Global Journal of Computer Science and Technology: D
Neural & Artificial Intelligence
Volume 15 Issue 1 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Enhance the Performance of Chaotic Generator in the Filed of Cryptography: A Secret Key Generation Approach

By Sona Mishra, Richa Shrivastava & Abhinav Tiwari
University of R.G.P.V., India

Abstract- The main focus of this research paper is to propose and improvement of the data security using encryption and decryption method in ANN based chaotic generator of original value. The Binary value sequence of ASCII CODE is converted with two initial parameter, and converted value is again decrypted with same initial parameter. In which consists of Binary value of ASCII Code, chaotic neural network algorithm was used for encryption and decryption and it generates the chaotic sequence of random value for each A to Z letter. The generated random value is the encrypted binary ASCII values of A to Z sequence of original ASCII Code binary value, with same initial parameter. For simulation MATLAB software is used. This paper also includes improved experimental results and complete demonstration that ANN Based Chaotic Generator is successfully perform the cryptography.

Keywords : *ann based chaotic generator, chaotic neural network, cryptography.*

GJCST-D Classification : *D.4.6*

Strictly as per the compliance and regulations of:

Enhance the Performance of Chaotic Generator in the Filed of Cryptography: A Secret Key Generation Approach

Sona Mishra [α], Richa Shrivastava [σ] & Abhinav Tiwari [ρ]

Abstract- The main focus of this research paper is to propose and improvement of the data security using encryption and decryption method in ANN based chaotic generator of original value. The Binary value sequence of ASCII CODE is converted with two initial parameter, and converted value is again decrypted with same initial parameter. In which consists of Binary value of ASCII Code, chaotic neural network algorithm was used for encryption and decryption and it generates the chaotic sequence of random value for each A to Z letter. The generated random value is the encrypted binary ASCII values of A to Z sequence of original ASCII Code binary value, with same initial parameter. For simulation MATLAB software is used. This paper also includes improved experimental results and complete demonstration that ANN Based Chaotic Generator is successfully perform the cryptography.

Keywords: ann based chaotic generator, chaotic neural network, cryptography.

I. Introduction

Cryptography is the exchange of information among the users without leakage of information to others. Many public key cryptography are available which are based on number theory but it has the drawback of requirement of large computational power, complexity and time consumption during generation of key [1].

Cryptosystems are commonly used for protecting the integrity, confidentiality, and authenticity of information resources. In addition to meeting standard specifications relating to encryption and decryption, such systems must meet increasingly stringent specifications concerning information security. This is mostly due to the steady demand to protect data and resources from disclosure, to guarantee the authenticity of data, and to protect systems from web based attacks. For these reasons, the development and evaluation of cryptographic algorithms is a challenging task [2].

This paper is study and performance of ANN Based Chaotic Generator in the filed of Cryptography. The rest of the paper is organized as follows: section 2 discusses background and related work in the field of chaotic neural network based cryptography, section 3 discusses implementation section 4 discusses experimental report and test result and finally section 5 discusses conclusion.

Author α σ ρ : VITS Jabalpur, University of R.G.P.V. Bhopal M.P.
e-mails: sona.mishra2909@gmail.com, amit_2440@yahoo.co.in

II. Background and Related Work

Ilker DALKIRAN, Kenan DANIS¸MAN 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 Artficial Neural Network (ANN). ANNs have some distinctive capabilities like learning from experiences, generalizing from a few data and nonlinear relationship between inputs and outputs. The proposed ANN was trained in diffrent structures using different learning algorithms. To train the ANN, 24 different sets including the initial conditions of Chua's circuit were used and each set consisted of about 1800 input-output data. The experimental results showed that a feed-forward Multi Layer Perceptron (MLP), trained with Bayesian Regulation back propagation algorithm, was found as the suitable network structure. As a case study, a message wasfirst encrypted and then decrypted by the chaotic dynamics obtained from the proposed ANN and a comparison was made between the proposed ANN and the numerical solution of Chua's circuit about encrypted and decrypted messages [3].

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.[4].

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 [5].

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[2].

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 [6].

An Empirical Investigation of Using ANN Based N-StateSequential Machine and Chaotic Neural Network in the Field of Cryptography. In this work using two artificial neural networks in the field of cryptography. First One is ANN based n-state sequential machine and Other One is chaotic neural network[10].

a) Problem Definition

In now a day's secret key generation in the field of cryptography continues to be an active research field, as shown by the large number of papers being published. In this previous published research work now we are study their performance and various different way to perform cryptography [9]. We considered chaos based cryptography [3] [10]. but I 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 Unauthorized user or hackers easily guess or predict secret key and view our confidential data and damage or modify it.

b) Proposed Work

In Cryptography, secret key generation scheme was proposed by ANN based Chaotic Generator. ANN based chaotic Generator system used chaotic neural network scheme for encryption and decryption [7]. 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 [10] using binary value of ASCII Code of A to Z letter instead of decimal value. 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 adopted ANN based chaotic generator approach from et.al. [3] and increase the level of security from et. al. [10] and demonstrate by experimental result.

III. Implementation

a) Secret Key Cryptography Through chaotic neural network

A network is called chaotic neural network if its weights and biases are determined by chaotic sequence. In this section we use a algorithm for performing encryption and decryption using chaotic neural network.

ANN based chaotic generator Using CNN scheme for encryption and decryption.

Step 1. The chaotic Logistic map.

$$\mu x(i-1)(1-x(i-1))$$

Set the value of M.

Step 2. The secret key is the control parameter μ and the initial point x (0) of the Logistic map, which are all L-bit binary decimals. Determine parameter μ and initial point x (0).

Step 3. The initialization procedure:

Generate the chaotic sequence x(1), x(2), x(3)… .. x(M) by the formula x(n + 1) = μx(n) (1 – x(n)) and create b(0), b(l), ..., b(8M – 1) from x(l), x(2),..., x(M) by the generating scheme that 0.b(8m – 8)b(8m – 7)….. b (8m – 2) b(8m – l) … is the binary representation of x(m) for m = 1, 2,. . .,M.

Step 4. The encryption procedure:

Depending upon the chaotic sequence a weight matrix and a bias matrix is obtained and the net input is obtained. Then a hard limiter is applied as a transfer function in order to obtain the digital encrypted data. For decryption the same network is used and the same initial value is used to generate the chaotic sequence and for decrypting the data successfully.

For n=0 to M-1

$$g(n) = \Sigma_{i=0}^{7} d_i \; 2^i \Sigma_{i=0}^{7} d_i \; 2^i$$

For i=0 to 7

$$w_{ji}w_{ji} = \begin{cases} 1 & j=i, b(8n+i)=0 \\ -1 & j=i, b(8n+i)=1 \\ 0 & j \neq i \end{cases} \begin{cases} 1 & j=i, b(8n+i)=0 \\ -1 & j=i, b(8n+i)=1 \\ 0 & j \neq i \end{cases}$$

$_J \in \{0,1,2,,4,5,6,7\} \in \{0,1,2,,4,5,6,7\}$

$$\theta_i\theta_{i=} \begin{cases} -\frac{1}{2}\, b(8n+i) = 0 \\ \frac{1}{2}\, b(8n+i) = 1 \end{cases} \begin{cases} -\frac{1}{2}\, b(8n+i) = 0 \\ \frac{1}{2}\, b(8n+i) = 1 \end{cases}$$

End

For i=0 to 7

$$d_i'd_i' = f\ (\textstyle\sum_{j=0}^{7} w_{ji}\, d_i + \theta_i)(\sum_{j=0}^{7} w_{ji}\, d_i + \theta_i)$$

Where f(x) is 1 if x>=0

End

Where f(x) is 1 if x>=0

End

$$g\,'(n) = \textstyle\sum_{i=0}^{7} d_i' 2^i \sum_{i=0}^{7} d_i' 2^i$$

End

g = digital signal of length M and g (n) 0 ≤ M-1 , be the one- byte value of the signal g at position n.

Step 5. The decryption procedure

The decryption procedure is the same as the above one except that the input signal to the decryption Chaotic neural network should be g'(n) and its output signal should be g"(n).

b) ANN based chaotic Generator

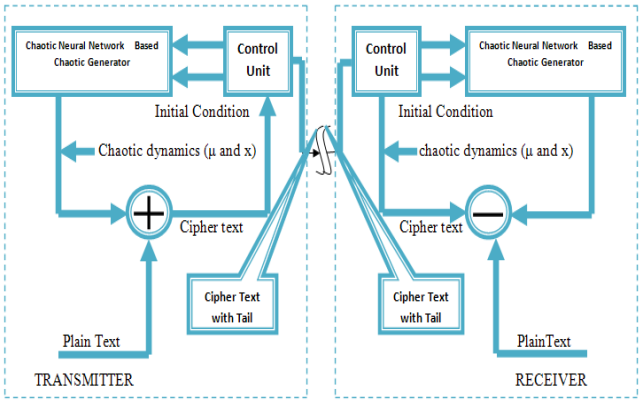

Figure : ANN based chaotic Generator

Working of Encryption and Decryption Using ANN Based Chaotic Generator

1. In the transmitter, software based control unit decides the values of initial conditions and the ANN based chaotic generator produces the outputs according to those initial conditions.
2. In our experiment ASCII Char A to Z Binary value was chosen as a plain-text.
3. The cipher-text is obtained by adding normalized data to the chaotic dynamic (μ and x).
4. A tail which consists of initial condition, and normalization parameters, is tied to the cipher-text by the control unit and then the cipher-text with tail is transmitted.
5. In the decryption phase, the tail is firstly discriminated from the cipher-text and the initial conditions are extracted from the tail by the control unit.
6. Then, the initial conditions are applied to the ANN based chaotic generator and the chaotic dynamic (μ and x) is produced by the generator, initial condition x and control parameter is act as secret key.
7. Finally the plain-text is obtained by subtracting the chaotic dynamic (μ and x) from the cipher-text. The size of cipher-text is equal to the size of plain-text. But tying the tail to the cipher-text enlarges the size of encrypted data. The size of tail is only 8 bytes

IV. Experiment and Test Result

a) Secret Key Cryptography by chaotic neural network

A chaotic network is a neural network whose weights depend on a chaotic sequence. The chaotic sequence highly depends upon the initial conditions and the parameters, x (0) and μ are set. It is very difficult to decrypt an encrypted data correctly by making an exhaustive search without knowing x (0) and μ ().

b) ANN based chaotic Generator

Example- Binary value of ASCII CODE 'A' Encryted with deiffrent Initial Conditions (Values of x (0) and μ ()).

			x(0)= 0.75 μ=3.9		x(0)= 0.85 μ=3.5		x(0)= 0.90 μ=3.2	
		DEC	Bin	DEC	Bin	DEC	Bin	DEC	Bin
A	=	97	01100001	199	11000111	233	11011111204	204	11001100

Decryption with same Initial conditions as below --

x(0)= 0.75 μ=3.9

		DEC	Bin	DEC	Bin
A	=	199	11000111	97	01100001

x(0)= 0.85 μ=3.5

		DEC	Bin	DEC	Bin
A	=	233	11011111	97	01100001

x(0)= 0.90 μ=3.2

		DEC	Bin	DEC	Bin
A	=	204	11001100	97	01100001

It is clear from Example 01. that the binary value sequence of ASCII CODE A is encrypted and decrypted correctly by knowing the exact values of x (0) and μ otherwise we get the wrong value sequences and also cleared that the Binary values of ASCII Code is more strong as compared to decimal values of ASCII Code , no longer pridiction is possible of binanry values. Initial point x (0) and control parameter μ is act as a secret key.

V. Conclusion

It is clear that the binary value sequence of ASCII CODE is encrypted and decrypted correctly by knowing the exact values of x (0) and μ otherwise we get the wrong value sequences .And also clear that the binanry value is more strong enough as compre to decimal values. In this paper we successfully perform encryption and decryption with the help of Chaotic neural network and improve the level of security with the help of using binanry value of ASCII Code instead of decimal values . Network was trained with the help of back propagation algorithm in neural network. Above experiment clear that the Binary value of ASCII CODE is encrypted and its decrypted with same value of parameter , encrypted value is decrypt only correctly by knowing the exact values of x (0) and μ otherwise we get the wrong generated value sequences . ANN based Chaotic generator provide high range of security in the field of cryptography.

References Références Referencias

1. Shweta B. Suryawanshi and Devesh D. Nawgaje- a triple-key chaotic neural network for cryptography in image processing International Journal of Engineering Sciences & Emerging Technologies, April 2012. ISSN: 2231 – 6604 Volume 2, Issue 1, pp: 46-50 ©IJESET .
2. T. SCHMIDT, dept. of computer science, ryerson university, canada - a review of applications of artificial neural networks in cryptosystems.
3. 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
4. Jason L. Wright , Milos Manic - Neural Network Approach to Locating Cryptography in Object Code. Emerging Technologies and Factory Automation INL Laboratory.
5. 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.
6. 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
7. Harpreet Kaur , Tripatjot Singh Panag CRYPTOGRAPHY USING CHAOTIC NEURAL NETWORK International Journal of Information Technology and Knowledge Management July-December 2011, Volume 4, No. 2, pp. 417-422
8. E.C. Laskari , G.C. Meletiou, D.K. Tasoulis , M.N. Vrahatis , Studying the performance of artificial neural networks on problems related to cryptography , Nonlinear Analysis: Real World Applications 7 (2006) 937 – 942
9. Design and Realization of A New Chaotic Neural Encryption/Decryption Network" by Scott Su, Alvin Lin, and Jui-Cheng Yen.
10. Nitin Shukla, Abhinav Tiwari, —An Empirical Investigation of UsingANN Based N-State Sequential Machine and Chaotic Neural Network in the Field of Cryptographyǁ, Global Journal of Computer Science and Technology Neural & Artificial Intelligence, Vol. 12, Issue.10,No. 1,17-26, 2012.