International Journal of Information Technology and Knowledge Management
July-December 2011, Volume 4, No. 2, pp. 417-422

CRYPTOGRAPHY USING CHAOTIC NEURAL NETWORK

Harpreet Kaur[1]& [2]Tripatjot Singh Panag

The goal of any cryptographic system is the exchange of information among the intended users without any leakage of information to others who may have unauthorized access to it. In 1976, Diffie and Hellmann found that a common secret key could be created over public channel accessible to any opponent. Since then many public key cryptography have been presented which are based on number theory and they demand large computational power. Moreover the process involved in generating public key is very complex and time consuming. To overcome this disadvantage, the neural network can be used to generate common secret key. In this particular paper chaotic neural network is proposed for data encryption. Chaos is defined as stochastic behavior occurring in deterministic system [6]. It is known that chaotic systems are non – periodical and also sensitive to initial conditions, system parameters and topological transitivity [4]. The main reason of using chaotic system in cryptography is especially noise like non – periodic dynamics of these systems.

Keywords: Neural Network, Chaos, Cryptography

1. Introduction

Artificial neural network (ANN) takes its name from the network of nerve cells in the human brain. McCulloch and Pitts have developed the neural networks for different computing machines. There are extensive applications of all kinds of ANN in the field of communication, control, instrumentation and forecasting. The ANN is capable of performing on nonlinear input and output systems in the workspace due to its large parallel interconnections between different layers and its nonlinear processing characteristics. An artificial neuron basically consists of a computing element that performs the weighted sum of the input signal and the connecting weight. The sum is added with the bias or threshold and the resultant signal is then processed for nonlinear function of sigmoid or hyperbolic tangent type. The structure of a neural network (NN) may be single layer or it may be multilayer. In multilayer structure, there can be one or many artificial neurons in each layer. In the multilayer neural network or multilayer perceptron (MLP), the input signal propagates through the network in a forward direction, on a layer-by-layer basis [11]. Neural networks have been used in data protection because of complicated and time–varying structures [3, 5, 8]. For example multilayer perception networks are used to construct block cipher [8] and the cellular and clipped Hopfield neural network are used to construct the stream ciphers [3, 5].

[1]Asstt. Professor, Department of Electronics and Communication Engineering, NWIET, Moga
[2]Asstt. Professor, Department of Electronics and Communication Engineering, B.B.S.B.E.C Fatehgarh Sahib
E-mail : [1]harpreetkaur29@gmail.com, [2]panagtripat@gmail.com

2. Chaos

There is no generally accepted definition of chaos. From a practical point of view chaos can be defined as bounded steady-state behavior that is not an equilibrium point, not periodic, and not quasi-periodic. The key question is, "If it is not any of these, then what is it?" To start the discussion, several examples of chaotic trajectories are shown here. It is evident from Fig. 1 is that the trajectories are, indeed, bounded, that they are not periodic, and that they don't have the uniform distribution characteristic of quasi-periodic solutions. A chaotic spectrum is not composed solely of discrete frequencies, but has a continuous, broad-band nature. The noise-like spectrum is characteristic of chaotic systems. The limit set for chaotic behavior is not a simple geometrical object like a circle or a torus, but is related to fractals and Cantor sets. Another property of chaotic systems is sensitive dependence on initial conditions, given two different initial conditions arbitrarily close to one another, the trajectories emanating from these points diverge at a rate characteristic of the system until, for all practical purposes, they are uncorrelated.

2.1 Chaotic Neural Network

A network is called chaotic neural network if its weights and biases are determined by chaotic sequence. In this section, we consider the following Hopfield neural networks which exhibit chaotic phenomenon.

$$\dot{x}(t) = -Cx(t) + Af(x(t)) + Bf(x(t-\tau(t)) + I, \quad (1)$$

$$\dot{x}_i(t) = -c_i x_i(t) + \sum_{j=1}^{n} a_{ij} f_j\left(x_j(t)\right) + \sum_{j=1}^{n} b_{ij} f_j\left(x_j(t-\tau_{ij}(t))\right) + I_i,\ i = 1, 2, ..., n,$$

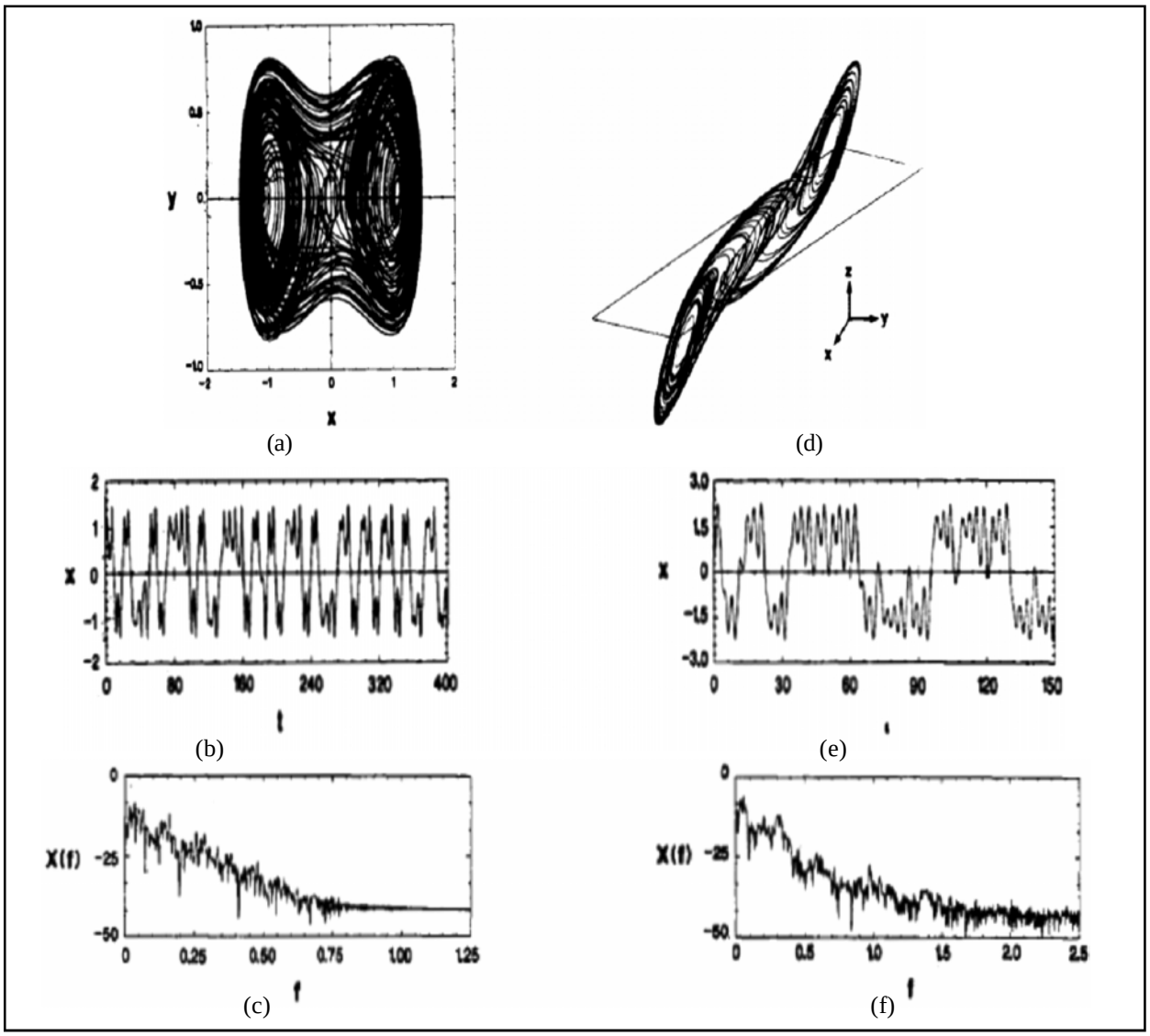

Fig.1 : Chaotic Trajectories

(a) 2nd order non autonomous system

(b) Time waveform of 1st component of 2nd order non autonomous system

(c) Spectrum of 1st component of (a)

(d) 3rd order autonomous system

(e) Time waveform of 1st component of 3rd order non autonomous system

(f) Spectrum of 1st component of (c)

where n denotes the number of units in a neural network, $x(t) = (x_1(t), x_2(t), \ldots\ldots\ldots x_n(t))^T \in R^n$ is the state vector associated with the neurons, $I = (I_1, I_2, \ldots\ldots\ldots, I_n)^T \in R^n$ is external input vector.

$f(x(t)) = (f_1(x_1(t)), f_2(x_2(t)), \ldots\ldots\ldots\ldots\ldots, f_n(x_n(t)))^T \in R^n$ corresponds to the activation functions of neurons, $\tau(t) = \tau_{ij}(t)$ $(i, j = 1, 2, \ldots, n)$ are the time delays, the initial conditions of (1) are given by $x_i(t) = \phi_i(t) \in C([-r, 0], R)$ with $r = \max_1 \le i, j \le n, t \in R\{\tau_{ij}(t)\}$, where $C([-r, 0], R)$ denotes the set of all continuous functions from $[-r, 0]$ to R. $C = \text{diag}(c_1, c_2, \ldots, c_n)$ is a diagonal matrix, $A = (a_{ij})n*n$ and $B = (b_{ij})n*n$ are the connection weight matrix and the delayed connection weight matrix, respectively. As is known to all that (1) can exhibit chaotic phenomenon.

$$\begin{bmatrix} \frac{dx_1(t)}{dt} \\ \frac{dx_2(t)}{dt} \end{bmatrix} = -C\begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} + A\begin{bmatrix} \tanh(x_1(t)) \\ \tanh(x_2(t)) \end{bmatrix} + B\begin{bmatrix} \tanh(x_1(t-\tau(t))) \\ \tanh(x_2(t-\tau(t))) \end{bmatrix} \quad (2)$$

2.2 Algorithm for Cryptography Using Chaotic Neural Network

1. Set the value of M.
2. Determine parameter μ and initial point x(0).
3. 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.
4. for n = 0 to M – 1

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

for i = 0 to 7

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

$j \in \{0, 1, 2, 3, 4, 5, 6, 7\}$

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

end

for i = 0 to 7

$$d_i' = f\left(\sum_{j=0}^{7} \omega_{ji} d_i + \theta_i \right)$$

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

end

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

end

2.3 Encryption and Decryption Using ANN Based Chaotic Generator

Cryptology is a discipline that covers many different studies which are about overcoming security and identification holes on communication systems. Cryptography is a process which consists of two parts that are called as encryption and decryption processes. The encryption process can be defined as converting the original message which is named as plain-text to an inscrutable form which is named as cipher-text by an algorithm with secret keys. Decryption process is the inverse form of encryption process. The block diagram of a crypto-system is given in Fig.2, a plain-text is encrypted using the secret keys in the transmitter and then the cipher-text is transmitted throughout an unsecure channel. At the receiver, the cipher-text is decrypted by the decryption algorithm using the secret keys and the plain-text is obtained again. Cryptanalysts can also monitor the unsecure channel. In general, obtaining plain-text from cipher-text without secret key has major priority. Learning the decryption algorithm, learning the key, sometimes learning that the same message is sent again, part of the key, time the message was sent are also important. Unknown decryption algorithm is the worst situation for cryptanalysts. Cryptanalysts try to decrypt all cipher-texts without the secret keys and/or the decryption algorithm. They use diûerent attack algorithms and achieve the estimated texts which is only similar to the plain text but not exactly the same. If a cryptanalyst achieves the plain-text without having the secret keys and/or the decryption algorithm, it is easily said that the crypto-system is failed.

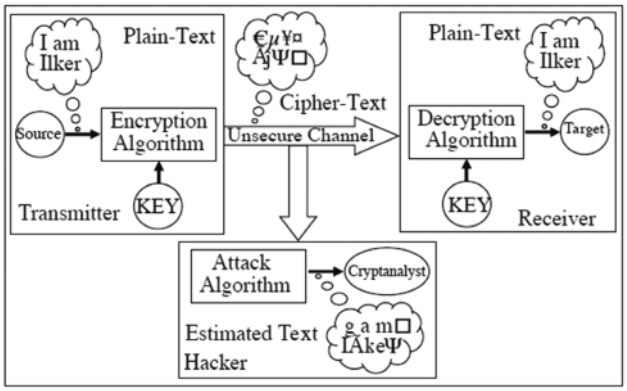

Fig.2: Block Diagram of Conventional Cryptography

A plain-text was encrypted and then obtained cipher-text was decrypted by using the chaotic dynamics. 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. The block diagram of the process is given in Fig.3.

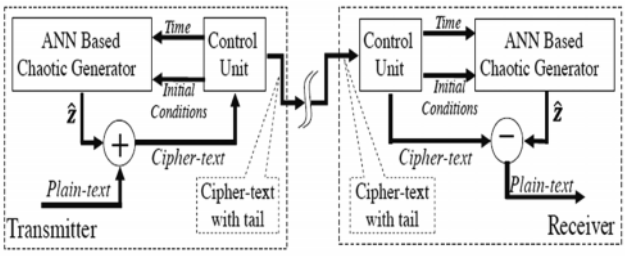

Fig.3: Block Diagram of ANN Based Chaotic Cryptography

2.4 Criteria for Designing Chaotic Cryptosystems

When designing chaotic equations for data encryption, it is important to consider the time for data encryption (and

decryption) and the level of security. The following were several important criteria for the design of a good chaotic cipher [9, 10].

2.5.1. The Computation Time For Encryption and Decryption

The computation time for encryption and decryption depends on the complexity of equations and the value of state variable

(A) The Complexity of Equations

The lower the complexity of the equations, the shorter the computation time will be. If the complexity of equation was low, it would obviously reduce the computation time during data encryption and decryption. On the other hand, if the complexity of equation was high, a longer time would be needed for data encryption and decryption. So in order to choose an equation with lower complexity, a discrete chaotic map is suggested. If the nature of chaotic equation was a discrete map, it would only involve basic arithmetic operations like summations, subtractions, multiplications and divisions etc. On the other hand, if the nature of chaotic equation was a continuous flow, it would involve differential or integration type operations when calculating the value of next state variable.

(B) The Value(s) of State Variable(s)

From the data complexity point of view, an integral value of state variable is more preferable. If the value of state variable was an integer, it would take a shorter time for computing the value of the next state variable. On the other hand, if the value of state variable was a floating point number, it would need a longer time for computing the value of the next state variable.

2.5.2. The Level of Security

Most chaotic encryption methods are basically symmetric key encryption in which both encryption and decryption key being use the same set of chaotic equations. In most of the case, the parameters of these chaotic equations and their initial values of state variable will be used as the encryption keys (the symmetric keys). Hence, the level of security will depend on two primitive factors: the key length and the output of encrypted cipher.

(A) Key Length and Numbers of Keys

If the key length or numbers of keys are small, it would shorten the time of cryptanalysis of the keys. However, it will impose an intrinsic problem for setting the key length because for most chaotic equations, it would only allow a relatively narrow range of parameter to be chosen with chaotic behavior.

The traditional key value of chaotic equation is floating point number. It means that the key length would be increased based on the precision value of floating point number. However, floating point number would substantially increase the computation time. This would also lead to contradiction for designing a good chaotic encryption method as computational complexity and system efficiency is one of the major factors for the design of cryptosystem, especially in a real-time cryptosystem.

(B) Number of Set of Chaotic Equations

A large number of sets of chaotic equations will induce difficulties in cryptanalysis (and hence a better security level). If the number of set of chaotic equations was small, it would be easier for cryptanalysis.

3. RESULT AND DISCUSSION

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.

Table 1
Same Input Encrypted with Different Initial Conditions (Values of x(0) and **μ)**

Input	Output with x(0) = 0.75 & μ = 3.9	Output withx x(0) = 0.55 & μ = 1.5	Output with x(0) = 1.32 & μ = 4.7
36	190	64	219
3	150	17	252
7	153	15	248
43	167	47	212
85	248	87	170
52	95	53	203
236	60	236	19
98	98	98	157
79	44	79	176
10	217	10	10

Table 2
Encrypted Data of Table 1 (Column 2) Decrypted Using Same and Different Initial Conditions

Input	Output Obtained Using Same Initial Condition	Output Obtained Using Different Initian Condition	
	Output with $x(0) = 0.75$ & $\mu = 3.9$	Output with $x(0) = 0.55$ & $\mu = 1.5$	Output with $x(0) = 2.43$ & $\mu = 5.4$
190	36	218	65
150	3	132	105
153	7	145	102
167	43	163	88
248	85	250	7
95	52	94	160
60	236	60	195
98	98	98	157
44	79	44	211
217	10	217	217

Table 3
Encrypted Data of Table 1 (Column 3) Decrypted Using Same and Different Initial Conditions

Input	Output Obtained Using Same Initial Condition	Output Obtained Using Different Initian Condition	
	Output with $x(0) = 0.55$ & $\mu = 1.5$	Output with $x(0) = 3.65$ & $\mu = 6.5$	Output with $x(0) = 0.75$ & $\mu = 3.9$
64	36	191	218
17	3	238	132
15	7	240	145
47	43	208	163
87	85	168	250
53	52	202	94
236	236	19	60
98	98	157	98
79	79	79	44
10	10	10	217

Table 4
Encrypted data of Table 1 (Column 4) Decrypted Using Same and Different Initial Conditions

Input	Output Obtained Using Same Initial Condition	Output Obtained Using Different Initian Condition	
	Output with $x(0) = 1.32$ & $\mu = 4.7$	Output with $x(0) = 0.75$ & $\mu = 3.9$	Output with $x(0) = 0.55$ & $\mu = 1.7$
219	36	65	155
252	3	105	248
248	7	102	249
212	43	88	212
170	85	7	170
203	52	160	203
19	236	195	19
157	98	157	157
176	79	211	176
10	10	217	10

It is clear from table 2, 3 and 4 that we can decrypt an encrypted data correctly by knowing the exact values of x(0) and μ otherwise we get the wrong data as shown in column 3 and 4 of table 2,3 and 4.

4. CONCLUSION

Chaos is statistically indistinguishable from randomness, and yet it is deterministic and not random at all. Chaotic system will produce the same results if given the same inputs, it is unpredictable in the sense that you can not predict in what way the system's behavior will change for any change in the input to that system. A binary sequence generated from a chaotic system, the biases and weights of neurons are set. So, in the chaotic systems, it is well-known that it has sensitive dependence on initial conditions and there exist trajectories that are dense, bounded, but neither periodic nor quasi-periodic in the state space.

Hence, the chaotic binary sequence is unpredictable. It is very difficult to decrypt an encrypted data correctly by making an exhaustive search without knowing x(0) and μ. Hence, CNN is one of guaranteed high security.

REFERENCES

[1] "An Introduction to Neural Network" by Ben Krose and Patrick van der Smagt Eighth Edition, November 1996.

[2] C. Boyd, "Modem Data Encryption", Electronics & Communication Journal, pp. 271-278, Oct. 1993.

[3] C.K. Chan and L.M. Cheng, "Pseudorandom Generator Based on Clipped Hopfield Neural Network," In: Proceedings of the 1998 IEEE International Symposium on Circuits and Systems, 3, (1998) 183-186.

[4] E. Bilotta, P.Pantano and F.Stranges, "A gallery of chua Attractors Part-I," Int.J.Bifurcation Chaos, 17 (1), pp.1-60, 2007.

[5] G. Cauwenberghs, "Delta – Sigma Cellular Automata for Analog VLSI Random Vector Generation," IEEE Transaction on Circuits and Systems II: Analog and Digital Signal Processing, 46, No.3, pp. 240-250, March 1999.

[6] I.N Stewart, "God Does It Play With The Dice?" The New Mathematics of Chaos, London, Penguin, 1997.

[7] J.C. Yen and J. I. GUO, "A New Image Encryption Algorithm and Its VLSI, Architecture," 1999 IEEE Workshop on Signal Processing Systems, Grand Hotel, Taipei, Taiwan, Oct. 18-22, pp. 430-437, 1999.

[8] L.P.Yee and D. L.C Silva, "Applications of Multilayer Perception Networks in Symmetric Block Ciphers," Proceeding of the 2002 International Joint Conference on Neural Networks, 2, pp. 1455-1458, 12-17 May 2002.

[9] M.S. Baptista, "Cryptography with Chaos," Physics Letters A, 240, pp.50-54, 1998.

[10] S. Li, "Analyzes and New Designs of Digital Chaotic Cipher", phD Dissertation, Xi' an Jiaotong University, 1993.

[11] Zurada, Jacek M. "Introduction to Artificial Systems", West Publishing CO, St. Paul. 1992.