Encryption and Decryption using Multi-Layer Artificial Neural Network

Sameer Dixit[1], Amit Srivastava[2], Kamlash Chandra Maurya[3]
Assistant Professor, Computer Science Engineering, Integral University, Lucknow, India[1, 2, 3]

Abstract- *Cryptography is the science of using mathematics to encrypt and decrypt data. Today cryptography is more than secret writing, more than encryption and decryption. Authentication is as fundamental a part of our lives as privacy. 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 by artificial neural network. Artificial neural network is the best way to generate secret key. We are using artificial neural networks in the field of cryptography. Method is ANN based n-state sequential machine. In our project, we have learned different neural network architectures as well as training algorithms.*

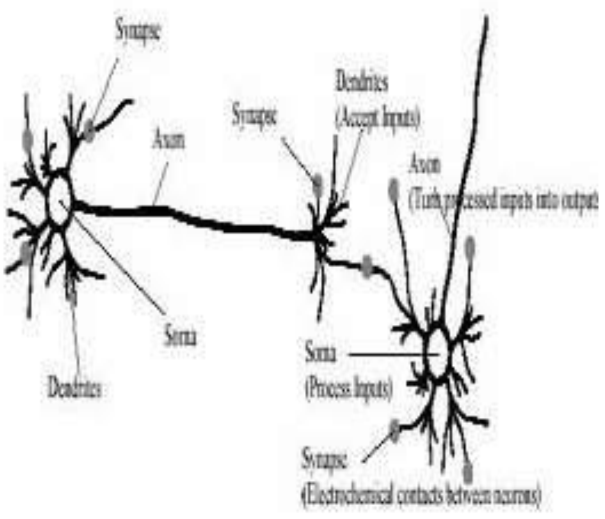
Keywords- Artificial neural network, cryptography

I. INTRODUCTION

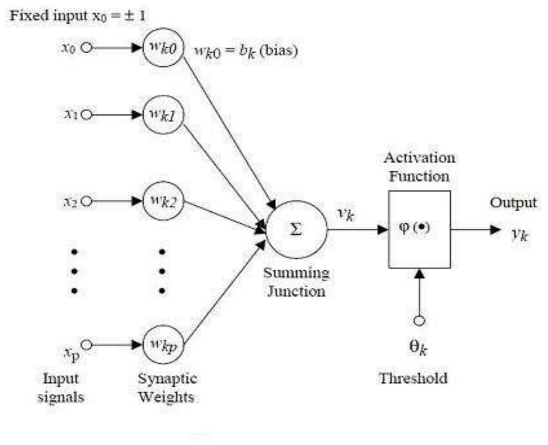
Artificial Neural Network

An ANN is efficient information processing system which resembles in characteristics with a biological neural network.

The biological neuron consists of three main parts.
Soma or cell body – where the cell nucleus is located.
Dendrites – where the nerve is connected to the cell body.
Axon – This carries the impulses of the neuron.

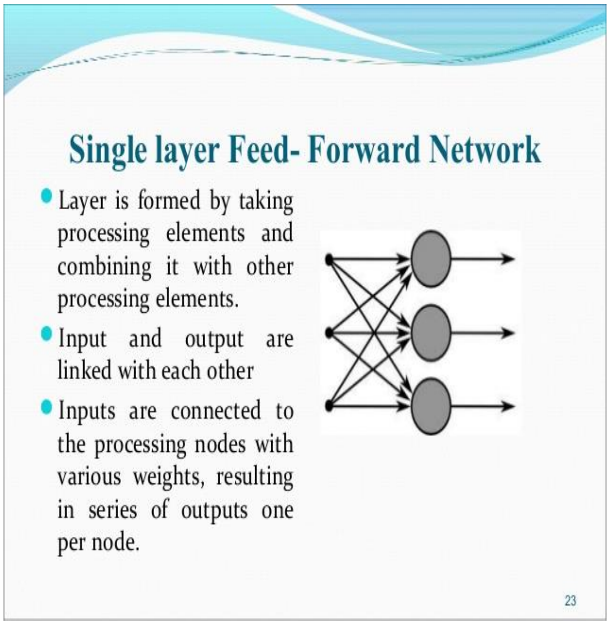


Mathematical Representation of ANN



$Y_{in} = bk + \Sigma\ xpwkp$ output $y = f\ (Yin)$

II. NETWORK ARCHITECTURES



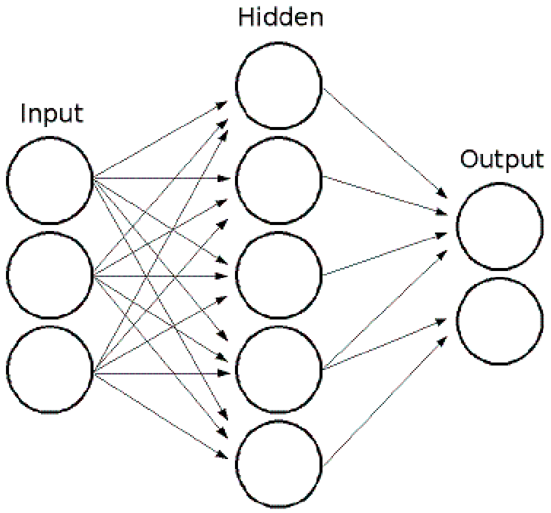
Single layer Feed- Forward Network

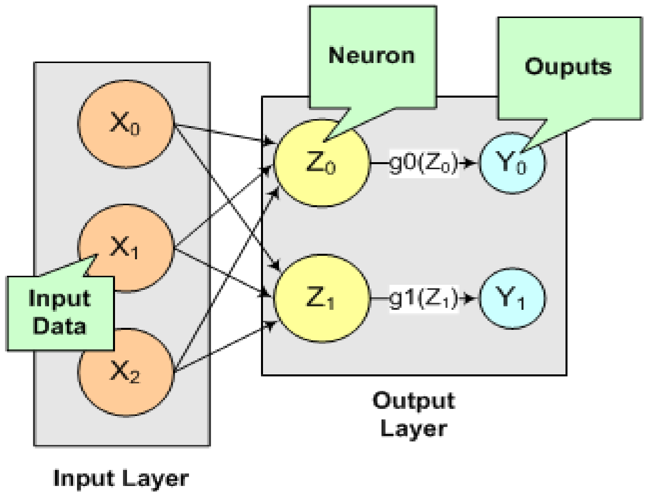
- Layer is formed by taking processing elements and combining it with other processing elements.
- Input and output are linked with each other
- Inputs are connected to the processing nodes with various weights, resulting in series of outputs one per node.

23

Multilayer Feed-Forward Network

A multilayer feed forward neural network is an interconnection of perceptrons in which data and calculations flow in a single direction, from the input data to the outputs. The number of layers in a neural network is the number of layers of perceptrons. The simplest neural network is one with a single input layer and an output layer of perceptrons. Technically, this is referred to as a one-layer feed forward network with two outputs because the output layer is the only layer with an activation calculation.





A Single-Layer Feedforward Neural Net

In this single-layer feed forward neural network, the network's inputs are directly connected to the output layer perceptrons, Z_1 and Z_2. The output perceptrons use activation functions, g_1 and g_2, to produce the outputs Y_1 and Y_2.
Since

$$Z_1 = \sum_{i=1}^{3} W_{1,i} x_i - \mu_1 \quad \text{and} \quad Z_2 = \sum_{i=1}^{3} W_{2,i} x_i - \mu_2 ,$$

$$Y_1 = g_1(Z_1) = g_1(\sum_{i=1}^{3} W_{1,i} x_i - \mu_1) ,$$

and

$$Y_2 = g_2(Z_2) = g_2(\sum_{i=1}^{3} W_{2,i} x_i - \mu_2) .$$

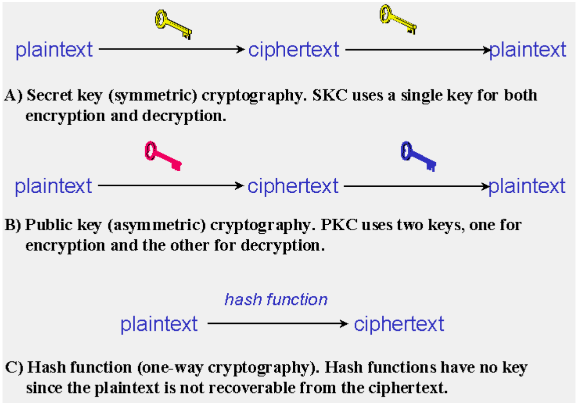
When the activation functions g_1 and g_2 are identity activation functions, the single-layer neural net is equivalent to a linear regression model. Similarly, if g_1 and g_2 are logistic activation functions, then the single-layer neural net is equivalent to logistic regression. Because of this correspondence between single-layer neural networks and linear and logistic regression.

III. CRYPTOGRAPHY

Cryptography is one of the techniques 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

- *Secret Key Cryptography (SKC):* Uses a single key for both encryption and decryption; also called *symmetric encryption*. Primarily used for privacy and confidentiality.
- *Public Key Cryptography (PKC):* Uses one key for encryption and another for decryption; also called *asymmetric encryption*. Primarily used for authentication, non-repudiation, and key exchange.
- *Hash Functions:* Uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint. Primarily used for message integrity.



A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

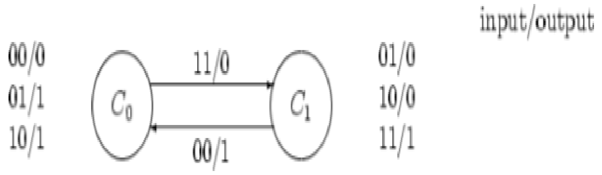
APPLICATION OF NEURAL NETWORK

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.

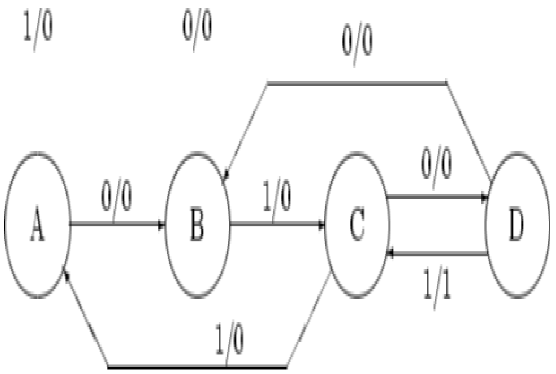
Serial adder

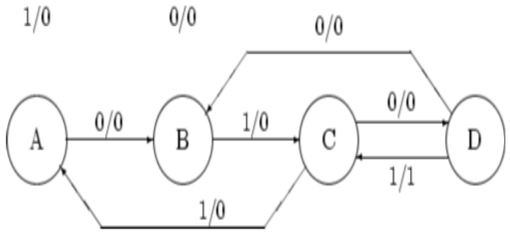
It accepts two serial strings as input and produces the sum of the two bit streams as output.



Serial Detector

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





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.

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 isnot 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.

IV. CONCLUSION

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. 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.

REFERENCES

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

[2] Novel image encryption/decryption scheme based on chaotic neural networks by Nooshin Bigdeli, Yousef Faridn, Karim Afshar.

[3] C. Boyd, "Modem Data Encryption," Electronics & Communication Journal, pp. 271-278, Oct. 1993. 131 N. Bourbakis and C. Alexopoulos, "Picture Data