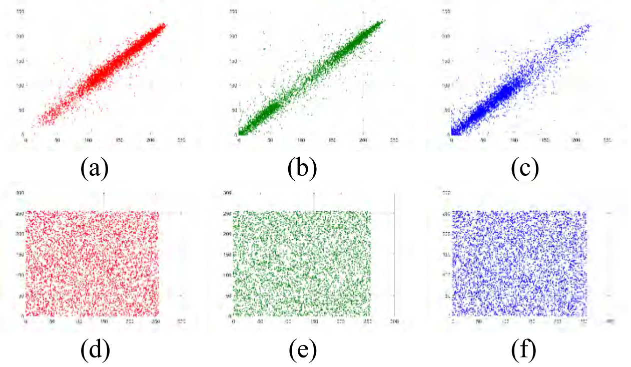

(a) (b) (c)
(d) (e) (f)

FIGURE 11. Distribution of adjacent pixels in three components. (a) horizontal, (b) vertical and (c) diagonal direction of Baboon. (d) horizontal, (e) vertical and (f) diagonal direction of encrypted Baboon.

D. ROBUSTNESS ANALYSIS

Robustness is another indicator to evaluate image encryption algorithms. There are three important elements of information security: confidentiality, integrity and availability. The statistical randomness can guarantee confidentiality, while the robustness can guarantee integrity and availability. Some typical robustness analysis such as the noise and the occlusion attacks will be discussed as follows.

1) NOISE ATTACK

In reality, when transmitted in the communication channel, the encrypted image may be affected by various noises. The image distortion caused by various noises makes it very difficult to recover the original image. Thus, the robustness resisting noise attack is of great significance to evaluate the performance of the encryption algorithm. We added three typical noises (Gaussian, speckle and salt-and-pepper noises) to the encrypted images and then decrypted them. The results are shown in Figs. 12-14.

2) OCCLUSION ATTACK

Due to the instability of the network, the encrypted image may lose some information when transmitted in the network. Occlusion attack is used to test the capacity of recovering original images from cipher images that have lost some information. Baboon and House (256 × 256) are used in occlusion attack, and the results are shown in Fig. 15.

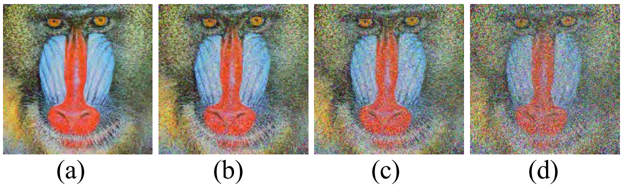

(a) (b) (c) (d)

FIGURE 12. Salt-and-pepper noise attack of Baboon (256 × 256). Decrypted images with density value (a) 0.1, (b) 0.2, (c) 0.3, (d) 0.5.

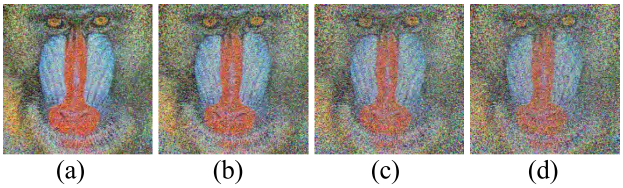

(a) (b) (c) (d)

FIGURE 13. Speckle noise attack of encrypted Baboon (256 × 256). Decrypted images with variance value (a) 0.05, (b) 0.1, (c) 0.2, (d) 0.3.

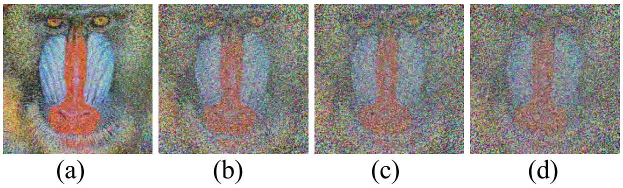

(a) (b) (c) (d)

FIGURE 14. Gaussian noise attack of encrypted Baboon (256 × 256). Decrypted images with variance value (a) 0.01, (b) 0.1, (c) 0.2, (d) 0.3.

3) JPEG COMPRESSION

JPEG is a common compression standard. In the quantization process of JPEG algorithm, a lot of information of the encrypted image will be lost, which makes it difficult to recover. In this simulation, we compress the encrypted images by JPEG with the compression rate of 1:2.5 and then decrypt them. We use four images (256 × 256) to evaluate the robustness against JPEG compression attacks. The results are shown in Fig. 16.

E. CLASSIC CRYPTOGRAPHY ATTACK

In this subsection, we analyze the ability of our encryption algorithms to resist some typical cryptography attacks, including differential attack, chosen-plaintext attack and communication attack.

1) DIFFERENTIAL ATTACK

Differential attack is a very typical attack in image encryption. The attackers usually repeatedly change some different pixels in the original images and then encrypted it. By doing so, they may find the association between two different cipher images. Therefore, for an ideal encryption algorithm, a slight change in an original image can lead to entirely different encrypted image. There are two criteria called the number of pixel change rate (NPCR) and the unified average changing

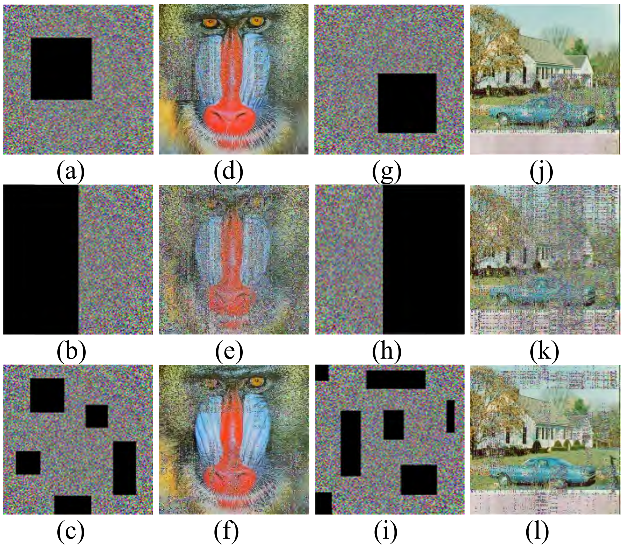


FIGURE 15. Results of occlusion attack: (a)-(c) three different occlusion attack of encrypted Baboon. (d)-(e) decrypted images of (a)-(c), respectively. (g)-(i) three different occlusion attack of encrypted House. (j)-(l) decrypted images of (g)-(i), respectively.

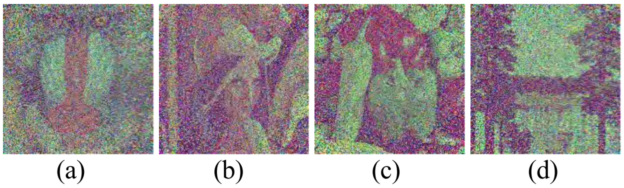


FIGURE 16. Results of JPEG compression attack. Decrypted images of (a) Baboon, (b) Lena, (c) Peppers, and (d) Lake.

intensity (UACI) to test the ability of an encryption algorithm to resist the differential attack, which can be calculated as follows:

$$NPCR = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} D(i,j)}{M \times N} \times 100\% \tag{21}$$

$$D(i,j) = \begin{cases} 1 & if \ \ P(i,j) \neq C(i,j) \\ 0 & else \end{cases} \tag{22}$$

$$UACI = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} \frac{|P(i,j)-C(i,j)|}{255}}{M \times N} \times 100\% \tag{23}$$

where $P(i,j)$ and $C(i,j)$ are pixel values of the original image and its corresponding encrypted image, respectively.

For encryption algorithms of great performance, NPCR is always above 99% and UACI is always 25%, And For original images of different characteristic, the value of NPCR and UACI varies. In our experiment, we use different pairs of original and encrypted images to test NPCR and UACI. The results are shown in Table 9.

TABLE 9. The results of differential attack.

	NPCR			UACI		
	R	G	B	R	G	B
Lena	0.9960	0.9959	0.9964	0.3306	0.3059	0.2760
Peppers	0.9961	0.9962	0.9962	0.2892	0.3383	0.3384
Baboon	0.9962	0.9962	0.9962	0.2988	0.2844	0.3104
Birds	0.9963	0.9960	0.9961	0.3140	0.3002	0.3479
House	0.9961	0.9961	0.9963	0.3022	0.3128	0.3123
Lake	0.9961	0.9961	0.9961	0.2799	0.3415	0.3428
Fruits	0.9960	0.9961	0.9961	0.3282	0.3417	0.3296
Black	0.9958	0.9961	0.9963	0.5014	0.5000	0.4996
White	0.9959	0.9962	0.9963	0.4999	0.4997	0.5002

TABLE 10. The comparisons of four typical attacks.

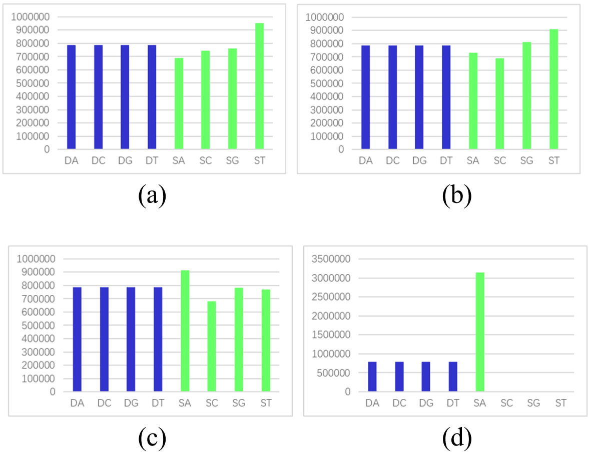
Attack	Known	Unknown
Ciphertext-only	Only string of ciphertext (its corresponding plaintext is unknown)	Plaintext, Secret key
Known-plaintext	String of ciphertext and corresponding ciphertext	Secret key
Chosen-ciphertext	Choose some specific ciphertext and construct its corresponding plaintext	Secret key
Chosen-plaintext	Choose some specific plaintext and construct its corresponding ciphertext	Secret key

2) CHOSEN-PAINTEXT ATTACK

According to Kerkhoff's principle, when cryptanalyzing a cryptosystem, the attacker knows everything about the cryptosystem except the secret key. There are four typical cryptography attacks including ciphertext-only attack, known-plaintext attack, chosen-plaintext attack and chosen-ciphertext attack [68]. The comparisons of these attacks are shown in Table 10.

According to Table 10, chosen-plaintext attack is the most effective and powerful. If one encryption algorithm can defend against chosen-plaintext attack, it can also resist other cryptography attacks. In our algorithm, a slight change in the original image can lead to significant differences in the chaotic matrix, which indicates that the chaotic matrix is very sensitive to original images. Moreover, the proposed algorithm is sensitive to the control parameters k, m, n, g and the salt key. For different plain images, the original keys are different and subsequently generate various control parameters. And for different users, the salt keys are also different. Additionally, the process of DNA diffusion in our algorithm makes the encrypted value of each pixel influenced by other encrypted pixels.

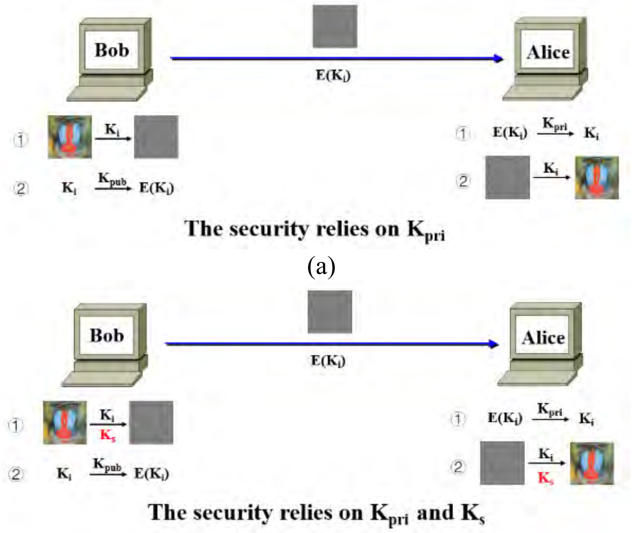
For traditional static DNA encoding, the mapping between pixel value and DNA value is fixed, linear and simple, which makes it easy for attackers to find such mapping. We find that the distribution of 'AGCT' can measure how complex the mapping is. In traditional encoding methods, the distribution of 'AGCT' in DNA-encoded matrix tends to be uneven. For instance, if there are more '11' in an original image, there will be more 'T' by static encoding. In order to avoid such a risk of chosen-plaintext attack, we choose dynamic DNA encoding to make 'AGCT' distribution as uniform as possible. In Fig. 17, we compare the distribution of 'AGCT' between static DNA encoding and dynamic DNA encoding.



(a) (b)

(c) (d)

FIGURE 17. The distribution of 'AGCT' of (a) Lena, (b)Baboon, (c) Peppers and (d) Blank. Results in blue and yellow bars are dynamic and static DNA encoding, respectively.


Bob
Alice
E(K$_i$)
①
K$_i$
②
K$_{pub}$
K$_{pri}$
K$_s$
The security relies on K$_{pri}$
The security relies on K$_{pri}$ and K$_s$

(a)

(b)

FIGURE 18. The difference of key exchange between (a) traditional method and (b) our method.

Therefore, based on the discussion above, the mechanism of key generation, DNA encoding, DNA confusion and DNA diffusion can guarantee that our encryption algorithm can well resist the chosen-plaintext attack and other cryptography attacks

3) COMMUNICATION ATTACK

In this subsection, we will focus on the security analysis of communication. In digital communications, attackers may intercept and capture the one-time pad of the encrypted image. Although the one-time pad can be encrypted before sending, it is not a wise idea that the security of the image transformation system only relies on whether the one-time pad will be deciphered. To avoid the risk of such an attack, we introduce another two security mechanisms compared with the traditional methods.

Firstly, the salt key is introduced into our encryption system. After generating the one-time pad by hashing the original image, we combine it with a 512-bit salt key to hash them together in order to generate the initial key. Even if the one-time pad is intercepted and deciphered by attackers during communication, it is impossible for attackers to generate the initial key without the salt key. Additionally, the key of control parameters in the chaotic system also guaranteed the security of the encryption system. Even if attackers somehow get the salt key to generate the initial key, they can't generate the correct chaotic sequence without the control parameters. Based on what we have discussed, we can conclude that the proposed algorithm can better defend against the communication attack. The comparison between traditional methods and our method is shown in Fig. 18.

V. CONCLUSION

In this paper, a novel encryption method is proposed by using the dynamic DNA and the 4-D memristive hype-chaos. Firstly, the one-time pad and the salt key are combined to generate the initial parameters of the memristive chaotic system of which the chaotic matrix relies on. Secondly, the dynamic encoding method based on the chaotic matrix is introduced for the process of DNA encoding. Then, dynamic DNA confusion and diffusion are used to enhance the security of the encryption algorithm. Meanwhile, the process of dynamic DNA diffusion is calculated by blocks, which can guarantee the robustness of the proposed encryption. After DNA decoding and combining of three components, the ultimate encrypted image is obtained. Simulation results verify both the security and robustness of the proposed encryption algorithm. Additionally, our encryption algorithm can defend against varieties of typical attacks. Therefore, our encryption algorithm is quite suitable for image encryption.

REFERENCES

[1] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption," *Nonlinear Dyn.*, vol. 92, no. 2, pp. 305–313, Apr. 2018.

[2] X. Wang, L. Feng, and H. Y. Zhao, "Fast image encryption algorithm based on parallel computing system," *Inf. Sci.*, vol. 486, pp. 340–358, Jun. 2019.

[3] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, Aug. 2011.

[4] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Math. Appl.*, vol. 59, no. 10, pp. 3320–3327, May 2010.

[5] J. Zhang, C. Feng, M. Zhang, and Y. Liu, "One-time pad image encryption based on physical random numbers from chaotic laser," *Opt. Rev.*, vol. 25, no. 5, pp. 540–548, Oct. 2018.

[6] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dyn.*, vol. 62, no. 3, pp. 615–621, Nov. 2010.

[7] Y.-Q. Zhang and X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Appl. Soft. Comput.*, vol. 26, pp. 10–20, Jan. 2015.

[8] C. Pak and L. L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Process.*, vol. 138, pp. 129–137, Sep. 2017.

[9] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Opt. Laser Technol.*, vol. 101, pp. 30–41, May 2018.

[10] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Opt. Lasers Eng.*, vol. 66, pp. 10–18, Mar. 2015.

[11] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.

[12] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2," *Nonlinear Dyn.*, vol. 83, no. 3, pp. 1123–1136, Feb. 2016.

[13] M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography," *Signal Process.*, vol. 125, pp. 187–202, Aug. 2016.

[14] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Appl. Soft Comput.*, vol. 37, pp. 24–39, Dec. 2015.

[15] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Opt. Lasers Eng.*, vol. 73, pp. 53–61, Oct. 2015.

[16] 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 Comput. Appl.*, vol. 31, no. 1, pp. 219–237, Jan. 2019.

[17] A. Akhavan, A. Samsudin, and A. Akhshani, "Cryptanalysis of an image encryption algorithm based on DNA encoding," *Opt. Laser Technol.*, vol. 95, pp. 94–99, Oct. 2017.

[18] X. Su, W. Li, and H. Hu, "Cryptanalysis of a chaos-based image encryption scheme combining DNA coding and entropy," *Multimedia Tools Appl.*, vol. 76, no. 12, pp. 14021–14033, Jun. 2017.

[19] W. Feng, Y. He, H. Li, and C. L. Li, "Cryptanalysis and improvement of the image encryption scheme based on 2D logistic-adjusted-sine map," *IEEE Access*, vol. 7, pp. 12584–12597, 2019.

[20] C. Li, D. Lin, B. Feng, J. Lü, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018.

[21] Y. C. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process.*, vol. 97, pp. 172–182, Apr. 2014.

[22] T. Zhang, S. Li, R. Ge, M. Yuan, and Y. Ma, "A novel 1D hybrid chaotic map-based image compression and encryption using compressed sensing and Fibonacci–Lucas transform," *Math. Problems Eng.*, vol. 2016, Apr. 2016, Art. no. 7683687.

[23] A. Girdhar and V. Kumar, "A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences," *Multimedia Tools Appl.*, vol. 77, no. 20, pp. 27017–27039, Oct. 2018.

[24] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Opt. Lasers Eng.*, vol. 90, pp. 225–237, Mar. 2017.

[25] A. U. Rehman and X. F. Liao, "A novel robust dual diffusion/confusion encryption technique for color image based on Chaos, DNA and SHA-2," *Multimedia Tools Appl.*, vol. 78, no. 2, pp. 2105–2133, Jan. 2019.

[26] T. Hu, Y. Liu, L. H. Gong, and C.-J. Ouyang, "An image encryption scheme combining chaos with cycle operation for DNA sequences," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 51–66, Jan. 2017.

[27] M. Kaur and V. Kumar, "Efficient image encryption method based on improved Lorenz chaotic system," *Electron. Lett.*, vol. 54, no. 9, pp. 562–563, May 2018.

[28] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys," *Signal Process.*, vol. 148, pp. 272–287, Jul. 2018.

[29] I. Hussain, T. Shah, and M. A. Gondal, "An efficient image encryption algorithm based on S_8 S-box transformation and NCA map," *Opt. Commun.*, vol. 285, no. 24, pp. 4887–4890, Nov. 2012.

[30] A. U. Rehman, X. Liao, R. Ashraf, S. Ullah, and H. Wang, "A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2," *Optik*, vol. 159, pp. 348–367, Apr. 2018.

[31] Y.-L. Luo and M.-H. Du, "A self-adapting image encryption algorithm based on spatiotemporal chaos and ergodic matrix," *Chin. Phys. B*, vol. 22, no. 8, Aug. 2013, Art. no. 080503.

[32] Y. Zheng and J. Jin, "A novel image encryption scheme based on Hénon map and compound spatiotemporal chaos," *Multimedia Tools Appl.*, vol. 74, no. 18, pp. 7803–7820, Sep. 2015.

[33] X. Wang, L. Feng, S. Wang, Z. Chuan, and Y. Zhang, "Spatiotemporal chaos in coupled logistic map lattice with dynamic coupling coefficient and its application in image encryption," *IEEE Access*, vol. 6, pp. 39705–39724, 2018.

[34] X.-Q. Fu, B.-C. Liu, Y.-Y. Xie, W. Li, and Y. Liu, "Image encryption-then-transmission using DNA encryption algorithm and the double chaos," *IEEE Photon. J.*, vol. 10, no. 3, Jun. 2018, Art. no. 3900515.

[35] Y. Xie, J. Li, Z. Kong, Y. Zhang, X. Liao, and Y. Liu,, "Exploiting optics chaos for image encryption-then-transmission," *J. Lightw. Technol.*, vol. 34, no. 22, pp. 5101–5109, Nov. 15, 2016.

[36] 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 Process., Image Commun.*, vol. 52, pp. 6–19, Mar. 2017.

[37] 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," *Chin. Phys. B*, vol. 25, no. 10, Oct. 2016, Art. no. 100503.

[38] N. Du, N. Manjunath, Y. Shuai, D. Buerger, I. Skorupa, R. Schueffny, C. Mayr, D. N. Basov, M. Di Ventra, O. G. Schmidt, and H. Schmidt, "Novel implementation of memristive systems for data encryption and obfuscation," *J. Appl. Phys.*, vol. 115, no. 12, Mar. 2014, Art. no. 124501.

[39] P. Li, J. Xu, J. Mou, and F. Yang, "Fractional-order 4D hyperchaotic memristive system and application in color image encryption," *EURASIP J. Image Video Process., Jan*, vol. 2019, p. 22, Dec. 2019.

[40] J. Ma, Z. Chen, Z. Wang, and Q. Zhang, "A four-wing hyper-chaotic attractor generated from a 4-D memristive system with a line equilibrium," *Nonlinear Dyn.*, vol. 81, no. 3, pp. 1275–1288, Aug. 2015.

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

[42] R. Enayatifar, A. H. Abdullah, and I. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Opt. Lasers Eng.*, vol. 56, pp. 83–93, May 2014.

[43] X. Chai, Z. Gan, Y. Lu, Y. Chen, and D. Han, "A novel image encryption algorithm based on the chaotic system and DNA computing," *Int. J. Mod. Phys. C*, vol. 28, no. 5, May 2017, Art. no. 1750069.

[44] Q. Zhang, L. Liu, and X. Wei, "Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps," *Int. J. Electron. Commun.*, vol. 68, no. 3, pp. 186–192, Mar. 2014.

[45] S. Sun, "A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling," *IEEE Photon. J.*, vol. 10, no. 2, Apr. 2018, Art. no. 7201714.

[46] G. Maddodi, A. Awad, D. Awad, M. Awad, and B. Lee, "A new image encryption algorithm based on heterogeneous chaotic neural network generator and dna encoding," *Multimedia Tools Appl.*, vol. 77, no. 19, pp. 24701–24725, Oct. 2018.

[47] X. Wu, K. Wang, X. Wang, and H. Kan, "Lossless chaotic color image cryptosystem based on DNA encryption and entropy," *Nonlinear Dyn.*, vol. 90, no. 2, pp. 855–875, Oct. 2017.

[48] X.-Y. Wang, H.-L. Zhang, and X.-M. Bao, "Color image encryption scheme using CML and DNA sequence operations," *Biosystems*, vol. 144, pp. 18–26, Jun. 2016.

[49] X. Zhang, Z. Zhou, and Y. Niu, "An image encryption method based on the Feistel network and dynamic DNA encoding," *IEEE Photon. J.*, vol. 10, no. 4, Aug. 2018, Art. no. 3901014.

[50] D. Huo, D.-F. Zhou, S. Yuan, S. Yi, L. Zhang, and X. Zhou, "Image encryption using exclusive-OR with DNA complementary rules and double random phase encoding," *Phys. Lett. A*, vol. 383, no. 9, pp. 915–922, Feb. 2019.

[51] Q. Zhang, L. Guo, and X. P. Wei, "Image encryption using DNA addition combining with chaotic maps," *Math. Comput. Model.*, vol. 52, nos. 11–12, pp. 2028–2035, Dec. 2010.

[52] Q. Zhang, L. Guo, X. Xue, and X. Wei, "An image encryption algorithm based on DNA sequence addition operation," in *Proc. 4th Int. Conf. Bio-Inspired Comput.*, Oct. 2009, pp. 1–5.

[53] X.-Y. Wang, Y.-Q. Zhang, and Y.-Y. Zhao, "A novel image encryption scheme based on 2-D logistic map and DNA sequence operations," *Nonlinear Dyn.*, vol. 82, no. 3, pp. 1269–1280, Nov. 2015.

[54] A. Kulsoom, D. Xiao, Aqeel-ur-Rehman, and S. A. Abbas, "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules," *Multimedia Tools Appl.*, vol. 75, no. 1, pp. 1–23, Jan. 2016.

[55] A. U. Rehman, X. Liao, A. Kulsoom, and S. A. Abbas, "Selective encryption for gray images based on chaos and DNA complementary rules," *Multimedia Tools Appl.*, vol. 74, no. 13, pp. 4655–4677, Jul. 2015.

[56] X. Wang and M. Wang, "A hyperchaos generated from Lorenz system," *Phys. A, Stat. Mech. Appl.*, vol. 387, no. 14, pp. 3751–3758, Jun. 2008.

[57] X. Wang, Y. Hou, S. Wang, and R. Li, "A new image encryption algorithm based on CML and DNA sequence," *IEEE Access*, vol. 6, pp. 62272–62285, 2018.

[58] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Process.*, vol. 155, pp. 44–62, Feb. 2019.

[59] H. Liu, X. Wang, and A. Kadir, "Color image encryption using Choquet fuzzy integral and hyper chaotic system," *Optik*, vol. 124, no. 18, pp. 3527–3533, Sep. 2013.

[60] H. Liu and A. Kadir, "Asymmetric color image encryption scheme using 2D discrete-time map," *Signal Process.*, vol. 113, pp. 104–112, Aug. 2015.

[61] C. Dong, "Color image encryption using one-time keys and coupled chaotic systems," *Signal Process., Image Commun.*, vol. 29, no. 5, pp. 628–640, May 2014.

[62] A. Alabaichi, "True color image encryption based on DNA sequence, 3D chaotic map, and key-dependent DNA S-box of AES," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 2, pp. 304–321, Jan. 2018.

[63] P. Zhen, G. Zhao, L. Min, and X. Jin, "Chaos-based image encryption scheme combining DNA coding and entropy," *Multimedia Tools Appl.*, vol. 75, no. 11, pp. 6303–6319, Jun. 2016.

[64] L. Yao, C. Yuan, J. Qiang, S. Feng, and S. Nie, "An asymmetric color image encryption method by using deduced gyrator transform," *Opt. Lasers Eng.*, vol. 89, pp. 72–79, Feb. 2017.

[65] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," *Signal Process.*, vol. 141, pp. 109–124, Dec. 2017.

[66] X. Wang, Y. Zhao, H. Zhang, and G. Kang, "A novel color image encryption scheme using alternate chaotic mapping structure," *Opt. Lasers Eng.*, vol. 82, pp. 79–86, Jul. 2016.

[67] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 18, no. 11, pp. 3075–3085, Nov. 2013.

[68] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process.*, vol. 92, no. 4, pp. 1101–1108, Apr. 2012.

ZHENTAO LIU is currently pursuing the B.S. degree with the College of Electronics and Information Engineering, Sichuan University, Chengdu, China. His research interests include image encryption and data security.

CHUNXIAO WU is currently pursuing the B.S. degree with the College of Electronics and Information Engineering, Sichuan University, Chengdu, China. Her research interests include image encryption and data security.

JUN WANG received the Ph.D. degree from the Department of Electronic and Computer Engineering, Hanyang University, Seoul, Korea, in 2011. He was a Postdoctoral Fellow with the University of Wisconsin-Madison, Madison, USA, from 2011 to 2012. He was a short-time Visiting Scholar with the School of Instrumentation and Optoelectronic Engineering, Beihang University, from 2018 to 2019. He has been an Associate Professor with the College of Electronics and Information Engineering, Sichuan University, Chengdu, China, since 2012. He has published more than 40 publications. His current research interests include image encryption, holographic 3D display, and image processing.

YU HEN HU received the B.S.E.E. degree from National Taiwan University, Taipei, Taiwan, in 1976, and the M.S. and Ph.D. degrees in electrical engineering from the University of Southern California, Los Angeles, USA, in 1980 and 1982, respectively. He was with the Electrical Engineering Department, Southern Methodist University, Dallas, USA. He is currently a Professor with the Electrical and Computer Engineering Department, University of Wisconsin-Madison, Madison, USA. He has authored more than 300 journals and conference papers and edited and coauthored several books. His current research interests include multimedia signal processing and communication, design methodology, and implementation of embedded algorithms and systems, and nano-scale IC design methodologies. He served as the Secretary for the IEEE Signal Processing Society and the Board of Governors of the IEEE Neural Networks Council, and the Chair of the IEEE Multimedia Signal Processing Technical Committee and the IEEE Neural Network Signal Processing Technical Committee. He served as an Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING, the IEEE SIGNAL PROCESSING LETTERS, the *Journal of Very Large Scale Integration Systems Signal Processing*, the *IEEE Multimedia Magazine*, and the *European Journal of Applied Signal Processing*.