Journal of Computer Science 6 (1): 29-35, 2010
ISSN 1549-3636

Attack of Against Simplified Data Encryption Standard Cipher System Using Neural Networks

[1]Khaled M. Alallayah, [2]Waiel F. Abd El-Wahed, [1]Mohamed Amin and [3]Alaa H. Alhamami
[1]Department of Mathematical and Computer Science, Faculty of Science, Al Menoufia University, Egypt
[2]Department of Operation research and Decision, Faculty of computers, El-Menoufia University, Egypt
[3]Faculty of Computing Studies, Amman Arab University for Graduate Studies, Amman, Jordan

Abstract: Problem statement: The problem in cryptanalysis can be described as an unknown and the neural networks are ideal tools for black-box system identification. In this study, a mathematical black-box model is developed and system identification techniques are combined with adaptive system techniques, to construct the Neuro-Identifier. **Approach:** The Neuro-Identifier was discussed as a black-box model to attack the target cipher systems. **Results:** In this study this model is a new addition in cryptography that presented the methods of block (SDES) crypto systems discussed. The constructing of Neuro-Identifier mode achieved two objectives: The first one was to construct emulator of Neuro-model for the target cipher system, while the second was to (cryptanalysis) determine the key from given plaintext-ciphertext pair. **Conclusion:** Present the idea of the equivalent cipher system, which is identical 100% to the unknown system and that means that an unknown hardware, or software cipher system could be reconstructed without known the internal circuitry or algorithm of it.

Key words: System identification, artificial neural network, emulation, SDES, cryptanalysis, cipher system, black box and neuro-identifier

INTRODUCTION

Block cipher systems belong to symmetric cryptographic systems, where the same key is used for encryption and decryption process. The major difference between block ciphers and other symmetric cryptographic systems are that; block ciphers are characterized by the fact that the decipherment of a bit of data depends not only on the key but also on some of the other bits of data. The principles behind the design of most block ciphers are the concepts of diffusion and confusion. The idea of confusion is to make the relation between a cryptogram and the corresponding key a complex one. This aims to make it difficult for the statistics to point out the key as having comes from any particular area of the key space. The concept of diffusion is to spread the statistics of message into statistical structure, which involves long combinations of the letters in the cryptogram and hence whitening all the statistical feature of the neutral language. In this study, a brief discussion of block ciphers background and techniques is presented. DES cipher is chosen as a case study of block cipher because, it was (and still) the challenge of most of the researchers over the last 25 years. 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 (Bruce, 1996). The cryptanalysis problem can be described as an identification problem and the goal of the cryptography is to build a cryptographic system that is hard to identify (Pieprzyk and Jennifer, 1989; Alallayah *et al*., 2010). 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 (Alallayah *et al*., 2010; Lennart, 1987). Artificial Neural Networks (ANNs) are simplified models of the central nervous system. 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 (Simon, 1998; Patterson, 1998; Sarle, 2002). Neural networks can be regarded as a black-box that transforms an input vector

Corresponding Author: Khaled M. Alallayah, Department of Mathematical and Computer Science, Faculty of Science, Al Menoufia University, Egypt Tel: +20-165316919/+20-0643208651

of m-dimensional space to an output vector in n-dimensional space. This makes them ideal tools for black-box system identification (Ball *et al*., 2002; Zbikowski and Dzielinski, 1995). In this study, you will implement a simplified version of the DES block cipher algorithm. Naturally enough, it is called SDES and it is designed to have the features of the DES algorithm but scaled down so it is more tractable to understand. A survey of previous cryptographic work especially for DES is presented. The proposed Emulation mode using Neuro-Identifier (NID) against SDES is described in detail with the results obtained during the study.

System identification: There are two approaches for system identification (Alallayah *et al*., 2010; Lennart, 1987), depending on the available information, which describe the behavior of the system. The first approach is the State-Space approach (internal description), which describes the internal state of the system and is used whenever the system dynamical equations are available. The second approach is the Black-Box approach (input-output description) which is used when no information is available about the system except its input and output (Saggar *et al*., 2007). Figure 1 shows an unknown system with x_m input signals and y_n output signals. The central concept in identification problems is identifiability (Lennart, 1987). The problem is whether the identification procedure will yield a unique value of the parameter (q) and/or whether the resulting Model (M) is equal to the true system, i.e., a model structure is globally identified at:

$$(\theta^{*}) \text{ if: } M(\theta) = M(\theta^{*}), \theta \in D_M \Rightarrow \theta = \theta^{*} \quad (1)$$

Where:

M = A model structure

q = A parameter vector, ranging over a set of values D_M (Zbikowski and Dzielinski, 1995)

Input-output descriptions: The input-output description of a system gives a mathematical relationship between the input and output of the system. In developing this description, the knowledge of the internal structure of a system may be assumed to be unavailable; the only access to the system is by means of the input and output terminals (Tsong, 1999; Alallayah *et al*., 2010). Under this assumption, a system may be considered a Black-Box as shown in Fig. 1. Clearly what one can do to a black box, is to apply inputs and measure their corresponding outputs and then try to abstract key properties of the system from these input-output pairs. An input-output model assumes that the new system output can be predicted by the past inputs and outputs of the system (Saggar *et al*., 2007; Liu and Truong, 1995).

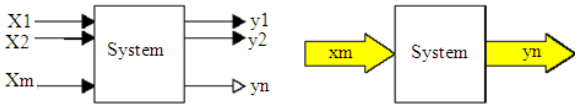

Fig. 1: System with m inputs and n outputs

A Black-Box model of system identification assumes no prior knowledge about the system except it's input and output, i.e., no matter what analysis is used, it always lead to the same input-output description.

Moreover, a Black-Box model allows finite-dimensional identification techniques to be applied, which may require in nonlinear system identification. In developing the input-output description, before an input is applied, the system must be assumed to be relaxed or at rest and that the output is excited solely and uniquely by the input applied thereafter and the system is said to be causal if the output of the system at time k does not depend on the input applied after time k (Tsong, 1999). The system can be described as follows:

$$y(k) = H\,x \quad (2)$$

where, H is some function that specifies uniquely the output y in terms of the input x of the system. Although the subject of system identification is well developed for linear systems, the same is not true for the nonlinear case. However, linearization of nonlinear systems can be obtained by several methods, among them is the approximate linearization technique for nonlinear systems (Cinar, 1996; Alallayah *et al*., 2010; Saggar *et al*., 2007).

For Single-Input Single-Output (SISO), the input-output model identification problem is to devise a mathematical model which, when excited with the input sequence [x(k), k = 1,2,…, m], will produce an estimated output [y(k), k = 1,2,…, n], such that:

$$y(k) = f(y(k-1),y(k-2),\ldots,y(k-n),x(k-1),x(k-2),\ldots, x(k-m)) \quad (3)$$

Where:

[x(k), y(k)] = Representing the input-output pairs of the system at time k

n and m = Positive integers representing the number of past outputs and the number of past inputs respectively

f = A static nonlinear function which maps the past inputs and outputs to a new output. f is called describing function

That means; for any discrete-time, unknown nonlinear system there would be suitable positive

integers (m and n) and a multidimensional mapping f(.) in such a way that the system output at a given instant could be approximated by Eq. 3. If a system is linear f is a linear function and Eq. 3 can be rewritten as (Simon, 1998; Pieprzyk and Jennifer, 1989; Alallayah *et al*., 2010):

$$y(k) = a_1y(k-1)+a_2y(k-2),\ldots+a_ny(k-n)+b_1x(k-1)+b_2 x(k2), \ldots.+b_mx(k-m) \quad (4)$$

where, a_i (i = 1,2,…,n) and bi (i = 1,2,…,m) are real constants. Equation 4 can be rewritten in matrix notation:

$$y(k) = \sum_{t=0}^{n} \alpha_i k(y-1) \sum_{j=0}^{m} \beta j_k (x-j) \quad (5)$$

For Multi-Input Multi-Output (MIMO), y(k) and x(k) are of dimensions m and p respectively, equation (5) can be rewritten as (Alallayah *et al*., 2010):

$$y(k) = \sum_{t=0}^{n} A_i k(y-1) \sum_{j=0}^{m} B_j k(x-j) \quad (6)$$

where, Ai and Bj an (m × m) and (m × p) matrices respectively.

Cryptographic system: An encryption algorithm is a single parameter family of invertible transformations (mappings) of the message space (M) into the cryptogram (ciphertext) space (C) using finite length key k from keyspace (K). See a reversible encryption algorithm (Schaefer, 1996; Bruce, 1996) in Eq. 2:

$$E_k: M \rightarrow C$$

Such that:

$$E_k (m) = c,\ k \in K,\ m \in M,\ c \in C \quad (7)$$

An inverse decryption algorithm:

$$D_k = E^{-1}{}_k : D_k: C \rightarrow M$$

Such that:

$$D_k(c) = D\ k[E_k (m)] = m \quad (8)$$

The keys should uniquely define the enciphered message i.e.:

$$E_{k1} (m) \neq E_{k2} (m) \text{ if } k_1 \neq k_2 \quad (9)$$

According to the previous discussion of the properties of the system and the definition of a cryptographic system, it might be concluded that: A cryptographic system is, relaxed, causal, time invariant and nonlinear system.

Neuro-Identifier (NID): Identification of a system consists of finding a model relationship. Consider the system described in Eq. 3. Identification then consists of determining the system orders and approximation of the unknown function by neural network model using a set of input and output data (Blankenship and Ghanadan, 1996; Leaster and Sjoberg, 2000; Lester and Jonas, 1998). The procedure begins with the choice of neural model which is defined by its architecture and an associated learning algorithm. This choice can be made through trial and error. Once the neural model is chosen and system input-output data are available, learning can begin. Different structures are trained and compared using learning set and simulation set of data and a criterion (error goal) (Thomas, 2008; Jiang and Zhou, 2006). The optimal structure then, is the one having the fewest units (neurons) for which the criterion is met. Neuro-Identifiers (NIDs) are basically Multi-Layer Feed-Forward artificial neural networks (MLFF) with an input layer (buffer layer), a single or multiple nonlinear hidden layer with biases and a linear/or nonlinear output layer (Yu *et al*., 2000; Saggar *et al*., 2007). The results of research have shown that linear identifiers are not capable of identifying nonlinear systems. Hybrid identifiers can identify simple nonlinear systems but not complex ones (Bin and Babri, 1998; Yu *et al*., 2000; Tanomaru, 1994). Figure 2 shows the structure of the multi-layer feed-forward neural network identifier NID, with two nonlinear hidden layers, which is used in this research. The size of the neural network (number of neurons in the hidden layer) is crucial in designing the whole structure. There is no mathematical formulation to calculate the optimal size of such networks. However, with many free units the NID will learn faster, avoid local minima and exhibit a better generalization performance (Simon, 1998; Zbikowski and Dzielinski, 1995). The essential constraint on increasing the size of hidden layers is the limitation of the hardware architecture used in the experimental study.

Training algorithm: The Levenberg-Marquardt (LM) algorithm is (MLFF), the most ideally used optimization algorithm. It outperforms simple gradient descent and other conjugate gradient methods in a wide variety of problems. This document aims to provide an intuitive explanation for this algorithm.

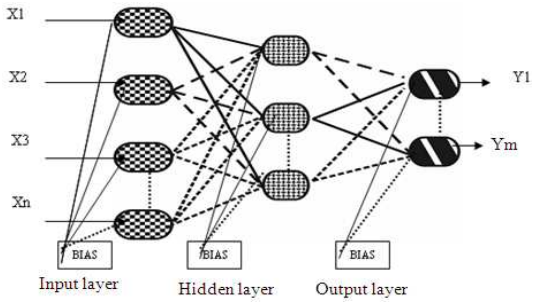

Fig. 2: Multi-layer feed forward neuro-identifier architecture

The LM algorithm is first shown to be a blend of vanilla gradient descent and Gauss-Newton iteration. Subsequently, another perspective on the algorithm is provided by considering it as a trust-region method (Alallayah *et al*., 2010; Leaster and Sjoberg, 2000).

Algorithm:

1- Initialize network (Weights and Biases)
2- For each training pair 3-7 until performance criteria.
3- Sums weighted input and apply activation function to compute output:

$h_0i = \sum I = 1\ Xi\ Wij + bi.\quad hi = f(h_0j)$

4- Compute output of network:

$yy = bp + \sum I = 1\ hi\ Wpi.\qquad y = f(yy)$

5- Calculate error term. $\delta = (y\text{-}yd)$
6- Calculate correction term:

$Wb = [w1b1\ w2b2\ \ldots\ wpbp]$

$\Delta Wb = (J^T.J + \eta I)\text{-}1.\ (-J^T.\delta)$

7- Update biases and weights:

$Wij\ (new) = wij\ (old) + \Delta\ Wb$

8- End.

Using NID in cryptanalysis: Cryptographic systems are a 2-input, 1-output systems, it takes a plaintext character (or bit /block of bits) and a key character to produce a ciphertext character. Hence a 2-neurons input layer is used to present the training data to the identifier, while a single neuron output layer is used. The described neural network identifier was used to identify cryptographic systems in two approaches with the following objectives:

Emulation approach: Construct of a neuro-model for the target unknown cipher system (Alallayah *et al*., 2010):

- Encryption cipher:
  - Input data: TP, TK. -Desired output data: TC
- Decryption cipher:
  - Input data: TC, TK. -Desired output data: TP

Cryptanalysis approach: Input data: TP, TC. Desired Output data: TK.

The first objective is to construct a neuro-model which imitates the internal (transfer) function of the cryptographic system (hardware or software). After training and on convergence, the constructed model will resemble the target system completely. The construction of such a model will be useful in studying the behavior of the unknown system and it can be used as a real system in encryption and decryption in cases where the real system cannot be. The aim of the second objective, is to obtain clearly a pure cryptanalysis target (total break). This could be done by introducing plaintext-cipher text as input to the system, which yields the key as output. The training data is built using the target cipher system algorithm by applying selected input signals (characters or bits) and collecting the output response of the system. The resulting data are split into two groups; the first group is used to train the neural network, while the second group is used to test (simulate) the trained network.

Block ciphers (SDES): IBM initiated a cryptographic research concentrating on nonlinear block ciphers in the late 1960's and has produced several important cryptographic systems. In January 1977, the National Bureau of Standard (NBS) adopted one of these as the national data encryption standard (DES). IBM systems have their roots in Shannon's brilliant 1949 paper connecting cryptography with information theory (Whitfield and Hellman, 1979). Shannon suggested using product ciphers to build a strong system out of simple, individually weak components. He suggested using products of the form $B_1Mb_2M\ldots,B_nM$, where M is a mixing transformation and Bi is simple cryptographic transformations. High-speed electronic circuitry allows the product system to be implemented almost as economically as single BM pairs. The data are encrypted in number of "rounds" (iterations) each consisting of a single pair B_iM and each using the same hardware. The same key is used in encryption and

decryption process. The fundamental building block of DES is a single combination of substitution followed by permutation (diffusion and confusion) on the text based on the key. This is known as a round. DES has 16 rounds; i.e., it applies the same combination of substitution and permutation 16 times (Thomas, 2008). The output of the ith round become the input to the (i+1) round. Block ciphers probably of the most important cryptographic primitives. Although they are used for many different purposes, their essential goal is to ensure confidentiality. This study is concerned by their quantitative security, that is, by measurable attributes that reflect their ability to guarantee this confidentiality. Well know results. Starting with Shannon's Theory of Secrecy, we move to practical implications for block ciphers, recall the main schemes on which nowadays block ciphers are based and introduce the Luby-Rackoff security model (Nalini and Rao, 2006). We describe distinguishing attacks and key-recovery attacks against block ciphers (Ball *et al*., 2002). The system uses a transformation of the bits within a block for the fixed mixing transformation T and substitution on four bits groups of the block for the simple cryptographic transformation Si. Any k-bit S-box can be implemented as 2 k word memory with k-bit words. The Neuro-Identifier (NID), as described above, has been used in this research in block cryptosystem identification, as a black-box model. The objective of the attack, is to determine the key from the given plaintext-ciphertext pair. Black-box attack has been applied to SDES. SDES encryption takes a 10 bit raw key (from which two 8 bit keys are generated as described in the handout) and encrypts an 8 bit plaintext to produce an 8 bit ciphertext. Implement the SDES algorithm in a class called SDES.

Definitions:

$K = (k_0k_1\ldots..k_9)$ where $k_1 \in \{0, 1\}$ key
$M = (m_0m_1\ldots..m_7)$ where $m_1 \in \{0, 1\}$ message
$P_4 = (1,3,2,0)$ shifting sequence = (1,2)
$P_8 = (5,2,6,3,7,4,9,8)$ $P_{10} = (2,4,1,6,3,9,0,8,7,5)$
$IP = (1,5,2,0,3,7,4,6)$ $IP^{-1} = (3,0,2,4,6,1,7,5)$

$$SB_0 = \begin{bmatrix}1032\\3210\\0213\\3132\end{bmatrix} \quad SB_1 = \begin{bmatrix}0123\\2013\\3010\\2103\end{bmatrix}$$

Algorithm:
Simplified DES algorithm (SDES):

1. $P_{10}(K) \Rightarrow s = (s_0s_1s_2s_3s_4)(s_5s_6S_7S_8S_9)$
2. Shift(K) $\Rightarrow t = (s_1s_2s_3s_4s_0s_6s_7s_8s_9s_5)$
3. Ps(t) $\Rightarrow k_1 = (t_5t_2t_6t_3t_7t_4t_9t_8)$ 1^{st} subkey
4. Shift (t,2) $\Rightarrow u = (t_2t_3t_4t_0t_1t_7t_8t_9t_5t_6)$
5. $P_8(u) \Rightarrow k_2 = (u_5u_2u_6u_3u_7u_4u_9u_8)$ 1^{st} subkey
6. IP(m) $\Rightarrow m = (m_1m_5m_2m_0m_3m_7m_4m_6)$
7. $IP^{-1} \Rightarrow n = (n_3n_0n_2n_4n_6n_1n_7n_5)$
8. T(m) $\Rightarrow m = (m_4m_5m_6m_7m_1m_2m_3)$
9. Arrange n in diagram $D = \begin{array}{c|c|c|c} n_7 & n_4 & n_5 & n_6 \\ n_5 & n_6 & n_7 & n_4 \end{array}$
10. $D+k_1 = \begin{array}{c|c|c|c|c|c} n_7+k_{10} & n_4+k_{11} & n_5+k_{12} & n_6+k_{13}\ p_{00} & p_{01}\ p_{02} & p_{03} \\ n_5+k_{14} & n_6+k_{15} & n_7+k_{16} & n_4+k_{17}\ p_{10} & p_{11}\ p_{12} & p_{13} \end{array}$
11. $SB_0[(p_{00}p_{03}), (p_{01}p_{02})] = q_0q_1\ SB_1[(p_{10}p_{13}), [(p_{11}p_{12})] = q_2q_3$
12. $P_4(q) \Rightarrow (q_1q_3\ q_2q_0$
13. $S_1(nq) \Rightarrow (n_0+q_1, n_1+q_3, n_2+q_2, n_3+q_0, n_4+n_{5+}\ n_{6+}\ n_7)$
14. Repeat step 10-13using 2nd sub key k_2 instead tofroms$_2$
15. Encrypt $(IP^{-1}\circ S_2\circ T\circ S_1\circ IP)$
16. Decrypt $(IP^{-1}\circ S_2\circ T\circ S_1\circ IP)$

Training of SDES cipher: During the training, the error goal (sum squared error) is defined as ($0.00001 = 10^{-5}$), which gives 100% accuracy. After the training process has finished and the Neuro-Identifier has converged to the defined error goal, the Weights (W) and Biases (B) matrices are saved to be used later in the simulation phase. As an experimental result obtained from this research, emulation modes (encryption and decryption modes), a sub set of the training data was sufficient to capture the behavior of the algorithm. Table 1 shows the results of NID training for SDES cipher in both modes (encryption and decryption modes). Table 2 shows the results of NID training for SDES cipher in Cryptanalysis modes. Figure 3 shows the error curve of NID training for SDES cipher in encryption of emulation mode. Figure 4 shows the error curve of NID training for SDES cipher in cryptanalysis mode.

Simulation of SDES cipher: The simulation phase includes execution of the trained neural identifier in both approaches (cryptanalysis and emulation) using the saved Weights (W) and Biases (B) and the simulation data set (SP, SK, SC). Simulation of SDES cipher in both approaches (cryptanalysis and emulation) gives 100% accuracy for any length of key.

Table 1: That the creation of emulation models in SDES Cipher

Cipher system	Mode	Train set	NN size	No. epoch	No. of flops	Execution time (sec)
SDES	Encry.	1024	32*32	1640	4.871 e11	1.943 e4
	Decry	1024	32*32	2861	9.735 e11	2.932 e5

Table 2: That the creation of cryptanalysis models in SDES

Cipher system	Train set	NN size	No. epoch.	No. of flops	Execution time (sec)
SDES	1024	32*32	7869	9.4887 e15	8.3243 e11

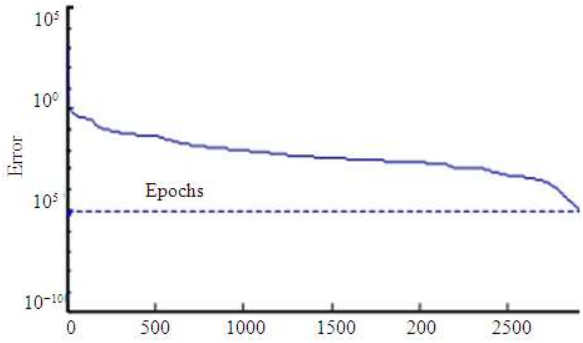

Fig. 3: Error curve emulation for SDES cipher

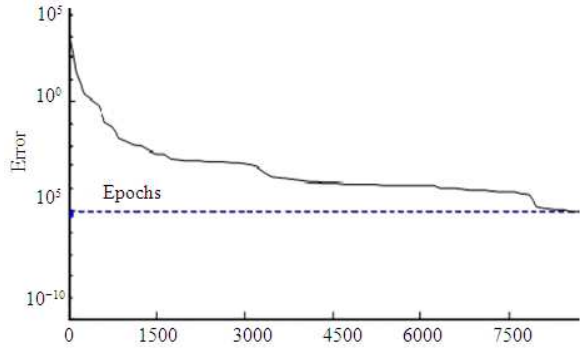

Fig. 4: Error curve cryptanalysis for SDES cipher

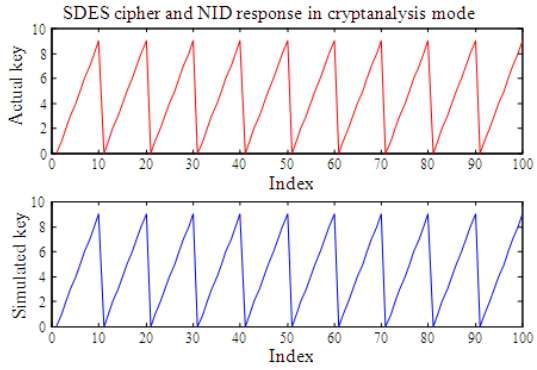

Fig. 5: Actual and behaviors of simulated NID response for SDES cipher.

The possible key of SDES cipher is any combination of lowercase alphabetic characters with maximum length of (1024 = 32*32) which is the size of the training set. Figure 5 shows actual and simulated key of length (300 characters) for SDES cipher.

CONCLUSION

- The Levenberg-Marquardt (LM) algorithm from neural network is used to train the Neuro-Identifier which gives good approximation capabilities, faster convergence, more stable performance surface. This study present the idea of the equivalent cipher system, which is identical 100% to the unknown system and that means that an unknown hardware, or software cipher system could be reconstructed without known the internal circuitry or algorithm of it.
- Most of identification techniques can identify certain cipher systems, but not all of them, the presented method is a generalized method that could identify many cipher system and build the equivalent system from the input-output observations.
- Emulation cryptography is a generalized method that could be used to all cryptographic systems. The only changeable parameter is the size of the hidden layers which should be made large enough to accommodate the key space of the target cipher system. The total number of neurons in the hidden layers is at most equal to the number of training samples, giving that the training samples are sufficient to describe the target system behavior. The feature of generalization is due to the characteristic of modeling.

REFERENCES

Alallayah, K.M., W.F.M. Amin and A.H. Hamami, 2010. Attack and construction of simulator for some of cipher systems using neuro-identifier. Int. Arab J. Inform. Technol., 7.

Ball, G., S. Mian, F. Holding, R.O. Allibone and J. Lowe *et al*., 2002. An integrated approach utilizing artificial neural networks and SELDI mass spectrometry for the classification of human tumours and rapid identification of potential biomarkers. Bioinformatics, 18: 395-404. http://www.ncbi.nlm.nih.gov/pubmed/11934738

Bin, H.G. and H.A. Babri, 1998. Upper bounds on the number of hidden neurons in feed forward networks with arbitrary bounded nonlinear activation functions. IEEE. Trans. Neural Networks, 9: 224-229. http://cat.inist.fr/?aModele=afficheN&cpsidt=2134110

Blankenship, G.L. and R.G. Ghanadan, 1996. Adaptive control of nonlinear systems via approximate linearization. IEEE. Trans. Control, 41: 618-625. http://cat.inist.fr/?aModele=afficheN&cpsidt=3058423

Bruce, S., 1996. Applied Cryptography, Protocols, Algorithms and Source Codes in C. 2nd Edn., John Wiley and Sons, Inc., New York, ISBN: 0471128457, pp: 784.

Cinar, A., 1996. Nonlinear time series models for multivariable dynamic processes chemometrics and intelligent laboratory systems. Coden Cilsen, 30: 147-158.

Jiang, Z. and Y. Zhou, 2006. Using gene neural networks to drug target identification. J. Integrat. Bioinform., 2005-12-07.

Leaster, N.S.H. and J. Sjoberg, 2000. Efficient training of neural nets for non-linear adaptive filtering using a recursive levenberg-marquardt algorithm. IEEE. Trans. Sign. Process., 48: 1915-1927. DOI: 10.1109/78.847778

Lennart, L., 1987. System Identification, Theory for the User. Englewood Cliffs. Prentice-Hall, Inc., Oxford University Press, New York, USA., ISBN: 0138816409, pp: 519.

Liu, X. and P.D. Truong, 1995. Neural Networks for Identifications, Prediction and Control. Springer-Verlag Ltd., New York, ISBN: 3540199594, pp: 238.

Lester, S.H. and N. Jonas, 1998. Some Aspects of Neural Nets and Related Model Structures for Nonlinear System Identification. Kluwer Academic Publishers, Chapter in Monograph.

Nalini, N. and G.R. Rao, 2006. Cryptanalysis of simplified data encryption standard via optimization heuristics. Proceeding of the 3rd International Conference on Intelligent Sensing and Information Processing, Dec. 14-17, IEEE Computer Society, Bangalore, pp: 74-79. DOI: 10.1109/ICISIP.2005.1619415

Patterson, D.W., 1998. Artificial Neural Networks, Theory and Application. Prentice Hall, Singapore, ISBN: 0132953536, pp: 400.

Pieprzyk, J. and S. Jennifer, 1989. Cryptography, an Introduction to Computer Security. Upper Saddle River, Prentice Hall, New Jersey, ISBN: 0-13-194986-1, pp: 375.

Saggar, M., T. Mericli, S. Andoni and R. Iikkulainen, 2007. System identification for the Hodgkin-Huxley model using artificial neural networks. Proceeding of the International Joint Conference on Neural Networks, Aug. 12-17, IEEE Xplore Press, Orlando, FL., pp: 2239-2244. DOI: 10.1109/IJCNN.2007.4371306

Sarle, W.S., 2002. Neural Networks FAQ. Newsgroup: http://comp.ai.neural-nets.ftp://ftp.sas.com/pub/neural/FAQ.html

Schaefer, E.F., 1996. A simplified data encryption standard algorithm. Cryptologia, 20: 77-84. http://direct.bl.uk/bld/PlaceOrder.do?UIN=003312008&ETOC=RN&from=searchengine.

Simon, H., 1998. Neural Networks: A Comprehensive Foundation. 2nd Edn., Prentice Hall PTR Upper Saddle River, New Jersey, USA.

Tanomaru, J., 1994. Comparative study of two neural network approaches for nonlinear identification. Proceeding of the International Symposium on Speech, Image Processing and Neural Networks, Apr. 13-16, IEEE Xplore Press, Hong Kong, pp: 487-490. DOI: 10.1109/SIPNN.1994.344865.

Thomas, B.A., 2008. Quantitative security of block ciphers: designs and cryptanalysis tools. PhD Theses. http://biblion.epfl.ch/EPFL/theses/2008/4208/4208_abs.pdf

Tsong, C.C., 1999. Linear System Theory and Design. 3rd Edn., Oxford University Press, Oxford.

Whitfield, D. and M.E. Hellman, 1979. Privacy and authentication: An introduction to cryptography. Proc. IEEE., 67: 397-427 .

Yu, W., M.A. Moreno and X. Li, 2000. Observer based neuro identifier. IEE Proc. Control Theor. Applied, 147: 145-152.

Zbikowski, R. and A. Dzielinski, 1995. Neural Approximation: A Control Perspective. In: Neural Network Engineering in Dynamic Control Systems, Advances in Industrial Control, Hunt, K.J., G.R. Irwin and K. Warwick (Eds.). Springer-Verlag, Berlin, pp: 1-25.