Journal of Kerbala University , Vol. 10 No.4 Scientific . 2012

Simulating DES Algorithm Using Artificial Neural Network

Noor Dhia Kadhm Al-Shakarchy
Computer ScienceDepartment,Science College,Karbala University, Karbala, IRAQ
Email: noor.dhiya@yahoo.com

Abstract:

Data Encryption Standard (DES) algorithm considers one of complicated algorithms that have users confidence for a long time. This algorithm enjoy with wide spread in business progress, banking, and governmental.

When DES algorithm entered running space, and many experiments and researches in cryptanalysis continuous to break this algorithm. In this research we using artificial neural networks to attack this algorithm by designing artificial neural network system simulating the main design of DES algorithm. The main idea of proposed system depends on represented the plaintext / ciphertext process; so that(Expansion permutation, and S-boxes substitution, and P-boxes permutation) process represented in proposed artificial neural network model; because the key is unknown and the purpose of proposed system obtained it. The proposed system used in two ways as cryptanalysis by provide a ciphertext as input to the network and the output obtained from the network system is the plaintext. The second used to the network is as cryptography system that's by inputs plaintext as input to the network system and the output obtained from the network is ciphertext.

الخلاصة :

تعتبر خوارزمية التشفير القياسية (DES) واحدة من الخوارزميات المعقدة التي حازت على ثقة المستفيدين لعدة سنوات. هذه الخوارزمية تتمتع بانتشار واسع في مجال الأعمال التجارية والمصرفية والاستخدامات الحكومية.

منذ أن دخلت خوارزمية DES و محاولات الباحثين والمختصين في مجال كسر الشفرة مستمرة من اجل أيجاد طريقة لكسرها. في هذا البحث تم استخدام الشبكات العصبية الاصطناعية لمهاجمة هذه خوارزمية عن طريق تصميم شبكة عصبية اصطناعية تحاكي التصميم الأساسي للخوارزمية. الفكرة الأساسية للنظام المقترح تعتمد على تمثيل العمليات التي تجري على النص الصريح / النص المشفر. وهذه العمليات هي عملية النشر والاستبدال وصناديق التعويض وعملية الاستبدال. ويتم تمثيل هذه العمليات فقط على اعتبار إن المفتاح غير معروف ويستهدف النموذج المقترح الحصول عليه. يستخدم النظام المقترح في اتجاهين الأول كنظام لكسر الشفرة عن طريق إدخال النص المشفر كمدخلات للشبكة العصبية المقترحة وينتج النص الصريح كمخرجات للنظام العصبي المقترح. الاستخدام الآخر للنظام المقترح كنظام تشفير وذلك عن طريق إدخال النص الصريح كمدخلات للنظام المقترح و النص المشفر ينتج كمخرجات للشبكة.

1- Introduction:

Security of cryptographic systems is directly related to the difficulty associated with inverting encryption transformations of the system. The protection afforded by the encryption procedure can be evaluated by the uncertainty facing an opponent in determining the permissible keys [1,2, 3]. Data Encryption Standard (DES) is one of block cipher algorithms that partitions the data to blocks each block consist of 64 bits. These blocks entered to DES algorithm with 64 bits blocks of key to produce 64 bits block of ciphertext. This algorithm consist of many linked confusion and diffusion operations; which considered the main technique to built cryptography algorithms. The structure of DES algorithm consist of mixing substitution followed by a permutation operations these done on plaintext and key together which named round. DES algorithm contained 16 round doing the same operation. Since many years the researches and cryptanalyst study the weakness and strength points of DES algorithm. These studies toward three objects these are [2, 3, 4]:

1- The key
2- Number of rounds
3- S- boxes

Artificial Neural Networks (ANNs) are simplified models of the central nervous system. ANN are based on the basic model of the human brain with capability of generalization and learning. The purpose of this simulation to the simple model of human neural cell is to acquire the intelligent features of these cells. They are networks of highly interconnected neural computing elements that have the ability to respond to input stimuli. Among the capabilities of ANN, are their ability to learn adaptively from dynamic environments to establish a generalized solution through approximation of the underlying mapping between input and output [1, 5, 6, 7].

Neural network has the possibility of learning. The process of determining the weights by which the best match between the desired output and the artificial neural network output is called training process. Training will be most effective if the training data is spread throughout the input space. Learning algorithms are classified into supervised learning process and unsupervised learning process. Supervised learning is the learning with a "teacher" in the form of a function that provides continuous feedback on the quality of solutions. These tasks include pattern classification, function approximation and speech recognition, etc [6, 7, 8].

Unsupervised learning refers to the learning with old knowledge as the prediction reference. These tasks include estimation problem, clustering, compression or filtering [9]. In this work, the architecture of the neural network is the back propagation neural network and the learning algorithm is back propagation learning algorithm [9]

The work flow for the neural network design process has seven primary steps [10]:

1- Collect data
2- Create the network
3- Configure the network
4- Initialize the weights and biases
5- Train the network
6- Validate the network
7- Use the network

These steps discuses and applied on proposed system in practical part in section 6.

The Data Encryption Standard (DES), has been a worldwide standard for 20 years. Although it is showing signs of old age, it has held up remarkably well against years of cryptanalysis and is still secure against all but possibly the most powerful of adversaries [2].it's one of block cipher algorithms, which divided the plaintext to blocks each block consist of 64 bits. This algorithm designed depending of confusion and diffusion process that's lead to random ciphertext.

Neural networks are used in many different application domains in order to solve various information processing problems. They have proven to be successful in pattern recognition, pattern classification, system identification, function approximation, prediction, optimization, and controlling [1]. System identification is concerned with inferring models from observation and studying system behavior and properties. System identification deals with the problem of building mathematical models of dynamical systems based on observed data from the system[10] . There are two approaches for system identification, depending on the available information, which describe the behavior of the dynamic system. the first approach is state- space approach (internal description), which describes the internal state of the system, and used whenever the system dynamical equations are available. The second approach is; input-output description which is used when no information is available about the system except its input and output [8].

The proposed system aims to construct artificial neural network system simulates the main structure of DES algorithm. Therefore the proposed system depend on state- space (internal description) identification. Back Propagation Algorithm is used to learn the proposed neural network by modifying the weights connected between the neurons until the desired plaintext value obtained. The proposed system used plaintext – ciphertext pairs to learn the network by entered the ciphertext as the input to the network then learning to attempt to occurrence the result identical to obverse plaintext. After the learning process finished the connection weights represent the encryption key . and then used this system to cryptanalysis other ciphertext.

2-related work:

When DES algorithm entered running space, the researches beginning to attack and cryptanalysis this algorithm. The primary studies and researches depending on exhaustive search by using trial and error concept [11, 3]. Another way present by Hellman named Formal coding. This way looking for key bits using XOR-SUM-OF-PROUDUCTS[3]. These ways needs very long time and treated with huge data, therefore, the modern way used different concept. In 1990, Eli Biham, and Adi Shamir presented Differential cryptanalysis[3,12]. This way depend on chooses plaintext-ciphertext pairs, which it's plaintext different, and cryptanalysis the different between them during encryption progress using same key. this way right theoretical but practically it's need very long time and very large computational ability. In 1993, Mitsuru Matsui present Linear Cryptanalysis by using Linear Approximation way to describe encryption process[3,12]. In recent years genetic algorithms used in cryptanalysis. By using genetic algorithm cipher text only attack is adopted and variety of optimum keys is produced based on fitness function[13,14]. The neural network take place wide interested in cryptanalysis of classical and stream cipher either using Known neural network or by using black- box[1, 8, 9, 15].

In this paper we used neural network to cryptanalysis DES algorithm by designing a network simulate the main design of DES.

3-The Proposed System:

Suppose there are many plaintext – ciphertext pairs encrypted using unknown one key. These pairs used to learn the network by entered the ciphertext as the input to the network then learning to attempt to occurrence the result identical to obverse plaintext. After the learning process finished the connection weights represent the encryption key . and then used this system to cryptanalysis other ciphertext. Each round of DES algorithm consist of four main process, these are:

a. Key compression and permutation.
b. Expansion permutation.
c. S-boxes substitution.
d. P-boxes permutation.

The first process doing on key, and the other process (b, c, d) done on the text.

The main idea of proposed system depend on represented the plaintext / ciphertext process; therefore the latest three process represented in proposed artificial neural network model; take in considerations the key is unknown and the purpose of proposed system obtained it.

The following (figure1) represent the proposed artificial neural network structure of DES algorithm.

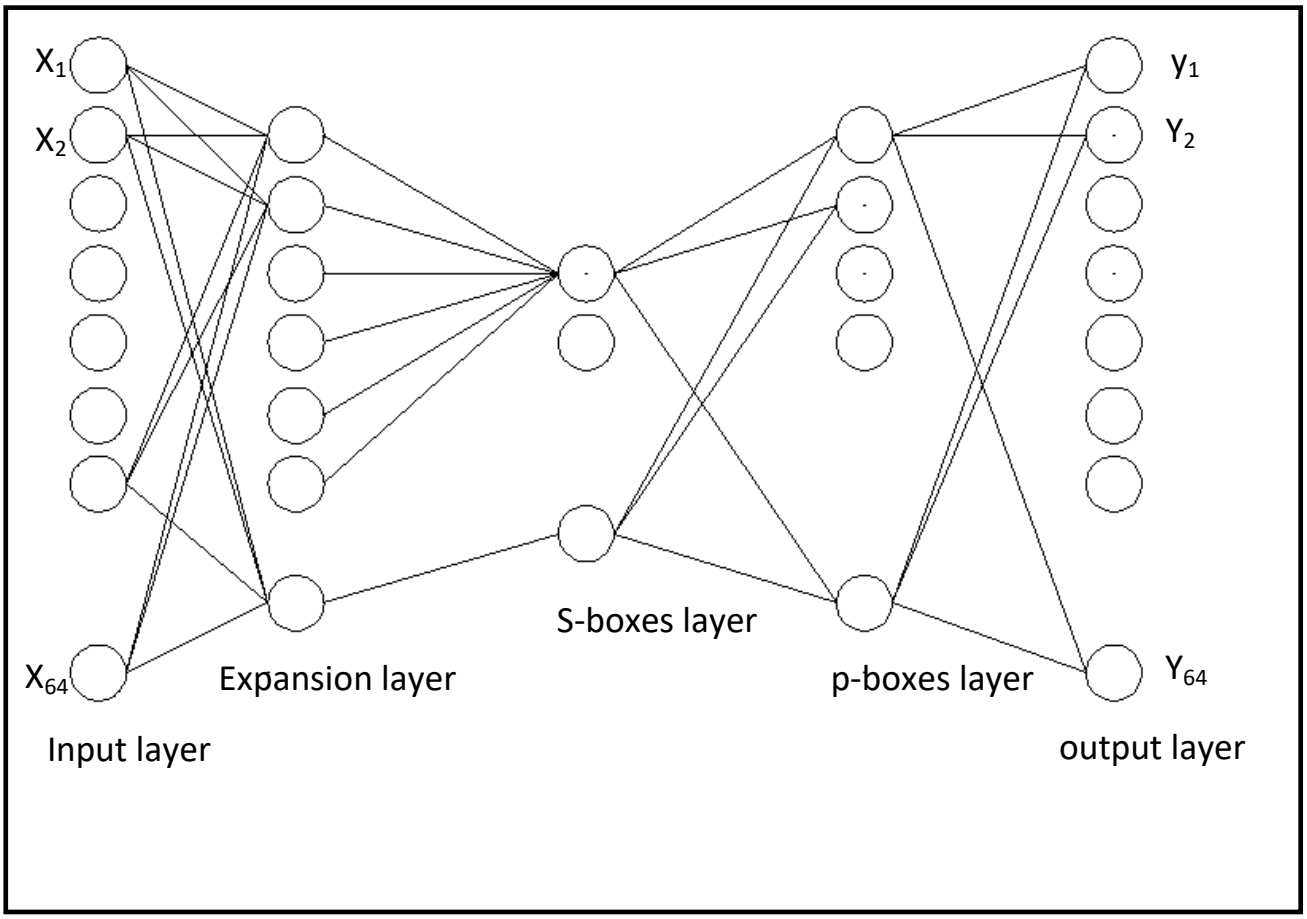

Figure 1
The proposed DES artificial neural network model

The proposed artificial neural network consist of five layers, these layer in order:

a) Input layer:

This layer consist of 64 neuron (node), each neuron represents one bit from ciphertext therefore this layer named also ciphertext layer.

b) Expansion Permutation layer:

Consist of 48 neuron, each neuron represents one bit of block obtained from Expansion Permutation process.

c) S-boxes layer:

Consist of 8 neuron, each neuron represents one box from 8 s-boxes. In this layer the connection between the expansion permutation layer output and s-boxes layer must be corresponding to the main design of DES algorithm. That's by dividing the expansion permutation output to groups each group contain 6 neurons, then connect each group to one of s-boxes in orders. The first group that contain the first six neurons (e1; e2, e3, e4, e5, e6) from expansion permutation layer connected to first neuron of s-boxes layer (s1), and the second group that contain the succeed six neurons (e7; e8, e9, e10, e11, e12) connected to the second neuron of s-boxes…and so on.

d) P-boxes layer:

Consist of 48 neurons. In this layer the entered text to s-boxes returned with exchanging its positions.

e) Output layer:

This layer consist of 64 neuron (node), each neuron represent one bit from plaintext therefore this layer named also plaintext layer.

5-The network learning:

To learning the proposed neural network suppose finding many plaintext – ciphertext pairs encrypted using same key. In practical side of this research we used 5 pairs of plaintext – ciphertext in learning process. The ciphertext represents the input of the neural network after dividing it to 64 bit blocks , the corresponding plaintext divided to 64 bit block also. Where each ciphertext block faced the corresponding plaintext block. The plaintext block represent the desired value from proposed model.

The following Back Propagation learning algorithm steps until the desired plaintext value obtained are :

a. determine random values to all weights (W) conected between neurons, the range of these values between (0.1 – 0.3) .
b. select random ciphertext – plaintext pair block (X D) and compute the output values to each layer feed forward direction to obtained final output values from the neural network (O).
   $O_j = f(\sum_{Oj-1} W_{ij})$.
c. Compute the difference between the desired value (D) and the final output value (O)
   $\delta_j = (O_j - D_j) f(H_j)$.
d. Compute the difference value (δ) to all previous layers using Back Propagation method:
   $\delta_j = f'(H_{j-1}) (\sum \delta_j W_j)$.
e. Updating weights values (W):
   $W_{ij}(new) = W_{ij}(old) + \Delta W_{ij}$
   $\Delta W_{ij} = \mu \delta O_j$
   f.Repeats the steps (b, c, d, e) with another learning data pair until the desired plaintext value obtained.

6-Experemental Results:

The proposed model attempt to simulate the main design of DES algorithm using artificial neural networks. The aim of this model obtained random distribution to neural network weights identical the DES random distribution that done on plaintext and key to produced the ciphertext.

Phase 1: Design System: this phrase determined the structure of the proposed system as shown in figure-1 above. It's include the number of hidden layers and the number of neurons of each layer with input and output layers to be agreement with the main structure and properties of DES algorithm.

Phase 2:The work flow for the proposed neural network design: this process done using Matlab implementation by the following steps:

Step 1: Collect Data (preparing data):

Open the Matlab Toolbox and look for the Neural Network Toolbox. You should be able to see the NN Network/Data Manager screen. this screen used to entered data (the input and desired data). Each data represent as vector of binary bits. Let P denote the input (plaintext) and T denote the target/output (ciphertext).

Step 2: Create the Network:

In order to use a network we need to first design it, then train it. After this the network is ready for simulations to be performed on it. We change all the parameters on the screen to the values as indicated on the following:

Network name = DES
Network type = Feed-forward back propocation
Input data = P (entered and saved in step 1)
Target data = T (entered and saved in step 1)
Training function= Trainlm
Adaptive learning function= Learngdm
Performance function = Mse
Number of layers = 5

Then determine the number of neurons and transfer function to each layer .all these shown in figure-2

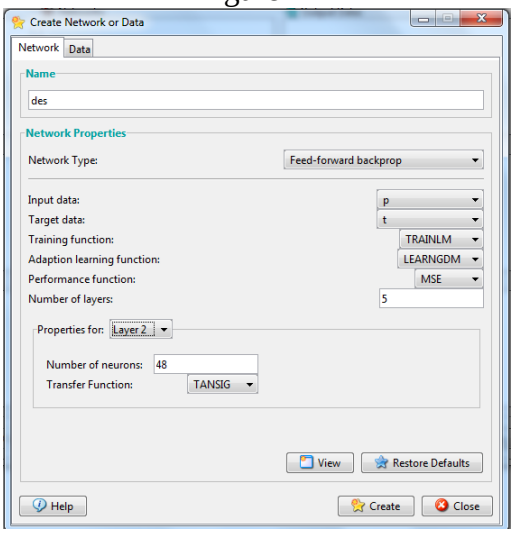

Figure 2
Create network or data screen

Step 3: Configure the Network:

In order to show a network configuration we chose the DES network from data/network manager screen then we can show the configuration of the design network in view page as shown in figure 3 below.

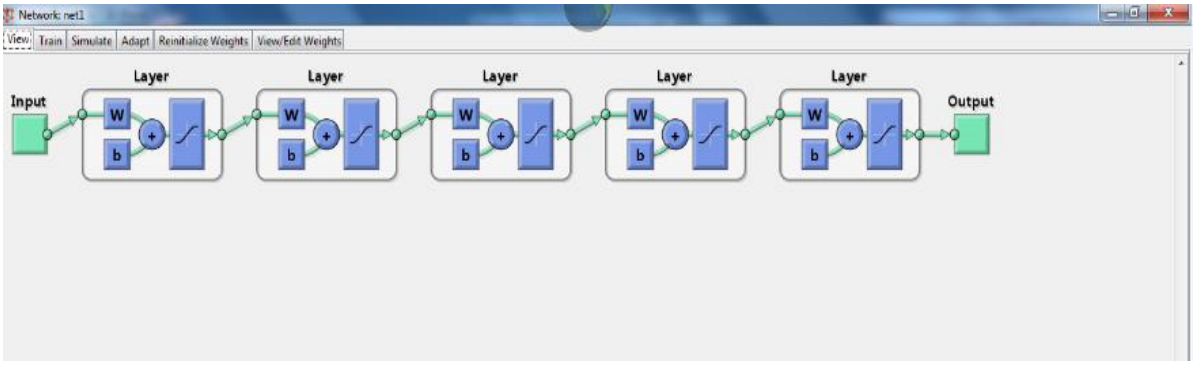

Figure 3
Proposed network confoguration

Step 4: Initialize the weights and bises :

This done using the same screen in figure-3 but with view / edit weights page or reinitialized weights page.

Step 5: Network Training:

In order to use a network training we chose the train page in then chose train page as shown in same figure-3 . The train page allowed to determine the training parameters and training information as shown in figure-4 and figure-5 :

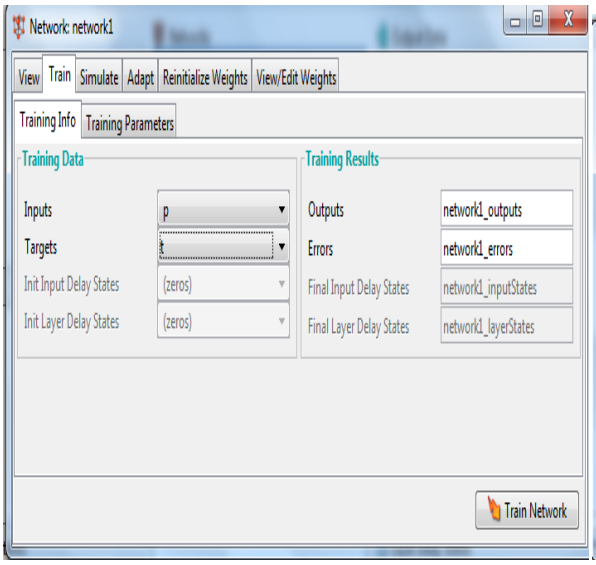

Figure 4
Training parameters of train page

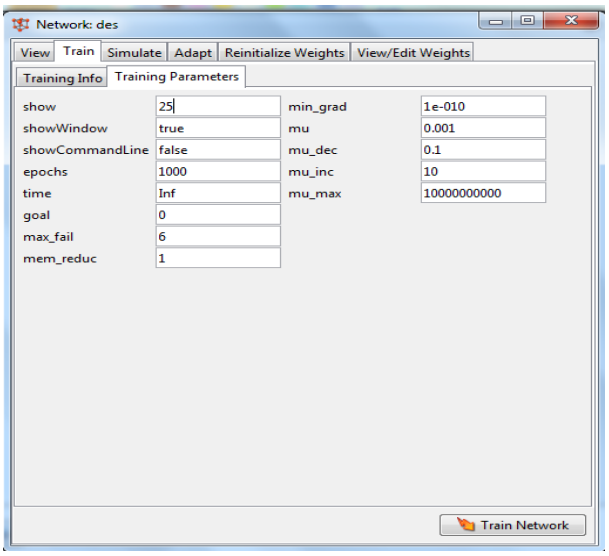

Figure 5
Training parameters of train page

When the network completed the performance curve which determine the convergence of the training curve with error rate as shown in figure-6:

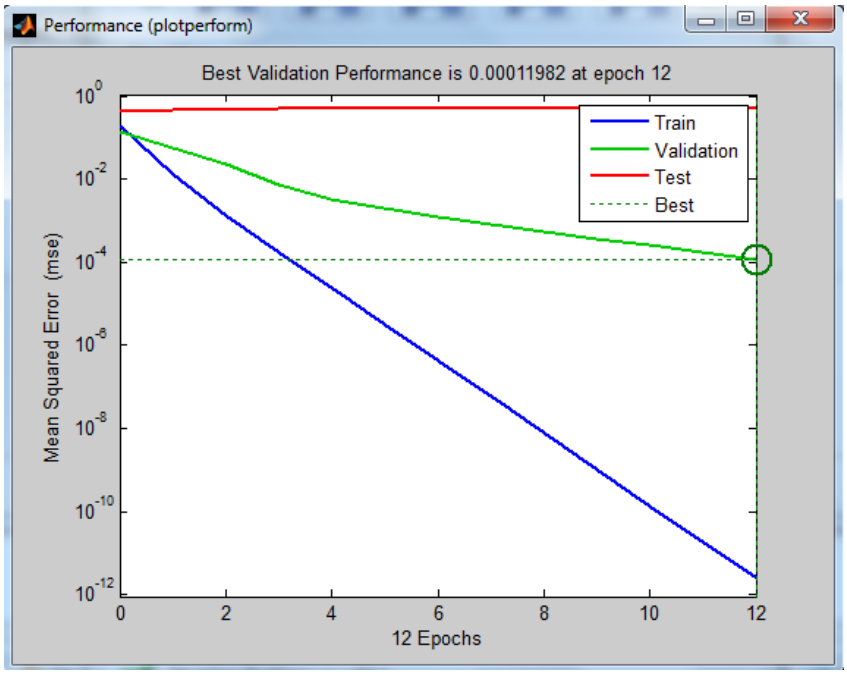

Figure 6
The performance curve

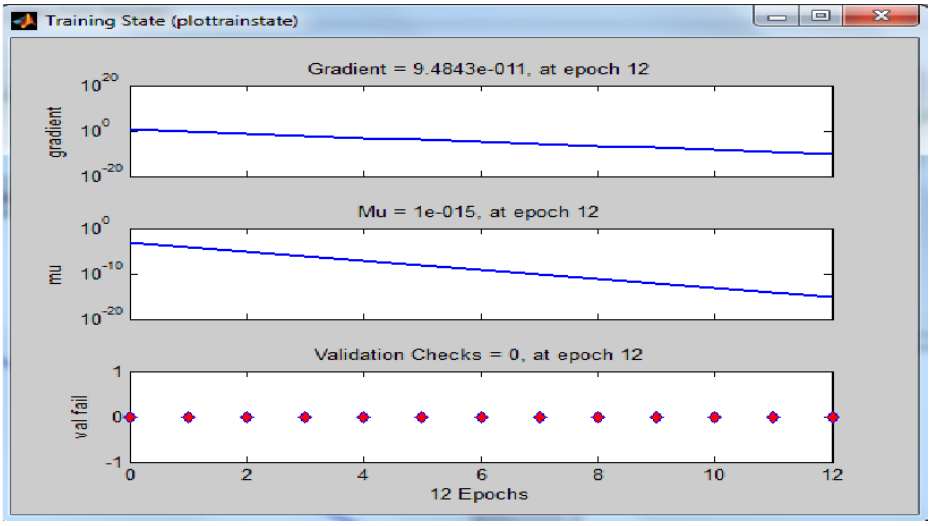

Figure 7
Training state curves

Step 6: validate the network:

The network become validation and if this network reached to convergence during the training with minimum error rate. In this case the proposed system becomes ready to used as DES main algorithm.

Step 7: Use the network:

This step is doing using the same figure 3 but with simulate page shown in figure-8 and the out put of the simulation data saved in network / data management. As shown in figure-9.

If we used the network as cryptanalysis system we used ciphertext as input to the network and the output (the plaintext) obtained from the network system. another used to the network is as cryptography system that's by inputs plaintext as input to the network system and the output (ciphertext) obtained from the network.

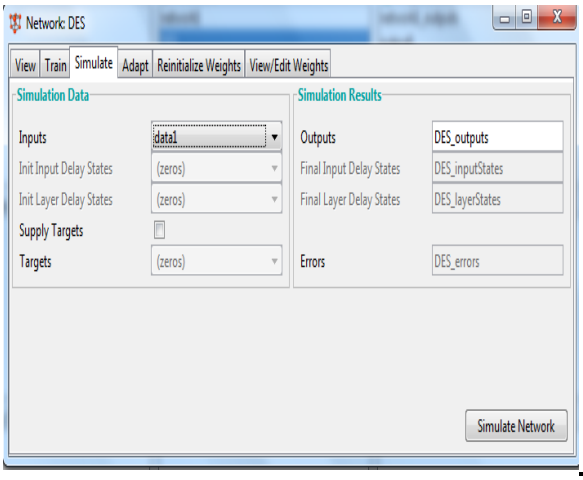

figure 8
DES simulation screen

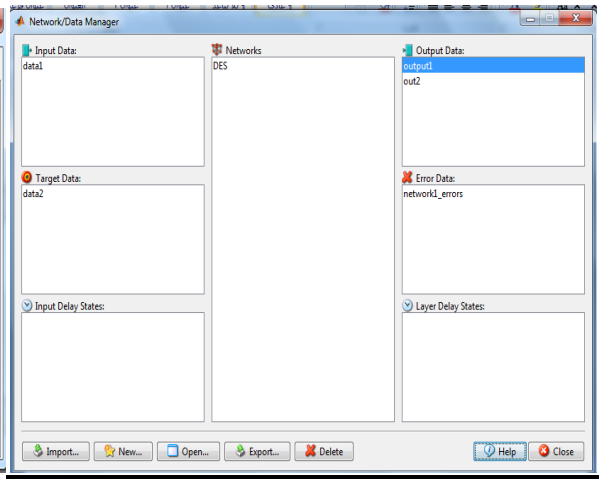

figure 9
Network / data management screen

7-Conclusion:

1- After the training completed connections weights of neurons represent the key used in encryption or decryption process. And we can extracting this weights (key) by printed or showing it. That's main advantages comparative with use neural networks as black box when in black box we can't print or

show the connections weights and that's mean we can't take place the key used in encryption or decryption process.

2- We can use the proposed system in cryptanalysis by using ciphertext as input to network and produce the plaintext as output of the network using the same key all that in simulation step (step 7 above).
3- We can use the proposed system to encrypt a message by entered the plaintext as input to network and produced ciphertext as output by simulation step (step 7).
4- This model attempt to simulate the main design to DES algorithm to produced random distribution of neuron weights similar to random distribution done on plaintext and key by DES algorithm.
5- Finally one of difficulties and Limitation is the obtaining of ciphertext – plaintext pairs encrypted using same key.

Reference:

[1]Khaled Alallayah, Mohamed Amin, Waiel Abd El-Wahed, and Alaa Alhamami, "Attack and Construction of Simulator for Some of Cipher Systems Using Neuro-Identifier", The International Arab Journal of Information Technology, October 2010 .
[2]Bruce Shnieier, "Applied Cryptography, Protocols, Algorithms, and Source Code in C", John Wiley and Sons, second edition, 1997.
[3]Bruce Shnieier, " Differential and Linear Cryptanalysis", Dr. Dobbs Journal, 1996.
[4]Henry Beker, and Fred Piper, " Cipher System, the protection of communications, 1983.
[5]Dan W. Patterson, "Artificial Neural Networks, Theory and Application", prentice hall, 1996.
[6]Bart Kosko, " Neural Networks and Fuzzy Systems", university of southern California, 1992.
[7] Romariz A., "Neural Network Applied to Nonlinear Modeling," www.ene.unb.br/romariz/, Last Visited 1996.
[8]Mahmood Kl. Ibrahem, "Black – Box Attack using Neuro Identifier", ph.D., university of technology, Baghdad, 2000.
[9]Karam M. Z. Othmani, Mohammed H. AL Jammas, " Implementation of Neural – Cryptographic System using FPGA" , Iraq , 2011.
[10] Mark Hudson Beale, Martin T. Hagan, Howard B. Demuth, "Neural Network Toolbox™", User's Guide, by The Math Works, Inc. 2011.
[11] Nalini N1 and G. Raghavendra Rao2, "Cryptanalysis of Block Ciphers via Improvised Particle Swarm Optimization and Extended Simulated Annealing Techniques", Department of Computer Science and Engineering, Siddaganga Institute of Technology1, National Institute of Engineering2, Karnataka, India, 2006.
[12] Dr. K. S. Ooi, " Cryptanalysis of S-DES" , Brain Chin Vito, 2002.
[13] Vimalathithan.R, Dr.M.L.Valarmathi, "Cryptanalysis of S-DES using Genetic Algorithm", India, 2009.
[14] S.Siva Sathya, T.Chithralekha and P.AnandaKumar, "Nomadic Genetic Algorithm for Cryptanalysis of DES 16", International Journal of Computer Theory and Engineering, Vol. 2, No. 3, June, 2010.
[15] Alallayah, Khaled M.; Wahed, Waiel F. Abd El-; Amin, Mohamed Alhamami, Alaa H., "Attack of against simplified data encryption standard cipher system using neural networks", Journal of Computer Science, 2010.