INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

SECURED DATA PROCESSING OF BACK PROPAGATION NETWORK USING PRIVATE KEY

Dr.V.Jeyalakshmi[1], L.Saikishore[2] and P.Jayarajan[3]

[1] *Professor, Dept. Electronics and Communication Engineering*
[2] *PG Student- M.Tech. Applied Electronics*
[3]*Associate Professor, Dept. Electronics and Communication Engineering,*
Dr.MGR Educational and Research Institute, University,Chennai, Tamil Nadu, India.
Author Correspondence: [2] *PG Student- M.Tech. Applied Electronics*
Email address kishorelakshmipathy@gmail.com / jpjeya@gmail.com

Abstract

The aim of this research is to build a ciphering technique by using artificial neural network to protect data against unauthorized access to the data being transferred. The encryption data includes three stages: first Stage: - Training a network by using back propagation to obtain weights. Second Stage:- Encryption data by using the weights obtained from first stage and consider the weights of first layer as a public key. Third Stage:- Decryption data by using the weights obtained from the first stage and consider the weights of second layer as a private key. The three stages are attained 100% success for data encryption process and data getting back process. This technique is similar to coding asymmetric, and have the ability of coding a group of data such as:- text, characters, numbers and waves. This work is executed by computer type P4 with whole equipments and Mat lab language version 7.

Key words: Encryption, Decryption, Back Propagation Network.

1. Introduction

Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. In order to recover the contents of an encrypted signal easily, a correct decryption key is required. The key is an algorithm that "undoes" the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to "break" the cipher. The more complex encryption algorithm, the more difficult it is to eavesdrop on the communications without access to the key. Encryption data is implemented by using the weights which obtained from hidden layer. Decryption data is implemented by using weights obtained from output layer. The aim of this research is to build a powerful ciphering system to obtain a dynamic encrypted data and this make it more powerful against unauthorized access.

2. Related works

In 2000, Diflie and Hellmann found a method based on numbers theories for creating a secret key over a public channel accessible to any attackerIn 2000, Toru Ohira identified the Papadimitratos, P. Haas, Z.J.]"Secure data communication in mobile adhoc networks", This paper appears in: Selected Areas in Communications, IEEE Journal on Publication Date: Feb. 2006,Volume: 24, Banner, R. Orda, A "Multipath Routing Algorithms for Congestion Minimization", This paper appears in: Networking, IEEE/ACM Transactions on Publication Date: April 2007 Papadimitratos, P. Haas, Z.J and E.G.Sirer, "Path set selection in mobile ad hoc Networks" in Proc 3 rd ACM MobiHoc,Lausanne, Switzerland, Jun 2002 pp 1-11.D. Johnson, D. Maltz and J. Broch., "DSR The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks", chapter 5Karlof and D. Wagner "Secure Routing in Sensor Networks: Attacks and Countermeasures" in Proc. of the 1st IEEE Workshop on Sensor Network Protocols and Applications, publication date:april2003.

N. Milanovic, M. Malek, A. Davidson and V. Milutinovic "Routing and Security in Mobile Ad Hoc Networks", IEEE Computer Magazine, vol. 37, no. 2, February 2004. encryption process by a coupling dynamics with nonlinear threshold function and various time delays between different bits, or neurons, in the original data [2]. In 2003, The thesis of Amera I. has develop a Hebbian network through qualitative primary weight which had a large size for ciphering process [3]. This research was to build a ciphering system by using back propagation neural network technique. N.Milanovic, M. Malek, A.Davidson and V. Milutinovic"Routingand Security in Mobile Ad Hoc Networks", IEEE Computer Magazine, vol. 37, no. 2, February 2004.

3. Structure of BPN

A single layer neural network has many restrictions. This network can accomplish very limited classes of tasks. Back-propagation can also be considered as a generalization of the delta rule for non-linear activation functions and multi-layer networks. It is a systematic method of training multi-layer artificial neural networks. Figure 1 show the structure of bpn and it consists of at least three layers of units: an input layer, at least one intermediate hidden layer, and an output layer.

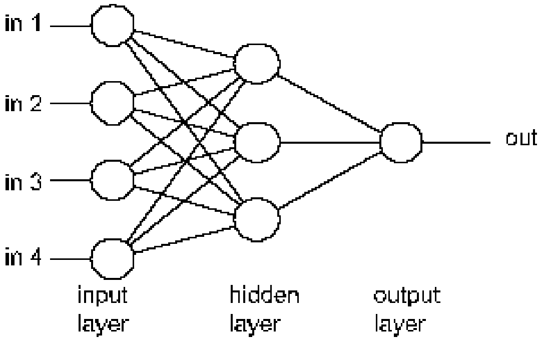

Figure1: structure of BPN

a. Algorithms

Cryptographic algorithms can generally be grouped into two different categories: 1. Symmetric key cryptosystems, which use the same key to both encrypt and decrypt the communication 2. Asymmetric cryptosystems, which use two different keys instead of a single key — one key to encrypt the communication and another to decrypt the communication

4. SECURE DATA PROCESSING

To safely transfer data via an unsecured Internet connection, companies make use of Virtual Private Network (VPN) solutions. A VPN represents the coming together of two separate networks to form a self-contained logical network. This technology enables subsidiaries to be connected to the company headquarters, or employees to set up a home office. But it also gives members of staff who work out in the field the opportunity to establish a secure connection with the company in order to exchange data.

A VPN is a purely software-based solution: no special network hardware is required to create one. To use a public network such as the Internet to establish a VPN connection between the computer at a home office and the company network, for example, the VPN client software replicates the configuration of the company network virtually on the home office computer. The client software connects via the Internet to the VPN dial-in node, and after successful authentication, enables communication between the devices using a secured VPN protocol such as IPsec, TLS/SSL or PPTP. The home office workstation thus becomes a component of the private company network. A secure connection established between the VPN dial-in node and the remote device via a public network, such as the Internet, is referred to as a VPN tunnel.

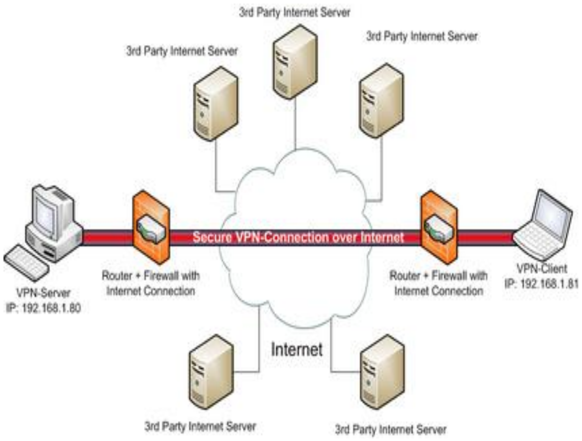
3rd Party Internet Server
3rd Party Internet Server
3rd Party Internet Server
Secure VPN-Connection over Internet
Router + Firewall with Internet Connection
Router + Firewall with Internet Connection
VPN-Server
IP: 192.168.1.80
VPN-Client
IP: 192.168.1.81
Internet
3rd Party Internet Server
3rd Party Internet Server

Figure2: Data processing using private key

5. IMPLEMENTATION OF BPN IN SECURED DATA

To communicate with each other, Speech is probably the most efficient way. It is possible to use speech as a useful interface to interact with machines. Speech recognition research work has been started since 1930. However Bangla speech recognition research work has been started since around 2000. In our system, we have captured speech from ten different speakers, which may an early attempt for developing speaker independent isolated Bangla digit speech recognition system in Bangla language. With a rich heritage, Bangla is an important language. It is spoken by approximately 8% of the world population

The encryption done for various input data using Matlab code and its corresponding compressed output has shown in the following Figure.3, Figure.4 and Figure.5

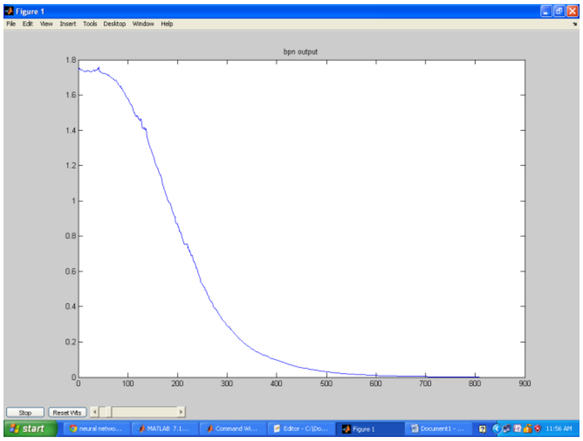

Figure3:train input[11;10;01;00]

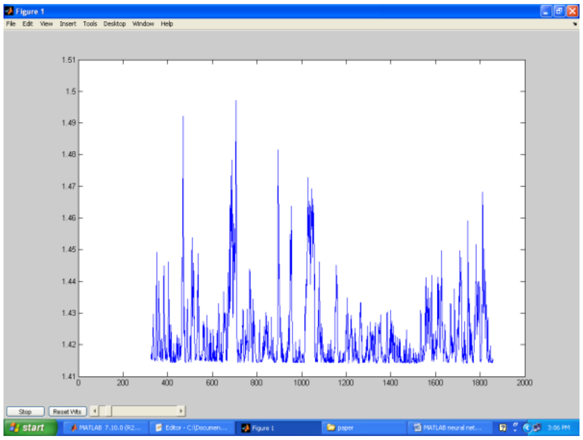

Figure4: train input[11; 11;11;11]

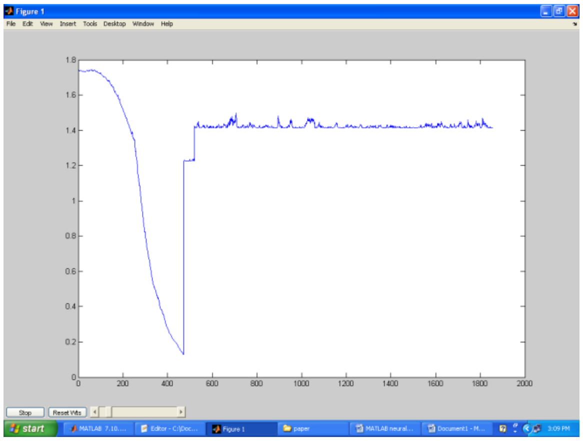

Figure5: Train input[00;01;10;11]

6. CONCLUSION

The suggested ciphering system obtains dynamic encrypted data, this make it more powerful against unauthorized access. This system used the back propagation neural network having number of input nodes equals to the number of hidden nodes and also equal to the number of output nodes. The target which the network used to train is equal to the input data in size and values. Then ciphering process consisted of three stages: 1-Training a network by using back propagation network and consider the target is equal to the input. 2-Encryption data by using the weights which obtained from input layer to hidden layer and consider these weights as a public key. 3- Decryption data by using the weights which obtained from hidden layer to output layer and consider this weights as a private key. This technique succeeded to encrypt different types of data (texts, signals type wav and binary images) and gave another advantage, when re-encrypting the same input data sample we obtained different encrypted data.

REFERENCES

[1] Stinson D. R, 1995, Cryptography: Theory and Practice , CRC press, 1995.

[2] Toru Ohira 2000, Toward encryption with neural networkanalog, Bruges (Belgium), 26-28 April

[3] Amera I., 2003, Using Hebbian network for cipher, Thesis in computer and mathematical sciencesuniversity of Mosul/Iraq.

[4] Fausett .L, 1994, Fundamental of Neural Networks,Architectures, Algorithms and Applications, PrinticeHall Int. Snc.

[5] Suresh. S, Omkar S.N, and Mani .V, 2005, Parallel Implementation of Back-Propagation Algorithm inNetworks of Workstations, IEEE Transactions On Parallel And Distributed Systems, Vol. 16, No. 1,January.

[6] The Math Works Inc. 1998, Neural Network Toolbox, ForUse with MATLAB", Ver. 6.5, MA, USA.

[7] Istook E., Martinez.T, 2013 Improved backpropagation learning in neural networks with windowed momentum, International journal of neural systems and circuit to cancer,key note.

[8] Sayood. K, 2006, Introduction of data compression, 3rd.ed elesevier 2006.

[9] yang.J, 2006, Losseless compression using 2-level and multilevel and multilevel Boolean minimization.