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

An Empirical Investigation of Using ANN Based N-State Sequential Machine and Chaotic Neural Network in the Field of Cryptography

By Nitin Shukla & Abhinav Tiwari
University of RGPV Bhopal Madhya Pradesh India

Abstract - 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]. To overcome these drawbacks, we analyzed neural network is the best way to generate secret key. In this paper we proposed a very new approach in the field of cryptography. We are 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. For simulation MATLAB software is used. This paper also includes an experimental results and complete demonstration that ANN based n-state sequential machine and chaotic neural network is successfully perform the cryptography.

Keywords : ANN, n-state Sequential Machine, Chaotic Neural Network, Cryptography.

GJCST-E Classification: D.4.6

AN EMPIRICAL INVESTIGATION OF USING ANN BASED N-STATE SEQUENTIAL MACHINE AND CHAOTIC NEURAL NETWORK IN THE FIELD OF CRYPTOGRAPHY

Strictly as per the compliance and regulations of:

An Empirical Investigation of Using ANN Based N-State Sequential Machine and Chaotic Neural Network in the Field of Cryptography

Nitin Shukla [α] & Abhinav Tiwari [σ]

Abstract - 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]. To overcome these drawbacks, we analyzed neural network is the best way to generate secret key. In this paper we proposed a very new approach in the field of cryptography. We are 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. For simulation MATLAB software is used. This paper also includes an experimental results and complete demonstration that ANN based n-state sequential machine and chaotic neural network is successfully perform the cryptography.

Keywords : ANN, n-state Sequential Machine, Chaotic Neural Network, Cryptography.

I. Introduction

An Artificial Neural Network (ANN) is an information processing paradigm that is inspired by the way biological nervous systems, such as the brain, process An ANN is configured for a specific application, such as pattern recognition or data classification, through a learning process[12]. Learning in biological systems involves adjustments to the synaptic connections that exist between the neurons.

[12]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.

This paper is an investigation of using ANN based n-state sequential machine and chaotic neural network in the field of cryptography .the rest of the paper is organized as follows: section 2 discusses background and related work in the field of ANN based cryptography, section 3 proposed method related to n-state sequential machine and chaotic neural network section 4 discusses implementation section 5 discusses experimental report and test result and finally section 6 discusses conclusion.

II. Background and Related Work

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[2].

John Justin M, Manimurugan S introduced A Survey on Various Encryption Techniques. This paper focuses mainly on the different kinds of encryption techniques that are existing, and framing all the techniques together as a literature survey. Aim an extensive experimental study of implementations of various available encryption techniques. Also focuses on image encryption techniques, information encryption techniques, double encryption and Chaos-based encryption techniques. This study extends to the performance parameters used in encryption processes and analysing on their security issues[3].

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 Artificial 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-

Author α : Assistant Professor in Computer Science Dept. from S.R.I.T. Jabalpur University of RGPV Bhopal Madhya Pradesh India.
Author σ : M.Tech. Scholar S.R.I.T. Jabalpur University of RGPV Bhopal Madhya Pradesh India.

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[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].

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. Secondly, such stream cipher system is required to be implemented using FPGA technology, therefore, minimum hardware requirements has to be considered[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].

Wenwu Yu, Jinde Cao introduced Cryptography based on delayed chaotic neural networks. In this Letter, a novel approach of encryption based on chaotic Hopfield neural networks with time varying delay is proposed. We use the chaotic neural network to generate binary sequences which will be used for masking plaintext. The plaintext is masked by switching of chaotic neural network maps and permutation of generated binary sequences. Simulation results were given to show the feasibility and effectiveness in the proposed scheme of this Letter. As a result, chaotic cryptography becomes more practical in the secure transmission of large multi-media files over public data communication network[9]

III. Proposed Method

A number of studies have already investigated different machine learning methodologies, specifically neural networks and their applications in cryptography, but It is uncommon technique to using Artificial Neural network based n-state sequential machine and Chaotic neural network in the field of cryptography .

a) Sequential Machine

A sequential Machine output depends on state of the machine as well as the input given to the sequential machine. Therefore Michel I .Jordan Network was designed because in which output are treated as input. We are used these type of input as a state.

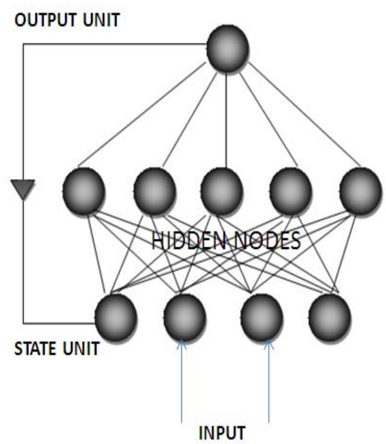


Fig. 3.1 : Michel I .Jordan Neural Network

Multilayer network has been designed with the help of Michel I .Jordan Network Fig 3.1 .In this network has 3 layers an input layer, a hidden layer and an output layer. The size of the input layer depends on the number of inputs and the number of outputs being used to denote the states. The learning algorithm used for this network is back propagation algorithm and the transfer function in the hidden layer is a sigmoid function. For implementation of sequential machine a serial adder and a sequential decoder is used.

b) Cryptography Achieved by Artificial neural network based n-state sequential machine

As a sequential machine can be achieved by using a Michel I. Jordan neural network, therefore data are successfully encrypted and decrypted. In this case the starting state of the n-state sequential machine can act as a key. Data is used to train the neural network as it provides the way the machine moves from one state to another.

c) Cryptography Achieved by a chaotic neural network

Cryptography scheme was done by a chaotic neural network. A network is called chaotic neural network if its weights and biases are determined by chaotic sequence. Specially encryption of digital signal we used chaotic neural network.

IV. Implementation

a) Sequential Machine

A finite state sequential machine was implemented using a Michael I. Jordan network is used. Jordan networks are also known as "simple recurrent networks". Using back propagation algorithm for train Jordan Neural network. The application of the generalized delta rule thus involves two phases:

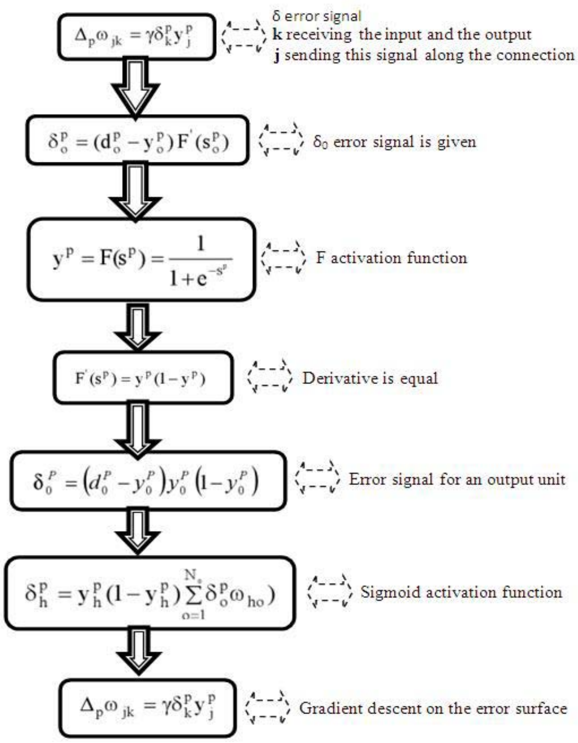


Fig. 4.1 : Weight adjustments with sigmoid activation function

First Phase: The input x is presented and propagated forward through the network to compute the output values yp for each output unit. This output is compared with its desired value do, resulting in an error signal δp for each output unit.

The Second Phase: This involves a backward pass through the network during which the error signal is passed to each unit in the network and appropriate weight changes are calculated.

b) Cryptography achieved by Using ANN based sequential machine

The reason for using sequential machine for implementation is that the output and input can have any type of relationship and the output depends on the starting state. The starting state is used as a key for encryption and decryption. If the starting state is not known, it is not possible to retrieve the data by decryption even if the state table or the working of the sequential state is known. For training of the neural network, any type of sequential machine can be used with the key showing the complexity or the level of security obtained.

c) Cryptography Achieved Through chaotic neural network

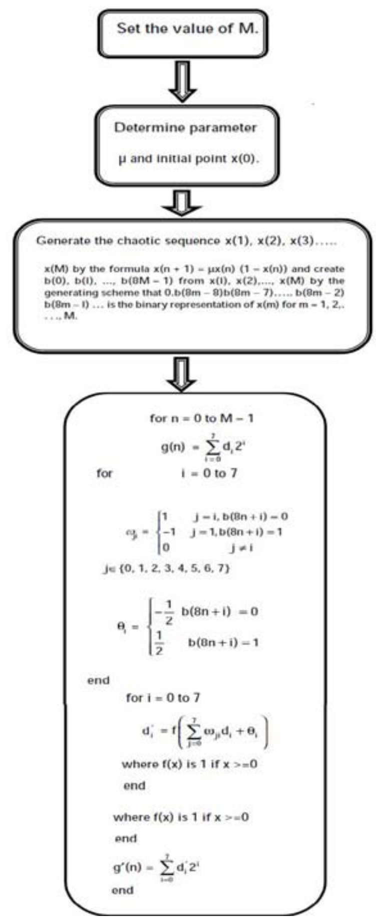


Fig. 4.2 : CNN based Algorithm for encryption

A chaotic neural network in which weights and biases are determined by a chaotic sequence.

g = digital signal of length M and g (n)

0 ≤ M-1 , be the one- byte value of the signal g at position n .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).

V. Experiment and Test Result

a) Sequential Machine

A general n-state Sequential Machine was implemented. As an example, the serial adder was implemented using this machine.

Input 1	Input 2	Current state	Output	Next state
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

Table 5.1 : State table of the Serial Adder

Table 5.1 demonstrate the state table of the Serial Adder The current state represents any previous carry that might be present whereas the next state represents the output carry. Serial Adder State table data is entered into the program. The following Command window implemented in MATLAB show different stages of the execution.

```
Command Window
Enter The Number Of INPUT 2
Enter The Number Of OUTPUT1
Enter The Number Of State 2
Enter INPUT And STATE[0 0 0]
Enter OUTPUT And STATE[0 0]
Enter INPUT And STATE[0 1 0]
Enter OUTPUT And STATE[1 0]
Enter INPUT And STATE[1 0 0]
Enter OUTPUT And STATE[1 0]
Enter INPUT And STATE[1 1 0]
Enter OUTPUT And STATE[0 1]
Enter INPUT And STATE[0 1 1]
Enter OUTPUT And STATE[0 1]
Enter INPUT And STATE[1 0 1]
Enter OUTPUT And STATE[0 1]
Enter INPUT And STATE[1 1 1]
Enter OUTPUT And STATE[1 1]
Enter INPUT And STATE[0 0 1]
Enter OUTPUT And STATE[0 1]
```

Fig. 5.2 : Enter the training data in the n-State sequential machine

N-state sequential machine program is implemented and enter training data .First it ask user to enter input ,output and state here we enter 2 input, 1 output and 2 states. With the help of back-propagation algorithm, to minimize the error function.

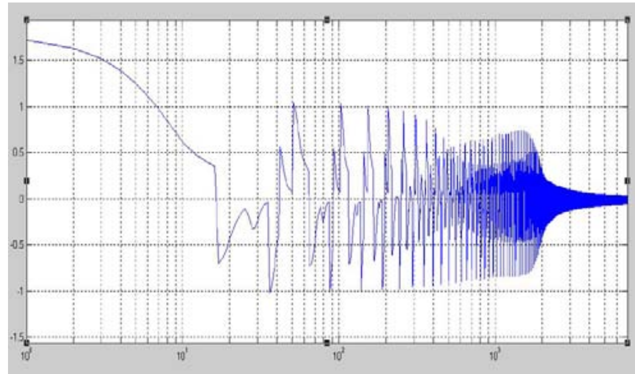


Fig. 5.3 : Shows the plot of the error function against the number of iterations

```
Command Window
Enter The INPUT[0 0]

out1 =

     0     0

Enter The INPUT[1 0]

out1 =

     1     0

Enter The INPUT[1 1]

out1 =

     0     1

Enter The INPUT[1 1]

out1 =

     1     1

Enter The INPUT[0 1]

out1 =

     0     1
```

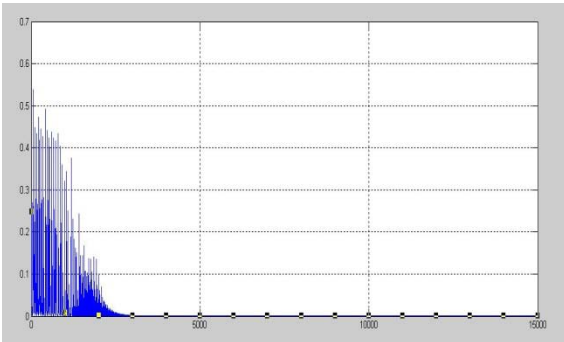
Fig. 5.4 : Final output of sequential machine

Above Command window show Final Output of the sequential machine implemented as a Serial Adder. There is initial state is informed to the user for the input bits to be added. The output is the sum and the carry bit. After that the execution of program has been completed it is automatically jumps to the new carry state. This output is considered as previous carry state.

Following Graph illustrate Mean Square Error when we Enter input 0,1 and 2 .we apply this input in two feed forward Adder One is of Multilayer single output feed forward Adder and other is Multilayer multiple output feed forward Adder.

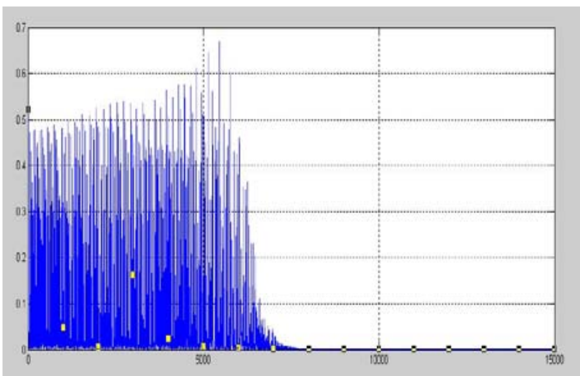
First we apply Input Number 0,1 and 2 on Multilayer single output feed forward and find MSE on Linear scale .

Enter Input 0:



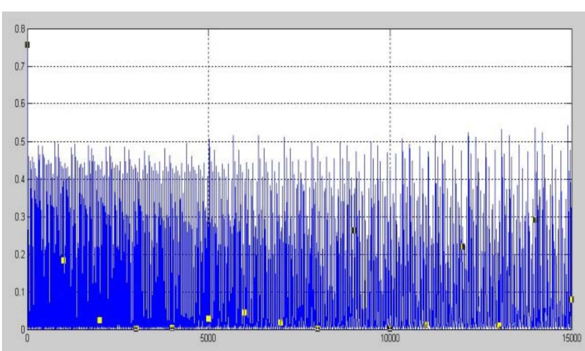
(a) MSE of Multilayer single output feed forward

Enter Input 1:



(b) MSE of Multilayer single output feed forward

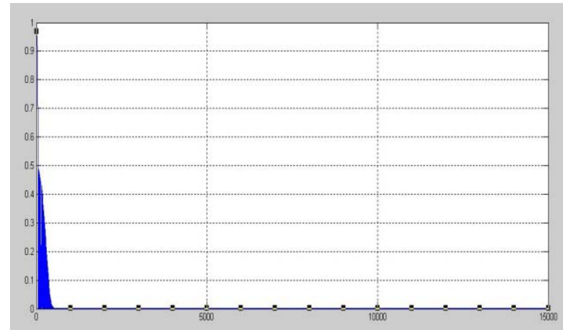
Enter Input 2:



(c) MSE of Multilayer single output feed forward

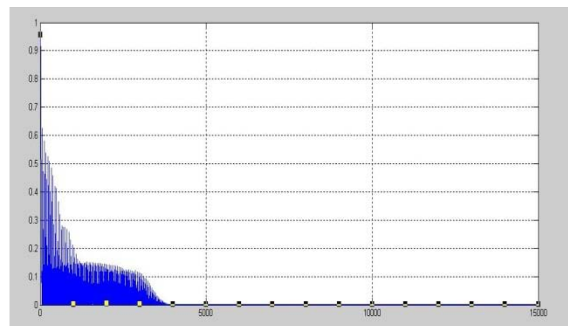
Secondly we apply Input Number 0,1 and 2 on Multilayer multiple output feed forward Adder and find MSE on Linear scale.

Enter Input: 0:



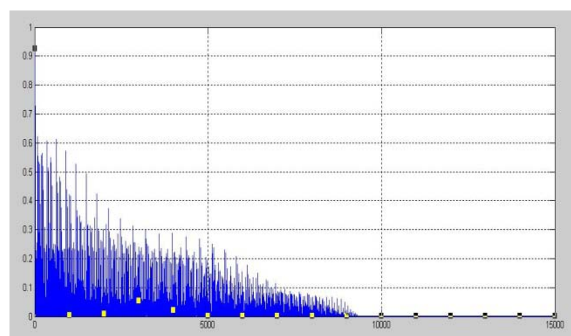
(d) MSE of Multilayer multiple output feed forward

Enter Input : 1:



(e) MSE of Multilayer multiple output feed forward

Enter Input : 2:

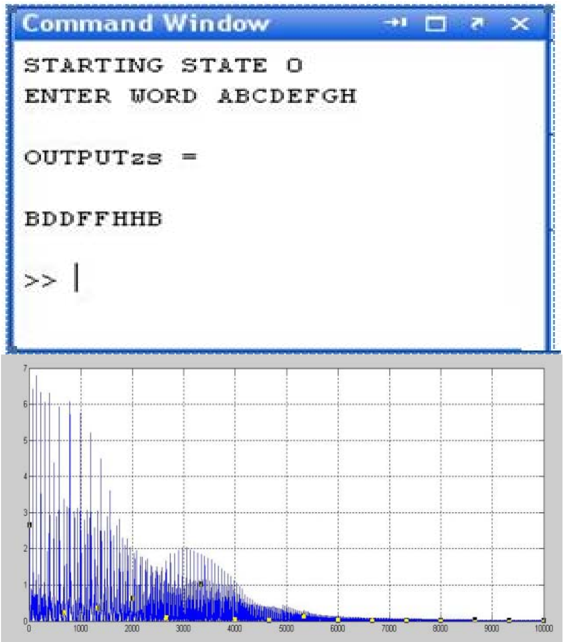


(f) MSE of Multilayer multiple output feed forward

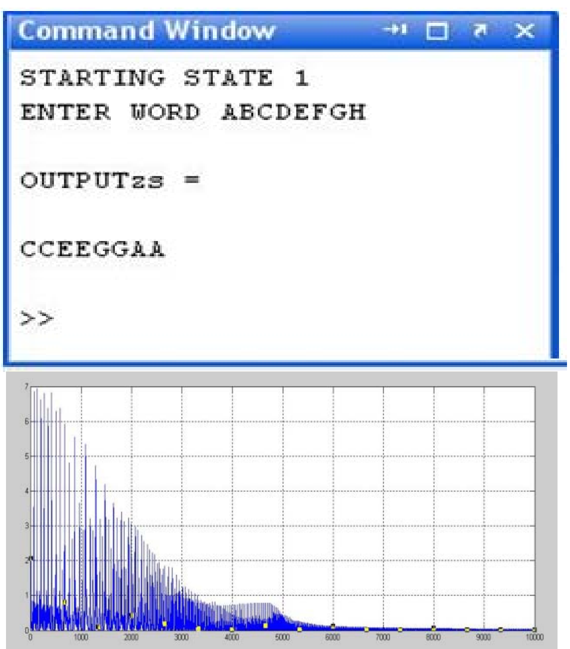
All these graph shows Mean Square Error on linear scale .Comparative study is done between Multilayer single output feed forward Adder and Multilayer multiple output feed forward Adder. Multilayer multiple output feed forward Adder generate smaller number of patterns and thus reduced the training time as well as the number of neurons in compare to and Multilayer single output feed forward Adder.

b) Cryptography achieved Through ANN based Sequential Machine

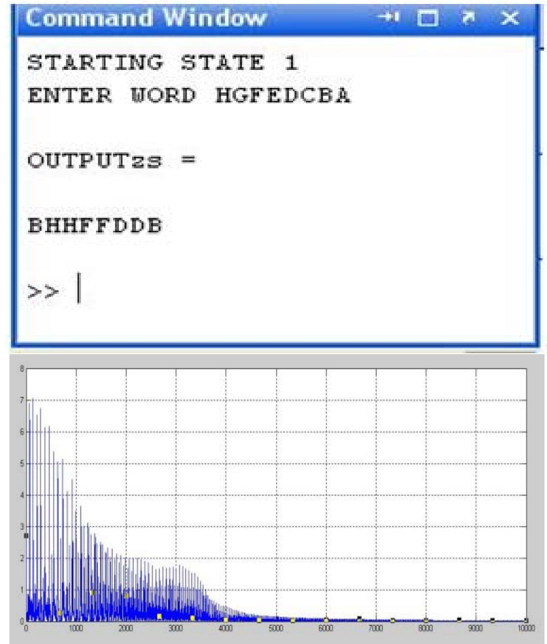
In this section with the help of ANN based n-state sequential machine successfully convert a Letter A to H in Encrypted form. it ask user to enter state, if the starting state is 0 then the input letter is shifted by one and generated encrypted letter similarly is the starting state is 1 the letter is shifted by 2.The state is automatically move to next state .If the next input is again A the output will be C as the current state now is 1. For H, state 0 will flip the letter to A while state 1 will flip the output to B. This method can be used to encrypt a word containing only the letters A to H.



(a) Output using n-state sequential machine based Encryption on code window and output graph on linear scale starting state 0



(b) Output using n-state sequential machine based Encryption on code window and output graph on linear scale starting state 1



(c) Output using n-state sequential machine based Encryption on code window and output graph on linear scale starting state 1

c) Cryptography Achieved 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().

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

Same Input Encrypted with Different Initial Conditions (Values of x(0) and μ())				
INPUT	ASCII CODE	Output with x(0)= 0.75 μ=3.9	Output with x(0)= 0.85 μ=3.5	output with x(0)= 0.90 μ=3.2
A	97	199	233	204
B	98	195	112	98
C	99	200	239	11
D	100	253	108	31
E	101	220	226	1
F	102	17	115	25
G	103	187	234	56
H	104	101	109	235
I	105	6	236	49
J	106	138	115	226
K	107	107	229	36
L	108	32	110	225
M	109	180	238	42
N	110	119	112	254
O	111	225	224	45
P	112	184	113	225
Q	113	63	243	49
R	114	168	83	227
S	115	103	252	51
T	116	245	116	229
U	117	160	244	53
V	118	83	84	231
W	119	209	248	55
X	120	219	120	233
Y	121	209	248	57
Z	122	231	88	235

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

Encrypted Data of Table 1 (Column 2) Decrypted Using Same and Different Initial Conditions				
		Output Obtained Using Same Initial Condition	Output Obtained Using Different Initial Condition	
INPUT	ASCII CODE	output with x(0)= 0.75 μ=3.9	output with x(0)= 0.85 μ=3.5	output with x(0)= 0.90 μ=3.2
A	199	97	79	106
B	195	98	209	195
C	200	99	68	160
D	253	100	245	134
E	220	101	91	184
F	17	102	4	110
G	187	103	54	228
H	101	104	96	230
I	6	105	131	94
J	138	106	147	2
K	107	107	229	36
L	32	108	34	173
M	180	109	55	243
N	119	110	105	231
O	225	111	110	163
P	184	112	185	41
Q	63	113	189	127
R	168	114	137	57
S	103	115	232	39
T	245	116	245	100
U	160	117	33	224
V	83	118	113	194
W	209	119	94	145
X	219	120	219	74
Y	209	121	80	145
Z	231	122	197	118

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

Encrypted Data of Table 1 (Column 3) Decrypted Using Same and Different Initial Conditions				
Output Obtained Using Same Initial Condition			Output Obtained Using Different Initial Condition	
INPUT	ASCII CODE	output with x(0)= 0.75 μ=3.9	output with x(0)= 0.85 μ=3.5	output with x(0)= 0.90 μ=3.2
A	233	79	97	68
B	112	209	98	112
C	239	68	99	135
D	108	245	100	23
E	226	91	101	134
F	115	4	102	12
G	234	54	103	181
H	109	96	104	238
I	236	131	105	180
J	115	147	106	251
K	229	229	107	170
L	110	34	108	227
M	238	55	109	169
N	112	105	110	224
O	224	110	111	162
P	113	185	112	224
Q	243	189	113	179
R	83	137	114	194
S	252	232	115	188
T	116	245	116	229
U	244	33	117	180
V	84	113	118	197
W	248	94	119	184
X	120	219	120	233
Y	248	80	121	184
Z	88	197	122	201

Table 4 : Encrypted Data of Table 1 (Column4) Decrypted Using Same and Different Initial Conditions

Encrypted Data of Table 1 (Column 4) Decrypted Using Same and Different Initial Conditions				
Output Obtained Using Same Initial Condition			Output Obtained Using Different Initial Condition	
INPUT	ASCII CODE	output with x(0)= 0.75 μ=3.9	output with x(0)= 0.85 μ=3.5	output with x(0)= 0.90 μ=3.2
A	204	106	68	97
B	98	195	112	98
C	11	160	135	99
D	31	134	23	100
E	1	184	134	101
F	25	110	12	102
G	56	228	181	103
H	235	230	238	104
I	49	94	180	105
J	226	2	251	106
K	36	36	170	107
L	225	173	227	108
M	42	243	169	109
N	254	231	224	110
O	45	163	162	111
P	225	41	224	112
Q	49	127	179	113
R	227	57	194	114
S	51	39	188	115
T	229	100	229	116
U	53	224	180	117
V	231	194	197	118
W	55	145	184	119
X	233	74	233	120
Y	57	145	184	121
Z	235	118	201	122

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 table 2,3 and 4.

VI. Conclusion

Our experiments lead to the following conclusions.

1. Form the experiment section 4 (A) it clear that Sequential Machine was successfully trained with the help back propagation algorithm of ANN. With the help of back-propagation algorithm, to minimize the error function. We also compare same inputs passes between two feed forward adders. Our experiment and test result was also showing Mean square Error between them. Multilayer multiple output feed forward adder show better result as compare to Multilayer multiple output feed forward Adder. Multilayer multiple output feed forward Adder generate smaller number of patterns and thus reduced the training time as well as the number of

neurons in compare to and Multilayer single output feed forward Adder.

2. In the experiment section 4 (B) it is clears that ANN based n- state sequential machine successfully con-vert a Letter A to H in Encrypted form.
3. In the experiment section 4 (c) it is clears from table 2, 3 and 4 that we can decrypt an encrypt data correctly by knowing the exact values of x (0) and μ otherwise we get the wrong data . ASCII CODE decimal value of alphabet A to Z securely encrypted and decrypted using chaotic neural network. Test result and related graph clearly identified parameter on which training time reduces. Artificial neural network successfully built and trained sequential machine and chaotic neural network for performing 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. 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
3. Jason L. Wright , Milos Manic - Neural Network Approach to Locating Cryptography in Object Code. Emerging Technologies and Factory Automation INL Laboratory.
4. John Justin M, Manimurugan S - A Survey on Various Encryption Techniques , International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012
5. 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
6. 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
7. 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.
8. 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
9. Wenwu Yu, Jinde Cao - Cryptography based on delayed chaotic neural networks Department of Mathematics, Southeast University, Nanjing 210096, China Received 1 February 2006; received in revised form 10 March 2006; accepted 28 March 2006 Available online 17 April 2006Communicated by A.R. Bishop
10. 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
11. Jay Kumar Ankit Sinha ,Guncha Goswami, Manisha Kumari ,Ratan Singh - Modeling and Simulation of Backpropogation Algorithm Using VHDL International Journal of Computer Applications in Engineering Sciences [VOL I, ISSUE II, JUNE 2011] [ISSN: 2231-4946]
12. T. SCHMIDT, dept. of computer science, ryerson university, canada - a review of applications of artificial neural networks in cryptosystems
13. Srividya, G.; Nandakumar, P, 'A Triple-Key chaotic image encryption method', Communications and Signal Processing (ICCSP), 2011 International Conference on Feb. 2011 ,266 – 270
14. T.Godhavari, 'Cryptography using neural network', IEEE Indicon 2005 Conference, Chennai, India, 11-13 Dec. 2005,258-261.
15. Miles E. Smid and Dennis K. Branstad. 'The Data Encryption Standard: Past and Future', proceedings of the ieee, vol. 76, no. 5, may 1988,550-559.
16. Shweta B Suryawanshi and Devesh D Nawgaje., 'Chaotic Neural Network for Cryptography in Image Processing'. IJCA Proceedings on 2nd National Conference on Information and Communication Technology NCICT(3):, November 2011. Published by Foundation of Computer Science, New York, USA.
17. "Design and Realization of A New Chaotic Neural Encryption/Decryption Network" by Scott Su, Alvin Lin, and Jui-Cheng Yen.
18. "Capacity of Several Neural Networks With Respect to Digital Adder and Multiplier" by Daniel C. Biederman and Esther Ososanya.
19. "Artificial Intelligence A Modern Approach" by Stuart J. Russell and Peter Norvig.
20. Digital design, fourth edition by M. Morris Mano and Michael D. Ciletti
21. "Machine Learning, Neural and Statistical Classification" by D. Michie, D.J. Spiegelhalter, C.C. Taylor February 17, 1994.
22. Wasserman, Philip D. Neural Computing, Theory and Practice. Van Nordstrand Reinhold, New York. 1989.

23. M. E. Smid and D. K. Branstad, "The Data Encryption Standard: Past and Future," Proceedings of The IEEE, vol. 76, no. 5, pp. 550-559, 1988.
24. C. Boyd, "Modem Data Encryption," Electronics & Communication Journal, pp. 271-278, Oct. 1993. 131 N. Bourbakis and C. Alexopoulos, "Picture Data Encryption Using SC4N Pattern," Pattern Recognition, vol. 25, no. 6, pp. 567-581, 1992.
25. J. C. Yen and J. I. GUO, "A New Image Encryption Algorithm and Its VLSI Architecture," 1999 IEEE Workshop on Signal Procs. Systems, Grand Hotel, Taipei, Taiwan, Oct. 18-22, pp. 430-437, 1999.