# Remote sensing multi-image encryption based on a dual-memristor brain-inspired chaotic neural network

Bian huiyang(卞慧洋)[1], Zhou Silong(周思龙)[3], Xiong Li(熊丽)[123*],
An Xinlei(安新磊)[1], and Yang Qigui(杨启贵)[4]

[1]School of Mathematics and Physics, Lanzhou Jiaotong University, Lanzhou, 730000, China

[2]State Key Laboratory of Integrated Chips and Systems, Fudan University, Shanghai, 200433, China

[3]School of Physics and Electromechanical Engineering, Hexi University, Zhangye, 734000, China

[4]School of Mathematics, South China University of Technology, Guangzhou, 510641, China

**Abstract**

Remote sensing multi-image transmission faces strong spatial correlation, heterogeneous image dimensions, packet disorder, and integrity risks. To address these issues, a dual-memristor brain-inspired chaotic neural network is constructed by introducing two flux-controlled memristive synapses with nonlinear saturating memductance and weak flux coupling into a four-neuron Hopfield network, providing key-dependent and reproducible chaotic states. Based on this network, a multi-image encryption framework is developed by integrating reversible RGB-pixel interleaving, metadata-aware sub-packaging, session key derivation, trajectory-based packet masks, packet scheduling, authentication, and self-described reconstruction. The receiver regenerates identical chaotic states and spatial mappings from the master key and authenticated session information, enabling packet-wise decryption and lossless recovery without transmitting complete permutation sequences. Experiments on five 256 × 256 RGB remote sensing images achieve zero-MSE recovery, an average ciphertext entropy of 7.9972 bits, an average absolute adjacent-pixel correlation of 0.002763, and NPCR and UACI values of 99.6006% and 33.4432%, respectively. The authentication-tag overhead is 4.17%. These results demonstrate effective statistical and differential security, integrity verification, and reversible multi-image protection.

**Keywords:** Remote sensing image encryption; dual memristor; chaotic neural network; nonlinear saturating memductance

**PACS:** 05.45.-a, 05.45.Pq, 07.05.Pj

## 1. Introduction

With the rapid development of satellite observation, unmanned aerial platforms, and networked remote sensing systems, massive remote sensing images are continuously acquired and transmitted through open communication networks. These images often contain sensitive geographic and infrastructural information, making secure transmission an essential requirement. In practical applications, multiple remote sensing images with different scenes, resolutions, or dimensions are frequently transmitted together. Therefore, an effective multi-image encryption scheme should

† Corresponding author. E-mail: xl-427814@163.com

provide not only strong cryptographic security but also reliable packet organization, integrity verification, and accurate reconstruction.

Chaos-based encryption has been extensively studied because of the sensitivity, randomness, and reproducibility of chaotic systems. However, conventional low-dimensional chaotic systems often exhibit limited complexity and insufficient interactions among internal states, restricting their adaptability to session-dependent multi-image encryption. An effective solution is to introduce memory-dependent nonlinear elements into neural networks to generate richer chaotic dynamics. The motivation for incorporating memristors into neural networks originates from their ability to emulate biological synaptic plasticity. Chua first proposed the memristor, and Strukov et al. experimentally demonstrated its physical realization [1-2]. Unlike conventional resistive elements, the conductance of a memristor depends on its historical internal state, enabling it to replace a fixed synaptic weight with a dynamically regulated coupling coefficient. This property provides a natural foundation for constructing brain-inspired chaotic neural networks.

Motivated by this mechanism, researchers have introduced memristive synapses into neural systems to enrich nonlinear dynamics. Lin et al. developed a dual-memristor brain-inspired neural network for information protection, while related studies investigated neuronal dynamics under electromagnetic effects [3-4]. Memristive Hopfield networks have demonstrated multistability, coexisting attractors, and offset-controlled behaviors [5-6]. Subsequent studies further explored polymorphous chaos, multi-scroll attractors, memristive chaotic circuits, spiking neural networks, and energy-related neural dynamics [7-12]. More recently, memristive associative memory circuits, dual-memristor chaotic circuits, memristor-based transformer networks, and multi-scroll Hopfield neural networks have further enriched the dynamical behaviors and engineering applications of memristive neural systems [13-16]. Although these studies significantly advanced the understanding of memristive neural dynamics, they mainly focused on nonlinear behaviors themselves. The coordinated evolution of multiple memristive states and its application to reproducible cryptographic state generation remain insufficiently explored.

Meanwhile, chaos-based image encryption has evolved from conventional chaotic sequence generation toward hybrid architectures. Representative studies by Xiong et al. [17], Li et al. [18], and Jian et al. [19] introduced memristive chaotic systems and neural dynamics into image encryption to enhance nonlinear complexity and key sensitivity. Subsequent approaches employed asymmetric chaotic maps, coupled systems, and robust diffusion mechanisms to improve confusion and diffusion performance [20-22]. Transform-domain encryption, compressive sensing, and asymmetric strategies further enhanced computational efficiency and security [23-25], while dynamic diffusion, key optimization, scrambling algorithms, and hyperchaotic systems strengthened statistical security and resistance to differential attacks [26-30]. For remote sensing applications, Tian et al. [31] developed a DNA-convolution-based method, while related studies incorporated hyperchaotic compression and wavelet-transform techniques [32-33]. Multiple-image encryption

was subsequently explored using S-box and DNA operations, cross-plane processing, and hyperchaotic models [34-36]. Nevertheless, most existing schemes process complete images or fixed-size image arrays as a whole, offering limited support for heterogeneous packet-oriented multi-image transmission. Moreover, packet metadata, transmission order, and integrity are rarely protected together with encrypted image data, thereby increasing synchronization overhead and reducing reconstruction reliability.

To overcome these limitations, this paper proposes a dual-memristor brain-inspired chaotic neural network (DMBCNN) by introducing two flux-controlled memristive synapses with nonlinear saturating memductance into a four-neuron Hopfield network. Weak coupling between the two internal flux states is established to enhance cooperative state evolution and generate reproducible, key-dependent chaotic trajectories. Based on the proposed DMBCNN, whose high-dimensional nonlinear dynamics and reproducible chaotic trajectories provide a reliable entropy source for synchronized encryption, a packet-oriented remote sensing multi-image encryption framework is developed by integrating reversible global RGB-pixel interleaving, metadata-aware sub-packaging, plaintext-digest-based session initialization, trajectory-derived packet masks, packet scheduling, authentication, and self-described reconstruction. Consequently, the receiver can regenerate identical chaotic states from the master key and authenticated session information, enabling packet-wise decryption and exact reconstruction without transmitting complete permutation sequences.

The main innovations and contributions are summarized as follows. (i) A dual-memristor Hopfield network integrating nonlinear saturating memductance and weak flux coupling is constructed; its bifurcation, multistability, and chaos are systematically investigated. (ii) A session-dependent initialization mechanism is proposed to derive packet-level keys from the master key, plaintext digest, nonce, and packaging metadata. (iii) A packet-oriented remote sensing multi-image encryption framework is developed to support authenticated transmission and exact reconstruction of heterogeneous remote sensing images.

The remainder of this paper is organized as follows. Section 2 introduces the proposed Dual-Memristor Brain-Inspired Chaotic Neural Network. Section 3 analyzes its dynamical characteristics. Section 4 presents the encryption and decryption framework. Section 5 reports the experimental and security analyses. Finally, Section 6 concludes the paper.

## 2 Modeling of a Dual-Memristor Brain-Inspired Chaotic Neural Network with Nonlinear Saturating Memductive Synapses

Rather than directly adopting an existing memristive Hopfield network, this study introduces two nonlinear saturating memristive synapses into a four-neuron architecture. Weak magnetic-flux coupling between the internal states is introduced to coordinate memristive evolution. Accordingly, a dual-memristor brain-inspired chaotic network with coupled state-dependent synaptic weights is established. The synaptic coupling strengths are dynamically regulated by the two interacting

memristive states. This design enhances nonlinearity, parameter tunability, and initial-condition sensitivity, while providing reproducible chaotic states for the subsequent encryption framework.

### 2.1 Nonlinear Saturating Memristor Model

A memristor can characterize nonlinear memory effects associated with its internal state, and is therefore suitable for modeling plastic neural synapses. In this study, a flux-controlled memristor is employed to describe synaptic coupling, and its basic port relationship is given by

$$i = W(\phi)v \tag{1}$$

where $v$ and $i$ denote the voltage across the memristor and the current flowing through it, respectively. $\phi$ represents the internal state variable of the memristor, and $W(\phi)$ is the memductance function.

To enhance the nonlinear modulation capability of the memristive synapse, a memductance function with nonlinear saturation characteristics is defined as follows:

$$W(\phi) = a + b\phi + \eta \tanh(\lambda\phi) \tag{2}$$

where a and b are the linear memductance parameters, $\eta$ is the modulation intensity of the nonlinear saturating memductance, and $\lambda$ denotes the saturation rate. In this expression, $a+b\phi$ is the linear memductance term, while $\eta\tanh(\lambda\phi)$ is the nonlinear saturating modulation term.

Since the hyperbolic tangent function is bounded, the nonlinear modulation term gradually approaches saturation when $\phi$ becomes large. Therefore, the proposed memductance function can enhance the nonlinear modulation capability of the memristive synapse while preventing excessive growth of the memductance value, which is beneficial for improving the numerical stability of the system.

When $\eta$=0, Eq. (2) is reduced to the linear memductance function given by

$$W(\phi) = a + b\phi \tag{3}$$

Therefore, the nonlinear saturating memductance model adopted in this study can be regarded as an extended form of the linear memductance function.

The internal state function of the memristor is described by a multi-segment nonlinear function $h(\phi)$, whose general form can be expressed as follows:

$$h(\phi) = \phi - \sum_{i=1}^{N} \tanh(\rho(\phi + 2i - 1)) + \tanh(\rho(\phi + 2i + 11)) \tag{4}$$

where $\rho$ is a large positive parameter used to control the steepness of the segmented function, and N is the structural control parameter of the memristor internal state function. By changing N, the zero-point distribution of $h(\phi)$ can be adjusted, thereby providing conditions for the generation of multi-structure attractors.

In this study, the single-attractor case is mainly considered. Therefore, $N_1$=$N_2$=0 is adopted in the basic simulations, and the memristor internal state function is reduced to

$$h(\phi) = \phi \tag{5}$$

To verify the basic characteristics of the constructed nonlinear saturating memductive synapse, its port response under different input frequencies and its power-off behavior are analyzed. The results are shown in Fig 1.

As shown in Fig 1(a), under sinusoidal voltage excitation, the voltage-current curve of the memristor exhibits typical pinched hysteresis loops. The hysteresis loop area also changes with the input frequency, indicating that the proposed model has typical memristive characteristics.

As shown in Fig 1(b), several negative-slope zero-crossing points, denoted as $Q_4$~$Q_5$, are observed in the POP curve. This indicates that the memristor can maintain multiple stable states without external input, reflecting its nonvolatile memory property.

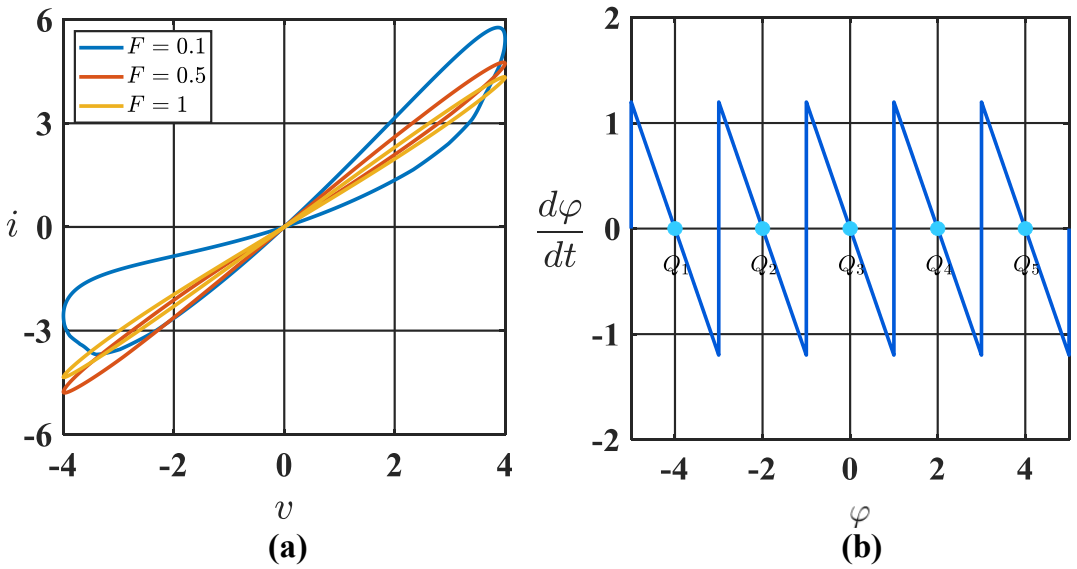



Fig 1 Nonlinear saturating memristive synapse characteristics. (a) Pinched hysteresis loops under different frequencies; (b) POP curve with multiple stable equilibrium points.

## 2.2 Construction of the Dual-Memristor Brain-Inspired Chaotic Neural Network

The Hopfield neural network is a typical recurrent neural network, whose dynamic behavior is closely related to neuronal states, synaptic weights, and activation functions. In this study, a four-neuron Hopfield network is adopted as the basic framework, and the hyperbolic tangent function is selected as the neuronal activation function, namely:

$$f(x) = \tanh(x) \tag{6}$$

The hyperbolic tangent function is continuous, bounded, and nonlinearly saturated, and can be used to describe the nonlinear response of neuronal outputs. In conventional Hopfield neural networks, synaptic weights are usually fixed constants. As a result, the memory regulation capability and nonlinear complexity of the system are limited. To enhance the dynamic regulation capability of the network, two

nonlinear saturating memristive synapses are introduced, so that part of the synaptic weights can vary with the internal states of the memristors.

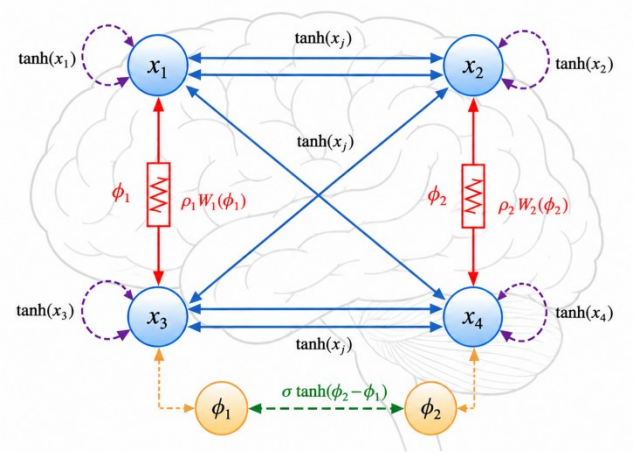



Fig 2 Topological structure of the proposed dual-memristor brain-inspired chaotic neural network.

Let $\phi_1$ be the internal state of the first memristive synapse, which is used to regulate the coupling between neurons $x_1$ and $x_3$. Let $\phi_2$ be the internal state of the second memristive synapse, which is used to regulate the coupling between neurons $x_2$ and $x_4$. The nonlinear saturating memductance functions of the two memristive synapses are defined as follows:

$$W_1(\varphi_1) = a + b\varphi_1 + \eta_1 \tanh(\lambda\varphi_1) \tag{7}$$

$$W_2(\varphi_2) = a + b\varphi_2 + \eta_2 \tanh(\lambda\varphi_2) \tag{8}$$

$$C_{12} = \sigma \tanh(\varphi_1 - \varphi_2) \tag{9}$$

$$C_{21} = \sigma \tanh(\varphi_2 - \varphi_1) \tag{10}$$

where $\sigma$ denotes the weak coupling strength between the internal states of the two memristors. Since the coupling term is defined by the hyperbolic tangent function, it is bounded and nonlinearly saturated. When the difference between $\phi_1$ and $\phi_2$ is small, the coupling term approximately provides linear regulation. When the difference becomes large, the coupling term gradually reaches saturation, thereby preventing system divergence caused by excessive coupling.

Accordingly, a dual-memristor brain-inspired chaotic neural network with nonlinear saturating memductive synapses and weak magnetic flux coupling is established as follows:

$$\begin{cases} \dot{x} & 3\tanh(x_2) + \rho_1 W_1(\phi_1)\tanh(x_3) - 13\tanh(x_4) \\ \dot{x} & \tanh(x_1) + 1.5\tanh(x_2) + 7\tanh(x_3) - \rho_2 W_2(\phi_2)\tanh(x_4) \\ \dot{x} & 4\tanh(x_2) + 1.8\tanh(x_3) + 4\tanh(x_4) \\ \dot{x} & 0.7\tanh(x_1) + 2\tanh(x_4) \\ \dot{\phi} = c & x_3) - d_1 h_1(\phi_1) + \sigma\tanh(\phi_2 - \phi_1) \\ \dot{\phi} = c & (x_4) - d_2 h_2(\phi_1) + \sigma\tanh(\phi_1 - \phi_2) \end{cases} \tag{11}$$

where $x_1$,$x_2$,$x_3$,$x_4$ denote the state variables of the four neurons, and $\phi_1$,$\phi_2$ represent the internal state variables of the two memristive synapses. $\rho_1$ and $\rho_2$ are the coupling strengths of the two memristive synapses, respectively. $c_1$, $c_2$, $d_1$, $d_2$ are the parameters of the memristor state equations, while $h_1\varphi_1$ and $h_2\varphi_2$ are the internal state functions of the memristors.

In Eq. (11), $\rho_1 W_1(\phi_1)\tanh(x_3)$ and $\rho_2 W_2(\phi_2)\tanh(x_4)$ represent the nonlinear modulation effects of the two memristive synapses on the neuronal coupling channels, respectively. Since $W_1(\phi_1)$ and $W_2(\phi_2)$ vary dynamically with the internal states of the memristors, the synaptic weights of the system are no longer fixed constants, but exhibit memory, nonlinearity, and tunability.

It can be seen from the above model that the constructed dual-memristor brain-inspired chaotic neural network has the following main features. First, the nonlinear saturating memductance functions enhance the nonlinear modulation capability of synaptic weights. Second, the weak magnetic flux coupling terms describe the cooperative evolution between the two memristor internal states. Finally, the multi-segment internal state functions can regulate the equilibrium structure of the system through structural parameters, providing conditions for the formation of multi-structure attractors. Therefore, the model has strong parameter tunability and initial-condition sensitivity, and is suitable for generating complex chaotic sequences. When $\eta_1 = \eta_1 = 0$, $\sigma = 0$ the nonlinear saturating memductance terms and the weak magnetic flux coupling terms vanish simultaneously. In this case, the system is reduced to a dual-memristor neural network with linear memductance. Therefore, the system described by Eq. (11) can be regarded as an extended model of the conventional dual-memristor neural network with linear memductance.

### 2.3 Parameter Settings and Model Description

For the subsequent numerical simulations and chaotic sequence generation, Eq. (11) is numerically integrated using the fourth-order Runge–Kutta method. Unless otherwise specified, the basic system parameters are set as listed in Table 1.

Table 1 System parameter settings.

| Parameter | value |
|---|---|
| a | 1 |
| b | 0.01 |
| $c_1$,$c_2$ | 2.2, 2.2 |
| $d_1$,$d_2$ | 1.2, 1.2 |
| $\rho$1,$\rho$2 | 3, 5 |
| η | 0.04 |
| λ | 1.2 |
| σ | 0.005 |
| p | $10^4$ |
| $N_1$,$N_2$ | 0, 0 |
| Δt | 0.01 |

In the basic simulations, the initial states of the system are usually set as $x_1(0)=x_2(0)=x_3(0)=x_4(0)=\varphi_1(0)=\varphi_2(0)=0.1$. When the regulation effect of memristor initial values is investigated, $\phi_1(0)$ and $\phi_2(0)$ can be adjusted according to the specific dynamic experiment. Since $N_1=N_2=0$ is adopted in the basic simulations, it follows that $h_1(\phi_1)=\phi_1$, $h_2(\phi_2)=\phi_2$. Based on the above model and parameter settings, the chaotic dynamic characteristics of the system will be analyzed in the next section through single-parameter bifurcation, Lyapunov exponent spectra, two-parameter bifurcation, three-dimensional phase trajectories, and basins of attraction. The suitability of the proposed dual-memristor brain-inspired chaotic neural network as the entropy source for synchronized image encryption will also be verified.

## 3 Chaos Dynamics Analysis

### 3.1 Single-Parameter Bifurcation and Lyapunov Exponent Analysis

To further verify the dynamic complexity of the dual-memristor brain-inspired chaotic neural network established in Chapter 2, numerical simulations are carried out in this chapter. The bifurcation characteristics, Lyapunov exponent spectra, multi-parameter dynamic distributions, multi-structure attractors, and basins of attraction are analyzed.

Unless otherwise specified, the system parameters are set according to the basic parameter settings given in Chapter 2, and numerical integration is performed using the fourth-order Runge–Kutta method. By varying the memristive synaptic coupling strengths, memristor initial states, and related control parameters, the evolution of the system from periodic and quasi-periodic states to chaotic states is investigated.

To analyze the influence of memristive synaptic coupling strength on the system dynamics, $\rho_1$ and $\rho_2$ are selected separately as control parameters. The local maxima bifurcation diagrams of the state variable $x_1$ are plotted, and the corresponding Lyapunov exponent spectra are calculated.

Numerical simulations are performed using the fourth-order Runge–Kutta method with an integration step of $\Delta t=0.01$. The initial condition is set as $x_1(0)=x_2(0)=x_3(0)=x_4(0)=\phi_1(0)=\phi_2(0)=0.1$ The system parameters are set as,$a=1$, $b=0.01$, $c_1=c_2=2.2$, $d_1=d_2=1.2$ with the nonlinear saturating memductance parameters $\eta=0.04$, $\lambda=1.2$. The weak magnetic flux coupling strength is taken as $\sigma=0.005$. The memristor function control parameters are set to $N_1=N_2=0$, and thus $h(\phi)=\phi$.

When $\rho_1$ is scanned, $\rho_2=5$ is fixed, whereas when $\rho_2$ is scanned, $\rho_1=3$ is fixed. Both parameters are varied over the interval [0,10]. To improve the resolution of the numerical results, the parameter scanning step is set to 0.01 for the bifurcation diagrams and 0.005 for the Lyapunov exponent spectra. For each parameter value, the system is integrated up to t=5000 using the fourth-order Runge–Kutta method with an integration step of $\Delta t=0.01$, and the transient data before t=500 are discarded. The local maxima of $x_1$ are then extracted to construct the bifurcation diagrams. The complete Lyapunov exponent spectrum is calculated using the variational equations and the QR-decomposition method, with orthogonalization performed every five integration steps.

As shown in Fig 3, with the variation of $\rho_1$ and $\rho_2$, the maxima distribution of the state variable $x_1$ exhibits clear branch splitting, dense scattered points, and periodic windows. This indicates that the system undergoes transitions among periodic, quasi-periodic, and chaotic states in different parameter intervals. When the points in the bifurcation diagram are densely distributed without an obvious regular pattern, complex chaotic oscillations are produced. When the points are concentrated on a finite number of branches, the system is closer to periodic motion.

The above results can be further verified by the Lyapunov exponent spectra. When the largest Lyapunov exponent satisfies $L_1>0$, the system is sensitive to initial conditions and operates in a chaotic state. When $L_1<0$, periodic or quasi-periodic behavior is observed. The variation trend of the Lyapunov exponent spectra is basically consistent with the complex regions in the bifurcation diagrams, indicating that the two analysis methods can confirm each other.

Since $\rho_1$ and $\rho_2$ act on different memristive synaptic coupling channels, namely

$$\rho_1 W_1(\phi_1)\tanh(x_3), \quad \rho_2 W_2(\phi_2)\tanh(x_4) \tag{12}$$

Their effects on the system dynamics are different to some extent. The simulation results show that the memristive coupling strength can effectively regulate the nonlinear oscillatory behavior of the system, leading to rich dynamic characteristics over a wide parameter range. Therefore, the constructed dual-memristor brain-inspired chaotic neural network exhibits good parameter tunability and complex chaotic behavior.

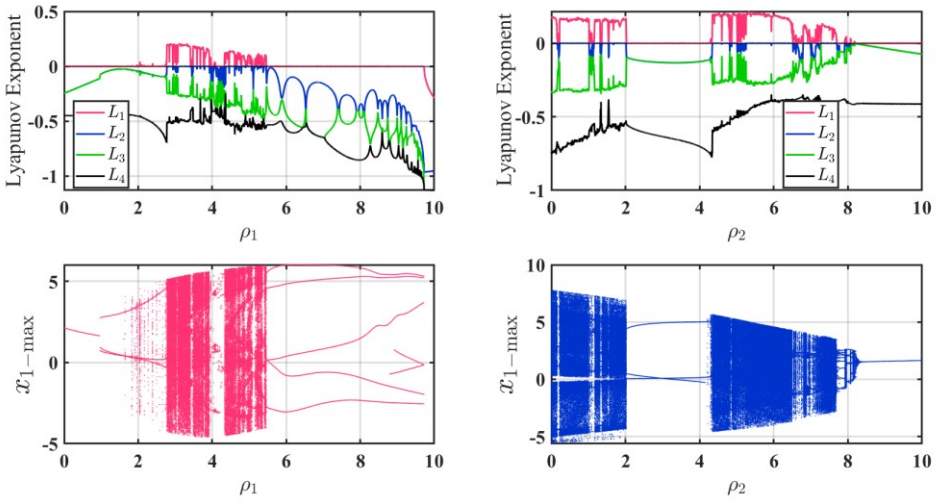



Fig 3 Lyapunov exponent spectra and bifurcation diagrams with respect to $\rho_1$, $\rho_2$.

### 3.2 Two-Parameter Bifurcation Analysis

To further analyze the dynamic evolution of the system under the joint action of multiple parameters, the memristive coupling strengths ($\rho_1$,$\rho_2$) and the memristor state parameters ($\phi_1$,$\phi_2$) are selected as two-parameter scanning objects. The effective-level diagrams, standard deviation diagrams, and three-dimensional distribution diagrams are plotted. Compared with single-parameter bifurcation, two-parameter bifurcation can more intuitively reveal the distribution of complex dynamic regions on the parameter plane.

First, the ($\rho_1$,$\rho_2$) parameter plane is scanned. Numerical simulations are per formed using the fourth-order Runge–Kutta method with an integration step of $\Delta t=0.01$. The total integration time is set to t=1800, and the transient data bef ore t=500 are discarded. The initial condition is given by $x_1(0)=x_2(0)=x_3(0)=x_4(0)=\phi_1(0)=\phi_2(0)=0.1$. The fixed system parameters are set as $a=1$, $b=0.01$, $c_1=c_2=2.2$, $d_1=d_2=1.2$, and the steepness coefficient of the segmented function is set to $p=10^4$. In this simulation, both $\rho_1$ and $\rho_2$ are scanned over [0,10], with a scan ning step of 1. For each parameter pair ($\rho_1$,$\rho_2$), the local maxima of the memri stor state variable $\phi_1$ are extracted. The number of effective maximum levels a nd the standard deviation of these local maxima are calculated to characterize t he orbit complexity and oscillation amplitude, respectively.

Fig 4 (a) and (b) show the effective-level distribution and the standard-deviation distribution of the local maxima of $\phi_1$ on the ($\rho_1$,$\rho_2$) plane, respectively. The color scale in (a) represents the number of effective levels, whereas that in (b) represents the standard deviation of the local maxima of $\phi_1$. Both quantities are dimensionless. As can be observed, different regions on the parameter plane exhibit clear color differences, indicating that the system dynamics are significantly changed by the joint variation of the two coupling strengths. When the number of effective levels is high, the distribution of local maxima becomes richer, suggesting stronger orbit complexity. This case usually corresponds to chaotic or complex oscillatory states. When the number of effective layers is low, the orbit structure is relatively simple, which may correspond to periodic or weak oscillatory states. The standard deviation diagram reflects the dispersion of the local maxima of $\phi_1$. Regions with larger standard deviations indicate a wider fluctuation range of the local maxima of $\phi1$ and stronger oscillatory variability. Fig 4(c) further presents the three-dimensional distribution of the number of effective levels over the ($\rho_1$,$\rho_2$) plane, where both the surface height and the color scale represent the number of effective levels. This indicates that a cooperative regulation effect exists between the two memristive coupling strengths. Since $\rho_1$ and $\rho_2$ act on different memristive synaptic coupling channels, the effective coupling strength of the system is jointly changed, resulting in different degrees of dynamic complexity under different parameter combinations.

Second, to investigate the influence of memristor state parameters on the system dynamics, the ($\phi_1$,$\phi_2$) parameter plane is further scanned. In this procedure, the integration step is still set to $\Delta t=0.01$, the total integration time is t=1200, and the transient process before t=400 is discarded. The fixed parameters are given as $a=1$, $b=0.01$, $c_1=c_2=2.2$, $d_1=d_2=1.2$, $\eta=0.04$, $\lambda=1.2$, $\sigma=0.005$, with $\rho_1=\rho_2=2.2$. The scanning ranges of $\phi_1$ and $\phi_2$ are both set to [0,6], with a step size of 0.02. For each parameter pair ($\phi_1$,$\phi_2$), the local maxima of the state variable $x_1$ are extracted, and the effective layers, standard deviation, variation range, and mean value are calculated.

Fig 4(d) and (e) show the effective-level distribution and the standard-deviation distribution of the local maxima of $x_1$ on the ($\phi_1$,$\phi_2$) plane, respectively. The color scale in (d) represents the number of effective levels, whereas that in (e) represents the standard deviation of the local maxima of $x_1$. Both quantities are dimensionless. It can be seen that variations in the memristor state parameters have a significant

influence on the dynamic complexity of the system output $x_1$. Regions with a larger number of effective levels indicate that more local-maximum levels are produced under the corresponding parameter combinations, suggesting a more complex orbit structure. In contrast, regions with lower effective layers indicate more regular system motion. The standard deviation distribution further shows that $\phi_1$ and $\phi_2$ affect not only the orbit complexity, but also the oscillation amplitude of the system. Fig 4(f) presents the corresponding three-dimensional distribution, where both the surface height and the color scale represent the number of effective levels of the local maxima of $x_1$.

Since $\phi_1$ and $\phi_2$ are directly involved in the calculation of the memductance function,

$$W_i(\phi_i) = a + b\phi_i + \eta tanh(\lambda\phi_i) \tag{13}$$

Their variations change the equivalent weights of the memristive synapses, thereby affecting the nonlinear coupling relationship between neurons. Meanwhile, the weak magnetic flux coupling terms $\sigma\tanh(\phi_2-\phi_1)$ and $\sigma\tanh(\phi_1-\phi_2)$ introduce interactions between the two memristor states, which further enriches the complex dynamic distribution on the parameter plane.

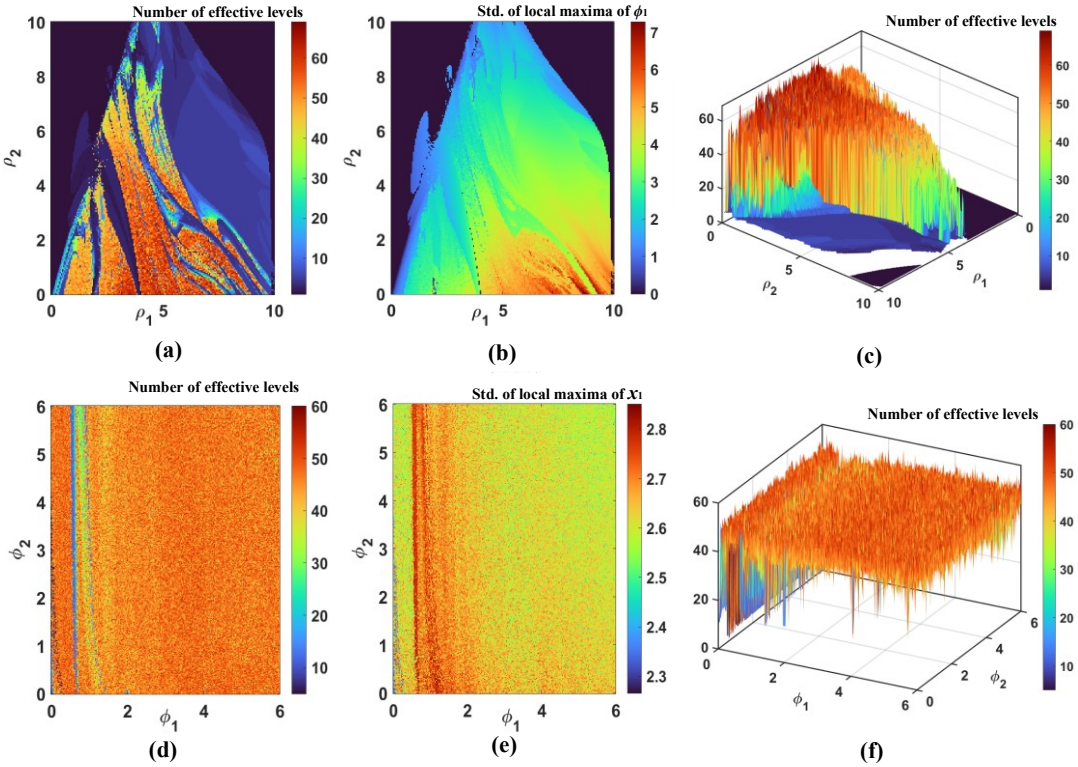



Fig 4 Two-parameter bifurcation analysis on the ($\rho_1$, $\rho_2$) and ($\phi_1$, $\phi_2$) planes. All quantities represented by the color scales are dimensionless.

In summary, the two-parameter bifurcation results show that distinct complex, regular, and transition regions exist on both the ($\rho_1$,$\rho_2$) and ($\phi_1$,$\phi_2$) planes. The memristive coupling strengths mainly affect the nonlinear coupling intensity of the system, whereas the memristor state parameters influence the orbit structure by changing the memductance functions and the magnetic flux coupling relationship.

These two types of two-parameter analyses jointly demonstrate that the constructed dual-memristor brain-inspired chaotic neural network has rich parameter regulation capability and complex dynamic characteristics.

### 3.3 Three-Dimensional Phase Portrait of the Single Chaotic Attractor

To visually illustrate the chaotic motion of the system under typical parameter conditions, a fixed set of parameters is selected in this section, and the three-dimensional phase trajectory together with its two-dimensional projections is plotted. The system parameters are set as $a$=1, $b$=0.01, $c_1$=$c_2$=2.2, $d_1$=$d_2$=1.2, $\rho_1$=3,$\rho_2$=5, $\eta$=0.04, $\lambda$=1.2, $\sigma$=0.005. The control parameters of the memristor internal state functions are chosen as $N_1$=$N_2$=0, so that the internal state function is reduced to h(ϕ)=ϕ. The initial condition is set as $x_1(0)$=$x_2(0)$=$x_3(0)$=$x_4(0)$=$\phi_1(0)$=$\phi_2(0)$=0.1.

Numerical simulation is carried out using the fourth-order Runge–Kutta method with an integration step of Δt=0.01. The total integration time is t=5000, and the transient process before t=500 is discarded. To obtain a clearer attractor, one phase point is sampled every 15 integration steps, and $x_1$, $x_2$, and $x_3$ are selected to form the three-dimensional phase space.

Fig 5 shows the three-dimensional chaotic attractor in the $x_1$,$x_2$,$x_3$ phase space and its projections on the three coordinate planes. It can be observed that the trajectory does not converge to an equilibrium point or a simple closed orbit. Instead, it is continuously stretched and folded within a bounded phase-space region, forming a complex curled structure. This indicates typical aperiodic chaotic motion.

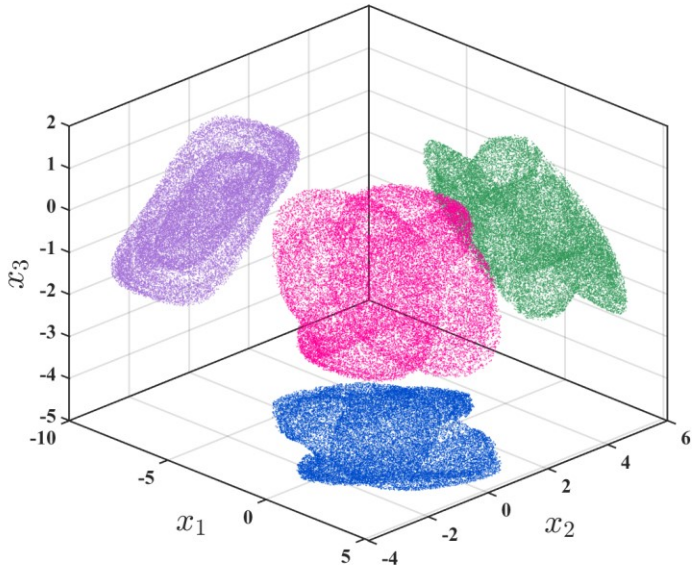



Fig 5 Three-dimensional chaotic attractor and its projections.

The projections on the $x_1$-$x_2$, $x_1$-$x_3$, and $x_2$-$x_3$ planes also show complex distributions, suggesting strong nonlinear coupling among the state variables. Due to the nonlinear saturating memductance function and the weak dual-memristor flux coupling, the effective coupling strength between neurons is dynamically regulated by the memristor states $\phi_1$ and $\phi_2$, which further increases the trajectory complexity.

Therefore, the three-dimensional phase portrait verifies that a stable single chaotic attractor can be generated by the proposed dual-memristor brain-inspired neural network under typical parameter settings. This result is consistent with the previous single-parameter bifurcation and Lyapunov exponent analyses.

### 3.4 Basins of Attraction

To analyze the dependence of the system on initial conditions and parameter variations, the basins of attraction on the $\phi_1(0)$–$\phi_2(0)$ initial-value plane and the $\rho_1$–$\rho_2$ parameter plane are plotted. In the simulations, the fourth-order Runge–Kutta method is used with a step size of $\Delta t=0.01$, and the transient data are discarded. Different colors denote different attractor classes identified by the ordered pair $(\phi_{1,c},\phi_{2,c})$, where $\phi_{1,c}$ and $\phi_{2,c}$ are the structural centers nearest to the long-term mean values of the memristor state variables $\phi_1$and $\phi_2$, respectively. Gray regions represent divergent trajectories. The color-scale labels are categorical and dimensionless. As shown in Fig 6(a), different attractor basins are interlaced on the $\phi_1(0)$–$\phi_2(0)$ initial-value plane, and their boundaries are relatively complex. This indicates that small changes in the memristor initial values may drive the system into different attractors. As shown in Fig 6(b), clear switching among different attractor classes can also be observed on the $\rho_1$–$\rho_2$ parameter plane, suggesting that the memristive coupling strengths can effectively regulate the final dynamical state of the system. These results show that the system has evident initial-condition sensitivity, multistability, and attractor coexistence, further confirming the complex dynamics of the proposed dual-memristor brain-inspired chaotic neural network.

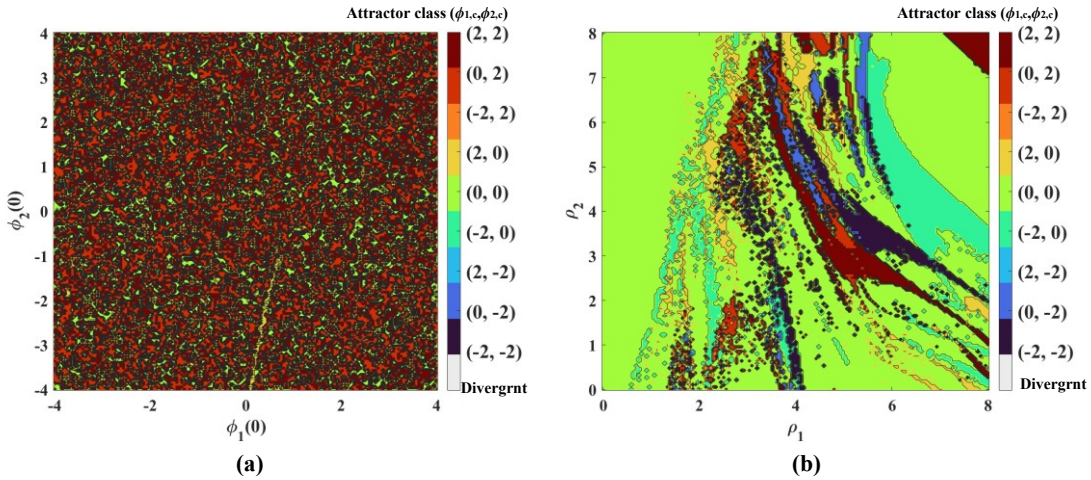



Fig 6 Basins of attraction of the proposed dual-memristor brain-inspired chaotic neural network. (a) Basin distribution on the $\phi_1(0)$-$\phi_2(0)$ initial-value plane. (b) Basin distribution on the ρ1 parameter plane. The color scale denotes the attractor class $(\phi_{1,c},\phi_{2,c})$, while the gray region represents divergent trajectories. The color-scale labels are categorical and dimensionless.

In this chapter, the dynamics of the proposed dual-memristor brain-inspired chaotic neural network are analyzed. Through single-parameter bifurcation diagrams and Lyapunov exponent spectra, it is verified that periodic, quasi-periodic, and chaotic states can be generated when the memristive coupling strengths are varied.

The two-parameter bifurcation results further show that complex, regular, and transition regions exist on the parameter planes, indicating strong parameter regulation capability.

Meanwhile, the three-dimensional phase portrait shows the chaotic attractor structure under typical parameters, where obvious stretching, folding, and aperiodic oscillations are observed. The basin analysis indicates that the system is sensitive to memristor initial values and coupling parameters, with multistability and attractor coexistence. These analyses clarify how nonlinear saturating memductance and weak flux coupling regulate bifurcation, multistability, and chaos, providing the dynamical basis for subsequent encryption.

## 4 DMBCNN-Based Global Pixel Interleaving Sub-packaging Framework for Multi-Source Remote Sensing Image Encryption and Decryption

DMBCNN constructed in Section 2 is adopted as the entropy source of the proposed encryption framework because it can synchronously regenerate identical chaotic states at both communication terminals, and an integrated encryption-decryption framework with global pixel interleaving and sub-packaging is established for secure transmission of multiple remote sensing images. RGB pixels are taken as basic units at the transmitter. A reversible global spatial scrambling sequence is derived via the master key $K_{\text{master}}$, 24-byte nonce N, image serial numbers and image dimensions, and spatial positions of pixels are rearranged while three channels of each pixel are kept bound. Interleaved images are then divided into blocks with metadata encoded. A global diget $H_p$ of the complete set of interleaved plaintext packets is calculated, and a session root key $K_{\text{root}}$ is derived from Kmaster, N and global sub-packaging metadata $Q$. Six-dimensional initial states and key-related parameters of DMBCNN are generated by HNISM with fused seeds. Brain memory windows $B_j$ for all data packets are extracted along state trajectories, and packet-level keys $K_{\text{packet,j}}$ and equal-length masks $G_j$ are further derived from the windows. Operations including $C_j=P_j \oplus G_j$ , authentication tag generation, packet sequence scheduling and self-descriptive encapsulation are implemented accordingly. $Q$, $N$, $H_p$ and global scrambling descriptions are recovered from authenticated ciphertext headers at the receiver. The identical $K_{\text{root}}$ is reconstructed with the same master key, and $B_j$, $K_{\text{packet,j}}$ and $G_j$ are synchronously regenerated by identical HNISM, DMBCNN parameters and packet sequences.$P_j=C_j \oplus G_j$ is executed after successful packet-level authentication, and interleaved images are obtained via packet combination. Inverse global pixel scrambling is finally performed to recover the original multi-image set. The closed loop covering overall encryption, transmission and decryption is illustrated in Fig 7.

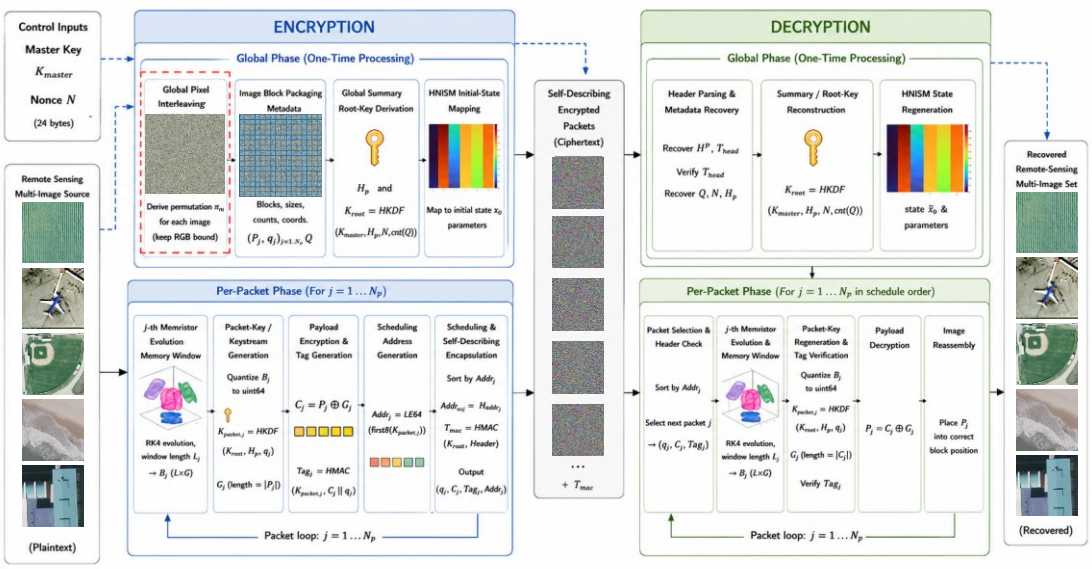



Fig 7 Closed-loop framework of DMBCNN-based encryption and decryption for multi-source remote sensing images.

## 4.1 Global Pixel Interleaving, Multi-Image Sub-Packaging and Self-Described Data Structure

Let $N_I$ RGB remote sensing images be the inputs, where the mmm-th image is denoted by $I_m \in R^{H_m \times W_m \times 3}$. As illustrated in Fig 8, an image-specific permutation $\pi_m$ is deterministically generated from the master key $K_{\text{mathrm}}$, nonce N, image index, and image dimensions, enabling identical spatial mapping at both transmitter and receiver without transmitting the scrambling sequence. Each image is scrambled independently to eliminate cross-image interference, while RGB pixels are treated as indivisible units, preserving channel correspondence and modifying only their spatial locations. The resulting global permutation disperses adjacent pixels, suppresses spatial correlation, and facilitates subsequent packetization. The interleaved image is finally divided into non-overlapping B×B blocks, with boundary blocks retaining their original dimensions without padding. The total number of generated packets is defined as

$$N_P = \sum_{m=1}^{N_I} \left\lceil \frac{H_m}{B} \right\rceil \left\lceil \frac{Wm}{B} \right\rceil \tag{14}$$

The j-th data packet is expressed as

$$P_j = (P_j, q_j) \tag{15}$$

Here, $P_j$ denotes the image payload in the interleaved domain, while $q_j$ records the corresponding image index, packet number, spatial position, and block dimensions. All packets together form the encrypted packet set, and global metadata $Q$ is generated to describe image dimensions, packaging parameters, and packet numbers. Instead of transmitting the complete scrambling sequence, the scrambling description $M_\pi$ only stores the algorithm configuration and image-related information, allowing the receiver to reconstruct the identical permutation $\pi_m$ using $K_{\text{master}}$, nonce $N$, and image descriptions. This avoids additional transmission overhead and ensures

consistent interleaving and inverse interleaving. Finally, ($q_j$, $P_j$) is encrypted together with authentication tags and scheduling information to generate self-described ciphertext packets, enabling independent parsing, packet recovery, and multi-image reconstruction.

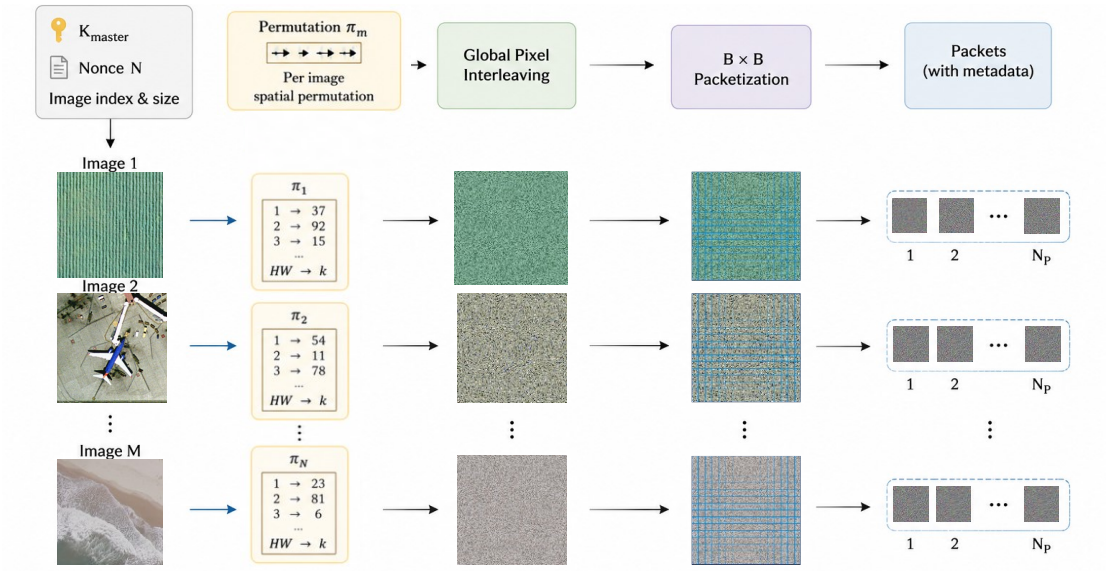



Fig 8 Schematic diagram of global pixel interleaving and multi-image sub-packaging structure.

## 4.2 Global Digest, Session Root Key and HNISM Initialization

All globally interleaved data packets are concatenated by transmitters in fixed generation order. Linearization is performed inside each packet under MATLAB column-major order, and a complete interleaved plaintext byte stream is obtained.

$$P_{all} = vec_{col}(P_1) \| vec_{col}(P_2) \| \cdots \| vec_{col}(P_{N_P}) \tag{16}$$

A 256-bit global plaintext digest is calculated on this basis.

$$H_P = SHA-256(P_{all}) \tag{17}$$

Let $K_{\text{master}}$ denote the master key, $N$ the 24-byte nonce, and enc($Q$) the globally sub-packaged metadata encoded in fixed field sequence. The session root key $K_{\text{root}}$ is derived by transmitters via $K_{\text{master}}$ , $N$ and enc($Q$). After self-described packet headers are parsed at receivers, $N$, $Q$, encrypted protected digest $H_{\text{p}}^{\text{enc}}$ and global scrambling description $M_\pi$ are acquired first. Identical $K_{\text{root}}$ is reconstructed with the same $K_{master}$, $N$ and enc($Q$), and digest masks are generated from $K_{\text{root}}$ for $H_p$ recovery. Extended header authentication tags are recalculated by receivers with $H_{\text{p}}^{\text{enc}}$, $Q$ and $M_\pi$ afterwards, and comparisons are carried out against tags stored in packet headers. Subsequent HNISM initialization, DMBCNN state regeneration and inverse scrambling are executed only after successful verification. Consistent cryptographic states between two terminals are guaranteed by $K_{\text{root}}$ and $H_{\text{p}}$, while consistent spatial mapping after image combination is ensured by $M_\pi$.

$$K_{root} = SHA-256(K_{master} \| N \| enc(Q)) \tag{18}$$

No confidentiality is required for the nonce, yet uniqueness must be maintained under a single master key. Identical root keys and state trajectories generated by repeated sessions are therefore prevented. Identical nonces are allowed to be reused merely in paired security tests. Controlled variables and comparable experimental results are guaranteed accordingly. Corresponding nonces are retrieved from ciphertext headers by receivers during standard encryption and decryption processes. Session reconstruction is completed together with master keys and metadata.

After the calculation of global digest and session root key is finished, $K_{\text{root}}$ , $H_p$ and nonce $N$ are fused into initialization seeds by transmitters. Identical initialization computation is implemented by receivers after the same $K_{\text{root}}$ is reconstructed, $H_p$ is recovered and header authentication is passed. Uniform HNISM inputs are therefore acquired:

$$S = SHA-256(K_{root} \| H_P \| N) \tag{19}$$

Consistent domain separation rules are adopted by HNISM at both encryption and decryption terminals. Three hash branches corresponding to left brain, right brain and memristive brain are generated separately:

$$H_L = SHA-256(S \| LEFT-BRAIN) \tag{20}$$

$$H_R = SHA-256(S \| RIGHT-BRAIN) \tag{21}$$

$$H_M = SHA-256(S \| MEMRISTOR-BRAIN) \tag{22}$$

Three hash outputs are concatenated in identical order at both terminals, parsed into twelve uint64 values in little-endian order and normalized to satisfy $u_i \in [0,1]$. Mapping variables are then constructed via the identical nonlinear relation:

$$L_1 = \text{mod}[\sin(\pi u_1) + u_7^2 + u_3 u_9, 1] \tag{23}$$

$$L_2 = \text{mod}[\cos(\pi u_2) + u_8^2 + u_4 u_{10}, 1] \tag{24}$$

$$R_1 = \text{mod}[\sin(2\pi u_3) + u_9^2 + u_1 u_{11}, 1] \tag{25}$$

$$R_2 = \text{mod}[\cos(2\pi u_4) + u_{10}^2 + u_2 u_{12}, 1] \tag{26}$$

$$M_1 = \text{mod}[|L_1 - R_1| + \sin(\pi u_5) + u_{11}^2, 1] \tag{27}$$

$$M_2 = \text{mod}[|L_2 - R_2| + \sin(\pi u_6) + u_{12}^2, 1] \tag{28}$$

Let $z=[L_1,R_1,L_2,R_2,M_1,M_2,u_7,...,u_{12}]$. Identical six-dimensional initial states are acquired at both encryption and decryption terminals as

$$x_k(0) = 0.05 + 0.90|z_k|, \qquad k = 1,2,....,6 \tag{29}$$

Small-range key-dependent perturbations are applied to critical coupling parameters and saturation parameters by HNISM. Identical initial states and perturbed

parameters can be regenerated at both terminals on condition that $K_{\text{master}}$, $N$, $Q$ and $H_{\text{p}}$ are completely consistent. Any alteration to input values will trigger overall variations in subsequent state trajectories, brain memory windows and packet-level keys:

$$\rho_1^{'} = \rho_1 + 0.20(z_7 - 0.5), \qquad \rho_2^{'} = \rho_2 + 0.20(z_8 - 0.5) \tag{30}$$

$$\eta' = \max\{\eta + 0.005(z_9 - 0.5), 0.001\} \tag{31}$$

$$\lambda' = \lambda + 0.10(z_{10} - 0.5), \qquad \sigma' = \max\{\sigma + 0.001(z_{11} - 0.5), 10^{-5}\} \tag{32}$$

### 4.3 Sub-Packet Encryption, Authentication and Self-Descriptive Encapsulation

Bytewise XOR operations are carried out by transmitters on the $j$-th plaintext payload to generate ciphertexts. Reverse XOR operations are implemented by receivers with identical masks after authentication passes, and the two processes satisfy

$$C_j = P_j \oplus G_j, \qquad P_j = C_j \oplus G_j \tag{33}$$

Authentication tags are generated via packet-level keys by transmitters to detect tampering on ciphertext payloads and address metadata

$$T_j = SHA-256(K_j \| vec(C_j) \| enc(q_j)) \tag{34}$$

Tags are recalculated with regenerated $K_{\text{packet,j}}$ by receivers for ciphertext payload $C_j$ and packet metadata $q_j$ in identical field sequences before decryption, and comparisons are made against $Tag_j$ transmitted with packets. The corresponding data packet is rejected immediately without decryption and data rewriting if mismatches exist. $P_j$=$C_j$⊕$G_j$ is calculated only after successful verification. Packet-level tags in programs of this paper are computed by SHA-256($K_{\text{packet,}}$ ‖ vec($C_j$) ‖ enc($q_j$)). Descriptions in figures and main text are presented in line with practical implementations rather than standard HMAC expressions.

64-bit scheduling addresses are generated from each packet-level key by transmitters.

$$A_j = LE64(first_8[SHA-256(K_j \| ADDR)]) \tag{35}$$

Here, first8 represents the extraction of the first 8 bytes from hash outputs, and LE64 denotes the parsing into uint64 values under little-endian format. Ciphertext packets are sorted by transmitters according to respective packet scheduling addresses to form transmission or storage sequences. Nonce, $Q$, $H_{\text{p}}^{\text{enc}}$, packet sequence, ciphertext packets and $M_\pi$ are stored within CipherPackage. Stored packet sequences are read by receivers to restore the original logical order of data packets. The $j$-th ciphertext packet is remapped to the j-th brain memory window and packet-level key accordingly. ($q_j$,$C_j$,$Tag_j$) is then sent into the authentication and decryption procedure.

$$C_S = [C_{\pi(1)}, C_{\pi(2)}, ..., C_{\pi(N_P)}] \tag{36}$$

Identical global states can be reconstructed by receivers as transmitters, and direct exposure of plaintext digests is prevented simultaneously. Masks expanded from root keys are adopted by transmitters to protect $H_{\mathrm{p}}$:

$$H_P^{enc} = H_P \oplus G(K_{root}, 32) \tag{37}$$

Extended header authentication tags are further generated by transmitters. Protected digest $H_{\mathrm{p}}^{\mathrm{enc}}$, global metadata Q and global scrambling description $M_\pi$ are all included for integrity protection. After packet headers are parsed by receivers, $K_{\mathrm{root}}$ is reconstructed first based on $K_{\mathrm{master}}$, $N$ and $Q$. The tag is recalculated afterwards using $K_{\mathrm{root}}$, $H_{\mathrm{p}}^{\mathrm{enc}}$, $Q$ and $M_\pi$. $H_{\mathrm{p}}$ is recovered by receivers and synchronization of HNISM and DMBCNN is initiated when tags match. Decryption is terminated directly in case of tag mismatch.

### 4.4 Multi-Image Reconstruction and Computational Complexity

After header verification and packet sequence recovery are completed, $B_{\mathrm{j}}$, $K_{\mathrm{packet,j}}$ and $G_j$ are regenerated sequentially by receivers according to packet indices. $P_j=C_j \oplus G_j$ is implemented after $Tag_j$ verification. Subsequently, each plaintext payload is written back to corresponding positions based on the image serial number, interleaved domain coordinates and actual block dimensions stored in $q_j$. $N_I$ interleaved images are obtained after combination. Finally, scrambling sequence $M_\pi$ of each image is regenerated by receivers with $K_{\mathrm{master}}$, $N$, image serial numbers and image dimensions, and inverse scrambling operations are performed to restore original spatial coordinates. Both pixel scrambling and XOR operations are strictly invertible transformations. Identical global inputs, state trajectories, packet indices and scrambling parameters are adopted at both terminals. Exact byte-by-byte reconstruction can thus be realized under the premise that keys and ciphertext packets are all correct. Let $N_B$ denote the total bytes of valid payload, $\mathrm{N_P}$ the quantity of data packets, and $L$ the length of brain memory windows. The dominant computational complexity is expressed as

$$O(N_P + LN_P + N_P \log N_P + T_0 + L) \tag{38}$$

The five 256×256 RGB images adopted in experiments contain a total valid payload of 983,040 bytes. When B=16, a total of 1,280 data packets are generated. The 32-byte authentication tag for each packet occupies a total of 40,960 bytes, accounting for 4.17% of the valid payload.

## 5 Simulation Results and Security Analysis

### 5.1 Experimental Environment and Parameter Settings

All experiments are implemented under MATLAB R2023b. The test platform is equipped with an Intel Core i5-11400H CPU and 16 GB RAM. The experimental images were selected from the publicly available UC Merced Land Use dataset [37]. The dataset contains 2,100 RGB aerial images covering 21 land-use classes, with 100 images in each class. Each image has a spatial size of 256×256 and a ground sampling distance of approximately 0.3 m per pixel. The images were manually

cropped from large aerial orthophotos in the United States Geological Survey National Map Urban Area Imagery collection. Five images from the agricultural, airplane, baseball-diamond, beach, and buildings classes were used in this study. The original RGB images were directly used without resizing, cropping, channel conversion, or other preprocessing. The key parameter settings are specified as $B$=16, $L$=64, $T_0$=1000, and $\Delta t$=0.01. Global spatial scrambling, which generates scrambling sequences independently for each image with RGB pixels as basic units, is enabled in the scheme. The total valid payload of the five test images reaches 983,040 bytes.

### 5.2 Encryption Results and Reversibility

Ciphertext images show random noise textures. When the correct secret key, nonce, complete metadata and global scrambling description are fully matched, all five images can be perfectly recovered byte by byte through packet sequence restoration, packet-by-packet decryption, image stitching and inverse global pixel scrambling. The mean square error (MSE) of lossless decryption is 0.

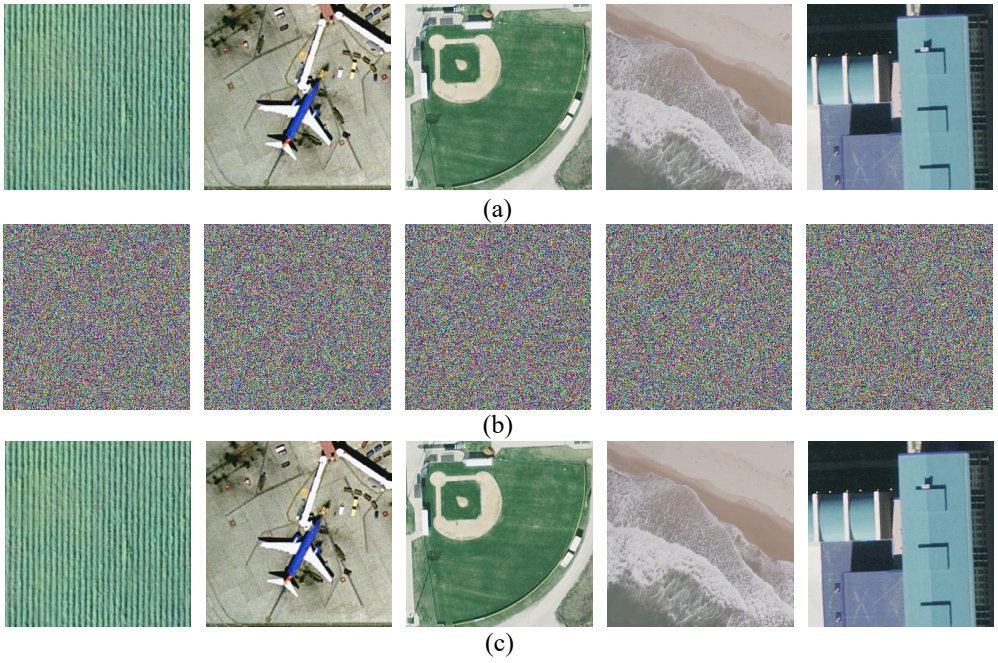



Fig 9 Plaintext, ciphertext and accurate recovery results of five remote sensing images.

Fig 9 visually verifies the confidentiality and reversibility of the proposed scheme. Distinct ground feature structures including roads, buildings, vegetation and water bodies exist in plaintext images, while all outlines, textures, color distributions and spatial correlations are concealed in ciphertexts, making it impossible to directly distinguish any ground object category. When decrypted with the correct master key, nonce, complete metadata and scrambling description, all five images can be restored byte by byte with a pixel-level MSE of 0. This demonstrates that the entire procedure consisting of global pixel interleaving, packet segmentation, packet sequence scheduling, mask generation, image combination and inverse scrambling is fully reversible.

### 5.3 Histogram, Chi-Square Test and Information Entropy

Chi-square test and Shannon information entropy are adopted to evaluate ciphertext distribution:

$$\chi^2 = \sum_{i=0}^{255} \frac{(v_i - e_i)^2}{e_i} \tag{39}$$

where $v_i$ and $e_i$ denote the observed frequency and the expected frequency under uniform distribution, respectively. The critical value of the chi-square test is 293.2478 at a significance level of 0.05.

$$H(X) = -\sum_{i=0}^{255} p(x_i) \log_2 p(x_i) \tag{40}$$

Table 2 Information entropy and chi-square uniformity test results of five basic ciphertext images.

| Image | $H_R$ | $H_G$ | $H_B$ | entropy | $\chi_R^2$ | $\chi_G^2$ | $\chi_B^2$ | Result |
|---|---|---|---|---|---|---|---|---|
| 1 | 7.99738 | 7.99682 | 7.99740 | 7.99720 | 237.187 | 287.742 | 235.578 | Pass |
| 2 | 7.99709 | 7.99729 | 7.99736 | 7.99725 | 262.539 | 246.781 | 237.593 | Pass |
| 3 | 7.99707 | 7.99723 | 7.99692 | 7.99707 | 265.632 | 250.773 | 278.804 | Pass |
| 4 | 7.99699 | 7.99734 | 7.99737 | 7.99723 | 272.664 | 241.648 | 239.734 | Pass |
| 5 | 7.99694 | 7.99724 | 7.99739 | 7.99719 | 277.976 | 249.437 | 238.062 | Pass |

The overall average entropy of the five basic ciphertext images reaches 7.997193 bit, and the chi-square statistics of all 15 RGB channels are lower than the critical value of 293.2478. A further statistical summary covering 5 plaintext images and 10 ciphertext images shows that the average entropy of plaintexts is 6.841250 bit, while that of ciphertexts is 7.997162 bit. The average deviation between ciphertext entropy and the ideal value of 8 is merely 0.002838 bit. Among the 30 channels of the 10 ciphertext images, 28 channels pass the uniformity test; only the R and B channels of Cipher_Modified_02 fail to pass. After aggregating all ciphertext data for statistics, the entropy values of the R, G and B channels are 7.999733, 7.999698 and 7.999689 respectively, with corresponding chi-square values of 242.7250, 274.1195 and 282.4734. All three channels pass the uniformity test.

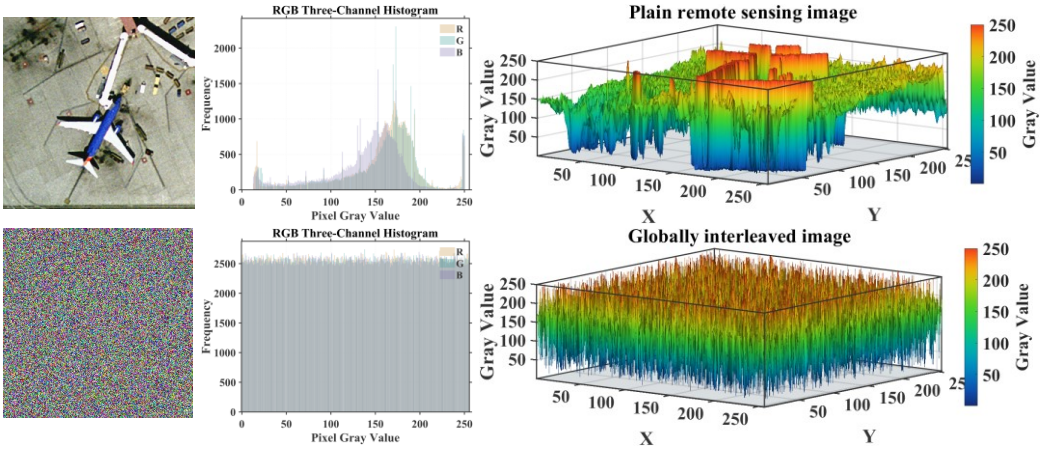



Fig 10 Comparison of RGB channel histograms between plaintext and ciphertext images.

Fig 10 compares the statistical distributions of plaintext and ciphertext images. The plaintext RGB histograms show distinct peaks and uneven distributions related to scene content, whereas the ciphertext histograms are nearly uniform over [0,255]. This is consistent with the chi-square and entropy results in Table 2: all 15 ciphertext channels pass the uniformity test, with an average entropy of 7.997193 bit. For 10 ciphertext images, the average entropy remains 7.997162 bit, indicating that global interleaving and packet-based encryption preserve ciphertext randomness.

### 5.4 Correlation of Adjacent Pixels

The Pearson correlation coefficients of adjacent pixels are calculated along horizontal, vertical, and two diagonal directions:

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)D(y)}} \tag{41}$$

Table 3 Correlation coefficients of adjacent pixels in the original and encrypted Image.

| Table 3 | Channel | Horizontal | Vertical | Diagonal | Anti-diagonal |
|---|---|---|---|---|---|
| Original Image | R | 0.944520 | 0.938855 | 0.901556 | 0.892325 |
| | G | 0.934465 | 0.928661 | 0.885103 | 0.875913 |
| | B | 0.939018 | 0.933463 | 0.894075 | 0.884250 |
| Encrypted Image | R | 0.000941 | 0.000060 | −0.005490 | 0.001258 |
| | G | 0.000342 | −0.002971 | 0.013232 | 0.001018 |
| | B | −0.001121 | 0.001433 | −0.000184 | 0.000372 |

The average correlation coefficient of adjacent pixels in the plaintext image is 0.910666 over four directions and three color channels, indicating strong spatial correlation. After encryption, all correlation coefficients are distributed around zero, ranging from − 0.005490 to 0.013232, with an average absolute value of only 0.002763. These results demonstrate that the proposed scheme effectively removes the linear correlation between adjacent pixels and exhibits excellent resistance against statistical attacks.

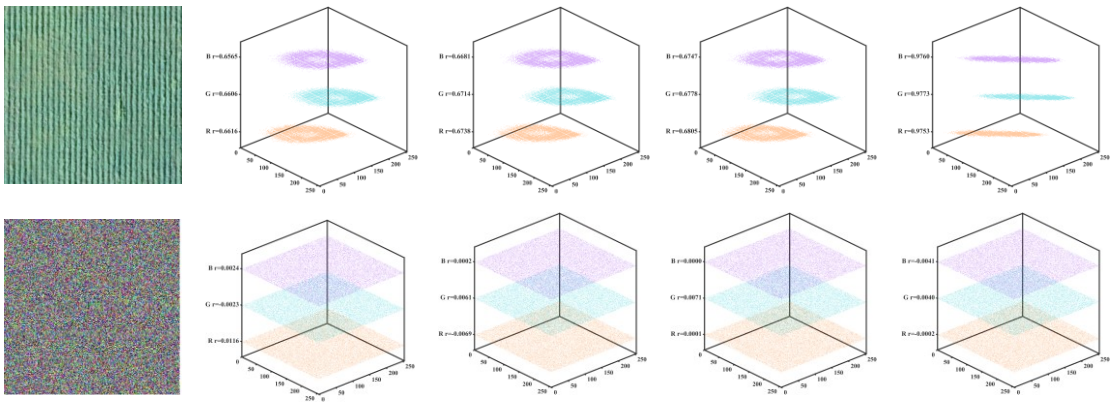


Fig 11 Adjacent pixel correlation distribution of plaintext and ciphertext images in four directions.

Fig 11 shows that adjacent pixels in plaintext images are densely distributed along the main diagonal, indicating strong spatial correlation. The highest correlation occurs in the vertical direction, reflecting the continuity of roads, building edges, and ground objects in remote sensing images. After encryption, pixel pairs are uniformly

scattered without visible linear patterns. The ciphertext correlation coefficients range from − 0.010155 to 0.008507, with a maximum absolute value of 0.010155 and an average absolute value of only 0.002922 over four directions, demonstrating that adjacent-pixel correlation is effectively eliminated.

### 5.5 Complete Multi-Image Differential Attack Analysis

Only one 8-bit plaintext sample in the complete set of five images is modified, while the master key, nonce and all other experimental conditions remain unchanged. Five groups of differential ciphertext pairs are generated, and the NPCR and UACI values of the R, G, B channels and the full ciphertext region are calculated and counted respectively:

$$NPCR = \frac{1}{N}\sum_{i=1}^{N} D_i \times 100\%, \tag{42}$$

$$D_i = 1(C_i \neq C_i') \tag{43}$$

$$UACI = \frac{1}{N}\sum_{i=1}^{N} \frac{|C_i - C_i'|}{255} \times 100\% \tag{44}$$

Table 4 NPCR and UACI statistics of five groups of differential ciphertext pairs under single plaintext pixel modification.

| Statistical Scope | Average NPCR (%) | Average UACI (%) |
|---|---|---|
| R channel | 99.6103 | 33.5240 |
| G channel | 99.6024 | 33.4313 |
| B channel | 99.5892 | 33.3744 |

Table 5 Comparison of NPCR and UACI.

| Algorithm | Proposed | [28] | [25] | [15] | [16] | [22] |
|---|---|---|---|---|---|---|
| NPCR(%) | 99.6006 | 99.6078 | 99.6148 | 99.6060 | 99.5000 | 99.6086 |
| UACI(%) | 33.4432 | 33.4551 | 33.4654 | 33.5126 | 33.4825 | 33.4694 |

The per-channel data of five groups are listed in Table 4. The overall average NPCR and UACI are close to theoretical thresholds. Table 5 compares the above indicators with existing chaotic encryption methods. It proves our scheme has competitive performance and strong resistance to differential attacks. Any tiny pixel change of plaintext can spread over all ciphertexts through DMBCNN state trajectories.

### 5.6 Noise Attack Analysis

To quantify the practical impact of diverse noise models on ciphertexts, the ciphertext sample change rate is defined as

$$R_{change} = \frac{N_{changed}}{N_{total}} \times 100\% \tag{45}$$

To assess noise resistance, Gaussian, salt-and-pepper, and speckle noise were added to ciphertext images at intensities of 0.5%, 1%, and 3%. As shown in Table 6, salt-and-pepper noise causes the least degradation, with the average PSNR and SSIM decreasing from 32.20 dB and 0.9410 at 0.5% noise to 24.34 dB and 0.7201 at 3%. Gaussian noise produces the most severe deterioration, with PSNR values of 16.47, 15.23, and 13.30 dB, while speckle noise yields intermediate results. Overall, reconstruction quality decreases steadily with increasing noise intensity, but complete decoding failure does not occur.

Table 6 Quality evaluation metrics of decrypted images under different noise types and intensities.

| Noise Intensity | Gaussian | Salt-and-pepper | Speckle |
|---|---|---|---|
| 0.5% | 16.47 | 32.20 | 19.20 |
| 1% | 15.23 | 28.93 | 17.85 |
| 3% | 13.30 | 24.34 | 15.78 |

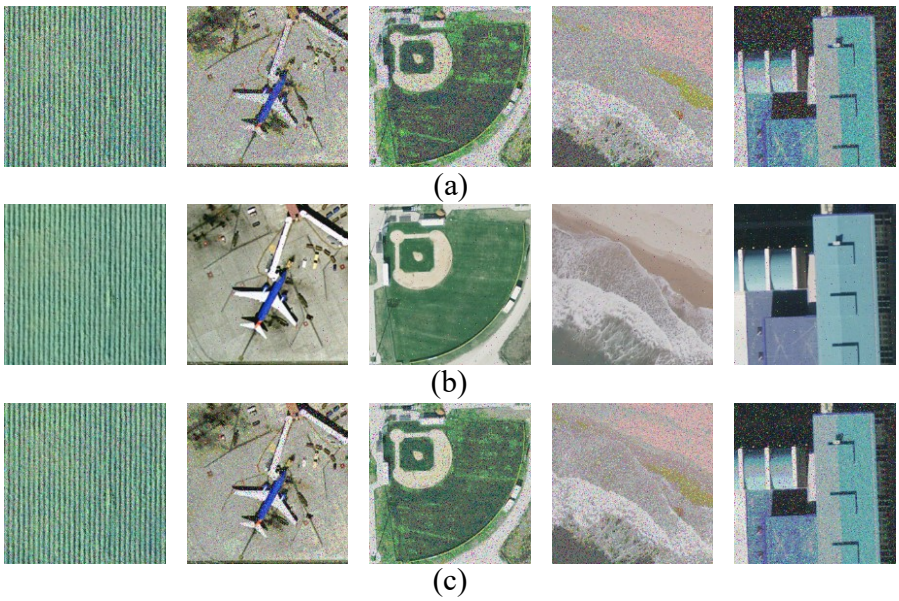



Fig 12 Comparison of decryption recovery effects under different noise types with 1% noise intensity.

Fig 12 shows representative decrypted images under 1% noise. Salt-and-pepper noise preserves recognizable image content, whereas Gaussian and speckle noise produce globally distributed artifacts due to the dispersion effect of pixel permutation. These results demonstrate the scheme’s robustness to common noise interference, particularly salt-and-pepper noise.

### 5.7 Robustness Analysis of Ciphertext Under Various Spatial Occlusion Modes

To evaluate the ability of global pixel permutation to mitigate local ciphertext damage, three occlusion patterns (central rectangle, four-corner, and cross) are tested under identical data loss ratios of 10%, 20%, and 50%. As summarized in Table 7, increasing the occlusion ratio gradually reduces the average PSNR from about 19.1 dB to 12.1 dB and the average SSIM from 0.43 to 0.10. Under the same data loss ratio, the three occlusion patterns exhibit nearly identical performance. For example, at 20%

occlusion, the average PSNR is 16.08, 16.12, and 16.10 dB for the three patterns, respectively, with comparable SSIM values.

Table 7 Quality evaluation metrics of decrypted images under different spatial occlusion modes and ratios.

| Occlusion Mode | Occlusion Ratio | Average PSNR (dB) | Average SSIM | Average MSE |
|---|---|---|---|---|
| Center | 10% | 19.11 | 0.4239 | 802.24 |
| | 20% | 16.08 | 0.2661 | 1609.77 |
| | 50% | 12.08 | 0.1032 | 4041.11 |
| FourCorners | 10% | 19.17 | 0.4303 | 789.03 |
| | 20% | 16.12 | 0.2686 | 1596.33 |
| | 50% | 12.06 | 0.1036 | 4061.85 |
| Cross | 10% | 19.15 | 0.4266 | 794.27 |
| | 20% | 16.10 | 0.2661 | 1601.42 |
| | 50% | 12.10 | 0.1035 | 4023.04 |

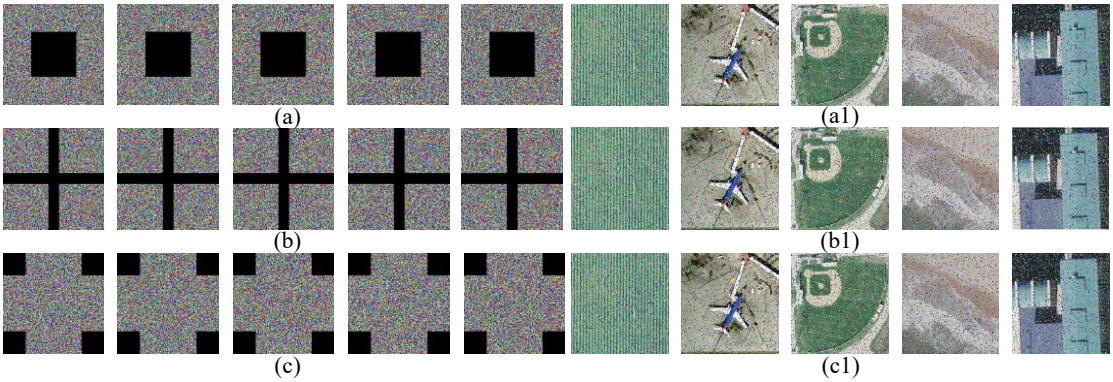



Fig 13 Occlusion attack examples and decrypted results under 20% spatial occlusion. (a-c) Center rectangle, cross and four-corner occluded ciphertexts; (a1-c1) Corresponding decrypted results.

Fig 13 further visualizes decrypted results under 20% occlusion. All reconstructed images exhibit evenly distributed global noise rather than localized concentrated distortion, which proves that global permutation successfully scatters ciphertext errors across the whole image. Consequently, the proposed encryption scheme possesses favorable robustness and consistent decoding performance against occlusion attacks with diverse spatial distributions.

### 5.8 Encryption and Decryption Time Analysis

To evaluate the computational efficiency of the proposed method, encryption and decryption time tests were conducted on five 256×256 RGB remote-sensing images. The five images contain a total of 327,680 pixels and are divided into 1,280 data packets. The core encryption time, core decryption time, and overall running time were measured separately, as summarized in Table X. As shown in Table X, the core encryption time for the five-image batch is 1.4677 s, while the core decryption time is 1.4415 s. The corresponding throughputs are 0.223 MPixel/s and 0.227 MPixel/s, respectively. The similar encryption and decryption times indicate that synchronized state regeneration and inverse global pixel interleaving do not introduce significant additional computational overhead. All recovered images passed the exact recovery

verification, confirming that the proposed method achieves lossless decryption while maintaining stable computational efficiency.

Table 8 Computational efficiency of the proposed encryption and decryption framework.

| Item | Encryption | Decryption |
|---|---|---|
| Core processing time (s) | 1.4677 | 1.4415 |
| Total running time (s) | 3.9211 | 1.8454 |
| Throughput (MPixel/s) | 0.223 | 0.227 |
| Exact recovery verification | — | 5/5 passed |

## 6. Conclusion

In this paper, a dual-memristor brain-inspired chaotic neural network (DMBCNN) with nonlinear saturating memductive synapses and weak flux coupling was proposed, and a packet-oriented remote sensing multi-image encryption framework was developed based on its reproducible chaotic dynamics. The dynamical behaviors of the proposed system were systematically investigated through bifurcation diagrams, Lyapunov exponent spectra, two-parameter bifurcation analysis, three-dimensional phase portraits, and basins of attraction, demonstrating rich chaotic characteristics, strong parameter tunability, and multistability. Exploiting these properties, the proposed encryption framework integrates reversible global RGB-pixel interleaving, metadata-aware sub-packaging, session-dependent initialization, packet scheduling, authentication, and self-described reconstruction to support secure transmission of heterogeneous remote sensing images. Experimental results demonstrate that the proposed scheme achieves lossless image recovery, excellent statistical characteristics, high resistance to differential, noise, and occlusion attacks, and reliable packet authentication with only a small communication overhead. By establishing a close connection between nonlinear chaotic dynamics and practical packet-oriented image encryption, the proposed framework provides an effective and reliable solution for secure remote sensing image transmission. Future work will focus on hardware implementation, real-time optimization, and extending the proposed framework to large-scale remote sensing communication systems and other multimedia security applications.

## Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant No. 62461022, the Open Project of State Key Laboratory of Integrated Chips and Systems under Grant No. SKLICS-K202501, and the Gansu Province University Industry Support Plan Project under Grant No. 2025CYZC-060.

## References

[1] Chua L O 1971 *IEEE Trans. Circuit Theory* **18** 507
[2] Strukov D B, Snider G S, Stewart G R and Williams R S 2008 *Nature* **453** 80
[3] Lin H R, Duan C X, Deng X H and Min G 2025 *J. Electron. Inf. Technol.* **47** 2194
[4] Zhang S, Yao W, Xiong L, Wang Y J, Tang L H, Zhang X and Yu F 2024 *Chaos Solitons Fractals* **187** 115408

[5] Chen C J, Chen J Q, Bao H, Chen M and Bao B C 2019 *Nonlinear Dyn.* **95** 3385
[6] Bao H, Hua M J, Ma J, Chen M and Bao B C 2023 *IEEE Trans. Ind. Electron.* **70** 10526
[7] Lin H R, Zhang Y, Deng X H, Jiang L and Min G 2026 *Nonlinear Dyn.* **114** 93
[8] Lin H R, Wang C H, Sun Y C and Wang T 2023 *IEEE Trans. Circuits Syst. II Express Briefs* **70** 311
[9] Messadi M, Kemih K, Moysis L and Volos C 2023 *Integration* **88** 91
[10] Deng Z K, Wang C H, Lin H R, Deng Q L and Sun Y C 2024 *Sci. Sin. Inform.* **54** 2554
[11] Ma J 2026 *J. Lanzhou Univ. Technol.* **52** 165
[12] Ma J 2023 *J. Zhejiang Univ.-Sci. A* **24** 109
[13] Yao W, Gao K, Sun Y C, Wen S P, Xiong L and Chen G R 2026 *Nonlinear Dyn.* **114** 789
[14] Ma X J, Mou J, Xiong L, Banerjee S, Cao Y H and Wang J Y 2021 *Chaos Solitons Fractals* **152** 111363
[15] Yang C F, Wang X P and Zeng Z G 2022 *IEEE Trans. Circuits Syst. I Regul. Pap.* **69** 1395
[16] Zhang S, Zheng J H, Wang X P, Zeng Z G and He S B 2020 *Nonlinear Dyn.* **102** 2821
[17] Xiong L, Wang Y and An X L 2024 *Phys. Scr.* **99** 065230
[18] Li X X, He Q Q, Yu T Y, Cai Z and Xu G Z 2024 *Chin. Phys. B* **33** 030505
[19] Jian C L, Tian Z A, Liang B, Hu C Y, Wang Q and Chen J X 2023 *Chin. Phys. B* **32** 100503
[20] Lin B, Liu M and Ye G D 2026 *Chin. Phys. B* **35** 050502
[21] Su J M, Fang S H, Hong Y and Wen Y 2024 *Chin. Phys. B* **33** 070502
[22] Li H, Deng L B and Gu Z Q 2020 *IEEE Access* **8** 30127
[23] Wen H P, Feng Z Y, Bai C X, Lin Y T, Zhang X Y and Feng W 2024 *Phys. Scr.* **99** 055254
[24] Zhang L and An X L 2024 *IEEE Access* **12** 2573
[25] Du S M and Ye G D 2023 *Alexandria Eng. J.* **66** 979
[26] Lu W R, Jin C H, Wang J H, Liu X Y, Liu J Y and Zhai Z H 2025 *J. King Saud Univ. Comput. Inf. Sci.* **37** 254
[27] Ding D W, Xie D, Zhang H W, Yang Z L and Liu C A 2025 *IEEE Trans.* Circuits Syst. Video Technol. **35** 6522
[28] Wang W T, Sun J Y, Wang G and Zhang H 2023 *Multimed. Tools Appl.* **82** 45233
[29] Ma K Y, Teng L, Wang X Y and Meng J 2021 *Multimed. Tools Appl.* **80** 24737
[30] Gao X Y, Sun B, Cao Y H, Banerjee S and Mou J 2023 *Chin. Phys. B* **32** 030501
[31] Tian J X, Zhang X Q, Liu M, Jin S C, Shi D X and Yang S W 2025 *J. Supercomput.* **81** 566
[32] Li Z, Yang S Q, Tan W J and Wu X M 2025 *Nonlinear Dyn.* **113** 2769
[33] Tian J X, Jin S C, Zhang X Q, Yang S W and Shi D X 2024 *Chin. Phys. B* **33** 050502
[34] Safdar M U, Shah T and Ali A 2025 *Signal Process. Image Commun.* **138** 117353
[35] Zhang Z B and Zhang J D 2024 *Vis. Comput.* **40** 8615
[36] Zhou Z Q, Xu X M, Yao Y X, Jiang Z H and Sun K H 2023 *Chaos Solitons Fractals* **173** 113630
[37] Yang Y and Newsam S 2010 *Proc. 18th ACM SIGSPATIAL Int. Conf. Adv. Geogr. Inf. Syst.* 270