Hindawi
Security and Communication Networks
Volume 2022, Article ID 4260804, 14 pages
https://doi.org/10.1155/2022/4260804

*Research Article*

# A New V-Net Convolutional Neural Network Based on Four-Dimensional Hyperchaotic System for Medical Image Encryption

**Xiaowei Wang,[1] Shoulin Yin,[1] Muhammad Shafiq,[2] Asif Ali Laghari,[3] Shahid Karim,[4] Omar Cheikhrouhou,[5,6] Wajdi Alhakami,[7] and Habib Hamam[8,9,10]**

[1] *Software College, Shenyang Normal University, Shenyang, China*
[2] *Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou, China*
[3] *Department of Computer Science, Sindh Madressatul Islam University, Karachi, Pakistan*
[4] *Faculty of Science and Technology, ILMA University, Karachi, Pakistan*
[5] *CES Laboratory, National School of Engineers of Sfax, University of Sfax, Sfax 3038, Tunisia*
[6] *Higher Institute of Computer Science of Mahdia, University of Monastir, Mahdia 5111, Tunisia*
[7] *Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia*
[8] *Faculty of Engineering, Moncton University, Moncton, NB E1A3E9, Canada*
[9] *Spectrum of Knowledge Production & Skills Development, Sfax 3027, Tunisia*
[10] *School of Electrical Engineering, Department of Electrical and Electronic Engineering Science, University of Johannesburg, Johannesburg 2006, South Africa*

Correspondence should be addressed to Muhammad Shafiq; srsshafiq@gmail.com

Received 7 December 2021; Revised 31 December 2021; Accepted 10 January 2022; Published 14 February 2022

Academic Editor: Celestine Iwendi

In the transmission of medical images, if the image is not processed, it is very likely to leak data and personal privacy, resulting in unpredictable consequences. Traditional encryption algorithms have limited ability to deal with complex data. The chaotic system is characterized by randomness and ergodicity, which has advantages over traditional encryption algorithms in image encryption processing. A novel V-net convolutional neural network (CNN) based on four-dimensional hyperchaotic system for medical image encryption is presented in this study. Firstly, the plaintext medical images are processed into 4D hyperchaotic sequence images, including image segmentation, chaotic system processing, and pseudorandom sequence generation. Then, V-net CNN is used to train chaotic sequences to eliminate the periodicity of chaotic sequences. Finally, the chaotic sequence image is diffused to change the raw image pixel to realize the encryption processing. Simulation test analysis demonstrates that the proposed algorithm has better effect, robustness, and plaintext sensitivity.

## 1. Introduction

At present, there are two main ways for information transmission, one is text and the other is image. Therefore, in addition to words, images also contain a lot of important and confidential information. In the current era of computer network, images are mostly stored in the form of digital images, which is simple, quick, and easy to find. However, at the same time, it also increases the risk of information leakage, especially when images are transmitted on the network; they are easy to attack. In this context, image information encryption is an important means to prevent information leakage [1–5].

There are many research studies on image encryption protection. The traditional encryption algorithms mainly consist of randomly disturbing the row or column of image information to encrypt, randomly disturbing the image pixel information for encryption and decryption, zooming in and out the image information of the pixel point, and so on [6–8]. They are easy to crack. To solve the problems in the above methods, chaos-based encryption algorithm appears, which is the most widely used image encryption algorithm at present [9, 10]. Although it has higher encryption effect, this method has two defects. One is that all the image information is encrypted into ciphertext image, resulting in a sharp increase in the amount of information after image encryption, occupying a large amount of storage space. Secondly, the generated chaotic sequence by pure use of the chaotic system shows local linearity and strong correlation, that is, it will show a certain degree of periodicity and so on. The existence of this feature makes the image security relatively lower [11–15].

In this article, aiming at the periodicity shortcoming of chaotic encryption algorithm, V-net CNN is used to learn chaotic sequence to break the periodicity of chaotic sequence to improve the confidentiality of image encryption. The validity and practicability of the new scheme are proved by testing, which provides a reference for image encryption.

## 2. 4D Hyperchaotic System

The 4D hyperchaotic system [16, 17] studied in this paper is as

$$\dot{w} = \mathrm{d}x. \tag{1}$$

When parameters $a = 35$, $b = 3$, $c = 33$, and $d = 8$, a typical hyperchaotic attractor exists in system (1). The phase diagram is shown in Figure 1. Figure 1(a) is the $x$-$y$-$z$ three-dimensional projection phase diagram. Figure 1(b) is the $y$-$z$-$w$ three-dimensional projection phase diagram.

*2.1. Analysis of Chaos Characteristics.* The dissipative property of the new system (1) is analyzed. Dissipation value is $\nabla V = (\partial\dot{x}/\partial x) + (\partial\dot{y}/\partial x) + (\partial\dot{z}/\partial x) + (\partial\dot{w}/\partial x)$; when $\nabla V < 0$, the system is wasteful. If the system parameters are substituted, $\nabla V = -a - b = -38 < 0$; if the dissipation condition is satisfied, the trajectory of the system eventually contracts asymptotically to a particular limit set of zero volume at an exponential rate and is eventually fixed to an attractor.

Four Lyapunov exponents are obtained, LE1 = 0.343, LE2 = 0.052 2, LE3 = −0.305, and LE4 = −36.640, of which two Lyapunov exponents are greater than zero, that is, system (1) is a hyperchaotic system.

*2.2. Stability Analysis.* Adding the time-delay term $\tau$ to the second nonlinear formula of hyperchaotic system (1), the time-delay model equation is shown as

$$\dot{y} = cx(t-\tau) - xz - w. \tag{2}$$

When the hysteresis term $\tau\ = 0$, system (1) is locally asymptotically stable at $E_0 = (0, 0, 0, 0)$, and the Jacobi matrix is

$$J = \begin{pmatrix} -a & a & 0 & 0 \\ ce^{-\lambda\tau} & 0 & 0 & -1 \\ 0 & 0 & -b & 0 \\ d & 0 & 0 & 0 \end{pmatrix}. \tag{3}$$

The feature equation is as follows:

$$(\lambda + b)\left(\lambda^3 + a\lambda^2 - ac\lambda e^{-\lambda\tau} + a\ d\right) = 0. \tag{4}$$

According to the substitution law, $P_1 = a$, $P_2 = -ac$, and $P_3 = ad$, if only the virtual root is considered, when $\tau\ = 0$, the characteristic equation of system (1) is

$$\lambda^3 + P_1\lambda^2 + P_2\lambda + P_3 = 0. \tag{5}$$

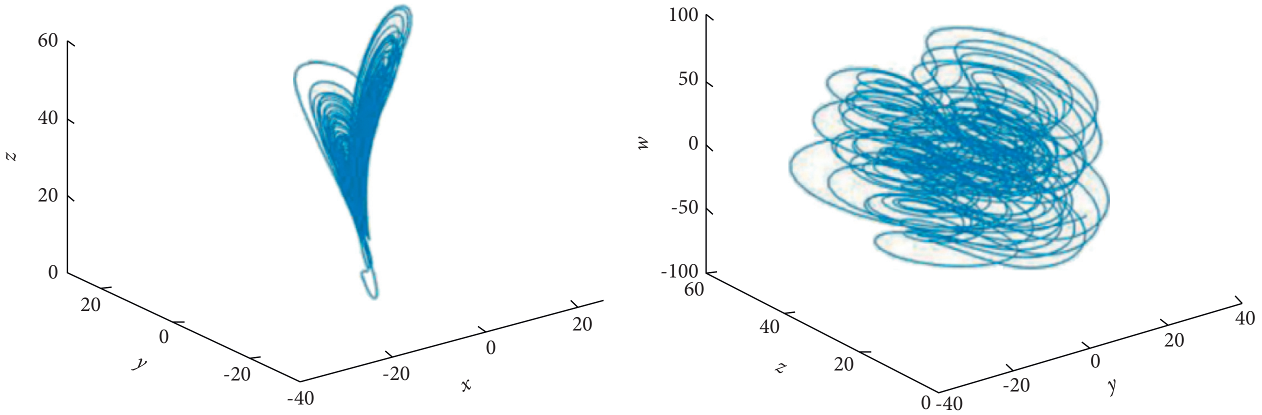
According to Routh–Hurwitz criterion, if $P_1, P_2, P_3 > 0$ and $P_1P_2 - P_3 > 0$, then the real parts of the characteristic roots of equation (3) are all negative. By substituting corresponding parameters into the above inequalities, it can be seen that the time-delay system (1) is locally asymptotically stable at $E_0 = (0, 0, 0, 0)$.

## 3. Proposed Image Encryption

Computer technology is developing day by day; image storage is mostly realized in the form of the digital image. The image has many information, especially in some special fields (national defense, military, finance and personal privacy, etc.), the information in the image is confidential and not allowed to be disclosed. So, how to ensure the safety of image information is very important. Image information encryption is the main solution at present [18]. Among them, chaotic encryption is the most commonly used method. Its principle is to superimpose one or more chaotic signals on the useful signals to be transmitted at the sending end so that the signals in the transmission channel have the shape of random noise and then achieve the purpose of encryption and secure communication. This method has high encryption speed, lossless compression, and high security, but the generated chaotic sequence still shows a certain degree of periodicity. This paper improves and optimizes a chaotic sequence image encryption algorithm based on V-Net CNN. The proposed method is shown in Figure 2.

*3.1. Chaotic Sequence Generation.* Chaotic sequence generation is the first step in image encryption, which aims to transform plaintext image into random sequence. The specific process includes three parts: image segmentation, chaotic system processing, and pseudorandom sequence generation.

*3.1.1. Plaintext Image Segmentation.* The function of plaintext image segmentation is convenient for chaotic system processing. In general, the monitoring image of the target sequence is divided into any one of the ten different sizes in Table 1. The size of each round block is determined



(a)

(b)

Figure 1: System (1) chaotic attractor phase diagram.

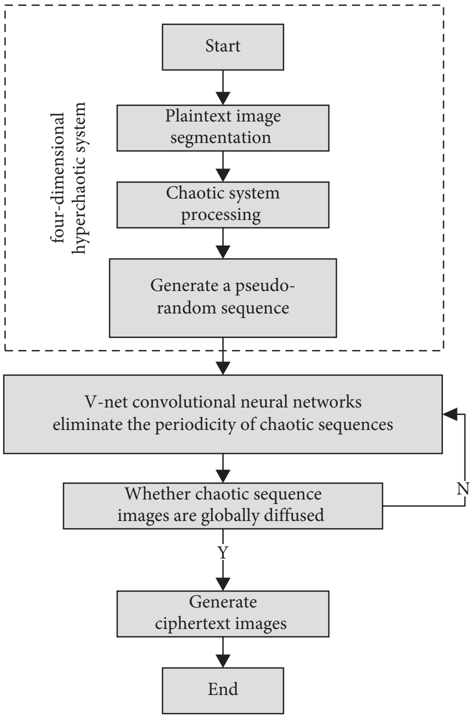

four-dimensional hyperchaotic system
Start
Plaintext image segmentation
Chaotic system processing
Generate a pseudo-random sequence
V-net convolutional neural networks eliminate the periodicity of chaotic sequences
Whether chaotic sequence images are globally diffused
N
Y
Generate ciphertext images
End

Figure 2: Proposed medical image encryption.

Table 1: Block size table of each round plaintext image

| Mod10 | Block size | Mod10 | Block size |
|---|---|---|---|
| 0 | 16 | 5 | 56 |
| 1 | 24 | 6 | 64 |
| 2 | 32 | 7 | 72 |
| 3 | 40 | 8 | 80 |
| 4 | 48 | 9 | 96 |

Note that there is no overlap between these subblocks. In the postprocessing, these subblocks are used as units for correlated operation.

by the session key used during the encryption of that particular round.

*3.1.2. Chaotic System Processing.* A chaotic system is used to generate real number sequence for plaintext image subblock. There are five commonly used chaotic systems, namely, logistic chaotic system, Chebyshev chaotic system, Skew Tent chaotic system, Henon chaotic system, and Lorenz chaotic system [19–23]. The description of the above five chaotic systems is as follows:

(A) Logistic chaotic system:

$$r_{n+1} = ar_n(1 - r_n), \tag{6}$$

here $r_n \in [0, 1], a \in (1, 5), n = 0, 1, 2, \ldots$.

(B) Chebyshev chaotic system:

$$x_n = \cos(k \arccos(x_n)), \tag{7}$$

where $x_i \in (-1, 1), i = 1, 2, \ldots, N$, and $k$ is the system control parameter. When $k \geq 2$, the Chebyshev map enters the chaotic state:

(C) Skew Tent chaotic system:

$$f(x) = \begin{cases} \dfrac{x}{\delta'}, & x \in (0, \delta], \\ \dfrac{(1 - x)}{(1 - \delta)'}, & x \in (\delta, 1]. \end{cases} \tag{8}$$

When $\delta \in (0, 1)$, the system is chaos.

(D) Henon chaotic system:

$$\begin{cases} x_{n+1} = -\alpha x_n^2 + y_n + 1, \\ y_{n+1} = \beta x_n, \end{cases} \tag{9}$$

where $\alpha$ and $\beta$ are the system control parameters; when $0.54 < \alpha < 2$ and $0 < |\beta| < 1$, the system is in the chaos state.

(E) Lorenz chaotic system:

$$t = ex - zx - y. \tag{10}$$

*3.1.3. Pseudorandom Sequence Generation.* After chaotic system processing, the sequence generated is real number sequence, which also needs to be converted into pseudorandom sequence, namely, chaotic sequence. There are three generation methods for pseudorandom sequence, namely, threshold method, binary sequence method, and quantitative extraction method [24]. The following is a specific analysis.

(A) Threshold methoddefine a threshold function $\Theta_t(w)$ as

$$\Theta_t(w) = \begin{cases} 0, \text{ when } & w < t, \\ 1, \text{ when } & w \geq t. \end{cases} \tag{11}$$

Its complement is $\Theta\prime(w) = 1 - \Theta_t(w)$. $t$ is the set threshold. $w$ is the value of chaotic sequence. Equation (11) is applied to the real number sequence to obtain the pseudorandom sequence.

(B) Binary sequence method: the chaotic sequence value $w(|w| \leq 1)$ can be written as the binary form of

$$\begin{aligned} &|w| = 0, A_1(w), A_2(w), \ldots, A_i(w), \ldots, \\ &A_n(w) \in \{0, 1\}, \end{aligned} \tag{12}$$

$A_i(w)$ can be expressed as

$$A_i(w) = \sum_{r=1}^{2^i-1} (-1)^{r-1}\{\Theta_{r/2^i}(w) + \Theta'_{-r/2^i}(w)\}. \tag{13}$$

So, it can get a pseudorandom sequence.

(C) Quantitative extraction method: if the obtained chaotic sequence is not in the range of [0, 1], the chaotic sequence $\{w_i\}_{i=0}^{\infty}$ is normalized to the interval [0, 1] to obtain $\{x_i\}_{i=0}^{\infty}$. In the representation of $x_i$ as a binary number, it takes the lowest or middle $N$ bits as required. The binary bits corresponding to each $x_i$ value are combined to obtain the key sequence used for encryption.

*3.2. V-Net Convolutional Neural Networks Eliminating the Periodicity of Chaotic Sequences.* 3D V-Net full convolutional neural network [25, 26] is used in this paper. 3D convolutional neural network can convolve 32 layers of medical images at the same time. Besides learning image features, the 3D convolutional neural network can also learn the position change information of images between different layers. 3D convolutional neural network is a network model with the huge parameter system. In order to make the model perform better, the overall flow of V-Net CNN is shown in Figure 3.

In the process of downsampling, the high-level feature map contains semantic category information, while the low-level feature map retains image details. In the process of downsampling, convolutional neural network will lose important category information. As the downsampling process goes on, the image gradient gradually disappears. To preserve the semantic information of high-level images, the convolution results of high-level images are sent to the upsampling process through the connection layer. However, the complete upsampling process undoubtedly increases the training difficulty. In this paper, the feature maps in the lower sampling process are connected to the upper sampling process by multiplying certain weight values through the global average weight module. The specific approach is to first average pool the feature maps output by the first four layers in the downsampling process and then calculate the corresponding weight values by Softmax function. The formula for calculating the weight is as follows:

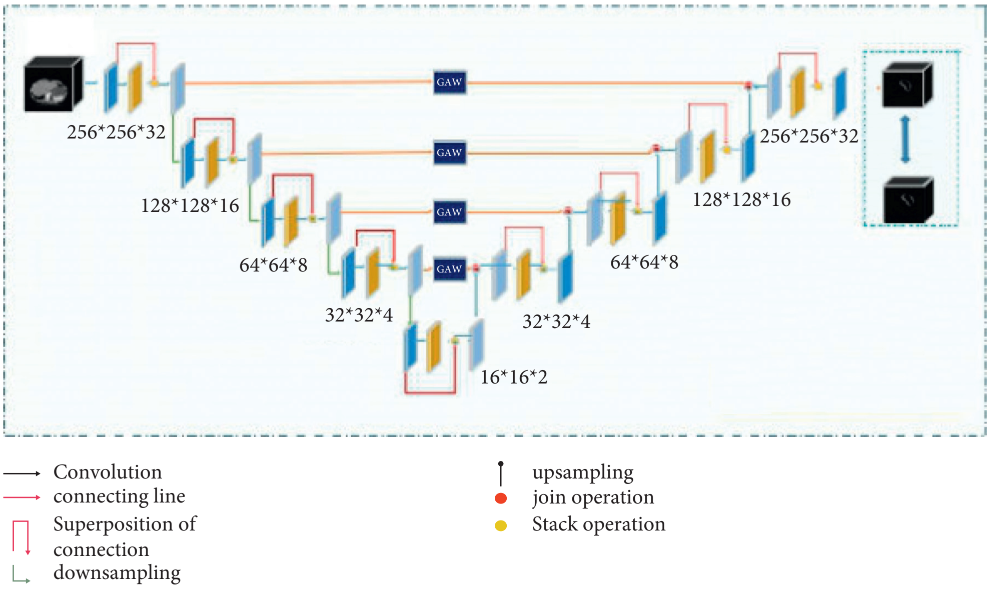


Figure 3: V-Net CNN structure.

$$W_i = \frac{\exp(\mathrm{GAP}(F_i))}{\sum_{i=1}^{4} \exp(\mathrm{GAP}(F_i))}, \tag{14}$$

where $F_i$ represents the convolution output result of the $i$th layer. The purpose of global average pooling (GAP) is to eliminate the influence of different scales on weight values in the process of downsampling. Global average weight (GAW) module is adopted to effectively utilize multiscale feature information to improve the learning efficiency of deep learning. The weight acquisition process is shown in Figure 4.

Level set (LS) loss function is a loss function based on the level set method [27], which is the first application of the level set method in loss function of deep learning network. LS loss is denoted as

$$\begin{aligned} F(c1, c2, \varphi) = {} & \mu \cdot \mathrm{Length}(\varphi) + \nu \cdot \mathrm{Area}(\varphi) \\ & + \lambda_1 \int_\Omega |\mu_0(x, y) - c1|^2 H(\varphi(x, y)) \mathrm{d}x\mathrm{d}y \\ & + \lambda_2 \int_\Omega |\mu_0(x, y) - c2|^2 (1 - H(\varphi(x, y))) \mathrm{d}x\mathrm{d}y, \end{aligned} \tag{15}$$

where $\mu \geq 0$, $\nu \geq 0$, and $\lambda_1, \lambda_2 > 0$ is the fixed value parameter. $\Omega$ is the whole image area. $\varphi$ is the level set function. Length$(\varphi)$ and Area$(\varphi)$ represent the curve length and area regularization terms, respectively. $\mu_0(x, y)$ is the pixel at (x,y) in the image. H is a differentiable step function, where $\alpha$ is a hyperparameter used to improve the gradient of the function, which is set to 2.5 in the experiment:

$$H(x) = \frac{1}{\pi}\left(\arctan \alpha x + \frac{\pi}{2}\right). \tag{16}$$

The idea of LS loss is to first use step function to set all the inside edges of the outer wall of prediction results and ground truth to 1 and the outside edges to 0. When calculating the loss, multiply the predicted result and the ground truth and then sum to calculate the loss and perform the same operation after taking the reverse. The purpose of this is to give enough weight to the edges. This loss function is suitable for the segmentation of single outer edge objects, but not for the segmentation of medical objects with both inner and outer edges. Based on the level set, we propose a regularized level set loss function (LSR Loss), which can optimize the edge through LS loss and constrain the internal details of gastric wall through regularization, giving full play to the respective advantages of the level set method and the deep learning method. LSR loss is defined as

$$\mathrm{LSR\,loss} = \frac{1}{\lambda_1} \sum_\Omega |G_l(x, y) - c_{l1}|^2 H(\varphi(x, y)) + \frac{1}{\lambda_2} \sum_\Omega |G_l(x, y) - c_{l2}|^2 (1 - H(\varphi(x, y))) + \frac{1}{\lambda_3} \sum_\Omega |G_l(x, y) - \varphi(x, y)|^2, \tag{17}$$

where $\Omega$ represents the entire image region, $G_I(x, y)$ represents the pixel value in ground truth, and $\varphi(x, y)$ represents the pixel value of the image predicted by the network. Here,

$$\begin{aligned} c_{l1} &= \frac{\sum_\Omega G_l(x, y) H(\varphi(x, y))}{\sum_\Omega \Omega H(\varphi(x, y))}, \\ c_{l2} &= \frac{\sum_\Omega G_l(x, y)(1 - H(\varphi(x, y)))}{\sum_\Omega (1 - H(\varphi(x, y)))}. \end{aligned} \tag{18}$$

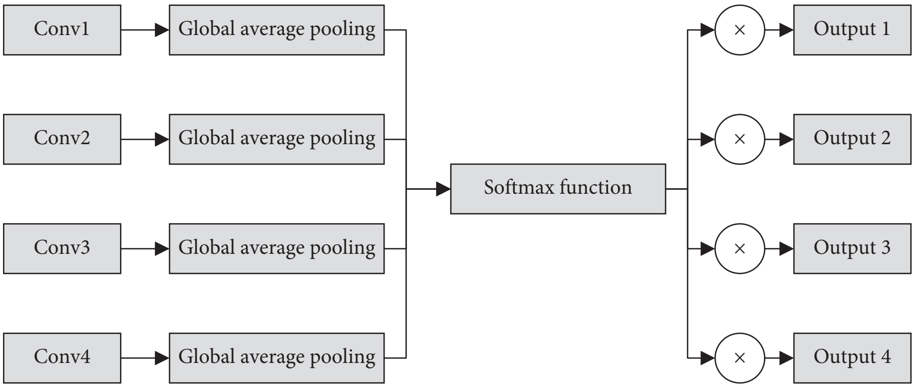


Figure 4: Global average weight module.

When the neural network predicted value $\varphi(x, y)$ and the corresponding position of the image were more accurate, the values of $c_{l1}$ and $c_{l2}$ would be closer to 1. Then, the difference between the GT and the predicted value will be equivalent to taking the opposite, and then, it will be close to 0 when multiplied by $\varphi(x, y)$ corresponding to the predicted value. However, when the image boundary error, the loss value will be very large. Therefore, $\lambda_1$ and $\lambda_2$ are added in this paper to constrain the size of the loss function to normalize it.

Step 1: input the plaintext images generated in the previous into the V-net convolutional neural network structure as training samples.

Step 2: the first layer is conducted convolution operation on the plaintext image, namely, the weighted sum.

Step 3: downsampling the plaintext image after convolution operation, that is, pooling.

Step 4: repeat Step 2 and Step 3 to extract key features of plaintext images and reduce the amount of data processing.

Step 5: enter the full connection layer and connect all key features of plaintext images together.

Step 6: output the training results, and judge whether the error between the convolution result and the actual output is less than the set threshold. If the result is less than the threshold value, the V-net convolutional neural network training has been completed. If it is greater than the threshold value, error backpropagation is required to adjust the thresholds and weights of each layer until the convolutional neural network training is completed.

*3.3. Chaotic Sequence Image Diffusion.* After the above processing, the periodicity of chaotic sequence is eliminated. However, its pixel value has not changed, so there are still certain security risks. In this case, chaotic images need to be diffused [28]. Diffusion treatment is as follows.

Formula (19) is used to replace each component of chaotic sequence:

$$\begin{aligned}FR(j) &= FR(j) \oplus PX(j) \oplus FR(j-1) \oplus FJ(j-1) \oplus FB(j-1)\\ FG(j) &= FG(j) \oplus PY(j) \oplus FG(j-1) \oplus FR(j-1) \oplus FB(j-1)\\ FB(j) &= FB(j) \oplus PZ(j) \oplus FB(j-1) \oplus FG(j-1) \oplus FR(j-1),\end{aligned} \tag{19}$$

where FR, FG, and FB are the RGB components of chaotic sequences. The matrices PX, PY, and PZ are pixel matrices. ⊕ is XOR operation.

It does the substitution again and changes the pixel value further. A diffusion function needs to be introduced here. The expression of the diffusion function is as follows:

$$S_i = \left(Y_i + S_{i-1}\right) \mathrm{mod} U \oplus e, \tag{20}$$

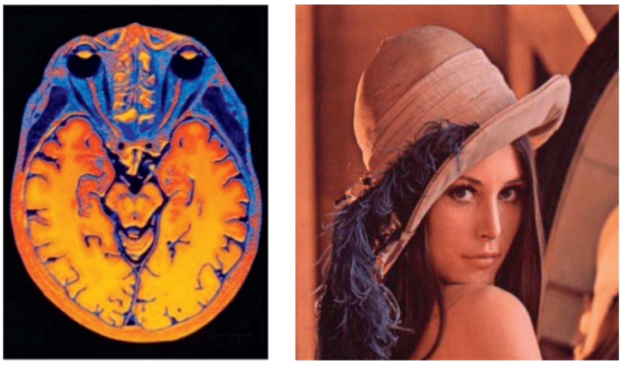
where $S_i$ represents the ciphertext of the current pixel point, $Y_i$ is the plaintext of the current pixel and the ciphertext of the previous pixel, $U$ represents the maximum value of pixel point, ⊕ represents XOR operation, and $e$ represents a random value.

Again the substitution formula is as follows:

$$\begin{aligned}FR(j) &= (FB(j) + FG(j))S_i \oplus FR(j),\\ FG(j) &= (FR(j) + FB(j))S_i \oplus FG(j),\\ FB(j) &= (FR(j) + FG(j))S_i \oplus FB(j).\end{aligned} \tag{21}$$

## 4. Experiments and Analysis

Two images of Lena and Skull with a size of $512 \times 512$ pixels are selected for simulation and analysis experiment. Setting logistic chaos system $\mu = 3.9999$, two-dimensional logistic chaos system have $\mu_1 = 0.9$, $\mu_2 = 0.9$, and $r = 0.1$. Experimental hardware environment is 64 GB memory, Windows10 operating system environment. The software simulation platform is Matlab 2017a. To evaluate the overall effect of the encryption algorithm, the following security performance analysis is made from the histogram, information entropy, correlation coefficient analysis, robustness, key space and sensitivity, and antidifferential attack. Figure 5 is the original image. Figures 5(a) and 5(b) are Skull image and Lena image, respectively. Figure 5 is from this paper Vaseghi et al. 2021 (Under the Creative Commons Attribution License/Public Domain) [29].



(a) (b)

Figure 5: Original image.

*4.1. Image Gray Histogram.* Generally speaking, the histogram distribution is relatively uniform, which can effectively prevent attackers from analyzing the histogram to obtain plaintext information. Figures 6(a)–6(d) show the plaintext image of Lena, ciphertext image of Lena, skull plaintext image, and skull ciphertext image, respectively. It is observed that the distribution of ciphertext histogram is uniform. Therefore, this new algorithm can resist histogram analysis attacks and conceal the statistical characteristics of plaintext images.

*4.2. Information Entropy.* The information entropy is mainly used to measure the uncertainty or randomness of information source. Conversely, chaos has a high entropy. It is reflected in the image; the more uniform distribution of the pixel gray value denotes the higher entropy value and the stronger randomness. For 8-bit images, the entropy value should be as close as possible to the ideal value 8. The calculation of information entropy is as follows:

$$H(R) = \sum_{i=0}^{255} p(R_i) lb(p(R_i)), \tag{22}$$

where $p(R_i)$ is the occurrence frequency of pixel value $i$ in the ciphertext image $R$. Table 2 is the comparison of global information entropy with other methods including FRFT [29], ASFS [30], and CENN [31].

However, there are some deficiencies in the global information entropy and the measurement of the image before and after encryption is not accurate. Therefore, based on the global information entropy, Lin et al. [3] proposed a more rigorous local information entropy test. The core idea is to randomly select nonoverlapping subblocks in the target image, represented as $L_1, L_2, \ldots, L_k$. Each subblock contains $T_b$ pixels, and then, calculate the global information entropy of each subblock. The local information entropy $\overline{H}_{k,T_b}$ of the image is

$$\overline{H}_{k,T_b} = \sum_{i=1}^{k} \frac{H(L_i)}{k}. \tag{23}$$

It selects $k = 30$ and $T_b = 1936$ to carry out local information test on the gray image. Through the local information entropy test, this algorithm is compared. Table 3 shows that the local information entropy test of the proposed algorithm has a relatively high pass rate.

*4.3. Correlation Coefficient Analysis.* If its value is close to 0, the correlation between image pixels is weaker. If its value is close to 1, the pixels are more relevant. The lower correlation coefficient denotes that it can better avoid the attacker obtaining the meaningful information from the ciphertext image [5].

The correlation coefficient is calculated by the following formula:

$$\begin{aligned} r_{xy} &= \frac{\operatorname{cov}(u, v)}{\sqrt{D(u)}\sqrt{D(v)}} \\ \operatorname{cov}(u, v) &= \frac{1}{N} \sum_{i=1}^{N} (x_i - E(u))(y_i - E(v)) \\ D(u) &= \frac{1}{N} \sum_{i=1}^{N} (u_i - E(u))^2 \\ E(u) &= \frac{1}{N} \sum_{i=1}^{N} u_i. \end{aligned} \tag{24}$$

The test results of correlation coefficients between test images and ciphertext are shown in Tables 4 and 5. It can be observed that the adjacent pixels of the plaintext test image have a strong correlation, while the adjacent pixels of the ciphertext image basically have no correlation.

Figure 7 and 8 show the plaintext and ciphertext images of Lena and Skull in three directions. As can be seen from the figures, the relationship between the adjacent pixels of the plaintext image in each direction is linear, while the relationship between the adjacent pixels of the ciphertext image is relatively discrete, with basically no correlation and good encryption effect.

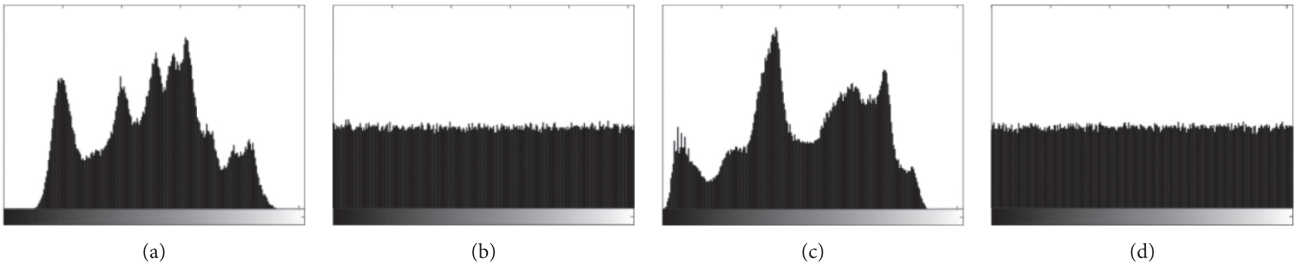

(a) (b) (c) (d)

Figure 6: Plaintext and ciphertext histograms.

Table 2: Comparison of information entropy.

| Method | Lena | Skull |
|---|---|---|
| FRFT | 7.9972 | 7.9994 |
| ASFS | 7.9992 | 7.9995 |
| CENN | 7.9992 | 7.9993 |
| Proposed | 7.9996 | 7.9997 |

Table 3: Local IE comparison.

| Image | Size | Plaintext entropy | FRFT | ASFS | CENN | Proposed |
|---|---|---|---|---|---|---|
| Lena | 256 × 256 | 6.7094 | 7.9031 | 7.9034 | 7.9032 | 7.9021 |
| Skull | 256 × 256 | 7.3118 | 7.9028 | 7.9031 | 7.9029 | 7.9024 |

Table 4: The correlation coefficient of adjacent pixels of Lena image

| Direction | Proposed | | FRFT | ASFS | CENN |
|---|---|---|---|---|---|
| | Plaintext | Ciphertext | | | |
| Horizontal | 0.97423 | −0.0006 | 0.0020 | −0.0003 | −0.0009 |
| Vertical | 0.98592 | 0.0024 | 0.0099 | 0.0105 | 0.0139 |
| Diagonal | 0.96275 | 0.0002 | −0.0049 | 0.0078 | −0.0006 |

Table 5: The correlation coefficient of adjacent pixels of Skull image

| Direction | Proposed | | FRFT | ASFS | CENN |
|---|---|---|---|---|---|
| | Plaintext | Ciphertext | | | |
| Horizontal | 0.97762 | 0.0001 | 0.0018 | 0.0029 | 0.0195 |
| Vertical | 0.97742 | 0.0035 | −0.0098 | −0.0007 | −0.0092 |
| Diagonal | 0.96126 | −0.0026 | 0.0012 | 0.0009 | 0.0165 |

*4.4. Robustness Analysis.* With the rapid development of computer and password cracking technology, attackers can intercept ciphertext images and add or modify them to attack ciphertext and images, causing interference to decryption. A new encryption algorithm should have strong robustness after encrypting the plaintext image and be able to resist various attacks and decrypt successfully. Clipping attack, noise attack, and JPEG compression are carried out on the ciphertext image. Figures 9(a)–9(c) are clipping 25%, Gaussian noise mean square error 50, JPEG compression, clipped 25% decryption, Gaussian noise decryption, and JPEG compression decryption, respectively. We also conduct data loss and noise attack for Skull image. Figure 10 is the data cut with 64 × 64. Figure 11 is the 4% salt and pepper noise. Figures 12 and 13 are the corresponding decrypted image for Figures 10 and 11, respectively. The results show that our proposed encryption method has good robustness.

*4.5. Key Space and Sensitivity.* Large key space can resist key exhaustive blasting effectively. According to [5], only when the key space is greater than or equal to $2^{100}$ can it better provide reliable security guarantee for the algorithm. The proposed algorithm uses seven groups of keys, and each group of keys has a floating point accuracy of $10^{16}$. Therefore, the key space is $(10^{16})^7 = 10^{112}$, which is larger than $2^{100}$, so it can resist the explosive attack.

For different keys, the decrypted image should not contain any information about the plaintext image, which requires the encryption algorithm to be sensitive to the key. The sensitivity of the key is tested below. Minor changes are made to one of the 7 groups of keys $k_i = k_i \pm \delta\,(\delta = 10^{-16})$, other keys remain unchanged, and the plaintext image is compared with the mean square error. $R$ is the ciphertext image to be compared:

$$\overline{M} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|I(i,j) - R(i,j)\right|^{2}. \qquad (25)$$

As shown in Figure 14 and Table 5, Figure 14(a) is the unchanged image and Figures 14(b)–14(h) are the image decrypted with the wrong key including (b) $k_1 + \delta$, (c) $k_2 + \delta$, (d) $k_3 + \delta$, (e) $k_4 + \delta$, (f) $k_5 + \delta$, (g) $k_6 + \delta$, and (h) $k_7 + \delta$. By comparing with the image decrypted correctly in Figure 14(a), it can be seen that the plaintext image cannot be recovered and the information related to plaintext cannot be obtained after minor changes in the key. It can be observed from Table 6 that the mean square error values are above 0.8, which is almost the same as the mean square error values of ciphertext images and plaintext images, and the entropy values are also above 7.99 (close to 8), which proves that the image decrypted with the error key is very different from the plaintext image and further indicates that the new algorithm in this paper has a high key sensitivity.

*4.6. Differential Attack Resistance.* If the method is more sensitive to plaintext, it is more resistant to differential attacks. The sensitivity to plaintext can be measured by the indexes NPCR [32, 33] and UACI [34, 35]. When there is only one pixel difference between two plaintext images, the ciphertext image obtained after encryption changes greatly.

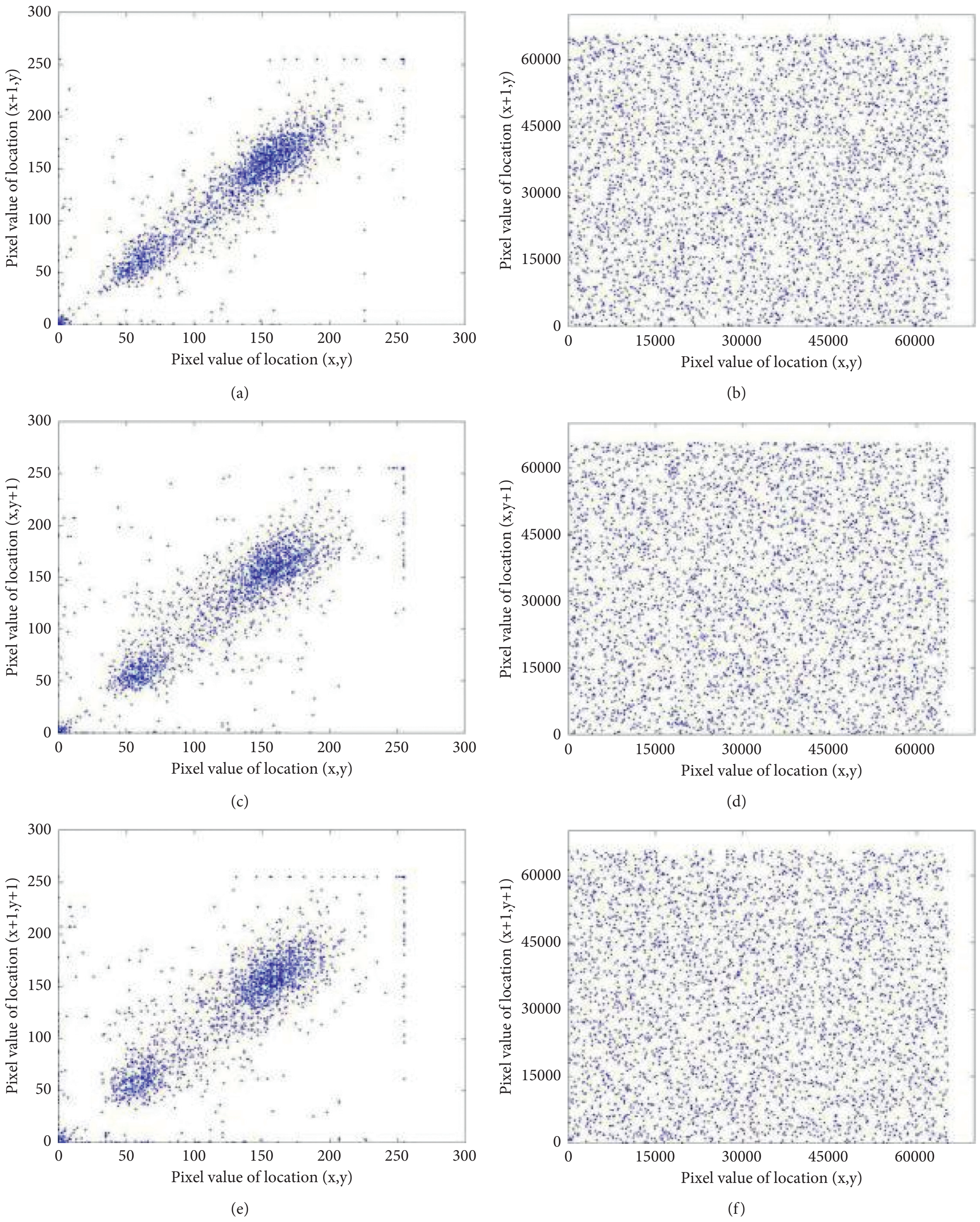
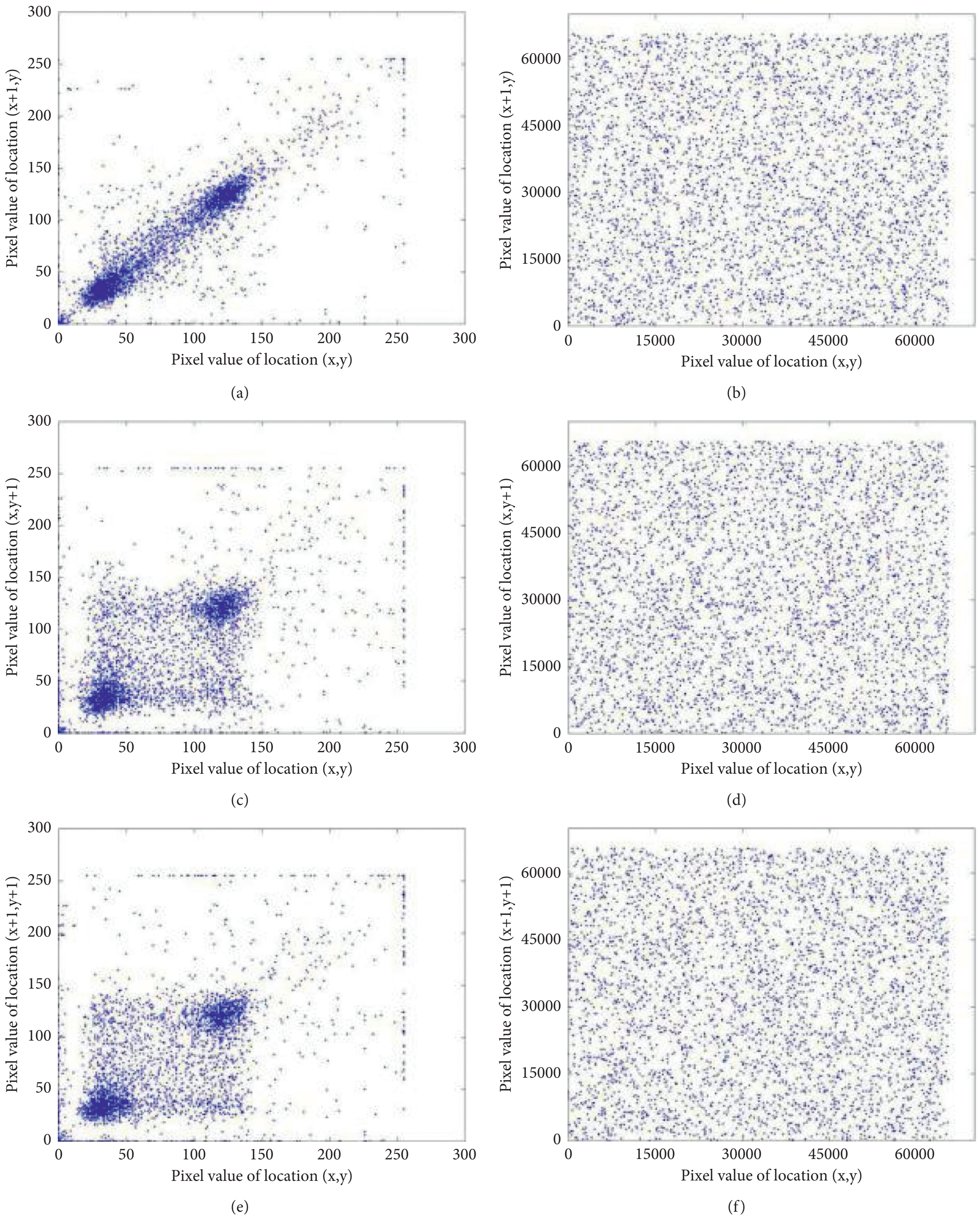


Figure 7: Analysis of the correlation coefficient between Lena plaintext and ciphertext.



(a)

(b)

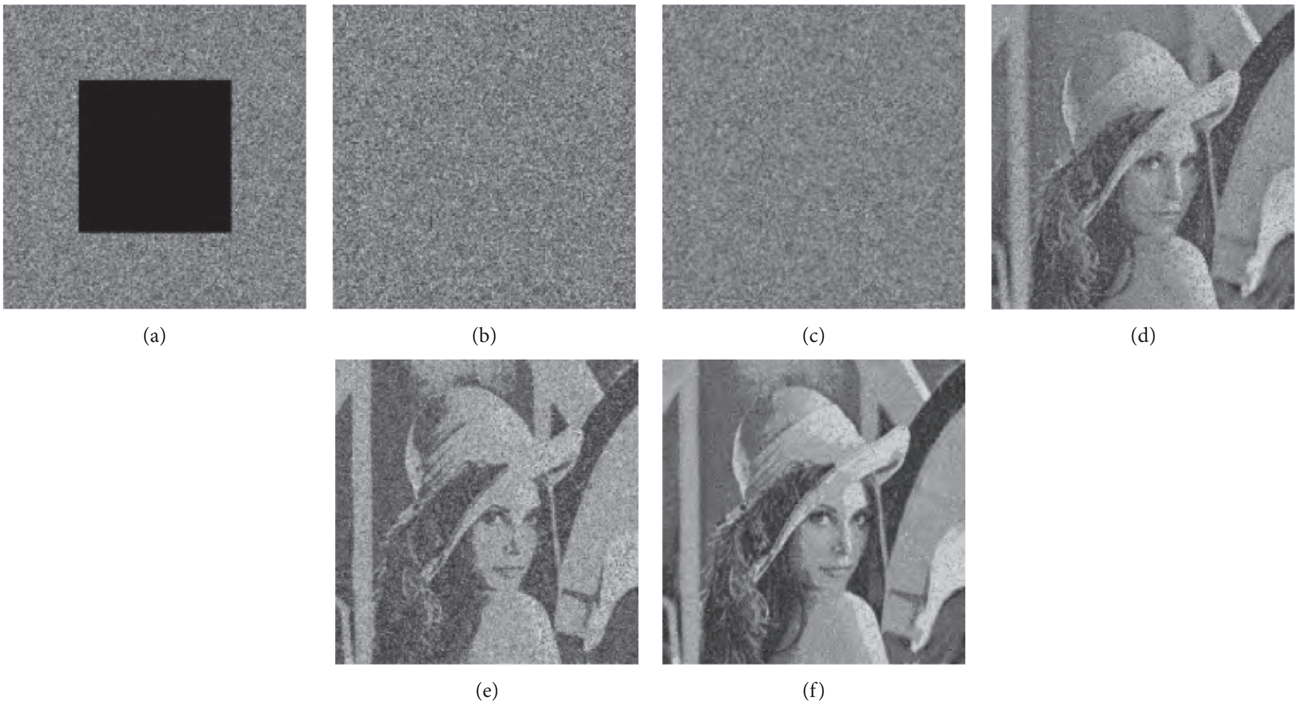
(c)

(d)

(e)

(f)

Figure 8: Analysis of the correlation coefficient between Skull plaintext and ciphertext.


(a) (b) (c) (d)

(e) (f)

Figure 9: Robustness test of Lena image.

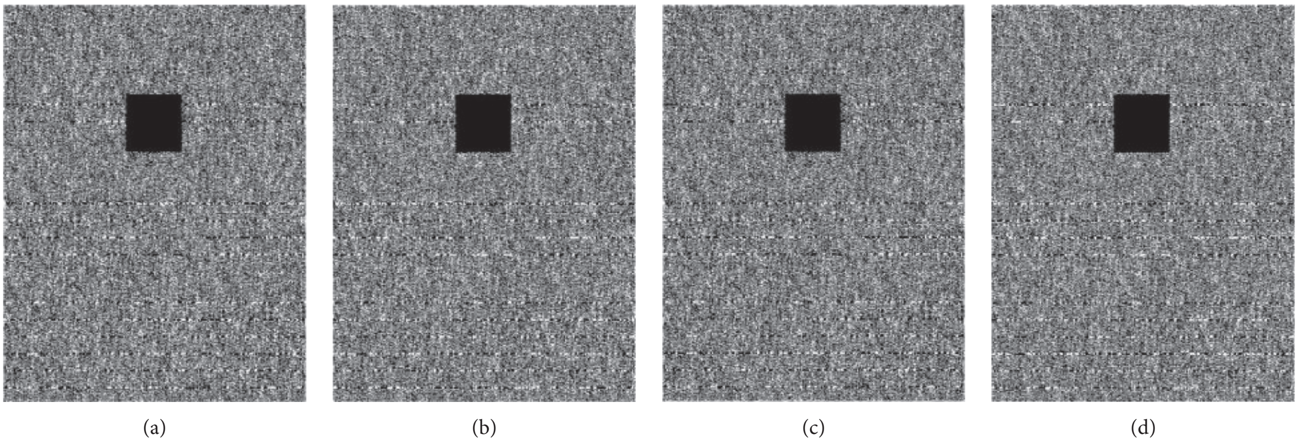

(a) (b) (c) (d)

Figure 10: The data loss in encrypted images.

Let the pixel of point $(i, j)$ in the two ciphertext images be $u_1(i, j)$ and $u_2(i, j)$; then, NPCR and UACI are calculated as

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

$$D(i, j) = \begin{cases} 0, & u_1(i, j) = u_2(i, j) \\ 1, & u_1(i, j) \neq u_2(i, j) \end{cases} \quad \mathrm{UACI} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\left| u_1(x, y) - u_2(i, j) \right|}{255} \times 100\%. \tag{26}$$

$N = 99.6094070$ and $U = 33.4635070$ are the expected values of the two indicators. In this study, one hundred groups of Lena images are selected for testing, and each group contains the image with one bit value changed. We

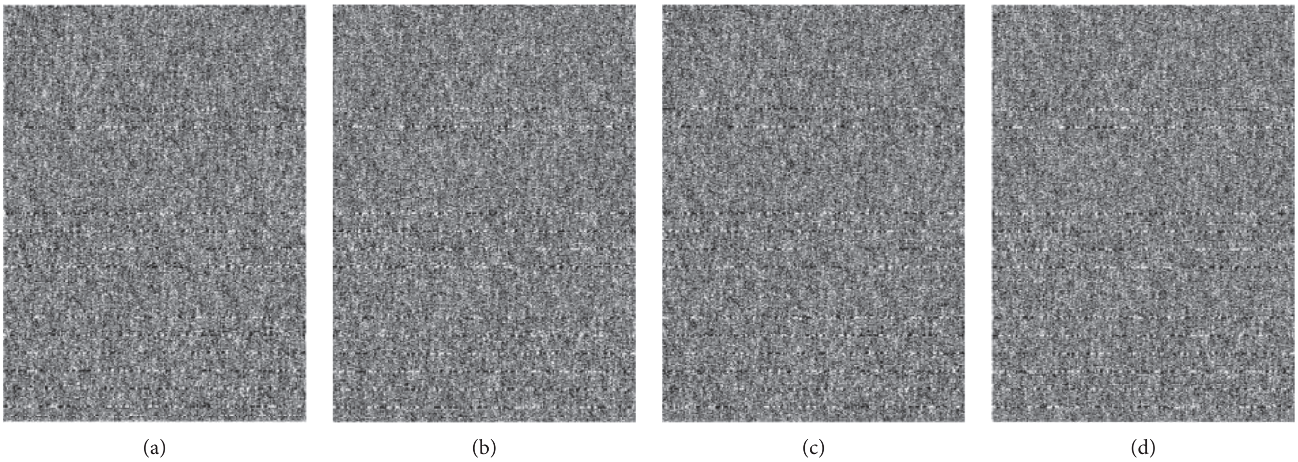


Figure 11: The encrypted images with adding 4% salt and pepper noise.

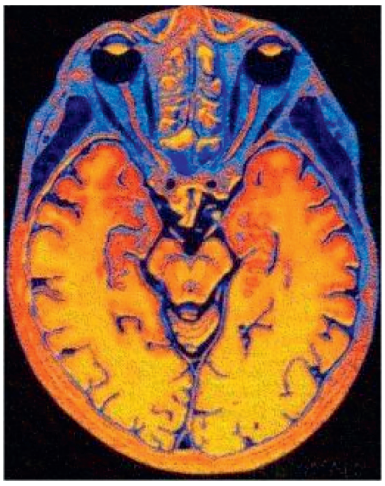


Figure 12: Decrypted image with data loss.

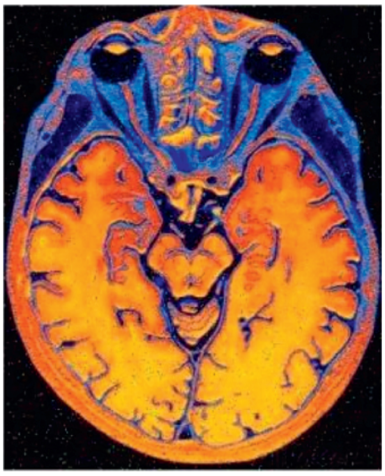


Figure 13: Decrypted image with noise.

take the average values of the two indicators, and the test results are shown in Table 7. The obtained NPCR and UACI by the proposed algorithm are closer to the ideal value. And the algorithm is highly sensitive to plaintext, which can effectively resist differential attack and selective plaintext attack.

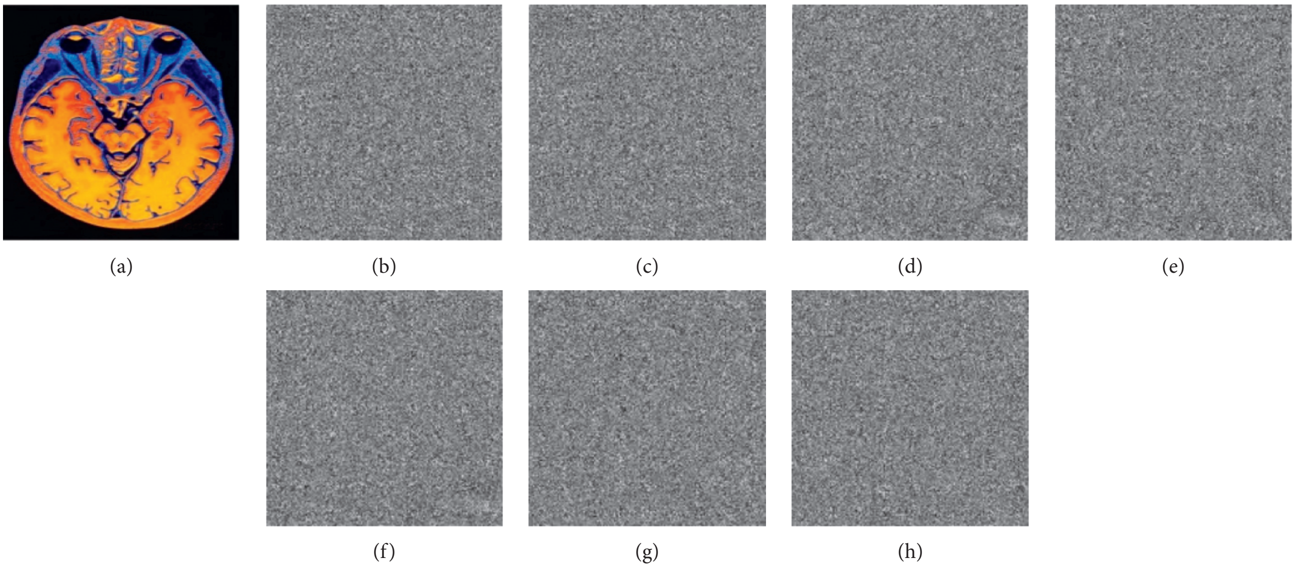

(a) (b) (c) (d) (e) (f) (g) (h)

Figure 14: Decrypted image with correct key and wrong key.

Table 6: Mean square error of decryption and plaintext with correct key and wrong key.

| Key | Global information entropy | Mean square error |
|---|---|---|
| Unchanged | 7.5968 | 0.8428 |
| $k_1 + \delta$ | 7.9993 | 0.8427 |
| $k_2 + \delta$ | 7.9989 | 0.8117 |
| $k_3 + \delta$ | 7.9988 | 0.8073 |
| $k_4 + \delta$ | 7.9991 | 0.8150 |
| $k_5 + \delta$ | 7.9989 | 0.8135 |
| $k_6 + \delta$ | 7.9991 | 0.8353 |
| $k_7 + \delta$ | 7.9991 | 0.8372 |

Table 7: Plaintext sensitivity test results.

| Method | NPCR | UACI |
|---|---|---|
| FRFS | 99.5651 | 30.9132 |
| ASFS | 99.5998 | 33.4602 |
| CENN | 99.6188 | 33.4823 |
| Proposed | 99.6102 | 33.4659 |

## 5. Conclusion

In summary, with the rapid development of computer network, images are mostly presented in the form of digital images, which are not only convenient to save but also fast to transmit. However, at the same time, image information is more likely to be leaked and stolen due to the openness of the network. Therefore, V-Net convolutional neural network is used to improve and optimize the general chaotic encryption algorithm, which has a certain degree of periodicity. Simulation results show that the proposed method improves the encryption effect.

## Data Availability

The data that support the findings of this study can be obtained from the corresponding author upon request.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This project was supported by Taif University researchers, supporting project no. TURSP-2020/107, Taif University, Taif, Saudi Arabia. The authors would like to acknowledge the Scientific Research Funds of Education Department of Liaoning Province in 2021 (General Project) (LJKZ1311) for its support, which facilitated the publication of this paper.

## References

[1] X. Wang, X. Qin, and C. Liu, “Color image encryption algorithm based on customized globally coupled map lattices,” *Multimedia Tools and Applications*, vol. 78, 2019.

[2] R. Ren, Z. Li, L. Deng, and X. Shan, “Non-orthogonal polarization multiplexed metasurfaces for tri-channel polychromatic image displays and information encryption,” *Optics Express*, vol. 10, 2021.

[3] T. Lin, H. Li, J. Liu, and S. Yin, “An efficient and secure Cipher-Text retrieval scheme based on mixed homomorphic encryption and Multi-Attribute Sorting Method under Cloud Environment,” *International Journal on Network Security*, vol. 20, no. 5, pp. 872–878, 2018.

[4] H. Wen-Wen, Z. Ri-Gui, and J. Shexiang, “Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms,” *Quantum Information Processing*, vol. 19, no. 3, pp. 1–29, 2020.

[5] L. Teng, H. Li, and S. Yin, “Im-MobiShare: An improved privacy preserving scheme based on asymmetric encryption and bloom filter for users location sharing in social network,” *Journal of Computers*, vol. 30, no. 3, pp. 59–71, 2019.

[6] Z. Yong, C. Aiguo, and T. Yingjun, “Plaintext-related image encryption algorithm based on perceptron-like network - ScienceDirect,” *Information Sciences*, vol. 526, pp. 180–202, 2020.

[7] R. Wang, G.-Q. Deng, and X.-F. Duan, “An image encryption scheme based on double chaotic cyclic shift and Josephus problem,” *Journal of Information Security and Applications*, vol. 58, no. 2, Article ID 102699, 2021.

[8] R. G. Zhou and Y. B. Li, “Quantum image encryption based on Lorenz hyper-chaotic system,” *International Journal of Quantum Information*, vol. 18, 2020.

[9] G. Li-Hua, C. Shan, and H. Xiang-Tao, “Quantum image encryption algorithm based on quantum image XOR operations,” *International Journal of Theoretical Physics*, vol. 55, 2016.

[10] Z. H. Gan, X. L. Chai, and D. J. Han, “A chaotic image encryption algorithm based on 3-D bit-plane permutation,” *Neural Computing & Applications*, pp. 1–20, 2018.

[11] G. d. Li and L. l. Wang, “Double chaotic image encryption algorithm based on optimal sequence solution and fractional transform,” *The Visual Computer*, vol. 35, no. 9, pp. 1267–1277, 2019.

[12] S. Yin, H. Li, and L. Teng, “A novel proxy Re-encryption scheme based on identity property and stateless broadcast encryption under cloud environment,” *International Journal on Network Security*, vol. 21, no. 5, pp. 797–803, 2019.

[13] S. Yin, J. Liu, and L. Teng, “Improved elliptic curve cryptography with homomorphic encryption for medical image encryption,” *International Journal on Network Security*, vol. 22, no. 3, pp. 419–424, 2020.

[14] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, “CorrAUC: a malicious bot-IoT traffic detection method in IoT network using machine-learning techniques,” *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3242–3254, 2021.

[15] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, “IoT malicious traffic identification using wrapper-based feature selection mechanisms,” *Computers & Security*, vol. 94, Article ID 101863, 2020.

[16] J. Yang, Z. Wei, and I. Moroz, “Periodic solutions for a four-dimensional hyperchaotic system,” *Advances in Difference Equations*, vol. 1, 2020.

[17] S. Gu, B. Du, and Y. Wan, “A new four-dimensional non-Hamiltonian conservative hyperchaotic system,” *International Journal of Bifurcation and Chaos*, vol. 30, 2020.

[18] I. Jemal, M. A. Haddar, C. Omar, and A. Mahfoudhi, “Performance evaluation of convolutional neural network for web security,” *Computer Communications*, vol. 175, pp. 58–67, 2021.

[19] Z. Wang, X. Huang, and N. Li, “Image encryption based on a delayed fractional-order chaotic logistic system,” *Chinese Physics B*, vol. 21, no. 5, pp. 107–112, 2012.

[20] H. Lai, M. A. Orgun, J. Xiao, J. Pieprzyk, L. Xue, and Y. Yang, “Provably secure three-party key agreement protocol using Chebyshev chaotic maps in the standard model,” *Nonlinear Dynamics*, vol. 77, no. 4, pp. 1427–1439, 2014.

[21] S. S. Jamal, A. Anees, M. Ahmad, M. F. Khan, and I. Hussain, “Construction of cryptographic S-boxes based on mobius transformation and chaotic tent-sine system,” *IEEE Access*, vol. 7, Article ID 173273, 2019.

[22] T. S. Ali and R. Ali, “A novel medical image signcryption scheme using TLTS and Henon chaotic map,” *IEEE Access*, vol. 8, Article ID 71974, 2020.

[23] S. Kanwal, S. Inam, O. Cheikhrouhou, K. Mahnoor, A. Zaguia, and H. Hamam, “Analytic study of a novel color image encryption method based on the chaos system and color codes,” *Complexity*, vol. 2021, no. 1, 19 pages, Article ID 5499538, 2021.

[24] S. Gbashi, P. B. Njobeh, and N. E. Madala, “Parallel validation of a green-solvent extraction method and quantitative estimation of multi-mycotoxins in staple cereals using LC-MS/MS,” *Scientific Reports*, vol. 10, no. 1, 2020.

[25] F. Milletari, N. Navab, and S. A. Ahmadi, “V-net: fully convolutional neural networks for volumetric medical image segmentation,” 2016, https://arxiv.org/abs/1606.04797.

[26] C. Zhao, J. H. Keyak, and J. Tang, “ST-V-Net: incorporating shape prior into convolutional neural networks for proximal femur segmentation,” *Complex & Intelligent Systems*, 2021.

[27] Y. Kim, S. Kim, T. Kim, and C. Kim, “CNN-based semantic segmentation using level set loss,” in *Proceedings of the 2019 IEEE Winter Conference on Applications of Computer Vision (WACV)*, pp. 1752–1760, WACV), Waikoloa Village, HI, USA, January, 2019.

[28] L. Meng, S. Yin, C. Zhao, H. Li, and Y. Sun, “An improved image encryption algorithm based on chaotic mapping and discrete wavelet transform domain,” *International Journal on Network Security*, vol. 22, no. 1, pp. 155–160, 2020.

[29] B. Vaseghi, S. Mobayen, S. S. Hashemi, and A. Fekih, “Fast reaching finite time synchronization approach for chaotic systems with application in medical image encryption,” *IEEE Access*, vol. 9, Article ID 25911, 2021.

[30] C. T. Selvi, J. Amudha, and R. Sudhakar, “Medical image encryption and compression by adaptive sigma filterized synorr certificateless signcryptive Levenshtein entropy-coding-based deep neural learning,” *Multimedia Systems*, pp. 1–16, 2021.

[31] S. J. Sheela, K. V. Suresh, and D. Tandur, “Cellular neural network-based medical image encryption,” *SN Computer Science*, vol. 1, no. 6, 2020.

[32] M. Shafiq, Z. Tian, A.. , A. Bashir, A. Jolfaei, and X. Yu, “Data mining and machine learning methods for sustainable smart cities traffic classification,” *A Survey. Sustainable Cities and Society*, vol. 60, 2020.

[33] I. Ahmad, T. Rahman, A. Zeb et al., “Analysis of security attacks and taxonomy in underwater wireless sensor networks,” *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 1444024, 15 pages, 2021.

[34] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, “Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city,” *Future Generation Computer Systems*, vol. 107, pp. 433–442, 2020.

[35] M. Sajjad, T. Safdar Malik, S. Khurram et al., “Efficient joint key authentication model in E-healthcare,” *Computers, Materials & Continua*, vol. 71, no. 2, pp. 2739–2753, 2022.