Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.16, No.1, 2026

A Color Image Encryption Algorithm Based on Fractional-order Coupled Neuron System and Fibonacci Q-matrix

Fanqi Meng[1] Min Liu[2*]
1.Yancheng Teachers University, Yancheng 224002, China
2.The First people's Hospital of Yancheng, Yancheng 224000, China
E-mail of the corresponding author: lmin89@163.com

The research is financed by Yancheng Fundamental Research Program. No. YCBK2025016

Abstract

With the rapid growth of Internet-based digital communication, digital image information is increasingly exposed to risks such as interception, tampering, and data loss during transmission. Consequently, the design of secure image encryption algorithms has become highly important for protecting digital images. In this paper, a novel chaotic color image encryption scheme based on a fractional-order coupled neurons system (FCNS) and the Fibonacci Q-matrix is presented. The proposed algorithm is thoroughly analyzed through statistical security tests to verify its effectiveness. Experimental results show that the scheme can resist various well-known attacks and satisfy the security requirements for digital image transmission.

Keywords: Coupled neurons system, Fibonacci Q-matrix, Image encryption

DOI: 10.7176/JIEA/16-1-01

Publication date: April 30th 2026

1. Introduction

With the rapid development of digital technology, the secure transmission of digital images has become increasingly important, since unencrypted image data is vulnerable to unauthorized access, eavesdropping, tampering, and privacy leakage during communication. Therefore, image encryption plays a crucial role in protecting the confidentiality and integrity of image information, especially in military, commercial, medical, and other security-sensitive fields. Owing to their uncertainty and nonlinear dynamic behaviors, neuron systems with chaotic discharge properties have shown significant advantages in image encryption, as the randomness and complexity generated by chaotic dynamics can effectively enhance encryption performance and improve resistance to cryptographic attacks. In recent years, a variety of neuron-based image encryption methods have been reported. For example, Lai et al. [1] designed an image encryption algorithm based on a neuron model coupled with a memristor, Yildirim [2] proposed an RGB image encryption scheme using DNA encoding and a neuron model, Patel et al. [3] combined neural networks with DNA encoding for image encryption, Tlelo-Cuautle et al. [4] applied the Hindmarsh–Rose neuron model to image encryption, Sun et al. [5] proposed medical image encryption algorithms based on ring neural networks and fully connected neural networks, and Hu et al. [6] utilized the chaotic properties of the Hopfield neural network for image encryption.

Most existing chaotic image encryption algorithms are constructed based on integer-order differential equations. As a generalized form of integer-order differential equations, fractional-order differential equations can better describe systems with memory and hereditary properties, and fractional-order chaotic systems usually exhibit more complex dynamical behaviors than their integer-order counterparts [7]. Owing to these advantages, fractional-order systems have attracted increasing attention in the field of image encryption. For instance, Duan et al. [8] proposed a color image encryption scheme based on fractional discrete Tchebyshev moments, Xu et al. [9] developed an image encryption algorithm using a fractional-order Hopfield neural network, and Yu et al. [10] extended the Hopfield neural network to a fractional-order six-dimensional memristive Hopfield neural network for image encryption. Motivated by these studies, this paper proposes a novel fractional-order coupled neurons system. After analyzing its dynamical characteristics, an image encryption algorithm is further designed by exploiting the chaotic behaviors of the proposed system.

The Fibonacci sequence refers to a sequence in which each term after the first two is obtained by summing the

two preceding terms. In image encryption, the Fibonacci Q-matrix can be effectively employed in the diffusion stage to modify pixel gray values and enhance encryption performance. Owing to its advantages, the Fibonacci Q-matrix has been widely introduced into image security schemes. For example, Biban et al. [11] combined an 8D hyperchaotic system with the Fibonacci Q-matrix for image encryption, Sajeer et al. [12] developed a medical image watermarking method based on a hyperchaotic system and the Fibonacci Q-matrix, and Liang et al. [13] proposed an image encryption algorithm by integrating a genetic algorithm with the Fibonacci Q-matrix. Inspired by these studies, this paper proposes a novel color image encryption algorithm based on the FCNS and the Fibonacci Q-matrix.

The rest of this paper is organized as follows. Section 2 introduces the mathematical foundations. Section 3 describes the proposed encryption algorithm based on the FCNS and the Fibonacci Q-matrix. Section 4 presents the simulation results and analyzes the security performance. Finally, Section 5 concludes the paper.

2. Mathematical Foundations

2.1 Fractional-order Coupled Neurons System

With the advancement of neuroscience, fractional-order neuron models have been recognized as more general and accurate than integer-order neuron models. Among the existing definitions of fractional derivatives, the Caputo definition is often preferred because it has a clearer physical meaning. The Caputo-type fractional-order differential equation is given by [14]

$$D_t^q f(t) = \frac{1}{\Gamma(w-q)} \int_0^t \frac{f^w(\tau)}{(t-\tau)^{q-w+1}} d\tau, \tag{1}$$

where $\Gamma(\cdot)$ is the gamma function and $t \geq 0,\ w \in Z^+,\ w-1 < q < w$.

According to the definition of Caputo type fractional-order differential equation, the fractional-order extended neuronal model is defined in Eq. (2).

$$\begin{cases} D_t^q x_1 = ax_1^3 \quad bx_1^2 \mid x_2 \quad x_3 \mid I_{ext}, \\ D_t^q x_2 = c - dx_1^2 - x_2 - ex_4, \\ D_t^q x_3 = r(S(x_1 + 1.56) - x_3), \\ D_t^q x_4 = h(-x_4 + f(x_2 + g)), \end{cases} \tag{2}$$

where $x_1,\ x_2,\ x_3,\ x_4$ represent the membrane potential, slow current associated with recovery variable, adaption current, and slow transformation between cytoplasm respectively. The parameters $a,\ b,\ c,\ d,\ r,\ S,\ e,\ h,\ f,\ g$ are real constants, q is the order of the fractional-order differential equation and I_{ext} is the external current input.

Furthermore, we constructed a fractional order coupled neural system consisting of two neurons. The model is as follows:

$$\begin{cases} D_t^q x_1 = ax_1^3 - bx_1^2 + x_2 - x_3 + I_{ext} + p(x_1 - y_1), \\ D_t^q x_2 = c - dx_1^2 - x_2 - ex_4, \\ D_t^q x_3 = r(S(x_1 + 1.56) - x_3), \\ D_t^q x_4 = h(-x_4 + f(x_2 + g)), \\ D_t^q y_1 = ay_1^3 - by_1^2 + y_2 - y_3 + I_{ext} + p(y_1 - x_1), \\ D_t^q y_2 = c - dy_1^2 - y_2 - ey_4, \\ D_t^q y_3 = r(S(y_1 + 1.56) - y_3), \\ D_t^q y_4 = h(\ y_4 \mid f(y_2 \mid g)), \end{cases} \tag{3}$$

where p represent the coupling coefficient. When the initial values of FCNS $x_1 = 0.1,\ x_2 = 0.2,\ x_3 = 0.1,\ x_4 = 0.1,\ y_1 = -0.12,\ y_2 = -0.2,\ y_3 = 0.2,\ y_4 = -1.1$ and the parameters are set as $a = 1,\ b = 3,\ k = 0.1,\ c = 1,\ c = 0.1,\ r = 0.02,\ S = 4,\ h = 0.02,\ f = 0.88,\ g = 0.9,\ d = 5,\ \beta = 0.2,\ p = 0.1,\ I_{ext} = 3.1$ and $q = 0.98$, using the predictor–corrector algorithm to solve the above equation. The time sequence diagram, phase diagram and bifurcation diagram of FCNS are shown in Fig.1. These results show that the FCNS possesses complex chaotic dynamics.

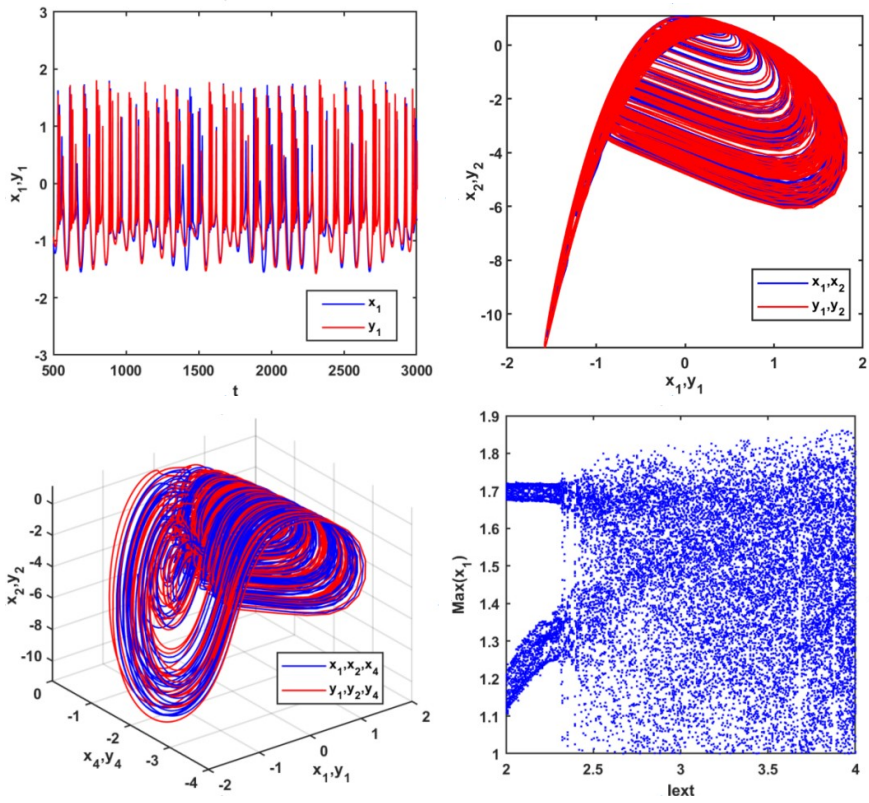


Figure 1. The time sequence diagram, phase diagram and bifurcation diagram of FCNS.

2.2 Fibonacci Q-matrix

The elements of the Fibonacci [15] sequence F_n are:

$$\begin{cases} F_0 = 0, & n = 0 \\ F_1 = F_2 = 1, & n = 1 \\ F_n = F_{n-1} + F_{n-2}. & n > 1 \end{cases} \tag{4}$$

The FQ-matrix is defined as:

$$Q = \begin{bmatrix} F_2 & F_1 \\ F_1 & F_0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}. \tag{5}$$

The nth FQ-matrix is given by:

$$Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}, \tag{6}$$

where F_n is the Fibonacci number, and the determinants of the FQ-matrix is:

$$Det(Q^n) = F_{n+1}F_{n-1} - F_n^2 = (-1)^n. \tag{7}$$

The inverse FQ-matrix is defined as:

$$Q^{-n} = \begin{bmatrix} F_{n-1} & -F_n \\ -F_n & F_{n+1} \end{bmatrix}. \tag{8}$$

3. Image Encryption Scheme

3.1 Encryption Algorithm

The detailed steps of the image encryption methodology based on FCNS and Fibonacci Q-matrix are as follows:

Step 1: Given a color image I with size $M \times N$ and divide it into IR, IG, IB components.

Step 2: Set the initial values $a, b, k, c, d, e, r, S, h, f, g, q, \beta, x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4$ of FCNS as the secret key. The FCNS generates the chaotic sequences $Sx_1, Sx_2, Sx_3, Sx_4, Sy_1, Sy_2, Sy_3, Sy_4$.

Step 3: Obtain a vector H' using Sx_1, Sx_2, Sx_3, Sx_4, Sy_1, Sy_2, Sy_3, Sy_4. The size of the sequence H' is $M \times N$.

Step 4: The chaotic sequence H is calculated by Eq. (9) to obtain H',

$$CH' = (round(|H| \times 10^7)) mod\ 256. \tag{9}$$

Step 5: Convert the sequence CH' into the matrix CH of size $M \times N$. Perform XOR operation IR, IG, IB with CH to obtain CR, CG, CB, respectively. Convert CR, CG, CB to vector CR', CG', CB'.

Step 6: Obtain the vector LH' by shorting the sequence H' in descending order and calculate the permuted vector PR', PG', PB' according to Eq. (10).

$$\begin{cases} [\sim, LH'] = sort(H', descend'), \\ PR' - CR'(LH'), \\ PG' - CG'(LH'), \\ PB' = CB'(LH'). \end{cases} \tag{10}$$

Step 7: Convert the sequence PR', PG', PB' into the matrix PR, PG, PB of size $M \times N$, and separate it into subblocks of size 2×2.

Step 8: Get the matrix KR, KG, KB by multiplying each subblock with the FQ matrix based on Eq. (11), respectively.

$$\begin{bmatrix} K(X)_{i,j} & K(X)_{i,j+1} \\ K(X)_{i+1,j} & K(X)_{i+1,j+1} \end{bmatrix} = \begin{bmatrix} P(X) & P(X)_{i,j+1} \\ P(X)_{i+1,j} & P(X)_{i+1,j+1} \end{bmatrix} \begin{bmatrix} 89 & 55 \\ 55 & 34 \end{bmatrix} mod\ 256, \tag{11}$$

where $i - 1:3:\ldots:M$, $j - 1:3:\ldots:N$ and X represents R, G, and B components.

Step 9: Merge the R, G, and B components to obtain an encrypted image S.

3.2 Decryption Algorithm

The decryption steps of the image decryption algorithm are the inverse steps of the encryption algorithm. The chaotic sequences are obtained by FCNS using the same key as the encryption algorithm. The main steps of the decryption algorithm are as follows:

Step 1: Separate R, G, B into subblocks of size 2×2 and use the diffusion equation with FQ matrix on image blocks to obtain PR, PG, PB according to Eq. (12).

$$\begin{bmatrix} P(X)_{i,j} & P(X)_{i,j+1} \\ P(X)_{i+1,j} & P(X)_{i+1,j+1} \end{bmatrix} = \begin{bmatrix} K(X)_{i,j} & K(X)_{i,j+1} \\ K(X)_{i+1,j} & K(X)_{i+1,j+1} \end{bmatrix} \begin{bmatrix} 34 & -55 \\ -55 & 89 \end{bmatrix} mod\ 256, \tag{12}$$

where $i = 1:3:\ldots:M$, $j = 1:3:\ldots:N$ and X represents R, G, and B components.

Step 2: Convert image PR, PG, PB into vector PR', PG', PB'. The vector H' generated in the encryption step for returning each pixel to its original position by using Eq. (13).

$$IQ(X)'(H'_i) = P(x)'_i, \quad i = 1:MN, \tag{13}$$

where X represents R, G, and B components.

Step 3: Convert the sequence IQR', IQG', IQB' into the matrix IQR, IQG, IQB, and then performs XOR operation with CH generated in the encryption step to get IR, IG, IB.

Step 4: Merge IR, IG, IB to obtain the decrypted image.

4. Simulation result and Security analyses

4.1 Encryption and decryption results

The color images of Tree (Fig.2-(a), size 256×256), House (Fig.2-(b), size 512×512) and Airplane (Fig.2-(c), size 512×512) were used to test the performance of encryption algorithm. The secret key $x_1 = 0.1$, $x_2 = 0.2$, $x_3 = 0.1$, $x_4 = 0.1$, $x_5 = 0.12$, $x_6 = 0.2$, $y_1 = 0.2$, $y_2 = 0.2$, $y_3 = 1.1$, $a = -1$, $b = 3$, $c = -1$, $e = -0.1$, $r = 0.02$, $S = 4$, $h = 0.02$, $f = 0.88$, $g = 0.8$, $d = 5$, $\beta = 0.2$, $m = -0.1$, $L_{ext} = 3.1$ and $q = 0.98$. As shown in Figure 2 (d-f), all encrypted images are noisy, unrecognizable and have no image features. Figure 2(g–i) presents the decrypted images corresponding to the encrypted images. The experimental results verify that the proposed algorithm is effective for the encryption and decryption of color images.

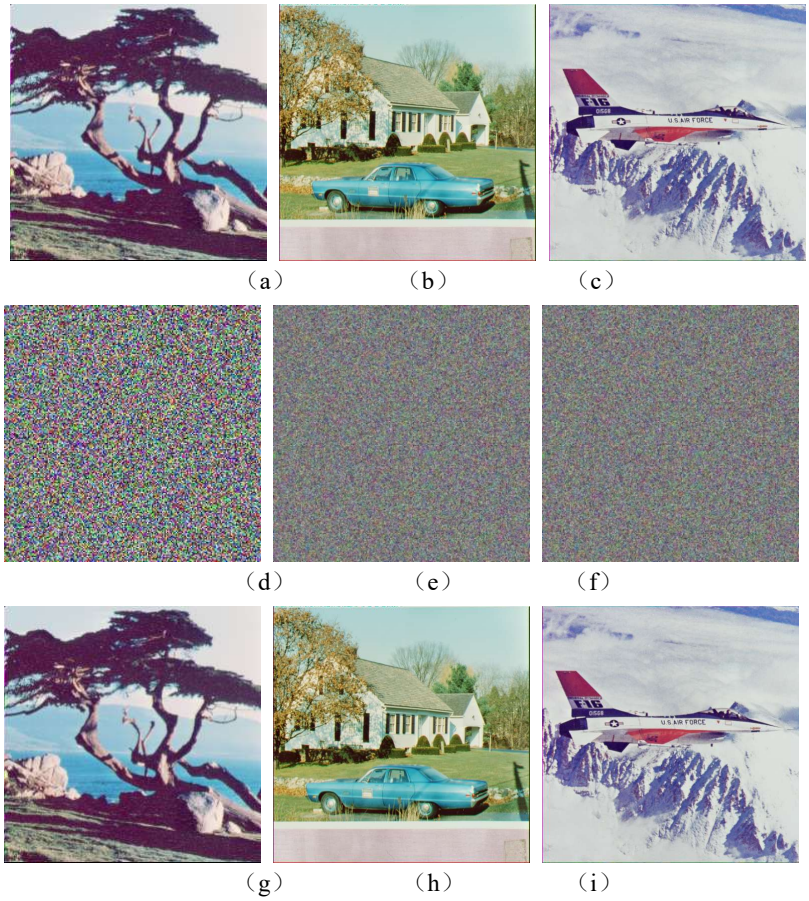


Figure 2. Original (a-c), encrypted (d-f) and decrypted (g-i) of test images.

4.2 Key space analysis

The larger the key space, the higher the security of the algorithm. When the key space is greater than 2^{100}, the encryption algorithm can withstand brute force attacks [19]. In this paper, the secret key consists of fourteen parameters $a, b, r, S, h, f, l_{ext}, \beta, q, g, k, c, d, e$ and eight initial values $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4$ of FCNS. If the accuracy of the system is 10^{-10}, the total key space is $10^{22\times10} \approx 2^{700} > 2^{100}$. Therefore, the proposed scheme possesses a much larger key space, which is sufficient to resist brute-force attacks and ensures higher security performance.

4.3 Key sensitivity analysis

High key sensitivity is an essential characteristic of a secure and reliable encryption scheme. In this study, slight perturbations were applied to x_1, y_3, a, S, and q in the secret key for the Tree image. The corresponding decrypted results in Figure 3 show that even a very small change in the secret key leads to unsuccessful decryption of the original image. These results confirm that the proposed algorithm has strong key sensitivity and therefore provides improved security.

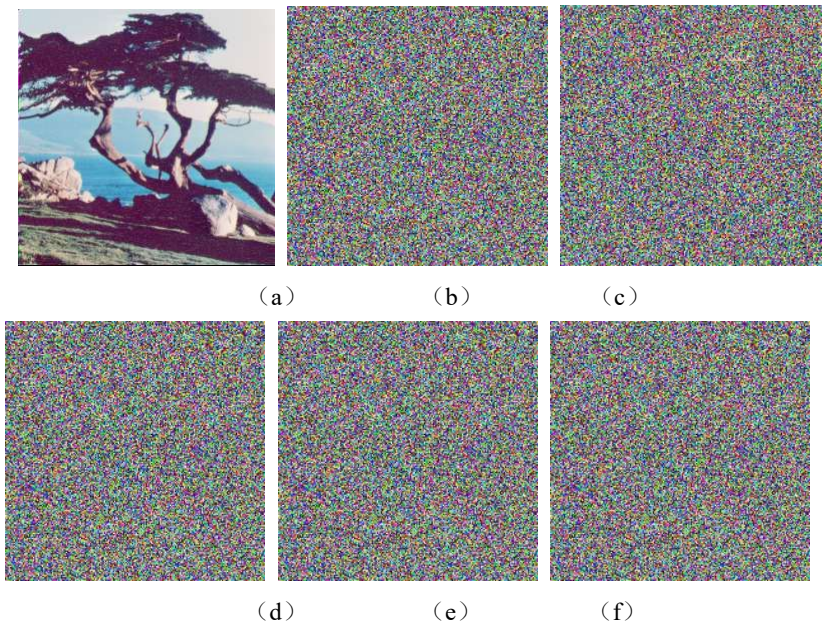


Figure 3. Key Sensitively test. (a) Original image, (b) $x_1 + 10^{-10}$, (c) $y_3 + 10^{-10}$, (d) $a + 10^{-10}$, (e) $S + 10^{-10}$, (f) $q + 10^{-10}$.

4.4 Information entropy analysis

Any random variable inherently contains a certain degree of uncertainty, and information entropy (IE) is an important measure used to characterize the uncertainty or complexity of an image. A larger information entropy value indicates greater uncertainty in the image information and less exploitable information content. For an encrypted image, the ideal information entropy is 8, which implies that an attacker can hardly extract useful information from the ciphertext image. The information entropy is defined in Eq. (14).

$$IE(x) - \sum_{i=0}^{N-1} H(x_i) \log_2 \frac{1}{P(x_i)}, \quad (14)$$

where N is the gray level of image, $H(x)$ means that the probability of occurrence of pixel x_i. Table 1 presents the IE results of the test images together with those reported in some references. All the obtained values are close to the ideal value, indicating that the proposed algorithm can effectively conceal image information and resist common attacks.

Table 1 Information entropy analysis.

Test Image	Original image			Encrypted image			
	Red	Green	Blue	Red	Green	Blue	Average
Tree	7.2104	7.4136	6.9207	7.997	7.9973	7.9971	7.9971
House	7.4156	7.2295	7.4354	7.9993	7.9994	7.9994	7.9994
Airplane	6.7178	6.799	6.2138	7.9994	7.9993	7.9993	7.9993

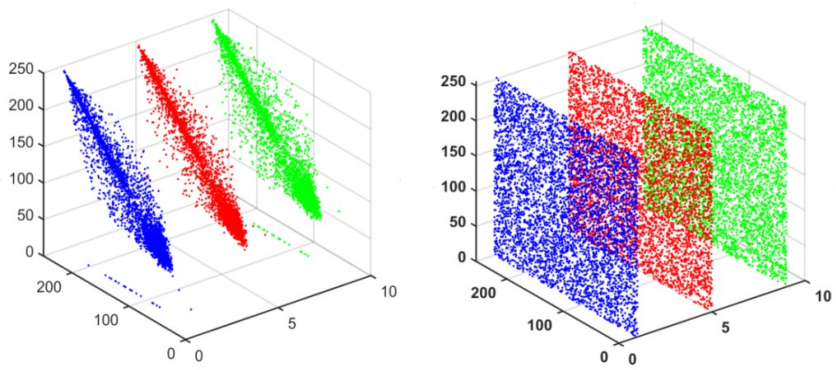
4.5 Correlation analysis

Correlation analysis is used to measure the relationship between adjacent pixels in digital images. In plaintext images, neighboring pixels usually have high correlation in the horizontal, vertical, and diagonal directions. If this correlation is not sufficiently reduced, the encrypted image may remain vulnerable to statistical attacks. Therefore, an effective encryption algorithm should make the correlation coefficients of adjacent pixels close to 0. To evaluate this property, N pairs of adjacent pixels are selected from the plaintext image, and their correlation coefficients in the three directions are calculated using the following formula.

$$\begin{cases} E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i, \\ D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2, \\ Cov(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i \quad E(x))(y_i \quad E(y)), \\ r_{xy}=\frac{Cov(x,y)}{\sqrt{D(x)}\times\sqrt{D(y)}}, \end{cases} \tag{15}$$

where x_i, y_i are the intensity values of the selected adjacent pixels, $Cov(x,y)$ is the covariance of x and y, $E(x)$ and $D(x)$ are the mathematical expectations and variances of x, r_{xy} is the correlation.

Figure 4 shows the distributions of 5000 randomly selected adjacent pixel pairs in the horizontal, vertical, and diagonal directions for the original and encrypted Tree image, while Table 2 lists the corresponding correlation coefficients for the test image. The results show that adjacent pixels in the original image have high correlation, whereas those in the encrypted image are distributed more uniformly and have correlation coefficients close to 0. This indicates that the proposed algorithm effectively reduces the strong correlation among adjacent pixels and improves resistance to statistical attacks.



（a） （b）

Figure 4. Distribution of adjacent pixels. (a) The horizontal, vertical, diagonal of plaintext image, (b) The horizontal, vertical, diagonal of ciphertext image.

Table 2 The results of correlation analysis.

Test Image		Plaintext image			Ciphertext image		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Tree	R	0.95813	0.93154	0.91154	0.007845	0.0251	-0.008455
	G	0.96661	0.94503	0.9303	-0.01349	-0.0367	-0.000644
	B	0.96048	0.93839	0.92374	0.0096625	0.00775	-0.009777

4.6 Histogram analysis

The histogram is an important statistical characteristic of an image. In general, the flatter the histogram of an encrypted image, the more difficult it is for an attacker to obtain useful statistical information from the plaintext image. Figure 5 shows the histogram of the plaintext and ciphertext images for Tree. The results indicate that the histogram of the encrypted image is much more uniform than those of the original image, which demonstrates that the proposed algorithm can effectively obscure the pixel distribution and resist statistical attacks.

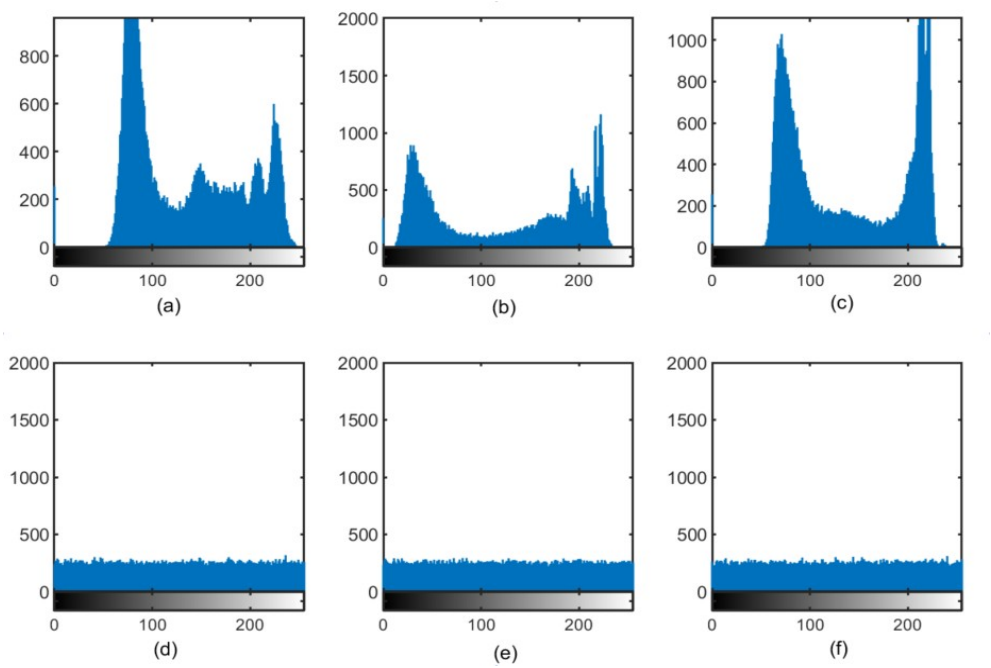


Figure 5. Histogram of image. (a-c) Histogram of original Tree R. G. B, (d-f) Histogram of encrypted Tree R. G. B.

4.7 Execution time analysis

Execution time analysis is an important criterion for evaluating the efficiency and practicality of an encryption algorithm, especially in real-time and resource-constrained applications. Faster execution generally indicates better performance. The time complexity of the proposed algorithm is $\Theta(M \times N)$, where M and N denote the height and width of the image, respectively. All experiments were carried out on a computer equipped with an Intel® Core™ Ultra 7 processor running at 3.8 GHz and 32 GB of RAM. For the test image Tree (size 256×256), the encryption time is 0.12s and the decryption time is 0.14s, indicating that the proposed algorithm has high computational efficiency.

5. Conclusion

In this paper, a fractional-order coupled neuron model is proposed and its chaotic behaviors are verified through bifurcation and phase diagram analysis. Based on the chaotic properties of this neuron system and the Fibonacci Q-matrix, a color image encryption algorithm is constructed. The security of the proposed algorithm is analyzed in terms of key space, key sensitivity, statistical characteristics, correlation, and information entropy. Experimental results show that the proposed algorithm achieves good security performance and can effectively ensure the secure transmission of digital image information.

References

[1] Lai, Q.; Lai, C.; Zhang, H.; Li, C. B. Hidden coexisting hyperchaos of new memristive neuron model and its application in image encryption. *Chaos Solitons Fractals.* **2022**, *158*, 112017.

[2] Yildirim, M. DNA encoding for RGB image encryption with memristor based neuron model and chaos phenomenon. *Microelectronics J*. **2020**, 104, 104878.

[3] Patel, S.; Thanikaiselvan, V.; Pelusi, D.; Nagaraj, B.; Arunkumar, R.; Amirtharajan, R. Colour image encryption based on customized neural network and DNA encoding. *Neural Comput. Appl.* **2021**, *33(21)*, 14533-14550.

[4] Tlelo-Cuautle, E.; Díaz-Muñoz, J. D.; González-Zapata, A. M.; Li, R.; León-Salas, W. D.; Fernández, F. V.; Guillén-Fernández, O.; Cruz-Vega, I. Chaotic Image Encryption Using Hopfield and Hindmarsh–Rose Neurons Implemented on FPGA. *Sensors.* **2020**, *20*, 1326.

[5] Sun, J.; Li, C.; Wang, Z.; Wang, Y. A Memristive Fully Connect Neural Network and Application of Medical Image Encryption Based on Central Diffusion Algorithm. *IEEE Trans. Industrial Inf.* **2023**, 1-11.

[6] Hu, Z.; Wang, C. Hopfield neural network with multi-scroll attractors and application in image encryption. *Multimed Tools Appl.* **2024**, *83*, 97–117.

[7] Liu, T.; Yan, H.; Banerjee, S.; Mou, J. A fractional-order chaotic system with hidden attractor and self-excited attractor and its DSP implementation. *Chaos Solitons Fractals.* **2021**, *145*, 10791.

[8] Duan, C. F., Zhou, J., Gong, L. H., Wu, J. Y., Zhou, N. R. New color image encryption scheme based on multi-parameter fractional discrete Tchebyshev moments and nonlinear fractal permutation method. *Optics and Lasers in Engineering*. **2022**, 150, 106881.

[9] Xu, S. C.; Wang, X. Y.; Ye, X. L. A new fractional-order chaos system of Hopfield neural network and its application in image encryption. *Chaos Solitons Fractals.* **2022**, 157, 111889.

[10] Yu, F.; Kong, X.; Chen, H.; Yu, Q.; Cai, S.; Huang, Y.; Du, S. A 6D Fractional-Order Memristive Hopfield Neural Network and its Application in Image Encryption. *Front. Phys.* **2022**, 10, 847385.

[11] Biban, G.; Chugh, R.; Panwar, A. Image encryption based on 8D hyperchaotic system using Fibonacci Q-Matrix. *Chaos Solitons Fractals* **2023**, 170, 113396.

[12] Sajeer, M.; Ashutosh, M. A robust and secured fusion based hybrid medical image watermarking approach using RDWT-DWT-MSVD with Hyperchaotic system-Fibonacci Q Matrix encryption. *Multimed. Tools Appl.* **2023**, 82, 37479–37501.

[13] Liang, Z.; Qin, Q.; Zhou, C. An image encryption algorithm based on Fibonacci Q-matrix and genetic algorithm. *Neural Comp. Appl*. **2022**, 34(21), 19313-19341.

[14] Podlubny, I. Fractional Differential Equations. Academic Press, New York (1999)

[15] Hosny, K. M.; Kamal, S. T.; Darwish, M. M.; Papakostas, G. A. New image encryption algorithm using hyperchaotic system and Fibonacci Q-matrix. *Electronics* **2021**, 10, 1066.

[19] Kocak, O.; Erkan, U.; Toktas, A.; Gao, S. PSO-based image encryption scheme using modular integrated logistic exponential map. *Expert Syst. Appl.* **2024**, 237, 121452.