Design of Higher-Dimensional Hyperchaotic System based on Combined Control and its Encryption Application

Kun Zhao, Jianbin He*
School of Mathematics and Statistics
Minnan Normal University, Zhangzhou 363000, China

Abstract—**According to the anti-control principle of chaos, a combined control method is proposed based on a class of asymptotically stable linear systems with multiple controllers. A higher-dimensional hyperchaotic system is investigated by the Lyapunov exponents method and equilibrium points analysis, and it exists the largest number of positive Lyapunov exponents. The chaotic pseudo-random sequences of the higher-dimensional hyperchaotic system can pass all NIST tests after preprocessing, and behave better chaotic characteristics. Meanwhile, a new encryption algorithm of image information with position scrambling, sequential diffusion and reverse diffusion is designed based on the chaotic pseudo-random sequences. The experiments of image information are given to verify the effectiveness and feasibility of the encryption algorithm. Finally, the security analyses are also discussed by the key sensitivity, differential attack and statistical analysis. It is shown that the encryption algorithm has large enough key space and can be applied to secure communication.**

Keywords*—*Hyperchaotic system; positive lyapunov exponent; chaotic pseudo-random sequence; image encryption

I. Introduction

With the rapid development of computer network technology and intelligent equipment, the digital information may be stolen or even destroyed by the attacker when it is transmitted through the public network, such as the personal privacy information, images and videos. In particular, some information is used in military, medical, political and other important fields, so it is very necessary to protect the integrity and confidentiality of the information transmission process. Information hiding and information encryption are two important information protection technologies. Information hiding is to hide information in another information carrier and transmit it through public channel, and it includes information hiding algorithm, digital watermarking, hidden channel technology and anonymous communication technology, etc. The information encryption is to design encryption algorithms to improve the security and efficiency by the characteristics of digital information. Usually, the image encryption includes uncompressed and compressed image encryption [1].

The chaos-based image encryption is one of widely used security method. It can not only prevent the loss of image information, but also convert original image into unrecognized encrypted image. The chaos-based image encryption generally includes two important steps: scrambling and diffusion encryption. The scrambling method can scramble the position of the plaintext image without changing the pixel value of the image, and it reduces the correlation between adjacent pixels of the image. The diffusion method changes the pixel value of the image through XOR operation, which makes the distribution of the encrypted image information more uniform and random. Therefore, the combination of scrambling and diffusion encryption is very effective for the image encryption.

Since Lorenz found the chaos from the mathematical model of meteorology, chaos theory has attracted extensive attention of scientists. Chaotic system is usually generated from a nonlinear dynamic system, and the characteristics of initial condition sensitivity, non-periodicity, long-term unpredictability and pseudo-randomness are very suitable for image encryption and other information encryption [2]–[7]. Moreover, some of the chaos-based encryption algorithms are analysed and may be not resist the chosen-plaintext attacks [8]. In [9], the security loopholes of an image encryption algorithm based on random walk and hyperchaotic systems are found, and the attack method is proposed to successfully break the encryption scheme. Therefore, the security of encryption algorithm based on chaotic system is one of the most important factors for information secure communication, and more secure chaos-based encryption algorithm need to be analysed and proposed. Compared with the lower-dimensional chaotic system, the higher-dimensional hyperchaotic system has more positive Lyapunov exponents, and the pseudo-random sequences generated by iteration are more complex chaotic characteristics. The encryption algorithm based on the higher-dimensional hyperchaotic system can be used for information secure communication [10]. The positive Lyapunov exponent is one of useful methods to show whether the nonlinear dynamic system exists chaos or not. Generally, the chaotic system has one positive Lyapunov exponent, while the hyperchaotic system has two or more positive Lyapunov exponents [11]. The number and size of positive Lyapunov exponents can reflect the chaotic characteristics of the system, and the hyperchaotic system with multiple positive Lyapunov exponents has more complex dynamic characteristics.

In recent years, the research on higher-dimensional hyperchaotic systems with multiple positive Lyapunov exponents has attracted much attention [12]–[14]. In [15], an effective image encryption algorithm of confusion and diffusion encryption is proposed based on chaotic system, and it is very sensitive to the initial variables. A new chaos-based image encryption algorithm is investigated in [16], and the security test shows

[*] Corresponding authors.

that the algorithm has good security performance and can resist a variety of special attacks. An image encryption algorithm based on chaotic system and DNA sequence operation is proposed, which not only has good encryption effect, but also can resist various typical attacks [17]. A S-box encryption algorithm based on chaotic system is designed for secure and fast image encryption, and NIST tests are used to verify the randomness of the sequences [18]. A color image encryption scheme is proposed based on non-uniform cellular automata and hyperchaos, the security analysis shows that the scheme has a very large key space and can resist various attacks [19]. A new image encryption algorithm is proposed by the confusion and diffusion based on chaos and SHA-256, and it can resist the chosen-plaintext attack and overcome the difficulty of key management in the "one-time password" encryption scheme [20]. A modified logistic chaotic map are created to designed encryption technique with better security and efficiency [21]. An image encryption algorithm is designed by combining fractional Fourier transform, DNA sequence operation and chaos theory, and the algorithm has good encryption effect, large key space and high key sensitivity [22]. A technique for encrypting RGB image components by using nonlinear chaotic function and DNA sequence is presented in [23]. In [24], the theoretical security of a medical privacy protection scheme based on DNA encoding and chaotic maps is reanalyzed, and the scheme is rigorously proven to be insecure against the chosen-plaintext attack. Based on a combination of multidimensional chaotic systems, an cryptosystem for the color image encryption is described in [25], and the level of security and the computational complexity is improved. By using higher-dimensional chaotic maps and some conventional cryptographic techniques, a class of chaotic cryptosystems is designed to enhance the security of cryptosystems [26].

The research of higher-dimensional hyperchaotic systems is one of hot topic. Some criteria and methods for constructing higher-dimensional hyperchaotic systems are proposed [27], [28]. In this paper, a higher-dimensional hyperchaotic system is investigated by the combination of multiple controllers, and a new 11-dimensional hyperchaotic system with nine positive Lyapunov exponents is designed. The main contributions of this paper are as follows: (1) Through the combination of multiple controllers, a class of higher-dimensional hyperchaotic systems with the largest number of positive Lyapunov exponents is studied; (2) Based on the chaotic sequences generated by the iteration of higher-dimensional hyperchaotic system, an encryption algorithm is proposed by combining the position scrambling, sequential diffusion and inverse diffusion. (3) The feasibility and security of the new encryption algorithm based on 11-dimensional hyperchaotic system are verified through the simulation experiments.

The rest of this paper is organized as follows. Section II is the design method of hyperchaotic system. Section III is the design of encryption algorithm. The security analysis of the encryption algorithm is given in Section IV. Section V concludes the paper.

II. Construction of Higher-Dimensional Hyperchaotic Systems

A. Chaotic Anti-Control System with Combined Controllers

According to the anti-control method of higher-dimensional hyperchaotic systems, a nominal asymptotically stable linear dynamical system is given by [29]

$$\dot{X} = PAP^{-1}X \tag{1}$$

where $X = (x_1, x_2, \cdots, x_n)$, the matrix A and the similarity transformation matrix P are given as follows:

$$\begin{cases} A = \begin{pmatrix} A_1 & 0 & 0 & 0 & 0 \\ 0 & A_2 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & A_{m-1} & 0 \\ 0 & 0 & \cdots & 0 & A_m \end{pmatrix}_{n\times n} \\ \text{if } n \text{ is even}, m = \dfrac{n}{2} \\ A = \begin{pmatrix} A_1 & 0 & 0 & 0 & 0 \\ 0 & A_2 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & A_m & 0 \\ -1 & -1 & \cdots & -1 & \tau \end{pmatrix}_{n\times n} \\ \text{if } n \text{ is odd}, m = \dfrac{n-1}{2} \end{cases}$$

$$P = \begin{pmatrix} 0 & 1 & \cdots & 1 & 1 \\ 1 & 0 & \cdots & 1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \cdots & 0 & 1 \\ 1 & 1 & \cdots & 1 & 0 \end{pmatrix}_{n\times n}$$

and $A_i = \begin{pmatrix} \lambda_i & \psi_{i1} \\ \psi_{i2} & \lambda_i \end{pmatrix}$

is a block matrix, where $\psi_{i1} \times \psi_{i2} < 0, \tau < 0$.

Next, a uniformly bounded controller $f(\sigma X, \varepsilon)$ and control matrix C are designed for the system (1), such that

$$\dot{X} = PAP^{-1}X + Cf(\sigma X, \varepsilon) \tag{2}$$

The combination of controllers $f(\sigma X, \varepsilon)$ and the control matrix C are given by

$$f(\sigma X, \varepsilon) = \begin{pmatrix} \varepsilon_1 \sin(\sigma_1 x_1 + \varphi_1) + \varepsilon_2 \cos(\sigma_2 x_1 + \varphi_2) \\ \varepsilon_1 \sin(\sigma_1 x_2 + \varphi_1) + \varepsilon_2 \cos(\sigma_2 x_2 + \varphi_2) \\ \vdots \\ \varepsilon_1 \sin(\sigma_1 x_{n-1} + \varphi_1) + \varepsilon_2 \cos(\sigma_2 x_{n-1} + \varphi_2) \\ \varepsilon_1 \sin(\sigma_1 x_n + \varphi_1) + \varepsilon_2 \cos(\sigma_2 x_n + \varphi_2) \end{pmatrix}$$

$$C = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & 1_{(i,j)} & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}_{n\times n}$$

where $\varepsilon_1, \sigma_1, \varphi_1, \varepsilon_2, \sigma_2, \varphi_2$ are controller parameters, $1_{(i,j)}$ denotes that the element in row i and column j is equal to 1, i.e., the controller is in the state of working.

When the dimension $n = 11$, the matrices A_i $(i = 1, 2, 3, 4, 5)$ are given by

$$\begin{cases} A_1 = \begin{pmatrix} -0.01 & 1.00 \\ -6.00 & -0.01 \end{pmatrix}, A_2 = \begin{pmatrix} -0.01 & 18.00 \\ -2 & -0.01 \end{pmatrix} \\ A_3 = \begin{pmatrix} -0.01 & 15.00 \\ -1.00 & -0.01 \end{pmatrix}, A_4 = \begin{pmatrix} -0.01 & 22.00 \\ -2.50 & -0.01 \end{pmatrix} \\ A_5 = \begin{pmatrix} -0.01 & 3.00 \\ -20.00 & -0.01 \end{pmatrix} \end{cases}$$

and $\tau = -0.01, \varepsilon_1 = 76, \sigma_1 = 8, \varphi_1 = 6, \varepsilon_2 = 68, \sigma_2 = 5, \varphi_2 = 4$, the control position $(i, j) = (11, 10)$, therefore, the controlled system is given as follows:

$$\dot{X} = PAP^{-1}X + \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ f(x_{10}) \end{bmatrix}_{11\times 1} \tag{3}$$

where the combined controller

$$f(x_{10}) = 76\sin(8x_{10} + 6) + 68\cos(5x_{10} + 4)$$

and it is shown in Fig. 1.

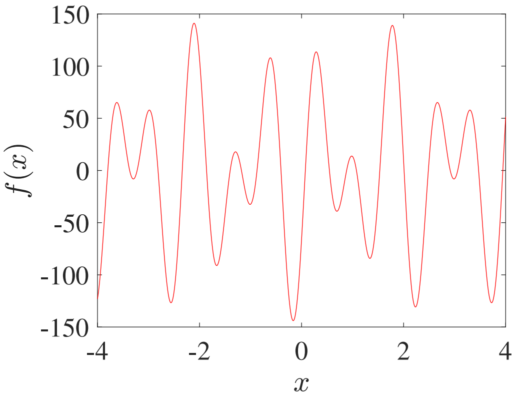


Fig. 1. The Function of Combined Controller $f(x_{10})$ (x Denotes x_{10})

B. Chaotic Attractors and Lyapunov Exponent

By the calculation on the software of Matlab R2021a, the Lyapunov exponents of system (3) are given by

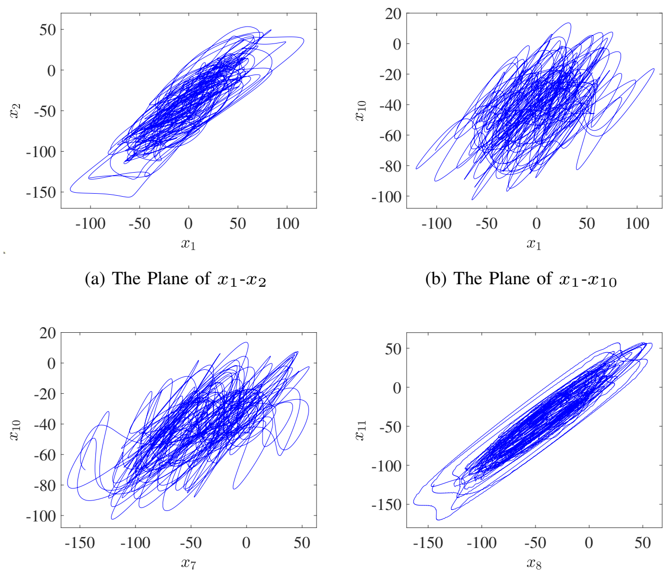
$$\begin{cases} \mathrm{LE}_1 = 4.37, \mathrm{LE}_2 = 0.49, \mathrm{LE}_3 = 0.41 \\ \mathrm{LE}_4 = 0.35, \mathrm{LE}_5 = 0.29, \mathrm{LE}_6 = 0.26 \\ \mathrm{LE}_7 = 0.22, \mathrm{LE}_8 = 0.16, \mathrm{LE}_9 = 0.02 \\ \mathrm{LE}_{10} = 0.00, \mathrm{LE}_{11} = -6.68 \end{cases}$$

Obviously, the 11-dimensional hyperchaotic system has 9 positive Lyapunov exponents, so it has strong chaotic characteristics.

Furthermore, the initial values

$$X(0) = (0.2, 0.1, 0.3, 0.1, 0.2, 0.1, 0.5, 0.6, 0.7, 0.4, 0.2)$$

then the phase diagrams of chaotic attractor are shown in Fig. 2.



(a) The Plane of x_1-x_2

(b) The Plane of x_1-x_{10}

(c) The Plane of x_7-x_{10}

(d) The Plane of x_8-x_{11}

Fig. 2. Attractor of the Controlled Hyperchaotic System (3)

C. Equilibrium Point Analysis of the Controlled System

Obviously, the only one equilibrium point of the system (1) is

$$X_e = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

and the corresponding eigenvalues of Jacobi matrix at the equilibrium point X_e are given by

$$\begin{cases} \lambda_{1,2} = -0.01 \pm 7.7460\mathrm{i} \\ \lambda_{3,4} = -0.01 \pm 7.4162\mathrm{i} \\ \lambda_{5,6} = -0.01 \pm 6.0000\mathrm{i} \\ \lambda_7 = -0.01 \\ \lambda_{8,9} = -0.01 \pm 3.8730\mathrm{i} \\ \lambda_{10,11} = -0.01 \pm 2.4495\mathrm{i} \end{cases}$$

Since all eigenvalues are negative, so the system (1) is asymptotically stable.

However, the controlled system (3) has multiple equilibrium points, and the equilibrium points of the controlled system (3) can be obtained by Eq. (4).

Therefore, the corresponding solutions can be obtained by the Cramer rule [11]:

$$\begin{aligned} x_i &= \frac{|E_i|}{|D|} \\ &= (-1)^{(11+i)} \frac{-f(x_{10})}{|D|} |M_{11,i}| \\ &\quad (i = 1, 2, \cdots, 11) \end{aligned}$$

where $D = PAP^{-1}$, E_i is the matrix that the ith column of the matrix D is replaced by the controller vector in right-

$$\begin{pmatrix} 2.74 & -0.25 & 22.75 & -19.25 & 5.25 & -12.25 & 3.75 & -15.25 & 4.75 & 1.75 & 8.75 \\ 3.75 & 1.74 & 4.75 & -17.25 & 7.25 & -10.25 & 5.75 & -13.25 & 6.75 & 3.75 & 10.75 \\ 1.45 & 2.45 & 22.44 & -19.55 & 4.95 & -12.55 & 3.45 & -15.55 & 4.45 & 1.45 & 8.45 \\ 2.00 & 0.00 & 23.00 & -19.01 & 3.00 & -12.00 & 4.00 & -15.00 & 5.00 & 2.00 & 9.00 \\ -0.45 & -2.45 & 20.55 & 0.55 & 3.04 & -14.45 & 1.55 & -17.45 & 2.55 & -0.45 & 6.55 \\ 1.85 & -0.15 & 22.85 & -19.15 & 5.35 & -12.16 & 2.85 & -15.15 & 4.85 & 1.85 & 8.85 \\ 0.25 & -1.75 & 21.25 & -20.75 & 3.75 & 1.25 & 2.24 & -16.75 & 3.25 & 0.25 & 7.25 \\ 1.95 & -0.05 & 22.95 & -19.05 & 5.45 & -12.05 & 3.95 & -15.06 & 2.95 & 1.95 & 8.95 \\ -0.05 & -2.05 & 20.95 & -21.05 & 3.45 & -14.05 & 1.95 & 0.95 & 2.94 & -0.05 & 6.95 \\ 2.35 & 0.35 & 23.35 & -18.65 & 5.85 & -11.65 & 4.35 & -14.65 & 5.35 & 2.34 & 3.35 \\ 1.65 & -0.35 & 22.65 & -19.35 & 5.15 & -12.35 & 3.65 & -15.35 & 4.65 & 2.65 & 8.64 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ f(x_{10}) \end{pmatrix} \tag{4}$$

hand side of the Eq. (4), and $M_{11,i}$ is the algebraic cofactor of E_i, i.e., the solutions x_i of the controlled system (3) are given by

$$\begin{cases} x_1 = \dfrac{11339f(x_{10})}{-106923}, & x_2 = \dfrac{10152750f(x_{10})}{106923} \\ x_3 = \dfrac{10156849f(x_{10})}{106923}, & x_4 = \dfrac{10155828f(x_{10})}{106923} \\ x_5 = \dfrac{10160590f(x_{10})}{106923}, & x_6 = \dfrac{10155606f(x_{10})}{106923} \\ x_7 = \dfrac{10167011f(x_{10})}{106923}, & x_8 = \dfrac{10155721f(x_{10})}{106923} \\ x_9 = \dfrac{10161661f(x_{10})}{106923}, & x_{10} = \dfrac{10252559f(x_{10})}{106923} \\ x_{11} = \dfrac{10157933f(x_{10})}{106923} \end{cases} \tag{5}$$

Hence, one has

$$\frac{106923}{10252559}x_{10} = -76\sin(8x_{10}+6) - 68\cos(5x_{10}+4)$$

if one lets

$$y_1 = \frac{106923}{10252559}x_{10}$$

and

$$y_2 = -76\sin(8x_{10}+6) - 68\cos(5x_{10}+4)$$

then the intersection points (x_{10}, y_1) of $y_1 = y_2$ are shown in Fig. 3, and the equilibrium points of the controlled system are given by Eq. (5).

III. Design of Encryption Algorithm

A. Data Preprocessing

An image encryption scheme is designed based on 11-dimensional hyperchaotic system. Firstly, the 4th-order Runge-Kutta method is used to discretize the 11-dimensional hyperchaotic system, where the Runge-Kutta formula is given by

$$\begin{cases} X_{i+1} = X_i + \dfrac{h}{6}(K_1 + 2K_2 + 2K_3 + K_4) \\ K_1 = f(t_i, X_i), K_2 = f(t_i + \dfrac{h}{2}, X_i + \dfrac{h}{2}K_1) \\ K_3 = f(t_i + \dfrac{h}{2}, X_i + \dfrac{h}{2}K_2), K_4 = f(t_i + h, X_i + hK_3) \\ \qquad (i = 1, 2, \cdots n, \cdots) \end{cases}$$

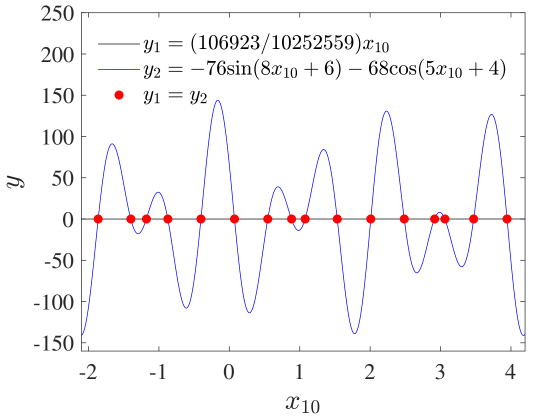


Fig. 3. The Intersection Points of y_1 and y_2 in Equation (4)

The initial values of the hyperchaotic system $X(0)$, and the step $h = 0.001$, then the image encryption algorithm are given as follows:

Step 1: The number of pre-iterations is equal to $\big(2000 + \mathrm{mod}(\mathrm{sum}, \sigma_1 \times \varepsilon_1 \times \varphi_1)\big)$ and it is used to counteract the transient effect of chaotic iteration, where sum is sum of pixel values of original image, mod is the modular function, and $\sigma_1, \varepsilon_1, \varphi_1$ are controller parameters. The pseudo-random sequences generated by the iteration of 11-dimensional hyperchaotic system are $X = (X_1, X_2, \cdots, X_{11})$.

Step 2: The operations of rounding, modulo and shifting are used to generate the pseudo-random sequences $Z =$

$(Z_1, Z_2, \cdots, Z_{11})$, i.e.,

$$\begin{cases} Z_1 = \text{fix}(\text{mod}(\text{mod}(X_1, 1) \times 10^{12}, 1) \times 10^9) \\ Z_2 = \text{fix}(\text{mod}(\text{mod}(X_2, 1) \times 10^{14}, 1) \times 10^9) \\ Z_3 = \text{fix}(\text{mod}(\text{mod}(X_3, 1) \times 10^{13}, 1) \times 10^9) \\ Z_4 = \text{fix}(\text{mod}(\text{mod}(X_4, 1) \times 10^{13}, 1) \times 10^9) \\ Z_5 = \text{fix}(\text{mod}(\text{mod}(X_5, 1) \times 10^{12}, 1) \times 10^9) \\ Z_6 = \text{fix}(\text{mod}(\text{mod}(X_6, 1) \times 10^{13}, 1) \times 10^9) \\ Z_7 = \text{fix}(\text{mod}(\text{mod}(X_7, 1) \times 10^{12}, 1) \times 10^9) \\ Z_8 = \text{fix}(\text{mod}(\text{mod}(X_8, 1) \times 10^{14}, 1) \times 10^9) \\ Z_9 = \text{fix}(\text{mod}(\text{mod}(X_9, 1) \times 10^{11}, 1) \times 10^9) \\ Z_{10} = \text{fix}(\text{mod}(\text{mod}(X_{10}, 1) \times 10^{13}, 1) \times 10^9) \\ Z_{11} = \text{fix}(\text{mod}(\text{mod}(X_{11}, 1) \times 10^{15}, 1) \times 10^9) \end{cases}$$

where the function fix represents the rounding operation, and the pseudo-random sequences Z can pass most tests of NIST.

Step 3: In order to ensure that the encryption algorithm has better encryption effect, the pseudo-random sequences Z are further obtained by

$$\begin{cases} W_1 = \text{mod}((Z_1 - Z_2 + Z_3), MN) + 1 \\ W_2 = \text{mod}((Z_4 + Z_5), 256) \\ W_3 = \text{mod}((Z_6 + Z_7 + 1), 256) \\ W_4 = \text{mod}((Z_8 + Z_9 + 1), 256) \\ W_5 = \text{mod}((Z_{10} + Z_{11}), 256) \end{cases}$$

Then the new pseudo-random sequences $W = (W_1, W_2, \cdots, W_5)$ can pass the NIST test, and they are given in Section V.

B. Encryption Algorithms

The encryption algorithms include scrambling encryption, sequential diffusion encryption and reverse diffusion encryption. The image information is chosen as an example, and the flow chart of information encryption is shown in Fig. 4.

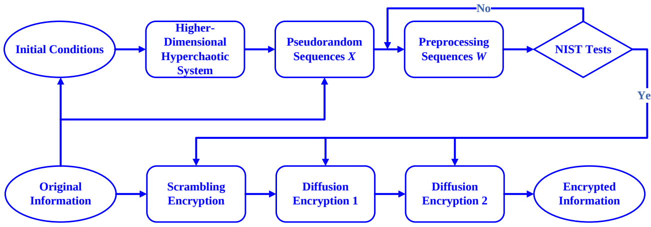


Fig. 4. The Flow Chart of Information Encryption

a) Position Scrambling Encryption

The original image P_1 is in the size of $M \times N$, and the pixel position of P_1 is scrambled based on the pseudo-random sequence W_1, then the scrambled image P_2 is obtained by

$$P_2(i) = P_1(W_1(i)), \ (i = 1, 2, \cdots, MN)$$

b) Sequential Diffusion Encryption

The scrambled image P_2 is encrypted by using pseudo-random sequences W_3 and W_4, and the steps of encryption are as follows:

Step 1: The first pixel value $P_2(1)$ of the scrambled image is encrypted by the first value $W_3(1)$ of the random sequence via the XOR operation, i.e.,

$$P_3(1) = P_2(1) \oplus W_3(1)$$

Step 2: Add the pseudo-random sequence $W_2(i)$ to the pixel values of scrambled image $P_2(i)$, and subtract the integer part of $P_2(i-1)/\varphi$, then the encrypted information $P_3'(i)$ is obtained by the modulus of 256, i.e.,

$$P_3'(i) = \text{mod}((P_2(i) + W_2(i) - \text{fix}(P_2(i-1)/\varphi)), 256) \\ (i = 2, 3, \cdots, MN)$$

Step 3: The sequence $P_3^{'}$ is encrypted with the random sequence W_3 by the XOR operation, and the encrypted image is given by

$$P_3(i) = P_3'(i) \oplus W_3(i), \quad (i = 2, 3, \cdots, MN)$$

c) Reverse Diffusion Encryption

Use the random sequence W_4 and W_5 to perform reverse diffusion encryption on the sequential diffusion encrypted image P_3, and the encryption steps are given as follows:

Step 1: The $P_3(MN)$ is encrypted by the pseudo-random sequence $W_5(MN)$, i.e.,

$$P_4(MN) = P_3(MN) \oplus W_5(MN).$$

Step 2: Through subtraction, multiplication and modulo operations, the pixel values of P_3 are encrypted from the pseudo-random sequence W_4, i.e.,

$$P_4'(i) = \text{mod}(W_4(i) - P_3(i) + P_3(i+1), 256) \\ (i = MN - 1, MN - 2, \cdots, 1)$$

Step 3: Similarly, the P_4' is encrypted by the pseudo-random sequence W_5 by the XOR operation, one has

$$P_4(i) = P_4'(i) \oplus W_5(i), (i = MN - 1, MN - 2, \cdots, 1)$$

C. Decryption Process

The decryption is the inverse operation of the encryption, and it is given in follows:

Step 1: The $P_4(MN)$ and $W_5(MN)$ is used to obtain the value $P_3(MN)$ of sequential diffusion encryption, i.e.,

$$P_3(MN) = P_4(MN) \oplus W_5(MN)$$

Step 2: By addition, subtraction, multiplication and modulo operations, the P_3 is decrypted by the pseudo-random sequences W_4 and W_5, and it is given by

$$P_3(i) = \text{mod}(W_4(i) + P_4(i+1) - (P_4(i) \oplus W_5(i)), 256) \\ (i = MN - 1, MN - 2, \cdots, 1)$$

Step 3: Similarly, the $P_2\left(1\right)$ of scrambled encrypted image is obtained by the XOR operation of $P_3\left(1\right)$ and $W_3\left(1\right)$, i.e.,

$$P_2(1) = P_3(1) \oplus W_3(1)$$

Step 4: By the XOR, addition, division, subtraction and modulo operation, the scrambled encrypted image P_2 is decrypted by the pseudo-random sequences W_2 and W_3, and it is given by

$$\begin{aligned} P_2(i) = \mathrm{mod}((&P_3(i) \oplus W_3(i) + fix(P_3(i-1)/\varphi) \\ &- W_2(i)), 256), \quad (i = 2, 3, \cdots, MN) \end{aligned}$$

Step 5: The pixel value $P_2(i)$ of the scrambled image is exchanged with the pseudo-random sequence $W_1(i)$, and then one can get the original imageP_1, i.e.,

$$P_1(i) = P_2(W_1(i)), \quad (i = MN, MN-1, \cdots, 1)$$

Therefore, the decryption process is completed, and the receivers can get the recovered information from the ciphertext.

IV. Experimental Results

Based on the 11-dimensional hyperchaotic system in Eq. (3), the numerical simulation results are given by the proposed encryption and decryption algorithm in Section III. The encryption algorithm is tested by the Lena image in Fig. 5 (a) with the size of 512×512 and the Cameraman image in Fig. 5 (e) with the size of 256×256 based on the Matlab software, and the sum of pixel values of Lena image and Cameraman image are 32515895 and 7780728, respectively. By the initial values

$$X(0) = (0.2, 0.1, 0.3, 0.1, 0.2, 0.1, 0.5, 0.6, 0.7, 0.4, 0.2)$$

and other parameters of controlled system in Eq. (3), the results of encryption and decryption are shown in Fig. 5. The encrypted images Fig. 5 (b) and (f) are chaotic and disordered, and the original information can not be distinguished, so the encryption algorithm is effective.

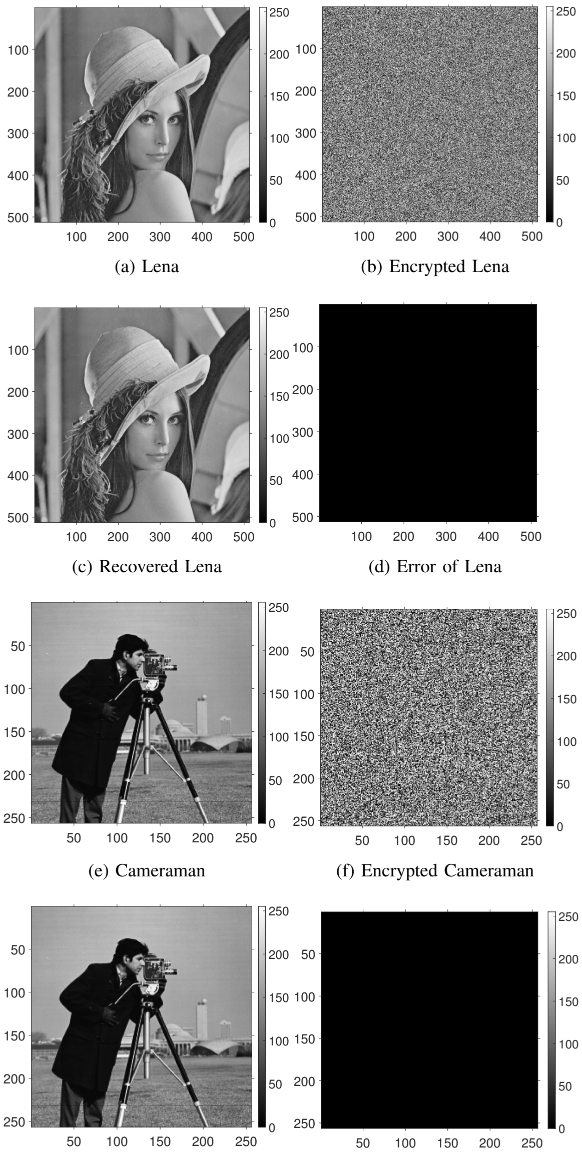
In the encryption algorithm, the sum of image pixel values is used to obtain the key of the encryption. Obviously, the sum of pixel values of different images is different, so the different images will generate different keys to the encryption, i.e., the cryptosystem has the effect of "one-time-pad". Hence, one cannot get any information of the plaintext image from the encrypted image, and the encryption algorithm is effective for secure communication.

Meanwhile, the error images in Fig. 5 (d) and (h) show that the errors between the recovered image and the original image are equal to zero, and Fig. 5 (c) and (g) show the original information can be recovered successfully by the decryption algorithm.

The hyperchaotic system is highly sensitive to the initial values $X(0), A, P, \varepsilon_i, \sigma_i$ $(i = 1, 2)$, etc., and the initial values are used as the encryption keys. If one of the keys is wrong, the ciphertext image cannot be successfully recovered, because the different initial values will generate different chaotic sequences. For example, if the value of the controller parameter is changed from $\varepsilon_1 = 76$ to $\varepsilon_1 = 75$, then the Lena image is encrypted by the corresponding pseudo-random sequences W, but the experiments show that the Lena image cannot be recovered successfully. Similarly, if the initial values $X(0)$ are changed to

$$X(0) = (0.1, 0.1, 0.3, 0.1, 0.2, 0.1, 0.5, 0.6, 0.7, 0.4, 0.2)$$

the experimental results show that the Lena image cannot be recovered successfully, so the encryption algorithm is also sensitive to the initial values $X(0)$.



(a) Lena

(b) Encrypted Lena

(c) Recovered Lena

(d) Error of Lena

(e) Cameraman

(f) Encrypted Cameraman

(g) Recovered Cameraman

(h) Error of Cameraman

Fig. 5. Experiments Results of Image Encryption and Decryption

V. Security Analysis

A. Analysis of Key Sensitivity

A good encryption algorithm must be sensitive to the small change of the key, i.e., if there is a small change of the key, then the ciphertext image can not recovered completely. The key space is depended on the sensitivity of matrix A, similar transformation matrix P, controller parameter $\varepsilon_1, \sigma_1, \varphi_1$ and the initial values $X(0)$ of controlled system. As there are 121 elements in matrix A and similar transformation matrix P, one needs to keep other keys unchanged but change only one key with small error, and then the experimental results of decipher images are given in Fig. 6. Fig. 6 (a) shows the decrypted image obtained by using the correct keys, and the ciphertext image can be recovered successfully. Fig. 6 (b)-(d) shows the decrypted image with the small error key, but the ciphertext image cannot be recovered successfully. Through experimental tests, Table I shows the ciphertext can not be decrypted successfully when the errors of key is greater than or equal to the minimum values.

TABLE I. Test Results of Key Sensitivity

Error of key	Recovered successfully
$\vert x_1 - x_1' \vert \geqslant 10^{-16}$	No
$\vert x_2 - x_2' \vert \geqslant 10^{-15}$	No
$\vert x_3 - x_3' \vert \geqslant 10^{-16}$	No
$\vert x_4 - x_4' \vert \geqslant 10^{-17}$	No
$\vert x_5 - x_5' \vert \geqslant 10^{-16}$	No
$\vert x_6 - x_6' \vert \geqslant 10^{-16}$	No
$\vert x_7 - x_7' \vert \geqslant 10^{-16}$	No
$\vert x_8 - x_8' \vert \geqslant 10^{-15}$	No
$\vert x_9 - x_9' \vert \geqslant 10^{-16}$	No
$\vert x_{10} - x_{10}' \vert \geqslant 10^{-16}$	No
$\vert x_{11} - x_{11}' \vert \geqslant 10^{-15}$	No
$\vert \sigma_1 - \sigma_1' \vert \geqslant 10^{-15}$	No
$\vert \varepsilon_1 - \varepsilon_1' \vert \geqslant 10^{-14}$	No
$\vert \varphi_1 - \varphi_1' \vert \geqslant 10^{-15}$	No
$\vert A(i,j) - A(i,j)' \vert \geqslant 10^{-15}$, $(i,j = 1,2,\cdots,11)$	No
$\vert P(i,j) - P(i,j)' \vert \geqslant 10^{-15}$, $(i,j = 1,2,\cdots,11)$	No

The experimental results show that the image can not be decrypted successfully by using the key with small error. In Table I, it can be estimated that the key space of the encryption algorithm is

$$\begin{aligned} KS = {} & 10^{14} \times (10^{15})^5 \times (10^{15})^{121} \times (10^{15})^{121} \times (10^{16})^7 \\ & \times 10^{17} \\ = {} & 10^{3848} \gg 2^{210} \end{aligned}$$

B. Histogram and Chi-Square Test

Histogram describes the distribution of image pixel value. The more uniform the distribution of pixel value, the better the effect of the encryption algorithm. Fig. 7 shows the histograms of the plaintext image and the encrypted image, respectively.

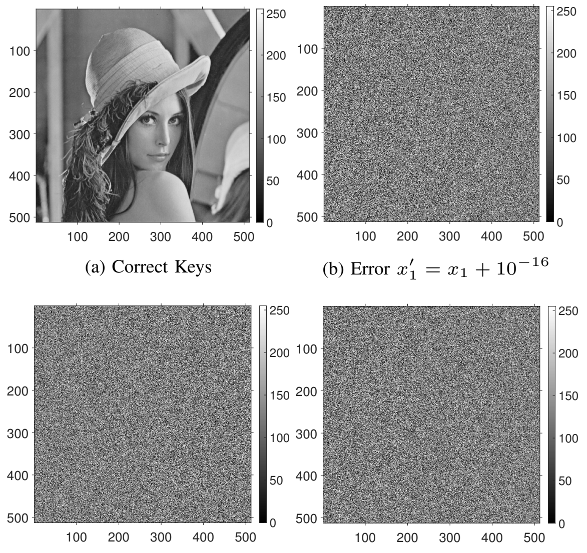
In addition, the Chi-square test is used to illustrate that the cryptosystem has very good confusion characteristics [30]. The grayscale level of a grayscale image is 256, and then

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

where f_i is the frequency of each 0 to 255 pixel level in the histogram of the encrypted image, g_i is the ideal frequency of uniform distribution, i.e.,

$$g_i = \frac{MN}{256}, \quad (i = 0, 1, \cdots, 255)$$

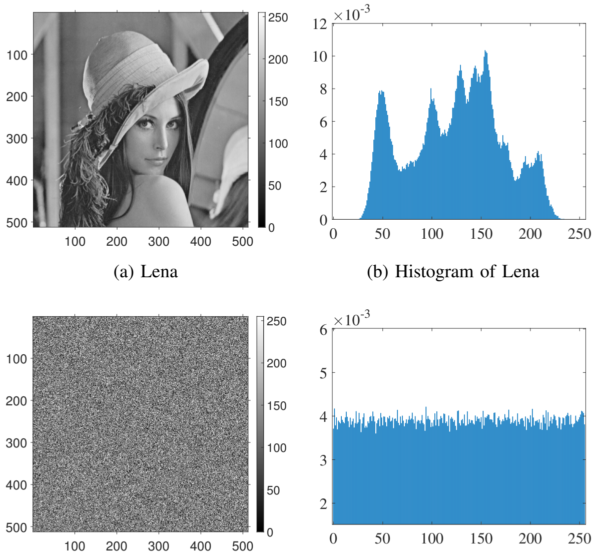
where M and N are the length and width of the image,



(a) Correct Keys (b) Error $x_1' = x_1 + 10^{-16}$

(c) Error $x_2' = x_2 + 10^{-15}$ (d) Error $x_3' = x_3 + 10^{-16}$

Fig. 6. Decryption Results of Encrypted Image with Different Keys



(a) Lena (b) Histogram of Lena

(c) Encrypted Lena (d) Histogram of Encrypted Lena

Fig. 7. Histogram of Lena and the Corresponding Encrypted Image

respectively. If the χ^2 distribution with a degree of freedom of 255 and the significance level is 0.05, then $\chi^2_{0.05}(255) = 293.25$. In Table II, the χ^2 test of original images is significantly greater than 293.25, but the encrypted images are all less than 293.25. Therefore, the distribution of the histogram of the encrypted image is uniform, and it do not disclose any information by the statistical analysis.

TABLE II. χ^2 TESTS

Image	Lena	Cameraman	Barbara
Original Image	158350	110970	144100
Encrypted Image	223.64	238.89	215.80

C. Information Entropy

Information entropy is used to describe the randomness of image information, and it's defined as follows [31]:

$$H = -\sum_{i=1}^{n} p_i \log_2(p_i)$$

where p_i is the probability of the i-th gray value. For grayscale images, the expected entropy of image information is equal to 8. The entropy of three different images and encrypted images are shown in Table III. The entropy of encrypted images is close to 8, so the encryption algorithm is suitable to encrypt the plaintext information and it has good encryption effect.

TABLE III. INFORMATION ENTROPY

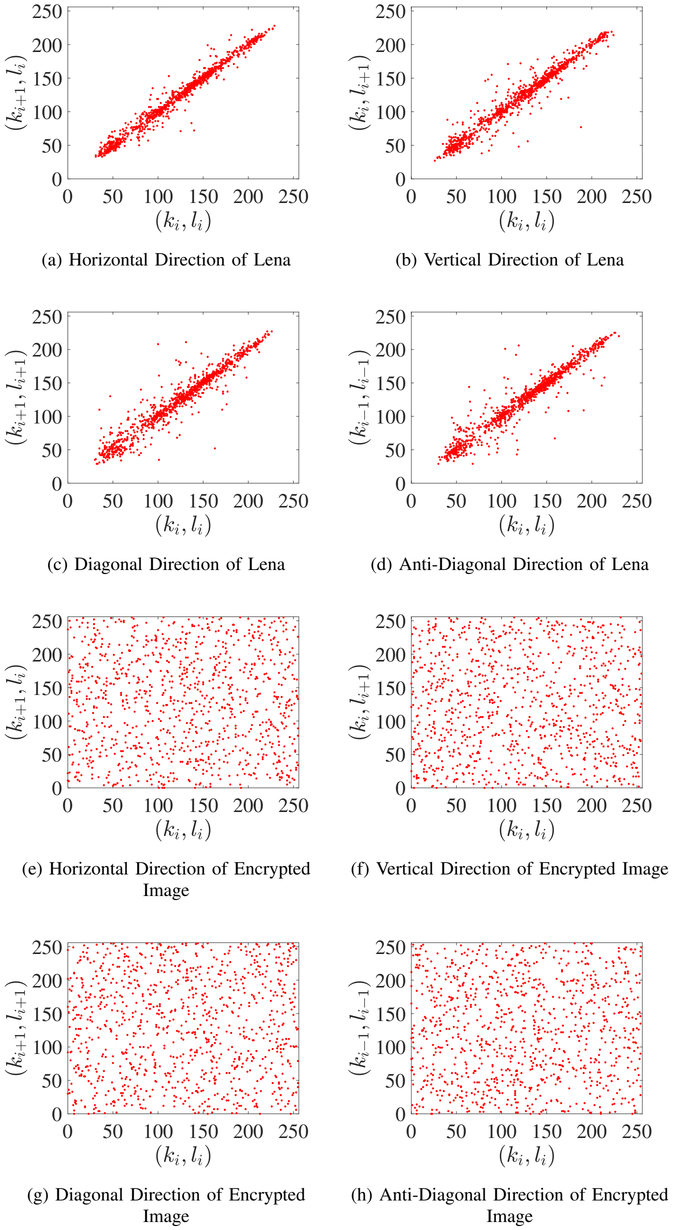
Image	Plaintext Image	Encrypted Image
Lena	7.4456	7.9915
Cameraman	7.0097	7.9902
Barbara	7.4664	7.9916
Lena in Ref. [32]	7.4456	7.9907
Lena in Ref. [33]	7.4456	7.9768

D. Analysis of Correlation Coefficient

The high correlation between the pixels of the plaintext image makes the image look clear and one may distinguish the image information. The correlation coefficient of unencrypted image is usually large, and the encryption algorithm will reduce the correlation between pixels to zero or close to zero. If N pairs of adjacent pixels are taken from the image and their gray value is (e_i, f_i) $(i = 1, 2, \cdots, N)$, the formula of correlation coefficient for vectors $\boldsymbol{e} = \{e_i\}$ and $\boldsymbol{f} = \{f_i\}$ is given as follows [34]:

$$\begin{cases} r_{\boldsymbol{ef}} = \dfrac{\operatorname{cov}(\boldsymbol{e}, \boldsymbol{f})}{\sqrt{D(\boldsymbol{e})}\sqrt{D(\boldsymbol{f})}} \\ \operatorname{cov}(\boldsymbol{e}, \boldsymbol{f}) = \dfrac{1}{N}\displaystyle\sum_{i=1}^{N}(e_i - E(\boldsymbol{e}))(f_i - E(\boldsymbol{f})) \\ D\left(\boldsymbol{e}\right) = \dfrac{1}{N}\displaystyle\sum_{i=1}^{N}\left(e_i - E(\boldsymbol{e})\right)^2, E\left(\boldsymbol{e}\right) = \dfrac{1}{N}\displaystyle\sum_{i=1}^{N} e_i \end{cases}$$

If the e_i denotes the pixel value in position (k_i, l_i), and the f_i denotes the pixel value in position (k_{i+1}, l_i), then the calculation result is the correlation coefficient in the horizontal direction. Similarly, 1000 pairs of pixel points of Lena are randomly selected in the vertical, horizontal, diagonal and anti-diagonal directions, and the corresponding correlation coefficients are shown in Table IV. Meanwhile, the correlations of Lena and the encrypted images are given in Fig. 8, the correlation coefficient of the encrypted image of proposed algorithm has been close to 0.



(a) Horizontal Direction of Lena

(b) Vertical Direction of Lena

(c) Diagonal Direction of Lena

(d) Anti-Diagonal Direction of Lena

(e) Horizontal Direction of Encrypted Image

(f) Vertical Direction of Encrypted Image

(g) Diagonal Direction of Encrypted Image

(h) Anti-Diagonal Direction of Encrypted Image

Fig. 8. Correlation Analysis of Lena Image

E. Differential Analysis

A secure cryptographic system should be highly sensitive to small changes in the key or plaintext image during encryption

TABLE IV. CORRELATION COEFFICIENTS OF PLAINTEXT AND CIPHERTEXT

Image	Horizontal	Vertical	Diagonal	Average
Lena	0.9831	0.9737	0.9666	0.9745
Encrypted	−0.0092	−0.0116	0.0114	0.0086
Ref. [35]	0.0141	0.0296	0.0054	0.0164
Ref. [36]	−0.0253	0.0026	0.0091	0.0123

and decryption. Especially, if the small changes in the plaintext image will produce completely different encrypted images, then it will be more effectively to resist chosen-plaintext attacks. NPCR and UACI are often used to analyze whether the encryption algorithm has a good encryption effect and security. NPCR is the proportion of different pixel numbers in all pixel points. UACI represents the average difference of the pixel values of the encrypted image when the original image is with one pixel (or some pixels) different in pixel values. The calculation formulas are given as follows [37]:

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

where x is the encrypted image, and x' is the new encrypted image when the plaintext is changed by one pixel or some pixels. If the 97 in 99-th pixel value of Lena image is changed to 98, the 132 in 99-th pixel value of Barbara image is changed to 133, and the 156 in 99-th pixel value of Cameraman image is changed to 157, then the NPCR and UACI of corresponding encrypted images are shown in Table V, and they are very close to the expected values (NPCR ≈ 99.6094%, UACI ≈ 33.4635%). So the encryption algorithm can resist plaintext attacks and has significant encryption effect.

TABLE V. NPCR AND UACI OF ENCRYPTED IMAGE(%)

Image	NPCR	UACI
Lena	99.6174	33.5231
Cameraman	99.6323	33.3901
Barbara	99.6281	33.3537
Ref. [38]	99.8700	33.2900
Ref. [39]	99.2402	33.3873

F. NIST Test

NIST test is used to verify the random characteristics of random sequences, and it includes 15 tests, such as single bit frequency, longest-run-of-ones and non-overlapping template matching [40]. If the random sequence can pass all NIST test, i.e., the p-values are greater than 0.01, then the random sequence has good randomness. The pseudo-random sequences Z are obtained by the chaotic sequences X, and the results of NIST test for pseudo-random sequences Z are shown in Table VI, i.e., most tests of NIST are passed. Similarly, the results of NIST test for pseudo-random sequences W are shown in Table VII, and all the p-values are greater than 0.01, so the NIST test is passed.

VI. CONCLUSION

Through the combined controllers of trigonometric function, a class of asymptotically stable nominal linear systems are controlled to be hyperchaotic system, and a 11-dimensional hyperchaotic systems with 9 positive Lyapunov exponents is constructed. Meanwhile, an encryption algorithm of scrambling, sequential diffusion and inverse diffusion is designed based on the new hyperchaotic system. The encryption algorithm has many key parameters and initial values, and the key is related to plaintext information. To some extent, it has a large enough key space and can resist exhaustive attack and chosen-plaintext attack, etc. An example of image encryption is given by the simulation experiments, and it shows that the encryption algorithm based on higher-dimensional hyperchaotic system is feasible, effective and secure. Therefore, the chaos-based encryption algorithm can be applied to the secure communication in the near future, such as the encryption of images, video and other multimedia information.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions. This research was supported by the National Natural Science Foundation of China (Grant No. 11847051), the Natural Science Foundation of Fujian Province of China (Grant Nos. 2022J01895 and 2019J05107), Fujian Key Laboratory of Granular Computing and Applications, Institute of Meteorological Big Data-Digital Fujian and Fujian Key Laboratory of Data Science and Statistics (Minnan Normal University), China.

REFERENCES

[1] K. M. Hosny, S. T. Kamal, and M. M. Darwish, "A color image encryption technique using block scrambling and chaos," *Multimedia Tools and Applications*, vol. 81, no. 1, pp. 505–525, 2022.

[2] Z. Madouri, N. H. Said, and A. A. Pacha, "Image encryption algorithm based on digital filters controlled by 2d robust chaotic map," *Optik*, vol. 264, p. 169382, 2022.

[3] K. Jain, A. Aji, and P. Krishnan, "Medical image encryption scheme using multiple chaotic maps," *Pattern Recognition Letters*, vol. 152, pp. 356–364, 2021.

[4] M. Hamdi, J. Miri, and B. Moalla, "Hybrid encryption algorithm (HEA) based on chaotic system," *Soft Computing*, vol. 25, no. 3, pp. 1847–1858, 2021.

[5] Y. Zhao and L. Liu, "A bit shift image encryption algorithm based on double chaotic systems," *Entropy*, vol. 23, no. 9, p. 1127, 2021.

[6] J. Chen, D. Yan, S. Duan, and L. Wang, "Memristor-based hyper-chaotic circuit for image encryption," *Chinese Physics B*, vol. 29, no. 11, p. 110504, 2020.

[7] D. S. Malik and T. Shah, "Color multiple image encryption scheme based on 3d-chaotic maps," *Mathematics and Computers in Simulation*, vol. 178, pp. 646–666, 2020.

[8] S. Liu, C. Li, and Q. Hu, "Cryptanalyzing two image encryption algorithms based on a first-order time-delay system," *IEEE MultiMedia*, vol. 29, no. 1, pp. 74–84, 2022.

TABLE VI. NIST Test of Pseudo-Random Sequences Z

Test Items	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	Z_7	Z_8	Z_9	Z_{10}	Z_{11}
Frequency	0.9832	0.4348	0.6943	0.9944	0.2191	0.1228	0.1473	0.2878	0.1636	0.4208	0.5707
Frequency within a Block	0.8171	0.8927	0.7162	0.5393	0.4954	0.6526	0.9727	0.8223	0.3696	0.6062	0.2408
Runs	0.0677	0.8830	0.6384	0.3477	0.0061	0.9138	0.2216	0.2231	0.1433	0.3569	0.3886
Longest-Run-of-ones	0.8324	0.1244	0.3561	0.1394	0.9312	0.1289	0.6307	0.2157	0.6795	0.3849	0.4017
Binary matrix rank	0.0171	0.0000	0.0100	0.0171	0.0000	0.0000	0.0001	0.0000	0.0000	0.0555	0.0000
Discrete fourier transform	0.8618	0.7496	0.8846	0.9076	0.9076	0.6014	0.0519	0.1468	0.5617	0.5045	0.4333
Non-overlapping template matching	0.4893	0.7417	0.0216	0.3558	0.4551	0.8057	0.9046	0.2643	0.9285	0.6491	0.6057
Overlapping template matching	0.7772	0.4224	0.8261	0.2226	0.6515	0.2850	0.1263	0.3467	0.6426	0.1901	0.1616
Maurer's universal statistical	0.5107	0.7102	0.0458	0.4620	0.8034	0.1403	0.6694	0.8622	0.5631	0.1625	0.0324
Linear complexity	0.3866	0.7242	0.5818	0.4825	0.2231	0.2128	0.1809	0.7538	0.6493	0.7724	0.0120
Serial	0.6960	0.2418	0.3559	0.9198	0.0830	0.6367	0.1989	0.0726	0.0009	0.2406	0.0984
Approximate entropy	0.6596	0.8243	0.5361	0.1740	0.6640	0.9041	0.1823	0.5347	0.6192	0.2154	0.6175
Cumulative sums	0.8460	0.9963	0.5493	0.7691	0.7876	0.9185	0.9963	0.5493	1.0000	0.0807	0.2471
Random excursions	0.7036	0.3428	0.5153	0.5799	0.6196	0.6665	0.3548	0.1823	0.4403	0.8451	0.1190
Random excursions variant	0.4867	0.1584	0.2085	0.6523	0.5079	0.6144	0.6058	0.3360	0.1458	0.7315	0.0500

TABLE VII. NIST Test of Pseudo-Random Sequences W

Test Items	W_1	W_2	W_3	W_4	W_5
Frequency	0.5035	0.2368	0.5452	0.8407	0.4139
Frequency within a Block	0.0971	0.0691	0.9898	0.9419	0.4977
Runs	0.2244	0.7435	0.9714	0.2807	0.4323
Longest-Run-of-ones	0.6785	0.2117	0.1600	0.5415	0.5751
Binary matrix rank	0.1087	0.2395	0.0560	0.0116	0.2666
Discrete fourier transform	0.5814	0.7277	0.4333	0.8390	0.5423
Non-overlapping template matching	0.0649	0.0876	0.8835	0.7137	0.7514
Overlapping template matching	0.4290	0.0828	0.2784	0.7073	0.9158
Maurer's universal statistical	0.9723	0.6845	0.2071	0.6439	0.1407
Linear complexity	0.9124	0.1711	0.8215	0.1285	0.2014
Serial	0.6145	0.7881	0.2658	0.1512	0.1737
Approximate entropy	0.9262	0.6077	0.7772	0.6742	0.3726
Cumulative sums	0.9998	0.5579	1.0000	0.7036	0.1673
Random excursions	0.6888	0.9516	0.9058	0.8177	0.7348
Random excursions variant	0.9562	0.6307	0.9703	0.9804	0.6885

[9] H. Fan, H. Lu, C. Zhang, M. Li, and Y. Liu, "Cryptanalysis of an image encryption algorithm based on random walk and hyperchaotic systems," *Entropy*, vol. 24, no. 1, p. 40, 2021.

[10] W. Liu, K. Sun, and S. He, "SF-SIMM high-dimensional hyperchaotic map and its performance analysis," *Nonlinear Dynamics*, vol. 89, no. 4, pp. 2521–2532, 2017.

[11] C. Shen, S. Yu, J. Lü, and G. Chen, "A systematic methodology for constructing hyperchaotic systems with multiple positive lyapunov exponents and circuit implementation," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 61, no. 3, pp. 854–864, 2013.

[12] C. Chen, K. Sun, and S. He, "A class of higher-dimensional hyperchaotic maps," *The European Physical Journal Plus*, vol. 134, no. 8, pp. 1–13, 2019.

[13] C. Shen, S. Yu, J. Lü, and G. Chen, "Constructing hyperchaotic systems at will," *International Journal of Circuit Theory and Applications*, vol. 43, no. 12, pp. 2039–2056, 2015.

[14] Z. Peng, W. Yu, J. Wang, Z. Zhou, J. Chen, and G. Zhong, "Secure communication based on microcontroller unit with a novel five-dimensional hyperchaotic system," *Arabian Journal for Science and Engineering*, vol. 47, no. 1, pp. 813–828, 2022.

[15] E. Yavuz, R. Yazıcı, M. C. Kasapbaşı, and E. Yamaç, "A chaos-based image encryption algorithm with simple logical functions," *Computers & Electrical Engineering*, vol. 54, pp. 471–483, 2016.

[16] F. Özkaynak and A. B. Özer, "Cryptanalysis of a new image encryption algorithm based on chaos," *Optik*, vol. 127, no. 13, pp. 5190–5192, 2016.

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

[18] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-Box," *Chaos, Solitons & Fractals*, vol. 95, pp. 92–101, 2017.

[19] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption

based on hybrid hyper-chaotic system and cellular automata," *Optics and Lasers in Engineering*, vol. 90, pp. 225–237, 2017.

[20] S. Zhu, C. Zhu, and W. Wang, "A new image encryption algorithm based on chaos and secure hash sha-256," *Entropy*, vol. 20, no. 9, p. 716, 2018.

[21] A. Gupta, D. Singh, and M. Kaur, "A novel image encryption using memetic differential expansion based modified logistic chaotic map," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 7, 2019.

[22] M. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A novel chaos based optical image encryption using fractional fourier transform and dna sequence operation," *Optics & Laser Technology*, vol. 121, p. 105777, 2020.

[23] I. AlBidewi and N. Alromema, "Ultra-key space domain for image encryption using chaos-based approach with DNA sequence," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 5, 2021.

[24] L. Chen, C. Li, and C. Li, "Security measurement of a medical communication scheme based on chaos and DNA coding," *Journal of Visual Communication and Image Representation*, vol. 83, p. 103424, 2022.

[25] M. I. Moussa, E. I. Abd El-Latif, and N. Majid, "Enhancing the security of digital image encryption using diagonalize multidimensional nonlinear chaotic system," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 1, 2022.

[26] S. T. Liu and L. Zhang, "Surface chaos-based image encryption design," in *Surface Chaos and Its Applications*. Springer, 2022, pp. 321–346.

[27] 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.

[28] C. Shen, S. Yu, J. Lü, and G. Chen, "Designing hyperchaotic systems with any desired number of positive lyapunov exponents via a simple model," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 61, no. 8, pp. 2380–2389, 2014.

[29] J. He and S. Yu, "Construction of higher-dimensional hyperchaotic systems with a maximum number of positive lyapunov exponents under average eigenvalue criteria," *Journal of Circuits, Systems and Computers*, vol. 28, no. 09, p. 1950151, 2019.

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

[31] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[32] 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, no. 9, pp. 4370–4406, 2021.

[33] 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.

[34] 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.

[35] J. Gayathri and S. Subashini, "An efficient spatiotemporal chaotic image cipher with an improved scrambling algorithm driven by dynamic diffusion phase," *Information Sciences*, vol. 489, pp. 227–254, 2019.

[36] R. Guesmi and M. Farah, "A new efficient medical image cipher based on hybrid chaotic map and dna code," *Multimedia tools and applications*, vol. 80, no. 2, pp. 1925–1944, 2021.

[37] J. Cai and J. He, "A new hyperchaotic system generated by an external periodic excitation and its image encryption application," *Journal of Advanced Computational Intelligence and Intelligent Informatics*, vol. 26, no. 3, pp. 418–430, 2022.

[38] 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.

[39] 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.

[40] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert *et al.*, "Nist special publication 800-22: A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications," *NIST Special Publication*, vol. 800, p. 22, 2010.