Engineering Applications of Artificial Intelligence 25 (2012) 753–765

Contents lists available at SciVerse ScienceDirect

Engineering Applications of Artificial Intelligence

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

A novel image encryption/decryption scheme based on chaotic neural networks

Nooshin Bigdeli, Yousef Farid *, Karim Afshar

EE Department, Imam Khomeini International University, Daneshgah Blv., Qazvin, Iran

ARTICLE INFO

Article history:
Received 9 March 2011
Received in revised form
10 November 2011
Accepted 6 January 2012
Available online 9 February 2012

Keywords:
Secure communication
Cipher-image
Chaotic neuron layer (CNL)
Permutation neuron layer (PNL)
Tent map

ABSTRACT

This paper presents a novel image encryption/decryption algorithm based on chaotic neural network (CNN). The employed CNN is comprised of two 3-neuron layers called chaotic neuron layer (CNL) and permutation neuron layer (PNL). The values of three RGB (Red, Green and Blue) color components of image constitute inputs of the CNN and three encoded streams are the network outputs. CNL is a chaotic layer where, three well-known chaotic systems i.e. Chua, Lorenz and Lü systems participate in generating weights and biases matrices of this layer corresponding to each pixel RGB features. Besides, a chaotic tent map is employed as the activation function of this layer, and makes the relationship between the plain image and cipher image nonlinear. The output of CNL, i.e. the diffused information, is the input of PNL, where three-dimensional permutation is applied to the diffused information. The overall process is repeated several times to make the encryption process more robust and complex. A 160-bit-long authentication code has been used to generate the initial conditions and the parameters of the CNL and PNL. Some security analysis are given to demonstrate that the key space of the new algorithm is large enough to make brute-force attacks infeasible and simulations have been carried out with detailed numerical analysis, demonstrating the high security of the new image encryption scheme.

1. Introduction

In the recent years, secure private communication methods have aroused the interest of many researchers all over the world. The most general architecture for image encryption is the permutation–diffusion architecture. There are two iterative stages in this kind of image cryptosystems (Chen et al., 2004). The permutation stage changes the position of image pixels but does not alter their values. In the diffusion stage, the pixel values are modified sequentially so that a tiny change in one pixel is spread out to almost all pixels in the whole image. The whole permutation–diffusion round repeats for a number of times so as to achieve a satisfactory level of security. For this architecture, generation of secret keys and control parameter are essential issues in increasing security and complexity of the algorithm.

A good encryption algorithm should be sensitive to the cipher keys, and the key space should be large enough to make brute-force attacks infeasible. In order to achieve such type of security, employing chaotic systems in generating the secret keys and parameters has become one of the most important topics in secure communications (Lian, 2009). In the literature, lots of encryption methods are proposed which are based on using chaotic systems in this era (Wei et al., 2006; Joshi et al., 2009; Tong and Cui, 2008; Tong and Cui, 2009; Wong et al., 2008). For the special properties such as parameters and initial-value sensitivity, ergodicity and quasi-randomness, chaos is used in data protection, widely (Lian, 2009).

Due to their good properties such as high nonlinearity, parameter sensitivity and learning ability, neural networks have been widely used as the other choice for information protection, such as data encryption, data authentication and intrusion detection (Lian, 2009; Chan and Cheng, 2001; Xiao et al., 2005). Neural networks' confusion and diffusion properties have been used to design encryption algorithms, such as the stream ciphers (Chan and Cheng, 2001; Karras and Zorkadis, 2003) or the block ciphers (Lain et al., 2004; Lian, 2009).

As a combination of neural networks and chaos, a chaotic neural network (CNN), has both the characteristic of neural network and chaos. Especially it has more complex dynamic behavior and so, it is expected to have better performance as an image encryption tool. Therefore, such combinations have been employed in some researches as more efficient methods for information protection and information encryption (Lian, 2009). As an instance, in (Lian et al., 2006) a three-layer neural network has been used to construct a hash function. The three

* Corresponding author. Tel./fax: +98 281 8371155.
E-mail addresses: bigdeli@ikiu.ac.ir (N. Bigdeli), yousef.farid@ikiu.ac.ir, y.farid.e.control@gmail.com (Y. Farid), afshar@ikiu.ac.ir (K. Afshar).

0952-1976/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.engappai.2012.01.007

neuron-layers are used to realize data confusion, diffusion and compression. And the multi-block hash mode is presented to support the plaintext with variable length. Socek and Culibrk (Socek and Culibrk, 2005) analyzed a clipped Hopfield neural network-based encryption system for digital images and videos, and pointed how to ensure the security of stream through improving some scheme, such as randomness properties of the generated key-stream. In (Lian, 2009), a CNN structure is proposed for block cipher in which the employed chaotic activation function in the so-called chaotic neuron layer realizes data diffusion and a linear neuron layer realizes data confusion. This structure implies good computing security, but due to constant weight and bias matrices, it seems vulnerable to attacks.

In this paper, the idea in (Lian, 2009) has been generalized to achieve a novel block cipher based on CNN. These cryptosystem is based on a 3-input 3-output neural network structure that comprised of two 3-neuron layers called chaotic neuron layer (CNL) and permutation neuron layer (PNL). The values of three RGB (Red, Green and Blue) color components of image constitute inputs of the CNN and three encoded streams are the network outputs. The weights and biases matrices of CNL are generated by three well-known chaotic systems i.e. Chua, Lorenz and Lü systems. Besides, a chaotic tent map is employed as the activation function of this layer. The output of CNL, i.e. the diffused information, is the input of PNL. In PNL a linear permutation in conjunction with a 2-dimentional nonlinear shuffling are applied to the data to obtain three-dimensional permutation. The overall process is repeated several times to make the encryption process more robust and complex. Simulations show that the suggested image encryption scheme has the advantage of large key space and high security.

The rest of this paper is organized as follows. In Section 2, a short background about the employed chaotic systems and chaotic function and their behavior is presented. The proposed encryption and decryption methods are described in Section 3 and the performance security analysis results of the proposed algorithm is brought in Section 4. In Section 5 the paper is concluded.

2. Preliminary Materials

As stated earlier, in order to implement the chaotic neural network for image encryption, some chaotic systems are used for generating secret keys as well as neural network parameters. The details of implementing this network will be described in Section 3. Beforehand, a short introduction to the employed chaotic systems, the tent map and the Cat map permutation algorithm will be presented in this section.

2.1. The employed chaotic systems

A. **Chua system:** The chaotic Chua system is modeled by the following equations (Botmart and Niamsup, 2007):

$$\begin{aligned}\dot{x}_1 &= a_1(y_1 - f(x_1))\\ \dot{y}_1 &= x_1 - y_1 + z_1\\ \dot{z}_1 &= -b_1 y_1\end{aligned} \tag{1}$$

where a_1, b_1 are constant parameters and $f(x_1) = 2x_1{}^3 - x_1/7$. With $a_1 = 10$, and $b_1 = 100/7$ system has chaotic behavior (Botmart and Niamsup, 2007). The projection of chaotic attractors for a Chua system with $a_1 = 10$, $b_1 = 100/7$ are shown in Fig. 1(a)–(c).

B. **Lorenz system**: The dynamics of chaotic Lorenz system may be represented by the following equations (Li and Yin, 2009):

$$\begin{aligned}\dot{x}_2 &= a_2(y_2 - x_2)\\ \dot{y}_2 &= -x_2 z_2 - y_2 + c_2 x_2\\ \dot{z}_2 &= x_2 y_2 - b_2 z_2\end{aligned} \tag{2}$$

where a_2, b_2, and c_2 are its constant parameters. With $a_2 = 10$, $b_2 = 8/3$, $c_2 = 28$, system has chaotic behavior (Li and Yin, 2009) which has been illustrated in Fig. 1(d)–(f) via the projection of system attractors of its state space trajectories.

C. **Lü system:** The chaotic Lü system model can be described as (Lü et al., 2002):

$$\begin{aligned}\dot{x}_3 &= a_3(y_3 - x_3)\\ \dot{y}_3 &= -x_3 z_3 + c_3 x_3\\ \dot{z}_3 &= x_3 y_3 - b_3 z_3\end{aligned} \tag{3}$$

where a_3,b_3, c_3 are parameters. With $a_3 = 36$,$b_3 = 3$, $c_3 = 20$, system has chaotic behavior (Lü et al., 2002). Trajectories of the state variables of this chaotic system are also shown in Fig. 1(g)–(i).

2.2. The tent map and its properties

The discrete chaotic tent map is a 1-D piecewise-linear map defined by the following equation (Masuda and Aihara, 2002):

$$f_{Tent}(a,x) = \begin{cases} \left\lceil \frac{S}{a} x \right\rceil, & 1 \le x \le a \\ \left\lfloor \frac{S}{S-a}(S-x) \right\rfloor + 1, & a < x \le S \end{cases} \tag{4a}$$

where $a (a \in [1,S])$ is an integer determined by user, and, $\lfloor x \rfloor$ and $\lceil x \rceil$ denotes floor and ceiling of x, respectively. Generally, S is selected according to the plaintext. For an 8-bit image, $S = 256$ is intuitive. The discrete tent map is a one-to-one mapping. In order to illustrate the impact of tent map on a time series, a 16×16 block of Lena image is selected and arranged in the form of time series and then applied as the input to the tent map system. The resulting time series is shown in Fig. 2. As seen, the output of the tent map system has chaotic behavior, while the input of this system has a quasi-periodic behavior.

The inverse of above-mentioned tent map is also defined as (Masuda and Aihara, 2002):

$$f^{-1}{}_{Tent}(a,y) = \begin{cases} \lfloor ay/S \rfloor & \text{if } \left(\lfloor ay/S \rfloor - \lceil ay/S \rceil = -1 \text{ and } \frac{\lfloor ay/S \rfloor}{a} > \frac{-\lceil (a/S-1)y \rceil}{S-a} \right) \text{ or } \lfloor ay/S \rfloor - \lceil ay/S \rceil = 0 \\ \lceil (a/S-1)y + S \rceil & \text{if } \lfloor ay/S \rfloor - \lceil ay/S \rceil = -1 \text{ and } \frac{\lfloor ay/S \rfloor}{a} \le \frac{-\lceil (a/S-1)y \rceil}{S-a} \end{cases} \tag{4b}$$

2.3. CAT map permutation algorithm

In the permutation stage of image cryptosystems, three types of two-dimensional chaotic maps are usually employed: the Standard map, Cat map and generalized Baker map. Cat map is the commonest map used in the literature. Suppose the size of the original grayscale image D is $N \times N$ and the coordinates of the pixel positions are $S_I = \{(x,y) | x,y = 1,2,\ldots,N\}$. Cat map is described as (Xiao et al., 2009):

$$\begin{pmatrix} \hat{x} \\ \hat{y} \end{pmatrix} = Q \begin{pmatrix} x \\ y \end{pmatrix} \bmod(N) = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod(N) \tag{5}$$

where, p and q are positive integers which are called Cat map control parameters and the (x,y) and $(\hat{x},\hat{y})$ are the original and the new positions, respectively. Since $\det(Q) = 1$, the map is area-preserving.