CS 7530: Advanced Cryptography, Summer 2022, Instructor – Ahyoung Lee

Efficiency improvement of DES Algorithm using Artificial Neural Networks.

Grishma Saparia
Department of Computer Science
Kennesaw State University Marietta, GA
gsaparia@students.kennesaw.edu

ABSTRACT

The Purpose of cryptography is to change the data into unreadable form to prevent the access from any third person. In cryptography the data or information is transferred from the sender to receiver in a way which is encrypted and no unauthorized user can access it. There are various algorithms in cryptography which is based on number theory. Artificial Neural Network (ANN) is a computational model which is based on the human neuron system. The features of ANN include learning and modelling complex and non-linear data, generalization, fast data processing, no conditions on input data, easy execution and availability of hardware/software. In this paper we compare the execution time of DES and DES using ANN. Hence, we execute DES using ANN to reduce the execution time.

KEYWORDS

Data Encryption Standard (DES), Artificial Neural Network (ANN), Cryptography

1 INTRODUCTION

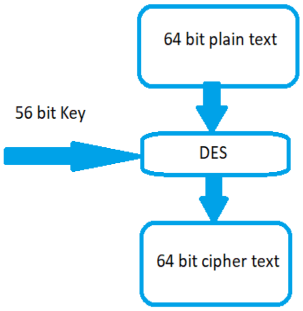
An Artificial Neural Network (ANNs) are models in which several processing elements receive input and generate output according to their predefined activation function. In a sense, ANN use learning algorithm that are capable of independently making adjustment as they receive input. They are therefore an excellent tool for modelling non-linear statistical data. To model complex pattern and predict problems, ANN use the brain’s processing as a basis. Therefore, biological neural network is the basis of ANN. [1]

Cryptography is a set of methods for securing communication and information based on mathematical concepts and rules-based calculation know as algorithms, which transforms a message in a way which is hard to decrypt. Furthermore, these algorithms can be used for web browsing, credit card transactions and email communications in addition to generating cryptography key and providing data privacy. Cryptography can be divided into two broad categories know as public key and Secret key. In Secret for encryption and decryption only a single key is used. In public key, two keys are used know as private and public key. User can share public key but private key must be kept confidential. Various Secret key algorithm includes DES, 3DES, AES, RC4, RC5, etc. Various Public key algorithm includes RAS, DSA, ECDSA, etc. Modern computer networks increasingly handle the transmission of confidential information. One safeguard for such transmissions is the use of encryption technology.

In this work we propose and evaluate a novel encryption technique the Data Encryption Standard (DES) that uses Artificial Neural Networks (ANN) for both encryption and decryption. Also, we analyze and compare the performance of the proposed system in matlab environment. [2]

2 DATA ENCRYPTION STANDARD (DES)

Data Encryption Standard encrypts the given data in a block of 64 bits. Therefore, it is known as symmetric key block cipher. The length of the key used is 56 bits. For encryption/decryption the same key is used.



DES ALGORITHM STEPS

(1) The 64-bit plain text is given to the initial permutation (IP)
(2) The function performs IP on the given 64-bit plain text.
(3) IP makes two blocks of the permuted text known as Left Text (LT) and Right Text (RT).
(4) Both LT and RT go through encryption process of 16 rounds having its own keys.
- A 48-bit key is generated from 56 bit key with the help of key transformations.
- The RT is converted from 32 bits to 48 bits using text expansion permutation.
- Now 48 bits key and 48 bits RT is XOR and passed to the next step.
- 32 bits are produced from 49 bits input using s-box substitution.
- p-box permutation is used to permute these 32 bits.
- The above output is XOR with 32 bits LT.
- Swapping is performed where the XOR 32 bits now becomes RT and old RT becomes LT.
- Now the process is repeated for more 15 rounds where RT is given to the next round.

(5) Once all the 16 rounds are completed, final permutation round is performed. [3]

3 ARCHITECTURES OF NEURAL NETWORK

Various types of architectures of neural networks are:
- Single layer feed forward network.
- Multi-layer feed forward network.
- Single layer Recurrent network.
- Multi-layer Recurrent network.

In single layer feed forward network, we have only two layers know as input and output. Here the input layer does not perform computations. Different weights are applied to the input layer, which forms the output layer.

In Multi-layer feed forward network, we have a hidden layer which is not related to the output layer. Because it has a hidden layer, it is computationally stronger.

In Single layer Recurrent network, the output is directed to the processing unit either to itself or other processing units.

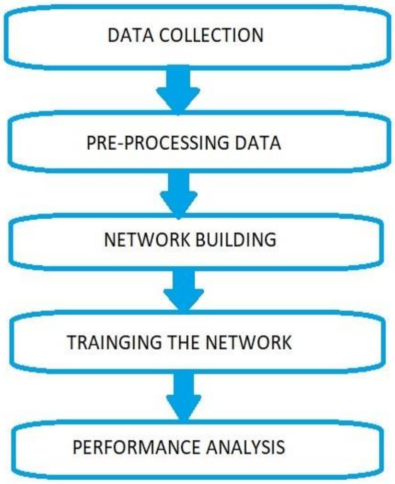
In Multi-layer Recurrent network, the output is directed to the processing unit of the same layer or the other layer forming multiple layer Recurrent network.

4 NEURAL NETWORK LEARNING PARADIGNS

The network adapts itself to get the desired output. Various data is fed to the network according to which it learns and gives a desired output. There are various learning techniques in machine learning which are categorized as supervised, unsupervised and reinforcement learning. Supervised learning uses a teacher to learn whereas unsupervised learning does not learn with a teacher. Learning process is important through which we can adjust the weight. When the network adjusts and adapts to the desired output, that is when the weights are adjusted, the network obtains human like reasoning to any particular inputs. Therefore, various mathematical algorithms are required to get the desired output.

5 DESIGNING ANN NETWORK

There is basic five steps to design an ANN network which are:
(1) Data Collection.
(2) Pre-processing the data.
(3) Network building.
(4) Training the network.
(5) Performance analysis.



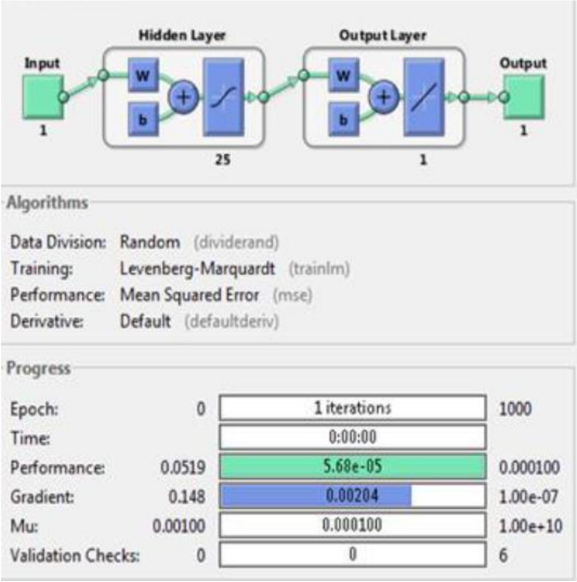
DATA COLLECTION
Collecting the relevant data is the initial step in designing ANN network.

PRE-PROCESSING DATA
Pre-processing data follows various steps like filling the missing data, normalize the data and randomize the data. It is done to increase the efficiency of the network.

NETWORK BUILDING
In this step of network building, it specifies various functions like transfer function, learning function, training function, etc. Here the number of hidden layers is also defined and the number of neurons in each layer. In this work I have used Radial bias function and multilayer perceptron.

TRAINING THE NETWORK
In training the network the weight of the networks is adjusted in order to the actual output near to the desired output (measured output).

PERFORMANCE ANALYSIS
In this step of performance analysis, the unknown data in fed to the network to test the performance of the developed network and check if the actual output is close to the measured output.



Algorithms

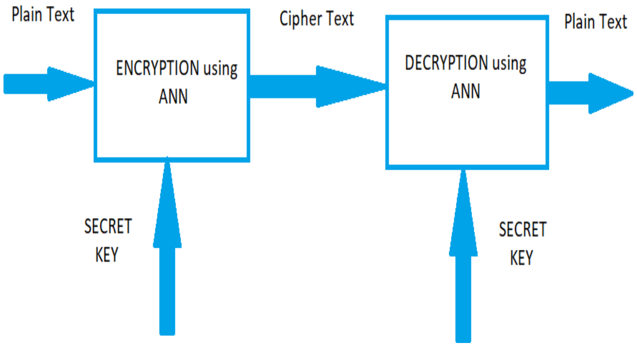
Data Division: Random (dividerand)
Training: Levenberg-Marquardt (trainlm)
Performance: Mean Squared Error (mse)
Derivative: Default (defaultderiv)

Progress

Epoch:	0	1 iterations	1000
Time:		0:00:00	
Performance:	0.0519	5.68e-05	0.000100
Gradient:	0.148	0.00204	1.00e-07
Mu:	0.00100	0.000100	1.00e+10
Validation Checks:	0	0	6

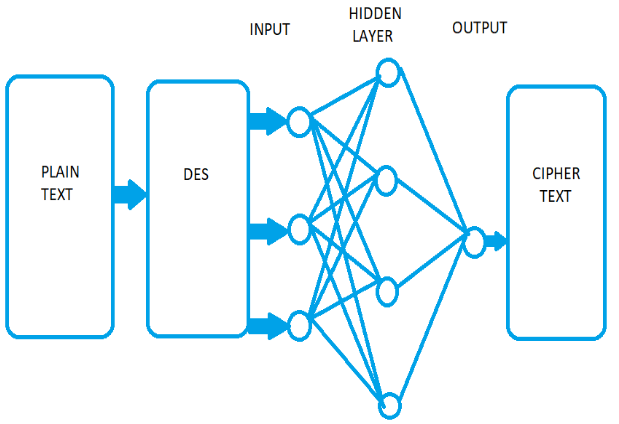
6 PROPOSED DESIGN OF ARTIFICIAL NEURAL NETWORK USING DES

The study and practice of concealing information using methods based on randomness is known as cryptography. Therefore, the ANN in neural cryptography must be a type of random tropology where there is a random change in the structure of network.



In this work ANN and DES were combined. We employee a neural network termed a feed forward network in this design. These networks are really simple and link input and output.

This style of organization is sometimes known as top-down or bottom-up approach. Here the feed forward networks architecture's backpropagation approach is applied as the learning algorithm. The output of NN is cipher text and the input is plain text that has been encrypted using DES method by NN.



7 RESULTS

In this work, the results are implemented using the matlab environment. The result is the comparison of execution time between the Data Encryption Standard Algorithm and Data Encryption Standard with ANN.

Table 1 – Displays the DES and (DES) ANN execution time needed for various text file size throughout the encryption process.

Number of seconds needed for encryption	Number of seconds needed for encryption	File size in KB
DES	(DES) ANN	
0.549	0.365	4
0.723	0.502	6
1.193	1.015	8
1.361	1.102	10

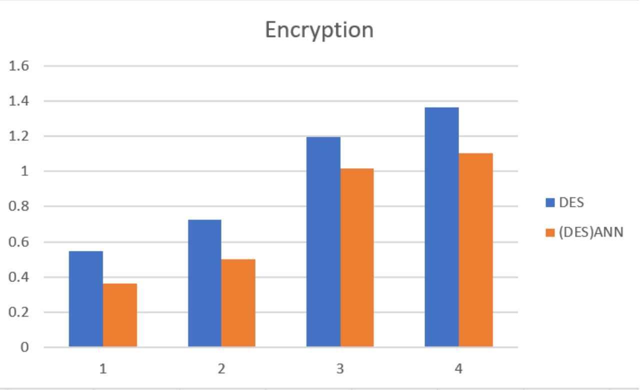
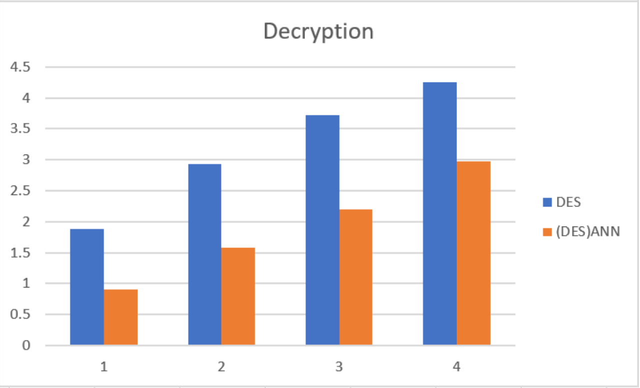


Table 2 – Displays the DES and (DES) ANN execution time needed for various text file size throughout the decryption process.

Number of seconds needed for decryption	Number of seconds needed for decryption	File size in KB
DES	(DES) ANN	
1.878	0.912	4
2.931	1.574	6
3.714	2.198	8
4.257	2.972	10



8 CONCLUSIONS

Neural network has a lot to offer to the world of computing. They are adaptive and strong because they can learn on their own. Consecutive approach may not completely be replaced by neural network but there are more and more applications for them. In this work I have implemented DES and DES using ANN. I have compared the execution time of both and have observed that implementation of DES using ANN take less time to execute compared to normal DES. Since, ANN can process information in parallel, quickly and uniformly, using ANN in the realm of cryptography is a fantastic technique.

REFERENCES

[1] Enzo Grossia, Massimo Buscemab (2008). "*Introduction to Artificial Neural Network"*. European Journal of Gastroenterology & Hepatology. 10.1097/MEG.0b013e3282f198a0

[2] Tope Komal1 , Rane Ashutosh2 , Rahate Roshan3 (2015). "*Encryption and Decryption using Artificial Neural Network.*" ,IARJSET , Vol. 2, Issue 4, pp 81-83.

[3] Yousif Elfatih Yousif, Dr. Amin Babiker A/Nabi Mustafa, Dr. Gasm Elseed Ibrahim Mohammed (2015). "Review on Comparative Study of Various Cryptography Algorithms." IARJSET, Vol. 4.

[4] A.Nadeem (2016) *"A performance comparison of data encryption algorithms*" IEEE information and communication.

[5] S. Willian (2009) *"Cryptography and network security : Principle and practices."* 4th edition.

[6] D. Roza, S. Mohsen (2021) "Artificial Neural Network System" International Journal of Imaging. (ISSN 0974-0627).