ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 4, April 2015

Encryption and Decryption using Artificial Neural Network

Tope Komal[1], Rane Ashutosh[2], Rahate Roshan[3], Asst. Prof. S.M.Nalawade[4]

Bachelor of Engineering, Computer Engineering, Sinhgad Institute of Technology, Lonavala, India[1,2,3]

Assistant Professor, Computer Engineering, Sinhgad Institute of Technology, Lonavala, India[4]

Abstract: The project elaborating Artificial Neural Network, its various characteristics and business applications. A Neural Network is a machine which is designed to work like brain. It has the ability to perform complex calculations with ease. 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. 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. In our project, we have learned different neural network architectures as well as training algorithms. Sequential machine is successfully implemented using a Jordan network, trained with back-propagation algorithm. This sequential machine was used for encryption with the starting key as the key for decryption process. Chaotic neural network is also used for Cryptography.

Keywords: Artificial neural network, cryptography, sequential machine, chaotic neural network, Jordan network

I. INTRODUCTION

A neural network is a machine which is designed for modelling the way in which the brain performs a particular task. The network is implemented by using electronic components or it is simulated in software on a digital computer. A neural network is a parallel distributed processor which is made up of simple processing units. These units have a natural propensity to store the experimental knowledge and making it available for use. Neural networks, with their remarkable ability to derive meaning from complicated or imprecise data, can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computer technique. 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. A neural network is a machine that is designed to model the way in which the brain performs a particular task. The network is implemented by using electronic components or is simulated in software on a digital computer. A neural network is a massively parallel distributed processor made up of simple processing units, which has a natural propensity for storing experimental knowledge and making it available for use. It resembles the brain in two respects:

1. Knowledge is acquired by the network from its environment through a learning process.
2. Interneuron connection strengths, known as synaptic weights, are used to store the acquired knowledge.

Neural networks, with their remarkable ability to derive meaning from complicated or imprecise data, can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computer techniques. Other advantages include:

1. Adaptive learning: An ability to learn how to do tasks based on the data given for training or initial experience.
2. Self-Organization: An ANN can create its own organization or representation of the information it receives during learning time.
3. Real Time Operation: ANN computations may be carried out in parallel, and special hardware devices are being designed and manufactured which take advantage of this capability.

II. ANN STRUCTURE

Artificial neural network contains simple processing units. These units communicate with each other by sending signals to each other. There are some aspects of ANN are:

1. A set of processing units i.e. neuron or cell
2. A state of activation for every unit (yk), which is equivalent to the output of the unit
3. Interunit connections. Each connection is having weights
4. A propagation rule, which determines effective input Sk of a unit
5. An activation function Fk, which determines the new level of activation based on the effective input sk(t)
6. An external input (aka bias, offset) θk for each unit
7. A method for information gathering (the learning rule)

DOI 10.17148/IARJSET.2015.2419

8. An environment within which the system must operate, providing input signals and if necessary error signals.

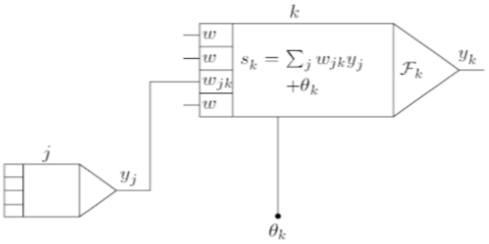

Fig. 1 Basic component of ANN

III. NETWORK ARCHITECTURES

There are three network architectures:

1. Single Layer feed forward networks – In this layer, the input layer consist of sourcenode that results the output in the form of neuron. It is feed forward type of network.
2. Multilayer feed forward networks – It only adds an extra layer known as hidden layer. Because of this hidden layer higher level of statistic is obtained.
3. Recurrent Network – This network contains at least one feedback loop. In this loop, output of a neuron is fed back into its own input which increases learning capability. And it also increases performance.

IV. BACKPROPAGATION

There are so many restrictions in single layer feed forward network. So we use backpropagation to reduce the errors. The errors for the units of the hidden layer are determined by back-propagating the errors of the units of the output layer. This method is Backpropagation learning rule. It can also be considered as generalization of delta rule for multilayer function.

4.1 Generalized Delta Rule –

This formula computes δ's for all units in the network. This generalized delta rule is for feed-forward network of non- linear units.

$$\delta_h^p = \mathcal{F}'(s_h^p) \sum_{o=1}^{N_o} \delta_o^p w_{ho}.$$

Fig. 2 Delta rule

V. CRYPTOGRAPHY

There are so many aspects of security and so many applications are also to use higher level security. Cryptography is one of the technique which is used to obtain security. Cryptography is the science of writing plain data into secret code to provide security. Cryptography is used when communication is done over untrusted medium. Cryptography not only protects data but also used to authenticate the user. 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.

There are three types of cryptographic schemes used to accomplish these goals:

1. Secret key cryptography –

With secret key cryptography, a single key is used for both encryption and decryption. As shown in the figure, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key (or ruleset) to decryptthe message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

2. Public-key cryptography –

A two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key. In PKC, one of the keys is designated the public key and may be advertised as widely as the owner wants. The other key is designated the private key and is never revealed to another party. It is straight forward to send messages under this scheme.

3. Hash functions –

Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense, use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents, often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.

VI. APPLICATION OF NEURAL NETWORK

6.1 Sequential Machine

A sequential machine is a device in which the output depends in some systematic way on variables other than the immediate inputs to the device. The other variables are state variables given to the machine which depends on the state of the machine. Output of sequential machine depends on input to sequential machine and state of the machine. So Jordan network resembles the sequential machine. The network has an input layer, a hidden layer and output layer.

The size of network layer depends on the number of inputs and number of outputs on the state. We have used Back Propagation algorithm as learning algorithm. And transfer function in hidden layer is sigmoid function. Sequential adder and sequential detector is used for implementation of sequential machine.

6.1.1 Serial adder

It accepts two serial strings as input and produces the sum of the two bit streams as output.

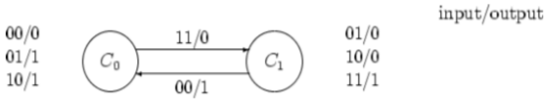

Fig. 3 Sequential Adder

6.1.2 Serial Detector

A state machine is required which gives outputs logic 1 whenever a particular sequence is detected in the input data stream, and otherwise which gives output as zero. One bit is supplied at a time.

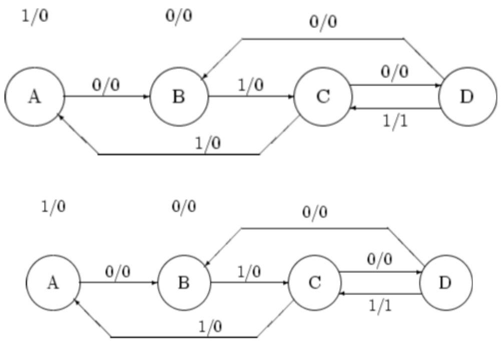

Fig. 4 Sequential Detector

6.2 Combinational Logic

Combinational logic contains input variables, output variables, logic gates and interconnections. For Combinational logic output value is solely determined from input values. The interconnected logic gates accepts signals from inputs and produces output at outputs. Each input and output variable exists physically as a binary signal that represents logic 1 or logic 0. For n input variables, there are 2ˆn possible binary input combinations. For each binary combination of the input variables, there is one possible binary value on each output. A combinational circuit can be specified by a truth table that lists the output values for each combination of the input variables.

VII. CRYPTOGRAPHY USING SEQUENTIAL MACHINE

A sequential machine has been implemented using the back- propagation algorithm. For use of sequential machine for encryption and decryption, a state diagram is drawn and a state table is obtained. Training set is generated using this state table. The input set includes all the possible inputs and states possible whereas the output consists of the encrypted or decrypted output and the next state. The output is dependent on the starting key used in sequential machine. If starting key is not known then it is not possible to retrieve decrypted data even though knowing the working of sequential machine and state table. The encrypted data will depend upon the present state of the machine. Therefore, the starting state along with the input will generate an output and then the state will change according to the state table. In case of two states, if it not known whether the state is „0‟ or „1‟, the data cannot be decrypted and hence the starting state acts as a key.

VIII. CRYPTOGRAPHY USING CHOTIC NETWORK

Chaos is statistically indistinguishable from randomness and still it is deterministic and not random. Chaotic system will produce different results for same input. It means you cannot predict the working of this system. It changes every time. Therefore this system cannot be break easily. When the weights and biases are determined by chaotic sequence then this network is known as chaotic neural network. Chaotic neural networks offer greatly increase memory capacity. The chaotic neural network can be used to encrypt digital signal. It provides high security.

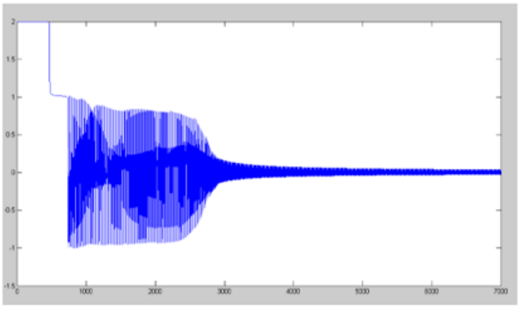

Fig. 5 plotted graph of error function after learning process

IX. CONCLUSION

Artificial Neural Networks is a powerful technique that has the ability to emulate highly complex computational machines. We have used this technique to build simple sequential machine and combinational logic using back-propagation algorithm. Artificial Neural Networks can be used to implement much complex combinational as well as sequential circuits. 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 analysed. Better results can be achieved by improvement of code or by use of better training algorithms. Thus, ANN can be used as a new method of encryption and decryption of data.

REFERENCES

[1]. 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.

[2]. 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

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

[4]. 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.