Neurocomputing 166 (2015) 487–495

Contents lists available at ScienceDirect

Neurocomputing

journal homepage: www.elsevier.com/locate/neucom

# A novel memristive electronic synapse-based Hermite chaotic neural network with application in cryptography

Xinli Shi [a], Shukai Duan [a,*], Lidan Wang [a], Tingwen Huang [b], Chuandong Li [a]

[a] School of Electronic and Information Engineering, Southwest University, Chongqing, China
[b] Department of Electrical and Computer Engineering Texas A&M University, Doha, Qatar

ARTICLE INFO

Article history:
Received 10 August 2014
Received in revised form
30 October 2014
Accepted 5 March 2015
Communicated by He Huang
Available online 28 April 2015

Keywords:
Hermite neural network
Memristor
Chaotic
Encryption
Decryption

ABSTRACT

The memristor is a kind of non-linear passive two-terminal electrical device, which is widely applied in neural networks currently. In this paper, a new synaptic weight update learning rule of Hermite neural network is proposed by combining Hermite polynomials with memristors to build a memristive Hermite chaotic neural network (MHCNN). The chaotic series is generated by the weights of the neural network and chaotic initial value. And ultimately we can obtain the ciphertext by encrypting the plaintext. The use of memristors results in a very special neural network, which can not only change the polynomial in neural network but also achieve the diversity, and the confidentiality of communication is also improved effectively.

## 1. Introduction

The concept of memristor was initially proposed by Chua in 1971 [1]. However, it is until the year of 2008 that HP Lab declared the physical realization of the memristor [2–4]. Since then, wide attention around the world was put on this newly-found element. Several years' researches have witnessed the proposals of a number of new memristor models [5–13]. Because of its unique switch mechanism, natural memory function, continuous input and output characteristics and nanoscale size, the memristor has shown great potential in nonvolatile memory, artificial neural networks and intelligent information etc. and aroused lots of studies in these fields [14–22]. For example, Afifi et al. studied the realization of STDP learning rules based on the pulsing neuromorphic networks with memristor cross-array [14]. Sangho et al. demonstrated that memristors can be used to implement programmable analog circuits, leveraging memristor's fine-resolution programmable resistance without causing perturbations due to the parasitic components [15]. Duan et al. proposed memristor-based resistive random access memory (MRRAM) and verified its effectiveness in storing ASCII characters and gray-scale images in binary format [16]. Duan et al. also studied chaotic circuity [17,27–31] and memristor-based cellular nonlinear/neural network [18]. Wang et al. maked important studies of memristor model and chaos generation [19]. Among all the memristor's properties shown before, the uniqueness of nanoscale size has attracted much attention and interests. Because of that characteristic, a small voltage through it will cause strong change in electric field and then lead to nonlinear ionic drift, which brings about the proposal of nonlinear memristor models and related research.

As is known, the applications of digital information have made great contribution to the rapid development of modern technology and network. The process of gaining information becomes simpler and easier, however, the secrecy of communication calls forth the researchers' attention gradually. In secret communication, cryptography is one of the basic methods, which is about the practice and study of techniques for secure communication in the presence of third parties, in other words, it is about constructing and analyzing protocols that will overcome the influence of adversaries and are related to various aspects in information security, such as data confidentiality, data integrity, authentication and non-repudiation. Meanwhile, chaos, with the special superiority in secure communication, is a seemly irregular inner random motion in a deterministic system and a chaotic system has the properties of complex pseudo-randomness and extreme sensitivity to initial values, therefore it is reasonable to incorporate the conception of chaotic system into communication encryption. Some valuable work has been done [23–26]. In 1990, Carroll firstly built a synchronous chaotic circuit [23]. Several years later, Milanovic proposed the synchronization of chaotic neural networks [24].

* Corresponding author.
E-mail address: duansk@swu.edu.cn (S. Duan).

http://dx.doi.org/10.1016/j.neucom.2015.03.018
0925-2312/© 2015 Elsevier B.V. All rights reserved.

After that, scholars started to apply the chaotic series to cryptology with great enthusiasm. Their research shows that chaotic synchronization encryption algorithm requires keeping highly consistent between the sender and the receiver, otherwise, several problems will be produced, such as parameters' mismatching, inconformity between sent time and received time etc., which makes the scholars embark on the study of asynchronous encryption algorithm.

This paper realizes the Hermite neural network's synaptic weight update by memristors and obtains a special neural network, which not only changes the polynomial in neural network but also achieves diversity. Specifically, we trained the memristive Hermite neural network (MHNN) by using Logistic chaotic series and obtained memristive Hermite chaotic neural network (MHCNN), whose structure is special and meets the requirements of encryption, for the receiver to decrypt the plaintext asynchronously. It must be stated here that encryption and decryption in this paper use the same network which must be sent secretly. Moreover, both the cross-correlation function values between different chaos initial values tend to be zero and the entirely different ciphertexts improve the security of communication.

The rest of the paper is organized as follows. In Section 2, the nonlinear memristor model is introduced. The relationships between the main variables are given by numerical simulation. The changed rate of memristive conductance is described as the synapse weight update rule based on theoretical derivation. In Section 3, memristive Hermite neural network and learning algorithm are described. Section 4 gets a MHCNN by using a chaotic series to train the proposed MHNN. Then the MHCNN is applied to encrypt one paragraph of secretary-general's message on World Water Day in 2013. Section 5 uses another memristor model with forgetting effects to build a memristive Hermite neural network, which is applied to encrypt the same plaintext. The results under different memristor models are compared. Finally, the conclusions are given in Section 6.

## 2. The memristive electronic synapse

The physical model of the memristor consists of a two-layer thin film of $TiO_2$ sandwiched between two platinum electrodes. One of the layers is a thin film of $TiO_2$ which is doped with oxygen vacancies. It is described as $TiO_{2-x}$ and called as doped layer. The other layer is described as $TiO_2$, which is a pure thin film of $TiO_2$ and called as undoped layer. Generally, an external excitation $v(t)$ applied across the memristor may cause oxygen vacancies drift under the action of electric field and the boundary between the two regions would be moved correspondingly with the total memristance changed eventually.

The resistance of the memristor can be calculated [21]

$$M(t)=R_{on}\left(\frac{\omega(t)}{D}\right)+R_{off}\left(1-\frac{\omega(t)}{D}\right) \tag{1}$$

When $\omega=D$ or $\omega=0$, the memristance equals $R_{on}$ or $R_{off}$ respectively. Setting $x=(\omega/D)\in\ [0,1]$, (1) can be described as follows:

$$M(t)=R_{off}+(R_{on}-R_{off})x(t) \tag{2}$$

$$M(0)=R_{off}+(R_{on}-R_{off})x_0,\ \text{when}\ \ t=0. \tag{3}$$

The movement rate of boundary between doped and undoped regions

$$\frac{dx}{dt}=ki(t)f(x),\ \ k=\frac{\mu_v R_{on}}{D^2}. \tag{4}$$

The average ionic mobility is $\mu_v\ \approx 10^{-14}\ m^2\ s^{-1}\ V^{-1}$. Real memristor is a nanoscale device, and enormous electric fields will be produced when it is applied with a small voltage. And it can produce significant nonlinearities in the ionic transport, so a proper window function $f(x)$ on the right side of Eq. (4) is multiplied to simulate the nonlinear ionic drift. In general, classic window functions include Joglekar window function and Biolek window function. Here, we choose Joglekar window function, which can be described as

$$f(x)=1-(2x-1)^{2p}$$

where $p$ is a positive integer. The relationships between the memristor's main variables vary with the change of parameter $p$, which are exhibited in Fig. 1.

The memristor model tends to be linear as the value of parameter $p$ becomes bigger. The nonlinearity of a memristor becomes the most obvious when $p=1$, which simulates the nonlinear behaviors of memristors better than other values. So we choose the window function of $p=1$.

$$f(x)=4x-4x^2 \tag{5}$$

Substitute Eq. (5) into Eq. (4), and assume that there is no input when $t=0$, $q_0=0$. Finally, $x(t)$ can be described by

$$x(t)=1-\frac{1}{Ae^{4kq(t)}+1} \tag{6}$$

where

$$A=\frac{R_{off}-R_{on}}{R_0-R_{on}}. \tag{7}$$

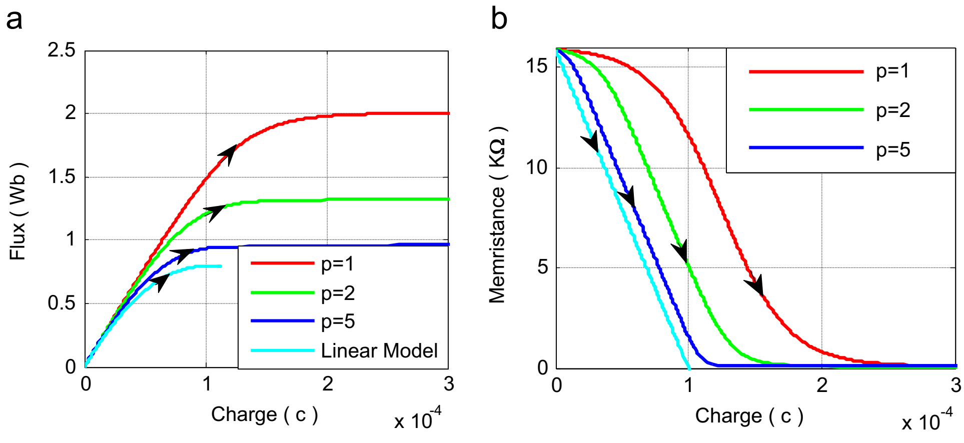

**Fig. 1.** (a) Relationships between the charge and the flux for different values of parameter $p$. (b) Relationships between the charge and the memristance for different values of parameter $p$.