ACADEMICIA: An International Multidisciplinary Research Journal
ISSN: 2249-7137 Vol. 11, Issue 11, November 2021 SJIF 2021 = 7.492
A peer reviewed journal

A REVIEW ON USE OF NEURAL NETWORKS IN CRYPTOGRAPHY

Dr. Shambhu Bhardwaj*

*Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, INDIA
Email id: shambhu.bhardwaj@gmail.com
DOI: 10.5958/2249-7137.2021.02572.6

ABSTRACT

Data security has become a top worry for everyone linked to the internet, as it has merged with our lives and grown at a breakneck pace over the past few decades. Data security guarantees that only the intended recipients have access to our information and prohibits any data modification or change. Various techniques and approaches have been developed to attain this degree of security. Cryptography is a set of methods for encrypting data using particular algorithms that render the data unreadable to the naked eye until decoded using preset procedures by the sender. Secret information is rendered illegible for unauthorized users using cryptography. Many cryptographic methods exist, but they are more complicated approaches that need more computing capacity. This article examines how neural networks aid cryptography and how neural networks and cryptography may be used together to improve security.

KEYWORDS: *Cryptography, Cryptosystem, Data Security, Neural Network, Key Generation.*

1. INTRODUCTION

Cryptography is a method of ensuring message secrecy. In Greek, the word has a particular meaning: "hidden writing." Nowadays, however, people and organizations' privacy is protected by high-level encryption, which ensures that information transmitted is safe and only the authorized recipient has access to it. Cryptography is an ancient technology that is continuously being explored, with historical origins. Examples date back to 2000 B.C., when the ancient Egyptians employed “secret” hieroglyphics, as well as other evidence from ancient Greece and Rome, such as hidden inscriptions and the renowned Caesar cipher(1)(2). Hundreds of millions of individuals use cryptography on a regular basis to secure data and information, but the majority are unaware of it. Cryptographic systems, in addition to being very valuable, are also exceedingly fragile, since a single programming or specification mistake may undermine them(3)(4).

1.1 Cryptography and Cryptosystem:

Cryptography is the process of concealing and transferring non-readable information or data via a public or private network. The following are the fundamentals of security services:

1. Confidentiality: It guarantees that only the trusted user may view the communication.
2. Authentication: it establishes a person's identification.
3. Integrity: It guarantees that the message sent to the recipient is not tampered with.

4. Non-repudiation: It establishes that the sender transmitted the communication that the sender claims not to have sent.

Keys serve an essential part in cryptographic security (Figure 1). In cryptography, there are two kinds of data encryption: symmetrical and asymmetrical. In symmetric encryption, the same key is used for encryption and decryption; the key may be shared, secret, or private. In asymmetric encryption, different keys are utilized for encryption and decoding.

Cryptosystem is a term used in cryptography to describe a collection of algorithms used to provide security services, most often for secrecy (encryption). A cryptosystem usually consists of three algorithms: one for key creation, encryption, and decryption. Plaintext refers to the initial communication, which is encrypted into cipher text (CT), which is decoded on the receiver's side and referred to as plaintext (PT)(5)(6).

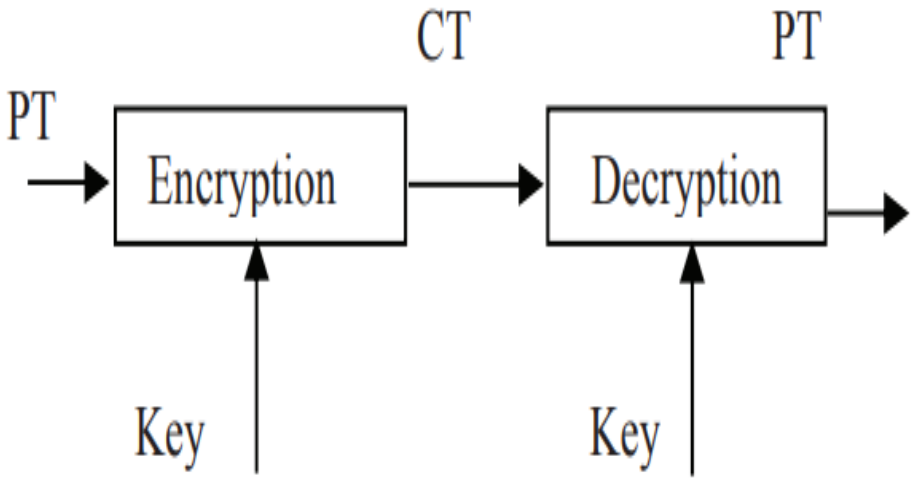

Figure 1: Illustrates the encryption and decryption technique using cryptography secret key.

1.2. Neural Networks:

Brain Networks are a class of statistical learning models that are based on biological neural networks and are used to estimate functions that are dependent on a large number of inputs and are often unknown. The interconnection between neurons in various layers of the system is referred to as a neural network. The first layer contains input neurons that provide data to the second layer, which then sends it to the third layer of output neurons through synapses. More layers of neurons will be present in a more complicated system. The synapses keep track of factors called "weights" that are used to modify data during calculations. Three kinds of parameters are often used to define a neural network(7)(8).

1. The pattern of interconnection between the various layers of neurons.
2. Learning process: for upgrading the interconnection's weights.
3. Activation function: this function transforms the weighted input of a neuron to its activation output.

The kinds of neural networks range from simple one- or two-layer single-direction logic to complex multi-input many-directional feedback loops and layers. In general, algorithms are used in the programming of these systems to define control and structure of their functions. To alter the parameters of the throughput and the changing connections to the neurons, most systems utilize "weights." Neural networks may be self-teaching or learn from a "teacher" outside of themselves.

2. LITERATURE REVIEW

A. Yayik et al. discussed in his paper, neural network based cryptology is performed. There are two phases to the system. In the first step, neural network-based pseudo-random numbers (NPRNGs) are produced, and the outputs are checked for randomness using randomness tests developed by the National Institute of Standards and Technology (NIST). In the second step, NPRNGs are used to create a neural network-based cryptosystem. Data that has been encrypted using non-linear methods is subjected to decryption efforts using two identical artificial neural networks in this cryptosystem (ANNs). Non-linear encryption is represented utilizing relation-building functionality in the first neural network. The second neural network uses decision-making functionality to decode the encrypted data(9).

S. Suryawanshi et al. discussed cryptography is the exchange of information among the users without leakage of information to others. Many public key cryptography systems are available that are based on number theory, but they have the disadvantage of requiring a lot of computing power, complexity, and time to generate the key. A neural network may be used to create a secret key to avoid these disadvantages. Many techniques use a chaotic neural network for cryptography; however, in this study, the network employs a 'triple key' to encrypt and decode data. Three distinct parameters set by the user are utilized to jumble the picture data, making it harder for hackers to access the data and therefore increasing security. MATLAB software is used for simulation. The results of the experiments indicate that the algorithm is capable of performing cryptography and is very sensitive to minor changes in key parameters(10).

2. WHY NEURAL NETWORK COMBINE WITH CRYPTOGRAPHY

There are many types of public key cryptography, each of which requires increasingly sophisticated methods and computing capacity. Various encryption methods are available to decrypt and encrypt data, and many assaults, such as brute force and man-in-the-middle attacks, may recover the key, which can be used to retrieve the original message, i.e. plaintext. The key for Advanced Encryption Standard (AES128) may be retrieved using a Biclique attack with a computational cost of 2126.1. The computational complexity of the Biclique attack on AES-192 and AES-256 are 2189.7 and 2254.4, respectively. AES-192 and AES-256 are vulnerable to related key attacks(11,12)(13).

A related key attack is any kind of cryptanalysis in which the attacker may witness the operation of a cipher using many distinct keys, the values of which are originally unknown but for which the attacker knows a mathematical connection. The RSA (129-digit) and RSA (193-digit) algorithms are likewise susceptible. Because cryptography methods are complex and there are conflicting tasks, a neural network-based technique is used. A good answer to this issue is Neural Cryptography. Strong network security may be achieved by combining neural networks with

encryption. The key to encryption and decryption is the neural network. The secret lies in the form of neural network weights, which are tough to break(14)(13)(15).

3. DIFFERENT NEURAL NETWORK BASED APPROCHES IN CRYPTOGRAPHY

3.1 Steganalysis:

Steganalysis involves the concealment of communication. Previously, Steganalysis was employed to conceal or prevent information from being revealed inside a complex graphic. Currently, digital steganography focuses on concealing hidden information inside redundant picture bits that must be sent. The primary goal is to increase the usage of steganography so that the attacker cannot covertly enter the message or discover that it contains a secret message. Steganography has now been combined with neural networks. Various methods, such as discrete cosine transformation (DCT) and wavelet texture decomposition, were used to analyze the first data. Images are classified using neural networks to determine if they contain hidden information or not. If the neural networks are impacted by an image concealing procedure, various weight sequences are produced as a result. Non-linear classifiers are more efficient or effective than linear classifiers because neural networks have a great capacity to learn from training data to approximate compute non-linear issues(16,17)(18).

3.2 Pseudo random number generator:

The cryptosystem's security is enhanced by randomness. There are a variety of statistical techniques that may be used to determine the randomness of a bit sequence. Multi-layer perception (MLP) neural networks are used in the pseudo random number generator. Neural networks have strong generalization capabilities after being trained on many well-known input vectors, allowing them to provide logical output to complex numbers, provided the input pattern is recognized. When the network is over-fitted, it will be unable to anticipate the input pattern when it receives unknown input patterns, resulting in unexpected outputs. MLP neural networks may be used as a powerful independent random generator or as a means of enhancing existing generators by feeding pseudo random numbers generated by linear computational generators into neural networks(19).

3.3. Digital Watermarking:

Watermarking safeguards digital information (text, picture, audio, and video) from being seen by an unauthorized user or attacker. Watermarking systems are categorized according to their requirements: Incorporation of a domain watermark, Detection and extraction of watermarks Watermark's ability to withstand assaults, as well as its visibility. Neural networks have characteristics that help watermarking methods function better. The “watermarked image” is created by mixing the original picture with the randomly produced watermark(20). The wavelet decomposition technique is used to extract significant coefficients. This additional data is fed into a trained neural network, which effectively extracts data to get the watermark. With the assistance of this data, the attached picture was created. The algorithm's security improves as the number of training patterns for a particular network grows(21)(22).

3.4 Key Generation, Management, and Exchange:

A neural key exchange mechanism based on the synchronization of two tree parity machines is described. Tree parity machine is a particular kind of multi-layer feed forward neural network that consists of K input neurons, N hidden neurons, and L weight range. In each phase, the two neural networks get the same random inputs and learn their shared outputs. The idea of synchronization through reciprocal learning is born as a result of this. A time-dependent weight vector is used to synchronize two devices. This idea was used to create a safe secret key for synchronization. The single secret key produced is used to encrypt and decode confidential information. Any algorithm, such as AES, may be used for encryption and decryption(23).

4. DISCUSSION

The fundamental idea of a cryptographic system is to encrypt information or data in such a manner that an unauthorized person cannot deduce its meaning. Cryptography is often used to transfer data across an unsecured channel, such as the internet, or to ensure that unauthorized individuals do not comprehend what they are looking at in a situation where they have obtained the information.

In cryptography, the obfuscated data is known as "plaintext," and the process of concealing it is known as "encryption." The encrypted plaintext is known as "ciphertext." This is accomplished via a set of principles known as "encryption algorithms." Typically, the encryption process uses a "encryption key," which is given to the encryption algorithm together with the data as input. The receiving side may recover the information using a "decryption algorithm" and the proper "decryption key."

A neural network is a computer that is used to simulate how the brain accomplishes a certain job. Electronic components are used to build the network, or it is emulated via software on a computer. A neural network is a massively parallel distributed processor composed of basic processing units that has a natural proclivity for accumulating and making accessible experimental information. In two ways, it mimics the brain:

1. Through a learning process, the network acquires knowledge from its surroundings.
2. Synaptic weights, or the strength of interneuron connections, are utilized to store learned information.

With its amazing capacity to extract meaning from complex or imprecise data, neural networks may be used to identify patterns and discover trends that are too complex for people or other computer methods to notice. Other benefits include:

1. *Adaptive Learning:* The capacity to learn how to do tasks using data provided during training or prior experience. 10
2. *Self-Organization:* During learning, an ANN may organize or represent the information it receives in its own way.
3. *Real-Time Processing:* ANN calculations may be performed in parallel, and specific hardware devices are being developed to take use of this capacity.

Artificial Neural Networks (ANNs) are a basic yet effective method for simulating extremely complex computing machines. We utilized this approach to create a basic combinational logic and sequential machine utilizing the back-propagation algorithm in this project. A comparison of

two distinct neural network designs has been conducted, with their benefits and drawbacks discussed. ANNs may be used to build both combinational and sequential circuits that are quite complicated. In data communication systems, data security is a major issue. Two approaches are used to explore the application of ANN in the area of cryptography. Data encryption is developed using a sequential machine-based approach. Also examined is a chaotic neural network for digital signal cryptography. Better results may be obtained by improving the code or using more effective training methods. As a result, Artificial Neural Networks may be used to encrypt and decrypt data in novel ways.

The following are some potential neural cryptography attacks:

1. Simple attack: the attacker has a neural network with the same structure as the neural networks of the two participants. The attacker begins with random starting weights and trains their neural network with the identical inputs as the two sides' neural networks.
2. Geometric attack: In this assault, both sides utilize the identical learning process, but the attacker uses the output of the attacker machine. It also makes advantage of the local fields of its neural network's hidden unit.
3. Majority attack: This is the chance of correctly predicting the internal representation of one of the two neural networks. This is accomplished via the use of multiple networks.
4. Genetic attack: In this case, the attacker only has one network to deal with. The attacker uses additional networks as the synchronization progresses.

5. CONCLUSION

Different Neural Network-based methods that may be used with cryptography are described in this article. Visual cryptography coupled with neural networks differs significantly from conventional encryption and may be used to deal with very complicated access schemes. The neural network-based Steganalysis method produces more accurate results than previous approaches. The key generated by neural networks is in the form of the weights of the neural network. The attacker finds it difficult to synchronize with the two parties since the key generation procedure between the two sides is extremely rapid.

REFERENCES:

1. Khokher A, Talwar R. Evaluation of a content-based image retrieval system using features based on colour means. Int J Inf Commun Technol. 2012;
2. Kalra GS, Talwar R, Sadawarti H. Blind digital image watermarking robust against histogram equalization. J Comput Sci. 2012;
3. Hadke PP, Kale SG. Use of Neural Networks in cryptography: A review. In: IEEE WCTFTR 2016 - Proceedings of 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare. 2016.
4. Gill J, Singh B, Singh S. Training back propagation neural networks with genetic algorithm for weather forecasting. In: SIISY 2010 - 8th IEEE International Symposium on Intelligent Systems and Informatics. 2010.
5. Www W:, El-Zoghabi AA, Yassin AH, Hussien HH. Survey Report on Cryptography Based

on Neural Network. Certif J. 2008;

6. Kamini, Sharma P. Algorithmic review of WTLS and TLS for recommending measures for implementing CSP in the network gateway. In: Proceedings: Turing 100 - International Conference on Computing Sciences, ICCS 2012. 2012.

7. Volna E, Kotyrba M, Kocian V, Janosek M. Cryptography based on neural network. In: Proceedings - 26th European Conference on Modelling and Simulation, ECMS 2012. 2012.

8. Kaur P, Rattan D, Bhardwaj AK. Enhancement of fault tolerance of intrusion detection system using AES and DES based heart beat events. In: International Conference and Workshop on Emerging Trends in Technology 2011, ICWET 2011 - Conference Proceedings. 2011.

9. Yayik A, Kutlu Y. NEURAL NETWORK BASED CRYPTOGRAPHY. Neural Netw World. 2014;

10. Suryawanshi SB, Nawgaje Dd. A Triple-Key Chaotic Neural Network For Cryptography In Image Processing. Int J Eng Sci Emerg Technol. 2012;

11. S. A, N. N. Cryptography based on Artificial Neural Networks and Chaos Theory. Int J Comput Appl. 2016;

12. Sethi A, Mittal A, Tiwari R, Singh D. Elliptic curve cryptography using chaotic neural network. Int J Pure Appl Math. 2018;

13. Ghai W, Kumar S, Athavale VA. Using gaussian mixtures on triphone acoustic modelling-based punjabi continuous speech recognition. In: Advances in Intelligent Systems and Computing. 2021.

14. Khatri M, Kumar A. Stability Inspection of Isolated Hydro Power Plant with Cuttlefish Algorithm. In: 2020 International Conference on Decision Aid Sciences and Application, DASA 2020. 2020.

15. Solanki MS, Goswami L, Sharma KP, Sikka R. Automatic Detection of Temples in consumer Images using histogram of Gradient. In: Proceedings of 2019 International Conference on Computational Intelligence and Knowledge Economy, ICCIKE 2019. 2019.

16. Wu S, Zhong S, Liu Y. Deep residual learning for image steganalysis. Multimed Tools Appl. 2017;

17. Karampidis K, Kavallieratou E, Papadourakis G. A review of image steganalysis techniques for digital forensics. J Inf Secur Appl. 2018;

18. Anand V. Photovoltaic actuated induction motor for driving electric vehicle. Int J Eng Adv Technol. 2019;8(6 Special Issue 3):1612–4.

19. Singh DP, Deivedi SK, Hashim SR, Singhal RG. Synthesis and antimicrobial activity of some new quinoxaline derivatives. Pharmaceuticals. 2010;

20. Tripathi L, Singh R. Anticonvulsant and neurotoxicity evaluation of some novel cyclohexyl-[4-substituted benzylidene/2-oxo-1,2-dihydro-indol-3-ylidene] thiosemicarbazides. Asian J Chem. 2011;

21. Uma Surya Sai B, Samyukta R, Vandana P, Surekha K, Paramkusam A V. Digital watermarking using matlab. Int J Appl Eng Res. 2017;

22. Sonar PK, Singh R, Khan S, Saraf SK. Isolation, characterization and activity of the flowers of Rhododendron arboreum (Ericaceae). E-Journal Chem. 2012;

23. Kumar A, Jain RK, Yadav P, Chakraborty RN, Singh BK, Nayak BK. Effect of gamma irradiation on the etching properties of Lexan and Makrofol-DE polycarbonate plastics. J Radioanal Nucl Chem. 2013;