Image Authentication Based on Neural Networks

Shiguo Lian
SAMI Lab, France Telecom R&D Beijing
Beijing, P.R China, 100080
shiguo.lian@orange-ftgroup.com

Abstract

Neural network has been attracting more and more researchers since the past decades. 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. In this paper, by investigating neural networks' properties, the low-cost authentication method based on neural networks is proposed and used to authenticate images or videos. The authentication method can detect whether the images or videos are modified maliciously. Firstly, this chapter introduces neural networks' properties, such as parameter sensitivity, random similarity, diffusion property, confusion property, one-way property, etc. Secondly, the chapter gives an introduction to neural network based protection methods. Thirdly, an image or video authentication scheme based on neural networks is presented, and its performances, including security, robustness and efficiency, are analyzed. Finally, conclusions are drawn, and some open issues in this field are presented.

Keywords neural network, security, encryption, authentication, intrusion detection

1 Introduction

Neural network [1] is used to refer to artificial neural network [2], while has been used to refer to biological neural network [3]. The biological neural network is a network of biological neurons, which is in relation with nervous system. The artificial neural network is composed of artificial neurons, which is the simulation of biological neural network.

According to the learning ability, artificial neural network has been used in artificial intelligence [4]. For example, it is used to guide the robot to play chess, it is used in pattern recognition [5,6], such as pattern classification or object recognition, it is used in function approximation [7], such as time series prediction or modeling, and it is also used in data processing [8,9], such as filtering, clustering, blind signal separation and compression.

Additionally, neural network can be used to model non-linear statistical data, which can model complex relationships between inputs and outputs. Sometimes, it can generate chaos phenomenon [10]. According to this property, it has complex dynamic action, which can be used to protect data content. For example, the random sequence produced by neural network can be used to encrypt data [11], and the neural networks that generate chaos phenomenon can be used in secret communication [12].

In this chapter, some of neural network's properties suitable for content protection are introduced, some
content protection schemes based on neural network is analyzed, a multimedia authentication scheme based on neural network is proposed together with some evaluation on its performances, and future work is also presented.

The rest of the paper is arranged as follows. In Section 2, some properties of neural network are presented. Some content protection schemes based on these properties are given in Section 3. In Section 4, the multimedia authentication scheme based on neural network is proposed. And its performances are analyzed in Section 5. In Section 6, some open issues in neural network based content protection are presented. And the conclusions are drawn in Section 7.

2 Neural Network’s Properties Suitable for Content Protection

2.1 Learning Ability

Neural network has the possibility of learning. Given a specific task to solve and a class of functions, neural network can use a set of observations to solve the task in an optimal sense. Generally, according to the learning task, neural network's learning ability can be classified into three categories, i.e., supervised learning, unsupervised learning and reinforcement learning [13][14][15]. Supervised learning is the learning with a "teacher" in the form of a function that provides continuous feedback on the quality of solutions. These tasks include pattern classification, function approximation and speech or gesture recognition, etc. Unsupervised learning refers to the learning with old knowledge as the prediction reference. These tasks include estimation problem, clustering, compression or filtering. Reinforcement learning refers to the learning with dynamic estimation and decision. These tasks include control tasks, games and other decision making tasks. This property can be used to detect the intruders that enter a secret system without permission.

2.2 One-way Property

One-way property means that it is easy to compute the output from the input while difficult to compute the input from the output. In neural network, there are often more inputs than outputs, which make it difficult to decide the inputs when knowing only the outputs. Taking a simple neuron model for example, the input is composed of n elements \( p_0, p_1, \ldots, p_{n-1} \), while the output is a unique element \( c \). It is defined as

\[
c = f \left( \sum_{j=0}^{n-1} w_j p_j + b \right).
\]  

As can be seen, it is easy to compute \( c \) from \( P = [p_0, p_1, \ldots, p_{n-1}] \), while difficult to compute \( P \) from \( c \). The difficulty is equal to solve a singular equation. Thus, it is a one-way process from the input \( P \) to the output \( c \). This property is often required by hash functions [16][17] that are used to authenticate data's integrity.

2.3 Random Similarity

According to the complex relation between the nodes of neural network, neural network can produce the
sequences with random properties. For example, some neural networks have chaotic dynamics [10,18,19], which produce the output sequence with random properties [20], as shown in Fig. 1. Here, the sequence's autocorrelation is similar to impulse function, while the cross-correlation is near to zero.

![Fig. 1 The sequence produced by a chaotic neural network](image1)

2.4 Parameter Sensitivity

For the neural network that has chaotic dynamics, its output is often sensitive to the inputs or such control parameter as weight [18]. It is caused by the parameter sensitivity of chaos system [21]. Taking the neural network proposed in [10] for example, although there is a slight difference in the initial value, the output changes greatly after more than 20 times of iteration, as shown in Fig. 2. This property makes the initial value suitable for the key that controls the data encryption or decryption.

![Fig. 2 The initial-value sensitivity of a chaotic neural network](image2)
3 Content Protection Based on Neural Networks

3.1 Intrusion Detection

According to the learning ability, neural network has been used in intrusion detection [22]. Intrusion detection is an important technology in network security, which can detect illegal intruders or illegal intrusions. Using neural network's supervised learning, as shown in Fig. 3, the intrusive operations can be distinguished from normal operations [23]. Furthermore, if some classification information is provided beforehand, the intrusive operations can even be classified [24]. The unsupervised learning and reinforcement learning can be used to detect new intrusive operations automatically.

![Intrusion detection based on neural network](image)

**Fig. 3** Intrusion detection based on neural network

3.2 Data Authentication

The one-way property makes neural network a suitable choice for hash function [16][17]. Hash function is a technique for data integrity authentication, which takes a message of arbitrary length as input and produces an output of fixed length. The hash value is often much shorter than the message, which makes it suitable for digital signature or data authentication. As a hash function, it should be easy to compute the hash value from the message, while difficult to compute the message from the hash value. This property is called one-way property. According to this case, neural network may be used to design hash function. Till now, some hash functions based on neural network have been presented [25][26], which were reported to have some advantages compared with existing schemes, such as high time-efficiency or flexible extension. For example, in [25], a hash function based on multi-layer neural network is presented, as shown in Fig. 4, which produces the hash value with the message as input.
3.3 Data Encryption

According to the properties of random similarity and parameter sensitivity, neural network has been used in data encryption [20]. Data encryption is the technology that converts a message into unintelligible form under the control of the key. Till now, two kinds of encryption algorithms have been reported, i.e., stream cipher and block cipher. Stream cipher uses neural network to generate a pseudorandom sequence that modulates a message and uses the parameter as the key. The general architecture is shown in Fig. 5. For example, the ciphers [27,28,29] are constructed based on the random sequences generated from the neural networks. As a combination of neural networks and chaos, chaotic neural networks (CNN) are used in secret communication [30]. Chan et al. [31] took advantage of Hopfield neural networks’ chaotic property to produce pseudo-random sequence that is used to encrypt messages, Karras et al. [32] proposed the method to evaluate the property of the pseudorandom sequence generated from chaotic neural networks, and Caponetto [33] designed a secure communication scheme based on cell neural networks. Block cipher makes use of neural networks’ properties to encrypt a message block by block. In this cipher, the initial value or control parameter acts as the key. For example, Yue et al. [34] constructed the image encryption algorithm based on chaotic neural networks, Yen et al. [35] used perception neurons to construct a block cipher, Lian et al. [36] proposed an image cipher based on chaotic neural network, and Yee et al. [37] designed a symmetric block cipher based on the multi-layer perception network.
4 Multimedia Content Authentication Based on Neural Networks

With the development of multimedia technology and network technology, multimedia data are used more and more widely, such as digital camera, video conference, video-on-demand, audio broadcasting, etc. These applications are in relation with human’s activities in commerce, life, education, politics or even military. Thus, the security of multimedia content becomes urgent. For example, an image may be distributed from one person to another without control over Internet. During the distribution, the image's content may be tampered maliciously. For example, the person in an image is replaced by another one, an object in the image is removed, or some new objects are added to the image. To tell whether the image is tampered or not, multimedia content authentication technique [38,39] is invented, which generates authentication code from the original image, compare it with the new code generated from the received image, and tell the authentication result.

Based on the one-way property and learning ability of neural network, the multimedia content authentication scheme based on neural network is presented. In the following content, the scheme is described in detail, and its performances are also evaluated.

4.1 Architecture of the Proposed Scheme

The proposed multimedia content authentication scheme is shown in Fig. 6. Here, the media data, original authentication code and key are used to feed a neural network, which produces a secret parameter. Compared with media data, the secret parameter is of small size. Then, the secret parameter and the key are stored or transmitted in a secure way, while the media data are distributed freely. During distribution, media data may be tampered maliciously.

In authentication, the received media data, secret parameter and key are used to feed the same neural network, which produces the computed authentication code. By comparing the original authentication code and the computed one, the authentication result is produced. That is, if there is only slight difference between them, then the multimedia data are not tampered, otherwise, they are tampered. To authenticate multimedia data successfully, two conditions are required. Firstly, the secret parameter and key are correct. Secondly, the received media data are same to or not very different from the original media data.
4.2 The Scheme Based on a Simple Neuron

Based on a simple neural network, a practical content authentication scheme is proposed, as shown in Fig. 7(a). In this scheme, media data are partitioned into blocks, and each bit of the authentication code corresponds to a block and a simple neuron. For each simple neuron, a code bit \( s (s=0 \text{ or } 1) \) and the media block composed of \( n \) pixels act as the input and control parameter. The pixels of a media block are normalized into the pixels \( p_0, p_1, \ldots, p_{n-1} \) ranging in \([-1,1]\) by subtracting the mean and dividing the maximal amplitude. The random sequence \( w_0, w_1, \ldots, w_{n-1} \) \((w_i \in [0,1], i=0,1,\ldots,n-1)\) is generated by a random number generator with \( K \) as the random seed. The received media block is \( p'_0, p'_1, \ldots, p'_{n-1} \), and the detected watermark bit is \( s' \). The simple neuron shown in Fig. 7(b) is denoted by

\[
\begin{align*}
\text{Neural network} & \quad \left\{ \begin{array}{l}
\text{Random number generator} \quad W_0, W_1, \ldots, W_{n-1} \\
\text{K}
\end{array} \right. \\
& \quad \left\{ \begin{array}{l}
s \quad \rightarrow \quad b \\
\text{Neural network} \quad \left\{ \begin{array}{l}
\text{Random number generator} \quad W_0, W_1, \ldots, W_{n-1} \\
\text{K}
\end{array} \right. \\
& \quad \left\{ \begin{array}{l}
p'_0, p'_1, \ldots, p'_{n-1} \\
s'
\end{array} \right.
\end{align*}
\]
Fig. 7 The proposed practical scheme based on neural network

\[ s = f(\sum_{j=0}^{n-1} w_j p_j + b) = \text{Sign}(\sum_{j=0}^{n-1} w_j p_j + b) = \begin{cases} 
1, & \sum_{j=0}^{n-1} w_j p_j + b > 0 \\
0, & \sum_{j=0}^{n-1} w_j p_j + b \leq 0
\end{cases} \quad (2) \]

4.3 Generation of Secret Parameter

To compute the secret parameter, the neuron layer is fed by the parameters \( p_0, p_1, \ldots, p_{n-1}, w_0, w_1, \ldots, w_{n-1} \) and \( s \). That is, by solving Eq. (2), we get

\[ b = \begin{cases} 
> -\sum_{j=0}^{n-1} w_j p_j, & s = 1 \\
\leq -\sum_{j=0}^{n-1} w_j p_j, & s = 0
\end{cases} \quad (3) \]

Set \( T \) as an adjustable parameter ranging in \([0, 0.5]\). Then, we get

\[ b = \begin{cases} 
T - \sum_{j=0}^{n-1} w_j p_j, & s = 1 \\
-T - \sum_{j=0}^{n-1} w_j p_j, & s = 0
\end{cases} \quad (4) \]

Here, \( T \) can be fixed or determined by experiments. For \( T \) is in relation with the robustness of the authentication system, it will be discussed in detail in Section 5.

4.4 Content Authentication

As shown in Fig. 7(a), the new authentication code is computed according to the following method.
Here, the neuron layer is fed by the parameters \( p'_0, p'_1, \ldots, p'_{n-1}, w_0, w_1, \ldots, w_{n-1} \) and \( b \). That is, to get \( s' \) from Eq. (5). It is straightforward.

Thus, if the media data \( p'_j \) (\( j=0,1,\ldots,n-1 \)) is not changed compared with \( p_j \) (\( j=0,1,\ldots,n-1 \)), then it is easy to get

\[
s' = \begin{cases} 1, & T > 0 \\ 0, & -T \leq 0 \end{cases}
\]  

Thus, the authentication code can be extracted correctly.

Otherwise, the media data are changed, and the authentication code is determined by

\[
s' = \begin{cases} 1, & T + (\sum_{j=0}^{n-1} w_j p'_j - \sum_{j=0}^{n-1} w_j p_j) > 0 \\ 0, & -T + (\sum_{j=0}^{n-1} w_j p'_j - \sum_{j=0}^{n-1} w_j p_j) \leq 0 \end{cases}
\]  

In this case, the authentication code is determined by the change. If the change is smaller than \( T \), the authentication code can still be computed correctly. Otherwise, the wrong code will be computed.

5 Performance Evaluation

5.1 Security

In the proposed scheme, the authentication code is computed under the control of the key and the secret parameter. Without them, it is difficult to compute the authentication code correctly. Thus, the security of the proposed scheme depends on two aspects, i.e., the secrecy of the key and parameter, and the brute-force attack (when not knowing the key and the parameter).

In the first aspect, the key \( K \) and the parameter \( b \) can be transmitted over a secret channel. For example, they are encrypted with such ciphers as DES, RSA, AES, etc [20]. These ciphers keep the security of the key and the parameter.

In the second aspect, for the attackers not knowing the key and the parameter, they must guess the parameters \( w_0, w_1, \ldots, w_{n-1}, b \) or solve the following equation.

\[
s' = \begin{cases} 1, & \sum_{j=0}^{n-1} w_j p'_j + b > 0 \\ 0, & \sum_{j=0}^{n-1} w_j p'_j + b \leq 0 \end{cases}
\]  

However, for not knowing these parameters, it is not easier than guess the authentication bit directly with
brute-force attack. For example, if \( N \) bits are computed from an image, then the brute-force space is \( 2^N \). It is difficult when \( N \) is big enough, e.g., no smaller than 64.

5.2 Sensitivity to Malicious Tampering

The authentication scheme can detect the regions tampered by malicious operations. An example is shown in Fig. 8. Here, Fig. 8(a), (b) and (c) show the original images, tampered images and detected tampered regions, respectively. In Fig. 8(c), the black area denotes the tampered regions.

![Figure 8 Detection of malicious tampering](image)

5.3 Robustness

The authentication code can be computed correctly when media data are not changed during transmission or distribution. The proposed scheme is robust to some operations applied to the media data, such as adding noise or recompression. The performance depends on two parameters, i.e., the adjustable parameter \( T \) and the block size \( B \).

5.3.1 Robustness against noise

The block size affects the correct detection rate (Cdr) when the media data are changed with some operations. Generally, the bigger the size is, the higher the correct detection rate is. Fig. 9(a) shows the relation between the block size and the correct detection rate. Here, Gaussian noise is added to the media data, \( B \) varies from 4 to 32, and \( T=0.2 \). As can be seen, for the same noise strength, the correct detection rate increases with the rise of the block size.
The adjustable parameter $T$ also affects the correct detection rate ($C_{dr}$) in the condition of adding noise. Fig. 9(b) shows the relation between $T$ and $C_{dr}$. Here, Gaussian noise is added, $T$ varies from 0 to 0.3, and $B=8$. As can be seen, the correct detection rate increases with $T$ when the noise strength is certain. When $B\geq 8$, $T\geq 0.2$ and Gaussian noise’s variance is no bigger than 0.01, the correct detection rate is often no smaller than 80%.

![Graph](image_url)

(a) Relation between $C_{dr}$ and $B$

![Graph](image_url)

(b) Relation between $C_{dr}$ and $T$

**Fig. 9** Robustness against adding noise
5.3.2 Robustness against recompression

The proposed scheme is robust against JPEG compression. The correct detection rate (Cdr) is in relation with the adjustable parameter T. Fig. 10 shows the relation between Cdr and T. Here, the image is Lena 512*512, the compression quality ranges from 100 to 40, T ranges from 0 to 0.3, and B=8. As can be seen, Cdr increases with the rise of T if the compression quality is certain. When T\geq0.2 and the compression quality is no smaller than 70, the correct detection rate is no smaller than 85%.

![Fig. 10 Robustness against JPEG Compression](image)

5.3.3 Some means to improve the robustness

According to the experiments and analyses, the following means can be adopted to improve the correct detection rate when the media data are operated. The first one is to increase T, the second one is to enlarge the block size, and the third one is to compute the authentication bit repeatedly. It should be noted that the detection precision will be reduced by using the latter two means.

5.4 Time Efficiency

The computing or authentication process can be implemented efficiently. Table 1 shows the results on some images. Here, the computer is of 1.7GHz CUP and 256M RAM, and the computing/authentication program is implemented in C code. As can be seen, the computing/authentication time is no more than 1 second, when the image’s size is no bigger than 512×512. Considering that each block can be computed or authenticated independently, neural networks’ parallel properties can be used to improve the efficiency of the implementation.
6 Open Issues

Using neural network to protect data content is straightforward in some extent because of neural network's properties. For example, the learning ability enables neural network to know and identify intrusion operations, and the learning ability enables neural network to understand or even remember multimedia content. However, for artificial neural network's intelligence is much lower than biological neural network, there are still some open issues in the engineering applications, especially, in content protection.

Firstly, neural network has some properties suitable for content protection, but which property is suitable for which protection scheme is still uncertain. In this chapter, only four properties are introduced, including learning ability, one-way property, random similarity and parameter sensitivity. Maybe, several properties are all required by one scheme. It needs the cooperation between both the researchers in neural network and the researchers in content protection.

Secondly, neural network's properties should be investigated before being used in content protection. Not all neural networks are suitable for content protection. Some principles need to be constructed to guide the design of neural network based content protection.

Thirdly, as a content protection scheme, the performances should be evaluated thoroughly before being used in practical applications, which includes the scheme based on neural network. Till now, some means have been proposed to evaluate the new schemes based on neural network [40]. However, the work is far from enough.

Fourthly, using the learning ability to authenticate images is still challenging. It is expected for neural network to learn and remember an image and later to tell whether the tampered copy is illegal or not. Although it is challenging, artificial neural network's development may make it true.

7 Conclusions and Future Work

In this paper, some existing research work in neural network based content protection is firstly introduced, including neural network's properties suitable for content protection and some content protection schemes based on neural network. Then, a multimedia content authentication scheme is proposed, which makes use of neural network's learning ability and one-way property to detect malicious tampering on multimedia content. The performance evaluation shows the scheme's practicality. Furthermore, some open issues in this
research field are presented. Finally, some conclusions are drawn.

References

[1] Abdi, H., Valentin, D., Edelman, B.E. (1999). Neural Networks. Thousand Oaks: Sage.
[2] Anderson, James A. (1995). *An Introduction to Neural Networks*. ISBN 0-262-01144-1.
[3] Arbib, Michael A. (Ed.) (1995). *The Handbook of Brain Theory and Neural Networks*.
[4] Bezdek J. C. On the Relationship between Neural Networks, Pattern Recognition and Intelligence. The International Journal of Approximate Reasoning, 1992, 6(2): 85-107.
[5] Grossberg S. Neural Networks and Neural Intelligence. Cambridge, Mass: MIT Press, 1988.
[6] Hajek P, et al. Uncertain Information Processing Expert Systems. Boca Raton, Florida: CRC Press, 1992.
[7] Dai Q, Chen SC, Zhang BZ. Improved CBP neural network model with applications in time series prediction. NEURAL PROCESSING LETTERS 18 (3): 197-211 DEC 2003.
[8] Y. D. Jou, “Design of real FIR filters with arbitrary magnitude and phase specifications using a neural-based approach,” IEEE Trans. Circuit and Systems-II, vol. 53, no. 11, October 2006.
[9] S. Kulkarni, B. Verma, and M. Blumenstein, 1997, Image Compression using a Direct Solution Method based Neural Network, Proceedings of the Tenth Australian Joint Conference on Artificial Intelligence, Perth, Australia, 114-119.
[10] Gabriele Manganaro, P. Arena, L. Fortuna. Cellular Neural Networks: Chaos, Complexity and VLSI Processing, Springer Series in Advanced Microelectronics, 1999.
[11] Ohira T. Neural network model with delay toward encryption. Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks (IJCNN), Vol.5, pp. 417-421, 2000.
[12] TAO YANG, L.-B. Yang and C.-M. Yang. Application of neural networks to unmasking chaotic secure communication. PHYSICA D 124 (1-3): 248-257 DEC 1 1998.
[13] Costa, F., Frasconi, P., Lombardo, V., and Soda, G. Towards Incremental Parsing of Natural Language using Recursive Neural Networks. Applied Intelligence, 19(1/2):9-25, 2003.
[14] Richard S. Sutton and Andrew G. Barto Reinforcement Learning: An Introduction. MIT Press, Cambridge, MA, 1998.
[15] Mandic, D. & Chambers, J. (2001). *Recurrent Neural Networks for Prediction: Architectures, Learning algorithms and Stability*. Wiley.
[16] Secure Hash Standard. FIPS 180-2, 2002.
[17] R. Rivest: The MD5 Message Digest Algorithm. RFC 1321, 1992.
[18] J. Cao, J. Lu, Adaptive synchronization of neural networks with or without time-varying delays, Chaos, 16(2006), art. no. 013133.
[19] J. Lu, J. Cao, Adaptive complete synchronization of two identical or different chaotic (hyperchaotic) systems with fully unknown parameters, Chaos, 15(2005), art. no. 043901.
[20] Richard A. Mollin. An Introduction to Cryptography. CRC Press, 2006.
[21] Devaney, Robert L. (2003). *An Introduction to Chaotic Dynamical Systems, 2nd ed.*, Westview Press. ISBN 0-8133-4085-3.
[22] Stephen Northcutt, Judy Novak. Network Intrusion Detection: An Analyst's Handbook, 2nd Edition, New Riders Publishing, 2000.
[23] Bivens A, Palagiri C, Smith R, et al. Network-Based Intrusion Detection Using Neural Networks. Proceeding of ANNIE-2002. New York: ASME Press, 2002, 579-584.

[24] Rhodes B, Mahaffey J, Cannady J. Multiple Self-Organizing Maps for Intrusion Detection. Proceedings of the 23rd National Information Systems Security Conference. Baltimore: MD Press, 2000, 32-42.

[25] Lian S., Sun J., Wang Z. Secure Hash Function Based on Neural Network. Neurocomputing, Vol. 69, No. 16-18, 2006.

[26] Lian S., Liu Z., Ren Z., Wang H., “Hash function based on Chaotic Neural Networks,” 2006 IEEE International Symposium on Circuits and Systems (ISCAS 2006), May 21-24, 2006, Kos, Greece, pp. 221-224.

[27] Chan C, Cheng L. Software Generation of Random Number by using Neural Network. 5th ICANNGA, Praugs, Czech Republic, April 2001.

[28] Guo D, Cheng L, Cheng L. A New Symmetric Probabilistic Encryption Scheme Based on Chaotic Attractors of Neural Networks. Applied Intelligence, Volume 10, No. 1, Jan. 1999.

[29] Cauwenberghs G. Delta-sigma cellular automata for analog VLSI random vector generation. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, Vol.46, No.3, March 1999: 240 – 250.

[30] Rachel M, Einat K, Wolfgang K. Public Channel Cryptography by Synchronization of Neural Networks and Chaotic Maps. Physical Review Letters, Vol. 91, No. 11, Sep 12, 2003: 118701/1-118701/4.

[31] Chan C, Cheng L. The convergence properties of a clipped Hopfield network and its application in the design of keystream generator. IEEE Transactions on Neural Networks, Vol. 12, No. 2, pp. 340-348, March 2001.

[32] Karras D, Zorkadis V. On neural network techniques in the secure management of communication systems through improving and quality assessing pseudorandom stream generators. Neural Networks, Vol. 16, No. 5-6, June - July, 2003: 899-905

[33] Caponetto R, Lavorgna M, Occhipinti L. Cellular neural networks in secure transmission applications. Proceedings of the IEEE International Workshop on Cellular Neural Networks and their Applications, 1996: 411-416.

[34] Yue T, Chiang S. A neural network approach for visual cryptography. Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks, 2000, Vol.5, 24-27 July 2000: 494 – 499.

[35] Yen J, Guo J. A Chaotic Neural Network for Signal Encryption/Decryption and Its VLSI Architecture. In: Proc. 10th (Taiwan) VLSI Design/CAD Symposium, (1999) 319-322.

[36] Lian S, Chen G, Cheung A, Wang Z. A Chaotic-Neural-Network-Based Encryption Algorithm for JPEG2000 Encoded Images. 2004 IEEE Symposium on Neural Networks (ISNN2004), Dalian, China, Springer LNCS, 3174, 627-632.

[37] Yee L, Silva D. Application of multilayer perception networks in symmetric block ciphers. Proceedings of the 2002 International Joint Conference on Neural Networks, Vol. 2, 12-17 May 2002: 1455 – 1458.

[38] Lin, C.-Y., Chang, S.-F.: A Robust Image Authentication Method Surviving JPEG Lossy Compression.
In: Proceedings of SPIE Storage and Retrieval of Image/Video Databases, San Jose, Jan 1998.

[39] Fridrich, J., Goljan, M., Du, R.: Invertible Authentication. In: Proceeding of SPIE, Security and Watermarking of Multimedia Contents, San Jose, California, Jan 2001.

[40] Li C, Li S, Zhang D, Chen G. Cryptanalysis of a Chaotic Neural Network Based Multimedia Encryption Scheme. The 2004 Pacific-Rim Conference on Multimedia (PCM2004), Springer LNCS, 3333, 418-425.