Hyperchaotic memristive ring neural network and application in medical image encryption

Hairong Lin · Chunhua Wang · Li Cui · Yichuang Sun · Xin Zhang · Wei Yao

Abstract Neural networks are favored by academia and industry because of their diversity of dynamics. However, it is difficult for ring neural networks to generate complex dynamical behaviors due to their special structure. In this paper, we present a memristive ring neural network (MRNN) with four neurons and one non-ideal flux-controlled memristor. The memristor is used to describe the effect of external electromagnetic radiation on neurons. The chaotic dynamics of the M-RNN is investigated in detail by employing phase portraits, bifurcation diagrams, Lyapunov exponents and attraction basins. Research results show that the MRN-N not only can generate abundant chaotic and hyperchaotic attractors but also exhibits complex multistability dynamics. Meanwhile, an analog MRNN circuit is experimentally implemented to verify the numerical simulation results. Moreover, a medical image encryption scheme is constructed based on the MRNN from a perspective of practical engineering application. Performance evaluations demonstrate that the proposed medical image cryptosystem has several advantages in terms of keyspace, information entropy, and key sensitivity, compared with cryptosystems based on other chaotic systems. Finally, hardware experiment using the field-programmable gate array (FPGA) is carried out to verify the designed cryptosystem.

H. Lin. [ID] C. Wang ([✉]) [ID].
College of Computer Science and Electronic Engineering Hunan University, Changsha 410082, China
H. Lin
E-mail: haironglin@hnu.edu.cn
C. Wang
E-mail: wch1227164@hnu.edu.cn
L. Cui.
School of Information and Electrical Engineering, Hunan University of Science and Technology, Xiangtan, 411201, China.
Y. Sun.
School of Engineering and Computer Science, University of Hertfordshire, Hatfield AL10 9AB, U.K.
X. Zhang.
College of Electrical and Information Engineering, Hunan University, Changsha 410082, China.
W. Yao.
School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha, 410114, China.

1 Introduction

Since the birth of the famous Hopfield neural network (HNN) in 1984, it has been widely investigated due to its rich brain-like chaotic dynamics [1]. As is well known, the brain has abundant chaotic behaviors associated with brain information processing. The HNN is regarded as a typical paradigm to study the dynamics of brain activities [2]. Moreover, numerous researchers have found that the HNN has many applications which heavily depend on its dynamical behavior in different areas such as combinatorial optimization and secure communication [3,4]. Undoubtedly, the study of chaotic dynamics in HNNs is beneficial to better understand neural activities of the human brain and is also potentially useful for developing new neuromorphic systems.

Over the past two decades, many important chaotic phenomena have been revealed from different HNNs. For example, transient chaos [5], chaos [6–8] and hyperchaos [9] can be generated from some small HNNs by adjusting their synaptic weights. In particular, many researchers in recent years have focused on the memristive HNNs because of their complex chaotic dynamics.

As a kind of nonlinear circuit component, the memristor is considered as an organic link between the magnetic field and electric field, whose resistance can be altered by regulating the voltage or current [10]. In view of this, the memristor is usually used to emulate neural synapses or to describe the effect of electromagnetic radiation on the cell membrane of the neuron [11–14]. Due to the special nonlinearity, the neural networks with memristor, namely memristive neural networks have more complex chaotic dynamics like hyperchaos [15], coexisting behaviors [16], multistability [17], extreme multistability [18], and so on [19–22]. In particular, Pham *et al.* [23] found the hidden attractors in a memristive HNN with three neurons. Bao *et al.* discovered coexisting asymmetric attractors in a hyperbolic-type memristive HNN with three neurons [24]. Chen *et al.* observed coexisting multiple attractors, namely multistability in a memristive HNN with two neurons [25]. Lin *et al.* reported a multi-stable memristive four-neuron-based HNN which can generate coexisting infinite attractors [26]. Very recently, Zhang *et al.* proposed a memristive HNN with initial boosted coexisting multi-double-scroll attractors [27]. However, these studies are mainly focused on the neural network with mixed structures, and there is little work on the neural network with other structures, especially ring structures. On the other hand, it will be useful to investigate the chaotic dynamics of a neural network from the structure and topology viewpoint.

In fact, ring neural networks (RNNs) have limited biological relevance and can be seen as building blocks for networks with more realistic connection topologies. The RNNs are also a kind of cyclic feedback system whose stability has been studied extensively. For example, the asymptotic stability and global stability of the RNNs with time delays were studied in [28]. The stability of the delayed RNNs was investigated in [29]. Furthermore, exponential stability was revealed in a delayed RNN with a small-world connection [30]. Specially, the chaotic dynamics of the discrete-time-delayed RNNs were explored in [31]. But as far as we know, no previous study has researched the chaotic behavior of the continuous-time RNNs. Therefore, modeling, research, simulation, circuit realization and engineering application of RNNs to further understand brain activities and develop new neuromorphic computing systems are significant and valuable.

With the rapid growth of information technology and medicine, there are more and more digital medical images that need to use in several medical fields such as telediagnosis, telesurgery, and so on [32]. The extensive use and transfer of medical images have attracted many researchers to develop various medical image encryption schemes. Due to the feature of bulky data size, stronger correlation and high redundancy, the traditional encryption algorithms like AES, DES and RSA are not suitable for encrypting medical images [33]. Consequently, in recent years, researchers have proposed many new medical image encryption algorithms [34,35]. Among them, the chaos-based medical image encryption schemes have attracted wide attention due to the outstanding characteristics of chaos such as stochasticity, ergodicity, and sensitivity to initial states [36–39]. So far, several researchers have presented a great number of medical image encryption schemes based on various chaotic systems such as edge maps [40], Lorenz system [41], sine map [42] and logistic map [43]. Recently, some medical image encryption schemes using chaotic neural networks have attracted the extensive attention of academic and industrial fields because of their neural and chaotic characteristics. For instance, Njitacke *et al.* proposed a biomedical image encryption scheme based on a simple Hopfield neural network [44]. Due to the complex multistability dynamics of the neural network, the proposed cryptosystem achieved higher information entropy and lower correlation. Furthermore, Doubla *et al.* [45] designed a medical image encryption algorithm based on a tabu learning two-neuron network. The test results demonstrated that the algorithm is highly secure compared to other chaos-based encryption algorithms. As we all know, compared with the traditional neural networks, memristive neural networks have more complex chaotic behaviors, especially hyperchaos, which makes the encryption more secure in theory. To our knowledge, memristive neural networks-based medical image cryptosystems have not been reported until now.

Motivated by the above analysis, this paper first presents a memristive ring neural network (MRNN) based on the HNN and a flux-controlled memristor. Then, the complex hyperchaos and multistability are revealed by using several numerical analysis methods. To the best of our knowledge, this is the first time that the chaotic dynamics of the ring neural network is investigated. Afterward, we further design and implement an analog circuit of the MRNN based on commercially available electric elements. Finally, we give a medical image encryption scheme and explore its application feasibility by using a hyperchaotic sequence generated by the MRNN. Theoretical analysis and experimental results show that the designed medical image encryption scheme has larger keyspace, better information entropy, higher key sensitivity, and higher NPCR and UACI compared with the cryptosystems based on other chaotic systems.

The rest of this article is organized as follows. Section 2 constructs an MRNN and discusses its equilibrium point stability. Section 3 analyzes the chaotic dynamics of the MRNN. Section 4 designs and implements an analog MRNN circuit. Section 5 presents a medical image encryption scheme based on the MRNN, and its FPGA experiment is implemented. Section 6 concludes the paper.

2 Memristive ring neural network

2.1 Model Description

Hopfield neural network with chaos is usually utilized to mimic the chaotic behavior of the brain neural systems. An Hopfield neural network consisting of n neurons can be expressed as follows: [1]

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

where C_i, R_i and v_i are respectively capacitance, resistance, and voltage 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, $\tanh(.)$ 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 depend on its w_{ij}.

In this paper, we regard the neural network composed of four neurons, and its topology structure is shown in Fig.1. As can be seen, N_1-N_4 are four neurons, and the four neurons are made up of a ring neural network. Here, C_i=1, R_i=1, I_i=0 (i=1,2,3,4). Because of magnetic flux characteristics, the memristor can be used to describe the influence of electromagnetic radiation on the neurons. When the neuron N_1 is stimulated by the external electromagnetic radiation [46], the MRNN can be modeled and written as follows:

$$\begin{cases} \dot{x}_1 = -x_1 + 1.9 \tanh(x_1) + 0.1 \tanh(x_2) - 11 \tanh(x_4) \\ \quad - \rho\varphi^2 x_1 \\ \dot{x}_2 = -x_2 - 0.1 \tanh(x_1) + 1.5 \tanh(x_2) + 7 \tanh(x_3) \\ \dot{x}_3 = -x_3 - 4 \tanh(x_2) + 1.8 \tanh(x_3) + 4 \tanh(x_4) \\ \dot{x}_4 = -x_4 + 0.81 \tanh(x_1) + 0.2 \tanh(x_3) + 2 \tanh(x_4) \\ \dot{\varphi} = x_1 - \mu\varphi \end{cases}, \quad (2)$$

where x_i stands for the membrane voltage of neuron N_i, and φ shows the magnetic flux across the membrane of neuron N_1. The system parameters ρ and μ represent the feedback coefficient of electromagnetic radiation and the effect of magnetic flux on the generation
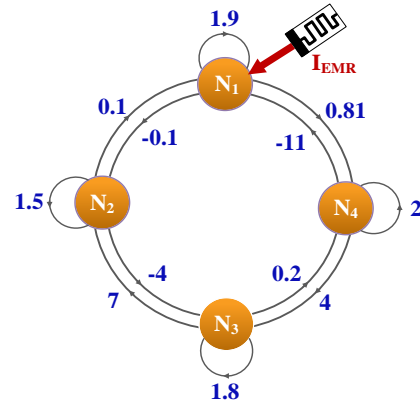

Fig. 1: Topological connection of the MRNN.

of membrane voltage x_1, respectively. Additionally, φ^2 denotes memductance of a flux-controlled memristor. Here, it is used to represent the coupling between φ and x_1. According to the function of flux-controlled memristor, the influence of external electromagnetic radiation can be considered as an additional forcing current I_{EMR}=$\rho\varphi^2 x_1$.

2.2 Equilibrium Point and Stability Analysis

The equilibrium points of the MRNN and their stabilities are revealed by numerical analysis methods. Setting (2) equal to zero, the equilibrium points of the MRNN can be solved. Assuming E=$(x, y, m, n, z)^T$ is an equilibrium point of the MRNN (2). According to equilibrium equation of the MRNN, we can get

$$m = \text{atan}((y + 0.1 \tanh(x) - 1.5 \tanh(y))/7), \quad (3)$$

$$n = \text{atan}((-\rho x^3/\mu^2 - x + 1.9 \tanh(x) + 0.1 \tanh(y))/11), \quad (4)$$

$$z = x/\mu. \quad (5)$$

And x, y are the intersection points of the functions h_1 and h_2.

$$\begin{cases} h_1(x, y) = -m - 4 \tanh(y) + 1.8 \tanh(m) + 4 \tanh(n) \\ h_2(x, y) = -n + 0.81 \tanh(x) + 0.2 \tanh(m) + 2 \tanh(n) \end{cases}. \quad (6)$$

Extensive numerical simulation results show that there is only one zero intersection point (x, y)=$(0, 0)$. That is to say, the MRNN has only one zero equilibrium point $E_0(0, 0, 0, 0, 0)$. The Jacobian matrix at the

zero equilibria can be obtained by

$$J = \begin{bmatrix} 0.9 & 0.1 & 0 & -11 & 0 \\ -0.1 & 0.5 & 7 & 0 & 0 \\ 0 & -4 & 0.8 & 4 & 0 \\ 0.81 & 0 & 0.2 & 1 & 0 \\ 1 & 0 & 0 & 0 & -\mu \end{bmatrix}, \qquad (7)$$

For the zero equilibrium point $E_0(0, 0, 0, 0, 0)$, the characteristic polynomial equation is reduced as

$$\begin{aligned} P(\lambda) &= det\,|\lambda E_1 - J| \\ &= (\lambda + \mu)(\lambda^4 - 3.2\lambda^3 + 3.77\lambda^2 - 1.93\lambda - 250.2276), \\ &= 0 \end{aligned} \qquad (8)$$

where E_1 is a fourth-order unit matrix. MATLAB numerical calculations show that there are one real root $\lambda_1 = -\mu$ and four complex roots $\lambda_2 = 0.6337 \pm 5.1863j$ and $\lambda_3 = 0.9663 \pm 3.0345j$. Therefore, the zero equilibrium point is an unstable saddle-focus point, which is considered as a necessary condition for the generation of chaos. That is to say, the attractors generated by the MRNN are self-excited attractors.

3 Dynamical analysis of the MRNN

In this part, the complicated dynamics of the presented MRNN is investigated by adopting basic dynamic analysis methods such as phase plots, bifurcation diagrams, Lyapunov exponents, and basins of attraction. The MATLAB R2017a with the ODE45 algorithm is employed in numerical simulation. Besides, the start time 500, time step 0.01, and time length 2000 are adopted.

3.1 Hyperchaotic Dynamics

Firstly, fix the parameter $\rho = 0.4$ and the initial states are set to (0.1, 0.1, 0.1, 0.1, 0.1). When varying μ in the region of [0, 1.4], the bifurcation diagram of the state variable x_1 and the corresponding first five Lyapunov exponents are shown in Fig.2(a) and Fig.2(b), respectively. It can be seen from Fig.2 that the MRNN can generate complex dynamical behaviors including period, quasi-period, chaos and hyperchaos. For example, with μ increasing from 0 to 1.4, the dynamical trajectory of the MRNN starting from period enters into chaos at $\mu = 0.15$ by the forward period-doubling bifurcation (FPDB) route, and then the chaotic behavior degrades into periodic behavior at $\mu = 0.21$ by the reverse period-doubling bifurcation (RPDB) route. Afterward, the periodic behavior changes to chaotic behavior again at $\mu = 0.27$. Interestingly, with μ increasing to 0.38, the MRNN enters into hyperchaos with two positive Lyapunov exponents from chaotic behaviors by a short
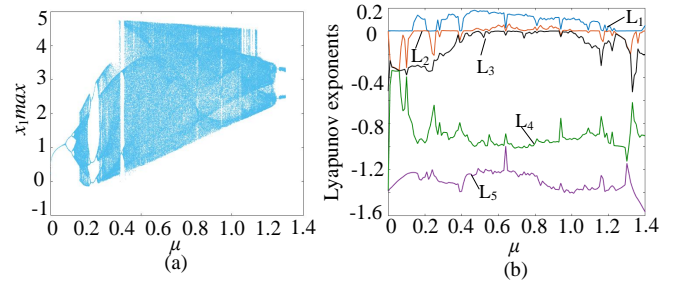

Fig. 2: The μ-dependent dynamics with $\rho = 0.4$ and initial states (0.1, 0.1, 0.1, 0.1, 0.1). (a) Bifurcation diagram. (b) First five Lyapunov exponents.
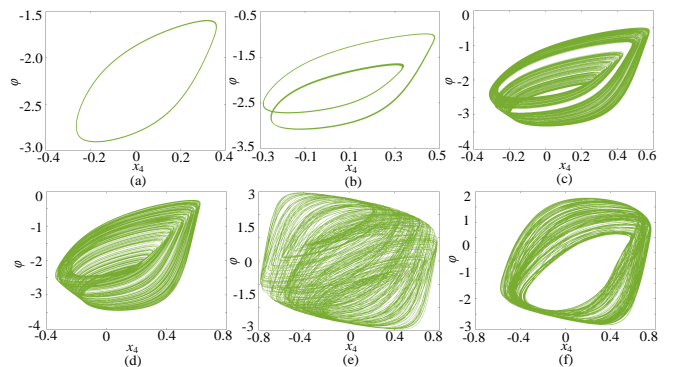

Fig. 3: Dynamical behaviors of the MRNN for different values of μ. (a) Limit ring attractor with $\mu = 0.05$. (b) Period-2 attractor with $\mu = 0.1$. (c) Quasiperiodic attractor with $\mu = 0.14$. (d) Chaotic attractor with $\mu = 0.16$. (e) Hyperchaotic attractor with $\mu = 0.6$. (f) Chaotic attractor with $\mu = 1.1$.

FPDB route again. It can be seen that the MRNN exhibits a wide range of hyperchaos until $\mu = 1$. Then hyperchaotic behavior again turns into chaotic behavior. It is noted that this chaos has a different topology from foregoing chaos. Finally, chaos settles into a period state at $\mu = 1.3$. It can also be seen that the Lyapunov exponents and the bifurcation diagram matches well with each other. The phase portraits of the MRNN with different values of μ are given to illustrate its dynamical evolution with the parameter μ, as shown in Fig.3. Results show that when the parameter μ are set to 0.05, 0.1, 0.14, 0.16, 0.6 and 1.1, we can get limit ring attractor, periodic attractor, quasiperiodic attractor, chaotic attractor, hyperchaotic attractor and chaotic attractor with different topologies, respectively.

Additionally, by calculating Lyapunov exponents, it will be shown in this work that the MRNN has a hyperchaotic attractor for the value of parameters and initial values as $\rho = 0.4$ and $\mu = 0.6$ and (0.1, 0.1, 0.1, 0.1, 0.1). The Lyapunov exponents for the MRNN are computed

for t=1e5 seconds as fowwows:

$$LE_1 = 0.1611, LE_2 = 0.0512,$$
$$LE_3 = 0, LE_4 = -0.9991, LE_5 = -1.223 \tag{9}$$

The existence of two positive Lyapunov exponents in (9) makes it clear that the MRNN is hyperchaotic. Furthermore, the Kaplan-Yorke dimension of the hyperchaotic MRNN is calculated by following formula:

$$D_{KY} = 3 + \frac{LE_1 + LE_2 + LE_3}{|LE_4|} = 3.2125 \tag{10}$$

The MRNN has high complexity because it has a large value of D_{KY}.

3.2 Multistability Dynamics

Multistability is a complex dynamical phenomenon that there are coexisting multiple different attractors in the chaotic system under different initial states [47–50]. In this subsection, the multistability with coexisting four different attractors is discovered from the MRNN. Similarly, fix the parameter ρ=4 and the initial states are set to (0.1, 0.1, 0.1, 0.1, 0.1) colored in wathet blue, (-0.1,-0.1,-0.1,-0.1,-0.1) colored in pink, (0.1, 0.1, 0.1, 1, 1) colored in blue green, and (-0.1, -0.1, -0.1, -1, -1) colored yellow. When varying μ in the region of [0, 1], four bifurcation diagrams of the state variable x_1 are shown in Fig. 4(a). As can be seen, in Fig.4(a), the MRNN has different bifurcation diagrams under different initial states. In other words, the MRNN generates coexisting behaviors. For instance, for the wathet blue bifurcation route, the dynamical state starting from period enters into chaos at μ=0.12 by the FPDB route. Thereafter, the chaotic behavior degrades into periodic behavior at μ=0.78 by the RPDB route. Note that there are several periodic windows in the chaotic region. Similarly, the pink bifurcation route is the same as the wathet blue bifurcation route. But their phase positions are different. Furthermore, for the yellow bifurcation route, the dynamical state exhibits a wide range of period behavior in the region $\mu \in$(0, 0.55). After that, the periodic behavior becomes chaotic behavior until μ=0.78. Similarly, the blue green bifurcation route is the same as the yellow bifurcation route except for phase-amplitude. Evidently, when $\mu \in$(0, 0.55) the MRNN has four different bifurcation routes under four different initial states. That is to say, the MRNN exhibits complex multistability. Fig.4(b) gives the corresponding first five Lyapunov exponents. To further verify the multistability, we have given a set of phase plots with different initial states, as shown in Fig.5. As can be seen from Fig.5, the MRNN generates four attractors including two symmetry period attractors and
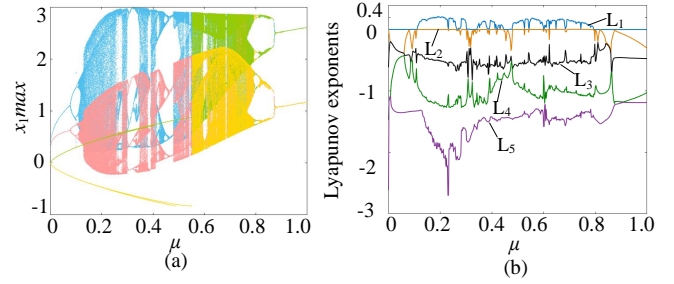

Fig. 4: The μ-dependent dynamics with ρ=4 . (a) Bifurcation diagram under initial states (0.1, 0.1, 0.1, 0.1, 0.1) colored in wathet blue, (-0.1, -0.1, -0.1, -0.1, -0.1) colored in pink, (0.1, 0.1, 0.1, 1, 1) colored in blue green, (-0.1, -0.1, -0.1, -1, -1) colored in yellow. (b) First five Lyapunov exponents under initial state (0.1, 0.1, 0.1, 0.1, 0.1).
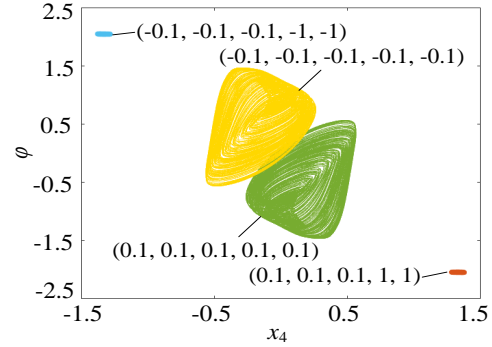

Fig. 5: Coexisting multiple attractors with ρ=4 and μ=0.2.

two symmetry chaos attractors under four sets of different initial states. Consequently, the MRNN exhibits a complex multi-stable phenomenon.

Further, the basin stability analysis reveals the multistability dynamics of the MRNN. Here, when μ=0.2, ρ=4 and x_{10}=x_{20}=x_{30}=0.1 are kept, the local attraction basin in the x_{40}-φ_0 plane is drawn as shown in Fig.6. As can be observed, the local attraction basin displays interesting manifold structures and clear basin boundaries, and the specified initial value regions are made up of different colored zones labeled by r_0-r_4, among which the colored zones are labeled by r_1-r_4 correspond to the attractors with different positions in Fig.6. Furthermore, the blue green region represents stable point attractors. The numerical results in Fig.5 and Fig.6 show that the dynamic behaviors in the MRNN strongly depend on its initial states. That is to say, the MRNN exhibits sensitive multistability.
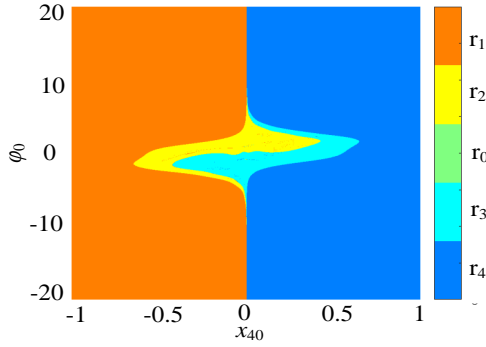
Fig. 6: For ρ=4, μ=0.2, chaotic basin of attraction in the x_{40}-φ_0 plane, and the colorbar shows the coexistence of two chaotic attractors and two periodic attractors.

## 4 Validation by Hardware experiments

In fact, the physical realization of neural network models is significant to exploit neuromorphic hardware systems. Generally speaking, nonlinear systems can be physically implemented by using FPGA [51] or analog circuits [52]. It is well known that an analog neural network circuit is able to get real-time calculation and can copy the behavior of a real neural system. Consequently, the proposed MRNN is successful implemented through take advantage of basic electronic circuit elements such as transistors, resistors, capacitors, operational amplifiers, and analog multipliers.

4.1 Design of the MRNN circuit

Before realizing the MRNN circuit, we firstly introduce two circuit units: memristor circuit [12] and hyperbolic tangent function circuit [8], as shown in Fig.7. In Fig.7(a), the circuit equation can be written as

$$\begin{cases} i = g^2 v_\varphi{}^2 v_i/R_L \\ C dv_\varphi/dt = v_i/R_a - v_\varphi/R_b \end{cases}, \tag{11}$$

where g=1 expresses the gain of the multiplier M. Moreover, for the hyperbolic tangent function circuit in Fig.7(b), the resistance of resistors are set as R_A=1.5 kΩ, R_B=0.5 kΩ, R_C=1 kΩ, and R_D=1.5 kΩ. According to (2), the circuit structure of MRNN can be designed in Fig.8. In the circuit, four out voltages v_1, v_2, v_3, v_4 represent four membrane voltages x_1, x_2, x_3, x_4, respectively. The synaptic weight coefficients in MRNN are replaced by the resistors R_1-R_{12}. Based on the circuit in Fig.8,
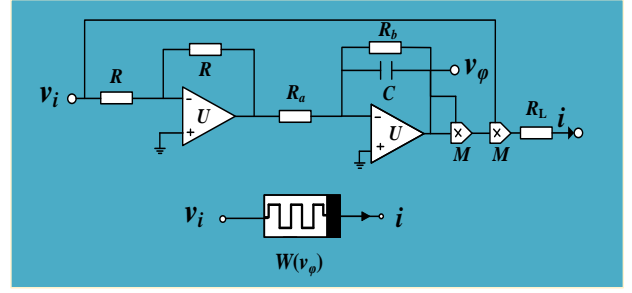
(a)
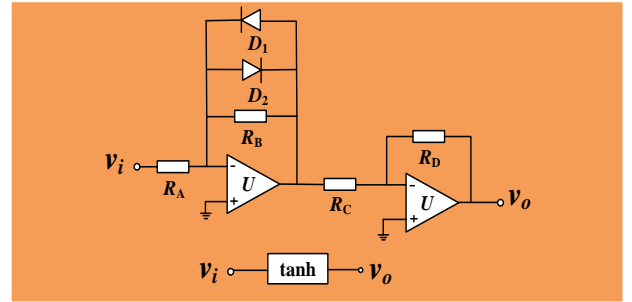
(b)

Fig. 7: Circuit units. (a) Memristor circuit (b) Hyperbolic tangent function circuit.

the circuit state equations can be written by

$$\begin{cases} RC\frac{dv_1}{dt} = -v_1 + \frac{R}{R_1}\tanh(v_1) + \frac{R}{R_2}\tanh(v_2) - \frac{R}{R_3}\tanh(v_4) \\ \qquad - \frac{R}{R_L}g^2 v_\varphi{}^2 v_1 \\ RC\frac{dv_2}{dt} = -v_2 - \frac{R}{R_4}\tanh(v_1) + \frac{R}{R_5}\tanh(v_2) + \frac{R}{R_6}\tanh(v_3) \\ RC\frac{dv_3}{dt} = -v_3 - \frac{R}{R_7}\tanh(v_2) + \frac{R}{R_8}\tanh(v_3) + \frac{R}{R_9}\tanh(v_4) \\ RC\frac{dv_4}{dt} = -v_4 + \frac{R}{R_{10}}\tanh(v_1) + \frac{R}{R_{11}}\tanh(v_3) + \frac{R}{R_{12}}\tanh(v_4) \\ RC\frac{dv_\varphi}{dt} = \frac{Rv_1}{R_a} - \frac{Rv_\varphi}{R_b} \end{cases}, \tag{12}$$

Assuming that C_1=C_2=C_3=C_4=C, RC=10 us, and R=10 kΩ, then C can be chosen as 1 nF. Regarding the constant synaptic weight coefficients, resistors can be calculated as R_a=10 kΩ, R_1=5.263 kΩ, R_2=100 kΩ, R_3=0.909 kΩ, R_4= 100 kΩ, R_5=6.667 kΩ, R_6=1.428 kΩ, R_7=2.5 kΩ, R_8= 5.556 kΩ, R_9=2.5 kΩ, R_{10}=12.346 kΩ, R_{11}=50 kΩ, R_{12}=5 kΩ. Besides, R_b=R/μ and R_L=R/ρ are adjustable resistors.

4.2 Measurement of the MRNN Circuit

The designed MRNN circuit is physically constructed on the experimental breadboard via adopting commercially available circuit elements including R/metal resistors and precision potentiometers, C/ceramic capacitors, D/1N4007, M/AD633JN, U/TL082CP, and
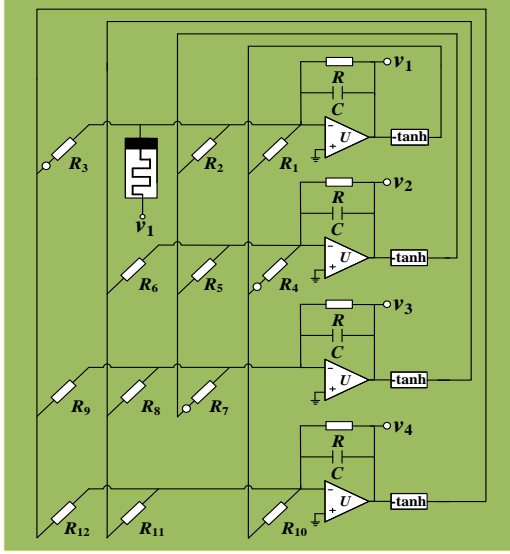
Fig. 8: Memristive ring neural network circuit.

±15V DC voltage supplies. Numerous experiments indicate that the designed MRNN circuit can realize results agree with the numerical simulation results in section 3. For example, when ρ=0.4 and with different μ, namely R_L=25 kΩ and different R_b varies, the experimental results are given in Fig.9(a)-(f), respectively. The experimental results in Fig.9 verify the numerical results in Fig.3. It is remarked that because there are parasitic parameters in the practical neural network circuit, the values of resistors have some difference, which can be remedied by fine-tuning the adjustable resistors.
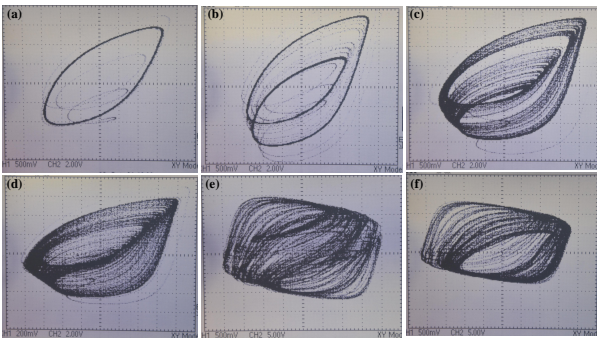

Fig. 9: Hardware experiment results. (a) Limit ring attractor with R_b=200 kΩ. (b) Period-2 attractor with R_b=100 kΩ. (c) Quasiperiodic attractor with R_b=70 kΩ. (d) Chaotic attractor with R_b=62 kΩ. (e) Hyperchaotic attractor with R_b=16.5 kΩ. (f) Chaotic attractor R_b=9 kΩ.

5 Application in Medical Image Encryption

In recent years, chaos-based image encryption schemes have attracted wide attention [53, 54]. Generally, hyperchaos with at least two positive Lyapunov exponents has more complicated dynamics than the ordinary chaos with only one positive Lyapunov exponent and it is more applicable for a lot of chaos-based security applications [55]. In addition, chaotic systems with multistability dynamics have become potential candidates for chaos-based image encryption applications compared to normal chaotic systems due to their high initial sensitivity [56]. In this section, a medical image encryption scheme based on the MRNN with hyperchaos and multistability is designed.

5.1 Design of Medical Image Encryption Scheme

As shown in Fig.10, the entire structure of the MRNN-based medical image encryption scheme is mainly composed of four parts: chaotic sequence generator, secret key generator, image encryption module and decryption module. Assuming that a gray-scale plain image P is used as the encryption object, those modules can be briefly described as follows.

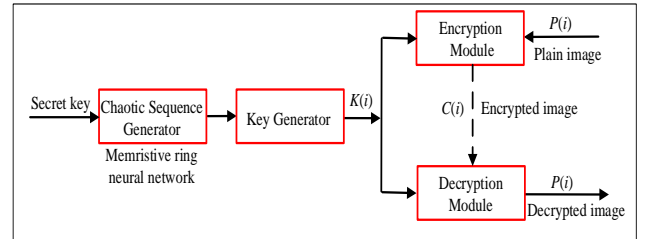

Fig. 10: The structure of the medical image encryption scheme based on the MRNN.

(1) Chaotic sequence generator: Install system parameters and initial states, then iterate the memristive ring neural network (2) with the fourth-order Runge-Kutta algorithm from initial states $(x_{10}, x_{20}, x_{30}, x_{40}, \varphi_0)$. The MRNN is iterated continuously. We can get five chaotic sequences $(x_{1i}, x_{2i}, x_{3i}, x_{4i}, \varphi_i)$ kept the same length as the plain image.

(2) Key generator: These sequences are reprocessed as follows:

$$K_1(i) = |x_{1i}| + |x_{2i}| + |x_{3i}| + |x_{4i}| + |\varphi_i|, \quad (13)$$

$$K_2(i) = \mathrm{mod}(\mathrm{floor}((|x_{1i}| + |x_{2i}| + |x_{3i}| + |x_{4i}| + |\varphi_i|) * 10^{15}), 256), \quad (14)$$

Table 1: NIST statistical test results of the proposed MRNN

No.	Test index	Prop.	P-value
01	Frequency	0.992	0.699313
02	Block Frequency	0.990	0.494392
03	Cum. Sums (F)	0.992	0.249284
	Cum. Sums (R)	0.98	0.494392
04	Runs	0.985	0.657933
05	Longest Runs	0.992	0.574903
06	Rank	0.991	0.739918
07	FFT	0.987	0.383827
08	NOT*	0.992	0.816537
09	OT	0.990	0.534146
10	Universal	0.990	0.474986
11	Approx. Entropy	0.992	0.455937
12	Random Exc.*	0.989	0.867692
13	Random Exc. Var.*	0.985	0.834308
14	Serial (1st sub-test)	0.987	0.474986
	Serial (2nd sub-test)	0.992	0.911413
15	Linear complexity	0.990	0.834308

where the floor(x) means the values of x to the nearest integers less than or equal to x.

(3) Encryption module: This module contains two parts, namely, permutation and substitution. First, the secret key K_1 is used to permutate original image. The plain image is permutated as

$$P_1(i) = P(index(K_1(i))) \tag{15}$$

Then the permutation image P_1 is further encrypted as

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

where the symbol $\oplus$ exprees the special XOR operation bit-by-bit. The MRNN is operated until all the elements are encrypted. Then each element in the encrypted set is turned into decimal numbers. Finally, the cipher image can be generated.

(4) Decryption module: The cipher image is decrypted by a reverse process.

In our experiemnts, setting the secret key (ρ, μ, x_{10}, x_{20}, x_{30}, x_{40}, φ_0)=(0.4, 0.6, 0.1, 0.1, 0.1, 0.1, 0.1), a hyperchaotic pseudorandom sequence (Lyapunov exponents: L_1, L_2, L_3, L_4, L_5)=(0.1611, 0.0512, 0, -0.9991, -1.223) generated by (13) is used for image encryption. In experiment, the pre-iterate number N_0 of the chaotic system is set as 500, and the time step is chosen as 0.005. Before image encryption, the hyperchaotic sequence is tested by using the NIST SP800-22 test suite. Table 1 gives the test results of the hyperchaotic sequence generated by the MRNN. From the results, it is clear that they can successfully pass all the sub-tests of the test suite. This suggests that the MRNN enjoys complicated chaotic dynamics and can generate random numbers with high randomness.
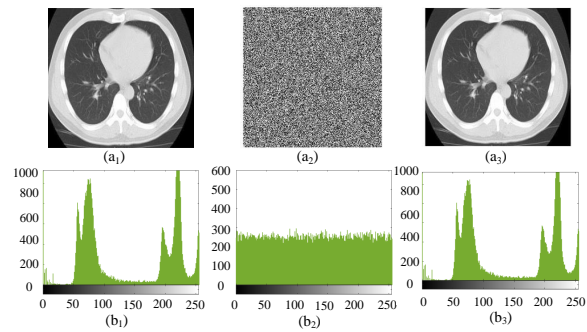

Fig. 11: Simulation results of the proposed medical image encryption scheme: (a_1) Original medical image. (b_1) Histogram of the original medical image. (a_2) Encrypted medical image. (b_2) Histogram of the encrypted medical image. (a_3) Decrypted medical image. (b_3) Histogram of the decrypted medical image.

5.2 Experimental Results and Analysis

In this subsection, the efficiency of the presented medical image cryptosystem is evaluated. Some classic metrics like keyspace, histogram, correlation coefficient, entropy, secret key sensitivity, NPCR, UACI, noise attacks and SSIM are measured [44,54]. In whole experiments, one medical image Lung of size 256×256 is employed as the test image, as shown in Fig.11(a_1).

(1) Keyspace compute: A large keyspace show that the image encryption algorithm possess ability to oppose the exhaustive attack. The presented encryption scheme adopts two parameters and five initial values 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 $(10^{16})^7 = 10^{112} \approx 2^{336}$. 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 medical image encryption schemes, such as [44, 45]. From this, we can conclude that the new encryption scheme has a greater keyspace.

(2) Histogram test: The histogram denotes the frequency distribution of pixel values in the image. Usually, a well-designed image encryption scheme can ensure the histogram of the encrypted image has a even distribution to withstand any statistical attacks. Fig.11 (a_1)-(a_3) and Fig.11 (b_1)-(b_3) shows the original medical image, encrypted medical image, and decrypted medical image, as well as their histograms, respectively. Clearly, the encrypted medical image has a uniform histogram. Fig.11 visually illustrates that the designed medical image encryption scheme is able to overcome statistical attacks well.
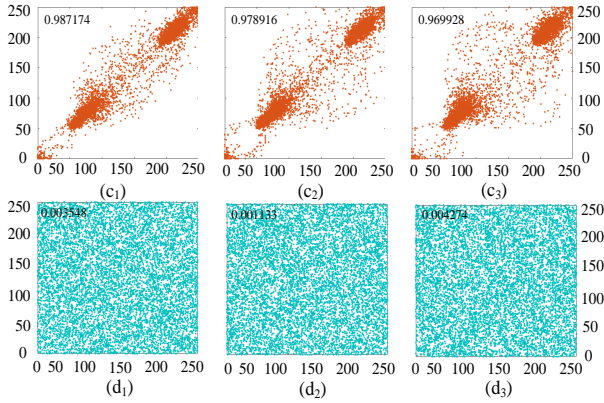
(c₁) ... (c₂) ... (c₃)
(d₁) ... (d₂) ... (d₃)

Fig. 12: Distribution of correlation for original medical image and encrypted medical image. (c$_1$, d$_1$) Horizontal. (c$_2$, d$_2$) Vertical. (c$_3$, d$_3$) Diagonal.
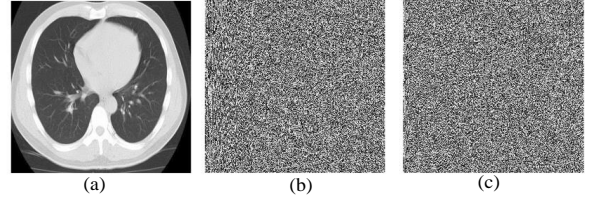

(a) ... (b) ... (c)

Fig. 13: Key sensitivity analysis. (a) The decrypted image with the correct secret key. (b) The decrypted image with the wrong secret key $\rho = 0.4 + 10^{-14}$. (c) The decrypted image with the wrong secret key $x_{40} = 0.1 + 10^{-14}$.

(3) Correlation analysis: As we all know, the original image own a large correlation coefficient in the horizontal, vertical, and diagonal directions. However, from the view of security, the correlation coefficients of the encrypted image are wish to be close to zero in the each directions. The correlation coefficients of each pair of pixels in image can be derived as [44]

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

where

$$\begin{cases} E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \\ E(y) = \frac{1}{N}\sum_{i=1}^{N} y_i \end{cases}, \quad (18)$$

where the values of two adjacent pixels can be represented by x and y. The total number of pixels can be denoted by N. Therefore, to calculate the correlation coefficient in every directions, 10000 pairs of adjacent pixels are randomly chosen from the original and encrypted image. Fig.12 shows the results of correlation coefficients of the original and encrypted images. The results manifest that the original image has a higher correlation value, nevertheless the encrypted image has a lower correlation value. From the outcomes stated about correlation coefficient, the proposed image encryption scheme can efficiently improve the correlation between adjacent pixels of the original image.

(4) Entropy analysis: The information entropy is an crucial index to evelute the randomness of encrypted images. Generally, the information entropy can be expressed mathmatically by following equations [44]

$$H(P) = \sum_{i=0}^{2^N-1} P(x_i)\log_2\frac{1}{P(x_i)}, \quad (19)$$

where $P(x_i)$ indicates the probability of the existence of the symbol x_i, and N represents the bit depth of the image P. The ideal value for a greyscale image is 8. Here, the derived entropy value of the encrypted image is 7.9978, which is close to the ideal value of 8. In other words, the designed image encryption scheme has a good information entropy.

(5) Sensitivity discussion:The key sensitivity is a vital indicator for evaluating the accuracy of a cryptosystem. A good image encryption algorithm should be sensitive to the security keys. In this image encryption algorithm, the system parameters and initial values $(\rho, \mu, x_{10}, x_{20}, x_{30}, x_{40}, \varphi_0)$ are regared as secret keys. We use the correct secret key to decrypt the encrypted medical image shown in Fig.11(a$_2$) and to produce the corresponding decrypted medical image shown in Fig.13(a). A minor modification is carried out in the correct secret key to check the sensitiveness of the keys. For instance, the decrypted image with the wrong secret key $\rho = 0.4 + 10^{-14}$, and the decrypted image with the wrong secret key $x_{40} = 0.1 + 10^{-14}$ are demonstrated in Fig.13(b) and Fig.13(c), respectively. The results show that the designed medical image encryption method has good key sensitivity to small key changes.

(6) NPCR and UACI analysis: The number of pixel change rates (NPCR) and unified average change intensity (UACI) are used to evaluate the change in the encrypted images after changing a single-pixel value of the plain image. Usually, NPCR and UACI can be expressed by [44]

$$NPCR(C_1, C_2) = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{D(i,j)}{M.N} \times 100\%, \quad (20)$$

$$D(i,j) = \begin{cases} 0, & if C_1(i,j) = C_2(i,j) \\ 1, & if C_1(i,j) \neq C_2(i,j) \end{cases}, \quad (21)$$

$$UACI(C_1, C_2) = \frac{1}{M.N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%, \quad (22)$$

where C_1 and C_2 are two different encrypted images with both sizes equal to MN, whose corresponding original images only have a single-pixel difference. $C_1(i,j)$ and $C_2(i,j)$ represent the gray values of the pixels in position (i,j). The outcomes of NPCR and UACI for the experimented images are given in Table 3. As we all know, for a robust encryption scheme, the ideal values of NPCR and UACI are 99.6094% and 33.4635%, respectively. The presented encryption scheme can generate the values of NPCR and UACI above the ideal values. Therefore, the proposed encryption scheme has a high sensitivity to tiny pixel changes in the original image.

(7) Data loss and noise attacks: Generally, the images are easy to suffer from noise and partial data loss in the encryption system. Thus, the data loss attack and the noise attack can be used to evaluate the robustness of the proposed image encryption scheme. First, we cut off some parts of the encrypted image and then decrypt it. The results of data loss attacks for the different lost areas are given in Fig.14(a$_1$-a$_3$) and Fig.14(b$_1$)-(b$_3$). Interestingly, the main information in the original image can be recovered with the decryption. Then, we added Gaussian noise to the encrypted image with different proportions. Fig.14(c$_1$-c$_3$) and Fig.14(d$_1$)-(d$_3$) show the outcomes of the noise attacks. Although some data in decrypted images are changed, the original information still can be displayed. This means that the encrypted scheme has strong robustness.

(8) SSIM analysis: The structural similarity (SSIM) is a measure of similarity between two images. For two images x and y, SSIM can be calculated as follows [57]:

$$SSIM(x,y) = \frac{(2\mu_x \mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}, \quad (23)$$

where μ_x and μ_y are average values of x and y, respectively. σ_x^2 and σ_y^2 are a variance of x and y, respectively. σ_{xy} is the covariance between x and y. $c_1 = (k_1 L)^2$ and $c_2 = (k_2 L)^2$ are two constants, where $k_1 = 0.01$, $k_2 = 0.03$, and L is the dynamic range of pixel values. Table 2 gives the calculation results of SSIM for all the decrypted images compared with the original image. It can be seen from Table 2 that the encrypted image Fig.11(a$_2$) and the correct decrypted image Fig.11(a$_3$)
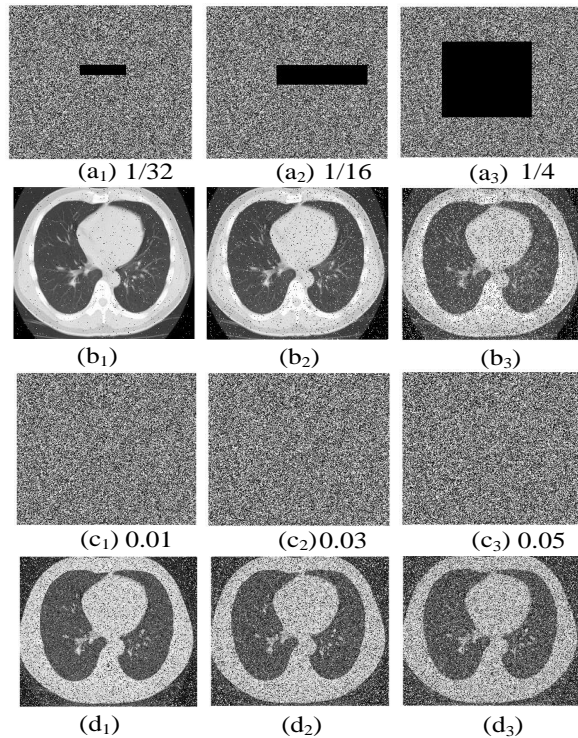

Fig. 14: The robustness of the proposed encryption scheme to partial data loss and noise attacks. (a$_1$-a$_3$) The encrypted image with 1/32, 1/16, and 1/4 loss, respectively. (b$_1$-b$_3$) Corresponding decryption images. (c$_1$-c$_3$) The encrypted image with 0.01, 0.03, and 0.05 Gaussian noise, respectively. (d$_1$-d$_3$) Corresponding decryption images.

have ideal SSIM values of 0 and 1, respectively. Furthermore, the incorrect decrypted images Fig.13(b) and Fig.13(c) exhibit very low values of SSIM, which means that the encryption scheme has a high key sensitivity. On the contrary, the decrypted images Fig.14(b$_1$-b$_3$) and Fig.14(d$_1$-d$_3$) exhibit high values of SSIM, which means that the main image information can be well recovered when the original images suffered from data loss and noise attacks.

Table 2: The values of SSIM between different decrypted images and the original image.

Images	SSIM
Fig.11(a$_2$)	-0.0013
Fig.11(a$_3$)	1
Fig.13(b)	0.0062
Fig.13(c)	0.0044
Fig.14(b$_1$)	0.9837
Fig.14(b$_2$)	0.9388
Fig.14(b$_3$)	0.7594
Fig.14(d$_1$)	0.7611
Fig.14(d$_2$)	0.6293
Fig.14(d$_3$)	0.5536

Table 3: Performance comparision of various encryption scheme

Refs	Image type	System type	Dynamical property	Keyspace	Entropy Original Encrypted	Key sensitivity	NPCR(%) UACI(%)	Hardware verification
2019[53]	Lena (256×256)	3D Chaotic system	Chaotic Multi-scroll	2^{144}	7.3740 7.9898	–	–	No
2020[54]	Lena (256×256)	3D Chaotic system	Chaotic Multi-wing	2^{288}	7.3740 7.9976	10^{-9}	–	Yes
2021[56]	Lena (256×256)	4D Chaotic system	Chaotic multistability	–	7.4699 7.9979	10^{-12}	–	No
2020[44]	Chest (256×256)	3D HNN	Chaotic multistability	2^{288}	7.3110 7.9992	–	99.6175 –	No
2021[45]	Cell (256×256)	4D tabu learning two-neuron	Chaotic multistability	–	7.9059 7.9989	10^{-10}	99.6200 33.6512	No
This work	Lung (256×256)	5D MRNN	Hyperchaotic multistability	2^{336}	6.8961 7.9978	10^{-14}	99.6299 33.6548	Yes

Meanwhile, based on different chaotic systems, Table 3 provides the performance comparison of encryption results between different image encryption schemes. Apparently, compared with the recent results of [44, 45, 53, 54, 56], it shows that the proposed medical image encryption scheme has a larger keyspace and more sensitive secret keys. Consequently, these results suggest that the designed medical image encryption scheme can effectively resist statistical attacks. Meanwhile, the proposed encryption scheme has a larger information entropy difference, which means that it can more effectively resist entropy attacks. Furthermore, the designed medical image encryption scheme has higher NPCR and UACI and good experimental results, which indicates that it can be applied to protect medical image data in practical information communication.

5.3 FPGA Demonstration

The field-programmable gate array (FPGA) is widely used in industrial electronics because of its features such as ultra-low power, programmable reusability, and strong controllability [58]. Here an FPGA-based hardware test platform is implemented to test the proposed MRNN-based medical image encryption scheme. The hardware devices contain one Xilinx Virtex-6 FPGA development board and one monitor. The hardware structure of the cryptosystem consists of five parts: medical image RAM (random access memory), chaotic sequence controller, medical image encryption module, medical image decryption module, and VGA display controller. It can be seen in Fig.15 that the image R-MA is used to store and output the original medical image from medical image acquisition devices. And the generation and buffering of chaotic sequences generated by the memristive ring neural network can be realized in chaotic sequence controller. In the process of
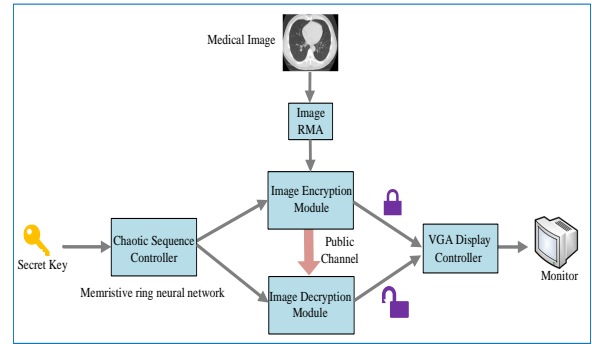

Fig. 15: Block diagram of FPGA-based image encryption and decryption.

medical image encryption, the image encryption module synchronously receive the chaos sequences and original medical images. The image encryption module is used to complete image encryption. Hereafter, the V-GA display controller receive the encrypted image. In the end, the original and encrypted medical images can be displayed on the monitor. On the other hand, for the process of image decryption, the decryption module synchronously receive the chaos sequences and the encrypted image. Meanwhile, the image decryption module completes the function of decryption. Eventually, the decrypted image can be output on the computer via using the VGA display controller.

Based on FPGA technology, hardware experiments is carried out on the medical image cryptography system with a fixed-point number. Using Xilinx ZYNQ-7000 series XC7Z020 FPGA chip, the hardware structure of the biomedical image cryptosystem in Fig.15 is implemented. The functions of the five modules are completed through adopting Verilog HDL programming, and the realization process of the chaos sequences can refer to work in [54]. In the hardware experiment, medi-
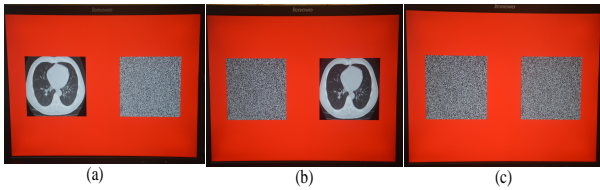
Fig. 16: FPGA-based implementation results of the MRNN-based image cryptosystem. (a) Original and encrypted image. (b) Encrypted and correctly decrypted image. (d) Encrypted and incorrectly decrypted image.

cal images are stored in the RAM of the ZYNQ-XC7Z020 chip. The experimental results are shown in Fig.16, where the original image and the encrypted image are shown in Fig.16(a) with the secret key $(\rho, \mu, x_{10}, x_{20}, x_{30}, x_{40}, \varphi_0)$=(0.4, 0.6, 0.1, 0.1, 0.1, 0.1, 0.1). Fig.16(b) shows the encrypted image and correct decrypted image with the correct secret key. And the encrypted image and the wrong decrypted image are shown in Fig.16(c) under incorrect secret key $(0.4+10^{-14}, 0.6, 0.1, 0.1, 0.1, 0.1, 0.1)$. Evidently, the experimental results based on FPGA are consistent with the simulation results based on MATLAB. Besides, the time for image encryption and image decryption on the FPGA platform are 0.214238 s and 0.209756 s, respectively. These times are much lower than the corresponding times of 0.689214 s and 0.657105 s in the MATLAB numerical simulations. In other words, based on the FPGA, the medical image cryptosystem can greatly promote the speed of data treating and the time of algorithm operation. Undoubtedly, the hardware experiment results verify the effectiveness and availability of the presented medical image scheme based on the memristive ring neural network.

6 Conclusion

In this paper, a MRNN with four neurons has been proposed. Research results show that the MRNN can generate abundant chaotic dynamics including FPDB, RPDB, chaotic attractors, hyperchaotic attractors, co-existing attractors and multistability. All numerical results were experimentally verified by an analog MRNN circuit. Moreover, a medical image encryption scheme based on the proposed MRNN is designed. Simulation results including keyspace analysis, histogram analysis, correlation analysis, entropy analysis, key sensitivity analysis, NPCR and UACI analysis, data loss and noise attacks analysis, and SSIM analysis demonstrate that the designed medical image encryption scheme has good security. The effectiveness of the medical image cryptosystem was testified by the FPGA hardware platform. The obtained results have demonstrated that the presented MRNN-based medical image encryption can be useful in several practical medical applications such as mobile health care services and wireless medical networking for protecting medical images.

Acknowledgment

Data Availability Statements

All data generated or analysed during this study are included in this published article (and its supplementary information files).

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflicts of interest.

References

1. Hopfield, J. J.: Neural network and physical system with emergent collective computational abilities. Proc. Nat. Acad. Sc. **79**, 2554-2558 (1982)
2. Ma, J., Tang, J.: A review for dynamics in neuron and neuronal network. Nonlinear Dyn. **89**(3), 1569-1578 (2017)
3. Yang, H., Wang, B., Yao, Q., et al.: Efficient hybrid multifaults location based on hopfield neural network in 5G co-existing radio and optical wireless networks, IEEE Trans. Cogn. Commun. Netw. **5**(4), 1218-1228 (2019)
4. Wang, X., Li, Z.: A color image encryption algorithm based on Hopfield chaotic neural network. Opt. Lasers Eng. **115**, 107-118 (2019)
5. Yang, X., Yuan. Q.: Chaos and transient chaos in simple Hopfield neural networks. Neurocomputing. **69**(1-3), 232-241 (2005)
6. Rech, P.: Chaos and hyperchaos in a Hopfield neural network. Neurocomputing. **74**(17), 3361-3364 (2011)
7. Bao, B., Chen, C., Bao, H., et al.: Dynamical effects of neuron activation gradient on Hopfield neural network: numerical analyses and hardware experiments. International Journal of Bifurcation and Chaos. **29**(4), 1930010 (2019)
8. Lin. H., Wang. C., Chen. C., et al. Neural bursting and synchronization emulated by neural networks and circuits. IEEE Trans. Circuits Syst. I-Regul. Pap. **68**(08), 3397-3410 (2021)

9. Njitacke, Z., Isaac, S., Kengne, J., et al.: Extremely rich dynamics from hyperchaotic Hopfield neural network: hysteretic dynamics, parallel bifurcation branches, coexistence of multiple stable states and its analog circuit implementation. The European Physical Journal Special Topics. **229**(6), 1133-1154 (2020)

10. Strukov, D., Snider, G., Stewart, D., et al.: The missing memristor found. Nature. **453**(7191), 80-83 (2008)

11. Wu, J., Ma, S.: Coherence resonance of the spiking regularity in a neuron under electromagnetic radiation. Nonlinear Dyn. **96**(3), 1895-1908 (2019)

12. Lin, H., Wang, C., Yao, W., et al.: Chaotic dynamics in a neural network with different types of external stimuli. Commun Nonlinear Sci Numer Simul. **90**, 105390 (2020)

13. Etémé, A., Tabi, C., Beyala, J., et al.: Chaos break and synchrony enrichment within Hindmarsh-Rose-type memristive neural models. Nonlinear Dyn. **105**(1), 785-795 (2021)

14. Zhang, S., Zheng, J., Wang, X., et al.: A novel no-equilibrium HR neuron model with hidden homogeneous extreme multistability. Chaos, Solitons and Fractals. **145**, 110761 (2021)

15. Li, Q., Tang, S., Zeng, H., et al.: On hyperchaos in a small memristive neural network. Nonlinear Dyn. **78**(2), 1087-1099 (2014)

16. Chen, C., Bao, H., Chen, M., et al.: Non-ideal memristor synapse-coupled bi-neuron Hopfield neural network: Numerical simulations and breadboard experiments. AEU-Int. J. Electron. Commun. **111**, 152894 (2019)

17. Bao, B., Yang, Q., Zhu, L., et al.: Chaotic bursting dynamics and coexisting multistable firing patterns in 3D autonomous Morris-Lecar model and microcontroller-based validations. Int. J. Bifurcation Chaos. **29**(10), 1950134 (2019)

18. Lin, H., Wang, C., Cui, Li., et al.: Brain-like initial-boosted hyperchaos and application in biomedical image encryption. IEEE Trans. Ind. Inform. DOI: 10.1109/TII.2022.3155599. (2020)

19. Leng, Y., Yu, D., Hu, Y., et al.: Dynamic behaviors of hyperbolic-type memristor-based Hopfield neural network considering synaptic crosstalk. Chaos. **30**(3), 033108 (2020)

20. Wang, Z., Parastesh, F., Rajagopal, K., et al.: Delay-induced synchronization in two coupled chaotic memristive Hopfield neural networks. Chaos, Solitons and Fractals. **134**, 109702 (2020)

21. Chen, C., Min, F., Zhang, Y., et al.: Memristive electromagnetic induction effects on Hopfield neural network. Nonlinear Dyn. **106**, 2559-2576 (2021)

22. Njitacke, Z., Tsafack, N., Ramakrishnan, B., et al.: Complex dynamics from heterogeneous coupling and electromagnetic effect on two neurons: Application in images encryption. Chaos, Solitons and Fractals. **153**, 111577 (2021)

23. Pham, V., Jafari, S., Vaidyuanathan, S., et al.: A novel memristive neural network with hidden attractors and its circuitry implementation. Science China Technological Sciences. **59**(3), 358-363 (2016)

24. Bao, B., Qian, H., Xu, Q., et al.: Coexisting behaviors of asymmetric attractors in hyperbolic-type memristor based Hopfield neural network. Front. Comput. Neurosci. **11**, 81 (2017)

25. Chen, C., Chen, J., Bao, H., et al.: Coexisting multistable patterns in memristor synapse-coupled Hopfield neural network with two neurons. Nonlinear Dyn. **95**(4), 3385-3399 (2019)

26. Lin, H., Wang, C., Hong, Q., et al.: A multi-stable memristor and its application in a neural network. IEEE Trans. Circuits Syst. II-Express Briefs. **67**(12), 3472-3476 (2020)

27. Zhang, S., Zheng, J., Wang, X., et al.: Initial offset boosting coexisting attractors in memristive multi-double-scroll Hopfield neural network. Nonlinear Dyn. **102**(4), 2821-2841 (2020)

28. Xu, X.: Complicated dynamics of a ring neural network with time delays. J. Phys. A-Math. Theor. **41**(3), 035102 (2008)

29. Khokhlova, T., Kipnis, M.: The breaking of a delayed ring neural network contributes to stability: The rule and exceptions. Neural Netw. **48**, 148-152 (2013)

30. Zhao, D., Wang, J.: Exponential stability and spectral analysis of a delayed ring neural network with a small-world connection. Nonlinear Dyn. **68**(1), 77-93 (2012)

31. Kaslik, E., Balint, S.: Complex and chaotic dynamics in a discrete-time-delayed Hopfield neural network with ring architecture. Neural Netw. **22**(10), 1411-1418 (2009)

32. Panayides, A. S., Amini, A., Filipovic, N. D., et al.: AI in medical imaging informatics: current challenges and future directions. IEEE J. Biomed. Health Inform. **24**(7), 1837-1857 (2020)

33. Ravichandran, D., Praveenkumar, P., Rayappan, J.: DNA chaos blend to secure medical privacy. IEEE Trans. Nanobiosci. **16**(8), 850-858 (2017)

34. Dzwonkowski, M., Rykaczewski, R.: Secure quaternion feistel cipher for DICOM images. IEEE Trans. Image Process. **28**(1), 371-380 (2018)

35. Ding, Y., Tan, F., Qin, Z., et al.: DeepKeyGen: a deep learning-based stream cipher generator for medical image encryption and decryption. IEEE Trans. Neural Netw. Learn. Syst. doi: 10.1109/TNNLS.2021.3062754 (2021)

36. Belazi, A., Talha, M., Kharbech, S., et al.: Novel medical image encryption scheme based on chaos and DNA encoding. IEEE Access. **7**, 36667-36681 (2019)

37. Sambas, A., Vaidyanathan, S., Tlelo-Cuautle, E., 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. **8**, 137116-137132 (2020)

38. Telem, A., Fotsin, H., Kengne, J.: Image encryption algorithm based on dynamic DNA coding operations and 3D chaotic systems. Multimedia Tools and Applications. **80**(12), 19011-19041 (2021)

39. Zhao, C., Ren, H.: Image encryption based on hyperchaotic multi-attractors. Nonlinear Dynamics. **100**(1), 679-698 (2020)

40. Cao, W., Zhou, Y., Chen, C., et al.: Medical image encryption using edge maps. Signal Processing. **132**, 96-109 (2017)

41. Amirtharajan, A.: A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach. Med. Biol. Eng. Comput. **58**(7), 1445-1458 (2020)

42. Sangavi, V., Thangavel, P.: An exotic multi-dimensional conceptualization for medical image encryption exerting Rossler system and Sine map. J. Inf. Secur. Appl. **55**, 102626 (2020)

43. Kamal, S. T., Hosny, K. M., Elgindy, T. M., et al.: A new image encryption algorithm for grey and color medical images. IEEE Access. **9**, 37855-37865 (2021)

44. Njitacke, Z. T., Isaac, S. D., Nestor, T., et al.: Window of multistability and its control in a simple 3D Hopfield neural network: application to biomedical image encryption. Neural Comput. Appl. **33**(12), 6733-6752 (2021)

45. Doubla, I. S., Njitacke, Z. T., Ekonde, S., et al.: Multistability and circuit implementation of tabu learning two-neuron model: application to secure biomedical images in IoMT. Neural Comput. Appl. **33**, 14945-14973 (2021)

46. Lin, H., Wang, C., Deng, Q., et al.: Review on chaotic dynamics of memristive neuron and neural network. Nonlinear Dyn. **106**(1), 959-973 (2021)
47. Pham, V. T., Volos, C., Jafari, S., et al.: Coexistence of hidden chaotic attractors in a novel no-equilibrium system. Nonlinear Dyn. **87**(3), 2001-2010 (2017)
48. Mannan, Z. I., Adhikari, S. P., Kim, H., et al.: Global dynamics of Chua Corsage Memristor circuit family: fixed-point loci, Hopf bifurcation, and coexisting dynamic attractors. Nonlinear Dyn. **99**(4), 3169-3196 (2020)
49. Moon, S., Baik, J. J., Hong, S. H.: Coexisting attractors in a physically extended Lorenz system. Int. J. Bifurcation Chaos. **31**(05), 2130016 (2021)
50. Veeman, D., Mehrabbeik, M., Natiq, H., et al.: A new chaotic system with coexisting attractors. Int. J. Bifurcation Chaos. **32**(03), 2230007 (2022)
51. Rajagopal, K., Karthikeyan, A., Srinivasan, A.: Dynamical analysis and FPGA implementation of a chaotic oscillator with fractional-order memristor components. Nonlinear Dyn. **91**(3), 1491-1512 (2018)
52. Kengne, Z., Jafari, S., Njitacke, Z. T., et al.: Dynamic analysis and electronic circuit implementation of a novel 3d autonomous system without linear terms. Commun Nonlinear Sci Numer Simul. **52**, 62-76 (2017)
53. Wang, N., Li, C., Bao, H., et al.: Generating multi-scroll Chua's attractors via simplified piecewise-linear Chua's diode. IEEE Trans. Circuits Syst. I-Regul. Pap. **66**(12), 4767-4779 (2019)
54. Lin, H., Wang, C., Yu, F., et al.: An extremely simple multi-wing chaotic system: dynamics analysis, encryption application and hardware implementation. IEEE Trans. Ind. Electron. **68**(12), 12708-12719 (2021)
55. Stankevich, N., Kuznetsov, A., Popova, E., et al.: Chaos and hyperchaos via secondary Neimark-Sacker bifurcation in a model of radiophysical generator. Nonlinear Dyn. **97**(4), 2355-2370 (2019)
56. Zhang, S., Li, C., Zheng, J., et al.: Generating any number of initial offset-boosted coexisting Chua's double-scroll attractors via piecewise-nonlinear memristor. IEEE Trans. Ind. Electron. **69**(07), 7202-7212 (2021)
57. Wang, Z., Bovik, A. C., Sheikh, H. R., et al. Image quality assessment: from error visibility to structural similarity. IEEE Trans. Image Process. **13**(04), 600-612 (2004)
58. Wang, F., Wang, R., Iu, H. H. C., et al. A novel multi-shape chaotic attractor and its FPGA implementation. IEEE Trans. Circuits Syst. II-Express Briefs. **66**(12), 2062-2066 (2019)