

A Neural Network Implementation of Chaotic Sequences for Data Encryption

Harshal Shriram Patil

M.Tech Scholar

Astral Institute of Technology and Research,
Indore, M.P., India

patil.harshal.s@gmail.com

Ms.Amita Shrivastava

Assistant Professor

Astral Institute of Technology and Research,
Indore, M.P., India

amita2016shrivastava@gmail.com

ABSTRACT

Cryptography has remained as one of the most sought after fields of research in since the past century. With the advent of digital technology resulting in extremely high data transfer rates, newer encryption algorithms which would ensure high level of data security yet have low space and time complexities are being investigated. In this paper we propose a chaotic neural network based encryption mechanism for data encryption. The heart of the proposed work is the existence of chaos in the neural network which makes it practically infeasible to any attacker to predict the output for changing inputs.[1],[2] We illustrate the design of the chaotic network and subsequently the encryption and decryption processes. Finally we examine the performance of the encryption algorithm with standard data encryption algorithms such as DES, AES, Blowfish, Elliptic curve cryptography to prove the efficacy of the proposed algorithm.[1],[2] The parameters chosen for the analysis are throughput, avalanche effect and bit independence criteria.

Keywords: - Cryptography, chaos, artificial neural network (ANN), chaos, chaotic neural network, throughput, avalanche effect, bit independence criteria.

1. INTRODUCTION

Data encryption and decryption mechanisms have been studied for over centuries now. With the advancements in digital technology, extremely high data rates have been practically feasible now days. Also, complex mathematical algorithms can be implemented on small chips thus opening up an extremely challenging new area of research in the field of cryptography. With applications from military and defense, banking and intellectual property all depending on digital data transmission,

the need for extremely secure as well as efficient encryption standards has raised manifold. With digital technology becoming accessible to various attackers too, the need for secure algorithms for data encryption becomes even more important.

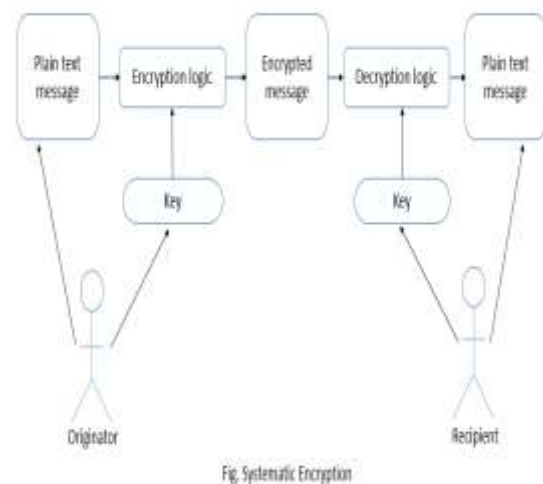


Fig1. Model of Cryptography

The above figure depicts the basic encryption and decryption model[1]. The original data of the originator is referred to as the plain text. The plain text undergoes the encryption algorithm or the encryption logic to produce the encrypted message referred to as the cipher text. Finally the cipher text undergoes the decryption logic or algorithm to yield back the plain text. The adversary or the attackers attack the cipher text and try to get the plain text. The aim of any encryption algorithm is to nullify the efforts of the attackers in obtaining the plain text.

2. ARTIFICIAL NEURAL NETWORK

Work on artificial neural network has been motivated right from its inception by the recognition that the human brain computes in an

entirely different way from the conventional digital computer.[5] The brain is a highly complex, nonlinear and parallel information processing system. It has the capability to organize its structural constituents, known as neurons, so as to perform certain computations many times faster than the fastest digital computer in existence today. The brain routinely accomplishes perceptual recognition tasks, e.g. recognizing a familiar face embedded in an unfamiliar scene, in approximately 100-200 ms, whereas tasks of much lesser complexity may take days on a conventional computer. 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.

The biological model of the neuron is shown in the figure. It consists of the cell body, axon hillock, action potential, synaptic terminal, axon of pre

synaptic neuron and dendrites. Signals from different parts of the body travel through different parts and reach the neuron where the neuron processes it and produces an output. It should be noted though that the output of a neuron may also be fed to another neuron. A collection of such neurons is called a neural network. The neural network can perform simple to complex tasks depending on the structure of the neural network.

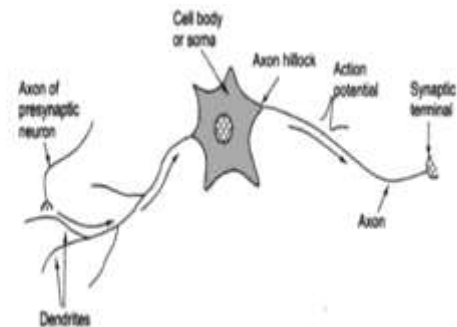


Fig.2 Biological model of neuron

After studying the basic biological model of the neural network, a mathematical model is envisaged to be designated. The mathematical model for such a neural network is given by:

$$\sum_{i=1}^n X_i W_i + \theta$$

Where X_i represents the signals arriving through various paths, W_i represents the weight corresponding to the various paths and θ is the bias. The above concept can be visualized by the following diagram:

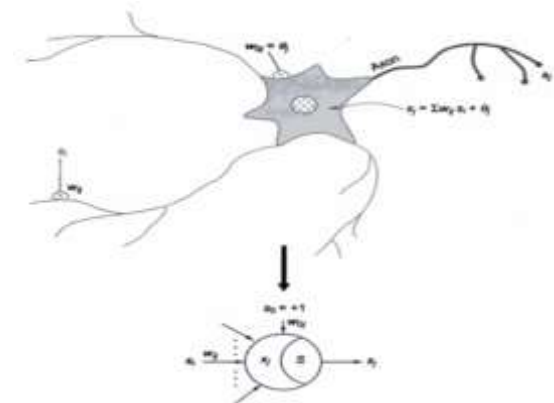


Fig.3 Mathematical model of a neural network

The above diagram exhibits the derived mathematical model of the neural network. It can be seen that various signals traversing different paths have been assigned names X and each path has been assigned a weight W. The signal traversing a particular path gets multiplied by a corresponding weight W and finally the overall summation of the signals multiplied by the corresponding path weights reaches the neuron which reacts to it according to the bias Θ .

3. ENCRYPTION USING ANN

Encryption using an artificial neural network is a relatively new field of research.[5],[8] The reason behind employing neural networks for encryption is the highly **parallel and non-linear** nature of the human brain. The aforesaid characteristics of the human brain are tried to be replicated using an artificial neural network. The main aim in designing such a network is the presence of 'chaos'.[9],[12]

Chaos refers to the following condition:

If the output of a system is deterministic for a particular input, but the output cannot be predicted if the input is changed from its present state leads to the existence of chaos in the system. Mathematically, the above condition can be expressed as:

$$Y(i) = f(X(i)) \quad \forall X(i);$$

But Y(i) is random for X(i+ Δ);

where Δ stands for a change in X.

Such a mathematical condition can be generated by what is called a 'chaotic neural network' i.e. a neural network that exhibits the property of chaos. Chaos is the property that makes it extremely complicated for the attackers to break the encryption algorithm and decipher the cipher text. The requirement for such a chaotic neural network is the adaptive nature of the path weights for different conditions. As the path weight variable changes adaptively, the design of the neural network changes for various inputs thus making it infeasible for the attacker to decipher the cipher text. The above condition can be mathematically expressed as:

$$W(i) = f'(X(i));$$

where f' represents the function or condition that keeps changing the path weight according to the input available to the chaotic network.

Since the path weights change according to the available inputs, therefore the encryption taking place through the chaotic neural network keeps changing dynamically.

The different activation functions that can be used for deciding the output of the neural network are given below:[5]

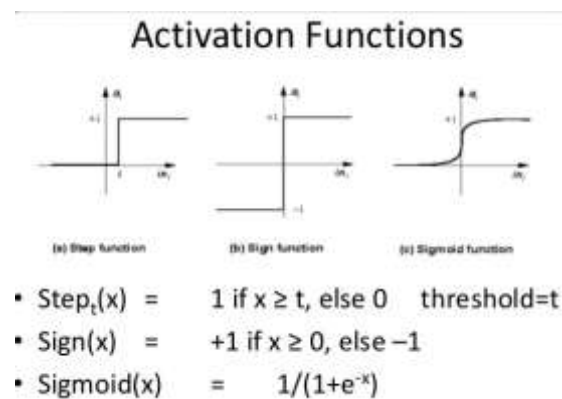


Fig.4 Different Activation Functions

The above figure describes the common activation functions generally used in chaotic neural networks. Since we need to use hard thresholding or gardlimiting function in our proposed work, therefore we use the step function which decides about a threshold 't'.

4. PARAMETERS USED IN THE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS:

Prior to discussing the proposed methodology, we need to understand the parameters based on which we would eventually compare the proposed work and the existing techniques for data encryption. The following are the most important cryptographic parameters based on which cryptographic algorithms are evaluated.

4.1 Throughput:

Mathematically, throughput is defined as:

$$\text{Throughput} = \frac{\text{Size of data to be encrypted}}{\text{total execution time}}$$

The throughput is a parameter which is a measure of the execution efficiency of the algorithm. The

higher the throughput, the more is the size of data that can be encrypted within a particular interval of time. Since any algorithm has to be eventually implemented on a computing machine or hardware, therefore the time and space complexity of cryptographic algorithms is a crucial aspect. Throughput is also a measure of the above.

4.2 Avalanche Effect:

The avalanche effect is defined as the number of bits flipped in the cipher text for one bit change in the plain text. Higher the value of avalanche effect more is the randomness in the cipher text. Thus with high values of avalanche effect, recognizing existing patterns in the cipher text becomes very difficult for any attacker.

4.3 Bit Independence Criteria (BIC)

Bit independence criteria refers to the process that each bit in the cipher text change independently of each other thereby not yielding any visible pattern in the cipher text. This also enhances the randomness of the data.

6. PROPOSED METHODOLOGY

The crux of the entire proposed methodology can be explained using the block diagram of proposed method. The block diagram of proposed method is explained under the following different heading.

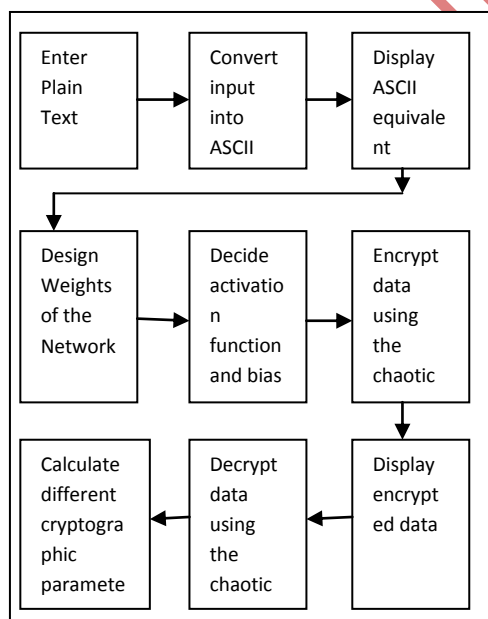


Fig.5 Block Diagram of Proposed Methodology

The proposed methodology can be explained according to the following algorithm:

Initially the plain text is entered by the user and it is displayed and stored. Subsequently, the plain text is converted into its ASCII equivalent and the ASCII equivalent of the plain text is displayed.

Next, the chaotic neural network is designed based on the input adaptive weights, activation function and bias. The critical aspect here is to design a neural network that exhibits the property of chaos.

Once the chaotic neural network is designed, the ASCII equivalent of the input is applied to the network to obtain the cipher text. Subsequently the cipher text is displayed.

The cipher text is then applied to the chaotic network again for decryption and then the plain text is extracted from the cipher text. The plain text obtained through the decryption mechanism is displayed.

Finally cryptographic parameters such as throughput, avalanche effect and bit independence criteria are calculated and compared with the values of the existing cryptographic techniques such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish, Elliptic Curve Cryptography.

7. SIMULATION RESULTS AND DISCUSSION

In this study, the simulations have been carried out using MATLAB platform for different sizes of text data the results of which are illustrated and explained below:

The MATLAB command window is displayed after taking the plain text as 'HARSHAL' and running the code:

Evaluation of different cryptographic parameters: [25]

1) Throughput:

S.No	ALGORITHM	THROUGHPUT
1	Data Encryption Standard (DES)	3.45
2	Advanced Encryption Standard (AES)	4.17
3	PROPOSED ALGORITHM	(10/0.299464)=33.39
4	BLOWFISH	25.892

Table1. Comparative study of throughput

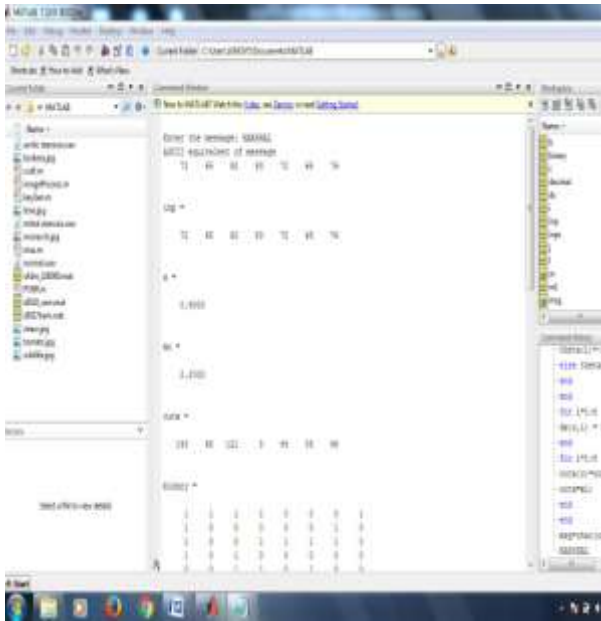


Fig.6 Command Window during encryption (1)

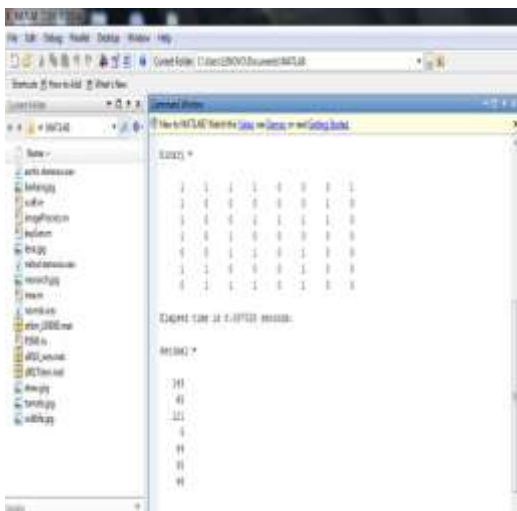


Fig.7 Command Window during encryption (2)

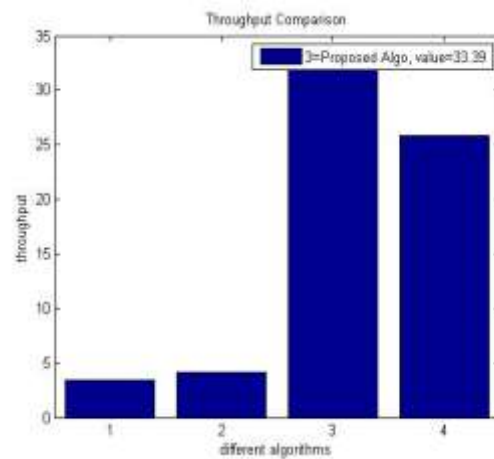


Fig.8 Comparative study of throughput.

2) Avalanche Effect

S.No	ALGORITHM	AVALANCHE EFFECT
1	Data Encryption Standard (DES)	60%
2	Advanced Encryption Standard (AES)	70%
3	PROPOSED ALGORITHM	40%
4	BLOWFISH	38%
5	CAESAR CIPHER	2%
6	VIGENERE CIPHER	4%

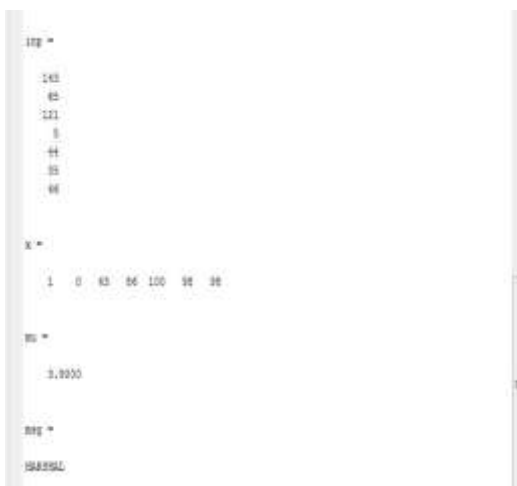


Fig.7 Command Window during decryption (3)

7	PLAYFAIR CIPHER	8%
---	-----------------	----

Table2. Comparative study of Avalanche Effect

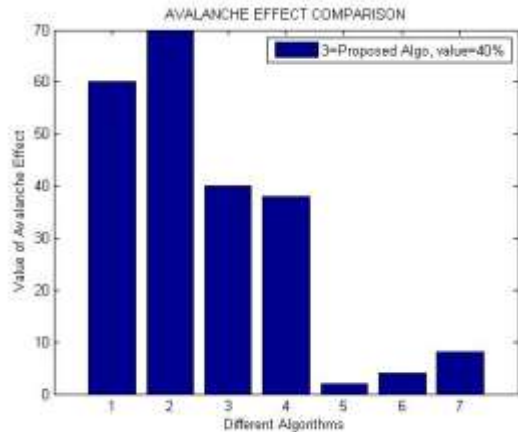


Fig.9 Comparative study Avalanche Effect

3) Bit Independence Criteria(BIC)

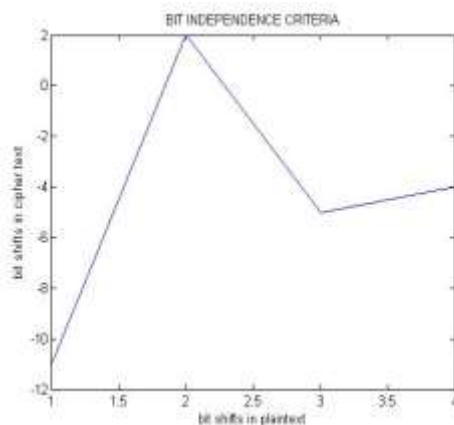


Fig.10 Comparative study BIC

Discussion of Results:

The Command Window displays the flow of the results obtained as the plain text is entered by the user. The ASCII equivalent of the plain text, its decimal equivalent, the cipher text and the plain text extracted from the cipher text can be seen from the command window.

The cryptographic parameters computed are the throughput, avalanche effect and bit independence criteria. A comparative analysis with popular data encryption standards such as the DES, AES, Blowfish, Elliptic Curve Cryptography etc has been

shown. The comparative analysis shows a tabulated form of values of the different parameters and their graphical equivalent. The comparative results help us in visualizing the efficacy of the proposed algorithm.

Conclusion

It can be concluded from the above mentioned results that the proposed algorithm achieves a higher throughput compared to the standard data encryption algorithms. This has a very important repercussion that the proposed algorithm can be treated as a light weight algorithm which can find its applications not only on computational machines with substantial resources but also on computational platforms with limited resources such as mobile computing. The Avalanche effect is comparable to standard algorithms. The Bit Independence Criteria clearly exhibits the fact that the bits in the cipher text change independently of each other and satisfy the condition for chaos. It can be thus concluded that the proposed algorithm for data encryption using a chaotic neural network holds good as an effective yet light weight encryption variant.

References

- [1] William Stallings, —Cryptography and Network Security: Principles and Practice, (5th Edition), Prentice Hall, 2010.
- [2] T. P.Wasnik , Vishal S. Patil , Sushant A. Patinge , Sachin R. Dave , Gaurav J. Sayasikamal, —Cryptography as an instrument to network security, International Journal of Application or Innovation in Engineering & Management (IJAIEEM), Vol. 2, Issue 3, 72-80, 2013.
- [3] Wolfgang Kinzel, IdoKanter, —Neural Cryptography, Proceedings TH2002 Supplement, Vol. 4, 147 – 153, 2003.
- [4] Einat Klein, Rachel Mislovaty, IdoKanter, Andreas Ruttor, Wolfgang Kinzel, —Synchronization of neural networks by mutual

learning and its application to cryptography, In proceeding of: Advances in Neural Information Processing Systems 17, Neural Information Processing Systems NIPS, 2004.

[5] N. Prbakaran, P. Vivekanandan, —A New Security on Neural Cryptography with Queries, Int. J. of Advanced Networking and Applications, Vol. 2, Issue. 1, 437-444, 2010.

[6] R. M. Jogdand, Sahana S. Bisalapur, —Design of an efficient neural key generation, International Journal of Artificial Intelligence & Applications (IJAI), Vol.2, No.1, 60- 69, 2011.

[7] Pratap Singh, Harvir Singh, —Cryptography in structure adaptable digital neural networks", National monthly refereed journal of research in science & technology, Vol.1, Issue.12, 35-44, 2012.

[8] Ajit Singh, Aartinandal, —Neural Cryptography for Secret Key Exchange and Encryption with AES, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue.5, 376- 381, 2013.

[9] Wenwu Yu, Jinde Cao, —Cryptography based on delayed chaotic neural networks, Physics Letters A, Vol. 356, (4) Elsevier, 333– 338, 2006.

[10] Jiyun Yang, Xiaofeng Liao, Wenwu Yu, Kwok-wo Wong, Jun Wei, —Cryptanalysis of a cryptographic scheme based on delayed chaotic neural networks, Chaos, Solitons& Fractals, Vol. 40, Issue.2, 821- 825, 2009.

[11] Rajender Singh, Rahul Misra, Abhishek Chaudhary, —Power consumption using artificial neural network in the field of cryptography, Journal of information, Knowledge and research in

computer Engineering, Vol.2, Issue.2, 443- 446, 2012.

[12] Shweta B. Suryawanshi, Devesh D. Nawgaje, —A triple-key Chaotic neural network for cryptography in image processing, International Journal of Engineering Sciences & Emerging Technologies, Vol. 2, Issue. 1, 46-50, 2012.

[13] Nitin Shukla, Abhinav Tiwari, —An Empirical Investigation of Using ANN Based N-State Sequential Machine and Chaotic Neural Network in the Field of Cryptography, Global Journal of Computer Science and Technology Neural & Artificial Intelligence, Vol. 12, Issue.10, No. 1, 17-26, 2012.

[14] Tariq A. fadil, Shahrul N. yaakob, Badlishah ahmad, abid yahya, —Encryption of mpeg-2 video signal based on chaotic neural network, Journal of Engineering and Technology, Vol. 3, 35-42, 2012.

[15] Navita Agarwal, Prachi Agarwal, —Use of Artificial Neural Network in the Field of Security, MIT International Journal of Computer Science & Information Technology, Vol. 3, No. 1, 42–44, 2013.

[16] B. Geetha vani, E. V. Prasad, —A Hybrid Model for Secure Data Transfer in Audio Signals using HCNN and DD DWTL, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No.7, 202-208, 2013.

[17] Khaled M. G. Noaman, Hamid Abdullah Jalab, —Data security based on neural networks, Task Quarterly 9, No. 4, 409–414, 2005.

[18] Khalil Shihab, —A Back propagation Neural Network for Computer Network Security, Journal of Computer Science 2 (9): 710-715, 2006.

- [19] Seref S., NeclaÖ. , —Neural Solutions for Information Securityl, Politeknik Dergisi, Journal of Polytechnic, Vol. 10, No. 1, 21-25, 2007. [20] Ilker Dalkiran, Kenan Danis, —Artificial neural network based chaotic generator for cryptologyl, Turk J Elec Eng& Comp Sci, Vol.18, No.2, 255-240, 2010.
- [21] Siddeeq. Y. Ameen, Ali H. Mahdi, —AES Cryptosystem Development Using Neural Networks, International Journal of Computer and Electrical Engineering, Vol. 3, No. 2, 315- 318, 2011.
- [22] Karam M. Z. Othman, Mohammed H. AL Jammal, —Implementation of neural - cryptographic system using FPGA, Journal of Engineering Science and Technology, Vol. 6, No. 4, 411 – 428, 2011.
- [23] Eva Volna, Martin Kotyrba, Vaclav Kocian, Michal Janosek, —Cryptography based on neural networkl, Proceedings 26th European Conference on Modelling and Simulation, 2012.
- [24] VV Desai, VB Deshmukh, HD Rao Pseudo Random Number Generator Using Elman Neural Network, IEEE Explore 2011.
- [25] G.Patidar, Nitin Agarwal ‘A Block based encryption model to improve avalanche effect for data security’ IJSRP 2013.