IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 14 February 2023, accepted 22 February 2023, date of publication 1 March 2023, date of current version 7 April 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3250758

RESEARCH ARTICLE

An Algorithm Based on Hodgkin-Huxley Model and Latin Square for Image Encryption

CHENCHEN HE, ZHONG CHEN, XIYU SUN, AND LUJIE WANG
College of Computer Science and Technology, Hengyang Normal University, Hengyang 421002, China
Hunan Provincial Key Laboratory of Intelligent Information Processing and Application, Hengyang 421002, China

Corresponding author: Zhong Chen (chenzhong@hynu.edu.cn)

This work was supported in part by the Scientific Research Fund of Hunan Provincial Education Department under Grant 19A066, and in part by the Science and Technology Innovation Program of Hunan Province under Grant 2016TP1020.

ABSTRACT Image transmission is happening more frequently in this era of technologically sophisticated digital information. Additionally, more individuals are becoming aware of its importance. In order to secure images, many academics are participating in research, which is advantageous for guaranteeing data security. In order to strengthen the security of images during transmission, we have investigated new encryption algorithms to guarantee this. First, a current representing the Lorenz chaotic system is introduced into the neuron model. The neuron model generates sequences after receiving the current signal. The next move is made as the current shifts depending on whether the resulting sequences are chaotic or not. If so, the subsequent operation is carried out; otherwise, the current is altered until chaotic sequences are produced. Second, a global scrambling with de-duplication technique is used to scramble the image using the resulting chaotic sequences. To complete the dislocation effect, the Latin square is used to dislocate the image after the initial dislocation. Fourth, the image that has been scrambled is subjected to two rounds of additive mode diffusion. They are diffusion in the forward additive mode and diffusion in the inverse additive mode. Lastly, to improve the diffusion effect, the image is diffused in the finite domain. Eventually, the encrypted image is obtained. After evaluation tests and comparison with related literature, it can be found that the algorithm of this study has certain advantages. Also, the resistance to attack is good. It can protect the security of the image.

INDEX TERMS Image encryption, Lorenz system, Hodgkin-Huxley model, Latin square.

I. INTRODUCTION

The development of technology has facilitated the advancement of life quality [1]. High-tech electrical products are gradually becoming more prevalent in everyday life. The frequent use of intelligent devices is a notable performance [2]. As technology advances, electronic data are increasingly the preferred form of communication with partners. The study of data security is particularly crucial in this situation of constant information exchange [3]. The security of the images, in addition to the data, is crucial to the transmission process [4]. Therefore, it follows that the study of network security is also related to the security of images. Because of the limitations of data transmission technologies at the beginning of technological development, image encryption was not widely used [5]. Additionally, digital communication did not gain much popularity. These caused the importance of image encryption not to be adequately portrayed. As the information era has progressed, it appears that user-to-user communication can no longer be fully satisfied by straightforward data exchange [6]. Images appear to be better able to convey the feelings that users want to express and to convey more information. In this instance, visual communication between consumers is becoming more common. Users may not care whether image information is shared in some circumstances [7]. It is clear from various perspectives in life that the exposure of information would harm the users' privacy. For instance, patient-related data, which contain personal data

The associate editor coordinating the review of this manuscript and approving it for publication was Yiming Tang.

about the patient and any associated medical issues, is data that relates to patients. Nobody wants other people to learn about their trouble areas [8]. In biometric images, it is mainly used for facial fingerprints and irises, which are used for smartphone payments, ticket entry and so on. Sharing daily life with friends is a regular occurrence for people. Unscrupulous individuals may use it in the incorrect locations if they know this. The safety will be in danger if someone learns about the trip and tries to do a harm [9]. The military's worth is considerably evident. The national capital has anything to do with a nation's military secrets. The negative impact of leakage is likewise impossible to calculate [10]. Thus, the topic of image information security research is never out of date.

Image encryption has made extensive use of chaos encryption. The main reason is that some characteristics of chaotic systems can be applied to encrypt the image which can ensure the security of images. Besides, Chai et al. [11] found that there are two categories of digital images' chaotic-based encryption systems. The one is low-dimensional systems. A typical representative of this type is the one-dimensional mapping. The other is high-dimensional systems. It mainly including hyperchaotic systems. When using, the low-dimensional chaotic mapping is more widely used. This is due to its simple structure and ease of use. However, it also has the problem of small key space that makes it low security [12]. In [13], it utilizes the Knuth-Durstenfeld algorithm to encrypt digital images using a chaotic system of hidden attractors. Because of the hidden attractor, the attraction basin does not intersect any small neighborhood of the equilibrium. It is hard for an attacker to make the attractor in balance if it is reconstructed. The scheme uses DNA sequence operations for diffusing image pixel values and has good encryption performance. In [14], Hu and Li designed a system. The system constructed on a certain unit transformation. It combined two one-dimensional chaos systems to get better performance. But The randomness of this system does not enable. Until today, researchers have not stopped studying chaotic image encryption.

Image encryption is also used in other fields where related technologies are used. A complex network is a good example. In [15], it proposed a system that researched fractional-order discrete Hopfield neural network and its dynamic behavior and synchronization to apply in image encryption. In [16], it used periodic self-triggered impulsive sampling to make neural networks into a state of chaotic synchronization and apply it in image encryption. In [17], the delaying time of Markovian jumping is discussed. The bidirectional associative memory neural networks are discussed, too. Synchronization criteria as well as their applications in image also cannot be ignored. In [18], it designed an impulsive synchronization by using coupled delayed neural networks and actuator saturation and used it to encrypt the image. In [19], it uses periodic self-triggered intermittent sampled-data control to investigates the exponential synchronization issue. The synchronization issue is based on time-varying multi-weights network with time delays. And this paper applies it in image encryption. To a large extent, applying research in these other fields to image encryption provides new ideas for image information assurance.

On the other hand, research on image encryption combined with deep learning has also seen some. He et al. [20] achieved good results by using the network structure of long short-term memory (LSTM) for image dislocation. Though they didn't use the learning function of deep learning in diffusion stage. The result of the experiment was tested that has good resistance. Sangiorgio furtherly verified that using LSTM to predict chaotic time series gives good results and achieves good robustness [21]. This kind of technical tools are also not yet developed enough. But it has encouraged additional image encryption researchers to join it.

Aside from traditional chaotic digital encryption methods, neuron models have also made some research results in image encryption. Xu and Chen [22] use Hopfield neural network applying in optical image encrypted. To generate chaotic sequences and chaotic random phase masks, the algorithm employs a Hopfield neural network. Initially, the initial image is decomposed into subsignals by a wavelet packet transform and after the scrambling, the adaptive classification is performed on the subsignals again. And the subsignals are divided into two categories. The dual random phase coding encoded in the 4F system [23]. What's more, the Fresnel region is implemented on the two layers. Using their standard deviations, the subsignals are transformed differently to ensure information security. In [24], it uses BP neural network to compress and encrypt images. Xu and Chen [25] proposed a remote sensing image encryption way which was based on chaotic neurons and tent mapping. In this method, it used the hash value of the plaintext image to generate the initial key. As an example, the research uses GF-2 multispectral image. And the experiment was carried out in the actual site. It has good application value. The neuron model has good application prospects. It is convenient to be built on Field Programmable Gate Array. Neuron application to image encryption has not been studied much. It still has places that can be mined.

The Lorenz chaos system is classical in image encryption and has excellent chaotic properties [26]. The HH model is a biological model. It has been used in text encryption, showing a good effect [27]. Nevertheless, it has never been used to encrypt images. In the traditional method, the Lorenz system is used in image encryption to generate direct chaotic sequences and perform other operations on the image [28]. In this paper, in the first permutation process, chaotic sequences are generated. Before confusion, a de-duplication operation is performed on the generated chaotic sequences, which can ensure the non-duplication of chaotic sequences. The image is transformed into a one-dimensional vector and performs a first-tail permutation operation. This approach gives the effect of non-repetition to a certain

extent, thus achieving the purpose of global dislocation. The SHA-256 algorithm is used in the second scrambling stage to construct the orthogonal Latin square to encrypt the image. This method uses keys more resistant to attacks and constructs a more complex Latin square. In the diffusion phase, in addition to the additive modulo-diffusion algorithm, finite fields are also used in it. The finite domain is a piece of very important knowledge in the field of information security. The concept of domain is a generalization of the number field and the quadratic operations. Its importance can be imagined. Using finite domain can achieve a better diffusion effect. A combination of these methods is used in this paper, which possesses some innovation. After some relative evaluation tests, it shows that the improvement of each technology makes the total encryption effect, and it also presents well.

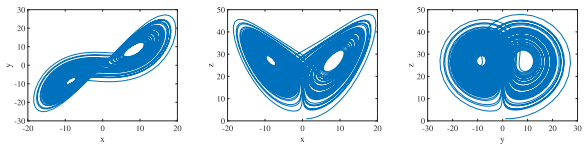
II. PRELIMINARIES

A. LORENZ SYSTEM

The Lorenz system [29] was obtained in 1963 by the American scientist Lorenz during his research on weather forecasting by three-dimensional reduction of the Rayleigh-Bernard thermal convection problem for infinite-dimensional dynamical systems. Lorenz chaos mapping is a three-dimensional dynamical system that generates chaotic flows. Lorenz oscillators are a kind of attractor known for their double-new line shape. The equation of the Lorenz system is shown as Eq (1):

$$\begin{cases} \frac{dx}{dt} = \sigma(y - x) \\ \frac{dy}{dt} = \alpha x - zx - y \\ \frac{dz}{dt} = xy - \beta z \end{cases} \tag{1}$$

when the parameters $\sigma = 10, \alpha = 28, \beta = 8/3$, the initial values are [1,1,1]. The phase space diagrams of the system are shown as Fig. 1:



(a) (b) (c)

FIGURE 1. The projections of Lorenz attractor. (a) x-y plane. (b) x-z plane. (c) y-z plane.

B. HODGKIN-HUXLEY MODEL

The Hodgkin-Huxley model (HH model) is a model applying in computational neuroscience. It is the closest mold to the biological reality [30]. The electrical activity of neuronal which is at the ionic level is described. Ion channels are found in the membrane of neuronal cells including sodium and potassium. Besides there are also leaky channels. This kind of channels can control a few inorganic salt ions. The ability of ions to flow through the channel depends on the gating protein. This property is the selective permeability of the cell membrane. It is this property that allows neurons to generate abundant electrical activity. The ability of ions to flow through the channel depends on the gating protein. This property is the selective permeability of the cell membrane. It is this property that allows neurons to generate abundant electrical activity. Mathematically, the effect of ion channel conductance is the same as the binding of gating proteins. This has an effect on the state of the ion channel. The HH model can be equated the cell membrane as a circuit diagram which is shown as Fig. 2:

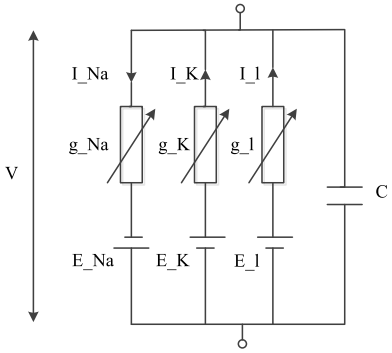


FIGURE 2. HH model equivalent circuit diagram.

This model can be expressed using a fourth-order differential equation as follows:

$$\begin{cases} \frac{dV}{dt} = \frac{1}{C_M}(I - \bar{g}Nam^3h(V - V_{Na}) \\ \qquad -\bar{g}Kn^4(V - V_k) - \bar{g}l(V - V_l)) \\ \frac{dm}{dt} = \alpha_m(1 - m) - \beta_m m \\ \frac{dh}{dt} = \alpha_h(1 - h) - \beta_h h \\ \frac{dn}{dt} = \alpha(1 - n) - \beta_n n \end{cases} \tag{2}$$

where V is the transmembrane voltage; M is the activation variable of sodium ion; h is the inhibition variable of sodium ion; n is the activation variable of potassium ion; I is external stimulus current; V_{Na} denotes equilibrium potential of sodium ion.V_K and V_l denote equilibrium potential of potassium ion and equilibrium potential of leakage ion respectively; $\bar{g}Na$, $\bar{g}K$ and $\bar{g}l$ represent the maximum conductivity of sodium ion channel, potassium ion channel and leakage ion channel, respectively.α_m,β_m,α_h,β_h,α_n and β_n are derived from experimental data. They can be described as follows:

$$\alpha_m(V) = \frac{\bar{\alpha}_m(V - \bar{V}_m)}{1 - \exp[-(V - \bar{V}_m)/K_{\alpha_m}]} \tag{3}$$

$$\beta_m(V) = \bar{\beta}_m \exp(-V/K_{\beta_m}) \tag{4}$$

$$\alpha_h(V) = \bar{\alpha}_m \exp(-V/K_{\alpha_h}) \tag{5}$$

$$\beta_h(V) = \frac{\bar{\beta}}{1 + \exp[-(V - \bar{V}_h)/K_{\beta_h}]} \tag{6}$$

$$\alpha_n(V) = \frac{\bar{\alpha}_n(V - \bar{V})}{1 - \exp[-(V - \bar{V}_n)/K_{\alpha_n}]} \tag{7}$$

$$\beta_n(V) = \bar{\beta}_n \exp(-V/K_{\beta_n}) \tag{8}$$

The study of chaos in this model can be approached from two aspects. On the one hand, the effect of external chaotic signals on the HH model can be studied. On the other hand, the chaotic nature of the HH model can be investigated by introducing periodic current stimuli. The chaotic sequence generated by Lorenz system is used as the current input into the HH model in this paper.

C. ORTHOGONAL LATIN SQUARE

There is a global game called Sudoku derived from the Latin square. A Latin square is an $n \times n$ square in which there are exactly n different elements. And each element appears only once in the same row or column [31]. The term Latin square comes from the Swiss mathematician and physicist Euler. He used Latin alphabet as a symbol for the elements in a Latin square. A common four-dimensional Latin square and a common five-dimensional Latin square are shown as Fig. 3 respectively:

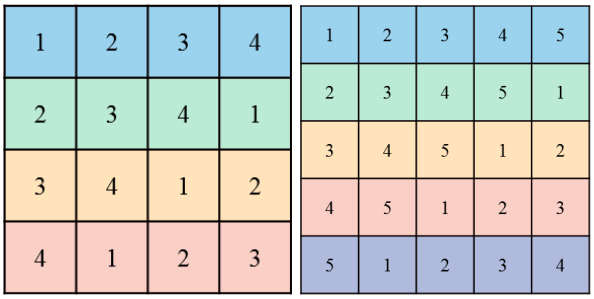


FIGURE 3. (a) is a 4×4 Latin square. (b) is a 5×5 Latin square.

Two Latin squares which have the same placement can combine into a tuple and combined into a new matrix. When every element in this new matrix is unique, the sum of Latin squares is orthogonal to each other. In this case, the sum is a pair of orthogonal Latin squares. If the order is fixed, orthogonal Latin square family is made up of a set of all two orthogonal Latin squares. When n is 3, if there are two Latin squares A_1 and A_2, they can form an orthogonal Latin square A_3. The process is shown as Fig. 4:

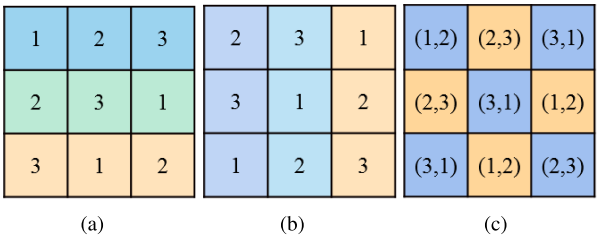


FIGURE 4. Construct a 3×3 orthogonal Latin square. (a) is A_1. (b) is A_2. (c) is A_3.

There are various methods to despeckle the image with the research of encryption algorithms. Some common desarrangement methods are row desarrangement, column desarrangement, fractal desarrangement, etc. These strategies have been used to encrypt images. In this paper, it uses such methods for the second scrambling of the image. The speed of image scrambling using orthogonal Latin square is very fast [32]. This gives good security to the image during transmission.

D. ADDITIVE MODE DIFFUSION ALGORITHM

The additive mode diffusion algorithm is a diffusion algorithm that is widely used in image encryption [33]. There are two algorithm processes: forward encryption and reverse encryption. Unlike ordinary calculations, the calculation of pixel values in images cannot be done only according to arithmetic values, as it cannot be displayed if the pixel value exceeds 256. For this reason, the calculated pixel value is also modulo 256 to ensure that the pixel value can be displayed properly. The positive process is from i to MN, and its calculation expression is as follows:

$$C_i = (C_{i-1} + S_i + P_i) \bmod 256 \tag{9}$$

The positive process reduction equation is as follows:

$$P_i = (2 \times 256 + C_i - C_{i-1} - S_i) \bmod 256 \tag{10}$$

The negative process is from MN to 1, the formula is as follows:

$$C_i = (C_{i+1} + S_i + P_i) \bmod 256 \tag{11}$$

The inverse process reduction equation is as follows:

$$P_i = (2 \times 256 + C_i - C_{i+1} - S_i) \bmod 256 \tag{12}$$

where C represents the cipher text cipher, P represents the plain text image, and S is the pseudo-random number vector.

E. FINITE FIELD

In cryptography, a finite field is an important domain. Its representation is GF(p), where p is a prime number. The modulo operation is the computational algorithm it implies. It's also a finite collection of integers. This paper's diffusion is based on finite fields GF (257). GF (257) = {0, 1, . . . , 256}. In the multiplication operation,0 in easily gives loss of information. Therefore, a better approach is to eliminate 0 before performing the calculation. So, in the text the remaining 255 elements are used. This diffusion of finite fields allows to diffuse all the pixel points at any position of the image. The two-dimensional image matrix of the image is reshaped into a one-dimensional vector in rows or columns, defined as P. C and S are the cipher vectors. As for the forward diffusion algorithm, i is from 1 to MN, and its inverse operation is shown in Eq. (13) and Eq. (14):

$$C_i = C_{i-1} \times S_i \times P_i \tag{13}$$

$$P_i = C_i \div C_{i-1} \div S_i \tag{14}$$

where M is the number of rows in the matrix and N is the number of columns in the matrix. The reverse diffusion

algorithm is i from MN to 1, and its inverse operation are shown in Eq. (15) and Eq. (16), respectively:

$$C_i = C_{i+1} \times S_i \times P_i \tag{15}$$

$$P_i = C_i \div C_{i+1} \div S_i \tag{16}$$

The multiplication used above is satisfied with finite field. The division used above is also satisfied with finite field. It is used in the diffusion phase of this paper.

III. PROPOSED STRATEGIES

A. ENCRYPTION PROCESS

This research uses Lorenz system, Hodgkin-Huxley model, orthogonal Latin square additive mode diffusion, and finite field to realize an image encryption algorithm. The encryption process is described as follows:

Step1: The Lorenz system generates a chaotic sequence and inputs it to the HH model in the form of current. The effects of external chaotic signals on the firing patterns of Hodgkin-Huxley neurons were studied by Lorenz system simulation and injected into neurons in the form of electric current. Introducing external chaotic signals. The expression of the HH model is as follows:

$$C_M \frac{dV}{dt} + \overline{g}_{Na} m^3 h(V - V_{Na}) + \overline{g}_K n^4 (V - V_K) + \overline{g}_l (V - V_l) = I_{chaos} \tag{17}$$

where $I_{chaos} = x(t)$ is the chaos current.

Step2: The HH model discharges and judges whether the HH model has entered a chaotic state by observing the value of the Lyapunov exponent. If the conditions are met, proceed to the next step. Otherwise, continue to discharge. To study the relationship between the HH model's discharge law and the Lorenz system's control parameter α, unbounded variables need to be fixed values. It makes that $\sigma = 10$, $\beta = 8/3$, $x_0 = y_0 = z_0 = 1$, starting from $\alpha = 0$, the experiment was performed on $\alpha \in (0,100)$ continuously changing α with a step size of 0.1, and the response curve of the transmembrane voltage to the control parameter α was obtained and is shown as Fig. 5:

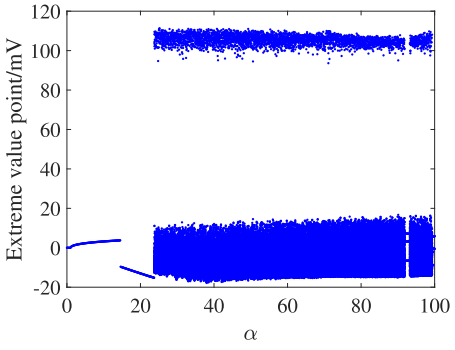
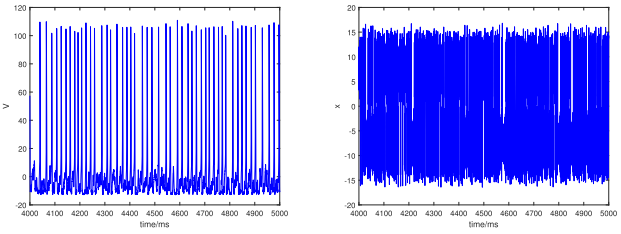


FIGURE 5. Plot of the distribution of extreme value points.

When $\alpha = 24$, the external stimulus current $I_{chaos} = x(t)$ generated by the Lorenz system is a chaotic current. The neuronal firing pattern is chaotic firing. The transmembrane voltage is taken as a random value. The diagram of this state is shown as Fig. 6.



(a) (b)

FIGURE 6. (a) is $\alpha = 24$ v-t chart. (b) is $\alpha = 24$ sequence chart.

Step3: The values of the relevant parameters of the HH model in the chaotic state are recorded. And the model will generate chaotic sequences.

Step4: While receiving an image that needs to be encrypted, scramble it according to the chaotic sequences generated in Step3.

Step5: Use the scrambled image and the key hash value set to construct an orthogonal Latin square using the SHA-256 algorithm, and perform further scrambling operations on the image according to the constructed orthogonal Latin square. The main approach can be seen as a three-step process. First, calculate the hash value of the plaintext image input from the previous step and the hash value of the key set by yourself through the SHA-256 algorithm. Use these them to construct two 16×16 Latin square matrixes. Then construct a large 256×256 orthogonal Latin square from these two small Latin squares. Finally, according to the constructed Latin square matrix, the image matrix, after being scrambled in the previous step, is scrambled again to achieve the effect of a fully scrambled image.

Step6: Use the pseudo-random sequence generated in Step3 to perform two addition modulo diffusion on the image after the operation Step5.

Step8: Perform a finite field diffusion operation on the image diffused from last step to fully diffuse the image.

Step9: The image obtained is the encrypted image.

The flowchart of the encryption process of this paper is shown as Fig. 7.

B. DECRYPTION PROCESS

The decryption process is the inverse of the encryption process. The steps are as follows and the flowchart is shown as Fig. 8.

Step1: Receive the Lorenz system discharge status parameters recorded from the encryption process. The Lorenz system generates a chaotic sequence and inputs it to the HH model in the form of current

Step2: The HH model discharges and enters a chaotic state and generates a chaotic sequence.

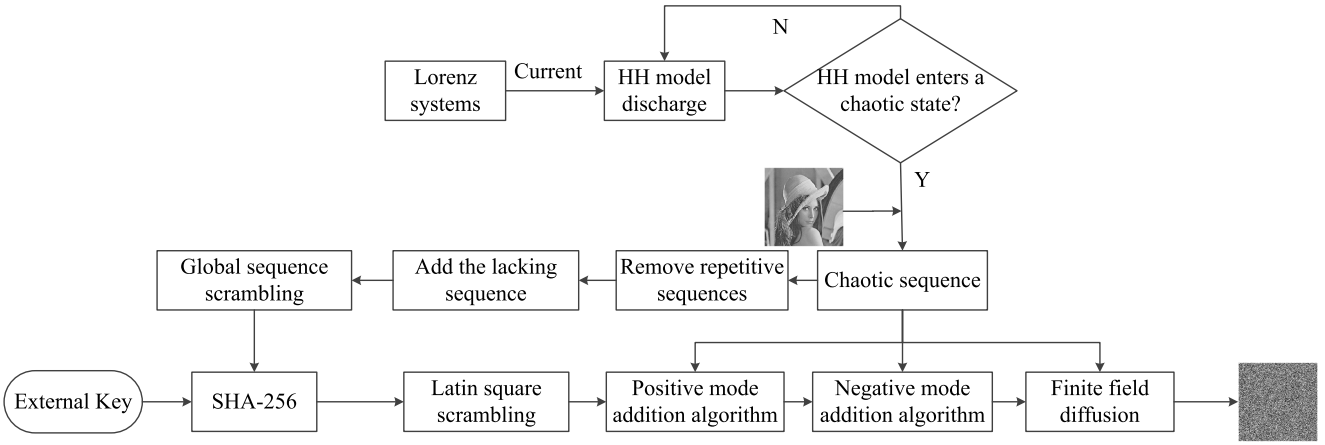


FIGURE 7. Encryption flow chart.

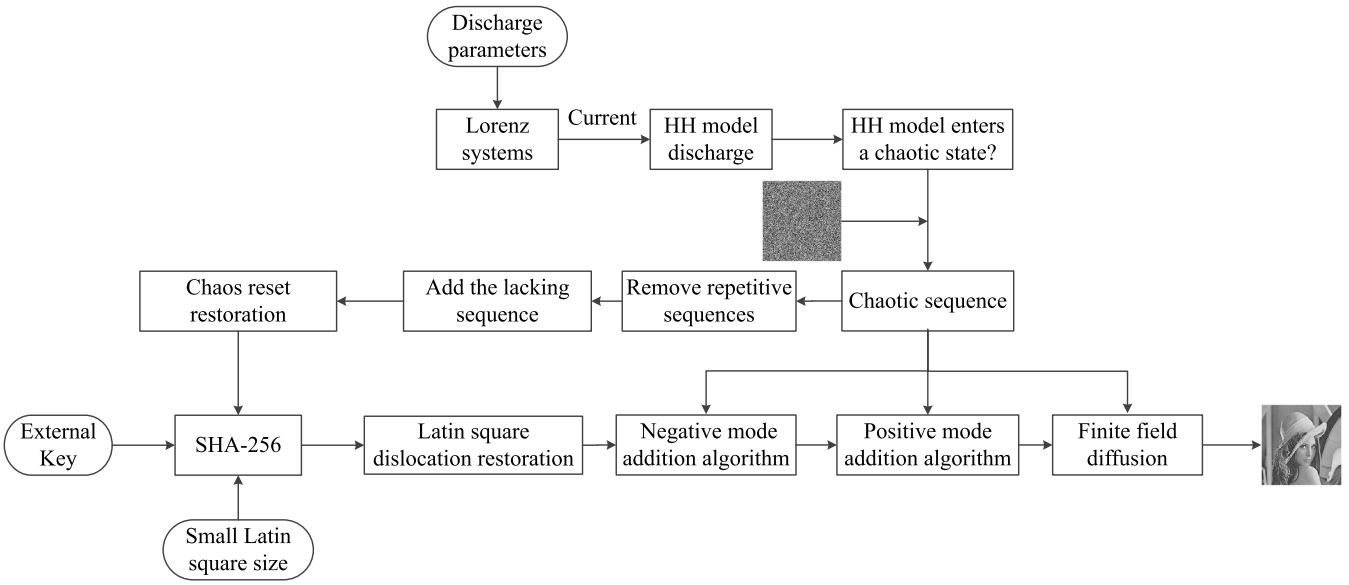


FIGURE 8. Decryption flow chart.

Step3: Input the encrypted image, perform the operation of removing duplicates from the generated chaotic sequences, and add the missing sequences according to the specific sequences.

Step4: The generated chaotic sequence is used to perform chaotic sequence dislocation reduction on the encrypted image.

Step5: Receive the image generated in Step4 and perform a second chaos reduction of the image using the key values used and the size of the small Latin square.

Step6: The image in Step5 is subjected to the additive mode diffusion inverse operation.

Step7: The image generated in Step6 is subjected to a finite field diffusion inverse operation.

Step8: The cipher image finishes decrypting.

IV. RESULT AND EVALUATION

A. CORRELATION COEFFICIENT

The correlation coefficient is a test of the correlation between adjacent pixels. Usually, the adjacent pixels of encrypted images are lower. In order to evaluate the correlation between adjacent pixels, the correlation coefficient is used in the experiment. It can't be less than -1 and can't be greater than 1. The goodness of the algorithm depends on how close the value of the correlation is to zero [34]. The calculation formula is defined as:

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{18}$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{19}$$

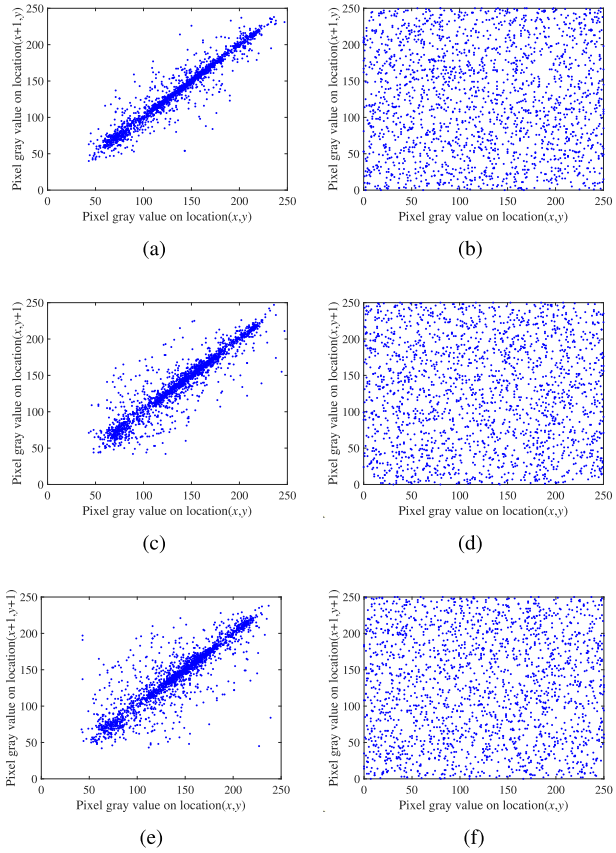


FIGURE 9. Correlation of two adjacent pixels. (a),(c) and (e) are from original image.(b),(d) and (f) are from cipher image.(a) and (b) horizontal direction; (c) and (d) vertical direction; (e) and (f) diagonal direction.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{20}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \tag{21}$$

where r_{xy} means the correlation coefficient. x is the gray value of a pixel randomly, and y is near it. N represents the number of selected sample points, $E(x)$ is the mean, $D(x)$ is the variance, and $cov(x, y)$ is the covariance.

An algorithm produces different results for different images. Encrypt different images using this algorithm and perform correlation tests. By comparing with other related articles, the results are listed in Table 1. In the part of experiment, the correlation coefficient of Lena and encrypted Lena are shown as Fig 9.

Through the encryption algorithm in this experiment, the correlation between adjacent pixels will be extremely low. Compared with related literature, it can be found that the scrambling effect is better than most algorithms.

B. NOISE AND DATA CUT ATTACK

Digital images are vulnerable to attacks during transmission. Common attacks include noise attacks, clipping attacks and so on [40]. For this case, a better treatment is to restore as much of the original image as possible.

In order to test the effectiveness of the encryption algorithm against attacks, this paper simulates the cipher image under attack and tests the effect of restoring the original image after being attacked. The pepper noise attacks of 0.002 and 0.005 and the cut attacks of 32 × 32 and 64 × 64 are used. The results of the experiments are shown as Fig. 10.

Peak Signal to Noise Ratio (PSNR) is a quantitative metric to evaluate the quality of the decrypted image. The value needs to be big enough to ensure the high quality but no more than 35. The mean squared error (MSE) can measure the archival squared error. The Structural Similarity (SSIM) are used for quantitative measurement. For an image, if the size is MN, PSNR, MSE and SSIM values can be calculated using the following relationship.

$$PSNR = 10 \times \log_{10}\frac{255^2}{MSE}(db) \tag{22}$$

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(I_O(i,j) - I_D(i,j))^2 \tag{23}$$

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + I_O(i,j))(2\sigma_{xy} + I_D(i,j))}{(\mu_x^2 + \mu_y^2 + I_O(i,j))(\sigma_x^2 + \sigma_y^2 + I_D(i,j))} \tag{24}$$

The PSNR and MSE when four attacks were tested on ''Lena'' are listed in Table 2.

According to the images after the restoration of the attack and on the parameter values, the information of the original image can still be recovered to some extent even after some attacks.

C. NPCR AND UACI

Number of Pixels Change Rate (NPCR) is a index to measure the rate of change of pixel values. It changes a pixel value from original image and encrypts it, and then analyzing the effect with the original image after encryption. Unified Average Changing Intensity (UACI) uses the same image as it does. But the function of this index is to measure the average intensity of the change between images. They can be defined as follows:

$$NPCR(C_1, C_2) = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{D(i,j)}{M \times N} \times 100\% \tag{25}$$

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

$$UACI = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C_1(i,j) - C_2(i,j)|}{M \times N \times T} \times 100\% \tag{27}$$

where M, N, T are the width, height gray value of the image respectively. C_1 is the cipher image of original image. C_2 is

TABLE 1. Correlation coefficient.

		Lena	Baboon	Pepper	Plane	Boat	Average
Proposed	Horizontal	0.0082	0.0049	0.0033	0.0035	0.0034	0.00470
	Vertical	0.0041	0.0032	0.0031	0.0052	0.0033	0.00383
	Diagonal	0.0038	0.0039	0.0043	0.0034	0.003	0.00373
Hua et al. [35]	Horizontal	0.0074	0.0113	0.0196	0.0055	0.0014	0.00904
	Vertical	0.0096	0.0005	0.0165	0.0014	0.0181	0.00922
	Diagonal	0.0193	0.0136	0.0210	0.0083	0.0066	0.01376
Wu et al. [36]	Horizontal	0.0037	0.0026	0.0016	0.0001	0.0001	0.00162
	Vertical	0.0032	0.0009	0.0059	0.0031	0.0031	0.00324
	Diagonal	0.0041	0.0052	0.0034	0.0015	0.0015	0.00314
Niyat et al. [37]	Horizontal	0.0061	0.006	0.0049	0.0054	0.0085	0.00618
	Vertical	0.0116	0.0058	0.0031	0.0089	0.0092	0.00772
	Diagonal	0.0018	0.0016	0.0079	0.0021	0.0024	0.00316
Enayatifar et al. [38]	Horizontal	0.0023	0.0059	0.0037	0.0062	0.0073	0.00508
	Vertical	0.0019	0.0041	0.0258	0.0074	0.0109	0.01002
	Diagonal	0.0011	0.0028	0.0079	0.0009	0.0016	0.00286
Hosny et al. [39]	Horizontal	0.0069	0.0065	0.0211	0.0229	0.0138	0.01424
	Vertical	0.0479	0.0337	0.0129	0.0103	0.0093	0.02282
	Diagonal	0.0075	0.0244	0.0013	0.0100	3.4412×10^{-6}	0.01080
Wang X [32]	Horizontal	0.0021	0.0005	-0.0025	0.0023	-0.0068	-0.00088
	Vertical	0.0060	0.0051	-0.0040	-0.0013	0.0041	0.00198
	Diagonal	-0.0005	-0.0034	-0.0015	0.0037	-0.0044	-0.00122

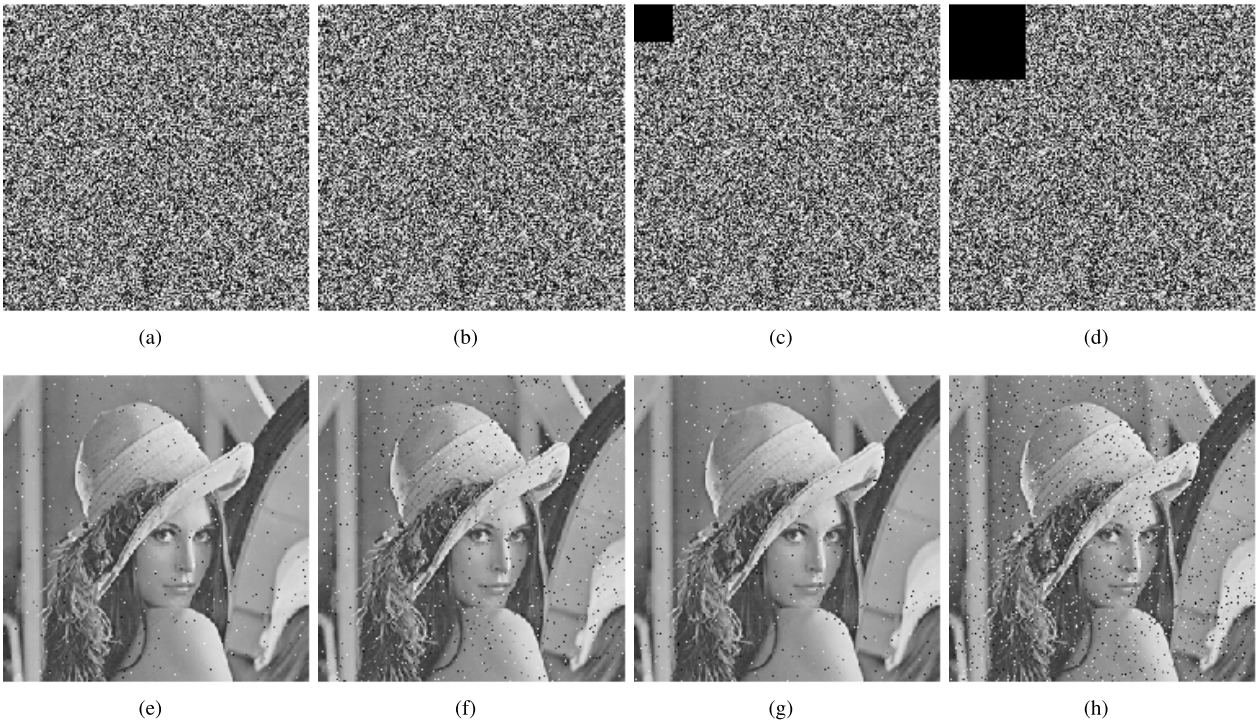


FIGURE 10. (a) noisy encrypted image with 0.002, (b) noisy encrypted image with 0.005; (c) encrypted image with 32 × 32 data cut. (d) encrypted image with 64 × 64 data cut. (e-h) the encryption image of (a-d).

also the cipher image but has change the value of one of pixels of the image originally. The NPCR and UACI tested in the experiment are shown in Table 3 including other papers which also have used the same images.

The comparison of the tabular data shows that the algorithm in this paper achieves a good level compared with other related papers.

D. HISTOGRAM ANALYSIS

Histogram analysis begins with statistics on the sample data and ends with a two-dimensional graphic expressing the distribution state of the data. The coordinates represent the grayscale picture level as well as the quantity or probability of the associated pixel appearing in the image. This indicator is a critical assessment metric for the encryption algorithm's

TABLE 2. PSNR and MSE values for noise and data cut attacks.

Standard Grayscale Images	Lena			Baboon			Pepper		
	PSNR	MSE	SSIM	PSNR	MSE	SSIM	PSNR	MSE	SSIM
Salt and Pepper with noise level 0.002	31.441	26.6935	0.996	31.5539	26.8004	0.9961	31.7749	27.0427	0.9961
Salt and Pepper with noise level 0.005	27.7443	22.9968	0.9908	27.8204	23.0669	0.9898	27.6965	22.9642	0.9901
Data cut with block size 32×32	22.7471	17.9996	0.9839	22.8281	18.0746	0.9839	22.8507	18.1185	0.9838
Data cut with block size 64×64	16.7814	12.034	0.9364	16.7266	11.9731	0.9361	16.7496	12.0174	0.936

TABLE 3. NPCR and UACI of grayscale images for different image encryption algorithms.

image	Lena		Baboon		Pepper		Plane		Boat		Average	
	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
Proposed	99.615	33.509	99.612	33.487	99.610	33.488	99.613	33.475	99.611	33.483	99.612	33.488
Hua et al. [35]	99.585	33.558	99.631	33.453	99.623	33.681	99.603	33.475	99.568	33.363	99.602	33.506
Wu et al. [36]	99.620	33.417	99.593	33.382	99.608	33.495	99.623	33.623	99.612	33.661	99.611	33.516
Niyat et al. [37]	99.622	33.416	99.608	33.413	99.660	33.442	99.653	33.509	99.605	33.506	99.630	33.457
Enayatifar et al. [38]	99.519	33.585	99.105	33.252	98.498	32.948	99.418	33.525	99.251	33.393	99.158	33.341
Hosny et al. [39]	99.625	33.423	99.594	33.461	99.603	33.427	99.602	33.505	99.608	33.419	99.606	33.447
Wang X [32]	99.605	33.472	99.593	33.461	99.605	33.506	99.602	33.460	99.607	33.512	99.602	33.482

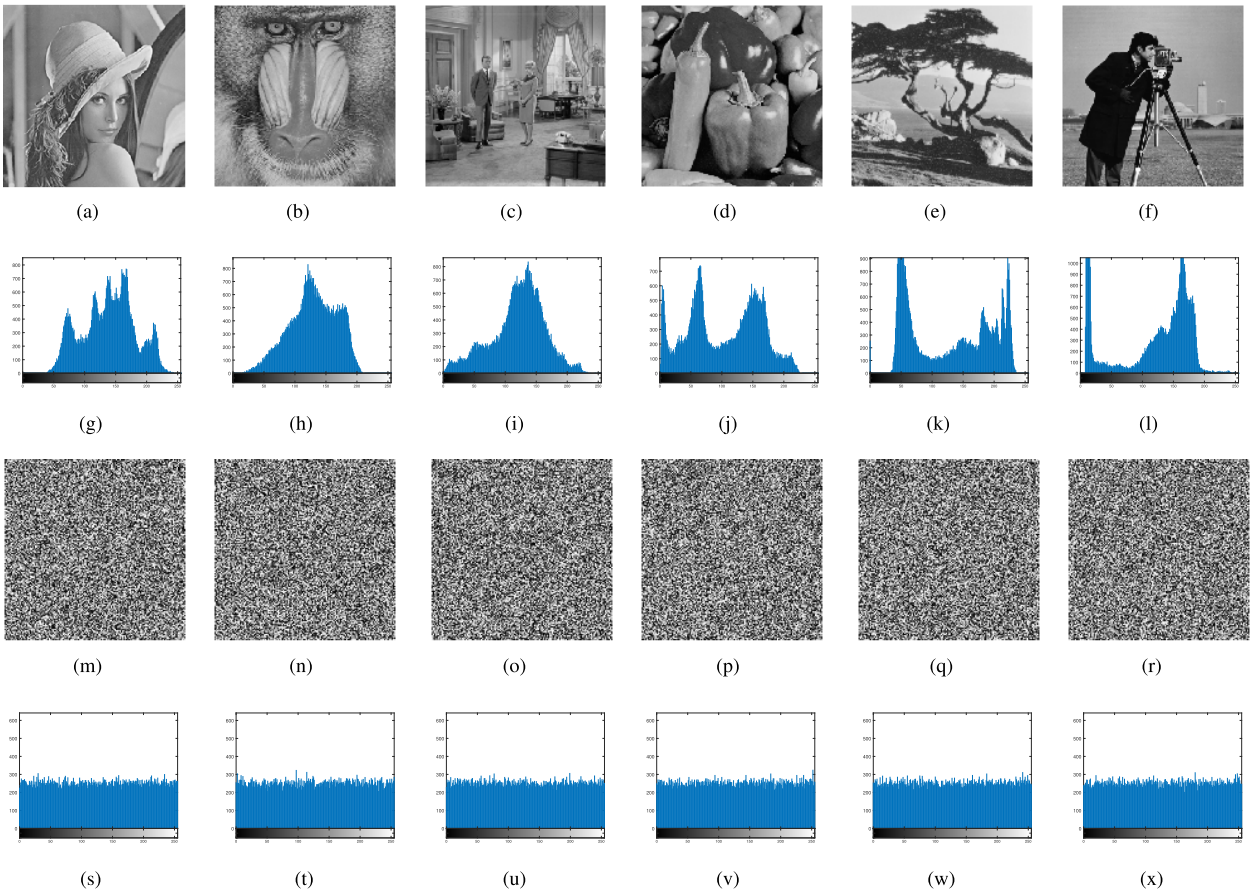


FIGURE 11. (a-f) are the original images, (g-l) are the histogram of (a-f), (m-r) are the encryption images of (a-f), (s-x) are the histogram of (m-r) respectively.

statistical performance. The higher the resilience to statistical assaults, the more uniform the histogram distribution. The histogram of some images and their cipher images is shown as Fig. 11.

TABLE 4. The information entropy of plain image and cipher image.

image	Lena	Baboon	Pepper	Plane	Boat
Plain image	7.3312	7.3312	7.3312	6.7131	7.2309
Cipher image	7.9973	7.9973	7.9973	7.9970	7.9971

When the histograms of the original image and the cipher image are compared, it is clear that the former displays noticeable variations while the latter is pretty uniform. Pixel values cannot be identified directly. The confidentiality functions admirably.

E. INFORMATION ENTROPY

Information entropy is an assessment metric that measures the unpredictability of the data sequence to provide feedback on the uncertainty of the response image information. The higher the information entropy is, the larger uncertainty and the bigger the amount of information is. But the value of this parameter is typically thought to be no greater than 8 [4]. It can be defined by the following equation:

$$H = -\sum_{i=0}^{L} p(i)\log_2 p(i) \tag{28}$$

where L denotes the gray value of the image and P(i) represents the probability of occurrence of gray value i.

In this experiment, the different images and the information entropy values of these images after using this algorithm are calculated under the same conditions and they are listed in Table 4.

It can be found that the image information entropy of the ordinary image is significantly different from the theoretical value after the encryption algorithm. The algorithm has good performance.

F. KEY SPACE ANALYSIS

The key space needs to be big enough so that it can prevent exhaustive attack. In this study, four control parameters, x_0, y_0, z_0 and ExternalKey, are used in the proposed scheme. Whereas in diffusion, the keystream has 128 bits, the master keystream and the sub-keystream have four types to choose from. If the precision of each parameter in computer lives up to 10^{-14}, key space is $10^{14} \times 4^{256}$, suggesting a large key space. In summary, If the attacker uses an exhaustive method, the likelihood that he will be able to crack the encrypted image will be very low.

G. NIST TEST

A good encryption algorithm should be accompanied by a high degree of randomness. Therefore, the algorithm uses NIST SP800-22 to test the randomness of sequences generated by chaotic systems. This test set contains 15 test items. The P-value is used to determine whether the test criteria are met. Each of the test items contains a P-value. Each test would get its own P-value. The value needs in [0, 1]. A threshold value needs to be set for the experiment. Only when p is greater than this threshold α is the test passed [41]. In this test, we make $\alpha = 0.01$, and the length of the chaotic sequence is 10^6. The result of the test is listed in TABLE 5.

TABLE 5. NIST SP 800-22 randomness test for cipher images.

Test	P-value	Proportion
Frequency	0.2909	Pass
Block frequency	0.2208	Pass
Cumulative Sums	0.3259	Pass
Runs	0.0834	Pass
Longest run of ones	0.3122	Pass
Rank	0.7558	Pass
FFT	0.4750	Pass
Non-overlapping lemplate	0.5054	Pass
Overlapping template	0.2461	Pass
Universal statistical	0.0473	Pass
Approximate entropy	0.3905	Pass
Random excursions	0.1102	Pass
Random excursions variant	0.0865	Pass
Serial	0.2504	Pass
Linear complexity	0.7602	Pass

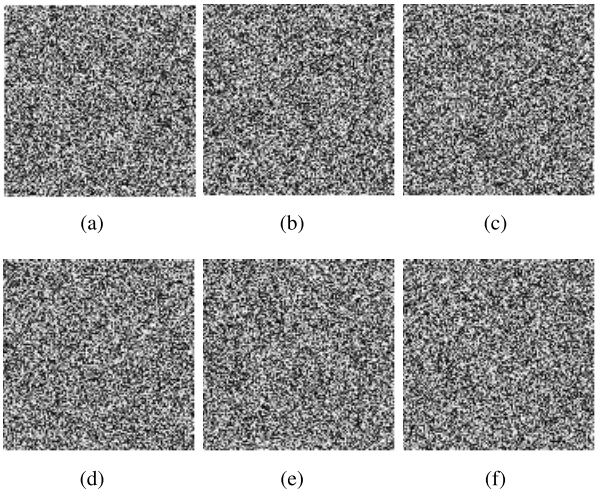


FIGURE 12. (a) is the original encrypted image. (b-f) are the decryption result after changing k_1, k_2, k_3, k_4 and k_5 respectively.

H. KEY SENSITIVITY

During the encryption process, the initial parameters are changed, creating changes in the decoded picture and testing the algorithm's key sensitivity. A successful method with high key sensitivity requires a large movement in the cipher image, even if it is a little change in the original value. The following Fig. 12 shows the decryption images after changing an initial key.

As for the result of the experiment, the encryption algorithm designed has high sensitivity that can guarantee for the security of image.

V. CONCLUSION

In this paper, an encryption algorithm based on neuron model discharge is proposed. And it employs a combination of

orthogonal Latin square confusion to enhance image confidentiality. Firstly, a chaotic signal is generated using a chaotic system, and a chaotic sequence is generated by injecting a neuron model discharge in the form of a current. In this process it is necessary to note whether the neuronal model reaches a chaotic state. Secondly, the duplicate sequences in the chaotic sequences are removed and the sequences are complemented, and then the image is globally dislocated. Thirdly, the image scrambles by an orthogonal Latin square to achieve a fuller dislocation effect. The orthogonal Latin square is composed using the SHA-256 algorithm. Fourthly, the image after permutation in the previous step is diffused twice by adding a modulus. Finally, one more finite field diffusion is performed. By using this algorithm to encrypt several images, the average NPCR and UACI values obtained are 99.612 and 33.488, respectively. It is higher than the average effect of most studies. Adequate confidentiality measures are performed on the image itself. The algorithm was tested and found to be strongly resistant to noise attacks and cut attacks. It has a good secrecy effect. In the next step, we can study in terms of encrypted color images.

REFERENCES

[1] M. T. Elkandoz and W. Alexan, "Image encryption based on a combination of multiple chaotic maps," *Multimedia Tools Appl.*, vol. 81, no. 18, pp. 1–22, 2022.

[2] X. Gao, J. Mou, S. Banerjee, Y. Cao, L. Xiong, and X. Chen, "An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 4, pp. 1535–1551, Apr. 2022.

[3] G. Ye, M. Liu, and M. Wu, "Double image encryption algorithm based on compressive sensing and elliptic curve," *Alexandria Eng. J.*, vol. 61, no. 9, pp. 6785–6795, Sep. 2022.

[4] X. Wang, L. Feng, and H. Y. Zhao, "Fast image encryption algorithm based on parallel computing system," *Inf. Sci.*, vol. 486, pp. 340–358, Jun. 2019.

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

[6] C. Li, D. Lin, J. Lü, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," *IEEE Multimedia*, vol. 25, no. 4, pp. 46–56, Dec. 2018.

[7] L. D. Singh and K. M. Singh, "Medical image encryption based on improved ElGamal encryption technique," *Optik*, vol. 147, pp. 88–102, Oct. 2017.

[8] C. Li, G. Luo, Q. Ke, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 127–133, Jan. 2017.

[9] W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Opt. Lasers Eng.*, vol. 84, pp. 26–36, Sep. 2016.

[10] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption," *Nonlinear Dyn.*, vol. 92, no. 2, pp. 305–313, Apr. 2018.

[11] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Process.*, vol. 155, pp. 44–62, Feb. 2019.

[12] C. Pak and L. L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Process.*, vol. 138, pp. 129–137, Sep. 2017.

[13] S. Wang, C. Wang, and C. Xu, "An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm," *Opt. Lasers Eng.*, vol. 128, May 2020, Art. no. 105995.

[14] G. Hu and B. Li, "Coupling chaotic system based on unit transform and its applications in image encryption," *Signal Process.*, vol. 178, Jan. 2021, Art. no. 107790.

[15] L. Chen, H. Yin, T. Huang, L. Yuan, S. Zheng, and L. Yin, "Chaos in fractional-order discrete neural networks with application to image encryption," *Neural Netw.*, vol. 125, pp. 174–184, May 2020.

[16] X. Tan, C. Xiang, J. Cao, W. Xu, and L. Rutkowski, "Synchronization of neural networks via periodic self-triggered impulsive control and its application in image encryption," *IEEE Trans. Cybern.*, vol. 52, no. 8, pp. 8246–8257, Aug. 2022.

[17] M. Prakash, P. Balasubramaniam, and S. Lakshmanan, "Synchronization of Markovian jumping inertial neural networks and its applications in image encryption," *Neural Netw.*, vol. 83, pp. 86–93, Nov. 2016.

[18] D. Ouyang, J. Shao, H. Jiang, S. K. Nguang, and H. T. Shen, "Impulsive synchronization of coupled delayed neural networks with actuator saturation and its application to image encryption," *Neural Netw.*, vol. 128, pp. 158–171, Aug. 2020.

[19] H. Zhou, Z. Liu, D. Chu, and W. Li, "Sampled-data synchronization of complex network based on periodic self-triggered intermittent control and its application to image encryption," *Neural Netw.*, vol. 152, pp. 419–433, Aug. 2022.

[20] Y. He, Y.-Q. Zhang, X. He, and X.-Y. Wang, "A new image encryption algorithm based on the OF-LSTMS and chaotic sequences," *Sci. Rep.*, vol. 11, no. 1, pp. 1–22, Mar. 2021.

[21] M. Sangiorgio and F. Dercole, "Robustness of LSTM neural networks for multi-step forecasting of chaotic time series," *Chaos, Solitons Fractals*, vol. 139, Oct. 2020, Art. no. 110045.

[22] X. Xu and S. Chen, "An optical image encryption method using Hopfield neural network," *Entropy*, vol. 24, no. 4, p. 521, Apr. 2022.

[23] P. Fulde and M. Loewenhaupt, "Magnetic excitations in crystal-field split 4f systems," *Adv. Phys.*, vol. 34, no. 5, pp. 589–661, Jan. 1985.

[24] F. Yang, J. Mou, Y. Cao, and R. Chu, "An image encryption algorithm based on BP neural network and hyperchaotic system," *China Commun.*, vol. 17, no. 5, pp. 21–28, May 2020.

[25] X. Xu and S. Chen, "A remote sensing image encryption method combining chaotic neuron and tent map," *J. Comput.*, vol. 32, no. 2, pp. 108–123, 2021.

[26] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D logistic-sine-coupling map for image encryption," *Signal Process.*, vol. 149, pp. 148–161, Aug. 2018.

[27] C. A. Murugan and P. Karthigaikumar, "Survey on image encryption schemes, bio cryptography and efficient encryption algorithms," *Mobile Netw. Appl.*, vol. 2018, pp. 1–6, May 2018.

[28] T. S. Ali and R. Ali, "A new chaos based color image encryption algorithm using permutation substitution and Boolean operation," *Multimedia Tools Appl.*, vol. 79, nos. 27–28, pp. 19853–19873, Jul. 2020.

[29] J. H. Curry, "A generalized Lorenz system," *Commun. Math. Phys.*, vol. 60, no. 3, pp. 193–204, Oct. 1978.

[30] J. Guckenheimer and R. A. Oliva, "Chaos in the Hodgkin–Huxley model," *SIAM J. Appl. Dyn. Syst.*, vol. 1, no. 1, pp. 105–114, Jan. 2002.

[31] M. Xu and Z. Tian, "A novel image cipher based on 3D bit matrix and Latin cubes," *Inf. Sci.*, vol. 478, pp. 1–14, Apr. 2019.

[32] X. Wang, Y. Su, M. Xu, H. Zhang, and Y. Zhang, "A new image encryption algorithm based on Latin square matrix," *Nonlinear Dyn.*, vol. 107, no. 1, pp. 1277–1293, 2022.

[33] R. Lin and S. Li, "An image encryption scheme based on Lorenz hyperchaotic system and RSA algorithm," *Secur. Commun. Netw.*, vol. 2021, pp. 1–18, Apr. 2021.

[34] X. Wang and S. Gao, "Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory," *Inf. Sci.*, vol. 507, pp. 16–36, Jan. 2020.

[35] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, no. 1, pp. 403–419, Apr. 2019.

[36] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," *Signal Process.*, vol. 153, pp. 11–23, Dec. 2018.

[37] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Opt. Lasers Eng.*, vol. 90, pp. 225–237, Mar. 2017.

[38] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem, and M. Lee, "Image encryption using a synchronous permutation-diffusion technique," *Opt. Lasers Eng.*, vol. 90, pp. 146–154, Mar. 2017.

[39] K. M. Hosny, S. T. Kamal, M. M. Darwish, and G. A. Papakostas, "New image encryption algorithm using hyperchaotic system and Fibonacci Q-matrix," *Electronics*, vol. 10, no. 9, p. 1066, Apr. 2021.

[40] C. Song, S. Sudirman, M. Merabti, and D. Llewellyn-Jones, "Analysis of digital image watermark attacks," in *Proc. 7th IEEE Consum. Commun. Netw. Conf.*, Jan. 2010, pp. 1–5.
[41] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-Allen and Hamilton Inc., McLean, VA, USA, Tech. Rep., 2001.

CHENCHEN HE received the B.S. degree from the School of Computer Science and Technology, Hengyang Normal University, Hunan, China, where she is currently pursuing the master's degree in electronic information. She majors in digital image encryption and image processing.

ZHONG CHEN received the M.S. degree in applied mathematics from the Department of Applied Mathematics, Southwest Jiaotong University, China, in 2004, and the Ph.D. degree in mechanical engineering from Hunan University, China, in 2018. He is currently an Associate Professor with the School of Computer Science and Technology, Hengyang Normal University, Hunan, China. His main research interests include digital image encryption, nonlinear dynamics, and deep learning.

XIYU SUN received the B.S. degree from the School of Mechanical Engineering, Hunan Institute of Science and Technology, China. He is currently pursuing the master's degree in electronic information with Hengyang Normal University, Hunan, China. His research interests include chaotic encryption and image processing.

LUJIE WANG received the B.S. degree in computer science and technology from the Xiangnan College, in 2021. She is currently pursuing the master's degree in electronic information with Hengyang Normal University, Hunan, China. Her current research interests include image encryption and image privacy protection.