




# Grid Multi-Butterfly Memristive Neural Network With Three Memristive Systems: Modeling, Dynamic Analysis, And Application in Police IoT

Hairong Lin , *Member, IEEE*, Xiaoheng Deng , *Senior Member, IEEE*, Fei Yu, and Yichuang Sun , *Senior Member, IEEE*

**Abstract**—Nowadays, the Internet of Things (IoT) technology has been widely applied in the police security system. However, with more and more image data that concerns crime scenes being transmitted through the police IoT, there are some new security and privacy issues. Therefore, how to design a safe and efficient secret image sharing solution suitable for police IoT has become a very urgent task. In this work, a grid multi-butterfly memristive Hopfield neural network (HNN) with three memristive systems is constructed and its complex dynamics are deeply analyzed. Among them, the first memristive system is modeled by emulating a self-connection synapse, the second memristive system is modeled by coupling two neurons, and the third memristive system is modeled by describing external electromagnetic radiation. Dynamic analyses show that the proposed memristive HNN can not only generate two kinds of 1-directional (1D) multi-butterfly chaotic attractors but also produce complex grid (2D) multi-butterfly chaotic attractors. More importantly, by switching the initial states of the second and third memristive systems, the grid multi-butterfly memristive HNN exhibits initial-boosted plane coexisting multi-butterfly attractors. Moreover, the number of butterflies contained in a multi-butterfly attractor and coexisting attractors can be easily adjusted by changing memristive parameters. Based on these complex dynamics, an image security solution is designed to show the application of the newly constructed grid multi-butterfly memristive HNN to police IoT security. Security performances indicate the designed scheme can resist various attacks and has high robustness. Finally, the test results are further demonstrated through RPI-based hardware experiments.

**Index Terms**—Grid multi-butterfly attractor, memristive neural network, initial-boosted behavior, chaos-based application, IoT.

## I. INTRODUCTION

WITH the rise of global terrorism and crime rates, the application of the Internet of Things (IoT) technology in the police security system is getting more and more important [1]. There is no doubt that it not only improves operational efficiency for policemen and police stations, but also provides service convenience for plaintiffs and lawyers. In recent years, the police IoT has rapidly developed and continuously improved.

Manuscript received Feb 26, 2024; This work is supported by the National Natural Science Foundation of China (62201204, 62172441, 62172438), the Natural Science Foundation of Hunan Province (2023JJ40168, 2023JJ30696), the Joint Funds for Railway Fundamental Research of National Natural Science Foundation of China (U2368201), Key Project of Shenzhen City Special Fund for Fundamental Research(JCYJ20220818103200002). (*Corresponding author: Xiaoheng Deng.*)

Hairong Lin and Xiaoheng Deng are with the School of Electronic Information, Central South University, Changsha 410083, China, and also with the Shenzhen Research Institute, Central South University, Shenzhen 518000, China (dxh@csu.edu.cn)

Fei Yu is with the School of Computer and Communication Engineering in Changsha University of Science and Technology, Changsha, 410114, China.

Yichuang Sun is with the School of Engineering and Computer Science, University of Hertfordshire, Hatfield AL10 9AB, U.K.

However, there are still security problems in the process of IoT data transmission and storage, which deserve serious consideration and attention. Currently, many researchers have currently proposed valuable solutions for the secure transmission of data in the police IoT environment [2, 3]. Nevertheless, they do not propose a specific secure transmission scheme for image data. Image data has the characteristics of a large amount of information and high visibility, so it is more vulnerable to security threats during transmission. Undoubtedly, a large number of crime scene images should be safely protected both in storage and transmission. If the data is leaked, it will seriously affect prisoners' privacy, social stability, and even national security. Thus, to ensure the security of image transmission, developing an image security solution applied in the police IoT is very significant. As we all know, for protecting image information, the commonest and simplest way is encryption, and its security level often depends on the secret key [4]. In general, the randomness of the secret key is higher, and the security of the encryption system is higher. Therefore, this issue can be tackled using memristive HNN-based image encryption among various encryption methods, and this is due to the complex chaos properties of memristive HNNs.

Artificial neural networks have been widely applied in various intelligent systems, such as robots, self-driving, and so on [5]. Over the past century, a variety of neural network models have been developed by simulating the network structure and working mechanism of the biological nervous systems [6]. Among them, the Hopfield neural network (HNN) is considered an ideal artificial neural network model for imitating brain's dynamic behaviors [7]. Since the HNN was proposed in 1982, it has rapidly developed and continuously improved. Various HNNs with different dynamical behaviors including chaos, hyperchaos, and coexisting behaviors have been designed and realized [8, 9], which has important implications for the development of artificial intelligence.

In 2008, Hewlett-Packard lab reported a novel electronic device, named memristor [10]. The memristor has many unique features like nanoscale, adjustability, strong nonlinearity, and memory function, which has been employed in various fields [11, 12]. In particular, it can be used to construct memristive neural networks due to its memory function and magnetic flux characteristics [13, 14]. Due to the introduction of memristors, memristive neural networks become closer to practical biological nervous systems and have many advantages in various applications. For example, the memristor's memory function makes the memristive neural network largely improve the ability to learn [15]. A memristive neural network circuit has high integration and low power because of the memristor's nanoscale size. Moreover, the memristive neural networks can also be

applied to various artificial intelligence systems such as online learning, medical diagnosis, and information security [16, 17]. Especially, the memristive HNNs can produce complex dynamical behaviors closer to the brain than the traditional HNNs [18, 19], which is of great significance for understanding brain function and developing intelligent systems.

In recent years, many memristive HNNs with complex dynamical behaviors have been designed by three modeling methods. The first modeling method is that using memristors to emulate neural synapses [20]. For instance, employing two memristors to emulate two self-connection synapses, a bi-neuron memristive HNN with initial coexisting behaviors was proposed in [21]. Adopting the same modeling method, grid multi-scroll attractors have been revealed in a memristive HNN [22]. The second modeling approach uses memristors to represent magnetic coupling. For example, applying a memristor to coupling two neural networks, a memristive HNN with zero-Hopf bifurcation dynamics was constructed [23]. The third modeling method is that employing memristors to describe the electromagnetic induction effect. In [24], a scroll-growth and scroll-control memristive HNN with two neurons was modeled by using a memristor to describe the effect of electromagnetic radiation. Based on a similar modeling approach, coexisting multi-scroll attractors [25] and symmetric multi-scroll attractors [26] have been found in memristive HNNs. Recently, the study of the memristive HNNs by considering different modeling methods has attracted much attention [27]. Especially, a novel memristive HNN with extreme multistability was proposed by synchronously considering the first and third modeling methods [28]. Similarly, in [29], synthesizing the second and third methods, a memristive HNN with complex dynamics was constructed. However, the case of simultaneously considering the three modeling mechanisms in a neural network has not been investigated until now.

Chaotic systems have extensive applications in cryptography because of their ability to generate pseudo-random signal [30, 31]. Chaotic signal is a natural random signal with ergodicity, unpredictability, and sensitivity to initial states, which can be employed to produce pseudo-random numbers in information encryption [32]. Over the past decades, various chaotic systems have been designed to implement cryptosystems [33, 34]. The research results show that the cryptosystem based on chaos has the advantages of simple structure, fast encryption speed and high security [35, 36]. Chaotic memristive HNNs have important applications for data encryption in information transmission [37, 38], which has attracted increasing attention from many scholars and engineers. For example, in [39], a hyperchaotic memristive HNN was used to encrypt medical image data. Similarly, a ring memristive HNN with complex chaos was applied to WBAN [40]. Recently, because multi-scroll chaotic signals have more complex dynamical behaviors and greater randomness [41], the multi-scroll memristive HNNs are considered to have more advantages in information protection. In particular, in [42], a privacy protection scheme applied in medical IoT was designed and implemented, in which the key is generated by a grid multi-scroll memristive HNN. Furthermore, based on a hyperchaotic multi-scroll memristive HNN, an encryption communication solution is successfully designed to protect commercial data [43]. Undoubtedly, these applications show the great potential of memristive HNNs in information security.

Based on the previous work, it is clear that chaotic memristive neural networks can solve many image encryption problems. Although these efforts yielded interesting results, the security

of the encryption methods still needs to be further improved, especially the dynamic complexity of neural networks. In this article, a new memristive HNN with three memristive systems is proposed by synthetically considering three modeling methods. Analysis results show that different from previously reported memristive HNNs, the presented memristive HNN has expandable plane equilibrium points dependent on control parameters. Such a unique property enables the memristive HNN to exhibit control parameters-related dynamical behaviors including controllable 1D multi-butterfly chaotic attractors and grid multi-butterfly chaotic attractors. To our knowledge, this is the first time that the grid multi-butterfly chaotic attractors have been found in HNNs. Furthermore, the proposed memristive HNN can generate plane coexisting infinitely many multi-butterfly chaotic attractors. This is an initial-boosted plane coexisting behavior, which is very important for many chaos-based engineering applications, and the existing HNNs do not have this property. Compared with the multi-scroll attractors, the multi-butterfly attractors have more complex dynamical trajectories, higher randomness, and more secret key parameters [44, 45]. Therefore, based on the constructed grid multi-butterfly memristive HNN, we design an image security solution in police IoT. Encryption performance analysis shows the designed security solution has high security. Finally, we develop a hardware test platform to demonstrate the security solution.

The main novelty and contributions of this article are summarized as follows. 1) Present a novel memristive HNN model based on three modeling methods with the possibility of chaotic butterfly attractors in its dynamics. 2) Grid multi-butterfly attractors and initial-boosted plane coexisting multi-butterfly attractors are revealed first in the HNNs. 3) Based on the proposed grid multi-butterfly memristive HNN model, design a permutation-diffusion encryption scheme for image data encryption. 4) The design scheme is exploited for secure crime scene images for potential application in the field of police IoT. 5) Experimentally analyze and validate the security of the designed image security solution to ensure that it is suitable for the specified application.

The rest of this paper is organized as follows. Sect.II constructs a new grid multi-butterfly memristive HNN with three memristive systems. Sect.III studies the dynamical behaviors of the grid multi-butterfly memristive HNN. Sect.IV designs an image security solution applied in police IoT based on the grid multi-butterfly memristive HNN and its security performances are experimentally analyzed and demonstrated. Sect.V concludes this paper.

## II. MEMRISTIVE HOPFIELD NEURAL NETWORK

In this section, two novel flux-controlled memristor models are designed first. Then a memristive HNN with three memristive systems is proposed. Finally, its equilibrium point characteristics are analyzed.

### A. Memristor Model Design

According to the modeling method of the memristor [11], two new flux-controlled memristor models are designed **as follows**

$$\begin{cases} i = W_1 v = \alpha(\varphi_1^2 + \varphi_1 - \beta)v \\ d\varphi_1/dt = ((\tanh(v))^2 - 1)\varphi_1 + \tanh(v) \end{cases} \quad (1)$$

$$\begin{cases} i = W_2 v = \mu xv \\ dx/dt = \varepsilon v - \sigma f \end{cases} \quad (2)$$

where

$$f = \begin{cases} x - \text{sgn}(x), N = 0 \\ x - \left( N + \text{sgn}(x) + \sum_{i=1}^N \text{sgn}(x - 2i) \right), N = 1, 2, 3, \dots \end{cases} \quad (3)$$

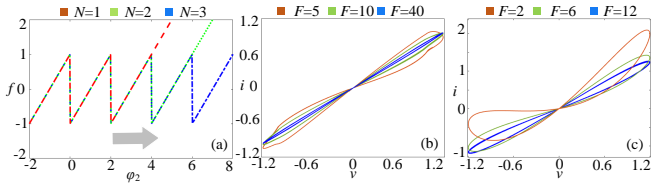


Fig. 1: Characteristics of the two memristors. (a) The curve of the function  $f$  under different control parameter values. (b) Frequency-relied pinched hysteresis loops of the memristor in (1). (c) Frequency-relied pinched hysteresis loops of the memristor in (2).

where  $v$  and  $i$  are voltage and current, respectively,  $\phi_1$  and  $x$  are internal state variables of the two memristors,  $W_1$  and  $W_2$  are the memductance functions, as well as  $\alpha$ ,  $\beta$ ,  $\mu$ ,  $\varepsilon$ , and  $\sigma$  are memristor parameters. The function  $f$  is described by Eq.(3), which can be adjusted by changing the control parameter  $N$ , as shown in Fig.1(a). Unlike previous piecewise-linear memristors in [20, 22], the designed memristor in Eq.(2) has only one control parameter.

The frequency-relied voltage-current ( $v$ - $i$ ) feature of the two memristors is analyzed under sinusoidal voltage  $v=Asin(Ft)$  with  $A \in (0, 10)$ . For the equation (1), setting memristor parameters  $\alpha=-1$ ,  $\beta=1$ , and initial state  $\phi_{10}=0$ , signal amplitude  $A=1.2$ , when  $F=(5, 10, 40)$ , the frequency-relied  $v$ - $i$  loci are plotted in Fig.1(b). As can be seen, the  $v$ - $i$  loci exhibit three pinched hysteresis loops. Furthermore, as the frequency increases, the area of the pinched hysteresis loop decreases gradually, which means that Eq.(1) is a memristor model. For Eq.(2), setting  $\mu=1$ , and  $\varepsilon=2.2$ ,  $\sigma=2$ ,  $N=2$ , and initial state  $x_0=0$ ,  $A=1.2$ , when  $F=(2, 6, 12)$ , the frequency-relied  $v$ - $i$  loci are plotted in Fig.1(c). Similarly, the  $v$ - $i$  loci exhibit three pinched hysteresis loops, which shows that Eq.(2) is a memristor model.

### B. Memristive HNN Description

HNN is kind of excellent artificial neural network model which can simulate complex chaotic behaviors of the human brain. Generally, the mathematical model of the original HNN with  $n$  neurons can be expressed by [7]

$$C_i \dot{x}_i = -x_i/R_i + \sum_{j=1}^n w_{ij} \tanh(x_j) + I_i \quad (i, j \in N^*) \quad (4)$$

where  $x_i$ ,  $C_i$ ,  $R_i$ , and  $I_i$  are respectively membrane potential, membrane capacitor, membrane resistor, and external stimulate current of neuron  $i$ .  $w_{ij}$  is the synaptic weight coefficient from neuron  $j$  to neuron  $i$ . Additionally,  $\tanh(\cdot)$  represents the neuron activation function. Based on the original HNN in Eq.(4), by setting  $C_1=C_2=1$ ,  $R_1=R_2=1$ ,  $I_1=I_2=0$ ,  $w_{11}=0$ ,  $w_{12}=1$ ,  $w_{21}=-1.5$ , and  $w_{22}=2$ , a novel bi-neuron HNN is constructed as follows

$$\begin{cases} \dot{x}_1 = -x_1 + \tanh(x_2) \\ \dot{x}_2 = -x_2 - 1.5 \tanh(x_1) + 2 \tanh(x_2) \end{cases} \quad (5)$$

A memristor is an ideal bionic electronic element due to its special nonlinearity, memory function, and flux feature. In neural network modeling, the memristor is often used to mimic neural synapses, to represent magnetic coupling, or to describe the electromagnetic induction effect. Based on these modeling theories, a new memristive HNN is proposed by simultaneously introducing three memristors into the constructed bi-neuron HNN. As shown in Fig.2, in the proposed memristive HNN model, the memristor  $M_1$  is used to emulate the self-connection synapse of neuron 2, the memristor  $M_2$  is used to represent the magnetic coupling between neuron 1 and neuron 2, and the memristor  $M_3$  is used to describe external electromagnetic

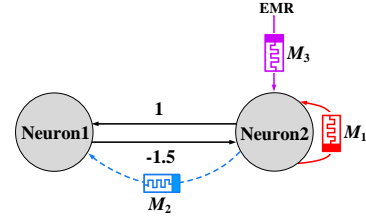


Fig. 2: Structure of the memristive HNN with three memristive systems

induction effect of neuron 2. Because the three memristors play different roles in the bi-neuron HNN, which means that the proposed memristive HNN has three memristive systems. Here, the memristor  $M_1$  is realized by using the model in Eq.(1), and the memristors  $M_2$  and  $M_3$  are implemented using the model in Eq.(2). As a result, the memristive HNN with three memristive systems can be expressed by

$$\begin{cases} \dot{x}_1 = -x_1 + \tanh(x_2) + k_2(x_1 - x_2)W_2 \\ \dot{x}_2 = -x_2 - 1.5 \tanh(x_1) + k_1 W_1 \tanh(x_2) - k_2(x_1 - x_2)W_2 + k_3 x_2 W_3 \\ \dot{\phi}_1 = (x_2^2 - 1)\phi_1 + x_2 \\ \dot{\phi}_2 = \varepsilon_1(x_1 - x_2) - \sigma_1 f_1 \\ \dot{\phi}_3 = \varepsilon_2 x_2 - \sigma_2 f_2 \end{cases} \quad (6)$$

where  $k_1$ ,  $k_2$ , and  $k_3$  are three memristive coupling coefficients that denote coupling strength between the neural network and the three memristors.  $\sigma_1$  and  $\sigma_2$  are memristor parameters.

### C. Equilibrium Point Characteristic

The distribution and stability of the equilibrium points of the memristive HNN in Eq.(6) are analyzed by using theoretical and numerical analysis methods. Assuming the equilibrium point set of the memristive HNN is described by  $E=(x_1^*, x_2^*, \phi_1^*, \phi_2^*, \phi_3^*)$ , it can be solved by Eq.(7).

$$\begin{cases} -x_1^* + \tanh(x_2^*) + k_2(x_1^* - x_2^*)W_2 = 0 \\ -x_2^* - 1.5 \tanh(x_1^*) + k_1 W_1 \tanh(x_2^*) - k_2(x_1^* - x_2^*)W_2 + k_3 x_2^* W_3 = 0 \\ (x_2^{*2} - 1)\phi_1^* + x_2^* = 0 \\ \varepsilon_1(x_1^* - x_2^*) - \sigma_1 f_1 = 0 \\ \varepsilon_2 x_2^* - \sigma_2 f_2 = 0 \end{cases} \quad (7)$$

Further simplification leads to

$$\begin{cases} x_2^* = (\sigma_2/\varepsilon_2)f_2 \\ x_1^* = x_2^* + (\sigma_1/\varepsilon_1)f_1 \\ \phi_1^* = x_2^*/(1-x_2^{*2}) \\ F_1(\phi_3^*, \phi_2^*) = -x_1^* + \tanh(x_2^*) + k_2(x_1^* - x_2^*)W_2 \\ F_2(\phi_3^*, \phi_2^*) = -x_2^* - 1.5 \tanh(x_1^*) + k_1 W_1 \tanh(x_2^*) - k_2(x_1^* - x_2^*)W_2 + k_3 x_2^* W_3 \end{cases} \quad (8)$$

Clearly, the solutions of  $\phi_3^*$  and  $\phi_2^*$  are determined by the functions  $f_1$  and  $f_2$ , respectively. That is to say, the number and position of the equilibrium points are dependent on the control parameters  $N_1$  and  $N_2$ . Taking  $N_1=N_2=1$  as an example, when  $k_1=0.34$ ,  $k_2=0.1$ ,  $k_3=0.15$ ,  $\alpha=-0.25$ ,  $\beta=60$ ,  $\mu=0.1$ ,  $\varepsilon_1=\varepsilon_2=2.2$ ,  $\sigma_1=4.3$ ,  $\sigma_2=5$ , the distribution of the equilibrium points on the  $\phi_3$ - $\phi_2$  plane can be given by plotting the function curves  $F_1$  and  $F_2$ , as shown in Fig.3. Noted that we used the ezplot function in the above calculation process. As we can see from Fig.3, under this condition, the memristive HNN has plane equilibrium points which can be divided into four types  $E_1$ - $E_4$ . Numerical analyses show that  $E_1$  and  $E_2$  are unstable saddle points and stable focus points, respectively. The two kinds of equilibrium points can generate a self-excited chaotic attractor labeled by the dotted coil on the left in Fig.3. Furthermore, both  $E_3$  and  $E_4$  are unstable saddle points that plays a role in connecting two chaotic attractors. Namely, the equilibrium points are synchronously extended along  $\phi_3$  and  $\phi_2$  directions



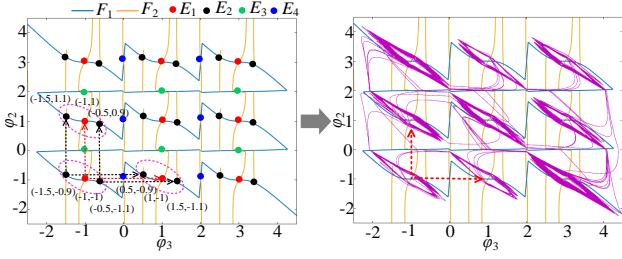


Fig. 3: Distribution of the equilibrium points of the memristive HNN with  $N_1=N_2=1$  and the generated  $3 \times 3$  grid chaotic attractor.

labeled by the dotted line in Fig.3. Consequently, with the increase of control parameters  $N_1$  and  $N_2$ , the equilibrium points will be extended on the  $\varphi_3$ - $\varphi_2$  plane. Obviously, the increase of the control parameters  $N_1$  and  $N_2$  in the system leads to the extension of the equilibrium points, which can generate the phenomenon of grid chaotic attractor reconstruction, as shown in the right of Fig.3 with the initial values (0.1, 0.1, 0.1, 0.1, 0.1). Further analysis shows that the number of equilibrium points  $E_1$  is equal to  $(N_1+2) \times (N_2+2)$ , which means that the memristive HNN can generate a  $(N_1+2) \times (N_2+2)$  grid attractors.

### III. DYNAMIC ANALYSIS

This section analyzes the chaotic dynamical behaviors of the proposed memristive HNN by using numerical simulation methods such as bifurcation diagrams, Lyapunov exponents (LEs), phase plots, basin of attraction, and time series. Note that Matlab ode45 algorithm with a time-step of 0.02 is adopted in numerical simulation. Some parameter values are fixed as  $\alpha=0.25$ ,  $\beta=60$ ,  $\mu=0.1$ ,  $\sigma_1=4.3$ ,  $\sigma_2=5$ ,  $x_{10}=x_{20}=\varphi_{10}=0.1$ .

#### A. Periodic and Chaotic Butterfly Attractors

Firstly, the dynamical behaviors of the memristive HNN under  $\varepsilon_1=\varepsilon_2=1.2$ ,  $N_1=N_2=0$ , and  $\varphi_{20}=\varphi_{30}=0.1$  are analyzed by taking the three memristive coupling coefficients  $k_1$ ,  $k_2$  and  $k_3$  as variable parameters. Setting  $k_1=0.34$ ,  $k_2=0.1$ , and  $k_3=0.15$ , when any two parameters are fixed, the dynamical behavior related to the third parameter can be investigated. Based on this method, the bifurcation diagrams related to  $k_1$ ,  $k_2$  and  $k_3$ , and corresponding LEs are plotted in Fig.4. From Fig.4, the memristive HNN exhibits different dynamical behaviors highly dependent on the three memristive coupling coefficients. Interestingly, in Fig.4(a), with the increase of  $k_1$  from 0 to 1, the memristive HNN begins unbounded behavior, then enters into stable chaotic behavior through a forward period-doubling bifurcation route. On the contrary, in Fig.4(b) and (c), with the increase of  $k_2$  and  $k_3$ , the proposed memristive HNN model begins chaotic behavior, then degenerates to a periodic state by multiple reverse period-doubling bifurcation routes. More interestingly, these dynamical behaviors have complex dynamical trajectories exhibiting the Lorenz-type butterfly-shaped attractors. As shown in Fig.5, various chaotic and periodic butterfly attractors are obtained from the memristive HNN by selecting different memristive coupling coefficients. Among them, chaotic double-butterfly attractor, forward chaotic butterfly attractor, reversed chaotic butterfly attractor, periodic butterfly attractor, transient chaotic double-butterfly attractor, and periodic butterfly attractor are obtained as shown in Fig.5(a)-(f), respectively. Therefore, under the influence of the three memristive systems, the proposed memristive HNN generates complex periodic, transient chaotic, and chaotic butterfly and double-butterfly attractors.

#### B. 1D and Grid Multi-butterfly Attractors

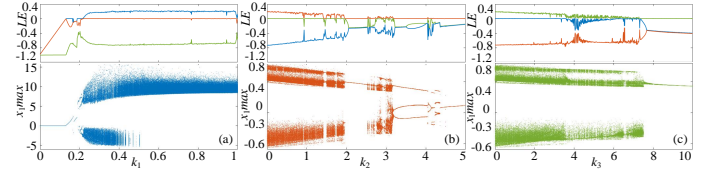


Fig. 4: The memristive coupling parameters-relied dynamical behaviors depicted by bifurcation diagrams and Lyapunov exponents. (a)  $k_2=0.1$ ,  $k_3=0.15$ . (b)  $k_1=0.34$ ,  $k_3=0.15$ . (c)  $k_1=0.34$ ,  $k_2=0.1$ .

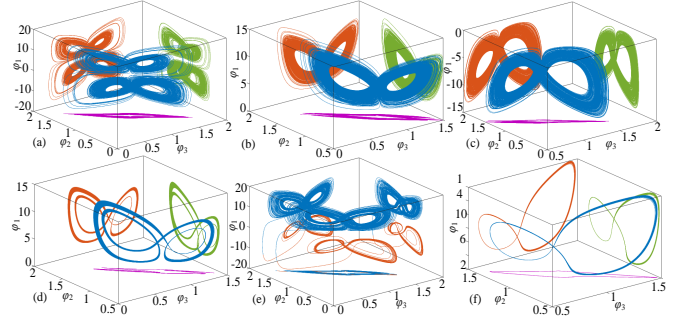


Fig. 5: Complex dynamical behaviors depicted by 3D phase plot in  $\varphi_3$ - $\varphi_2$ - $\varphi_1$  space. (a) Chaotic double-butterfly attractor with  $k_1=0.34$ ,  $k_2=0.1$ , and  $k_3=0.15$ . (b) Forward chaotic butterfly attractor with  $k_1=0.7$ ,  $k_2=0.1$ , and  $k_3=0.15$ . (c) Reversed chaotic butterfly attractor with  $k_1=0.34$ ,  $k_2=2.8$ , and  $k_3=0.15$ . (d) Periodic butterfly attractor with  $k_1=0.34$ ,  $k_2=2.9$ , and  $k_3=0.15$ . (e) Transient chaotic double-butterfly attractor with  $k_1=0.34$ ,  $k_2=0.1$ , and  $k_3=4.8$ . (f) Periodic butterfly attractor with  $k_1=0.34$ ,  $k_2=0.1$ , and  $k_3=9$ .

Next, the dynamical behaviors of the memristive HNN under  $k_1=0.34$ ,  $k_2=0.1$ ,  $k_3=0.15$ , and  $\varphi_{20}=\varphi_{30}=0.1$  are analyzed by taking the system parameters  $\varepsilon_1$ ,  $\varepsilon_2$  and control parameters  $N_1$ ,  $N_2$  as variable parameters. When setting  $\varepsilon_1=2.2$ ,  $\varepsilon_2=1.2$ , and  $N_2=0$ , the control parameter  $N_1$  is increased from 0 to 7, the bifurcation diagram of the state variable  $\varphi_2$  and the corresponding LEs are plotted in Fig.6(a). Fig.6(a) shows that with the increase of parameter  $N_1$ , the double-butterfly attractor is reconstructed along  $\varphi_2$  direction to generate a multi-butterfly chaotic attractor. Also, the number of butterflies contained in multi-butterfly chaotic attractors can be freely controlled by adjusting  $2(N_1+2)$ . It should be noted that the number of butterflies seen in Fig.6 is  $(N_1+2)$  or  $(N_2+2)$  because this multi-butterfly attractor is double-layered. As shown in Fig.7, different numbers of multi-butterfly attractors are generated from the memristive HNN under different control parameters  $N_1$ . On the contrary, when setting  $\varepsilon_1=1.2$ ,  $\varepsilon_2=2.2$ , and  $N_1=0$ , the control parameter  $N_2$  is increased from 0 to 7, the bifurcation diagram of the state variable  $\varphi_3$  and the corresponding LEs are plotted in Fig.6(b). Under this condition, the memristive HNN can generate any number of multi-butterfly attractors along  $\varphi_3$  direction, as shown in Fig.8. Amazingly, when setting  $\varepsilon_1=\varepsilon_2=2.2$ , by selecting different control parameters  $N_1$  and  $N_2$ , the arbitrary number of grid multi-butterfly chaotic attractors can be observed in the memristive HNN, as shown in Fig.9. Such complex dynamical behavior has not been found in previous neural network models. Moreover, the number of the grid multi-butterfly attractors can be computed by  $(N_1+2) \times (N_2+2)$ . Consequently, the proposed memristive HNN can not only produce 1D multi-butterfly attractors but also grid multi-butterfly attractors.

#### C. Initial-Boosted Plane Coexisting Multi-butterfly attractors

Finally, the dynamical behaviors of the memristive HNN under  $k_1=0.34$ ,  $k_2=0.1$ ,  $k_3=0.15$ , and  $N_1=N_2=2$  are analyzed by taking the initial states  $\varphi_{20}$  and  $\varphi_{30}$  as variable parameters.

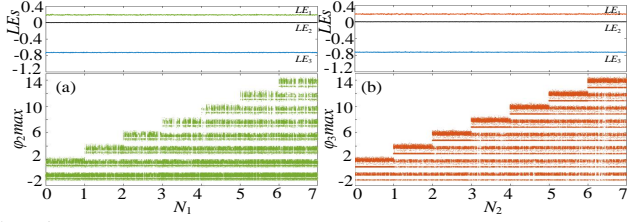


Fig. 6: The control parameters-relied dynamical behaviors depicted by bifurcation diagrams and Lyapunov exponents. (a)  $\varepsilon_1=2.2$ ,  $\varepsilon_2=1.2$ ,  $N_2=0$ . (b)  $\varepsilon_1=1.2$ ,  $\varepsilon_2=2.2$ ,  $N_1=0$ .

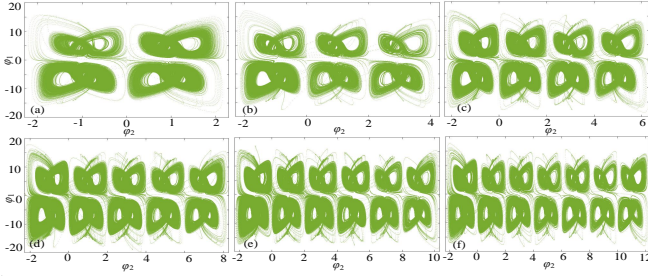


Fig. 7:  $\varphi_2$ -direction multi-butterfly attractors under  $\varepsilon_1=2.2$ ,  $\varepsilon_2=1.2$ ,  $N_2=0$ . (a) 2-double-butterfly attractor with  $N_1=0$ . (b) 3-double-butterfly attractor with  $N_1=1$ . (c) 4-double-butterfly attractor with  $N_1=2$ . (d) 5-double-butterfly attractor with  $N_1=3$ . (e) 6-double-butterfly attractor with  $N_1=4$ . (f) 7-double-butterfly attractor with  $N_1=5$ .

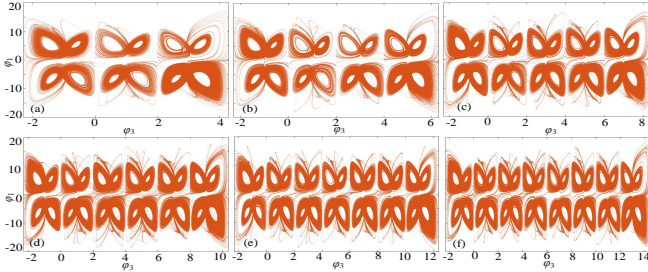


Fig. 8:  $\varphi_3$ -direction multi-butterfly attractors under  $\varepsilon_1=1.2$ ,  $\varepsilon_2=2.2$ ,  $N_1=0$ . (a) 3-double-butterfly attractor with  $N_2=1$ . (b) 4-double-butterfly attractor with  $N_2=2$ . (c) 5-double-butterfly attractor with  $N_2=3$ . (d) 6-double-butterfly attractor with  $N_2=4$ . (e) 7-double-butterfly attractor with  $N_2=5$ . (f) 8-double-butterfly attractor with  $N_2=6$ .

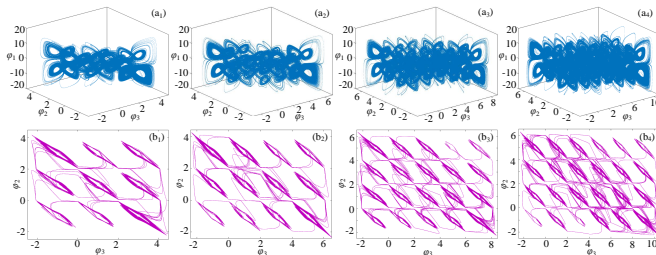


Fig. 9: Grid multi-butterfly attractors under  $\varepsilon_1=2.2$  and  $\varepsilon_2=2.2$ . (a1) (b1) 3 $\times$ 3-double-butterfly attractor with  $N_1=N_2=1$ . (a2) (b2) 4 $\times$ 3-double-butterfly attractor with  $N_1=2$  and  $N_2=1$ . (a3) (b3) 5 $\times$ 4-double-butterfly attractor with  $N_1=3$  and  $N_2=2$ . (a4) (b4) 6 $\times$ 4-double-butterfly attractor with  $N_1=4$  and  $N_2=2$ .

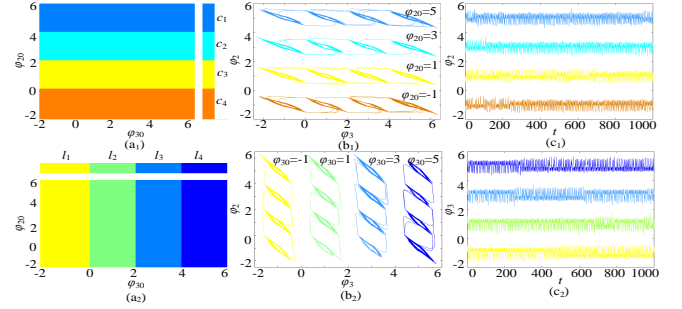


Fig. 10: Initial state-relied chaotic dynamics. (a1) Basin of attraction on the  $\varphi_{30}$ - $\varphi_{20}$  plane under  $\varepsilon_1=1.2$ ,  $\varepsilon_2=2.2$ . (b1) Coexisting four 4-butterfly attractors on  $\varphi_2$  direction. (c1) Coexisting four chaotic sequences on  $\varphi_3$  direction. (a2) Basin of attraction on the  $\varphi_{30}$ - $\varphi_{20}$  plane under  $\varepsilon_1=2.2$ ,  $\varepsilon_2=1.2$ . (b2) Coexisting four 4-butterfly attractors on  $\varphi_3$  direction. (c2) Coexisting four chaotic sequences on  $\varphi_3$  direction.

When setting  $\varepsilon_1=1.2$ ,  $\varepsilon_2=2.2$ , we plot the local basin of attraction on the  $\varphi_{30}$ - $\varphi_{20}$  plane, as shown in Fig.10(a1). As can be seen, the local basin of attraction has complicated manifold structures and clear basin boundaries, and the color-painted indicates different attracting regions of dynamical behaviors. When setting  $\varphi_{30}=1$ , by selecting different  $\varphi_{20}$  as -1, 1, 3, and 5, coexisting four 4-double-butterfly attractors can be found from the memristive HNN, as shown in Fig.10(b1). That is to say, the memristive HNN generates coexisting multi-butterfly attractors. Meanwhile, four chaotic sequences with different positions can be obtained as shown in Fig.10(c1), which means that their oscillating amplitudes can be non-destructively adjusted by switching the initial state  $\varphi_{20}$ . Adopting the same analysis method, setting  $\varepsilon_1=2.2$ ,  $\varepsilon_2=1.2$ , the local basin of attraction on the  $\varphi_{30}$ - $\varphi_{20}$  plane is plotted as shown in Fig.10(a2). By setting  $\varphi_{20}=1$ , by selecting different  $\varphi_{30}$  as -1, 1, 3, and 5, coexisting four 4-double-butterfly attractors generated by the memristive HNN and corresponding four chaotic sequences are given in Fig.10(b2) and (c2), respectively. Obviously, the memristive HNN model exhibits initial-boosted coexisting multi-butterfly attractors.

In addition, as shown in Fig.11(a), when keeping the above parameters unchanged except for  $k_1=0.7$ ,  $\varepsilon_1=\varepsilon_2=2.2$ , the basin of attraction shows wonderful grid structures including squares of the same size. Each square indicates an attracting region of a kind of dynamical behavior. By selecting different initial states  $\varphi_{20}=(-1, 1, 3, 5)$  and  $\varphi_{30}=(-1, 1, 3, 5)$ , plane coexisting 16 butterfly attractors can be observed from the memristive HNN, as shown in Fig.11(b). Further simulation shows that when continuing to increase the values of  $N_1$  and  $N_2$ , the number of the plane coexisting attractors finally tends to infinity under different initial states. That is to say, the memristive HNN can provide sustained and robust chaotic sequences and their oscillating amplitudes can be non-destructively adjusted in two directions by switching the initial states. Additionally, keeping the above parameter value unchanged, when changing  $k_1=0.34$  or  $k_3=9$ , the memristive HNN can generate plane coexisting double-butterfly attractors and plane coexisting periodic attractors, as shown in Fig.11(c) and (d), respectively. Thus, the proposed memristive HNN exhibits complex initial-boosted plane coexisting multi-butterfly attractors.

To sum up, under the influence of the three memristive systems, the proposed memristive HNN can generate abundant multi-butterfly chaotic attractors including  $\varphi_2$ -direction multi-butterfly attractors,  $\varphi_3$ -direction multi-butterfly attractors, grid multi-butterfly attractors, and plane coexisting multi-butterfly



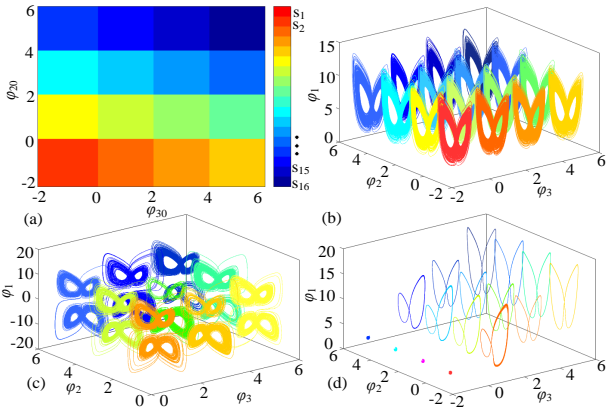


Fig. 11: Initial-boosted plane coexisting behaviors under  $\varepsilon_1=\varepsilon_2=1.2$ . (a) Basin of attraction on the  $\varphi_{30}$ - $\varphi_{20}$  plane. (b) Plane coexisting 16 butterfly attractors under  $k_1=0.7$ . (c) Plane coexisting 9 double-butterfly attractors under  $k_1=0.34$ . (d) Plane coexisting 12 periodic attractors and 4 stable points under  $k_1=0.34$  and  $k_3=9$ .

TABLE I: RELATIONSHIP BETWEEN SYSTEM PARAMETERS, CONTROL PARAMETERS, AND DYNAMICAL BEHAVIORS.

$\varepsilon_1$	$\varepsilon_2$	Dynamical behaviors	Number of butterflies
2.2	1.2	$\varphi_2$ -direction multi-butterfly attractors	$2(N_1+2)$
1.2	2.2	$\varphi_3$ -direction multi-butterfly attractors	$2(N_2+2)$
2.2	2.2	Grid multi-butterfly attractors	$2(N_1+2)(N_2+2)$
1.2	1.2	Plane coexisting multi-butterfly attractors	$2(N_1+2)(N_2+2)$

attractors. More importantly, the number of butterflies of the multi-butterfly attractors can be easily controlled by adjusting control parameters  $N_1$  or  $N_2$ , as shown in Table I.

#### IV. APPLICATION IN THE POLICE IOT

With the rapid development of wireless communication technology, the Internet of Things (IoT) has been widely applied in the police system [1, 2]. Although the use of the police IoT makes the work of policemen and judges more efficient and convenient, it also brings the risk of information leakage to the handling of cases. Especially, a large number of crime scene images are easily leaked during network processing and transmission, which undoubtedly increases the difficulty of case detection and criminal tracking, and may even lead to public security incidents. Therefore, the security of crime scene image data is extremely important. Because the data of the crime scene images have special features, such as large capacity, high redundancy, and high correlation between pixels, the traditional encryption methods cannot fulfill the demands for image encryption [46]. Here we propose an image security solution based on a grid multi-butterfly memristive HNN to protect the privacy information of the crime scene images in police IoT.

##### A. Security Solution for The Police IoT

The security solution of the police IoT is designed as shown in Fig.12 which mainly contains four parts: Encryption terminal, MEC (Mobile edge computing) servers, Decryption terminal, and Pseudo-random number generator. When the police station  $PS-n$  obtains crime scene image data (Original images), the image data is encrypted through a chaos-based encryption algorithm at the encryption terminal. Usually, the chaotic encryption algorithm is preinstalled on the local server of both the encryption and decryption ends. That is to say, when the encryption terminal receives both the original images and the secret keys, its local server will perform the encryption operation. Then the encrypted data (Cipher images) is sent online to the nearest MEC server, and the encrypted data is further sent to other

MEC servers or the PSs. Once other police stations receive both the cipher image data and the secret keys, the corresponding local server will perform the decryption operation. As we can see in Fig.12, the original crime scene images can be obtained through chaotic decryption in the  $PS-m$  (decryption terminal), so as to realize the confidential transmission of the crime scene images. In these processes, the key step is the implementation of chaos-based encryption and decryption algorithms. Here, as shown in Fig.13, an encryption algorithm with a permutation-diffusion structure is designed based on the proposed grid multi-butterfly memristive HNN. In the encryption application, the grid multi-butterfly memristive HNN is used to generate chaotic sequences with grid multi-butterfly attractors or initial-boosting dynamics. Then the generated chaotic sequences are used to produce pseudo-random numbers which are applied to encrypt image data. The specific implementation steps are as follows:

Step 1: Assume that the size of the original image  $P$  is  $M \times N$  pixels. Considering the parameters and initial values ( $\alpha$ ,  $\beta$ ,  $\mu$ ,  $\varepsilon_1$ ,  $\varepsilon_2$ ,  $\lambda_1$ ,  $\lambda_2$ ,  $k_1$ ,  $k_2$ ,  $k_3$ ,  $N_1$ ,  $N_2$ ,  $x_{10}$ ,  $x_{20}$ ,  $\varphi_{10}$ ,  $\varphi_{20}$ , and  $\varphi_{30}$ ) as secret keys, iterate the grid multi-butterfly memristive HNN in Eq.(6) with the fourth-order Runge-Kutta algorithm with sampling interval 0.02. Each iteration will produce five chaotic values  $x_1(i)$ ,  $x_2(i)$ ,  $\varphi_1(i)$ ,  $\varphi_2(i)$  and  $\varphi_3(i)$ . Discard the data of the first 500 iterations of the system.

Step 2: The system is continuously iterated  $M \times N + 500$  times. Meanwhile, the produced chaotic values are used to generate two pseudo-random sequences  $S_1(i)$  and  $S_2(i)$ , as follows

$$\begin{cases} S_1(i) = Abs((x_1(i) + x_2(i))/2) \\ S_2(i) = mod(floor((Abs(\varphi_1(i)) \\ + Abs(\varphi_2(i)) + Abs(\varphi_3(i)))/3) \times 10^{15}), 256) \end{cases} \quad (9)$$

where the floor( $x$ ) denotes the nearest integers less than or equal to  $x$ .

Step 3: A processed image  $P_1$  is obtained by using the pseudo-random sequence  $S_1$  to perform a permutation to the original image  $P$ , where the permutation algorithm is described by

$$P_1(i) = P(index(S_1(i))) \quad (10)$$

Step 4: Employ the pseudo-random sequence  $S_2$  to perform the XOR operation to  $P_1$  as follows

$$C(i) = P_1(i) \oplus S_2(i) \quad (11)$$

Step 5: Perform the above encryption processes for  $n$  rounds. Consequently, the cipher image  $C$  is yielded. Decryption is the reverse process of the encryption operation.

##### B. Security Performance Analysis

The security performance of the designed encryption algorithm is verified by using four grayscale  $256 \times 256$  crime scene images (Trail, Bullet hole, Shoeprint, and Fingerprint) in Fig.14(a1)-(a4) as encryption objects. Here, the number of encryption round is set as 2, where the signal generated by the  $5 \times 4$ -double-butterfly attractor in Fig.9(a3) is used in the first round of encryption and the signal generated by the plane coexisting double-butterfly attractors in Fig.11(c) is employed in the second round. All the parameters are the same as those given in Sec. III.

(1) Keyspace: The presented encryption algorithm uses 12 parameters and 5 initial values as its secret keys, which makes unauthorized decryption very difficult. Suppose that all bites adopt double-precision data, so the keyspace of the cryptosystem is  $(10^{16})^{17} = 10^{272} \approx 2^{816}$ . Therefore, the keyspace of the designed encryption algorithm is much larger than  $2^{100}$ , which shows that it has a strong ability to resist violent attacks.

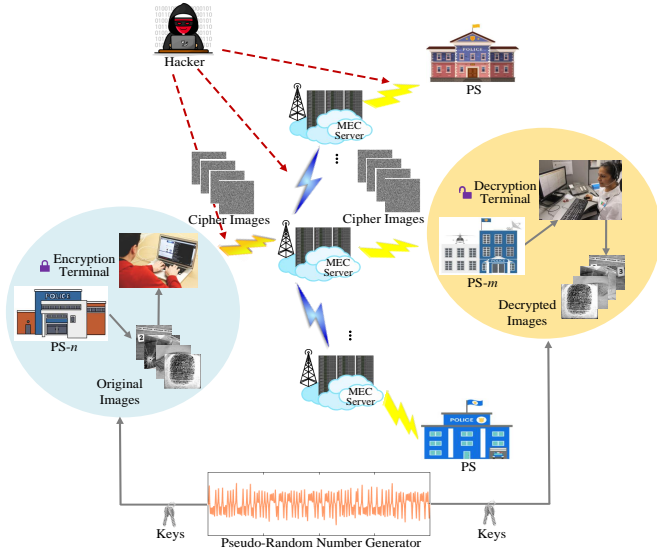


Fig. 12: Security framework of the police IoT.

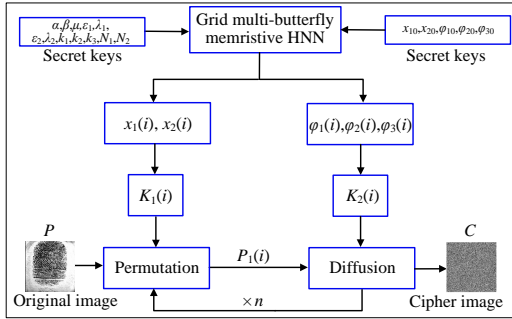


Fig. 13: Flow chart of the proposed image encryption algorithm.

(2) Histogram: The original images and corresponding cipher images are given in Fig.14(a1)-(a4) and Fig.14(c1)-(c4), respectively. It is evident that the cipher images become very chaotic after encryption. Meanwhile, their histograms are given in Fig.14(b1)-(b4) and Fig.14(d1)-(d4), respectively. Clearly, the histograms of the cipher images are very uniform and are completely different from those of the original images. Thus, the designed encryption algorithm provides a strong ability to resist statistical attacks.

(3) Correlation: The robustness of the encryption algorithm can be tested by computing correlation coefficients. Here, by randomly selecting 10000 pairs of adjacent pixels in the four original images and cipher images, the correlation coefficients in three directions are given in Fig.15. We can clearly see that the correlation coefficients of the original images are close to 1, but those of the cipher images are very close to 0. In other words, the designed encryption algorithm can largely reduce the correlation of the original images. Hence, the grid multi-butterfly memristive HNN provides strong robustness for the

TABLE II: TEST RESULTS OF THE ENTROPY, NPCR, UACI, AND TIME.

Images		Entropy	NPCR	UACI	Time
Trail	Original	7.1691	99.6068	33.4656	0.156
	Encrypted	7.9976			
Bullet hole	Original	7.6766	99.6039	33.4652	0.163
	Encrypted	7.9976			
Shoeprint	Original	6.9416	99.6108	33.3678	0.162
	Encrypted	7.9977			
Fingerprint	Original	7.4244	99.6082	33.4647	0.159
	Encrypted	7.9977			

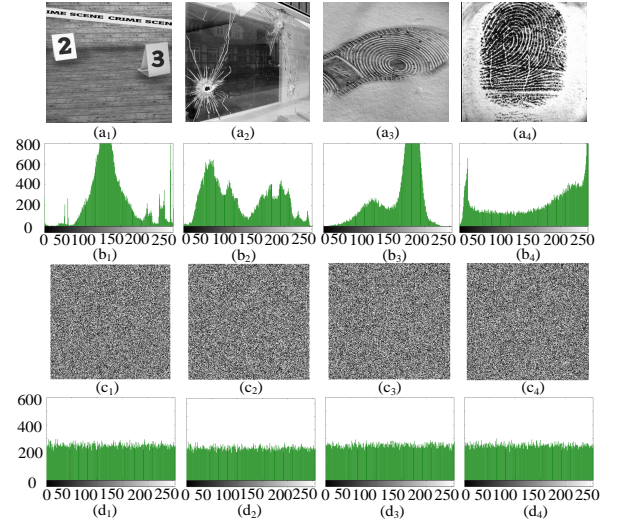


Fig. 14: Test results of the histograms. (a1-a4) Original images. (b1-b4) Histograms of the original images. (c1-c4) encrypted images. (d1-d4) Histograms of the cipher images.

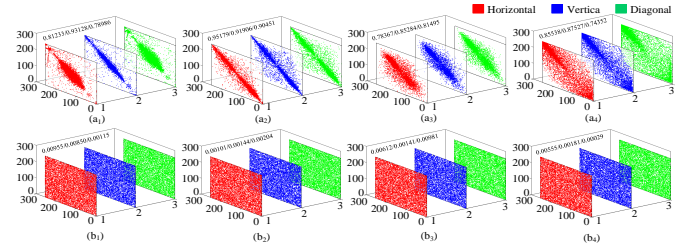


Fig. 15: Test results of the correlation. (a1-a4) Correlation of the original images. (b1-b4) Correlation of the corresponding cipher images.

encryption algorithm.

(4) Entropy: The statistical characteristics of image information can be reflected by entropy. According to Shannon's theorem, the entropy of an image should be as close to 8 as possible. Generally, the entropy can be calculated by

$$H(P) = \sum_{i=0}^{2^N-1} P(x_i) \log_2 \frac{1}{P(x_i)} \quad (12)$$

where  $N$  is the bit depth of the image  $P$  and  $P(x_i)$  is the probability of the presence of a pixel  $x_i$ . According to equation (12), the entropy of the four original images and cipher images are given in Table II. It is obvious that the entropy values of the original images are largely improved after encryption. The entropy values of the cipher images are very close to the ideal value 8. Therefore, the designed encryption algorithm has a strong ability to resist statistical attacks.

(5) NPCR and UACI: The ability of differential attacks can be evaluated by using the number of pixels change rate (NPCR) and the unified average change intensity (UACI). Assuming that there are two  $M \times N$  cipher images  $C_1$  and  $C_2$ , whose corresponding original images only have a single-pixel difference. The NPCR and UACI can be described by

$$\begin{cases} NPCR(C_1, C_2) = \sum_{i=1}^M \sum_{j=1}^N \frac{D(i,j)}{M \cdot N} \times 100\% \\ UACI(C_1, C_2) = \frac{1}{M \cdot N} \sum_{i=1}^M \sum_{j=1}^N \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \end{cases} \quad (13)$$

where

$$D(i, j) = \begin{cases} 0, & \text{if } C_1(i, j) = C_2(i, j) \\ 1, & \text{if } C_1(i, j) \neq C_2(i, j) \end{cases} \quad (14)$$

According to the above mathematical expressions, the average values of NPCR and UACI in four images are listed in Table



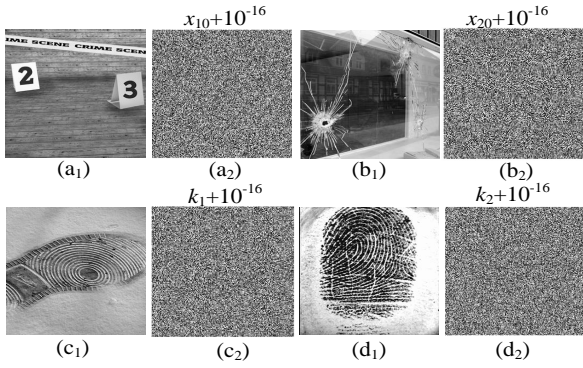


Fig. 16: Test results of key sensitivity. (a1-d1) Decrypted images with the accurate keys. (a2-d2) Decrypted images with inaccurate keys.

II. Evidently, the NPCR and UACI values are very close to the expected values of 99.6094% and 33.4635%, respectively. In other words, it is very sensitive to small changes in original images. Therefore, the designed encryption algorithm has a strong ability to oppose various differential attacks.

(6) Key Sensitivity: Usually, the more sensitive the secret keys, the more secure the encryption algorithm. Here, the secret keys  $x_{10}$ ,  $x_{10}$ ,  $k_1$ , and  $k_2$  are selected as test objects. First, the right secret keys are used to decrypt the cipher images. The decryption images are given in Fig.16(a1)-(d1), and the corresponding encryption time of the scheme is listed in Table. II. Then, the wrong secret keys with a tiny change are used for decrypting the same cipher images, and the decryption results are given in Fig.16(a2)-(d2). As can be seen, even if the secret key is changed a little ( $10^{-16}$ ), the decrypted image is absolutely different from the original image. As a consequence, the proposed encryption algorithm has a very high sensitivity to the secret key.

(7) Robustness: The robustness of the encryption scheme can also be evaluated by testing the opposing ability of data loss and noise attacks. To test the algorithm's ability to resist data loss, some parts of the cipher images are cut and then decrypted. The cipher images with different sizes of data loss and corresponding decrypted images are shown in Fig.17(a1)-(a4) and Fig.17(b1)-(b4), respectively. Obviously, even if 50 percent of the data in a cipher image is lost, it can basically recover the original information. Furthermore, to test the algorithm's ability to resist noise attacks, different strengths of salt and pepper noise and Gaussian noise are added to cipher images. The corresponding decrypted images are shown in Fig.17(c1)-(c4) and Fig.17(d1)-(d4), respectively. It can be seen that some pixel values have changed in the decrypted images, but the general information of the original images can still be displayed. This means that the designed encryption algorithm can effectively resist data loss and noise attacks, and has good robustness.

(8) Chosen plaintext and ciphertext attacks: In cryptanalysis, chosen plaintext attack and chosen ciphertext attack are two important attack methods. Generally, if an encryption algorithm can resist the chosen plaintext attack, it indicates that the algorithm has sufficient security level to resist other attacks including ciphertext-only attack and known-plaintext attack. To test the ability to defend the chosen plaintext attack, it is evaluated by using some special images including all-white and all-black images as input images. The size of the tested images is  $256 \times 256$ . Fig.18 gives the experimental results including the all-white and all-black plain images, their encrypted images, and corresponding histograms. As we can see, the histograms of

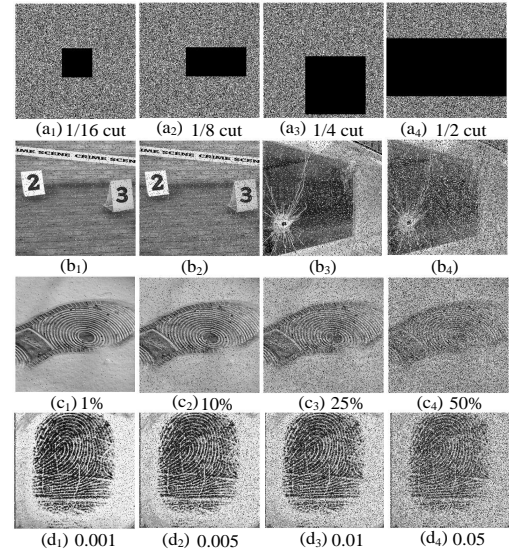


Fig. 17: Test results of data loss and noise attacks. (a1-a4) Cipher images under partial data loss. (b1-b4) Corresponding decrypted images. (c1-c4) Decrypted images of the cipher images under salt and pepper noise. (d1-d4) Decrypted images of the cipher images under Gaussian noise.

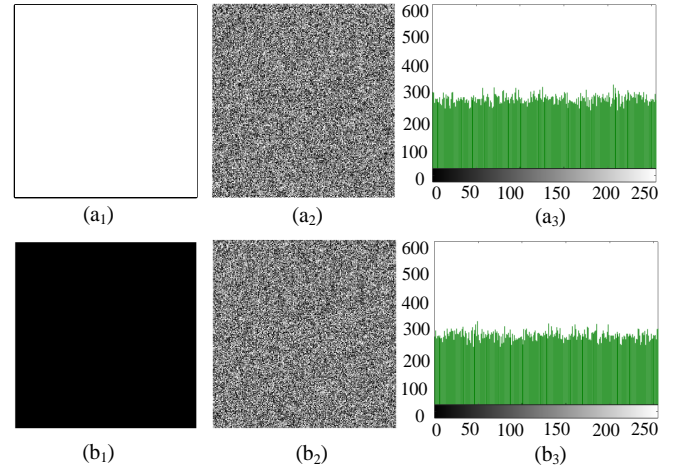


Fig. 18: Experiment results of special images. (a1-a3) All-white image, its encrypted image, and corresponding histogram, respectively. (b1-b3) All-black image, its encrypted image, and corresponding histogram, respectively.

the cipher images are evenly distributed, so the attacker cannot obtain useful information by encrypting some special images. Furthermore, the presented encryption algorithm can resist the chosen ciphertext attack because its keystream depends on the private key. From the above analysis, the proposed encryption algorithm has a strong ability to resist the chosen plaintext and ciphertext attacks.

Next, the advantages and disadvantages of the proposed encryption algorithm are discussed. The existing data security and privacy solutions present in the police IoT usually use traditional encryption algorithms, such as DES, IDEA, and RSA. Because the image data owns features of large sizes and high correlation among pixels, the traditional encryption algorithms are generally not suitable for a mass of image data encryption. Compared with these traditional encryption algorithms, the proposed chaos-based encryption algorithm is a kind of symmetric encryption algorithm, which has more simpler encryption structure and faster speed. Additionally, a performance comparison of encryption algorithms based on



TABLE III: PERFORMANCE COMPARISON OF THE ENCRYPTION ALGORITHMS BASED ON DIFFERENT MEMRISTIVE HNNs.

Refs	Image type	Dynamical behavior	Keyspace	Entropy	Key sensitivity	NPCR UACI	High robustness	Application
2020 [20]	Ordinary images (256×256)	Multi-scroll attractors	--	7.9977	$10^{-8}$	--	No	Matlab simulation
2022 [39]	Medical images (256×256)	Initial-boosted hyperchaos	$2^{480}$	7.9981	$10^{-12}$	99.6101 33.4672	Yes	FPGA experiment
2023 [22]	Ordinary images (256×256)	Grid multi-scroll attractors	--	7.9978	--	--	Yes	Matlab simulation
2023 [42]	Medical images (256×256)	Grid multi-scroll attractors	--	7.9977	--	99.6078 33.4875	No	Medical IoT
2023 [43]	Commercial images (256×256)	Hyperchaotic multi-scroll attractors	$2^{480}$	7.9976	--	99.5953 33.5107	Yes	Company IoT
This work	Crime scene images (256×256)	Grid multi-butterfly attractors	$2^{816}$	7.9977	$10^{-16}$	99.6082 33.4647	Yes	Police IoT

different memristive HNNs is given in Table III. It is clear that because the presented memristive HNN has complex grid multi-butterfly attractors, the designed encryption algorithm has a larger keyspace, more sensitive secret keys, and more ideal NPCR/UACI. Meanwhile, it also enjoys high robustness in terms of data loss and noise attacks. Although the proposed encryption algorithm has many advantages, it also has a weakness, that is, its key management is a complicated process because the key management directly determines its security.

### C. Experimental Demonstration

In this sub-section, the effectiveness of the proposed image security solution is confirmed by simulating the police IoT environment in reality. We use the fingerprint image as an example, and hardware experiment is implemented on RPI (Raspberry Pi). Hardware devices mainly contain a Dell Intel CoreTM i7 CPU 2.5GHz desktop computer, a router, and three 4b RPI, and the chaotic signal is realized in Python language under the EMQX 4.3.10 MQTT protocol. As shown in Fig.19, the three RPIs act as a publisher (encryption terminal), an intermediate server (EMC server), and a subscriber (decryption terminal), respectively, and are connected to the same WiFi. The IP addresses of the publisher, server, and subscriber are set as 192.168.123.188, 192.168.123.29, and 192.168.123.151, respectively. Taking the fingerprint image as the encrypted object, which is sent and received under EMQX(the open-source MQTT agent for IoT). The detailed experiment steps can be referred to in the literature [42]. In this experiment, there are three key steps. First, the original fingerprint image and secret keys are read and stored in the publisher, as shown in Fig.19(a). Then, the publisher further performs the preprocessing operations  $S_1$  and  $S_2$  to generate a cipher image, as shown in Fig.19(b). Meanwhile, the cipher image data is sent to the subscriber. Finally, the received cipher image is decrypted in the subscriber, and a decrypted image is directly displayed and saved, as shown in Fig.19(c). Therefore, the experiment has achieved the purpose of encrypting the crime scene image in the police IoT. there is no doubt that it is expected to be applied in the practical police IoT to reinforce information security.

## V. CONCLUSION

To protect the transmitted crime scene image data in the police IoT, a grid multi-butterfly memristive neural network model is presented in this work. First, the grid multi-butterfly memristive neural network model is constructed by comprehensively considering three bionic modeling methods. Then, its dynamical properties are analyzed by using various nonlinear analysis methods including the bifurcation diagram, Lyapunov exponents, phase portrait, and basin of attraction. Dynamic analysis results show that the presented memristive HNN can

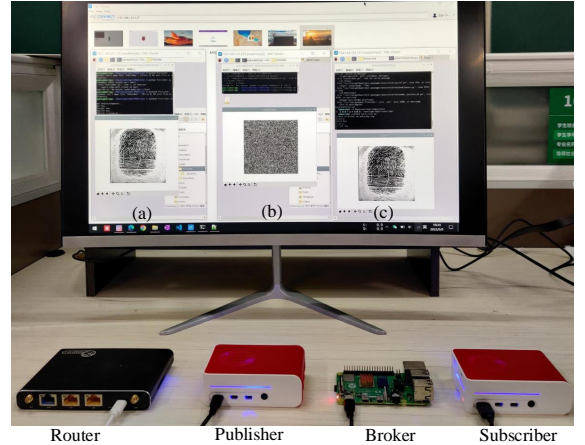


Fig. 19: Experimental demonstration based on RPI. (a) Original image. (b) Cipher image. (c) Decrypted image.

generate various complex dynamical behaviors including periodic and chaotic butterfly attractors, transient chaotic and chaotic double-butterfly attractors, 1D and grid multi-butterfly attractors, and initial-boosted plane coexisting multi-butterfly attractors. Meanwhile, the number and position of butterflies contained in the multi-butterfly attractors can be freely controlled by changing control parameters and initial states. Finally, the grid multi-butterfly memristive HNN is used to design the pseudo-random number generator to encrypt crime scene image data useful in the police IoT. Security performance evaluation shows that the encryption algorithm can effectively protect the information of the crime scene images and is superior to some existing encryption algorithms. Besides, we developed a hardware platform based on RPI under the MQTT protocol to verify the designed image security solution. Experimental results showed that our security solution can successfully realize security transmission of crime scene image data, which provides a significant reference for policing departments. One major limitation of this proposed security solution is that Key management is not easy, which can increase the chance of the brute force attack. In the future, we will consider more security enhancement mechanisms like the use of asymmetric key generation, integrating DNA encryption technology, and adding a deep neural network.

## REFERENCES

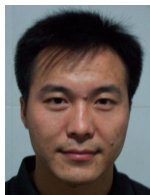
- [1] C. Huang, T. Chou, S. Wu, "Towards convergence of AI and IoT for smart policing: a case of a mobile edge computing-based context-aware system," *J. Glob. Inf. Manag.*, vol. 29, no. 6, pp. 1-21, 2021.
- [2] A. Tundis, H. Kaleem, M. Mühlhäuser, "Detecting and tracking criminals in the real world through an IoT-based system," *Sensors.*, vol.20, no. 13, art. no. 3795, 2020.

- [3] J. Jung, B. Kim, J. Cho, et al, "A secure platform model based on ARM platform security architecture for IoT devices," *IEEE Internet Things J.*, vol. 9, no. 7, pp. 5548-5560, 2022.
- [4] L. Li, Y. Chen, H. Peng, et al, "Chaotic deep network for mobile D2D communication," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 8078-8096, 2020.
- [5] B. Yan, G. Wang, J. Yu, et al, "Spatial-temporal chebyshev graph neural network for traffic flow prediction in IOT-based ITS," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9266-9279, 2022.
- [6] K. Li, H. Bao, H. Li, et al, "Memristive Rulkov neuron model with magnetic induction effects," *IEEE Trans. Ind. Informat.*, vol. 18, no. 3, pp. 1726-1736, 2021.
- [7] J. J. Hopfield, "Neural network and physical system with emergent collective computational abilities," *Proc. Nat. Acad. Sci. USA.*, vol. 79, pp. 2554-2558, Apr. 1982.
- [8] Q. Deng, C. Wang, H. Lin, "Memristive Hopfield neural network dynamics with heterogeneous activation functions and its application," *Chaos, Solitons Fractals.*, vol. 178, art. no. 114387, 2024.
- [9] C. Chen, F. Min, J. Cai, et al, "Memristor synapse-driven simplified Hopfield neural network: hidden dynamics, attractor control, and circuit implementation," *IEEE Trans. Circuits Syst. I.*, DOI: 10.1109/TCSI.2024.3349451, 2024.
- [10] D. B. Strukov, G. S. Snider, D. R. Stewart, et al, "The missing memristor found," *Nature.*, vol. 453, no. 7191, pp. 80-83, 2008.
- [11] J. Sun, Y. Wang, P. Liu et al, "Memristor-based circuit design of PAD emotional space and its application in mood congruity," *IEEE Internet Things J.*, vol. 10, no. 18, pp. 16332-16342, 2023.
- [12] Q. Deng, C. Wang, J. Sun, et al, "Nonvolatile CMOS memristor, reconfigurable array, and its application in power load forecasting," *IEEE Trans. Ind. Informat.*, DOI: 10.1109/TII.2023.3341256, 2023.
- [13] D. Tang, C. Wang, H. Liu, et al, "Dynamics analysis and hardware implementation of multi-scroll hyperchaotic hidden attractors based on locally active memristive Hopfield neural network," *Nonlinear Dyn.*, vol. 112, no. 2, pp. 1511-1527, 2024.
- [14] Q. Hong, L. Yang, S. Du, et al, "Memristive recurrent neural network circuit for fast solving equality-constrained quadratic programming with parallel operation," *IEEE Internet Things J.*, vol. 9, no. 23, pp. 24560-24571, 2022.
- [15] O. Krestinskaya, K. N. Salama, A.P. James, "Learning in memristive neural network architectures using analog backpropagation circuits," *IEEE Trans. Circuits Syst. II.*, vol. 66, no. 2, pp. 719-732, 2019.
- [16] J. Sun, C. Li, Z. Wang, et al, "A memristive fully connect neural network and application of medical image encryption based on central diffusion algorithm," *IEEE Trans. Ind. Informat.*, vol. 20, no. 3, pp. 3778-3788, 2024.
- [17] D. Ding, H. Xiao, Z. Yang, et al, "Coexisting multi-stability of Hopfield neural network based on coupled fractional-order locally active memristor and its application in image encryption," *Nonlinear Dyn.*, vol. 108, no. 4, pp. 4433-4458, 2022.
- [18] D. Vignesh, J. Ma, S. Banerjee, "Multi-scroll and coexisting attractors in a Hopfield neural network under electromagnetic induction and external stimuli," *Neurocomputing.*, vol. 564, Art. no. 126961, 2024.
- [19] R. Li, E. Dong, J. Tong, et al, "A novel multiscroll memristive Hopfield neural network," *Int. J. Bifurcation Chaos.*, vol. 32, no. 09, Art. no. 2250130, 2022.
- [20] S. Zhang, J. Zheng, X. Wang, et al, "Initial offset boosting coexisting attractors in memristive multi-double-scroll Hopfield neural network," *Nonlinear Dyn.*, vol. 102, pp. 2821-2841, 2020.
- [21] H. Bao, M. Hua, J. Ma, et al, "Offset-control plane coexisting behaviors in two-memristor-based Hopfield neural network," *IEEE Trans. Ind. Electron.*, vol. 70, no. 10, pp. 10526-10535, 2023.
- [22] Q. Lai, Z. Wan, P. D. K. Kuate, "Generating grid multi-scroll attractors in memristive neural networks," *IEEE Trans. Circuits Syst. I.*, vol. 70, no. 3, pp. 1324-1336, 2023.
- [23] T. Dong, X. Gong, T. Huang, "Zero-Hopf Bifurcation of a memristive synaptic Hopfield neural network with time delay," *Neural Netw.*, vol. 149, pp. 146-156, 2022.
- [24] F. Li, L. Bai, Z. Chen, et al, "Scroll-growth and scroll-control attractors in memristive bi-neuron Hopfield neural network," *IEEE Trans. Circuits Syst. II.*, vol. 71, no. 4, pp. 2354-2358, 2024.
- [25] D. Vignesh, J. Ma, S. Banerjee, "Multi-scroll and coexisting attractors in a Hopfield neural network under electromagnetic induction and external stimuli," *Neurocomputing.*, vol. 564, Art. no. 126961, 2024.
- [26] Q. Wan, F. Li, S. Chen, et al, "Symmetric multi-scroll attractors in magnetized Hopfield neural network under pulse controlled memristor and pulse current stimulation," *Chaos, Solitons, Fractals.*, vol. 169, Art. no. 113259, 2023.
- [27] J. Sun, Y. Zhai, P. Liu, et al, "Memristor-based neural network circuit of associative memory with overshadowing and emotion congruent effect," *IEEE Trans. Neural Netw. Learn. Syst.*, DOI: 10.1109/TNNLS.2023.3348553, 2024.
- [28] L. Huang, Y. Zhang, J. Xiang, et al, "Extreme multistability in a Hopfield neural network based on two biological neuronal systems," *IEEE Trans. Circuits Syst. II.*, vol. 69, no. 11, pp. 4568-4572, 2022.
- [29] Q. Wan, Z. Yan, F. Li, et al, "Complex dynamics in a Hopfield neural network under electromagnetic induction and electromagnetic radiation," *Chaos.*, vol. 32, Art. no. 073107, 2022.
- [30] A. K. Singh, K. Chatterje, A. Sing, "An image security model based on chaos and DNA cryptography for IIoT images," *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 1957-1964, 2023.
- [31] F. Toktas, U. Erkan, Z. Yetgin, "Cross-channel color image encryption through 2D hyperchaotic hybrid map of optimization test functions," *Expert Syst. Appl.*, vol. 249, Art. no. 123583, 2024.
- [32] O. Kocak, U. Erkan, A. Toktas, et al, "PSO-based image encryption scheme using modular integrated logistic exponential map," *Expert Syst. Appl.*, vol. 237, Art. no. 121452, 2024.
- [33] W. Feng, Q. Wang, H. Liu, et al, "Exploiting newly designed fractional-order 3D Lorenz chaotic system and 2D discrete polynomial hyperchaotic map for high-performance multi-image encryption," *Fractal and Fractional.*, vol. 7, no. 12, Art. no. 887, 2023.
- [34] W. Feng, X. Zhao, J. Zhang, et al, "Image encryption algorithm based on plane-level image filtering and discrete logarithmic transform," *Mathematics.*, vol. 10, no. 15, Art. 2751, 2022.
- [35] H. Wen, Y. Lin, "Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding," *Expert Syst. Appl.*, vol. 237, Art. no. 121514, 2024.
- [36] W. Feng, Z. Qin, J. Zhang, et al, "Cryptanalysis and improvement of the image encryption scheme based on Feistel network and dynamic DNA encoding," *IEEE Access.*, vol. 9, pp. 145459-145470, 2021.
- [37] Q. Deng, C. Wang, H. Lin, "Chaotic dynamical system of Hopfield neural network influenced by neuron activation threshold and its image encryption," *Nonlinear Dyn.*, vol. 112, pp. 6629-6646, 2024.
- [38] Q. Lai, Z. Wan, H. Zhang, et al, "Design and analysis of multiscroll memristive hopfield neural network with adjustable memductance and application to image encryption," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 34, no. 10, pp. 7824-7837, 2023.
- [39] H. Lin, C. Wang, L. Cui, et al, "Brain-like initial-boosted hyperchaos and application in biomedical image encryption," *IEEE Trans. Ind. Informat.*, vol. 18, no. 12, pp. 8839-8850, 2022.
- [40] D. Jiang, Z. T. Njitacke, J. D. D. Nkappok, et al, "A new cross ring neural network: dynamic investigations and application to WBAN," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 7143-7152, 2023.
- [41] S. Zhang, C. Li, J. Zheng, et al, "Generating any number of initial offset-boosted coexisting Chua's double-scroll attractors via piecewise-nonlinear memristor," *IEEE Trans. Ind. Electron.*, vol. 69, no. 7, pp. 7202-7212, 2022.
- [42] F. Yu, H. Shen, Q. Yu, et al, "Privacy protection of medical data based on multi-scroll memristive Hopfield neural network," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 2, pp. 845-858, 2023.
- [43] C. Wang, D. Tang, H. Lin, et al, "High-dimensional memristive neural network and its application in commercial data encryption communication," *Expert Syst. Appl.*, vol. 242, Art. no. 122513, 2024.
- [44] Q. Hong, Y. Li, X. Wang, et al, "A versatile pulse control method to generate arbitrary multidirection multibutterfly chaotic attractors," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 38, no. 8, pp. 1480-1492, 2019.
- [45] Y. Yang, L. Huang, N. V. Kuznetsov, et al, "Generating multiwing hidden chaotic attractors with only stable node-foci: analysis, implementation and application," *IEEE Trans. Ind. Electron.*, vol. 71, no. 4, pp. 3986-3995, 2024.
- [46] R. Wu, S. Gao, H. H. C. Iu, et al, "Securing Dual-Channel Audio Communication With a Two-Dimensional Infinite Collapse and Logistic Map," *IEEE Internet Things J.*, vol. 11, no. 6, pp. 10214-10223, 2024.



**Hairong Lin** (Member, IEEE) received M.S. and Ph.D. degrees in information and communication engineering and computer science and technology from Hunan University, Changsha, China, in 2015 and 2021, respectively. From 2022 to 2023, he was a Postdoctoral Fellow with the School of Computer Science and Electronic Engineering, Hunan University, China. He is currently an Associate Professor at the School of Electronic Information, Central South University, Changsha, China. He is a member of the Chaos and Nonlinear Circuit Professional Committee of Circuit

and System Branch of China Electronic Society. He has presided over four national and provincial projects, and published more than 50 papers in related international journals, such as IEEE-TIE, IEEE-TII, IEEE-TCAD, etc. His research interests include chaotic cryptography, information and network security, complex networks, and Internet of Things.



**Xiaoheng Deng** (Senior Member, IEEE) received the Ph.D. degree in computer science from Central South University, Changsha, Hunan, P.R. China, in 2005. Since 2006, he has been an Associate Professor and then a Full Professor with the department of Communication Engineering, Central South University. He is Joint professor of Shenzhen Research Institute, Central South University and the director of data sensing and switching equipment provincial engineering center. He is a senior member of CCF, a member of CCF Pervasive Computing Council, a senior member of IEEE

and a member of ACM. He has been a chair of CCF YOCSEF CHANGSHA from 2009 to 2010. His research interests include edge computing, Internet of Things, wireless networking and communication, data mining, and pattern recognition.



**Fei Yu** received the M.E. and Ph.D. degree from College of Information Science and Engineering, Hunan University, Changsha, China, in 2010 and 2013, respectively. He is currently a distinguished Associate Professor at School of Computer and Communication Engineering in Changsha University of Science and Technology, Changsha, China. He focuses on nonlinear system and circuit, complex network and their applications.



**Yichuang Sun** (M'90–SM'99) received the B.Sc. and M.Sc. degrees from Dalian Maritime University, Dalian, China, in 1982 and 1985, respectively, and the Ph.D. degree from the University of York, York, U.K., in 1996, all in communications and electronics engineering. Dr. Sun is currently Professor of Communications and Electronics, Head of Communications and Intelligent Systems Research Group, and Head of Electronic, Communication and Electrical Engineering Division in the School of Engineering and Computer Science of the University of Hertfordshire, UK. His

research interests are in the areas of wireless and mobile communications, RF and analogue circuits, microelectronic devices and systems, and machine learning and deep learning.

Professor Sun was a Series Editor of IEE Circuits, Devices and Systems Book Series (2003-2008). He has been Associate Editor of IEEE Transactions on Circuits and Systems I: Regular Papers (2010-2011, 2016-2017, 2018-2019). He is also Editor of ETRI Journal, Journal of Semiconductors, and Journal of Sensor and Actuator Networks. He was Guest Editor of eight IEEE and IEE/IET journal special issues: High-frequency Integrated Analogue Filters in IEE Proc. Circuits, Devices and Systems (2000), RF Circuits and Systems for Wireless Communications in IEE Proc. Circuits, Devices and Systems (2002), Analogue and Mixed-Signal Test for Systems on Chip in IEE Proc. Circuits, Devices and Systems (2004), MIMO Wireless and Mobile Communications in IEE Proc. Communications (2006), Advanced Signal Processing for Wireless and Mobile Communications in IET Signal Processing (2009), Cooperative Wireless and Mobile Communications in IET Communications (2013), Software-Defined Radio Transceivers and Circuits for 5G Wireless Communications in IEEE Transactions on Circuits and Systems-II (2016), and the 2016 IEEE International Symposium on Circuits and Systems in IEEE Transactions on Circuits and Systems-I (2016). He has also been widely involved in various IEEE technical committee and international conference activities.