Multimedia Content Protection Based on Chaotic Neural Networks

Shiguo Lian
SAMI Lab, France Telecom R&D Beijing
2 Science South Rd, Haidian District, Beijing, 100080, China
shiguo.lian@orange-ft.com

For chaotic neural network has both chaos’ and neural network’s properties, it is regarded as the most close one to human’s thinking, and has been attracting more and more researchers since the past decade. The properties, such as parameter sensitivity, random similarity, learning ability, etc., make it suitable for information protection, such as data encryption, data authentication, intrusion detection, etc. For its simple structure generates complicated or random sequences, it has been used to design the encryption algorithms that are of lower time-cost than traditional computing-based ones, such as DES, IDEA or AES. These algorithms are suitable for multimedia encryption or authentication.

In this chapter, by investigating chaotic neural networks’ properties, the low-cost cipher and hash function based on chaotic neural networks are proposed and used to encrypt and authenticate images or videos. First, this chapter gives a brief introduction to chaotic neural network based data encryption, including stream ciphers, block ciphers and hash functions. Second, the chapter analyzes chaotic neural networks’ properties that are suitable for data encryption, such as parameter sensitivity, random similarity, diffusion property, confusion property, one-way property, etc. Thirdly, the chapter gives some proposals to design chaotic neural network based cipher or hash function, and uses these ciphers to construct media encryption and authentication methods. In media encryption, the stream cipher and partial encryption method are constructed, which are used to encrypt images or videos. In media authentication, the chaotic neural network based hash function and media authentication method are designed, which can detect the malicious tampering of the media content. The analyses and experiments show the practicability of these encryption algorithms. Finally, conclusions are drawn, and some open issues in this field are presented.

S. Lian: Multimedia Content Protection Based on Chaotic Neural Networks, Studies in Computational Intelligence (SCI) 57, 51–78 (2007)
www.springerlink.com © Springer-Verlag Berlin Heidelberg 2007
2.1 Introduction

In recent years, it is founded that there is chaos phenomenon in human’s brain [1, 2], and chaos theory can be used to explain some abnormal activities in the brain [3]. Thus, chaos dynamics provides a chance for the research in neural networks, such as using neural networks to generate chaos or constructing chaotic neural networks. After knowing the existence of chaos in human’s brain, some scientists propose the theory of chaotic neural networks. The earliest work was done by Aibara [4] and Inoue et al [5, 6] in 1990 and 1991. From then on, chaotic neural networks attract more and more researchers, and are used in more and more applications, such as algorithm optimization, pattern recognition and some other applications. Among these applications, information security is a challenging and interesting one.

Neural networks are used to design data protection schemes because of their complicated and time-varying structures [7]. For example, the ciphers [8, 9] are constructed based on the random sequences generated from the neural networks. For the property of initial-value sensitivity, ergodicity or random similarity, chaos is also introduced to data protection. For example, the block cryptosystem is designed via iterating a chaotic map [10], and the one-way hash is constructed based on the chaotic map with changeable parameters [11]. As a combination of neural networks and chaos, chaotic neural networks (CNN) are expected to be more suitable for data encryption. For example, it is reported [12] that faster synchronization can be obtained by jointing neural network’s synchronization and chaos’ synchronization.

Due to both of the properties, chaotic neural networks are regarded more suitable for data encryption. Till now, various chaotic neural network based encryption algorithms have been reported, which can be classified into two classes: stream cipher and block cipher. The first one uses neural networks to construct stream ciphers, in which, neural network is used to produce pseudo-random sequences. Cauwenberghs [13] made use of VLSI to construct cell neurons that produce the random vectors suitable for data encryption. Chan et al [14] took advantage of Hopfield neural networks’ chaotic property to produce pseudo-random sequence that is used to encrypt plaintexts. Karras et al [15] proposed the method to evaluate the property of the pseudorandom sequence generated from chaotic neural networks, and reported that the sequence generated from chaotic neural networks may be of better performance than the one generated from conventional methods. Caponetto et al [16] designed a secure communication scheme based on cell neural networks. These stream ciphers’ security depends on the sequences’ randomness.

The second one uses neural network to construct block ciphers, which makes use of chaotic neural networks’ properties to encrypt plaintext block by block. Yue et al [17] constructed the image encryption algorithm based on chaotic neural networks, which encrypts several gray images into some binary images. Yen et al [18] used perception neurons to construct a block cipher, in which, the weight matrix and threshold vector are used as keys, and the...