J Inf Process Syst, Vol.18, No.1, pp.59~74, February 2022
https://doi.org/10.3745/JIPS.03.0171

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

A Hierarchical Bilateral-Diffusion Architecture for Color Image Encryption

Menglong Wu*, Yan Li, and Wenkai Liu

Abstract
During the last decade, the security of digital images has received considerable attention in various multimedia transmission schemes. However, many current cryptosystems tend to adopt a single-layer permutation or diffusion algorithm, resulting in inadequate security. A hierarchical bilateral diffusion architecture for color image encryption is proposed in response to this issue, based on a hyperchaotic system and DNA sequence operation. Primarily, two hyperchaotic systems are adopted and combined with cipher matrixes generation algorithm to overcome exhaustive attacks. Further, the proposed architecture involves designing pixel-permutation, pixel-diffusion, and DNA (deoxyribonucleic acid) based block-diffusion algorithm, considering system security and transmission efficiency. The pixel-permutation aims to reduce the correlation of adjacent pixels and provide excellent initial conditions for subsequent diffusion procedures, while the diffusion architecture confuses the image matrix in a bilateral direction with ultra-low power consumption. The proposed system achieves preferable number of pixel change rate (NPCR) and unified average changing intensity (UACI) of 99.61% and 33.46%, and a lower encryption time of 3.30 seconds, which performs better than some current image encryption algorithms. The simulated results and security analysis demonstrate that the proposed mechanism can resist various potential attacks with comparatively low computational time consumption.

Keywords
Bilateral-Diffusion, Color Image Encryption, DNA Sequence Operation, Hyperchaotic System

1. Introduction

With the rapid development of communication and networks, multimedia information transmission between various devices has put forward higher requirements. Due to the rapid development of transmission mechanisms, the consequent security issues have attracted substantial attention in industry and academia. However, since the digital image has the characters of high correlation between adjacent pixels, some current encryption algorithms, such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest-Shamir-Adleman (RSA) algorithm, are not suitable for image encryption [1-5]. Hence, it is vital to enhance the efficiency of image encryption by pursuing other security technologies.

Currently, chaotic systems are very suitable for cryptosystems and have become a major trend in many image encryption algorithms [6,7]. Its particular attributes, including high aperiodicity and randomicity

Manuscript received October 21, 2020; first revision July 13, 2021; accepted December 26, 2021.

* **Corresponding Author:** Menglong Wu (wumenglong@126.com)
School of Information Science and Technology, North China University of Technology, Beijing, China (wumenglong@126.com, liyan99559@163.com, liuwk_ncut@126.com)

and its great sensitivity to initial values, make it adapt to image encryption, and a large number of research achievements are proposed in this area [8-10]. So far, however, chaotic systems can only be applied to produce pseudo-random number sequences for image encryption areas, indicating that other efficient encryption algorithms or techniques are required to confuse the plain image greatly. Meanwhile, since Adleman [11] first introduced DNA computing into the experiment in 1994, a new image encryption method, called the DNA method, has been widely used. DNA-based image encryption methods are known for their great superiorities, such as large parallelism, high storage, and low energy consumption, making it very appropriate to encrypt images with high redundancy information [12-15]. In addition, it is worth noting that encrypting images with the DNA computing method under a single DNA encoding rule will bring a large number of equivalent computations and leads to insufficient system security. Therefore, the combination of the chaotic system and DNA operation aroused great interest in image encryption, which reveals superior experimental results, and plenty of scholars are continuing to work on this subject [16-21].

Nevertheless, some current image encryption algorithms with DNA operation and chaotic systems are found not powerful enough to resist differential attacks. For example, Liu et.al [14] proposed a novel color image encryption algorithm based on dynamic DNA and 4D chaotic system. However, the algorithm suffered an imperfect unified average changing intensity (UACI) of 33.06%, 30.59% and 27.60% for each R, G, B channel, since the confusion process merely relies on XOR operation and the diffusion process is executed in groups. Li et al. [21] proposed a color image encryption algorithm using a fractional-order 4D hyperchaotic system and DNA sequence operations. However, although the algorithm involves the utilization of DNA encoding, DNA complementary and DNA addition operation, the system security still needs to be improved. To be specific, the information entropy of cipher image is 7.9973 in G channel and 7.9967 in B channel under the proposed algorithm, yet many of the image encryption algorithms realized better information entropy which is larger than 7.9990. Meanwhile, the UACI of the proposed algorithm in the R channel is 33.2483%, which is not close enough to the theoretical value 33.4635%.

Based on the above discussion, this paper proposed a hierarchical bilateral-diffusion architecture for color image encryption based on two hyperchaotic systems and DNA sequence operations. Primarily, several cipher matrixes are generated with high sensitivity to resist exhaustive attacks by compounding and weighting the hyper-chaotic Lorenz system and Chen's hyper-chaotic system. Then, the pixel-permutation algorithm is performed to disorder the plain image and provide preferable conditions for subsequent diffusion procedures. Next, a forward pixel-diffusion algorithm is designed to alter each pixel value of the image matrix. After, DNA based bilateral block-diffusion algorithm is proceeded for block-level diffusion with ultra-low power consumption, under the utilization of DNA encoding, DNA decoding, DNA complementary operation, and DNA algebraic operation. Finally, the backward pixel-diffusion is executed to enhance the system security further and obtain the cipher image. The experimental results illustrated in Section 4 and Section 5 verified the practicability and security of the proposed image encryption mechanism with a strong ability to against statistical attacks, differential attacks, and brute-force attacks, as well as low computational time consumption.

The rest of the paper is organized as follows. The preliminary work including chaotic systems and DNA sequence operation are illustrated in Section 2. The proposed hierarchical bilateral-diffusion architecture for color image encryption is described in Section 3. The simulation results and computational speed analysis are exhibited in Section 4. The security analysis is given in Section 5. Finally, the conclusion is given in Section 6.

2. Preliminary Work

2.1 Chaotic System

Chaotic systems are widely applied in various image encryption algorithms due to its superior peculiarities, aperiodicity, randomicity, and its great sensitivity to initial values. In the proposed system, two 4-D hyperchaotic systems, hyper-chaotic Lorenz system and Chen's hyper-chaotic system, are involved for an even better randomicity. The hyper-chaotic Lorenz system is described in Eq. (1), where a, b, c, r are four control parameters. When $a = 10, b = 8/3, c = 28$ and $-1.52 \leq r \leq -0.06$, the system is under the state of hyperchaotic. Meanwhile, the Chen's hyper-chaotic system is defined in Eq. (2). The five control parameters, a, b, c, d, k are set as $a = 36, b = 3, c = 28, d = -16$ and $-0.7 \leq k \leq 0.7$ to guarantee the system is under the state of hyperchaotic.

$$\begin{cases} \dot{x} = a(y - x) + w \\ \dot{y} = \ cx - y - xz \\ \dot{z} = xy - bz \\ \dot{w} = -yz + rw \end{cases} \tag{1}$$

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = -xz + dx + cy - q \\ \dot{z} = xy - bz \\ \dot{q} = x + k \end{cases} \tag{2}$$

2.2 DNA Sequence Operation

A DNA sequence consists of four basic nucleic acids, namely, A (adenine), C (cytosine), G (guanine), and T (thymine). The DNA sequences are supposed to satisfy the Watson-Crick complement rules, where A and T are complementary, C and G are complementary. Based on this, the binary sequences and DNA sequences can be converted mutually under the DNA encoding/decoding rule defined in Table 1. As shown in Table 1, there are 8 encoding/decoding rules in total, and each DNA code is represented with 2 bits binary sequence: 00, 01, 10 or 11.

Table 1. The DNA encoding/decoding rules

	0	1	2	3	4	5	6	7
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

DNA complementary and algebraic operations are the core processes of DNA-based encryption algorithms. Since DNA complementary operation abides by the single mapping principle, the DNA complementary rules must satisfy the formulas defined in Eq. (3), where $B(x_i)$ is a base pair of x_i and they are complementary.

$$\begin{cases} x_i \neq B(x_i) \neq B\big(B(x_i)\big) \neq B\Big(B\big(B(x_i)\big)\Big) \\ x_i = B\Big(B\Big(B\big(B(x_i)\big)\Big)\Big) \end{cases} \tag{3}$$

Based on Eq. (3), there are 6 available DNA complementary rules, as shown below:

$$\begin{aligned} &(AT)(TC)(CG)(GA), (AT)(TG)(GC)(CA), (AC)(CT)(TG)(GA), \\ &(AC)(CG)(GT)(TA), (AG)(GT)(TC)(CA), (AG)(GC)(CT)(TA) \end{aligned} \tag{4}$$

DNA algebraic operation is based on traditional binary algebraic operations, such as, addition, subtraction, XOR and XNOR. According to DNA encoding rule 1, the definitions of DNA addition, subtraction, XOR and XNOR operations based on two DNA codes are given in Table 2.

Table 2. The DNA algebraic rules of addition, subtraction, XOR and XNOR operations

	Addition (+)				**Subtraction (−)**				**XOR (⊕)**				**XNOR (⊙)**			
	A	**G**	**C**	**T**	**A**	**G**	**C**	**T**	**A**	**G**	**C**	**T**	**A**	**G**	**C**	**T**
A	A	G	C	T	A	T	C	G	A	G	C	T	T	C	G	A
G	G	C	T	A	G	A	T	C	G	A	T	C	C	T	A	G
C	C	T	A	G	C	G	A	T	C	T	A	G	G	A	T	C
T	T	A	G	C	T	C	G	A	T	C	G	A	A	G	C	T

3. Proposed Methodology

In this paper, a hierarchical bilateral-diffusion architecture is proposed for color image encryption, utilizing the hyperchaotic system and DNA operation. The concrete design of the proposed mechanism consists of three main parts: (1) cipher matrixes generation, (2) pixel-permutation and pixel-diffusion algorithm, and (3) bilateral block-diffusion algorithm based on DNA sequence operation, which will be further discussed as follows.

3.1 Cipher Matrixes Generation

In all cryptosystems, to overcome exhaustive attacks, the cipher keys are required to be long and sensitive enough. In this paper, since ten cipher matrixes are required for image encryption and decryption, two 4D hyperchaotic systems, the hyper-chaotic Lorenz system and Chen's hyper-chaotic system, are utilized to satisfy the requirements of high randomicity and sensitivity. The design concept of the cipher matrixes generation is shown in Fig. 1, which can work by iterating the chaotic sequences with two hyperchaotic systems and integrating the intermediate variables into cipher matrixes through a specific generation algorithm. Suppose the plain image is in size of $M \times N$ and the number of DNA blocks is t, the whole ten cipher matrixes can be generated by the following steps.

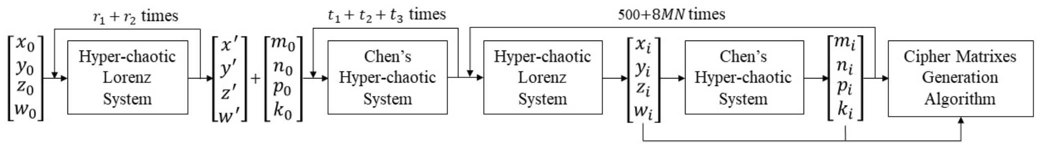


Fig. 1. The design concept of cipher matrixes generation.

Step 1: Take four initial values x_0, y_0, z_0, w_0 as inputs of hyper-chaotic Lorenz system with control parameters r_1, r_2 and iterate for $r_1 + r_2$ times to gain four chaotic values, denoted as x', y', z', w'.

Step 2: Plus four initial values m_0, n_0, p_0, k_0 with chaotic values x', y', z', w' and take them as inputs of Chen's hyper-chaotic system with control parameters t_1, t_2, t_3. Then, iterate them for $t_1 + t_2 + t_3$ times.

Step 3: Continually put the obtained chaotic values into hyper-chaotic Lorenz system and Chen's hyper-chaotic system in sequence, where the intermediate sequences of hyper-chaotic Lorenz system is denoted as $x_{\mathrm{i}}, y_{\mathrm{i}}, z_{\mathrm{i}}, w_{\mathrm{i}}$ and the intermediate sequences of Chen's hyper-chaotic system is denoted as $m_{\mathrm{i}}, n_{\mathrm{i}}, p_{\mathrm{i}}, k_{\mathrm{i}}$.

Step 4: Iterate the chaotic sequences for $500 + 8MN$ times and generate four cipher matrixes in size of $M \times 4N$ under the definitions in Eqs. (5)–(8).

$$A_{i,j} = \left(\frac{1-r_1}{t_1+t_2} \times x_{(2i+1)\times N-(i+1)\times j} + \frac{r_1 r_2}{t_2+t_3} \times m_{(2i+1)\times N-(i+1)\times j}\right) \times 10^{14}, mod\ 256 \tag{5}$$

$$B_{i,j} = \left(\frac{r_1 r_2}{t_1+t_3} \times y_{(2i+1)\times N-(i+1)\times j} + \frac{1-r_2}{t_1+t_2} \times n_{(2i+1)\times N-(i+1)\times j}\right) \times 10^{14}, mod\ 256 \tag{6}$$

$$C_{i,j} = \left(\frac{1-r_2}{t_1+t_2} \times z_{(2i+1)\times N-(i+1)\times j} + \frac{1-r_1}{t_2+t_3} \times p_{(2i+1)\times N-(i+1)\times j}\right) \times 10^{14}, mod\ 256 \tag{7}$$

$$D_{i,j} = \left(\frac{1-r_2}{t_2+t_3} \times w_{(2i+1)\times N-(i+1)\times j} + \frac{r_1 r_2}{t_1+t_3} \times k_{(2i+1)\times N-(i+1)\times j}\right) \times 10^{14}, mod\ 8 \tag{8}$$

Step 5: Divide $A_{M\times 4N}$ into four pixel-permutation cipher matrixes, $X_{M\times N}, Y_{M\times N}, Z_{M\times N}, H_{M\times N}$; and then Reshape $B_{M\times 4N}$ and $C_{M\times 4N}$ into two pixel-diffusion cipher matrixes with the size of $2M \times 2N$, denoted as $U_{2M\times 2N}$ and $V_{2M\times 2N}$; Divide $D_{M\times 4N}$ into DNA encoding cipher matrix $E_{1\times\mathrm{t}}$, DNA decoding cipher matrix $F_{1\times\mathrm{t}}$, DNA complementary cipher matrix $S_{1\times\mathrm{t}}$ and DNA algebraic cipher matrix $T_{1\times\mathrm{t}}$.

Step 6: Execute modulus operation to $S_{1\times\mathrm{t}}$ and $T_{1\times\mathrm{t}}$, where $S_{1\times\mathrm{t}}$ is set in the range of $[0,5]$ and $T_{1\times\mathrm{t}}$ is set in the range of $[0,3]$.

3.2 Pixel-Permutation and Pixel-Diffusion Algorithm

Permutation and diffusion are two vital operations in the image encryption algorithm. In the designed system, a pixel-permutation algorithm is used to confuse the order of pixels in the plain image, and the pixel-diffusion algorithm is used to alter the subsequent pixels values of the image matrix, which will be further combined with DNA based block-diffusion algorithm for an impressive performance on statistical attack and differential attack.

The designed pixel-permutation algorithm acts as the primal confusing method to the plain image, which exchanges pixels in coordinate (i,j) and (m,n) through cipher matrixes $X_{M\times N}, Y_{M\times N}, Z_{M\times N}, H_{M\times N}$. The exchanging rules of the two pixels are defined in Eqs. (9) and (10). There, all the pixel values will be entirely scrambled by repetitively executing the algorithm from coordinate $(1,1)$ to (M,N).

$$m = -\ln\frac{1}{\sqrt{X_{i,j}+2}} \times Y_{i,j} + e^{\sqrt{Z_{i,j}+100}} + H_{i,j}\ , mod\ M \tag{9}$$

$$n = -\ln\frac{1}{\sqrt{Z_{i,j}+2}} \times H_{i,j} + e^{\sqrt{X_{i,j}+100}} + Y_{i,j}\ , mod\ N \tag{10}$$

On the other hand, pixel-diffusion algorithms are considered the vital role of image encryption against differential attack, since even single-pixel can greatly influence others. Therefore, two pixel-diffusion algorithms are introduced to the system for better performance, pixel-diffusion I and pixel-diffusion II, which scan the image matrix in the opposite direction. Specifically, the pixel-diffusion I algorithm is a forward-diffusion algorithm that starts from the first element and alters the remaining pixels value in the sequence. Suppose the input image matrix is $P_{M\times N}$, the obtained image matrix after pixel-diffusion I algorithm can be calculated by Eq. (11), denoted as $I_{M\times N}$, where $U_{2M\times 2N}$ is the cipher matrix and a, b are two cipher keys. The diffusion operation is accomplished by executing the algorithm from coordinate $(1,1)$ to (M, N).

$$\begin{cases} I_{1,1} = P_{1,1} \oplus U_{a,b} \oplus U_{b,a} \\ I_{1,j} = P_{1,j} \oplus U_{1,j+a} \oplus I_{1,j-1} \\ I_{i,1} = P_{i,1} \oplus U_{i+b,j} \oplus I_{i-1,1} \\ I_{i,j} = P_{i,j} \oplus U_{i+a,j+b} \oplus I_{i-1,j} \oplus I_{i,j-1} \end{cases} \tag{11}$$

On the contrary, the pixel-diffusion II algorithm is a backward-diffusion algorithm that starts from the last element and alters the remaining pixels value in the negative direction. Similarly, suppose the input image matrix is $P_{M\times N}$, and the obtained image matrix $I_{M\times N}$ can be calculated by Eq. (12), where $V_{2M\times 2N}$ is the cipher matrix and c, d are two cipher keys. The diffusion operation is accomplished by executing the algorithm from coordinate (M, N) to $(1, 1)$.

$$\begin{cases} I_{M,N} = P_{M,N} \oplus V_{c,d} \oplus V_{d,c} \\ I_{M,j} = P_{M,j} \oplus V_{M,j+c} \oplus I_{M,j+1} \\ I_{i,N} = P_{i,N} \oplus V_{i+d,N} \oplus I_{i+1,N} \\ I_{i,j} = P_{i,j} \oplus V_{i+c,j+d} \oplus I_{i+1,j} \oplus I_{i,j+1} \end{cases} \tag{12}$$

3.3 Bilateral Block-Diffusion Algorithm based on DNA Operation

As a matter of fact, confusing the original image with only XOR-based diffusion algorithm is seen as a deficient method when encountering strongly differential attacks. Therefore, this paper presents a bilateral block-diffusion algorithm for better sensitivity, utilizing DNA encoding, DNA decoding, DNA complementary operation and DNA algebraic operation. Under the peculiar diffusion structure of forward pixel-diffusion, DNA based bilateral block-diffusion and backward pixel-diffusion, the image encryption mechanism shows an impressive ability to overcome statistical attacks and differential attacks.

The proposed block-diffusion algorithm is constituted by forward DNA diffusion algorithm and backward DNA diffusion algorithm. It diffuses the image by two bilateral directions, where the forward diffusion starts from block 1 to block t and backward diffusion starts from block t to block 1. DNA complementary operation and DNA algebraic operation are the core operations of DNA diffusion, which acts on each current DNA block with the previous DNA block. For instance, if the current block is block i, then the previous block of forward DNA diffusion is block $i - 1$, and the previous block of backward DNA diffusion is block $i + 1$.

The adopted DNA complementary operation is a substitution operation with iteration, and the results are determined by the DNA complementary rules in Eq. (4). Suppose the current DNA block is denoted as K, the previous DNA block is denoted as J, and the block after DNA complementary operation is denoted as R. Then, the calculation principle of an intact DNA complementary process can be illustrated as follow:

$$R_{i,j} = \begin{cases} K_{i,j}, if\ J_{i,j} = A \\ B(K_{i,j}), if\ J_{i,j} = T \\ B\left(B(K_{i,j})\right), if\ J_{i,j} = C \\ B\left(B\left(B(K_{i,j})\right)\right), if\ J_{i,j} = G \end{cases} \tag{13}$$

where $K_{i,j}, J_{i,j}, R_{i,j}$ are the elements in block K, J, R respectively, and $B(K_{i,j})$ represents a one-time complementary operation to $K_{i,j}$. In the designed algorithm, cipher matrix $S_{1\times t}$ is required to select the complementary rule, and the elements in block J are used to decide the iterations of complementary substitution.

On the other hand, the adopted DNA algebraic operation is a subsequent process to DNA complementary operation, which alters the elements in block R with block J. The DNA algebraic rule is decided by the elements in the cipher matrix $T_{1\times t}$, where $T_{i,j} = 0$ represents addition operation, $T_{i,j} = 1$ represents subtraction operation, $T_{i,j} = 2$ represents XOR operation and $T_{i,j} = 3$ represents XNOR operation.

3.4 The Intact Steps of Proposed Image Encryption Mechanism

The proposed encryption mechanism for a color image is described in Fig. 2, involving one pixel-permutation algorithm, two pixel-diffusion algorithms and the DNA based bilateral block-diffusion algorithm. The complete image encryption steps are illustrated as follows.

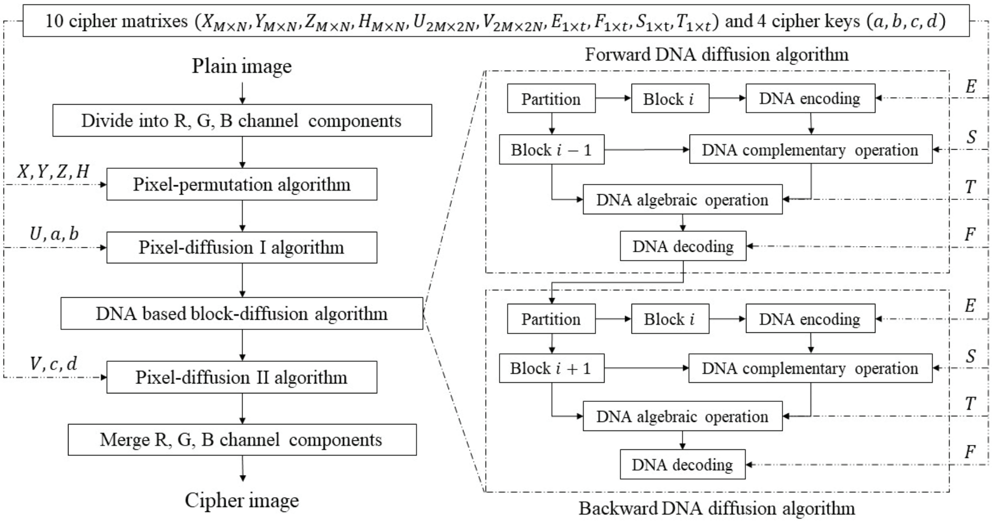

10 cipher matrixes ($X_{M\times N}, Y_{M\times N}, Z_{M\times N}, H_{M\times N}, U_{2M\times 2N}, V_{2M\times 2N}, E_{1\times t}, F_{1\times t}, S_{1\times t}, T_{1\times t}$) and 4 cipher keys ($a, b, c, d$)
Plain image
Divide into R, G, B channel components
X, Y, Z, H
Pixel-permutation algorithm
U, a, b
Pixel-diffusion I algorithm
DNA based block-diffusion algorithm
V, c, d
Pixel-diffusion II algorithm
Merge R, G, B channel components
Cipher image
Forward DNA diffusion algorithm
Partition
Block i
DNA encoding
E
Block $i-1$
DNA complementary operation
S
DNA algebraic operation
T
DNA decoding
F
Partition
Block i
DNA encoding
E
Block $i+1$
DNA complementary operation
S
DNA algebraic operation
T
DNA decoding
F
Backward DNA diffusion algorithm

Fig. 2. The constitution of the proposed color image encryption mechanism.

Step 1: Input cipher keys $x_0, y_0, z_0, w_0, m_0, n_0, p_0, k_0, r_1, r_2, t_1, t_2, t_3$ to gain ten cipher matrixes.
Step 2: Separate the plain image into R, G, B channel matrixes in the size of $M \times N$.

Step 3: Execute pixel-permutation algorithm to the image matrix from coordinate $(1,1)$ to (M,N), through cipher matrixes $X_{M\times N}, Y_{M\times N}, Z_{M\times N}, H_{M\times N}$; Then, run pixel-diffusion I algorithm to the obtained matrix from coordinate $(1,1)$ to (M,N), through cipher matrix $U_{2M\times 2N}$ and cipher keys a,b.

Step 4: Proceed the DNA based forward block-diffusion algorithm as follows: partition the image matrix into t blocks and convert into DNA blocks under the encoding rules defined in matrix $\mathrm{E}_{1\times\mathrm{t}}$; keep the first DNA block unchanged; For each of the remaining $t-1$ blocks, make DNA complementary operation and DNA algebraic operation with the previous block sequentially, based on cipher matrixes $S_{1\times\mathrm{t}}$ and $T_{1\times\mathrm{t}}$; then, convert all the DNA blocks into a decimal matrix with the decoding rules defined in matrix $\mathrm{F}_{1\times\mathrm{t}}$.

Step 5: Similarly, proceed the DNA based backward block-diffusion algorithm as follows: partition and convert the matrix into t DNA blocks with matrix $\mathrm{E}_{1\times\mathrm{t}}$, and remain block t unchanged; from block $t-1$ to block 1, execute DNA complementary operation and DNA algebraic operation based on cipher matrixes $S_{1\times\mathrm{t}}$ and $T_{1\times\mathrm{t}}$; convert the DNA blocks into a decimal matrix with matrix $\mathrm{F}_{1\times\mathrm{t}}$.

Step 6: From coordinate (M,N) to $(1,1)$, convert the matrix with pixel-diffusion II algorithm through cipher matrix $V_{2M\times 2N}$ and cipher keys c,d in sequence.

Step 7: For each component matrix of R, G, B channel, loop execute the transformation from step 3 to step 6. Then, merge the three-channel matrixes into one final cipher image.

4. Experimental Results and Computational Speed Analysis

4.1 Experimental Results of Image Encryption and Decryption

The experimental of the proposed image encryption mechanism is tested in this part. Four color images are utilized to test the encryption and decryption performance, named "Lena" in the size of $512\times 512\times 3$, "street" in the size of $1280\times 720\times 3$, "waterfall" in the size of $800\times 600\times 3$, and "mountain" in the size of $1024\times 680\times 3$, as shown in Fig. 3(a)–3(d), respectively. Meanwhile the experiments are implemented using MATLAB R2018b on a computer with Intel Core i5 processor and 8 GB RAM in Windows 10 operating system.

The initial value and other control parameters are described in Table 3, where x_0, y_0, z_0, w_0 are four initial value of hyper-chaotic Lorenz system, m_0, n_0, p_0, k_0 are four initial value of Chen's hyper-chaotic system, r_1, r_2, t_1, t_2, t_3 are the control parameters of the two chaotic systems and a,b,c,d are the parameters of two pixel-diffusion algorithms. The encryption for the four plain images is shown in Fig. 3. It can be seen from the experimental results that the cipher images are unrecognizable and shown no correlation to the plain images. Besides, the cipher images are all decrypted successfully. Hence, the feasibility of the proposed image encryption algorithm has been verified.

Table 3. Specific parameters of the simulation

Item	Value
Chaotic systems	$x_0 = 26.7837, y_0 = -8.9013, z_0 = 59.4985, w_0 = -247.3752,$ $m_0 = 37.5082, n_0 = -16.3594, p_0 = 69.4987, k_0 = 137.4891,$ $r_1 = 58, r_2 = 231, t_1 = 48, t_2 = 9, t_3 = 168$
Pixel-diffusion algorithms	$a = 78, b = 215, c = 97, d = 38$

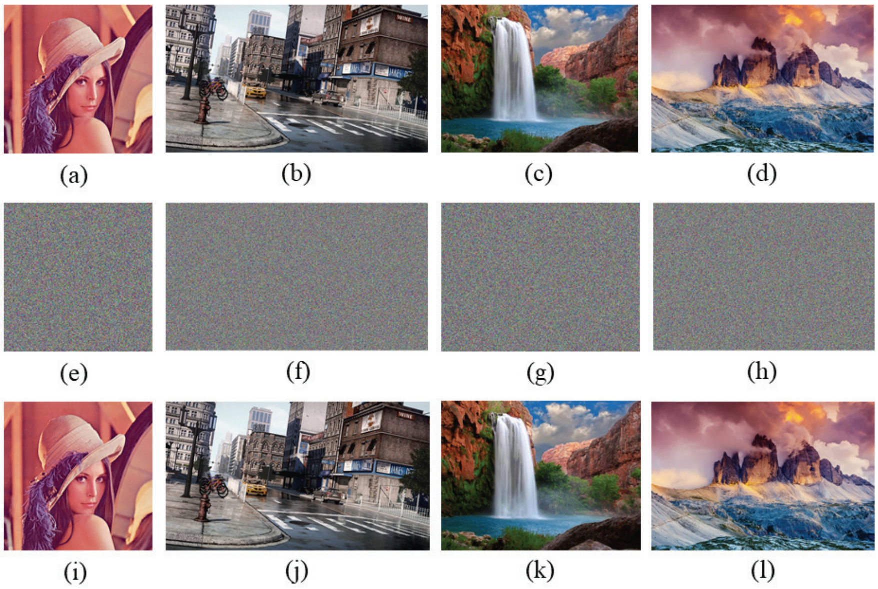


Fig. 3. Experimental results of image encryption for different color images. (a–d) Four plain images. (e–h) The corresponding cipher images. (i–l) The corresponding decrypted images.

4.2 Computational Complexity Analysis

The computational complexity can influence the computational speed greatly for both encryption and decryption processes. Therefore, to verify whether the proposed encryption mechanism is suitable enough for color image encryption, this section gives the time complexity of the encryption process for theoretical support and analysis, as follows. Firstly, the input color image with the size of $M \times N$ is separated into three pixel-matrixes, so the time complexity is $O(3 \times M \times N)$. The pixel-permutation process exchanges the pixel value in each pixel-matrix of three channels, so the time complexity is also $O(3 \times M \times N)$. The pixel-diffusion process alters the pixel value in the three pixel-matrixes, so the time complexity for pixel-diffusion I and pixel-diffusion II algorithm are both $O(3 \times M \times N)$. For DNA based block-diffusion process, the time complexity for DNA encode/decode is $O(12 \times M \times N)$, since 4 DNA codes are needed to represent one pixel value. Similarly, the time complexity for DNA complementary and algebraic operation is also $O(12 \times M \times N)$, since the operations are all based on the DNA codes after DNA encodes. Thus, the overall time complexity of the proposed image encryption mechanism is $O(12 \times M \times N)$.

4.3 Computational Speed Performance

Computational time is a significant indicator in the image encryption area. For a well-designed image encryption algorithm, the computational time is required to be as low as possible when guaranteeing system security. In this part, the image encryption algorithm is executed 100 times to gain the average encryption time of 3.30 seconds, with an image size of $512 \times 512 \times 3$. Since the bilateral-diffusion architecture only involves low computational operations such as addition, subtraction, XOR, and XNOR operation, the proposed algorithm has shown an excellent speed performance of image encryption. Besides, the design of DNA-based block diffusion also saved plenty of computing time and achieved better encryption efficiency. Table 4 gives the experimental results and compares them with other algorithms [2,4,13,22] in computational times, which indicates that the proposed algorithm has achieved better computational speed performance.

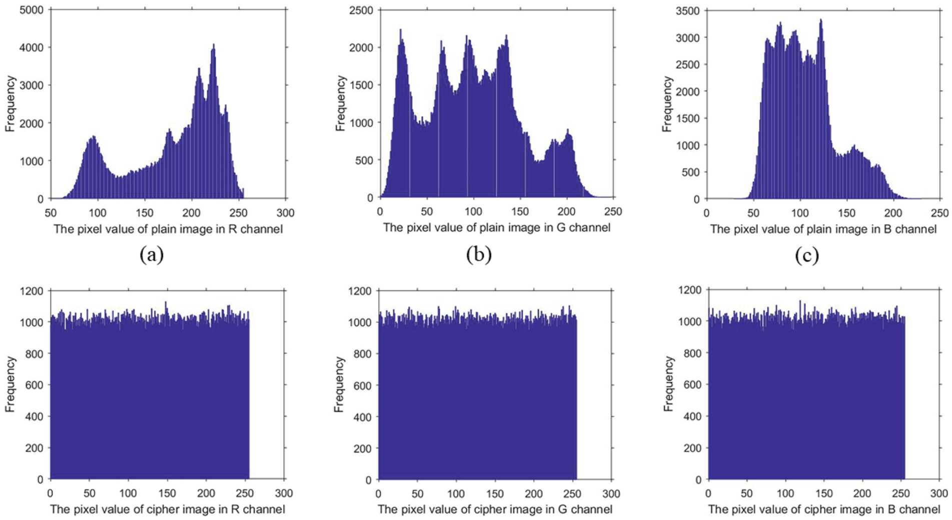
Table 4. Execution time under the proposed method and the comparison with other algorithms

Algorithm	Execution time (s)
Proposed method	3.30
Kang and Guo [2]	9.0016
Shakiba [4]	13.9
Rehman et al. [13]	5.47
Wu et al. [22]	3.76

5. Security Analysis

5.1 Histogram Analysis

The image histogram can directly reveal the distribution of the pixel values. The histograms of plain image and cipher image in R, G, B channels are given in Fig. 4. It can be noticed that the histograms of plain images are tended to some specific shapes, and the pixel values are concentrated to several fixed intervals, while the histograms of cipher images show their excellent uniformity. Hence, it is exceedingly difficult to extract the related information and recover the plain image. Therefore, the proposed algorithm can overcome the statistical attacks from histogram analysis.



(a) (b) (c)

(d) (e) (f)

Fig. 4. The image histograms of (a–c) plain image and (d–f) cipher image in R, G, B channel, respectively.

5.2 Correlation Analysis

Correlation analysis is another statistical attack, which intends to search the relation of adjacent pixels in the cipher images and recover the plain images. Since the correlations of adjacent pixels in plain images are usually very large in horizontal, vertical, and diagonal directions, reducing the correlation of adjacent pixels in the image encryption algorithm is vital. In this part, 10000 pairs of adjacent pixels are selected randomly to evaluate the correlations between plain and cipher images. Fig. 5 gives the distribution diagrams of adjacent pixels in plain image and cipher image. It shows that the correlations of the adjacent pixels in the plain image are very strong, which the distribution is very close to a straight line. Meanwhile, the distribution diagrams of the cipher image are tended to be very disordered, which indicates that the correlation of cipher image is very little.

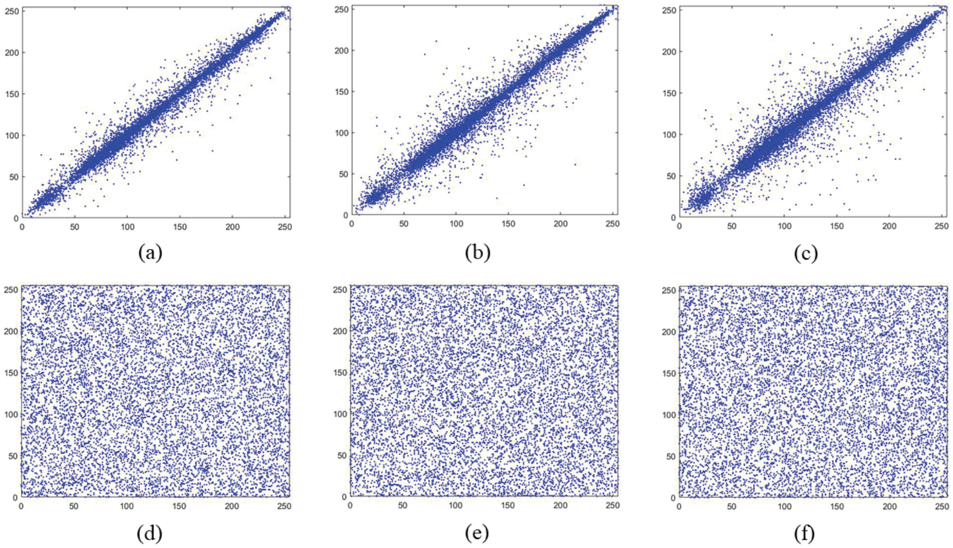
Further, the correlation coefficient acts as a vital measurement criterion to quantify the correlation of images. Eqs. (14)–(17) given the formulas of the correlation coefficient, where x, y are adjacent pixel values and N is the sample size.

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{14}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{15}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i \tag{16}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{17}$$



(a) (b) (c)

(d) (e) (f)

Fig. 5. The distribution of adjacent pixels in plain image and cipher image. (a–c) Horizontal, vertical, and diagonal distribution of plain image. (d–f) Horizontal, vertical, and diagonal distribution of cipher image.

The experimental results of the correlation coefficient in plain image and cipher image are shown in Table 5. The correlation coefficients are supposed to be very close to theoretical value zero, and our test results are satisfied with the demands. Table 5 also lists the comparison with other image encryption algorithms [5,13,14,20]. All the experimental results are very close to zero, which shows that the proposed algorithm has a great ability to against statistical attacks.

Table 5. Correlation coefficient under the proposed method and the comparison with other algorithms

Correlation coefficient	Horizontal	Vertical	Diagonal
Lena	0.9900	0.9807	0.9719
Proposed method	0.0036	0.0068	-0.0029
Wu et al. [5]	-0.0080	0.0098	-0.0058
Rehman et al. [13]	-0.0238	-0.0013	0.0006
Liu et al. [14]	0.0011	-0.0013	-0.0019
Chai et al. [20]	-0.0027	0.0033	-0.0035

5.3 Information Entropy Analysis

The information entropy can measure the uncertainty of an information source, which can be calculated by Eq. (18).

$$H(x) = -\sum_{i=0}^{L-1} p_i \, log_2 \, p_i \tag{18}$$

Hence, the uncertainty of the cipher image can be evaluated by calculating the image information entropy. The comparison with other algorithms is given in Table 6 [1,2,14,21]. It can be noticed that all the experimental results are very close to theoretical value 8 in each channel component, which indicates that the cipher image is of great randomness to resist entropy attack.

Table 6. Information entropy under the proposed method and comparison with other algorithms

Information entropy	R channel	G channel	B channel
Lena	7.2600	7.5949	6.9660
Proposed method	7.9993	7.9992	7.9993
Arpaci et al. [1]	7.9949	7.9945	7.9941
Kang and Guo [2]	7.9980	7.9979	7.9978
Liu et al. [14]	7.9992	7.9993	7.9994
Li et al. [21]	7.9991	7.9973	7.9967

5.4 Differential Attack Analysis

The differential attack is a strong attack in which the attackers may change the pixel values in plain images and seek the difference between the cipher images to crack the cipher keys. The number of pixel change rate (NPCR) and UACI are two test indexes to evaluate whether the encryption algorithm can resist differential attacks. They are defined in Eqs. (19)–(21), where $P(i,j)$ and $C(i,j)$ are the pixel values of two cipher images in the size of $M \times N$.

$$NPCR = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} D(i,j)}{M \times N} \times 100\% \tag{19}$$

$$D(i,j) = \begin{cases} 1 & if \;\; P(i,j) \neq C(i,j) \\ 0 & else \end{cases} \tag{20}$$

$$UACI = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{|P(i,j) - C(i,j)|}{255}}{M \times N} \times 100\% \tag{21}$$

In this part, two plain images with one-pixel value difference are selected for the differential attack test, and the experimental results are given in Table 7. The theoretical value of NPCR and UACI are 99.6094% and 33.4635%, respectively. The comparisons with other algorithms are also given in Table 7 [2,14,21]. It can be noticed that our algorithm has the best performance in both NPCR and UACI tests compared to other image encryption algorithms. Therefore, our algorithm has a strong ability to resist the differential attack.

Table 7. Experimental results (%) and the comparison with other algorithms of differential attack

Algorithm	R channel		G channel		B channel	
	NPCR	UACI	NPCR	UACI	NPCR	UACI
Proposed method	99.61	33.49	99.62	33.43	99.60	33.47
Kang and Guo [2]	99.65	33.46	99.65	33.47	99.65	33.44
Liu et al. [14]	99.60	33.06	99.59	30.59	99.64	27.60
Li et al. [21]	99.60	33.25	99.62	33.50	99.61	33.39

5.5 Cipher Key Analysis

5.5.1 Key space analysis

As a well-designed image encryption algorithm, the key space should be larger than 2^{100} to resist brute-force attacks. The cipher key of the proposed system is constituted by four initial values of hyper-chaotic Lorenz system, x_0, y_0, z_0, w_0, four initial values of Chen's hyper-chaotic system, m_0, n_0, p_0, k_0, five control parameters in the chaotic systems, r_1, r_2, t_1, t_2, t_3 and four parameters of pixel-diffusion algorithms, a, b, c, d. The initial values x_0, y_0, m_0, n_0 are in the range of $(-40,40)$, z_0, p_0 are in the range of $(1,81)$, w_0, k_0 are in the range of $(-250,250)$. All the initial values are floating numbers with the accuracy of 10^{-14}. The control parameters r_1, r_2, t_1, t_2, t_3 and a, b, c, d are integers in the range of $[0,255]$. Hence, the key space of the proposed algorithm can be calculated by Eq. (22).

$$(80)^6 \times (500)^2 \times (10^{14})^8 \times (256)^9 \cong 3.0948501 \times 10^{150} \cong 2^{500} \tag{22}$$

The comparisons with other existing algorithms [1,5,21,23,24] are as shown in Table 8. It is noticed that only the key space in [21] is larger than ours and the key space in our scheme is much larger than the theoretical value 2^{100}. Hence, it indicates that our algorithm has a strong ability to against the brute-force attacks.

Table 8. The key space of the proposed method and the comparison with other algorithms

Algorithm	Key space	Theoretical value
Proposed method	$2^{500} \approx 10^{150}$	$> 2^{100}$
Arpaci et al. [1]	2^{232}	$> 2^{100}$
Wu et al. [5]	2^{349}	$> 2^{100}$
Li al. [21]	2^{576}	$> 2^{100}$
Hraoui et al. [23]	2^{159}	$> 2^{100}$
Wu et al. [24]	10^{117}	$> 2^{100}$

5.5.2 Key sensitivity analysis

As a well-designed cryptosystem, the cipher key is supposed to be very sensitive for a slight altering. In this part, the key sensitivity is tested by changing the parameters slightly when decryption to seek the difference between the correctly decrypted image and the parameters changed decrypted images. The experimental results are as shown in Fig. 6, where Fig. 6(a) is a decrypted image with correct cipher key, while Fig. 6(b)–6(e) are decrypted images with slightly changed cipher keys. It can be noticed from Fig. 6 that all the changed cipher keys are failed in image recovery and show no correlation with the plain image. Therefore, the proposed system has a high key sensitivity against blind decryption.

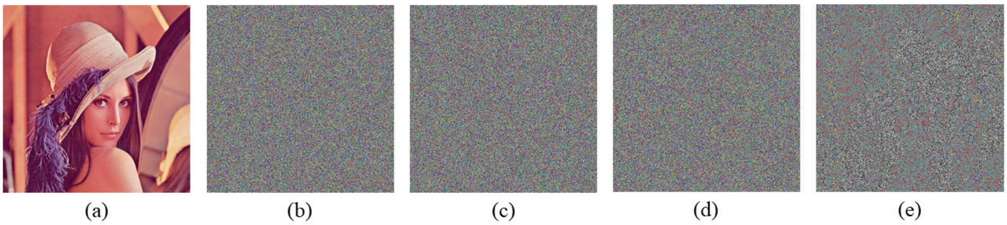


Fig. 6. Experimental results of the key sensitivity test: (a) decrypted image with the correct key, (b) decrypted image with $x_0 = 26.7836$, (c) decrypted image with $m_0 = 37.5081$, (d) decrypted image with $r_1 = 59$, and (e) decrypted image with $a = 77$.

6. Conclusion

This paper proposes a hierarchical bilateral diffusion architecture for color image encryption based on the hyperchaotic system and DNA sequence operation. To against exhaustive attacks, hyper-chaotic Lorenz system and Chen's hyper-chaotic system are compounded and weighted to generate cipher matrixes, which results in highly key sensitive with a key space of 2^{500}. On the other hand, to guarantee system security without sacrificing too much computational time, this paper innovated the encryption mechanism with hierarchical bilateral diffusion architecture to resist various potential attacks. Under the specific diffusion architecture of forward pixel-diffusion, DNA based block-diffusion, and backward pixel-diffusion, the plain image shows excellent ability against statistical attacks and differential attacks. Specifically, our scheme reduces the correlation coefficient of plain image from 0.9809 to 0.0044 and increases the information entropy of plain image from 7.2736 to 7.9993 to overcome statistical attacks. Also, the experimental results of differential attacks indicate that the NPCR and UACI can reach 99.61% and 33.46% on average, which is very close to the theoretical value 99.6094% and 33.4635%. Meanwhile, the computational time consumption under the proposed image encryption scheme is relatively lower than some current image encryption algorithms, costing only 3.30 seconds to encrypt one image. All the experimental results demonstrate that the proposed mechanism is highly efficient in encrypting images with prominent characteristics, such as large key space, stronger key sensitivity, low time consumption, and superior ability to resist varieties of typical attacks. Thus, the proposed diffusion architecture provides an effective method for color image encryption, with expansive application prospects including wireless communication, network data transmission, and big data storage. In the future, this work may achieve even better performance and broader application scenarios under the combination of various image processing techniques, such as image steganography and image compression.

Acknowledgement

This paper is funded by Beijing Natural Science Foundation - Haidian Original Innovation Joint Fund Project (No. L182039).

References

[1] B. Arpaci, E. Kurt, and K. Celik, “A new algorithm for the colored image encryption via the modified Chua’s circuit,” *Engineering Science and Technology: An International Journal*, vol. 23, no. 3, pp. 595-604, 2020.

[2] X. Kang and Z. Guo, “A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system,” *Signal Processing: Image Communication*, vol. 80, article no. 115670, 2020. https://doi.org/10.1016/j.image.2019.115670

[3] A. Ur Rehman, D. Xiao, A. Kulsoom, M. A. Hashmi, and S. A. Abbas, “Block mode image encryption technique using two-fold operations based on chaos, MD5 and DNA rules,” *Multimedia Tools and Applications*, vol. 78, no. 7, pp. 9355-9382, 2019.

[4] A. Shakiba, “A randomized CPA-secure asymmetric-key chaotic color image encryption scheme based on the Chebyshev mappings and one-time pad,” *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 5, pp. 562-571, 2021.

[5] X. Wu, J. Kurths, and H. Kan, “A robust and lossless DNA encryption scheme for color images,” *Multimedia Tools and Applications*, vol. 77, no. 10, pp. 12349-12376, 2018.

[6] S. M. Seyedzadeh, B. Norouzi, M. R. Mosavi, and S. Mirzakuchaki, “A novel color image encryption algorithm based on spatial permutation and quantum chaotic map,” *Nonlinear Dynamics*, vol. 81, no. 1, pp. 511-529, 2015.

[7] X. Hu, L. Wei, W. Chen, Q. Chen, and Y. Guo, “Color image encryption algorithm based on dynamic chaos and matrix convolution,” *IEEE Access*, vol. 8, pp. 12452-12466, 2020.

[8] S. S. Askar, A. A. Karawia, and A. Alshamrani, “Image encryption algorithm based on chaotic economic model,” *Mathematical Problems in Engineering*, vol. 2015, article no. 341729, 2015. https://doi.org/10.1155/2015/341729

[9] X. Zhang and X. Wang, “Digital image encryption algorithm based on elliptic curve public cryptosystem,” *IEEE Access*, vol. 6, pp. 70025-70034, 2018.

[10] Z. Tang, J. Song, X. Zhang, and R. Sun, “Multiple-image encryption with bit-plane decomposition and chaotic maps,” *Optics and Lasers in Engineering*, vol. 80, pp. 1-11, 2016.

[11] L. M. Adleman, “Molecular computation of solutions to combinatorial problems,” *Science*, vol. 266, no. 5187, pp. 1021-1024, 1994.

[12] S. K. Pujari, G. Bhattacharjee, and S. Bhoi, “A hybridized model for image encryption through genetic algorithm and DNA sequence,” *Procedia Computer Science*, vol. 125, pp. 165-171, 2018.

[13] A. U. Rehman, H. Wang, M. M. A. Shahid, S. Iqbal, Z. Abbas, and A. Firdous, “A selective cross-substitution technique for encrypting color images using chaos, DNA Rules and SHA-512,” *IEEE Access*, vol. 7, pp. 162786-162802, 2019.

[14] Z. Liu, C. Wu, J. Wang, and Y. Hu, “A color image encryption using dynamic DNA and 4-D memristive hyper-chaos,” *IEEE Access*, vol. 7, pp. 78367-78378, 2019.

[15] J. Kalpana and P. Murali, “An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos,” *Optik*, vol. 126, no. 24, pp. 5703-5709, 2015.

[16] X. Li, L. Wang, Y. Yan, and P. Liu, “An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems,” *Optik*, vol. 127, no. 5, pp. 2558-2565, 2016.

[17] 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, 2016.

[18] X. Chai, Y. Chen, and L. Broyde, “A novel chaos-based image encryption algorithm using DNA sequence operations,” *Optics and Lasers in engineering*, vol. 88, pp. 197-213, 2017.

[19] B. Mondal and T. Mandal, “A light weight secure image encryption scheme based on chaos & DNA computing,” *Journal of King Saud University-Computer and Information Sciences*, vol. 29, no. 4, pp. 499-504, 2017.

[20] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, “A color image cryptosystem based on dynamic DNA encryption and chaos,” *Signal Processing*, vol. 155, pp. 44-62, 2019.

[21] P. Li, J. Xu, J. Mou, and F. Yang, “Fractional-order 4D hyperchaotic memristive system and application in color image encryption,” *EURASIP Journal on Image and Video Processing*, vol. 2019, article no. 22, 2019. https://doi.org/10.1186/s13640-018-0402-7

[22] X. Wu, B. Zhu, Y. Hu, and Y. Ran, “A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps,” *IEEE Access*, vol. 5, pp. 6429-6436, 2017.

[23] S. Hraoui, F. Gmira, M. F. Abbou, A. J. Oulidi, and A. Jarjar, “A new cryptosystem of color image using a dynamic-chaos hill cipher algorithm,” *Procedia Computer Science*, vo. 148, pp. 399-408, 2019.

[24] J. Wu, X. Liao, and B. Yang, “Color image encryption based on chaotic systems and elliptic curve ElGamal scheme,” *Signal Processing*, vol. 141, pp. 109-124, 2017.

Menglong Wu **https://orcid.org/0000-0003-1818-9019**

He received his Ph.D. in communications and information systems from Beijing University of Posts and Telecommunications. He is currently an associate professor of Information Science and Technology at the North China University of Technology. He mainly engaged in optical communication.

Yan Li **https://orcid.org/0000-0001-9158-5849**

She received B.S. degree in Electronic and Information Engineering from the North China University of Technology in 2018. She is currently a graduate student in Electronics and Communication Engineering from the North China University of Technology since 2018.

Wenkai Liu **https://orcid.org/0000-0001-8050-0942**

He graduated from the Institute of Semiconductors, Chinese Academy of Sciences as a Ph.D. candidate in 2002. He is currently a professor of Information Science and Technology at the North China University of Technology. He mainly engaged in optical communication, photonic devices and photonic integration.