Design of Chaotic Systems with Multiple Scrolls via Anti-Control Method and its Encryption Application

Shiya Wang, Jianbin He, *Member, IAENG*

***Abstract*—As the widespread application of multimedia communication technology, information transmission security has become increasingly important. The multi-scroll chaotic system exhibits complex dynamic behavior, and it is usually used to the design of encryption algorithm for image and video information by the sensitivity of initial values. The chaotic systems with multiple scrolls are investigated by a transformation method of nth order complex polynomial, and two examples of chaotic systems with four and six scrolls are given by the chaos anti-control theory, respectively. Based on the chaotic system with six scrolls, a simple encryption algorithm is designed for image information by scrambling and confusing operations. A hash sequence generated from the original information is given to obtain the initial keys, and three pseudo-random sequences are designed through the operations of multiplication and modulo. Furthermore, the security analysis is discussed by key space and correlation coefficient, etc. The presented encryption method exists a large key space, and it can resist to common attacks, such as differential attack, crop attack and noise attack. The practicality and effectiveness are verified by the encryption experiments of image information in the end.**

***Index Terms*—Multi-scroll chaotic system; Image encryption; Pseudo-random sequences; Security evaluation.**

I. Introduction

WITH the development of Internet and the popularity of smart phones, network communication is becoming increasingly popular, and it provides an important way to exchange information. Internet communication has become an important part of our daily life. However, there are some security risks associated with the sharing and storage of information in cyberspace, such as information leakage, theft, and tampering, which may lead to financial, economic, and privacy damages [1], [2]. The information security is an important scientific issue, and it is closely related to our life and society security. Chaos-based theories provide a special way for image encryption technology. The encryption algorithm of image information by integrating chaos theories with cryptography is significantly better than using cryptography alone. A deterministic chaotic system is very sensitive to the initials and parameters of system, and it can generate pseudo-random sequences [3], [4], so it is suitable for designing cryptographic encryption algorithms.

In 1989, Matthews first introduces chaos into cryptography [5]. In 1997, Friedrich proposes the scrambling-diffusion algorithm for image encryption, and the research of chaos-based encryption has been received widespread attention [6]. Since a typical chaotic encryption scheme is proposed in 1998 [7], much research work on chaos-based encryption has been widely studied by scholars around the world. Recently, some image encryptions are investigated for the information security. In reference [8], the synchronization of time-delayed systems is used to transmit the information of encrypted image. A method of secure communication is designed through the synchronization of chaotic systems by designing linear feedback controllers [9]. By the confusion and diffusion encryption, a symmetric algorithm is designed by Logistic map [10]. In reference [11], an encryption algorithm is introduced by 4-D Logistic map, and the pixel values of image is encrypted by DNA rules. Similarly, a new encryption is given by 2-D Hénon-sine map and DNA coding, the feasibility and practicality of the encryption algorithm are shown by the experimental results of image information [12]. In reference [13], a chaotic system with two scrolls is proposed based on four quadratic nonlinear terms. By the improved Logistic map, sine mapping and tent mapping, an encryption algorithm is proposed for image information via row scrambling and sawtooth transformation [14]. In reference [15], a new chaotic system is presented for a finance system with two nonlinearities. As some encryption based on dissipative chaotic system may be attacked by reconstruction, an image encryption is designed by the new dissipative chaos model, and it avoids the risks in encryption algorithms [16]. An improved encryption technique is proposed by multiple discrete dynamical chaotic systems [17]. Based on Logistic map and deep autoencoder, an encryption method is proposed for image information to effectively resists some attacks [18]. In reference [19], an encryption algorithm is presented for image by chaotic systems, and the key sequences are given by the plaintext image. By a sine-cosine chaotic map and DNA rules, the chaotic sequences are used to encrypt the index of row and column in plaintext image, and the coding and decoding are randomly selected based on pseudo-random sequences [20]. A pixel-split encryption algorithm is designed by 2-D Salomom map, the high and low bits are selectively exchanged for the image pixels, resulting in that the encrypted image is recovered by the corrected key [21]. A parallel algorithm is introduced to cipher the image in bit-level, and multiple threads are used to generate keystream for diffusion [22]. The encryption of confusion and diffusion is proposed by an improved one-dimensional chaotic map, and it has successfully passed multiple security

Manuscript received June 8, 2024; revised November 2, 2024. This work was supported by the Natural Science Foundation of Fujian Province (No.2022J01895), the Digital Fujian Meteorological Big Data Research Institute, the Key Laboratory of Data Science and Statistics, and the Fujian Key Laboratory of Granular Computing and Applications.

Shiya Wang is a postgraduate student in the School of Mathematics and Statistics, Minnan Normal University, Zhangzhou, 363000, China. (e-mail: shiyawang15@163.com)

Jianbin He is an Assistant Professor in the School of Mathematics and Statistics, Minnan Normal University, Zhangzhou, 363000, China. (e-mail: hejianbin@mnnu.edu.cn).

tests [23]. An encryption algorithm of bit-level permutation is proposed based on hyperchaotic system, and it can resist statistical analysis and differential attack [24]. Obviously, chaotic systems have been widely studied with many other disciplines, and the image encryption application of chaos has received much attention and extensive research. Various efficient and secure methods are proposed for the image encryption, such as the chaotic function of MS Tent map [25], and the security of information encryption is improved by designing new chaos-based encryption algorithms [26]–[28].

Therefore, the chaotic system with n-scroll chaotic attractors is studied through the variable transformation method of nth order polynomials for complex numbers. The chaotic system with multiple scrolls is applied to generate chaotic sequences, and new pseudo-random sequences are obtained through preprocessing techniques such as the operations of multiplication and modulo. Therefore, the image information is ciphered by scrambling and confusion encryption via the pseudo-random sequences. The main content is summarized as follows: (1) New chaotic systems with n-scroll are designed by the variable transformation method of nth order polynomials for complex numbers. (2) Based on the chaotic system with six scrolls, three sequences are generated by using a hash function and iterative processing. A chaos-based algorithm is designed for image by the block scrambling and pixel encryption. (3) The security of encryption algorithm is discussed by key sensitivity, crop attack, and noise attack, etc. The effectiveness and security are verified by numerical experiments.

The design and analysis of chaotic system with multiple scrolls are given in Section II. In Section III, an encryption algorithm for image is investigated via the chaotic system with six scrolls, and the effectiveness is verified by the results of the simulation experiments. The security of proposed method is discussed in Section IV. In Section V, a conclusion is given.

II. Design of New Chaotic Systems with Multiple Scrolls

By the anti-control theory of chaotic system [29], [30], a continuous and uniformly bounded controller $u = \varepsilon \sin(ky)$ is designed to control an asymptotically stable linear system, so that the obtained dynamical system can generate chaotic behavior, i.e.,

$$\begin{cases} \dot{x} = \sigma x - ly + az, \\ \dot{y} = rx - my - bz, \\ \dot{z} = -fx + ny - cz + \varepsilon \sin(ky), \end{cases} \tag{1}$$

where x, y, z are the variables, and $\sigma, l, a, r, m, b, f, n, c$ denote the parameters of new dynamical system, k and ε denote control parameters. If the values of these parameters are given as follows:

$$\begin{cases} \sigma = 4.195, l = 4.295, a = 1.295 \\ r = 3.1, m = 3.2, b = 6.1, f = 7.605 \\ n = 7.605, c = 1.905, k = 4.7, \varepsilon = 3.4. \end{cases} \tag{2}$$

then a chaotic system is generated with a positive Lyapunov exponent [30].

A. Design of New Chaotic System with Four Scrolls

According to the proposed method in reference [31], a new chaotic system with multiple scrolls is obtained by using variable transformation. If the complex number $w = s + t\mathrm{i}$, one has $w^2 = (s^2 - t^2) + 2st\mathrm{i}$, then the variable transformation is

$$\begin{cases} x = s^2 - t^2, \\ y = 2st, \\ z = z. \end{cases} \tag{3}$$

By the variable transformation in Eq. (3), the Jacobian matrix of variable transformation is $(\dot{x}, \dot{y}, \dot{z})^T = \boldsymbol{J} \cdot (\dot{s}, \dot{t}, \dot{z})^T$, and one has

$$\boldsymbol{J} = \begin{pmatrix} 2s & -2t & 0 \\ 2t & 2s & 0 \\ 0 & 0 & 1 \end{pmatrix}, \tag{4}$$

so, the inverse Jacobian matrix $\boldsymbol{J}$ can be obtained by

$$\boldsymbol{J}^{-1} = \begin{pmatrix} \dfrac{s}{2\left(s^2+t^2\right)} & \dfrac{t}{2\left(s^2+t^2\right)} & 0 \\ \dfrac{-t}{2\left(s^2+t^2\right)} & \dfrac{s}{2\left(s^2+t^2\right)} & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{5}$$

If the variable transformation (3) is substituted on the right side of system (1), then the new systems with variables (s, t, z) are represented as

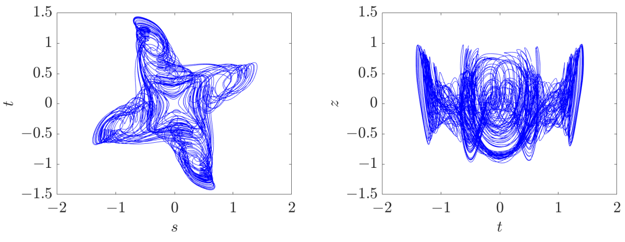
$$\begin{cases} \dot{x} = \sigma(s^2 - t^2) - 2lst + az, \\ \dot{y} = r(s^2 - t^2) - 2mst - bz, \\ \dot{z} = -f(s^2 - t^2) + 2nst - cz + \varepsilon \sin(2kst). \end{cases} \tag{6}$$

Based on the variable transformation equation $(\dot{s}, \dot{t}, \dot{z})^T = \boldsymbol{J}^{-1} \cdot (\dot{x}, \dot{y}, \dot{z})^T$, the new multi-scroll chaotic system is

$$\begin{cases} \dot{s} = \dfrac{\sigma M_0 - 2ls^2t + rN_0 - 2mst^2 + z(as - bt)}{2(s^2 + t^2)}, \\ \dot{t} = \dfrac{-\sigma N_0 + 2lst^2 + rM_0 - 2ms^2t - z(as + bt)}{2(s^2 + t^2)}, \\ \dot{z} = -f(s^2 - t^2) + 2nst - cz + \varepsilon \sin(2kst), \end{cases} \tag{7}$$

where $M_0 = s^3 - st^2$ and $N_0 = s^2t - t^3$.

Therefore, a new chaotic system with four scrolls in Eq. (7) is obtained by the initials $(s_0, t_0, z_0) = (0.1, 0.21, 0.15)$ and parameters in Eq. (2), and the attractors of system (7) are given in Fig. 1.



(a)

(b)

Fig. 1. The multi-scroll chaotic attractor in Eq. (7). (a) Attractor of s vs. t. (b) Attractor of t vs. z.

B. Design of New Chaotic System with Six Scrolls

Similarly, if the complex number $w = u + v\mathrm{i}$, and one has $w^3 = (u^3 - 3uv^2) + (3u^2v - v^3)\mathrm{i}$, then the variable transformation is given by

$$\begin{cases} x = u^3 - 3uv^2, \\ y = 3u^2v - v^3, \\ z = z. \end{cases} \tag{8}$$

According to variable transformation in Eq. (8), the Jacobian matrix of variable transformation is $(\dot{x}, \dot{y}, \dot{z})^T = \boldsymbol{J} \cdot (\dot{s}, \dot{t}, \dot{z})^T$, and one has

$$\boldsymbol{J} = \begin{pmatrix} 3u^2 - 3v^2 & -6uv & 0 \\ 6uv & 3u^2 - 3v^2 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \tag{9}$$

so, the inverse Jacobian matrix $\boldsymbol{J}$ can be obtained by

$$\boldsymbol{J}^{-1} = \begin{pmatrix} \dfrac{u^2 - v^2}{3\left(u^2 + v^2\right)^2} & \dfrac{2uv}{3\left(u^2 + v^2\right)^2} & 0 \\ \dfrac{-2uv}{3\left(u^2 + v^2\right)^2} & \dfrac{u^2 - v^2}{3\left(u^2 + v^2\right)^2} & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{10}$$

The system (1) with new variables (u, v, z) can be given by

$$\begin{cases} \dot{x} = \sigma(u^3 - 3uv^2) - l(3u^2v - v^3) + az, \\ \dot{y} = r(u^3 - 3uv^2) - m(3u^2v - v^3) - bz, \\ \dot{z} = -f(u^3 - 3uv^2) + n(3u^2v - v^3) - cz \\ \qquad + \varepsilon \sin[k(3u^2v - v^3)]. \end{cases} \tag{11}$$

Therefore, the new chaotic system with six-scroll is

$$\begin{cases} \dot{u} = \dfrac{\sigma M_1 - lN_1 + r\left(2u^4v - 6u^2v^3\right) - mM_2}{3\left(u^2 + v^2\right)^2} \\ \qquad + \dfrac{z\left(au^2 - av^2 - 2buv\right)}{3\left(u^2 + v^2\right)^2}, \\ \dot{v} = \dfrac{\sigma\left(6u^2v^3 - 2u^4v\right) + lM_2 + rM_1 - mN_1}{3\left(u^2 + v^2\right)^2} \\ \qquad - \dfrac{z\left(2auv + bu^2 - bv^2\right)}{3\left(u^2 + v^2\right)^2}, \\ \dot{z} = -f\left(u^3 - 3uv^2\right) + n\left(3u^2v - v^3\right) - cz \\ \qquad + \varepsilon \sin\left[k\left(3u^2v - v^3\right)\right], \end{cases} \tag{12}$$

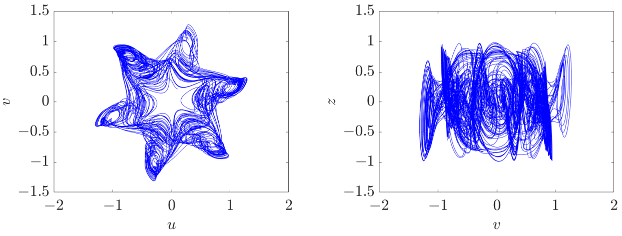
where $M_1 = u^5 - 4u^3v^2 + 3uv^4$, $M_2 = 6u^3v^2 - 2uv^4$ and $N_1 = 3u^4v - 4u^2v^3 + v^5$.

If the initials are $(u_0, v_0, z_0) = (0.1, 0.21, 0.15)$ and the parameters are given in Eq. (2), then a six-scroll chaotic system in Eq. (12) is obtained, and the chaotic attractor with six scrolls is given in Fig. 2.

III. Design of Chaotic Encryption Algorithm

A. Design of Keystream

An encryption algorithm is proposed for image information by the chaotic system with six scrolls in Eq. (12). Firstly, the fourth-order Runge-Kutta algorithm is applied to the discretization of three-dimensional system (12), and it is given by



(a) (b)

Fig. 2. The multi-scroll chaotic attractor in Eq. (12). (a) Attractor of u vs. v. (b) Attractor of v vs. z.

$$\begin{cases} K_1 = f(t(i), X(i)), \\ K_2 = f(t(i) + h/2, X(i) + K_1h/2), \\ K_3 = f(t(i) + h/2, X(i) + K_2h/2), \\ K_4 = f(t(i) + h, X(i) + hK_3), \\ X(i+1) = X(i) + h(K_1 + 2K_2 + 2K_3 + K_4)/6, \end{cases} \tag{13}$$

where $i = 1, 2, \cdots, n, \cdots$. Based on Matlab R2020a and Eq. (13), if the initial values $(u_0, v_0, z_0) = (0.1, 0.21, 0.15)$, the step $h = 0.001$ and the time $T = 2000$, then three chaotic sequences are given by

$$\boldsymbol{X} = (\boldsymbol{X}_1, \boldsymbol{X}_2, \boldsymbol{X}_3). \tag{14}$$

Therefore, the sequences $\{\boldsymbol{X}_1, \boldsymbol{X}_2, \boldsymbol{X}_3\}$ are used to scramble and diffuse plaintext information, and the new sequences are given by following five steps.

Step 1: A plain image $\boldsymbol{P}$ of size $M \times N$ is chosen, and a sequence $\boldsymbol{W}$ with 256 bits of image $\boldsymbol{P}$ is generated by the hash function of SHA-256.

Step 2: The sequence $\boldsymbol{W}$ is divided into three parts, and they are converted to decimal values $\{\boldsymbol{W_1}, \boldsymbol{W_2}, \boldsymbol{W_3}\}$. Then new sequences $\{\boldsymbol{V_1}, \boldsymbol{V_2}, \boldsymbol{V_3}\}$ are obtained by removing the first three and the last three values of $\{\boldsymbol{W_1}, \boldsymbol{W_2}, \boldsymbol{W_3}\}$.

Step 3: Three secret keys $\{R_1, R_2, R_3\}$ are obtained by summing and modulus M of sequences $\{\boldsymbol{V_1}, \boldsymbol{V_2}, \boldsymbol{V_3}\}$, and they are given by

$$R_i = (\sum_{j=1}^{n_i} \boldsymbol{V}_i(j)) \bmod 256, \tag{15}$$

where n_i is the length of $\boldsymbol{V_i}$ $(i = 1, 2, 3)$.

Step 4: New sequences $\{\boldsymbol{Z}_1, \boldsymbol{Z}_2, \boldsymbol{Z}_3\}$ are obtained by $\{R_1, R_2, R_3\}$, and they are given as follows:

$$\begin{cases} \boldsymbol{Z_1} = \mathrm{fix}\left(\mathrm{mod}(\boldsymbol{X_1} \times 100 \times R_1, 1) \times 10^5\right), \\ \boldsymbol{Z_2} = \mathrm{fix}\left(\mathrm{mod}(\boldsymbol{X_2} \times 100 \times R_2, 1) \times 10^5\right), \\ \boldsymbol{Z_3} = \mathrm{fix}\left(\mathrm{mod}(\boldsymbol{X_3} \times 100 \times R_3, 1) \times 10^5\right). \end{cases} \tag{16}$$

Therefore, the pseudo-random sequences $\{\boldsymbol{Z}_1, \boldsymbol{Z}_2, \boldsymbol{Z}_3\}$ can pass NIST test, and they are used to the encryption algorithm.

Step 5: In order to apply the pseudo-random sequences $\{\boldsymbol{Z}_1, \boldsymbol{Z}_2, \boldsymbol{Z}_3\}$ to image encryption, new sequences $\{\boldsymbol{Z}'_1, \boldsymbol{Z}'_2, \boldsymbol{Z}'_3\}$ are obtained by a modulo operation, i.e.,

$$\begin{cases} \boldsymbol{Z'_1} = \boldsymbol{Z_1} \bmod 64, \\ \boldsymbol{Z'_2} = \boldsymbol{Z_2} \bmod 64, \\ \boldsymbol{Z'_3} = \boldsymbol{Z_3} \bmod 256. \end{cases} \tag{17}$$

B. Design of Encryption Algorithm

Based on the chaotic system with multiple scrolls, the flowchart of image encryption application is shown in Fig. 3. The plain image $\boldsymbol{P}$ is firstly scrambled in blocks, and it is encrypted by sequences in Eq. (17). The proposed method of image encryption is sensitive to plaintext by using the hash function of SHA-256.

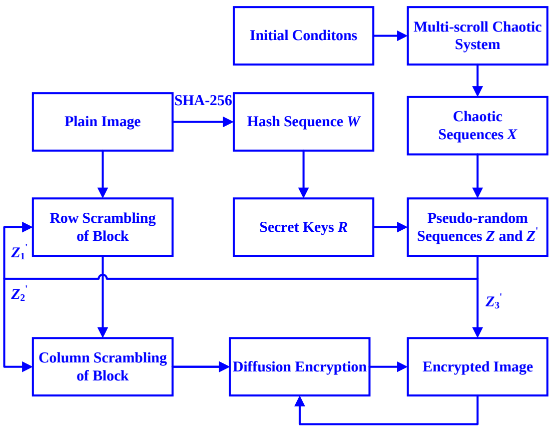


Fig. 3. Flowchart of image encryption by the chaotic system with six scrolls in Eq. (12).

According to the encryption algorithm, the scrambling and diffusion encryptions are designed by the sequences $\boldsymbol{Z}_i'$ $(i = 1, 2, 3)$, and it is given as follows:

(1) Row Scrambling of Blocks

Step 1: The plaintext is divided into image blocks of size 8×8, and the number of blocks is $M/8 \times N/8$.

Step 2: The sequence $\boldsymbol{Z}_1'$ is used for row scrambling of blocks. The ith and $\boldsymbol{Z}_1'(i)$th blocks are exchanged if $\boldsymbol{Z}_1'(i) > 32$ $(i = 1, 2, \cdots, M/8)$.

On the contrary, the ith and $\boldsymbol{Z}_1'(i)$th blocks are exchanged if $\boldsymbol{Z}_1'(i) \leqslant 32$ $(i = M/8, (M-1)/8, \cdots, 1)$. According to the row scrambling of blocks, then the encrypted image $\boldsymbol{P}_1$ is obtained by

$$\begin{cases} \boldsymbol{P}_1(i) = \boldsymbol{P}(\boldsymbol{Z}_1'(i)), (i = 1, 2, \cdots, M/8), & \boldsymbol{Z}_1'(i) > 32, \\ \boldsymbol{P}_1(i) = \boldsymbol{P}(\boldsymbol{Z}_1'(i)), (i = M/8, \cdots, 2, 1), & \boldsymbol{Z}_1'(i) \leqslant 32. \end{cases}$$

(2) Column Scrambling of Blocks

Similarly, the pseudo-random sequence $\boldsymbol{Z}_2'$ is used for column scrambling of blocks. The ith and $\boldsymbol{Z}_2'(i)$th blocks of scrambled image are exchanged from 1 to $N/8$ if $\boldsymbol{Z}_2'(i) \geqslant 32$. Otherwise, the ith and $\boldsymbol{Z}_2'(i)$th blocks of scrambled image are exchanged from $N/8$ to 1 if $\boldsymbol{Z}_2'(i) < 32$, and the column scrambled image $\boldsymbol{P}_2$ is

$$\begin{cases} \boldsymbol{P}_2(i) = \boldsymbol{P}_1(\boldsymbol{Z}_2'(i)), (i = 1, 2, \cdots, N/8), & \boldsymbol{Z}_2'(i) > 32, \\ \boldsymbol{P}_2(i) = \boldsymbol{P}_1(\boldsymbol{Z}_2'(i)), (i = N/8, \cdots, 1), & \boldsymbol{Z}_2'(i) \leqslant 32. \end{cases}$$

(3) Diffusion Encryption

Step 1: The sequence $\boldsymbol{Z}_3'$ is applied to the diffusion encryption of image $\boldsymbol{P}_2$, and the first pixel in $\boldsymbol{P}_2$ is ciphered by sequence $\boldsymbol{Z}_3'$, i.e., $\boldsymbol{P}_3(1) = \boldsymbol{P}_2(1) \oplus \boldsymbol{Z}_3'(1)$.

Step 2: The rest of $\boldsymbol{P}_2$ is encrypted by the previous pixel of $\boldsymbol{P}_2$ and the sequence $\boldsymbol{Z}_3'$, then the encrypted image $\boldsymbol{P}_3$ is

$$\boldsymbol{P}_3(i) = \boldsymbol{P}_2(i) \oplus \boldsymbol{P}_2(i-1) \oplus \boldsymbol{Z}_3'(i), (i = 2, 3, \cdots, M \times N).$$

C. Decryption Algorithm

The decryption algorithm is designed by the reverse operation of encryption algorithm, and it is given as follows:

Step 1: The first pixel of encrypted image $\boldsymbol{P}_3$ is decrypted by the sequence $\boldsymbol{Z}_3'$, i.e., $\boldsymbol{P}_2(1) = \boldsymbol{P}_3(1) \oplus \boldsymbol{Z}_3'(1)$.

Step 2: The rest of image $\boldsymbol{P}_3$ is decrypted by the sequence $\boldsymbol{Z}_3'$ and $\boldsymbol{P}_2$, then the decrypted image $\boldsymbol{P}_2$ is obtained by

$$\boldsymbol{P}_2(i) = \boldsymbol{P}_3(i) \oplus \boldsymbol{Z}_3'(i) \oplus \boldsymbol{P}_2(i-1), (i = M \times N, \cdots, 3, 2).$$

Step 3: The scrambled image $\boldsymbol{P}_2$ is divided into $M/8 \times N/8$ blocks of size 8×8. The ith and $\boldsymbol{Z}_2'(i)$th blocks of matrix $\boldsymbol{P}_2$ are exchanged from $N/8$ to 1 if $\boldsymbol{Z}_2'(i) \leqslant 32$. On the contrary, the ith and $\boldsymbol{Z}_2'(i)$th blocks of matrix $\boldsymbol{P}_2$ are exchanged from 1 to $N/8$ if $\boldsymbol{Z}_2'(i) > 32$. Then the scrambled image $\boldsymbol{P}_1$ is decrypted by

$$\begin{cases} \boldsymbol{P}_1(i) = \boldsymbol{P}_2(\boldsymbol{Z}_2'(i)), (i = N/8, \cdots, 2, 1), & \boldsymbol{Z}_2'(i) \leqslant 32, \\ \boldsymbol{P}_1(i) = \boldsymbol{P}_2(\boldsymbol{Z}_2'(i)), (i = 1, 2, \cdots N/8), & \boldsymbol{Z}_2'(i) > 32. \end{cases}$$

Step 4: The ith and $\boldsymbol{Z}_1'(i)$th blocks of scrambled image $\boldsymbol{P}_1$ are exchanged from $M/8$ to 1 if $\boldsymbol{Z}_1'(i) < 32$. Otherwise, the ith and $\boldsymbol{Z}_1'(i)$th blocks of scrambled image $\boldsymbol{P}_1$ are exchanged from 1 to $M/8$ if $\boldsymbol{Z}_1'(i) > 32$. Therefore, the original image $\boldsymbol{P}$ is recovered by

$$\begin{cases} \boldsymbol{P}(i) = \boldsymbol{P}_1(\boldsymbol{Z}_1'(i)), (i = M/8, \cdots, 2, 1), & \boldsymbol{Z}_1'(i) \leqslant 32, \\ \boldsymbol{P}(i) = \boldsymbol{P}_1(\boldsymbol{Z}_1'(i)), (i = 1, 2, \cdots M/8), & \boldsymbol{Z}_1'(i) > 32. \end{cases}$$

D. Results of Experimental Simulation

According to the proposed algorithm of image encryption, the effectiveness is verified by Matlab R2020a. The Goldhill image is given as an example of encryption, which the size of image is 512×512, the initial values of system (12) are $(0.1, 0.21, 0.15)$. The results of the simulation experiment are shown in Fig. 4.

In Figs. 4(b) and 4(c), the information of original image $\boldsymbol{P}$ has already been encrypted by blocks scrambling. One cannot directly obtain the original information from the encrypted image $\boldsymbol{P}_3$ in Fig. 4(d), and the original image $\boldsymbol{P}$ has achieved good encryption results. In Fig. 4(e), the original image $\boldsymbol{P}$ is obtained by the proposed decryption algorithm with corrected keys. In Fig. 4(f), the error between the original image and recovered image is 0, so the decryption algorithm can correctly recover original information.

Remark 1: In the proposed encryption algorithm, different images will generate different keys $\{R_1, R_2, R_3\}$ due to the uniqueness of the hash sequence of image information. The original image cannot be successfully recovered if one of the keys is wrong. The keys include the hash sequence of plaintext, initial values, and parameters in system (12).

IV. Security Analysis

A. Key Space and Key Sensitivity

An algorithm of image encryption must have a large enough key space, and it is said to be good key sensitivity if the ciphered image cannot be recovered successfully by a key with minor error. Therefore, Goldhill image is given as an example to decrypt the corresponding ciphertext, when one key is changed while the others keep unchanged. Experimental results show the original image is only obtained

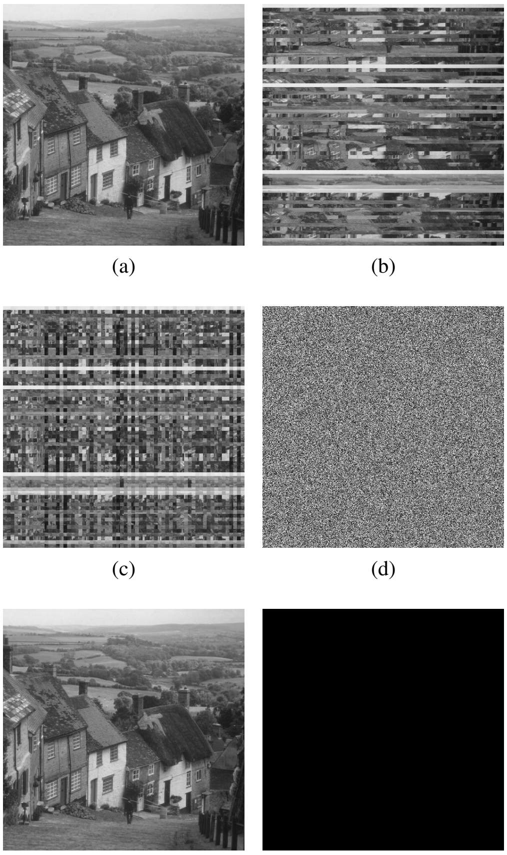


Fig. 4. The results of image encryption and decryption. (a) Original image $\boldsymbol{P}$; (b) Block scrambled image $\boldsymbol{P}_1$; (c) Block scrambled image $\boldsymbol{P}_2$; (d) Encrypted image $\boldsymbol{P}_3$; (e) Decrypted image with corrected keys; (f) The error between original image (a) and recovered image (e).

by the correct keys. By the decryption results with different keys in Table I, and the key space (Abbreviated to "KS") is calculated by

$$\mathrm{KS} = (10^{17})^3 \times (10^{16})^6 \times (10^{15})^4 \times 10^{14} = 10^{221} > 2^{734}.$$

Furthermore, the KS of different algorithms are given in Table II, and it is greater than the minimum requirement 2^{100} [32].

B. Histogram and χ^2 Tests

An algorithm of image encryption usually needs to analyze the distributions of grayscale values. It may be difficult for attacker to get pixel value through statistical analysis if the histogram of ciphered image is uniform. In Fig. 5, the histograms of Goldhill image and scrambled image are the same and uneven, but it is uniform for the ciphered image $\boldsymbol{P}_3$. So, it is very difficult to directly get information from the encrypted image by the statistical analysis.

The Chi-square test is given to calculate the fitting degree between the actual values and the theoretical values of two or more samples [36]. For a gray image of size $M \times N$, and the Chi-square test is given by

$$\chi^2 = \sum_{i=0}^{255} \frac{(f_i - g_i)}{g_i}, \ (i = 0, 1, 2, \cdots, 255),$$

where f_i is the frequency of each pixel $(0, 1, \cdots, 255)$, $g_i = (MN)/256$ is the expected frequency.

TABLE I
KEY SENSITIVITY OF ENCRYPTION ALGORITHM

Key errors	Recovered the original image
$\lvert u_0 - u_0' \rvert \geqslant 10^{-16}$	No
$\lvert v_0 - v_0' \rvert \geqslant 10^{-15}$	No
$\lvert z_0 - z_0' \rvert \geqslant 10^{-16}$	No
$\lvert \sigma - \sigma' \rvert \geqslant 10^{-16}$	No
$\lvert l - l' \rvert \geqslant 10^{-17}$	No
$\lvert a - a' \rvert \geqslant 10^{-15}$	No
$\lvert r - r' \rvert \geqslant 10^{-17}$	No
$\lvert m - m' \rvert \geqslant 10^{-15}$	No
$\lvert b - b' \rvert \geqslant 10^{-16}$	No
$\lvert f - f' \rvert \geqslant 10^{-15}$	No
$\lvert n - n' \rvert \geqslant 10^{-17}$	No
$\lvert c - c' \rvert \geqslant 10^{-16}$	No
$\lvert k - k' \rvert \geqslant 10^{-14}$	No
$\lvert \varepsilon - \varepsilon' \rvert \geqslant 10^{-16}$	No

TABLE II
THE KEY SPACE OF DIFFERENT ALGORITHMS

Algorithms	Key space
The proposed algorithm	2^{734}
Ref. [33]	2^{366}
Ref. [34]	2^{436}
Ref. [35]	2^{212}

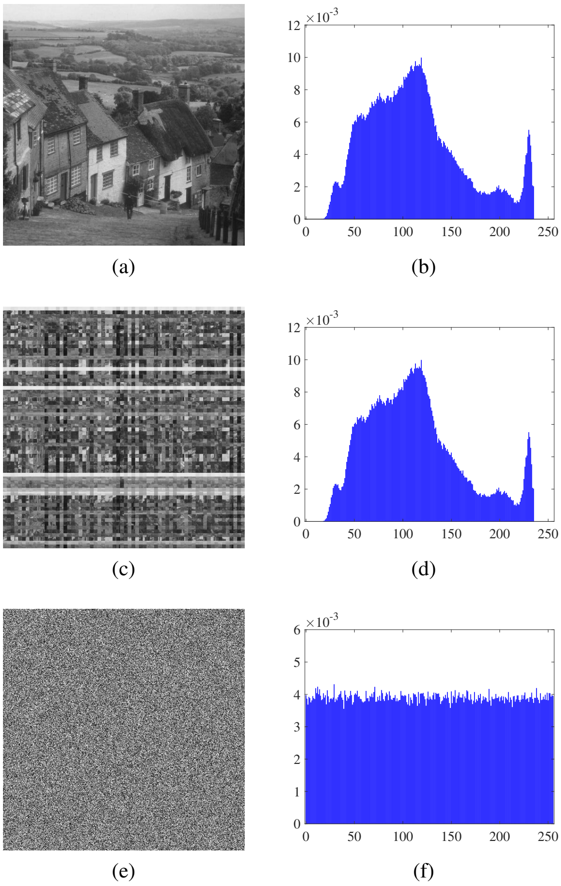


Fig. 5. Histogram analysis of images. (a) Goldhill image $\boldsymbol{P}$; (b) Histogram of $\boldsymbol{P}$; (c) Scrambled image $\boldsymbol{P}_2$; (d) Histogram of $\boldsymbol{P}_2$; (e) Encrypted image $\boldsymbol{P}_3$; (f) Histogram of $\boldsymbol{P}_3$.

The Chi-square $\chi^2_{0.05}(255) = 293.25$ if the freedom degree is 255 and the significance level is 0.05. In Table III, the results of Chi-square test of original images are greater than 293.25, while the results of the corresponding encrypted images are less than 293.25. Therefore, all the histograms of the encrypted images are uniformly distributed and have good confidentiality by the proposed encryption algorithm.

TABLE III
THE CHI-SQUARE TEST $\chi^2_{0.05}(255)$ OF DIFFERENT IMAGES

Images	Goldhill	Baboon	Peppers
Plaintext	1.6162×10^5	1.8760×10^5	1.3884×10^5
Ciphertext	265.8359	235.7070	272.2539

C. Information Entropy

For a gray image, the information entropy is given to show the random distribution of pixel values, and it is given by [37]

$$H = -\sum_{i=0}^{255} p_i \log_2(p_i), \tag{18}$$

where p_i is the probability of pixel i. In theory, the expected information entropy for an image with a grayscale level of 256 is equal to 8.

In Table IV, the results of information entropy for different plaintext and ciphertext are shown according to the formula in Eq. (18). Obviously, the information entropy of ciphertext is close to 8, so the ciphered image has effectively hidden the statistical information of the plaintext.

TABLE IV
THE RESULTS OF INFORMATION ENTROPY

Images	Plaintext	Ciphertext
Goldhill	7.4778	7.9913
Baboon	7.3579	7.9916
Peppers	7.5925	7.9914
Ref. [38]	7.4456	7.9768
Ref. [39]	7.5925	7.9757

D. Correlation Coefficient Analysis

Usually, the pixel value of an image is very similar to the adjacent pixel. If n pairs of adjacent pixel values (k_i, l_i) of an image are randomly given, then the correlation coefficient of vectors $\boldsymbol{k} = \{k_i\}$ and $\boldsymbol{l} = \{l_i\}$ $(i = 1, 2, \cdots, M \times N)$ is [40]

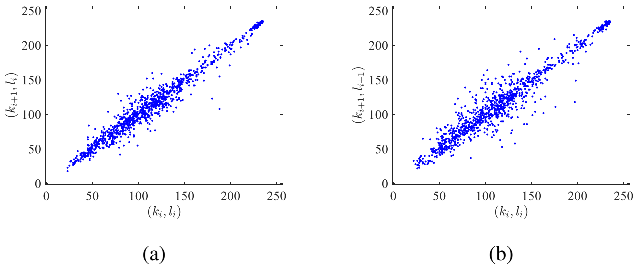
$$\begin{cases} r_{kl} = \dfrac{\operatorname{cov}(\boldsymbol{k}, \boldsymbol{l})}{\sqrt{D(\boldsymbol{k})}\sqrt{D(\boldsymbol{l})}}, \\ \operatorname{cov}(\boldsymbol{k}, \boldsymbol{l}) = \dfrac{1}{n}\displaystyle\sum_{i=1}^{n} (k_i - E(\boldsymbol{k}))(l_i - E(\boldsymbol{l})), \\ D(\boldsymbol{k}) = \dfrac{1}{n}\displaystyle\sum_{i=1}^{n} (k_i - E(\boldsymbol{k}))^2, E(\boldsymbol{k}) = \dfrac{1}{n}\displaystyle\sum_{i=1}^{n} k_i. \end{cases}$$

In Table V, the correlation coefficients are shown for the adjacent pixels in three directions when $n = 10000$, and they are close to zero when the original images are encrypted by the proposed encryption algorithm, i.e., the correlation of adjacent pixels has been significantly reduced.

In Fig. 6, the correlation diagrams of plaintext are given when $n = 1000$, and adjacent pixels have high correlation. In Fig. 7, the distribution of ciphered image is uniform, and one cannot get the pixel values from the low correlation of adjacent pixels.

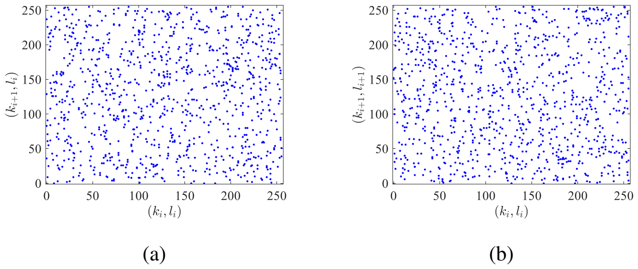
TABLE V
CORRELATION COEFFICIENTS OF IMAGES IN DIFFERENT DIRECTIONS

Images	Horizontal	Vertical	Diagonal	Average
Goldhill	0.9747	0.9733	0.9666	0.9547
Encrypted Goldhill	−0.0058	0.0167	0.0059	0.0056
Baboon	0.7549	0.8620	0.7259	0.7809
Encrypted Baboon	0.0079	−0.0002	−0.0131	0.0071
Pappers	0.9826	0.9765	0.9674	0.9755
Encrypted Pappers	0.0094	−0.0086	0.0044	0.0074
Ref. [41]	0.0241	−0.0222	0.0169	0.0211
Ref. [42]	0.0069	−0.0028	−0.0047	0.0048
Ref. [43]	0.0272	−0.0114	−0.0484	0.0290
Ref. [44]	0.0214	0.0465	−0.0090	0.0256



(a) (b)

Fig. 6. Correlation analysis of Goldhill image. (a) Pixel values (k_i, l_i) vs. (k_{i+1}, l_i) in horizontal direction; (b) Pixel values (k_i, l_i) vs. (k_{i+1}, l_{i+1}) in diagonal direction.



(a) (b)

Fig. 7. Correlation analysis of encrypted Goldhill image. (a) Pixel values (k_i, l_i) vs. (k_{i+1}, l_i) in horizontal direction; (b) Pixel values (k_i, l_i) vs. (k_{i+1}, l_{i+1}) in diagonal direction.

E. Crop Attack

Usually, the encrypted image may be damaged or destroyed when an attacker is unable to decipher it, so the ability to resist crop attack is important. In Fig. 8, the cropping image is deciphered with correct keys when one-sixteenth and one-quarter of the ciphered image is cut, respectively.

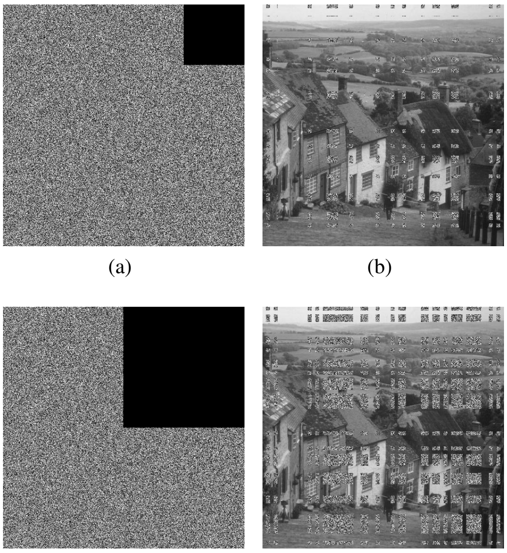


Fig. 8. Test results of crop attack. (a) encrypted image with cropping 1/16; (b) Deciphered image of cropping image (a); (c) Encrypted image with cropping 1/4; (d) Decrypted image of cropping image (c).

Obviously, the overall image is roughly deciphered from the cropping image.

In order to know more about the degree of image restoration after cropping attack, the proportion of different pixels, mean absolute error (Abbreviated to "MAE"), and mean relative error (Abbreviated to "MRE") between the recovered and original images are calculated by different cropping positions. In Table VI, the results of MAE and MRE are small when the encrypted image is damaged in different positions, and most areas of the cropping image can be decrypted successfully.

TABLE VI
COMPARISON RESULTS OF DIFFERENT SIZES OF CROP ATTACK

Size of crop attack	Position of crop attack	Proportion of different pixels	MAE	MRE
1/16	Upper-right	6.32%	4.74	1.86%
	Middle	6.38%	4.67	1.83%
	Lower-left	6.33%	4.66	1.83%
1/4	Upper-right	25.10%	18.81	7.38%
	Middle	25.20%	18.88	7.40%
	Lower-left	25.10%	18.65	7.31%

F. Noise Attack Analysis

An efficient algorithm of image encryption must resist to noise attacks, so the security of proposed algorithm is discussed by the salt & pepper noise (Abbreviated to "SPN"), gaussian noise (Abbreviated to "GN"), and speckle noise (Abbreviated to "SN"). The results of decrypted images are shown in Figs. 9-11 when the ciphered image $\boldsymbol{P}_3$ is disturbed by the three types of noise, respectively.

Obviously, the encrypted image can be successfully decrypted with noise at different levels. The overall image information can be recognized, even though there are some noise points in the decrypted image. The decrypted results of ciphered images with SPN are better than the ciphered image with GN and SN.

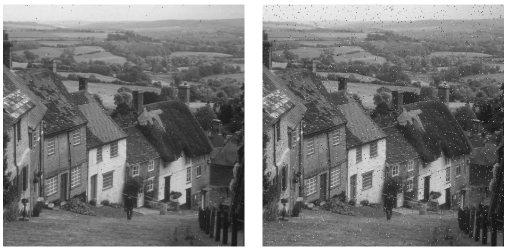


Fig. 9. The decrypted image when encrypted image is disturbed by SPN attack. (a) The density of SPN is 10^{-3}. (b) The density of SPN is 10^{-2}.

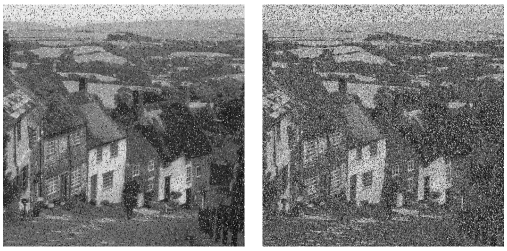


Fig. 10. The decrypted image when encrypted image is disturbed by GN attack. (a) The variance of GN is 10^{-3}. (b) The variance of GN is 10^{-2}.

In Table VII, the comparisons of the deciphered and the original images are discussed by the proportion of different pixels, MAE, and MRE. Most pixel values between the deciphered and original images are different, but MAE and MRE are relatively small. Also, the MAE and MRE of SPN are smaller than the GN and SN. Therefore, the proposed algorithm can resist to SPN, GN, and SN attacks to some extent.

TABLE VII
COMPARISON RESULTS OF DIFFERENT NOISE ATTACK

Noise variance	Types of noise	Proportion of different pixels	MAE	MRE
10^{-2}	SPN	90.92%	5.47	2.15%
	GN	99.06%	42.43	16.64%
	SN	98.54%	31.49	12.35%
10^{-3}	SPN	88.66%	3.35	1.31%
	GN	97.98%	23.55	9.23%
	SN	97.12%	16.80	6.59%

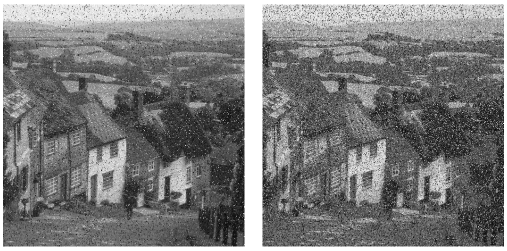


Fig. 11. The decrypted image when encrypted image is disturbed by SN attack. (a) The variance of SN is 10^{-3}. (b) The variance of SN is 10^{-2}.

G. Differential Attack

In order to compare the differences between two ciphertext images, the same encryption algorithm and keys are used to encrypt two plaintext images with a small error of pixel values, respectively. Based on differential attack, the differences of two ciphertext images are usually shown by the number of pixels change rate (Abbreviated to "NPCR") and the unified average changing intensity (Abbreviated to "UACI"). The calculation formulas are given by [45]

$$\begin{cases} \text{NPCR} = \dfrac{\sum_{i=1}^{M}\sum_{j=1}^{N} D_{i,j}}{M \times N} \times 100\%, \\ D_{(i,j)} = \begin{cases} 1, E(i,j) \neq E'(i,j), \\ 0, E(i,j) = E'(i,j), \end{cases} \\ \text{UACI} = \dfrac{\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{E(i,j)-E'(i,j)}{255}}{M \times N} \times 100\%, \end{cases}$$

where E and E' are ciphered images generated from two original images with a small error.

The pixel of position $(2, 43)$ in Goldhill image is changed from 166 to 167, then these two original images are used to obtain new encrypted images E and E' by the proposed encryption algorithm. Similarly, the pixel of position $(2, 43)$ in Baboon image is changed from 80 to 81, and the pixel of position $(2, 43)$ in Peppers image is changed from 76 to 77, then NPCR and UACI are shown in Table VIII, respectively. Obviously, they are close to the corresponding expected values 99.6094 and 33.4635. Therefore, the proposed algorithm can resist differential attack and improve the security of encrypted information.

TABLE VIII
Test results of NPCR and UACI (%)

Images	NPCR	UACI
Goldhill	99.6040	33.5376
Baboon	99.6128	33.4632
Pappers	99.6243	33.4950
Ref. [46]	99.8700	33.2900
Ref. [47]	99.2400	33.3873
Ref. [48]	99.5400	28.2700
Ref. [44]	99.5800	33.4400

H. NIST Test

The National Institute of Standards and Technology (Abbreviated to "NIST") provides 15 tests to show whether a sequence is random [49]. The sequence is said to be random if the results of NIST test are greater than 0.01.

In Table IX, the results of NIST test are given for sequences $\{\boldsymbol{Z_1}, \boldsymbol{Z_2}, \boldsymbol{Z_3}\}$ in Eq. (16), so the sequences $\{\boldsymbol{Z_1}, \boldsymbol{Z_2}, \boldsymbol{Z_3}\}$ pass NIST test.

TABLE IX
The results of NIST test for sequences $\boldsymbol{Z_i}$ $(i = 1, 2, 3)$

Test items	$\boldsymbol{Z_1}$	$\boldsymbol{Z_2}$	$\boldsymbol{Z_3}$
Frequency	0.6163	0.8677	0.0519
Frequency within a block	0.9978	0.1538	0.8343
Runs	0.1223	0.8165	0.6787
Longest-run of-ones	0.1453	0.9241	0.5479
Binary matrix rank	0.4944	0.8832	0.1025
Discrete fourier transform	0.2023	0.6163	0.3669
Non-overlapping template matching	0.4906	0.5078	0.5167
Overlapping template matching	0.3838	0.7598	0.7981
Maurer's universal statistical	0.8978	0.8514	0.0428
Linear complexity	0.9114	0.4559	0.4373
Serial	0.6571	0.2899	0.1848
Approximate entropy	0.2757	0.4190	0.0179
Cumulative sums	0.3970	0.6167	0.7495
Random excursions	0.4604	0.1750	0.4790
Random excursions variant	0.3283	0.3723	0.4686

V. Conclusion

A class of chaotic systems with multiple scrolls is investigated through the transformation of nth order polynomials for complex numbers, and two examples of chaotic systems with four-scroll and six-scroll chaotic attractors are proposed. Similarly, many new chaotic systems with multiple scrolls can be designed according to the proposed method, and it provides a new approach to design chaotic systems with multiple scrolls. The sequences of chaotic system with six scrolls are applied to design encryption algorithm, and they can pass NIST test. A simple encryption algorithm of image information is investigated by the blocks scrambling and pixels diffusion encryption. The effectiveness and feasibility are verified by the experimental results of image encryption. According to the secure analyses, the proposed algorithm can resist some common attacks, such as crop attack and noise attack. The chaos-based encryption algorithm is suitable for multimedia information, and it will be applied to the information encryption of image or video in the future.

References

[1] H. Gao and T. Gao, "Double verifiable image encryption based on chaos and reversible watermarking algorithm," *Multimedia Tools and Applications*, vol. 78, no. 6, pp. 7267–7288, 2019.

[2] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Information Sciences*, vol. 480, pp. 403–419, 2019.

[3] X. Sun, Q. Tu, J. Chen, C. Zhang, and X. Duan, "Probabilistic load flow calculation based on sparse polynomial chaos expansion," *IET Generation, Transmission & Distribution*, vol. 12, no. 11, pp. 2735–2744, 2018.

[4] T. Huang, C. Li, W. Yu, and G. Chen, "Synchronization of delayed chaotic systems with parameter mismatches by using intermittent linear state feedback," *Nonlinearity*, vol. 22, no. 3, p. 569, 2009.

[5] R. Matthews, "On the derivation of a "chaotic" encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[6] J. Fridrich, "Image encryption based on chaotic maps," in *1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation*, vol. 2. IEEE, 1997, pp. 1105–1110.

[7] M. Baptista, "Cryptography with chaos," *Physics letters A*, vol. 240, no. 1-2, pp. 50–54, 1998.

[8] S. Banerjee, D. Ghosh, A. Ray, and A. R. Chowdhury, "Synchronization between two different time-delayed systems and image encryption," *Europhysics Letters*, vol. 81, no. 2, p. 20006, 2007.

[9] J. He, J. Cai, and J. Lin, "Synchronization of hyperchaotic systems with multiple unknown parameters and its application in secure communication," *Optik*, vol. 127, no. 5, pp. 2502–2508, 2016.

[10] G. Ye and X. Huang, "An efficient symmetric image encryption algorithm based on an intertwining Logistic map," *Neurocomputing*, vol. 251, pp. 45–53, 2017.

[11] S. Stalin, P. Maheshwary, P. K. Shukla, M. Maheshwari, B. Gour, and A. Khare, "Fast and secure medical image encryption based on nonlinear 4D Logistic map and DNA sequences (NL4DLM_DNA)," *Journal of Medical Systems*, vol. 43, pp. 1–17, 2019.

[12] J. Chen, L. Chen, and Y. Zhou, "Cryptanalysis of a DNA-based image encryption scheme," *Information Sciences*, vol. 520, pp. 130–141, 2020.

[13] A. Sambas, S. Vaidyanathan, M. Mamat, M. A. Mohamed, "Investigation of chaos behavior in a new two-scroll chaotic system with four unstable equilibrium points, its synchronization via four control methods and circuit simulation." *IAENG International Journal of Applied Mathematics*, vol. 50, no. 1, pp. 12–21, 2020.

[14] X. Wang and X. Chen, "An image encryption algorithm based on dynamic row scrambling and zigzag transformation," *Chaos, Solitons & Fractals*, vol. 147, p. 110962, 2021.

[15] B. Subartini, S. Vaidyanathan, A. Sambas, S. Zhang, "Multistability in the finance chaotic system, its bifurcation analysis and global chaos synchronization via integral sliding mode control." *IAENG International Journal of Applied Mathematics*, vol. 51, no. 4, pp. 995–1002, 2021.

[16] X. Liu, X. Tong, Z. Wang, and M. Zhang, "A new n-dimensional conservative chaos based on generalized hamiltonian system and its' applications in image encryption," *Chaos, Solitons & Fractals*, vol. 154, p. 111693, 2022.

[17] N. Munir, M. Khan, A. Al Karim Haj Ismail, and I. Hussain, "Cryptanalysis and improvement of novel image encryption technique using hybrid method of discrete dynamical chaotic maps and brownian motion," *Multimedia Tools and Applications*, vol. 81, no. 5, pp. 6571–6584, 2022.

[18] Y. Sang, J. Sang, and M. S. Alam, "Image encryption based on Logistic chaotic systems and deep autoencoder," *Pattern Recognition Letters*, vol. 153, pp. 59–66, 2022.

[19] Y. Zhang, Y. He, J. Zhang, and X. Liu, "Multiple digital image encryption algorithm based on chaos algorithm," *Mobile Networks and Applications*, vol. 27, no. 4, pp. 1349–1358, 2022.

[20] Q. Liang and C. Zhu, "A new one-dimensional chaotic map for image encryption scheme based on random DNA coding," *Optics & Laser Technology*, vol. 160, p. 109033, 2023.

[21] Q. Lai, G. Hu, U. Erkan, and A. Toktas, "A novel pixel-split image encryption scheme based on 2D salomon map," *Expert Systems with Applications*, vol. 213, p. 118845, 2023.

[22] W. Song, C. Fu, Y. Zheng, M. Tie, J. Liu, and J. Chen, "A parallel image encryption algorithm using intra bitplane scrambling," *Mathematics and Computers in Simulation*, vol. 204, pp. 71–88, 2023.

[23] S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," *Optik*, vol. 272, p. 170316, 2023.

[24] D. Wei, M. Jiang, and Y. Deng, "A secure image encryption algorithm based on hyper-chaotic and bit-level permutation," *Expert Systems with Applications*, vol. 213, p. 119074, 2023.

[25] D. Sweetania, S. MT, and S. Madenda, "Development of a new chaotic function-based algorithm for encrypting digital images." *International Journal of Advanced Computer Science & Applications*, vol. 15, no. 4, 2024.

[26] Q. Lai and Y. Liu, "A cross-channel color image encryption algorithm using two-dimensional hyperchaotic map," *Expert Systems with Applications*, vol. 223, p. 119923, 2023.

[27] X. Liu, X. Tong, M. Zhang, and Z. Wang, "A highly secure image encryption algorithm based on conservative hyperchaotic system and dynamic biogenetic gene algorithms," *Chaos, Solitons & Fractals*, vol. 171, p. 113450, 2023.

[28] H. Wen and Y. Lin, "Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding," *Expert Systems with Applications*, vol. 237, p. 121514, 2024.

[29] S. Yu and G. Chen, "Anti-control of continuous-time dynamical systems," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 6, pp. 2617–2627, 2012.

[30] Y. Ye and J. He, "Constructing a new multi-scroll chaotic system and its circuit design," *Mathematics*, vol. 12, no. 13, 1931, p. 1–14, 2024.

[31] R. Miranda and E. Stone, "The proto-lorenz system," *Physics Letters A*, vol. 178, no. 1-2, pp. 105–113, 1993.

[32] X. Wang and J. Yang, "A privacy image encryption algorithm based on piecewise coupled map lattice with multi dynamic coupling coefficient," *Information Sciences*, vol. 569, pp. 217–240, 2021.

[33] F. Yang, J. Mou, H. Yan, and J. Hu, "Dynamical analysis of a novel complex chaotic system and application in image diffusion," *IEEE Access*, vol. 7, pp. 118 188–118 202, 2019.

[34] J. He, W. Qiu, and J. Cai, "Synchronization of hyperchaotic systems based on intermittent control and its application in secure communication," *Journal of Advanced Computational Intelligence and Intelligent Informatics*, vol. 27, no. 2, pp. 292–303, 2023.

[35] X. Gao, "Image encryption algorithm based on 2D hyperchaotic map," *Optics & Laser Technology*, vol. 142, p. 107252, 2021.

[36] S. El Assad and M. Farajallah, "A new chaos-based image encryption system," *Signal Processing: Image Communication*, vol. 41, pp. 144–157, 2016.

[37] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[38] G. Kaur, R. Agarwal, and V. Patidar, "Color image encryption scheme based on fractional hartley transform and chaotic substitution–permutation," *The Visual Computer*, vol. 38, no. 3, pp. 1027–1050, 2022.

[39] V. Folifack Signing, T. Fozin Fonzin, M. Kountchou, J. Kengne, and Z. T. Njitacke, "Chaotic Jerk system with hump structure for text and image encryption using DNA coding," *Circuits, Systems, and Signal Processing*, vol. 40, pp. 4370–4406, 2021.

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

[41] J. Zheng and L. Liu, "Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D Logistic sine map," *IET Image Processing*, vol. 14, no. 11, pp. 2310–2320, 2020.

[42] Y. Luo, J. Lin, J. Liu, D. Wei, L. Cao, R. Zhou, Y. Cao, and X. Ding, "A robust image encryption algorithm based on Chua's circuit and compressive sensing," *Signal Processing*, vol. 161, pp. 227–247, 2019.

[43] W. Wang, M. Si, Y. Pang, P. Ran, H. Wang, X. Jiang, Y. Liu, J. Wu, W. Wu, N. Chilamkurti *et al.*, "An encryption algorithm based on combined chaos in body area networks," *Computers & Electrical Engineering*, vol. 65, pp. 282–291, 2018.

[44] P. Zhen, G. Zhao, L. Min, and X. Jin, "Chaos-based image encryption scheme combining DNA coding and entropy," *Multimedia Tools and Applications*, vol. 75, pp. 6303–6319, 2016.

[45] F. Musanna, D. Dangwal, S. Kumar, and V. Malik, "A chaos-based image encryption algorithm based on multiresolution singular value decomposition and a symmetric attractor," *The Imaging Science Journal*, vol. 68, no. 1, pp. 24–40, 2020.

[46] P. T. Akkasaligar and S. Biradar, "Selective medical image encryption using DNA cryptography," *Information Security Journal: A Global Perspective*, vol. 29, no. 2, pp. 91–101, 2020.

[47] P. N. Lone, D. Singh, and U. H. Mir, "A novel image encryption using random matrix affine cipher and the chaotic maps," *Journal of Modern Optics*, vol. 68, no. 10, pp. 507–521, 2021.

[48] C.-K. Huang, C.-W. Liao, S. Hsu, and Y. Jeng, "Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system," *Telecommunication Systems*, vol. 52, pp. 563–571, 2013.

[49] V. Kumar, J. B. B. Rayappan, R. Amirtharajan, and P. Praveenkumar, "Quantum true random number generation on IBM's cloud platform," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 8, pp. 6453–6465, 2022.

Shiya Wang received the B. S. degree from Heze University, China, in 2022. She is currently studying for a M. S. degree at School of Mathematics and Statistics, Minnan Normal University, China. Her research interests include multi-scrolls attractors and its encryption application.

Jianbin He received the Ph. D. degree from Guangdong University of Technology, China, in 2017. He was a Lecturer at School of Mathematics and Statistics, Minnan Normal University, China, in 2017-2020. He is currently a associate professor at School of Mathematics and Statistics, Minnan Normal University, China, in 2020. His research interests include chaos theory and its application, chaos-based cryptography.