Extreme Learning Machine Based Sub-key Generation for Cryptography System

Hayfaa Abdulzahra Atee[1*], Robiah Ahmad[2*], Norliza Mohd Noor[3],

Abdul Monem S. Rahma[4]

[1]Foundation of Technical Education, Higher Education and Scientific Research, Baghdad, Iraq
[2,3]Department of Engineering, UTM Razak School of Engineering and Advanced Technology,
UTM Kuala Lumpur, 54100 Jalan Semarak, Kuala Lumpur, Malaysia
[4]Computer Science Department, University of Technology, Baghdad, Iraq

* [1,2]corresponding authors: haifaa_atee@yahoo.com and robiahahmad@utm.my

Abstract

The key generation process is the substantial step in any cryptosystem. Incorporating Artificial Neural Network (ANN) in the algorithmic work of cryptography achieves good performance in realizing high accuracy and security. In this paper, ANN based sub-key generation algorithm is presented. Extreme learning Machine (ELM) type is adopted for one hidden layer neural network. Initial key includes all needed information about ANN topology, activation function, and seeds for Pseudo-Random Number Generation (PRNG) in each round to initialize input-hidden layer weights and data. Sub-key in each round is generated from output layer weights. Evaluation measures have proved complete sensitivity and inevitability of this approach. In addition, it contributes in reducing the risks of breaking the symmetric key algorithms due to the generated independent sub-key in each round. Thus, it can be integrated in any cryptosystem for sub-key generation.

Keywords. ELM, ANN, Sub-key generation, Cryptographic systems

1 Introduction

Cryptography algorithms are used to exchange information between parties in safe way, and to prevent leaking information to unauthorized individuals. Typically, the cryptographic systems consist of algorithms and keys. In general, a key is a secret value (usually a long string of bits). A key is agreed by authorized users and it is used with the algorithm to encrypt and decrypt the message [1]. The two basic typical types of cryptographic algorithms are: symmetric key cipher (secret key cipher) that uses same key for both encryption and decryption process, and asymmetric key cipher (public key cipher) that uses different keys for encryption and decryption process [2].

The National Institute of Standards and Technology in 2012 has emphasized on the importance of the keys in meeting the required security, reliability of cryptographic processes, and the effectiveness of the protocols associated with the keys [3]. Therefore, the encrypted data security is dependent fully on two substantial elements: security of the key, and strength of the cryptographic algorithm [4]. Key sensitivity is critical for preventing cryptosystems against statistical and differential attack. Thus, it is advised to provide the large space key of cryptosystem with a high sensitivity [5]. Generally, the concept of sensitivity measures the amount of output changes with respect to specific change in the input. In sub-key generation, sensitivity denotes the percentage of sub-keys change with respect of one bit change in the initial key. High level of sensitivity between two keys implies incapability of decrypting data (texts or images) notwithstanding the high similarity between the two keys [6].

Number theory has been the most inspiring field of the algorithmic work of sub-keys generating in cryptosystems. Unfortunately, it suffers from many drawbacks such as consuming a large computational power due to complexity and time consumption. The ANNs has a good potential to resolve many problems and overcome all above drawbacks due to the parallel nature of ANN that reduces the computation time significantly. Also, the ANNs are attractive to researchers due to its capabilities such as fast computation, less data requirement, generalization, learning, and software and hardware availability and compatibility [7]. ELM based ANN has good promising properties to be used in a data encryption/decryption system. Firstly, it is a mathematical structure with universal approximation capabilities. Thus, it can simulate any data generating operation regardless how complicated its analytical formulation is. Secondly, ELM has a random nature comparing with other types of neural networks; this is because the input hidden layer weights are generated randomly in each iteration unlike other types of ANN. Thirdly, ELM has perfect sensitivity to all parameters that can be regarded 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. In this research, ELM based Sub-key generation for cryptographic system is proposed and presented to generate a key with high level of sensitivity and security in order to use in cryptographic algorithms. In addition to high sensitivity and high level of security in terms of key space, this approach reduces the risks of breaking the key due to the generating independent sub-key in each round.

2 Methodology

The philosophy of our sub-key generating paradigm is to take an advantages and attributes of ELM in order to design a system for sub-key generation. This system be regarded as a part of a total data encryption/decryption system. These attributes will provide our sub-key generation with chaotic nature, high sensitivity, and initial key sensitivity.

The procedure starts with defining the key as K= {k1, k2, k3,…k_n} , where n= No of key elements is 15. We dedicate the first five elements for the ELM determination. It is intended by the ELM determination, which defines the number of inputs, the number of outputs, the type of activation function, the number of hidden layer neurons, and the data size. For example, if: K_{1-5} = {k1, k2, k3, k4, k5} = {3,1,1,100,100}, it means ELM with 3 inputs, 1 output, first type of activation function (we consider four kinds in this article: Sin, Radial Basis Function, Sigmoid, and Hardlim) 100 neurons in hidden layer, and 100 data size. The remaining of the key elements K_{6-15} = {8,1,7,8,5,3,2,8,2,1} is considered seeds for the rounds of the sub-keys. Figure 1 shows the flowchart of the algorithm.

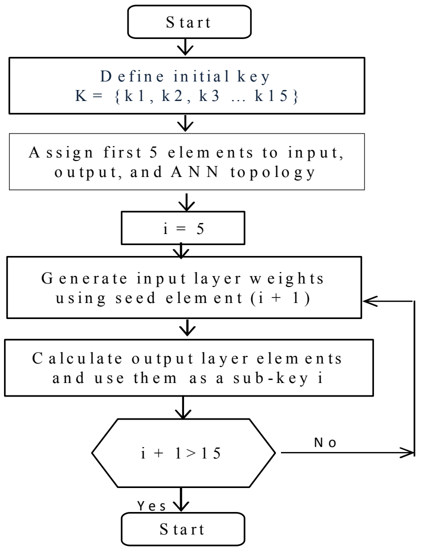

Start
Define initial key
K = {k1, k2, k3 ... k15}
Assign first 5 elements to input, output, and ANN topology
i = 5
Generate input layer weights using seed element (i + 1)
Calculate output layer elements and use them as a sub-key i
i + 1>15
No
Yes
Start

Figure 1. Flowchart of generating sub-key in cryptography system

3 Results, Evaluation, and Discussion

3.1 Key Space: Brute-Force Space

In cryptosystems, key space is one of the important qualities that determine the strength of the key. Key space refers to the group of all possible keys that can be used to generate a key. Brute force attacks theoretically can break any cryptosystem. Practically, long keys with relatively long size protect cryptosystem from such attacks. Typically, the key length is determined by N, which denotes the number of bits. Thus, a cryptosystem with N key length provide 2^N possible case of search (key space). As recommended by [8] keys with length more than 64 bits provide high security to such attacks. We considered N=120 in our algorithm with the possible number of trial equal $=2^{120}$, which requires longer times for cryptoanalysis to test all possible keys to break the encryption algorithm.

3.2 Parameter Sensitivity

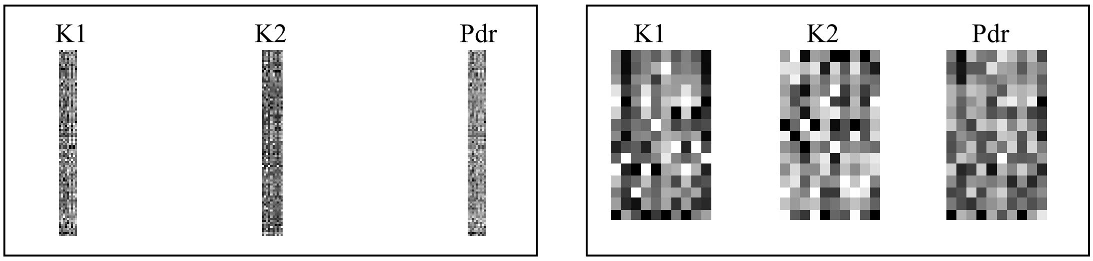
Secure cryptosystems require not only a large key space but also a high sensitive key. Typically, sensitivity can be measured based on changes in ciphertext when one bit of the key is changed. This current sub-key-generation algorithm has not been incorporated in a complete cryptosystem yet. Therefore, the sensitivity is measured based on changes in sub-keys when one element bit of the key is changed. One common sensitive parameter is the position difference rate (Pdr), which can be computed as [5]:

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

$Dif\_Round\_Keys\ \_Set(K1,K2)$ represents the number of differences of the generated round keys from the initial keys K1, K2 respectively. We consider that K1, K2 has the same elements of K with changing one bit only. N denotes the number of bits of round-keys set. In the current algorithm, the position reference rate (Pdr) has been evaluated to be more than 99%. Twenty keys have been tested; the results show high level of sensitivity. Table 1 and Figure 2 show the differences values between sub-keys of K1 and K2 respectively.

Table 1. The differences values between K1 and K2

K1	K2	Pdr (no. of neurons=15)	Pdr (no. of neurons=25)	Pdr (no. of neurons=50)	Pdr (no. of neurons=100)
011 ….011	011 ….00000101	0.9995	0.9980	0.9990	0.9910
011 ….011	011 ….00001001	0.9995	0.9995	0.9985	0.9925
011 ….011	011 ….00010001	0.9965	0.9985	0.9980	0.9930
011 ….011	011 ….00100001	0.9985	0.9990	0.9995	0.9945
011 ….011	011 ….01000001	0.9985	0.9990	0.9990	0.9940
011 ….011	011 ….10000001	0.9990	0.9965	0.9970	0.9945
011 ….101	011 ….00001001	1	0.9985	0.9985	0.9935
011 ….101	011 ….00010001	0.9970	0.9975	0.9980	0.9940
011 ….101	011 ….00100001	0.9990	0.9980	0.9995	0.9955
011 ….101	011 ….01000001	0.9990	0.9980	0.9990	0.9950



(a) **(b)**

Figure 2. The difference between K1 and K2: (a): 100 neurons (b) 15 neurons

4 Conclusion

ANN type ELM based sub-key generation algorithm has been developed. Initial key with a length of 120 bits has been used to protect against Brute-force attack. Primary key includes information about ANN topology, activation function, and seeds for pseudo-random number generation in each round to initialize input-hidden layer weights and data. High sensitive sub-keys are generated; sub-key in each round is generated from output layer weights. After evaluation, the sub-keys sensitivity has reached more than 99% with key space 2^{120}. Future work is to test this algorithm with AES and compare it with other sub-keys generation algorithm.

ACKNOWLEDGMENT

The authors would like to thank the UTM Razak School of Engineering and Advanced Technology, UTM Kuala Lumpur, Malaysia under the Research University Grant Project Vote 04H55 for the financial support provided throughout the course of this research.

References

1. Patil, V. S., Patinge, S. A., Dave, S. R., & Sayasikamal, G. J. Cryptography as an Instrument to Network Security. International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol.2(3), pp.72–80, 2013.
2. Marwaha, P., & Marwaha, P. Visual Cryptographic Steganography in Images. In IEEE (Ed.), Second International Conference on Computing, Communication and Networking Technologies, pp. 1–6, 2010.
3. Radack, S. Generating Secure Cryptographic Keys: A CRritical Component of Cryptographic Key Management and the Protection of Sevsitive Iiformation /Itl Bulletin for August 2012, pp. 1–5, US, 2012.
   Retrieved from http://csrc.nist.gov/publications/nistbul/itlbul2012_12.pdf
4. Othman, K. M. Z., & Jammas, M. H. a L. Implementation of Neural - Cryptographic System Using FPGA. Journal of Engineering Science and Technology, vol. 6(4), pp. 411–428, 2011.
5. Lian, S., Sun, J., & Wang, Z. A block cipher based on a suitable use of the chaotic standard map. Chaos, Solitons and Fractals, 26, pp. 117–129, 2005.
   doi:10.1016/j.chaos.2004.11.096
6. Ranmuthugala, M. H. P., & Gamage, C. Chaos theory based cryptography in digital image distribution. International Conference on Advances in ICT for Emerging Regions (ICTer), pp. 32–39, 2010.
   Colombo: IEEE. Doi:10.1109/ICTER.2010.5643275
7. El-Zoghabi, A. A., Yassin, A. H., & Hussien, H. H. Survey Report on Cryptography Based on Neural Network. International Journal of Emerging Technology and Advanced Engineering (Ijetae), vol. 3(12), pp. 456–462, 2013.
   Retrieved from http://www.ijetae.com/files/Volume3Issue12/IJETAE_1213_81.pdf
8. Lian, S. A block cipher based on chaotic neural networks. Neurocomputing, 72, 1296–1301, 2009. doi:10.1016/j.neucom.2008.11.005