ISSN 2229-3531 (Print)
JCIT Vol. 9(6), 75-79 (2018). Periodicity-2-Monthly
ISSN 2455-9997 (Online)

JOURNAL OF COMPUTER & INFORMATION TECHNOLOGY
An International Open Free Access Peer Reviewed Research Journal of Computer Science Engineering & Information Technology
website:- www.compitjournal.org
Estd. 2010

Analytical Study on Artificial Neural Network

KRITI ARYA[1], HARSH KUMAR SINGH[2], MANOJ KUMAR[3] and BHAVANI KANWAR[4]

[1]M.tech (ECE), BRCM College of Engineering and Technology, Bahal (Haryana) (India)
kritikarya16@gmail.com
[2]M.tech (CSE) , BRCM College of Engineering and Technology, Bahal (Haryana) (India)
harsh007chaudhary@gmail.com
[3]Assistant Professor (ECE), BRCM College of Engineering and Technology, Bahal (Haryana), (India)
manojkumar@brcm.edu.in
[4] M. tech (CSE), Shekhawati Instituite of Engineering and Technology, Sikar (Rajasthan), (India)
bhavaninirwan@gmail.com
Email address of Corresponding Author: [1]kritikarya16@gmail.com, [2]harsh007chaudhary@gmail.com
[3]manojkumar@brcm.edu.in, [4]bhavaninirwan@gmail.com
http://dx.doi.org/10.22147/jucit/090602

Acceptance Date 30th December 2018 **Online Publication Date 31st December, 2018**

Abstract

The goal of this study is to be investigate the use of Artificial Neural Networks (ANNs) in several kinds of digital circuits as well as in the field of Cryptography. Cryptography utilizes mathematical techniques for information security. Information security is presently a compulsory component of commercial applications, military communications and also social media implementation. It maintains the privacy that is the core of information security. Any cryptography needs confidentiality, authentication, integrity and non-repudiation from those authorized to have it. Authentication relates to the identification of two parties entering into communication, while integrity addresses the unauthorized variation of an element inserted into the system. Interacting neural networks have been figured diagnostically. At training step two networks receive a common random input vector and learn their mutual output bits. It could also be attractive for us to study the role of fuzzy based Advanced neural network, Genetic algorithms and Fuzzy neural network. The main goal for the use of fuzzy logic in ANN is to test whether fuzzy rule based approach has merits in dealings with the cyber security threats in the system.

Key words: Artificial Neural Networks, Cryptography and soft computing techniques.

Introduction

In current scenario, information security has become an imperative perspective in the universe. Other way, the people have to be assured that the information to be read by only the sender and receiver. The fundamental need to provide security is utilizing cryptography. In our work, we are consolidating neural network and cryptography. Work on artificial neural network has been encouraged right from its inception by the recognition that the human brain computes in an entirely different way from

the conventional digital computer. A Neural Network is a machine that is designed to model the way in which the brain performs a task or function of interest. It can perform complex calculations effortlessly. The brain is a extremely complex, nonlinear and parallel information processing system. It has the capacity to organize its structural constituents, known as neurons, so as to perform certain computations many times faster than the fastest digital computer in existence today. The network is executed by using electronic components or is simulated in software on a digital computer. A neural network is an enormously parallel distributed processor made up of simple processing units, which has a natural propensity for storing experimental knowledge and making it available for utilize. By using the fuzzy logic in Advance Cyber Security System we can develop a system that consists of a rule depository and mechanism to access or run the given rules. The main goal is to protect the network system and also provide warning to the system administrator to be alert from various cyber threats.

Literature Review: Kanter and Kinzel[5] : proposed a new key exchange protocol between two parties using the notion of chaotic synchronization, which makes it possible for two weakly interacting chaotic systems to converge even though each one of them continues to move in a chaotic way. Kinzel and Kanter[13] give there views on interacting neural networks and cryptography in Solid State Physics. Yee and Silva[6] provides various applications of Multilayer Perception Networks in Symmetric Block Ciphers. A prototype symmetric block cipher is proposed. It employs a Multilayer-Perceptron (MLP) Network that decides on the algorithm used for encryption. The MLP Network is in turn dependent on the secret key. Klein *et al.*[3] performed the neural synchronization of two tree parity networks with mutual outputs by means of the hebbian learning rule; weight and bias values were then used as a secret key. Prabakaran *et al.*[10] discuss that the goal of any cryptographic system is the exchange of information among the intended users. We can generate a common secret key using neural networks and cryptography. Prabakaran and Vivekanandan[8] proposed a secret key using neural cryptography, based on synchronization of Tree Parity Machines (TPMs) by mutual learning. Dalkiran and Danis[7] introduced a research paper on Artificial neural network based chaotic generator for cryptology. In this paper, to overcome disadvantages of chaotic systems, the dynamics of Chua's circuit \namely x, y and z were modeled using Artificial Neural Network (ANN). Malik and Singh[4] discuss an inventory model with variable demand for decaying items and soft computing techniques. Shweta and Devesh[11] presented a triple key chaotic neural network for image cryptography. The triple parameters are used to perform the various operations on image so as to scramble the data in particular way which look like random but actually it is in particular sequence. A. Mathur[2] presents an algorithm for data encryption and decryption which is based on ASCII values of characters in the plaintext. This algorithm is used to encrypt data by using ASCII values of the data to be encrypted. The secret used will be modifying o another string and that string is used as a key to encrypt or decrypt the data. Singh and Nandal[1] tell that how neural network cryptography can be used for secret key exchange and for encryption of information with AES. Singh *et al.* (2014) presented a review on inventory control with soft computing techniques.

Cryptography: Cryptography can be characterized as the exchange of data into a mingle code that can be deciphered and sent across a public or private network. Cryptography is the execution, implementation and study of hiding information. It is a critical part of secure communication. Cryptograph not only protects data from robbery or alternation but can be used as well for user authentication.

Cryptography has two core styles of encrypting data:

A. Symmetric encryptions use the same key for encryption and decryption process, and also can be defined as a secret-key, shared-key, and private-key.

B. Asymmetric cryptography uses different encryption keys for encryption and decryption process. In this case an finale user on a network, public or private, has a pair of keys; one for encryption and one for decryption.

These keys can be identified as a public and a private key, which can be shown in below mentioned figure

- **Integrity:** Assuring the receiver that the received message has not been modified in any way from the original.
- **Non-repudiation:** A mechanism to prove that the sender actually sent this message.
- **Authentication:** The process of proving one's identity.
- **Privacy/confidentiality:** It make sure that no one can read the message except the intended receiver

Artificial Neural Network(ANN): Artificial Neural Network is an information processing and modeling system which emulates the learning capacity of biological systems in understanding unknown process or its behavior. Artificial neural network have evolved various generalizations of mathematical models of human cognition or neural biology.

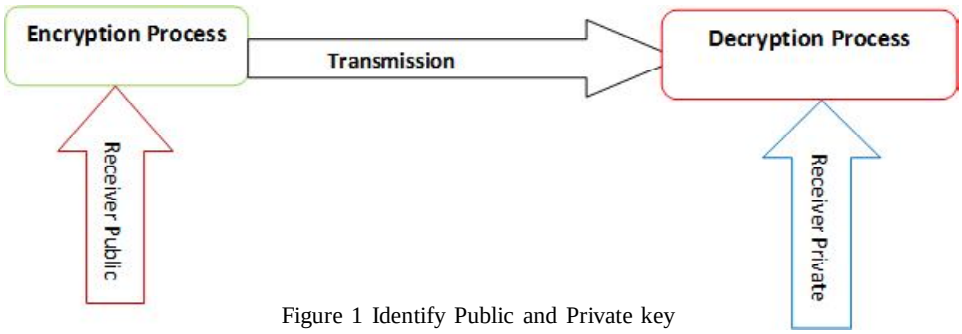

Figure 1 Identify Public and Private key

Based on the assumptions that:

1. Information procures at numerous basic components called neuron.
2. Signals are moved between neurons over connection links.
3. Each connection link has associated weight.
4. Each neuron applies an activation function generally nonlinear to its net input (sum of weighted input signals) to determine its output signal.

An ANN is a network of very simple processors (units), each possibly having a (small amount of) local memory. The units are connected by unidirectional communication channels which transfer numeric data. The units operate on their local data and on the inputs they receive through the connections. The design encouragement is what distinguishes neural networks from other mathematical techniques. A neural network is a processing device, either an algorithm, or actual hardware, whose design was motivated by the design and operations of human brains and components. There are various different types of Neural Networks, each of which has different strengths particular to their applications. The abilities of varying networks can be related to their structure, dynamics and learning methods.

Soft Computing: Soft Computing is a fusion of methodologies that were designed to model and enable solutions to the real world problems which are not modeled, or too difficult to model, mathematically. These problems are typically similar with fuzzy, complex, and dynamical systems, with uncertain parameters. These systems are the only one that can model the real world and are of most interest to the modern science. Soft computing techniques are more powerful and systematic as they provide the feasible and less costly solutions compared to hard computing techniques. It is a multi-disciplinary field. Recent developments in sciences and computers have improved modeling and understanding of situations in all areas of human activity. In effect, the shining example for soft computing is the human mind. With the fuzzy logic based technique, imprecision, doubtful and human oriented knowledge representation is possible, still self learning and generalization of rules can not be possible. There are several methods for soft computing family from which Fuzzy Logic (FL) and Genetic Algorithm (GA) are the most important techniques. Fuzzy logic provides a methodology that enables human reasoning capabilities to be applied to knowledge-based systems. It also provides a mathematical strength to capture the uncertainties associated with human cognitive processes like thinking and reasoning. Fuzzy logic and neural networks have computational properties that make them suitable for particular problems. Development of fuzzy logic was motivated by the need for conceptual framework, since knowledge is by its nature both lexically imprecise and non categorical.

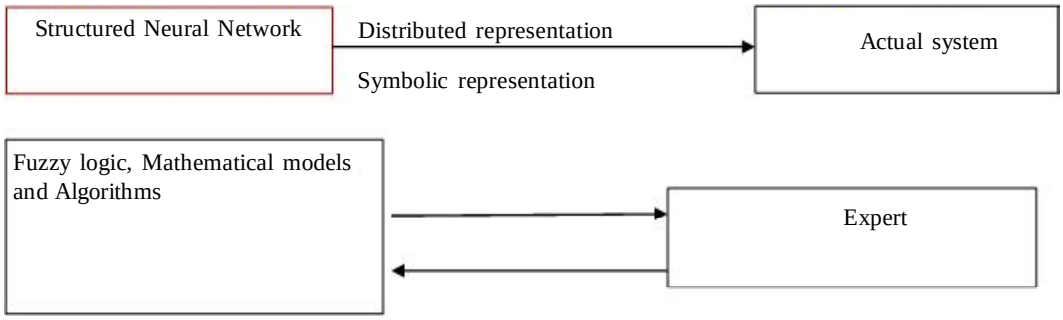

Figure 2 Neural Fuzzy Logic

The Levenberg Marquardt method is used in conjunction with the back propagation method to train a neural network. It has been designed to provide a way to the second order training speed without computing the Hessian matrix in a way similar to that of quasi Newton methods. The cryptographic framework is the exchange of information among the intended users without any leakage of information to others who may have unauthorized access to it. This idea of synchronization by mutual learning can be applied to secret key exchange protocol over a public channel has been studied and generated key is used for encryption and decryption given message. This strategy of symmetric key exchange method based on the fast synchronization of two identically structured Tree Parity Machines (TPMs). The algorithm does not work on extensive numbers and methods from number theory.

Conclusion

In this study we execute encryption and decryption of shift and RSA (Rivest, Shamir and Adleman) cryptosystems, in artificial neural network. The network construction depends simply on the parameters used in the training algorithm and the number of hidden neurons. The main object is to obtain an efficient training pattern with the help of proper algorithm and parameters, such that the errors are minimized with better accuracy. A fuzzy rule based cyber system warns administrators from coming threats. It is used by various commercial and government organizations to develop a more secured knowledgeable and friendly environment. We shell try to analyze the various ANN algorithms present and then try to modify the existing system of cryptographic method to create a more reliable and effective system. The purpose of this study is to overcome these drawbacks, artificial neural networks (ANNs) have been applied to solve many problems and to implement the secure system in digital communication and internet application or any system deal with data transportation and to reject the attacker in uncomplicated and inexpensive hard ware system.

Acknowledgement

We are heartily thankful to Mr. Manoj Kumar (Assistant Professor (ECE), BRCM College of Engineering and Technology, Bahal, Haryana, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject. Lastly, I offer my regards and blessings to all of those who supported me in any respect during the completion of this study work.

References

1. A. Singh, A. Nandal, "Neural Cryptography for Secret Key Exchange and Encryption with AES," International Journal of Advanced Research in Computer Science and Software Engineering, *3(5)*, pp. 376-381 (2013).
2. A. Mathur, "A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms," International Journal on Computer Science and Engineering, *4(9)*, pp. 1650 (2012).
3. E. Klein, R. Mislovaty, I. Kanter, A. Ruttor, W. Kinzel, "Synchronization of neural networks by mutual learning and its application to cryptography," Proc. Advances in Neural Information Processing Systems 17, Neural Information Processing Systems NIPS, (2004).
4. A. K. Malik and Yashveer Singh, "An Inventory Model for Deteriorating Items with Soft Computing Techniques and Variable Demand, International Journal of Soft Computing and Engineering, 317-321 (2011).
5. I. Kanter, W. Kinzel, "Neural cryptography," Proc. 9th International conference on Neural Information Processing, Singapore, (2002).
6. L. P. Yee and D. L. Silva, "Applications of Multilayer Perception Networks in Symmetric Block Ciphers," Proc. 2002 International Joint Conference on Neural Networks, (2002).
7 I. Dalkiran, K. Danis, "Artificial neural network based chaotic generator for cryptology," Turk J Elec Eng & Comp Sci, *18(2)*, pp. 255-240 (2010).
8. N. Prabakaran, P. Vivekanandan, "A New Security on Neural Cryptography with Queries," Int. J. of Advanced Networking and Applications, *2(1)*, pp. 437-444 (2010).
9. Singh *et. al*, "Inventory Control with Soft Computing

Techniques", International Journal of Innovative Technology and Exploring Engineering (IJITEE), (2018).

10. N. Prabakaran, P. Loganathan, and P. Vivekanandan, "Neural Cryptography with Multiple Transfers Functions and Multiple Learning Rule," (2008).
11. B. S. Shweta, D. N. Devesh, "A triple-key Chaotic neural network for cryptography in image processing," International Journal of Engineering Sciences & Emerging Technologies, *2(1)*, pp. 46-50 (2012).
12. Yashveer Singh, Kriti Arya, A. K. Malik, "Inventory Control with Soft Computing Techniques", International Journal of Innovative Technology and Exploring Engineering, 80-82, (2018).
13. TW. Kinzel and I. Kanter, "Interacting neural networks and cryptography," Advances in Solid State Physics, B. Kramer *et al*. ed., Springer, Berlin, *42*, pp. 383, (2002).