High-dimensional memristive neural network and its application in commercial data encryption communication

Chunhua Wang[a], Dong Tang[a], Hairong Lin[a,*], Fei Yu[b] and Yichuang Sun[c]

[a] *the College of Computer Science and Electronic Engineering, Hunan University, Changsha, 410082, China*
[b] *the School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha, 410114, China*
[c] *the School of Engineering and Computer Science, University of Hertfordshire, AL109AB Hatfield, U.K.*

ARTICLE INFO

Keywords:
memristive neural networks
hyperchaotic multi-scroll attractors
multi-stability
IoT application
commercial image encryption

ABSTRACT

With the development of economic globalization, demands for digital business data sharing among different subsidiary companies are constantly emerging. How to achieve secure transmission of commercial data in the Internet of Things (IoT) is a challenging task. In this paper, we propose a memristive neural network-based method for encrypted communication of commercial data. First, a high-dimensional memristive Hopfield neural network (MMHNN) model with three memristive synapses and seven neurons is proposed and its complex dynamical behaviors are deeply analyzed. The results of theoretical analysis and numerical simulations show that the proposed MMHNN can generate quasi-periodic, periodic, chaotic and hyperchaotic attractors, as well as some controllable 1-direction (1D), 2D, 3D hyperchaotic multi-scroll attractors and other types of parametric regulatory dynamics and initial value regulation dynamics. In addition, an analog equivalent circuit for the MMHNN is constructed, and the circuit simulations experimental results demonstrate the correctness and feasibility of the multi-scroll attractors phenomena. Finally, a novel MMHNN-based encryption scheme for IoT commercial data images is proposed by applying hyperchaotic spatial multi-scroll attractors, and the performance analysis shows that the proposed system achieves good encryption performances, especially in terms of keyspace, information entropy, correlation and differential attacks. The hardware experiments further verify the effectiveness and superiority of the proposed commercial data encryption scheme based on the MMHNN.

1. Introduction

As an important part of the new generation of information technology, the Internet of Things (IoT) can realize the interconnection of everything, which greatly promotes the intelligent development of industry, agriculture, transportation, medical care, office and other fields (Perez et al., 2023). However, the IoT data transmission process is highly vulnerable to cyber attacks, and if data security is not guaranteed, the deep application of IoT will be difficult to realize (Meneghello et al., 2019; Azimjonov and Kim, 2024). Due to the initial value sensitivity, randomness and unpredictability of chaotic systems, chaos-based confidential communication has become a hot research topic in the field of information security (Erkan et al., 2023; Sasikala, 2024; Ayubi et al., 2023). However, some existing chaotic systems are not complex enough and less secure. Therefore, building a complex chaotic system can further promote the development of IoT in the field of secure data transmission.

Numerous studies have shown that the human brain is a very complex nonlinear system capable of generating a variety of complex chaotic dynamical phenomena (Yang et al., 2023a; Verma et al., 2022). Researchers have constructed various types of artificial neural networks, such as Hopfield neural network (HNN), Hodgkin-Huxley (HH), Fitzhugh-Nagumo model (FHN), Spiking neural network (SNN) (Hopfield, 1984; Yang et al., 2023b; Deng et al., 2023), among which the HNN model has been widely studied because of its simple structure and rich dynamical phenomena. The memristor is considered to be an ideal component for modeling neural synapses due to its memory, non-volatile and low power consumption (Chua, 2015; Wang et al., 2017; Yang et al., 2023c). Neural networks based on memristive synapses are capable of generating rich dynamical phenomena such as transient chaos (Boya et al., 2022), chaos (Ding et al., 2023b; Wan et al., 2022), hyperchaos (Ding et al., 2023a), coexisting attractors (Boya et al., 2023; Huang et al., 2022), hidden attractors (Doubla et al., 2022a,b), and multi-scroll attractors (Yu et al., 2022, 2023; Zhang et al., 2020), which are more suitable for chaotic encryption applications than other chaotic systems.

Among them, the multi-scroll attractors allow phase trajectories to jump between different topologies, greatly increasing the complexity of traversal (Lin et al., 2023a,b). How to construct multi-scroll neural networks has received much attention in the recent years, and existing studies have mainly focused on controlling the number of scrolls by introducing multiple segmentation functions in the internal state variables of the memristor, in the memductance, in the external electromagnetic radiation or the external current stimulation (Lin et al., 2023c; Lai et al., 2023b; Zhang et al., 2021; Wan et al., 2023; Lin et al., 2023d). For example, (Zhang et al., 2020) constructed the first memristive HNN (MHNN) capable of generating multi-scroll attractors by introducing segmented sgn functions into the memristor state variables. Based on a similar approach, (Lin et al., 2023c,d) discovered the multi-structure attractors and space initial-offset be-

---

*Corresponding author
wch1227164@hnu.edu.cn (C. Wang); tdong@hnu.edu.cn (D. Tang); haironglin@hnu.edu.cn (H. Lin); yufeiyfyf@csust.edu.cn (F. Yu); y.sun@herts.ac.uk (Y. Sun)

haviors for the first time by introducing multiple memristive synapses into HNN. (Lai et al., 2023b) constructed a multi-scroll HNN with infinite coexisting attractors by introducing newly designed memristor adjustable memductance as a synapse, which can be used to highly improve the security performance of image encryption algorithm. (Zhang et al., 2021) constructed a memristive HR model capable of generating hidden multi-scroll attractors by introducing multi-segmental functions directly into the memductance functions. (Wan et al., 2023) investigated the influence of introducing multi-segmental functions into the HNN through memristors, electromagnets, and currents on multi-scroll generation. However, the segmentation functions used in these studies are overly conditional and require different segmentation functions depending on the number of scroll parity, which may complicate the operation to a certain extent. The above literature focuses on the generation of multi-scroll using different methods and models, there are no studies on the effect of memristor on scroll generation when it performs different types of functions, and only few reports on memristive neural networks with multiple complex dynamics. Thus, we study the influence of the types of memristive synapses on HNN and construct a multi-memristive HNN capable of generating multiple complex dynamics.

Chaotic systems are widely used in the field of image encryption, and most of the existing chaotic systems are simulated and tested by MATLAB, or physically implemented using discrete components, DSPs, FPGAs, etc. (Zhang et al., 2023; Hu and Wang, 2023; Biban et al., 2023; Kong et al., 2024). For example, (Ma et al., 2023) proposed a fast encryption algorithm based on hyperchaotic systems and tested it in MATLAB. (Wang et al., 2019) constructed a multi-scroll Chua hardware circuit using discrete components and implemented image encryption applications based on it. (Li et al., 2021) implemented a fractional-order chaotic system using DSP and applied it to image encryption. (Mohamed et al., 2023) implemented image encryption based on a memristive chaos system using FPGA. However, there are few studies based on practical application scenarios of IoT, while some of the encryption algorithms also have problems such as low security and vulnerability to attacks (Lai and Liu, 2023; Ye et al., 2022; Wei et al., 2023; Lai et al., 2023a). Thus applying chaotic neural network encryption to practical IoT applications is of great significance to promote encryption technology from theory to application.

Based on the above, to generate HNN with multiple complex dynamics, a new multi-segmental function-based memristor is constructed in this paper, and three types of multi-memristor Hopfield neural networks (MMHNN) are modeled by introducing multiple of the above memristors as different types of synapses into a 7-HNN coupled by two asymmetric sub-networks. Through theoretical analysis and numerical simulations, we reveal that the proposed MMHNN has a variety of complex dynamical behaviors including the controlled number of hyperchaotic multi-scroll attractors and coexisting attractors in 1 direction (1D), 2D and 3D. In addition, an MMHNN realization circuit is constructed using discrete components, and the feasibility of the design is further verified by simulation experiments in Multisim. Finally, the chaotic sequences generated by the proposed MMHNN are applied as keys in an IoT commercial image encryption system based on the message queuing telemetry transport (MQTT) protocol, and the related encryption performances are tested.

The main innovations of this paper are as follows:

1) A new memristor model is proposed, a 7-HNN consisting of two asymmetric sub-neural networks is constructed, and the effects of different types and numbers of memristive synapses on the MMHNN are considered.
2) Rich dynamical phenomena are observed in the MMHNN, among which the hyperchaotic 2D and 3D grid multi-scroll attractors, coexisting multi-state non-chaotic attractors, coexisting hyperchaotic 1D and 2D grid multi-scroll attractors are reported for the first time in HNN.
3) An MMHNN simulation circuit is designed. By adjusting the corresponding switches in the memristor, an arbitrary number of multi-scroll hyperchaotic attractors can be obtained.
4) Based on the MMHNN model, an IoT commercial data security sharing solution is provided, and the corresponding encryption performance is tested.

The remaining of the paper is organized as follows. In Section 2, a new memristor model and three different types of memristive HNN are established. Section 3 analyses the multi-directional multi-scroll attractors and multi-type extreme multi-stability of the MMHNN. Section 4 presents the simulation results of the proposed MMHNN model circuit. Section 5 proposes an IoT commercial image encryption system using the MMHNN. Section 6 concludes the paper.

2. Design of Hopfield neural network model

By introducing a segmentation function into the memristor, this section designs a new memristor model and introduces the above memristors model as different types of synapses into the HNN to examine its effect on multi-scroll generation.

2.1. Memristor Model

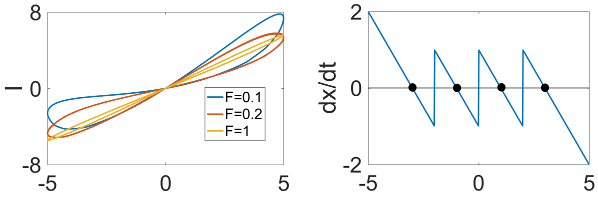
In this study, based on the definition of a generic memristor (Chua, 2015), we design a new model of a non-ideal magnetron memristor whose relations can be described as follows:

$$\begin{cases} i = W(\varphi)v = (a + b\varphi)v \\ \dot{\varphi} = g(\varphi, v) = cv - dg(\varphi) \end{cases} \tag{1}$$

$$g(\varphi) = \varphi - h[M - N + \mathrm{sgn}(\varphi) + \sum_{i=1}^{M} \mathrm{sgn}(\varphi - 2hi) + \sum_{j=1}^{N} \mathrm{sgn}(\varphi + 2hj)] \tag{2}$$

where $W(\varphi)$ is the memductance value, $g(\varphi, v)$ is the internal state function of the memristor. a, b, c and d are the four positive parameters controlling the memristor. v, i and φ are the voltage, current and internal flux state variables in the memristor, respectively. M and N in $g(\varphi)$ are used to control the number of scrolls ($M, N \geq 0$), and a total of $M + N + 2$-scroll attractors can be generated. h is used to control the width of the attractor ($h > 0$), here $h = 1$ is fixed.

To verify the fingerprints of the proposed mathematical model of the memristor, the parameters are set to $a = 1$, $b = 0.1$, $c = 1.2$, $d = 1$, $M = N = 1$, and the input voltage is set to $v = Asin(2\pi Ft)$, where A and F are amplitude and frequency, respectively, setting $A = 5$, $F = 0.1, 0.2, 1$, $\varphi_0 = 0.1$. Fig. 1(a) depicts the numerical simulation results of the $V - I$ relationship curves at three frequencies, from which it can be seen that the model has a slant eight-pinched hysteresis loop, and the area of the hysteresis loop gradually decreases with the increase of the excitation frequency. When the frequency increases to infinity, the pinched hysteresis loop tends to be a single-valued function. Therefore, the designed model meets the three fingerprints of the memristor. Fig. 1(b) depicts the numerical simulation results of the POP curve, and it can be seen that there are four intersection points (more than two) with a negative slope of the curve and X-axis, so the memristor model is non-volatile. In summary, the memristor model proposed in this paper is a non-volatile memristor.



(a) (b)

Fig. 1: Characteristics of the memristor when $M = N = 1$. (a) the hysteresis loops with different frequencies; (b) POP curve.

2.2. MMHNN model

As a simplified neural network model, HNN has the properties of simple structure and rich chaotic dynamics. According to the HNN defined by the circuit equations (Lin et al., 2023c), the ith neuron in an HNN consisting of n neurons can be described as follows:

$$C_i \dot{x}_i = -\frac{x_i}{R_i} + \sum_{j=1}^{n} w_{ij} \tanh\left(x_j\right) + I_i, \left(i, j \in N^*\right) \quad (3)$$

where C_i, x_i and R_i represent the membrane capacitance, membrane voltage and membrane resistance inside and outside the cell membrane of neuron i, respectively. W_{ij} is the synaptic weight coefficient between neuron i and neuron j, $tanh(x_j)$ and I_i represent the neuronal activation function and external current, respectively. Setting $C_i = 1$, $R_i = 1$, and $I_i = 0$. By the trial-and-error method, a 7-HNN model coupled with a 4-HNN and a 3-HNN is constructed in this paper. By introducing different numbers of memristors as different types of synapses to different locations in the MMHNN, very rich and complex dynamics can be generated.

Case-I: The membrane potential difference between neuron 1 and neuron 5 in the two-coupled sub-neural network is modeled by memristive synaptic weight $\mu_1 W_1(\varphi_1) = \mu_1(a_1 + b_1\varphi_1)$. The MMHNN can be described as:

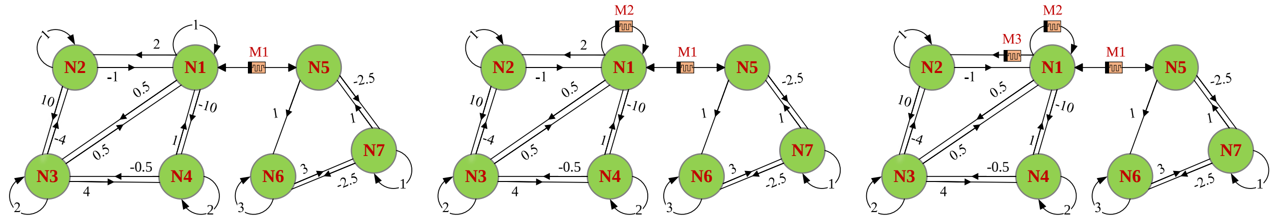
$$\begin{cases} \dot{x}_1 = -x_1 + \tanh(x_1) + 2\tanh(x_2) + 0.5\tanh(x_3) \\ \qquad - 10\tanh(x_4) - \mu_1 W_1(\varphi_1)(x_1 - x_5) \\ \dot{x}_2 = -x_2 - \tanh(x_1) + \tanh(x_2) + 10\tanh(x_3) \\ \dot{x}_3 = -x_3 + 0.5\tanh(x_1) - 4\tanh(x_2) + 2\tanh(x_3) + 4\tanh(x_4) \\ \dot{x}_4 = -x_4 + \tanh(x_1) - 0.5\tanh(x_3) + 2\tanh(x_4) \\ \dot{x}_5 = -x_5 + \tanh(x_6) - 2.5\tanh(x_7) + \mu W_1(\varphi_1)(x_1 - x_5) \\ \dot{x}_6 = -x_6 + 3\tanh(x_6) + 3\tanh(x_7) \\ \dot{x}_7 = -x_7 + \tanh(x_5) - 2.5\tanh(x_6) + \tanh(x_7) \\ \dot{\varphi}_1 = c_1(x_1 - x_5) - d_1 g(\varphi_1) \end{cases} \tag{4}$$

Case-II: On the basis of Case-I, the self-synaptic weight of neuron 1 is replaced by the memristive synaptic weight $\mu_2 W_2(\varphi_2) = \mu_2(a_2 + b_2\varphi_2)$. The MMHNN can be described as:

$$\begin{cases} \dot{x}_1 = -x_1 + \mu_2 W_2(\varphi_2)\tanh(x_1) + 2\tanh(x_2) + 0.5\tanh(x_3) \\ \qquad - 10\tanh(x_4) - \mu_1 W_1(\varphi_1)(x_1 - x_5) \\ \dot{x}_2 = -x_2 - \tanh(x_1) + \tanh(x_2) + 10\tanh(x_3) \\ \dot{x}_3 = -x_3 + 0.5\tanh(x_1) - 4\tanh(x_2) + 2\tanh(x_3) + 4\tanh(x_4) \\ \dot{x}_4 = -x_4 + \tanh(x_1) - 0.5\tanh(x_3) + 2\tanh(x_4) \\ \dot{x}_5 = -x_5 + \tanh(x_6) - 2.5\tanh(x_7) + \mu W_1(\varphi_1)(x_1 - x_5) \\ \dot{x}_6 = -x_6 + 3\tanh(x_6) + 3\tanh(x_7) \\ \dot{x}_7 = -x_7 + \tanh(x_5) - 2.5\tanh(x_6) + \tanh(x_7) \\ \dot{\varphi}_1 = c_1(x_1 - x_5) - d_1 g(\varphi_1) \\ \dot{\varphi}_2 = c_2\tanh(x_1) - d_2 g(\varphi_2) \end{cases} \tag{5}$$

Case-III: On the basis of Case-II, continue to replace the mutual synaptic weight between neuron 1 and neuron 2 with memristive synaptic weight $\mu_3 W_3(\varphi_3) = \mu_3(a_3 + b_3\varphi_3)$. The MMHNN can be described as:

$$\begin{cases} \dot{x}_1 = -x_1 + \mu_2 W_2(\varphi_2)\tanh(x_1) + \mu_3 W_3(\varphi_3)\tanh(x_2) \\ \qquad + 0.5\tanh(x_3) - 10\tanh(x_4) - \mu_1 W_1(\varphi_1)(x_1 - x_5) \\ \dot{x}_2 = -x_2 - \tanh(x_1) + \tanh(x_2) + 10\tanh(x_3) \\ \dot{x}_3 = -x_3 + 0.5\tanh(x_1) - 4\tanh(x_2) + 2\tanh(x_3) + 4\tanh(x_4) \\ \dot{x}_4 = -x_4 + \tanh(x_1) - 0.5\tanh(x_3) + 2\tanh(x_4) \\ \dot{x}_5 = -x_5 + \tanh(x_6) - 2.5\tanh(x_7) + \mu W_1(\varphi_1)(x_1 - x_5) \\ \dot{x}_6 = -x_6 + 3\tanh(x_6) + 3\tanh(x_7) \\ \dot{x}_7 = -x_7 + \tanh(x_5) - 2.5\tanh(x_6) + \tanh(x_7) \\ \dot{\varphi}_1 = c_1(x_1 - x_5) - d_1 g(\varphi_1) \\ \dot{\varphi}_2 = c_2\tanh(x_1) - d_2 g(\varphi_2) \\ \dot{\varphi}_3 = c_3\tanh(x_2) - d_2 g(\varphi_3) \end{cases}$$



(a) (b) (c)

Fig. 2: Topological connection of the MMHNN. (a) Case-I; (b) Case-II; (c) Case-III.

(6)

where μ_1, μ_2 and μ_3 are the memristor coupling strengths. The MMHNN topology in Case-III is shown in Fig. 2.

3. Dynamical analysis and numerical simulations

In this section, numerical simulations are completed using the ODE45 algorithm on the MATLAB R2016b platform to reveal the complex dynamics including multi-directional multi-scroll hyperchaotic attractors and multi-stability of the proposed MMHNN through equilibrium point analysis, phase orbits, bifurcation diagrams, Lyapunov exponents, basins of attraction and time series. The start time, time step and time length are 0, 0.01 and 4000, respectively.

3.1. Equilibrium point analysis

Here, Case-II is taken as an example to analyze the equilibrium and stability of the MMHNN system. By setting the right side of MMHNN equation (5) to zero, the equilibrium equation of MMHNN can be obtained as follows:

$$\begin{cases} -x_1 + \mu_2 W_2(\varphi_2)\tanh(x_1) + 2\tanh(x_2) + 0.5\tanh(x_3) \\ \quad - 10\tanh(x_4) - \mu_1 W_1(\varphi_1)(x_1 - x_5) = 0 \\ -x_2 - \tanh(x_1) + \tanh(x_2) + 10\tanh(x_3) = 0 \\ -x_3 + 0.5\tanh(x_1) - 4\tanh(x_2) + 2\tanh(x_3) + 4\tanh(x_4) = 0 \\ -x_4 + \tanh(x_1) - 0.5\tanh(x_3) + 2\tanh(x_4) = 0 \\ -x_5 + \tanh(x_6) - 2.5\tanh(x_7) + \mu W_1(\varphi_1)(x_1 - x_5) = 0 \\ -x_6 + 3\tanh(x_6) + 3\tanh(x_7) = 0 \\ -x_7 + \tanh(x_5) - 2.5\tanh(x_6) + \tanh(x_7) = 0 \\ \quad c_1(x_1 - x_5) - d_1 g(\varphi_1) = 0 \\ \quad c_2\tanh(x_1) - d_2 g(\varphi_2) = 0 \end{cases} \tag{7}$$

The above equations are complex and difficult to solve by conventional methods, so here they are solved by MATLAB. Taking $g(\varphi_i)$ with $M_1 = N_1 = M_2 = N_2 = 0$ as an example, fixing the other parameters as $a_1 = a_2 = 1$, $b_1 = b_2 = 0.05$, $c_1 = 4$, $c_2 = 1.4$, $d_1 = 2$ and $d_2 = 1$, $\mu_1 = 5$, $\mu_2 = 1$. Through software calculation, we can get the set of equilibrium points $E_q = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, \varphi_1, \varphi_2) = (0, 0, 0, 0, 0, 0, 0, \varphi_1{}^*, \varphi_2{}^*)$, where $\varphi_1{}^*$, $\varphi_2{}^*$ are the solutions of $g(\varphi_i) = 0$. Under the above parameter conditions, the system has nine equilibrium points, and the equilibrium points correspond to the eigenvalues and stability shown in Table 1. It can be seen that the equilibrium points generated by the system are all unstable saddle points (USF), and according to Shil'nikov's theorem, it is known that the MMHNN is capable of generating self-excited chaos. Further study yields that the number of equilibrium points is determined by the internal state variable function $g(\varphi_i) = 0$, and a total of $(2M_1 + 2N_1 + 3) * (2M_2 + 2N_2 + 3)$ equilibrium points can be generated. When M_i and N_i tend to infinity, the system has infinitely many equilibrium points, at which point the system generates attractors as hidden attractors.

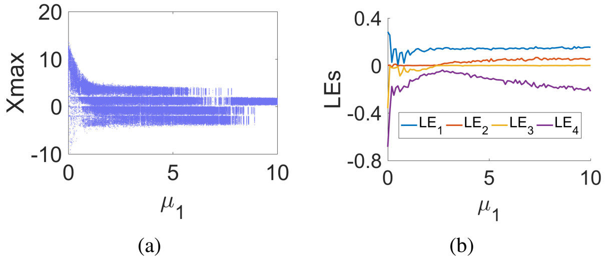
3.2. Multi-directional hyperchaotic multi-scroll attractors

In Case-I, the parameters are fixed as $\mu_1 = 5$, $a_1 = 1$, $b_1 = 0.05$, $c_1 = 4$, $d_1 = 2$, the initial state is (0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1), and $M_1 = N_1 = 1$ is chosen. The corresponding first four Lyapunov exponents and bifurcation diagrams of the MMHNN are plotted for different values of the memristive coupling strength μ_1, respectively. From Fig. 3(a), it can be seen that the bifurcation diagram has four segments of bars consisting of dense points in the appropriate interval and the number of bars corresponds to the position and attractor. From Fig. 3(b), it can be seen that there are two positive Lyapunov exponents in all the regions [2, 10], so this MMHNN is hyperchaotic. Fig. 4 plots the different numbers of hyperchaotic multi-scroll attractors produced by the system for different values of M_1 and N_1. Further analysis leads to the conclusion that simulating membrane potential differences with memristive synapses enable MMHNN to generate arbitrary m-scroll hyperchaotic attractors ($m = M_1 + N_1 + 2$) by controlling M_1 and N_1 in the memristive synaptic equation of state without changing the original properties of the neural network.

In Case-II, keeping the other parameters in Case-I unchanged, the parameters of the memristor Mem2 are set to $\mu_2 = 1$, $a_2 = 1$, $b_2 = 0.05$, $c_2 = 1.4$, $d_2 = 1$ and $M_2 = N_2 = 1$, the initial state is (0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1). The corresponding first four Lyapunov exponents and bifurcation diagrams of the MMHNN for different values of the memristive coupling strength μ_2 are plotted in Fig. 5, and we can see that by varying the values of μ_2, the system can exhibit a variety of complex dynamics such as quasi-

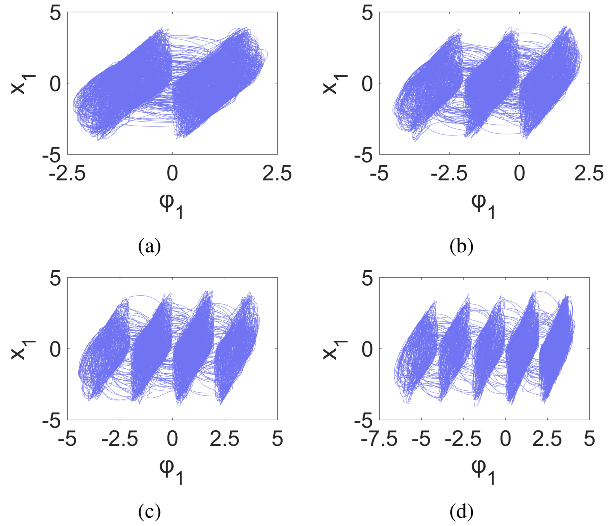
Table 1
Equilibrium points and corresponding eigenvalues and stabilities

Equilibrium points	Eigenvalues	Stabilities
E1 (0, 0, 0, 0, 0, 0, 0, -1, -1)	-9.408, -2, -1, 0.2672 ± 6.668i, 0.5762 ± 2.773i, 0.5856 ± 1.729i	USF
E2 (0, 0, 0, 0, 0, 0, 0, -1, 0)	99, -9.387, -2, 0.2678 ± 6.67i, 0.5802 ± 2.777i, 0.5952 ± 1.73i	USF
E3 (0, 0, 0, 0, 0, 0, 0, -1, 1)	-9.365, -2, -1, 0.2685 ± 6.672i, 0.5843 ± 2.781i, 0.6047 ± 1.731i	USF
E4 (0, 0, 0, 0, 0, 0, 0, 0, -1)	198, -9.932, -1, 0.271 ± 6.664i, 0.5763 ±2.773i, 0.5937 ± 1.725i	USF
E5 (0, 0, 0, 0, 0, 0, 0, 0, 0)	198, 99, -9.91, 2716 ± 6.666i, 0.5802 ± 2.777i, 0.6032 ± 1.725i	USF
E6 (0, 0, 0, 0, 0, 0, 0, 0, 1)	198, -9.889, -1, 0.2723 ± 6.668i, 0.5843 ± 2.782i, 0.6127 ±1.726i	USF
E7 (0, 0, 0, 0, 0, 0, 0, 1, -1)	-10.45, -2, -1, 0.2747 ± 6.661i, 0.5763 ± 2.773i, 0.6011 ± 1.721i	USF
E8 (0, 0, 0, 0, 0, 0, 0, 1, 0)	99, -10.43, -2, 0.2753 ± 6.663i, 0.5803 ± 2.778i, 0.6106 ± 1.722i	USF
E9 (0, 0, 0, 0, 0, 0, 0, 1, 1)	-10.41, -2, -1, 0.2759 ± 6.665i, 0.5843 ± 2.782i, 0.62 ± 1.722i	USF



(a) (b)

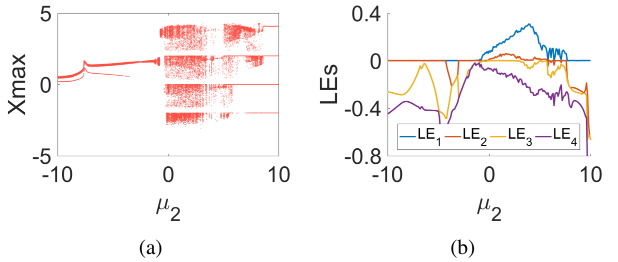
Fig. 3: Dynamics of the MMHNN under the influence of the value μ_1. (a) bifurcation diagrams; (b) Lyapunov exponents.



(a) (b) (c) (d)

Fig. 4: Multi-scroll hyperchaotic attractors of the MMHNN with different values of M_1 and N_1. (a) 2-scroll when $M_1 = N_1 = 0$; (b) 3-scroll when $M_1 = 1$, $N_1 = 0$; (c) 4-scroll when $M_1 = N_1 = 1$; (d) 5-scroll when $M_1 = 1$, $N_1 = 2$.

periodic in the regions [-10, -4.3] and [-3, -1.4], periodic in the regions [-4.3, -3] and [7.8, 10], chaotic in the regions [-1.4, -0.1], [3.5, 4.3] and [5.8, 7.8], and hyperchaotic in the regions [-0.1, 3.5] and [4.3, 5.8]. Further, by using memristive synapses instead of arbitrary self-synapses in the neural network, and then by changing M_i and N_i in both memristor equations of state, the system can generate an arbitrary number of $m * n$ grid hyperchaotic attractors in the two-dimensional direction (where $n = M_2 + N_2 + 2$). The results for partial grid multi-scroll hyperchaotic attractors are shown in Fig. 6.



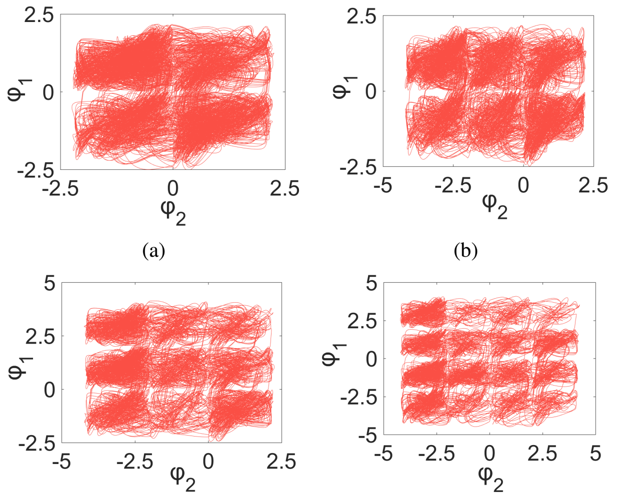
(a) (b)

Fig. 5: Dynamics of the MMHNN under the influence of the value μ_2. (a) bifurcation diagrams; (b) Lyapunov exponents.

Similarly, in Case-III, keeping the other parameters in Case-II unchanged, the parameters of the memristor Mem3 are fixed as $\mu_3 = 2$, $a_3 = 1$, $b_3 = 0.05$, $c_3 = 1.4$, $d_3 = 1$ and $M_3 = N_3 = 1$, the initial state is (0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1). Fig. 7 depicts the first four Lyapunov exponents and bifurcation diagrams corresponding to the MMHNN for different values of the memristive coupling strength μ_3. Fig. 8 plots the different numbers of multi-scroll attractors generated by the system in different dimensions for the memristive synapses with the case of $M_1 = 0$, $N_1 = 0$, $M_2 = 0$, $N_2 = 1$, $M_3 = 1$, and $N_3 = 1$. By analogy, using memristive synapses to replace any mutual synapses in the neural network, and then modifying M_i and N_i in the three memristor equations of state, the system can generate an arbitrary number of $m * n * l$ hyperchaotic spatial multi-scroll attractors in the three-dimensional direction (where $l = M_3 + N_3 + 2$).

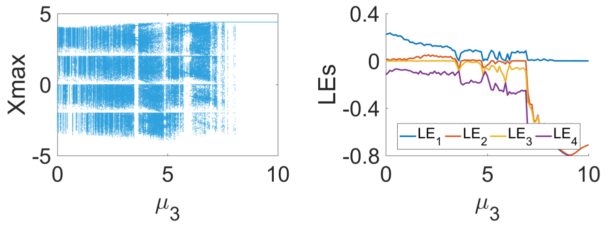
3.3. Multitype coexisting attractors

By changing the initial value of the system, the system may have coexisting attractors with different locations or different topologies, and when the number of these coexisting attractors tends to infinity, the system has extreme multistability (Doubla et al., 2022a). This subsection reveals that



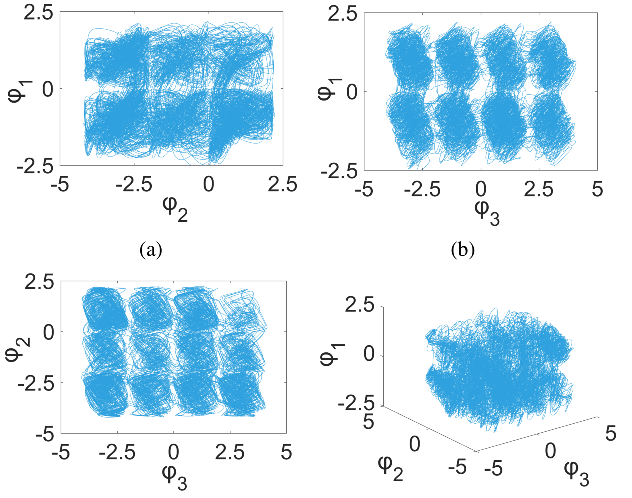
(a) (b) (c) (d)

Fig. 6: Multi-scroll grid hyperchaotic attractors of the MMHNN with different values of M_i and N_i. (a) 2*2 scroll when $M_1 = N_1 = 0$, $M_2 = N_2 = 0$; (b) 2*3 scroll when $M_1 = N_1 = 0$, $M_2 = 0$, $N_2 = 1$; (c) 3*3 scroll when $M_1 = 1$, $N_1 = 0$, $M_2 = 0$, $N_2 = 1$; (d) 4*4 scroll when $M_1 = N_1 = 1$, $M_2 = N_2 = 1$.



(a) (b)

Fig. 7: Dynamics of the MMHNN under the influence of the value μ_3. (a) bifurcation diagrams; (b) Lyapunov exponents.

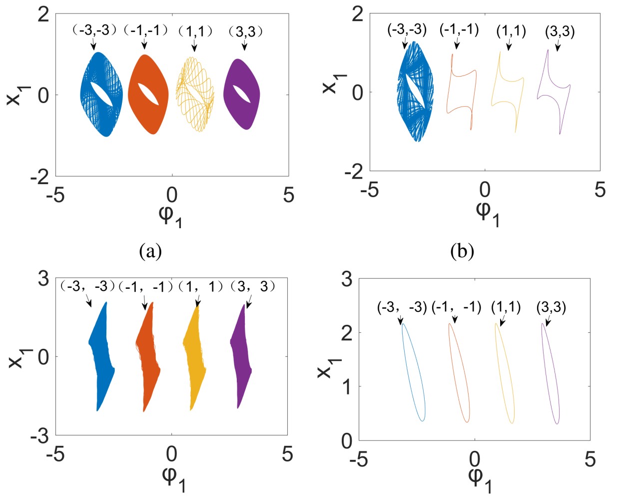


(a) (b) (c) (d)

Fig. 8: Multi-scroll spatial hyperchaotic attractors of the MMHNN with different values of M_i and N_i. (a) 2*3 scroll; (b) 2*4 scroll; (c) 3*4 scroll; (d) 2*3*4 scroll.

the MMHNN model proposed in this paper has extreme multistability that depends on the initial value regulation.

According to the analysis in Section III.B, it can be seen from the first four Lyapunov exponents that the MMHNN has multiple dynamical phenomena such as periodic, quasi-periodic, chaotic, and hyperchaotic by modifying the synaptic weight values. In order to explore whether the above phenomena have coexisting behaviors, take Case-III as an example, with other parameters unchanged, now set $\mu_2 = -5$, -3.5, -1 and -0.5, as well as $\mu_3 = 8.5$ in turn, the initial state is $(0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, \varphi_{10}, \varphi_{20}, 0.1)$, $M_i = N_i = 1$ $(i = 1, 2, 3)$, and the phase orbits generated by the initial values φ_{10} and φ_{20} at $\pm1, \pm3$ are explored. According to Fig. 9, it can be seen that the system has various coexisting dynamics such as coexisting quasi-periodic attractors, coexisting multi-type non-chaotic attractors, coexisting chaotic attractors, and coexisting periodic attractors. In particular, when $\mu_2 = -3.5$, each of the generated attractors has a different shape and can vary between quasi-periodic and periodic, but always remains non-chaotic.



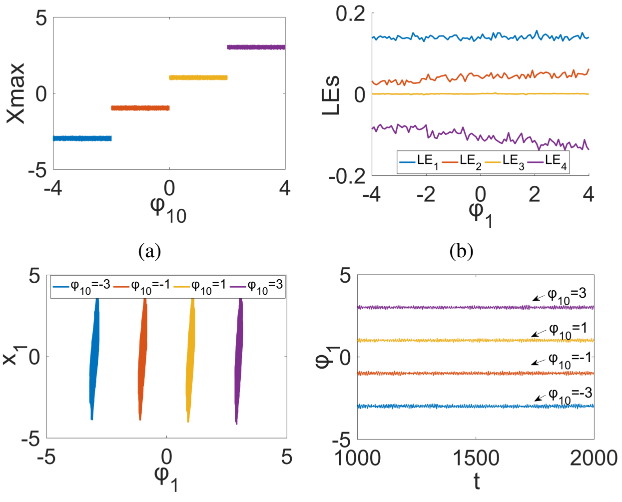
(a) (b) (c) (d)

Fig. 9: Multitype coexisting attractors under the influence of initial value φ_{10} and φ_{20}. (a) coexisting quasi-periodic attractors when $\mu_2 = -5$; (b) coexisting multi-type non-chaotic attractors when $\mu_2 = -3.5$; (c) coexisting chaotic attractors when $\mu_2 = -1$; (d) coexisting periodic attractors when $\mu_3 = -8.5$.

3.4. Coexisting hyperchaotic multi-scroll attractors

In Case-I, change $c_1 = 0.5$, $M_1 = N_1 = 1$, other parameters remain unchanged, the initial state is $(0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, \varphi_{10})$. The bifurcation diagram and the corresponding first four Lyapunov exponents obtained when the value φ_{10} is varied in the region of [-4, 4], and the phase orbit and the timing diagrams generated for the cases $\varphi_{10} = \pm1$,

±3 are shown in Fig. 10. It can be seen that the change of the initial value only affects the position of the attractor without changing the chaotic state, and further study reveals that by modifying the initial value φ_{10} of the state variable of the memristor Mem1, the system can generate up to m coexisting hyperchaotic attractors.

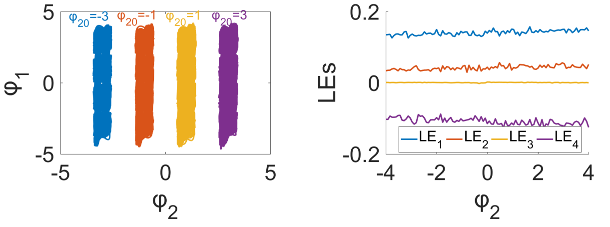


(a) (b)

(c) (d)

Fig. 10: Dynamics of MMHNN under the influence of the value φ_{10}. (a) bifurcation diagrams; (b) Lyapunov exponents; (c) phase orbits; (d) time series.

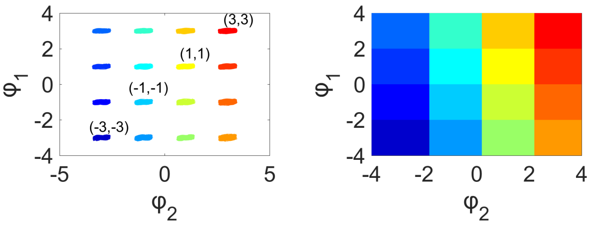
In Case-II, change $c_2 = 0.5$, $M_1 = N_1 = M_2 = N_2 = 1$, other parameters are unchanged, and the initial state is (0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, φ_{20}). Fig. 11(a) shows the phase orbit of four 4-scroll coexisting attractors generated in the $\varphi_2 - \varphi_1$ plane for $\varphi_{20} = \pm 1, \pm 3$. Fig. 11(b) shows the corresponding first four Lyapunov exponents when φ_{20} varies in the region of [-4, 4]. Further analysis yields that by modifying the initial value φ_{20} of the state variable of the memristor Mem2, the system can generate up to n coexisting m-scroll hyperchaotic attractors.



(a) (b)

Fig. 11: Dynamics of the MMHNN under the influence of the value φ_{20}. (a) phase orbits; (b) Lyapunov exponents.

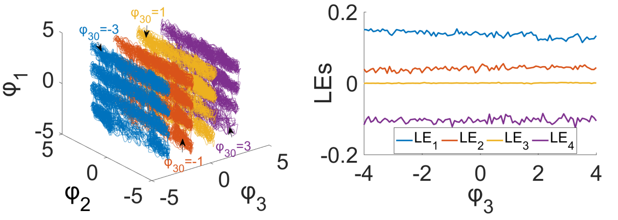
In the above case, we further change $c_1 = 0.5$ with the initial state of (0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, φ_{10}, φ_{20}). Fig. 12(a) shows the phase orbit of 16 coexisting hyperchaotic attractors generated in the φ_2-φ_1 plane for the cases φ_{10}, $\varphi_{20} = \pm 1, \pm 3$. Fig. 12(b) shows the local attraction basins of the system when φ_{10} and φ_{20} vary in the region of [-4, 4], with one color of the attraction basins corresponding to one attractor. Further study leads to the conclusion that the system can generate a number of $m * n$ coexisting hyperchaotic attractors by modifying the initial values φ_{10} and φ_{20} of the state variables of the memristors Mem1 and Mem2.



(a) (b)

Fig. 12: Dynamics of the MMHNN under the influence of the values φ_{10} and φ_{20}. (a) phase orbits; (b) local attraction basins.

In Case-III, now let c_3=0.5, $M_1 = N_1 = M_2 = N_2 = M_3 = N_3 = 1$, other parameters are unchanged, and the initial state is (0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, φ_{30}). Fig. 13(a) shows the phase orbit of the four 4*4 grid multi-scroll coexisting attractors generated in the $\varphi_3 - \varphi_2 - \varphi_1$ space for the $\varphi_{30} = \pm 1, \pm 3$ case. Fig. 13(b) shows the corresponding first four Lyapunov exponents when φ_{30} is varied in the region of [-4, 4]. By analogy, by modifying the initial value φ_{30} of the state variable of the memristor Mem3, the system can generate l number of $m * n$ grid coexisting multi-scroll hyperchaotic attractors.



(a) (b)

Fig. 13: Dynamics of the MMHNN under the influence of the value φ_{30}. (a) phase orbits; (b) Lyapunov exponents.

4. Circuit implementation of MMHNN

The physical implementation of the neural network model is essential to determine its dynamic behavior and to develop neuromorphic hardware systems. In this section, an analog MMHNN model circuit is constructed using the modular design approach and verified by simulation tests.

4.1. Realization of the memristor circuit

The memristor circuit is shown in Fig. 14, where E, E_0, E_1, $-E_1$, …, E_n, $-E_n$ are the bias voltages and have $E =$

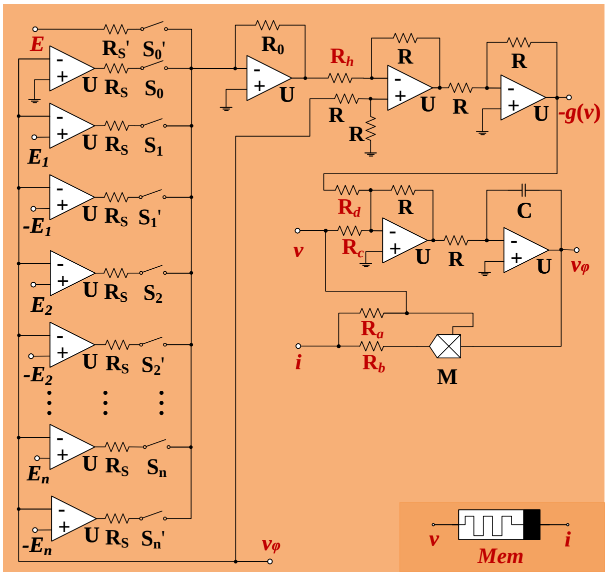


Fig. 14: Equivalent circuit of the memristor.

Table 2
Number of the scrolls determined by the memristor

S_0	S_1	S_1'	S_2	S_2'	...	S_n	S_n'	S_0'	M and N	Scrolls
off	on	on	on	on	...	on	on	on	M=0, N=0	2
off	off	on	on	on	...	on	on	off	M=0, N=1	3
off	on	off	on	on	...	on	on	off	M=1, N=0	3
off	off	off	on	on	...	on	on	on	M=1, N=1	4
off	off	on	off	on	...	on	on	off	M=0, N=2	4
off	on	off	on	off	...	on	on	off	M=2, N=0	4
...	...	...	...	...	...	...	...	...	...	...
off	off	off	off	off	...	off	off	on	M=m, N=n	m+n+2

$(N-M)$ V, $E_i = 2hi$ V. S_0', S_0, S_1, S_1', …, S_n and S_n' are the selection switches. By controlling different switch combinations, various types of memristors can be realized as shown in Table 2. The circuit equation can be described as:

$$\begin{cases} i = (1/R_a + v_\varphi/R_b)v \\ C\dot{v}_\varphi = v/R_c - g(v_\varphi)/R_d \end{cases} \tag{8}$$

where g is the gain of analog multiplier and $g = 0.1$, $R_s = 13.5$ kΩ, $R_s' = 1$ kΩ, $R_0 = 1$ kΩ, $R = 10$ kΩ, $C = 10$ nF, $R_a = R/a$, $R_b = gR/b$, $R_c = R/c$, $R_d = R/d$.

4.2. Realization of the MMHNN circuit

The proposed model of MMHNN consists of the tanh circuit (Lai et al., 2023b), the memristor circuit, and the HNN circuit with a total of three circuit modules, as shown in Fig. 15. Among them, the hollow circle represents the inverter, and the output capacitor voltages v_1, v_2, v_3, v_4, v_5, v_6 and v_7 are used to simulate the membrane potential of the neuron. Resistors R_1-R_{19} are used to simulate the synaptic weight coefficients between neurons. The memristive synaptic weight coefficients are implemented by the memristor Mem$i$. Taking Case-III as an example, its circuit equation can be described according to Kirchhoff's law as follows:

$$\begin{cases} RC\dot{v}_1 = -v_1 + (\frac{R}{R_{a2}} + \frac{Rv_{\varphi2}}{R_{b2}})\tanh(v_1) + (\frac{R}{R_{a3}} + \frac{Rv_{\varphi3}}{R_{b3}})\tanh(v_2) \\ \qquad + \frac{R}{R_1}\tanh(v_3) - \frac{R}{R_2}\tanh(v_4) - (\frac{R}{R_{a1}} + \frac{Rv_{\varphi1}}{R_{b1}})(v_1 - v_5) \\ RC\dot{v}_2 = -v_2 - \frac{R}{R_3}\tanh(v_1) + \frac{R}{R_4}\tanh(v_2) + \frac{R}{R_5}\tanh(v_3) \\ RC\dot{v}_3 = -v_3 + \frac{R}{R_6}\tanh(v_1) - \frac{R}{R_7}\tanh(v_2) + \frac{R}{R_8}\tanh(v_3) \\ \qquad + \frac{R}{R_9}\tanh(v_4) \\ RC\dot{v}_4 = -v_4 + \frac{R}{R_{10}}\tanh(v_1) - \frac{R}{R_{11}}\tanh(v_3) + \frac{R}{R_{12}}\tanh(v_4) \\ RC\dot{v}_5 = -v_5 + \frac{R}{R_{13}}\tanh(v_6) - \frac{R}{R_{14}}\tanh(v_7) + (\frac{R}{R_{a1}} + \frac{Rv_{\varphi1}}{R_{b1}})(v_1 - v_5) \\ RC\dot{v}_6 = -v_6 + \frac{R}{R_{15}}\tanh(v_6) + \frac{R}{R_{16}}\tanh(v_7) \\ RC\dot{v}_7 = -v_7 + \frac{R}{R_{17}}\tanh(v_5) - \frac{R}{R_{18}}\tanh(v_6) + \frac{R}{R_{19}}\tanh(v_7) \\ RC\dot{v}_{\varphi1} = \frac{R}{R_{c1}}(v_1 - v_5) - \frac{R}{R_{d1}}g(v_{\varphi1}) \\ RC\dot{v}_{\varphi2} = \frac{R}{R_{c2}}\tanh(v_1) - \frac{R}{R_{d2}}g(v_{\varphi2}) \\ RC\dot{v}_{\varphi3} = \frac{R}{R_{c3}}\tanh(v_2) - \frac{R}{R_{d3}}g(v_{\varphi3}) \end{cases} \tag{9}$$

In our simulation we use $C = 10$ nF, $R = 10$ kΩ, $R_1 = 20$ kΩ, $R_2 = 1$ kΩ, $R_3 = 10$ kΩ, $R_4 = 10$ kΩ, $R_5 = 1$ kΩ, $R_6 = 20$ kΩ, $R_7 = 2.5$ kΩ, $R_8 = 5$ kΩ $R_9 = 2.5$ kΩ, $R_{10} = 10$ kΩ, $R_{11} = 20$ kΩ, $R_{12} = 5$ kΩ, $R_{13} = 10$ kΩ, $R_{14} = 4$ kΩ, $R_{15} = 3.33$ kΩ, $R_{16} = 3.33$ kΩ, $R_{17} = 10$ kΩ, $R_{18} = 4$ kΩ, $R_{19} = 10$ kΩ. In addition, $R_{ai} = R/\mu_i a_i$, $R_{bi} = gR/\mu_i b_i$, $R_{ci} = R/c_i$, $R_{di} = R/d_i$, $R_{a1} = 2$ kΩ, $R_{b1} = 4$ kΩ, $R_{c1} = 2.5$ kΩ, $R_{d1} = 5$ kΩ, $R_{a2} = 10$ kΩ, $R_{b2} = 20$ kΩ, $R_{c2} = 7.14$ kΩ, $R_{d2} = 10$ kΩ, $R_{a3} = 5$ kΩ, $R_{b3} = 10$ kΩ, $R_{c3} = 7.14$ kΩ, $R_{d3} = 10$ kΩ.

The MMHNN circuit proposed in this paper was implemented in the Multisim 14.0 platform using electronic components such as M/AD633JN, U/TL082CP, T/MPS2222A and ±15 V DC voltage source. The experimental results of different types of multi-scroll grid hyperchaotic attractors generated in different planes when memristor Mem1 turns off S_0, memristor Mem2 turns off S_0 and S_1, and memristor Mem3 turns off S_0, S_1 and S_1' are shown in Fig. 16. The experimental results show that the circuit simulation results are in good agreement with the numerical simulation results, which further verifies the feasibility of the design.

Now turn off S_0, S_1 and S_1' of the memristor Mem2 and modify $R_{c2} = 20$ kΩ, and keep other circuit parameters unchanged. The initial values of the ten capacitors are set to 0.1 V, 0.1 V, 0.1 V, 0.1 V, 0.1 V, 0.1 V, 0.1 V, 0.1 V, φ_{20} V and 0.1 V, where φ_{20}=±1, ±3. The experimental results for the four cases are shown in Fig. 17, and it can be seen that with different initial capacitor voltages, the MMHNN can generate four 1-scroll hyperchaotic coexisting attractors, as well as 4-scroll hyperchaotic coexisting attractors with equal size and similar shape in the different plane, and their positions

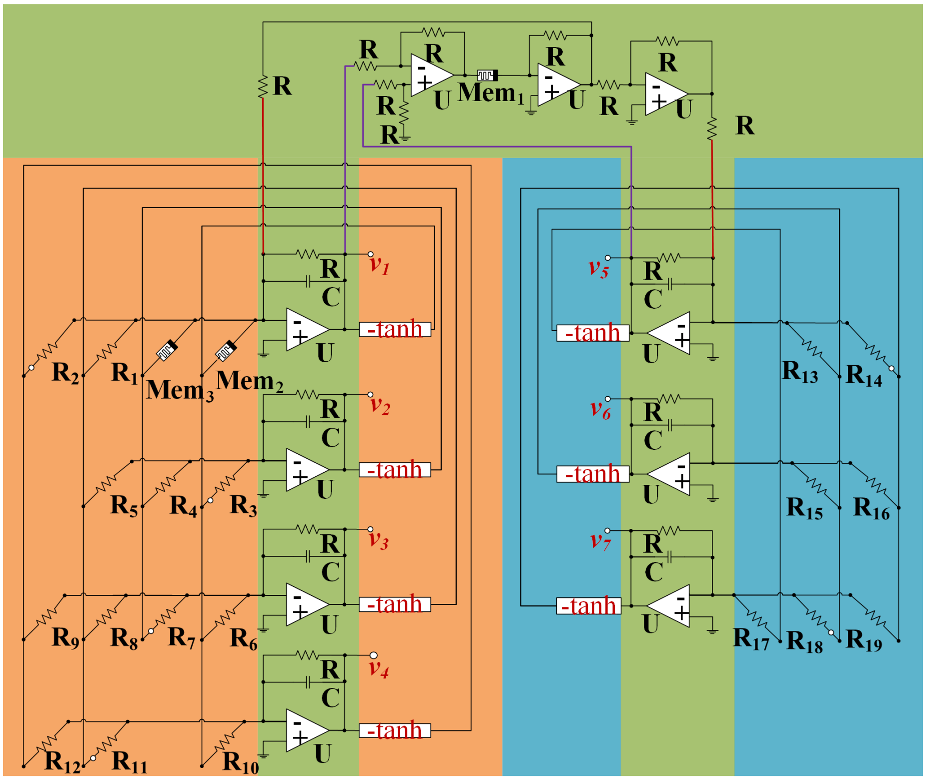
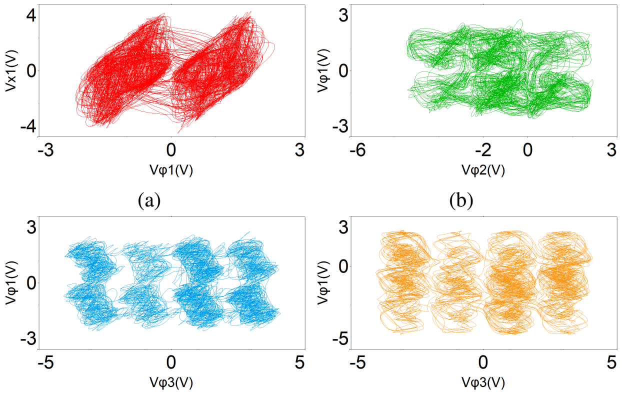


Fig. 15: Circuit realisation of the MMHNN.



(a)

(b)

(c)

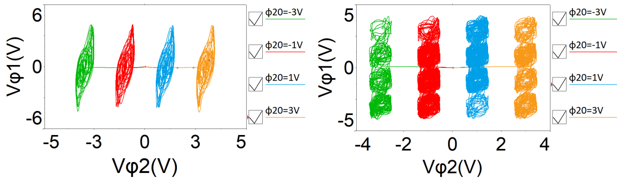
(d)

Fig. 16: Results of the MMHNN circuit: (a) 1*2 scroll. (b) 2*3 scroll.(a) 2*4 scroll. (b) 3*4 scroll.

are only affected by the initial capacitor voltage. Therefore, the MMHNN has extreme multi-stability regulated by the initial value of the memristor.

5. Commercial data encryption system

Compared with the ordinary chaotic system, the model of MMHNN proposed in this paper can generate a controllable number of multi-scroll hyperchaotic attractors in multi-dimensional space, and the phase trajectory can jump randomly between multiple different attractors in the plane and space. Moreover, it has two positive Lyapunov exponents and is very sensitive to initial values and parameters. The attractors have different characteristics under different parameter conditions, and there are multiple coexisting attractors under different initial conditions, with extreme multistability. The nonlinear chaotic dynamic behavior is very complex, which is particularly suitable for chaotic encryption. This part introduces the application of the MMHNN model in commercial data image encryption protection, and analyzes the related test indices of encryption effect.



(a)

(b)

Fig. 17: Results of the MMHNN circuit. (a) 1*1 scroll coexisting; (b) 1*4 scroll coexisting.

5.1. Business data security sharing solution

With the development of economic globalization and intelligent office, business groups will set up different branches in different places. When confidential conference data information is sent between the head office and subsidiaries, if the confidential data is tampered with and leaked, it will inevitably have serious consequences for the development of the company(Meneghello et al., 2019). Therefore, data transmission security is the top priority. Based on the above, this article provides an IoT-based business data sharing solution using the MQTT protocol.

The business data transfer flowchart is shown in Fig. 18, where each company is treated as a network node and assigned an IP address, and business data is sent and received between companies through servers. Suppose n companies need to share data commercially, that is, one company can send information to more than one company. When Company 1's data needs to be sent to Company 2-n, Company 1 publishes the data information, and Company 2-n subscribes to the specific topics needed to recover the data.

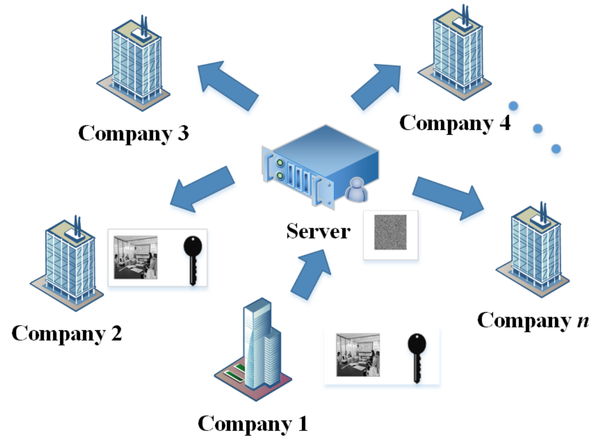


Fig. 18: Business data transfer flowchart.

MQTT is a client-server-based messaging publish and subscribe transport protocol. The ability to provide one-to-many message distribution is lightweight, open, and easy to implement (Yu et al., 2023). The topology structure of the MQTT-based IoT application scenario is shown in Fig. 19, where the server controls the wireless connection from the publisher to the subscriber. To ensure data privacy and security, all data will be encrypted before being sent by the publisher, and the subscriber can get decrypted data only after subscribing to the key.

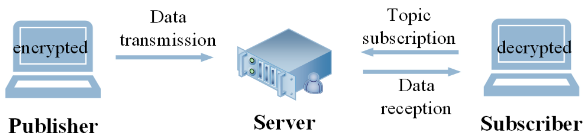


Fig. 19: Data sharing structure of the MQTT.

5.2. Design of commercial image encryption system

In this paper, a conference image is taken as an example. The image encryption system based on MMHNN is implemented on Raspberry Pi through Python programming under MQTT protocol, and the practical feasibility of the system is verified by using a computer, a router and three Raspberry Pis. The test results are shown in Fig. 20. Three Raspberry Pis act as the publisher, server and subscriber, and connected to the same WiFi. Where the publisher runs under IP 192.168.123.137, the server runs under IP 192.168.123.233 and the subscriber runs under IP 192.168.123.151.

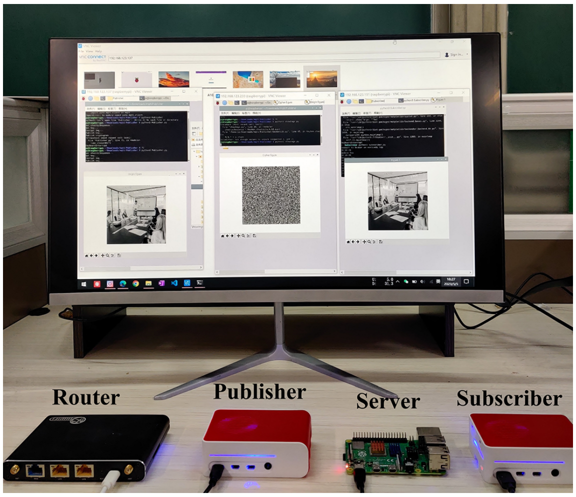


Fig. 20: Physical test results of the IoT-based conference image encryption system.

Here, we choose the chaotic sequence of 4*4*4 hyperchaotic space multi-scroll attractors generated by MMHNN when $M_i = N_i = 1$ in Case-III as the key. Under EMQX (an open source MQTT broker of the IoT), a "256×256 Conference" image shown in Fig. 21(a) is used as the encrypted object to complete sending and receiving. The key steps of the experiment are as follows:

Step 1: Run the publisher, server and subscriber, connect them all to WiFi provided by the router, and obtain the IP address of each Raspberry Pi.

Step 2: The subscriber specifies the required topic image "256×256 Conference", and subscribes the key and image under the corresponding topic.

Step 3: The publisher selects the image subject file name "256×256 Conference" to be sent for data reading and post-processing operation $K(i) = \mathrm{mod}(floor(((x_1(i) + x_2(i) + x_3(i) + x_4(i) + x_5(i) + x_6(i) + x_7(i) + \varphi_1(i) + \varphi_2(i) + \varphi_3(i))/10) \times 10^{15}), 256)$ and $P(i) = P(index(K(i)))$.

Step 4: Generate the corresponding key (0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1) according to the initial value of model (6). The publisher sends messages about the topic key to the subscriber, which reads and stores the key data.

Step 5: The publisher executes the encryption operation $C(i) = P(i) \oplus K(i)$ to obtain the encrypted image as shown in Fig. 21(b) and send it.

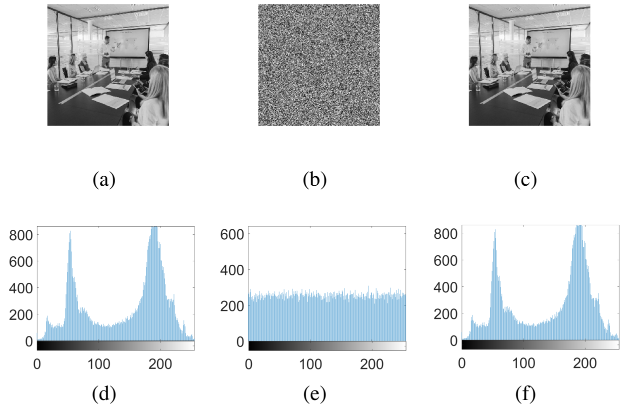
Step 6: After receiving the data related to the image topic, the subscriber uses the received key to decrypt the ciphertext. Decryption is the reverse process of the encryption operation. Using the received key, the subscriber executes the decryption operation $P(i) = C(i) + K(i)$ to obtain the decrypted image, as shown in Fig. 21(c). The decrypted image is directly displayed and saved.

5.3. Encryption performance analysis

To verify the effectiveness of the designed image encryption system, classical metrics such as image histogram, key space, information entropy, correlation coefficient and data loss are analyzed.

5.3.1. Histogram analysis

The histogram is used to evaluate the intensity distribution of the different pixel values in the image. From Fig. 21, it can be seen that the histogram of the encrypted image has a uniform distribution of different pixel intensities, while the decrypted image is able to recover the original features well, indicating that the cryptosystem is well resistant to statistical attacks.


(a) (b) (c)

(d) (e) (f)

Fig. 21: Histogram analysis. (a) original image; (b) encrypted image; (c) decrypted image; (d) original histogram; (e) encrypted histogram; (f) decrypted histogram.

5.3.2. Keyspace analysis

The size of the key space is generally proportional to the resistance to exhaustive attacks. The proposed chaotic image encryption system uses 10 initial values as keys, making unauthorized decryption very difficult. Assuming a precision of 10^{16} for floating-point data (Lin et al., 2023c), the key space of the cryptosystem is about $(10^{16})^{10} = 10^{160} \gg 2^{100}$, indicating that the cryptosystem has sufficient resistance to exhaustive attacks.

5.3.3. Entropy analysis

information entropy is an important index to evaluate the randomness of an image. Ideally, the image information entropy is equal to 8 and is calculated as follows (Yu et al., 2023):

$$H(s) = \sum_{i=0}^{L} P(s_i) \log_2 P(s_i) \tag{10}$$

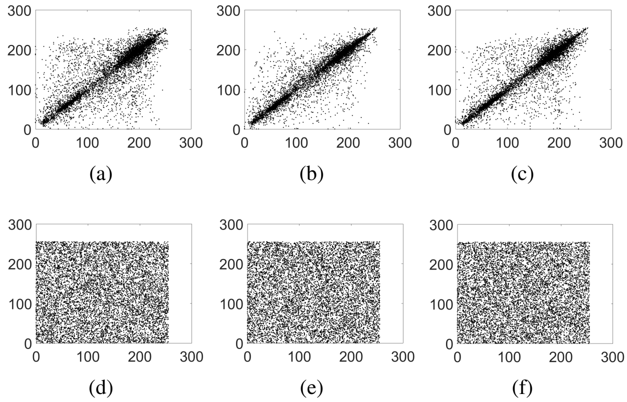
Where L is the gray level and $P(s_i)$ is the probability of occurrence of the gray value s_i. Through the above formula calculation, it can be concluded that the information entropy value of the cryptographic image is 7.9976, which is very close to the ideal value, indicating that the cryptographic system has good encryption performance.

5.3.4. Correlation analysis

Correlation is used to describe the degree of correlation between two adjacent pixels in an image, which can be calculated by the following equation (Yu et al., 2023):

$$Cov(x, y) = \frac{\sum_{i=1}^{N} \left(x_i - E(x)\right)\left(y_i - E(y)\right)}{\sqrt{\sum_{i=1}^{N} \left(x_i - E(x)\right)^2} \sqrt{\sum_{i=1}^{N} \left(y_i - E(y)\right)^2}} \tag{11}$$

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 average values of x_i and y_i, respectively. According to the above formula, 10000 pairs of adjacent pixels are randomly selected in three directions in this paper, and the calculation results of their correlation coefficients are shown in Fig. 22 and Table 3. The correlation coefficients of original images are close to 1 in any direction, and the correlation coefficients of encrypted images tend to be 0 in any direction, indicating that the cryptosystem can effectively reduce the correlation between adjacent pixels of images.


(a) (b) (c)

(d) (e) (f)

Fig. 22: Correlation analysis of Fig. 21(a) and Fig. 21(b). (a) plaintext horizontal direction; (b) plaintext vertical direction; (c) plaintext diagonal direction; (d) ciphertext horizontal direction; (e) ciphertext vertical direction; (f) ciphertext diagonal direction.

5.3.5. Differential attack

The differential attack is used to analyze the plaintext sensitivity of a test algorithm, usually using the number of pixel change rate (NPCR) and the uniform average change intensity (UACI) as evaluation metrics Yu et al. (2022). The closer the NPCR and UACI calculations are to the ideal values (99.6094% and 33.4635%), the better the algorithm is at resisting differential attacks. The definitions are as follows

Table 3
Performances comparison of different encryption schemes

Paper	Image (256*256)	Type	Entropy	Horizontal	Vertical	Diagonal	NPCR/%	UACI/%	Verification method
Lin et al. (2023c)	Lung	Original	7.4130	0.960806	0.922348	0.902746	/	/	MATLAB simulation
		Encrypted	7.9977	-0.000726	0.005403	-0.003982			
Biban et al. (2023)	Lena	Original	7.4292	0.9604	0.9814	0.9405	99.6109	33.4347	MATLAB simulation
		Encrypted	7.9974	0.0029	0.0030	0.0095			
Liang and Zhu (2023)	Cameraman	Original	7.0097	0.960054	0.934912	0.909579	99.6098	33.6011	MATLAB simulation
		Encrypted	7.9974	0.007039	0.004852	0.000585			
Rezaei et al. (2023)	Peppers	Original	/	/	/	/	99.1041	32.8916	MATLAB simulation
		Encrypted	7.9970	0.0079	0.0093	0.0031			
Ours	Conference	Original	7.4998	0.903977	0.937909	0.865492	99.5953	33.5107	IoT application
		Encrypted	7.9976	-0.000544	0.008988	0.003973			

Yu et al. (2023):

$$NPCR = \frac{\sum_{xy} D(x, y)}{WH} \times 100\% \tag{12}$$

$$D(x, y) = \begin{cases} 0 & \text{if } A(x, y) = B(x, y) \\ 1 & \text{if } A(x, y) \neq B(x, y) \end{cases} \tag{13}$$

$$UACI = \frac{1}{WH} \left(\sum_{xy} \frac{|A(x, y)| - |B(x, y)|}{255} \right) \times 100\% \tag{14}$$

where W and H are the width and height of the image respectively, and $A(x, y)$ and $B(x, y)$ are the grayscale values of the pixels at (x, y) for the two ciphertext images. The values of NPCR and UACI calculated by the algorithm in this paper are 99.5953% and 33.5107% respectively. Both of these are close to the ideal values, indicating that the algorithm has good performance against differential attacks.

5.3.6. *Robustness analysis*

The robustness of encryption algorithms can often be tested through data loss and noise attacks. That is to say, a good image encryption scheme should be able to resist data loss and noise attacks. To test the algorithm's ability to resist data loss, we cut off some parts of the encrypted image and then decrypted it. As shown in Fig. 23(a1)-(a4) and Fig. 23 (b1)-(b4), data loss attacks for the different lost parts are successfully decrypted for the original image to be recovered. For testing the algorithm's resistance to noise attacks, salt and pepper noise with different densities are added to the encrypted images. It can be seen from Fig. 23(c1-c4) that some pixel values in the decrypted images have been changed, however, the approximate information of the original images can still be recovered successfully. The experimental results show the proposed encryption algorithm has high robustness.

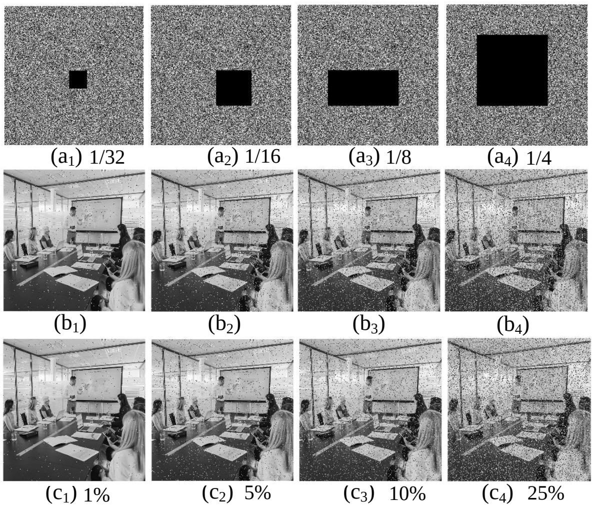


Fig. 23: Test results of the robustness of the algorithm. (a1)-(a4) The encrypted images with 1/32, 1/16, 1/8, and 1/4 data loss, respectively; (b1)-(b4) Corresponding decrypted images; (c1)-(c4) The decrypted images suffered by 1%, 5%, 10%, and 25% salt and pepper noise, respectively.

In addition, Table 3 shows the encryption performances comparison results of different image encryption schemes based on various chaotic systems in recent relevant studies. Compared with most of the current encryption schemes that are only simulated and tested in computers using MATLAB, the proposed MMHNN model-based commercial image encryption system for IoT in this paper is not only carried out by physical tests but also has certain advantages in encryption performance with good encryption effect. The results show that it can further promote the application of memristor neural network chaotic systems in practical IoT scenarios.

6. Conclusion

In this paper, a new simplified model of memristor based on multi-segmental function is proposed, and a high-dimensional multiple memristive HNN model is constructed by using multiple memristors as different types of synapses. The theoretical analysis and numerical simulation reveal that the MMHNN has abundant chaotic dynamics, including a controllable number of 1D, 2D, 3D hyperchaotic multi-scroll attractors, 1D and 2D grid hyperchaotic coexisting attractors, and the number of these attractors can be controlled by the parameters of the memristor equation of state and the initial value of the system. At the same time, the equivalent simulation circuit is constructed by using discrete components, and the simulation results further verify the accuracy of the design and analysis. Finally, a commercial image encryption system for IoT is implemented based on the proposed MMHNN model. The experimental results show that the scheme has better security performances than other similar schemes, and has wide application potential in the field of encryption.

Compared with the existing research, the structure of the memristor model designed in this paper is simpler, it does not need to switch the memristor for different odd-even scroll numbers, and the size of the scroll can be controlled. In addition, we investigate the influence of memristive synapse type on multi-scroll attractors generation and further verify the universality of memristive synapse replacement location, this is the first time that such multiple dynamic phenomena are generated in the HNN model. The test results of the encryption system further confirm the superiority and application potential of the model. However, this paper does not discuss whether the memristor model can be used to replace external stimuli such as electromagnetic radiation or external currents to generate multi-scroll attractors. In addition, whether the multi-scroll attractors generated by the memristor model are universal and whether it can be further extended to other neural network models or chaotic systems is also worth further discussion.

CRediT authorship contribution statement

Chunhua Wang: Supervision, Editing, Funding acquisition. **Dong Tang:** Methodology, Investigation, Writing - original draft. **Hairong Lin:** Validation, Writing - original draft. **Fei Yu:** Writing - review & editing, Software. **Yichuang Sun:** Writing - review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgments

This work is supported by The National Natural Science Foundation of China (62201204, 62271197, 61971185), The China Postdoctoral Science Foundation (2022M71104), and The Natural Science Foundation of Hunan Province, China (2023JJ40168).

References

Ayubi, P., Setayeshi, S., Rahmani, A.M., 2023. Chaotic Complex Hashing: A simple chaotic keyed hash function based on complex quadratic map. Chaos, Solitons & Fractals 173. doi:10.1016/j.chaos.2023.113647.

Azimjonov, J., Kim, T., 2024. Stochastic gradient descent classifier-based lightweight intrusion detection systems using the efficient feature subsets of datasets. Expert Systems with Applications 237, 121493. doi:10.1016/j.eswa.2023.121493.

Biban, G., Chugh, R., Panwar, A., 2023. Image encryption based on 8d hyperchaotic system using fibonacci q-matrix. Chaos, Solitons & Fractals 170, 113396. doi:10.1016/J.CHAOS.2023.113396.

Boya, B.F.B.A., Kengne, J., Kenmoe, G.D., Effa, J.Y., 2022. Four-scroll attractor on the dynamics of a novel Hopfield neural network based on bi-neurons without bias current. Heliyon 8, e11046. doi:10.1016/j.heliyon.2022.e11046.

Boya, B.F.B.A., Ramakrishnan, B., Effa, J.Y., Kengne, J., Rajagopal, K., 2023. Effects of bias current and control of multistability in 3d hopfield neural network. Heliyon 9, e13034. doi:10.1016/j.heliyon.2023.e13034.

Chua, L., 2015. Everything you wish to know about memristors but are afraid to ask. Radioengineering 24, 319–368. doi:10.13164/re.2015.0319.

Deng, Z., Wang, C., Lin, H., Sun, Y., 2023. A memristive spiking neural network circuit with selective supervised attention algorithm. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 42, 2604–2617. doi:10.1109/TCAD.2022.3228896.

Ding, D., Chen, X., Yang, Z., Hu, Y., Wang, M., Niu, Y., 2023a. Dynamics of stimuli-based fractional-order memristor-coupled tabu learning two-neuron model and its engineering applications. Nonlinear Dynamics 111, 1791–1817. doi:10.1007/s11071-022-07886-6.

Ding, S., Wang, N., Bao, H., Chen, B., Wu, H., Xu, Q., 2023b. Memristor synapse-coupled piecewise-linear simplified hopfield neural network: Dynamics analysis and circuit implementation. Chaos, Solitons & Fractals 166, 112899. doi:10.1016/J.CHAOS.2022.112899.

Doubla, I.S., Ramakrishnan, B., Tabekoueng, Z.N., et al, 2022a. Infinitely many coexisting hidden attractors in a new hyperbolic-type memristor-based hnn. The European Physical Journal Special Topics 231, 2371–2385. doi:10.1140/epjs/s11734-021-00372-x.

Doubla, I.S., Ramakrishnan, B., Tabekoueng, Z.N., Kengne, J., Rajagopal, K., 2022b. Hidden extreme multistability and its control with selection of a desired attractor in a non-autonomous hopfield neuron. AEU-International Journal of Electronics and Communications 144, 154059. doi:10.1016/J.AEUE.2021.154059.

Erkan, U., Toktas, A., Lai, Q., 2023. 2d hyperchaotic system based on schaffer function for image encryption. Expert Systems with Applications 213, 119076. doi:10.1016/j.eswa.2022.119076.

Hopfield, J.J., 1984. Neurons with graded response have collective computational properties like those of two-state neurons. Proceedings of the National Academy of Sciences 81, 3088–3092. doi:10.1073/pnas.81.10.3088.

Hu, Z., Wang, C., 2023. Hopfield neural network with multi-scroll attractors and application in image encryption. Multimedia Tools and Applications doi:10.1007/s11042-023-15670-w.

Huang, L., Zhang, Y., Xiang, J., Liu, J., 2022. Extreme multistability in a hopfield neural network based on two biological neuronal systems. IEEE Transactions on Circuits and Systems II: Express Briefs 69, 4568–4572. doi:10.1109/TCSII.2022.3183340.

Kong, X., Yu, F., Yao, W., Xu, C., Zhang, J., Cai, S., Wang, C., 2024. A class of 2n+1 dimensional simplest hamiltonian conservative chaotic systems and fast image encryption schemes. Applied Mathematical Modelling 125, 351–374. doi:10.1016/j.apm.2023.10.004.

Lai, Q., Hu, G., Erkan, U., Toktas, A., 2023a. A novel pixel-split image encryption scheme based on 2d salomon map. Expert Systems with Applications 213, 118845. doi:10.1016/j.eswa.2022.118845.

Lai, Q., Liu, Y., 2023. A cross-channel color image encryption algorithm using two-dimensional hyperchaotic map. Expert Systems with Applications 223, 119923. doi:10.1016/j.eswa.2023.119923.

Lai, Q., Wan, Z., Zhang, H., Chen, G., 2023b. Design and analysis of multiscroll memristive hopfield neural network with adjustable memductance and application to image encryption. IEEE Transactions on Neural Networks and Learning Systems 34, 7824–7837. doi:10.1109/TNNLS.2022.3146570.

Li, X., Mou, J., Xiong, L., Wang, Z., Xu, J., 2021. Fractional-order double-ring erbium-doped fiber laser chaotic system and its application on image encryption. Optics & Laser Technology 140, 107074. doi:10.1016/J.OPTLASTEC.2021.107074.

Liang, Q., Zhu, C., 2023. A new one-dimensional chaotic map for image encryption scheme based on random dna coding. Optics & Laser Technology 160, 109033. doi:10.1016/J.OPTLASTEC.2022.109033.

Lin, H., Wang, C., Du, S., Yao, W., Sun, Y., 2023a. A family of memristive multibutterfly chaotic systems with multidirectional initial-based offset boosting. Chaos, Solitons & Fractals 172. doi:10.1016/j.chaos.2023.113518.

Lin, H., Wang, C., Sun, Y., 2023b. A universal variable extension method for designing multiscroll/wing chaotic systems. IEEE Transactions on Industrial Electronics doi:10.1109/TIE.2023.3299020.

Lin, H., Wang, C., Xu, C., Zhang, X., Iu, H.H., 2023c. A memristive synapse control method to generate diversified multi-structure chaotic attractors. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 42, 942–955. doi:10.1109/TCAD.2022.3186516.

Lin, H., Wang, C., Yu, F., Hong, Q., Xu, C., Sun, Y., 2023d. A triple-memristor Hopfield neural network with space multi-structure attractors and space initial-offset behaviors. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems doi:10.1109/TCAD.2023.3287760.

Ma, X., Wang, C., Qiu, W., Yu, F., 2023. A fast hyperchaotic image encryption scheme. International Journal of Bifurcation and Chaos 33, 2350061. doi:10.1142/S021812742350061X.

Meneghello, F., Calore, M., Zucchetto, D., et al., 2019. Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices. IEEE Internet of Things Journal 6, 8182–8201. doi:10.1109/j.iot.2019.2935189.

Mohamed, S.M., Sayed, W.S., Madian, A.H., Radwan, A.G., Said, L.A., 2023. An encryption application and fpga realization of a fractional memristive chaotic system. Electronics 12, 1219. doi:10.3390/ELECTRONICS12051219.

Perez, A.J., Siddiqui, F., Zeadally, S., Lane, D., 2023. A review of iot systems to enable independence for the elderly and disabled individuals. Internet of Things 21, 100653. doi:10.1016/j.iot.2022.100653.

Rezaei, B., Ghanbari, H., Enayatifar, R., 2023. An image encryption approach using tuned henon chaotic map and evolutionary algorithm. Nonlinear Dynamics 111, 9629–9647. doi:10.1007/S11071-023-08331-Y.

Sasikala, T.S., 2024. A secure multi-modal biometrics using deep ConvGRU neural networks based hashing. Expert Systems with Applications 235. doi:10.1016/j.eswa.2023.121096.

Verma, P., Nagarajan, S., Raj, A., 2022. Spectral graph theory of brain oscillations–Revisited and improved. NeuroImage 249, 118919. doi:10.1016/j.neuroimage.2022.118919.

Wan, Q., Li, F., Chen, S., Yang, Q., 2023. Symmetric multi-scroll attractors in magnetized hopfield neural network under pulse controlled memristor and pulse current stimulation. Chaos, Solitons & Fractals 169, 113259. doi:10.1016/J.CHAOS.2023.113259.

Wan, Q., Yan, Z., Li, F., Chen, S., Liu, J., 2022. Complex dynamics in a hopfield neural network under electromagnetic induction and electromagnetic radiation. Chaos 32, 073107. doi:10.1063/5.0095384.

Wang, N., Li, C., Bao, H., Chen, M., Bao, B., 2019. Generating multi-scroll chua's attractors via simplified piecewise-linear chua's diode. IEEE Transactions on Circuits and Systems I: Regular Papers 66, 4767–4779. doi:10.1109/TCSI.2019.2933365.

Wang, Z., Joshi, S., Savel'ev, S.E., Jiang, H., Midya, R., Lin, P., Hu, M., Ge, N., Strachan, J.P., Li, Z., et al., 2017. Memristors with diffusive dynamics as synaptic emulators for neuromorphic computing. Nature materials 16, 101–108. doi:10.1038/nmat4756.

Wei, D., Jiang, M., Deng, Y., 2023. A secure image encryption algorithm based on hyper-chaotic and bit-level permutation. Expert Systems with Applications 213, 119074. doi:10.1016/j.eswa.2022.119074.

Yang, F., Hu, X., Ren, G., Ma, J., 2023a. Synchronization and patterns in a memristive network in noisy electric field. The European Physical Journal B 96. doi:10.1140/epjb/s10051-023-00549-4.

Yang, F., Wang, Y., Ma, J., 2023b. Creation of heterogeneity or defects in a memristive neural network under energy flow. Communications in Nonlinear Science and Numerical Simulation 119. doi:10.1016/j.cnsns.2023.107127.

Yang, F., Xu, Y., Ma, J., 2023c. A memristive neuron and its adaptability to external electric field. Chaos 33, 023110. doi:10.1063/5.0136195.

Ye, G., Wu, H., Liu, M., Shi, Y., 2022. Image encryption scheme based on blind signature and an improved lorenz system. Expert Systems with Applications 205, 117709. doi:10.1016/j.eswa.2022.117709.

Yu, F., Shen, H., Yu, Q., Kong, X., Sharma, P.K., Cai, S., 2023. Privacy protection of medical data based on multi-scroll memristive hopfield neural network. IEEE Transactions on Network Science and Engineering 10, 845–858. doi:10.1109/TNSE.2022.3223930.

Yu, F., Yu, Q., Chen, H., Kong, X., Mokbel, A.A.M., Cai, S., Du, S., 2022. Dynamic analysis and audio encryption application in iot of a multi-scroll fractional-order memristive hopfield neural network. Fractal and Fractional 6, 370. doi:10.3390/fractalfract6070370.

Zhang, S., Zheng, J., Wang, X., Zeng, Z., 2021. Multi-scroll hidden attractor in memristive hr neuron model under electromagnetic radiation and its applications. Chaos 31, 011101. doi:10.1063/5.0035595.

Zhang, S., Zheng, J., Wang, X., Zeng, Z., He, S., 2020. Initial offset boosting coexisting attractors in memristive multi-double-scroll hopfield neural network. Nonlinear Dynamics 102, 2821–2841. doi:10.1007/s11071-020-06072-w.

Zhang, X., Jiang, D., Nkapkop, J.D.D., Njitacke, Z.T., Ahmad, M., Zhu, L., Tsafack, N., 2023. A memristive autapse-synapse neural network: application to image encryption. Physica Scripta 98, 035222. doi:10.1088/1402-4896/ACBB38.