Cryptography Based on Artificial Neural Network

Shital Daulat Jagtap, Mr. P. BalaRamudu, Mr. Manoj Kumar Singh

Abstract- Cryptography is the technique of changing data or information into unreadable for unauthorized persons. In cryptography process information transfer from sender to receiver in a manner that prevents from unauthorized third person. There are so many cryptography methods are available which based on number theory. The cryptography based on number system has some disadvantages such as large computational power, complexity and time consumption. To overcome all the disadvantages of number theory based cryptography, Artificial neural network based cryptography used.The ANN have many characteristics such as learning, generation, less data requirement, fast computation, ease of implementation and software and hardware availability. It is very useful for many applications.

Index terms- Cryptography, Artificial Neural Network, Decryption, Encryption, Key generation, Chaotic map.

I. INTRODUCTION

A neural network is a machine which is designed for modelling the way in which the brain performs a particular task.Cryptography is defined as the exchange of data into mix code.Cryptography has two types of encryption data:

Symmetrical encryption andAsymmetrical encryption

A. Symetrical encryption

Symmetrical encryption use the same key for encryption and decryption process and it defines secret-keys, shared keys and private keys.

B. Asymmetric encryption

Asymmetric cryptography uses different key for encryption and decryption process. It has pair of keys one for encryption and one for decryption.

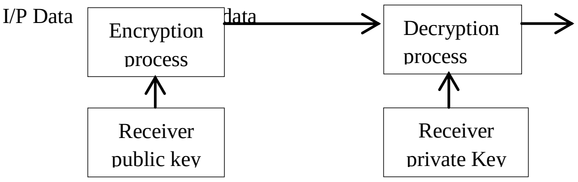


Figure 1: Cryptography public key component

Cryptography is the system that provides encryption and decryption through hardware components or program code in an application.

II. ARTIFICIAL NEURAL NETWORK (ANN)

ANN are parallel adaptive networks. It consist of simple nonlinear computing elements called neurons. It function as the human nervous system. It implemented by using electronic components or simulating softwares.

There are different types of ANN:

1. Recurrent Neural Network
2. General regression neural network
3. Chaotic Neural Network
4. Multilayer Network
5. Neural cryptography

The behaviour of an ANN (Artificial Neural Network) depends on both the weights and the input-output function (transfer function) that is specified for the units. This function typically falls into one of three categories:

1. linear (or ramp)
2. threshold
3. sigmoid

For linear units, the output activity is proportional to the total weighted output.

For threshold units, the output is set at one of two levels, depending on whether the total input is greater than or less than some threshold value.

For sigmoid units, the output varies continuously but not linearly as the input changes. Sigmoid units bear a greater resemblance to real neurones than do linear or threshold units, but all three must be considered rough approximations.

To make a neural network that performs some specific task, we must choose how the units are connected to one another and set the weights on the connections appropriately. The connections determine whether it is possible for one unit to influence another. The weights specify the strength of the influence.

III. CRYPTOGRAPHY USING ARTIFICIAL NEURAL NETWORK

The block diagram of the proposed ANN model is given in Figure 3 . As shown in the figure, three initial conditions and time variable were applied to the inputs and three chaotic dynamics ˆ*x*, ˆ*y* and ˆ*z* were obtained from the outputs of the ANN. For the training and test phases of the ANN, approximately 1800 input-output data pairs which belong to 24 different initial condition sets were obtained from Equation (4). A quarter of those 1800 data pairs were sorted to use in the test phase and the rest of data were used in the training phase

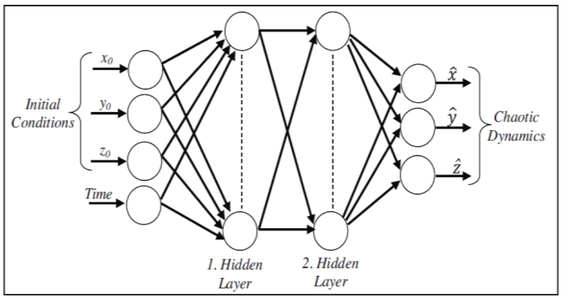


Figure 2:The block diagram of trained ANN model.

A. *Cryptography*

Cryptography is the science of providing secure services. Until 1970s cryptography was considered the domain of military and governments only. However the ubiquitous use computers and the advent of internet has made it an integral part of our daily lives. Today cryptography is at the heart of many secure applications such as online banking, online shopping, online government services such personal income taxes, cellular phones, and wireless LANS (Local Area Networks) etc. In this paragraph we provide an introduction to some cryptographic primitives which are used to design secure applications.

B. *Requirements for cryptography*

Cryptography is generally used in practice to provide four services: *privacy*, *authentication*, *data integrity* and *non-repudiation*. The goal of privacy is to ensure that communication between two parties remain secret. This often means that the contents of communication are secret; however in certain situations the of fact communication took place and must be a secret as well. Encryption is generally used to provide privacy in modern communication. Authentication of one or both parties during a communication is required to ensure that information is exchanged with the legitimate party. Passwords are common examples of one-way authentication in which users authenticate themselves to gain access to system.

C. *Symmetric key encryption*

In symmetric key encryption a secret key is shared between the sender and receiver. The word "symmetric" refers to the fact that both sender and receiver use the same key to encrypt and decrypt the information.

Block Ciphers: A block cipher is symmetric key cryptographic primitive which takes as input an *n*-bit block of plaintext and a secret key and outputs an *n*-bit block of cipher text using a fixed transformation. Figure 4 shows the general structure of a block cipher. The common block sizes are 64 bits, 128 bits and 256 bits. For a fixed key the block cipher defines a permutation on the *n*-bit input.

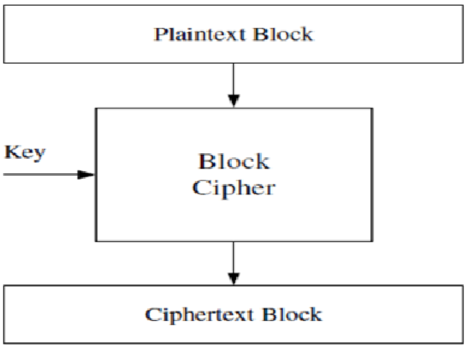


Figure 3: General structure of a block cipher

IV. COMBINATIONAL LOGIC MACHINE

A combinational circuit is one for which the output value is determined solely by the values of the inputs. A combinational circuit consists of input variables, output variables, logic gates and interconnections. The interconnected logic gates accept signals from the inputs and generate signals at the output. The n input variables come from the environment of the circuit, and the m output variables are available for use by the environment. Each input and output variable exists physically as a binary signal that represents logic 1 or logic 0.

For n input variables, there are 2n possible binary input combinations. For each binary combination of the input variables, there is one possible binary value on each output. Thus, a combinational circuit can be specified by a truth table that lists the outputvalues for each combination of the input variables. A combinational circuit can also be described by m Boolean function, one for each output variable. Each such function is expressed as function of the n input variables.

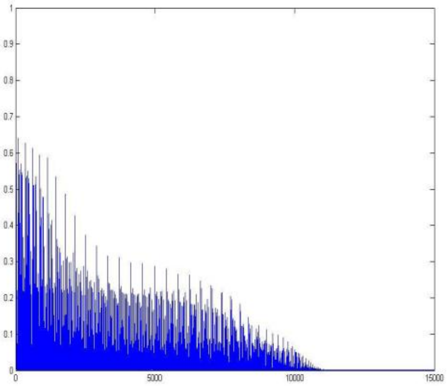


Figure 4:MSE of a fully connected neural network Type 1

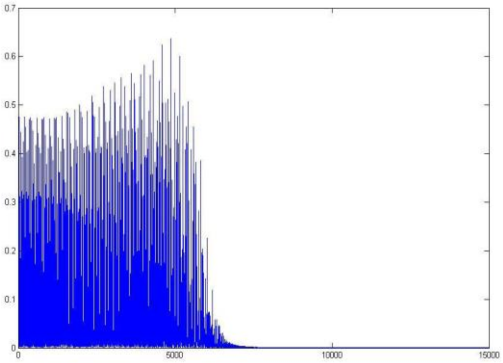


Figure 5: MSE of a one output per network Type 2(b0)

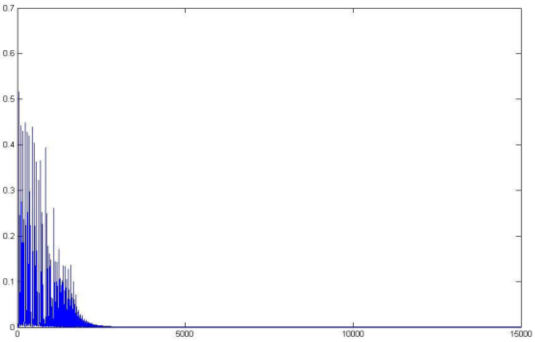
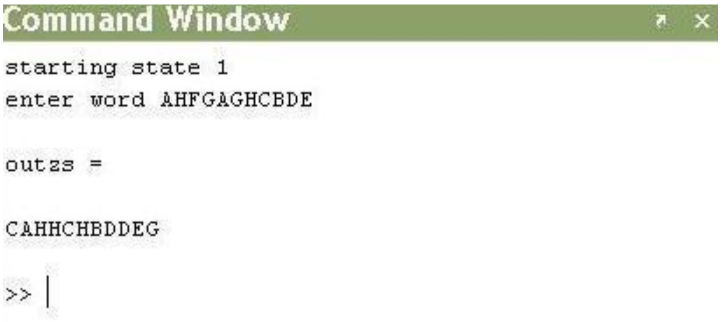


Figure 6:MSE of a one output per network Type 2(b1)

V. *CRYPTOGRAPHY USING ANN BASED SEQUENTIAL MACHINE*

A 3-bit encryption machine was successfully built using an ANN based sequential machine. The sequential machine used had 2 states (0 and 1) and the input is the 3-bit data to be encrypted. Letters A to H were used to represent all the possible 3-bit inputs. If the state is 0, the input letter is shifted by one to generate the encrypted letter while if the state is 1, the letter is shifted by 2. During this operation, the state is automatically switched. Thus, if the starting state is 0 and the input is A, the output will be B and the state switches to 1. 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.



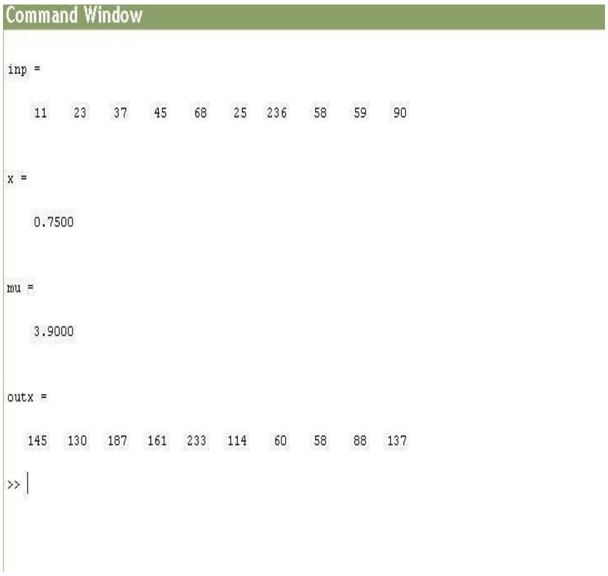
```
starting state 1
enter word AHFGAGHCBDE

outzs =

CAHHCHBDDEG

>> |
```

Figure 7:Output using sequential machine based Encryption

Figure 7 shows the implementation of the above method. The word “AHFGAGHCBDE” is to be encrypted using the starting state of 1. The output in this case will be “CAHHCHBDDEG”.

VI. *CRYPTOGRAPHY USING 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)** = 0.75,and ,µ = 3.9 are set. It is very difficult to decrypt an encrypted data correctly by making an exhaustive search without knowing **x(0)** and µ.



```
inp =

   11   23   37   45   68   25  236   58   59   90


x =

   0.7500


mu =

   3.9000


outx =

  145  130  187  161  233  114   60   58   88  137

>> 
```

Figure 8:Output using chaotic neural network based Encryption

Here a sequence of ten numbers is used for encryption and the initial parameters for the chaotic network are used as mentioned. The output or the encrypted data is then used for decryption. It can easily be seen that the output is in a chaotic state.

VII. CONCLUSION

Artificial Neural Networks is a simple yet powerful technique which has the ability to emulate highly complex computational machines. In this project, we have used this technique to built simple combinational logic and sequential machine using back-propagation algorithm. A comparative study ha been done between two different neural network architectures and their merits/demerits are mentioned. ANNs can be used to implement much complex combinational as well as sequential circuits.

Data security is a prime concern in data communication systems. 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 analyzed. Better results can be achieved by improvement of code or by use of better training algorithms. Thus, Artificial Neural Network can be used as a new method of encryption and decryption of data.

VIII. MATLAB CODE

A. Sequential machine

```
clc;
clear all;
close all;
inputs_x=input('enter the no of inputs');
output_x=input('enter the no of output');
statx=input('enter the no of states');
% no of bits for states
for tem=1:100
if 2^tem >=statx
states=tem;
break
end
end

hls=5;%2^(inputs_x+output_x+2); % size of the hidden layer
% weight initialization----------------------
w1=rand(hls,(inputs_x+states+1));
w2=rand((output_x+states),hls+1);
neta=1;
a=1;
sx=0;
p=[];
fortex=1:(2^(inputs_x)*statx);
training_setx(tex,:)=input('enter input and state');
training_outx(tex,:)=input('enter output and state');
end

for x=1:7000
training_set=training_setx(a,:);
training_out=training_outx(a,:);
% output hidden layer---------------------
inputu=[1 training_set];
sum_h=(w1*(inputu)')';
o_h=1./(1+exp(-sum_h));
% output layer ---------------------------
input_h=[1 o_h];
sum_out=(w2*(input_h)')';
out=1./(1+exp(-sum_out));
% delta ------------------------------------
delta_out=(out.*(1-out)).*(training_out - out);
delta_h=(delta_out*w2).*input_h.*(1-input_h);
% update of weight --------------------------

% output layer --------------------------------
for t=1:(output_x+states)
w2(t,:) = w2(t,:) + neta*delta_out(t)*input_h;
end
% hidden layer ---------------------------------
for t=1:hls
w1(t,:) = w1(t,:) + neta*delta_h(t+1)*inputu;
end
```

REFERENCES

[1] William Stallings, “*Cryptography and Network Security: Principles and Practices*”, second edition.

[2] Aloha Sinha, Kehar Singh, "*A Technique for Image Encryption using Digital Signature*", Optics Communications, Vol.2 No.8 (2203), 229-234.

[3] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, R. Tourki, “*A Modified AES Based Algorithm for Image*

Encryption", World Academy of Science, Engineering and Technology 27 2007.

[4] K.Deergha Rao, Ch. Gangadhar, "*Modified Chaotic Key-Based Algorithm for Image Encryption and its VLSI Realization", *IEEE, 15th International. Conference on Digital Signal Processing (DSP), 2007.

[5] Saroj Kumar Panigrahy, Bibhudendra Acharya, Debasish Jen, "*Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm*", 1st International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008.

[6] Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan, Dai Wei-di, "*Digital Image Encryption Algorithm Based on Chaos and Improved DES*", IEEE International Conference on Systems, Man and Cybernetics, 2009.

[7] Min Long, Li Tan, "*A chaos-Based Data Encryption Algorithm for Image/Video*", IEEE, Second International Conference on Multimedia and Information Technology, 2010.

[8] HiralRathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, "*Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)*" International Journal of Computer Technology and Electronics Engineering (IJCTEE), Vol.1, No.3 (2010/2011).

[9] Kuldeep Singh, Komalpreet Kaur, "*Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it"*, International Journal of Computer Applications (0975 - 8887) Vol.23, No.6, June 2011.

[10] Qais H. Alsafasfeh, Aouda A. Arfoa, "*Image Encryption Based on the General Approach for Multiple Chaotic Systems*", Journal of Signal and Information Processing, 2011.

[11] 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.

[12] 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.

[13] 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.

[14] C. J. Kuo and M. S. Chen, "A New Signal Encryption Technique and Its Attack Study," IEEE International Conference on Security Technology, Taipei, Taiwan.

AUTHORS

First Author Shital DaulatJagtap was born on October 24, 1987. She received the Bachelor of Engineering degree in Electronics from KarmavirDadasahebKannamawar College of Engineering, Nagpur, India, in 2011. Currently, she is pursuing the Master of Engineering degree in Electronics and Telecommunication from Sahyadri Valley College of Engineering and Technology,Rajuri,Pune, India.

Second Author Prof.P.Balaramudu,He received the Master of Technology degree in Electronics and Telecommunication. He has about 9 years of teaching experience.He is currently working as a Professor, Department of Electronicsand Telecommunications EngineeringSahyadri valley College of Engineering and Technology, Rajuri,Junnar,Pune, Maharashtra.

Third Author Mr. Manoj Kumar Singh He received the master of engineering degree in Digital Communication and PhD pursuing. He has about 6.5 years of teaching experience.He is currently working as a Professor, Department of Electronicsand Telecommunications EngineeringSahyadri valley College of Engineering and Technology, Rajuri,Junnar,Pune, Maharashtra.