IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 5 ISSUE : 1 Print / Issue Publication Date: 13-Jul-2020

ISSN : 2455-2143

DOI : 10.33564/IJEAST.2020.v05i01.004

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 1, ISSN No. 2455-2143, Pages 26-29
Published Online May 2020 in IJEAST (http://www.ijeast.com)

IMPROVING THE EFFICIENCY OF DES ALGORITHM USING NEURAL NETWORKS

Yousif Elfatih Yousif
Department of Computer Engineering
Faculty of Engineering, Alzaiem Alazhari University, Khartoum, Sudan

Abstract— **Cryptography is the technique of changing data or information into unreadable for unauthorized persons. In cryptography process information transfer from sender to receiver in a manner that prevents from unauthorized third person. There are so many cryptography methods are available which based on number theory. An Artificial Neural Network (ANN) have many characteristics such as learning, generation, less data requirement, fast computation, ease of implementation and software and hardware availability. It is very useful for many applications, in this paper we explore the implementation of DES cryptography algorithm using ANN to reduce the execution time. this paper provides comparison between normal DES and ANN DES.**

Keywords— **Cryptography, Artificial Neural Network, *execution time, DES***

I. INTRODUCTION

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. Work on artificial neural networks, commonly referred to as "neural networks "has been motivated right from its inception by the recognition that human brain computes in an entirely different way from the conventional digital computer. An artificial neural network, which is the formal name for the term neural networks used here, is one of many attempts to build an intelligent machine or to create artificial intelligence. It is based on biological neural networks. The basic idea to model this is to make a very simplified model of biological neurons and their synapses. [1]

Cryptography is a technique to hide the data over communication channel. The developed tangible and hardware tools are not Sufficient to protect the data from unauthenticated parties. Therefore, the experts, researchers and developers have to build and develop security systems, protect the information and prevent the attackers from playing with the very important source (information). For this reason, the term "Encryption/Decryption" was brought out, and it is the main factor that should be available in protection system and take for a real process to manipulate and generate the security system. It is an art to hide the data to strangers. As the technology grows day by day the need of data security over communication channel is increased to high extent. For securing the knowledge cryptography is used, and this cryptosystem can be distinguished in two major types: Secrete-Key Cryptography and Public Key Cryptography. the Secret key cryptography includes DES, AES, 3DES, IDEA, Blowfish algorithms etc. and public key cryptography includes RSA, DIGITAL SIGNATURE AND MESSAGE Digest algorithms.

Now a days computer networks are becoming more important for exchanging information. One of the most important requirements of these networks is to provide secure transmission of information from one place to another. Cryptography is one of the techniques which provide most secure way to transfer the sensitive information from sender to intended receiver [2].

II. METHODOLOGY

This paper is improving Performance of DES algorithm using an Artificial Neural Network, sophisticated implementation has been made with An Artificial Neural Network (ANN) for encrypting and decrypting of data. also designing and analyzing for the performance of Proposed technique was made and it compared to the normal technique in the MATLAB simulator environment, also this study was provided evaluation for two methods.

III. DATA ENCRYPTION STANDARD (DES)

DES is a block cipher. It encrypts the data in a block of 64 bits. It produces 64 bit cipher text. The key length is 56 bits. Initially the key is consisting of 64 bits. The bit position 8, 16, 24, 32,40,48,56, 64 discarded from the key length [3].

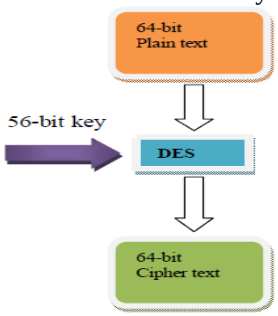

Fig. 1 The DES steps

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 1, ISSN No. 2455-2143, Pages 26-29
Published Online May 2020 in IJEAST (http://www.ijeast.com)

Algorithm:-
[1] In the first step, the initial 64-bit plain text block is handed over to Initial Permutation (IP) function.
[2] The Initial permutation is performed on plain text.
[3] The initial permutation produces two halves of permuted block: Left Plain text (LPT) and Right Plain
(RPT).
[4] Now, each of LPT and RPT goes through 16 rounds of the encryption process, each with its own key:
a. From the 56-bit key, a different 48-bit Sub-key is generated using Key Transformation.
b. Using the Expansion Permutation, the RPT is expended from 32 bits to 48 bits.
c. Now, the 48-bit key is XORed with 48-bit RPT and the resulting output is given in the next step.
d. Using the S-box substitution produce the 32-bit from 48-bit input.
e. These 32 bits are permuted using P-Box Permutation.
f. The P-Box output 32 bits are XORed with the LPT 32 bits.
g. The result of the XORed 32 bits is become the RPT and old RPT become the LPT. This process is called
as swapping.
h. Now the RPT again given to the next round and performed the 15 more rounds.
[5] After the completion of 16 rounds the Final Permutation is performed

IV. NEURAL NETWORK ARCHITECTURES

There are three network architectures:
1. Single Layer feed forward networks – In this layer, the input layer consists of source node that results the
output in the form of neuron. It is feed forward type of network. [5]
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 [6]

V. NEURAL NETWORK LEARING PARADIGNS

Like in any other intelligent based systems, a desired output of the network does not come by chance. The network rather adapts itself to a stimulus, and ultimately yields the desired output. The main difference here perhaps could be featured to the type of learning a particular network is subjected to.
Broadly speaking, there are different learning paradigms that can be used to train neural networks. Supervised and unsupervised learning are the most common, with reinforced and competitive learning techniques also gaining considerable popularities. The learning process is essential to adjust network weights in order to reduce the error. During the process of adapting and adjusting the synaptic weights, the network acquires knowledge similar to human-like reasoning. However, the learning process requires sets of mathematical algorithms describing how synoptic network weights and biases are attuned.

VI. DESIGNING ANN MODELS

Designing ANN models follows a number of systemic procedures. In general, there are five basics steps: (1) collecting data, (2) preprocessing data, (3) building the network, (4) train, and (5) test performance of model as shown in Fig 6.

1. Data Collection
Collecting and preparing sample data is the first step in designing ANN models.

2.Data Pre-Processing
After data collection, three data preprocessing procedures are conducted to train the ANNs more efficiently. These procedures are: (1) solve the problem of missing data, (2) normalize data and (3) randomize data.

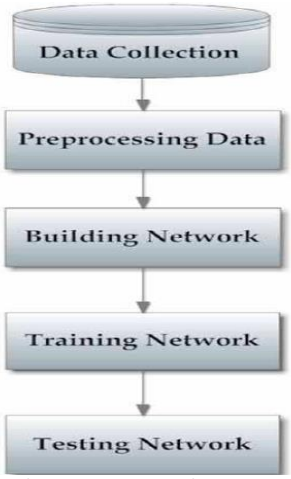

Fig. 2: Basic flow for designing artificial neural network model

3. Building the Network
At this stage, the designer specifies the number of hidden layers, neurons in each layer, transfer function in each layer, training function, weight/bias learning function, and performance function. In this work, multilayer perceptron (MLP) and radial basis function (RBF) networks are used.[38]

4. Training the Network
During the training process, the weights are adjusted in order to make the actual outputs(predicated) close to the target (measured) outputs of the network.

5. Testing the Network

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 1, ISSN No. 2455-2143, Pages 26-29
Published Online May 2020 in IJEAST (http://www.ijeast.com)

The next step is to test the performance of the developed model. At this stage unseen data are exposed to the model.

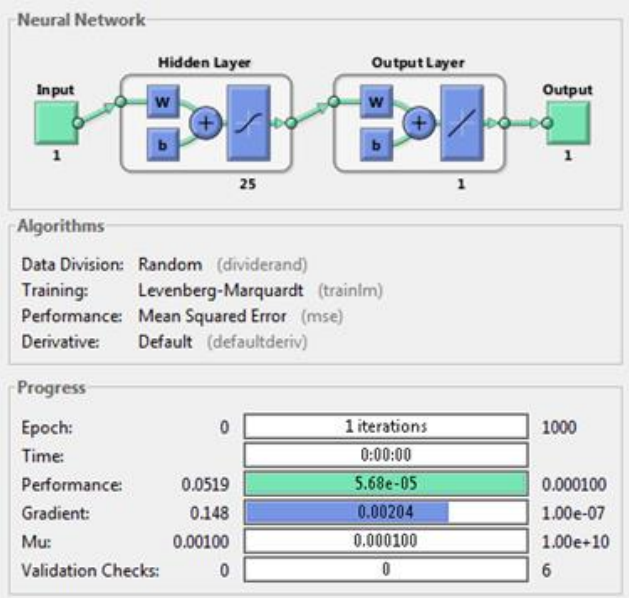

Fig 3: neural network model

VII. PROPOSED DESIGN OF DES ALGRITHM BASED ON ANN

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.

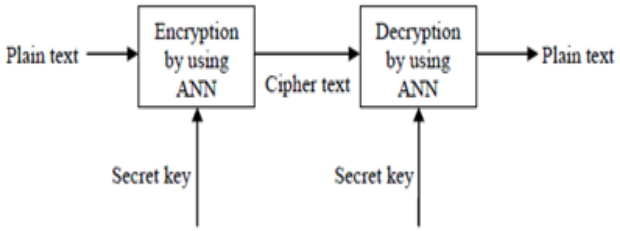

Fig 4 : Block of Cryptography by using ANN

In this paper, it was merged ANN with DES in this design we used a neural network called feed forward network, 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. the learning algorithm used here is the Backpropagation method in feedforward network architecture. the input is plain text that is encrypted by NN-using DES algorithm and output of NN is Cipher text.

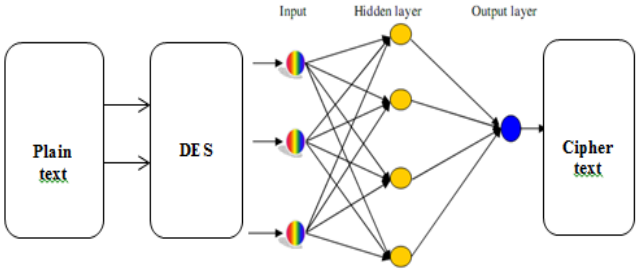

Fig. 3: Proposed Architecture of cryptography based on Neural network

VIII. RESULTS

The results reported is comparison between the normal DES and AAN DES. In this paper, the result implementation by environment of MATLAB

Table 1. Execution Time of DES algorithm for encryption

NO	Input file size in Kb	Time required for Encryption In seconds	
		(DES)Normal	(DES)ANN
1	3	0.459	0.256
2	6	0.677	0.402
3	9	1.033	0.788
4	12	1.36	1.019
5	15	1.716	1.293

Table 1 display the DES execution time required by different size text files for encryption process. Fig.4 show the difference in execution time for normal DES and ANN DES implementation for encryption process.

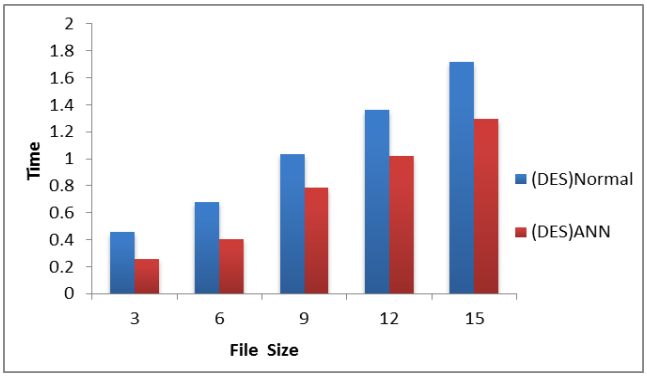

Fig.4: Comparison of Execution Time for Encryption

Table 2. Execution Time of DES algorithm for decryption

NO	Input file size in Kb	Time required for Decryption In seconds	
		(DES)Normal	(DES)ANN
1	3	1.778	0.712
2	6	2.874	1.41
3	9	3.922	2.152
4	12	4.691	2.734

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 1, ISSN No. 2455-2143, Pages 26-29
Published Online May 2020 in IJEAST (http://www.ijeast.com)

5	15	5.843	3.86

Table 2 display the execution time required by different size text files for decryption process. Fig.5 show the difference in execution time for normal DES and ANN DES implementation for decryption process.

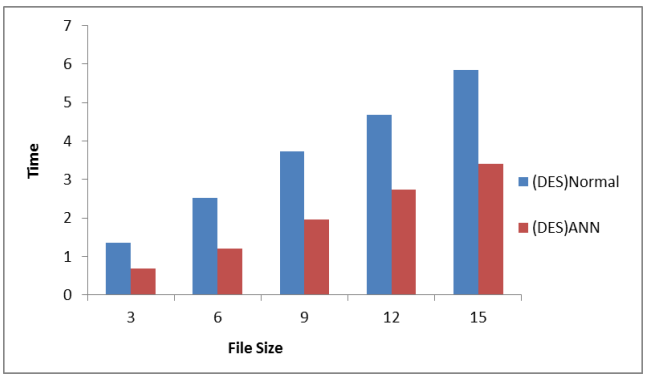

Fig.5: Comparison of Execution Time for decryption

IX. CONCLUSIONS

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 be replaced conservative methods, but for a growing list of applications
In this paper, we have designed and implemented of DES algorithm by using An Artificial Neural Network (ANN), After evaluation of execution time, we reported that ANN implementation of DES takes less time for performing the encryption and decryption than the normal implementation. Artificial Neural Networks is a powerful technique that has the ability to emulate highly complex computational machines. must used this technique to build cryptography systems.
The usage of ANN in the field of cryptography is brilliant method because the NN can process information in parallel, at high speed, and in a distributed manner.

X. REFERENCES

[1] Tope Komal , et al.; " Encryption and Decryption using Artificial Neural Network" , IARJSET , Vol. 2, Issue 4, April 2015 pp. 81-83
[2] Yousif Elfatih Yousif, Dr.Amin Babiker A/Nabi Mustafa, Dr.Gasm Elseed Ibrahim Mohammed" Review on Comparative Study of Various Cryptography Algorithms",IJARCSSE , Volume 5, Issue 4, April- 2015, pp. 51-55
[3] William Stallings, "Cryptography and Network Security: Principles and practices, Dorling Kindersley (india) pvt ltd., 4th edition(2009).
[4] Ajay Pal Singh , Parvez Rahi " Performance Enhancement in Public key Cryptosystems for Security using RSA Algorithm " , IJARCCE , Vol. 5, Issue 11, November 2016 , pp. 359-362
[5] Oludele Awodele , Olawale Jegede" Neural Networks and Its Application in Engineering ", InSITE, 2009
[6] Andrej Krenker , Janez Bešter and Andrej Kos " Introduction to the Artificial Neural Networks" , Methodological Advances and Biomedical Applications
[7] Manikandan.G, Rajendiran.P, Chakarapani.K, Krishnan.G, Sundarganesh.G, "A Modified Crypto
Scheme for Enhancing Data Security", Journal of Theoretical and Advanced Information Technology, Jan 2012.
[8] A.Nadeem, "A performance comparison of data encryption algorithms", IEEE information and communication technologies, pp.84-89, 2006.
[9] Diaasalama, Abdul kader, MohiyHadhoud, "Studying the Effect of Most Common Encryption Algorithms", International Arab Journal of etechnology, vol 2,no.1,January 2011.
[10] Atul Kahte.Cryptography and Network Security.Tata Mcgraw Hill, 2007.
[11] Shasi Mehlrotra seth, Rajan Mishra " ComparativeAnalysis of Encryption Algorithms For Data Communication", IJCST Vol. 2, Issue 2, June 2011.
[12] Wuling Ren. A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication. Second International Conference on Modeling, Simulation and Visualization Methods (WMSVM), 2010.

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

ABOUT IJEAST

International Journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high-quality research papers in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

FOCUS AREAS

- Engineering
- Applied Science
- Technology
- Innovation & Development
- Interdisciplinary Studies

PEER REVIEWED
All submissions are rigorously peer reviewed to ensure quality.

OPEN ACCESS
Free and unrestricted access to research for all.

GLOBAL REACH
Connecting researchers and professionals worldwide.

TIMELY PUBLICATION
We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

editor@ijeast.com
www.ijeast.com
India

2455-2143