PalArch's Journal of Archaeology of Egypt / Egyptology

DEVELOPMENT AND USE OF NEURAL NETWORKS FOR PURPOSE OF SECURE INFORMATION PROCESSING

Naofal Mohmad Hassein Azeez [1], *Ermakov Dmitrii Nikolaevich* [2]

[1, 2] Peoples' Friendship University of Russia (RUDN University)، 6, Mikluho-Maklaya Str., Moscow, Russia, 117198.

Email: [1]nawofel_aziz@qu.edu.iq, [2]ermakov_dn@pfur.ru

Naofal Mohmad Hassein Azeez, Ermakov Dmitrii Nikolaevich, Development and Use of Neural Networks for Purpose of Secure Information Processing -- Palarch's Journal of Archaeology of Egypt/Egyptology 19(1), 1436-1444. ISSN 1567-214x.

Keywords: Neural Networks, Secure Processing, Cryptography, Key Management, Generation, Exchange.

ABSTRACT:
The using encryption, private information is protected from prying eyes. These increasingly complicated and computationally intensive encryption algorithms exist because there are so many of them. For security, neural networks and encryption can be utilized together. These systems can be improved by using neural network architectures to detect anomalies, which can then distinguish between benign and malicious packets. A normalized and selected/reduced feature set is typically pre-processed onto the data before it is fed into the IDS in order to effectively predict anomalies. Training a neural network to optimize its performance takes into account the effects of pre-processing techniques. Described in this paper are the algorithms involved in pre-processing.

INTRODUCTION:

Cryptography and Cryptosystem

The practice of encrypting and transmitting information that cannot be decoded via a public or private network is known as cryptography. The following are the basic tenets of security services:

1. It assures that only the sender and the recipient have access to the message.
2. In order to authenticate oneself, one must provide proof of identity.

3. It ensures that the message received by the receiver hasn't been tampered with.
4. Non-repudiation is proof that a message that a sender claims to have sent was, in fact, transmitted.

Keys serve a crucial part in cryptographic security. Data can be encrypted in two ways: symmetrically or asymmetrically, depending on the type of cryptography used. The key used to encrypt and decrypt symmetric data is the same in both operations; the key may be a shared key, secret key, or private key, depending on the type of encryption. Asymmetric encryption employs separate keys for encryption and decryption. Algorithms used for security, most typically confidentially, are called a cryptosystem in cryptography (encryption). Three algorithms are usually used in a typical cryptosystem: A key generation key pair, an encryption key pair, and a decryption key pair. Text that has been encrypted into a ciphertext (CT) and then decided on the receiver side is called plaintext (PT) [1]. As shown in fig1.

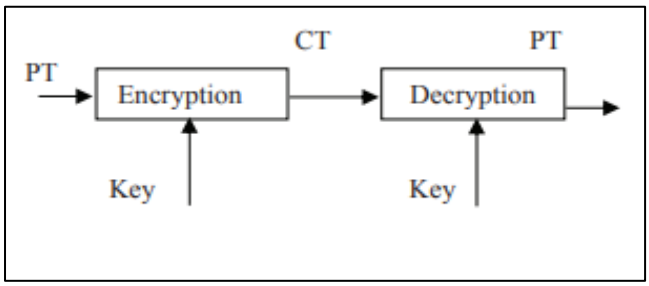

Figure 1. The text that has been encrypted into a ciphertext (CT) and then decided on the receiver side is called plaintext (PT).

Neural Networks

To estimate functions that depend on numerous inputs and are generally unknown, neural networks, a family of statistical learning models inspired by biological brain networks, are utilized. It is the interconnection of neurons in different layers of the system that is referred to as a "neural network". Input neurons in the first layer feed data to the second layer, which in turn feeds data to the third layer of output neurons via synapses. There will be more layers of neurons in a sophisticated system. Weights" are parameters stored in the synapses that influence the computation of data. Three types of parameters are commonly used to describe a neural network [2]:

1. Pattern of interconnection between the different neuronal layers.
2. For updating the weights of the interconnection, this is the learning process.
3. Function that translates a neuron's input to its output activity.

There are many different forms of neural networks, ranging from simple single-direction networks with one or two layers to complex multi-input networks with many directional feedback loops and layers. To organize and govern their operations, these systems usually rely on algorithms in their code.

"Weights" are commonly used in most systems to alter the interactions between the neuron and the throughput. The knowledge of neural networks can be acquired by self-learning or by external tutoring [3].

LITERATURE REVIEW

Only the sender and receiver of the data should be able to see the data, which is why it must be encrypted. Cryptography is essential for ensuring data privacy and confidentiality. We are integrating neural networks and cryptography into our work. Decisions may be made automatically using artificial neural networks by computing the proper weights (parameters) to ensure compatibility of the system and this is critical for stream cipher cryptography, which relies on these parameters to ensure strong security. When artificial neural networks were first developed, they were fueled by the knowledge that the brain processes information in a unique way. The brain is made up of billions of neurons connected by a vast network. Neuronal networks are similar in that they are massively parallel distributed processors that are made up of artificial neurons and connections between them. In order to compute the output, these are nonlinear dynamic machines that expand the expression of input data as a linear combination of synaptic inputs [4].

In modern business and technology, information security is widely considered to be necessary for the protection of confidential transactions and communications, as well as for defense against intruders. Data transmission across an unsecured channel while maintaining the confidentiality of the data transferred is known as cryptography. The confidentiality, authentication, and integrity of transmitted data should be ensured using cryptographic techniques (such as the stream cipher utilized in this study). As a rule, third parties are expected to be able to see encrypted data but cannot decipher it. Confidentiality is fundamental. It is possible to verify that the sender is who they claim to be through authentication procedures. Systems that lack authentication are open to fraud and denial-of-service attacks. Transmitted data must have verifiable integrity, which means that the recipient can verify that no data was lost or altered in the process of transmission. Improved cryptographic approaches are needed on all three of these fronts as cryptanalytic attacks become more sophisticated and less expensive [5]

According to a thorough literature review, there has been an increase in the use of neural networks in the field of cryptography in recent years. (A number of studies have examined the connection between cryptography, machine learning, and neural networks. (Neural networks have been investigated in many layers of cryptosystems in recent research papers. Key management, generation, and exchange protocols; the design of pseudo-random generators; prime factorization; hash functions; symmetric ciphers; authentication; and authorization are just a few of the most common instances of this. (The Tree Parity Machine (TPM) has been used in cryptography in a number of research. Based on TPM, mutual learning between two feed-forward neural networks with discrete and continuous weights was proposed and analytically analyzed by Kinzel and Kanter. Analytical solutions are reliant on auxiliary variables that are not self-averaging. By employing synchronization of Tree Parity Machines, their approach provides symmetric key exchange over a public

channel. It has been determined that an attacker seeking to impersonate one of the networks has a substantially longer learning period than the synchronization period, which has been studied analytically [6]. For illicit objectives, data sent through public infrastructure should be encrypted. Encryption relies on a data mapping technique that is impervious to prying eyes [7].

Symmetric and asymmetric encryption is two of the most often used encryption methods. Participants in the symmetric encryption approach share the same key. Both the encoding and decoding operations make use of this. The sender uses a key (K) to encrypt the message (M) and generate the codeword (W) (E). Members of an asymmetric encryption model are given two keys: a private key and a public key, both of which are assigned to each member. Encryption works in such a way that only the corresponding private key can decrypt a message encrypted with the public key, and the reverse is true for a message encrypted with the Private Key. Since the recipient's public key is required to decrypt private messages, they are sent via public infrastructure and encrypted before being delivered. The receiver's private key is used to decode the encoded message [8]. The sender of a message can also be authenticated using an encryption technique. A digital signature is a name given to this process. The sender encrypts the communication using his or her private key in order to sign it. To decrypt the message, the recipient utilizes the inverse function in conjunction with the sender's public key. Because only the sender has the key to decrypt the communication, the recipient knows who sent it. Messages that are encrypted can include the time and date of their creation to prevent them from being resent later. It's interesting to note that two levels of encryption can be employed to ensure the message's authenticity and confidentiality simultaneously [9]. The communication is first encrypted with the sender's private key. Second, the recipient's public key is used to encrypt the message again. Show in fig.2

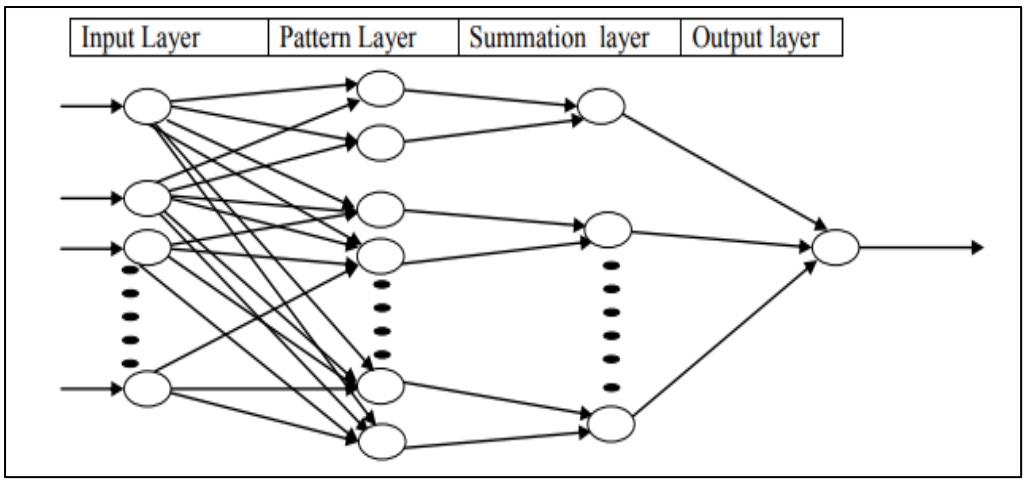

Figure 2. Single-layer feedforward networks, multi-layer feedforward networks, and recurrent networks can all be classified.

The number of neurons, their connections, and the processing that occurs throughout the network must all be specified in order to properly describe an

ANN. When training a neural network, the structure of the network's neurons has a direct impact on the learning algorithms used. Single-layer feedforward networks, multi-layer feedforward networks, and recurrent networks can all be classified [10].

Why Do Neural Networks Combine with Cryptography?

Some public-key cryptography methods need more advanced procedures and computational resources than others, making them more difficult to implement. To decrypt and encrypt the data, there are a variety of cryptography algorithms to choose from. Attacks such as brute force and man in the middle can recover the key, allowing the original message, or plaintext, to be deciphered [11]. Key recovery using the Biclique attack on AES128, which has a computational complexity of 2126.1, is possible for AES128. A Biclique attack on AES-192 and AES-256 requires 2189.7 and 2254.4 computational complexity, respectively. AES-192 and AES-256 are vulnerable to similar key attacks. Using cryptanalysis techniques such as related key attacks, the attacker can decipher a cipher's operation using several different keys, all of whose values are unknown to the attacker until the attacker discovers a mathematical link between them. It is also possible to compromise the RSA (193-digit) and RSA (129-digit). Because of the difficulty of the cryptographic algorithms and the conflicting demands of neural networks, a new technique based on neural networks has been developed (Gupta, 2019). This problem can be solved using Neural Cryptography. It is possible to secure networks with the use of neural networks and cryptography. Encryption and decryption are based on the neural network. Weights in the form of neural network weights are the key to solving this problem. Watermarking hybrid methods of digital images are classified. Watermarking of digital images is classified into spatial, transform, or hybrid processes based on their domain of working. Examples of spatial domain approaches include the least significant bit (LSB), the intermediate significant bit (ISB), and patchwork algorithms [12].

Different Neural Network-Based Approaches in Cryptography

Steganalysis

Cryptanalysis is the application of cryptanalysis to the study of steganography, and steganalysis is the study of steganographic messages. Steganalysis involves concealing communication. There are several ways to hide or avoid information in difficult drawings using Steganalysis. Digital steganography today focuses on hiding secret information among the superfluous bits of images that need to be transmitted. In order to prevent an attacker from entering the message or discovering that there is a secret message buried, steganography is used more frequently. Steganography has now been implemented using a neural network. Wavelet texture decomposition and discrete cosine transformation (DCT) were used to analyze the initial data. In order to determine whether an image has any hidden information, neural networks are employed. It is possible for neural networks to create alternative weight sequences if they have been impacted by an image concealment

technique [13]. There is a difference between linear and nonlinear classifiers because neural networks have a higher capacity to mimic nonlinear situations by learning from training inputs [14].

Pseudorandom Number Generator

The cryptosystem's security is boosted by randomness. Statistical methods can be used to determine the randomness of a bit sequence. Pseudo-random numbers are generated by utilizing neural networks with multiple layers of perception (MLP). Neural networks have significant generalization capabilities after being trained on a large number of well-known input vectors, but only if the input pattern is understood. Unpredictable results will be generated by an over-fitting process if a network is unable to forecast the input pattern when receiving unfamiliar input patterns. Additionally, MLP neural networks can be utilized to enhance current generation systems by taking the pseudo-random numbers generated by linear computational generators and feeding them into the neural networks as input. Random numbers can be generated using a pseudo-random number generator (PRNG) technique, which is a type of algorithm based on mathematical principles. The qualities of random numbers are approximated by PRNGs, which create a series of numbers. As a result, the numbers are deterministic and effective. As a substitute, they use algorithms to replicate the selection of a random value. To employ pseudo-random number generators, a user specifies a range (e.g., lowest to highest) from which the random number is drawn, and the number is displayed immediately [15].

Digital Watermarking

Unauthorized access to digital content (such as text, images, audio, and video) is prevented by the use of digital watermarking. Watermarking systems are categorized based on the needs of the user: Insertion of a domain watermark, detection, and extraction of watermarks Watermark's ability to withstand attacks and when the watermark can be seen. Watermarking approaches can benefit from neural network features. In order to create a "watermarked image," a random watermark is applied to the original image. Wavelet decomposition is used to identify significant coefficients. Trainers make use of this extra information. The watermark was successfully extracted using neural networks and neural networks. This data is used to create the image shown below. The algorithm's security is enhanced as the number of training patterns for a given network grows [16]. Classification of Digital Image Watermarking Hybrid Methods. Digital image watermarking can be classed as spatial, transform, or hybrid based on the working domain. The least significant bit (LSB), intermediate significant bit (ISB), and patchwork algorithm are examples of spatial domain approaches [17].

Managing, Generating, And Exchanging Keys

The two-tree parity mechanism is used as part of the key exchange protocol. This is a particular type of multi-layer feed-forward neural network in which each input neuron has K neuronal connections, each hidden neuron has N

neuronal connections, and each weight has L values [19]. In two neural networks, input is provided randomly, and they exchange information with each other. Mutual learning results in synchronization. Each machine has a synchronized weight vector. The secret key is constructed by using this principle. Sensitive data is encrypted and decrypted using the same secret key. Encryption and decryption can be performed with any algorithm, including AES [19].

Attacks

The following types of attacks can be launched on neural cryptography:

1. Attacker's neural network has the same structure as both parties' neural networks; therefore it's a simple assault. With random initial weights, the attacker uses the same inputs as two parties to train their neural network [20].
2. There are two parties involved in this attack, however, the attacker only has access to a single attacker machine's output, rather than both. The hidden unit of the neural network also employs local fields[21].
3. The chance of correctly predicting using more than two neural networks inside one network is called a "majority attack." Several networks are used to do this. In this case, the attacker has only one network to operate with. The attacker uses more networks as the synchronization process progresses [22].

CONCLUSION

In this paper, various neural network-based approaches to cryptography are described. It is possible to deal with extremely complex access schemes using visual cryptography and neural networks, which is a departure from standard methods. When compared to previous approaches, the neural network-based approach used in Steganalysis provides more accurate results. The weights of a neural network are used as a key when using neural networks to generate a password. The attacker has a difficult time synchronizing with the two parties since the key creation process is so quick. Data communication systems place a high priority on safeguarding transmitted data. Researchers have looked into the potential of ANN in cryptography using two different approaches. Data is encrypted using a sequential machine-based approach. The use of neural networks for digital signal encryption is also studied in this research. It is possible to get better outcomes by making changes to the code or by employing new training techniques. As a result, a new method of encrypting and decrypting data can be found in Artificial Neural Networks.

REFERENCES

Davinroy, M. (2018). Security analysis of deep neural networks operating in the presence of cache side-channel attacks. arxiv.org.

Ferreira, P. (2019). Cyberthreat detection from twitter using deep neural networks. ieeexplore.ieee.org.

Gupta, D. (2019). Hiding data in images using cryptography and deep neural network. arxiv.org.

He, T. L. (2019). Secure communication based on quantized synchronization of chaotic neural networks under an event-triggered strategy. ieeexplore.ieee.org.

Huang. (2018). Auto-gnn: Neural architecture search of graph neural networks. arxiv.org.

JBD Joshi. (2019). Cryptonn: Training neural networks over encrypted data. ieeexplore.ieee.org.

Kwon, H. (2019). Convolutional neural network-based cryptography ransomware detection for low-end embedded processors. mdpi.com.

Whitehouse. (2018). Formal security analysis of neural networks using symbolic intervals. usenix.org.

Y Feng. (2020). n approach to cryptography based on continuous-variable quantum neural network. nature.com.

Fadhel, M. A., & Omar, Z. B. (2021). Geometric piecewise cubic bézier interpolating polynomial with C2 continuity. Информатика и автоматизация, 20(1), 133-159.

I.F. Akyildiz, M. Pierobon, S. Balasubramaniam, Y. Koucheryavy, The internet of bio-nano things, IEEE Commun. Mag. 53 (2015) 32–40.

E. Kim, J. Li, M. Kang, D.L. Kelly, S. Chen, A. Napolitano, L. Panzella, X. Shi, K. Yan, S. Wu, et al., Redox is a global biodevice information processing modality, Proc. IEEE 107 (2019) 1402–1424.

S.M. Abd El-atty, R. Bidar, E.S.M. El-Rabaie, Molcom system with downlink/uplink biocyber interface for internet of bio-nanothings, Int. J. Commun. Syst. 33 (2020), e4171.

[14] L. Grebenstein, J. Kirchner, R.S. Peixoto, W. Zimmermann, F. Irnstorfer, W. Wicke,

A. Ahmadzadeh, V. Jamali, G. Fischer, R. Weigel, et al., Biological optical-tochemical signal conversion interface: a small-scale modulator for molecular communications, IEEE Trans.NanoBioscience 18 (2018) 31–42.

M. Kuscu, O.B. Akan, Modeling and analysis of sinw fet-based molecular communication receiver, IEEE Trans. Commun. 64 (2016) 3708–3721. D. Sadighbayan, M. Hasanzadeh, E. Ghafar-Zadeh, Biosensing based on field-effect transistors (fet): recent progress and challenges, Trac. Trends Anal. Chem. (2020)116067.

S. Park, J. Choi, M. Jeun, Y. Kim, S.S. Yuk, S.K. Kim, C.S. Song, S. Lee, K.H. Lee, Detection of avian influenza virus from cloacal swabs using a disposable well gate fet sensor, Adv. Healthc. Mater. 6 (2017) 1700371.

Y. Chen, R. Ren, H. Pu, X. Guo, J. Chang, G. Zhou, S. Mao, M. Kron, J. Chen, Fieldeffect transistor biosensor for rapid detection of ebola antigen, Sci. Rep. 7 (2017)1–8.

M. Salehirozveh, P. Dehghani, M. Zimmermann, V.A. Roy, H. Heidari, Graphene field effect transistor biosensors based on aptamer for amyloid-β detection, IEEE

Sensor. J. 20 (2020) 12488–12494.

V.A. Pham Ba, Y.M. Han, Y. Cho, T. Kim, B.Y. Lee, J.S. Kim, S. Hong, Modified floating electrode-based sensors for the quantitative monitoring of drug effects on cytokine levels related with

inflammatory bowel diseases, ACS Appl. Mater. Interfaces 10 (2018) 17100–17106.

V.A. Pham Ba, D.g. Cho, S. Hong, Nafion-radical hybrid films on carbon nanotube transistors for monitoring antipsychotic drug effects on stimulated dopamine release, ACS Appl. Mater. Interfaces 11 (2019) 9716–9723.

Kamel, A. A. K., Hussein, A. T. A., Shekban, A. H., Badr, N. R., Mezan, S. O., & Jabir, W. Q. (2021). Improvement of a New Analysis Technique of phenomenon of bulling and Cyberbullying among Students at different stages. Psychology and Education Journal, 58(4), 2729-2740.

S. Zafar, M. Nazir, T. Bakhshi, H.A. Khattak, S. Khan, M. Bilal, K.K.R. Choo, K. S. Kwak, A. Sabah, A systematic review of bio-cyber interface technologies and security issues for internet of bio-nano things, IEEE Access 9 (2021) 93529–93566, https://doi.org/10.1109/ACCESS.2021.3093442.