ACCOMPLISHMENT OF CRYPTOGRAPHY USING NEURAL NETWORK IN ARTIFICIAL INTELLIGENCE

Paritoshik[1], Parul Choudhary

[1]B.E. Student , KITE , Raipur (CG)

[2]Asst. professor , KITE , Raipur (CG)

Email id: paritoshik4@gmail.com, cparul2605@gmail.com

ABSTRACT

In the recent years there has been quite a development in the field of artificial intelligence one of which has been the introduction of the artificial neural networks (ANN). The ANN can be considered as an information processing unit which to a great extent resembles the working of the human brain. Its utilization has spread through various fields namely bioinformatics, stock market predictions, medical science, weather forecasting etc. One of these fields in which ANN has been indispensable is cryptography. Recently there has been quite a study going on various encryption methods based on neural nets comprising of single layer or multilayer perceptron models. This field of cryptography is more popularly known as Neural Cryptography. Cryptography is the one of the main categories of computer security that converts information from its normal form into an unreadable form. An Artificial Neural Network (ANN) is an information processing paradigm that is inspired by the way biological nervous systems, Neural Network (NN) has emerged over the years and has made remarkable contribution to the advancement of various fields of endeavor. The purpose of this paper is to using neural networks on Cryptography, In this paper also, I have examined and analysed the various architectures of NN.

Keywords*:-Artificial neural network, Cryptography, Decryption, Encryption,multilayer perceptron,optimal neural network.*

1. Introduction

Cryptography refers to the tools and techniques used to make messages secure for communication between the participants and make messages immune to attacks by hackers. Cryptography uses mathematical techniques for information security. The cryptography deals with building such systems of security of news that secure any from reading of trespasser. Systems of data privacy are called the cipher systems. The file of rules are made for encryption of every news is called the cipher key. Encryption is a process, in which we transform the open text, e.g. message to cipher text according to rules. Cryptanalysis of the news is the inverse process, in which the receiver of the cipher transforms it to the original text. The cipher key must have several heavy attributes. The best one is the singularity of encryption and cryptanalysis. The open text is usually composed of international alphabet characters, digits and punctuation marks. The cipher text has the same composition as the open text. Very often we find only characters of international alphabet or only digits. The reason for it is the easier transport per media. The next cipher systems are the matter of the historical sequence: transposition ciphers, substitution ciphers, cipher tables and codes. Simultaneously with secrecy of information the tendency for reading the cipher news without knowing the cipher key was evolved. Cipher keys were watched very closely. The main goal of cryptology is to guess the cipher news and to reconstruct the used keys with the help of

goodanalysis of cipher news. It makes use of mathematical statistics, algebra, mathematical linguistics, etc., as well as known mistakes made by ciphers too. The legality of the open text and the applied cipher key are reflected in every cipher system. Improving the cipher key helps to decrease this legality. The safety of the cipher system lies in its immunity against the decipher. The goal of cryptanalysis is to make it possible to take a cipher text and reproduce the original plain text without the corresponding key. Two major techniques used in encryption are symmetric and asymmetric encryption. In symmetric encryption, two parties share a single encryption-decryption key. The sender encrypts the original message (P), which is referred to as plain text, using a key (K) to generate apparently random nonsense, referred to as cipher text
(C), i.e.:
C = Encrypt (K, P)
(1) Once the cipher text is produced, it may be transmitted. Upon receipt, the cipher text can be transformed back to the original plain text by using a decryption algorithm and the same key that was used for encryption, which can be expressed as follows:
P = Decrypt (K, C)
(2) In asymmetric encryption, two keys are used, one key for encryption and another key for decryption. The length of cryptographic key is almost always measured in bits. The more bits that a particular cryptographic algorithm allows in the key, the more keys are possible and the more secure the algorithm becomes. The following key size recommendations should be considered when reviewing protection:
Symmetric key: • Key sizes of 128 bits (standard for SSL) are sufficient for most applications.
• Consider 168 or 256 bits for secure systems such as large financial transactions Asymmetric key:
• Key sizes of 1280 bits are sufficient for most personal applications
• 1536 bits should be acceptable today for most secure applications
• 2048 bits should be considered for highly protected applications. Hashes:
• Hash sizes of 128 bits (standard for SSL) are sufficient for most applications
• Consider 168 or 256 bits for secure systems, as many hash functions are currently being revised (see above). NIST and other standards bodies will provide up to date guidance on suggested key sizes.

2.Artificial Neural Network (Ann)

Artificial Neural Network is an information processing and modelling system which mimics the learning ability of biological systems in understanding unknown process or its behaviour. ANN is configured for a specific application, such as pattern recognition or data classification, through a learning process. Learning in biological systems involves adjustments to the synaptic connections that exist between the neurons. This is true of ANNs as well. ANNS have developed as generalizations of mathematical models of human cognition or neural biology. Based on the assumptions that:
1. Information procures at many simple elements called neuron.
2. Signals are passed between neurons over connection links.
3. Each connection link has associated weight. Which in a typical neural net multiplies the signal transmitted?
4. Each neuron applies an activation function usually nonlinear to its net input (sum of weighted input signals) to determine its output signal.

An Artificial Neural Network is a network of many very simple processors (units), each possibly having a (small amount of) local memory. The units are connected by unidirectional communication channels which carry numeric data. The units operate only on their local data and on the inputs they receive via the connections. The design motivation is what distinguishes neural networks from other mathematical techniques: A neural network is a processing device, either an algorithm, or actual hardware, whose design was motivated by the design and functioning of human brains and components.

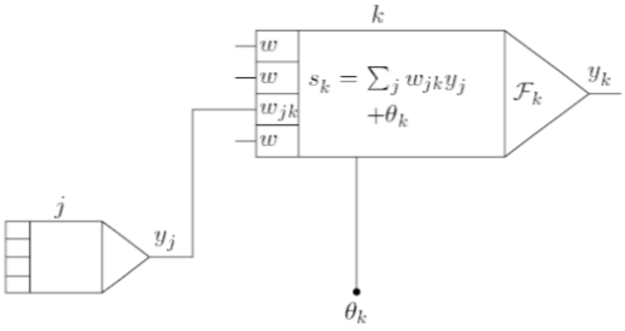


Figure 1: The bas

There are many different types of Neural Networks, each of which has different strengths particular to their applications. The abilities of different networks can be related to their structure, dynamics and learning methods.

3.Cryptography Techniques

Cryptography is usually referred to as ―the study of secret‖. Encryption is the process of converting normal text to unreadable form; while decryption is the process of converting encrypted text to normal text in the readable form. Important aspects of encryption and decryption are privacy, authentication, identification, trust and verification. As the security demand increases the cost of cryptography algorithm increases [1]. There are two types of cryptosystems; symmetric cryptosystems and asymmetric cryptosystems. Symmetric cryptosystems use the same key for encryption and decryption. On the other hand, asymmetric cryptosystems use two different keys; a public key for encryption and a private key for decryption. Furthermore, symmetric encryption algorithms are very efficient at processing large amounts of information and computationally less intensive than asymmetric encryption algorithms. There are two types of symmetric encryption algorithms: stream ciphers and block ciphers which provide bit-by-bit and block encryption respectively.

4. Architecture Of Neural Networks

Neural networks are not only different in their learning processes but also different in their structures or topology, can be divided the network architectures into the following classes:

□ □**Basic Architecture of a Feed-forward Network**

The feed-forward network topology illustrated in Fig.2 permits signals to travel one way only, from the input through the hidden layer to the output layer. These types of networks are somehow straight forward and associate inputs with outputs. This kind of organization is also referred to as bottom-up or top-down and commonly used in pattern recognition. Fig.2 also shows the commonest type of artificial neural network which consists of two layers. The hidden layer neurons are connected to the output layer neurons. The functions of each layer in the network are defined below:

a) The input layer neurons represent the pre-processed data fed into the network.

b) The input of each hidden layer neuron is defined by the sum of the input vector set and the connection weights between the input layer and hidden layer.

c) The input of the output neuron is determined by the weighted sum of outputs of the hidden layer neurons.

d) The output of a neuron is defined by the type of the transfer function used in that specific layer. This type of network is attractive because the hidden neurons are free to develop their individual representations from the input set.

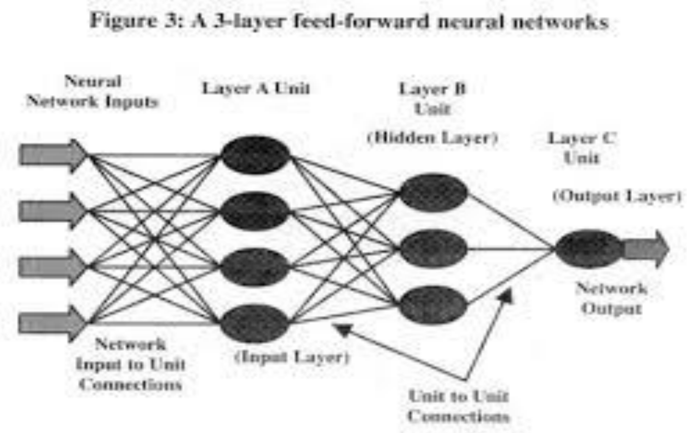


Fig. 2: Architecture of a feedforward neural network

The Perceptron – A Network for Decision Making

The perceptron, a basic neuron, invented by Rosenblatt in 1957 at the Cornell Aeronautical Laboratory in an attempt to understand human memory, learning, and cognitive processes prior to his demonstration on the first machine that could "learn" to recognize and identify optical patterns in the early 1960. The mathematical model of the perceptron or artificial neuron is modelled in the similar manner of the biological architectural set-up. Again, the three major components are considered: Axons and synapses of the neuron are modelled as inputs and weights respectively.[6] The strength of the connection between an input and a neuron is denoted by the value of the weight. The mathematical model of this topology is illustrated in Fig.3.

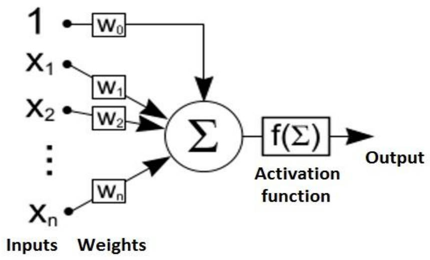


Fig.3: A perceptron model

5. Learning Of Artificial Neural Networks

By learning rule we mean a procedure for modifying the weights and biases of a network. The purpose of learning rule is to train the network to perform some task. They fall into three broad categories:

1. Supervised learning -The learning rule is provided with a set of training data of proper network behaviour. As the inputs are applied to the network, the network outputs are compared to the targets. The learning rule is then used to adjust the weights and biases of the network in order to move the network outputs closer to the targets.

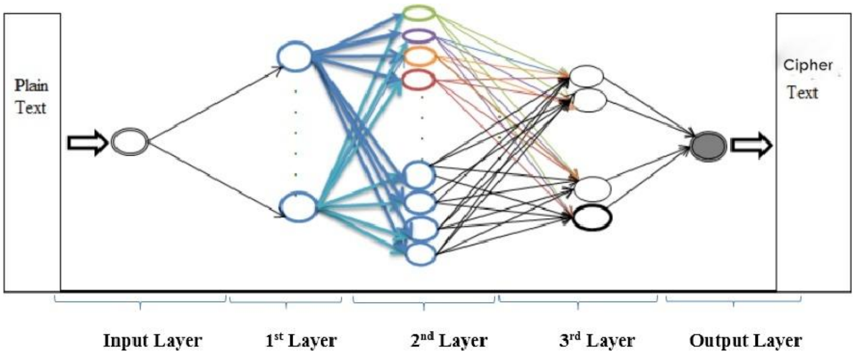
2. Reinforcement learning-it is similar to supervised learning, except that, instead of being provided with the correct output for each network input, thealgorithm is only given a grade. The grade is a measure of the network performance over some sequence of inputs.

3. Unsupervised learning-The weights and biases are modified in response to network inputs only. There are no target outputs available. Most of these algorithms perform some kind of clustering operation. They learn to categorize the input patterns into a finite number of classes.

6. Design Of Cryptography Based On Neural Networks

Cryptography is the practice and study of hiding information through techniques based on randomness. So, in neural cryptology, the ANN has to be a form of random topology. The structure of networks changes randomly. The training and transfer functions of the network are also selected randomly. ANN with random topology in cryptography is depicted in Fig. 4, the input is plain text that is encrypted by NN- using encryption algorithm and output of NN is Cipher text. The transfer functions and training algorithms are also selected according to the NN-based pseudo-random number generator.

Fig. 4.1:General structure of a block cipher



7. Methodology

Multilayer Perceptron Neural Networks are used. MLP NN is as shown in Figure 1. These were adapted by using backpropagation. .

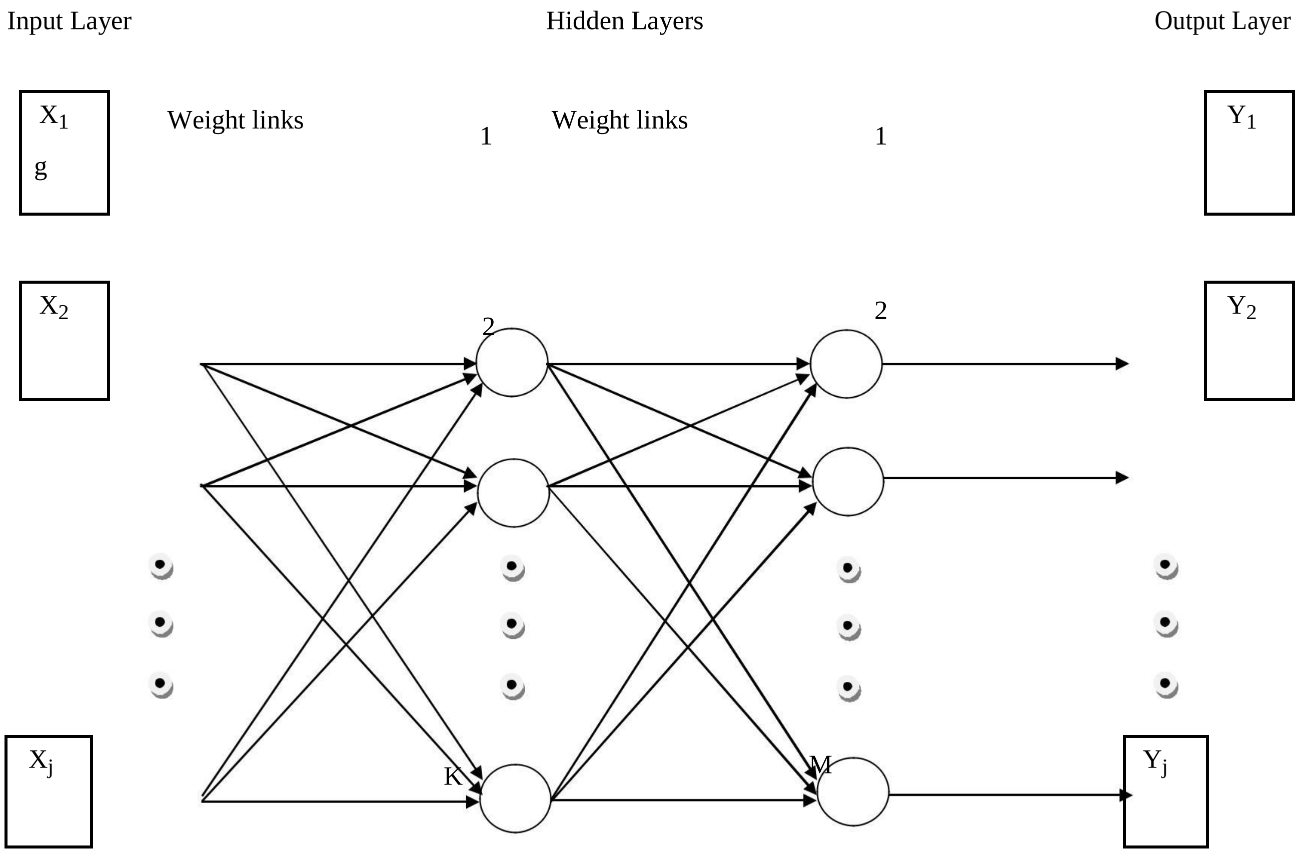


Figure 5 Multilayer Perceptron Neural Network

Usually a fully connected variant is used, so that each neuron from the n-th layer is connected to all neurons in the (n+1)-th layer, but there are no connections between neurons of the same layer. A subset of input units has no input connections from other input units; their states are fixed by the problem. Another subset of units is designated as output units; their states are considered the result of the computation. Units that are neither input nor output are called as hidden units [1]. A simple Artificial Neuron is as shown in Figure 2.

Basic computational unit is called as a neuron. It receives the inputs $x_1, x_2, x_3, \ldots\ldots, x_n$ which are associated withweights $w_1, w_2, w_3, \ldots\ldots\ldots, w_n$. This unit computes:

$$y_i = f(\ _j(w_{ij}x_j))$$

Where, w_{ij} refers to the weights from unit j to unit i and function f is unit's activation function

Backpropagation algorithm usually uses a logistic sigmoid activation function as follows:

$$f(t) = 1/(1+e^{-t})$$

Where, $-\infty < t < \infty$

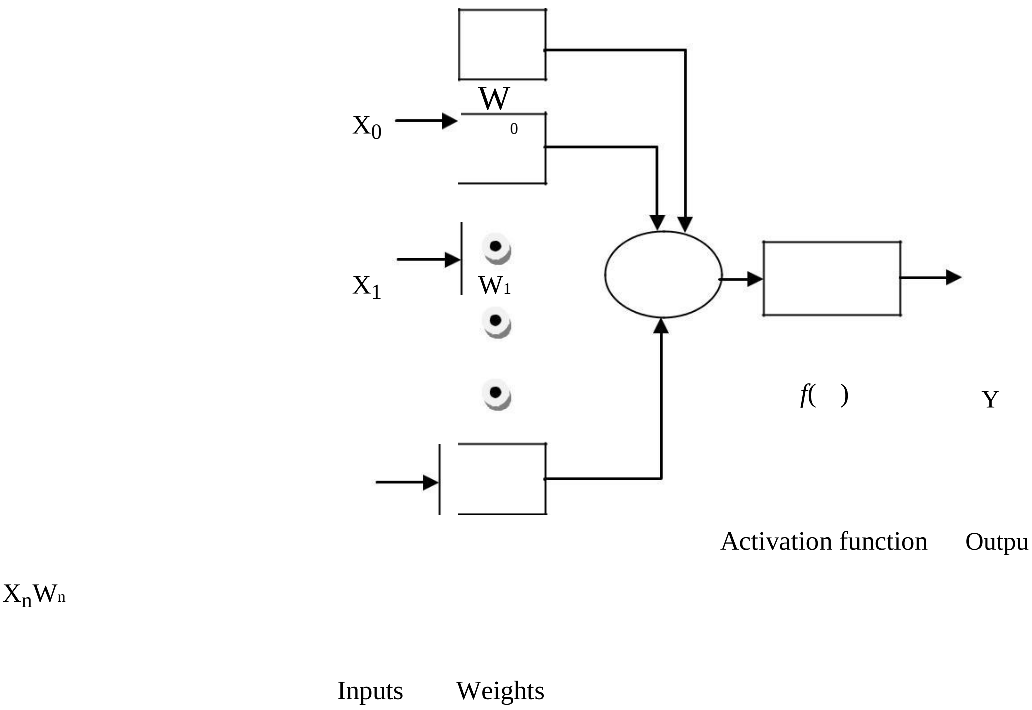


Figure 5 Simple Artificial Neuron

Backpropagation algorithm belongs to a group of "gradient descent methods". Backpropagation algorithm searches for the global minimum of the weight landscape by descending downhill in the most precipitous direction. The initial position is set at random selecting the weights of the network from some range. Backpropagation using a fully connected neural network is not a deterministic algorithm. The basic backpropagation algorithm can be summed up in the following equation (the delta rule) for the change to the weight *wji*from node *i*to node *j*:

$\boldsymbol{\Delta} wji= \eta\times\delta j\times yi$

That means weight change ($\boldsymbol{\Delta} wji$) is equal to the multiplication of learning rate (η), local gradient (δj) and input signal to node*j* (*yi*).

Where, the local gradient δj is defined as follows:

□ If node*j* is an output node, then

$\delta j = \varphi'(vj)\times ej$

Where, *ej*is error signal, $\varphi'()$ is the logistic function, *vj* is the total input to node *j* (i.e. $\Sigma iwjiyi$), *ej*is the error signal for node *j* (i.e. difference between desired output, actual output)

□ If node*j* is a hidden node, then

$\delta j = \varphi'(vj)$ &*Sigmak*δ*kwkj*

Where, *Sigmak*δ*kwkj*is the weighted sum of the δ's computed for the nodes in the next hidden or output layer that are connected to node *j* and *k* ranges over those nodes for which *wkj*is non-zero (i.e. nodes *k* that actually have connections from node *j*). The *δk* values have already been computed as they are in the output layer (or a layer closer to the output layer than node *j*) .

Design of optimal mlpnn

Neural networks are used as an encryption and decryption algorithm in cryptography. The block diagram is as shown in Figure 6.Parameters of both neural networks were then included into cryptography keys (i.e. Secret keys). Topology of each neural network is based on their training sets

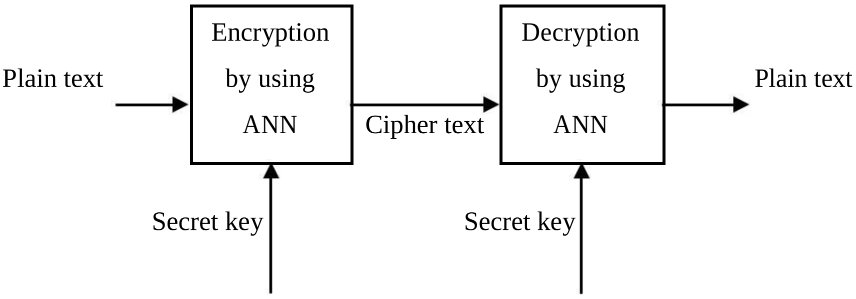


Figure 6. Block of Cryptography by using ANN

As an example of the encryption process, the encryption is performed on input string of digits where each digit is developed using 6-bits and also 6-bit output has to be produced after the encryption process (refer to Table 1).

Table 1: Training sets with plain digits and corresponding cipher text

THE PLAIN TEXT			THE CIPHER TEXT
Character	**ASCII code (DEC)**	**The chain of bits**	**The chain of bits**
0	48	110000	111111
1	49	110001	110010
2	50	110010	101100
3	51	110011	111010
4	52	110100	101010

5	53	110101	100011
6	54	110110	111000
7	55	110111	000111
8	56	111000	010101
9	57	111001	110011

Thus, both encryption and decryption systems were designed using MLP NN as follows:

- •6 bit input to single hidden layer MLP NN.
- •6 bit output from the single hidden layer MLP NN.
- •There is no predetermined number of units in the hidden layer.

Both networks were trained on binary representations of symbols (i.e. digits). In each training set, chains of numbers of the plain digits are equivalent to binary values of their ASCII code and the cipher text is a random chain of 6 bits

The security for all encryption and decryption systems is based on a secret key. Simple systems use a single key for both encryption and decryption (i.e. symmetric cryptography). The robust systems use two keys (one for encryption and another one for decryption i.e. asymmetric encryption). If we use the neural network as encryption and also decryption algorithm, their keys have adapted neural networks parameters; which are their topologies (architecture) and their configurations (weight values on connections in the given order)

Generally, for single hidden layer MLP NN each key is written as follow:

[Input, Hidden, Output, Weights coming from the input units, Weights coming from the hidden units] Where,

- •Input is the number of binary inputs to MLP NN.
- •Hidden is the number of neurons in the hidden layer.
- •Output is the number of binary output from MLP NN.
- •Weights coming from the input units are weight values coming from the input to hidden units in a predefined order.
- •Weights coming from the hidden units are weight values coming from the hidden units to output units in a predefined order

Parameter values of encrypting MLP NN in our experimental study are the following:

- •Input layer consists of 6 bit binary input.
- •Output layer consists of 6 bit binary output, used to define the encrypted output message.
- •Fully connected networks.
- •A sigmoid activates function.

In this model, a 6-bit plain text is entered and a 6-bit cipher text is the output.

For example, if we want to send the following message of some digits:

"258025001253456"

Encryption process is as follows:

The plain text is coded into the chain:

(110010110101111000110000110010110101110000110000110001110010110101110011110100110101110
110)

Now, break it down into blocks (N=6), thus:

110010 110101 111000 110000 110010 110101 110000 110000 110001 110010 110101 110011 110100 110101
110110

The corresponding cipher text is the following:

(1011001000110101011111111011001000111111111111111001010110010001111010101010100011111000)

The encrypted data will then be transmitted to the recipient.

After training the MLP NN for maximum 100 epochs (three times each with number of hidden neurons from 2 to 20) for the given data sets using MATLAB the plot of average mean square error (mse) verses number of neurons and plot of average accuracy verses number of neurons are obtained as shown in Figure 7 and Figure 8 respectively.

It is required to get minimum mse and maximum accuracy. When number of hidden neurons is 5, then both minimum error and maximum accuracy are achieved as per Figure 7 and Figure 8. Therefore, optimal configuration for the encryption MLP NN is 5 sigmoidal neurons in the hidden layer with 6 bit inputs and 6 bit outputs. Similarly, MLP NN for the decryption process could be design.

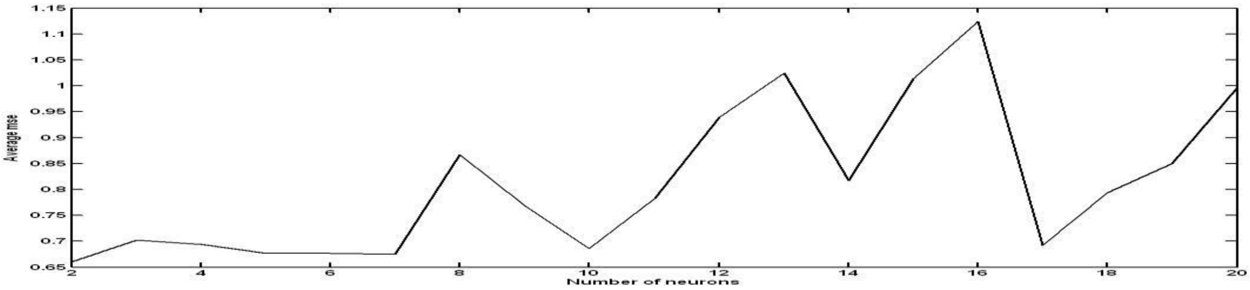


Figure 7 Plot of Average mse verses number of neurons

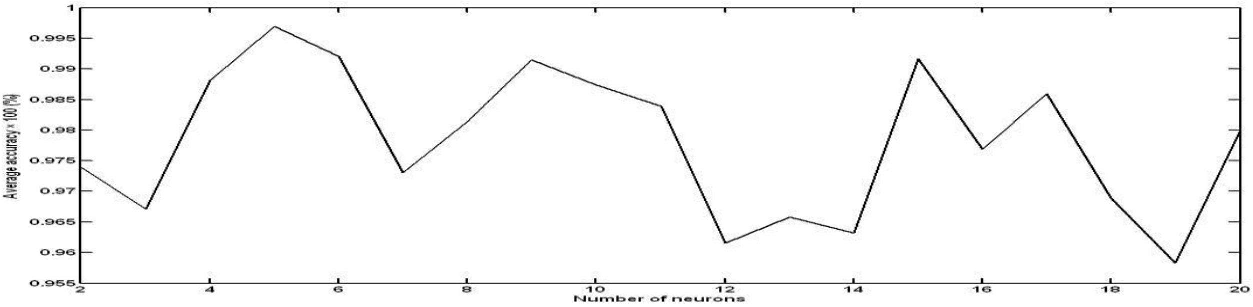


Figure 8 Plot of Average accuracy verses number of neurons

8. Conclusions

Next development in robust cryptography is represented by neural network application. Optimal neural network with minimum number of neurons is designed to get minimum error and maximum accuracy for cryptography application. The limitations of this type of system are few, but potentially significant. This is effectively a secret-key system, with the key being the weights and architecture of the network. With the weights and the architecture, breaking the encryption becomes trivial. However, both the weights and the architecture are needed for encryption and decryption. Knowing only one or the other is not enough to break it. The advantages to this system are that it appears to be exceedingly difficult to break without knowledge of the methodology behind it, as shown above. In addition, it is tolerant to noise. Most messages cannot be altered by even one bit in a standard encryption scheme.

- The computing world has a lot to gain from neural networks. Their ability to learn by example makes them very flexible and powerful.
- Neural network will never replace conventional methods, but for a growing list of applications, the neural network architecture will provide for a complement to these existing techniques.
- Artificial Neural Networks is a powerful technique that has the ability to emulate highly complex computational machines. We have used this technique to build cryptography systems.
- The use of ANN in the field of Cryptography is very good method because the NN can process information in parallel, at high speed, and in a distributed manner.

9. 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 Cmmunications, 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]An Introduction to the Modelling of Neural Networks, P. Peretto, ISBN 0-521-41451-2 hardback, ISBN 0-521-42487-9 paperback

[7]. Use of Artificial Neural Network in the Field of Security, ISSN 2230-7621, MIT International Journal of Computer Science & Information Technology Vol. 3, No. 1, Jan. 2013, pp. 42–44

[8] HiralRathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, “Design and Implementation of Image EncryptionAlgorithm 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 andNoise Effects on it”, International Journal of Computer Applications (0975 - 8887) Vol.23, No.6, June 2011.

[10] Michal Janosek, Eva Volna, Martin Kotyrba, Vaclav Kocian, “Cryptography based on Neural Network” Proceedings 26th European Conference on Modeling and Simulation, Year 2012. www.scs-europe.net/conf/ecms

[11] K. Mandal, Arindam Sarkar, “An Adaptive Neural Network Guided Secret Key based Encryption through Recursive Positional Modulo-2 Substitution for Online Wireless Communication (ANNRPMS)”, IEEE-International Conference on Recent Trends in Information Technology, pp. 107-112, June 3-5, 2011.