Data encryption based on a 9D complex chaotic system with quaternion for smart grid

Fangfang Zhang(张芳芳)[1], Zhe Huang(黄哲)[1], Lei Kou(寇磊)[2,†], Yang Li(李扬)[3], Maoyong Cao(曹茂永)[1], and Fengying Ma(马凤英)[1]

[1] *School of Information and Automation Engineering, Qilu University of Technology (Shandong Academy of Sciences), Jinan* 250353, *China*
[2] *Institute of Oceanographic Instrumentation, Qilu University of Technology (Shandong Academy of Sciences), Qingdao* 266000, *China*
[3] *School of Electrical Engineering, Northeast Electric Power University, Jilin* 132000, *China*

(Received 12 March 2022; revised manuscript received 31 May 2022; accepted manuscript online 8 June 2022)

With the development of smart grid, operation and control of a power system can be realized through the power communication network, especially the power production and enterprise management business involve a large amount of sensitive information, and the requirements for data security and real-time transmission are gradually improved. In this paper, a new 9-dimensional (9D) complex chaotic system with quaternion is proposed for the encryption of smart grid data. Firstly, we present the mathematical model of the system, and analyze its attractors, bifurcation diagram, complexity, and 0–1 test. Secondly, the pseudo-random sequences are generated by the new chaotic system to encrypt power data. Finally, the proposed encryption algorithm is verified with power data and images in the smart grid, which can ensure the encryption security and real time. The verification results show that the proposed encryption scheme is technically feasible and available for power data and image encryption in smart grid.

Keywords: 9-dimensional complex chaotic system, data encryption, quaternion, smart grid, real-time

PACS: 05.45.Pq, 93.85.Bc, 06.30.Ft **DOI:** 10.1088/1674-1056/ac76b2

1. Introduction

Because a power system requires real-time transmission of data communication, most security applications in the computer network cannot be implemented in the power system.[1] In the smart grid, most of the critical real-time data is transmitted on the network in plain text, and real-time data encryption is not involved in real-time control. The important data is still in the form of plain text, which poses major safety hazards to the safe and stable operation of the power system.[2,3] The safe operation of power equipment is directly effected by the function of remote adjusting, remote control and remote measure in the smart grid. Especially, when the power information network is maliciously attacked, it results in data loss, tampering and seriously threatens the normal operation of the power information network and then affects the power physical network.[4,5] Finally, the malicious attack causes a chain reaction in the power network. In extreme cases, the malicious attack propagate alternately between the power information network and power physical network. Therefore, the safe and stable operation of the power grid cannot be guaranteed. For example, once the power information network is attacked and the monitor data is tampered with abnormal data. It may cause the power equipment to shut down and bring huge economic losses. For purpose of preventing malicious attackers from sending false abnormal monitor data, it is inevitable to prevent data leakage.

In addition, when encountering the suspected abnormal monitor data, it is crucial to confirm the condition of the equipment as soon as possible. The maintenance personnel should take photos of the equipment and send them to the control center. Timely reporting of the power equipment status can effectively improve the operation efficiency of the smart grid. Due to data information security, the report is forced to delay. Therefore, it is of great practical significance to study an encryption algorithm that takes into account both confidentiality and real time.

A deterministic aperiodic model was proposed by Lorenz who is a meteorologist at MIT. He was convinced that chaos[6,7] is a science that uses fractal geometry to analyze and study the nonlinear dynamics shown in phenomenons such as the butterfly effect. Grassber designed a method to reconstruct the dynamic system. It makes the chaos enter the practical application stage by introducing the Lyapunov exponent. By the end of the 20th century, chaos theory began to integrate with other subjects, such as chaotic secure communication,[8,9] chaotic cryptography,[10,11] and chaotic economics. The chaotic signal, which has inherent randomness, ergodicity and sensitivity to initial conditions, is generated by a deterministic system. These characteristics are very similar to the diffusion and scrambling properties in the Shannon classical model. Therefore, chaos theory has a wide application prospect in the field of information security.

The dynamic behavior of high-dimensional complex chaotic systems is more complicated than real chaotic sys-

[†]Corresponding author. E-mail: koulei1991@hotmail.com
© 2023 Chinese Physical Society and IOP Publishing Ltd

tems. The real part and the imaginary part are independent in complex-valued chaotic systems, which improves the ergodicity of the chaotic system. Hence, high-dimensional complex chaotic systems can overcome the disadvantages of short period, uneven distribution of chaotic sequences and small key space. These belong to the low-dimensional chaotic system.

The basic mathematical concept of quaternion[12,13] was proposed by the famous mathematician Hamilton in 1843. He introduced a function called the complex plane function and obtained a four-dimensional space. The quaternion can be regarded as an extension of a simple complex number. The plural number is mainly composed of a real part and an international unit i as an imaginary number. In the same way, quaternion can also be regarded to be composed of a real part and three imaginary units i, j, and k.

Many researchers have developed a great number of encryption schemes for the smart grid. In February 2016, Liu *et al.*[14] proposed a lightweight authenticated communication scheme for the smart grid, which ensures a secure two-way communication between the smart meters and the neighborhood gateway. In June 2017, Saxena and Grijalva[15] proposed a novel scheme based on dynamic secrets and encryption with secret keys. The scheme generates a series of dynamic secrets over the communication network, which are used to generate secret keys for data encryption. In June 2019, Gope and Sikdar[16] proposed a lightweight and privacy-friendly masking-based spatial data aggregation scheme for secure forecasting of power demand in smart grids. In March 2020, Song *et al.*[17] designed a dynamic membership data aggregation scheme by the homomorphic encryption and ID-based signature. It reduces the complexity on a new user's joining and an old user's quitting. In May 2021, Qian *et al.*[18] proposed a lightweight t-times homomorphic encryption scheme, which can reduce the computational cost of smart devices further and resist quantum attacks.

Although scholars have proposed good encryption schemes for smart grid, there still exist two problems to be solved:

(1) There is no discussion on image transmission encryption for smart grid. Compared with traditional text information, digital image contains more data.

(2) The encryption and decryption time are not discussed.

In order to overcome the above shortcomings, a new complex chaotic system with quaternion is proposed in this paper. This new chaotic system is 9-dimensional and has good encryption performances. The novelty and contributions of this paper are summarized as follows:

(i) A novel complex chaotic system with quaternion is proposed. The dynamic characteristics are discussed. At the same time, there are a few studies on the chaotic system with quaternion.

(ii) In order to ensure real-time transmission in the smart grid, an encryption algorithm based on the novel chaotic system is proposed. The image and the check code, which are encryted by the encryption algorithm, can be sent in time.

(iii) Moreover, it can also protect information from being tampered. The control center can identify the correct information and will not be misled to turn off the equipment for no reason. Therefore, economic losses are avoided.

The specific content is arranged as follows: The dynamics characteristics of the proposed chaotic system are discussed in Section 2. An encryption algorithm is expounded and compared with other algorithms by the usage of some security performances in Section 3. In Section 4, the proposed encryption scheme is verified with data and images in the smart grid, and the security analysis is provided. The main work of this paper is summarized in Section 5.

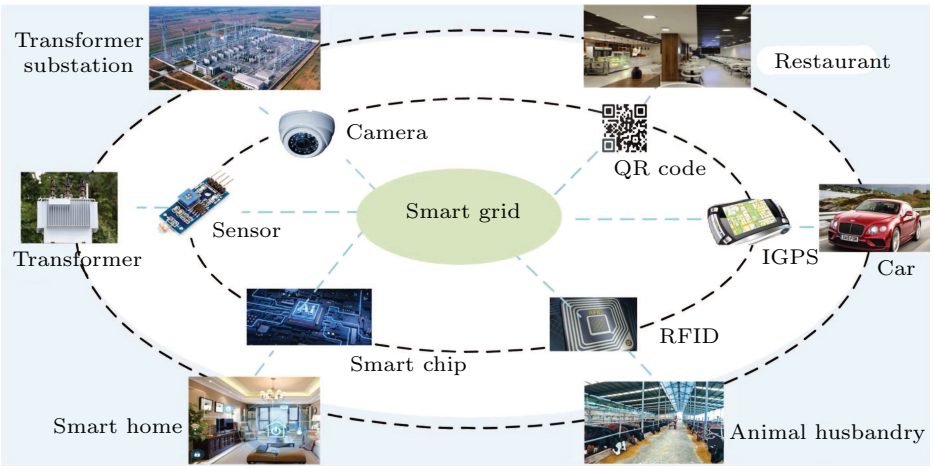


Fig. 1. The smart grid applications.

2. Complex chaotic system with quaternion

The mathematical expression of complex Chen chaotic system[19] is

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1), \\ \dot{x}_2 = (b-a)x_1 + bx_2 - x_1x_3, \\ \dot{x}_3 = (\bar{x}_1x_2 + x_1\bar{x}_2)/2 - cx_3, \end{cases} \tag{1}$$

where a, b are positive constants; and x_1, x_2, x_3 are independent variables.

Then the mathematical expression of the quaternion is given as follows:

$$\begin{cases} x_1 = u_1 + iu_2 + ju_3 + ku_4, \\ x_2 = u_5 + iu_6 + ju_7 + ku_8, \\ x_3 = u_9, \end{cases} \tag{2}$$

where u_i $(i = 1, 2, \ldots, 9)$ are independent variables; and i, j, k are imaginary units.

System (1) is extended to the quaternion field, and substitute Eq. (2) into Eq. (1). Finally we can separate the real part from the imaginary part and obtain

$$\begin{cases} \dot{u}_1 = a(u_5 - u_1), \\ \dot{u}_2 = a(u_6 - u_2), \\ \dot{u}_3 = a(u_7 - u_3), \\ \dot{u}_4 = a(u_8 - u_4), \\ \dot{u}_5 = (b-a)u_1 + bu_5 - u_1u_9, \\ \dot{u}_6 = (b-a)u_2 + bu_6 - u_2u_9, \\ \dot{u}_7 = (b-a)u_3 + bu_7 - u_3u_9, \\ \dot{u}_8 = (b-a)u_4 + bu_8 - u_4u_9, \\ \dot{u}_9 = u_1u_5 + u_2u_6 + u_3u_7 - cu_9, \end{cases} \tag{3}$$

where a, b, c are positive constants. Next, the dynamic characteristics of the system are intuitively analyzed from the chaos attractor, bifurcation diagram, 0–1 test, and complexity analysis.

2.1. Chaos attractor

Set $a = 27$, $b = 23$, $c = 1$. For initial conditions (0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1), the phase portraits of attractor are depicted in Fig. 2.

Lyapunov exponent[18] is a numerical characteristic representing the average exponential divergence rate of adjacent trajectories in phase space. It is an important index to analyze the dynamic characteristics. Only when there are positive, negative values and zero, the system is chaotic. The Lyapunov exponents of system (3) are LE1 = 2.028, LE2 = 1.913, LE3 = 1.863, LE4 = 1.502, LE5 = 0.000, LE6 = −0.316, LE7 = −5.380, LE8 = −5.524, LE9 = −5.809. The corresponding Lyapunov exponents are depicted in Fig. 3. The Lyapunov exponent of the proposed 9-dimensionol system is (+, +, +, +, 0, −, −, −, −). Therefore, the system is chaotic.

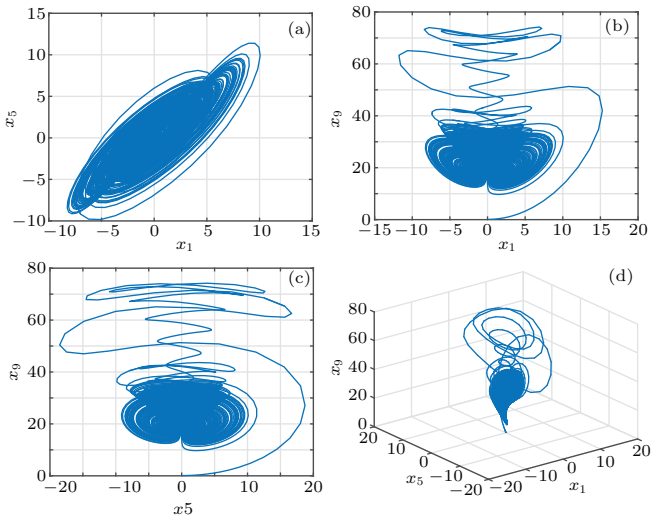


Fig. 2. Phase portraits of system (3): (a) $x_1 - x_5$, (b) $x_1 - x_9$, (c) $x_5 - x_9$, (d) $x_1 - x_5 - x_9$.

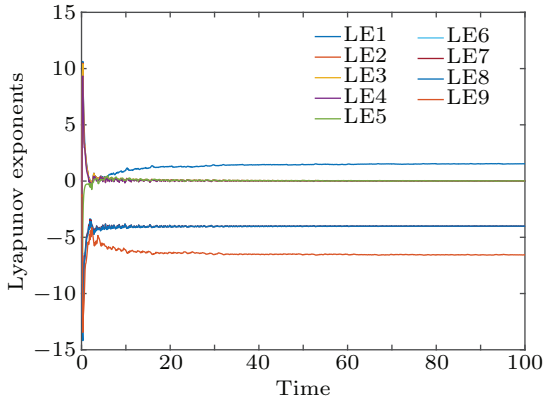


Fig. 3. The Lyapunov exponent spectrum of system (3).

2.2. Bifurcation diagram

With different values of system parameters, the dynamic motion state of the system will change. This phenomenon is called bifurcation.[19] When there is only one point in the bifurcation diagram, it shows that the system is in a steady state within this parameter range.

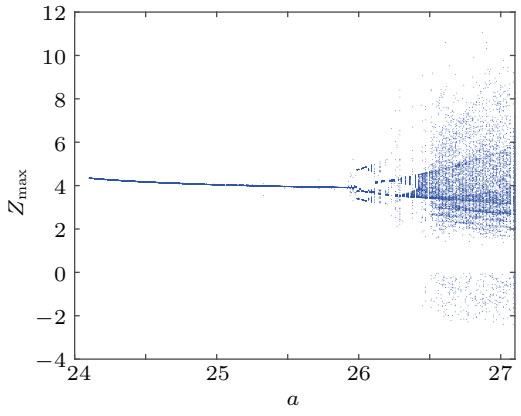


Fig. 4. The bifurcation of system (3).

On the contrary, when there are countless points in the bifurcation diagram, it means that the system is chaotic within

this parameter range. Therefore, the bifurcation diagram varying with parameters can be used to analyze the performance characteristics of the system. The bifurcation diagram of variable x_1 varying with parameter α is shown in Fig. 4. According to Fig. 4, the system ceaselessly branches between diverse states with the change of α, and the system comes to a chaotic state lastly.

2.3. The 0–1 test

By calculating the transformation variables of the sequence $s(n)$ and $p(n)$, the system state is judged. This method is called 0–1 test.

$$s(n) = \sum_{j=1}^{n} x(j)\sin(jc), \quad n = 1,2,\ldots,N, \tag{4}$$

$$p(n) = \sum_{j=1}^{n} x(j)\cos(jc), \quad n = 1,2,\ldots,N, \tag{5}$$

where $c \in (0,\pi)$, $x(j)$ $(j = 1,2,\ldots,N)$ is the test sequence.

Next, we verify the trajectory of $p(n)$–$s(n)$. If the trajectory shows the Brownian motion, the test sequence is chaotic. The "0–1 test" diagram of system (3) is shown in Fig. 5. It can be seen that the system (3) shows the Brownian motion. Therefore, it is chaotic.

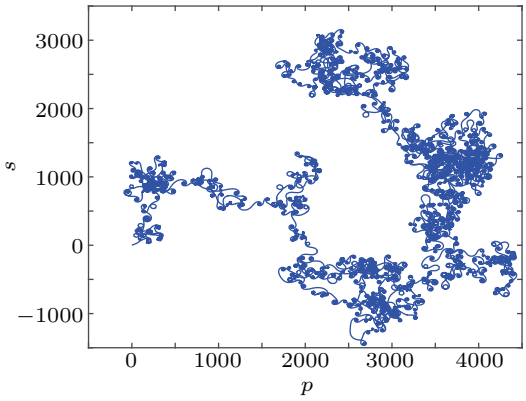


Fig. 5. The 0–1 test diagram.

2.4. Complexity analysis

The Shannon entropy (SE) algorithm and the chromatogram (C_0) algorithm are used to verify and analyze the complexity of chaotic systems when the two parameters change. The SE algorithm obtains the spectral entropy from the Shannon entropy algorithm. The C_0 algorithm divides the sequence into regular and irregular parts. Then it calculates the proportion of irregular parts in the whole sequence. The chromatogram of parameter α varying with parameter c is shown in Fig. 6. The darker the color is, the higher the complexity is.

Through the above indexes, the dynamic characteristics of the system (3) are analyzed. When $a = 1/7$, $b = 2/7$ and $c = 1$, the system (3) has complex dynamic behavior, inherent randomness and unpredictability. Then it can generate pseudo random sequences required by the proposed algorithm.

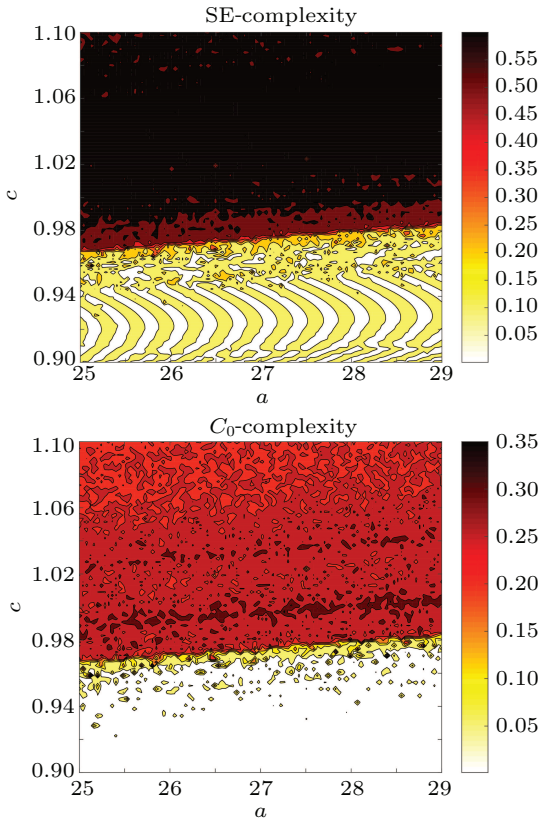


Fig. 6. The chromatogram of x_1 sequence: (a) SE algorithm, (b) C_0 algorithm.

3. The encryption algorithm and its comparison

Generally speaking, encrypted data will not be partially selected to ensure the integrity of data. However, when the equipment network breaks down, in order to ensure the real-time reporting of fault data, we can select partial sensitive or important information as the encryption region to decrease the encryption time.

It is of great importance to protect the sensitive information in the image, such as faces or devices. There is no need to keep the rest of the background area of the image confidential. Therefore, partial areas are only encrypted to ensure the real time.

In Section 2, the dynamic characteristics of chaotic system (3) are analyzed. The quasi random sequence with good pseudorandomness, low correlation and high complexity is generated by the chaotic system (3). Taking the pseudo-random sequence as the key sequence can ensure the security of encryption.

The flow chart of the proposed encryption algorithm is shown in Fig. 7.

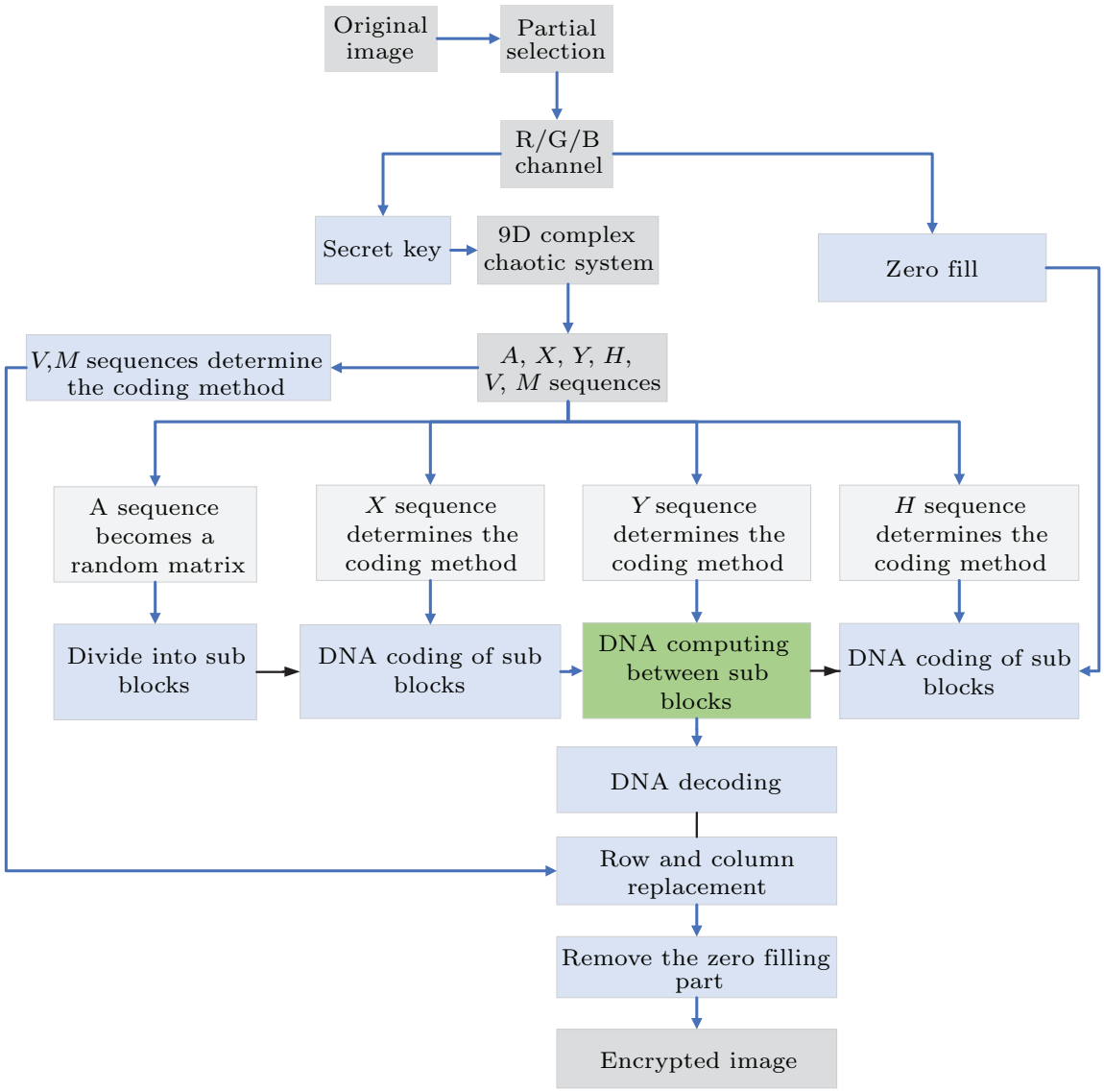


Fig. 7. The flow chart of image encryption algorithm.

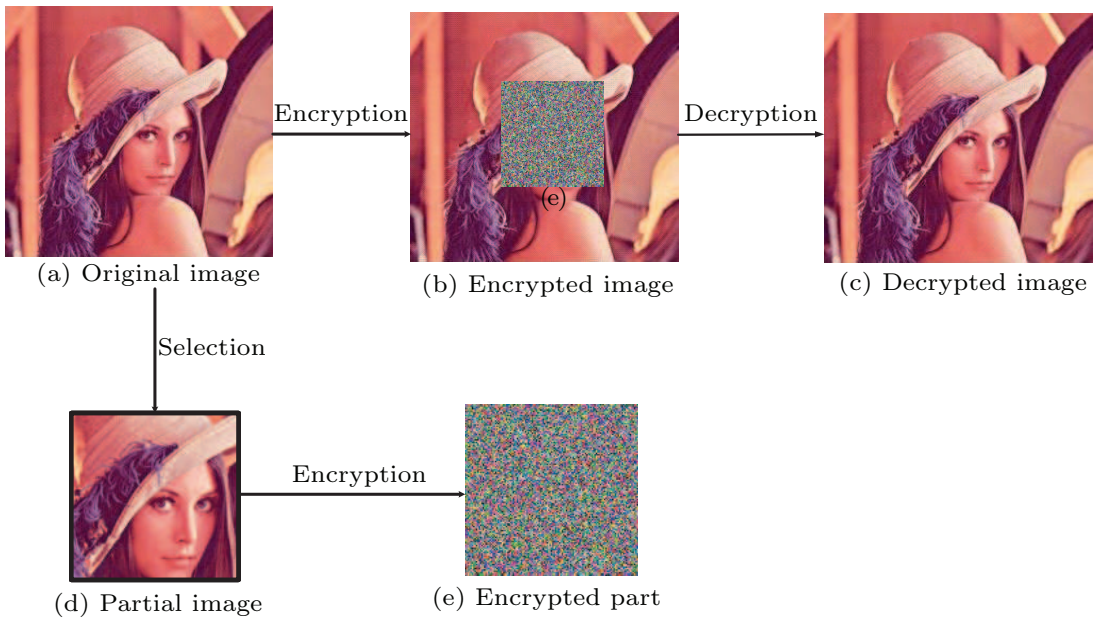


Fig. 8. The flow chart of experimental results.

The steps of the image encryption algorithm are as follows:

Step 1 Partially select image. Separate the image channel and change it into R, G and B channels. Then fill the remaining part in zero pixel value.

Step 2 Select the gray value of each channel and its combination as the key. Then the image is divided into 4×4 subblocks. Call it A1.

Step 3 Randomly select six sequences from the system (3). Then name them as A, X, Y, H, V, M sequences. Change the A sequence into a matrix of the same image size. It is divided into 4×4 subblocks. Name it as A2.

Step 4 Encode A1 and A2 using the DNA coding scheme. The coding rule is determined by the X and Y sequences, respectively. Name them B1 and B2.

Step 5 Encode B1 and B2 using the DNA computing scheme. The computing scheme is determined by the H sequence. Call it C1.

Step 6 Decoding C1 using the DNA coding scheme. Replace the row and column. The row and column replacement orders are determined by V and M sequences, respectively. Finally, the zero filling part is removed.

Set $a=27$, $b=23$, $c=1$ in system (3) and initial condition is the pixel average value of original image. In this encryption algorithm, the "Lena" image is an encrypted object. Select the area to be encrypted in the Lena image. The selected area should correspond to sensitive information that can identify an individual, such as a face. The rest is not encrypted.

The encryption process is depicted in Fig. 8, where Fig. 8(a) is the original image, Fig. 8(b) is the encrypted image, Fig. 8(c) is the decrypted image, and Fig. 8(d) is the partial image. The original features and information are masked in Fig. 8(e).

3.1. Reconstruction quality analysis

In order to measure the distortion of the decrypted image, structural similarity (SSIM) is introduced. SSIM contains three independent components: luminance, contrast and structure. The SSIM can be expressed as follows:

$$\begin{cases} U(X,Y)=\frac{2k_Xk_Y+D_1}{{k_X}^2+{k_Y}^2+D_1},\\ O(X,Y)=\frac{2n_Xn_Y+D_2}{n_X^2+n_Y^2+D_2},\\ T(X,Y)=\frac{n_{XY}+D_3}{n_Xn_Y+D_3},\\ SSIM=U(X,Y)O(X,Y)T(X,Y), \end{cases} \tag{6}$$

where k_X and k_Y are the mean of images X and Y; n_X and n_Y are the variance of images X and Y; n_{XY} is the covariance of images X and Y. D_1 and D_2 are two constants with small value when the denominator is up to zero; $D_3=D_1/2$. $U(X,Y)$ is the luminance, $O(X,Y)$ denotes contrast, $T(X,Y)$ represents structure. The SSIM of Figs. 8(a) and 8(c) is 1 by calculation.

Next, subtract the pixel value of the original image from each pixel value of the decrypted image. The result of this calculation is zero, which indicates that the image pixel value is restored to normal.

3.2. Correlation coefficient

In the horizontal, vertical and diagonal directions, the adjacent pixel values of plaintext and ciphertext images are randomly selected. Calculate the correlation coefficient between two adjacent pixels. The numerical range of correlation coefficient of adjacent pixels is $[-1,1]$. If the value is close to 1, the adjacent pixels are strong related. Contrarily, the adjacent pixels are weak related. The formula of the correlation coefficient r_{uv} between u_i and v_i is given as follows:

$$\begin{cases} E(u)=\frac{1}{N}\sum\limits_{i=1}^{N}u_i,\\ D(u)=\frac{1}{N}\sum\limits_{i=1}^{N}(u_i-E(u))^2,\\ \mathrm{Cov}(u,v)=\frac{1}{N}\sum\limits_{i=1}^{N}(u_i-E(u))(v_i-E(v)),\\ r_{uv}=\frac{\mathrm{Cov}(u,v)}{\sqrt{D(u)}\sqrt{D(v)}}, \end{cases} \tag{7}$$

where E indicates the average pixel value, D and Cov represent the variance and the covariance of pixels, respectively; r_{uv} is the correlation coefficient; N is the number of pixels; u_i, v_i $(i=1,\ldots,N)$ are pixels. As listed in Tables 1 and 2, though compared with other algorithms, the confidentiality is slightly inferior, this algorithm has an advantage in shortening the encryption and decryption time.

Table 1. Adjacent pixels and time comparison.

Cipher image	Horizontal	Vertical	Diagonal
Ref. [20]	+0.0083	-0.0054	−0.0010
Ref. [21]	−0.0168	+0.0445	−0.0022
Ref. [22]	−0.0024	+0.0035	+0.0014
Ref. [23]	+0.0010	−0.0031	−0.0008
Proposed method	−0.0112	+0.0326	−0.0032

Table 2. Encryption and decryption time.

Cipher image	Encryption time (s)	Decryption time (s)
Ref. [20]	0.669	0.659
Ref. [21]	2.796	2.788
Ref. [22]	1.840	1.827
Ref. [23]	0.670	0.661
Proposed method	0.170	0.177

3.3. Histogram

The frequency of all gray values can be intuitively seen from the histogram. The pixel distributions of each pixel level can be seen in Figs. 9(a)–9(c) with the histograms of the plaintext image. Figures 9(d)–9(f) are the histograms of the ciphertext image. The pixel distribution of the plaintext image is uneven. After encryption, the histogram of ciphertext image is almost uniform and is quietly different from those of the plaintext image. The results verify that the proposed encryption algorithm is resistant to statistical attacks.

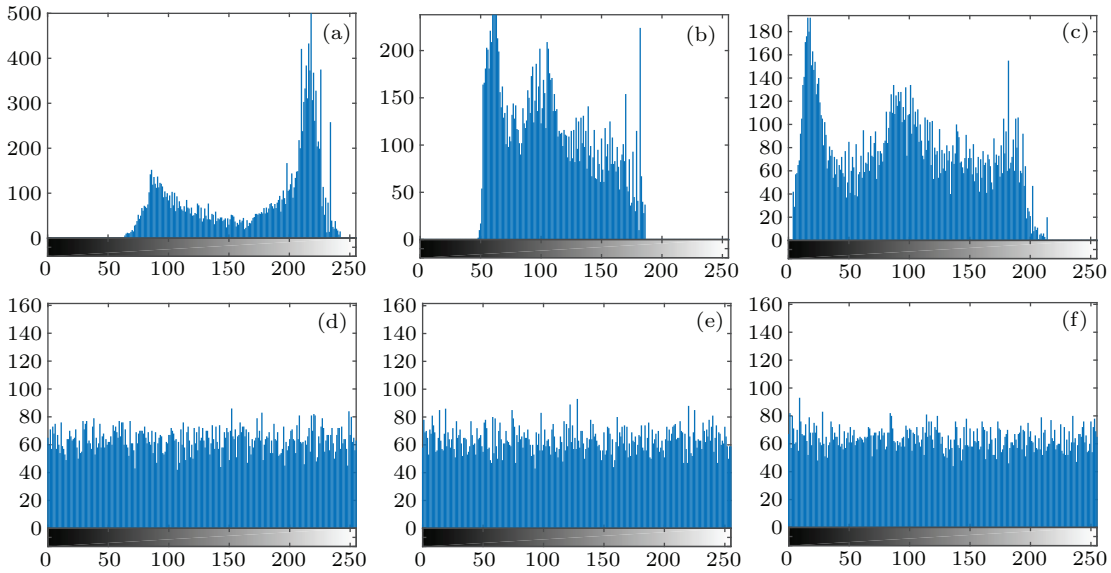


Fig. 9. Histograms: (a) R channel in plain image, (b) G channel in plain image, (c) B channel in plain image, (d) R channel in cipher image, (e) G channel in cipher image, (f) B channel in cipher image.

3.4. Information entropy

As a quantitative standard, information entropy is the relative complexity of the image information. The image information entropy with average gray value distribution is relatively close to 8. The formula of F is given as follows:

$$F = -\sum_{i=1}^{T} e(x_i)\log_2 e(x_i), \tag{8}$$

where T is the maximum gray value 255, and $e(x_i)$ is the gray value probability. As shown in Table 3, the information entropy of the proposed algorithm is slightly smaller, but the encryption time is greatly shortened. This means that this algorithm can effectively shorten the encryption time.

Table 3. The information entropy.

Image	Plaintext image	Ciphertext image
Ref. [20]	7.4375	7.9972
Ref. [21]	7.4375	7.9994
Ref. [22]	7.4375	7.9972
Ref. [23]	7.4375	7.9994
Proposed method	7.4375	7.9957

4. The encryption scheme in the smart grid

4.1. Image encryption

Two actual pictures of the distribution network are selected as the encryption objects. Their sizes are, respectively, 256×256 and 512×512. Call them image 1 and image 2.

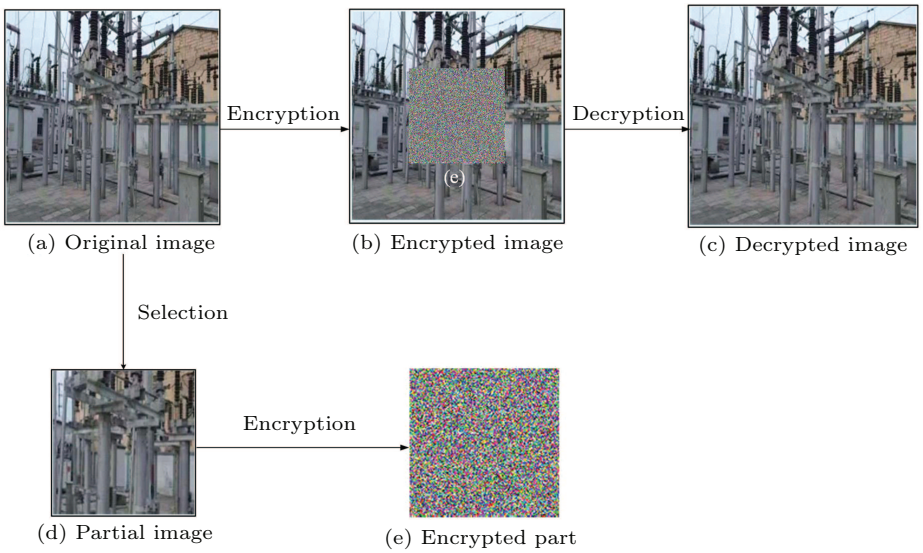


Fig. 10. The flow chart of experimental results.

Select the area to be encrypted in image 1 and image 2. The selected area should correspond to sensitive information that can identify the physical status of equipments. Therefore, the central area containing distribution network equipments is selected.

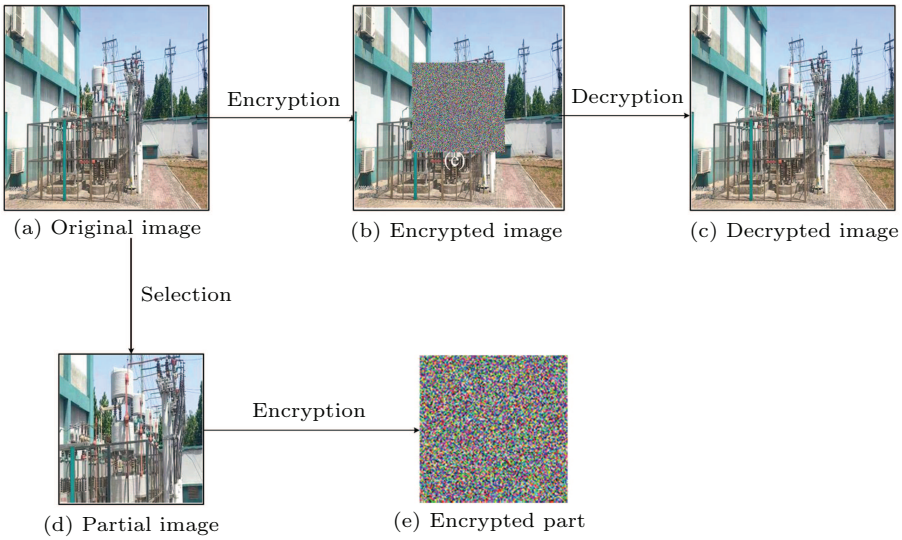


Fig. 11. The flow chart of experimental results.

The encryption process of image 1 is shown in Fig. 10, where Fig. 10(a) is the original image 1, Fig. 10(b) is the encrypted image 1, Fig. 10(c) is the decrypted image 1, and Fig. 10(d) is the partial image 1. The original features and information are masked in Fig. 10(e). Figure 11 shows the same encryption process of image 2.

Then, the encrypted image is analyzed by the histogram, correlation coefficient, information entropy, sensitivity of key and reconstruction quality.

4.1.1. Histogram

According to Figs. 12 and 13, the histogram after encryption is evenly distributed, which can effectively resist statistical attacks.

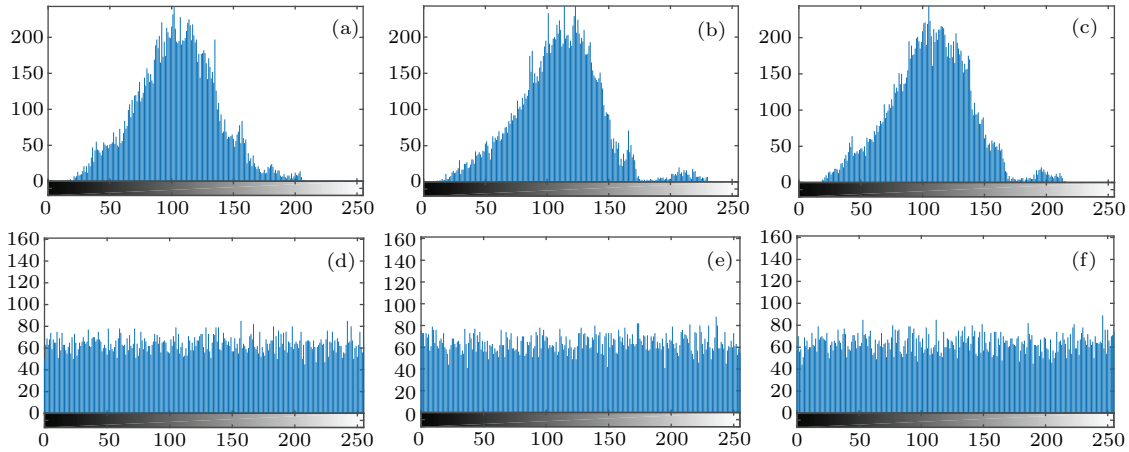


Fig. 12. Histograms of the original image 1 and the encrypted image 1: (a) R channel in plain image, (b) G channel in plain image, (c) B channel in plain image, (d) R channel in cipher image, (e) G channel in cipher image, (f) B channel in cipher image.

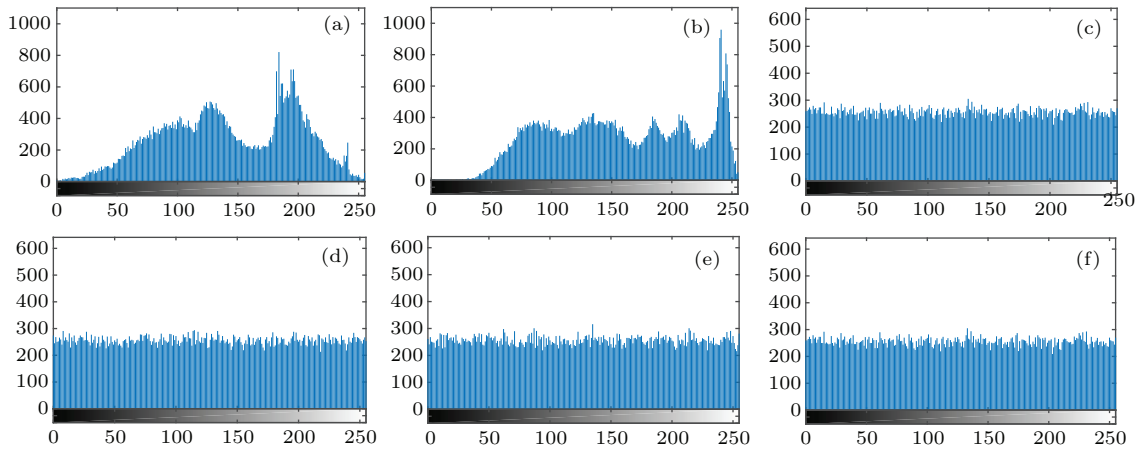


Fig. 13. Histograms of the original image 2 and the encrypted image 2: (a) R channel in plain image, (b) G channel in plain image, (c) B channel in plain image, (d) R channel in cipher image, (e) G channel in cipher image, (f) B channel in cipher image.

4.1.2. Correlation coefficient

According to Tables 4 and 5, the strong correlation between the pixels of the original image after a short time of encryption is weakened.

Table 4. Adjacent pixels comparison.

Image	Horizontal	Vertical	Diagonal
Image 1	0.9053	0.7714	0.7060
Image 2	0.9277	0.8423	0.8061
Cipher image 1	–0.0104	0.0011	0.0044
Cipher image 2	0.0133	–0.0042	–0.0137

Table 5. Encryption and decryption time.

Cipher image	Encryption time	Decryption time
Image 1	0.188s	0.226s
Image 2	0.611s	0.816s

4.1.3. Information entropy

According to Table 6, the information entropy of encrypted images with a short encryption time is close to the maximum. It means that this encryption algorithm takes into account both confidentiality and real time.

Table 6. The information entropy of image.

Image	Plaintext image	Ciphertext image
Image 1	7.0589	7.9964
Image 2	7.6724	7.9989

4.1.4. Sensitivity of key

Under the initial conditions (0.10002, 0.10002, 0.10002, 0.10002, 0.10002, 0.10002, 0.10002, 0.10002, 0.10002), the values of other parameters in system (3) remain unchanged. The generated sequences are used to decrypt the cipher images 1 and 2. According to Fig. 14, these sequences fail to decrypt the cipher images 1 and 2. The proposed encryption algorithm is sensitive to the key.

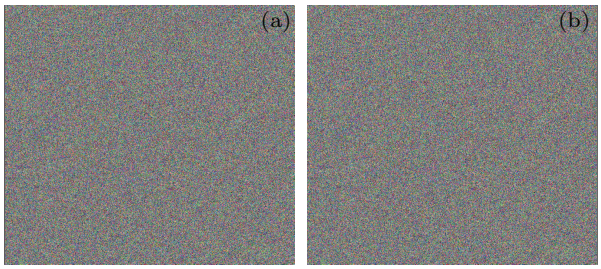


Fig. 14. The decryption results of wrong key: (a) the decryption results of cipher image 1, (b) the decryption results of cipher image 2.

4.1.5. Reconstruction quality analysis

According to Table 7, the reconstruction qualities of images 1 and 2 are excellent.

From the correlation coefficient, histogram, information entropy, sensitivity of key and reconstruction quality, the proposed encryption algorithm has good confidentiality and real time in the image transmission of the smart grid.

Table 7. Reconstruction quality analysis.

Image	Pixel-value difference	SSIM
Figs. 10(b) and 10(d)	0	1
Figs. 11(b) and 11(d)	0	1

4.2. Data encryption

Modbus protocol is adopted in the process of transmitting monitor data. The composition of Modbus protocol is as follows:

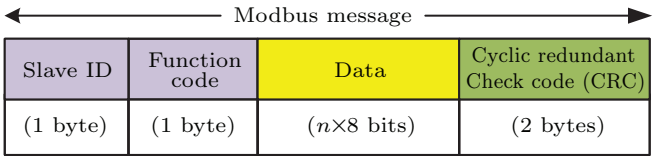


Fig. 15. The message frame composition in modbus RTU mode.

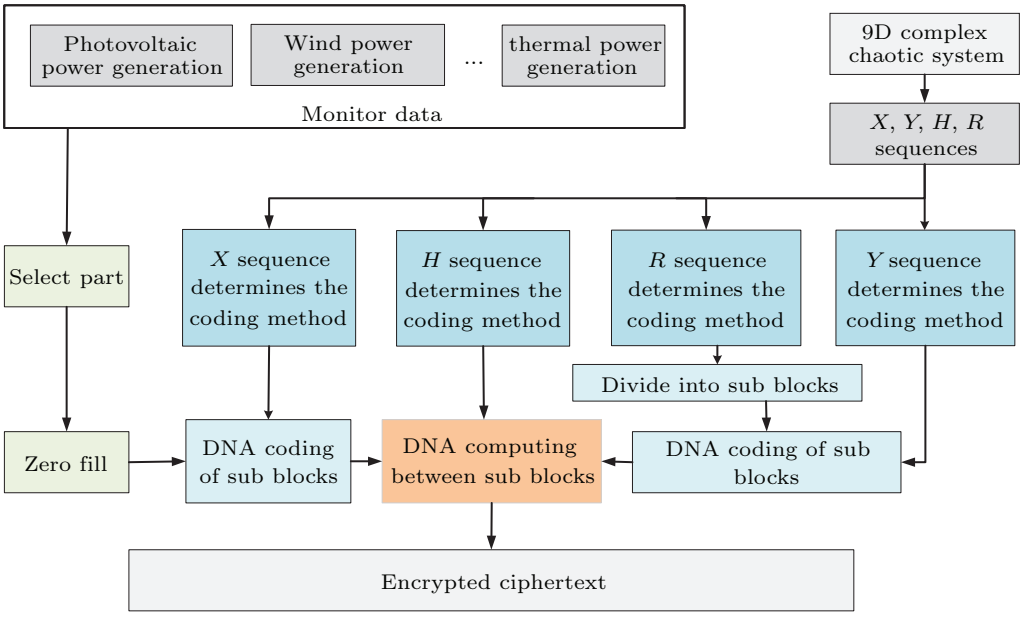


Fig. 16. The flow chart of the data encryption algorithm.

The cyclic redundant check (CRC) code is calculated by the transmitting device and placed at the end of the transmitted information frame. The receiving device recalculates the CRC of the received information and compares whether the calculated CRC is consistent with the received CRC. If they are inconsistent, it is considered that the data is abnormal. Therefore, CRC is selected for encryption in this paper. The flow chart of the data encryption algorithm is shown in Fig. 16. This encryption step is similar to the above image encryption step.

Next, the randomness of the sequence is analyzed by the NIST test. It is a recognized standard in the encryption field that can be used to evaluate the performance of pseudo-random sequences. Most scholars convince that it is a very common and effective method to test pseudo-random sequences. For convenience's sake, 10000000 real numbers, generated by system (3), are converted to binary sequences. Adopt them directly as the experimental data of the NIST test suit. If every single item in the NIST test exceeds 0.01 (maximum is 1), it indicates that this test is passed. At the same time, the larger the value is, the stronger the random characteristic of the test sequence is.

As shown in Table 8, the chaotic sequence generated by system (3) has good random performance and can effectively cover up the information of encrypted data.

Table 8. NIST test.

Test category	Value	The test
Approximate entropy	0.534146	pass
Block frequency	0.350485	pass
Cumulative sums	0.534146	pass
FFT	0.350485	pass
Frequency	0.911413	pass
Linear complexity	0.213309	pass
Longest run	0.739918	pass
NonOverlapping template	0.911413	pass
Overlapping template	0.066882	pass
Random excursions	0.213309	pass
Random excurions variant	0.122325	pass
Rank	0.739918	pass
Runs	0.739918	pass
Serial	0.739918	pass
Uiversal	0.534146	pass

5. Conclusion

A new 9D complex chaotic system with quaternion is proposed in this paper. Firstly, it is derived from the complex Chen system and quaternion. The expansion of variables from real field to complex field is realized. Secondly, to analyze the performances of the new chaotic system, Lyapunov exponent, phase diagrams, bifurcation diagram, 0–1 test and complexity are introduced. Finally, with the DNA code, an encryption algorithm is proposed based on system (3). The transmitted images and data are encrypted in the verification experiments.

To analyze the image encryption, we have introduced the histogram, correlation coefficient, information entropy, sensitivity of key and reconstruction quality. The data encryption is analyzed by the NIST test. The experimental results show that the proposed algorithm improves the real-time performance on the basis of confidentiality. It can be applied to the smart grid.

Acknowledgements

Project supported by the International Collaborative Research Project of Qilu University of Technology (Grant No. QLUTGJHZ2018020), the Project of Youth Innovation and Technology Support Plan for Colleges and Universities in Shandong Province, China (Grant No. 2021KJ025), the Major Scientific and Technological Innovation Projects of Shandong Province, China (Grant Nos. 2019JZZY010731 and 2020CXGC010901).

References

[1] Kim Y H, Son K J, Kang S H and Chang T G 2020 *IEEE Trans. Instrum. Meas.* **69** 9880
[2] Kitzig J, Schlaghecke S and Bumiller G 2019 *IEEE Trans. Instrum. Meas.* **68** 1014
[3] Abbasinezhad-Mood D, Ostad-Sharif A, Mazinani S M and Nikooghadam M 2020 *IEEE Trans. Ind. Inform.* **16** 7287
[4] Qian J, Cao Z, Dong X, Shen J, Liu Z and Ye Y 2021 *IEEE Trans. Smart. Grid* **12** 2625
[5] Xia X, Xiao Y and Liang W 2020 *IEEE Trans. Inf. Forensic Secur.* **15** 361
[6] Liu S T and Zhang L 2022 *Surface Chaos and Its Applications* (Singapore: Springer) p. 393
[7] Liu S T, Wang Y P, Bi Z M and Wang Y 2021 *Mathematical Principle and Fractal Analysis of Mesoscale Eddy* (Singapore: Springer) p. 258
[8] Cui S and Zhang J 2019 *IEEE Photon. J.* **11** 7905208
[9] He W, Luo T, and Tang Y 2020 *IEEE Trans. Neural Netw. Learn. Syst.* **31** 3334
[10] Zhu B, Wang F and Yu J 2021 *IEEE Photon. Technol. Lett.* **33** 383
[11] Hu Z and Chan C 2018 *IEEE Photon. Technol. Lett.* **30** 1455
[12] Wang J, Li T, Luo X, Shi Y Q and Jha S K 2019 *IEEE Trans. Circuits Syst. Video Technol.* **29** 2775
[13] Wang Y, Kou K I, Zou C and Tang Y Y 2021 *IEEE Trans. Image Process.* **30** 3637
[14] Liu Y, Cheng C, Gu T, Jiang T and Li X 2016 *IEEE Sens. J.* **16** 836
[15] Saxena N and Grijalva S 2017 *IEEE. Trans. Industr. Informatics* **13** 1482
[16] Gope P and Sikdar B 2019 *IEEE. Trans. Inf. Foren. Sec.* **14** 1554
[17] Song J, Liu Y, Shao J and Tang C 2020 *IEEE. Syst. J.* **14** 900
[18] Qian J, Cao Z, Dong X, Shen J, Liu Z and Ye Y 2021 *IEEE Trans. Smart. Grid.* **12** 2625
[19] Leng S, Xun J L, Zhang F F, and Li Z F 2019 *Proceedings of the 2019 International Conference on Big Data, Electronics and Communication Engineering*, November 24, 2019, Beijing, China, 2019, p. 51
[20] Sutter D, Fawzi O and Renner R 2021 *IEEE Trans. Inf. Theory* **67** 10
[21] Karimov T I, Druzhina O S, Karimov A I, Kolev G Y and Butusov D N 2021 *Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering*, January 26–29, 2021, Chengdu, China, p. 124
[22] Jie Z, Nan Z and Hua G 2020 *Opt. Laser Technol.* **131** 106437
[23] Kadir A, Hamdulla A and Guo W Q 2014 *Optik* **125** 1671