Nitesh Goel et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 3, Issue 2, June 2016, pp. 17-20

Cryptic Techniques Based On Neural Nets: A Review

Nitesh Goel[1] and Arpana[2]

[1]M.Tech Scholar, SGI, Samalkha, Kurukshetra University
[2]Associate Professor, SGI, Samalkha, Kurukshetra University

Abstract-**Neural cryptography is a nascent approach that attempts to resolve the key exchange problem encountered with non-classical computing through neural networks training based on identical input patterns. Of late, there has been a greater interest in the community to understand and study the security of cryptographic protocols implementation across different domains. Considering the search for successful and easy-to-use secure cryptanalytic measures, we focus the research to Neural Network – Secure Cryptography implementation providing a method, which would be exceedingly difficult to break without having exact knowledge of the methodology behind it. Neural networks are well known for their ability to selectively explore the solution space of a given problem. This feature finds a natural niche of application in the field of cryptanalysis.**

Keywords—**Neural Networks, Synchronization, key exchange, Cryptography, encryption, decryption**

I. INTRODUCTION

Neural networks cryptography is a new branch of cryptography which incorporates neural networks with cryptography. This cryptography is based on fact that neural networks can synchronize with each other by mutual learning process. At each point of the synchronization procedure, the network are fed a common pattern and deduce the output correspondingly. Once this is done, these neural networks adjust the weights based on the outputs. This leads to fully synchronized weight vectors.

The above mentioned synchronization process is very complex and dynamic in nature. Two neural networks can increase the effect of their moves by this mutual cooperation among each other. The individual weights of such networks often perform random walks, driven by a competition of attractive and repulsive stochastic forces. However, another network learned by the two participating neural networks faces a disadvantageous situation as it cannot manipulate the repulsive steps on its own. In other words, we can deduce that the bidirectional synchronization of neural networks is a faster and efficient way than the unidirectional training.

Due to its recent advancement, this field of cryptography has not yet been of much practical applications as of yet. Just like any new and developing field, progressive research findings on neural networks cryptography techniques and algorithms are bringing fresh and exciting ideas and implementations. This field and methodology is especially useful where the encryption keys are being generated continually and constant evolution of the system is taking place, both the neural networks and the insecure media used for communication. The ideas of mutual learning, self-learning and stochastic behavior of the artificial neural networks can also be alternatively used for the realization of symmetric key exchange protocols and mutual synchronization.

II. LITERATURE REVIEW

It has been amply proved that neural networks can satisfactorily reproduce any type of function. Employing this principle, neural networks provide a unique approach towards the cryptanalysis algorithms, proving them to an ideal as well as a powerful means to discover inverse-function for any ciphering algorithm. The mutual training and self-training ideas and display of stochastic behavior by neural networks are useful in various aspects of cryptanalysis, such as generating and hashing pseudo-random numbers, resolving key distribution issue employing the mutual synchronization provided by neural networks and of course, public-key generations in cryptographic techniques. Below section discusses the research work undertaken till now for the use of neural network in cryptosystems, by classifying them into three categories:

1. Synchronization neural networks

A New Security on Neural Cryptography with Queries, 2010

In this method proposed by N. Prabakaran, using neural cryptanalysis, a secret key was proposed generated by synchronizing Tree Parity Machines (TPMs) using the paradigm of mutual learning. The system consists of two dynamic systems that are identical, each of which starts with non-identical initial conditions and common input values synchronize them coupling those two individual systems. A common input vector is received by the neural networks upon computing the corresponding outputs and the synaptic weight vectors are updated at every time according to the similarity that occurs between the outputs. Until the synaptic weight vector match, there is no exchange over a public medium and this exchange can be employed as a private key for cryptanalysis of the messages exchanged. The synaptic weight vectors of the involved TPMs usually start with random numbers, generated using PRNGs (Pseudo Random Number Generators). This method was instrumental in fixing the security for numerical attacks.

Synchronization of neural networks by mutual learning and its application to cryptography, 2004

In this proposed model by Einat Klein, two separate neural networks are synchronized which are trained based on alternate outputs, through a chaos synchronization system to a weight vector which is equal time dependent that starts with different initial conditions. In this system, the logistic chaotic map is synchronized with the neural network. The two entities/networks involved in this model employed their individual neural networks for the logistics map. This results in the generation of the output bits, which are trained by mutual learning. A signal matching the chaotic maps is generated as two networks interact with each other. Thus, this process of neural cryptography improves the security and enhances the cryptographic system by applying the chaotic synchronization.

Neural Cryptography for Secret Key Exchange and Encryption with AES, 2013

This technique involved a synchronization key exchange algorithm for neural network cryptology. Ajit Singh proposed a model consisting of a feed-forward multi-layered neural network. This model also included two TPMs (Tree Parity Machines) which are basically in synchronized form. The synchronization is performed with random weights that are used as a single key for the cryptanalysis process. If the outputs of the two synchronizing machines are equal, the weights are modified based on the learning rule used. For the entire synchronization process, public medium is used for transmission of both the input and output vectors. By increasing the shared common key size, experimental results indicate that the model is both efficient and secure.

Design of an efficient neural key generation, 2011

This research work, proposed by R.M. Jogdand, generated, based on the neural networks, a common secret key. An identical input vector is received by the two separate communicating systems in this type of cryptographic technique. It generates an output bit and is then learned according to the output. The synaptic weights are initialized randomly in this type of model. The input is generated by a separate source and output is generated and exchanged between the training patterns. If the output of both the coordinating parties is matched, only then the weights may be modified. Upon synchronization, the altered weight acts as the singular key for both the processes of encryption and decryption. This process indicated the simulation results showing that the neural networks are secure according to this cryptosystem.

2. Chaotic Neural networks

Cryptography based on delayed chaotic neural networks, 2006

Wenwu Yu proposed an encryption techniques based on the chaotic hopfield neural networks with time varying delay. The chaotic neural network is used for generating binary sequences for masking the plaintext. The binary value of the binary sequence chooses the chaotic logistic map randomly, that used for generated the binary sequences. The plaintext is masked by switching of the chaotic neural network maps and permutation of generated binary sequences. Simulation results show that the proposed chaotic cryptography is more functional in the secure transmission of large multi-media files over public data communication network.

Cryptanalysis of a cryptographic scheme based on delayed chaotic neural networks, 2009

Due to the large key space, the key of the cryptosystem proposed by Wenwu Yu et.al, was very difficult to comprehend. Jiyun Yang analyzed the model proposed by Wenwu Yu. However, this key can be easily obtained by the selected plaintext attack, since the same key stream was used in the cryptanalysis process. This is done by employing two pairs of cipher text and plain text. However, the results of this model signify that this cryptographic scheme based on delayed chaotic neural networks is, in principle, insecure.

An Empirical Investigation of Using ANN Based N-State Sequential Machine and Chaotic Neural Network in the Field of Cryptography, 2012

This model, proposed by Nitin Shukla, presents two neural networks for the process of cryptanalysis. One of them is a chaotic neural network and the other is an n-state sequential machine. On the basis of backpropagation learning algorithm, one of the networks generates a finite state sequential machine employing a simple and recurrent neural network model. The initial state of the n-state sequential machine can be employed as the singular key for the cryptanalysis. On the other hand, the other network, i.e., the chaotic neural network generated the chaotic sequence by splitting the message into separate blocks and identifying the control parameter and the initial value. The generated chaotic sequence determines the synaptic weights and the biases and that will act as the common key for the cryptanalysis process. The experimental results of this model indicate that the two involved networks are secure, without mentioning about their efficiency.

A triple-key chaotic neural network for cryptography in image processing, 2012

Image processing acquires the center stage in this type of cryptanalysis modeling proposed by Shweta, B. It uses the triple key technique proposed by Rajender S. et.al, for image processing. Various operations to be performed on images use the triple parameters, which modifies the available data is such a way that it appears random, but it is aligned in some particular order. In this particular case, a hexadecimal key is included in this triple key chaotic neural networks model for image processing. This character, along with some manipulation and extraction processes, are further combined with the control parameters of the system and the starting values for the creation of the triple key chaotic neural networks to achieve an intermediate key. This algorithm can be applied to different sizes of color images and are able to successfully perform the cryptanalysis process.

3. Multi-layer Neural networks

Implementation of neural - cryptographic system using FPGA, 2011

Karam M. presented a stream cipher system based on pseudo Random Number Generator (PRNG) through using artificial Neural Networks (ANN). The PRNG model has a high statistical randomness properties for key sequence using ANN. The proposed neural pseudo random number generator consists of two stages; the first stage is generating a long sequence of patterns from perfect equation and initial value. So these patterns possess the randomness and unpredictable properties. The total number of equations and initial values depend on the number of bits that represented the initial value, the second stage is an artificial neural network (ANN) that gets the outputs of the previous stage and set it as input to the NN.

Artificial neural network based chaotic generator for cryptology, 2010

This model comprises of chaotic cryptosystems. These systems proposed by Ilker D. et.al, are hinge on the chaotic synchronization generator and the neural networks. Using the numerical solution of Chua's circuitry, this neural network model generates chaotic dynamics. There are three initial conditions and time variable in this proposed model as input. This input is made up of two hidden layers. Apart from them, output comprises of three chaotic dynamics. To find the best neural network structure based chaotic dynamics, multiple simulations are carried out on the neurons present in the hidden layers. Here, the common key for the cryptanalysis process are the chaotic dynamics. An advantage of the neural network based chaotic generator is the difference between the chaotic dynamics. This model does not suffer from any synchronization problem. This model also removes the disadvantage of having an analog circuit and numerical solution base chaotic circuit. This model can also be used on real time applications as per the experimental results obtained. It is considered to be efficient and highly secure system as well.

AES Cryptosystem Development Using Neural Networks, 2011

This model, proposed by Siddeeq. Y, is a modification of the AES – Advanced Encryption Standard. Based on the nonlinear neural networks, this new modification of AES is presented to be immune against many attacks. The cryptanalysis process is performed using a symmetric key cipher in this neural network. This key is used as the starting weights for the network that has been trained using the low cost algorithm. Output from the advanced encryption standard that has an efficient security, has been selected to be the objective of this model. Results achieved by this proposed AES cryptanalysis system based on neural networks have close proximity with the results achieved with the standard AES.

Cryptography based on neural network using ASCII code, 2012

It is based on multi-layered neural networks that are trained by the backpropagation learning algorithm proposed by Eva Volna. The plain text information is converted into the ASCII code by this proposed model. The sequence of bit used for each code is fractioned into 6 bit blocks which act as the input for the cryptanalysis process. The entire neural network structure comprising the input layer, output layer, hidden layers and the updated weights of the neural network. Simulation results of this model indicate that the system is found to be satisfactorily secure.

III. CONCLUSION

Although neural networks based cryptanalysis systems provide a good base for construction robust and complex cryptosystems, which require knowledge about the key and the topology of the network, it also must be aware of the synaptic weights of the neural networks and the number of adaptive iterations for the entire cryptology process. This makes it a very useful wireframe for building out cryptic systems. But, it still requires minimizing the error–rate by application of higher number of plain-text /cipher text combinations for the neural network based cryptanalysis process.

- Each of them incorporated an existing cipher or coding scheme into the neural network system
- With increasing key size, the time required for synchronization increases, thus compromising the security for the man-in-middle attacks.
- Many neural networks synchronization based researches place a constraint on the system by using one of the standard encryption algorithm.

REFERENCES

[1] "*A New Technique on Neural Cryptography with Securing of Electronic Medical Records in Telemedicine System*" – N.Prabakaran, Department of Mathematics, Anna University, 2008.

[2] A. Forouzan., "*Cryptography and Network Security*", First Edition. McGraw-Hill, (2007), USA.

[3] AtulKahate (2009), "*Cryptography and Network Security*", second edition, McGraw-Hill.

[4] William Stalling, "*Network Security Essentials (Applications and Standards)*", Pearson Education, 2004.

[5] Fausett, L.V. 1994 "*Fundamentals of Neural Networks*", Prentice-Hall, Inc., Englewood Cliffs, New Jersey.

[6] Adel A. El-Zoghabi, Amr H. Yassin, Hany H. Hussien, "*Survey Report on Cryptography Based on Neural Network*", IJETAE, 2013.

[7] Kinzel, W., 2002,"*Theory of Interacting Neural Network*".

[8] W. Kinzel, R. Metzler, and I. Kanter. "*Dynamics of interacting neural networks*". J. Phys. A: Math. Gen., 33(14):L141–L147, 2000

[9] L. Ein-Dor and I. Kanter. "*Confidence in prediction by neural networks*". Phys. Rev. E, 60(1):799–802, 1999.

[10] T. L. H. Watkin. "*Optimal learning with a neural network*". Europhys. Lett., 21(8):871–876, 1993.

[11] E. Klein, R. Mislovaty, I. Kanter, and W. Kinzel. "*Public-channel cryptography using chaos synchronization*". Phys. Rev. E, 72:016214, 2005.
[12] A. Klimov, A. Mityaguine, and A. Shamir. "*Analysis of neural cryptography*". In Y. Zheng, editor, Advances in Cryptology—ASIACRYPT 2002, page 288. Springer, Heidelberg, 2003.

