Diversified Butterfly Attractors of Memristive HNN With Two Memristive Systems and Application in IoMT for Privacy Protection

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

***Abstract*—Memristors are often used to emulate neural synapses or to describe electromagnetic induction effects in neural networks. However, when these two things occur in one neuron concurrently, what dynamical behaviors could be generated in the neural network? Up to now, it has not been comprehensively studied in the literature. To this end, this paper constructs a new memristive Hopfield neural network (HNN) by simultaneously introducing two memristors into one Hopfield-type neuron, in which one memristor is employed to mimic an autapse of the neuron and the other memristor is utilized to describe the electromagnetic induction effect. Dynamical behaviors related to the two memristive systems are investigated. Research results show that the constructed memristive HNN can generate Lorenz-like double-wing and four-wing butterfly attractors by changing the parameters of the first memristive system. Under the simultaneous influence of the two memristive systems, the memristive HNN can generate complex multi-butterfly chaotic attractors including multi-double-wing-butterfly attractors and multi-four-wing-butterfly attractors, and the number of butterflies contained in an attractor can be freely controlled by adjusting the control parameter of the second memristive system. Moreover, by switching the initial state of the second memristive system, the multi-butterfly memristive HNN exhibits initial-boosted coexisting double-wing and four-wing butterfly attractors. Undoubtedly, such diversified butterfly attractors make the proposed memristive HNN more suitable for chaos-based engineering applications. Finally, based on the multi-butterfly memristive HNN, a novel privacy protection scheme in the IoMT is designed. Its effectiveness is demonstrated through encryption tests and hardware experiments.**

***Index Terms*—Multi-butterfly attractor, Hopfield neural network, memristive system, initial-boosted behavior, privacy protection.**

I. Introduction

THE human brain which is a highly complex nonlinear system has abundant dynamical behaviors associated with unique memory, thinking, and learning abilities [1]. In order to explore the neural dynamics, various neural network models have been constructed by emulating the biological structure and working mechanism of the brain's nervous system [2, 3]. Among them, the Hopfield neural network [4], as a special nonlinear system, has been proven to be an excellent artificial neural network model for emulating the brain's dynamic behaviors. Over the past decades, a variety of dynamical behaviors, such as bursting oscillation [5], chaos [6], hyperchaos [7], coexisting chaos [8], and Chimera states [9] have been generated by different HNN models, and these models are of great significance in biology and engineering applications.

Sixteen years ago, in 2008, a novel nonlinear electronic device named memristor was found by Hewlett-Packard labs [10]. The memristor has greatly raised the development of nonlinear science due to its specific nonlinearity [11-13]. More significantly, it can store its memductance or memristance by adjusting its internal flux or charge, which makes it particularly useful for emulating biological neural synapses [14] or describing the electromagnetic induction effects [15]. Therefore, a memristor is considered one of the most propitious candidates for designing artificial neural networks as it naturally performs like a synapse and owns the features of memory, nonlinearity, and multistability [16]. For these reasons, memristive HNNs have many advantages in various applications. For instance, its memory function can improve the ability of associative memory in biomimetic neural network circuits [17]. Memristive HNNs can also be applied to various artificial intelligence systems including machine learning [18], image restoration [19], and information security [20]. Furthermore, employing memristors as synapses or describing electromagnetic induction effects in HNN can make memristive HNNs produce complex dynamical behaviors closer to the brain than the traditional HNNs [21-23], which is of great significance for understanding the brain's unique functions.

Hence, numerous research activities are focused on the design of memristive HNNs with complex dynamical behaviors. Due to the inherent multistability and strong nonlinearity of the memristors, memristive HNNs can generate the feature of coexisting behaviors and multi-attractors. On one hand, the memristors are used as synapses to design memristive HNNs. For example, by using two sinusoidal memristors to simulate autapses, a memristive HNN with plane coexisting behaviors was presented in [24]. Based on three non-ideal memristor synapses, a memristive HNN with a space multi-structure attractor was designed [25]. Furthermore, coexisting infinitely many hidden attractors [26], multi-double-scroll attractors [27], and grid multi-scroll attractors [28] have been found in memristive HNNs based on a similar modeling approach. On the other hand, the memristors

Manuscript received Jan 15, 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 (haironglin@csu.edu.cn; 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.

are used to describe the electromagnetic induction effect in the memristive HNNs. For instance, by employing a memristor to describe external electromagnetic radiation, the authors in [29] designed a memristive HNN with symmetric multi-scroll chaotic attractors. Adopting the same methods, multistyle chaotic attractors [30], scroll-growth and scroll-control attractors [31] have been generated in memristive HNNs. Additionally, in [32], a memristive HNN with extreme multistability was constructed by introducing two memristors to emulate the autapse and describe the electromagnetic induction effect respectively. However, the two memristors work on different neurons. If two different memristors act on one neuron in a neural network at the same time, what dynamical behaviors could be generated in the memristive HNN?

Chaotic signals with the characteristics of unpredictability, ergodicity, and sensitivity to initial values can be applied to generate security keys in information encryption [33-35]. The application of chaotic signals generated by HNNs to information encryption has important practical significance for data security in network communications [36], which has attracted increasing attention from many researchers. For example, in [37], a simple image encryption scheme was developed based on the HNN, which has good encryption performance. A parallel compressive sensing algorithm based on a ring HNN has been applied to data security in wireless body area networks [38]. Moreover, a medical image encryption algorithm was designed, where an encryption scheme with a permutation-diffusion structure was proposed based on a hyperchaotic memristive HNN [39]. In particular, because multi-scroll attractors have more complex dynamical behaviors and greater randomness [40], the multi-scroll memristive HNNs have been widely applied in information protection. For example, a privacy protection scheme in IoT was constructed, in which the key is generated by multi-scroll memristive HNN [41]. Furthermore, in [42], a hyperchaotic multi-scroll memristive HNN is successfully applied to commercial data encryption communication, which undoubtedly shows the great potential of memristive HNNs in information protection.

Inspired by the above analyses, we are motivated to design a novel memristive HNN model that can be used to study the dynamical behaviors of the neural system with one neuron simultaneously influenced by two different memristors and in the future can be used to generate security keys of the information protection. Toward this goal, we first design two different memristor models. Then, by introducing the two memristors into one neuron to imitate its autapse and describe its electromagnetic induction effect, a memristive HNN with two memristive systems is constructed. What's amazing is that the constructed memristive HNN can generate various complex butterfly attractors, including the Lorenz-like double-wing and four-wing butterfly chaotic attractors, multi-double-wing-butterfly and multi-four-wing-butterfly chaotic attractors, and initial-boosted coexisting double-wing and four-wing butterfly attractors. To the best of our knowledge, this is the first time the butterfly and multi-butterfly chaotic attractors are found in the HNNs. Compared with the aforementioned attractors, the multi-butterfly chaotic attractors integrate the attractor features of multi-wing attractors and multi-scroll attractors [43, 44], which have a more complex dynamical trajectory, higher randomness, and more secret key parameters. Therefore, generating security keys through the multi-butterfly memristive HNN is worthy of in-depth investigation. Finally, based on the multi-butterfly memristive HNN, we design a novel privacy protection scheme in IoMT. Good encryption results show the superiority of the scheme.

The main contributions of this article are summarized as follows. 1) Two new memristor models are designed that are used to simulate autapse and describe the electromagnetic induction effect. 2) A multi-butterfly memristive HNN model is constructed, which can be applied in information security. 3) Diversified butterfly attractors including butterfly attractors, multi-butterfly attractors, and initial-boosted butterfly attractors are discovered for the first time in HNNs. 4) A privacy protection scheme in IoMT is designed and hardware implemented based on the multi-butterfly memristive HNN, which has good encryption results.

The rest of the paper is organized as follows. Sect.II designs two memristor models and constructs a new memristive HNN with two memristive systems. Various butterfly attractors in the memristive HNN are revealed in Sect. III. In Sect.IV, a privacy protection scheme in IoMT is designed based on the multi-butterfly memristive HNN and its security performances are analyzed and experimentally demonstrated. Sect.V summarizes the paper.

II. Memristive Hopfield neural network

This section first designs two memristor models. Then a memristive Hopfield neural network with two memristive systems is constructed. Finally, the characteristics of equilibrium points are studied.

A. Design of the memristor models

According to the memristor theory [10], a generalized voltage-controlled memristor model can be expressed as

$$\begin{cases} i = W(\varphi)v \\ d\varphi/dt = f(\varphi,v) \end{cases} \tag{1}$$

where v, i, φ are voltage, current, and memristor state variables, respectively. $W(\varphi)$ and $f(\varphi,v)$ denote memductance function and state equation of the memristor, respectively. It is noted that the state equation for the memristor is associated not only with the applied voltage but also with its state variable. Therefore, the generalized memristor has more complex dynamics than the ideal memristor.

Based on equation (1), a novel generalized voltage-controlled memristor model is designed as follows

$$\begin{cases} i = W_1(\varphi_1)v = \alpha({\varphi_1}^2 - \varphi_1 - \beta)v \\ d\varphi_1/dt = f_1(\varphi_1,v) = (v^2-1)\varphi_1 - v \end{cases} \tag{2}$$

where $W_1(\varphi_1)$ is the memductance function, and α and β are two memristive parameters. To show its voltage-current (v-i) loci, a sinusoidal voltage v=$A\sin(2\pi Ft)$ is added to the input of the presented memristor. Setting α=-0.5, β=35, φ_{10}=0, signal amplitude A and signal frequency F are set as two adjustable parameters. Firstly let F=0.2, for A=0.8, 0.9, and 1, the amplitude-relied v-i loci are plotted in Fig.1(a). Secondly, for F=0.2, 0.4, and 0.8, with fixed A=1, the frequency-relied v-i loci are plotted in Fig.1(b). As can be seen, the v-i loci in Fig.1 perfectly illustrate the three fingerprints of the memristor [10].

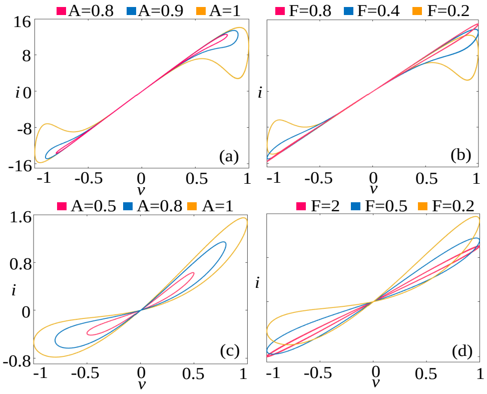


Fig. 1: The fingerprints of the two memristors. (a) Amplitude-relied *v*-*i* loci of the memristor M_1 with F=0.2. (b) Frequency-relied *v*-*i* loci of the memristor M_1 with A=1. (c) Amplitude-relied *v*-*i* loci of the memristor M_2 with F=0.2. (d) Frequency-relied *v*-*i* loci of the memristor M_2 with A=1.

As a result, the proposed equation (2) is a memristor model, named M_1.

Based on the equation (1), another generalized voltage-controlled memristor model is designed as follows

$$\begin{cases} i = W_2(\varphi_2)v = b\varphi_2 v \\ \mathrm{d}\varphi_2/\mathrm{d}t = cv - dh \end{cases} \tag{3}$$

where

$$h = \varphi_2 - \left(\mathrm{sgn}(\varphi_2) + \sum_{i=1}^{N} \mathrm{sgn}(\varphi_2 + 2i) - N \right), N \in N^* \tag{4}$$

where $W_2(\varphi_2)$ is the memductance function, b, c and d are three constant parameters, and N is a control parameter. The memristive characteristics are analyzed as follows. Setting b=1, and c=1.2, d=1, taking N=2 as an example, when the same sinusoidal voltage with frequency F=0.2 and different amplitudes A=(0.5, 0.8, 1.0) is applied in the memristor, the amplitude-relied *v*-*i* loci are plotted in Fig.1(c). When the amplitude A=1 and different frequencies F=(0.2, 0.5, 2), the frequency-relied *v*-*i* loci are plotted in Fig.1(d). Obviously, with the increase in frequency, the area of the pinched hysteresis loops of the memristor decreases gradually, which implies that the proposed equation is a memristor model, named M_2.

B. Construction of the memristive HNN

Hopfield Neural network similar to the brain nervous system can produce complex brain-like chaotic behaviors. The original HNN with n neruons is defined as [4]

$$C_i\dot{x}_i = -x_i/R_i + \sum_{j=1}^{n} w_{ij}\tanh(x_j) + I_i \quad (i,j \in N^*) \tag{5}$$

where C_i, R_i, and v_i are respectively membrane capacitor, membrane resistor, and membrane voltage of the neuron i. w_{ij} is the synaptic weight coefficient describing the connection strength from neuron j to neuron i. Besides, tanh(.) represents the neuron activation function, and I_i denotes an external input current. Based on equation (5), assuming C_i=1, R_i=1, I_i=0 (i=1,2) and selecting the appropriate synaptic weight coefficients, a bi-neuron HNN is proposed as follows.

$$\begin{cases} \dot{x}_1 = -x_1 + \tanh(x_2) \\ \dot{x}_2 = -x_2 - 1.5\tanh(x_1) + w_{22}\tanh(x_2) \end{cases} \tag{6}$$

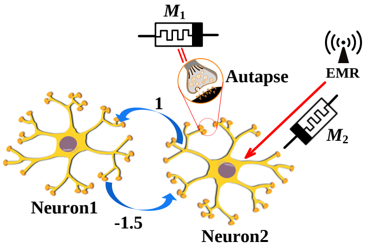


Fig. 2: Structure of the memristive HNN with two memristive systems

Memristors usually are used to mimic biological neural synapses or to describe electromagnetic induction effects. Now as shown in Fig.2, we simultaneously introduce two designed memristor models into the proposed bi-neuron HNN to construct a memristive HNN model. Among them, the memristor M_1 is used to simulate the autapse of neuron 2, while the memristor M_2 is used to describe the electromagnetic induction effect of neuron 2 under external electromagnetic radiation. Because the two memristors play different roles in the bi-neuron HNN, the constructed memristive HNN has two memristive systems. Consequently, the mathematical model of the memristive HNN can be described by

$$\begin{cases} \dot{x}_1 = -x_1 + \tanh(x_2) \\ \dot{x}_2 = -x_2 - 1.5\tanh(x_1) + k_1 W_1 \tanh(x_2) + k_2 W_2 x_2 \\ \dot{\varphi}_1 = ({x_2}^2 - 1)\varphi_1 - x_2 \\ \dot{\varphi}_2 = cx_2 - dh \end{cases} \tag{7}$$

where W_1 stands for the synaptic weight w_{22}, and k_1 is a constant representing the coupling strength of the memristor M_1. W_2x_2 represents the induction current induced by external electromagnetic radiation, and k_2 is a constant representing the feedback gain of the induction current.

C. Analysis of equilibrium points and stability

The characteristics of equilibrium points of the memristive HNN in equation (7) are analyzed by theoretical and numerical methods. Define E=(x_1*, x_2*, φ_1*,φ_2*) as an equilibrium point of the memristive HNN. Letting the left side of equation (7) be 0, the equilibrium points can be solved from the following equation

$$\begin{cases} 0 = -x_1 + \tanh(x_2) \\ 0 = -x_2 - 1.5\tanh(x_1) + k_1 W_1 \tanh(x_2) + k_2 W_2 x_2 \\ 0 = ({x_2}^2 - 1)\varphi_1 - x_2 \\ 0 = cx_2 - dh \end{cases} \tag{8}$$

The Jacobian matrix at the equilibrium point is generated as

$$J = \begin{bmatrix} -1 & \mathrm{sech}^2({x_2}^*) & 0 & 0 \\ -1.5\mathrm{sech}^2({x_1}^*) & \begin{matrix} k_1 W_1 \mathrm{sech}^2({x_2}^*) \\ +k_2 W_2 - 1 \end{matrix} & \begin{matrix} k_1 \alpha(2{\varphi_1}^* - 1) \\ \tanh({x_2}^*) \end{matrix} & k_2 b {x_2}^* \\ 0 & 2{x_2}^*{\varphi_1}^* - 1 & ({x_2}^*)^2 - 1 & 0 \\ 0 & c & 0 & -d \end{bmatrix} \tag{9}$$

Obviously, since the values of system parameters are uncertain, the stability of the nonzero equilibrium points cannot be determined. So here we discuss the stability of zero equilibrium point. When E=(0, 0, 0, 0), the Jacobian matrix is modified as follows

$$J = \begin{bmatrix} -1 & 1 & 0 & 0 \\ -1.5 & -1 - k_1\alpha\beta & 0 & 0 \\ 0 & -1 & -1 & 0 \\ 0 & c & 0 & -d \end{bmatrix} \tag{10}$$

Accordingly, the eigenvalue polynomial can be written by

$$\begin{aligned} P(\lambda) &= \det(I\lambda - J) \\ &= (\lambda + d)(\lambda + 1)(\lambda^2 + (2 + k_1\alpha\beta)\lambda + k_1\alpha\beta + 1.5) \end{aligned} \tag{11}$$

Thus, the Jacobian matrix has four non-zero roots as follows

$$\begin{cases} \lambda_1 = -d \\ \lambda_2 = -1 \\ \lambda_3 = -\frac{2+k_1\alpha\beta}{2} + \sqrt{-\frac{1+k_1\alpha\beta}{2}} \\ \lambda_4 = -\frac{2+k_1\alpha\beta}{2} - \sqrt{-\frac{1+k_1\alpha\beta}{2}} \end{cases} \tag{12}$$

According to the systems parameters $d > 0$, $\alpha < 0$, $\beta > 0$, the stability of the zero equilibrium point can be roughly evaluated and summarized as follows.

Case 1: $k_1\alpha\beta$=-2, $\lambda_{3,4}$=$\pm\sqrt{-\frac{1+k_1\alpha\beta}{2}}$. E is an unstable node point. The system is unstable.

Case 2: $-1 > k_1\alpha\beta > -2$, $\lambda_{3,4} < 0$. E is a stable node point. The system is stable.

Case 3: $k_1\alpha\beta < -2$, $\lambda_{3,4} > 0$. E is an unstable node point. The system is unstable.

Case 4: $k_1\alpha\beta > -1$, 1+$k_1\alpha\beta > 0$, 2+$k_1\alpha\beta > 0$, $\lambda_{3,4}$ are two imaginary roots. E is a stable node focus. The system is stable.

Case 5: $k_1\alpha\beta$=-1, $\lambda_{3,4} < 0$. E is a stable node point. The system is stable.

To analyze the non-zero equilibrum points of the system, equation (8) is further simplified by

$$\begin{cases} x_1 = \tanh(x_2) \\ \varphi_1 = x_2/({x_2}^2 - 1) \\ f_1(\varphi_2, x_2) = -x_2 - 1.5\tanh(x_1) + k_1 W_1 \tanh(x_2) + k_2 W_2 x_2 \\ f_2(\varphi_2, x_2) = c x_2 - d h \end{cases} \tag{13}$$

Next, the distribution of the equilibrium points is analyzed by the Matlab graph description method. In equation (13), the solution of x_2 is determined by the function h. Namely, the number and position of the equilibrium points are controlled by the control parameter N. Taking N=2 as an example, when k_1=1, k_2=1.5, α=-0.9, β=16, b=0.01, c=2, d=5, and initial states (x_{10}, x_{20}, φ_{10}, φ_{20})=(0.1, 0.1, 0.1, 0.1), the distribution of the equilibrium points on the φ_2-x_2 plane can be given by plotting the function curves f_1 and f_2, as shown in Fig.3. Numerical analyses show that all equilibrium points are divided into three types E_1, E_2, and E_3. E_1 is a kind of unstable saddle-focus point, which produces a chaotic trajectory in the shape of butterfly wings. Both E_2 and E_3 are unstable saddle points. Among them, the function of E_2 is to connect the two wings of the butterfly's attractor, and E_3's job is to connect two butterfly attractors. From Fig.3, the equilibrium points are synchronously extended along the φ2-axis. That is to say, with the increase of control parameter N, the number of equilibrium points will be extended along the φ_2 direction. Numerical simulation shows that the memristive HNN can generate a self-excited four-butterfly attractor, as shown in Fig.3. Obviously, the increase of the control parameter N in the system leads to the extension of the equilibrium points, which can generate the phenomenon of chaotic attractor reconstruction. Further analysis shows that the number of equilibrium points E_1, E_2, and E_3 are equal to 2(N+2), N+2, and N+1, respectively. And the number of the reconstructed butterfly attractors is equal to N+2. That is to say, the total number of the equilibrium points is $4m - 1$, where m is the number of the multi-butterfly attractors.

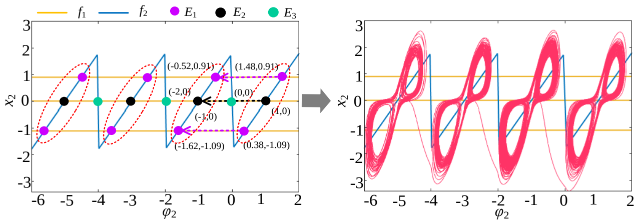


Fig. 3: Distribution of the equilibrium points of the memristive HNN with N=2 and the generated four-butterfly attractor.

III. Chaotic dynamic analysis

In this section, memristor-induced chaotic dynamics are investigated using several numerical measures such as bifurcation diagrams, Lyapunov exponents (LEs), phase plots, basin of attraction, and time series. Matlab ode45 algorithm with a time-step of 0.01 and end time of 10000 and Wolf's Jacobian matrix method are used for solving the differential equations and calculating the LEs, respectively.

A. *Double-wing and four-wing butterfly attractors*

The chaotic dynamics induced by the memristor M_1 are studied by taking α and β as variable parameters. For k_1=1, k_2=1.5, b=0.01, c=1.2, d=5, N=0, and x_{10}=x_{20}=φ_{10}=φ_{20}=0.1, the 2D bifurcation diagram depicted within α=[-10, 0] and β=[0, 60] is plotted in Fig.4. Fig.4 shows two important results: First, the memristive HNN generates infinite wide chaotic behavior (the area marked by color c); Second, the memristive HNN exhibits abundant intermittent chaos and period states with different periods (the areas marked by colors c_1-c_7, namely period 1 to period 7). It is noted that the area marked by the color c_0 denotes the unbounded behavior or stable points. To better reveal these dynamical behaviors, setting β=16, the 1D bifurcation diagram of the parameter α, as well as the first three LEs, are given in Fig.5(a) and (b), respectively. It can be seen from Fig.5(a) that the dynamical behaviors of the memristive HNN can be divided into four areas in $\alpha\in$[-2, 0]. In the area $\alpha_1\in$[-2, -0.78], the memristive HNN exhibits a wide range of chaotic behavior except for several periodic windows. Interestingly, this chaotic behavior has complex dynamical trajectories exhibiting Lorenz-like butterfly-shaped attractors, which have never been observed in previous neural network models. As shown in Fig.6(a), when α=-0.9 is chosen, a double-wing butterfly chaotic attractor can be obtained from the memristive HNN. Then through a forward period doubling bifurcation route, the memristive HNN enters into a novel chaotic area $\alpha_2\in$[-0.7, -0.22]. More interestingly, the novel chaotic area exhibits complex four-wing butterfly attractors, which is also the first observed in the existing neural networks. When α=-0.25 is selected from the memristve HNN, a four-wing butterfly chaotic attractor is obtained as shown in Fig.6(b). Finally, the memristive HNN enters into a periodic area α_3 and a stable point area α_4. Therefore, under the influence of the first memristive system, the proposed memristive HNN generates complex double-wing and four-wing butterfly chaotic attractors.

B. *Multi-butterfly chaotic attractors*

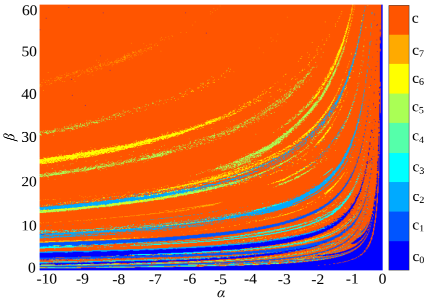


Fig. 4: Dynamics distributed in the α-β parameter plane under k_1=1, k_2=1.5, b=0.01, c=1.2, d=5, N=0, and x_{10}=x_{20}=φ_{10}=φ_{20}=0.1.

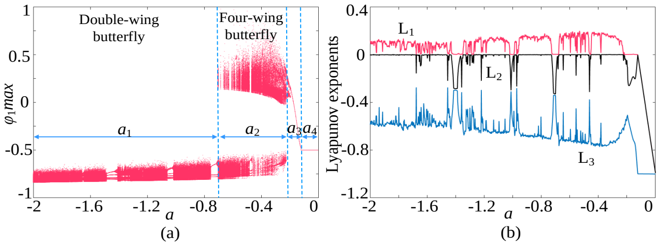


Fig. 5: The α-relied dynamical behaviors of the memristive HNN under β=16. (a) bifurcation diagram. (b) Lyapunov exponents.

The chaotic dynamics induced by the memristor M_2 are studied by taking N as a variable parameter. When α=-0.9, β=16, and c=2, the parameter N is increased from 1 to 7, and the bifurcation diagram of the state variable φ_2 as well as the first three LEs are depicted in Fig.7(a) and Fig.7(b), respectively. Fig.7 directly illustrates two important results: (i) With the increase of parameter N, the double-wing butterfly attractor is reconstructed to generate a multi-double-wing-butterfly chaotic attractor; (ii) The number of the multi-butterfly chaotic attractors can be controlled by single parameter N. As shown in Fig.8, different numbers of multi-double-wing-butterfly chaotic attractors can be obtained from the memristive HNN under different control parameter N. Amazingly, when α=-0.25, by selecting different control parameter N, arbitrary number of multi-four-wing-butterfly chaotic attractors can also be detected in the memristive HNN, as shown in Fig.9. Similarly, the number of the multi-four-wing-butterfly attractors can also be controlled by the control parameter N. Furthermore, both the numbers of butterflies contained in a multi-double-wing-butterfly attractor and a multi-four-wing-butterfly attractor are equal to N+2. Such interesting dynamics means that the memristive HNN can not only generate multi-double-wing-butterfly attractors but also multi-four-wing-butterfly attractors, which means that the proposed memristive HNN generates complex multi-butterfly chaotic attractors.

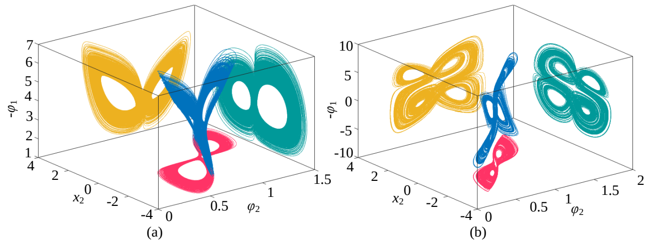


Fig. 6: Complex butterfly chaotic attractors in φ_2-x_2-φ_1 space. (a) Double-wing butterfly attractor with α=-0.9. (b) Four-wing butterfly attractor with α=-0.25.

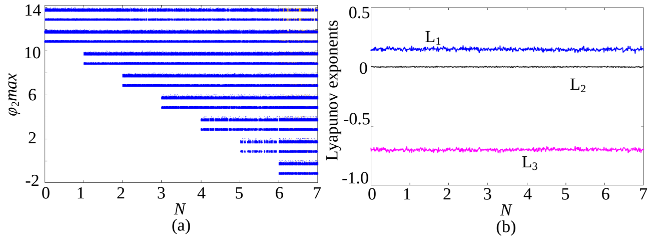


Fig. 7: The N-relied dynamical behaviors. (a) Bifurcation diagram. (b) Lyapunov exponents.

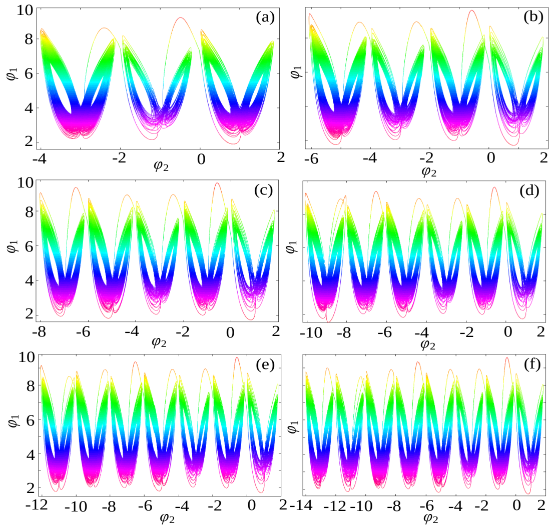


Fig. 8: Complex multi-double-wing-butterfly chaotic attractors under α=-0.9. (a)3-double-wing-butterfly attractor with N=1. (b) 4-double-wing-butterfly attractor with N=2. (c) 5-double-wing-butterfly attractor with N=3. (d) 6-double-wing-butterfly attractor with N=4. (e) 7-double-wing-butterfly attractor with N=5. (f) 8-double-wing-butterfly attractor with N=6.

C. Initial-boosted coexisting butterfly attractors

The chaotic dynamics induced by the memristor's initial states are studied. Initial-boosted coexisting behaviors play an important role in dynamical systems and have valuable applications [27]. It is wonderful that the presented multi-butterfly memristive HNN can generate initial-boosted coexisting double-wing and four-wing butterfly chaotic attractors. For instance, when setting k_1=1, k_2=1.5, α=-0.9, β=16, b=0.01, c=1.2, d=5, N=6, x_{10}=x_{20}=0.1, we plot the local basin of attraction in the φ_{20}-φ_{10} plane, as shown in Fig.10(a). As can be seen, the local basin of attraction has complicated manifold structures and clear basin boundaries, and the color-painted marked by s_1-s_8 indicates 8 attracting regions of dynamical behaviors. When φ_{10}=0.1, by selecting different memristor initial state φ_{20}=1, -1, -3, -5, -7, -9, -11, and -13, coexisting 8 double-wing butterfly chaotic attractors with the same topologies but different positions can be obtained as shown in Fig.10(b). That is to say, the memristive HNN enjoys complex dynamics of initial-boosted coexisting behaviors, which means that it has excellent robustness. Additionally, keeping the above parameter values unchanged except for α=-0.25, the bifurcation dynamics related to φ_{20} and corresponding LEs are depicted in Fig.11(a) and (b), respectively. Obviously, under different initial states φ_{20}, the memristive HNN can generate infinitely many chaotic attractors

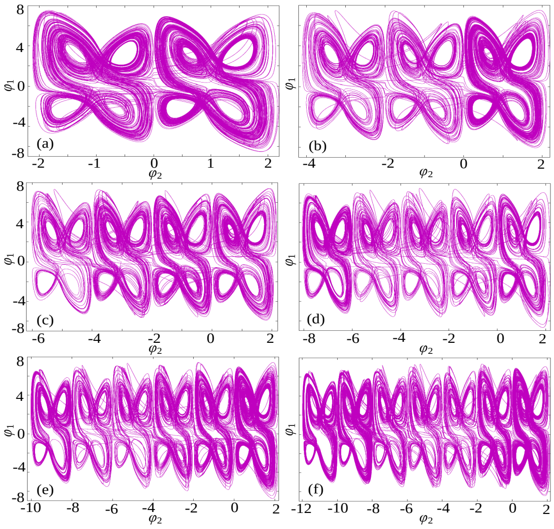


Fig. 9: Complex multi-four-wing-butterfly chaotic attractors under α=-0.25. (a) 2-four-wing-butterfly attractor with N=0. (b) 3-four-wing-butterfly attractor with N=1. (c) 4-four-wing-butterfly attractor with N=2. (d) 5-four-wing-butterfly attractor with N=3. (e) 6-four-wing-butterfly attractor with N=4. (f) 7-four-wing-butterfly attractor with N=5.

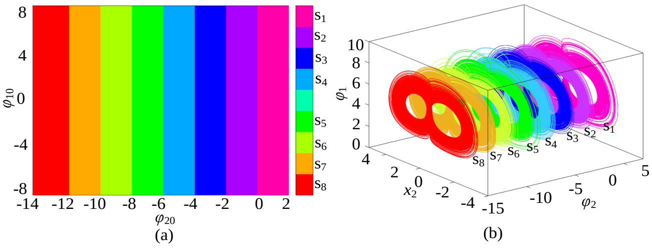


Fig. 10: Initial state-relied chaotic dynamics under k_1=1, k_2=1.5, α=-0.9, β=16, b=0.01, c=1.2, d=5, N=6, x_{10}=x_{20}=0.1. (a) Basin of attraction on the φ_{20}-φ_{10} plane. (b) Initial-boosted coexisting eight double-wing-butterfly attractors.

with the same topology at different positions. When selecting initial state φ_{20} as 1, -1, -3, -5, -7, and -9, the memristive HNN exhibits initial-boosted coexisting six four-wing butterfly attractors, as shown in Fig.11(c). Meanwhile, six chaotic sequences with different positions can be obtained as shown in Fig.11(d). Further simulation shows that when continuing to increase the value of parameter N, the number of the initial-boosted coexisting four-wing butterfly attractors finally tends to infinity. Namely, the memristive HNN can provide sustained and robust chaotic sequences and their oscillating amplitudes can be non-destructively adjusted by switching the memristor initial states.

D. Electronic Circuit Validation

In this subsection, the electronic circuit of the proposed memristive HNN is implemented by using the analog circuit design method, and various butterfly attractors are further verified through MULTISIM circuit simulation. Fig.12 gives the designed memristive HNN circuit which mainly contains three parts, namely the memristor circuit 1, the memristor circuit 2, and the neural network circuit. From Fig.12, the memristor circuit 1 consists of six analog multipliers (M), six resistors, one amplifier, and one capacitor. The memristor 2 is composed of a nonlinear function generator module, where S_1, S_2, ..., and S_i are selection switches. By selecting suitable switches, the control parameter N can be realized in the memristor circuit. The neural network circuit contains two neuron circuits and the neuronal active function is introduced from reference [36]. The circuit equation of the memristive MNN circuit can be written as

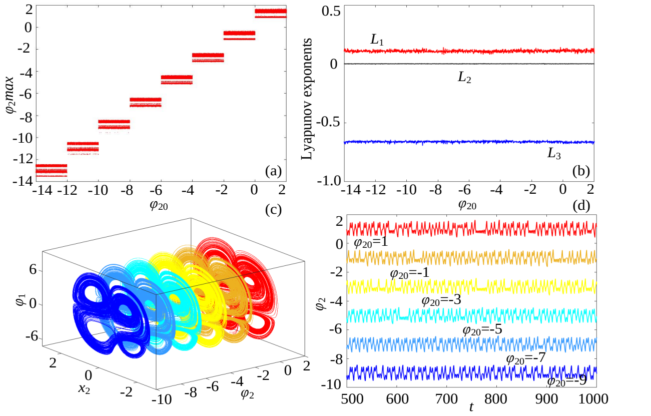


Fig. 11: φ_{20}-relied chaotic dynamics under k_1=1, k_2=1.5, α=-0.25, β=16, b=0.01, c=1.2, d=5, N=6, x_{10}=x_{20}=φ_{10}=0.1. (a) Bifurcation diagram. (b) Lyapunov exponents. (c) Initial-boosted coexisting six four-wing-butterfly attractors. (d) Coexisting six chaotic sequences.

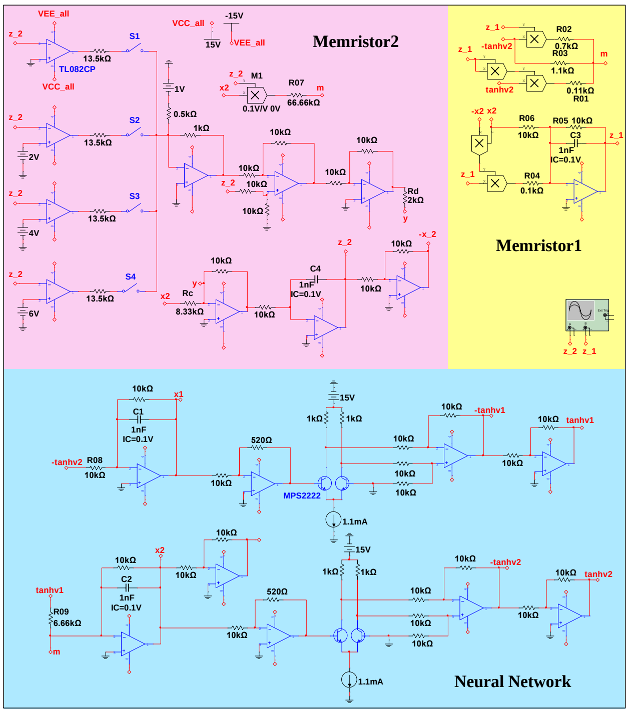
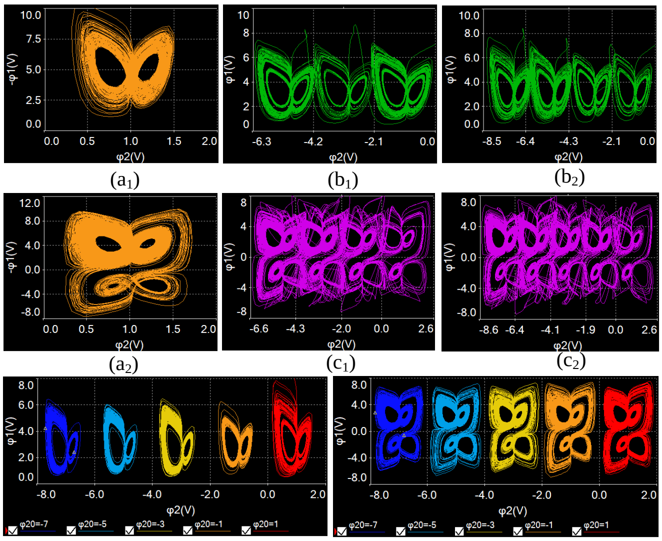


Fig. 12: Memristive HNN circuit structure.

$$
\begin{cases}
C\frac{dx_1}{dt} = -\frac{x_1}{R} + \frac{\tanh(x_2)}{R_8} \\
C\frac{dx_2}{dt} = -\frac{x_2}{R} - \frac{\tanh(x_1)}{R_9} - (\frac{g^2 z_1{}^2}{R_1} - \frac{g z_1}{R_2} - \frac{1}{R_3})\tanh(x_2) + \frac{g z_2 x_2}{R_7} \\
C\frac{dz_1}{dt} = \frac{g^2 x_2{}^2 z_1}{R_4} - \frac{z_1}{R_5} - \frac{x_2}{R_6} \\
C\frac{dz_2}{dt} = \frac{x_2}{R_c} - \frac{h(z_2)}{R_d}
\end{cases}
\tag{14}
$$

where x_1 and x_2 represent the membrane potentials x_1, x_2, z_1, and z_2 represent the memristor states φ_1 and φ_2, respectively. According to the memristive HNN mode (7), part adjustable circuit parameters can be obtained as $R_1 = Rg^2/\alpha k_1$, $R_2 = Rg/\alpha k_1$, $R3 = R/\alpha\beta k_1$, $R_4 = Rg^2$,



(a₁) (b₁) (b₂)

(a₂) (c₁) (c₂)

(d₁) (d₂)

Fig. 13: Experimental results. (a1) Double-wing butterfly attractor. (a2) Four-wing butterfly attractor. (b1) 3-double-wing-butterfly attractor. (b2) 4-double-wing-butterfly attractor. (c1) 4-four-wing-butterfly attractor. (c2) 5-four-wing-butterfly attractor. (d1) Coexisting five double-wing-butterfly attractors. (d2) Coexisting five four-wing-butterfly attractors.

$R_5 = R_6 = R$, $R_7 = Rg/k_2b$, $R_8 = R$, $R_9 = R/1.5$, $R_c = R/c$, $R_d = R/d$, $R = 10$ k, $C = 1nF$, and $g = 0.1$.

To confirm the effectiveness of the designed memristive HNN circuit, the circuit is simulated in the MULTISIM platform. Experiment results show that the designed circuit can generate results consistent with the numerical simulation results. For example, for α=-0.9, considering k_1=1, k_2=1.5, b=0.01, c=1.2, d=5, N=0, β=16, part resistors can be calculated as R_1=0.11 k, R_2=1.1 k, R_3=0.7 k, R_4=0.1 k, R_7=66.66 k, R_9=6.66 k, R_c=8.33 k, R_d=2 k. When only closing S_1, the double-wing butterfly attractor is captured as shown in Fig.13(a1); When changing R_c=5 k (c=2) and closing S_1 and S_2, 3-double-wing-butterfly attractor can be obtained as shown in Fig.13(b1); When closing S_1, S_2, and S_3, 4-double-wing-butterfly attractor can be obtained as shown in Fig.13(b2); When changing R9=6.66k(c=1.2) and selecting different initial capacitor voltages (1V, -1V, -3V, -5V, -7V), coexisting five double-wing butterfly attractors can be obtained as shown in Fig.13(d1). Furthermore, for α=-0.25, part resistors can be calculated as R_1=0.4 k, R_2=4 k, R_3=2.5 k, R_4=0.1 k, R_7=66.66 k, R_9=6.66 k, R_c=8.33 k, R_d=2 k. By repeating the above experimental steps, various four-wing butterfly attractors can be obtained as shown in Fig.13(a2), (c1), (c2), and (d2). Obviously, the circuit simulation results are consistent well with the numerical simulation results.

Additionally, TABLE I gives the summary of the comparison between different memristive HNN modes proposed in recent years. As can be seen from TABLE I, the previous memristive HNN models can only exhibit multi-scroll attractors. The proposed memristive HNN in this work not only can generate more complex multi-butterfly attractors but also requires a minimum of neurons and control parameters. Moreover, the previous memristive HNNs only consider one type of memristive system. The presented memristive HNN in this paper considers two different memristive systems and has more complicated dynamical behavior. Thus, it can be applied in the practical engineering field.

IV. Application to privacy protection in IoMT

Nowadays, the requirements for telemedicine based on the Internet of Medical Things (IoMT) are constantly emerging [45]. The transmission of a vast amount of medical image data that may contain critical or private information through IoMT can easily cause the disclosure of personal privacy information [46, 47]. Hence, it is necessary to take some measures to encrypt and protect medical image data in IoMT. Because the medical image data has special features including high redundancy, large capacity, and high correlation between pixels, the traditional encryption methods cannot fulfill the demands for medical image encryption [39]. Here, to protect the privacy of the medical image data in IoMT, a feasible privacy protection scheme is proposed, where the security key is generated by the constructed multi-butterfly memristive HNN.

A. Design of the Privacy Protection Scheme

Based on the multi-butterfly memristive HNN, the designed privacy protection scheme in IoMT is shown in Fig.14. The scheme consists of five parts: medical data acquisition, encryption terminal, key generator, mobile edge computing (MEC) server, and decryption terminal. When a patient obtains original medical images through various medical devices in a hospital, the original medical images are encypted by smart devices at IoMT device layer. Then the encrypted images in encryption terminal are sent online to MEC severs at edge layer. Clearly, the wireless network and MEC servers can only receive the cipher images, which means the attackers (Hacker) can not directly obtain the original medical images. Meanwhile, the cipher images are downloaded using smart IoMT devices by the doctors in other hospitals at different areas. Finally, the doctors use the key generated by the key generator to perform chaotic decryption to obtain the original medical images in decryption terminal, so as to realize the confidential transmission of the medical images. In this process, the key step is the implementation of encryption and decryption algorithms. A secure and efficient encryption algorithm is designed as follows: (i) Suppose that the original image P has $M \times N$ pixes. Set the system parameters and initial values (α, β, b, c, d, N, k_1, k_2, x_{10}, x_{20}, φ_{10}, φ_{20}) as security keys, then iterate the multi-butterfly memristive HNN (7) with the fourth-order Runge-Kutta algorithm. The previous 1000 numbers iterated by the system will be abandoned because of the transient state. Whereafter, the system is continuously iterated to generate four values, $x_1(i,\ j)$, $x_2(i,\ j)$, $\varphi_1(i,\ j)$, $\varphi_2(i,\ j)$. During iteration, the four values are used to generate two pseudo-random sequence matrixes $K_1(i,\ j)$ and $K_2(i,\ j)$, as follows

$$\begin{cases} K_1(i,j) = Abs(S(i,j)) \\ K_2(i,j) = mod(floor(Abs(S(i,j)))) \times 10^{15}, 256) \\ S(i,j) = (x_1(i,j) + x_2(i,j) + \varphi_1(i,j) + \varphi_2(i,j))/4 \end{cases} \tag{15}$$

where the floor(x) gives as output the greatest integer less than or equal to x. (ii) Then, a processed image P_1 is obtained by using K_1 to perform a permutation to P, where the permutation algorithm is described as P_1=P(index(K_1)). (iii) Next, Employ the matrix K_2 to perform the XOR operation to P_1 as

$$C(i,j) = P_1(i,j) \oplus K_2(i,j) \tag{16}$$

By performing the above encryption processes for two rounds, where the signal generated by the 8-double-wing-butterfly at-

TABLE I: PERFORMANCE COMPARISON BETWEEN DIFFERENT MEMRISTIVE HNNS.

Refs	Attractor Type	Neurons	Memristive Systems	Control Parameters	Initial-Boosting	Electronic Circuit
[29]	Multi-Scroll	3	1	3	No	Yes
[36]	Multi-Scroll	4	1	2	Yes	Yes
[28]	Grid Multi-Scroll	4	1	4	Yes	No
[41]	Grid Multi-Scroll	3	1	4	Yes	No
[42]	Hyperchaotic Multi-Scroll	7	1	2	Yes	Yes
This Paper	Multi-Butterfly	2	2	1	Yes	Yes

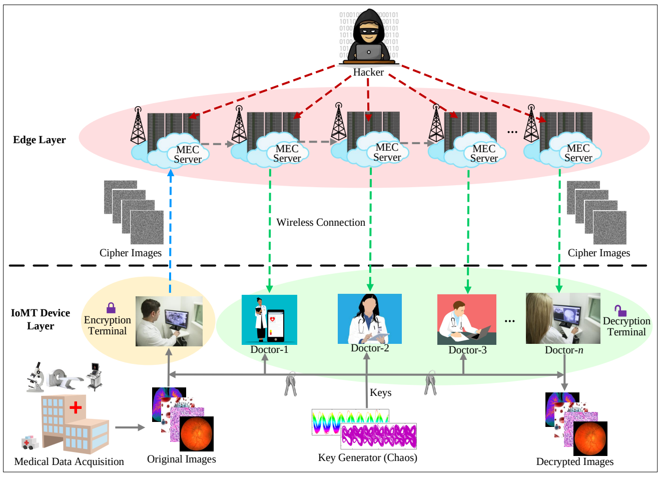


Fig. 14: Framework of the privacy protection in IoMT.

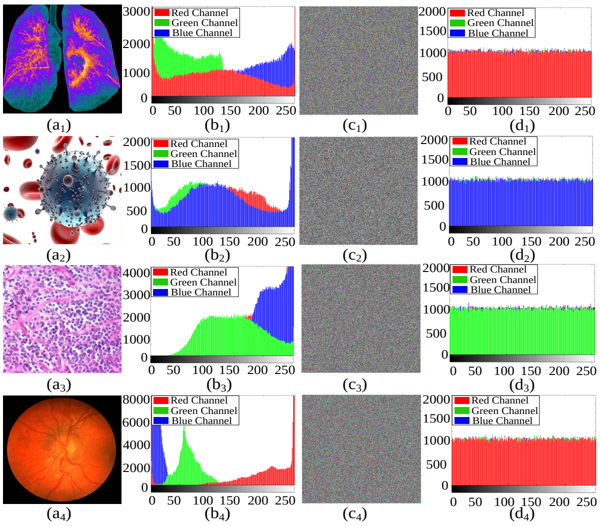


Fig. 15: Test results of the designed privacy protection scheme. (a) Original images. (b) Histograms of the original images. (c) Encrypted images. (d) Histograms of the encrypted images.

tractor in Fig.8(f) is used in the first round of encryption and the signal generated by 7-four-wing-butterfly attractor in Fig.9(f) is employed in the second round. All the parameters are the same as those given in Sec.III-B. As a result, the encrypted image C is yielded. Decryption is the reverse process of the encryption operation.

B. Analysis of the encryption performance

To verify the effectiveness of the designed privacy protection scheme, four (P1-P4) color medical images (512×512) from the publicly available DRIVE database [48] are used for the experimentation based on Matlab R2017a. Note that before performing the encryption process, the color images are divided into red, green, and blue components. To check the encryption performance, histogram, correlation coefficient, information entropy, differential attack, key sensitivity, and noise and data loss attack are analyzed as follows.

(1) Histogram: The histograms of the original images and encrypted images are given in Fig.15(b1-b4) and Fig.15(d1-d4), respectively. As can be seen, the histograms of the encrypted images are very uniform and are significantly different from those of the original images, which means that the designed privacy protection scheme has a strong ability to resist statistical analysis. Therefore, the multi-butterfly memristive HNN provides the encrypted images with a strong ability to resist statistical attacks.

(2) Correlation coefficient: Usually, the correlation coefficient ranges from 0 to 1. The larger the value, the lower the degree of correlation between the values of adjacent pixels in the image. It can be computed by [36]

$$\rho_{xy} = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{N}(y_i - E(y))^2}} \tag{17}$$

where x and y are the intensity values of two adjacent pixels, and N is the total number of pixels. $E(x)$ and $E(y)$ are the averages of x_i and y_i, respectively. For 10000 pairs of adjacent pixels in the four medical images, the correlation coefficients in three directions are listed in Table II. We can clearly see that the correlation coefficients of the original images are close to 1, but those of the encrypted images are very close to 0. That is to say, the multi-butterfly memristive HNN can largely reduce the correlation of the adjacent pixels in the images.

(3) Information Entropy: Information entropy reflects the statistical characteristics of image information. According to Shannon's theory, the information entropy can be calculated by [37]

$$H(P) = \sum_{i=0}^{2^N-1} P(x_i)\log_2\frac{1}{P(x_i)} \tag{18}$$

where N represents the bit depth of the image P and $P(x_i)$ represents the probability of the presence of a pixel x_i. Table I gives the information entropy of the four original medical images and their corresponding encrypted images. We can clearly find that there is a large improvement in information entropy after the original image is encrypted. And they are all very close to the ideal entropy value of 8. Hence, the multi-butterfly memristive HNN plays an important role in improving the information entropy of the original images.

(4) Differential attack: Attackers commonly use a slight change in the image to find the relationship between the original image and its encrypted image, namely differential attacks. The number of pixels change rate (NPCR) and the unified average change intensity (UACI) are usually used to evaluate the ability of differential attacks in encryption algorithms. They can be

TABLE II: TEST RESULTS OF THE CORRELATION COEFFICIENT, INFORMATION ENTROPY, AND DIFFERENTIAL ATTACK

Indexes		Correlation coefficient	Information entropy		Differential attack
Medical Images		Horizontal/Vertica/Diagonal	RGB	Red/Green/Blue	NPCR/UACI
P1	Original	0.99324/0.98773/0.98204	7.0266	6.7115/6.5272/7.0266	99.6087/33.4624
	Encrypted	0.00146/0.00065/-0.00224	7.9998	7.9994/7.9994/7.9994	
P2	Original	0.998346/0.98117/0.96882	6.1061	6.0642/6.0797/6.1087	99.6095/33.4641
	Encrypted	-0.00736/0.00161/0.00113	7.9998	7.9994/7.9996/7.9995	
P3	Original	0.97348/0.96969/0.94784	7.3480	6.8697/7.5988/6.4757	99.6105/33.4628
	Encrypted	0.00435/-0.00242/0.00107	7.9998	7.9997/7.9994/7.9994	
P4	Original	0.99892/0.99843/0.92868	6.1142	5.6857/5.5025/4.2734	99.6092/33.4634
	Encrypted	0.00274/0.00466/-0.00644	7.9998	7.9998/7.9998/7.9998	

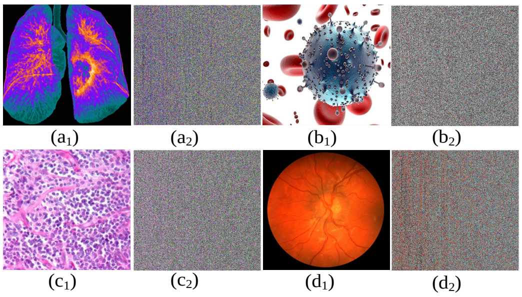


Fig. 16: Decryption results with different keys. (a1-d1) Decrypted images with the accurate keys; (a2) Decrypted image with the inaccurate key x_{10}=0.1+10^{-16}. (b2) Decrypted image with the inaccurate key x_{20}=0.1+10^{-16}. (c2) Decrypted image with the inaccurate key φ_{10}=0.1+10^{-16}. (d2) Decrypted image with the inaccurate key φ_{20}=0.1+10^{-16}.

computed as follows [38]

$$\begin{cases} NPCR(C_1,C_2) = \sum\limits_{i=1}^{M}\sum\limits_{j=1}^{N} \frac{D(i,j)}{M.N} \times 100\% \\ UACI(C_1,C_2) = \frac{1}{M.N}\sum\limits_{i=1}^{M}\sum\limits_{j=1}^{N} \frac{|C_1(i,j)-C_2(i,j)|}{255} \times 100\% \end{cases} \tag{19}$$

where

$$D(i,j) = \begin{cases} 0, & if C_1(i,j) = C_2(i,j) \\ 1, & if C_1(i,j) \neq C_2(i,j) \end{cases} \tag{20}$$

where C_1 and C_2 denote two cipher images, whose corresponding original images only have a single-pixel difference. Through calculation, the average NPCR and UACI values of R, G, and B components in four color images are listed in Table I. Obviously, the NPCR and UACI values are extremely close to the expected values of 99.6094% and 33.4635%, respectively. That is to say, it is very sensitive to small changes in the original images. Therefore, the designed privacey protection scheme has a strong ability to oppose differential attacks.

(5) Sensitivity analysis: The key sensitivity is an important index in the security of encryption algorithms. In general, the more sensitive the key, the more secure the encryption algorithm. Here, the keys x_{10}, x_{20}, φ_{10}, and φ_{20} are selected as test keys. When the four keys and their tiny change are used for decryption respectively, the decryption results are given in Fig.16. As can be seen, even if the key is changed a little (10^{-16}), the decrypted image is absolutely different from the original image. Consequently, the proposed privacy protection scheme has a very high sensitivity to the key.

(6) Data loss and noise attacks: The data loss and noise attacks are usually used to evaluate the robustness of an image encryption algorithm. On one hand, the images are easy to suffer from partial data loss in the process of image transmission. To test the algorithm's ability to resist data loss, we cut off some parts of the cipher image and then decrypt it. Fig.17(a1-a4) and (b1-b4) gives results of data loss attacks for the different lost areas, where the original images are recovered successfully via the decryption process. On the other hand, the encryption system has various noises including salt and pepper noise and Gaussian noise in the operation process. To test the algorithm's ability to resist noise attacks, we added the two kinds of noise to the encrypted image with different proportions. The outcomes of the noise attacks are shown in Fig.17(c1-c4) and (d1-d4). As can be seen, some pixel values in decrypted images are changed, but the approximate information of the original image could still be displayed. This means that the encrypted image still has a good decryption effect after being attacked by noise. Hence, the proposed privacy protection scheme can effectively resist data loss and noise attacks and has very high robustness.

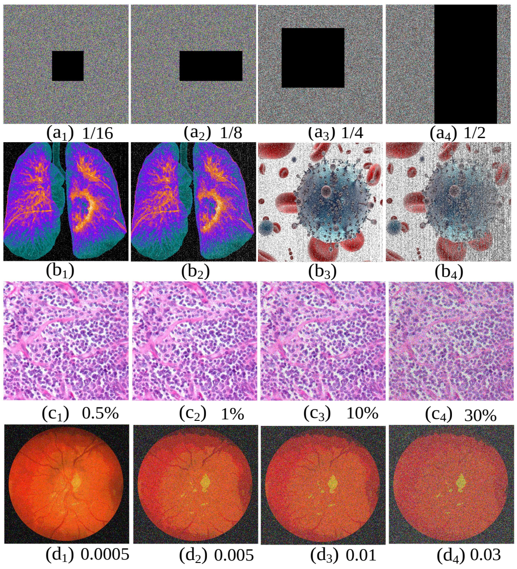


Fig. 17: Test results of data loss and noise attacks. (a1-a4) Encrypted images under partial data loss. (b1-b4) Decrypted images. (c1-c4) Decrypted images of the encrypted images under salt and pepper noise. (d1-d4) Decrypted images of the encrypted images under Gaussian noise.

C. Validation by Hardware experiments

To further verify the effectiveness of the proposed privacy protection scheme, we simulate the IoMT environment in reality, take medical image P4 as an example, and carry out hardware experiments on RPI (Raspberry PI). Hardware equipment includes a computer, a router, and three RPI, and the software is programmed in Python language under the MQTT protocol. As shown in Fig.18, the three RPIs act as publishers, intermediate servers, and subscribers, and are connected to WiFi. The publisher runs under IP 192.168.123.188, the subscriber runs under IP 192.168.123.29, and the publisher RPI and the subscriber RPI are connected to the intermediate server RPI

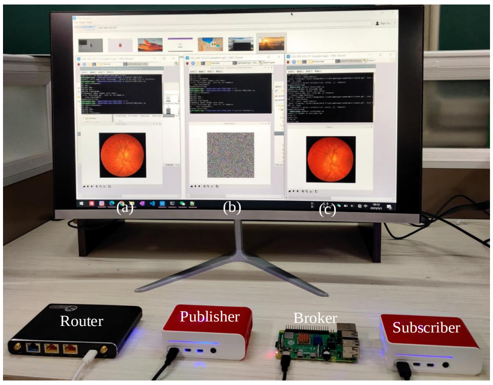


Fig. 18: Experimental demonstration based on IoMT. (a) Original image. (b) Encrypted image. (c) Decrypted image.

under IP 192.168.123.151 at the same time. The development environment mainly includes Dell Intel CoreTM i7 CPU 2.5GHz desktop computer, router, 4b RPI, Python 3.7, EMQX 4.3.10 MQTT protocol, and Rk-4 algorithm. As shown in Fig.18(a), we use the image P4 as the encrypted object, which is sent and received under EMQX(the open-source MQTT agent for IoMT). The key steps of this experiment are as follows:

Step 1: Run subscribers, intermediate servers, and publishers, connect to the router's WiFi, and get the IP address of each RPI.

Step 2: The subscriber specifies the theme and subscribes both the key and the image to the publisher.

Step 3: The publisher selects the file name of the image image to be sent, begins to read the original image data ”512×512-P4”, and performs the preprocessing operations $K_1(i,j) = Abs(S(i,j))$ and $K_2(i,j) = mod(floor(K_1) \times 10^{15}), 256)$.

Step 4: Set the key to (0.1, 0.1, 0.1, 0.1) which is the initial value of system (7). The publisher sends the key to the subscriber, who reads and stores the key.

Step 5: The publisher performs an XOR encryption operation $C(i,j) = P(i,j) \oplus K_2(i,j)$to get the encrypted image as shown in Fig.16, and sends the ciphertext to the subscriber. Because the proposed memristive HNN is extremely sensitive to the initial values, and the generated chaotic sequence is pseudorandom, the encrypted image is difficult to be leaked, destroyed and tampered with, so realizing the privacy protection of medical data.

Step 6: The subscriber receives the message from the publisher, then decrypts the received key and ciphertext, gets the decrypted image ”512×512-P4”, and directly displays and saves the decrypted image, as shown in Fig.18(c).

So far, the scheme has achieved the purpose of protecting the privacy of medical data.

Finally, a performance comparison of encryption results between encryption schemes based on different memristive HNNs is given in Table III. Apparently, this is the first time that the memristive HNN has been applied to color medical image encryption. Compared with similar works, since the proposed memristive HNN has complex multi-butterfly chaotic behavior, the designed privacy protection scheme has higher information entropy, more sensitive secret keys, and more ideal NPCR/UACI values. Meanwhile, it not only has very low correlation coefficients in every direction but also owns high robustness in terms of data loss and noise attacks. Moreover, the designed privacy protection scheme is experimentally verified in IoMT. Consequently, it can be applied to reinforce information security in real-world medical internet networks.

V. Conclusion

This paper designs two new voltage-controlled memristor models. Based on the two memristors, a novel memristive HNN with two memristive systems is constructed. Theoretical analysis and numerical simulation show the complex dynamical behaviors of the memristive HNN, including double-wing and four-wing butterfly chaotic attractors, multi-double-wing-butterfly and multi-four-wing-butterfly chaotic attractors, as well as initial-boosted coexisting infinitely many double-wing and four-wing butterfly chaotic attractors. Both the number of butterflies contained in the multi-butterfly attractors and the number of coexisting butterfly attractors can be controlled by only one control parameter of the memristor. Furthermore, chaotic sequences generated by the multi-butterfly memristive HNN are applied to privacy protection in IoMT, using medical images as an example. The privacy protection scheme is designed using the simplest permutation-diffusion structure based on the multi-butterfly memristive HNN. Test results demonstrate that the designed privacy protection scheme can effectively encrypt the information of the color medical images and is superior to some existing encryption schemes. Finally, a hardware platform based on RPI under the MQTT protocol is built to verify the effectiveness of the designed privacy protection scheme by simulating a practical IoMT environment. Experimental results show that the proposed privacy protection scheme can successfully realize the privacy protection of medical data, which provides a reference for the data security governance of the medical industry.

It is worth mentioning that the Lorenz-like butterfly and multi-butterfly chaotic attractors are found for the first time in the neural networks. How to use the proposed method to generate grid or space multi-butterfly chaotic attractors in the neural networks is worthy of being studied deeply. Another issue worthy of further investigation is that the multi-butterfly memristive HNN designed in this article successfully applies in IoMT, but whether this network applies to other information transmission fields such as vehicle networking, electronic payment, and smart home remains to be studied. In the future, we will be devoted to address these issues.

References

[1] M. Breakspear, “Dynamic models of large-scale brain activity,” *Nat. Neurosci.*, vol. 20, no. 3, pp. 340-352, 2017.

[2] Z. Aram, S. Jafari, J. Ma, et al, “Using chaotic artificial neural networks to model memory in the brain,” *Commun. Nonlinear Sci. Numer. Simul.*, vol. 44, pp. 449-459, 2017.

[3] Y. Liang, S. Chen, Z. Lu, et al, “A new compact model for third-order memristive neuron with box-shaped hysteresis and dynamics analysis,” *IEEE Trans Comput-Aided Des Integr Circuits Syst.*, vol. 42, no. 10, pp. 3352-3364, 2023.

[4] 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.

[5] H. Lin, C. Wang, C. Chen, et al, “Neural bursting and synchronization emulated by neural networks and circuits,” *IEEE Trans. Circuits Syst. I.*, vol. 68, no. 8, pp. 3397-3410, Aug. 2021.

[6] S. He, D. Vignesh, R. Li, et al, “Chaos and firing patterns in a discrete fractional Hopfield neural network model,” *Nonlinear Dyn.*, vol. 111, pp. 21307-21332, 2023.

[7] P. C. Rech. “Chaos and hyperchaos in a Hopfield neural network,” *Neurocomputing.*, vol. 74, no. 17, pp. 3361-3364, 2011.

[8] C. Chen, F. Min, Y. Zhang, et al, “ReLU-type Hopfield neural network with analog hardware implementation,” *Chaos, Solitons, Fractals.*, vol. 167, Art. no. 113068, 2023.

TABLE III: PERFORMANCE COMPARISON OF THE ENCRYPTION SCHEMES BASED ON DIFFERENT HNNS

Refs	Image type	Dynamical behavior	Entropy	Key sensitivity	Correlation (V,H,D)	NPCR UACI	High robustness	Validation method
[37] 2021	Gray medical images (256×256)	Multistability	7.9992	– –	0.0026 0.0026 – –	99.6175 – –	No	Matlab simulation
[39] 2022	Gray medical images (256×256)	Extreme multistability	7.9981	10^{-12}	0.0017 0.0008 0.0134	99.6101 33.4672	Yes	FPGA experiment
[38] 2023	Gray medical images (256×256)	Hyperchaos	7.9947	– –	0.0170 0.0030 0.0032	99.9779 33.3976	No	Matlab simulation
[41] 2023	Gray medical images (256×256)	Multi-scroll attractors	7.9977	– –	0.0006 0.0024 0.0047	99.6078 33.4875	No	IoT application
[42] 2023	Gray commercial images (256×256)	Hyperchaotic multi-scroll attractors	7.9976	– –	0.0005 0.0090 0.0040	99.5953 33.5107	Yes	IoT application
This work	Color medical images (512×512)	Multi-butterfly attractors	7.9998	10^{-16}	0.0040 0.0023 0.0027	99.6095 33.4632	Yes	IoMT application

[9] M. P. Asir, A. Prasad, N. V. Kuznetsov, et al, "Chimera states in a class of hidden oscillatory networks," *Nonlinear Dyn.*, vol. 104, pp. 1645-1655, 2021.

[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] C. Pan, Q. Hong, X. Wang, "A novel memristive chaotic neuron circuit and its application in chaotic neural networks for associative memory," *IEEE Trans Comput-Aided Des Integr Circuits Syst.*, vol. 40, no. 3, pp. 521-532, 2021.

[12] H. Bao, Z. Hua, H. Li, et al, "Memristor-based hyperchaotic maps and application in auxiliary classifier generative adversarial nets," *IEEE Trans. Ind. Informat.*, vol. 18, no. 8, pp. 5297-5306, 2021.

[13] F. Yuan, S. Li, Y. Deng, et al, "Cu-Doped TiO2x Nanoscale Memristive Applications in Chaotic Circuit and True Random Number Generator," *IEEE Trans. Ind. Electron.*, vol. 70, no. 4, pp. 4120-4127, 2022.

[14] V. T. Pham, S. Jafari, S. Vaidyanathan, et al, "A novel memristive neural network with hidden attractors and its circuitry implementation," *Sci. China Technol. Sci.*, vol. 59, no. 3, pp. 358-363, 2015

[15] X. Hu, C. Liu, L. Liu, et al, "Chaotic dynamics in a neural network under electromagnetic radiation," *Nonlinear Dyn.*, vol. 91, pp. 1541-1554, 2018.

[16] H. Ran, S. Wen, S. Wang, et al, "Memristor-based edge computing of ShuffleNetV2 for image classification," *IEEE Trans Comput-Aided Des Integr Circuits Syst.*, vol. 40, no. 8, pp. 1701-1710, 2021.

[17] S. Duan, X. Hu, Z. Dong, et al, "Memristor-based cellular nonlinear/neural network: Design, analysis, and applications," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 26, no. 6, pp. 1202-1213, Jun. 2015.

[18] O. Krestinskaya, K. N. Salama, A. P. James, "Learning in memristive neural network architectures using analog backpropagation circuits," *IEEE Trans. Circuits Syst. I.*, vol. 66, no. 2, pp. 719-732, Feb. 2019.

[19] Q. Hong, Y. Li, X. Wang, "Memristive continuous Hopfield neural network circuit for image restoration," *Neural Comput. Appl.*, vol. 32, pp. 8175-8185, 2020.

[20] 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.

[21] M. Wang, J. Peng, X. Zhang, et al, "Firing activities analysis of a novel small heterogeneous coupled network through a memristive synapse," *Nonlinear Dyn.*, vol. 111, pp. 15397-15415, 2023.

[22] 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.

[23] 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.

[24] 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, 2022.

[25] H. Lin, C. Wang, F. Yu, et al, "A triple-memristor Hopfield neural network with space multi-structure attractors and space initial-offset behaviors," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 42, no. 12, pp. 4948-4958, 2023.

[26] I. S. Doubla, B. Ramakrishnan, Z. N. Tabekoueng, et al, "Infinitely many coexisting hidden attractors in a new hyperbolic-type memristor-based HNN," *Eur. Phys. J.-Spec. Top*, vol. 231, no. 11, pp. 2371-2385, 2022.

[27] 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.

[28] 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, 2022.

[29] 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.

[30] H. Lin, X. Deng, F. Yu, et al, "Grid multibutterfly memristive neural network with three memristive systems: modeling, dynamic analysis, and application in police IoT," *IEEE Internet Things J.*, DOI: 10.1109/JIOT.2024.3409373, 2024.

[31] 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.

[32] 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.

[33] N. Lin, X. Chen, H. Lu, et al. "Chaotic weights: a novel approach to protect intellectual property of deep neural networks," *IEEE Trans Comput-Aided Des Integr Circuits Syst.*, vol. 40, no. 7, pp. 1327-1339, 2021.

[34] Y. Sha, J. Mou, S. Banerjee, et al, "Exploiting flexible and secure cryptographic technique for multi-dimensional image based on graph data structure and three-input majority gate," *IEEE Trans. Ind. Informat.*, vol. 20, no.3, pp. 3835-3846, 2024.

[35] W. Liu, K. Sun, S. He, et al, "The parallel chaotification map and its application," *IEEE Trans. Circuits Syst. I.*, vol. 70, no. 9, pp. 3689-3698, 2023.

[36] 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.

[37] Z. T. Njitacke, S. D. Isaac, T. Nestor, et al, "Window of multistability and its control in a simple 3D Hopfield neural network, pp. application to biomedical image encryption," *Neural Comput Appl.*, vol. 33, pp. 6733-6752, 2021.

[38] D. Jiang, Z. T. Njitacke, J. D. D. Nkapkop, 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, 2022.

[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] 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, 2021.

[41] 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, 2022.

[42] 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.

[43] 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.

[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.

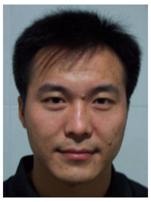
[45] Z. T. Njitacke, J. D. D. Nkapkop, V. F. Signing, et al, "Novel extreme multistable tabu learning neuron: circuit implementation and application to cryptography," *IEEE Trans. Ind. Informat.*, vol. 19, no. 8, pp. 8943-8952, 2023.

[46] 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, 2021.

[47] X. Deng, H. Tang, X. Pei, et al, "MDHE: a malware detection system based on trust hybrid user-edge evaluation in IoT network," *IEEE Trans. Inf. Forensics Security.*, vol. 18, pp.5950-5963, 2023.

[48] J. Staal, M. D. Abràmoff, M. Niemeijer, et al, "Ridge-based vessel segmentation in color images of the retina," *IEEE Trans. Med. Imaging.*, vol. 23, no. 4, pp. 501-509, 2004.

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 a 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 three national and provincial projects, and published more than 50 papers in related international journals, such as IEEE-TIE, IEEE-TII, IEEE-TCAD, IEEE-IoT, etc. His research interests include chaotic neural networks, information and network security, 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 Institue, 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 recognization.

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.