Hyperchaotic Image Encryption System Based on Deep Learning LSTM

Shuangyuan Li[1], Mengfan Li[2], Qichang Li[3], Yanchang Lv[4]
Information Construction Office, Jilin Institute of Chemical Technology, Jilin, China[1]
School of Information and Control Engineering, Jilin Institute of Chemical Technology, Jilin, China[2, 3, 4]

***Abstract*—This paper introduces an advanced method for enhancing the security of image transmission. It presents a novel color image encryption algorithm that combines hyperchaotic dynamics and deep learning medium and long short-term memory (LSTM) networks. Firstly, the chaotic sequence is generated using the Lorenz hyperchaotic system, then the Lorenz chaotic system is discretized and iteratively processed using the fourth-order Runge-Kutta (RK4) method, and then the deep learning LSTM model is used to transform the chaotic sequence processed by the Lorenz hyperchaotic system into a new sequence for training. Finally, according to the new chaotic signal, the Arnold disruption and Deoxyribo Nucleic Acid (DNA) encoding double disruption diffusion are performed to derive the ultimate encrypted image. Through the analysis of multiple color image simulation experiments, the algorithm presented in this paper can well realize the encryption on color images and can achieve lossless encryption, with strong resistance to differential attack, statistical attack and violent attack. Compared with the literature analysis, the correlation coefficient, information entropy and pixel change rate of this paper are closer to the ideal value, and it has higher security and better encryption effect.**

Keywords*—Image encryption; Lorenz Chaotic System; LSTM model; deep learning; DNA encoding

I. Introduction

With the advancement of information technology, big data, 5G and cloud computing technologies are inseparable from many areas of daily life, such as education, military, medicine and scientific conferences. However, while the Internet has brought great convenience, large amounts of data face numerous challenges, such as espionage, theft, usurpation, and modification, leading to numerous information security incidents. One such area is digital images, where the transmission of image data is an integral part of Artificial Intelligence (AI) systems. Through the use of image encryption technology, images can be encrypted so that they are not easily stolen or tampered with during transmission, thus ensuring the security of transmission. In the field of AI, personal image data, such as face recognition and human posture recognition, plays a significant role. Image encryption technology can be used to encrypt and protect these sensitive image data to ensure the security of personal privacy.

As an important carrier of information, digital image is a two-dimensional image composed of discrete pixels (picture element), each pixel represents a point in the image with specific position, brightness and color information. They can be generated by digital cameras, scanners or computers, and stored and processed in digital form. They contain important information in areas such as defense medicine, and education [1]. To guarantee the security of the transmission process, the most effective way is encryption. Traditional encryption methods include symmetric encryption, which is one of the earliest and simplest encryption methods that performs encryption and decryption operations on plaintext by using the same key, and some of the most commonly used symmetric encryption algorithms include the Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), and others [2]. Symmetric encryption offers the benefits of excellent efficiency and high speed, but it needs to secure the key transmission process. Asymmetric encryption, also known as public key encryption, involves a public key that can be used by anyone to encrypt data, while the private key is retained exclusively by the key holder for decrypting the data. Prominent asymmetric encryption methods encompass Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC), Digital Signature Algorithm (DSA) [3]. These algorithms are primarily developed for text-based application information and are less efficient in encrypting images with high image pixel correlation and extensive redundancy. It is difficult for traditional image encryption methods to overcome the difficulties in key distribution, resulting in illegal theft of ciphertext and low security. Deep learning algorithms have high complexity, good chaos characteristics and strong parameter sensitivity, and can be applied in the field of image encryption. Therefore, this paper, we investigate image encryption algorithms for chaotic systems with more complex performance and higher security.

II. Current Status of Research

With the dissemination of digital images in the network, the security of digital images has emerged as a significant concern [4]. To enhance data security, numerous image encryption algorithms have been introduced, including those based on chaotic systems [5], compression perception [6], DNA coding [7], S-box transform [8] and transform domain [9]. In the 1960s, Lorenz, a scientist from Massachusetts Institute of Technology (MIT) in the United States, proposed chaotic system for the first time, and attracted widespread attention and research, and scholars from various countries gradually utilized chaotic systems in picture encryption. In 1997, Fridrich pioneered the application of chaotic systems in image encryption for the inaugural time [10]. Usually, chaos-based image encryption algorithm mainly consists of disarray and diffusion, disarray is to diminish the correlation between adjacent pixels in a plaintext picture by changing the spatial

position between pixels, and diffusion refers to changing the pixel value of an image.

Chaotic systems are a class of dynamic nonlinear systems that exhibit non-stationarity, unpredictability and strong sensitivity. Due to their unpredictability and complexity they are widely used in information security and random number generation. Chaotic signal as the core of chaotic image encryption consists of the following two kinds of chaotic systems: one is a one-dimensional chaotic system, a nonlinear dynamical system containing only one independent variable, such as Logistic mapping, Henon mapping, Sine mapping, etc., which is simple in structure, high in operational efficiency, and has different dynamical characteristics, but the system key space is small and vulnerable to attacks, and can be determine the chaotic characteristics by analyzing the bifurcation map, periodicity and so on. Another kind of chaotic system is multi-dimensional chaotic system, which contains multiple variables and has more complex and diversified dynamics characteristics, such as Lorenz system, Chen system, etc. These systems introduce more state variables, have higher complexity and heightened sensitivity to starting conditions, making them prevalent in the realm of image encryption.

In order to enhance the security of image encryption, Alghamdi Yousef and Munir Arslan proposed an encryption algorithm with a nonlinear feedback shift register in their literature [11]. This algorithm improves security through multiple rounds of encryption, row substitution, column substitution, and bit-level substitution, resulting in higher quality and efficiency. The paper provides detailed insights into how the algorithm achieves these improvements. Chen Xin et al. proposed the algorithm of quantum chaos and DNA coding in literature [12], by studying the properties of IEA-QCDC, plaintext attack was used to obtain the key, and DNA coding operation was used to obtain the encrypted image, making full use of the security defects of IEA-QCDC and achieving better encryption effect. Ding Dawei, Wang Jin et al. proposed a fractional-order amnesia-coupled chaotic mapping (MCCM), using internal parameters, to make the system more stable and more conducive to the application in the field of chaotic engineering, through experimental analysis, the system exhibits a heightened level of dynamic complexity, leading to the development of a secure medical picture encryption scheme, which provides technical support for the security of the medical field, with good security and robustness [13]. Liang Qin et al. tackled the problem of insufficient security in one-dimensional chaotic systems. They introduced a novel one-dimensional chaotic system with the aim of bolstering security. They introduced a new one-dimensional chaotic system designed to enhance security. This new system, known as one-dimensional sine-cosine chaotic mapping (SCCM), leverages index mismatch of chaotic sequences in image rows and columns, and incorporates random DNA code selection to enhance the encryption process's resistance against plaintext attacks, resulting in improved encryption effectiveness [14]. Francesco Castro et al. introduced a secure fingerprint authentication image encryption scheme. The primary objective of this scheme is to bolster the security and resilience of safeguarding medical images. To address the issue of medical image insecurity during transmission and safeguard patient privacy, the scheme employs chaotic encryption with a replacement key for encrypting private images. Additionally, it implements a hybrid encryption approach based on the ECC and AES, resulting in improved security [15]. Meanwhile, as deep learning technology continuously advances, more algorithms that utilize the fusion of deep learning and chaotic systems are widely used. Ulises Manuel Ramirez Alcocer et.al introduced a deep learning approach that utilizes the LSTM network to monitor medical processes. This approach has been found to yield improved results in the medical field [16].

To summarize the state of multi-dimensional chaotic systems and the extensive application of deep learning, this paper introduces a novel approach that leverages LSTM networks to generate new chaotic signals. These signals are subsequently applied in chaotic systems and iterated using Lorenz mapping to create pseudo-random sequences. The algorithm further employs the Arnold algorithm and DNA coding for double disruption to enhance security. This leads to an expanded key space and increased resistance to attacks. Compared with the reference [17], the original equalization method using 3D histogram is discarded, and the LSTM model, which has better performance in long sequences, is used to enhance the sequence complexity. The traditional encryption method is only related to the image pixel arrangement, and the encryption is too single and simple, this paper increases the number of parameters through the addition of deep learning LSTM, so that the chaotic system reaches a super chaotic state, and at the same time, constructs the DNA encoding rules, which ultimately affects the factors to increase, and improves the security of the algorithm, as well as the encryption efficiency, and has a higher value of using it in the confidentiality.

III. BASIC THEORY

A. Lorenz Chaotic System

Lorenz chaotic system is a three-dimensional nonlinear system of ordinary differential equations, which is composed of three coupled nonlinear differential equations with good chaotic properties and initial value sensitivity, and is often widely used as a classical pseudorandom generator in the field of image encryption [18]. The Lorenz system is defined as depicted in Eq. (1).

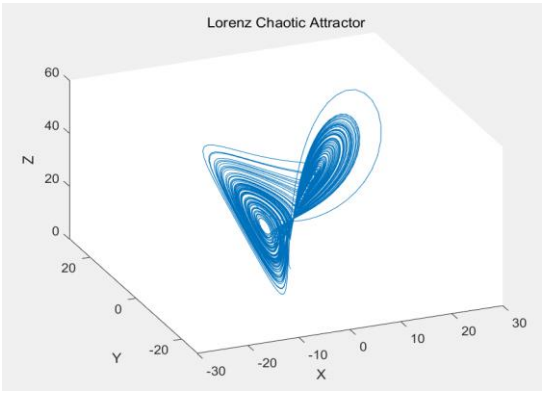


Fig. 1. Phase diagram of hyperchaotic lorenz attractor.

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

where, $\dot{x}$, $\dot{y}$, $\dot{z}$, $\dot{w}$ are the chaotic states of the system, for the control parameters a, b, c and r of the Lorenz system, when these parameters satisfy a=10, b=8/3, c=28, and $-1.52 \leq r \leq -0.06$, the system enters a state of hyperchaotic. The attractor phase diagram of the hyperchaotic Lorenz system can be observed in Fig. 1. When the system control parameter r=-1, the Lyapunov exponents in Eq. (1) are as follows in order: 0.3381, 0.1586, 0, and -15.1752. Notably, this sequence contains two Lyapunov exponents greater than zero. The chart of the Lyapunov exponent diagram is shown in Fig. 2.

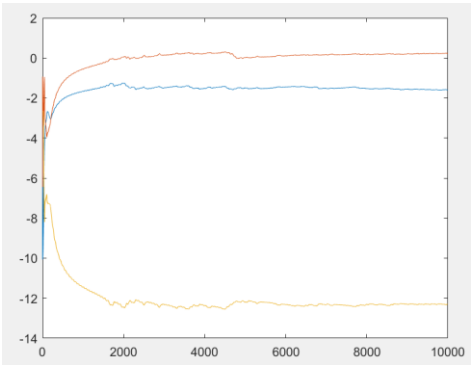


Fig. 2. Lyapunov exponent plot.

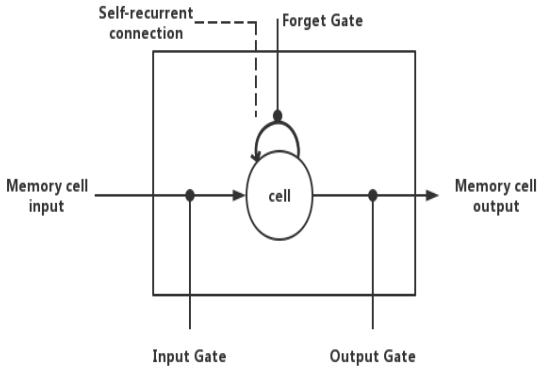


Fig. 3. LSTM model diagram.

B. LSTM Model

LSTM can be viewed as a specialized variant of Recurrent Neural Network (RNN), primarily developed to address the challenges related to gradient vanishing and gradient explosion when training with lengthy sequences [19]. LSTM's unique architecture and memory retention mechanisms make it particularly well-suited for a wide range of applications. RNN is a kind of neural network dealing with sequential data. Based on the RNN model, the LSTM model introduces a gating mechanism (Gates) to solve the short-term memory problem of RNN, which is able to capture long-term dependencies, thus enabling the recurrent neural network to better leverage long-range temporal information and have better performance in longer sequences. The LSTM model includes three key logical control units: the Input Gate, Output Gate, and Forgetting Gate. These units are connected to a multiplication element, forming the core structure of the LSTM model, as illustrated in Fig. 3. These components play a crucial role in controlling information flow and memory retention within the network, allowing it to excel in tasks involving longer sequences.

The cell is a memory unit that represents the memory of the neuron's state, providing the LSTM unit with the capability to store, retrieve, reset, and update long-term information. When the moment t, the LSTM neural network defines the formula as:

$$\begin{aligned} f_t &= \text{sigmid}\left(W_f \cdot [h_{t-1}, x_t] + b_f\right) \\ i_t &= \text{sigmid}(W_i \cdot [h_{t-1}, x_t] + b_i) \\ o_t &= \text{sigmid}(W_o \cdot [h_{t-1}, x_t] + b_o) \\ \tilde{c}_t &= \tanh(W_c \cdot [h_{t-1}, x_t] + b_c) \\ c_t &= f_t \times c_{t-1} + i_t * \tilde{c}_t \\ h_t &= o_t \times \tanh(c_t) \end{aligned} \tag{2}$$

where, f_t、i_t、o_t and c_t denote Forget Gate, Input Gate, Output Gate, and cell, respectively, as mentioned in Fig. 3. W_*, on the other hand, denotes the recursive connection weights of the corresponding gates, respectively, and sigmid and tanh denote the two activation functions.

C. Arnold Mapping

Arnold mapping is a chaotic mapping technique that repeatedly applies folding and stretching transformations within a bounded region, serving as a primary method for permutation. The transformation principle involves performing a shearing transformation along the x-axis, followed by a similar transformation along the y-axis. Finally, a modulo operation is used to implement cut-and-fill operations, altering the layout of image grayscale values by changing the pixel coordinates. The specific transformation formula is:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} mod \begin{pmatrix} M \\ N \end{pmatrix} \tag{3}$$

D. DNA Coding

In the field of biology, medicine and other applications, the information of many organisms in nature exists in DNA, and DNA can be arranged according to different rules and sequences to achieve the effect of disarray through the disarrangement of rows and columns. DNA consists of four kinds of DNA, which are adenine (A), thymine (T), guanine (G) and cytosine (C). In accordance with the rules of complementary base pairing in biology, A is paired with T, while G is paired with C. In computer systems, the complementarity of the two bases is determined by the fact that they are complementary to each other. In a computer system, the complementary pairing rules are similar to the pairing rules for binary coding, 0 and 1. Therefore, the four varieties of deoxyribonucleotides can be denoted using two binary digits, yielding a sum of 24 feasible codes. However, only eight coding rules, in accordance with DNA coding standards, are retained, as shown in Table I [20]. Every pixel in a grayscale image can be denoted using 8-bit binary numbers consisting of 0 and 1. Similarly, each pixel value can be encoded using a DNA sequence comprising four nucleotides. As an illustration,

the decimal number 232 can be expressed in binary as 11101000, and following the DNA coding rules, this binary sequence can be converted to the DNA sequence TGGA.

In the process of image encryption, DNA arithmetic rules are employed, encompassing DNA addition, DNA subtraction, and DNA dissimilarity operations. Adding and subtracting DNA sequences follow similar principles to traditional algebraic calculations [21], and the rules for these arithmetic operations are provided in Table II and Table III.

TABLE I. DNA CODING RULES

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

TABLE II. DNA ADDITION RULES

+	A	T	C	G
A	A	T	C	G
G	G	C	T	A
T	T	A	G	C
C	C	G	A	T

TABLE III. DNA SUBTRACTION RULES

-	A	T	C	G
A	A	T	C	G
G	G	G	C	A
T	T	T	A	C
C	C	C	G	T

IV. IMAGE ENCRYPTION

A. Encryption Algorithm

The image encryption algorithm presented in the paper follows the traditional rules of disarray and diffusion, and proposes a double disarray by combining Arnold mapping and DNA encoding. During the encryption process, the initial key of the original image P is first obtained using a hash function. Following this, a chaotic sequence is produced using the hyperchaotic Lorenz system, and the system is subjected to discretization and iterative processing using the Runge-Kutta method. The deep learning LSTM model is utilized to leverage temporal features for both training and analyzing the chaotic sequence, ultimately generating a novel chaotic sequence. Finally, double permutation is applied to shuffle and diffuse the pixels, resulting in the ultimate encrypted image. The primary encryption procedure of the algorithm are illustrated in Fig. 4.

B. Encryption Process

1) Key generator: The key for the plaintext image P is determined through the SHA-256 function, which serves as the fundamental component of the key generator. First take the plaintext image P as input, use the function to generate a 64-bit digest, convert it to 256-bit binary as output, and divide it into groups of every 8 bits to get a 32-bit segmented keystream $K = \{k_1, k_2, k_3, \cdots k_{32}\}$, where k_i, $i = 1,2,\cdots 32$ are all 8-bit hash values.

According to the generation rule of key flow, K is processed as follows, according to Eq. (4) to Eq. (7), the initial state parameters of the system $\{x_0, y_0, z_0, w_0\}$ can be computed, and through Eq. (8), we get the key s_0 which is related to the plaintext, and then we generate pseudo-random sequences S_1 , S_2 used for the subsequent Arnold diffusion.

$$x_0 = \left((k_{17} \oplus k_{18}) \oplus (k_{18} \oplus k_{19}) \oplus (k_{19} \oplus k_{20})\right) \times \sum_{j=1}^{j=32} \frac{k_j \times 2^{j-1}}{2^{47}} \quad (4)$$

$$y_0 = \left((k_{21} \oplus k_{22}) \oplus (k_{22} \oplus k_{23}) \oplus (k_{23} \oplus k_{24})\right) \times \sum_{j=1}^{j=32} \frac{k_j \times 2^{j-1}}{2^{47}} \quad (5)$$

$$z_0 = \left((k_{25} \oplus k_{26}) \oplus (k_{26} \oplus k_{27}) \oplus (k_{27} \oplus k_{28})\right) \times \sum_{j=1}^{j=32} \frac{k_j \times 2^{j-1}}{2^{47}} \quad (6)$$

$$w_0 = ((k_{29} \oplus k_{30}) \oplus (k_{30} \oplus k_{31}) \oplus (k_{31} \oplus k_{32})) \times \sum_{j=1}^{j=32} \frac{k_j \times 2^{j-1}}{2^{47}} \quad (7)$$

$$s_0 = \text{zeros}(1, n), n = 2MN \quad (8)$$

2) Preprocessing: The RK4 is a suitable method for solving differential equations. It achieves higher computational accuracy by approximating the differential equations in four discrete steps over a specific time interval of the solution. The discretized equations are as follows:

$$\begin{aligned} x_{n+1} &= x_n + \frac{h}{6}(k_1 + 2k_2 + 2k_3 + k_4) \\ k_1 &= f(t_n, x_n) \\ k_2 &= f\left(t_n + \frac{h}{2}, x_n + \frac{h}{2}k_1\right) \\ k_3 &= f\left(t_n + \frac{h}{2}, x_n + \frac{h}{2}k_2\right) \\ k_4 &= f(t_n + h, x_n + hk_3) \end{aligned} \quad (9)$$

In this method, the subsequent value x_{n+1} is calculated by multiplying the current value x_n with the period h and reckon slope. The slopes are represented as follows: k_1 is the slope at the start of the period, k_2 and k_3 correspond to the slopes in the middle of time, and k_4 indicates the slope at the conclusion of the time period. The Lorenz chaotic system is discretized using RK4 and iterated T+MN times, discarding the first T times to eliminate transient effects and increase safety, four new sequences x_1, y_1, z_1, w_1 are obtained.

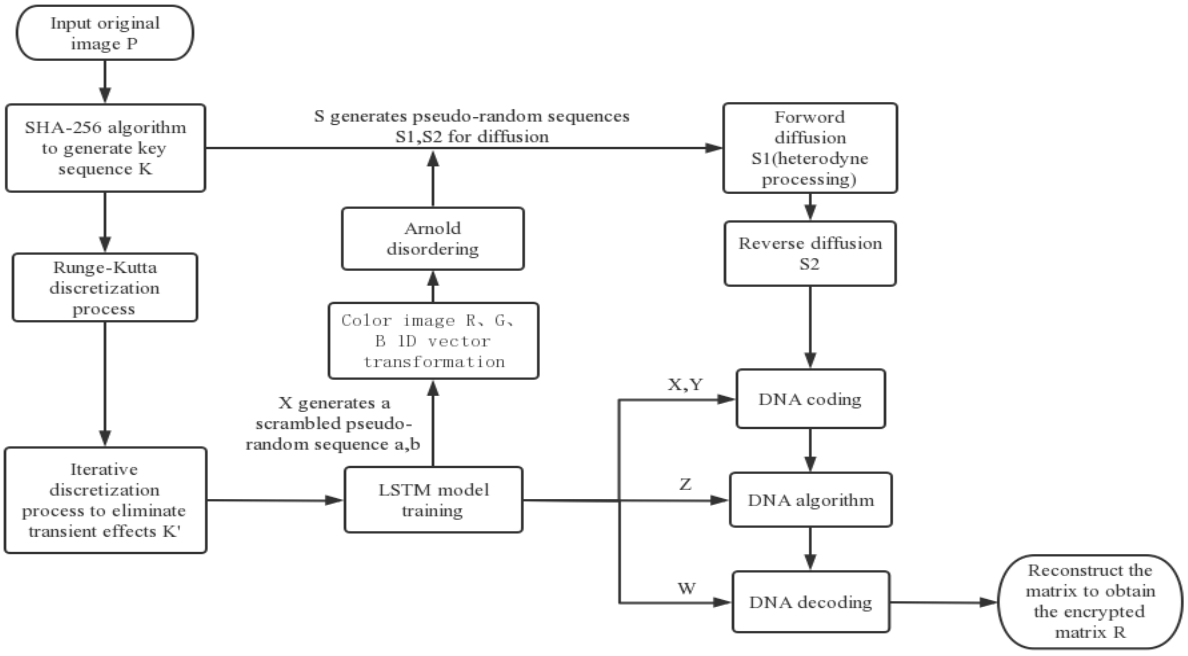


Fig. 4. Encryption flow chart.

3) LSTM training: By configuring the parameters of LSTM, the preprocessed sequences are trained, and a portion of the length l of the pseudo-random sequences x_1, y_1, z_1, w_1 are respectively selected for deep learning. The initial learning rate is represented as 'r', the learning rate decreasing factor is 'p', and the length of the selected training sequences is 'l'. Following the completion of the training process, four novel pseudo-random sequences, namely X, Y, Z, and W, are generated. During the training process, the root-mean-square error (RMSE) serves as a more effective metric for quantifying the disparity between predicted and actual values. It offers heightened sensitivity to anomalous data and is defined as the square root of the average of the squared differences between the predicted and actual values, divided by the number of observations, denoted as n. In Fig. 5, the RMSE is depicted as it evolves with the number of iterations during the training process. As the number of iterations increases, the RMSE becomes smaller and gradually approaches 0, signifying that the model can make more accurate data predictions.

4) Double disorder modeling: The color original image P, with dimensions M×N, is separated into three individual color channels: R, G, and B. The pseudo-random sequences a, b are generated using LSTM generated sequences X. The decomposed channels are initially converted into one-dimensional vectors, and then transformed into the coordinates using a, b to get the transformed coordinates q, as shown in Eq. (10), and then Arnold disambiguation is carried out.

$$\begin{aligned} a &= X(1:M*N) \\ b &= X(M*N+1:2*M*N) \\ q &= mod(b(i)+a(i)*i, M*N)+1 \end{aligned} \tag{10}$$

After disorganization, the key S_1, S_2 obtained in the key generation stage is used for forward and reverse diffusion according to Eq. (11) and Eq. (12) to obtain the new single-channel image. The key S_1 is used for forward diffusion, which is a kind of diffusion processing method based on different-or operation, and S_2 is the key for reverse diffusion, where B_i represents the three channels R, G, B, and B_i' represents the new R, G, B channels.

$$\begin{aligned} B_i &= (B_{i-1}+S_1+P_i) mod 256 \\ C_i &= (C_{i+1}+S_2+B_i) mod 256 \end{aligned} \tag{11}$$

$$B_i' = reshape(C_i, M, N) \tag{12}$$

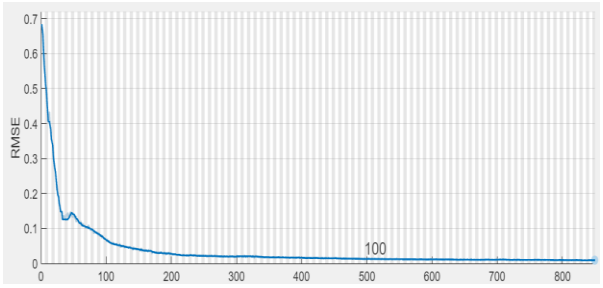


Fig. 5. RMSE variation curve.

Through DNA encoding, the bases A, T, G, C and the binary pixel values are disambiguated according to certain rules, which consumes less time and has a strong disambiguation effect and is highly applicable in image data encryption [22]. Each chunk of the graphic representation P is encoded according to the rules in Table I, and the encoding rules are determined by the pseudo-random sequence X to get the matrix P_i'. The obtained new three single channels are encoded according to Y to get the disarrayed matrix Q_i'. The encoded chunks are subjected to the DNA operation of P_i' and

Q_i' in accordance with the rules established by the sequence Z, and the encrypted matrix Q_i is obtained. Finally, DNA decoding of Q_i is performed using W. Each chunk are combined to create the ultimate encrypted image Q .

C. Decryption Process

The decryption process is the inverse application of the encryption. The individual channels of the encrypted picture are isolated, and the separated image is subjected to DNA coding inverse disambiguation, plus mode inversion, forward inverse diffusion. The Arnold inverse transformation is employed to extract the individual channels from the plaintext image, and subsequently, these channels are reconstructed and combined to obtain the original plaintext P.

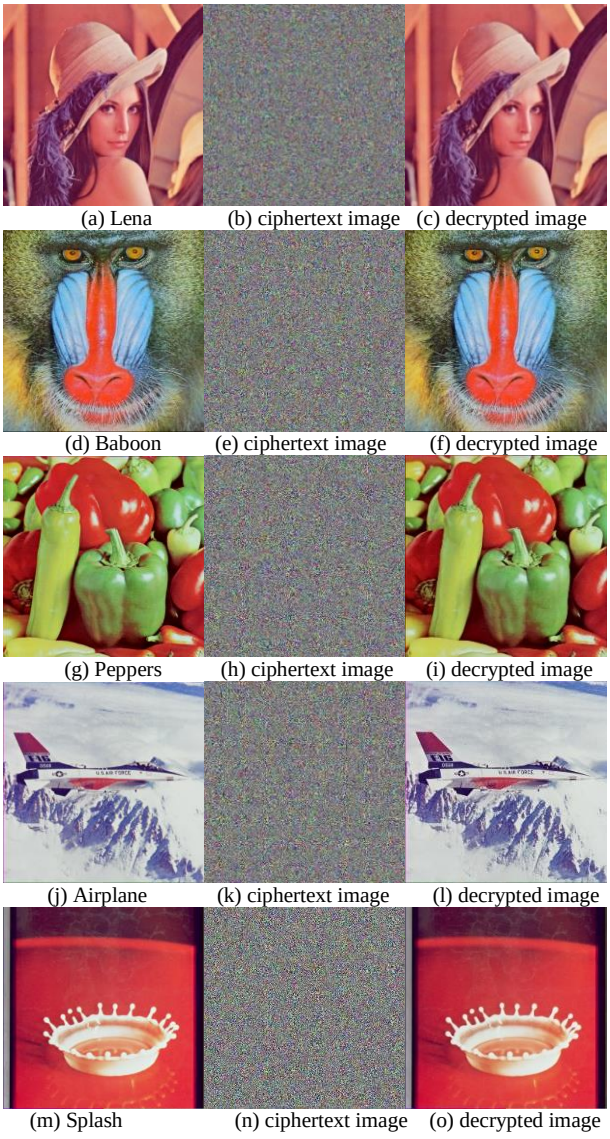
V. Encryption Effect Analysis

In this paper, we employ the MATLAB R2022b simulation platform to carry out encryption and decryption operations using the proposed algorithm, and we analyze its performance. The hardware specifications during the experiments include an Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz, 1.80 GH. The experiments were conducted using 512×512 pixel color images of Lena, Baboon, Peppers, Airplane, and Splash color images for simulation testing. And the tests are performed in terms of histogram analysis, adjacent pixel correlation analysis, information entropy, differential attack analysis, robustness analysis and key space analysis. Fig. 6 shows the encryption and decryption effect of the color image, the encrypted image is entirely devoid of any visible information from the original image, making it impossible for an attacker to extract any meaningful data from the image, enough to resist the common means of attack such as differential attack, violence attack, and the algorithm yields a strong encryption effect.

A. Histogram Analysis

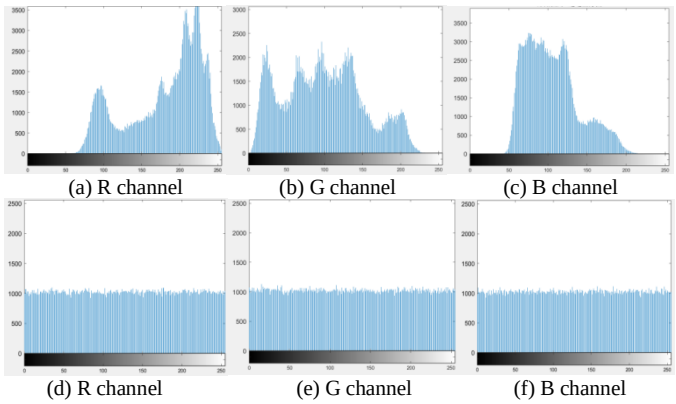
Histograms can display image information and offering a visual representation of the arrangement of individual grayscale values in picture. The frequency of occurrence is counted according to the size of the gray values. A better encryption algorithm should ideally render the histogram of the encrypted image so indistinct that a clear distinction cannot be discerned, the histogram can be evenly distributed. Histograms of plaintext images often exhibit clear statistical patterns, and attacks that exploit these patterns are known as statistical attacks [23]. To enhance the ability to resist statistical attacks, the histogram of the encrypted image should tend to a straight line, and there is a big difference between it and the plaintext histogram. For example, Fig. 7 shows the comparison of histograms before and after Lena's encryption.

From the above figure, it is evident that the pixels between the original plaintext images have strong statistical regularity and are more susceptible to statistical attacks, the distribution of elements in the encrypted Lena image exhibits greater uniformity, the encrypted histogram is smoother, and making it difficult to extract information from the encrypted image, thus enhancing security and increasing resistance to statistical attacks by potential attackers.



(a) Lena (b) ciphertext image (c) decrypted image
(d) Baboon (e) ciphertext image (f) decrypted image
(g) Peppers (h) ciphertext image (i) decrypted image
(j) Airplane (k) ciphertext image (l) decrypted image
(m) Splash (n) ciphertext image (o) decrypted image

Fig. 6. Encryption and decryption effect diagram.



(a) R channel (b) G channel (c) B channel
(d) R channel (e) G channel (f) B channel

Fig. 7. Histograms of lena images before and after R, G and B channel encryption: (a)-(c) Plaintext; (d)-(f) Ciphertext.

B. Correlation Analysis

During the image encryption process, the characteristics of image pixels make the correlation between neighboring pixels strong, and at the same time, it can disrupt the correlation between neighboring elements by disambiguating the pixels of the original picture, so as to achieve the purpose of resisting statistical attacks [24]. In a high-quality encryption algorithm, the lower the correlation between adjacent elements post-encryption, the more favorable the outcome. To evaluate an encryption algorithm's ability to withstand statistical attacks more effectively, we randomly selected 5000 pairs of pixel values from the Lena image in various orientations. And then examined the correlation coefficients in the three directions both before and after encryption, separately for the three single channels of the Lena image. The outcomes of this analysis are presented in Fig. 8, 9, and 10. This can be clearly seen from these pictures the strong correlations present in the plaintext image across all directions before encryption. However, post-encryption, the image exhibits a more uniform pixel distribution and scattered throughout the rectangular square matrix, there is no difference in the whole plane leading to a reduction in pixel-to-pixel correlations. The formula for calculating the correlation between two adjacent pixels can be expressed as follows:

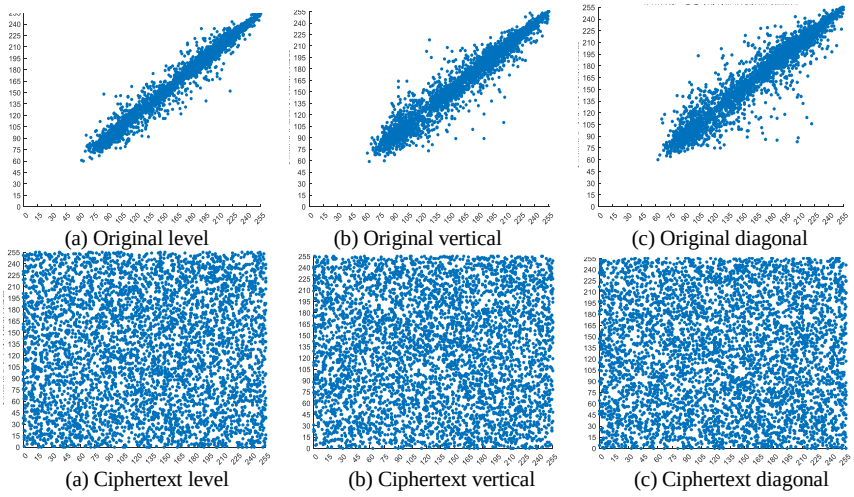
$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{13}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)^2 \tag{14}$$

$$\mathrm{cov}(x,y) = \frac{1}{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right) \tag{15}$$

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{16}$$

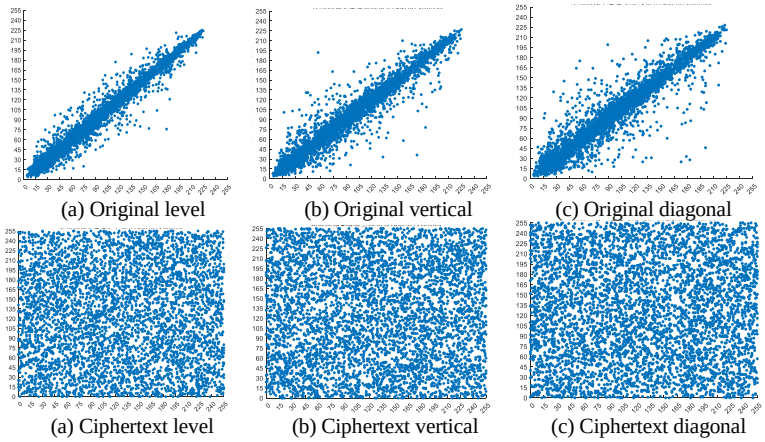
where $E(x)$ and $E(y)$ denote the mathematical expectation of x, y respectively, and $\mathrm{cov}(x,y)$ denotes the covariance of x, y . Through simulation test, compare and analyze the correlation coefficients before and after encryption of Lena and Baboon. Furthermore, a comparison was made with the correlations mentioned in the literature [25] [26], as shown in Table IV. The analysis reveals that the correlation of different channels (R, G, and B) in different directions before encryption is close to 1, indicating a higher correlation. In contrast, the correlation in the post-encryption image approaches the ideal value of 0. This algorithm offers a high level of security and exhibits enhanced resistance to statistical attacks.



(a) Original level (b) Original vertical (c) Original diagonal

(a) Ciphertext level (b) Ciphertext vertical (c) Ciphertext diagonal

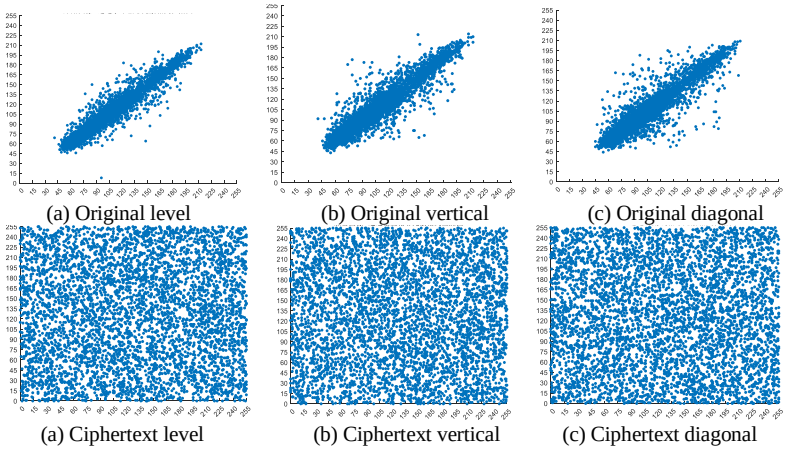
Fig. 8. Neighboring pixel correlation distribution before and after R-channel encryption of lena image.



(a) Original level (b) Original vertical (c) Original diagonal

(a) Ciphertext level (b) Ciphertext vertical (c) Ciphertext diagonal

Fig. 9. Distribution of neighboring pixel correlation before and after G-channel encryption of lena image.



(a) Original level (b) Original vertical (c) Original diagonal

(a) Ciphertext level (b) Ciphertext vertical (c) Ciphertext diagonal

Fig. 10. Distribution of correlation of neighboring pixels before and after encryption of B-channel of lena image.

TABLE IV. CORRELATION COEFFICIENTS OF DIFFERENT IMAGES IN THE THREE DIRECTIONS

Imagery	Directional	Lena			Baboon			Literature [25]	Literature [26]
		R	G	B	R	G	B		
Plaintext image	level	0.9805	0.9713	0.9387	0.9257	0.8673	0.9120	0.9726	0.9563
	vertical	0.9899	0.9836	0.9609	0.8664	0.7666	0.8852	0.9507	0.9242
	diagonal	0.9710	0.9565	0.9199	0.8531	0.7427	0.8510	0.9346	0.9015
Ciphertext image	level	-0.0036	0.0099	-0.0048	0.0022	-0.0488	0.0001	0.0042	0.0053
	vertical	0.0017	0.0182	0.0056	0.0024	-0.0146	-0.0046	0.0027	0.0059
	diagonal	-0.0036	0.0125	-0.0193	-0.0016	-0.0069	-0.0091	0.0070	0.0031

TABLE V. INFORMATION ENTROPY

Information entropy	R-channel		G-channel		B-channel	
Imagery	pre-encryption	post-encryption	pre-encryption	post-encryption	pre-encryption	post-encryption
Lena	7.2531	7.9993	7.5940	7.9993	6.9684	7.9993
Baboon	7.7067	7.9993	7.4744	7.9992	7.7522	7.9992
Peppers	7.3388	7.9993	7.4963	7.9993	7.0583	7.9994
Airplane	6.7178	7.9993	6.7990	7.9993	6.2138	7.9993
Splash	6.9481	7.9993	6.8845	7.9992	6.1265	7.9993

C. Information Entropy

Entropy is employed to characterize the intricacy of phenomena, and information entropy serves as a quantitative gauge of the level of randomness within a source, that is, it describes the complexity of a system. This metric can be applied to assess the randomness of an image by quantifying the dispersion of pixels with distinct grayscale values across different color channels. A distribution with higher uniformity indicates higher resistance to statistical attacks. Greater information entropy signifies increased complexity within the picture. An ideal encryption should possess an information entropy of 8. The calculation formula is:

$$H(x) = -\sum_{i=1}^{2N-1} P_i \log_2 P_i \quad (17)$$

In Eq. (17), P_i represents the occurrence rate of message i and $H(x)$ is the information entropy. Table V reveals that the information entropy of different channels in the encrypted image closely approaches the target value of 8. This suggests that the encrypted image significantly differs from the plaintext image and is less susceptible to leakage, thus indicating the algorithm in this paper has a higher level of security.

D. Differential Attack

A differential attack is one type of chosen plaintext attack, for a common method of cracking the ciphertext image, the attacker is able to the relationship between the picture before and after the encryption, to find out the law of the ciphertext image to be deciphered. The anti-differential performance mainly depends on the degree of sensitivity in the plaintext. In the encryption process, the Normalized Pixel Contrast Ratio (NPCR) and Unified Average Changing Intensity (UACI) are two variables to measure the two variables that quantify the disparity between two images and are quantitative tests to analyze the original and encrypted images [27]. NPCR measures the proportion of pixels that differ in the same positions between two images, relative to the total number of pixels in those images. UACI calculates the average magnitude

of changes between the images before and after transformations, and its formula is as follows:

$$NPCR = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} D(i,j)}{M \times N} \times 100\% \quad (18)$$

$$D(i,j) = f(x) = \begin{cases} 1, C_1(i,j) \neq C_2(i,j) \\ 0, otherwise \end{cases} \quad (19)$$

$$UACI = \frac{1}{M \times N}\frac{\Sigma(C_1(i,j) - C_2(i,j))}{255} \times 100\% \quad (20)$$

Among them, the ideal NPCR and UACI values are 99.6094% and 33.4635%, respectively. The algorithm's effectiveness in countering differential attacks improves as the measured values approach these ideal benchmarks. In this paper, a comparative analysis is conducted using the literature [28] [29], as illustrated in Table VI. The analysis demonstrates that the NPCR and UACI values in this algorithm closely approach the true values, indicating strong encryption efficacy and enhanced resistance to differential attacks.

TABLE VI. KEY SENSITIVITY

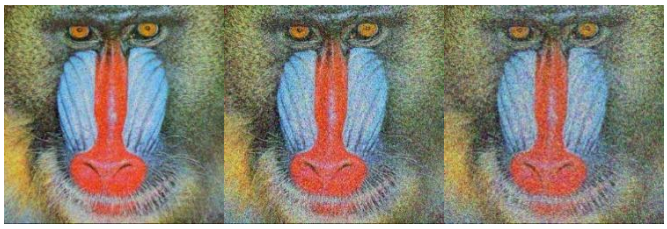
Imagery	NPCR/%	UACI/%
Lena	99.60	33.47
Baboon	99.62	33.45
Peppers	99.62	33.46
Airplane	99.61	33.47
Splash	99.61	33.47
Literature [28]	99.66	33.61
Literature [29]	99.61	33.48

E. Key Space

The key space represents the collection of all potential keys capable of generating an encryption key. The size of the key space is contingent upon the length of the security key, and a sufficiently extensive key space is effective in thwarting brute force attacks. When the key space of the whole algorithm reaches 2^{100}, it can show that the security of the algorithm can be guaranteed [30]. In the chaotic system used in this paper, the initial key is generated by the SHA-256 algorithm. Without considering the influence of other factors, the size of the security key is 256 bits, and the size of the key space is $2^{256} > 2^{100}$, which can withstand brute force attacks and exhibits a high level of security.

F. Robustness Analysis

Images are susceptible to interference from external factors during transmission, and the robustness of an encryption system is to assess how an image performs when subjected to various forms of interference. It is used to judge the encryption and decryption quality of an encryption system, with the aim of determining whether the system can effectively protect the encryption and integrity of the image when confronted with noise interference [31]. Salt and Pepper Noise (SPN) is a familiar type of noise in digital images that can significantly affect image quality, causing it to become unclear or distorted. The image decrypted with various levels of SPN added to the Baboon image is shown in Fig. 11. It is evident from the image that as the intensity of the added SPN increases, from (a) with intensity 0.1 to (c) with intensity 0.3, the quality of the deciphered image deteriorates and becomes increasingly blurry. However, it is still possible to discern the information in the original picture. This suggests that the algorithm introduced in this paper showcases substantial resistance to noise interference.



(a) (b) (c)

Fig. 11. Decrypted baboon images subjected to varying levels of SPN: (a) 0.1 (b) 0.2 (c) 0.3.

VI. CONCLUSION

This paper introduces a hyperchaotic image encryption algorithm based on LSTM. It involves processing the chaotic sequence generated by the Lorenz system in order to create new chaotic signals. This is achieved by leveraging the sequence data processing capabilities of the LSTM. Following this, the data undergoes iterative processing using the hyperchaotic system. Simultaneously, the Arnold algorithm, along with DNA coding and arithmetic rules, is applied to perform double diffusion of the data. This enhances the algorithm's complexity. In this paper, the above problems are described in detail and the experiment and analysis are carried out. The experimental results show that the algorithm can effectively ensure the privacy of the image through the encryption and decryption of the color RGB image. Meanwhile, comparisons with other algorithms, and an analysis of the algorithm's performance in terms of histograms, correlations, information entropy, and more, it has been verified that the encryption system exhibits strong resistance to differential attacks, statistical attacks, and brute-force attacks. It efficiently diminishes the correlation among adjacent pixels, thus bolstering the algorithm's complexity, security, and encryption efficacy. The DNA encoding technology employed in the algorithm falls within the realm of bioengineering, which suggests that the algorithm could be combined with biomedical treatments in the future to provide better protection for the transmission of medical data. In fact, there are many applications of deep learning algorithms to images, which can achieve good encryption effects and improve efficiency, which is the direction of future research and improvement.

ACKNOWLEDGMENT

The authors would like to thank the reviewers for taking time to guide the completion of this paper.

REFERENCES

[1] Hasan A A ,Ali A M K ,Talib A A .Image encryption based on 2DNA encoding and chaotic 2D logistic map[J].Journal of Engineering and Applied Science,2023,70(1).

[2] Yongsheng H ,Han W ,Luoyu Z .Color image encryption base on a 2D hyperchaotic enhanced Henon map and cross diffusion[J].Alexandria Engineering Journal,2023,73.

[3] Wuyan L, Limin Z, Zhongbao Y, et al. Image encryption algorithm based on hyperchaotic system and dynamic DNA encoding[J]. Physica Scripta,2023,98(11).

[4] Wu J, Chen D, Liu H. Computer Network Security in the Era of "Internet +"[J]. Journal of Artificial Intelligence Practice,2022,5(3).

[5] Wang Y, Wu C, Kang S, et al. Multi-channel chaotic encryption algorithm for color image based on DNA coding[J]. Multimedia Tools and Applications,2020,79(prepublish).

[6] Wen W, Hong Y, Fang Y, et al. A visually secure image encryption scheme based on semi-tensor product compressed sensing [J]. Signal Processing, 2020, 173(4): 107580-107597.

[7] Wang X, Wang Y, Zhu X, et al. A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level [J]. Optics and Lasers in Engineering, 2020, 125(8):105851-105863.

[8] Naseer Y, Shah T. Advance image encryption technique utilizing compression, dynamical system and s-boxes [J]. Mathematics and Computers in Simulation (MATCOM), 2020, 178(6): 207-217.

[9] Wu X, Kan H, Kurths J. A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps [J]. Application Software Computation, 2015, 37(6): 24-39.

[10] FRIDRICH J. Symmetric ciphers based on two-dimensional chaotic maps [J].International Journal of Bifurcation and Chaos, 1998, 8:1259-1284.

[11] Yousef A, Arslan M. An Image Encryption Algorithm Based on Trivium Cipher and Random Substitution[J]. SN Computer Science,2023,4(6).

[12] Xin C ,Simin Y ,Qianxue W , et al.On the cryptanalysis of an image encryption algorithm with quantum chaotic map and DNA coding[J].Multimedia Tools and Applications,2023,82(27).

[13] Dawei D, Jin W, Mouyuan W, et al. Controllable multistability of fractional-order memristive coupled chaotic map and its application in medical image encryption[J]. The European Physical Journal Plus,2023,138(10).

[14] Liang Qin,Zhu Congxu. A new one-dimensional chaotic map for image encryption scheme based on random DNA coding[J]. Optics and Laser Technology,2023,160.

[15] Castro F, Impedovo D, Pirlo G. A Medical Image Encryption Scheme for Secure Fingerprint-Based Authenticated Transmission[J]. Applied Sciences,2023,13(10).

[16] Alcocer R M U, Leal T E, Romero G, et al. A Deep Learning Approach for Predictive Healthcare Process Monitoring[J]. Information,2023,14(9).

[17] Malik S, Shah T. Color multiple image encryption scheme based on 3d-chaotic maps [J]. Mathematics and Computers in Simulation (MATCOM), 2020, 178(5): 646-666.

[18] Li T, Yan W, Chi Z. A new image encryption algorithm based on optimized Lorenz chaotic system[J]. Concurrency and Computation Practice and Experience,2020,34(13).

[19] Xinhe W. Water quality prediction based on AR and LSTM model[J]. Journal of Physics: Conference Series,2023,2580(1).

[20] WANG X, ZHAO M.An image encryption algorithm based on hyperchaotic system and DNA coding[J].Optics&Laser Technology,2021,143(14):107316.

[21] Thorat O, Mangrulkar R. Combining DNA sequences and chaotic maps to improve robustness of RGB image encryption[J]. International Journal of Computational Science and Engineering,2023,26(2).

[22] Ur M R, Arslan S, Bello A U. Securing Medical Information Transmission Between IoT Devices: An Innovative Hybrid Encryption Scheme Based on Quantum Walk, DNA Encoding, and Chaos[J]. Internet of Things,2023,24.

[23] Jian Z, Jifeng G, Donglei L. An efficient image encryption algorithm based on S-box and DNA code[J]. Measurement: Sensors,2023,29.

[24] Heping W, Yiting L. Cryptanalyzing an image cipher using multiple chaos and DNA operations[J]. Journal of King Saud University - Computer and Information Sciences,2023,35(7).

[25] Zhiqiang C, Wencheng W, Yuezhang D, et al. Novel One-Dimensional Chaotic System and Its Application in Image Encryption[J]. Complexity,2022,2022.

[26] Qin L, Congxu Z. A new one-dimensional chaotic map for image encryption scheme based on random DNA coding[J]. Optics and Laser Technology,2023,160.

[27] CHEN G R, MAO Y B, CHUI C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons and Fractals, 2004, 21(3): 749-761.

[28] Kari P A, Navin H A, Bidgoli M A, et al. A new image encryption scheme based on hybrid chaotic maps[J]. Multimedia Tools and Applications,2020,80(2).

[29] Chai, X., Fu, J., Zhang, J. et al. Exploiting preprocessing-permutation–diffusion strategy for secure image cipher based on 3D Latin cube and memristive hyperchaotic system. Neural Comput & Applic 33, 10371–10402 (2021).

[30] Geng S, Li J, Zhang X, et al. An Image Encryption Algorithm Based on Improved Hilbert Curve Scrambling and Dynamic DNA Coding[J]. Entropy,2023,25(8).

[31] Qiang L, Hanqiang H, Xiao-Wen Z, et al. Image encryption using fission diffusion process and a new hyperchaotic map[J]. Chaos, Solitons and Fractals: the interdisciplinary journal of Nonlinear Science, and Nonequilibrium and Complex Phenomena,2023,175(P1).