Journal of Engineering and Applied Sciences 11 (8): 1829-1834, 2016
ISSN: 1816-949X

Machine Learning Based Key Generating for Cryptography

[1, 2]Hayfaa A. Atee, [2]Robiah Ahmad, [2]Norliza Mohd Noor and [2, 3]Abidulkarim K. Ilijan
[1]Foundation of Technical Education, Higher Education and Scientific Research, Baghdad, Iraq
[2]Department of Engineering, Utm Razak School of Engineering and Advanced Technology,
Utm Kuala Lumpur, Jalan Sultan Yahya Petra, 54100 Kuala Lumpur, Malaysia
[3]College of Engineering, Almuthanna University, Samawa, Iraq

Abstract: An efficient key generation technique is demanding for a greatly secured cryptosystem. Traditional key generation techniques are very systematic which makes it subject to attack easily. The inclusion of Artificial Neural Network (ANN) algorithm in the cryptosystem is found to enhance the cryptographic performance in terms security and robustness to attack. Based on Extreme Learning Machine (ELM) for one hidden layer NN, we propose a sub-key generation approach for achieving a good cryptosystem. To initialize the input-hidden layer weights and data in each round, the initial key has been designed to include the ANN topology, activation function and seeds for Pseudo Random Number Generator (PRNG). The sub-key in each round is created using the output layer weights. Evaluation measures of the developed approach demonstrated complete sensitivity and predictability. Furthermore, the achieved remarkable reduction in the risks of breaking the symmetric key algorithm is attributed to the generation of independent sub-key in each round. Our secured sub-key generation approach may contribute towards the development of a secured cryptographic system.

Key words: ELM, ANN, sub-key generation, cryptographic systems, PRNG

INTRODUCTION

Algorithms in cryptographic systems are used for secured exchange of data information (videos, audios, text files, etc) without being leaked to unauthorized individuals or adversaries. Characteristically any cryptographic system is comprised of various algorithms and keys where the key in the form of a long string of bits provides a secret value. A key being agreed by authorized users is incorporated in the algorithm for further encryption and decryption of the information (Stallings, 2005). Symmetric key cipher (secret key cipher) and asymmetric key cipher (public key cipher) are the two basic cryptographic algorithms. The former type uses same key for both encryption and decryption process. Conversely, the later one uses different keys for encryption and decryption process (Sharma *et al*., 2014; Marwaha and Marwaha, 2010).

The prime importance of these keys mediated required security, reliability and the effectiveness of the cryptographic processes is instituted by the National Institute of Standards and Technology in 2014. The encrypted data security depends fully on two substantial elements such as the key space and sensitivity (Zhou *et al*., 2014) (a measure of security) and the strength of the cryptographic algorithm (Othman and Jammas, 2011). Absolutely, the key sensitivity is vital for preventing the cryptosystems against statistical and differential attack. It is acknowledged that large key space based cryptosystem provides high sensitivity (Baheti *et al*., 2014). Generally, this sensitivity measures the output alteration with respect to a specific input variation. In sub-key generation, sensitivity signifies the percentage of sub-keys change with respect to one-bit change in the initial key. High level of sensitivity between two keys implies the incapability of decrypting the data (texts or images) despite the high similarity between the two keys (Ranmuthugala and Gamage, 2010).

The algorithms for generating the sub-keys in cryptosystems that are developed using number theory suffers from many drawbacks such as large computational power consumption due to time complexity. The ANN based algorithms due to their parallel nature of functioning are found to be prospective for overcoming all such limitations. Furthermore, ANN based techniques significantly reduce the computational time, make the process faster, require less data with the capacity of generalization, learning, compatibility and accessibility of software as well as hardware. Thus, ANN based ELM systems are widely used for data encryption/decryption.

Corresponding Author: Hayfaa A. Atee, Foundation of Technical Education, Higher Education and Scientific Research, Baghdad, Iraq

The mathematical structure with universal approximation capabilities of such systemmake them ideal for cryptography. Despite analytical complication in the formulation it can simulate any data generating operation. On top, ELM is random in nature compared to other types of NNs. This is due to the random generation of input hidden layer weights in each iteration unlike other types of ANN. Besides, ELM possesses perfect sensitivity to all parameters which is considered as determinants of the ELM topology and mathematical definition. These parameters include the type of activation function, the number of hidden layer neurons and the number of input/output data. Despite intensive research a highly secured, efficient and accurate cryptographic system is far from being achieved.

This study proposed ELM based sub-key generation algorithm for cryptographic system. Using this approach, highly sensitive and secured keys are generated in terms of key space. Furthermore, the creation of randomized independent sub-key in each round has considerably reduced the risks of breaking the key due to attack.

Literature review: Development of successful encryption systems is decided by the synergistic combination of algorithm immunity and sub-key generation strength (Othman and Jammas, 2011). Over the years, several approaches are developed to generate sub-keys. Recently, NNs due to its successfulness in providing the key elements with sensitivity are suggested for generating strong keys. Different types of NNs rules and topologies are introduced for generating the key as well as for encrypting and decrypting the mined information (messages). To achieve such goal, a triple key encryption method based on logistic map is proposed (Zoghabi *et al*., 2013). The chaotic sequence is generated from the logistic map under a given 80 bits secret key. However, this algorithm possesses poor randomization and extra overhead for implementation.

To produce the round keys in the conventional Advanced Encryption Standard (AES), a NN-based key expansion method is developed. The proposed expansion schedule is comprised of four parts: the seed key generation for the input vector, the key scheduling for the desired output, the PRN generation for the initial weights of the NN and the round keys extraction upon NN training. Initially, some random values are allocated for the weight and bias values which are optimized using Levenberg-Marquardt (LM). Yet, this algorithm suffers from few limitations such as the output number of the key expansion training and the desired target are not identical as well as it needs more processes for adjusting the output to the desired target. To surmount such drawbacks, a novel scheme of AES is proposed (Li and Liu, 2013) where the independent round key is generated by the (2D) Henon map and the 2D Chebyshev map for improving the confusion of the algorithm. The 2D Henon map and the 2D Chebyshev map are sketched and then used to design the dynamic key of AES algorithm.

An ANN based stream cipher on PRNG is introduced (Othman and Jammas, 2011). The neural PRNG is achieved in two stages. First, a long sequence of pattern is generated from the perfect equation and initial value. Second, the ANN that obtained as the output from the previous stage is further assigned as input to the NN. The key generation using the Back-propagation NN (BNN) is comprised in three phases: feed-forward, back-propagation of the associated error and weights adjustment. A ANN based scheme for generating the secret key using a public channel is proposed. Interacting NNs are synchronized by considering the key generation in cryptography where the identical weights of the two partners are selected as the key for encryption. Two multi-layer NNs constructed the ANN. These networks are initiated using random initial weights and learning from each other where the communicator is unable to interchange any information before the initiation. This approach is not tested or analyzed against attacks.

A NN consisting of both chaotic and linear neuron layer is used (Lian, 2009). A block cipher system is constructed to convert the data from clear text to incomprehensible form under the user key control. The parameters are generated from the key and used to control the neuron layers. The developed cryptosystem is composed of diffusion and confusion processes. The chaotic neuron layer used to implement the diffusion process while the confusion process is implemented by the linear neuron layer where the number of iterations is ≥ 10. However, the charts showed that the cipher-bit change corresponding to key-bit change remains <60% with key space fewer than 264. Later, a novel approach is proposed to evaluate and validate the method (Ertugrul, 2014) for overcoming the synchronization problem of encrypt and/decrypt processes of ANNs. The proposed method approved the symmetric and asymmetric algorithms where the key is taken from the structure of ANN in terms of weights and biases of neurons. In this method, the key can be assigned randomly or defined by user. However, the key space and key sensitivity are not tested.

A NN with cryptography is combined (Jogdand and Bisalapur, 2011) to generate the secret key upon a public channel for calculating the interacting NNs analytically. The two communicating networks receiving identical input vector is used to generate the output bits. Then, it

learnt their mutual bits according to the output bits. The NNs generated the initial weights randomly while the inputs are generated by third parity. Finally, the outputs are generated and exchanged between communicators. When the output vectors of both machines are agreed with each other, then the corresponding weights are modified using the learning rule such as Hebbian, anti-Hebbian and random-walk. Upon synchronization, the synaptic weights are found to be same for both networks which are finally used as secret key. However, the secret key is generated by distribution center to achieve extreme security.

Using neural cryptography on a public communication channel, the synchronization of the Tree Parity Machines (TPMs) by mutual learning is applied (Prabakaran and Vivekanandan, 2010) to generate a secret key. The two NNs begin with a random number which are generated via the PRNGs and assigned to the weight vectors. Three transfer functions are trained such as the right-dynamic hidden unit that used anti-Hebbian learning rule, the left-dynamic hidden unit that used the random walk and the hidden unit that employed Hebbian learning rule. In each time step, the networks received the input vector for calculating and updating the weights vectors according to the matching process between the output and new weights vectors. These processes are continued until the weight vectors are matched. Next, the exchange is performed through a public channel for testing. A chaotic NN assisted triple key is used for image encryption (Suryawanshim and Nawgaje, 2012). Three different parameters are used to scramble the data image. Different operations are implemented on the image to scramble the date for achieving randomness. The achieved session key in the chaotic triple key being 20 hexadecimal characters produced 80 bits as a binarization. Some manipulations and extraction are executed on the key to attain the intermediate key which is further used to generate the chaotic sequence after merging with initial and control parameters.

ANN and ELM assisted cryptography: It is well known that cryptography is an art for converting clear text (plaintext) to ambiguous text (ciphertext). The main purpose of cryptography is to exchange the messages (data) secretly without being seen by phishers, unauthorized users and attackers. As aforementioned, for information encryption two basic techniques are used including the symmetric and the asymmetric one. A symmetric technique uses the same key (private key) for encryption and decryption processes. Alternatively, an asymmetric encryption technique uses two different keys such as public for encryption process and private for decryption process. All cryptographic algorithms need a

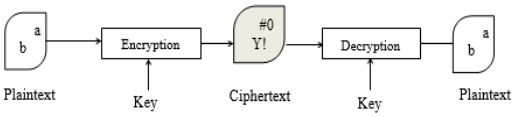

Fig. 1: Typical structure of encryption/decryption processes

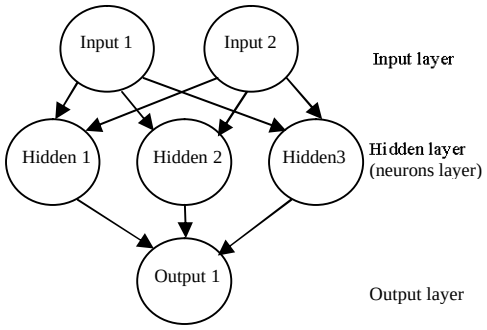

Fig. 2: Diagram of multilayer perceptron with one hidden layer

key to encrypt/decrypt the messages irrespective of their nature (Moldovyan and Moldovyan, 2007). The security of any cryptographic system being controlled by the key requires the generation of accurate key for achieving robust cryptographic algorithm. Figure 1 depicts the basic architecture of a typical cryptographic algorithm.

The ANN owing to their inherent nonlinear properties became attractive in cryptosystems for key generation or encryption process. It is extensively used for capturing and modeling the complex input/output relationship of assorted system. It can train and presents good performance when a set of input/output data belonging to the problem under study is available. Moreover, its notable features such as capability for generalizing the results, fastness, parallel structuring and processing, efficiency and reliability are overwhelming (Zoghabi *et al*., 2013). NNs are often exploited as non-linear statistical tools for data modeling. These are parallel adaptive networks involving simple nonlinear computing elements called neurons (Zoghabi *et al*., 2013) which are mathematical processing unit that receive one or more inputs to produce an output. Each neuron in the input layer possesses a related weight that defines its importance. The neuron just computes the weighted sum for all the outputs. The achieved output is reformed by transfer function (activation function) before being forwarded to another neuron in the next layer. Any NN consists of several neurons that are arranged in a particular structure. Figure 2 illustrates one of the most popular and successful type of NN called the Multi Layer Perceptron (MLP) network. The data flow into the NN of the input layer, pass over one or more hidden layers

before being exit via the output layer (Jogdand and Bisalapur, 2011). Originally, ANNs are intended to imitate intellectually some of human nervous system functionality for capturing its computational massive points (Ivancevic and Ivancevic, 2007).

Huang *et al*. (2006) first introduced the concept of ELM. It uses a Single-Layer Feed-forward Neural Networks (SLFN) to randomly select the hidden nodes and determines the output weights of SLFNs analytically. The ELM is considered as a one of new learning algorithm of ANNs. It overcomes the slow training speed and over-fitting problem present in other conventional NN learning algorithm by avoiding the multiple operations and the local minimization. It needs a single iteration in the learning process. ELM algorithm due to its robustness such as fast learning rate, controllability and well generalization ability is broadly used in different applications and assorted fields (Ding *et al*., 2015). To surmount the limitations associated with the existing encryption approach a robust method is needed.

MATERIALS NAD METHODS

The proposed ANN based ELM algorithm is comprised of one hidden layer with 100 neurons which is used to generate a key including 10 sub-keys. First, an initial key $K = \{k_1, k_2, k_3, \ldots, k_n\}$ is defined by the user where n (15) is the number of key elements. The first five elements are dedicated for the ELM determination which defined the number of inputs, outputs, type of activation function, number of hidden layer neurons and data size. For example, $K_{1\text{-}5} = \{k_1, k_2, k_3, k_4, k_5\} = \{3, 1, 1, 100, 100\}$ signifies ELM with 3 inputs, 1 output, first type of activation function (four kinds including Sin, Radial Basis Function, Sigmoid and Hardlim are considered), 100 neurons in hidden layer and 100 data. In ELM training, the first step is to initiate weights and biases in input-hidden layer. In addition, the remaining ten key elements, i.e., $K_{6\text{-}15} = \{8, 1, 7, 8, 5, 3, 2, 8, 2, 1\}$ are used as ten seeds set of the internal ten rounds of the sub-keys. Number ten has been selected considering the number of rounds in the advanced encryption standard AES. Each element of the seeds set is used to generate one sub-key by generating different weights and biases. This is generated randomly in each round belonging to a single iteration of ELM. Each sub-key is generated independently and separately of other sub-keys. All rounds are performed parallel and the ten sub-keys are generated simultaneously based on the nature of ANN and independent attributes of the proposed algorithm. It is worthy to mention that this approach of generating sub-keys is not subject to attack even in the case of seeds

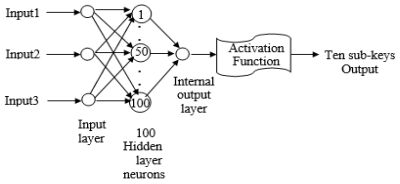

Fig. 3: Typical structure of encryption/decryption processes

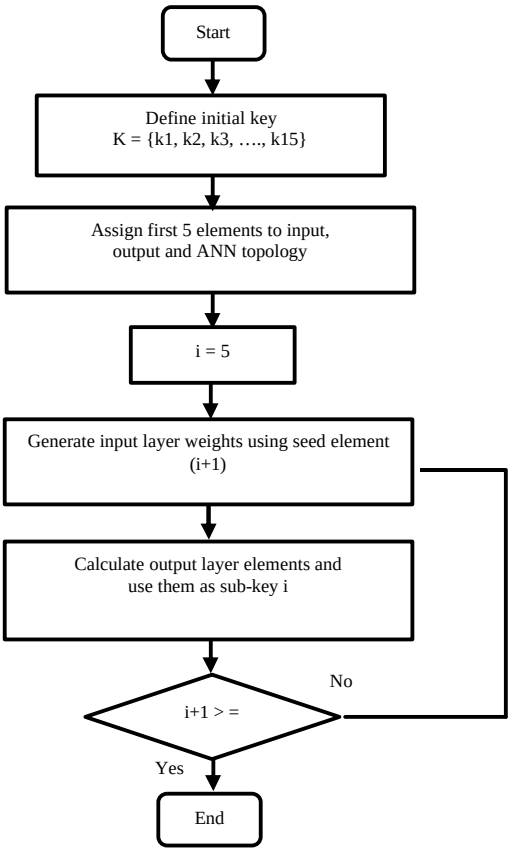

Fig. 4: Flow chart for generating the sub key using the proposed cryptosystem

are recognized by an attacker. This is because extra information are needed to determine the topology of the ANN and the ELM determinants. Also, by knowing these information users can easily change the content of the key and as a result change the whole machine learning based key generation approach. Figure 3 and 4 display the topological pattern and the flowchart of the proposed algorithm.

RESULTS AND DISCUSSION

Key space generation against brute-force attack: As mentioned earlier, the robustness of any cryptosystem is

decided by the key space which determined the strength of the key. Key space refers to the group of all possible keys that is used to generate a key. Theoretically, the brute-force attacks can break any cryptosystem. Practically, presence of elongated keys can well protect a cryptosystem from such attacks. Normally, the key length is determined by the number of bits (N). Thus, a cryptosystem with N key length provides 2^N possible case of search (key space). It is acknowledged (Lian, 2009) that the keys with length greater than 64 bits provide high security to such attacks. It this spirit, the proposed algorithm considered N = 120 with the possible number of trial equal to 2^{120}. This indeed requires longer times for cryptanalysis to test all possible keys for breaking the encryption algorithm.

Parameter sensitivity: Secure cryptosystems necessitate both a large key space and a high sensitive key. Typically, sensitivity can be measured based on changes in ciphertext when one bit of the key is altered. Yet, our proposed sub-key-generation algorithm has not been incorporated in a complete cryptosystem. The Position difference rate (Pdr) being one of the common sensitive parameter yields:

$$Pdr = \frac{Dif\_Round\_Keys\_Set\ (K, K1) + Dif\_Round\_Keys\_Set\ (K, K2)}{2N^2} \times 100$$

Where, Dif_Round_Keys_Set (K1, K2) represents the number of differences of the generated round keys from the initial keys (K1 and K2) where K1 and K2 possess the same elements of K with one-bit alteration only. The proposed algorithm is found to achieve a value of Pdr as much as 99%. Furthermore, the results revealed high level of sensitivity for all the tested twenty keys. Table 1 summarizes the values of Pdr and the achieved differences among the sub-keys K1 and K2 according to different values of the number of neurons in the network. Obviously, the algorithm of key generation has shown a consistently good performance regardless of the number of neurons in the neural network. Thus, it is feasible to use this key generation with high flexibility in terms of the values of the original key elements which determines the ANN topology including the number of neurons. In addition, the Pdr is shown in Fig. 5 with the two cases of 15 neurons and 100 neurons. As it can be observed the Pdr is still showing high sensitivity with respect to original key changes.

The strength of the proposed method is summarized in the following. Firstly, the key generation is based learning mechanism which makes it possible to simply change the learning data in case of breaking the key. As a result, no need for modifying the internal subsystem in case of an attack. Secondly, allocating separated technique for defining the seeds in the initial key will add more randomness to the process of key generation and as a result, more security to the whole system.

Table 1: The differences values between K1 and K2

K1	K2	Pdr 15 neurons	Pdr 25 neurons	Pdr 50 neurons	Pdr 100 neurons
011-00000011	011-00000010	0.9990	0.9965	0.9990	0.9920
011-00000011	011-00000001	0.9990	0.9990	0.9985	0.9925
011-00000011	011-00010111	0.9960	0.9980	0.9980	0.9930
011-00000011	011-00001011	0.9975	0.9985	0.9995	0.9945
011-00000011	011-00010011	0.9980	0.9995	0.9990	0.9935
011-00000011	011-00100011	0.9990	0.9975	0.9970	0.9940
011-00000011	011-01000011	1.0000	0.9985	0.9985	0.9935
011-00000011	011-10000011	0.9970	0.9975	0.9980	0.9940
011-00000101	011-00000100	0.9990	0.9985	0.9995	0.9955
011-00000101	011-00000111	0.9975	0.9980	0.9990	0.9950

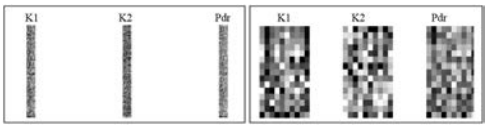

Fig. 5: The difference between K1 and K2 for: a) 100 neurons and b) 15 neurons

CONCLUSION

We developed ANN type ELM based sub-key generation algorithm useful for secured cryptosystem. The selection of initial key of length 120 bits is demonstrated to protect the developed cryptographic system against Brute-force attack. The primary key included the information including ANN topology, activation function and seeds for pseudo-random number generation in each round for initializing the input-hidden layer weights and data. The sub-keys those are generated from output layer weights are discerned to achieve high sensitivity. The evaluation revealed that the sub-keys sensitivity is >99% with key space of 2^{120}. It is worth to test this algorithm with AES and compare the results with other sub-keys generation algorithm.

REFERENCES

Baheti, A., L. Singh and A.U. Khan, 2014. Proposed method for multimedia data security using cyclic elliptic curve, chaotic system, and authentication using neural network. Proceedings of the 4th International Conference on Communication Systems and Network Technologies (CSNT), April 7-9, 2014, IEEE, New York, USA., ISBN:978-1-4799-3070-8, pp: 664-668.

Ding, S., H. Zhao, Y. Zhang, X. Xu and R. Nie, 2015. Extreme learning machine: Algorithm, theory and applications. Artif. Intell. Rev., 44:

Ertugrul, O.F., 2014. A novel approach to synchronization problem of artificial neural network in cryptography. Am. Assoc. Sci. Technol. Commun., 1: 27-32.

Huang, G.B., Q.Y. Zhu and C.K. Siew, 2006. Extreme learning machine: Theory and applications. Neurocomputing, 70: 489-501.

Ivancevic, V.G. and T.T. Ivancevic, 2007. Introduction: Human and computational mind. Comput. Mind A Complex Dyn. Perspect., 60: 1-269.

Jogdand, R.M. and S.S. Bisalapur, 2011. Design of an efficient neural key generation. Intl. J. Artif. Intell. Appl., 2: 60-69.

Li, J. and H. Liu, 2013. Colour image encryption based on advanced encryption standard algorithm with two-dimensional chaotic map. IET Inform. Secur., 7: 265-270.

Lian, S., 2009. A block cipher based on chaotic neural networks. Neurocomputing, 72: 1296-1301.

Marwaha, P. and P. Marwaha, 2010. Visual cryptographic steganography in images. Proceedings of the International Conference on Computing Communication and Networking Technologies (ICCCNT), July 29-31, 2010, IEEE, New York, USA., ISBN:978-1-4244-6592-7, pp: 1-6.

Moldovyan, A. and N. Moldovyan, 2007. Innovative Cryptography. 2nd Edn., Charles River Media, Boston, Massachusetts,.

Othman, K.M. and M.H.A.L. Jammas, 2011. Implementation of neural-cryptographic system using FPGA. J. Eng. Sci. Technol., 6: 411-428.

Prabakaran, N. and P. Vivekanandan, 2010. A new security on neural cryptography with queries. Int. J. Adv. Netw. Appl., 2: 437-444.

Ranmuthugala, M.H.P. and C. Gamage, 2010. Chaos theory based cryptography in digital image distribution. Proceedings of the International Conference on Advances in ICT for Emerging Regions, September 29-October 1, 2010, Colombo, Sri Lanka, pp: 32-39.

Sharma, M., R.B. Garg and S. Dwivedi, 2014. Comparative analysis of NPN algorithm and DES algorithm. Proceedings of the 2014 3rd International Conference on Reliability, Infocom Technologies and Optimization (ICRITO), October 8-10, 2014, IEEE, New York, USA., ISBN:978-1-4799-6896-1, pp: 1-6.

Stallings, W., 2005. Cryptography and Network Security Principles and Practices. 4th Edn., Prentice Hall, USA.

Suryawanshim S.B. and D. Nawgaje, 2012. A triple -key chaotic neural network for cryptography in image processing. Int. J. Eng. Sci. Emerg. Technol., 2: 46-50.

Zhou, Y., L. Bao and C.P. Chen, 2014. A new 1D chaotic system for image encryption. Signal Process., 97: 172-182.

Zoghabi, A.E., A.H. Yassin and H.H. Hussien, 2013. Survey report on cryptography based on neural network. Intl. J. Emerging Technol. Adv. Eng., 6: 456-462.