

# Brain-like initial-boosted hyperchaos and application in biomedical image encryption

Hairong Lin, Chunhua Wang, Li Cui, Yichuang Sun, *Senior Member, IEEE*, Cong Xu, and Fei Yu

**Abstract**—Neural networks have been widely and deeply studied in the field of computational neurodynamics. However, coupled neural networks and their brain-like chaotic dynamics have not been noticed yet. This paper focuses on the coupled neural network-based brain-like initial boosting coexisting hyperchaos and its application in biomedical image encryption. We first construct a memristive coupled neural network (MCNN) model based on two sub-neural networks and one multistable memristor synapse. Then we investigate its coupling strength-related dynamical behaviors, initial states-related dynamical behaviors, and initial-boosted coexisting hyperchaos using bifurcation diagrams, phase portraits, Lyapunov exponents and attraction basins. The numerical results demonstrate that the proposed MCNN can not only generate hyperchaotic attractors with high complexity but also boost the attractor positions by switching their initial states. This makes the MCNN more suitable for many chaos-based engineering applications. Moreover, we design a biomedical image encryption scheme to explore the application of the MCNN. Performance evaluations show that the designed cryptosystem has several advantages in the key space, information entropy, and key sensitivity. Finally, we develop a field-programmable gate array (FPGA) test platform to verify the practicability of the presented MCNN and the designed medical image cryptosystem.

**Index Terms**—Hopfield neural network, Hyperchaos, medical image encryption, memristor, FPGA implementation

## I. INTRODUCTION

IN 1984, a powerful artificial neural network model, known as the Hopfield neural network (HNN) [1], was first presented. Due to the intrinsic attributes of the HNN, including flexible topology, strong nonlinearity, rich chaotic dynamics, and easy circuit realization, the HNN is regarded as a typical paradigm of theoretical and experimental research on brain nervous networks. As we all know, the brain nervous network which is a complex nonlinear dynamical system has abundant chaotic behaviors [2]. Numerous physiological and physical experiments show that the chaotic behavior in the brain is highly related to thinking, memory, and learning which play a crucial role in the artificial intelligence field [3]. Indeed, brain-like chaos research is conducive to better understand the neural functions of the human brain and is also potentially useful for developing new neuromorphic systems [4]. In view of this, the brain-like chaos has become a research focus in academia and industrial fields since the birth of the famous Hopfield neural network.

After nearly half a century of in-depth study, many important achievements on the brain-like chaos have been made constantly. For example, normal chaos, transient chaos, and hyperchaos have been detected in some simple Hopfield neural networks

with several neurons [5]. In particular, the study of coexisting attractors in Hopfield neural networks has been of recent interest. Coexisting attractors are a phenomenon that there are two or more different chaotic attractors in the same dynamical system under different initial states [6], [7]. Such special dynamics exists in many biological neural systems, which reflects the diversity and complexity of the brain's nervous system [8]. Further studies revealed that some memristive Hopfield neural networks can yield coexisting attractors with independent basins of attraction [9]. For instance, in [10], the phenomenon of coexisting two asymmetric attractors is discovered in a memristive hyperbolic-type HNN with three neurons. In [11], the behavior of coexisting multiple attractors, namely multistability, is observed in the memristive HNN with two neurons. Furthermore, a memristive multistable four-neuron-based HNN with a more complex coexisting phenomenon of coexisting infinite number of chaotic attractors is revealed in [12]. Such a phenomenon means that the HNN generates extreme multistability that plays a key role in biological nervous systems. As it can be seen, in most of the previous outcomes, the researchers primarily focused on simple neural networks with few neurons. The complex neural networks with multiple neurons, especially for the coupled neural networks and their brain-like chaotic dynamics have not yet been explored.

Initial offset boosting behavior is a kind of new complex dynamics following multistability and extreme multistability [13]. This behavior means the coexistence of infinitely many attractors with the same shape and different positions. Particularly, the initial offset-boosted coexisting chaotic attractors can provide sustained and robust boosted chaotic sequences and their oscillating amplitudes can be non-destructively controlled by switching the initial states flexibly. These merits make them more practical for chaos engineering applications [14]. Over recent years, tremendous research efforts have been devoted to the initial offset boosting behavior in several dynamical systems, such as memristor-based continuous-time chaotic systems [15] and sine function-based discrete-time chaotic systems [16], [17]. Although researchers found that many dynamical systems can show the initial-boosted coexisting phenomenon, there are only a few results on such complex dynamics in the field of computational neurodynamics. Recently, Bao et al [18] discovered initial offset boosting firing behavior in a memristive HR neuron model with a sine memductance synapse. Moreover, Zhang et al [19] constructed a memristive HNN with a multi-piecewise cubic nonlinearity memristor autapse, from which initial offset boosting coexisting chaos was analyzed. To our knowledge, the phenomenon of initial boosting coexisting hyperchaos has not yet been observed in neural networks.

With the rapid development of chaos theory and computer technology, more and more scientists focus on brain-like chaos applications in various industrial fields [20]. Thanks to its abundant variety of bifurcations and chaos, the HNN has been used for information protection [21]. As a combination of neural networks and chaos, the chaotic Hopfield neural network has both the characteristics of neural networks and chaos. Particularly, compared with general dynamical systems, it has more complex dynamical behaviors. So, it is more suitable for information

Manuscript received October 12, 2021; This work is supported by The Major Research Project of the National Natural Science Foundation of China (91964108), The National Natural Science Foundation of China (61971185, 61504013), The Natural Science Foundation of Hunan Province (2020JJ4218). (Corresponding author: Chunhua Wang.)

Hairong Lin, Chunhua Wang, Cong Xu are with the College of Computer Science and Electronic Engineering, Hunan University, Changsha, 410082, China. (haironglin66@hnu.edu.cn; wch1227164@hnu.edu.cn)

Li Cui is with the school of information and electrical engineering, Hunan University of Science and Technology, Xiangtan, 411201, China.

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

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

protection and encryption, especially in biomedical applications. Over the last few decades, the HNNs have been widely applied in normal image encryption due to their chaotic characteristic [22]. Nonetheless, the HNN-based biomedical image encryption schemes are rarely reported in previous investigations. With the development of information technology, medical images play an important role, especially in the remote diagnosis and treatment of patients [23]. However, since the medical images own some intrinsic features such as large sizes and high correlation among pixels, traditional encryption algorithms such as DES, IDEA, and RSA are generally not suitable for practical medical image encryption. Very recently, Njitacke et al [24] presented a chaotic neural network-based medical image encryption scheme, and the advantage of neural networks with chaos in medical image encryption is well demonstrated. So far, however, the chaotic coupled neural networks have not been applied in biomedical image encryption. Indeed, coupling two neural networks in a single network may achieve many advantages over the single neural network like larger key space, uniform key distribution, extraordinary randomness, distribution and amplified chaotic range.

Motivated by the above analysis, this paper researches the brain-like chaotic dynamics of the coupled neural network and its application in biomedical image encryption. To the best of our knowledge, this is the first time that the brain-like chaotic dynamics of the coupled neural network is investigated. The main novelty and contributions of this study are summarized as follows:

- 1) We construct a memristive coupled neural network model based on two sub-neural networks and one memristor synapse.
- 2) The MCNN exhibits rich and complex brain-like initial-boosted dynamics, where infinitely many coexisting hyperchaotic attractors sharing the same shape but with different positions are generated. To the best of our knowledge, this peculiar feature has rarely been detected in other neural networks.
- 3) We design a biomedical image encryption cryptosystem by using the initial-boosted coexisting hyperchaotic sequences to show the practical application of the presented MCNN. In comparison with the existing chaos-based image encryption schemes, the designed cryptosystem has many merits, such as large key space, high information entropy, highly sensitive key, and good robustness.
- 4) FPGA-based hardware experiments are performed to demonstrate the existence of the initial-boosted coexisting hyperchaos and the effectiveness of the biomedical image cryptosystem.

The rest of the article is organized as follows. Section II describes the mathematical model of the new MCNN. Section III reveals the brain-like initial-boosted hyperchaotic dynamics of the MCNN. Section IV designs a biomedical image cryptosystem based on the MCNN and its security performances are analyzed. Section V elaborates an FPGA hardware platform to implement the MCNN and the medical image cryptosystem. Section VI summarizes the paper.

## II. MEMRISTIVE COUPLED NEURAL NETWORK

This section first proposes two small sub-neural networks. Then we designed a new memristor model and verifies its frequency/initial state-relied voltage-current loci. Finally, a memristive coupled neural network is constructed.

### A. Sub-Neural Networks Description

Hopfield neural network with brain-like chaos can be used to mimic the chaotic behaviors of the brain nervous system. The

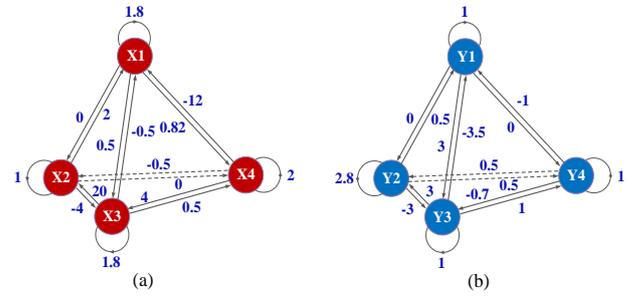


Fig. 1: Connection topologies of two sub-neural networks. (a) Sub-neural network  $X$ . (b) Sub-neural network  $Y$ .

mathematical formula of the Hopfield neural network which is composed of  $n$  neurons can be given by [1]

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

where  $C_i$ ,  $R_i$ , and  $v_i$  are respectively capacitance, resistance, and potential of the cell membrane in neuron  $i$ .  $w_{ij}$  is the synaptic weight coefficient describing the connection strength from neuron  $j$  to neuron  $i$ . Besides,  $\tanh(\cdot)$  represents the neuron activation function, and  $I_i$  denotes an external input current. It should be noted that the chaotic dynamics of the HNN highly depends on  $w_{ij}$ . Therefore, based on the original HNN in (1), selecting the appropriate synaptic weight coefficients by adopting the trial and error method, two different sub-neural networks with four neurons can be constructed, as shown in Fig.1. In Fig.1,  $X_i$  and  $Y_i$  are eight neurons, respectively. Assuming  $C_i=1$ ,  $R_i=1$ ,  $I_i=0$  ( $i=1,2,3,4$ ), the presented two sub-neural networks can be respectively described as follows:

$$\begin{cases} \dot{x}_1 = -x_1 + 1.8 \tanh(x_1) + 2 \tanh(x_2) - 0.5 \tanh(x_3) \\ \quad - 12 \tanh(x_4) \\ \dot{x}_2 = -x_2 + \tanh(x_2) + 20 \tanh(x_3) - 0.5 \tanh(x_4) \\ \dot{x}_3 = -x_3 + 0.5 \tanh(x_1) - 4 \tanh(x_2) + 1.8 \tanh(x_3) \\ \quad + 4 \tanh(x_4) \\ \dot{x}_4 = -x_4 + 0.82 \tanh(x_1) + 0.5 \tanh(x_3) + 2 \tanh(x_4) \end{cases}, \quad (2)$$

$$\begin{cases} \dot{y}_1 = -y_1 + \tanh(y_1) + 0.5 \tanh(y_2) - 3.5 \tanh(y_3) \\ \quad - \tanh(y_4) \\ \dot{y}_2 = -y_2 + 2.8 \tanh(y_2) + 3 \tanh(y_3) + 0.5 \tanh(y_4) \\ \dot{y}_3 = -y_3 + 3 \tanh(y_1) - 3 \tanh(y_2) + \tanh(y_3) \\ \quad - 0.7 \tanh(y_4) \\ \dot{y}_4 = -y_4 + 0.5 \tanh(y_2) + \tanh(y_3) + \tanh(y_4) \end{cases}, \quad (3)$$

where  $x_i$  and  $y_i$  are the membrane potentials of neurons  $X_i$  and  $Y_i$ , respectively.

### B. Memristor Model Design

Memristors can be employed to imitate biological neural synapses, to describe electromagnetic induction effects, or to simulate the magnetic coupling between neurons [25]. Based on the generalized memristor model [26], a flux-controlled memristor was proposed to emulate biological neural synapses recently [12]. Based on the flux-controlled memristor, an improved flux-controlled memristor is described as

$$\begin{cases} i = W(\varphi)v = \varphi v \\ d\varphi/dt = \sin(\pi\varphi) + v \end{cases}, \quad (4)$$

where  $v$ ,  $i$ , and  $W(\varphi)=\varphi$  are voltage, current, and memductance functions of the memristor. It is noted that the state equation for the memristor associates not only with the applied stimulus but also with its inner state flux variable  $\varphi$ .

To show the voltage-current loci of the memristor given in (4), a sinusoidal voltage  $v = A\sin(2\pi Ft)$  is added to the input of the presented memristor. Here,  $A$  and  $F$  are the amplitude and

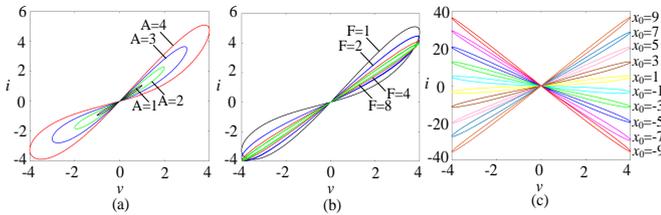


Fig. 2: The fingerprints of the memristor driven by  $v=A\sin(2\pi Ft)$ . (a) Amplitude-relied voltage-current loci for  $A=1, 2, 3,$  and  $4$  with  $F=1$  and  $x_0=0$ . (b) Frequency-relied voltage-current loci for  $F=1, 2, 4,$  and  $8$  with  $A=4$  and  $x_0=0$ . (c) Initial state-relied voltage-current loci for  $x_0=\pm 1, \pm 3, \pm 5, \pm 7,$  and  $\pm 9$  with  $A=4$  and  $F=1$ .

frequency of the sinusoidal voltage. Firstly let  $F=1$ . For  $A=1, 2, 3,$  and  $4$  with  $x_0=0$ , the amplitude-relied voltage-current loci in the  $v-i$  plane are plotted in Fig.2(a). Secondly, for  $F=1, 2, 4, 8,$  with fixed  $A=4, x_0=0$ , the frequency-relied voltage-current loci in the  $v-i$  plane are plotted in Fig.2(b). Finally, denote  $A=4, F=1$ . For  $x_0=\pm 9, \pm 7, \pm 5, \pm 3,$  and  $\pm 1$ , the initial state-relied voltage-current loci in  $v-i$  plane are drawn in Fig.2(c). As can be seen, the voltage-current loci in Fig.2 perfectly illustrates the three fingerprints of the memristor [26]. Additionally, Fig.2(c) shows that the designed memristor displays multiple different pinched hysteresis loops under different initial states. That is to say, the memristor is a multistable memristor, which means that it has the feature of multistability. As we all know, biological synapses are malleable due to their multistable nature. Therefore, the multistable memristor is the best candidate for simulating neural synapses.

### C. Memristive Coupled Neural Network Construction

As we all know, the human brain is composed of various encephalic regions with different neurological functions. And abundant evidences show that there are strong connections between different encephalic regions, and the functional connectivity between different brain regions exhibits complex nonlinear dynamics. For example, both the frontal lobe and the parietal lobe in the brain play a key role in language and thought [27]. Also, when the occipital lobe is damaged, not only visual impairment occurs, but also memory deficiency and motion perception disorder. Consequently, the study of the dynamical behavior of the coupled neural networks with two different sub-neural networks, namely encephalic regions, is significant and valuable. It is well known that synapses play an important role in the signal exchange and information encoding between neurons and neuronal networks. And memristor is usually used to emulate biological neural synapses between neurons [28]. When there is a membrane potential difference between two neurons, a magnetic induction current can be sensed. Base on this strategy, a reduced diagram is plotted for a new memristive coupled neural network with a memristor synapse in Fig.3, in which the two sub-neural networks represent two different encephalic regions in the brain. Considering the two sub-neural networks in (2) and (3), as well as the multistable memristor in (4), the memristive coupled neural

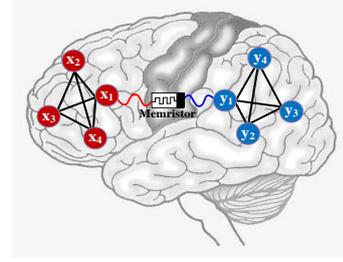


Fig. 3: Concept diagram of the memristive coupled neural network.

network is mathematically modeled by

$$\begin{cases} \dot{x}_1 = -x_1 + 1.8 \tanh(x_1) + 2 \tanh(x_2) - 0.5 \tanh(x_3) \\ \quad - 12 \tanh(x_4) + \rho\varphi(x_1 - y_1) \\ \dot{x}_2 = -x_2 + \tanh(x_2) + 20 \tanh(x_3) - 0.5 \tanh(x_4) \\ \dot{x}_3 = -x_3 + 0.5 \tanh(x_1) - 4 \tanh(x_2) + 1.8 \tanh(x_3) \\ \quad + 4 \tanh(x_4) \\ \dot{x}_4 = -x_4 + 0.82 \tanh(x_1) + 0.5 \tanh(x_3) + 2 \tanh(x_4) \\ \dot{y}_1 = -y_1 + \tanh(y_1) + 0.5 \tanh(y_2) - 3.5 \tanh(y_3) \\ \quad - \tanh(y_4) - \rho\varphi(x_1 - y_1) \\ \dot{y}_2 = -y_2 + 2.8 \tanh(y_2) + 3 \tanh(y_3) + 0.5 \tanh(y_4) \\ \dot{y}_3 = -y_3 + 3 \tanh(y_1) - 3 \tanh(y_2) + \tanh(y_3) \\ \quad - 0.7 \tanh(y_4) \\ \dot{y}_4 = -y_4 + 0.5 \tanh(y_2) + \tanh(y_3) + \tanh(y_4) \\ \dot{\varphi} = \sin(\pi\varphi) + (x_1 - y_1) \end{cases}, \quad (5)$$

where the additive nonlinear term  $\rho\varphi(x_1 - y_1)$  denotes the induction current which is induced by the two adjacent neurons  $X_1$  and  $Y_1$  with different membrane potentials. And  $\rho$  is the coupling strength of the memristive magnetic induction effect. The term  $\sin(\pi\varphi)$  represents an additional magnetic flux caused by the membrane potential fluctuation.

The equilibria of the MCNN and their stabilities are investigated by theoretical and numerical analysis methods. MATLAB numerical calculations show that there are infinitely discrete equilibria that can be expressed as

$$\begin{aligned} E &= \{(x_1^*, x_2^*, x_3^*, x_4^*, y_1^*, y_2^*, y_3^*, y_4^*, z^*) \\ &= (0, 0, 0, 0, 0, 0, 0, 0, k), k = 0, \pm 1, \pm 2, \pm 3, \dots, \pm n \end{aligned} \quad (6)$$

Obviously, the MCNN generates infinitely many equilibria along the axis- $z$  by changing phase space. Therefore, the multistable memristor synapse plays a key role in the generation of complex dynamics due to its infinite many equilibria. With help of MATLAB numerical calculation for different parameters  $k$  and  $\rho$ , the eigenvalues of the equilibrium points and their stabilities are given in Table I. According to Table I, the equilibrium point set  $E$  are always unstable saddle-focus points. Consequently, the chaotic and hyperchaotic attractors generated from the MCNN are self-excited attractors.

As we all know, the dynamics of synchronization in MCNNs has been widely investigated in past decades [29]-[31]. However, to the best of our knowledge, the chaotic dynamics of the MCNNs has never been studied. Actually, chaos plays an important role in brain neural systems [2]. Consequently, the research on chaotic dynamics of the MCNNs is valuable for better understanding brain functions.

### III. DYNAMICAL ANALYSIS OF THE MEMRISTIVE COUPLED NEURAL NETWORK

Chaotic behaviors widely exist in many specific areas of the brain, which plays crucial roles in the information processing and transmission between two different encephalic regions. In this section, the complex brain-like chaotic dynamics of the proposed memristive coupled neural network with eight neurons in (5) are revealed by using basic dynamic analysis methods including

TABLE I: ADJUSTABLE PARAMETERS, EIGENVALUES OF EQUILIBRIA, AND CORRESPONDING STABILITIES.

$k$	$\rho$	Eigenvalues	Stabilities
0	0.17/2.5	$(\pi, 1.1824, -0.1867, 0.2902 \pm 8.9328j, 1.0098 \pm 2.8740j, 0.4021 \pm 4.3827j)$	Unstable Saddle-focus
-1	0.17	$(-\pi, 1.1098, -0.1904, 0.2879 \pm 8.9310j, 0.3554 \pm 4.3645j, 0.9270 \pm 2.8723j)$	Unstable Saddle-focus
1	0.17	$(-\pi, 1.2554, -0.1835, 0.2928 \pm 8.9343j, 0.448 \pm 4.3927j, 1.0925 \pm 2.8728j)$	Unstable Saddle-focus
-1	2.5	$(-\pi, 1.9989, -0.0134, 0.2759 \pm 8.8982j, 0.4141 \pm 3.8945j, 0.0161 \pm 1.6369j)$	Unstable Saddle-focus
1	2.5	$(-\pi, 3.3347, -0.1639, 0.3268 \pm 8.9345j, 0.7290 \pm 4.1810j, 2.0588 \pm 1.9811j)$	Unstable Saddle-focus

bifurcation diagrams, Lyapunov exponents, phase portraits, and attraction basins. And all the numerical simulations are done in MATLAB R2017a with the ODE45 algorithm. Additionally, the start time, the time step, and the time length are set as 500, 0.01, and 3000, respectively.

#### A. Coupling Strength-Relied Dynamical Behaviors

Firstly, when the coupling strength  $\rho$  increases from 0 to 3, the  $\rho$ -based bifurcation diagram is plotted by Fig.4(a) under initial states  $(1, 1, 1, 1, 1, 0, 0, 1, 1)$ , where  $x_{1max}$  is the maxima of the membrane potential  $x_1$ . Moreover, the corresponding first six Lyapunov exponents are shown in Fig. 4(b). It can be seen from Fig.4 that the MCNN can generate complex dynamical behaviors including period, quasi-period, chaos, and hyperchaos. For example, the MCNN intermittently exhibits periodic and quasiperiodic attractors in the region  $\rho \in (0.17, 0.32)$ . And in the region  $\rho \in (0.33, 1.1)$ , the MCNN generates chaotic attractors with one positive Lyapunov exponent. Another promising finding is that hyperchaotic attractors with two positive Lyapunov exponents can be detected in the coupled neural network within the region  $\rho \in (1.2, 2.9)$ . The phase portraits of the MCNN with different values of  $\rho$  are given to illustrate its dynamical evolution with the coupling strength of the memristor synapse, as shown in Fig.5. Fig.5 suggests that the MCNN successively produces periodic, quasiperiodic, chaotic, and hyperchaotic attractors with the increase of  $\rho$  under initial states  $(1, 1, 1, 1, 1, 0, 0, 1, 1)$ .

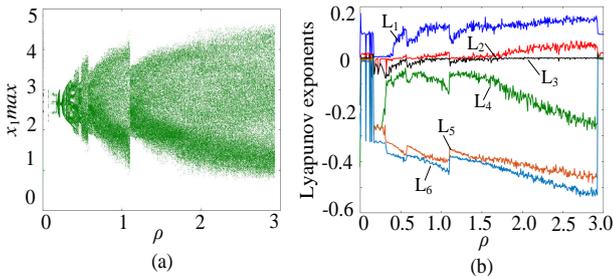


Fig. 4: The  $\rho$ -dependent dynamics with initial states  $(1, 1, 1, 1, 1, 0, 0, 1, 1)$ . (a) Bifurcation diagram. (b) First six Lyapunov exponents.

#### B. Initial State-Relied Dynamical Behaviors

High sensitivity to initial states is one of the main characteristics of the nervous systems. In this subsection, the phenomenon related to the initial states is revealed in the MCNN. When the coupling strength  $\rho=0.17$ , initial values  $x_{10}=x_{20}=x_{30}=x_{40}=1$ ,  $y_{10}=y_{40}=1$ ,  $y_{20}=y_{30}=0$ , and  $\varphi_0$  is increased from 10 to 50, the bifurcation diagram of the  $\varphi_0$  is depicted in Fig.6(a). Besides, Fig.6(b) displays the corresponding Lyapunov exponent spectra. Fig.6 directly illustrates three important results: (i) the proposed MCNN generates a coexisting phenomenon of periodic behavior, quasiperiodic behavior, chaotic behavior, and hyperchaotic behavior under different initial states; (ii) the MCNN generates coexisting infinite chaotic attractors with different shapes and positions with the increase of  $\varphi_0$ ; (iii) each chaotic attractor

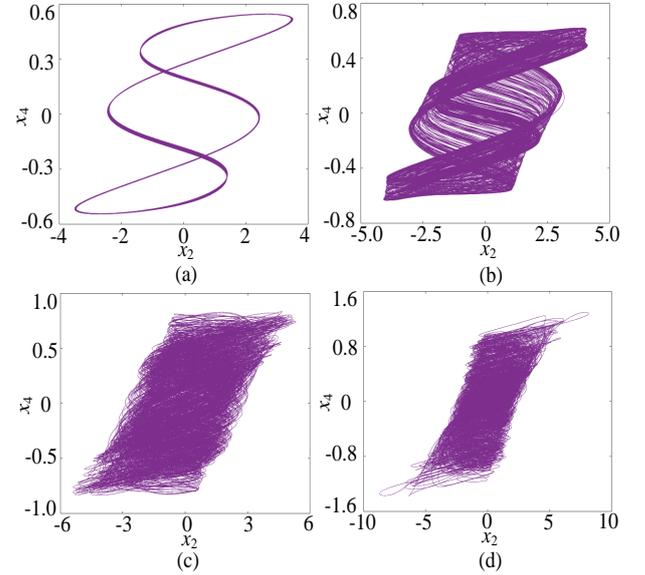


Fig. 5: Dynamical behaviors of the MCNN for different values of  $\rho$ . (a) Periodic attractor with  $\rho=0.17$ . (b) Quasiperiodic attractor with  $\rho=0.3$ . (c) Chaotic attractor with  $\rho=0.8$ . (d) Hyperchaotic attractor with  $\rho=2.5$ .

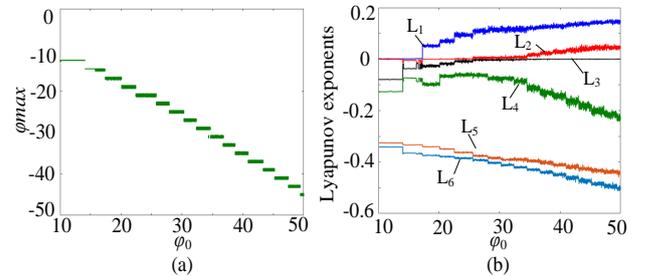


Fig. 6: The  $\varphi_0$ -dependent dynamics with the coupling strength  $\rho=0.17$  and initial states  $(1, 1, 1, 1, 1, 0, 0, 1, \varphi_0)$ . (a) Bifurcation diagram. (b) First six Lyapunov exponents.

has an independent initial state range  $\varphi_0 \in (k, k+2)$  where  $k$  is even number, which shows that the positions of chaotic attractors in the MCNN are controllable. Such complex dynamics means that the MCNN can not only generate coexisting behaviors with hyperchaos but also has initial tunable extreme multistability. Furthermore, when  $\rho=0.17$ , and  $x_{10}=x_{20}=x_{30}=x_{40}=y_{10}=y_{40}=1$ ,  $y_{20}=y_{30}=0$ , the phase portraits of the MCNN with different  $\varphi_0$  are plotted for further illustrating the initial-dependent coexisting dynamics as shown in Fig.7.

Furthermore, to reveal the dynamical effects of each initial state in the MCNN under the above condition, the results of the local attraction basin in the  $x_{10}$ - $\varphi_0$  plane are shown in Fig.8. As can be seen, the local attraction basin owns complicated manifold structures and basin boundaries, and the color-painted labeled by  $s_0$  to  $s_{10}$  indicate eleven attracting regions of dynamical behaviors. Among them,  $s_0$  region denotes unbounded behavior,  $s_1$  region represents periodic attractors,  $s_2$  region represents quasi-periodic attractors, and  $s_3$  to  $s_6$  regions express chaotic

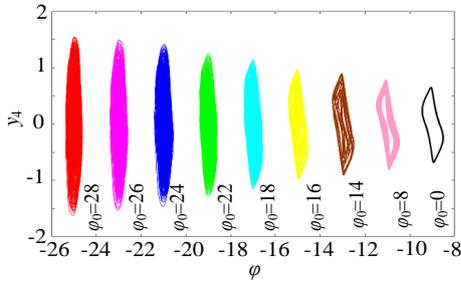


Fig. 7: Coexisting multiple attractors with different shapes and positions in the coupling neural network with  $\rho=0.17$  and different  $\varphi_0$ .

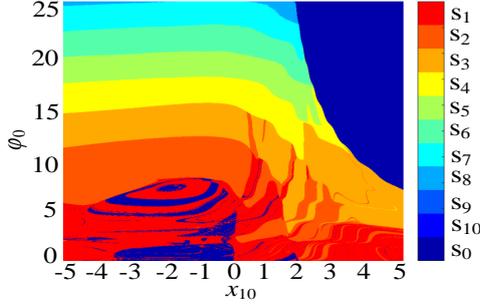


Fig. 8: For  $\rho=0.17$ , chaotic basin of attraction in the  $x_{10}$ - $\varphi_0$  plane.

attractors. Additionally, the regions labeled from  $s_7$  to  $s_{10}$  stand for hyperchaotic attractors. Consequently, the numerical results in Fig.8 show that the dynamical behaviors in the MCNN strongly rely on the initial state of the memristor.

### C. Initial-Boosted Coexisting Hyperchaotic Attractors

The initial boosting hyperchaotic phenomenon plays an important role in dynamical systems and has valuable applications [15]. But such a phenomenon has not been observed in neural networks. It is wonderful that the presented MCNN can generate initial boosting coexisting hyperchaos. For instance, we plot the bifurcation diagram of the  $\varphi_0$  under  $\rho=2.5$  and  $x_{10}=x_{20}=x_{30}=x_{40}=1$ ,  $y_{10}=y_{40}=1$ ,  $y_{20}=y_{30}=0$ , as shown in Fig.9(a). As can be seen, the MCNN displays a complicated initial boosting phenomenon. Also, the initially boosted dynamics is symmetric about the zero value of  $\varphi_0$ , which has never been reported in existing dynamical systems. Meanwhile, the corresponding constant Lyapunov exponents with two positive values in the whole range of the  $\varphi_0$  variation are given in Fig.9(b) besides two small periodic windows. Obviously, the MCNN has an infinite wide hyperchaotic range along  $\varphi_0$ -axis. That is to say, the MCNN enjoys complex dynamics of initial boosting coexisting hyperchaos, which means that it has excellent robustness. Additionally, to further inspect the initial boosted hyperchaotic dynamics, when keeping  $\rho=2.5$  and  $x_{20}=x_{30}=x_{40}=1$ ,  $y_{10}=y_{40}=1$ ,  $y_{20}=y_{30}=0$  unchanged, we draw the local attraction basin in the  $x_{10}$ - $\varphi_0$  plane, as shown in Fig.10. As can be seen, the local attraction basin has complex manifold structures and basin boundaries, and the specified initial value regions are composed of different colored zones marked by  $r_1$ - $r_8$ , among which the colored zones marked by  $r_1$ - $r_8$  correspond to the hyperchaotic attractors with different positions in Fig.11. Moreover, the greenyellow region  $r_0$  represents periodic attractor. Overall, these results manifest that the dynamical behaviors in the MCNN have strongly relied on the initial states of the memristor synapse. This is an important finding in the understanding of the brain neural systems.

Additionally, by calculating Lyapunov exponents, it will be shown in this section that the MCNN has complex hyperchaotic behavior for the parameter values and initial values of  $\rho=2.5$  and

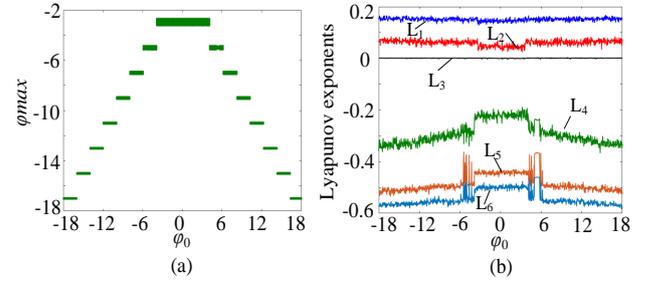


Fig. 9: The  $\varphi_0$ -dependent dynamics with the coupling strength  $\rho=2.5$  and initial states  $(1, 1, 1, 1, 0, 0, 1, \varphi_0)$ . (a) Bifurcation diagram. (b) First six Lyapunov exponents.

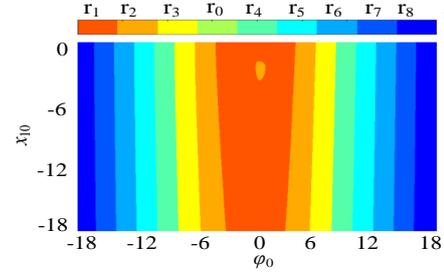


Fig. 10: For  $\rho=2.5$ , hyperchaotic basin of attraction in the  $x_{10}$ - $\varphi_0$  plane, and the colorbar shows the coexistence of 8 hyperchaotic attractors with different positions.

$(1, 1, 1, 1, 1, 0, 0, 1, 1)$ . The Lyapunov exponents for the MCNN are computed for 4195 iterations as follows:

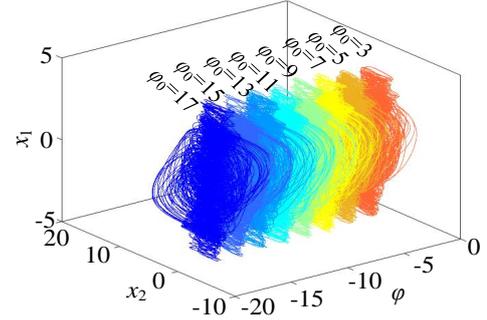


Fig. 11: Coexisting multiple hyperchaotic attractors with different positions in the MCNN with  $\rho=2.5$  and different  $\varphi_0$ .

$$\begin{aligned} LE_1 &= 0.1502, LE_2 = 0.0818, LE_3 = 0, \\ LE_4 &= -0.3142, LE_5 = -0.4967, LE_6 = -0.5561, \\ LE_7 &= -0.7443, LE_8 = -3.099, LE_9 = -42.27. \end{aligned} \quad (7)$$

The existence of two positive Lyapunov exponents in (7) makes it clear that the MCNN is hyperchaotic. Moreover, the Kaplan-Yorke dimension of the hyperchaotic neural network is calculated by the following formula:

$$D_{KY} = 3 + \frac{LE_1 + LE_2 + LE_3}{|LE_4|} = 3.7384. \quad (8)$$

Compared with the previous hyperchaotic neural network ( $D_{KY}=3.1403$ ) [5], the memristive coupled neural network has higher complexity since it has a larger value of  $D_{KY}$ .

## IV. APPLICATION IN BIOMEDICAL IMAGE ENCRYPTION

Thanks to many significant properties like inherent randomness, high sensitivity, and unpredictability, chaotic systems have been broadly employed in designing image cryptosystems [32]-[34]. Generally, the hyperchaotic systems have a large secret key space and good sensitivity, and its dynamics is more complex than that of the general chaotic system [35]. Furthermore, systems with initial-boosted coexisting behaviors have become

potential candidates for chaos applications compared to chaotic systems without coexisting attractors due to their high sensitivity. Interestingly, the coupled neural network would have a more attractive application prospect in image encryption schemes, as it has two sub-neural networks and more information. In other words, the coupled systems have a larger keyspace, so that the encryption schemes have higher security. Therefore, the proposed hyperchaotic MCNN can be used to design a more secure image encryption scheme.

### A. Design of Biomedical Image Encryption Scheme

The structure of the designed biomedical image encryption cryptosystem is given in Fig.12. As can be seen, the cryptosystem has three blocks: chaotic sequence generator, permutation module, and substitution module. Assuming that a gray-scale original image  $P(i)$  is used as the encryption object. Then, the process of encryption consists of three steps of operations.

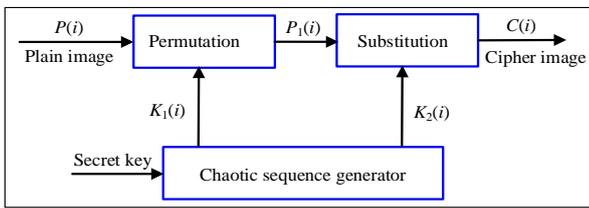


Fig. 12: Architecture of the MCNN-based biomedical image encryption scheme.

- 1) Chaotic sequence generator: Set system parameter  $\rho$  and initial states  $(x_{10}, x_{20}, x_{30}, x_{40}, y_{10}, y_{20}, y_{30}, y_{40}, \varphi_0)$ , discarded number  $N_0$ , and time step, then iterate the MCNN (5) with the fourth-order Runge-Kutta algorithm from initial states. The MCNN is pre-iterated  $N_0$  times to eliminate the adverse effects and to increase security. After the iteration of  $N_0$  times, the network is continuously iterated  $256 \times 256$  times. For each iteration, we can get nine values  $x_1(i), x_2(i), x_3(i), x_4(i), y_1(i), y_2(i), y_3(i), y_4(i), \varphi(i)$ . During iteration, the nine values are used to generate two different key values  $K_1(i)$  and  $K_2(i)$ , respectively. They are calculated by

$$K_1(i) = (x_{1i} + x_{2i} + x_{3i} + x_{4i} + \varphi_i)/5, \quad (9)$$

$$K_2(i) = \text{mod}(\text{floor}(((y_{1i} + y_{2i} + y_{3i} + y_{4i} + \varphi_i)/5) * 10^{15}), 256), \quad (10)$$

where the  $\text{floor}(x)$  denotes the elements of  $x$  to the nearest integers less than or equal to  $x$ . Then,  $K_1(i)$  is utilized for permutating the original image, and  $K_2(i)$  is used to substitute the pixel of the permuted image.

- 2) Permutation module: This module generates a permutation box. The chaotic key sequence  $K_1(i)$  is arranged in ascending order to obtain the index sequence index. According to the index sequence index, the plain image  $P(i)$  is globally scrambled to be a sequence  $P_1(i)$

$$P_1(i) = P(\text{index}(K_1(i))). \quad (11)$$

- 3) Substitution module: The introduction of non-linear operations in the pixel encryption process makes the plaintext and the ciphertext have a more complex non-linear relationship, which can enhance the security of the algorithm. So, the permutation image is encrypted as

$$C(i) = P_1(i) \oplus K_2(i), \quad (12)$$

where the symbol  $\oplus$  represents the exclusive XOR operation bit-by-bit. The MCNN is iterated until all the elements

are encrypted. Then every element in the encrypted set is converted into decimal numbers and we can obtain the cipher image.

### B. Experimental Results Analysis

To demonstrate the efficiency of the designed biomedical image encryption cryptosystem, we used a laptop with Intel Core™ i7 CPU 2.500 GHz and 6 GB RAM with preinstalled MATLAB R2017a. And some classic metrics like keyspace, histogram, correlation coefficient, information entropy, key sensitivity, differential attack, noise attack and chosen plain-text attack were measured [34]. In whole experiments, four medical images Chest, Angiography, Brain, and Lung each of size  $256 \times 256$  are employed as the test images, as shown in Fig.13( $a_1$ - $a_4$ ). Setting the secret key  $(\rho, x_{10}, x_{20}, x_{30}, x_{40}, y_{10}, y_{20}, y_{30}, y_{40}, \varphi_0) = (2.5, 1, 1, 1, 1, 0, 0, 1, 2)$ , two pseudorandom sequences generated by (9) and (10) are used for medical image encryption. In this process, to avoid the transient effect, the pre-iterate number  $N_0$  of the chaotic system is set as 500, and the time step is chosen as 0.001.

(1) Keyspace analysis: A good image encryption algorithm should possess a larger keyspace to resist the exhaustive attack in an effective manner. The presented encryption scheme adopts one parameter  $\rho$  and nine initial values  $x_{10}, x_{20}, x_{30}, x_{40}, y_{10}, y_{20}, y_{30}, y_{40}, \varphi_0$  as its key, which can ensure that unauthorized decryption becomes difficult. In our experiments, all bites adopt double-precision data, so the keyspace of the encryption scheme is  $(10^{16})^{10} = 10^{160} \approx 2^{480}$ . It is obvious that the encryption scheme has more than  $2^{100}$  keyspace and can resist all types of violent attacks. The keyspace is much larger than the latest similar encryption schemes, such as [19], [24], [32], [33]. From this, we can conclude that the new biomedical image encryption scheme has a great keyspace.

(2) Histogram analysis: As we all know, the intensity distribution of gray values in images can be described by a histogram. The histogram is a fundamental tool to reflect the distribution of the pixel intensity values in the images. Generally, an excellent image encryption system should make the histograms of the encrypted images as uniform as possible. Four original medical images, encrypted images, and their corresponding histograms are shown in Fig.13. From Fig.13( $c_1$ )-( $c_4$ ), it can be seen that all of the encrypted images look messy and completely lose the original image information. And from Fig.13( $d_1$ )-( $d_4$ ) and Fig.13( $b_1$ )-( $b_4$ ), the histograms of the cipher images are very uniform and are significantly different from those of the original images, which means that the designed biomedical image encryption scheme has strong ability to resist statistical attack.

(3) Correlation analysis: The correlation coefficients can measure the robustness of the image and reflect the degree of correlation between the gray values of adjacent pixels in the images. Usually, for regular images, the adjacent pixels have a strong correlation near to 1 in every direction. But for cipher images, the correlation coefficients should be close to 0. The correlation of each pair of pixels can be computed by[36]

$$\rho_{xy} = \frac{\sum_{i=1}^N (x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^N (x_i - E(x))^2} \sqrt{\sum_{i=1}^N (y_i - E(y))^2}}, \quad (13)$$

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. To evaluate the correlation coefficients, we randomly selected 10000 pairs of adjacent pixels in every direction. Then, the correlation coefficients of adjacent pixels of images Chest, Angiography, Brain, and Lung in three

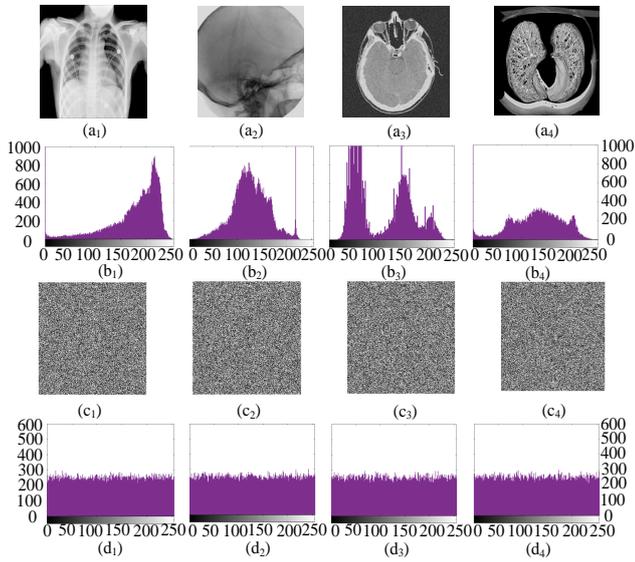


Fig. 13: Simulation results of the proposed encryption scheme: (a<sub>1</sub>-a<sub>4</sub>) Original image; (b<sub>1</sub>-b<sub>4</sub>) Histogram of the original image; (c<sub>1</sub>-c<sub>4</sub>) Cipher image; (d<sub>1</sub>-d<sub>4</sub>) Histogram of the cipher image.

TABLE II: CORRELATION COEFFICIENTS AND INFORMATION ENTROPY OF THE ORIGINAL IMAGES AND THEIR CIPHER IMAGES

Medical Images	Type	Horizontal	Vertical	Diagonal	Entropy
Chest	Original	0.993602	0.992463	0.987863	6.5336
	Encrypted	-0.001745	-0.000839	0.013351	7.9981
Angiography	Original	0.990111	0.993122	0.980891	6.0647
	Encrypted	0.001070	-0.004135	0.004224	7.9979
Brain	Original	0.935238	0.925998	0.908461	6.7450
	Encrypted	-0.012230	-0.007964	0.003396	7.9979
Lung	Original	0.934076	0.922685	0.897652	5.6348
	Encrypted	-0.009910	-0.000055	0.008239	7.9980

directions were calculated. Both the correlation coefficients of the original images and cipher images are listed in Table II. As shown in Table II, we can clearly see that the correlation coefficients of the adjacent pixels in the original images is close to 1, and the correlation coefficients of the adjacent pixels in the encrypted images is close to 0, which further proves that the image encryption scheme can completely break the correlation of the adjacent pixels in the images and thus effectively resist attacks. It is evident that the proposed biomedical image encryption scheme can efficiently reduce the correlation between adjacent pixels of the encrypted images.

(4) Entropy analysis: Information entropy reflects the statistical characteristics of images. The larger the information entropy value is, the higher the randomness of image information. A good image encryption scheme should make the information entropy value of the encrypted images close to 8 as far as possible to achieve the purpose of resistance to statistical attack. The information entropy can be defined as [36]

$$H(P) = \sum_{i=0}^{2^N-1} P(x_i) \log_2 \frac{1}{P(x_i)}, \quad (14)$$

where  $N$  represents the bit depth of the image  $P$  and  $P(x_i)$  represents the probability of the presence of a pixel  $x_i$ . For grayscale images,  $x_i \in [0, 255]$ ,  $N=8$ ,  $P(x_i) \in [0, 1]$ , and  $\sum(P(x_i))=1$ . The theoretical maximum information entropy is 8. The closer the information entropy is to 8, the more random the grayscale distribution of image pixels. For instance, we assume that there are only five types of pixels in a gray image, namely  $x_1-x_5$ . Their probability values are 0.2, 0.4, 0.05, 0.25 and 0.1, respectively. The information entropy of the image can be calculated by (14), namely  $H=2.0414$ . It means that the pixel distribution in this image is not uniform, that is to say, it has poor randomness property. We calculate the information entropy of the four original medical images and their corresponding encrypted

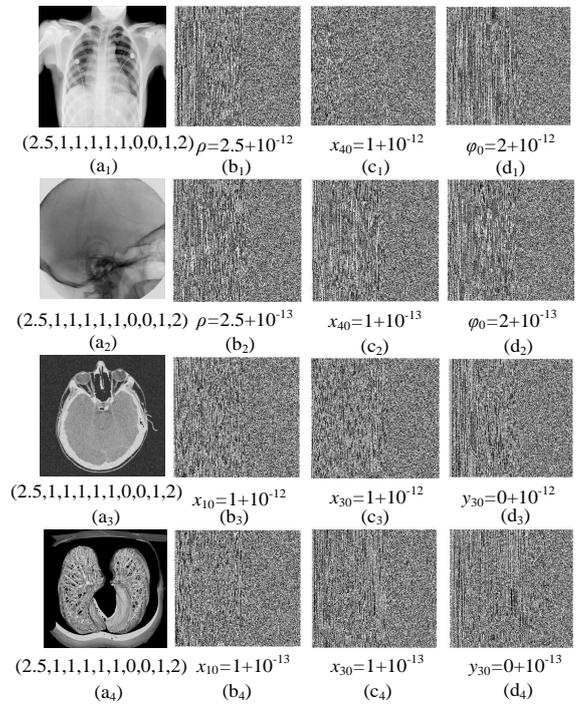


Fig. 14: Image decryption process with the secret key ( $\rho$ ,  $x_{10}$ ,  $x_{20}$ ,  $x_{30}$ ,  $x_{40}$ ,  $y_{10}$ ,  $y_{20}$ ,  $y_{30}$ ,  $y_{40}$ ,  $\varphi_0$ ). (a<sub>1</sub>)-(a<sub>4</sub>) Accurate decrypted image with the secret keys (2.5, 1, 1, 1, 1, 1, 0, 0, 1, 2); (b<sub>1</sub>)-(b<sub>4</sub>) Inaccurate decrypted image with the secret keys  $\rho=2.5+10^{-12}/10^{-13}$  and  $x_{10}=1+10^{-12}/10^{-13}$ ; (c<sub>1</sub>)-(c<sub>4</sub>) Inaccurate decrypted image with the secret keys  $x_{40}=1+10^{-12}/10^{-13}$  and  $x_{30}=1+10^{-12}/10^{-13}$ ; (d<sub>1</sub>)-(d<sub>4</sub>) Inaccurate decrypted image with the secret keys  $\varphi_0=2+10^{-12}/10^{-13}$  and  $y_{30}=1+10^{-12}/10^{-13}$ .

images. The calculation results are shown in Table IV. We can see that there is a large improvement in information entropy after the original image is encrypted. Furthermore, the results show that the information entropy of the image encrypted by this algorithm is closer to 8.

(5) Sensitivity analysis: The key sensitivity is an important index in the security of encryption algorithms. A good encryption scheme should be sensitive to the key. In our encryption algorithm, the system parameter  $\rho$  and initial values ( $x_{10}$ ,  $x_{20}$ ,  $x_{30}$ ,  $x_{40}$ ,  $y_{10}$ ,  $y_{20}$ ,  $y_{30}$ ,  $y_{40}$ ,  $\varphi_0$ ) are all used as secret keys. Fig.14(a<sub>1</sub>)-(a<sub>4</sub>) gives the accurate decrypted image. And Fig.14(b<sub>1</sub>)-(d<sub>4</sub>) illustrate the inaccurate decrypted images with a tiny change of the secret keys. As can be seen, even the secret key is changed very little ( $10^{-12}$ ), the decrypted images are completely different from the original images. Therefore, the key sensitivity test shows that the proposed biomedical image encryption scheme has perfect sensitivity to the key.

(6) Differential attack analysis: NPCR (number of pixel change rates) and UACI (unified average change intensity) can be used to represent the effect of a single-pixel change of the plain image on the cipher image.  $C_1$  and  $C_2$  denote two cipher images with both sizes equal to  $M \times N$ , whose corresponding plain images only have a single-pixel difference. The gray values of the pixels in position  $(i, j)$  of  $C_1$  and  $C_2$  are expressed by  $C_1(i, j)$  and  $C_2(i, j)$ , respectively. NPCR and UACI can be written by

$$NPCR(C_1, C_2) = \sum_{i=1}^M \sum_{j=1}^N \frac{D(i, j)}{M \cdot N} \times 100\%, \quad (15)$$

$$D(i, j) = \begin{cases} 0, & \text{if } C_1(i, j) = C_2(i, j) \\ 1, & \text{if } C_1(i, j) \neq C_2(i, j) \end{cases}, \quad (16)$$

$$UACI(C_1, C_2) = \frac{1}{M \cdot N} \sum_{i=1}^M \sum_{j=1}^N \frac{|C_1(i, j) - C_2(i, j)|}{255} \times 100\%. \quad (17)$$

According to references [24], the expected NPCR and UACI values of a 256 gray-scale image are 99.6094% and 33.4635%, respectively. Table III gives the NPCR and UACI values of the encrypted images for different plain medical images using the proposed encryption algorithms evaluated by the average value of 150 times running. In Table III, the presented encryption algorithm has NPCR and UACI values very close to the expected values. Therefore, it is very sensitive to small changes in the plain images. That is to say, it has a strong ability to oppose differential attacks.

TABLE III: OUTCOMES OF NPCR AND UACI TEST FOR THE EXPERIMENTED DATASET

Medical Image	NPCR(%)	UACI(%)
Chest	99.6104	33.4662
Angiography	99.6116	33.4675
Brain	99.6095	33.4682
Lung	99.6091	33.4668

(7) Data loss and noise attacks: An ideal encryption algorithm can effectively resist external attacks. The data loss attack and the noise attack are usually used to evaluate the robustness of an image encryption algorithm. In the process of image transmission, the images are easy to suffer from noise and partial data loss. An ideal image encryption algorithm should be robust to noise and partial data loss.

To test the algorithm's ability to resist data loss, we cut off some parts of the cipher image and then decrypt it. Fig.15(a<sub>1</sub>-a<sub>3</sub>) and (b<sub>1</sub>-b<sub>3</sub>) provide results of data loss attacks for the different lost areas, where the plain image is recovered successfully via the decryption process. Salt and pepper noise may arise in images when image signals are suddenly and strongly interfered within the transmission process. To test the algorithm's ability to resist salt noise attacks, we added salt and pepper noise to the encrypted image with different proportions. The outcomes of the noise attacks are shown in Fig.15(c<sub>1</sub>-c<sub>3</sub>) and (d<sub>1</sub>-d<sub>3</sub>). As can be seen, some pixel values in decrypted images are changed, but the approximate information of the plain image could still be displayed. This means that the encrypted image still has a good decryption effect after being attacked by salt and pepper noise. Consequently, the experimental results in Fig.15 show that the proposed encryption algorithm can effectively resist the noise and data loss attack and has very good security.

(8) Chosen plain-text attack: It is well known that a good encryption scheme needs to have good performance as opposed to chosen plain-text attack. Some attackers may choose plain images which are all-black or all-white to decipher the encryption scheme. However, in our encryption scheme, in addition to the fact that the position of image pixels can be changed by the permutation process, the size of pixel values can also be changed by the substitution process, thus this encryption method can ensure high security whatever original image is. Fig.16 gives the all-black and all-white plain image, their encrypted images and the histograms of the encrypted images. All of the tested images are 256×256. Fig.16 illustrates that the distributions of the histograms of the encrypted images of all-black and all-white images are both uniform. Thus the decipherer cannot obtain any useful information from the encrypted images and the encryption system cannot be broken. Therefore, it confirms that our image encryption algorithm can resist the chosen plain-text attacks.

Here we compare the results of the presented cryptosystem with those of the previous similar works, as shown in Table IV. Obviously, compared with the recent results of [19], [24], [32], [33], the chaotic system used in the designed encryption scheme has higher dimensions and more complex chaotic dynamics. Therefore, the proposed medical image encryption scheme has a larger keyspace, higher information entropy and more sensitive secret key, which enjoys higher security. It is noted

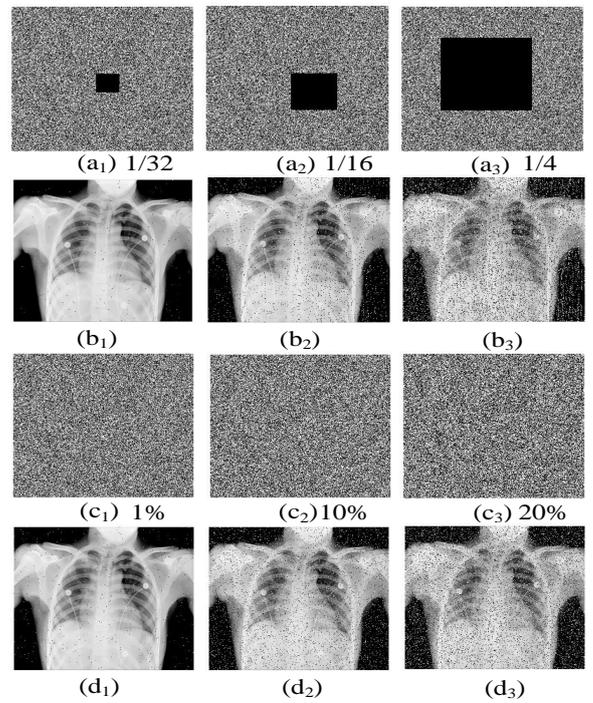


Fig. 15: The robustness of the proposed algorithm to partial data loss and noise attacks. (a<sub>1</sub>-a<sub>3</sub>) The encrypted image with 1/32, 1/16, and 1/4 loss, respectively. (b<sub>1</sub>-b<sub>3</sub>) Corresponding decryption images. (c<sub>1</sub>-c<sub>3</sub>) The encrypted image with 1%, 10%, and 20% salt and pepper noise, respectively. (d<sub>1</sub>-d<sub>3</sub>) Corresponding decryption images.

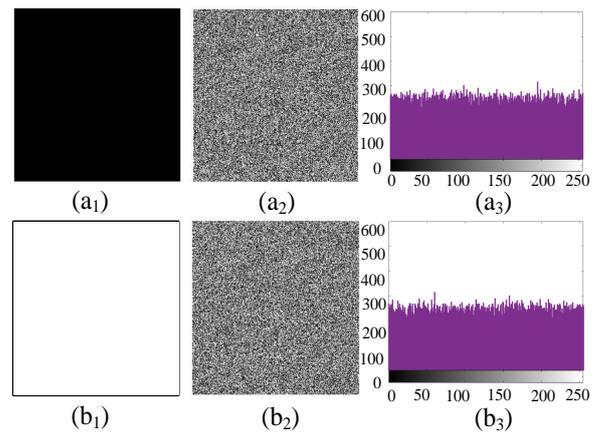


Fig. 16: The experimental results of chosen plaintext attack. (a<sub>1</sub>),(a<sub>2</sub>) and (a<sub>3</sub>) Black image, its encrypted image and corresponding histogram, respectively. (b<sub>1</sub>), (b<sub>2</sub>) and (b<sub>3</sub>) White image, its encrypted image and corresponding histogram, respectively.

that compared with [24], the proposed encryption scheme has a lower information entropy. Nevertheless, the difference between them is so small that it doesn't affect its safety. Furthermore, the designed medical image encryption scheme not only has very low correlation coefficients in every direction but also demonstrates its experimental results on the hardware platform. Consequently, these results suggest that the biomedical image encryption scheme based on the coupled HNN can more effectively resist the entropy attack and statistical attacks, and can be applied to protect image data in practical information communication.

## V. VALIDATION BY HARDWARE EXPERIMENTS

Due to the properties of ultra-low power, programmable reusability, and strong controllability, the field-programmable gate array (FPGA) is broadly applied in industrial electronics. Particularly, FPGA-based chaotic systems have been widely investigated in recent years [36], [37]. However, image cryptosystems based

TABLE IV: PERFORMANCE COMPARISON OF VARIOUS ENCRYPTION SCHEMES

Refs	Image type	System type	System Dimension	Information Entropy	Key sensitivity	Original image: Horizontal, Vertical, Diagonal	Cipher image: Vertical, Horizontal, Diagonal	Hardware demonstration
2019 [32]	Normal image Lena(256×256)	Multi-scroll chaotic system	3	7.9898	–	0.9233, 0.9672, 0.8949	-0.0062, 0.0061, -0.0277	No
2020 [33]	Normal image Lena(256×256)	Multi-wing chaotic system	3	7.9976	$10^{-9}$	0.972807, 0.939337, 0.921438	0.000827, 0.005238, -0.000455	Yes
2020 [19]	Normal image Lena(256×256)	Initial boosted chaotic HNN	4	7.9977	$10^{-8}$	0.97492, 0.98629, 0.96268	0.0004, 0.0007, 0.0012	No
2021 [24]	Medical image Chest(256×256)	Chaotic HNN	3	7.9992	$10^{-9}$	0.94505, 0.96653, 0.91917	0.0026, 0.0026, 0.07992	No
This work	Medical image Chest(256×256)	Initial-boosted hyperchaotic HNN	9	7.9981	$10^{-12}$	0.993602, 0.992463, 0.987863	-0.001745, -0.000839, 0.013351	Yes

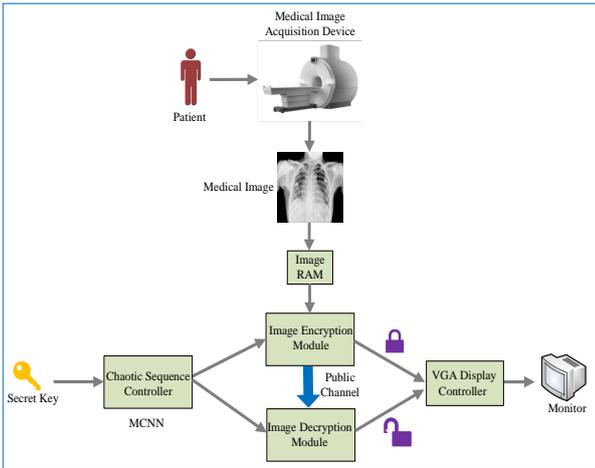


Fig. 17: Block diagram of the FPGA-based biomedical image cryptosystem

on chaotic neural networks are seldom implemented by FPGA hardware [38]. Thus we develop an FPGA-based hardware test platform to implement the proposed MCNN and the designed biomedical image encryption scheme. The hardware devices contain one Xilinx Virtex-6 FPGA development board and one monitor.

#### A. Design of The FPGA-Based Biomedical Image Cryptosystem

In this subsection, we design and implement an biomedical image cryptosystem on the FPGA platform. The hardware structure of the cryptosystem mainly includes five parts: image RAM (random access memory), chaotic sequence controller, image encryption module, image decryption module, and VGA display controller. As shown in Fig.17, the image RAM is used to store and output the original medical image from medical image acquisition devices. And the chaotic sequence controller completes the production and caching of chaotic sequences generated by the MCNN. In the process of medical image encryption, the original medical image and chaotic sequences are sent to the image encryption module synchronously. Then the original medical image is encrypted in the image encryption module. After that, the encrypted image is sent to the VGA display controller and finally is displayed on the monitor. In the process of image decryption, the encrypted medical image and chaotic sequences are sent to the image decryption module synchronously. Afterward, the encrypted medical image is decrypted in the image decryption module, and the decrypted image is displayed on the monitor by the VGA display controller.

#### B. FPGA-Based Implementation Results

The hardware structure of the biomedical image cryptosystem in Fig.17 is realized via employing a Xilinx Virtex-6 FPGA development board with a 32-bit IEEE 754-1985 floating-point standard. The functions of the five parts are implemented by Verilog HDL programming, where the generation process of the chaotic sequences can refer to our previous work in [33]. Various attractors realized by FPGA-based memristive coupled neural network (5) are shown in Fig.18. In the experiment, medical images are stored in the RAM of the ZYNQ-XC7Z020 chip. The experimental results are shown in Fig.19, where The hyperchaotic sequences generated from the hyperchaotic attractors is given in Fig.19(a), the original image and the encrypted image are shown in Fig.19(b) with the secret key  $(\rho, x_{10}, x_{20}, x_{30}, x_{40}, y_{10}, y_{20}, y_{30}, y_{40}, \varphi_0)=(2.5, 1, 1, 1, 1, 1, 0, 0, 1, 2)$ . Fig.19(c) gives the encrypted image and correct decrypted image with the correct secret key. And the encrypted image and the incorrect decrypted image are shown in Fig.19(d) under incorrect secret key  $(2.5, 1, 1, 1, 1+10^{-12}, 1, 0, 0, 1, 2)$ . Obviously, the FPGA-based experimentation results agree with the MATLAB-based simulation results. Table V gives the performance metrics of the designed hardware cryptosystem. Moreover, the times for image encryption and image decryption on the FPGA platform are 0.241543s and 0.228897s, respectively. These times are largely lower than the corresponding time 0.752145s and 0.682635s in MATLAB numerical simulations. That is to say, the biomedical image cryptosystem implemented by the FPGA can greatly improve the speed of data processing and the time of algorithm operation. Obviously, these experimental results verify the feasibility and reliability of the presented MCNN-based biomedical image encryption scheme.

## VI. CONCLUSION

In this article, based on two sub-neural networks and one multistable memristor synapse, a memristive coupled neural network (MCNN) model is proposed. Dynamical analysis shows that the MCNN exhibits complex brain-like chaotic dynamics including chaos and hyperchaos. Particularly, it is capable of generating brain-like initial-boosted hyperchaos under different initial states. Meanwhile, we design a MCNN-based biomedical image encryption scheme. Experimental results demonstrate that the designed biomedical image cryptosystem enjoys some advantages in terms of secret keyspace, information entropy, key sensitivity and robustness. Finally, we designed and implemented the MCNN and corresponding biomedical image cryptosystem on the FPGA platform. And hardware experimentation results have been given to verify the effectiveness of the theoretical analyses and numerical simulations. Nowadays, with the rapid development of brain science, the study of brain-like dynamics

TABLE V: PERFORMANCE METRICS OF HARDWARE CRYPTOSYSTEM

Metrics	Area/bit	Resource utilization	RAM/byte	Cycles/byte	Energy/bit	Power/mW	Throughput/Mbps
FPGA	LUTs: 3587 Regs: 2560	ALMs: 26% Regs: 15%	LUTRAM: 1425 BRAM: 96	1.15	52.89	21.65	527.24

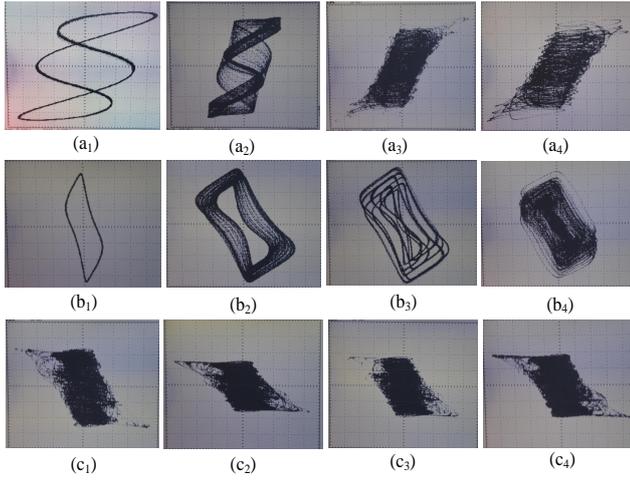


Fig. 18: Various attractors of the MCNN (5) from the FPGA implementation. (a<sub>1</sub>-a<sub>4</sub>) FPGA results of Fig.5. (b<sub>1</sub>-b<sub>4</sub>) FPGA results of Fig.7. (c<sub>1</sub>-c<sub>4</sub>) FPGA results of Fig.11.

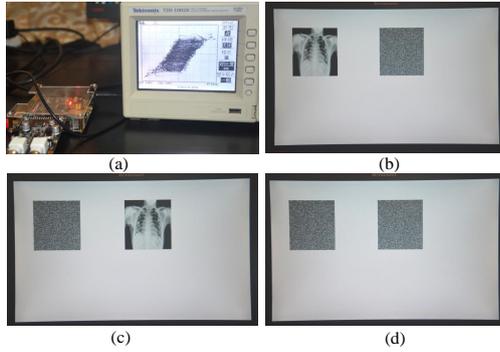


Fig. 19: FPGA-based measured results. (a) Hyperchaotic attractor. (b) Original and encrypted medical image. (c) Encrypted and correctly decrypted medical image. (d) Encrypted and incorrectly decrypted medical image.

has become an urgent requirement to deeply understand brain function and nerve disease. Consequently, modeling, analysis, simulation, implementation and application of the brain nervous system as attempted in this paper will be helpful in the exploitation of neuromorphic systems and the clinical diagnosis of neurogenic diseases.

Future research will focus on studying the brain-like dynamics of large-scale neural networks closer to the real brain nervous systems. Future applications will use this memristive coupled neural network to build an artificial intelligence system with brain functions.

## REFERENCES

- [1] J. J. Hopfield, "Neural network and physical system with emergent collective computational abilities," *Proc. Nat. Acad. Sc.*, vol. 79, pp. 2554–2558, 1982.
- [2] S. J. Schiff, K. Jerger, D. H. Duong, et al, "Controlling chaos in the brain," *Nature.*, vol. 370, no. 6491, pp. 615–620, 1994.
- [3] 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.
- [4] B. Hu, Z. H. Guan, N. Xiong, et al, "Intelligent impulsive synchronization of nonlinear interconnected neural networks for image protection," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3775–3787, 2018.
- [5] H. Lin, C. Wang, Y. Tan, "Hidden extreme multistability with hyperchaos and transient chaos in a Hopfield neural network affected by electromagnetic radiation," *Nonlinear Dyn.*, vol. 99, no. 3, pp. 2369–2386, 2020.
- [6] Q. Lai, P. D. K. Kuate, F. Liu, et al, "An extremely simple chaotic system with infinitely many coexisting attractors," *IEEE Trans. Cir. Sys.-II: Brief Papers.*, vol. 67, no. 6, pp. 1129–1133, 2019.
- [7] K. Tian, C. Grebogi, H. P. Ren, "Chaos generation with impulse control: application to non-chaotic systems and circuit design," *IEEE Trans. Circuits Syst. I-Regul. Pap.*, vol. 68, no. 7, pp. 3012–3022, 2021.
- [8] P. K. Reardon, J. Seidlitz, S. Vandekar, et al, "Normative brain size variation and brain shape diversity in humans," *Science.*, vol. 360, no. 6394, pp. 1222–1227, 2018.
- [9] Z. T. Njitacke, J. Kengne, H. B. Fotsin, "A plethora of behaviors in a memristor based Hopfield neural networks (HNNs)," *International Journal of Dynamics and Control.*, vol. 7, no. 01, pp. 36–52, 2019.
- [10] B. Bao, H. Qian, Q. Xu, et al, "Coexisting behaviors of asymmetric attractors in hyperbolic-type memristor based Hopfield neural network," *Front. Comput. Neurosci.*, vol. 11, Art. no. 18, 2017.
- [11] C. Chen, J. Chen, H. Bao, et al, "Coexisting multi-stable patterns in memristor synapse-coupled Hopfield neural network with two neurons," *Nonlinear Dyn.*, vol. 95, no. 4, pp. 3385–3399, 2019.
- [12] H. Lin, C. Wang, Q. Hong, et al, "A multi-stable memristor and its application in a neural network," *IEEE Trans. Cir. Sys.-II: Brief Papers.*, vol. 67, no. 12, pp. 3472–3476, 2020.
- [13] C. Li, X. Wang, G. Chen, "Diagnosing multistability by offset boosting," *Nonlinear Dyn.*, vol. 90, no. 2, pp. 1335–1341, 2020.
- [14] 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.*, doi.10.1109/TIE.2021.3099231, 2021.
- [15] F. Yuan, Y. Deng, Y. Li, et al, "The amplitude, frequency and parameter space boosting in a memristor–meminductor-based circuit," *Nonlinear Dyn.*, vol. 96, no. 1, pp.389–405, 2019.
- [16] H. Bao, Z. Hua, N. Wang, et al, "Initials-boosted coexisting chaos in a 2-D sine map and its hardware implementation," *IEEE Trans. Ind. Informat.*, vol. 17, no. 2, pp. 1132–1140, 2020.
- [17] H. Li, Z. Hua, H. Bao, et al, "Two-dimensional memristive hyperchaotic maps and application in secure communication," *IEEE Trans. Ind. Electron.*, vol. 68, no. 10, pp. 9931–9940, 2020.
- [18] H. Bao, W. Liu, J. Ma, et al, "Memristor initial-offset boosting in memristive HR neuron model with hidden firing patterns," *Int. J. Bifurcation Chaos.*, vol. 30, no. 10, Art. no. 2030029, 2020.
- [19] 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, no. 4, pp. 2821–2841, 2020.
- [20] H. Lin, C. Wang, Q. Deng, et al, "Review on chaotic dynamics of memristive neuron and neural network," *Nonlinear Dyn.*, vol. 106, no. 1, pp. 959–973, 2021.
- [21] F. Yu, Z. Zhang, H. Shen, et al, "Design and FPGA implementation of a pseudo-random number generator based on a Hopfield neural network under electromagnetic radiation," *Front. Physics.*, vol. 9, Art. no. 302, 2021.
- [22] M. Kobayashi, "Two-level complex-valued Hopfield neural networks," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 32, no. 5, pp. 2274–2278, 2020.
- [23] A. S. Panayides, A. Amini, N. D. Filipovic, et al, "AI in medical imaging informatics: current challenges and future directions," *IEEE J. Biomed. Health Inform.*, vol. 24, no. 7, pp. 1837–1857, 2020.
- [24] Z. T. Njitacke, S. D. Isaac, T. Nestor, et al, "Window of multistability and its control in a simple 3D Hopfield neural network: application to biomedical image encryption," *Neural Comput Appl.*, vol. 33, no. 12, pp. 6733–6752, 2021.
- [25] 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.
- [26] L. Chua, "Everything you wish to know about memristors but are afraid to ask," *Radioengineering.*, vol. 24, no. 2, pp. 319–368, 2015.
- [27] S. Rosemann, C. M. Thiel, "Audio-visual speech processing in age-related hearing loss: Stronger integration and increased frontal lobe recruitment," *Neuroimage.*, vol. 175, pp. 425–437, 2018.
- [28] Z. I. Mannan, S. P. Adhikari, C. Yang, et al, "Memristive imitation of synaptic transmission and plasticity," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 11, pp. 3458–3470, 2019.
- [29] S. Gong, Z. Guo, S. Wen, et al, "Finite-time and fixed-time synchronization of coupled memristive neural networks with time delay," *IEEE T Cybernetics.*, vol. 51, no. 06, pp. 2944–2955, 2021.
- [30] S. Wang, Z. Guo, S. Wen, et al, "Global synchronization of coupled delayed memristive reaction-diffusion neural networks," *Neural Networks.*, vol. 123, pp. 362–371, 2020.
- [31] C. Zhou, C. Wang, Y. Sun, et al, "Weighted sum synchronization of memristive coupled neural networks," *Neurocomputing.*, vol. 403, pp. 211–223, 2020.
- [32] N. Wang, C. Li, H. Bao, et al, "Generating multi-scroll chua's attractors via simplified piecewise-linear Chua's diode," *IEEE Trans. Circuits Syst. I-Regul. Pap.*, vol. 66, no. 12, pp. 4767–4779, 2019.
- [33] H. Lin, C. Wang, F. Yu, et al, "An extremely simple multi-wing chaotic system dynamics analysis, encryption application and hardware implementation," *IEEE Trans. Ind. Electron.*, vol. 68, no. 12, pp. 12708–12719, 2021.

- [34] A. Sambas, S. Vaidyanathan, E. Tlelo-Cuautle, et al, "A 3-D multi-stable system with a peanut-shaped equilibrium curve: Circuit design, FPGA realization, and an application to image encryption," *IEEE Access.*, vol. 8, pp. 137116-137132, 2020.
- [35] S. Vaidyanathan, A. Sambas, B. Abd-El-Atty, et al, "A 5-D multi-stable hyperchaotic two-disk dynamo system with no equilibrium point: Circuit design, FPGA realization and applications to TRNGs and image encryption," *IEEE Access.*, vol. 9, pp. 81352-81369, 2021.
- [36] A. Sambas, S. Vaidyanathan, E. Tlelo-Cuautle, et al, "A novel chaotic system with two circles of equilibrium points: multistability, electronic circuit and FPGA realization," *Electronics.*, vol. 8, no. 11, Art. no. 1211, 2019.
- [37] A. Sambas, S. Vaidyanathan, T. Bonny, et al, "Mathematical model and FPGA realization of a multi-stable chaotic dynamical system with a closed butterfly-like curve of equilibrium points," *Applied Sciences.*, vol. 11, no. 2, Art. no. 788, 2021.
- [38] J. Perez-Padron, C. Posadas-Castillo, J. Paz-Perez, et al, "FPGA realization and Lyapunov-Krasovskii analysis for a master-slave synchronization scheme involving chaotic systems and time-delay neural networks," *Math Probl Eng.*, vol. 2021, Art. no. 2604874, 2021.



**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. He has published over

330 papers and contributed 10 chapters in edited books. He has also published four text and research books: *Continuous-Time Active Filter Design* (CRC Press, USA, 1999), *Design of High Frequency Integrated Analogue Filters* (IEE Press, UK, 2002), *Wireless Communication Circuits and Systems* (IET Press, 2004), and *Test and Diagnosis of Analogue, Mixed-signal and RF Integrated Circuits - the Systems on Chip Approach* (IET Press, 2008). 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.



**Hairong Lin** received M.S. and Ph.D. degree in information and communication engineering and computer science and technology from Hunan University, China, in 2015 and 2021, respectively. He is currently a post-doctoral research fellow at the College of Computer Science and Electronic Engineering, Hunan University, Changsha, China. His main research interest includes neural system modeling, Chaotic dynamical analysis, nonlinear circuit and neuromorphic engineering. He has published some papers in related international journals, such as the *IEEE Transactions on Industrial Information*,

the *IEEE Transactions on Industrial Electronics*, the *IEEE Transactions on Circuits and Systems I-Regular Papers*, the *IEEE Transactions on Circuits and Systems II-Express Briefs*, the *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *Nonlinear Dynamics*, etc.



**Chunhua Wang** received the M.S. degree from Zhengzhou University, Zhengzhou, China, in 1994, and the Ph.D. degree from Beijing University of Technology, Beijing, China, in 2003. He is currently the Professor of College of Information Science and Engineering, Hunan University, Changsha, China. He is the Doctor tutor, director of advanced communication technology key laboratory of hunan universities, the member of academic committee of hunan university, the director of chaos and nonlinear circuit professional committee of circuit and system branch of China electronic society.

Now, his research interests include memristor circuit, complex networks, chaotic circuit, chaos secure communication, current-mode circuit and neural networks based on memristor. He has presided over 8 national and provincial projects, and published more than 120 papers, among which more than 100 were retrieved by SCI.



**Li Cui** received the bachelor degree in Information Engineering from Wuhan University of Technology in Wuhan, China in 2003 and Master degree in Control theory and control engineering in Hunan University of science and technology in Xiangtan, China in 2010. He is currently a lecturer with the school of information and electrical engineering of Hunan University of science and technology. His research interests include nonlinear systems and circuits, Manipulator control, complex networks and their applications.



**Cong Xu** received the Bachelor's degree in communications engineering from Hunan City University, Yiyang, China. She is currently pursuing the Ph. D degree in College of Computer Science and Electronic Engineering, Hunan University, China. Her research interests include memristor neural network and its applications.



**Fei Yu** 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.