RESEARCH ARTICLE OPEN ACCESS

An Outline of Cryptanalysis and Cryptography Using Neural Network Framework

Dr. Aruna J. Chamatkar *, Prof. Sachin Y. Zade ** Dr. P. K. Butey***
**(Associate Prof., MCA Department, Kamla Nehru Mahavidyalaya, Nagpur*
Email: aruna.ayush1007@gmail.com)
*** (Assistant Prof., MCA Department, Kamla Nehru Mahavidyalaya, Nagpur*
Email: zade.sachin02@gmail.com)
****(HOD, Department of Computer Science, Kamla Nehru Mahavidyalaya, Nagpur)*

ABSTRACT
The neural network framework used for a development in cryptography. Cryptographic techniques and tools are playing an important role in designing emerging network security technologies. Cryptography is a fundamental part of cryptographic technology and is considered one of the important aspects associated with its use. It is constant battle between cryptographers trying to secure information and cryptanalysts trying to break cryptosystems that moves the entire body of cryptology knowledge forward. Cryptanalysis is the methods for obtaining the meaning of encrypted information, without access to the secret information that is normally required to do so.

In this paper we mainly focusing an overview over cryptanalysis and cryptography gives the how neural network application used for this techniques of security mechanisms of cryptography.

Keywords – ANN, Cryptography , Cryptosystem , Decryption , Encryption.

Date of Submission: 01-09-2022 Date of Acceptance: 12-09-2022

I. INTRODUCTION

Cryptology is divided into cryptography and cryptanalysis. Cryptography is an emerging technology in which two parties secure network communication by application of different encryption and decryption. Cryptography is the art and science of making a cryptosystem that is capable of providing information security. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. The art and science of breaking the cipher text is known as cryptanalysis. The cryptographic process results in the cipher text for transmission or storage. It involves the study of cryptographic mechanism with the intention to break them. Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths. A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services.[1]

In this Paper, we mainly focus on the study of neural network framework on cryptosystem.

II. TYPES OF CRYPTOSYSTEMS

There are basically two types of Cryptosystems based on the manner in which Encryption and Decryption is carried out in the system.

A. Symmetric Key Encryption

B. Asymmetric Key Encryption

The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. It is practically impossible to decrypt the cipher text with the key that is unrelated to the encryption key.[11]

A. SYMMETRIC KEY ENCRYPTION

The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption. The study of symmetric cryptosystems is referred to as symmetric cryptography. Symmetric cryptosystems are also sometimes referred to as secret key cryptosystems.[2]

A few well-known examples of symmetric key encryption methods are − Digital Encryption

Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.

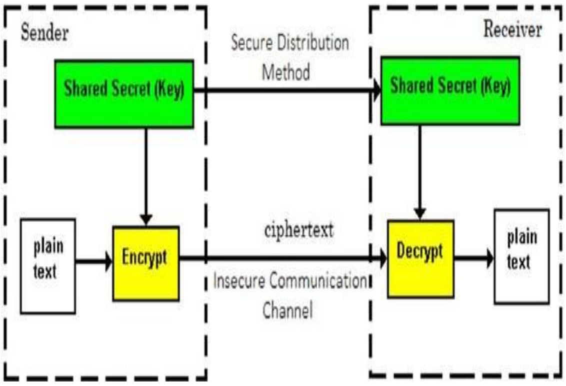

Fig. 1: Symmetric key Encryption

The salient features of cryptosystem based on symmetric key encryption are

1) Persons using symmetric key encryption must share a common key prior to exchange of information.
2) Keys are recommended to be changed regularly to prevent any attack on the system.
3) A robust mechanism needs to exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome.
4) In a group of **n** people, to enable two-party communication between any two persons, the number of keys required for group is **n × (n – 1)/2**.
5) Length of Key (number of bits) in this encryption is smaller and hence, process of encryption-decryption is faster than asymmetric key encryption.
6) Processing power of computer system required to run symmetric algorithm is less.

B. ASYMMETRIC KEY ENCRYPTION

The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting cipher text is feasible.

The salient features of this encryption scheme are as follows

1) Every user in this system needs to have a pair of dissimilar keys, private key and public key. These keys are mathematically related − when one key is used for encryption, the other can decrypt the cipher text back to the original plaintext.
2) It requires putting the public key in public repository and the private key as a well-guarded secret. Hence, this scheme of encryption is also called Public Key Encryption.
3) Though public and private keys of the user are related, it is computationally not feasible to find one from another. This is strength of this scheme.
4) When *Host1* needs to send data to *Host2*, he obtains the public key of *Host2* from repository, encrypts the data, and transmits.
5) *Host2* uses his private key to extract the plaintext.
6) Length of Keys (number of bits) in this encryption is large and hence, the process of encryption-decryption is slower than symmetric key encryption.
7) Processing power of computer system required to run asymmetric algorithm is higher.

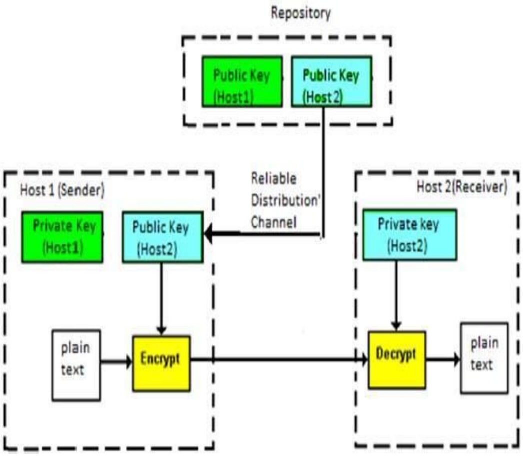

Fig. 2: Asymmetric key Encryption

III. NEURAL CRYPTOGRAPHY

An Artificial Neural Network is an information processing paradigm that is inspired by the way biological nervous systems, such as the brain, process information. The key element of this paradigm is the novel structure of the information processing system. It is composed of a large number of highly interconnected processing elements (neurons) working in unison to solve specific problems.[3][12]

The structured of neural network consist of different types layers

i) Input Layer-It contains those units (artificial neurons) which receive input from the outside world on which network will learn, recognize about or otherwise process.

ii) Hidden Layer-These units are in between input and output layers. The job of hidden layer is to transform the input into something that output unit can use in some way.

iii) Output Layer-It contains units that respond to the information about how it's learned any task.

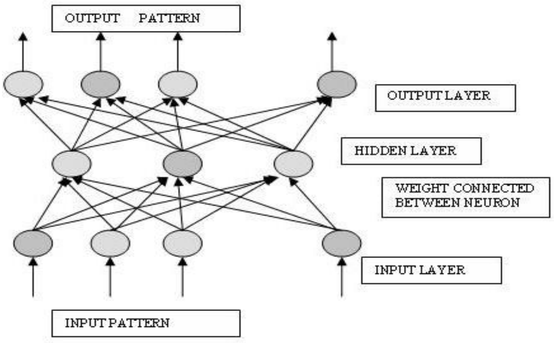

Fig. 3 : Basic structure of Neural Network

IV. WORKING OF NEURAL NETWORK FRAMEWORK IN CRYPTOSYSTEM

Artificial neural networks are used to classify functional blocks from a disassembled program as being either cryptography related or not. The resulting system, referred to as NNLC (Neural Net for Locating Cryptography). When training a neural network it is tempting to experiment with architectures until a low total error is achieved.[5]

In case of neural cryptography, both the communicating networks receive an identical input vector, generate an output bit and are trained based on the output bit. The two networks and their weight vectors exhibit a novel phenomenon, where the networks synchronize to a state with identical time-dependent weights. The generated secret key over a public channel is used for encrypting and decrypting the information being sent on the channel.[8]

We studied different types of neural network, we found back propagation neural network are more suitable for cryptography because it is very fast, simple and easy to analyze the program. The structure is iterative, recursive and efficient method through which it calculates the updated weight to improve the network until it is not able to perform the task for which it is being trained

There are some basic terms used in cryptography are as follows:

Plain text – The original message to be transferred to the other person.

Cipher text – The secret version of the plain text which is used for transferring.

Key – A secret code which is used to lock or unlock the plain text and the cipher text respectively.

Encryption – The process of converting plain text to cipher text.

Decryption – The process of converting cipher text to plan text.

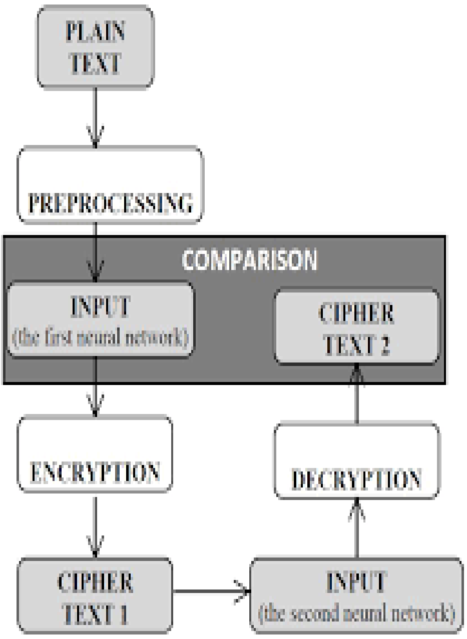

Fig. 4: Process of Neurl cryptography

The above procss of neural cryptography represents how encryption system works based on artificial neural network. D uring encryption no output error are found.[13]
In comparison with during decryption process,which is reverse of encryption there also this neural network work reliably.

V. CONCLUSION

In this paper , We define neural cryptanalysis as a cryptanalysis approach that leverages the learning ability of neural networks to measure the strengths of ciphers. In neural cryptology, two neural networks that have the same topology (layer size, transfer function, neuron number in each layer, weight and bias values) can achieve the same output when trained for the same input.

In this paper, study the structure of networks changes randomly. It means that the layer size and neuron numbers of each layer are generated by the neural-based pseudo-random number generator for each network structure. The training and transfer functions of the network are also selected randomly. This study also concluded that back propagation Neural network works more efficiently in case of cryptography system.

ACKNOWLEDGEMENTS

First author would like to acknowledge Dr. P. K. Butey for their cooperation and useful suggestion to research work.

REFERENCES

Journal Papers:

[1]. HiralRathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, “Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)” International Journal of Computer Technology and Electronics Engineering (IJCTEE), Vol.1, No.3 (2010/2011).

[2]. S.Z. Reyhani, M. Mahdavi, “User Authentication Using Neural Network in Smart Home Networks,” International Journal of Smart Home, Vol 1 no 2, pp147, July 2007.

[3]. Jacek M. Zurada- “ Introduction to Artificial Neural Network” Jaico Publishing House, 1999

[4]. Arvandi M., Wu S., Sadeghian A., Melek W. W., Woungang I.: Symmetric Cipher Design Using Recurrent Neural Networks. International Joint Conference on Neural Networks, pp.2039–2046, 2006.

[5]. Godhavari, T., Alamelu, N. R., & Soundararajan, R. (2005, December). Cryptography using neural network. In 2005 Annual IEEE India Conference-Indicon (pp. 258-261). IEEE.

[6]. M. Zeghid, M. Machhout, L. Khriji, A. Baganne, R.Tourki, “A Modified AES Based Algorithm for Image Encryption”, World Academy of Science, Engineering and Technology 27 2007.

[7]. K.Deergha Rao, Ch. Gangadhar, “Modified Chaotic Key-Based Algorithm for Image Encryption and its VLSI Realization”, IEEE, 15th International. Conference on Digital Signal Processing (DSP), 2007.

[8]. Saroj Kumar Panigrahy, Bibhudendra Acharya, Debasish Jen, “Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm”, 1st International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008.

[9]. Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan, Dai Wei-di, “Digital Image Encryption Algorithm Based on Chaos and Improved DES”, IEEE International Conference on Systems, Man and Cybernetics, 2009.

[10]. Min Long, Li Tan, “A chaos-Based Data Encryption Algorithm for Image/Video”, IEEE, Second International Conference on Multimedia and Information Technology, 2010.

[11]. Kuldeep Singh, Komalpreet Kaur, “Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it”, International Journal of Computer Applications (0975 - 8887) Vol.23, No.6, June 2011.

[12]. Chamatkar et al.” Implementation of Different Data Mining Algorithms with Neural Network” IEEE, International conference on International Conference on (ICCUBEA), Pune Feb. 2015

[13]. Eva volna et al.”Cryptograhy based on neural network” IEEE, ECMS 2012 Research gate may 2012

Books:

[14]. Cryptography and Network Security by Behrouz A. Forouzan

[15]. Guo D., Cheng L.-M., Cheng L. L.: A new symmetricprobabilistic encryption scheme based on chaotic attractors of neural networks. Appl. Intell., 10(1), pp. 71–84, r1999.

[16]. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of applied cryptography. CRC press.