INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue2)
Available online at: www.ijariit.com

Analysis and Improved Performance of ANN Based Chaotic Generator

Sona Mishra
M.Tech. Scholar
Electronics and Communication
V.I.T.S. Jabalpur

Amit Mishra
Asst. Professor
Electronics and Communication
V.I.T.S. Jabalpur

Abstract: The main objective of this research paper is to analysis on improved performance of ANN based chaotic generator. We are analyzing the performance of chaotic generator model during encryption and description and produced outcomes compare with earlier published work scenario. In this work Encryption and decryption of binary value has been completed by same value. Chaotic neural network algorithm used for producing random chaotic sequence.[1][2] Produced random chaotic sequence value is the encrypted binary ASCII values of A to Z sequence of original ASCII Code binary value, with same initial parameter. This paper provides review on the use of improved the performance of ANN based chaotic generator and provide high range of security in the field of cryptography.

Keywords: ANN Based Chaotic Generator, Chaotic Neural Network and Cryptography.

I. INTRODUCTION

The ability to build a secure channel is one of the most challenging fields of research in modern communication. Since the secure channel has many applications, in particular for mobile phone, satellite and internet-based communications, there is a need for fast, effective and secure transmission protocols. Nowadays, information security has become an important aspect in every organization. The people have to be assured that the information is to be read by only the sender and the receiver. There comes the role of Cryptography, which ensures the secure transmissions of data.

Cryptography is the exchange of confidential information among the users without leakage of information to a third person. Cryptology was as significant as weapons during the World War II and the Cold War. There were lots of studies to develop robust crypto-systems and to use them in communications. These studies have continued up to now. In spite of all such studies and implementations, this field has some loop holes or drawbacks. Howsoever there is topmost security, sometimes it happens that the data is leaked or stolen or manipulated by wrong hands. Such things can be of major concerns sometimes, especially of national importance or personal importance. To deal with such conflicts in cryptography, researchers have made use of artificial intelligence, a field which uses the concept of self-learning and adaptation by machine itself, i.e. and intelligent or smart machine which can change its behaviour as per the demand of the situation. Artificial Intelligence (AI) is a branch of computer science that emphasis on developing intelligent machines and software using applied logic. It claims the simulation of intelligence of humans by a machine by employing reasoning, learning, communication and manipulation. AI is found to have intense applications in various fields such as medical diagnosis, stock trading, robot control, law and remote sensing. One of the important and our field in AI is Artificial Neural Networks (ANN). An Artificial Neural Network (ANN) is a mathematical model consisting of an interconnected group of artificial neurons motivated by the working of brain. The brain learns from experience and adaptation to environment. Also, inter neuron connection strengths, called weights, are used to store the acquired knowledge. ANN is a nonlinear parallel adaptive system that is used to model variegated relationships between inputs and outputs. The output of a unit is decided by I/O characteristics while the overall working of ANN is determined by its structure and the training algorithm [3].

The chaotic systems are very sensitive to initial conditions. Even a small change in the initial condition can create chaos is the whole system and diverge the final output to a vast extent. Hence it is nearly impossible to define the exact set of initial conditions and generate the desired dynamics in any another machine. But the disadvantage of this method is the fewness of its system parameters. These parameters are the keys for the chaotic cryptosystems and hence it can be seen as a threat to the security of the system. In machine learning and cognitive science, artificial neural networks (ANNs) are a family of statistical learning models motivated by the biological neural networks (the central nervous systems of humans, principally the brain) and hence are used to estimate the functions that can depend on a large number of inputs and are commonly unknown. ANN is

systems of interconnected perception's (neurons) which send messages to each other. The contacts consist of the numeric weights which on the basis of training can be manipulated, making ANN adaptive to the inputs and skilled for learning [4].

II. BACKGROUND AND RELATED WORK

Karam M. Z. Othman , Mohammed H. Al Jammas introduced Implementation of Neural - Cryptographic System Using FPGA. In this work, a Pseudo Random Number Generator (PRNG) based on artificial Neural Networks (ANN) has been designed. This PRNG has been used to design stream cipher system with high statistical randomness properties of its key sequence using ANN. Software simulation has been build using MATLAB to firstly, ensure passing four well-known statistical tests that guaranteed randomness characteristics [5].

Eva Volna, Martin Kotyrba, Vaclav Kocian, Michal Janosek developed a Cryptography based on Neural Network. This paper deals with using neural network in cryptography, e.g. designing such neural network that would be practically used in the area of cryptography. This paper also includes an experimental demonstration [6].

Jason L. Wright, Milos Manic Proposed a research paper on Neural Network Approach to Locating Cryptography in Object Code. In this paper, artificial neural networks are used to classify functional blocks from a disassembled program as being either cryptography related or not. The resulting system, referred to as NNLC (Neural Net for Locating Cryptography) is presented and results of applying this system to various libraries are described [7].

T. SCHMIDT, H. RAHNAMA developed a review of applications of Artificial Neural Networks in Cryptosystems. This paper presents a review of the literature on the use of artificial neutral networks in cryptography. Different neural network based approaches have been categorized based on their applications to different components of cryptosystems such as secret key protocols, visual cryptography, design of random generators, digital watermarking, and steganalysis [8].

III.C ANALYSIS AND IMPROVEMENT

In the previous research work , we have analysis their performance and found that the adopted approaches of perform cryptography and generating secret key is very complex , time consuming and providing limited security during encryption in transmission end or decryption in receiving end. A Problem is arises unprivileged person easily crack secret key and view our confidential transaction or operation data and damage or modify it. Also found that Binary sequences generated from a chaotic system, the biases and weights of neurons are set. The chaotic neural network can be used to encrypt digital signals [1][2]. ANN based Chaotic generator provide high range of security in the field of cryptography .In this paper ANN based chaotic generator is proposed for data encryption and decryption, it produces the outputs according to initial conditions and control parameter .We improve the level of performance of chaos based cryptography using binary value of ASCII Code of A to Z letter instead of decimal value [1]. A plain-text was encrypted and then obtained cipher text was decrypted by using the chaotic dynamics (control parameter and initial point), initial condition and control parameter act as a secret key in the field of cryptography. It is accepted that the initial conditions which were used in the training phase of the ANN model and the system parameters are known by both the transmitter and the receiver. We have adopted ANN based chaotic generator approach from et.al. [9] and increase the level of security from et. al. [2].

Chaos is statistically indistinguishable from randomness and still it is deterministic and not random. Chaotic system will produce different results for same input. It means you cannot predict the working of this system. It changes every time. Therefore this system cannot be break easily. When the weights and biases are determined by chaotic sequence then this network is known as chaotic neural network. Chaotic neural networks offer greatly increase memory capacity. The chaotic neural network can be used to encrypt digital signal. It provides high security. The use of ANN in the field of Cryptography is investigated using two methods. A sequential machine based method for encryption of data is designed. Also, a chaotic neural network for digital signal cryptography is analysed. Better results can be achieved by improvement of code or by use of better training algorithms. Thus, ANN can be used as a new method of encryption and decryption of data [10].

REFERENCES

[1] Sona Mishra, Richa Shrivastava & Abhinav Tiwari - ENHANCE THE PERFORMANCE OF CHAOTIC GENERATOR IN THE FIELD OF CRYPTOGRAPHY: A SECRET KEY GENERATION APPROACH International Journal of Engineering Research-Online A Peer Reviewed International Journal Vol.3., Issue.5., 2015 (Sept.-Oct.).

[2] Nitin Shukla & Abhinav Tiwari University of RGPV Bhopal Madhya Pradesh India - An Empirical Investigation of Using ANN Based N-State Sequential Machine and Chaotic Neural Network in the Field of Cryptography , Global Journal of Computer Science and Technology Neural & Artificial Intelligence Volume 12 Issue 10 Version 1.0 Year 2012 Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350

[3] Mr. Mohana, K. V. K. Venugopal, Sathvik H. N.- Data Security using Genetic Algorithm and Artificial Neural Network

[4] S. Haykin, Neural Networks: A Comprehensive Foundation, Second Ed., New Jersey, Prentice Hall,1999.

[5] KARAM M. Z. OTHMAN , MOHAMMED H. AL JAMMAS - IMPLEMENTATION OF NEURAL - CRYPTOGRAPHIC SYSTEM USING FPGA . journal of Engineering Science and Technology Vol. 6, No. 4 (2011) 411 – 428 © School of Engineering, Taylor's University.

[6] Eva Volna ,Martin Kotyrba ,Vaclav Kocian,Michal Janosek - CRYPTOGRAPHY BASED ON NEURAL NETWORK , Department of Informatics and Computers University of Ostrava Dvorakova 7, Ostrava, 702 00, Czech Republic

[7] Jason L. Wright , Milos Manic - Neural Network Approach to Locating Cryptography in Object Code. Emerging Technologies and Factory Automation INL Laboratory
[8] T. SCHMIDT, dept. of computer science, ryerson university, canada - a review of applications of artificial neural networks in cryptosystems
[9] Ilker DALKIRAN, Kenan DANIS¸MAN - Artificial neural network based chaotic generator for cryptology ,Turk J Elec Eng & Comp Sci, Vol.18, No.2, 2010, © T¨UB˙ITAK
[10] Tope Komal1 , Rane Ashutosh2 , Rahate Roshan3 , Asst. Prof. S.M.Nalawade4 Encryption and Decryption using Artificial Neural Network International Advanced Research Journal in Science, Engineering and Technology Vol. 2, Issue 4, April 2015

