IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 29 March 2023, accepted 12 April 2023, date of publication 21 April 2023, date of current version 19 May 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3267485

RESEARCH ARTICLE

A Self-Adaptive Image Encryption Scheme Based on Chaos and Gravitation Model

QIUXIA QIN[1], ZHONGYUE LIANG[1], SHUANG LIU[1], AND CHANGJUN ZHOU[2]
[1]College of Computer Science and Engineering, Dalian Minzu University, Dalian 116600, China
[2]College of Mathematics and Computer Science, Zhejiang Normal University, Jinhua 321000, China

Corresponding authors: Shuang Liu (liushuang@dlnu.edu.cn) and Changjun Zhou (zhouchangjun@zjnu.edu.cn)

This work was supported by the Liaoning Province Economic and Social Development Research Project 2023 of Provincial Social Science Association under Grant 2023lslybkt-039.

ABSTRACT In order to improve the security of image transmission, this paper proposes a self-adaptive image encryption scheme based on chaos and gravitation model. The proposed scheme consists of three stages: key generation stage, double scrambling stage, and double diffusion stage. In the key generation stage, the plaintext-associated key generation mechanism (BPPAKG) based on the bit plane is used to obtain the key associated with the plaintext. Since the key ultimately depends on the plaintext image itself, this scheme has self-adaptability. The first stage of scrambling uses mixed chaotic transform and shift row transform to disturb pixel position, then changes the pixel value of the image based on the concept of gravitation to achieve the first stage of diffusion. To enhance the security performance of the scheme, the traditional encryption structure is extended, and the second stage of scrambling and diffusion is quickly realized by using diagonal scanning transform and XOR operation. Simulation and experimental results show that the scheme has good encryption and decryption performance and strong resistance to attack. In addition, compared with some latest proposed algorithms, it has better security.

INDEX TERMS Chaos, diagonal scanning transform, image encryption, gravitation model, self-adaptation.

I. INTRODUCTION

In recent years, the high demand for information exchange, and a large number of data transmissions and sharing, so multimedia technology has been rapid development. At the same time, it also causes the risk of data loss and destruction to some extent. As one of the important forms of data transmission, the digital image is very likely to be seriously damaged in channel transmission, and some criminals easily steal confidential information. Traditional encryption schemes (AES, RSE, etc. [1], [2], [3]) for image encryption have problems of weak security and low efficiency. Therefore, it is urgent to propose a more effective and secure image encryption scheme.

At present, some image encryption schemes using technologies in different fields have been proposed, such as chaos theory [4], [5], [6], DNA encryption [7], [8], [9], compressed sensing [10], [11], [12], cellular automata [13], [14], [15], etc.. Chaotic system has become the most widely used encryption technology because of its initial value sensitivity, pseudo-randomness, ergodic and aperiodic characteristics. Moreover, a recent survey shows that more than 32% of encryption schemes use chaos theory techniques [16].

In the chaotic image encryption scheme, the chaotic system and encryption structure become the most important components. Among them, there are two types of chaotic systems for encryption schemes, namely low-dimensional chaotic systems (LCM) and high-dimensional chaotic systems (HCM). Some experts and scholars mainly focus on the study of low-dimensional chaotic systems because of their simple structure and low computational cost. Zareai et al. [17] used Logistic mapping to develop image keys, which increased the key space of the scheme, but the performance of Logistic mapping would affect the security of the algorithm to a certain extent. Shamsa et al. [18] proposed an image encryption scheme based on Sine mapping and cyclic matrix; Sine

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

mapping was used for the substitution phase of images. Kumar and Girdhar [19] applied 2D Logistic mapping to the bit-level scrambling process of RGB channels, which can effectively encrypt color images. But low-dimensional chaotic systems, especially classical low-dimensional chaotic systems, usually lack complex chaotic behavior. To remedy this problem, many experts and scholars propose encryption schemes using high-dimensional chaotic systems. Qian et al. [20] have used various 3D chaotic maps for the encryption process, 3D logistic mapping for changing image pixel values, and 3D cat mapping for changing pixel positions. However, in this scheme, two high-dimensional chaotic maps are used for encryption at the same time, which will greatly increase the calculation cost. Telem et al. [21] proposed an image encryption scheme based on DNA coding and 3D chaotic system, which acts as a chaos generator to obtain the diffusion key. Liang et al. [22] obtained four groups of chaotic sequences based on the 4D chaotic system, and the chaotic sequences were successively used in the four-way diffusion process, effectively improving the diffusion effect of the encryption scheme. But the high computational cost of high-dimensional chaotic system seriously affects the efficiency of encryption and decryption. For encryption structures, since Fridrich [23] proposed the scramble-diffusion encryption structure in the first place, many experts and scholars have proposed a variety of encryption schemes based on this structure. Based on the traditional framework, Hua et al. [24] used the cross-plane idea to disturb the position of image rows and columns and change image pixel values in a non-sequential manner. Yang et al. [1] designed a novel four-dimensional memristor hyperchaos and proposed a novel image encryption algorithm based on this chaos. The algorithm uses the bit plane technology to disturb the image position, and then realizes the image encryption by DNA coding, DNA operation, positive order and reverse order diffusion. Kamal et al. [25] proposed an encryption scheme suitable for grayscale and color medical images, which used methods such as zigzag transform and rotation to perturb the images and then used chaotic keys to diffuse the images. Khalil et al. [26] applied a variety of chaos in the scrambling process and realized image diffusion quickly by using the XOR operation. The results show that this scheme has high anti-statistical attack capability. In general, the more rounds scrambled and diffused in an encryption scheme, the better the encryption performance, but also the longer the time.

Aiming at the problems of chaotic system and encryption structure, this paper proposes a self-adaptive image encryption scheme based on chaos and gravitation model. On the one hand, 2D-LTMM and 1D-SCS chaotic systems with superior chaotic performance and simple structure are selected according to the characteristics and shortcomings of low-dimensional chaotic systems and high-dimensional chaotic systems respectively. On the other hand, in order to improve the encryption performance, a second round of scrambling and diffusion is added to the traditional encryption structure, but in order not to affect the encryption efficiency, fast and efficient diagonal scanning transform and XOR operation are selected. Simulation results and experimental analysis show that the proposed scheme can obtain ciphertext images with high security and strong robustness at an acceptable running speed, and has the ability to resist known plaintext attacks, chosen plaintext attacks, differential attacks and noise attacks. The main contributions of this study are as follows:

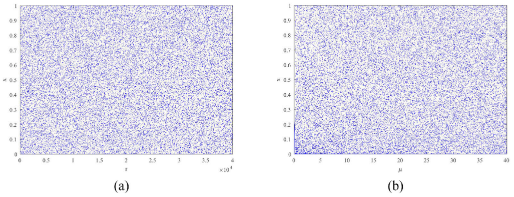


FIGURE 1. **1D-SCS bifurcation diagrams (a) bifurcation diagram (μ=5), (b) bifurcation diagram (r = 0.2807).**

(1) After comparison and analysis, 2D-LTMM and 1D-SCS systems with ultra-high chaos performance and low computational cost are selected to improve the randomness of the scheme.

(2) A bit plane-based plaintext associated key generation mechanism (BPPAKG) is proposed, which not only improves the sensitivity of the algorithm to plaintext but also realizes the one-time pad strategy.

(3) Based on the traditional scramble-diffusion structure, new scramble-diffusion stages are added to enhance the security of the algorithm without affecting the efficiency as far as possible.

(4) Simulation experiments and performance analysis show that the proposed scheme has a higher security level than some existing encryption schemes.

The rest of this paper is arranged as follows: Section II introduces the chaotic system, gravitation model, diagonal scanning transform and other related knowledge, Section III gives a detailed encryption and decryption scheme, Section IV carries out the simulation experiment and performance analysis of the proposed scheme, and Section V gives the conclusion.

II. RELATED WORK

A. CHAOTIC SYSTEMS

1) 1D-SCS

Based on Sine mapping, 1D-SCS [27] is extended. Since the chaos has two parameters, it has better chaotic characteristics than Sine. 1D-SCS are defined as follows:

$$x_{n+1} = (\mu(3+2r)(1-sin(\pi x_n)))mod 1 \tag{1}$$

where μ and r are system parameters, x is system variable. When $\mu \in (4, +\infty)$ and $r \in (0, +\infty)$, the system has good chaotic performance. To observe the dynamic behavior of the chaotic system, the bifurcation diagram of 1D-SCS is shown in Fig. 1. When the parameter μ or r is fixed, any value of the other parameter can make the data points evenly distributed

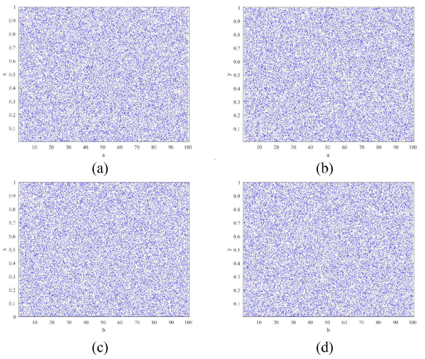


FIGURE 2. 2D-LTMM bifurcation diagrams (a) *a* for *x*, (b) *a* for *y*, (c) *b* for *x*, (d) *b* for *y*.

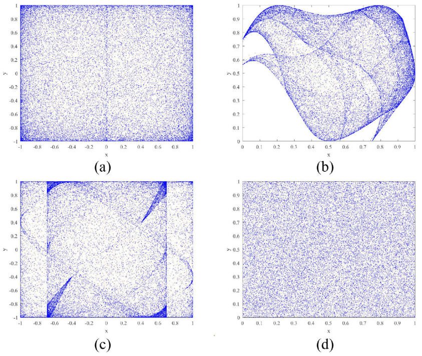


FIGURE 3. Trajectories (a) 2D-SCCM with $\alpha = 4$, $\beta = 4$, (b) 2D-LSMCL with $\alpha = 0.75$, $\beta = 3$, (c) 2D-HM with $\alpha = 2$, $\beta = 1$, (d) 2D-LTMM with $a = 50$, $b = 50$.

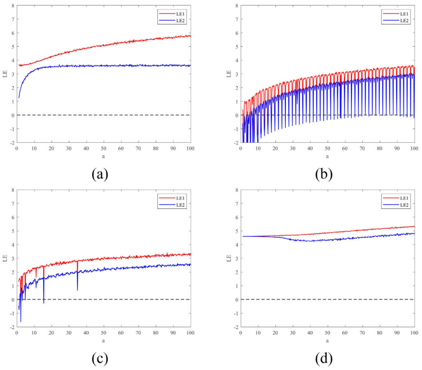


FIGURE 4. LEs (a) 2D-SCCM with $\alpha = 4$, $\beta = 4$, (b) 2D-LSMCL with $\alpha = 0.75$, $\beta = 3$, (c) 2D-HM with $\alpha = 2$, $\beta = 1$, (d) 2D-LTMM with $a = 50$, $b = 50$.

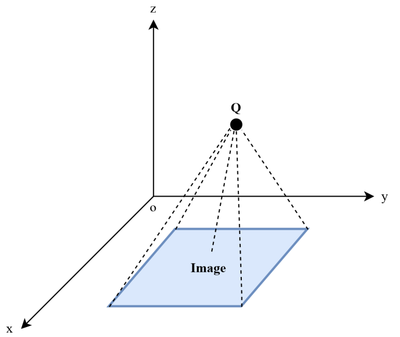


FIGURE 5. Diffusion principle based on gravitation model.

between [0, 1], indicating that the system has stable chaotic behavior.

2) 2D-LTMM

After the combination of Logistic and Tent maps, fixed value, dimension expansion and other operations, 2D-LTMM [24] is obtained. 2D-LTMM is defined as follows:

$$\begin{cases} x_{i+1} = \begin{cases} (4ax_i(1-x_i)+2by_i)mod1, y_i < 0.5 \\ (4ax_i(1-x_i)+2b(1-y_i))mod1, y_i \geq 0.5 \end{cases} \\ y_{i+1} = \begin{cases} (4ay_i(1-y_i)+2bx_i)mod1, x_i < 0.5 \\ (4ay_i(1-y_i)+2b(1-x_i))mod1, x_i \geq 0.5 \end{cases} \end{cases} \tag{2}$$

where a and b are system parameters, $a, b \in [1, 100]$, x and y are system variables. To evaluate the chaos performance of 2D-LTMM, the bifurcation diagram of 2D-LTMM is presented in this section and compared with the trajectory diagram of 2D-SCCM [28], 2D-LSMCL [29], 2D-HM [30] and Lyapunov index spectrum, as shown in Figs. 2, 3 and 4. The bifurcation diagram shows that 2D-LTMM variables have access to the entire data range. In addition, compared with other new two-dimensional chaotic systems, the trajectory of 2D-LTMM is more evenly distributed in the whole phase space, and the LEs (Lyapunov index) value is also larger, which means that the trajectory divergence ability of this chaos is stronger and the chaotic behavior is more complex.

B. GRAVITATION MODEL

Gravity is the force of attraction between any object in nature. The gravitational attraction between two objects is calculated as follows:

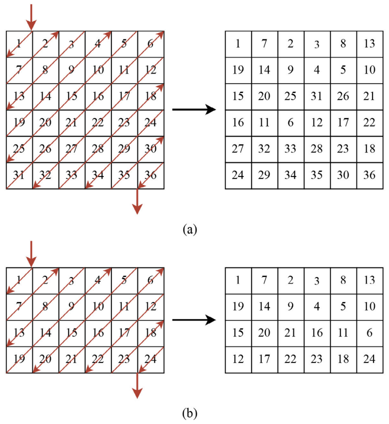
$$F = G\frac{Mm}{r^2} \tag{3}$$

where G is the gravitational constant, M and m are the masses of the two objects, and r is the distance between the two objects. Li et al. [31] extended the classical concept of gravitation to image encryption technology. It is assumed that Q is any point in space, there is an image P of $H \times W$ in the x-y plane, and every pixel in the image has gravitation with point Q, so this model can be used to change the pixel value of the image to achieve image diffusion. The diffusion principle based on the gravitation model is shown in Fig. 5.

The formula of the improved gravitation model is defined as follows [31]:

$$F_{u,v} = [G\frac{m(x,y,z)m(u,v)}{(x-u)^2+(y-v)^2+z^2}]mod256 \oplus P_{u,v} \tag{4}$$

where G is the universal gravitation constant, $m(x, y, z)$ is the mass of Q, $P_{u,v}$ is the image pixel value before it is changed, $m(u, v)$ is the mass of $P_{u,v}$, $F_{u,v}$ is the result after



$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 7 & 8 & 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 & 17 & 18 \\ 19 & 20 & 21 & 22 & 23 & 24 \\ 25 & 26 & 27 & 28 & 29 & 30 \\ 31 & 32 & 33 & 34 & 35 & 36 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 7 & 2 & 3 & 8 & 13 \\ 19 & 14 & 9 & 4 & 5 & 10 \\ 15 & 20 & 25 & 31 & 26 & 21 \\ 16 & 11 & 6 & 12 & 17 & 22 \\ 27 & 32 & 33 & 28 & 23 & 18 \\ 24 & 29 & 34 & 35 & 30 & 36 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 7 & 8 & 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 & 17 & 18 \\ 19 & 20 & 21 & 22 & 23 & 24 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 7 & 2 & 3 & 8 & 13 \\ 19 & 14 & 9 & 4 & 5 & 10 \\ 15 & 20 & 21 & 16 & 11 & 6 \\ 12 & 17 & 22 & 23 & 18 & 24 \end{bmatrix}$$

FIGURE 6. Diagonal scanning transform (a) 6 × 6 square matrix, (b) 6 × 4 non-square matrix.

pixel diffusion, [] is the integer operation, *mod*() is the mod function, $\oplus$ is the xor operation. In addition, $m(x, y, z)$ is set to 1 for ease of calculation.

C. DIAGONAL SCANNING TRANSFORM

Diagonal scanning transform refers to the process of sequential scanning of diagonal elements of matrix starting from the upper left corner of matrix and converting one-dimensional sequence obtained after scanning into two-dimensional matrix based on the dimension of image [32].

Compared with classical zigzag scanning, zigzag scanning is only for square matrices, and diagonal scanning is no longer limited to the shape of the matrix, not only for square matrices but also for non-square matrices. Fig. 6(a) demonstrates the diagonal scanning transform process of 6 × 6 square matrix, and Fig. 6(b) demonstrates the diagonal scanning transform process of 6 × 4 non-square matrix. The results show that the diagonal scanning transform can effectively disturb the position of pixels.

III. PROPOSED ENCRYPTION AND DECRYPTION ALGORITHM

This paper proposed a self-adaptive image encryption scheme based on chaos and gravitation model, including the key generation stage, chaotic sequence and chaotic matrix generation stage, the first scrambling stage, the first diffusion stage, the second scrambling stage and the second diffusion stage. Fig. 7 shows the encryption process for this scheme. For details about the encryption procedure, see Sections III-A-III-G.

A. KEY GENERATION

This section uses bit plane-based plaintext associated key generation mechanism (BPPAKG) and external key (EK) to obtain the key, which includes 2D-LTMM and 1D-SCS chaotic initial values and parameters, and random numbers used for diffusion.

Fig. 8 shows the schematic diagram of BPPAKG. The plaintext image $P(M \times N)$ is decomposed into four

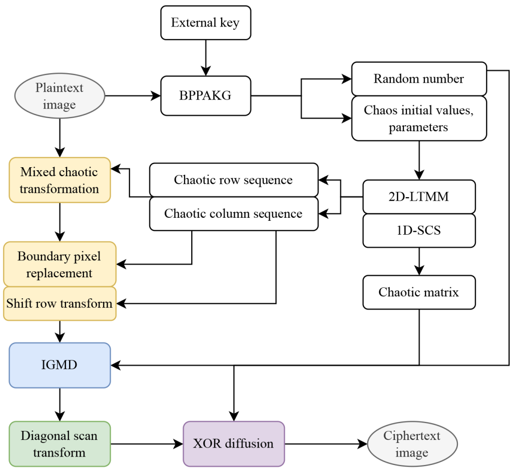


FIGURE 7. Encryption flowchart.

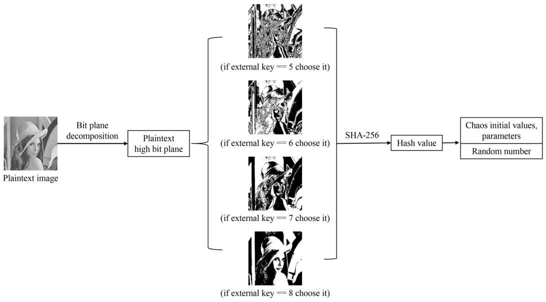

Plaintext image
Bit plane decomposition
Plaintext high bit plane
(if external key == 5 choose it)
(if external key == 6 choose it)
(if external key == 7 choose it)
(if external key == 8 choose it)
SHA-256
Hash value
Chaos initial values, parameters
Random number

FIGURE 8. Schematic diagram of BPPAKG.

high-position planes $(B_1 - B_4)$ containing a large amount of image information. Then, according to EK, one of the four planes is selected as the input of SHA-256 to obtain the plaintext hash value H. Since the key obtained depends on the plaintext image itself, BPPAKG makes the encryption scheme self-adaptive.

In addition, the key obtained after processing the plaintext hash value includes the initial value $x(0)$ of 1D-SCS, parameters r and μ; initial values of 2D-LTMM $x_1(0)$, $y_1(0)$, parameters a and b; random number X, Y, Z. The process from plaintext hash value H to the key is as (5)–(7), shown at the bottom of the next page. where $hex2dec()$ converts a hexadecimal number represented by a string into a decimal number, *mod*() is a complementary function.

B. CHAOTIC SEQUENCE AND CHAOTIC MATRIX GENERATION

In this section, two chaotic systems are used to obtain chaotic sequences and matrices. Among them, 2D-LTMM iteration obtained chaotic row sequence S_r and chaotic column sequence S_c, and 1D-SCS iteration obtained chaotic matrix CM. The specific process is as follows:

Step 1: Calculate the effective number *len* of 2D-LTMM iterations according to the plaintext size. The process is as follows:

$$len = max(M, N) \tag{8}$$

where $max()$ is used to find the maximum value of a given parameter.

Step 2: 2D-LTMM chaos iteration $len + 500$ times, chaotic sequences x_1 and y_1 are obtained after discarding the results of the first 500 times.

Step 3: Sort the chaotic sequence respectively to obtain two index sequences x_index and y_index. The process is as follows:

$$[\sim, x\_index] = sort(x_1) \tag{9}$$

$$[\sim, y\_index] = sort(y_1) \tag{10}$$

where $sort()$ is the sorting function.

Step 4: Obtain chaotic row sequence and column sequence by using two index sequences respectively, the process is as follows:

$$\begin{cases} S_r = x\_index \\ S_c = y\_index \end{cases} \tag{11}$$

Step 5: 1D-SCS chaotic iteration $len + 500$ times at the same time, chaotic sequence x is obtained after discarding the results of the first 500 times.

Step 6: Carry out modular processing on chaotic sequence x to obtain chaotic matrix CM, the process is as follows:

$$CM = mod(x \times 10^8, 256) \tag{12}$$

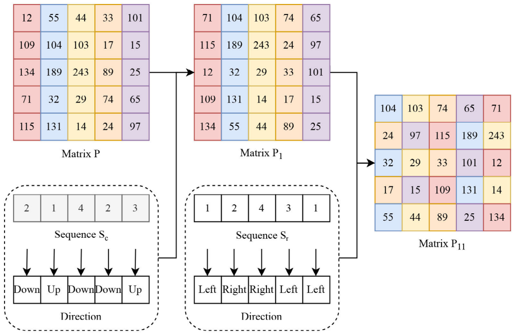
where $mod()$ is the complementary function.

C. FIRST SCRAMBLING STAGE

The first scrambling stage is mainly divided into two parts, including mixed chaotic transform and shifted row transform.

1) MIXED CHAOTIC TRANSFORM

Based on chaotic row sequence, chaotic column sequence and odd-even change, mixed chaotic transform is proposed. It includes cyclic column shift transform and cyclic row shift transform, which can effectively change the position of each pixel of the image through two transforms.



12	55	44	33	101
109	104	103	17	15
134	189	243	89	25
71	32	29	74	65
115	131	14	24	97

Matrix P

71	104	103	74	65
115	189	243	24	97
12	32	29	33	101
109	131	14	17	15
134	55	44	89	25

Matrix P_1

104	103	74	65	71
24	97	115	189	243
32	29	33	101	12
17	15	109	131	14
55	44	89	25	134

Matrix P_{11}

2	1	4	2	3
Down	Up	Down	Down	Up

Sequence S_c / Direction

1	2	4	3	1
Left	Right	Right	Left	Left

Sequence S_r / Direction

FIGURE 9. Mixed chaotic transform.

The schematic diagram of mixed chaotic transform is shown in Fig. 9. The column shift transforms first, then the row shift transform. In the process of column shift, the elements of chaotic column sequence S_c and the columns of matrix P show a corresponding relationship. When the ith element of S_c is even, the elements of the ith column of matrix P move down successively, and the step of the downward movement is determined by the value of the ith element of S_c. Conversely, when the ith element of S_c is odd, the ith column element of matrix P is cyclically shifted upward. In the process of row shift, the elements of the chaotic row sequence S_r and the rows of matrix P_1 show a corresponding relationship. When the jth element of S_r is even, the elements of the jth row of matrix P_1 shift to the right successively, and the step of the right shift is determined by the value of the jth element of S_r. Conversely, if the jth element of S_r is odd, the jth row of P_1 shifts to the left.

2) SHIFTED ROW TRANSFORM

To avoid the influence of image boundary elements on the encryption process, the boundary pixel is replaced first, and then the shifted row transform is carried out. The details are as follows:

Step 1: Replace image boundary pixel values with chaotic column sequence S_c, the process is as follows:

$$\begin{cases} P_{12}(1, i) = S_c(uint16(P_{11}(1, i)) + 1) \\ P_{12}(M, i) = S_c(uint16(P_{11}(M, i)) + 1) \\ i = 1, 2, \ldots, N \end{cases} \tag{13}$$

$$\begin{cases} x(0) = mod((hex2dec(H(1:3)) \times 10^6 + hex2dec(H(4:6)) \times 10^{10}), 1) \\ r = hex2dec(H(7:9) \times 10^6 + hex2dec(H(10:12)) \times 10^{10} \\ \mu = hex2dec(H(13:15) \times 10^6 + hex2dec(H(16:18)) \times 10^{10} \end{cases} \tag{5}$$

$$\begin{cases} x_1(0) = mod((hex2dec(H(19:21)) \times 10^6 + hex2dec(H(22:25)) \times 10^{10}), 1) \\ y_1(0) = mod((hex2dec(H(26:28)) \times 10^6 + hex2dec(H(29:32)) \times 10^{10}), 1) \\ a = hex2dec(H(33:35) \times 10^6 + hex2dec(H(36:39)) \times 10^{10} \\ b = hex2dec(H(40:42) \times 10^6 + hex2dec(H(43:46)) \times 10^{10} \end{cases} \tag{6}$$

$$\begin{cases} X = mod((hex2dec(H(47:49)) \times 10^6 + hex2dec(H(50:52)) \times 10^{10}), 100) \\ Y = mod((hex2dec(H(53:55)) \times 10^6 + hex2dec(H(56:58)) \times 10^{10}), 100) \\ Z = mod((hex2dec(H(59:61)) \times 10^6 + hex2dec(H(62:64)) \times 10^{10}), 100) \end{cases} \tag{7}$$

Step 2: According to the principle of cyclic shift $i-1$ step to the left of the ith row, the matrix is shifted to obtain matrix P_{13}.

D. FIRST DIFFUSION STAGE

The first round of image pixel diffusion is carried out based on the improved gravitation model. The specific process is as follows:

Step 1: To increase the randomness of the scheme and establish the correlation between pixel mass and pixel position, the calculation process of pixel mass $m(u, v)$ of image P_{13} is as follows:

$$m(u, v) = XYu^3 + YZv^3 + XYZ \tag{14}$$

where (u, v) is the coordinate of image P_{13} pixel, and X, Y, Z are the key random number.

Step 2: According to IGMD (Improved gravitation model diffusion), the diffused image P_{21} is obtained. The process is as follows:

$$\begin{cases} T(u, v) = mod(round(G \times m(u, v) \\ /[(X-u)^3 + (Y-u)^3 + Z^3]), 256) \\ P_{21}(u, v) = T(u, v) \oplus P_{13}(u, v) \\ u = 1, \ldots, M; v = 1, \ldots, N. \end{cases} \tag{15}$$

where G is the universal gravitation constant, $mod()$ is the mod function, $round()$ is the rounded function, and $\oplus$ is the xor operation.

E. SECOND SCRAMBLING STAGE

To completely disturb the position of image pixels, image P_{21} is scanned diagonally. The specific process is as follows:

Step 1: Image P_{21} is scanned according to the rule of diagonal scanning to obtain a one-dimensional scan sequence SD.

Step 2: Transform the scan sequence SD into a two-dimensional matrix P_{31} in the form of rows, the process is as follows:

$$\begin{cases} P_{31} = SD(1, (i-1) \times N + j) \\ i = 1, \ldots, M; j = 1, \ldots, N. \end{cases} \tag{16}$$

F. SECOND DIFFUSION STAGE

Based on XOR operation and chaotic matrix, two-round diffusion of image is realized. The specific process is as follows:

Step 1: Initial processing of the elements in the first row of image P_{31} is carried out as follows:

$$E(1, j) = P_{31}(1, j) \oplus SM(1, j), j = 1, \ldots, N. \tag{17}$$

Step 2: Perform XOR processing on the remaining elements of the image to obtain ciphertext image E. The process is as follows:

$$\begin{cases} E(i, j) = P_{31}(i, j) \oplus P_{31}(i-1, j) \oplus SM(i, j) \\ i = 2, \ldots, M; j = 1, \ldots, N. \end{cases} \tag{18}$$

where $\oplus$ is the xor operation.

G. ENCRYPTION PROCESS

This paper proposed a self-adaptive image encryption scheme based on chaos and gravitation model. The specific steps are as follows:

Step 1: The plaintext image P and the external key EK are used to generate keys such as chaotic initial values, parameters and random numbers, as shown in Section III-A.

Step 2: Chaotic system generates chaotic row sequence, chaotic column sequence and chaotic matrix through system iteration, as shown in Section III-B.

Step 3: The first scrambling round of the image is realized through mixed chaotic transform and shifted row transform of the plaintext image, as shown in Section III-C.

Step 4: The first-round scrambling matrix continues to diffuse based on the improved gravitation model, changing pixel values, as shown in Section III-D.

Step 5: The first-round diffusion matrix uses diagonal scanning transform to completely disrupt pixel positions, as shown in Section III-E.

Step 6: The second-round scrambling matrix completes the change of pixel value based on the XOR operation to obtain ciphertext image E, and the encryption is finished, as shown in Section III-F.

H. DECRYPTION PROCESS

The decryption process is the opposite of the encryption process. Firstly, note that the key and ciphertext image used must be consistent with those used and generated during the encryption process. Secondly, the decryption process is followed by the second round of diffusion inverse operation, the second round of scrambling inverse operation, the first round of diffusion inverse operation and the first round of scrambling inverse operation, and the order shall not be changed. Other operations are similar to encryption and will not be discussed again.

IV. SIMULATION EXPERIMENT AND PERFORMANCE ANALYSIS

A. SIMULATION EXPERIMENT

To verify the effectiveness of the self-adaptive image encryption scheme based on chaos and gravitation model, a personal computer (CPU: Intel(R) Core(TM) i7-1065G7 CPU @ 1.30GHz 1.50GHz), MATLAB R2020a is applied under Windows10 operating system performs encryption and decryption tests on 256 × 256 Lena, Peppers, Persons, Charts, and Lady images. Where the external key EK is set to 6, and the rest of the keys change as the input plaintext changes. The experimental results of encryption and decryption are shown in Fig. 10. As can be seen from Fig. 10, the ciphertext image cannot identify any information about the plaintext, and the decrypted image is visually consistent with the plaintext image, indicating that the scheme has a good encryption and decryption effect.

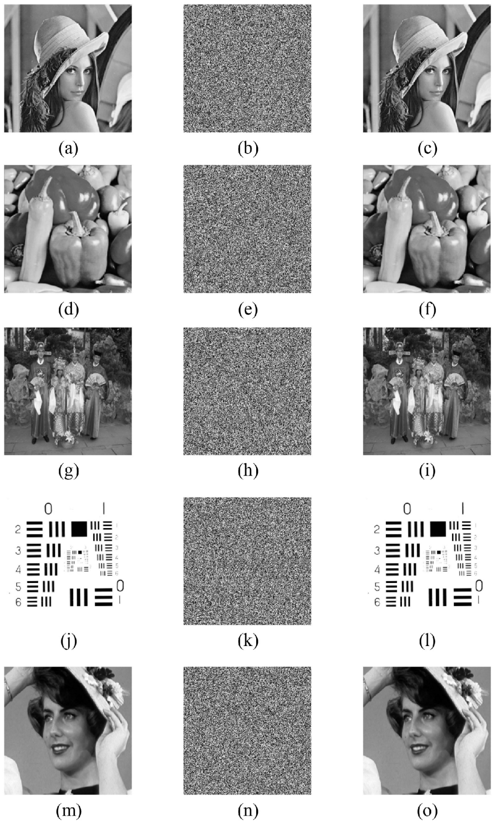


FIGURE 10. Experimental results of encryption and decryption (a) Lena plaintext image, (b) Lena ciphertext image, (c) Lena decrypted image, (d) Peppers plaintext image, (e) Peppers ciphertext image, (f) Peppers decrypted image, (g) Persons plaintext image, (h) Persons ciphertext image, (i) Persons decrypted image, (j) Charts plaintext image, (k) Charts ciphertext image, (l) Charts decrypted image, (m) Lady plaintext image, (n) Lady ciphertext image, (o) Lady decrypted image.

B. KEY SPACE ANALYSIS

Brute force attacks are the most direct way to break a cryptosystem, and criminals often use all possible keys to break a cryptosystem. Generally, when the key space is larger than 2^{100}, the algorithm is sufficient to resist violent attacks [33]. The key of this scheme mainly includes the external key EK, the initial value $x(0)$ of 1D-SCS obtained by BPPAKG mechanism, the parameters r, μ, the initial value $x_1(0)$ and $y_1(0)$ of 2D-LTMM, the parameters a and b, and the random numbers X, Y and Z. Assuming that the numerical calculation accuracy is 10^{-16}, the key space of this scheme is $(10^{-16})^{11} \geq 2^{528}$, which is much larger than 2^{100}.

In addition, the key space of this scheme is compared with other latest schemes, and the comparison results are shown in Table 1. As can be seen from Table 1, the key space of this scheme is larger than that of other encryption schemes, and it has a stronger ability to resist violent attacks.

C. KEY SENSITIVITY ANALYSIS

As an important part of the cryptosystem, the key should be highly sensitive, that is, the change of any bit of the key will have a great impact on the encryption result [37]. Since most of the keys in this scheme are generated by the hash function, and the hash value greatly affects the key, the plaintext hash value is changed one bit to evaluate the key sensitivity of this scheme. The experimental results are shown in Fig. 11. As can be seen from Fig. 11, it is difficult to get the correct decrypted image with the wrong key, indicating that the algorithm has good key sensitivity.

TABLE 1. Key space comparison of different schemes.

Proposed	Ref. [34]	Ref. [35]	Ref. [36]
$\geq 2^{528}$	2^{448}	2^{432}	2^{256}

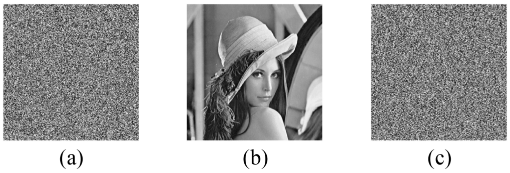


FIGURE 11. Key sensitivity experimental results (a) ciphertext image, (b) decrypted image with the correct key, (c) decrypted image with the incorrect key.

TABLE 2. Information entropy.

Image	Plaintext information entropy	Ciphertext information entropy
Lena	7.4202	7.9987
Peppers	7.5681	7.9984
Persons	7.3835	7.9985
Charts	1.5483	7.9484
Lady	7.4560	7.9986

D. INFORMATION ENTROPY ANALYSIS

Information entropy is a quantitative index of uncertainty in data information, which is often used to evaluate the randomness of images [38]. The formula for calculating information entropy is as follows:

$$H(m) = \sum_{i=1}^{L} P(m_i)log_2\frac{1}{P(m_i)} \tag{19}$$

where m_i represents the ith pixel value of image m, $P(m_i)$ is the probability of m_i occurrence, and L represents the gray level of the image. When $L = 256$, the information entropy of an ideal random image is 8. Table 2 shows the information entropy values of the five groups of images before and after encryption, and Table 3 shows the comparison results of Lena's information entropy of this scheme and other latest schemes.

It can be seen from the data in the table that there is an obvious numerical difference between the information entropy of the plaintext image and 8, while the information entropy of the image after encryption in this scheme is very close to 8. In addition, the comparison shows that the randomness of the ciphertext image obtained by this scheme is higher than that

TABLE 3. Lena information entropy comparison.

Algorithm	Information entropy
Proposed	7.9987
Ref. [34]	7.9960
Ref. [35]	7.9972
Ref. [36]	7.9975

TABLE 4. Correlation coefficient.

Image	Plaintext image			Ciphertext image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9380	0.9673	0.9119	0.0021	-0.0010	-0.0003
Peppers	0.9679	0.9795	0.9471	-0.0004	0.0012	-0.0057
Persons	0.9100	0.9449	0.8829	-0.0022	0.0008	0.0010
Charts	0.8791	0.8643	0.7597	-0.0016	0.0003	-0.0014
Lady	0.9838	0.9903	0.9823	-0.0050	0.0054	-0.0005

of other relevant schemes, and the ability to resist entropy attacks is stronger.

E. CORRELATION ANALYSIS

There is a high degree of correlation between adjacent pixels in a plaintext image, and pixels often leak information about their adjacent pixels [39]. In this case, the attacker can generally infer the information of the plaintext image from the known pixels, so the encryption scheme needs to break the strong correlation between adjacent pixels of the plaintext image. The calculation formula for the correlation coefficient is as follows:

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{20}$$

$$cov(x, y) = \frac{1}{N} \times \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \tag{21}$$

$$D(x) = \frac{1}{N} \times \sum_{i=1}^{N} (x_i - E(x)^2) \tag{22}$$

$$E(x) = \frac{1}{N} \times \sum_{i=1}^{N} x_i \tag{23}$$

where r_{xy}, $cov(x, y)$, $D(x)$ and $E(x)$ are correlation, covariance, variance and mean, respectively. In this section, 3000 pairs of adjacent pixels are randomly selected from the horizontal, vertical and diagonal directions of the test image respectively for correlation analysis. The experimental results are shown in Table 4 and Fig. 12. It can be seen that the correlation coefficient of ciphertext image is very close to 0, and the correlation scatter is evenly distributed in the coordinate axis, indicating that this scheme can effectively break the strong correlation between adjacent pixels of the image. In addition, the correlation of Lena image is compared with other latest schemes in Table 5. This scheme has a smaller correlation value, indicating better encryption performance.

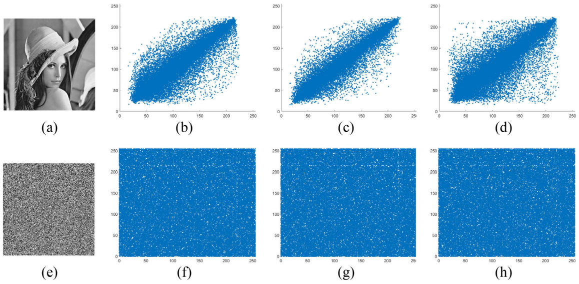


FIGURE 12. Lena correlation scatter diagram (a) plaintext image, (b) plaintext horizontal, (c) plaintext vertical, (d) plaintext diagonal, (e) ciphertext image, (f) ciphertext horizontal, (g) ciphertext vertical, (h) ciphertext diagonal.

TABLE 5. Lena correlation coefficients comparison.

Direction	Proposed	Ref. [34]	Ref. [35]	Ref. [36]
Horizontal	0.0021	0.0015	0.0003	-0.0021
Vertical	-0.0010	0.0024	0.0010	-0.0012
Diagonal	-0.0003	0.0002	0.0036	0.0017

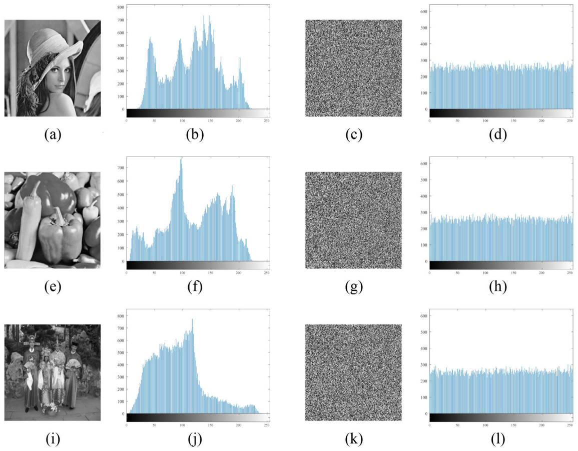


FIGURE 13. Histogram (a) Lena, (b) Lena histogram, (c) Lena ciphertext, (d) Lena ciphertext histogram, (e) Peppers, (f) Peppers histogram, (g) Peppers ciphertext, (h) Peppers ciphertext histogram, (i) Persons, (j) Persons histogram, (k) Persons ciphertext, (l) Persons ciphertext histogram.

F. HISTOGRAM ANALYSIS

The image histogram shows the distribution of image pixels, which can reflect important information about the image [40]. Therefore, to protect image security, the encryption scheme must have the ability to uniform the histogram. Fig. 13 shows the histograms of plaintext and ciphertext images. As can be seen from Fig. 13, the histogram of all ciphertext images achieves uniform distribution of pixels, which means that ciphertext images cannot provide effective information, thus verifying that this scheme can effectively resist statistical attacks.

TABLE 6. NPCR and UACI experiment results.

Image	NPCR(%)	UACI(%)
Lena	99.6093	33.4631
Peppers	99.5998	33.4572
Persons	99.6197	33.4704
Charts	99.6089	33.4625
Lady	99.5987	33.4591

TABLE 7. NPCR and UACI comparison.

Algorithm	NPCR(%)	UACI(%)
Proposed	99.6093	33.4631
Ref. [34]	99.5771	35.0820
Ref. [35]	99.6207	33.4125
Ref. [36]	99.6093	33.4798

G. DIFFERENTIAL ATTACK ANALYSIS

Differential attack is an important analysis method to test the plaintext sensitivity. If the difference between the ciphertext image and the plaintext image obtained after slightly changing the plaintext image is large, it indicates that the scheme has plaintext sensitivity. The rate of change of the number of image pixels (NPCR) and the average intensity of the difference between images (UACI) are often used as quantitative indicators of differential attack [41]. The calculation formulas of NPCR, and UACI are as follows:

$$NPCR = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\% \tag{24}$$

$$UACI = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{| C_1(i,j) - C_2(i,j) |}{255} \times 100\% \tag{25}$$

$$D(i,j) = \begin{cases} 0, C_1(i,j) = C_2(i,j) \\ 1, C_1(i,j) \neq C_2(i,j) \end{cases} \tag{26}$$

where C_1 is the ciphertext image, and C_2 is the ciphertext image obtained by changing one plaintext pixel. The expected values of NPCR and UACI were 99.6094% and 33.4635%, respectively. In this section, the value of one pixel is randomly changed for each test image, and then the NPCR and UACI values of ciphertext images before and after the change are calculated. The experimental results are shown in Table 6. The results in Table 6 show that the NPCR and UACI values of the proposed scheme are very close to ideal values. In addition, Lena's NPCR and UACI values are also compared in Table 7 with other latest schemes, and the comparative data show that this scheme has better differential attack resistance than other schemes.

H. NOISE ATTACK ANALYSIS

Image transmission in the channel will inevitably be affected by various factors, so it will cause distortion, degradation and pollution. These consequences may increase the difficulty for the receiver to decipher the ciphertext image, which requires the encryption scheme to be sufficiently robust [42]. In this section, salt and pepper noise of different intensities is added to the test image to evaluate the robustness of the scheme. The results are shown in Fig. 14. As can be seen from Fig. 14, the image quality of decrypted images obtained after noise interference is slightly decreased, but it still contains valid information consistent with the plaintext image. Therefore, the encryption scheme can reduce the result of noise generated by ciphertext images in the channel.

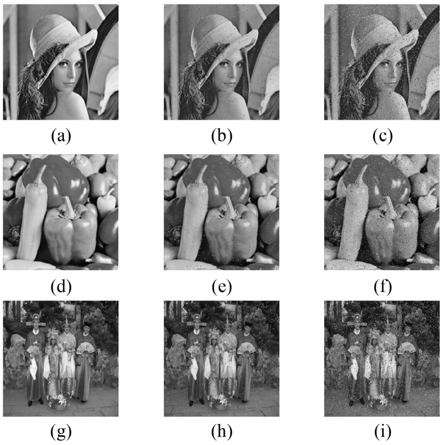


FIGURE 14. Noise attack experiment results (a) Lena, (b) Lena decrypted image with 0.01, (c) Lena decrypted image with 0.05, (d) Peppers, (e) Peppers decrypted image with 0.01, (f) Peppers decrypted image with 0.05, (g) Persons, (h) Persons decrypted image with 0.01, (i) Persons decrypted image with 0.05.

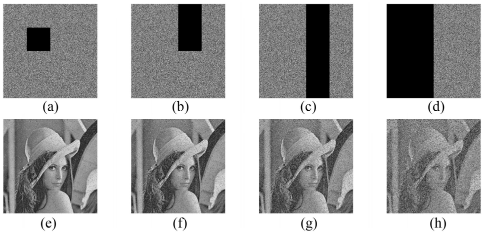


FIGURE 15. Experimental results of cropping attack (a) 1/16 encrypted image, (b) 1/8 encrypted image, (c) 1/4 encrypted image, (d) 1/2 encrypted image, (e) 1/16 decrypted image, (f) 1/8 decrypted image, (g) 1/4 decrypted image, (h) 1/2 decrypted image.

I. CROPPING ATTACK ANALYSIS

Plaintext images will inevitably suffer from malicious cutting in the channel transmission process, resulting in data loss [38]. To verify the robustness of the algorithm for data cropping, data of 1/2, 1/4, 1/8, and 1/16 of the Lena encrypted image were cropped respectively, and the decryption diagram was obtained, as shown in Fig. 15. As can be seen from Fig. 15, Lena's encrypted image after cropping can still restore the information of the plaintext image to the greatest extent after decryption, indicating that the algorithm can resist cropping attacks.

TABLE 8. Encryption and decryption time.

Time	Lena	Peppers	Persons	Charts	Lady
Encryption time (s)	0.0039	0.0046	0.0038	0.0052	0.0054
Decryption time (s)	0.0073	0.0082	0.0074	0.0084	0.0085

TABLE 9. Lena encryption and decryption time comparison.

Time	Proposed	Ref. [34]	Ref. [35]	Ref. [36]
Encryption time (s)	0.0039	0.0048	1.1247	0.0045
Decryption time (s)	0.0073	0.0085	1.2798	0.0079

J. TIME PERFORMANCE ANALYSIS

In general, the time performance and security performance of encryption schemes are contradictory. Encryption schemes must consider encryption time while ensuring security [43]. Therefore, this section tests the encryption and decryption time of images to evaluate the time performance of the encryption scheme. The experimental results are shown in Table 8. As can be seen from Table 8, the image encryption and decryption time are relatively short. In addition, Lena's encryption and decryption time is compared with other latest schemes, and the results are shown in Table 9. It can be seen that this scheme has a shorter running time, which can ensure safety and at the same time have acceptable running efficiency.

V. CONCLUSION

This paper proposed a self-adaptive image encryption scheme based on chaos and gravitation model. In this scheme, the key associated with the plaintext is obtained by the BPPAKG mechanism, which has self-adaptability and realizes a one-time pad. After the analysis and comparison of chaotic systems, 2D-LTMM and 1D-SCS systems with strong chaotic performance and simple structure are used in the encryption process to improve the randomness of the scheme. Double scrambling and double diffusion ensure the security of the encryption scheme. However, the encryption scheme does not involve complex methods and operations, but only uses efficient and fast transform and XOR operation, so this scheme has good time performance. Simulation experiment and performance analysis show that this scheme has a large enough key space, can effectively resist statistical attacks, differential attacks, key sensitivity attacks, noise attacks, known plaintext attacks, and chosen plaintext attacks, and has high encryption efficiency. In the future, we will study chaotic systems with better performance and use them in the encryption process. In addition, compressed sensing and other compression technologies are used in image encryption with a large amount of data to further shorten the running time.

REFERENCES

[1] Y. Yang, L. Wang, S. Duan, and L. Luo, "Dynamical analysis and image encryption application of a novel memristive hyperchaotic system," *Opt. Laser Technol.*, vol. 133, Jan. 2021, Art. no. 106553.

[2] X. Zhang and Y. Hu, "Multiple-image encryption algorithm based on the 3D scrambling model and dynamic DNA coding," *Opt. Laser Technol.*, vol. 141, Sep. 2021, Art. no. 107073.

[3] Y. Zhou, C. Li, W. Li, H. Li, W. Feng, and K. Qian, "Image encryption algorithm with circle index table scrambling and partition diffusion," *Nonlinear Dyn.*, vol. 103, no. 2, pp. 2043–2061, Jan. 2021.

[4] Z. Hua, Z. Zhu, Y. Chen, and Y. Li, "Color image encryption using orthogonal Latin squares and a new 2D chaotic system," *Nonlinear Dyn.*, vol. 104, no. 4, pp. 4505–4522, Jun. 2021.

[5] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, "A new algorithm for digital image encryption based on chaos theory," *Entropy*, vol. 23, no. 3, p. 341, Mar. 2021.

[6] B. Vaseghi, S. Mobayen, S. S. Hashemi, and A. Fekih, "Fast reaching finite time synchronization approach for chaotic systems with application in medical image encryption," *IEEE Access*, vol. 9, pp. 25911–25925, 2021.

[7] A. Babaei, H. Motameni, and R. Enayatifar, "A new permutation-diffusion-based image encryption technique using cellular automata and DNA sequence," *Optik*, vol. 203, Feb. 2020, Art. no. 164000.

[8] X. Wang and Y. Su, "Image encryption based on compressed sensing and DNA encoding," *Signal Process., Image Commun.*, vol. 95, Jul. 2021, Art. no. 116246.

[9] Q. Zhang and J. Han, "A novel color image encryption algorithm based on image hashing, 6D hyperchaotic and DNA coding," *Multimedia Tools Appl.*, vol. 80, no. 9, pp. 13841–13864, Apr. 2021.

[10] X. Chai, H. Wu, Z. Gan, D. Han, Y. Zhang, and Y. Chen, "An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing," *Inf. Sci.*, vol. 556, pp. 305–340, May 2021.

[11] J. S. Khan and S. K. Kayhan, "Chaos and compressive sensing based novel image encryption scheme," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102711.

[12] X. Wang, C. Liu, and D. Jiang, "A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT," *Inf. Sci.*, vol. 574, pp. 505–527, Oct. 2021.

[13] X. Chai, X. Fu, Z. Gan, Y. Zhang, Y. Lu, and Y. Chen, "An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata," *Neural Comput. Appl.*, vol. 32, no. 9, pp. 4961–4988, May 2020.

[14] Y. Dong, G. Zhao, Y. Ma, Z. Pan, and R. Wu, "A novel image encryption scheme based on pseudo-random coupled map lattices with hybrid elementary cellular automata," *Inf. Sci.*, vol. 593, pp. 121–154, May 2022.

[15] J. Zeng and C. Wang, "A novel hyperchaotic image encryption system based on particle swarm optimization algorithm and cellular automata," *Secur. Commun. Netw.*, vol. 2021, Feb. 2021, Art. no. 6675565.

[16] H. M. Ghadirli, A. Nodehi, and R. Enayatifar, "An overview of encryption algorithms in color images," *Signal Process.*, vol. 164, pp. 163–185, Nov. 2019.

[17] D. Zareai, M. Balafar, and M. R. F. Derakhshi, "A new Grayscale image encryption algorithm composed of logistic mapping, Arnold cat, and image blocking," *Multimedia Tools Appl.*, vol. 80, no. 12, pp. 18317–18344, May 2021.

[18] S. Kanwal, S. Inam, F. Hajjej, O. Cheikhrouhou, Z. Nawaz, A. Waqar, and M. Khan, "A new image encryption technique based on sine map, chaotic tent map, and circulant matrices," *Secur. Commun. Netw.*, vol. 2022, pp. 1–17, Oct. 2022.

[19] V. Kumar and A. Girdhar, "A 2D logistic map and Lorenz-Rossler chaotic system based RGB image encryption approach," *Multimedia Tools Appl.*, vol. 80, no. 3, pp. 3749–3773, Jan. 2021.

[20] X. Qian, Q. Yang, Q. Li, Q. Liu, Y. Wu, and W. Wang, "A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques," *IEEE Access*, vol. 9, pp. 61334–61345, 2021.

[21] A. N. K. Telem, H. B. Fotsin, and J. Kengne, "Image encryption algorithm based on dynamic DNA coding operations and 3D chaotic systems," *Multimedia Tools Appl.*, vol. 80, no. 12, pp. 19011–19041, May 2021.

[22] Z. Liang, Q. Qin, and C. Zhou, "An image encryption algorithm based on Fibonacci Q-matrix and genetic algorithm," *Neural Comput. Appl.*, vol. 34, no. 21, pp. 19313–19341, Nov. 2022.

[23] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 8, no. 6, pp. 1259–1284, Dec. 1998.

[24] Z. Hua, Z. Zhu, S. Yi, Z. Zhang, and H. Huang, "Cross-plane colour image encryption using a two-dimensional logistic tent modular map," *Inf. Sci.*, vol. 546, pp. 1063–1083, Feb. 2021.

[25] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37855–37865, 2021.

[26] N. Khalil, A. Sarhan, and M. A. M. Alshewimy, "An efficient color/grayscale image encryption scheme based on hybrid chaotic maps," *Opt. Laser Technol.*, vol. 143, Nov. 2021, Art. no. 107326.

[27] X. Wang and P. Liu, "A new image encryption scheme based on a novel one-dimensional chaotic system," *IEEE Access*, vol. 8, pp. 174463–174479, 2020.

[28] Z. Zhang, J. Tang, F. Zhang, H. Ni, J. Chen, and Z. Huang, "Color image encryption using 2D sine-cosine coupling map," *IEEE Access*, vol. 10, pp. 67669–67685, 2022.

[29] H. Zhu, Y. Zhao, and Y. Song, "2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption," *IEEE Access*, vol. 7, pp. 14081–14098, 2019.

[30] L. Teng, X. Wang, F. Yang, and Y. Xian, "Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion," *Nonlinear Dyn.*, vol. 105, no. 2, pp. 1859–1876, 2021.

[31] X. Li, J. Mou, L. Xiong, Z. Wang, and J. Xu, "Fractional-order double-ring erbium-doped fiber laser chaotic system and its application on image encryption," *Opt. Laser Technol.*, vol. 140, Aug. 2021, Art. no. 107074.

[32] A. S. Mahmood and M. S. M. Rahim, "Novel method for image security system based on improved SCAN method and pixel rotation technique," *J. Inf. Secur. Appl.*, vol. 42, pp. 57–70, Oct. 2018.

[33] M. A. El-Mowafy, S. M. Gharghory, M. A. Abo-Elsoud, M. Obayya, and M. I. F. Allah, "Chaos based encryption technique for compressed H264/AVC videos," *IEEE Access*, vol. 10, pp. 124002–124016, 2022.

[34] Y. Abanda and A. Tiedeu, "Image encryption by chaos mixing," *IET Image Process.*, vol. 10, no. 10, pp. 742–750, Oct. 2016.

[35] X. Wang and Y. Li, "Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence," *Opt. Lasers Eng.*, vol. 137, Feb. 2021, Art. no. 106393.

[36] Q. Lai, G. Hu, U. Erkan, and A. Toktas, "A novel pixel-split image encryption scheme based on 2D Salomon map," *Expert Syst. Appl.*, vol. 213, p. 11845, Mar. 2023.

[37] Z. Liang, Q. Qin, C. Zhou, and S. Xu, "Color image encryption algorithm based on four-dimensional multi-stable hyper chaotic system and DNA strand displacement," *J. Electr. Eng. Technol.*, vol. 18, no. 1, pp. 539–559, Jan. 2023.

[38] I. S. T. Khalid, S. M. Eldin, D. Shah, M. Asif, and I. Saddique, "An integrated image encryption scheme based on elliptic curve," *IEEE Access*, vol. 11, pp. 5483–5501, 2023.

[39] V. S. Lima, F. A. B. S. Ferreira, F. Madeiro, and J. B. Lima, "Light field image encryption based on steerable cosine number transform," *Signal Process.*, vol. 202, Jan. 2023, Art. no. 108781.

[40] Q. Qin, Z. Liang, S. Liu, X. Wang, and C. Zhou, "A dual-domain image encryption algorithm based on hyperchaos and dynamic wavelet decomposition," *IEEE Access*, vol. 10, pp. 122726–122744, 2022.

[41] J. Oravec, L. Ovsenik, and J. Papaj, "An image encryption algorithm using logistic map with plaintext-related parameter values," *Entropy*, vol. 23, no. 11, p. 1373, Oct. 2021.

[42] Z. Liang, Q. Qin, C. Zhou, N. Wang, Y. Xu, and W. Zhou, "Medical image encryption algorithm based on a new five-dimensional three-leaf chaotic system and genetic operation," *PLoS ONE*, vol. 16, no. 11, Nov. 2021, Art. no. e0260014.

[43] N. Tsafack, J. Kengne, B. Abd-El-Atty, A. M. Iliyasu, K. Hirota, and A. A. A. El-Latif, "Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption," *Inf. Sci.*, vol. 515, pp. 191–217, Apr. 2020.

QIUXIA QIN was born in Jinan, Shandong, China, in 1996. She is currently pursuing the master's degree. Her research interests include image encryption and artificial intelligence.

ZHONGYUE LIANG was born in Binzhou, Shandong, China, in 1994. She is currently pursuing the master's degree. She has published many articles in the field of image encryption as the first author in *Neural Computing and Applications*, *PLOS One*, and other journals. Her main research interests include image encryption and DNA computing.

SHUANG LIU was born in 1977. She received the D.Eng. degree. She was an Associate Professor. She is currently the Deputy Dean of the School of Computer Science and Engineering, Dalian Minzu University. Her research interests include image encryption, machine learning, and video information processing.

CHANGJUN ZHOU was born in 1977. He received the Ph.D. degree. He is currently a Distinguished Professor of Huanglong Scholar with the School of Mathematics and Computer Science, Zhejiang Normal University. His research interests include image encryption, intelligent computing, pattern recognition in new computing models, biological computing theory and its application, and software system development.