SCIENCE CHINA
Technological Sciences

•Article•

October 2021 Vol.64 No.10: 2281–2291
https://doi.org/10.1007/s11431-021-1845-x

Discrete memristive neuron model and its interspike interval-encoded application in image encryption

BAO Han[1*], HUA ZhongYun[2], LIU WenBo[1] & BAO BoCheng[3]

[1] *College of Automation Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China;*
[2] *School of Computer Science and Technology, Harbin Institute of Technology, Shenzhen, Shenzhen 518055, China;*
[3] *School of Microelectronics and Control Engineering, Changzhou University, Changzhou 213164, China*

Received February 4, 2021; accepted April 28, 2021; published online August 11, 2021

Bursting is a diverse and common phenomenon in neuronal activation patterns and it indicates that fast action voltage spiking periods are followed by resting periods. The interspike interval (ISI) is the time between successive action voltage spikes of neuron and it is a key indicator used to characterize the bursting. Recently, a three-dimensional memristive Hindmarsh-Rose (mHR) neuron model was constructed to generate hidden chaotic bursting. However, the properties of the discrete mHR neuron model have not been investigated, yet. In this article, we first construct a discrete mHR neuron model and then acquire different hidden chaotic bursting sequences under four typical sets of parameters. To make these sequences more suitable for the application, we further encode these hidden chaotic sequences using their ISIs and the performance comparative results show that the ISI-encoded chaotic sequences have much more complex chaos properties than the original sequences. In addition, we apply these ISI-encoded chaotic sequences to the application of image encryption. The image encryption scheme has a symmetric key structure and contains plain-text permutation and bidirectional diffusion processes. Experimental results and security analyses prove that it has excellent robustness against various possible attacks.

chaos complexity, chaotic bursting sequence, memristive neuron model, interspike interval (ISI), image encryption

Citation: Bao H, Hua Z Y, Liu W B, et al. Discrete memristive neuron model and its interspike interval-encoded application in image encryption. Sci China Tech Sci, 2021, 64: 2281–2291, https://doi.org/10.1007/s11431-021-1845-x

1 Introduction

Nowadays, due to the booming development of big data and cloud computing, multimedia has become the most valuable transmission carrier for digital information [1–4]. Then it is vitally important to protect the contents of multimedia and the encryption is a very effective technology for this [5]. Chaos is an important and interesting phenomenon in nonlinear dynamical systems and it can exhibit complex and unpredictable behavior. Chaotic systems are characterized by initial state sensitivity, internal randomness, and global stability. These features are very similar to the concepts of secure communication and image encryption [6]. Therefore, chaos-based cryptography is one of the most popular research topics in computer science and cryptography [7–9].

The biological neuron model is a special nonlinear dynamical model that can exhibit chaotic dynamics [10]. It has received much attention in recent years [11–15]. Usually, neuronal signaling relies on the change of neuron action spike voltage, in which bursting and spiking are both extremely important ways of information communication. Since the first biological neuron model with chaotic features was proposed by Aihara et al. [16], researchers have gradually found that artificially constructed nervous systems can well simulate complex electrical activities. Extended from the well-known Hodgkin-Huxley model [17], various neuron models have been proposed for generating chaotic spiking/bursting of electrical activities [18–21]. Similar to

*Corresponding author (email: hanbao@nuaa.edu.cn)

chaotic oscillating systems, the biological neuron model is also a mathematical equation that exhibits a variety of nonlinear behaviors and can produce spiking or bursting sequences [22,23]. When used in image encryption applications, the chaotic sequences generated by discrete chaotic systems are expected to have complex chaotic dynamics [24–28]. However, since the chaotic bursting sequences of neuron action spike voltages are usually accompanied by resting firing patterns, they have simple chaotic dynamics and cannot be applied directly to chaos-based engineering applications. To the best of our knowledge, the image encryption scheme based on the chaotic bursting sequences has not been reported yet. Thus, the application of the chaotic bursting sequences in image encryption is worth investigating.

When chaos is used in image encryption, the chaotic sequences are generally used to design encryption schemes to achieve the diffusion property [29–33]. To this end, many excellent image encryption schemes have been designed based on existing chaotic or hyper-chaotic systems. Hua et al. [30] presented a cosine-based chaotic system for generating a chaotic map with excellent chaotic performance and developed an image encryption algorithm using the newly generated chaotic map. Wang et al. [31] proposed an image encryption scheme that relied on hybrid multi-chaotic coupled map lattices and the experimental results indicate that the scheme has high security against common attacks. Zhang and Tang [32] developed a piecewise linear mapping-based symmetric key image cryptosystem, which has many advantages and can be applied to practical communication. Li et al. [33] constructed a two-dimensional (2D) memristor-based hyper-chaotic map that displays strong performance in secure communication. All these examples show that the chaotic systems can exhibit excellent performance when used as an indispensable part of cryptography schemes.

A chaotic bursting sequence can be readily generated by a biological neuron model and its interspike interval (ISI) is a key indicator to characterize the bursting sequence. To facilitate the application of the chaotic bursting sequence, this article first constructs a discrete memristive Hindmarsh-Rose (mHR) neuron model with hidden chaotic bursting dynamics and then proposes a novel ISI-based encoding algorithm to enhance the chaos complexity of the generated chaotic bursting sequence. The discrete mHR model has higher implementation efficiency and lower computational cost than the continuous model. Meanwhile, the ISI-encoded algorithm can effectively eliminate the low complexity sequences. Furthermore, the ISI-encoded chaotic sequences are applied for image encryption to verify the applicability of our encoding algorithm. The main contributions of this article are highlighted as follows. (1) We present a discrete mHR model with hidden chaotic bursting dynamics. (2) We propose an ISI-encoded algorithm that can be used to extract the chaotic bursting characteristics of the discrete mHR model. (3) Using these ISI-encoded chaotic sequences, we design an image encryption scheme, which has high robustness against various possible attacks.

The remainder of this article is considered as follows. Sect. 2 constructs a discrete mHR model and examines the ISIs of chaotic bursting sequences. Sect. 3 presents an ISI-encoded algorithm and evaluates the performance of four sets of ISI-encoded chaotic sequences. Sect. 4 demonstrates an image encryption application based on the ISI-encoded algorithm. Finally, Sect. 5 concludes the whole article.

2 Discretization of the mHR model

The HR neuron model is used to imitate the typical spiking activity of the action spike voltage generated by a single neuron. Derived from the well-known Hodgkin-Huxley model [17], the simplest 2D HR model was constructed to characterize the periodic spiking behavior of the single neuron [22] and it is modeled by

$$\begin{cases} \dot{x} = y - ax^3 + bx^2 + I, \\ \dot{y} = c - dx^2 - y, \end{cases} \tag{1}$$

where x, y, and I denote the spike voltage, recovery variable related to the spike voltage, and externally excited current, respectively. The four constants a, b, c, and d are generally set as a=1, b=3, c=1, and d=5 [34].

To better simulate the magnetic induction effects on the action spike voltage in biological neurons, a 3D HR model was recently proposed [34]. The mHR model is written by

$$\begin{cases} \dot{x} = y - ax^3 + bx^2 - m\tanh(\varphi)x, \\ \dot{y} = c - dx^2 - y, \\ \dot{\varphi} = -x, \end{cases} \tag{2}$$

in which φ stands for the magnetic flux and m represents the induction strength.

Recently, the continuous neuron models have received special much attention [35–38]. Compared with the continuous neuron models, the discrete neuron models have many advantages such as higher implementation efficiency and lower computational cost [29]. However, they have not been received much attention, yet. To investigate the properties of the discrete neuron models, a 2D discrete HR model was proposed in ref. [39] using the forward Euler method and its complex dynamical behaviors were exhibited by theoretical analyses and numerical simulations.

Using the same discretization technique in ref. [39], we can derive a discrete mHR model from the continuous mHR model in eq. (2). Denote x_n, y_n, and φ_n as the sampling values of variables x, y, and φ at the n-th iteration, respectively. Then the discrete mHR model can be defined as the fol-

lowing equations:

$$\begin{cases} x_{n+1} = x_n + \delta\left[y_n - ax_n^3 + bx_n^2 - m\tanh(\varphi_n)x_n\right], \\ y_{n+1} = y_n + \delta(c - dx_n^2 - y_n), \\ \varphi_{n+1} = \varphi_n - \delta x_n, \end{cases} \tag{3}$$

where δ is the iteration step size. When these parameters are assigned as some typical values, namely a=1, b=3, c=1, and d=5, it is easy to calculate that the discrete mHR model has no fixed point. In this case, the bursting patterns generated by the discrete mHR model are all hidden [40].

Similar to the continuous mHR model, the discrete mHR model can also exhibit hidden chaotic bursting behaviors. To investigate this property, we separately set the iteration step size as δ=0.05 and 0.1, and the induction strength as m=1.1 and 1.4. Thus, four sets of parameters can be obtained and used as representative examples. Under these parameter settings, the discrete mHR model shows the hidden chaotic bursting behaviors. Figure 1 displays four hidden chaotic bursting patterns in the φ-x plane while Figure 2 depicts the related four hidden chaotic bursting sequences of the action spike voltage. By comparing the behaviors shown in Figures 1 and 2 with the behaviors of the continuous mHR model, we can find that the discrete mHR model has similar attractor structures but slightly different dynamic amplitudes. Particularly, when m=1.4, the discrete mHR model can embody hidden chaotic bursting behavior, but the continuous mHR model can only show hidden periodic bursting behavior at this particular parameter, which is shown in ref. [34]. This difference is caused by the iteration step size δ used in eq. (3), which has a great influence on the dynamics of the discrete mHR model [39]. When the δ approaches a relatively small value, the dynamics exhibited by the discrete mHR model are consistent with that by the continuous mHR model.

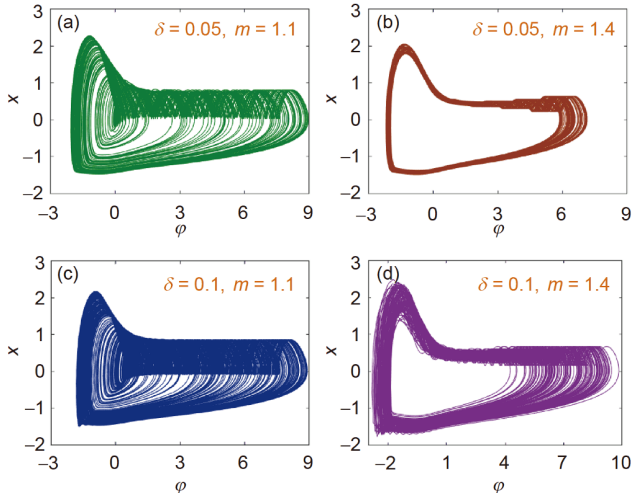

Figure 1 (Color online) Hidden chaotic bursting patterns in the φ-x plane under different parameter settings. (a) δ=0.05, m=1.1; (b) δ=0.05, m=1.4; (c) δ=0.1, m=1.1; (d) δ=0.1, m=1.4.

To demonstrate the bursting dynamics of the discrete mHR model, we investigate the induction strength-dependent bifurcation plots for different integration steps. Taking the iteration steps δ=0.05 and 0.1 as two examples, the bifurcation plots are depicted by calculating the ISI of action spike voltage x [41] and the simulated results are shown in Figure 3. When its induction strength m increases within the range of [0.4, 1.6], the discrete mHR model has pattern transitions from the periodic spiking, first to chaotic spiking, then to chaotic bursting, and finally to periodic bursting patterns. In addition, the simulated results manifest that the

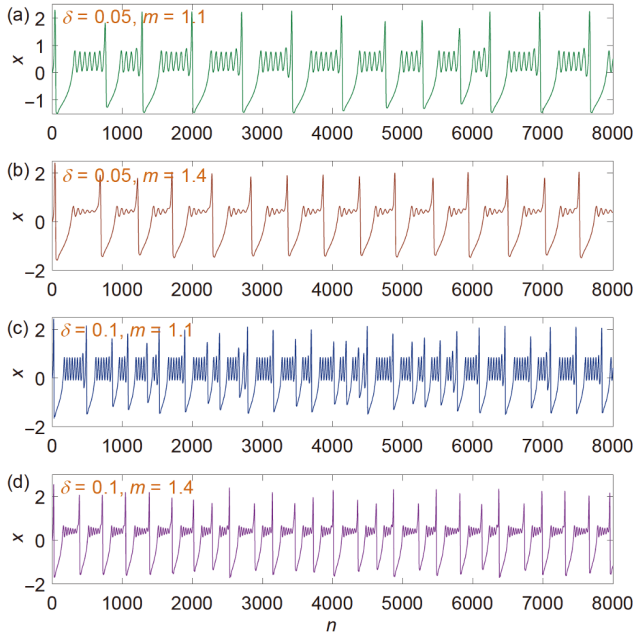

Figure 2 (Color online) Hidden chaotic bursting sequences of the action spike voltage under different parameter settings. (a) δ=0.05, m=1.1; (b) δ=0.05, m=1.4; (c) δ=0.1, m=1.1; (d) δ=0.1, m=1.4.

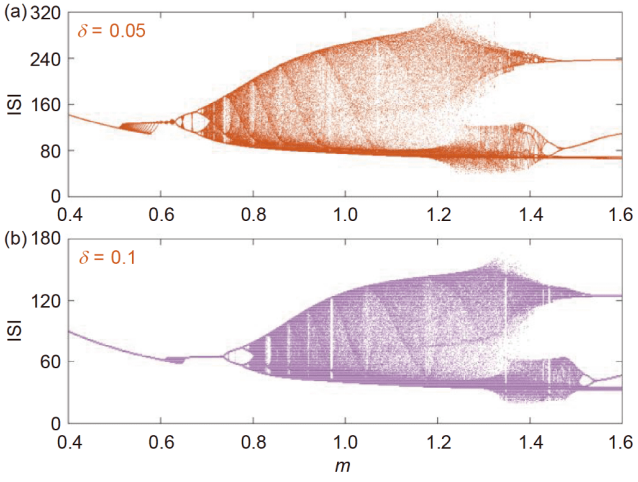

Figure 3 (Color online) The bifurcation behaviors of the ISI of action spike voltage x for different integration steps with the increment of induction strength m. (a) ISI-based bifurcation plot for δ=0.05; (b) ISI-based bifurcation plot for δ=0.1.

iteration step δ has an influence on the pattern evolution of the discrete mHR model. This results in the delay of the parameter-dependent bifurcation structure with the increments of the iteration steps.

3 Novel ISI-encoded algorithm

Discrete neuron models are different from traditional discrete chaotic systems and they have biologically interpretable spiking and bursting patterns of the action spike voltage. To make the action spike voltage sequence suitable for applications, a new chaotic sequence Z is obtained by encoding the ISI of action spike voltage and it is denoted as

$$\begin{aligned} Z_1 &= [S_1 \bmod M + 1] / (M+1), \\ Z_i &= \left[\left(S_i + 2\sum_{j=1}^{i-1} S_j\right) \bmod M + 1\right] / (M+1),\ i = 2, 3, ..., n, \end{aligned} \tag{4}$$

where M=255 is the maximum value of 8 bits and S_i is a positive integer representing the ISI of action spike voltage at the i-th iteration. Therefore, we present a novel ISI-encoded algorithm for generating chaotic sequence. This is the first algorithm for encoding the ISI of chaotic bursting sequences.

With the original chaotic bursting sequences given in Figure 2, a schematic diagram of the presented ISI-encoded algorithm for generating chaotic sequence is demonstrated in Figure 4. Here, we give an example of a chaotic bursting sequence with 9 spikes, whose ISIs are expressed as S_1 to S_9, and the iteration lengths of their ISIs are also given in the figure. Using the presented ISI-encoded algorithm described by eq. (4), the desired encoded chaotic sequences Z_1 to Z_9 can be obtained. Besides, Figure 4 also depicts the change of iteration length between the original chaotic bursting sequence and ISI-encoded chaotic sequence. Thus, to obtain the ISI-encoded chaotic sequences with the desired length, it is necessary to sub-sample the original chaotic bursting sequences with a much longer iteration length.

According to the ISI-encoded algorithm given in eq. (4), four sets of ISI-encoded chaotic sequences for the discrete mHR model are generated and shown in Figure 5. Clearly, these chaotic sequences have lower continuity and higher randomness than the original chaotic bursting sequences given in Figure 2. Moreover, their amplitude magnitudes are controllable and normalized within the interval [0,1], which are beneficial to practical engineering applications.

The performance of four sets of original chaotic bursting sequences and their encoded chaotic sequences can be evaluated using spectral entropy (SE) [42], permutation entropy (PE) [43], and sample entropy (SampEn) [44]. The length of all the sequences to be evaluated is set as 10000. Table 1 lists the calculated performance metrics for the original chaotic bursting sequences in Figure 2 and their encoded chaotic sequences in Figure 5. As can be observed, under the same parameter settings, the encoded chaotic sequences have more excellent performance metrics than the original chaotic bursting sequences.

To intuitively show the complexity affected by the iteration step size δ and induction strength m, we plot the performance metrics of the encoded sequences in the δ-m plane. Figure 6(a) and (b) show the calculation values of the SE and PE, respectively. The bright yellow-red areas stand for the large SE/PE values and the dark black-blue areas stand for the small ones. As can be seen, when m is within the range of [0.8, 1.4], the encoded chaotic sequences can obtain rela-

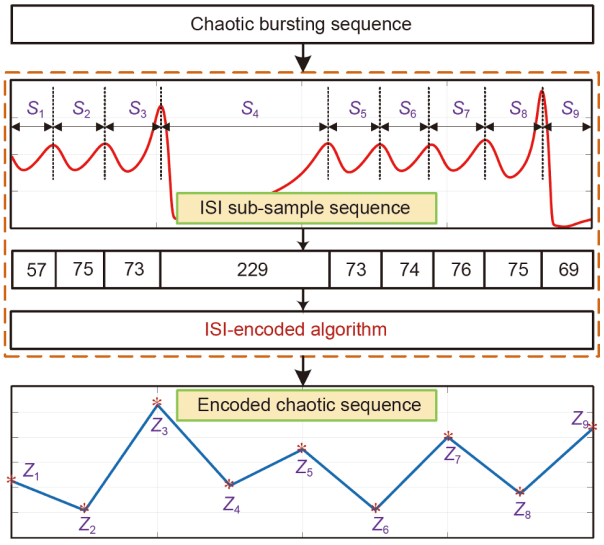

Figure 4 (Color online) Schematic diagram of the presented ISI-encoded algorithm for generating chaotic sequence.

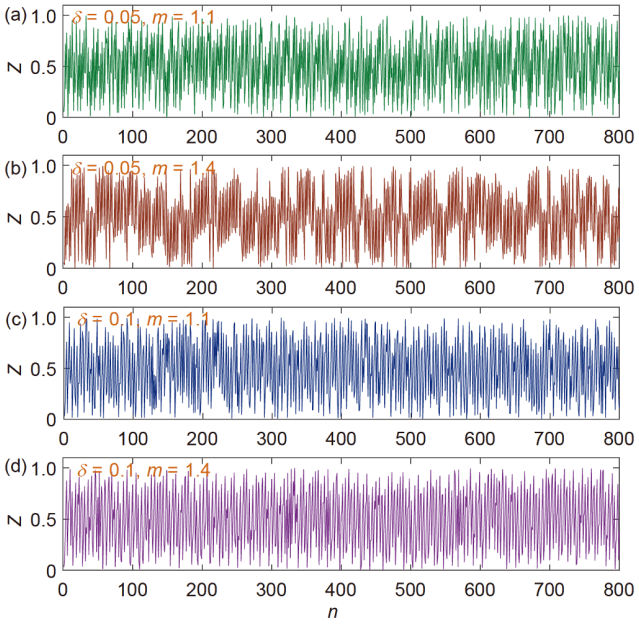

Figure 5 (Color online) Four sets of ISI-encoded sequences calculated by the original bursting sequences under different parameter settings. (a) δ=0.05, m=1.1; (b) δ=0.05, m=1.4; (c) δ=0.1, m=1.1; (d) δ=0.1, m=1.4.

Table 1 Performance evaluations of the bursting and encoded sequences

Parameter settings	Sequence types	SE	PE	SampEn
δ=0.05, m=1.1	Bursting sequence	0.4918	1.0315	0.0915
	Encoded sequence	0.9306	4.6367	0.7464
δ=0.05, m=1.4	Bursting sequence	0.3937	1.0231	0.0387
	Encoded sequence	0.9134	3.5656	0.8936
δ=0.1, m=1.1	Bursting sequence	0.6020	1.4141	0.2018
	Encoded sequence	0.9286	4.6621	0.6827
δ=0.1, m=1.4	Bursting sequence	0.5488	1.5242	0.0927
	Encoded sequence	0.8683	4.0016	0.6210

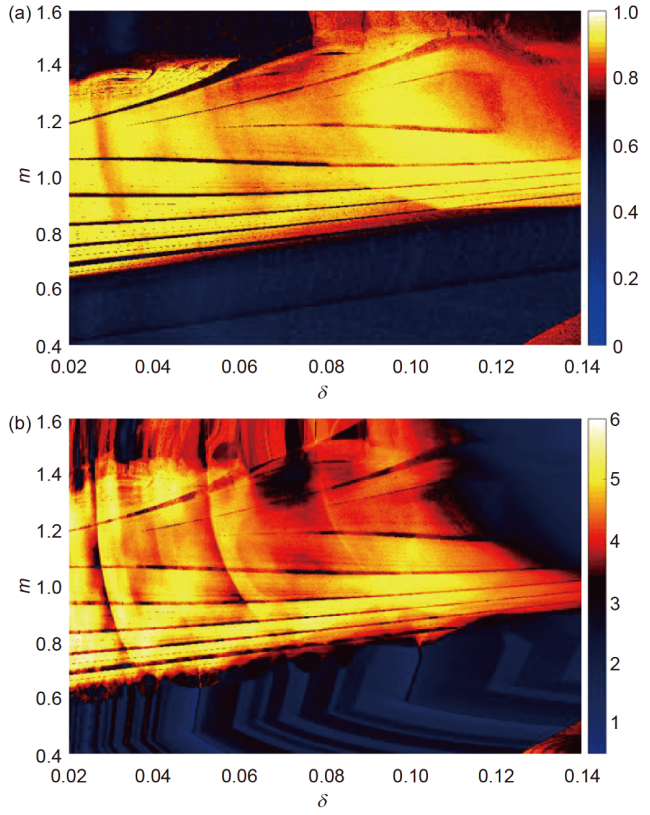

Figure 6 Performance metrics of the encoded sequences in the δ-m plane. (a) SE distribution diagram; (b) PE distribution diagram.

tively high SE/PE values, which allows the encoded chaotic sequences more suitable for data encryption applications.

Furthermore, to confirm the effectiveness of the ISI-encoded algorithm, we apply the presented algorithm to several representative dynamical systems, including two continuous neuron models and two continuous dynamical systems. The two neuron models are the Chay model [19] and memristive Morris-Lecar model [20], and the two continuous dynamical systems are the Lorenz system [45] and Chen system [46]. All these dynamical systems can produce chaotic bursting or spiking sequences under their typical parameters. Then, new encoded chaotic spiking sequences can be generated using the ISI-encoded algorithm. Table 2 shows the performance metrics of the original chaotic sequences and their encoded ones. From the results, one can see that the ISI-encoded algorithm can significantly increase the chaos complexity of chaotic sequences of the aforementioned neuron models and dynamical systems. Thus, the experimentations demonstrate that the ISI-encoded algorithm shows high performance in the continuous neuron models and chaotic systems.

4 Application in image encryption

Recently, various encryption schemes have been consecutively reported to protect the contents of digital images [47–51]. However, these encryption schemes have disadvantages in different aspects [52]. In this section, we introduce an image encryption scheme using the ISI-encoded algorithm and evaluate its advantages in terms of security. The parameters of the discrete mHR model are set as δ=0.1 and m=1.1 and the length of the encoded sequence is determined by the image size.

4.1 Image encryption scheme

The designed image encryption scheme involves the following steps.

Step 1. Read a greyscale plain-image **P** of size $H\times W$ as a 2D matrix.

Step 2. According to the ISI-encoded algorithm given in eq. (4), set the initial conditions (x_0, y_0, φ_0) as the security key and generate the sequence Z of length L by encoding the chaotic bursting sequence of the discrete mHR model. Then, convert Z to 8-bit integer sequences using the equation **XL**=floor($Z\times256$) and obtain the sequence **XL**. Reshape the sequence **XL** to be a 2D chaotic matrix **X** of size $H\times W$.

Step 3. Perform a permutation process to the plain-image **P** to obtain the permuted image matrix **P′** and the detailed operation of the permutation process is given in Algorithm 1. Afterward, transform the 2D permuted image matrix **P′** into a 1D image pixel sequence **PL′** for diffusion.

Step 4. Transform a greyscale plain-image **P** of size $H\times W$ to a 1D image pixel sequence **PL**=[**PL**(1), **PL**(2), ..., **PL**(L)],

Table 2 Performance comparisons for several representative dynamical systems

Systems with typical parameters	Sequence types	SE	PE	SampEn
Memristive Morris-Lecar neuron	Original sequence	0.4204	0.7170	0.0041
	Encoded sequence	0.9234	5.9827	2.0541
Chay neuron	Original sequence	0.5813	0.7432	0.0047
	Encoded sequence	0.8888	4.4517	2.2759
Lorenz system (a=10, b=8/3, c=28)	Original sequence	0.6474	1.1704	0.1331
	Encoded sequence	0.9265	5.2893	1.5294
Chen system (a=40, b=3, c=28)	Original sequence	0.6306	1.3790	0.2622
	Encoded sequence	0.9330	4.7774	1.4451

Algorithm 1 Permutation process

Input: Plain-image pixel matrix **P** and chaotic matrix **X**.

Output: Permuted image pixel matrix **P′**.

Let **P′**=zeros(H, W)

loc=sort(**X**(1, :)); **P′**(1, :)=**P**(1, loc)

for i=2:H **do**

  s=floor(i+**P**(i−1, :)+mean(**P**(i−1, :))) mod W

  loc=sort(**X**(i, s+1)); **P′**(i, :)=**P**(i, loc)

end for

loc=sort(**X**(:, 1)); **P′**(:, 1)=**P′**(loc, 1)

for j=2:W **do**

  s=floor(j+**P**(:, j−1)+mean(**P**(:, j−1))) mod H

  loc=sort(**X**(s+1, j)); **P′**(:, j)=**P**(loc, j)

end for

in which L=HW.

Step 5. Perform a diffusion process to the permutated image sequence **PL′** to obtain the cipher-image pixel sequence **CL** and the detained operation of the diffusion process is shown in Algorithm 2, where $C1\in\{1, 2, ..., 255\}$, $C2\in\{1, 2, ..., 255\}$, and maxoffset$\in\{1, 2, ..., 255\}$. To further improve the ability to resist the chosen-ciphertext attack, we use a bi-directional diffusion strategy and make the current pixel related to the previous encrypted one.

Step 6. Convert the 1D cipher-image pixel sequence **CL** to a 2D matrix with a size of $H\times W$ to obtain the cipher-image C.

The decryption operations are the inverse action of each step in the encryption operations.

Generally speaking, a good encryption algorithm should have high encryption efficiency. In our proposed encryption scheme, the complexities of Algorithms 1 and 2 are mainly caused by the sorting operations [26]. After computation, we can estimate the complexity of Algorithms 1 and 2 as $O(W^2+H^2)$ and $O(W^2H^2)$, respectively, where W and H are the width and height of the image. Besides, to obtain the actual operation time of these algorithms, we implement them using MATLAB R2015b and test their actual operation time using three different sizes of images. The experimentation results are listed in Table 3. The running environment is as follows:

Algorithm 2 Diffusion process

Input: Permuted-image pixel sequence **PL′** and chaotic sequence **XL**.

Output: Cipher-image pixel sequence **CL**.

Let **CL**=zeros(L, 1), offset1=0, offset2=0

CL(1)=(**PL′**(1)+**XL**(1)+$C$1) mod 256

for i=2:L **do**

  offset1=offset1+**CL**(i−1) mod maxoffset

  s=(i+offset1) mod L

  CL(i)=**PL′**(i)+**XL**(s+1)+**CL**(i−1)

end for

CL(L)=(**CL**(L)+**XL**(L)+$C$2) mod 256

for i=L−1:1

  offset2=offset2+**CL**(i+1) mod maxoffset

  s=(i+offset2) mod L

  CL(i)=(**CL**(i)+**XL**(s+1)+**CL**(i+1)) mod 256

end for

Table 3 Time complexity and operation time (s) of Algorithms 1 and 2 for the image with different sizes

Algorithm	Time complexity	128×128	256×256	512×512
Algorithm 1	$O(W^2+H^2)$	0.0081	0.0098	0.0307
Algorithm 2	$O(W^2H^2)$	0.0240	0.0827	0.3278

Intel (R) Core (TM) I5-7400 CPU@3.00 GHz, 16 GB RAM and Windows 7 operation system.

In our encryption scheme, the key parts are the plaintext-based permutation and bidirectional diffusion. In the permutation process, the permutation vector is related to the average pixel of the previous row/column. In the diffusion process, the choice of the ciphertext has an accumulative offset associated with the previous encrypted pixel, and this can cause the selection of the ciphertext to be globally offset as well. Therefore, our encryption scheme has strong ability to resist the chosen-plaintext attack.

4.2 Experimentations and security analysis

Our experiment sets the size of the tested image as 256×256, the security key as (x_0, y_0, φ_0)=(1, 1, 0), and the constant

parameters as $C1$=5, $C2$=10, and maxoffset=5. The security level of our encryption scheme is analyzed from the aspects of histogram, secret key space, information entropy, correlation coefficient, and image sensitivity.

(1) Histogram analysis

To defend against the statistical attack, a cipher-image with high security level is expected to have equal pixel numbers for each grayscale level. Figure 7 shows the experimentations of our encryption scheme. Figure 7(a)–(c) illustrate the plain-image, cipher-image, and decrypted image of the Lena image, while Figure 7(d)–(f) demonstrate the corresponding histograms of the images in Figure 7(a)–(c). As can be observed, the histogram of the plain-image has many patterns while our encryption algorithm can obtain cipher-image with a uniform distribution histogram. The histogram variance of an image can be used to quantify its pixel distribution and it is calculated by [53]

$$\mathrm{Var}(h)=\frac{1}{G_L^2}\sum_{i=1}^{G_L}\sum_{j=1}^{G_L}\frac{1}{2}\left(h_i-h_j\right)^2, \tag{5}$$

where G_L=256 is the grayscale level and h_i is the number of i-th grayscale level. Table 4 lists the histogram variances of the plain-images and cipher-images for the images Lena, Cameraman, Baboon, and Sailboat. The experimentations clarify that the variance of the cipher-images is substantially reduced, which makes the cipher-images sufficiently resistant to statistical attacks.

(2) Secret key space

A cryptographic algorithm with high security level has a sufficiently large key space and the encryption process is sensitive to any change of its secret key. According to the discussions in ref. [54], the secret key space must not be less than 2^{100} to resist brute force attacks. The key space of our encryption algorithm contains the initial values (x_0, y_0, φ_0) with a precision of 10^{-16}. Thus, it is easy to calculate that the key space of our proposed scheme is larger than 2^{160}, large enough to resist various types of brute force attacks.

To measure the key sensitivity, we tinily change each part of the secret key, shown in Table 5, and observe the encryption and decryption results using these tinily different keys. The original secret key (x_0, y_0, φ_0) is set as K_0=(0, 0, 0). Three tinily different keys are generated as K_1=(10^{-9}, 0, 0), K_2=(0, 10^{-9}, 0), K_3=(0, 0, 10^{-9}). Figure 8 shows the experimentations of secret key sensitivity analysis. One can see, only the correct secret key can totally recover the original image (see Figure 8(a)). With tinily different keys, the decrypted results are noise-like and do not contain any information of the original image (see Figure 8(c)–(e)). So our image encryption scheme is extremely sensitive to its secret key.

Table 4 Histogram variances for different images

Images	Plain-image	Cipher-image	Reduction rate (%)
Lena	36598	235	99.36
Cameraman	99064	239	99.76
Baboon	68447	259	99.62
Sailboat	40100	246	99.39

Table 5 Error keys used in decryption process

Keys	Error of x_0	Error of y_0	Error of φ_0
K_0	0	0	0
K_1	10^{-9}	0	0
K_2	0	10^{-9}	0
K_3	0	0	10^{-9}

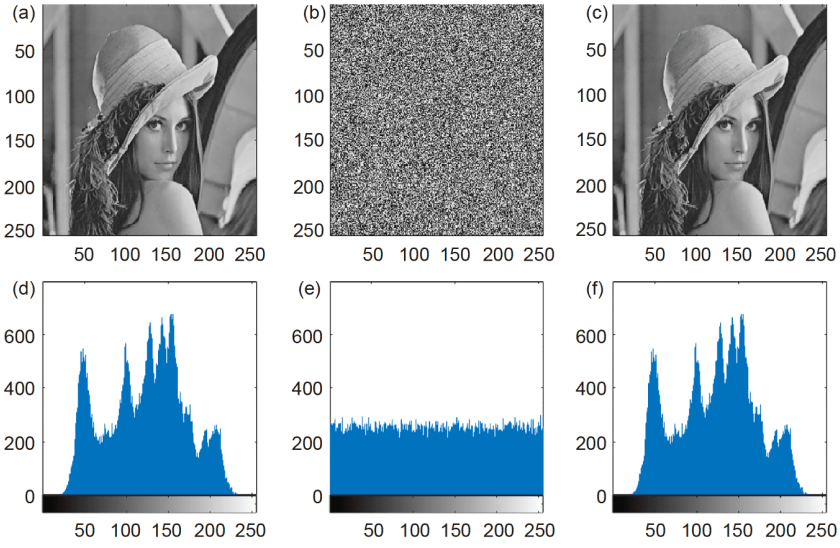

Figure 7 (Color online) Experimentations of our image encryption scheme for image Lena. (a) Plain-image; (b) cipher-image; (c) decrypted image; (d) histogram for the plain-image; (e) histogram for the cipher-image; (f) histogram for the decrypted image.

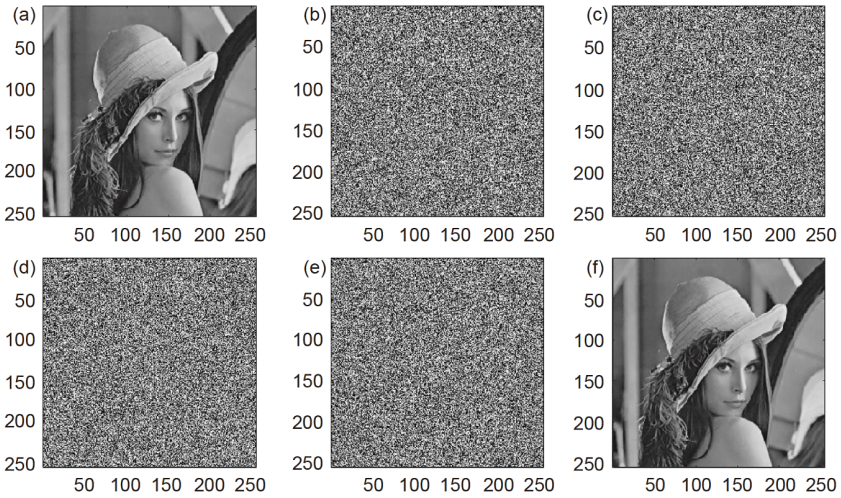

Figure 8 The secret key sensitivity analysis using image Lena. (a) Plain-image; (b) cipher-image using K_0; (c) decrypted image using K_1; (d) decrypted image using K_2; (e) decrypted image using K_3; (f) decrypted image using K_0.

(3) Information entropy

The information entropy is to test the distribution of a signal. It is able to measure the pixel distribution of an image. The information entropy of an image can be calculated as [55]

$$H(m) = \sum_{i=0}^{M-1} p(m_i)\log\frac{1}{p(m_i)}, \tag{6}$$

where M is the total number of possible pixel values, and $p(m_i)$ is the probability of the i-th value. For an 8-bit greyscale image, it has 256 possible pixel values. The theoretically maximum information entropy can be obtained when each possible value has the same probability. Thus, the maximum information entropy for an 8-bit greyscale image is $H(m)$=8. A larger information entropy indicates a more uniform distribution of the image pixels. Table 6 shows the information entropy of different images and their cipher-images by our encryption scheme. It can be viewed that, all the information entropies of these cipher-images verge on the theoretically maximum value 8. This indicates that our image encryption algorithm can generate cipher-images with uniform distribution pixels.

(4) Correlation coefficient

A natural image usually has high correlations among its adjacent pixels. Attackers can predict the image values using these correlations. Thus, an efficient image encryption algorithm should be able to decorrelate these high correlations. The correlation of an image can be calculated using the correlation coefficient and it is described by

$$C_{xy} = \frac{\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{i=1}^{N}x_i\right)\left(y_i - \frac{1}{N}\sum_{i=1}^{N}y_i\right)}{\sqrt{\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{i=1}^{N}x_i\right)^2}\sqrt{\sum_{i=1}^{N}\left(y_i - \frac{1}{N}\sum_{i=1}^{N}y_i\right)^2}}, \tag{7}$$

where x and y are two adjacent pixel sequences in the horizontal, vertical, or diagonal directions, and N is the number of pixels in one pixel sequence. Our experimentation randomly selects 2000 pairs of adjacent pixels from the plain-image and cipher-image. Figure 9 directly plots these adjacent pixel pairs. As can be seen from Figure 9(a)–(c) that the adjacent pixel pairs in the plain-image are most distributed on the diagonal lines of the phase plane. Figure 9(d)–(f) show that the adjacent pixel pairs in the cipher-image are randomly distributed on the whole phase plane. Table 7 [49,50,51,56] lists the correlation coefficients of the plain-image and its cipher-images encrypted by different image encryption schemes. Obviously, the correlation coefficients of the cipher-images are all close to 0, and our proposed scheme can obtain smaller absolute values than other schemes. This indicates that our proposed scheme has a high ability to decorrelate the strong correlation of natural images.

(5) Image sensitivity

An encryption scheme should be sensitive to the plain-image to defense differential attacks. Otherwise, attackers can build the connections between plaintext and ciphertext by choosing some plaintexts to encrypt and analyzing their related ciphertexts. The number of pixel change rate (NPCR) and uniform average change intensity (UACI) are two most commonly employed methods to assess the ability of an image encryption algorithm to resist the differential attacks [57]. The NPCR is described by

Table 6 Image information entropies and their cipher-images by our encryption scheme

Images	Plain-image	Cipher-image
Lena	7.4962	7.9974
Cameraman	7.1052	7.9974
Baboon	7.1352	7.9971
Sailboat	7.5795	7.9973

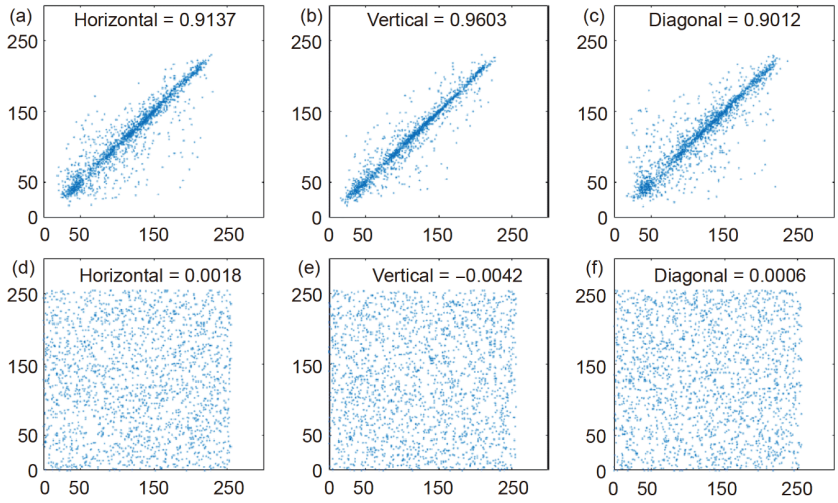

Figure 9 (Color online) Adjacent pixel plots for the image Lena and its cipher-image. The first row plots the adjacent pixel pairs of the plain-image in (a) horizontal, (b) vertical, and (c) diagonal directions; while the second row plots the adjacent pixel pairs of the cipher-image in (d) horizontal, (e) vertical, and (f) diagonal directions.

$$\mathrm{NPCR}(C_1,C_2)=\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}\left|\operatorname{sign}(C_1(i,j)-C_2(i,j))\right|, \quad (8)$$

where sign(·) is the sign function, C_1 and C_2 are two cipher-images obtained by encrypting two plain-images with only one pixel difference, and $H\times W$ represents the size of the image.

Afterward, the UACI can be obtained by

$$\mathrm{UACI}(C_1,C_2)=\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}\frac{|C_1(i,j)-C_2(i,j)|}{Q}, \quad (9)$$

where Q is the maximum allowed pixel value. Generally, for an 8-bit greyscale image, the expected NPCR and UACI are 99.60% and 33.46%, respectively. In our experimentation, we randomly adjust one pixel of the image Lena five times and calculate the related NPCRs and UACIs. Table 8 lists the experimental results, which demonstrate that our image encryption scheme is quite sensitive to the pixel variation.

Table 7 Adjacent pixel correlation coefficients of a plain-image and its cipher-images by different image encryption schemes

Schemes	Horizontal	Vertical	Diagonal
Plain-image	0.9137	0.9603	0.9012
Our scheme	0.0018	−0.0042	0.0006
Ref. [49]	0.0027	0.0488	−0.0090
Ref. [50]	0.0148	−0.0272	0.0130
Ref. [51]	−0.0059	−0.0146	0.0211
Ref. [56]	0.0335	−0.0174	−0.0295

Table 8 NPCRs and UACIs of image Lena with a pixel change in different positions

Position (Row, Col)	NPCR (%)	UACI (%)
(1, 1)	99.61	33.48
(53, 40)	99.63	33.43
(128, 128)	99.61	33.46
(156, 243)	99.63	33.45
(256, 256)	99.62	33.44

5 Conclusion

In this article, we first constructed a discrete mHR model to acquire four sets of hidden chaotic bursting sequences, and then proposed a novel algorithm to obtain the ISI-encoded sequences by encoding the ISIs of these chaotic bursting sequences, and finally applied these ISI-encoded sequences to image encryption application. To satisfy the requirements of the application, we constructed the discrete mHR model via discretizing a continuous 3D mHR neuron model. The numerical simulations show that the integration step size can influence the evolution of the bursting dynamics on the discrete mHR model, which led to a delay in the parameter-dependent bifurcation structure as the integration step size increases. Afterward, we proposed an ISI-encoded algorithm to sample the original bursting sequences. The performance comparisons manifest that the ISI-encoded sequences have higher complexity and better biological interpretability than the original bursting sequences. We also derived the scope of this algorithm by examining a couple of classical chaotic systems, and verified that our algorithm can improve the complexity of the chaotic sequences in continuous chaotic systems. Furthermore, an image encryption scheme with a symmetric key structure was proposed. The experimenta-

tions and security analyses proved that the image encryption scheme is robust to many possible attacks. In addition, the ISI-encoded sequences can also be employed in many other applications, e.g., secure communication [33], deep learning [58], neural text generation [59], and neural machine translation [60], which deserves further study.

This work was supported by the National Natural Science Foundation of China (Grant Nos. 51777016, 51607013 and 62071142).

1 Chen M, Mao S, Liu Y. Big data: A survey. Mobile Netw Appl, 2014, 19: 171–209
2 Yang C, Huang Q, Li Z, et al. Big data and cloud computing: Innovation opportunities and challenges. Int J Digit Earth, 2017, 10: 13–53
3 Yu S D, Liu L L, Wang Z Y, et al. Transferring deep neural networks for the differentiation of mammographic breast lesions. Sci China Tech Sci, 2019, 62: 441–447
4 Su L, Wang L Y, Li K, et al. Automated X-ray recognition of solder bump defects based on ensemble-ELM. Sci China Tech Sci, 2019, 62: 1512–1519
5 Tawalbeh L, Muheidat F, Tawalbeh M, et al. IoT privacy and security: Challenges and solutions. Appl Sci, 2020, 10: 4102
6 Baptista M S. Cryptography with chaos. Phys Lett A, 1998, 240: 50–54
7 Kocarev L. Chaos-based cryptography: A brief overview. IEEE Circ Syst Mag, 2001, 1: 6–21
8 Fadhel S, Shafry M, Farook O. Chaos image encryption methods: A survey study. Bull EEI, 2017, 6: 99–104
9 Hua Z, Zhu Z, Chen Y, et al. Color image encryption using orthogonal Latin squares and a new 2D chaotic system. Nonlinear Dyn, 2021, 104: 4505–4522
10 Bao B C, Zhu Y X, Ma J, et al. Memristive neuron model with an adapting synapse and its hardware experiments. Sci China Tech Sci, 2021, 64: 1107–1117
11 Rajamani V, Kim H, Chua L. Morris-Lecar model of third-order barnacle muscle fiber is made of volatile memristors. Sci China Inf Sci, 2018, 61: 060426
12 Chen M, Qi J W, Wu H G, et al. Bifurcation analyses and hardware experiments for bursting dynamics in non-autonomous memristive FitzHugh-Nagumo circuit. Sci China Tech Sci, 2020, 63: 1035–1044
13 Lu L L, Jia Y, Xu Y, et al. Energy dependence on modes of electric activities of neuron driven by different external mixed signals under electromagnetic induction. Sci China Tech Sci, 2019, 62: 427–440
14 Du L, Cao Z L, Lei Y M, et al. Electrical activities of neural systems exposed to sinusoidal induced electric field with random phase. Sci China Tech Sci, 2019, 62: 1141–1150
15 Lv M, Ma J, Yao Y G, et al. Synchronization and wave propagation in neuronal network under field coupling. Sci China Tech Sci, 2019, 62: 448–457
16 Aihara K, Takabe T, Toyoda M. Chaotic neural networks. Phys Lett A, 1990, 144: 333–340
17 Hodgkin A L, Huxley A F. A quantitative description of membrane current and its application to conduction and excitation in nerve. J Physiol, 1952, 117: 500–544
18 Bao H, Liu W, Chen M. Hidden extreme multistability and dimensionality reduction analysis for an improved non-autonomous memristive FitzHugh-Nagumo circuit. Nonlinear Dyn, 2019, 96: 1879–1894
19 Xu Q, Tan X, Zhu D, et al. Bifurcations to bursting and spiking in the Chay neuron and their validation in a digital circuit. Chaos Soliton Fract, 2020, 141: 110353
20 Bao H, Zhu D, Liu W, et al. Memristor synapse-based Morris-Lecar model: Bifurcation analyses and FPGA-based validations for periodic and chaotic bursting/spiking firings. Int J Bifurcat Chaos, 2020, 30: 2050045
21 Lin H, Wang C, Sun Y, et al. Firing multistability in a locally active memristive neuron model. Nonlinear Dyn, 2020, 100: 3667–3683
22 Hindmarsh J L, Rose R M. A model of the nerve impulse using two first-order differential equations. Nature, 1982, 296: 162–164
23 Rose R M, Hindmarsh J L. The assembly of ionic currents in a thalamic neuron I. The three-dimensional model. Proc Royal Soc Lond B, 1989, 237: 267–288
24 Tlelo-Cuautle E, Díaz-Muñoz J D, González-Zapata A M, et al. Chaotic image encryption using hopfield and Hindmarsh-Rose neurons implemented on FPGA. Sensors, 2020, 20: 1326
25 Yang Y, Wang L, Duan S, et al. Dynamical analysis and image encryption application of a novel memristive hyperchaotic system. Optics Laser Tech, 2021, 133: 106553
26 Hu G, Li B. Coupling chaotic system based on unit transform and its applications in image encryption. Signal Process, 2021, 178: 107790
27 Khan M, Masood F. A novel chaotic image encryption technique based on multiple discrete dynamical maps. Multimed Tools Appl, 2019, 78: 26203–26222
28 Wang S C, Wang C H, Xu C. An image encryption algorithm based on a hidden attractor chaos system and the Knuth-Durstenfeld algorithm. Optics Lasers Eng, 2020, 128: 105995
29 Hua Z Y, Zhou B H, Zhang Y X, et al. Modular chaotification model with FPGA implementation. Sci China Tech Sci, 2021, doi: 10.1007/s11431-020-1717-1
30 Hua Z, Zhou Y, Huang H. Cosine-transform-based chaotic system for image encryption. Inf Sci, 2019, 480: 403–419
31 Wang X, Guan N, Zhao H, et al. A new image encryption scheme based on coupling map lattices with mixed multi-chaos. Sci Rep, 2020, 10: 9784
32 Zhang Y, Tang Y. A plaintext-related image encryption algorithm based on chaos. Multimed Tools Appl, 2018, 77: 6647–6669
33 Li H, Hua Z, Bao H, et al. Two-dimensional memristive hyperchaotic maps and application in secure communication. IEEE Trans Ind Electron, 2021, doi: 10.1109/TIE.2020.3022539
34 Bao H, Hu A, Liu W, et al. Hidden bursting firings and bifurcation mechanisms in memristive neuron model with threshold electromagnetic induction. IEEE Trans Neural Netw Learn Syst, 2020, 31: 502–511
35 Yang Y, Liao X. Filippov Hindmarsh-Rose neuronal model with threshold policy control. IEEE Trans Neural Netw Learn Syst, 2019, 30: 306–311
36 Bao B, Hu A, Bao H, et al. Three-dimensional memristive Hindmarsh-Rose neuron model with hidden coexisting asymmetric behaviors. Complexity, 2018, 2018: 1–11
37 Djeundam S R D, Yamapi R, Kofane T C, et al. Deterministic and stochastic bifurcations in the Hindmarsh-Rose neuronal model. Chaos, 2013, 23: 033125
38 Lakshmanan S, Lim C P, Nahavandi S, et al. Dynamical analysis of the Hindmarsh-Rose neuron with time delays. IEEE Trans Neural Netw Learn Syst, 2017, 28: 1953–1958
39 Li B, He Z. Bifurcations and chaos in a two-dimensional discrete Hindmarsh-Rose model. Nonlinear Dyn, 2014, 76: 697–715
40 Jafari S, Sprott J C, Golpayegani S M R H. Elementary quadratic chaotic flows with no equilibria. Phys Lett A, 2013, 377: 699–702
41 Gu H, Pan B, Chen G, et al. Biological experimental demonstration of bifurcations from bursting to spiking predicted by theoretical models. Nonlinear Dyn, 2014, 78: 391–407
42 Bao H, Chen M, Wu H G, et al. Memristor initial-boosted coexisting plane bifurcations and its extreme multi-stability reconstitution in two-memristor-based dynamical system. Sci China Tech Sci, 2020, 63: 603–613
43 Bandt C, Pompe B. Permutation entropy: A natural complexity measure for time series. Phys Rev Lett, 2002, 88: 174102
44 Richman J S, Moorman J R. Physiological time-series analysis using approximate entropy and sample entropy. Am J Physiol Heart Circ

Physiol, 2000, 278: 2039–2049
45 Lorenz E N. Deterministic nonperiodic flow. J Atmos Sci, 1963, 20: 130–141
46 Chen G, Ueta T. Yet another chaotic attractor. Int J Bifurcat Chaos, 1999, 09: 1465–1466
47 Xu C, Sun J, Wang C. A novel image encryption algorithm based on bit-plane matrix rotation and hyper chaotic systems. Multimed Tools Appl, 2020, 79: 5573–5593
48 Wang B, Zhang B F, Liu X W. An image encryption approach on the basis of a time delay chaotic system. Optik, 2021, 225: 165737
49 Hua Z, Zhu Z, Yi S, et al. Cross-plane colour image encryption using a two-dimensional logistic tent modular map. Inf Sci, 2021, 546: 1063–1083
50 Ye G, Huang X. Spatial image encryption algorithm based on chaotic map and pixel frequency. Sci China Inf Sci, 2018, 61: 058104
51 Pak C, Huang L. A new color image encryption using combination of the 1D chaotic map. Signal Process, 2017, 138: 129–137
52 Preishuber M, Hutter T, Katzenbeisser S, et al. Depreciating motivation and empirical security analysis of chaos-based image and video encryption. IEEE Trans Inform Forensic Secur, 2018, 13: 2137–2150
53 Gan Z, Chai X, Han D, et al. A chaotic image encryption algorithm based on 3-D bit-plane permutation. Neural Comput Applic, 2019, 31: 7111–7130
54 Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifurcat Chaos, 2006, 16: 2129–2151
55 Luo Y, Du M, Liu J. A symmetrical image encryption scheme in wavelet and time domain. Commun Nonlinear Sci Numer Simul, 2015, 20: 447–460
56 Wang N, Li C, Bao H, et al. Generating multi-scroll Chua's attractors via simplified piecewise-linear Chua's diode. IEEE Trans Circ Syst I, 2019, 66: 4767–4779
57 Wu Y, Noonan J P, Agaian S. NPCR and UACI randomness tests for image encryption. Cyber J Multidiscip J Sci Tech, 2011, 1: 31–38
58 Yuan J, Wu Y, Lu X, et al. Recent advances in deep learning based sentiment analysis. Sci China Tech Sci, 2020, 63: 1947–1970
59 Jin H, Cao Y, Wang T, et al. Recent advances of neural text generation: Core tasks, datasets, models and challenges. Sci China Tech Sci, 2020, 63: 1990–2010
60 Zhang J, Zong C. Neural machine translation: Challenges, progress and future. Sci China Tech Sci, 2020, 63: 2028–2050