Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

A geographic information encryption system based on Chaos-LSTM and chaos sequence proliferation*#

Jia DUAN[1,2], Luanyun HU[1,2], Qiumei XIAO†‡[3], Meiting LIU[3], Wenxin YU[3]

[1]*Third Surveying and Mapping Institute of Hunan Province, Changsha 410000, China*

[2]*Hunan Engineering Research Center of Geographic Information Security and Application, Changsha 410000, China*

[3]*School of Information and Electrical Engineering, Hunan University of Science and Technology, Xiangtan 411201, China*

†E-mail: 1959582421@qq.com

Received Nov. 7, 2023; Revision accepted Apr. 8, 2024; Crosschecked Feb. 21, 2025

Abstract: In response to the strong correlation between the chaotic system state and initial state and parameters in traditional chaotic encryption algorithms, which may lead to periodicity in chaotic sequences, the chaos long short-term memory (Chaos-LSTM) model is constructed by combining chaotic systems with LSTM neural networks. The chaos sequence proliferation (CSP) algorithm is constructed to address the problem that the limited computational accuracy of computers can lead to periodicity in long chaotic sequences, making them unsuitable for encrypting objects with large amounts of data. By combining the Chaos-LSTM model and CSP algorithm, a geographic information encryption system is proposed. First, the Chaos-LSTM model is used to output chaotic sequences with high spectral entropy (SE) complexity. Then, a shorter chaotic sequence is selected and proliferated using the CSP algorithm to generate chaotic proliferation sequences that match the encrypted object; a randomness analysis is conducted and testing is performed on it. Finally, using geographic images as encryption objects, the chaotic proliferation sequence, along with the scrambling and diffusion algorithms, are combined to form the encryption system, which is implemented on the ZYNQ platform. The system's excellent confidentiality performance and scalability are proved by software testing and hardware experiments, making it suitable for the confidentiality peers of various encryption objects with outstanding application value.

Key words: Chaos; Long short-term memory (LSTM); Chaos sequence proliferation (CSP); ZYNQ platform; Image encryption
https://doi.org/10.1631/FITEE.2300755 **CLC number:** TP309

1 Introduction

With the deepening application of geographic information, various types of data are widely shared. The confidential information involved in geographic information data is extensive, and if leaked, it will lead to serious losses and harm. Therefore, it is crucial to provide a secure and inclusive communication system for different geographic information data. Encryption algorithms are the core of secure communication systems, and researchers have also proposed various encryption algorithms, such as the triple data encryption standard (Tezcan, 2022), elliptic curve cryptography (Ullah et al., 2023), the international data encryption algorithm (Sahu et al., 2016), fully homomorphic encryption (Martins et al., 2017), and quantum key distribution (Cao et al., 2022).

In addition, chaotic systems, neural networks, and their combinations are all used for secure communication. Alexan et al. (2023) proposed a secure communication algorithm combining multiple maps. Gabr et al. (2023) proposed an image encryption algorithm

‡ Corresponding author

* Project supported by the Open Topic of Hunan Engineering Research Center of Geographic Information Security and Application, China (No. HNGISA2023005)

Electronic supplementary materials: The online version of this article (https://doi.org/10.1631/FITEE.2300755) contains supplementary materials, which are available to authorized users

ORCID: Qiumei XIAO, https://orcid.org/0009-0004-8924-5799

that combines chaotic systems with unique image transformation techniques, promoting the application of chaotic encryption algorithms. Murillo-Escobar et al. (2022) provided a data confidentiality scheme based on chaotic cryptography and sequence spread spectrum technology. Lin et al. (2022) proposed using a memristor ring neural network to encrypt medical images. Based on the Takagi–Sugeno fuzzy neural network, Yan et al. (2023) designed a synchronization controller for image encryption. Xu et al. (2022) proposed a method for constructing multiple hash index chains based on a fractional order chaotic Hopfield neural network (HNN). Based on convolutional neural networks and chaos, Man et al. (2021) studied a dynamic adaptive diffusion encryption algorithm. De la Fraga et al. (2023) and Gonzalez-Zapata et al. (2023) studied the implementation method and topology of the echo state neural network (ESNN), using an improved ESNN to predict chaotic time series and enhancing the hardware of ESNN using the field programmable gate array (FPGA). Neural networks with learning capabilities can generate new sequences with chaotic characteristics by learning from existing chaotic time series. The different initial states of chaotic systems correspond to different periods, and their period lengths may be very short, which, to some extent, reduces the confidentiality of chaos encryption systems. In response to this issue, this paper combines chaotic systems and long short-term memory (LSTM) neural networks to construct a Chaos-LSTM model. By using LSTM neural networks to learn the characteristics of chaotic systems and generating new chaotic sequences through trained LSTM neural networks, the potential periodic risks of chaotic systems are avoided.

Chaos systems and neural networks with excellent secure communication performance have been proven by many researchers. However, further research is needed to develop secure algorithms that generate adaptive data volumes when faced with multiple secure objects. Due to the computational accuracy and performance of existing computers being unable to perform completely ideal simulation solutions, most chaotic systems implemented with limited accuracy may have properties that deviate from their theoretical results (Teh et al., 2020; Wan et al., 2020). Moreover, the limited computational accuracy of computers can ultimately lead to periods in chaotic sequences. The longer the output chaotic sequence of a chaotic system, the greater the possibility of periodicity. How to make chaotic sequences have longer periods and better randomness is the key to designing chaotic encryption algorithms (Chen et al., 2020; Irfan et al., 2020). To address this issue, this paper proposes chaos sequence proliferation (CSP), which proliferates the chaotic sequences through local mean sequences and cyclic XOR operations. With only a small number of chaotic sequences, sufficient chaotic sequences for encryption can be generated without the need for chaotic systems to generate growth sequences, avoiding the potential periodicity caused by excessively long chaotic sequences.

To demonstrate the actual application effect, Liu et al. (2024) discretized the memristor on a digital signal processor (DSP) and implemented a hyperchaotic mapping encryption algorithm. A novel pseudo-random number generator for encryption was developed by Yu F et al. (2022) using FPGA to achieve a memristor HNN. Tlelo-Cuautle et al. (2020) implemented Hopfield and Hindmarsh–Rose neurons for chaotic image encryption on FPGA. The application of FPGA has promoted the implementation of secure communication algorithms for offline applications in various applications. We also implement the designed encryption system on the ZYNQ hardware platform.

In summary, this paper proposes a geographic information encryption system based on Chaos-LSTM and CSP. The Chaos-LSTM model and CSP algorithm constructed in this paper can further enhance the randomness of the chaotic sequence on the basis of the chaotic system. Only a part of the output sequences of the chaotic system should be selected, avoiding the encryption performance deficiency caused by the low complexity of the chaotic sequences.

The remaining sections of this paper are organized as follows: in Section 2, a Chaos-LSTM model is constructed and the complexity of its output sequence is analyzed. In Section 3, a CSP algorithm is designed. The spectral entropy (SE) complexity (Xiong et al., 2021) calculation, TestU01 tests (De la Fraga et al., 2021), and the National Institute of Standards and Technology (NIST) tests (Pareschi et al., 2012) are performed on the proliferation sequences. In Section 4, taking geographic information images as the object, an image encryption system is constructed using a secret key; the Chaos-LSTM model, the CSP algorithm, the scrambling and diffusion algorithms, and the encryption

performance of the system are analyzed. In Section 5, the designed encryption system is implemented in ZYNQ. Section 6 provides the main conclusions and future research directions of this work.

2 Construction of Chaos-LSTM model

2.1 Chaos system

Lorenz (1963) established the Lorenz system while studying atmospheric convection models and first published the research results of chaos theory. Since then, the Lorenz system has been continuously discussed, becoming a classic chaotic system used to describe chaos phenomena. The chaotic system used in this paper is a simplified Lorenz system, the mathematical model of which is shown in Eq. (1):

$$\begin{cases} \dot{x} = 10(y-x), \\ \dot{y} = (24-4c)x - xz + cy, \\ \dot{z} = xy - 8z/3, \end{cases} \tag{1}$$

where x, y, and z are the system state variables and c is the system parameter. When $c\in[-1, 7.75]$, the simplified Lorenz system is in a chaotic state and the x, y, and z dimensions of the system output chaotic sequences $x(t)$, $y(t)$, and $z(t)$, respectively. It should be noted that, although the chaotic system used in this paper is the Lorenz system, this does not mean that the chaotic system can only use the Lorenz system; other chaotic systems with two-dimensional (2D) or above chaotic sequence outputs can also be used.

2.2 LSTM

The LSTM neural network is a special recurrent neural network with time-recursive characteristics that can effectively handle long-term dependency problems; its basic nodes are LSTM units that consist of four structures (Yu Y et al., 2019). The basic architecture of the standard LSTM unit is shown in Fig. 1.

In Fig. 1, x_t represents the input, h_t represents the cyclic information, y_t represents the output, c_t represents the cell state, $\mathrm{sig}(\cdot)$ is the Sigmoid function, and $\tanh(\cdot)$ is the hyperbolic tangent function.

The forget gate, shown in Eq. (2), is used to control whether to discard information from the previous cell state:

$$f_t = \mathrm{sig}(W_{fh}h_{t-1} + W_{fx}x_t + b_f). \tag{2}$$

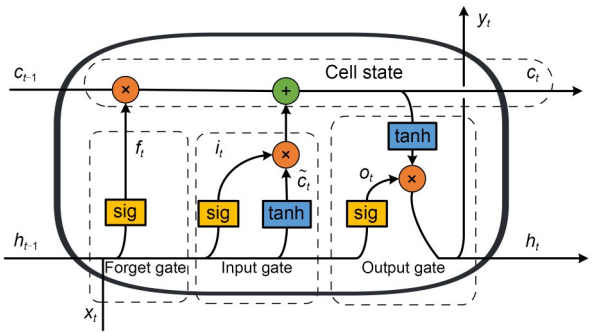

Fig. 1 Basic architecture of standard LSTM units

The input gate, as shown in Eq. (3), determines the importance of the input information:

$$\begin{cases} i_t = \mathrm{sig}(W_{ih}h_{t-1} + W_{ix}x_t + b_i), \\ \tilde{c}_t = \tanh(W_{\tilde{c}h}h_{t-1} + W_{\tilde{c}x}x_t + b_{\tilde{c}}). \end{cases} \tag{3}$$

The cell state, as shown in Eq. (4), is used to store and transmit the information, passing along the network throughout the entire time series:

$$c_t = c_{t-1}f_t + i_t\tilde{c}_t. \tag{4}$$

The output gate, as shown in Eq. (5), controls which information in the cell state will be transmitted to the output of the LSTM units:

$$\begin{cases} o_t = \sigma(W_{oh}h_{t-1} + W_{ox}x_t + b_o), \\ h_t = o_t\tanh(c_t), \\ y_t = h_t. \end{cases} \tag{5}$$

In Eqs. (2)–(5), W is the weight and b represents the bias.

Based on the above LSTM units, an LSTM recurrent neural network is constructed in this paper. The input layer is the sequence input layer. The LSTM layer sets the number of LSTM units to 128, the state activation function to $\tanh(\cdot)$, and the gate activation function to $\mathrm{sig}(\cdot)$. The dropout layer randomly discards the input elements with 50% probability and sets the elements to zero. The fully connected layer uses the Xavier initializer (Jia et al., 2014) to initialize the weights and initialize the bias with zero. The fifth layer is the regression layer, which outputs regression sequence data. The input and output dimensions of each layer are set to 1, forming the LSTM recurrent neural network, as shown in Fig. 2.

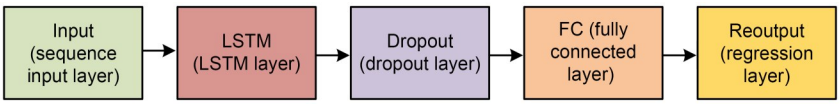

Fig. 2 LSTM recurrent neural network

2.3 Chaos-LSTM model

Training the LSTM recurrent neural network through chaotic sequences generated by the Lorenz system, the neural network is transformed into a Chaos-LSTM model that can generate new chaotic sequences. The chaotic sequence is inputted into it to predict the response of the data in the sequence; a new chaotic sequence of corresponding length is the output, and the network state of the model is updated. The Lorenz chaotic system and the LSTM neural network together constitute the Chaos-LSTM model. The flowchart of the Chaos-LSTM model processing is shown in Fig. 3.

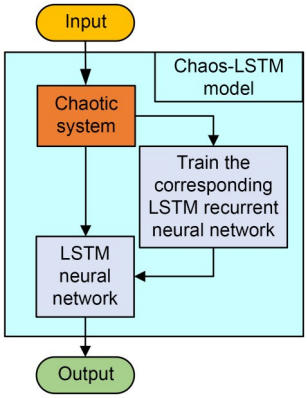

Fig. 3 Flowchart of the Chaos-LSTM model processing

In Fig. 3, the input is the initial values of state variables and the parameters of the Lorenz system, and the output is a new chaotic sequence $x'(t)$. When the parameter is set to c=2 and the initial values are set to $x(0)$= 1, $y(0)$=2, and $z(0)$=3, the comparison between the chaotic sequence $x(t)$ generated by the Lorenz system and the output new chaotic sequence $x'(t)$ is shown in Fig. 4a. The new chaotic sequence $x'(t)$ trained by the Chaos-LSTM model is different from the chaotic sequence $x(t)$.

Complexity is a quantitative indicator of the randomness of chaotic sequences. Currently, the complexity classification algorithms for chaotic systems can be divided into two types: behavioral complexity and

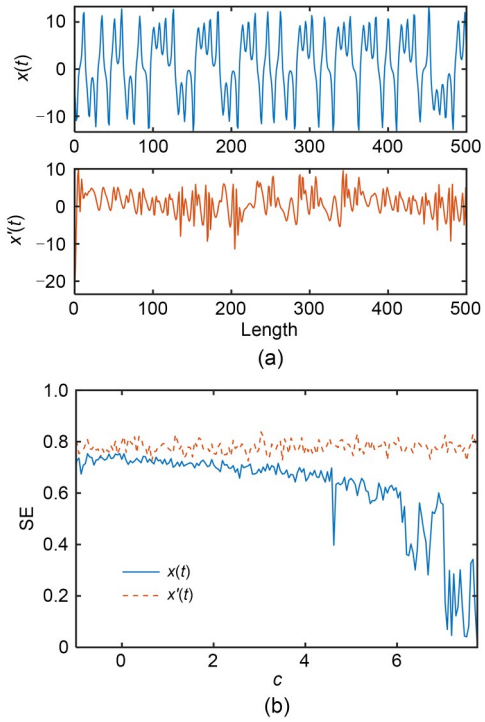

Fig. 4 Comparison between chaotic sequence $x(t)$ and the new chaotic sequence $x'(t)$ (a) and SE complexity comparison with system parameter c changing (b)

structural complexity. The SE complexity algorithm belongs to the structural complexity algorithm, which uses the Fourier transform to obtain the corresponding spectral entropy value by combining the energy distribution in the Fourier transform domain with Shannon entropy (Xiong et al., 2021). SE complexity can represent the complexity of a signal sequence. The simpler the spectrum structure of the sequence, the closer the SE measure value is to 0 and the smaller the complexity of the sequence. The more complex the spectral structure of the sequence, the closer the SE measure value is to 1, indicating a higher complexity of the sequence.

The SE complexity of the Lorenz system output sequence will change as system parameter c changes. Sequence $x(t)$ with a length of 500 and the corresponding sequence $x'(t)$ are selected for SE complexity comparison in Fig. 4b. SE complexity of the new chaotic

sequence $x'(t)$ is greater than that of the chaotic sequence $x(t)$ under different system parameters c. Compared to the chaotic sequence $x(t)$, the new chaotic sequence $x'(t)$ is closer to a random sequence.

3 Chaos sequence proliferation

3.1 Chaos sequence proliferation algorithm

For chaotic sequences generated by chaotic systems, it is difficult to ensure that each sequence has a sufficiently large period and high complexity. Although the Chaos-LSTM model improves the randomness of the output sequence based on the chaotic system, the periodicity of the chaotic sequence may still appear when the output sequence is sufficiently long. To ensure that the chaotic encryption sequence can match the data capacity of the encrypted object, have a longer periodicity, and maintain the randomness of the encryption sequence, this paper proposes the CSP algorithm. The algorithm selects only a portion of the chaotic sequences and generates sufficient encrypted sequences through proliferation, to some extent mitigating cryptographic weaknesses caused by the short periodicity of the chaotic sequences.

The encryption of color images with size $3\times M\times N$ is taken as an example, which requires an encrypted sequence of length $3\times M\times N$. The implementation steps of the CSP algorithm are as follows:

Step 1: input the parameter and the initial values of the chaotic system, and iteratively simulate the Lorenz system. Set the number of iterations to N, and generate three-dimensional (3D) floating-point chaotic sequences $x(t)$, $y(t)$, and $z(t)$ with length N.

Step 2: input floating-point chaotic sequence $x(t)$ into the trained LSTM neural network and output a new floating-point chaotic sequence $x'(t)$ with the same length as the chaotic sequence $x(t)$.

Step 3: convert floating-point chaotic sequences $x'(t)$ and $y(t)$ with length N into integer chaotic sequences $X(t)$ and $Y(t)$ through Eq. (6):

$$\begin{cases} X(t)=\text{floor}(x'(t)\times 2^n), \\ Y(t)=\text{floor}(y(t)\times 2^n), \end{cases} \tag{6}$$

where $\text{floor}(\cdot)$ is the rounding function and $n=16$. Eq. (6) represents moving the floating-point chaotic sequence to the left by n bits before performing the rounding operation.

Step 4: find all local extremum points in integer chaotic sequence $X(t)$, and calculate the average values u_i of all adjacent local extremum points through Eq. (7):

$$u_i=\frac{v_i+v_{i+1}}{2},\ 0<i<N. \tag{7}$$

Step 5: perform linear smooth interpolation on all local mean values to obtain an approximate local mean function sequence $u(t)$ with length N, and then convert floating-point sequence $u(t)$ to integer sequence $U(t)=\text{floor}(u(t))$.

Step 6: introduce chaotic sequence $Y(t)$, perform the XOR operation on local mean function sequences $U(t)$, $Y(t)$, and $X(t)$ to obtain CSP component DX_j:

$$\text{DX}_j(t)=U(t)\oplus Y(t)\oplus X(t), \tag{8}$$

where $\oplus$ represents the bitwise XOR operation.

Step 7: use the CSP component DX_j as the new chaotic sequence $X(t)$, repeat steps 4 to 6, cycle $3M$ times, and obtain $3M$ CSP components with length N.

The flowchart of CSP is shown in Fig. 5.

3.2 Randomness analysis of chaos proliferation sequences

Taking the chaotic sequence generated by the Lorenz system under the condition of parameter $c=2$ and the initial values $x(0)=1, y(0)=2$, and $z(0)=3$ as an example. Let $M=4$ and $N=500$, and generate 12 CSP components $\text{DX}_j, j=1, 2, \cdots, 12$ with length 500 using the CSP algorithm. The CSP components are shown in Fig. 6.

Calculate the SE complexity of the chaotic sequence $X(t)$ and all chaotic proliferation sequences, and conduct a comparative analysis, which is visually displayed in Table 1 and Fig. 7. In the coordinate axis shown in Fig. 7, the vertical axis represents SE complexity, and the horizontal axis represents each sequence; that is, sequences 1–12 represent DX_1–DX_{12}, and sequence 13 represents $X(t)$. The SE complexity of each chaotic proliferation sequence is greater than that of chaotic sequence $X(t)$. This means not only that the CSP algorithm can infinitely multiply the original chaotic sequence, but also that the extended chaotic

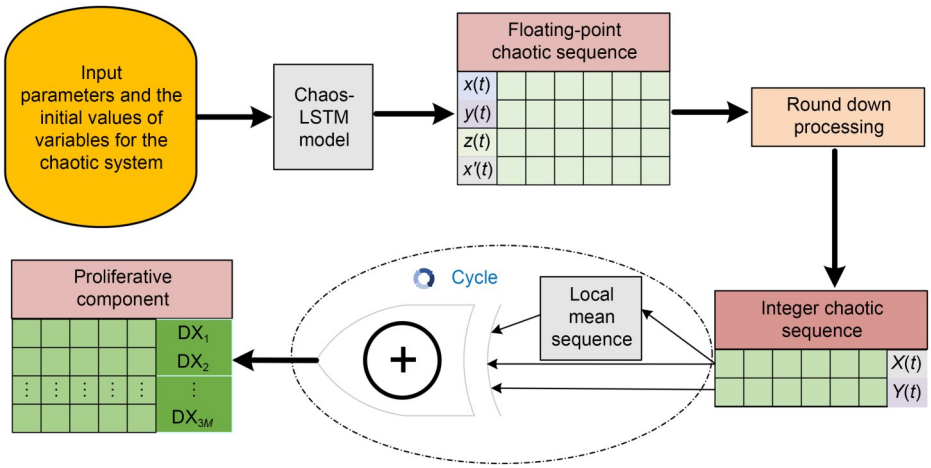

Fig. 5 Flowchart of CSP

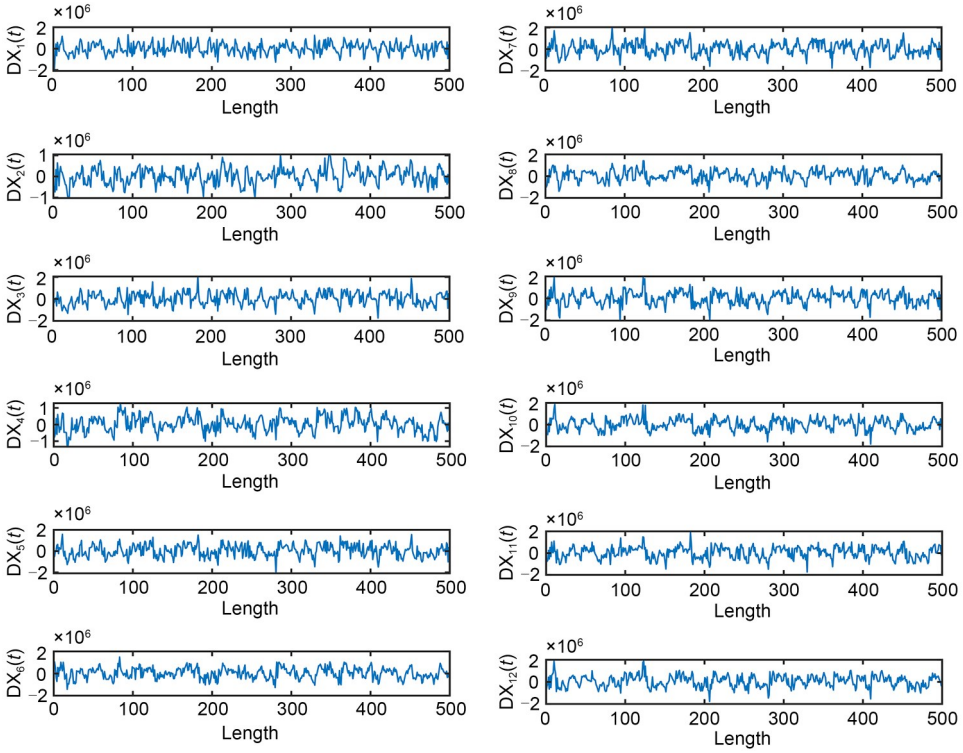

Fig. 6 Generated CSP component diagram

proliferation sequence is closer to a random sequence compared to the original chaotic sequence.

To verify the randomness of chaotic proliferation sequences, the chaotic proliferation sequences with length 10^6 are selected for NIST tests and TestU01 tests (De la Fraga et al., 2021). In the NIST tests, the P-values of all 15 tests are greater than 0.01 and the TestU01 tests are also passed, indicating that the chaotic proliferation sequences have good randomness and belong to the random sequence (supplementary materials, Section 1).

4 Secure communication system and experimental analysis

For confidential objects with different data sizes, the Chaos-LSTM model and CSP algorithm in this paper

Table 1 SE complexity of sequences

Sequence	SE complexity
$DX_1(t)$	0.8904
$DX_2(t)$	0.8258
$DX_3(t)$	0.8565
$DX_4(t)$	0.8087
$DX_5(t)$	0.8580
$DX_6(t)$	0.8168
$DX_7(t)$	0.8531
$DX_8(t)$	0.8175
$DX_9(t)$	0.8549
$DX_{10}(t)$	0.8295
$DX_{11}(t)$	0.8429
$DX_{12}(t)$	0.8308
$X(t)$	0.8078

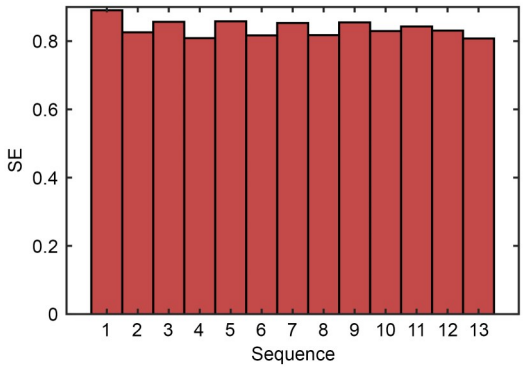

Fig. 7 Comparison of SE complexity of sequences

provide adaptive encrypted sequences. The complexity of the encrypted sequences, compared to the original chaotic sequences, is also significantly improved. Therefore, combining the Chaos-LSTM model and CSP algorithm with scrambling and diffusion algorithms to construct encryption algorithms can be used for encrypting various geographic information data.

Geographic information data refer to the general term for numbers, text, images, and graphics of geographical circles or environments, which contain the quantity, quality, distribution characteristics, connections, and patterns of inherent elements or substances. Digital images, a representative data structure, contain more information than text and sound, which are the foundation of video formation. So, taking the encryption of color geographic information images with a grayscale of $L=256$ and a size of $M\times N\times 3$ as an example, the structure of the geographic information encryption system based on Chaos-LSTM and CSP designed in this paper is shown in Fig. 8.

In Fig. 8, $[x_0, y_0, z_0, c, C_1, C_2]$ is the encryption key and $[x_0', y_0', z_0', c', C_1', C_2']$ is the decryption key, where the value ranges of the key are $c, c' \in [-1, 7.75]$, C_1, $C_1' \in [0, 255]$, and C_2, $C_2' \in [0, 255]$. The specific process of the encryption system is as follows:

Step 1: input the encryption keys x_0, y_0, z_0, and c into the Lorenz system to generate 3D floating-point chaotic sequences $x(t), y(t)$, and $z(t)$ with length N.

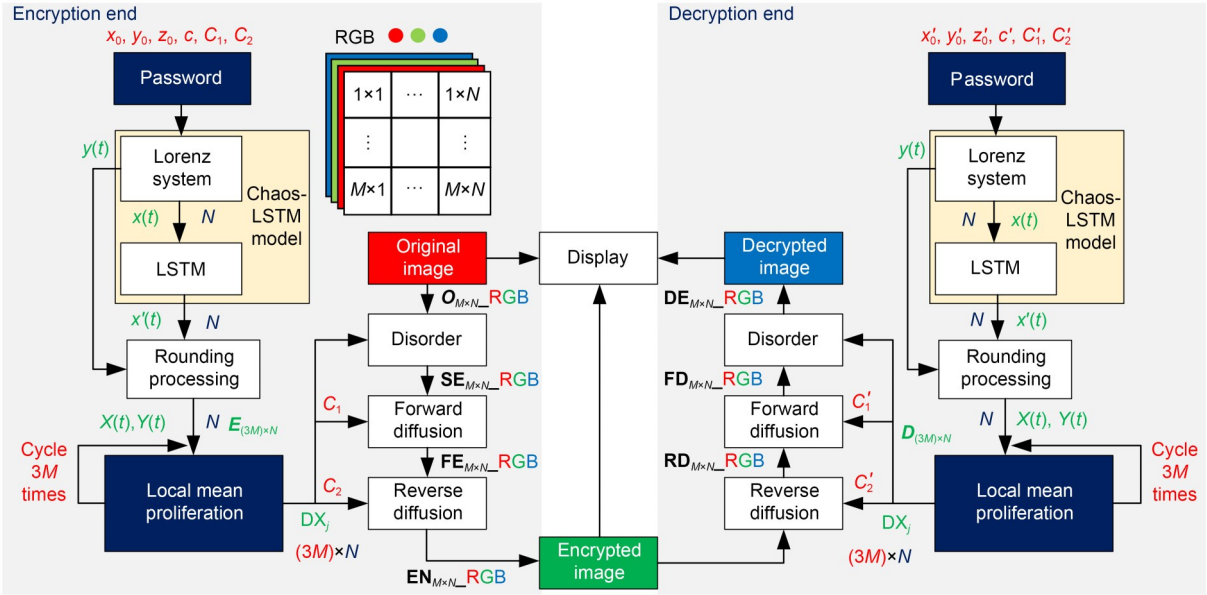

Fig. 8 Flowchart of the geographic information encryption system based on Chaos-LSTM and CSP

Step 2: input the sequence $x(t)$ into the Chaos-LSTM model and output a new chaotic sequence $x'(t)$ with the same length as sequence $x(t)$.

Step 3: convert floating-point chaotic sequences $x'(t)$ and $y(t)$ into integer chaotic sequences $X(t)$ and $Y(t)$ through the rounding processing module.

Step 4: input sequences $X(t)$ and $Y(t)$ into the local mean proliferation module to obtain the CSP component DX_j.

Step 5: take the proliferation component DX_j as the chaotic sequence $X(t)$, repeat step 4, and cycle $3M$ times to obtain CSP components DX_j, $j=1, 2, \cdots, 3M$ with length N.

Step 6: use CSP components DX_j as the encryption sequence $\boldsymbol{E}_{(3M)\times N}$, and set the encryption keys C_1 and C_2. Scramble the row of the original image $\boldsymbol{O}_{M\times N}$_RGB to obtain image $\mathbf{SE}_{M\times N}$_RGB, then perform forward diffusion to obtain image $\mathbf{FE}_{M\times N}$_RGB, and reverse diffusion to obtain image $\mathbf{EN}_{M\times N}$_RGB.

Step 7: transfer the encrypted image to the decryption end for decryption, the process of which is the reverse of the encryption process, and display the images.

In step 6, row scrambling, as shown in Eq. (9) at the bottom of this page, is performed to obtain the image $\mathbf{SE}_{M\times N}$_RGB.

$\boldsymbol{O}_{M\times N}$_RGB is the original image matrix, $\mathbf{SE}_{M\times N}$_RGB is the scrambled image matrix, and $\Updownarrow$ represents the matrix element exchange operation. $p=1, 2, \cdots, M$ and $q=1, 2, \cdots, \mathrm{floor}(N/2)$ are rows and columns of matrix positions, respectively.

Perform forward diffusion as shown in Eq. (10) at the bottom of this page on scrambled images to obtain $\mathbf{FE}_{M\times N}$_RGB.

$\mathbf{FE}_{M\times N}$_RGB represents the positive diffusion image matrix, $\oplus$ represents the bitwise XOR operation, and $u=1, 2, \cdots, 3M$ and v are rows and columns of matrix positions, respectively.

Reverse diffusion is performed on a positive diffusion image to obtain image $\mathbf{EN}_{M\times N}$_RGB, which is shown in Eq. (11) at the bottom of this page.

$\mathbf{EN}_{M\times N}$_RGB represents the reverse diffusion image matrix, which is the encrypted image matrix, and $m=1, 2, \cdots, 3M$ and n represent the rows and columns of matrix positions, respectively.

The proposed encryption system in this paper includes 32-bit chaotic system initial values and parameters x_0, y_0, z_0, and c and 8-bit diffusion algorithm initial values C_1 and C_2. The calculated key space size is $2^{32\times4}\times2^{8\times2}$, which is much larger than 2^{100}, indicating that it has the ability to resist exhaustive attacks.

$$
\begin{aligned}
\mathbf{SE}_{M\times N}\_\mathrm{R}&=\begin{cases}\boldsymbol{O}_{M\times N}\_\mathrm{RGB}\big(p, E_{(3M)\times N}(p,q)\big),\\ \Updownarrow\\ \boldsymbol{O}_{M\times N}\_\mathrm{RGB}\big(p, E_{(3M)\times N}(p, N-q+1)\big),\end{cases}\\
\mathbf{SE}_{M\times N}\_\mathrm{G}&=\begin{cases}\boldsymbol{O}_{M\times N}\_\mathrm{RGB}\big(p+M, E_{(3M)\times N}(p+M,q)\big),\\ \Updownarrow\\ \boldsymbol{O}_{M\times N}\_\mathrm{RGB}\big(p+M, E_{(3M)\times N}(p+M, N-q+1)\big),\end{cases}\\
\mathbf{SE}_{M\times N}\_\mathrm{B}&=\begin{cases}\boldsymbol{O}_{M\times N}\_\mathrm{RGB}\big(p+2M, E_{(3M)\times N}(p+2M,q)\big),\\ \Updownarrow\\ \boldsymbol{O}_{M\times N}\_\mathrm{RGB}\big(p+2M, E_{(3M)\times N}(p+2M, N-q+1)\big),\end{cases}\\
\mathbf{SE}_{M\times N}\_\mathrm{RGB}&=[\mathbf{SE}_{M\times N}\_\mathrm{R}, \mathbf{SE}_{M\times N}\_\mathrm{G}, \mathbf{SE}_{M\times N}\_\mathrm{B}].
\end{aligned}
\tag{9}
$$

$$
\mathbf{FE}_{M\times N}\_\mathrm{RGB}=\begin{cases}C_1\oplus\boldsymbol{E}_{(3M)\times N}(u,v)\oplus\mathbf{SE}_{M\times N}\_\mathrm{RGB}(u,v), v=1,\\ \mathbf{FE}_{M\times N}\_\mathrm{RGB}(u,v-1)\oplus\mathbf{E}_{(3M)\times N}(u,v)\oplus\mathbf{SE}_{M\times N}\_\mathrm{RGB}(u,v), v=2, 3, \cdots, N.\end{cases}
\tag{10}
$$

$$
\mathbf{EN}_{M\times N}\_\mathrm{RGB}=\begin{cases}C_2\oplus\boldsymbol{E}_{(3M)\times N}(m,n)\oplus\mathbf{FE}_{M\times N}\_\mathrm{RGB}(m,n), n=N,\\ \mathbf{EN}_{M\times N}\_\mathrm{RGB}(m,n+1)\oplus\boldsymbol{E}_{(3M)\times N}(m,n)\oplus\mathbf{FE}_{M\times N}\_\mathrm{RGB}(m,n), n=N-1, \cdots, 2, 1.\end{cases}
\tag{11}
$$

To measure the performance of the secure communication system, known plaintext attack, image histogram, correlation, key sensitivity, and information entropy, an encryption performance comparison and encryption quality analysis are conducted.

4.1 Analysis of known plaintext attacks

All black and white images are often used to evaluate the protection ability of encryption systems against known plaintext attacks. Let $[x_0, y_0, z_0, c, C_1, C_2]=[x_0', y_0', z_0', c', C_1', C_2'] = [1, 2, 3, 2, 0, 0]$; this key is used by default in this paper. All black and white images are encrypted and decrypted by the encryption system, as shown in Fig. 9. The results demonstrate that the proposed encryption system can effectively protect against known plaintext attacks.

4.2 Image histogram analysis

Histogram analysis, which reflects the distribution characteristics of pixel grayscale values in digital images, is performed on the geographic information images and the corresponding encrypted images, as shown in Fig. 10. From Fig. 10, the distribution of pixel grayscale values in the histograms of the geographic

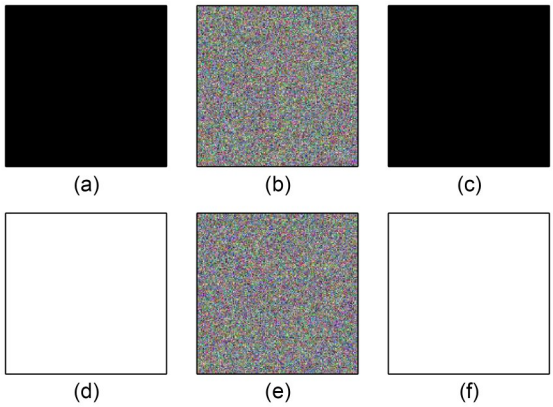

Fig. 9 Encryption experiments on an all black image (256×256) and an all white image (256×256): (a, d) original; (b, e) encrypted; (c, f) decrypted. (a)–(c) correspond to the all black image, and (d)–(f) correspond to the all white image

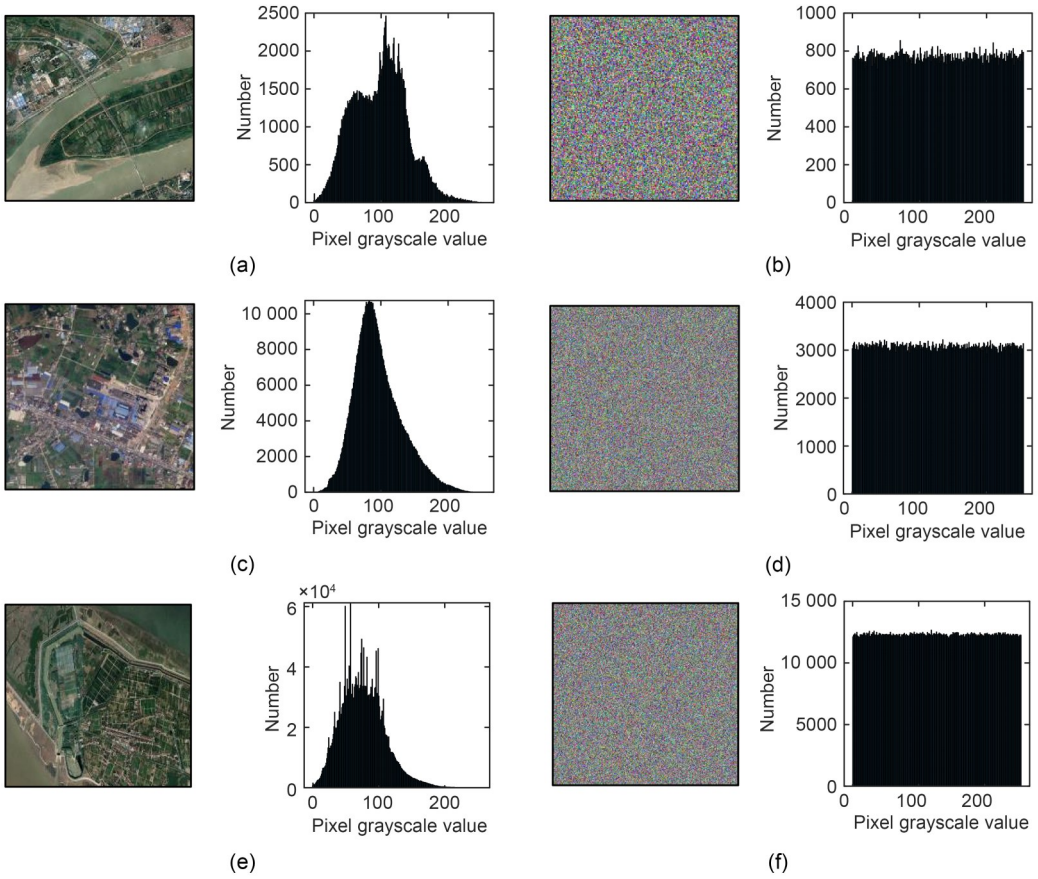

Fig. 10 Geographic information remote sensing images A, B, and C and their histograms: (a, c, e) original; (b, d, f) encrypted. (a) and (b) correspond to image A; (c) and (d) correspond to image B; (e) and (f) correspond to image C

information images is uneven, indicating significant differences in the grayscale values in the geographic information images. After images are encrypted, the distribution of pixel grayscale values in the histogram is unified, and the pixel grayscale information is well hidden. It is difficult to find patterns in the use of grayscale values in the encrypted image and crack the encryption system.

4.3 Correlation analysis

The encryption system needs to break the high correlation between general geographic information images to ensure confidentiality and security. Taking geographic information remote sensing image A as an example, Fig. 11 shows the correlation coefficients in various directions of the original and encrypted images.

Calculate the correlation between adjacent pixels in Fig. 11, as shown in Table 2.

The correlation coefficients in Table 2 are the average results of 1000 experiments, which shows that the correlation coefficients in image A are relatively high in all directions, with strong correlation, while those in the encrypted image are close to 0 in all directions, indicating an approximate lack of correlation.

4.4 Key sensitivity analysis

The key sensitivity analysis of encryption systems aims to prove that when the key changes, the encrypted image cannot be decrypted using the original key. Set the original key $K=[x_0, y_0, z_0, c, C_1, C_2]=[1, 2, 3, 2, 0, 0]$ and make minor changes to the original key to obtain $K'=[x_0, y_0, z_0, c, C_1, C_2]=[1, 2+10^{-12}, 3, 2, 0, 0]$. As shown in Fig. 12, the geographic information remote sensing image A is encrypted using the original key K, and then decrypted using K'.

On the contrary, Fig. 13 shows that image A is encrypted using the key K', and then decrypted using the original key K.

Figs. 12 and 13 show that there is only a small difference (10^{-12}) between the encryption key and the decryption key, but the decryption fails, reflecting the high key sensitivity of the constructed geographic information encryption system based on Chaos-LSTM and CSP.

4.5 Information entropy analysis

Information entropy H, as shown in Eq.(12), can reflect the uncertainty of image information.

$$H=-\sum_{i=0}^{L-1} p(i)\log_2 p(i), \tag{12}$$

where $L=256$ and $p(i)$ represents the occurrence probability of grayscale value i ($i=0, 1, \cdots, L-1$). The closer the H is to 8 (theoretical maximum value), the greater the uncertainty of the image information.

From Table 3, H of the original images is significantly less than 8, while that of the encrypted images is close to 8, indicating that the encrypted images have high uncertainty and good confidentiality effects.

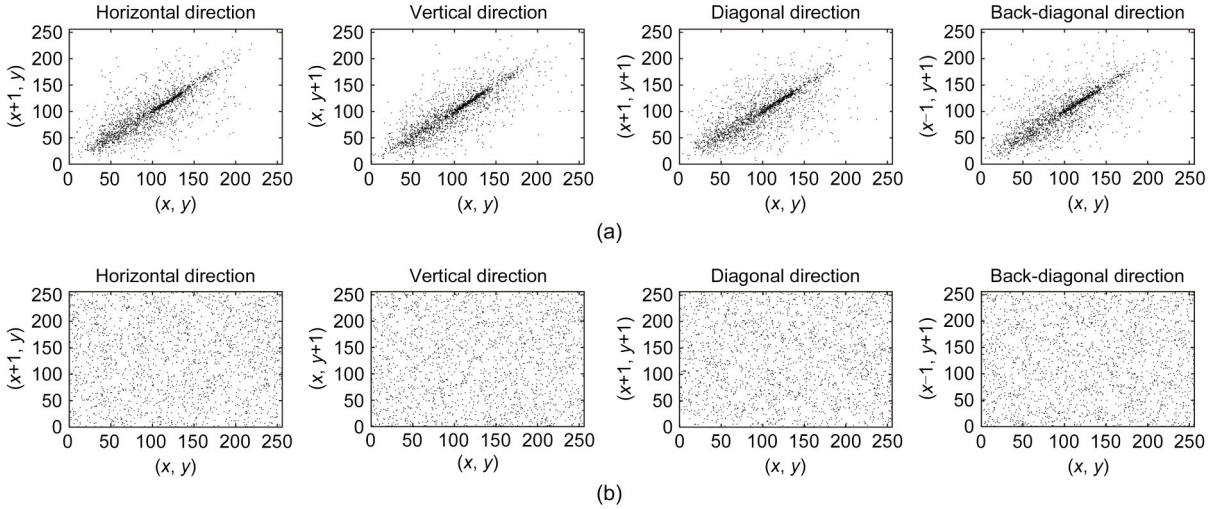

Fig. 11 Correlation coefficients in various directions of geographic information remote sensing image A: (a) original; (b) encrypted

Table 2 Correlation coefficients

Image A	Correlation coefficient			
	Horizontal	Vertical	Diagonal	Back-diagonal
Original	0.7710	0.7976	0.6864	0.7619
Encrypted	0.0149	−0.0179	0.0353	0.0328

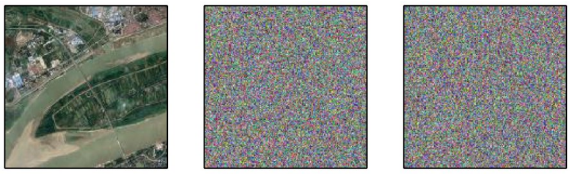

Fig. 12 Forward encryption and decryption of geographic information remote sensing image A: (a) original; (b) encrypted; (c) error decrypted

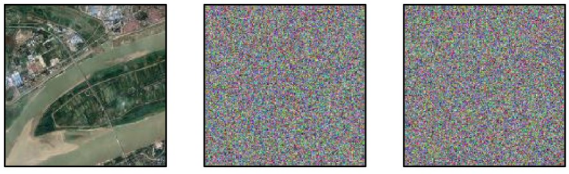

Fig. 13 Reverse encryption and decryption of geographic information remote sensing image A: (a) original; (b) encrypted image; (c) error decrypted

Table 3 Image information entropy

Image	State	*H*
Geographic information remote sensing image A (256×256)	Original	7.3368
	Encrypted	7.9992
Geographic information remote sensing image B (512×512)	Original	7.1322
	Encrypted	7.9997
Geographic information remote sensing image C (1024×1024)	Original	7.0290
	Encrypted	7.9999
All back image (256×256)	Original	0
	Encrypted	7.9992
All white image (256×256)	Original	0
	Encrypted	7.9991

4.6 Comparison of encryption performance

The number of pixels change rate (NPCR) refers to the proportion of different pixels between two images relative to the total number of pixels. The unified average changing intensity (UACI) refers to the average ratio of the difference between all corresponding pixel positions in two images to the maximum possible difference (Rehman et al., 2018).

We have encrypted the image Lena using the proposed algorithm and the algorithms proposed in the references (Wu et al., 2015, 2016; Hosseinzadeh et al., 2019). It is easy to conclude that our proposed method has a good confidentiality performance (supplementary materials, Section 2).

4.7 Encryption quality analysis

The encryption quality analysis is conducted on the encryption algorithm proposed in this paper, including the mean squared error (MSE), the peak signal-to-noise ratio (PSNR), the structural similarity index (SSIM), the chi-square test, and the floating frequency (Murillo-Escobar et al., 2019) (supplementary materials, Section 3).

5 Hardware circuit experiments

The experimental environment is based on the XILINX ZYNQ7000 platform, which includes the dual-core ARM Cortex-A9 component and the FPGA logic component. The geographic information encryption system formed by combining chaotic encryption sequences with scrambling and diffusion algorithms is mapped to ZYNQ. The experimental results are shown in Fig. 14, and the hardware resources used in the experiment are shown in Table 4.

The display screen in Fig. 14 displays the generated images from the ZYNQ experimental platform, and the images are exported as shown in Fig. 15, where

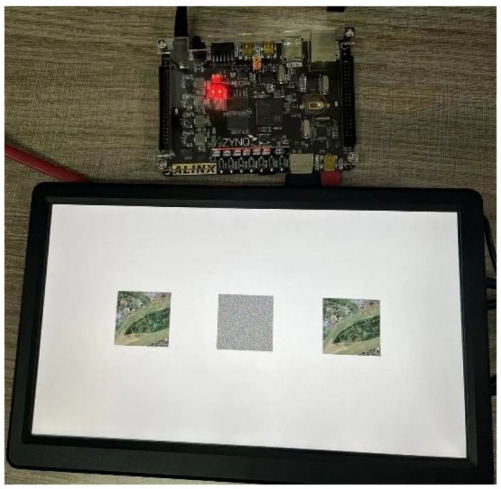

Fig. 14 Implementation and display of encryption system on ZYNQ experimental platform and screen

Table 4 Utilization of the FPGA hardware resources using ZYNQ7000 (xc7z020-2clg400I)

Resource	Utilization quantity	Utilization rate
LUT	5684	10.68%
LUTRAM	533	3.06%
FF	8843	8.31%
BRAM	66	47.14%
IO	9	7.20%
BUFG	2	6.25%
MMCM	1	25%

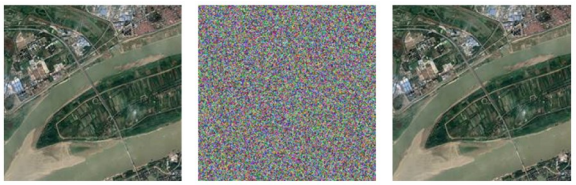

Fig. 15 Images in the display screen: (a) original; (b) encrypted; (c) decrypted

(a) is the original geographic information remote sensing image A, (b) is the encrypted image, and (c) is the decrypted image. The encrypted image is completely inconsistent with the original image, as shown by comparing (a) and (b); the original features of the image are hidden. The decrypted image is consistent with the original image when comparing (a) and (c), and the image is fully restored through the decryption circuit.

The proposed encryption system can perform secure communication correctly, and experimental and image data information can be hidden without losing data information. An excellent practical application effect is further proved by the hardware circuit experiment, which means that the geographic information encryption system based on Chaos-LSTM and CSP can be applied to multiple encryption scenarios.

6 Conclusions

To ensure the security and adaptability of chaotic encryption communication, a geographic information encryption system based on Chaos-LSTM and CSP is proposed in this paper, which is implemented on the ZYNQ platform. The encryption system's excellent confidentiality performance and practical application effects are proved by software testing and hardware experiments. The advantages and contributions of the proposed encryption system are as follows:

1. In chaotic encryption algorithms, the complexity of chaotic sequences determines the encryption performance. This paper combines chaotic systems and LSTM neural networks to construct a Chaos-LSTM model, avoiding the potential risk of output sequence periodization due to changes in the initial state and parameters of the chaotic system. The chaotic sequences generated by the proposed Chaos-LSTM model have higher SE complexity compared to those generated by the original chaotic system. There is no need for chaotic systems to generate long chaotic sequences, avoiding the periodicity that may occur due to excessively long chaotic sequences, and the new chaotic sequences have higher SE complexity.

2. The limited computational accuracy of computers can lead to periodicity in the output sequence of chaotic systems. The longer the chaotic sequence generated by the chaotic system, the greater the possibility of periodicity. This paper proposes and constructs the CSP algorithm for chaotic sequences. Through this algorithm, only a portion of the output sequences from the chaotic system needs to be selected to proliferate sufficient chaotic sequences for encryption.

3. The encryption system constructed in this paper can generate adaptive chaotic encryption sequences for encrypted objects, which can be applied to various encryption scenarios.

Future research direction: The constructed encryption system is currently used mainly for geographic information data encryption, and we will expand its application scenarios in future research. When the amount of information in the encrypted object is large, the encryption and decryption speed of the system is still relatively slow. We will continue to improve the algorithm and optimize the hardware to enhance the efficiency of the system's encrypted communication.

Contributors

Jia DUAN designed the research. Luanyun HU collected the data. Qiumei XIAO and Meiting LIU processed the data. Qiumei XIAO drafted the paper. Wenxin YU helped organize the paper. Qiumei XIAO finalized the paper.

Conflict of interest

All the authors declare that they have no conflict of interest.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

Alexan W, Elkandoz M, Mashaly M, et al., 2023. Color image encryption through chaos and KAA map. *IEEE Access*, 11:11541-11554. https://doi.org/10.1109/ACCESS.2023.3242311

Cao Y, Zhao YL, Wang Q, et al., 2022. The evolution of quantum key distribution networks: on the road to the Qinternet. *IEEE Commun Surv Tutor*, 24(2):839-894. https://doi.org/10.1109/COMST.2022.3144219

Chen X, Qian S, Yu F, et al., 2020. Pseudorandom number generator based on three kinds of four-wing memristive hyperchaotic system and its application in image encryption. *Complexity*, 2020:8274685. https://doi.org/10.1155/2020/8274685

De la Fraga LG, Mancillas-López C, Tlelo-Cuautle E, 2021. Designing an authenticated Hash function with a 2D chaotic map. *Nonl Dyn*, 104(4):4569-4580. https://doi.org/10.1007/s11071-021-06491-3

De la Fraga LG, Ovilla-Martínez B, Tlelo-Cuautle E, 2023. Echo state network implementation for chaotic time series prediction. *Microprocess Microsyst*, 103:104950. https://doi.org/10.1016/j.micpro.2023.104950

Gabr M, Korayem Y, Chen YL, et al., 2023. R^3—rescale, rotate, and randomize: a novel image cryptosystem utilizing chaotic and hyper-chaotic systems. *IEEE Access*, 11:119284-119312. https://doi.org/10.1109/ACCESS.2023.3326848

Gonzalez-Zapata AM, De la Fraga LG, Ovilla-Martinez B, et al., 2023. Enhanced FPGA implementation of echo state networks for chaotic time series prediction. *Integration*, 92: 48-57. https://doi.org/10.1016/j.vlsi.2023.05.002

Hosseinzadeh R, Zarebnia M, Parvaz R, 2019. Hybrid image encryption algorithm based on 3D chaotic system and choquet fuzzy integral. *Opt Laser Technol*, 120:105698. https://doi.org/10.1016/j.optlastec.2019.105698

Irfan M, Ali A, Khan MA, et al., 2020. Pseudorandom number generator (PRNG) design using hyper-chaotic modified robust logistic map (HC-MRLM). *Electronics*, 9(1):104. https://doi.org/10.3390/electronics9010104

Jia YQ, Shelhamer E, Donahue J, et al., 2014. Caffe: convolutional architecture for fast feature embedding. Proc 22nd ACM Int Conf on Multimedia, p.675-678. https://doi.org/10.1145/2647868.2654889

Lin HR, Wang CH, Cui L, et al., 2022. Hyperchaotic memristive ring neural network and application in medical image encryption. *Nonl Dyn*, 110(1):841-855. https://doi.org/10.1007/s11071-022-07630-0

Liu XC, Mou J, Zhang YS, et al., 2024. A new hyperchaotic map based on discrete memristor and meminductor: dynamics analysis, encryption application, and DSP implementation. *IEEE Trans Ind Electron*, 71(5):5094-5104. https://doi.org/10.1109/TIE.2023.3281687

Lorenz EN, 1963. Deterministic nonperiodic flow. *J Atmos Sci*, 20(2):130-141. https://doi.org/10.1175/1520-0469(1963)020<0130:DNF>2.0.CO;2

Man ZL, Li JQ, Di XQ, et al., 2021. Double image encryption algorithm based on neural network and chaos. *Chaos Sol Fract*, 152:111318. https://doi.org/10.1016/j.chaos.2021.111318

Martins P, Sousa L, Mariano A, 2017. A survey on fully homomorphic encryption: an engineering perspective. *ACM Comput Surv*, 50(6):83. https://doi.org/10.1145/3124441

Murillo-Escobar MA, Meranza-Castillón MO, López-Gutiérrez RM, et al., 2019. Suggested integral analysis for chaos-based image cryptosystems. *Entropy*, 21(8):815. https://doi.org/10.3390/e21080815

Murillo-Escobar MA, Cruz-Hernández C, Cardoza-Avendaño L, et al., 2022. Multibiosignal chaotic encryption scheme based on spread spectrum and global diffusion process for e-health. *Biomed Signal Process Contr*, 78:104001. https://doi.org/10.1016/j.bspc.2022.104001

Pareschi F, Rovatti R, Setti G, 2012. On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution. *IEEE Trans Inform Forens Secur*, 7(2):491-505. https://doi.org/10.1109/TIFS.2012.2185227

Rehman AU, Liao XF, Ashraf R, et al., 2018. A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2. *Optik*, 159:348-367. https://doi.org/10.1016/j.ijleo.2018.01.064

Sahu HK, Jadhav V, Sonavane S, et al., 2016. Cryptanalytic attacks on international data encryption algorithm block cipher. *Defence Sci J*, 66(6):582-589. https://doi.org/10.14429/dsj.66.10798

Teh JS, Alawida M, Sii YC, 2020. Implementation and practical problems of chaos-based cryptography revisited. *J Inform Secur Appl*, 50:102421. https://doi.org/10.1016/j.jisa.2019.102421

Tezcan C, 2022. Key lengths revisited: GPU-based brute force cryptanalysis of DES, 3DES, and PRESENT. *J Syst Archit*, 124:102402. https://doi.org/10.1016/j.sysarc.2022.102402

Tlelo-Cuautle E, Díaz-Muñoz JD, González-Zapata AM, et al., 2020. Chaotic image encryption using Hopfield and Hindmarsh–Rose neurons implemented on FPGA. *Sensors*, 20(5):1326. https://doi.org/10.3390/s20051326

Ullah S, Zheng JB, Din N, et al., 2023. Elliptic curve cryptography; applications, challenges, recent advances, and future trends: a comprehensive survey. *Comput Sci Rev*, 47:100530. https://doi.org/10.1016/j.cosrev.2022.100530

Wan YJ, Gu SQ, Du BX, 2020. A new image encryption algorithm based on composite chaos and hyperchaos combined with DNA coding. *Entropy*, 22(2):171. https://doi.org/10.3390/e22020171

Wu XJ, Kan HB, Kurths J, 2015. A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. *Appl Soft Comput*, 37:24-39. https://doi.org/10.1016/j.asoc.2015.08.008

Wu XJ, Wang DW, Kurths J, et al., 2016. A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. *Inform Sci*, 349-350:137-153. https://doi.org/10.1016/j.ins.2016.02.041

Xiong PY, Jahanshahi H, Alcaraz R, et al., 2021. Spectral entropy analysis and synchronization of a multi-stable fractional-order chaotic system using a novel neural network-based chattering-free sliding mode technique. *Chaos Sol Fract*, 144:110576. https://doi.org/10.1016/j.chaos.2020.110576

Xu SC, Wang XY, Ye XL, 2022. A new fractional-order chaos system of Hopfield neural network and its application in image encryption. *Chaos Sol Fract*, 157:111889. https://doi.org/10.1016/j.chaos.2022.111889

Yan S, Gu Z, Park JH, et al., 2023. Synchronization of delayed fuzzy neural networks with probabilistic communication delay and its application to image encryption. *IEEE Trans Fuzzy Syst*, 31(3):930-940. https://doi.org/10.1109/TFUZZ.2022.3193757

Yu F, Zhang ZN, Shen H, et al., 2022. FPGA implementation and image encryption application of a new PRNG based on a memristive Hopfield neural network with a special activation gradient. *Chin Phys B*, 31(2):020505. https://doi.org/10.1088/1674-1056/ac3cb2

Yu Y, Si XS, Hu CH, et al., 2019. A review of recurrent neural networks: LSTM cells and network architectures. *Neur Comput*, 31(7):1235-1270. https://doi.org/10.1162/neco_a_01199

List of supplementary materials

1 NIST tests and TestU01 tests

2 Comparison of encryption performance

3 Encryption quality analysis

Table S1 NIST and TestU01 tests of chaos proliferation sequences

Table S2 Comparison of NPCR, UACI, and information entropy

Table S3 Quality metrics analysis

Fig. S1 The plain and encrypted image of colored Lena

Fig. S2 Column floating frequency (CFF) and its mean

Fig. S3 Row floating frequency (RFF) and its mean