

Dynamics analysis and cryptographic implementation of a fractional-order memristive cellular neural network model

Xinwei Zhou(周新卫), Donghua Jiang(蒋东华), Jean De Dieu Nkapkop, Musheer Ahmad, Jules Tagne Fossi, Nestor Tsafack, and Jianhua Wu(吴建华)

Citation: Chin. Phys. B, 2024, 33 (**4**): 040506. DOI: 10.1088/1674-1056/ad03dd
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Coexistence behavior of asymmetric attractors in hyperbolic-type memristive Hopfield neural network and its application in image encryption

Xiaoxia Li(李晓霞), Qianqian He(何倩倩), Tianyi Yu(余天意),Zhuang Cai(才壮), and Guizhi Xu(徐桂芝)
Chin. Phys. B, 2024, 33 (**3**): 030505. DOI: 10.1088/1674-1056/acf281

Multiple mixed state variable incremental integration for reconstructing extreme multistability in a novel memristive hyperchaotic jerk system with multiple cubic nonlinearity

Meng-Jiao Wang(王梦蛟) and Lingfang Gu(辜玲芳)
Chin. Phys. B, 2024, 33 (**2**): 020504. DOI: 10.1088/1674-1056/acddd0

Bipolar-growth multi-wing attractors and diverse coexisting attractors in a new memristive chaotic system

Wang-Peng Huang(黄旺鹏) and Qiang Lai(赖强)
Chin. Phys. B, 2023, 32 (**10**): 100504. DOI: 10.1088/1674-1056/ace1d9

Dynamical analysis, geometric control and digital hardware implementation of a complex-valued laser system with a locally active memristor

Yi-Qun Li(李逸群), Jian Liu(刘坚), Chun-Biao Li(李春彪), Zhi-Feng Hao(郝志峰), and Xiao-Tong Zhang(张晓彤)
Chin. Phys. B, 2023, 32 (**8**): 080503. DOI: 10.1088/1674-1056/acd68b

Complex dynamic behaviors in hyperbolic-type memristor-based cellular neural network

Ai-Xue Qi(齐爱学), Bin-Da Zhu(朱斌达), and Guang-Yi Wang(王光义)
Chin. Phys. B, 2022, 31 (**2**): 020502. DOI: 10.1088/1674-1056/ac2b1b

---

Dynamics analysis and cryptographic implementation of a fractional-order memristive cellular neural network model

Xinwei Zhou(周新卫)[1], Donghua Jiang(蒋东华)[2,†], Jean De Dieu Nkapkop[3], Musheer Ahmad[4], Jules Tagne Fossi[5], Nestor Tsafack[6], and Jianhua Wu(吴建华)[1,‡]

[1]*Department of Information Engineering, Gongqing College, Nanchang University, Jiujiang* 332020, *China*
[2]*School of Computer Science and Engineering, Sun Yat-Sen University, Guangzhou* 511400, *China*
[3]*Department of Electrical Engineering and Industrial Computing, University Institute of Technology, Douala, Cameroon*
[4]*Department of Computer Engineering, Jamia Millia Islamia, New Delhi* 110025, *India*
[5]*Department of Physics, Faculty of Science, University of Yaounde, Cameroon*
[6]*Electrical Engineering Department and Industrial Computing of ISTAMA, University of Douala, Douala, Cameroon*

(Received 11 July 2023; revised manuscript received 30 September 2023; accepted manuscript online 17 October 2023)

Due to the fact that a memristor with memory properties is an ideal electronic component for implementation of the artificial neural synaptic function, a brand-new tristable locally active memristor model is first proposed in this paper. Here, a novel four-dimensional fractional-order memristive cellular neural network (FO-MCNN) model with hidden attractors is constructed to enhance the engineering feasibility of the original CNN model and its performance. Then, its hardware circuit implementation and complicated dynamic properties are investigated on multi-simulation platforms. Subsequently, it is used toward secure communication application scenarios. Taking it as the pseudo-random number generator (PRNG), a new privacy image security scheme is designed based on the adaptive sampling rate compressive sensing (ASR-CS) model. Eventually, the simulation analysis and comparative experiments manifest that the proposed data encryption scheme possesses strong immunity against various security attack models and satisfactory compression performance.

Keywords: cellular neural network, memristor, hardware circuit, compressive sensing, privacy data protection

PACS: 05.45.Pq, 47.20.Ky, 87.85.dq, 95.75.Mn **DOI:** 10.1088/1674-1056/ad03dd

1. Introduction

At present, numerous experimental studies have manifested that the activities of biological neurons in the brain are closely connected to certain distinct human abilities, including, but not limited to, learning and memory.[1] Over the past few decades, this has motivated several researchers to explore the working principle of the brain by constructing multifarious artificial neurons and neural network models to mimic its biological structure, such as the classical Hindmarsh–Rose neuron model[2] and the fully connected Hopfield artificial neural network model with rich dynamical behavior.[3] In particular, in 1988, a locally connected nonlinear analog signal processing system, called the cellular neural network (CNN), was first invented by Chua and Yang by combining the Hopfield neural network model with the topological structure of cellular automata.[4]

With regard to the CNN model, due to its local interconnection properties, it not only conforms to the human brain model, but also greatly decreases the difficulty of implementing its circuit, indicating that its proposal is of great significance for understanding the intricate behavior among biological neurons and designing neural network circuits. Subsequently, based on the original CNN model, Yang and his colleagues[5] applied fuzzy operation to it to design a fuzzy neural network model (FCNN) with multi-level information processing capabilities. Additionally, the delayed cellular neural network (DCNN) was proposed by introducing the time-delay input module in Ref. [6]. In these reports, the dynamic properties of the modified CNN were also investigated from the aspects of equilibrium points, periodic solutions, stability and astringency. Moreover, since the various CNN models possess the features of high-speed parallel processing and time-consuming independence of the signal scale, many researchers have devoted efforts to applying them to pattern-recognition and image-processing fields,[4,7] including image noise filtering, edge extraction, and character recognition. Meanwhile, a large number of studies exist that use multi-order CNN models with rich nonlinear dynamic behavior to form continuous chaotic systems to explore their applications in image security communication,[8] chaotic synchronization[9] and other aspects.

Accompanied with the advent of the post-pandemic era, increasing numbers of human interactions have been migrating online. In such social contexts, the integration-based CNN model with plenty of cell units, which can store the data information in a distributed manner with high reliability and can process large-scale tasks in parallel, has inherent advantages. Therefore, to enable it to gain wider application sce-

†Corresponding author. E-mail: jiangdh8@mail2.sysu.edu.cn
‡Corresponding author. E-mail: jhwu@ncu.edu.cn

© 2024 Chinese Physical Society and IOP Publishing Ltd

narios and more powerful processing capability, it must rely on very-large-scale integrated circuit (VLSI) technology with higher integration levels.[7] However, when the area of the integrated circuit (IC) that primarily uses a CMOS transistor as its basic component is compacted to the nanometer level, the nanometer-sized CMOS device will be affected by many physical effects in the microscopic field, such as short-channel effects and high-field effects, thereby affecting the stability and reliability of the IC. Therefore, the fourth passive basic-component nanometer-sized memristor with nonvolatile memory capability offers a feasible solution. Using it to replace the traditional electronic devices to construct the integrated neural network circuit can overcome the nano-bottleneck of CMOS technology and greatly improve the integration of integrated circuits.[10] In other aspects, since the template weights in a CNN determine its processing function for signals, to achieve multiple functions of a single network, the preset weights need to be altered frequently. In traditional CNN circuits, the weight module composed of multipliers cannot freely modify the template weight values inside. Moreover, it is usually too complicated to construct a changeable weight module through multiple logic circuits. If the memristor with non-volatile memory properties is utilized to build the weighted synaptic circuit, it will not only greatly simplify the complexity of the circuit, but will also further degrade the circuit volume, which will greatly promote the further development and popularization of CNNs.

Inspired by the above discussions, our innovations and contributions are listed as follows:

(1) A new tristable locally active memristor model is first proposed. Moreover, its performance is analyzed from the aspect of the pinched hysteresis loop in the voltage–current plane and the power-off plot.

(2) To enhance the engineering feasibility of the original CNN and its performance, including its memory properties and processing capability for signals, a novel fractional-order memristive CNN model with hidden attractors is constructed. Then, its circuit implementation and basic dynamic properties are investigated in hardware based on the STM32F407ZET6 microcontroller development board and software platforms.

(3) To trade off transmission efficiency and compression performance of privacy data, the adaptive sampling rate compressive sensing model is designed by combining the equivalent conditions of restricted isometry properties (RIP) and the ℓ_1 sparsity of the matrix. With the FO-MCNN model as the PRNG, the ASR-CS model is used for private data encryption.

The remaining sections of this paper are arranged as follows. First, Section 2 gives some preliminaries and basic model descriptions relevant to the work carried out in this paper. Then, in Section 3, the definition of the newly designed FO-MCNN model, its dynamic properties and circuit implementation are described and analyzed in detail. Additionally, the ASR-CS model is introduced in Section 4. Next, Sections 5 and 6 present the novel privacy image data security scheme, its simulation and security analysis results. The last section provides a brief overview of our work.

2. Preliminaries and model description

2.1. Basic CNN model

In a nonlinear dynamic field, the CNN is a network of coupled oscillators or is called cells. By coupling a sufficiently large number of cells, complex dynamic behavior can emerge, including limit cycles, chaos, hyperchaos and multistability. Figure 1 provides its equivalent circuit diagram, where R_x and R_y are linear resistors. Here, I and E_{ij} are independent current and voltage sources, respectively; C is a linear capacitor; and $I_{xu}(i,j;k,l)$ and $I_{xy}(i,j;k,l)$ are linear voltage-controlled current sources, respectively. When the output and the state variables of the cells in the CNN are shared with other cells, the CNN is termed as a state-controlled cellular neural network (SC-CNN).[11] It recently received significant attention from academia due to its applications in various fields, including image processing, very-large-scale integration implementation and parallel computing. In addition, SC-CNN hardware realization is easy as the circuit realization is without an inductor. The dimensionless equation of the SC-CNN is formulated by

$$\dot{x}_i = -x_i + \sum_{j=1}^{n} \alpha_{ij}\xi_j + \sum_{j=1}^{n} \beta_{ij}x_j + I_i, \tag{1}$$

where x_i is a state variable of the cells. Here, α_{ij}, β_{ij} and I_i represent the network parameters, and ξ_j is the output of each cell expressed by

$$\xi_j = g(x_j) = \frac{1}{2}\left(|x_j+1| - |x_j-1|\right). \tag{2}$$

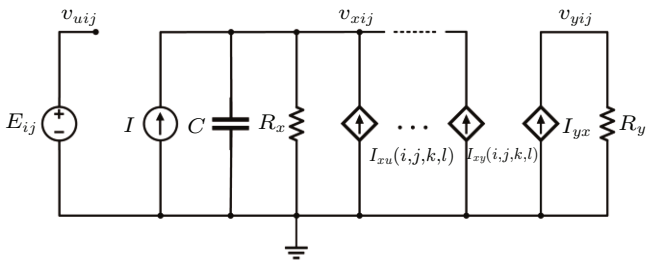


Fig. 1. The equivalent circuit diagram of cells.

2.2. Generic memristor model

The memristor is a passive electronic device that was predicted for the first time by Chua in 1971 as the fourth passive electronic component. The particularity of the memristor is that it can be exploited to save information as its resistance changes from a very large value to a very low value, respectively, interpreted as "1" and "0" logics. Various memristor

types have been proposed, including a locally active memristor (LAM).[12] This category is particularly characterized by negative memristance or negative memductance, which makes it much more accurate in terms of performance. This property also induces more complex dynamics in systems with memristors. The first-order memristors can be classified into four classes that include the ideal memristor, ideal generic memristor, generic memristor and extended memristor. Moreover, the first-order generic memristor can be mathematically defined by[13]

$$\begin{cases} i = M(x)v, \\ \dfrac{\mathrm{d}x}{\mathrm{d}t} = m(x,v), \end{cases} \tag{3}$$

where v and i are the voltage and current through the memristor, respectively, x is the internal variable of the memristor, and M is the memductance of the memristor. Here, m is a function between the voltage and the internal parameter. Equation (4) provides the general definition of $M(x)$ and $m(x,v)$ to achieve any generic memristor model

$$\begin{cases} M(x) = \sum\limits_{k=-i_1}^{i_2} a_k x^k, \\ m(x,v) = \sum\limits_{k=-j_1}^{j_2} b_k x^k + \sum\limits_{k=-l_1}^{l_2} c_k v^k + \sum\limits_{k=-n_1}^{n_2} \sum\limits_{o=-n_1}^{n_2} d_{ko} v^k x^o. \end{cases} \tag{4}$$

2.3. Fractional-order theory

The fractional derivative as the generalization of the integer derivative extends the derivative order of a function from integer to non-integer. It should be noted that the fractional derivative is a powerful tool used to describe the memory properties, and its mathematical definition has many forms, such as the Grunwald–Letnikov, the Riemann–Liouville and the Caputo definitions. Among these definitions, the Riemann–Liouville definition has the advantage of considering all types of functions, including discontinuous and non-differentiable functions at the origin, which applies to most real-world problems.[14] Consequently, this definition will be exploited in this work.

Definition 1 The Riemann–Liouville fractional-θ-order derivative of the function $f(x) \in C^{n+1}([t_0, +\infty))$ is expressed as

$${}^{\mathrm{RL}}D^{\theta}_{t_0,t} f(t) = \frac{1}{\Gamma(n-\theta)} \int_{t_0}^{t} \frac{f^{(n)}(\tau)}{(t-\tau)^{\theta+1-n}} \mathrm{d}\tau, \tag{5}$$

where the $\Gamma(\cdot)$ is the sigma function and n is a positive integer verifying $n-1 < \theta \leq n$.

2.4. Compressive sensing

In 2006, compressive sensing theory, combining sparse representation models of signal and reconstruction algorithms, including the convex optimization, the greedy and the Bayesian algorithms, was proposed by Donoho and Candes.[15,16] For the natural signal with sparsity, the emerging CS can perform down-sampling on it with a sampling rate far lower than that required in the Nyquist–Shannon theorem at the encoding end. Then, the original signal is recovered from a few projections with high probability at the decoding end.

More specifically, for a given real signal $x \in \mathbb{R}^{N\times 1}$, if it is k-sparse under an orthonormal basis Ψ with dimensions of $N \times N$, that is,

$$x = \Psi s. \tag{6}$$

Then, we can employ the matrix $\Phi \in \mathbb{R}^{M\times N}$ $(M \leq N)$ to sample the signal x and acquire a 1D compressed signal $y \in \mathbb{R}^{M\times 1}$. This process can be formulated as[17]

$$y = \Phi x = \Phi\Psi s = \Theta s, \tag{7}$$

where $\Theta = \Phi\Psi$ is often referred to as the sensing matrix.

Because Eq. (7) is an underdetermined equation system, other regular constraints need to be established to restore the original signal x. At present, relevant studies[18] have verified that the signal x is sufficiently sparse on the orthogonal basis Ψ. Moreover, while the sensing matrix Θ satisfies the RIP conditions, its definition is expressed as follows:

If a constant δ_i exists, for any integer $i = 1,2,3,\ldots$, Eq. (8) holds, where the δ_i is called the restricted isometry constant. Then, the matrix Θ is said to satisfy the RIP conditions

$$(1-\delta_i)\|s\|_2^2 \leq \|\Theta s\|_2^2 \leq (1+\delta_i)\|s\|_2^2. \tag{8}$$

Then, the sparse coefficients of the original real signal x can be restored precisely by solving the optimization problem. When the signal x is sparse enough, the reconstruction process can be defined as Eq. (9). In addition, it can rely on the linear programming approach to restore the sparse coefficients s. Then, the original signal x is obtained by executing the inverse transform of sparse representation on s,

$$\min \|s\|_1 \ \text{ s.t. } \ y = \Phi\Psi s. \tag{9}$$

Lemma 1[19] Let $\Phi \in \mathbb{R}^{m\times n}$ be the stochastic matrix, whose entries are independently identically distributed samples extracted from arbitrary distribution, which satisfies the concentration inequality for any signal $x \in \mathbb{R}^{n\times 1}$ and $0 < \varepsilon < 1$, shown as

$$P\left(\left|\|\Phi x\|_2^2 - \|x\|_2^2\right| \geq \varepsilon \|x\|_2^2\right) \leq 2\mathrm{e}^{-mc_0}, \tag{10}$$

where $c_0 > 1$ is a constant that depends only on ε. Then, if for any prescribed $\varepsilon \in (0,1)$, two constants $c_1, c_2 > 0$ exist, depending only on ε and $m \geq c_1 k \log_2(n/k)$ with probability not less than $1 - 2\mathrm{e}^{-c_2 m}$, the RIP holds. Here, the k represents the sparse level of signal x.

Remark 1 Although the RIP provides an approach to quantify the merits of sensing matrices, its computation poses a huge challenge. Hence, according to Lemma 1, it can be known that for a prescribed measurement matrix, if the inequality $m \geq c_1 k \log_2(n/k)$ is established, the original signal with sparsity can be accurately recovered.

Definition 2[20] Regarding a non-zero signal $x \in \mathrm{R}^{n\times 1}$, the grade of its ℓ_1 sparsity can be determined by

$$k(x) = \|x\|_1^2 / \|x\|_2^2. \tag{11}$$

Additionally, the result of this equation always meets the inequation $1 \leq k(x) \leq p$.

3. Novel fractional-order memristive CNN model

3.1. Definition of the new tristable LAM

In this work, following the numerical method of research for the parameters a_k, b_k, c_k and d_k in Eq. (4), the new memristor model is first proposed in the sequel

$$\begin{cases} i = M(x)v = \left(a_0 + a_2 x^2\right) v, \\ \dfrac{\mathrm{d}x}{\mathrm{d}t} = m(x,v) = b_0 + b_1 x + b_3 x^3 + b_5 x^5 + c_1 v. \end{cases} \tag{12}$$

By setting the parameters as $a_0 = -6$, $a_2 = 1.5$, $b_0 = -0.4$, $b_1 = -1.5$, $b_3 = 1.2$, $b_5 = -0.2$ and $c_1 = 1$, Fig. 2 clearly shows that the memductance $M(x)$ is negative for the internal parameter x between -2 and $+2$. Consequently, the designed memristor is termed as a locally active memristor for this set of internal state variables.

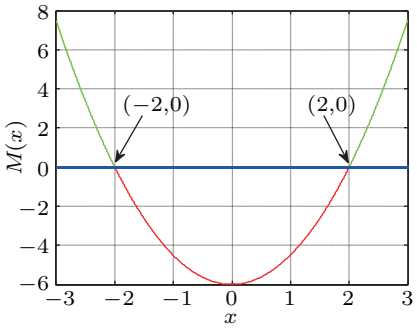


Fig. 2. Evolution of the memductance with respect to the internal variable of the memristor.

3.2. Performance analysis of the new tristable LAM

3.2.1. Pinched hysteresis loop in the voltage–current plane

Basically, a memristor is defined by a pinched hysteresis loop in the voltage–current plane.[21] In this section, we are interested in showing that the new memristor exhibits pinched characteristics. In this order, we need to apply to the designed memristor various sinusoidal excitations of the form $v = A\sin(2\pi F t)$. Some memristor parameters are fixed to $a_0 = -6$, $a_2 = 1.5$, $b_0 = -0.4$, $b_1 = -1.5$, $b_3 = 1.2$, $b_5 = -0.2$, and $c_1 = 1$. When the frequency and initial value are fixed, respectively, to $F = 1.5$ Hz and $x(0) = 1$, the amplitude of the sinusoidal excitation can be varied, and the pinched hysteresis loop in the voltage–current plane that depends on the amplitude is proposed in Fig. 3(a). It is observed in this figure that the lobe of the characteristic increases with the amplitude of the external excitation. When the amplitude and the frequency of the external excitation are respectively fixed to $A = 2$ V and $F = 1.5$ Hz, the pinched hysteresis loop in the voltage–current plane that depends on the initial value $x(0)$ is provided in Fig. 3(b). It is clearly seen that many hysteresis loops coexist in the current–voltage plane that depend solely on the initial value. When the initial value and the amplitude of the external excitation are respectively fixed to $x(0) = 2$ and $A = 2$ V the pinched hysteresis loop in the voltage–current plane that depends on the frequency of the external excitation is depicted in Fig. 3(c). It is observed from this figure that the loop tends to a unique function. Regarding the results of Fig. 3, we can conclude that the designed memristor satisfies the fingerprint characteristics of a memristor, as predicted in Ref. [13].

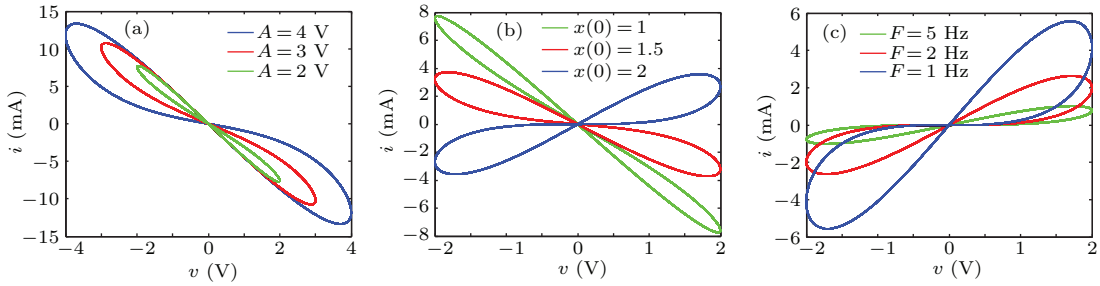


Fig. 3. The pinched hysteresis loop of the new memristor.

3.2.2. Non-volatile and tristable properties

A memristor with non-volatile properties can store the latest value of the memristor resistance, even when the power supply is interrupted. These properties can be evaluated using the power-off plot (POP).[22] While the power-off plot intersects the x-axis at least twice, the memristor presents non-volatile properties. The power-off plot intersection is the representation of the rate of change of the state variable $(\mathrm{d}x/\mathrm{d}t)$

with respect to the state variable x when the power supply is interrupted. Later, when $v=0$ the state of change of the memristor state variable is expressed as

$$\left.\frac{\mathrm{d}x}{\mathrm{d}t}\right|_{v=0} = m(x,0) = b_0 + b_1 x + b_3 x^3 + b_5 x^5. \tag{13}$$

Figure 4 presents the POP of the designed memristor. It is well known that for $\mathrm{d}x/\mathrm{d}t \le 0$, the state variable is moving from right to left; for $\mathrm{d}x/\mathrm{d}t \ge 0$, the state variable is moving from left to right; for $\mathrm{d}x/\mathrm{d}t = 0$, the state variable is fixed on the x-axis. The equilibrium points E_1, E_3 and E_5 are stable as the internal state variables of the memristor in the opposite regions converge to these points, whereas the equilibrium points E_2 and E_4 are unstable as the internal state variables of the memristor in the opposite regions diverge to these points. Hence, the proposed memristor model is tristable.

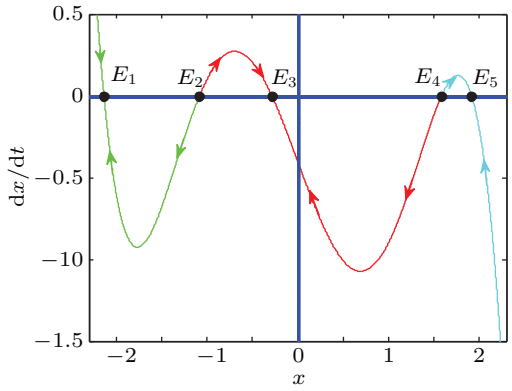


Fig. 4. A power-off plot of the proposed memristor.

3.3. Definition of the new FO-MCNN model

In this work, we exploited the combination of Eqs. (1) and (2) and the proposed tristable locally active memristor to induce chaos in both an integer-order and fractional-order 4×4 cell SC-CNN. The generalized form of the memristor integer- and fractional-order SC-CNN model is given by

$$\begin{cases} {}^{\mathrm{RL}}D^{\vartheta}_{t_0,t}x = -x + \alpha_{11}g(x) + \beta_{11}x + k\left(a_0 + a_2 w^2\right)y, \\ {}^{\mathrm{RL}}D^{\vartheta}_{t_0,t}y = -y + \beta_{21}x + \beta_{22}y + \beta_{23}z, \\ {}^{\mathrm{RL}}D^{\vartheta}_{t_0,t}z = -z + \beta_{32}y + \beta_{33}z, \\ {}^{\mathrm{RL}}D^{\vartheta}_{t_0,t}w = b_0 + b_1 w + b_3 w^3 + b_5 w^5 + c_1 y, \end{cases} \tag{14}$$

where the following real values are the system parameters: $\alpha_{11}=3.9$, $\beta_{11}=-1.6$, $\beta_{21}=1$, $\beta_{22}=0.8$, $\beta_{23}=1$, $\beta_{32}=-14$, $\beta_{33}=1$, $a_0=6$, $a_2=1.5$, $k=1$, $b_0=-0.5$, $b_1=-1.5$, $b_3=1.2$, $b_5=-1$, $c_1=1$. The integer-order 4×4 cell SC-CNN based on the tristable locally active memristor is gained for the case $\theta=1$, and the fractional-order 4×4 cell SC-CNN based on the tristable locally active memristor is gained for the case $0<\theta<1$. By setting the left-hand side of Eq. (14) to zero, we exploited the built-in "solve" function of Maple software to solve the resulting equation and some complex values were obtained. Consequently, the designed tristable locally active fractional-order memristive SC-CNN model can exhibit hidden attractors.

3.4. Numerical analysis of the new FO-MCNN model

To analyze the dynamics of the designed fractional order memristive CNN model, some numerical methods have been exploited. The well-known Runge–Kutta algorithm is exploited to solve the oscillator of Eq. (14). The transient is removed, and the solutions are registered after a sufficiently long time. Then, the time step is kept fixed at 0.005, and the extended precision mode is used for computations. It should be noted that the fixed time step in extended precision mode is known to reveal the suitable dynamics of oscillators and reduce errors when using the Runge–Kutta algorithm.[23] Various tools are exploited to reveal the model dynamic, including a bifurcation diagram, a phase portrait and a Lyapunov spectrum.

3.4.1. Case $\theta = 1$

When varying one of its parameters and saving the local maximum of state variables, the bifurcation graph is gained by solving Eq. (14). Note that the bifurcation diagram is usually exploited to show the dynamic of an oscillator with respect to the variation of one of its parameters. In this work, the parameter β_{22} is selected as the control parameter and is varied in the range $[0.2, 0.73]$. When the rest of the parameters are fixed as $\alpha_{11}=3.9$, $\beta_{11}=-1.6$, $\beta_{21}=1$, $\beta_{23}=0.1$, $\beta_{32}=-14$, $\beta_{33}=1$, $a_0=-6$, $a_2=1.5$, $k=-1$, $b_0=-0.4$, $b_1=-1.5$, $b_3=1.2$, $b_5=-0.2$, $c_1=1$ and $\theta=1$, the complete dynamics of the newly designed model are proposed in Fig. 5.

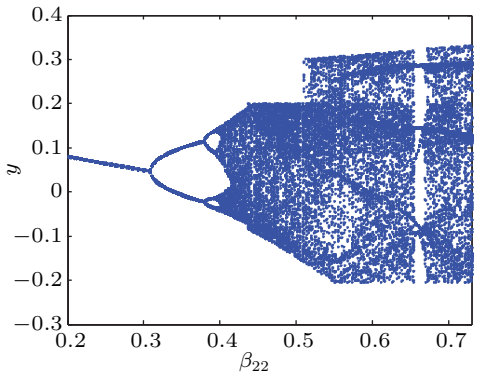


Fig. 5. A bifurcation diagram of the memristive integer-order CNN oscillator.

From this figure, it is observed that the dynamics of the system move from periodic to complicated structures. For the $\beta_{22}\in[0.2, 0.51]$, the dynamics move from the asymmetric period-1 limit cycle to the asymmetric chaotic strange attractor. At $\beta_{22}=0.51$, the symmetric attractors merge to form one asymmetric attractor, as shown in Fig. 6. Note that the bifurcation diagram can also be used to reveal multistability when the

control parameter is slowly varied upward and downward.[24] Additionally, the nonlinear function is at the origin of the complicated dynamics observed in any oscillator model. In our case, it is important to demonstrate that the memristance of the proposed memristor is not the source of the dynamics observed in the proposed oscillator. To achieve this goal, let us solve the proposed oscillator by slowly increasing the internal parameter $b_3 \in [0.45, 1.7]$ of the memristor related to its memristance. The remaining parameters are fixed as $\alpha_{11} = 3.9$, $\beta_{11} = -1.6$, $\beta_{21} = 1$, $\beta_{23} = 0.7$, $\beta_{32} = -14$, $\beta_{33} = 1$, $a_0 = -6$, $a_2 = 1.5$, $k = 1$, $b_0 = -0.4$, $b_1 = -1.5$, $b_3 = 1.2$, $b_5 = -0.2$, $c_1 = 1$ and $\theta = 1$. The obtained dynamics plotted in Fig. 7 confirm chaotic oscillators in the whole range. Therefore, the dynamics of the proposed CNN model are not associated with the memristance of the tristable locally active memristor.

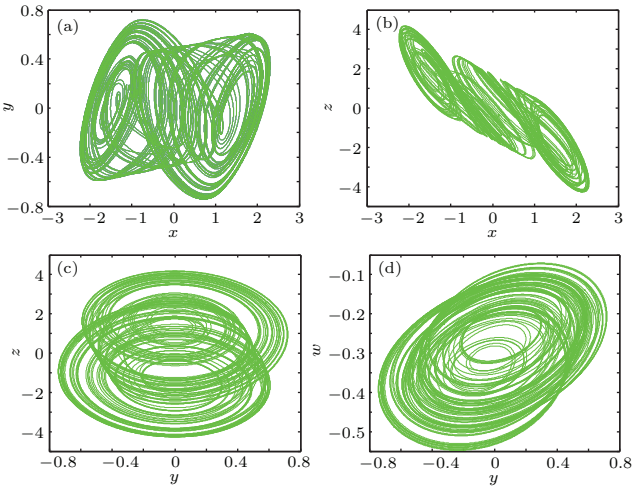


Fig. 6. Asymmetric attractors of the model obtained from the symmetric attractor merging process for $\theta = 1$.

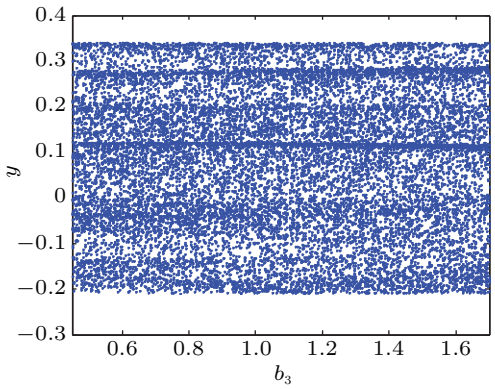


Fig. 7. A bifurcation diagram with respect to b_3.

3.4.2. Case $0 < \theta < 1$

In this section, the fractional case is considered. The Wolf algorithm is adopted to gain the Lyapunov spectrum of the designed oscillator. Here, β_{22} is selected as the control parameter and is varied in the range $[0.1, 1]$. When the rest of the parameters are fixed as $\alpha_{11} = 3.9$, $\beta_{11} = -1.6$, $\beta_{21} = 1$, $\beta_{23} = 0.7$, $\beta_{32} = -14$, $\beta_{33} = 1$, $a_0 = -6$, $a_2 = 1.5$, $k = -1$, $b_0 = -0.4$, $b_1 = -1.5$, $b_3 = 1.2$, $b_5 = -0.2$, $c_1 = 1$ and $\theta = 0.99$, Fig. 8 depicts the Lyapunov spectrum of the proposed FO-MCNN oscillator. It is clearly seen that the oscillator experiences a variety of dynamics, including limit cycles and chaos. However, it can be observed that the global dynamics remain the same with the integer-order case; namely, the system moves from the periodic to the asymmetric chaotic attractor with intertwined limit cycles and finally goes from this state to asymmetric chaotic attractors. Some projections of the chaotic symmetric attractors for the fractional-order case are plotted in Fig. 9. The results may seem identical to those proposed for the integer-order case (see Fig. 6). But it is important to note that the signal related to the memristor is amplified.

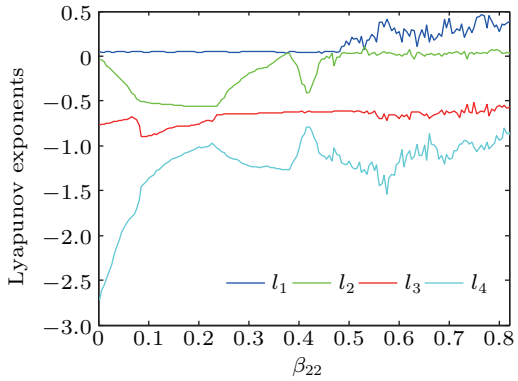


Fig. 8. The Lyapunov exponent of the memristive fractional-order CNN oscillator.

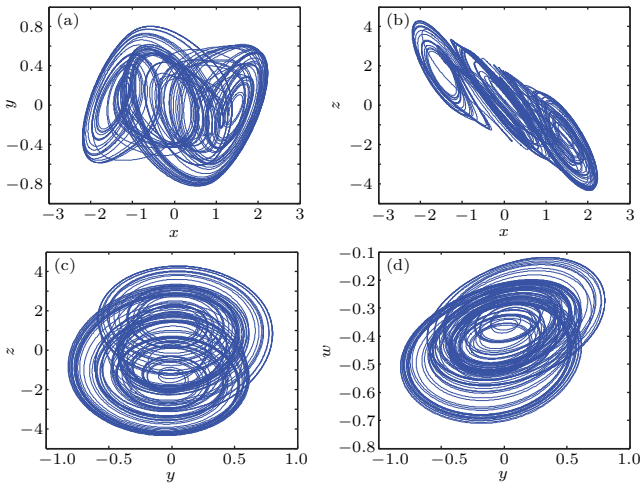


Fig. 9. Asymmetric attractors of the model obtained from the symmetric attractor merging process for $\theta = 0.99$.

3.5. Circuit implementation of the FO-MCNN model

The main objective of this section is to propose a circuit designed around an electronic board, making it possible to reproduce the different behaviors that the FO-MCNN oscillator can present. For this, we opt for a STM-32F407ZET microcontroller board. It is designed based on ARM-Cortex-M4 architecture processors, offering a 32-bit RISC registration set and operating at a frequency of up to 168 MHz. In addition, it is composed of two digital–analog converters (DAC), three

analog–digital converters (ADC), twelve 16-bits timers and many other functional units. Note that this card is compatible with the Arduino development environment (IDE), as well as the programming language in C or C++. The Arduino UNO card plays the role of data acquisition and has been helped by a computer, and the different behavior can be observed.

The STM32F4 board constitutes the FO-MCNN oscillator. The implementation of this oscillator consists of programming the STM32F407ZET microcontroller using the Runge–Kutta with a time step $h = 0.005$ in the Arduino development environment. Figure 10 shows a photograph of the experimental device and the data acquisition. By considering the different values of the parameters defined in Fig. 9, we present, in Fig. 11, the experimental results of the FO-MCNN oscillator. By closely observing these two figures, we affirm that the experimental device can be used to generate the various asymmetric attractors, as shown by the numerical results obtained in Fig. 9.



Fig. 10. The experimental device and data acquisition of the FO-MCNN oscillator.

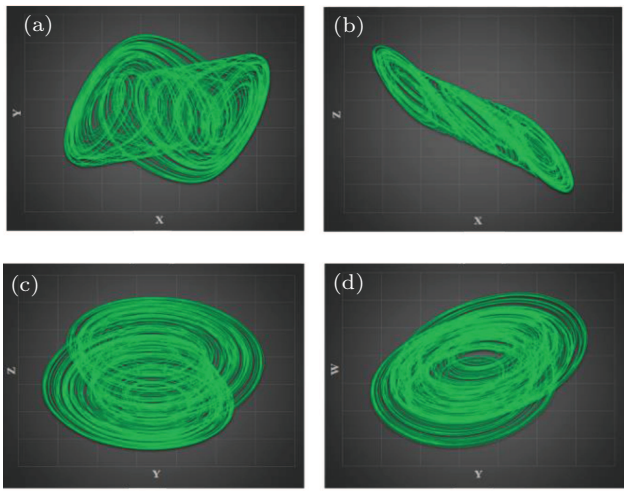


Fig. 11. Experimental asymmetric attractors of the model obtained from the process of merging the symmetric attractors for $\theta = 0.99$.

4. Adaptive sampling rate compressive sensing

For the moment, whether in wireless body area networks (WBANs) or other application scenarios, most CS-based multimedia data compression–encryption schemes have been proposed. In these reported works, a fixed sampling rate (denoted as S_r) was set without exception to observe the plaintext sparse coefficients. However, for the private images with different texture features, arranging a stationary S_r for all types of image data may lead to unstable reconstruction performance. In particular, in WBANs that require high data fidelity, this sampling approach is not practical. To solve this issue, a novel ASR-CS model is introduced in this section by combining Lemma 1 and the ℓ_1 sparsity level of the signal to acquire the balanced performance of data fidelity and transmission efficiency, whose framework is depicted in Fig. 12. Obviously, it primarily includes five operations: multi-layer sparse decomposition, 2D Cat confusion, construction of a measurement matrix with adaptive dimensions, linear observation and quantification. A detailed description of each step for this model follows.

First, the 2D multi-layer wavelet packet transform (ML-WPT) with good sparsity performance is adopted to decompose the natural image $P \in \mathbb{N}^{n\times n}$ before sampling to gain its sparse representation in the transform domain. Notably, many elements close to zero exist in its transform spectrum. After compulsively arranging these elements to 0 by quantifying with the preset threshold value T_s, the sparse coefficients $P_1 \in \mathbb{N}^{n\times n}$ can be produced.

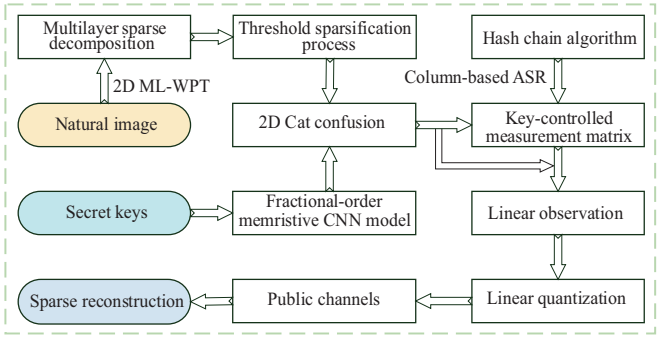


Fig. 12. The framework for adaptive sampling rate compressive sensing.

Then, under the control of the private keys, multiple highly unpredictable evolutional trajectories of the FO-MCNN system are solved using the Runge–Kutta algorithm. In the 2D Cat confusion process, the index matrixes $Q \in \mathbb{N}^{n\times n}$ and $T \in \mathbb{N}^{n\times n}$ are obtained by sorting two chaotic trajectories that are randomly selected from them. After the coordinates of the elements to be scrambled are generated through the Cat transform, the confusion operation is performed circularly on the plaintext coefficients from two dimensions. Moreover, this process can be represented by

$$\begin{cases} \begin{pmatrix} k_1 \\ k_2 \end{pmatrix} = \mathrm{mod}\left(\begin{pmatrix} 1 & Q_{i,j} \\ T_{i,j} & T_{i,j}\cdot Q_{i,j} \end{pmatrix}, \begin{pmatrix} n \\ n \end{pmatrix} \right) + \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \\ P_2(i,j) = P_1(k_1,k_2). \end{cases} \tag{15}$$

Next, according to Eq. (11), the ℓ_1 sparsity level of each column in the scrambled coefficient matrix P_2 is solved. Afterward, the largest sparsity level is selected to calculate the dimension of the key-controlled measurement matrix $\Phi \in \mathbb{N}^{m\times n}$, shown as Eq. (16). Then, the hash chain approach is employed to construct the hardware-friendly measurement matrix with statistical pseudo-randomness. The following Algorithm 1 exhibits the pseudocode of this construction process:

$$m = \left\lceil 2 \cdot \max\left(k\left(P_2(:,i)_{i=1}^{n}\right)\right) \cdot \log_2 \frac{n}{\max\left(k\left(P_2(:,i)_{i=1}^{n}\right)\right)} \right\rceil, \quad (16)$$

where $\lceil \cdot \rceil$ means rounding towards infinity.

Finally, the scrambled sparse coefficients P_2 are linearly projected onto the Φ to complete the compaction procedure, followed by the linear quantization operation. Finally, these two procedures can be formulated by

$$\begin{cases} P_3 = \Phi P_2, \\ P_4 = 255\left(P_3 - \min\left(P_3\right)\right)\left(\max\left(P_3\right) - \min\left(P_3\right)\right)^{-1}. \end{cases} \quad (17)$$

Algorithm 1: The construction of measurement matrix

Input: Private key W_1 and matrix dimension (m,n).

Output: Measurement matrix Φ.

(1): Initialize d that is set to floor $(n/128)$.

(2): Initialize pt with size of $(dm, 128)$, whose elements are all equal to zero.

(3): Initialize h_1 that is set to the message digest of private key W_1 generated by MD5 algorithm.

(4): **for** $i = 1 : 128$ **do**

(5): $pt\,(1,i) = \text{str2num}\,(h_1\,(i))$;

(6): **end**

(7): **for** $i = 2 : dm$ **do**

(8): $\text{temp} = pt\,(i-1,:)$;

(9): $h_2 = \text{hash}\,(\text{temp}, \text{MD5})$;

(10): **for** $j = 1 : 128$ **do**

(11): $pt\,(i,j) = \text{str2num}\,(h_2\,(i))$;

(12): **end**

(13): **end**

(14): Initialize $\Phi = pt$, rearrange it as size (m,n) with column-wise manner.

(15): Arrange the element value equal to zero in Φ to be -1.

Remark 2 In other aspects, several issues exist that need addressing in the ASR-CS model.

(1) Our proposed ASR-CS model is equally applicable to other sparse decomposition transforms, including, but not limited, to DCT, DWT and SWT.[25] Essentially, it depends on merits in terms of the decomposition effects they possess.

(2) Thresholding on the sparsely represented plain-text data and uniformly shuffling the principal components in the coefficient matrix to each column by the Cat confusion are two approaches used to enhance the reconstruction performance of the ASB-CS model.

(3) In Ref. [26], it is pointed out that the 01-sequence generated by the hash chain has good pseudo-randomness and statistical independence and can be utilized to construct the measurement matrix. But in this model, to cut down the energy loss during the observation procedure, we replace the element value equal to 0 in it with -1, while maintaining its hardware-friendly feature.

(4) Since the proposed ASB-CS model is capable of adaptively compressing and encrypting the plaintext image, it is hard to breach when the adversary has no prior knowledge of its sparsity, thereby effectively solving the technical challenges pointed out in Ref. [27].

5. Novel privacy data security scheme

The workflow of the proposed privacy data security scheme, which incorporates the newly designed FO-MCNN and ASR-CS models, is exhibited in the upper half of Fig. 13. Obviously, it consists of two encryption operation layers. Among them, the function of the first encryption layer is to compact the redundant part of the plaintext data as much as possible on the premise of accurately reconstructing the decrypted image. Although the proposed ASR-CS possesses a lightweight encryption effect, its essence is the linear projection,[28] which makes it arduous to defend various chosen-plaintext analysis-based security attack models. Therefore, in the second encryption layer, a life-based point-to-point confusion procedure and two-way diffusion procedure with avalanche effects are adopted to further enhance the security grade of the proposed cryptosystem. Moreover, the secret code streams used for each encryption operation are constructed by the 4D FO-MCNN model with complicated nonlinear dynamical behavior. Another concern is that it is recommended to frequently replace the private keys via some advanced key-sharing protocols to guarantee the security of communication, such as the Diffie–Hellman key exchange agreement algorithm and its derivatives.[29] Next, a detailed description of each step for this cryptosystem follows.

5.1. The first layer encryption

In view of the extremely high sensitivity of the one-way hash algorithm, the initial conditions of the FO-MCNN model are constructed via the 384-bit message digest of the secret key W_2, denoted as hv, agreed by both parties in communication. Then, it is equally divided and converted to the decimal data $\{h_i\}_{i=1}^{8}$. Afterward, the initial states of the designed novel CNN model are gained by executing

$$\begin{cases} x_0 = a_1 \cos\left(h_1 h_8 \pi\right) + b_1, \\ y_0 = a_2 \cos\left(h_2 h_7 \pi\right) + b_2, \\ z_0 = a_3 \cos\left(h_3 h_6 \pi\right) + b_3, \\ w_0 = a_4 \cos\left(h_4 h_5 \pi\right) + b_4, \end{cases} \quad (18)$$

where the parameters $\{a_i\}_{i=1}^{8}$ and $\{b_i\}_{i=1}^{8}$ are adopted to adjust its derived value fields.

With the Runge–Kutta algorithm and the initial states $[x_0, y_0, z_0, w_0]$, several hyperchaotic trajectories with high unpredictability are solved. Then, one of them is stochastically picked out to perform the point-to-point 2D Cat confusion operation. Finally, according to the model recorded in Section 4, the adaptive sampling rate compression operations are carried out on the grayscale plain image $P_1 \in \mathbb{N}^{n\times n}$, resulting in the compressed image $P_4 \in \mathbb{N}^{m\times n}$.

Remark 3 Most notably, for the identical plain images, different secret keys correspond to the compressed images with different sizes. Actually, under control of different secret code streams, the corresponding columns of the coefficient matrixes that will be generated after Cat permutation are not all the same, which will lead to diverse outcomes of Eq. (16). Meanwhile, this can illustrate that our proposed ASR-CS model has dynamic characteristics.

5.2. The second layer encryption

In this section, the game-of-life-based permutation operation is performed on $P_4 \in \mathbb{N}^{m\times n}$ to further decorrelate it, followed by two-way diffusion operation to conceal its statistical properties and gain the powerful avalanche properties. The detailed operation procedures for the second encryption phase are as follows.

First, two chaotic trajectories, denoted as $A \in \mathbb{R}^{m\times n}$ and $B \in \mathbb{R}^{m\times n}$, solved in the proposed FO-MCNN model, are rearranged into the 2D matrix in a column-wise manner. Then, the comparison operation, shown as Eq. (19), is performed on them to acquire the original binary matrix S, where the $S(i,j) = 1$ means a living cell, otherwise it is a dead cell. Then, the matrix S is updated n times according to the game-of-life rule introduced in Ref. [30], each time resulting in a matrix $\{G_l\}_{l=1}^{n}$. Moreover, the SM utilized to regulate the permutation stage can be obtained by executing

$$S(i,j) = \begin{cases} 1, & A(i,j) \geq B(i,j), \\ 0, & \text{otherwise}, \end{cases} \tag{19}$$

$$SM(i,j) = \sum_{l=1}^{n} G_l(i,j) \times 2^{n-1}. \tag{20}$$

Next, the SM is sorted in a row-wise and a column-wise manner separately to obfuscate the compressed image $P_4 \in \mathbb{N}^{m\times n}$ in both directions. In pursuit of extremely low correlation, the permutation process must be performed at least twice. Furthermore, the matrix produced by this process is denoted as $P_5 \in \mathbb{N}^{m\times n}$.

Afterward, according to Eq. (21), a pair of chaotic trajectories, denoted as $D \in \mathbb{R}^{1\times 2mn}$ and $E \in \mathbb{R}^{1\times 2mn}$, solved in the proposed FO-MCNN model, are separately projected into the integer fields $[0, 255]$ and $[1, 7]$, resulting in two cipher flows for the confusion stage, where the constant t_0 is the preset secret key,

$$\begin{cases} S_1 = \mod\left(\lceil (D + t_0) \times 10^{10} \rceil, 256\right), \\ S_2 = \mod\left(\lceil E \times 10^{5} \rceil, 7\right) + 1. \end{cases} \tag{21}$$

Eventually, after the game-of-life-based permutation stage, the two-way encryption operation is carried out on the P_5, which is defined as

$$\begin{cases} P_6(1) = B_0 \oplus P_5(1) \oplus S_1(1), \\ P_6(i) = P_6(i-1) \oplus (P_5(i) \ll S_2(i)) \oplus S_1(i), \\ P_7(mn) = C_0 \oplus P_6(mn) \oplus S_1(2mn), \\ P_7(mn-i) = P_7(mn-i+1) \oplus \big(P_6(mn-i) \\ \qquad\qquad \ll S_2(2mn-i)\big) \oplus S_1(2mn-i), \end{cases} \tag{22}$$

where the constants B_0 and C_0 are the preset secret keys and $\ll$ represents the circular shift operator.

Then, the cipher image $P_7 \in \mathbb{N}^{m\times n}$ without semantic features is produced.

Remark 4 In general, the bitwise XOR operator-based diffusion procedure possesses weak avalanche properties. Therefore, most of the existing encryption schemes rely on the plaintext eigenvalue to assist in the implementation of this kind of diffusion approach, thereby increasing the burden of key management. However, to solve this issue, bidirectional operation and the cyclic shift operator are adopted to make it possible for the minor difference in the plaintext data to spread out into the entire cipher image in our proposed scheme.

5.3. The corresponding decryption scheme

To accurately reconstruct the corresponding grayscale plain image from the encrypted image without semantic features, the encryptor must deliver some encryption parameters and initial states of the newly designed FO-MCNN model to the decryptor via the negotiatory key-sharing protocol. Additionally, as the proposed encryption scheme belongs to the category of symmetric cryptosystems. Thus, under the control of the cipher flows, the noise-like cipher image is subjected to the inverse processes of the two-way diffusion operations and the multi-round game-of-life-based permutation operations, as well as the decompression operations to obtain the reconstruction image, as manifested in the bottom half of Fig. 13. It is worth mentioning that when restoring the sparse coefficient matrix P_2, there are plenty of reconstruction algorithms to choose from, including, but not limited to, the regularized orthogonal matching pursuit, the stage-wise orthogonal matching pursuit and the orthogonal matching pursuit.

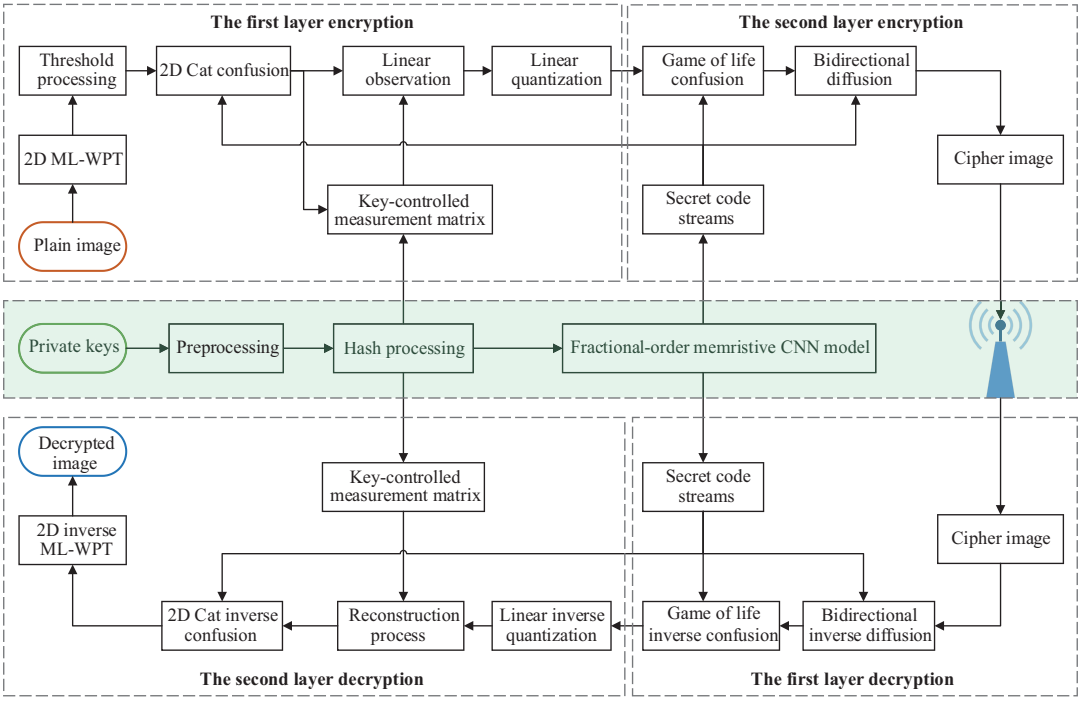


Fig. 13. The workflow for the proposed privacy-preserving cryptosystem.

6. Simulation results and analysis

6.1. Encryption and decryption results

In this section, the simulation environment incorporates 1.80 GHz i7-8550U CPU, 16.0 GB RAM, a 64-bit Windows 10 operating system and Matlab 2020b platform. Moreover, the parameters utilized to construct the initial states of the new FO-MCNN model are arranged as $W_1 = W_2 =$ "password", $\{a_i\}_{i=1}^4 = \{0.15, 0.05, 0.25, 0.35\}$ and $\{b_i\}_{i=1}^4 = \{-0.22, 0.15, -0.32, 0.52\}$. Then, the parameters in the bidirectional confusion stage are arranged as $B_0 = C_0 = 127$. Additionally, the original binary matrix S is updated 5 times, and the decompression approach is selected as the commonly used orthogonal matching pursuit algorithm.

To verify the universality and effectiveness of the proposed privacy data security scheme, six 512×512-sized plain images with different textural features are stochastically selected from the different publicly available image datasets for simulation experiments. Later, these images are subjected to a series of compression and encryption operations, as described previously. Then, the resulting simulation graphs and the corresponding numerically experimental data are elaborated in Fig. 14, where the first to the last columns correspond to plain images, final encrypted images, and their histograms, as well as reconstructed images, respectively. From the gained experimental results, (1) each encrypted image has different sizes. Encrypting the plain images with rich texture properties results in larger image sizes. Quite understandably, for the lossy compressive sensing technology, over-compressing the details of plaintext data will inevitably degrade its reconstruction effects. Meanwhile, all the reconstructed images have a high level of visual quality, with V_{PSNR} and V_{MSSIM} scores greater than 31.5 dB and 0.90. Therefore, V_{PSNR} and V_{MSSIM} are denoted as the PSNR and MSSIM among plain images and decrypted images, respectively. (2) In the visual aspect, each encrypted image is without semantic features and its histogram exhibits a uniform distribution, indicating that the statistical properties of the secret information it carries are effectively eliminated. Based on the above discussion, it can be concluded that the proposed data encryption scheme has good reconstruction quality while considering the transmission efficiency. In the follow-up, we will conduct a comprehensive analysis of it from the aspects of compressibility, security, robustness and time efficiency.

6.2. Compressibility analysis

In this section, the influence of different types of sparse decomposition approaches, such as DCT, DWT and WPT, and measurement matrices (Gaussian, chaotic and hash-chain-based measurement matrices) on the reconstruction performance of the proposed compression–encryption scheme will be analyzed, respectively.

Then, the corresponding experimental data are elaborated and plotted in Figs. 15 and 16, where the wavelet base and decomposition level are selected as "db3" and 3. The nonlinear map adopted to construct the chaotic measurement matrix is "logistic" with the control parameter μ of 4. Additionally, the secret keys and parameters used in the encryption and decryption phases are the same as those described in Subsection 6.1.

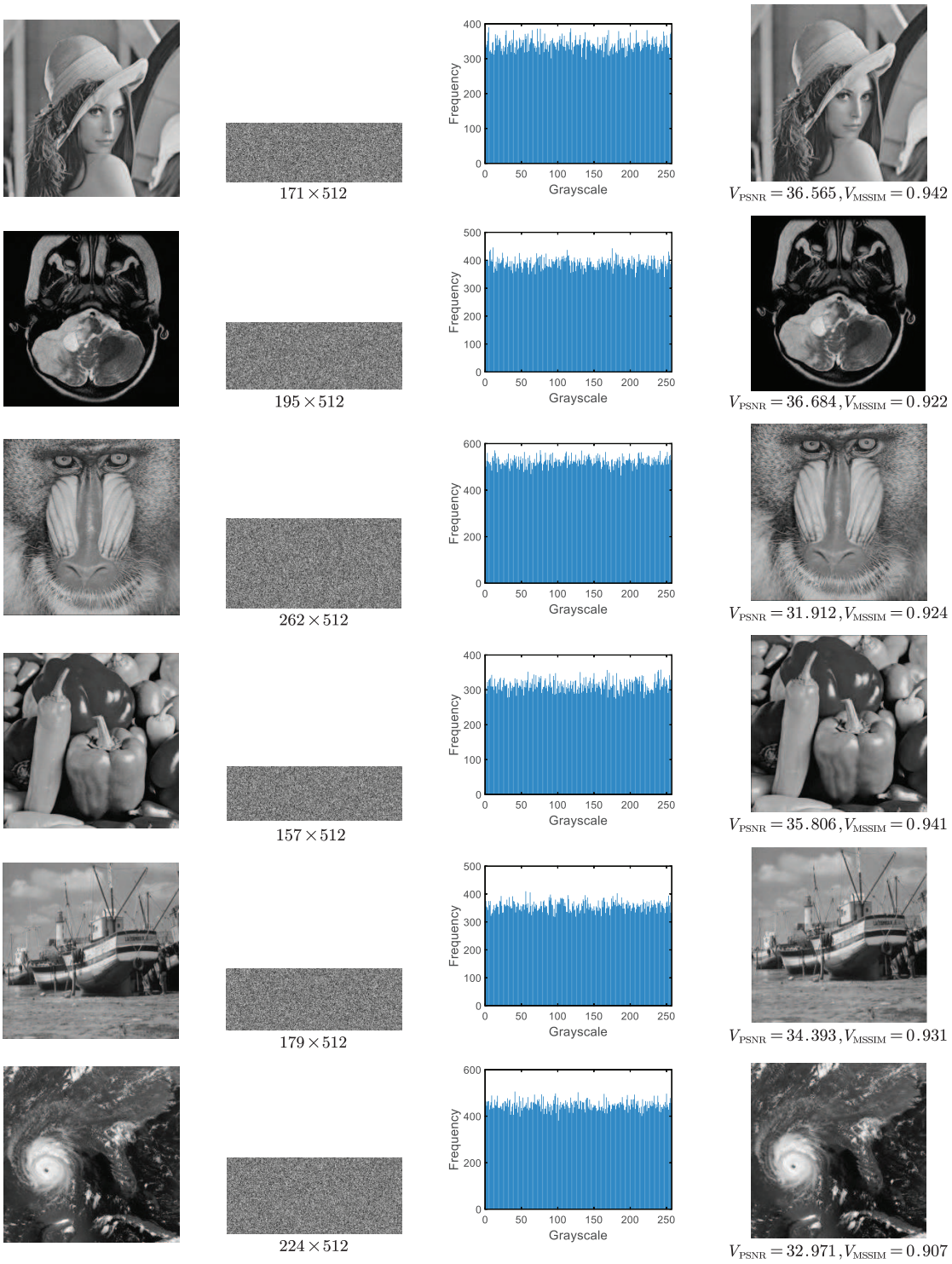


Fig. 14. Simulation results of the proposed scheme.

As displayed in Fig. 15, adopting the 2D DCT with weak sparse decomposition effects to sparsely represent plaintext data results in poor reconstruction quality. Afterward, by comparing the red curve and the blue curve, we can easily find that the WPT-based CS model utilized in this work can achieve better reconstruction effects, especially for the texture-rich plaintext data. This further illustrates its superiority in processing the details of the original plaintext data. Eventually, it is worth noting that the reconstructed images are quite readable, no matter which sparse basis is employed.

Figure 16 depicts the influence of three types of measurement matrices on the compression performance of our introduced cryptosystem. From the perspective of the overall experimental results, the hash-chain-based measurement matrix can obviously gain better reconstruction performance. Moreover, compared with the measurement matrices in the field of real numbers, including, but not limited to, Gaussian, Toeplitz and Bernoulli, this type of measurement matrix adopted in

our work possesses good hardware-friendly properties. Meanwhile, it will not cause quantization errors in any scenario as a result of the use of different soft hardware platforms with different accuracies.

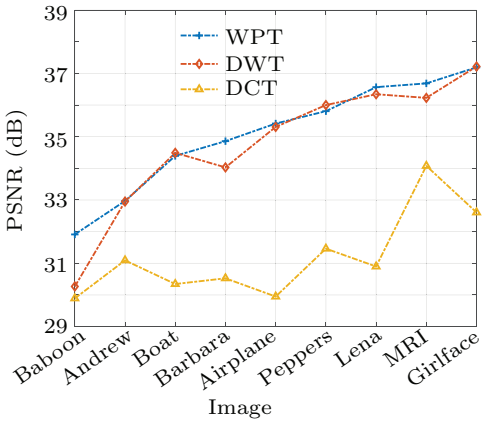


Fig. 15. The relationship among PSNR and images for different sparse decomposition approaches.

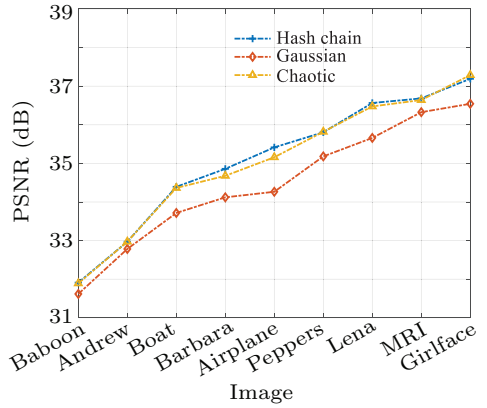


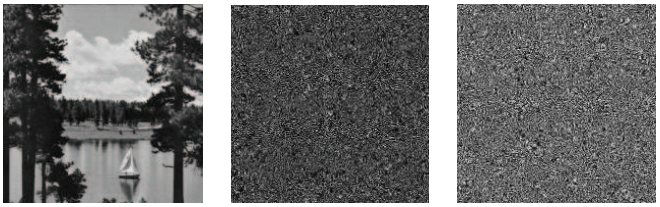
Fig. 16. The relationship among PSNR and images for different types of measurement matrices.

6.3. Security analysis

6.3.1. Anti-violent attack analysis

In secure communication fields, the capability of a cryptosystem to defend against violent attacks can be reflected by the key space and its sensitivity. In this scheme, the secret keys are mainly composed of the initial states for the newly designed FO-MCNN model and the assisted encryption parameters, including $\{a_i\}_{i=1}^4$, $\{b_i\}_{i=1}^4$, B_0 and C_0. Therefore, under the condition that the precision of the floating-point number in the simulation platform is 10^{-14}, the gross key space of this scheme is approximately 2^{714}, which is much larger than some recently designed encryption schemes.[31–34]

Next, taking the image "Sailboat" with a resolution of 512×512 as an instance to qualitatively analyze the key sensitivity level of this scheme, the gained experimental results are depicted in Fig. 17. Obviously, the reconstructed images, like encrypted images, are both without the semantic features associated with the plaintext data, after we modify an arbitrary bit in the message digest of secret keys. Actually, our scheme relies on the hash algorithm and the FO-MCNN model to guarantee its extreme sensitivity to keys. In brief, it is quite difficult to decipher the secret keys used in this encryption scheme using the exhaustive manner.



(a) Any element in the secret keys is not tainted.

(b) Any element in the 128-bit message digest of secret key W_1 is subtracted by one.

(c) Any element in the 384-bit message digest of secret key W_2 is added by one.

Fig. 17. The experimental results of the key sensitivity analysis.

6.3.2. Anti-statistical attack analysis

Besides histograms, information entropy (IE) and correlation coefficients (CC) are also indicators that are frequently used to assess the strength of encryption schemes against various statistical-analysis-based security attack models, which can be respectively formulated by[35]

$$\mathrm{IE} = -\sum_{i=1}^{F} P(x_i) \log_2 P(x_i), \tag{23}$$

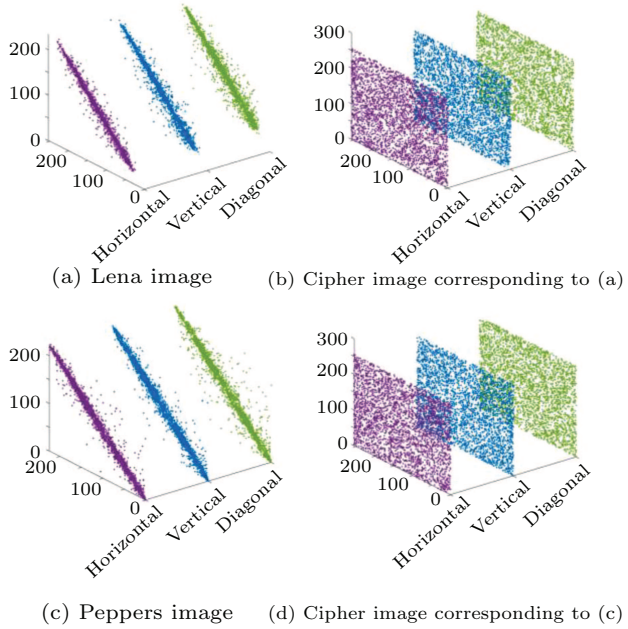
$$\mathrm{CC}(x,y) = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - E(y))^2}}, \tag{24}$$

where F is the grayscale level. Here, $P(x_i)$ is the occurrence probability of x_i, and $E(x)$ is the mathematical expectation of the sequence x with length of N. For a digital image with bit depth of 8, its F value is equal to 255. Moreover, the closer the IE and CC(x,y) values of the cipher image are to the standard values of 8 and 0, respectively, the better statistical pseudo-randomness it possesses, implying its superiority in terms of withstanding statistical attacks.

First, five plain images with apparent textures are chosen to perform comparative experiments on information entropy. Then, the IE scores of corresponding cipher images encrypted by our scheme and other relevant schemes are tabulated in Table 1, where the symbol N/A means that the source literature does not provide the relevant data. As can be seen from the gained numerical results, regardless of which scheme, each cipher image possesses a higher score than its plain image. Additionally, the proposed image encryption scheme, by combining the fractional-order MCNN oscillator and the ASR-CS model in this paper, can achieve entropy values that are closer to the desired value overall.

Table 1. Comparative results of information entropy values for different encryption schemes.

Name	Plain image	Cipher image					
		Proposed	Ref. [31]	Ref. [36]	Ref. [34]	Ref. [37]	Ref. [39]
Lena	7.4464	7.9981	7.9022	7.9973	7.9965	7.9938	7.9974
Peppers	7.5715	7.9974	7.9513	7.9993	7.9991	7.9956	N/A
Baboon	7.3579	7.9984	7.9728	7.9972	7.9950	7.9852	N/A
Cameraman	7.0911	7.9984	N/A	N/A	N/A	7.9846	N/A
Barbara	7.6321	7.9981	N/A	N/A	N/A	N/A	N/A



(a) Lena image (b) Cipher image corresponding to (a)

(c) Peppers image (d) Cipher image corresponding to (c)

Fig. 18. Adjacent pixel pairs in different images along the horizontal, vertical and diagonal directions.

When the parameter N is set to 6500 in Eq. (24), and the images "Lena" and "Peppers" with resolution of 512×512 act as test images, Fig. 18 plots the distribution of adjacent pixel pairs along the horizontal, vertical and diagonal directions for several images. It is obvious that the adjacent pixel pairs in the plain image are closely distributed along the diagonal direction, implying that strong correlation exists in it. The reason for this phenomenon is that the natural image with evident semantic features has data redundancy. After a series of the encryption operations described previously, the adjacent pixel pairs in the generated cipher image are uniformly distributed in phase space. In addition, Table 2 lists the comparative results of several encryption schemes in terms of the correlation coefficient. As can be observed from this table, the correlation coefficients acquired from the proposed scheme are much closer to 0 than other schemes. This indicates that our scheme can successfully eliminate strong correlations among local pixel pairs in plain images. From the above analysis, we know that our proposed scheme can effectively defend against statistical-analysis-based attacks.

Table 2. Comparative results of correlation coefficients for different encryption schemes.

Cipher image	Direction	Proposed	Ref. [36]	Ref. [31]	Ref. [34]	Ref. [39]
Lena	Horizontal	–0.0001	0.0019	0.0081	0.0029	0.0028
	Vertical	–0.0009	–0.0012	–0.0065	0.0080	0.0018
	Diagonal	–0.0019	0.0009	0.0182	–0.0003	0.0033
Peppers	Horizontal	–0.0001	0.0003	0.0082	N/A	N/A
	Vertical	0.0003	0.0014	0.0002	N/A	N/A
	Diagonal	0.0027	0.0007	0.0088	N/A	N/A

6.3.3. Anti-differential attack analysis

The differential analysis-based security attack models are another kind of approach favored by attackers. This refers to when the attacker attempts to establish several instrumental connections among the ciphertexts and the corresponding plaintexts to successfully decipher the sensitive information carried by the ciphertext under the conditions of unknown secret keys after performing a series of encryption operations on several constructed plain images with slight differences. Therefore, to withstand these kinds of attack models, the designed security scheme is required to possess good avalanche effects. Then, it can be quantitatively evaluated by these two indicators, NPCR and UACI,[28] whose mathematical definitions are listed in the following:

$$\begin{cases} V_{\mathrm{NPCR}} = \dfrac{1}{n^2}\displaystyle\sum_{i=1}^{n}\sum_{j=1}^{n} |\mathrm{Sign}\,(I_1(i,j) - I_2(i,j))|, \\ V_{\mathrm{UACI}} = \dfrac{1}{n^2}\displaystyle\sum_{i=1}^{n}\sum_{j=1}^{n} \dfrac{|I_1(i,j) - I_2(i,j)|}{255}, \end{cases} \tag{25}$$

where I_1 and I_2 represent two test images of size $n \times n$.

In addition, it is pointed out in Ref. [38] that the desired thresholds for NPCR and UACI are 0.996094 and 0.334635, respectively. Moreover, a larger value means better immunity in terms of differential analysis-based attack models. Subsequently, the NPCR and UACI grades for our proposed encryption scheme and several recently proposed ones are tabulated in Table 3. As a whole, the cipher images generated by the scheme introduced in this paper can gain higher NPCR and

UACI grades than those in Refs. [32–34,37]. In the experiments, we found that when the plain image is modified to a certain extent, two cipher images with inconsistent dimensions will be produced after encryption, which improves its resistance to various attacks. Most notably, this feature does not exist in other existing image security schemes.

Table 3. Comparative results of NPCR and UACI values for different encryption schemes.

Plain image	Test item	Proposed	Ref. [32]	Ref. [33]	Ref. [37]	Ref. [34]
Lena	NPCR	0.9997	0.9961	0.9965	0.9960	0.9962
	UACI	0.3472	0.3347	0.3346	0.3464	0.3339
Cameraman	NPCR	0.9934	0.9961	0.9963	0.9965	N/A
	UACI	0.3513	0.3345	0.3349	0.3454	N/A
Barbara	NPCR	0.9972	0.9961	0.9962	N/A	N/A
	UACI	0.3713	0.3346	0.3343	N/A	N/A
Peppers	NPCR	0.9976	0.9961	0.9960	0.9961	0.9961
	UACI	0.3346	0.3346	0.3346	0.3293	0.3339
Baboon	NPCR	0.9974	0.9961	0.9960	0.9961	0.9956
	UACI	0.3362	0.3346	0.3347	0.3298	0.3339

6.4. Robustness analysis

It is undeniable that the external interference or channel blockage existing in the public channel hinders the accurate reconstruction of the secret information carried by the cipher image at the decoding end. Therefore, taking the image "Lena" of size 512×512 as the test object, the noises (including salt & pepper noise, denoted as SPN, speckle noise, denoted as SN, and Gaussian noise, denoted as GN) and all-zeros mask matrices with different intensities are integrated respectively into its cipher image in the simulation platform to assess the robustness of the proposed privacy protection scheme. Later, the obtained experimental data and the simulated results graphs are elaborated in Figs. 19 and 20.

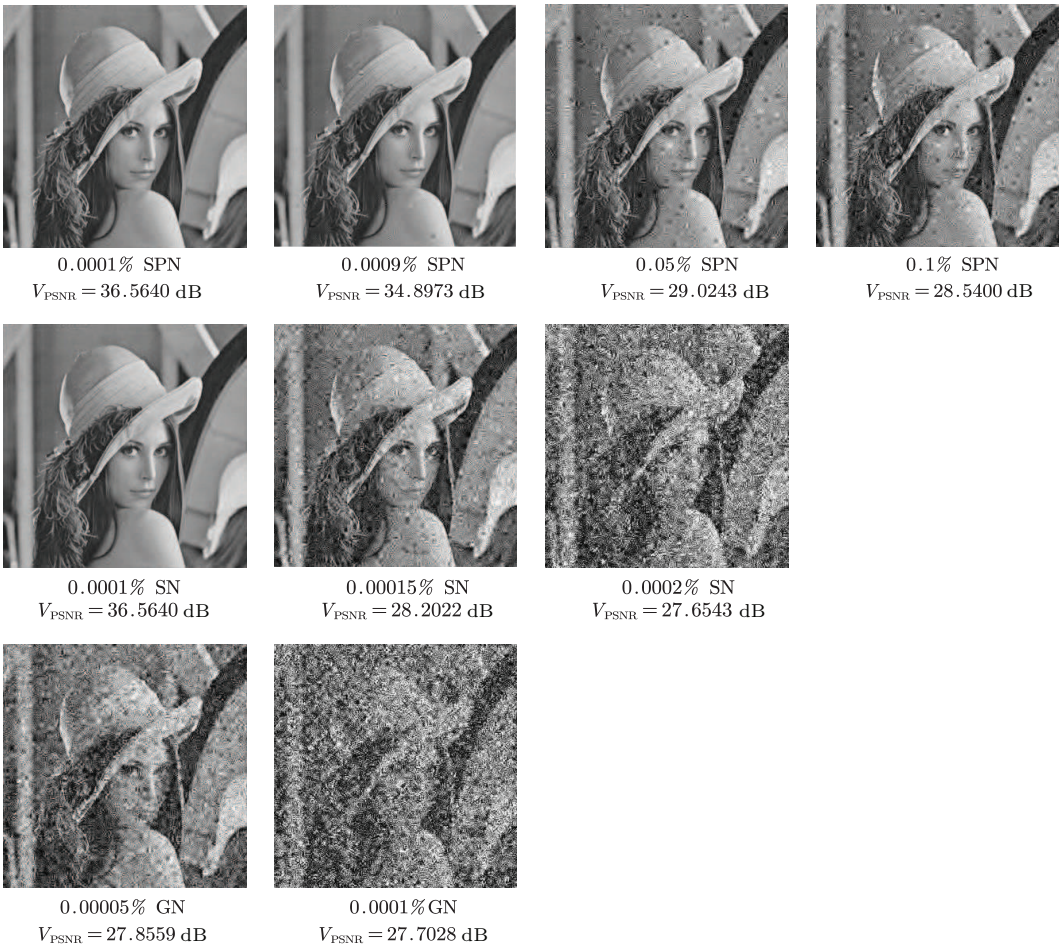


Fig. 19. Reconstructed images under different kinds of noise with multiple attack intensities.

As depicted in Fig. 19, it is confirmed that the reconstructed images are all highly readable when the intensity of the SPN varies from 0.0001% to 0.1%, implying that our proposed scheme possesses strong immunity against the salt & pepper noise

attacks. In other respects, due to the encryption operations introduced previously in Subsection 5.2 with strong diffusion effects, for the global modification-based additive noises, i.e., SN and GN, the proposed scheme has limited resistance to the attacks in this regard. Additionally, Fig. 21 provides the comparative results with Chai's scheme[40] in terms of SPN and SN attacks. Obviously, from the results of comparison experiments, it can be concluded that our scheme possesses outstanding superiority in withstanding SPN attacks and a certain number of SN attacks.

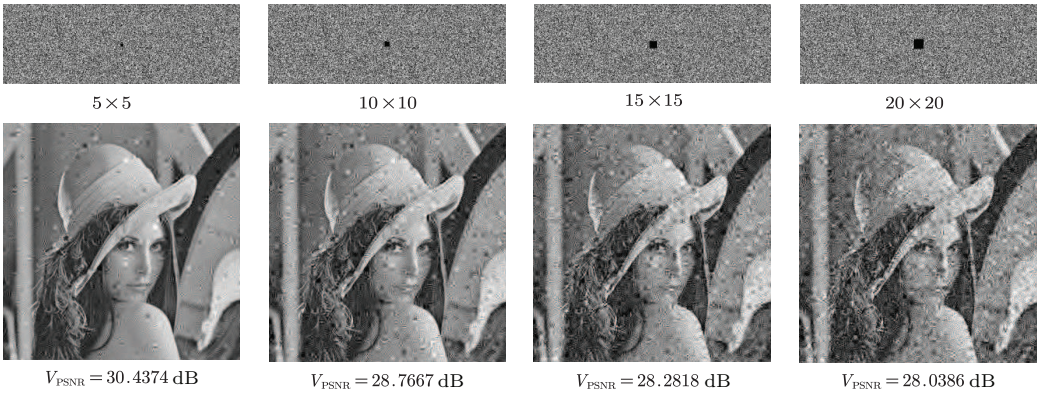


Fig. 20. Reconstructed images under multiple shearing attack intensities.

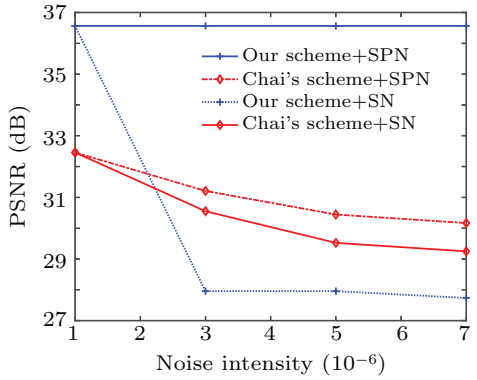


Fig. 21. Comparative results with Chai's scheme in terms of noise attacks.

Figure 20 manifests the experimental results of data packet dropout simulated with the occlusion manner. As shown, accompanied by the fact that the size of the mask matrix continues to increase, the semantic features of the reconstructed images also become increasingly blurred. However, the texture information they display is still readable and recognizable. In general, the scheme proposed in this paper has satisfactory robustness.

6.5. Efficiency analysis

In the last section, we will analyze the efficiency of the proposed scheme from the aspects of its time complexity and actual running time in the simulation platform. First, under the conditions that the dimension of the selected test object is $n\times n$ and the consumed time of the preprocessing stage is ignored, then the time complexity utilized to construct secret code streams and perform adaptive sampling rate compression on the test image, respectively, are $O\left(n^2\right)$ and $O\left((1+m+n)n\right)$ in the first layer encryption. Later, in the next stage, to successfully implement the permutation operation and the bidirectional diffusion operation with strong avalanche effects, as described previously, on the compressed image, the time complexity $O(11mn)$ is required. From the above results, due to the uncertainty of m, the test objects with different texture properties correspond to inconsistent actual time complexity in this scheme.

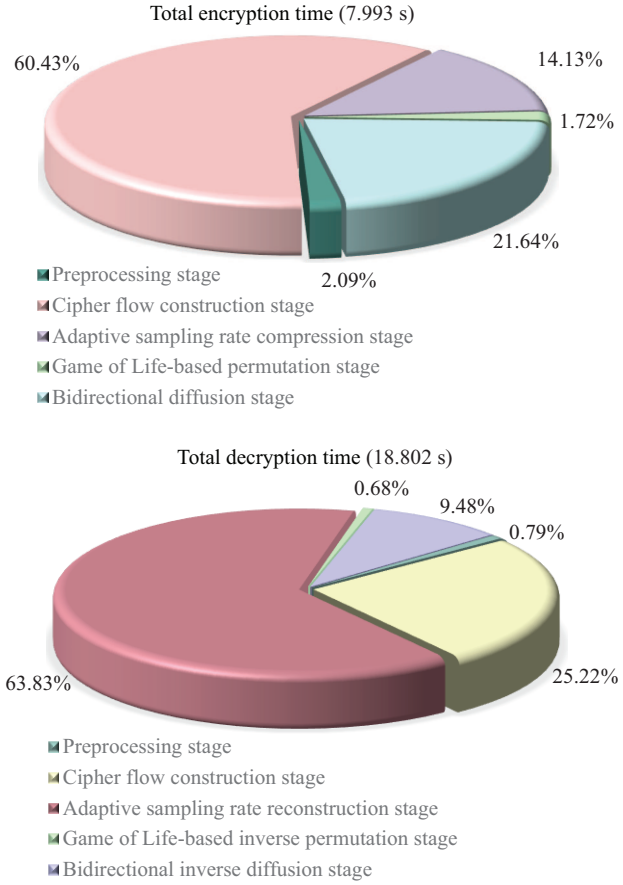


Fig. 22. Time proportions of each stage in encryption and decryption schemes for the 512×512-sized image "Lena".

The gross encryption and decryption time and the proportion of time occupied by each stage for this scheme are manifested in Fig. 22. It can be seen from this that the stage of constructing the highly pseudo-random cipher flows through the newly designed 4D FO-MCNN oscillator during the encryption process occupies more than 60% of the total running time. In practical application scenarios, the cipher flows can be constructed in advance to control each encryption operation performed on private images; thereby, the time spent at this stage can be ignored. Meanwhile, to guarantee the security of communication, it is extremely necessary to alter the cipher streams occasionally. Additionally, in the corresponding decryption process, most of the time is spent on accurately recovering the sparse coefficients of plaintext. Eventually, to further enhance the running efficiency of this scheme on the premise that it does not impact its security performance, it is suggested to lessen the number of loop iterations for the new FO-MCNN oscillator and the optimization process in the decryption terminal using the block-wise manner.

7. Conclusion

In this paper, a new four-dimensional cellular neural network model with fractional-order memristive form is constructed by introducing the newly designed local activity memristor with a tristable state into the original CNN system. Then, its dynamics analysis and hardware circuit design are carried out, thus providing the function of theoretical guidance for its potential practical application scenarios. Moreover, due to its distinct nonlinear dynamic behavior, this paper also presents its application in privacy data protection. Finally, the proposed image encryption scheme with hardware-friendly properties is investigated and compared from the following four aspects: security, compressibility, robustness, and time efficiency. The extensive experimental results indicate that our proposed scheme has good encryption effects and outperforms other relevant prior works. In our follow-up work, we will develop the application of the four-dimensional FO-MCNN in the field of multi-source object recognition.

References

[1] Ma J and Tang J 2017 *Nonlinear Dyn.* **89** 1569
[2] Hindmarsh J L and Rose R M 1982 *Nature* **296** 162
[3] Hopfield J J 1984 *Proc. Natl. Acad. Sci. USA* **81** 3088
[4] Chua L O and Yang L 1988 *IEEE Transactions on Circuits and Systems* **35** 1273
[5] Yang T, Yang L B, Wu C W and Chua L O 1996 *Fourth IEEE International Workshop on Cellular Neural Networks and Their Applications* pp. 181–186
[6] Cao J and Zhou D 1998 *Neural Networks* **11** 1601
[7] Hu X, Feng G, Duan S and Liu L 2017 *IEEE Transactions on Neural Networks and Learning Systems* **28** 1889
[8] Chen L, Yin H, Huang T, Yuan L, Zheng S and Yin L 2020 *Neural Networks* **125** 174
[9] Chen L, Cao J, Wu R, Tenreiro Machado J A, Lopes A M and Yang H 2017 *Neural Networks* **94** 76
[10] Jo S H 2010 *Nanoscale memristive devices for memory and logic applications* University of Michigan ProQuest Dissertations Publishing, 2010.3406295
[11] Lai Q, Wan Z, Zhang H and Chen G 2022 *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–14
[12] Jin P, Wang G, Iu H H C and Fernando T 2018 *IEEE Transactions on Circuits and Systems II: Express Briefs* **65** 246
[13] Chua L 1971 *IEEE Transactions on Circuit Theory* **18** 507
[14] Sweilam N H and AL-Mekhlafi S M 2022 *In Fractional-Order Modeling of Dynamic Systems with Applications in Optimization, Signal Processing and Control*, pp. 97–118
[15] Candes E J and Wakin M B 2008 *IEEE Signal Processing Magazine* **25** 21
[16] Donoho D L 2006 *IEEE Transactions on Information Theory* **52** 1289
[17] Zhou S, Deng X, Li C, Liu Y and Jiang H 2023 *IEEE Transactions on Multimedia* **25** 2022
[18] Baraniuk R G 2007 *IEEE Signal Processing Magazine* **24** 118
[19] Tang G and Nehorai A 2011 *IEEE Transactions on Signal Processing* **59** 5734
[20] Lopes M E 2013 *International Conference on Machine Learning* **28** 217
[21] Khalil N A, Said L A, Radwan A G and Soliman A M 2022 *Fractional Order Systems* 375
[22] Li C, Yang Y, Yang X, Zi X and Xiao F 2022 *Nonlinear Dyn.* **108** 1697
[23] Njitacke Z T, Sone M E, Fozin T F, Tsafack N, Leutcho G D and Tchapga C T 2021 *Euro. Phys. J.: Spec. Top.* **230** 1839
[24] Nestor T, de Dieu, N J, Jacques K, Yves E J, Iliyasu A M and Abd El-Latif A A 2020 *Sensors* **20**
[25] Hua Z, Zhang K, Li Y and Zhou Y 2021 *Signal Processing* **183**
[26] Li L, Peng H, Liu L and Yang Y 2018 *International Symposium on Security and Privacy in Social Networks and Big Data*, 18866867
[27] Ma Y, Li C and Ou B 2020 *Journal of Information Security and Applications* **54** 102566
[28] Zhu L, Song H, Zhang X, Yan M, Zhang T, Wang X and Xu J 2020 *Signal Processing* **175**
[29] Niu Z, Zheng M, Zhang Y and Wang T 2020 *IEEE Internet of Things Journal* **7** 734
[30] Wang X, Ren Q and Jiang D 2021 *Nonlinear Dyn.* **104** 4543
[31] Azam N A, Hayat U and Ayub M 2021 *Signal Processing* **187**
[32] Erkan U, Toktas A, Toktas F and Alenezi F 2022 *Information Sciences* **589** 770
[33] Naskar P K, Bhattacharyya S, Mahatab K C, Dhal K G and Chaudhuri A 2021 *Nonlinear Dyn.* **105** 3673
[34] Zou C, Wang X and Li H 2021 *Nonlinear Dyn.* **105** 859
[35] Hua Z, Li J, Chen Y and Yi S 2021 *Nonlinear Dyn.* **103** 807
[36] Cao C, Sun K and Liu W 2018 *Signal Processing* **143** 122
[37] Kaur G, Agarwal R and Patidar V 2020 *Engineering Science and Technology* **23** 998
[38] Hua Z, Zhu Z, Chen Y and Li Y 2021 *Nonlinear Dyn.* **104** 4505
[39] Li X, Zhou L and Tan F 2022 *Soft Computing* **26** 511
[40] Chai X, Fu J, Gan Z, Lu Y and Zhang Y 2022 *Nonlinear Dyn.* **108** 2671