International Journal of Latest Trends in Engineering and Technology
Vol.(8)Issue(2), pp.314-320
DOI: http://dx.doi.org/10.21172/1.82.042
e-ISSN:2278-621X

SECRET WRITING BY ARTIFICIAL NEURAL NETWORK

Neetu Singh[1] and Kanika Khetarpal[2]

Abstract—Cryptography is the practice or study of transmitting sensitive information in an encoded format over a network channel. In the age of modern technology cryptography has a key role to play. Huge amounts of information gets transmit every day over numerous networks that contain all kinds of personal and private data. This data is needed to be safeguarded from getting exploited by unauthorized people therefore a strong cryptographic system is needed. The paper focuses on the ways to achieve that goal by using the technique of artificial neural network in cryptography and to explore how this technique can be utilized as a powerful tool to protect the information from unauthorized users.
Key words: Artificial Neural Network (ANN), Neurons, Sigmoid Function, Dendrite, Axon, Synapse.

I. INTRODUCTION

Artificial Neural Network system is developed to process information similar to the human nervous system. Its architecture is modeled according to the architecture of actual human neural network system. The key part of its architecture is the design of how it processes the information. A neural network consists of a large number of neurons with complex interconnectivity. This complex network works with unity to solve a problem. Similar to human neural network, artificial neural networks also learns using examples. Different training sets or examples can train ANN for different applications like pattern recognition, cryptography, data classification etc. In a biological neural network, the synapses that connect neurons adjust based on the learning experience. ANN also functions similarly.

There are numerous advantages of an artificial neural network but most significant is that it learns by observing the information. This helps in using this network as a random approximation tool. This leads to developing a system to reach the solution in a most ideal and cost-effective way. Artificial neural networks are efficient in saving time and money by processing the information and reaching to an optimum solution using training examples instead of whole data sets.

There are three layers in an artificial neural network. First is input layer to gather the data for information processing. Second is a hidden layer to process the information and reach to an output. The third layer which provides with the output. The description is depicted in figure 1.

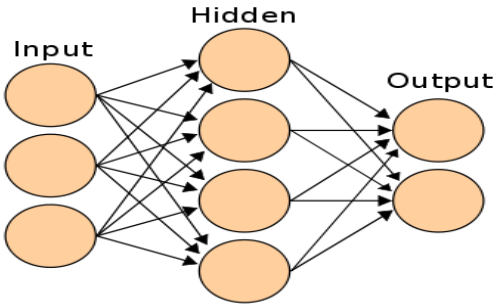


Fig.1 ANN Structure

[1] *Department of Computer Science Engineering Guru Tegh Bahadur Institute Of Technology, New Delhi, India*
[2] *Department of Computer Science Engineering Guru Tegh Bahadur Institute Of Technology, New Delhi, India*

II. Cryptography System Design

Cryptography is a process of converting any information or data given in plain text to cipher text (encrypted text) and then back again to the original plain text. Cryptography can also be associated with techniques like microdots and steganography. But mostly it's interpreted as an encryption/decryption process. The cryptographic techniques help in hiding the sensitive information and therefore transfer it to anyone safely.

There are numerous cryptographic techniques available to encode information and transmit it securely but with exponentially evolving technology a need for better and more secure cryptographic technique is required. With the help and proper usage of ANN the goal can be achieved as the complex network of the ANN system helps in achieving very secure encryption. It helps in performing complex operations on the data optimally and hence making the technique efficient. The combination of variable weights of internal network of processing units and variable number of processing units that can be used to encode the data makes the process of cryptanalysis by the attacker on encoded string very difficult to crack hence making the technique robust and reliable. The process of encryption and decryption on a string can be understood by figure 2.

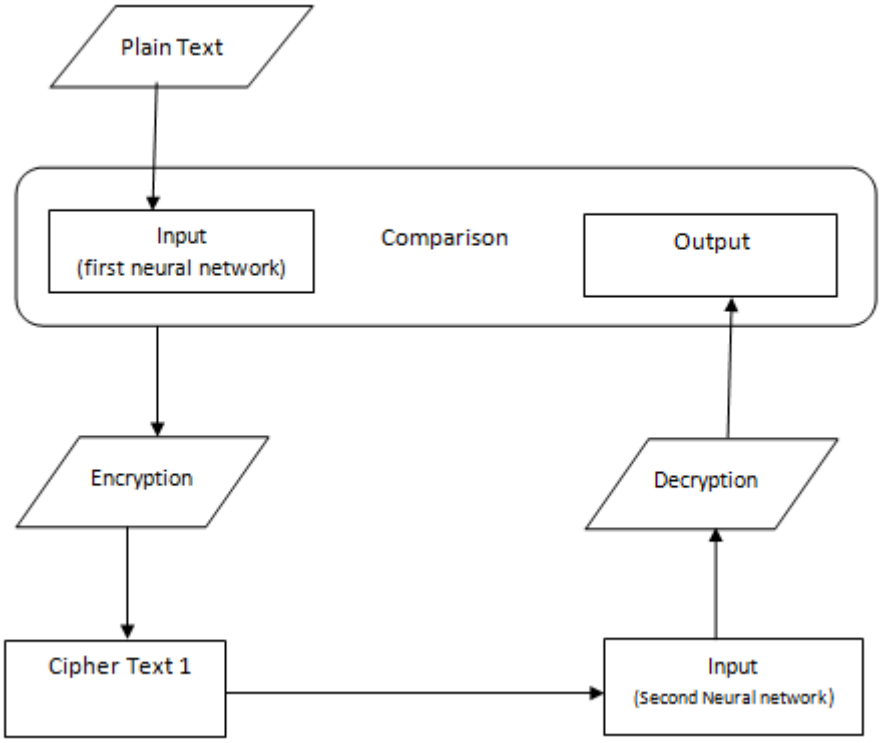


Fig.2 Design diagram of the ANN cryptography

III. Implementation

The cryptography is performed by using a combinational logic of *serial adder* and *a sequential machine*. The serial adder basically takes the two inputs and performs a summation of those to provide a single output whereas the sequential machine provides output on the basis of inputs as well as the previous state of the machine. The combination of both *serial adder* and *sequential machine* helps in delivering an informed and optimal output.

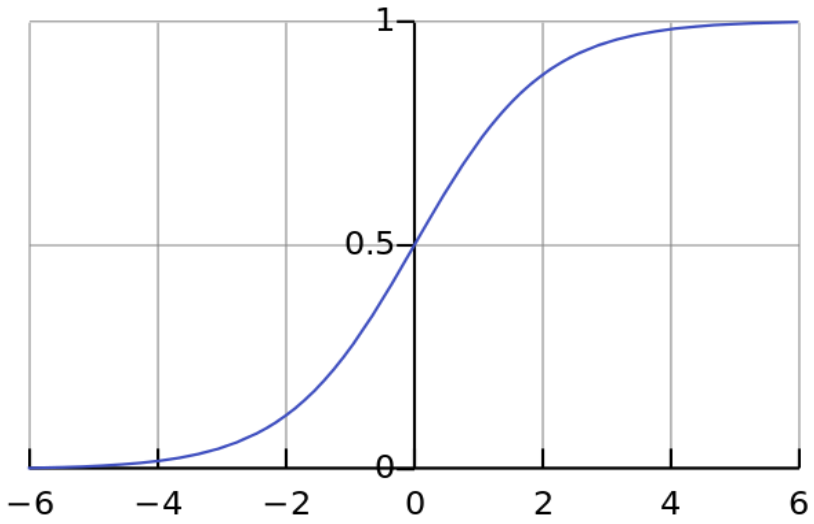
The formulation provided below helps in implementing the combinational logic.

Taking the sum of weighted neurons:

$$\sum weight_i \cdot input_i = weight1 \cdot input1 + weight2 \cdot input2 + weight3 \cdot input3 \quad (1)$$

Using the Sigmoid function to normalize the above method:

$$\frac{1}{1+e^{-x}} \qquad (2)$$



.
Fig.3 Plotted graph of Sigmoid Function

Therefore, by substituting the equation 1 in equation 2 we get final formula for the output of neuron:

$$\text{Output of neuron} = \frac{1}{1+e^{-(\sum weight_i input_i)}}$$

IV. Benefits and Limitations

4.1 Benefits

- The cryptography technique developed using the artificial neural network is very difficult to crack without having proper knowledge of its working.
- The neural network technique is utilized in various applications because to its numerous properties like maintaining the integrity of data, precision in results, strong security system etc.
- Neural Networks are used in medical sciences to detect diseases.
- The technique has the ability to stay accurate even with the introduction of noise or fluctuation in the encrypted message.
- This technique is tolerant to noise.

4.2 Limitations

This technique does not have a lot of limitations. The importance of both the design of the neural system as well as the input weights makes this cryptography technique strong and apt for actual implementation. The combination of design and weights forms the secret key which is needed for both encryption and decryption which acts as an advantage as well as a disadvantage because the loss or incorrect information of any of those can lead to loss of information. Also, the technique is based on complex computations which require significant CPU and memory usage.

V. MATLAB Code Snippet

```
clc;
clear all;
close all;
in_x=3;
out_x=3;
```

```
state_x=2;
for tem_i=1:100
 if 2^tem_i >=state_x
states=tem_i;
break
end
end
hls=6;
w1=rand(hls,(in_x+states+1));
w2=rand((out_x+states),hls+1);
 neta=1;
 a=1;
sx=0;
p=[];
training_setx=[];
training_setx=[0 0 0 0; 0 0 1 0; 0 1 0 0; 0 1 1 0;1 0 0 0;1 0 1 0;1 1 0 0;1 1 1 0; 0 0 0 1; 0 0 1 1; 0 1 0 1; 0 1 1 1;1 0
0 1;1 0 1 1;1 1 0 1;1 1 1 1];
 training_outx=[0 0 1 1; 0 1 0 1; 0 1 1 1;1 0 0 1;1 0 1 1;1 1 0 1;1 1 1 1;0 0 0 1; 0 1 0 0; 0 1 1 0;1 0 0 0; 1 0 1 0;1 1
0 0;1 1 1 0; 0 0 0 0; 0 0 1 0]; for x=1:10000 training_set=training_setx(a,:); training_out=training_outx(a,:);
inputu=[1 training_set];
sum_h=(w1*(inputu)')';
o_h=1./(1+exp(-sum_h)); input_h=[1 o_h];
sum_out=(w2*(input_h)')';
out=1./(1+exp(-sum_out));
delta_out=(out.*(1-out)).*(training_out - out);
delta_h=(delta_out*w2).*input_h.*(1-input_h);
for t=1:(out_x+states)
 w2(t,:) = w2(t,:) + neta*delta_out(t)*input_h;
end
for t=1:hls w1(t,:) = w1(t,:) + neta*delta_h(t+1)*inputu;
end
for t=1:(out_x+states)
if out(t)>=0.7 out1(t)=1;
elseif out(t)<=0.2 out1(t)=0;
else out1(t)=out(t);
end
end
 p=[p sum(out -training_out)];
 if out1==training_out
 a=a+1;
sx=sx+1;
end
 if a > ((2^in_x)*state_x)
a=a -((2^in_x)*state_x);
end
end
 plot(p.*p);
% testing the program
state_x=input('starting state ');
 ipo = input('enter word ','s');
finp=[];
for i=1:length(ipo) b=ipo(i);
switch b
case('A') set=[0 0 0];
case('B') set=[0 0 1];
 case('C') set=[0 1 0];
case('D') set=[0 1 1];
```

```
case('E') set=[1 0 0];
case('F') set=[1 0 1];
case('G') set=[1 1 0];
case('H') set=[1 1 1];
end
ipox=[set state_x];
 inputp=[1 ipox];
 sum_h=(w1*(inputp)')';
 o_h=1./(1+exp( -sum_h));
input_h=[1 o_h];
sum_out=(w2*(input_h)')';
out=1./(1+exp( -sum_out));
 for t=1:(states+out_x)
if out(t)>=0.7
out1(t)=1;
elseif out(t)<=0.2
out1(t)=0;
else
out1(t)=out(t);
 end
 end
finp=[finp;out1];
tem_ipch=[];
 state_x=out1( (out_x + 1):(out_x+states));
 end
outzs=[''];
 for f=1:length(ipo) tem_ipch=finp(f,:);
 tem_ipch=tem_ipch(1:3);
if tem_ipch==[0 0 0]
outzs=[outzs 'A'];
 end if tem_ipch==[0 0 1]
outzs=[outzs 'B'];
 end if tem_ipch==[0 1 0]
outzs=[outzs 'C'];
end if tem_ipch==[0 1 1]
 outzs=[outzs 'D'];
 end if tem_ipch==[1 0 0]
 outzs=[outzs 'E'];
 end if tem_ipch==[1 0 1]
outzs=[outzs 'F'];
 end if tem_ipch==[1 1 0]
outzs=[outzs 'G'];
 end if tem_ipch==[1 1 1]
outzs=[outzs 'H'];
 end
 end
outzs
```

VI. RESULTS AND CONCLUSION

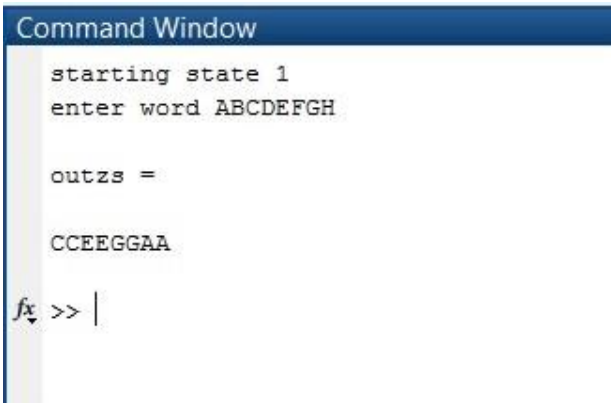


Fig.4 Encryption using ANN

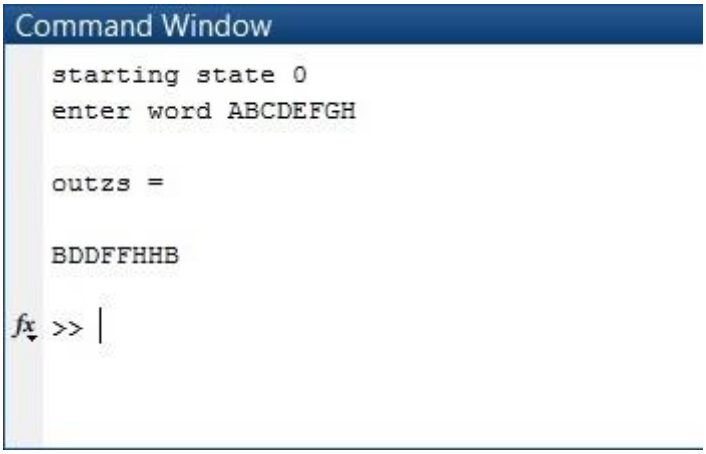


Fig.5 Encryption using ANN

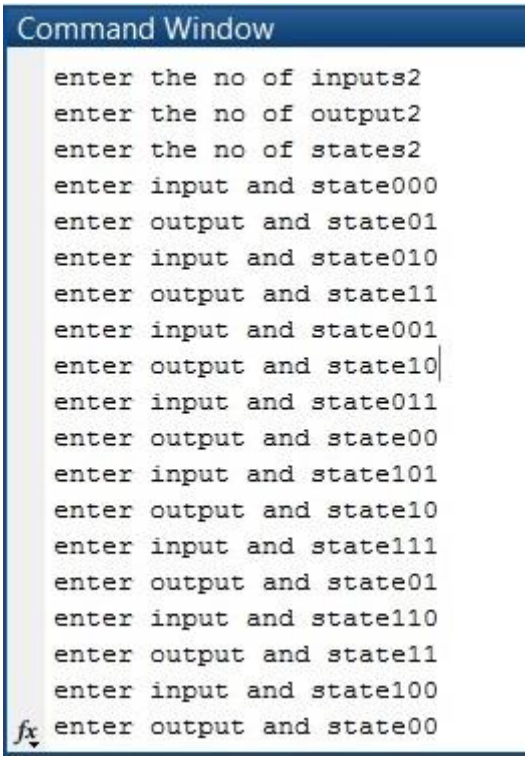


Fig.6 Output states

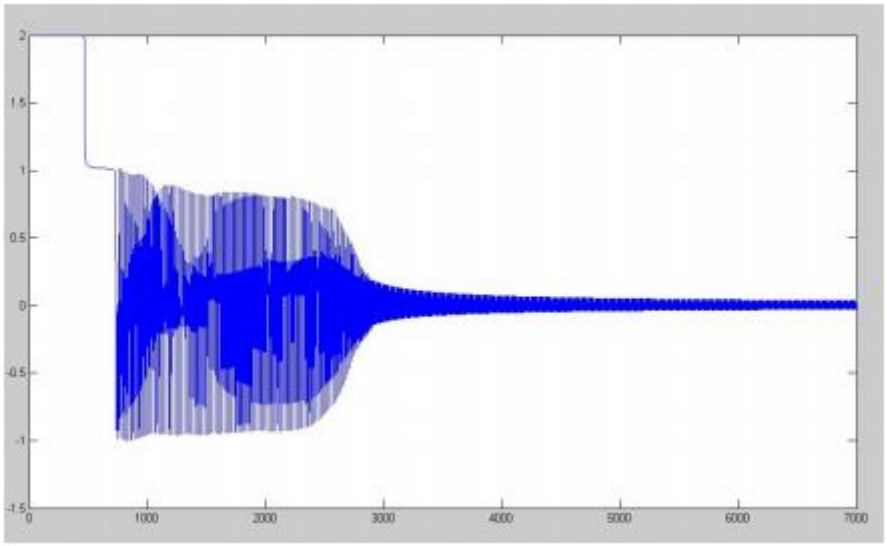


Fig.7 Graph of error function

In conclusion, it can be stated that Artificial Neural Network system is a powerful and a robust technique. This technique can be utilized to perform complex computations. Artificial Neural Networks can be used effectively in the stream of cryptography. It can be used for sequential machine based encryption also as a chaotic neural network for the cryptography of digital signals. The network can be trained with better training sets so as to get much better result. Hence it can be stated that artificial neural networks can be utilized as a better and a new method for encryption and decryption of data.

REFERENCES

[1] Desai V., Patil R., Rao D.: Using Layer Recurrent Neural Network to Generate Pseudo Random Number Sequences. International Journal of Computer Science Issues, 9(2), pp. 324–334, 2012.
[2] Godhavari T., Alainelu N. R., Soundararajan R.: Cryptography Using Neural Network. IEEE Indicon 2005 Conference, (I), pp. 11–13, 2005.
[3] Kannan Munukur R., Gnanam V.: Neural network based decryption for random encryption algorithms.
[4] Sa˘gıro˘glu S., Ozkaya N.: Neural Solutions for Information Security. Journal of Polytechnic, 10(1), pp. 21–25, 2007.
[5] Schneider B.: Applied Cryptography. Protocols, Algorithms, and Source codes in C, 1996
[6] William Stallings, "Cryptography and Network Security: Principles and Practices", second edition.
[7] Abdi H.: A neural Network Primer. Journal of Biological System_is, 1994
[8] Walker,J.: A pseudorandom number sequence test program, available in http://www.fourmilab.ch/random/, 04.14.14.
[9] Zeng K., Yang C.-H., Wei D.-Y., Rao T. R. N.: Pseudorandom bit generators in stream cipher cryptography. IEEE Computer, 24(2), pp. 8–17, 1991.
[10] Pointcheval D.: Neural Networks and their Cryptographic Applications. Pascale Charpin Ed. India, 1994.