IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 1, January 2024

DOI: 10.17148/IJARCCE.2024.13120

Neural Network based Message Concealment Scheme

Asst. Prof. Jyotsna Nanajkar[1], Sakshi Shinde[2], Piyush Mishra[3], Sanjeev Pandey[4], Ankit Tiwari[5]

Asst. Professor, Department of Information Technology, Zeal College of Engineering and Research, Pune, Maharashtra, India[1]

B.E. Student, Department of Information Technology, Zeal College of Engineering and Research, Pune, Maharashtra, India[2-5]

Abstract: Neural Cryptography represents an innovative intersection of cryptography and neural networks, particularly in the realms of cryptanalysis and encryption. This paper aims to showcase the capacity of Neural Networks to perform symmetric encryption even in adversarial scenarios, drawing inspiration from previous works in this domain. The fundamental goal of cryptography is to create a cypher that is resistant to deciphering without the corresponding key, thus safeguarding the plaintext. Messages are encrypted using robust cryptography, rendering brute-force attacks against the algorithm or key nearly insurmountable. Robust cryptography achieves this by utilizing exceptionally lengthy encryption keys and encryption algorithms resistant to various forms of attacks. The integration of neural networks marks the next evolutionary phase in the evolution of secure encryption. This paper delves into the practical application of neural networks in cryptography, exploring the development of neural networks tailored for cryptographic purposes.

Keywords: Cryptography key, encryption system, encryption algorithm, artificial neural network, chaos maps, logistic encryption.

I. INTRODUCTION

Cryptographic technology plays a crucial role in ensuring the security and integrity of data in software information systems [1]. However, the increasing use of cryptographic algorithms by malware, including computer viruses and Trojans, poses significant challenges to information security. These malicious entities can conceal their behaviours, making it difficult for antivirus engines to detect their presence. Additionally, they obscure static characteristics, such as malicious code and sensitive data, hindering reverse analysis by security researchers.

Detecting cryptographic functions in malware and identifying their types is essential for understanding malware working principles and extracting program features for in-depth analysis. This process holds vital significance for software security analysis and the overall protection of computer systems. Identifying specific cryptographic functions in binary programs, especially in malware, is a complex and labour-intensive task [2].

Analysts typically resort to reverse engineering methods like disassembly, decomplication, and dynamic debugging to analyse assembly code and uncover key information about cryptographic algorithms in programs.

Over the years, various approaches have been proposed to address this challenge, mainly falling into two categories: static and dynamic. Static approaches involve scanning the target binary or its assembly code to identify and match signatures associated with cryptographic algorithms, such as constant features or instruction features [3].

While static approaches are efficient and easy to implement, dynamic approaches leverage dynamic analysis methods to identify cryptographic functions during the running process. Although dynamic approaches offer higher accuracy, their efficiency is hampered by the need to process substantial information.

Presently, static approaches are more widely used due to their efficiency. [4] However, traditional static approaches often rely on shallow feature matching and may fail to recognize malicious code that intentionally conceals cryptographic function features.

II. MOTIVATION, AIM AND OBJECTIVE

The motivation behind the discussed text is to convey the significance of cryptography, particularly in safeguarding information against unauthorized access. [4] The text aims to highlight the fundamental principles of cryptography, emphasizing the importance of secure communication through encryption and the challenges addressed by cryptanalysis. Additionally, it delves into the intriguing intersection of cryptography and artificial neural networks, showcasing the potential advancements in secure communication.

The aim of the text is to provide a comprehensive overview of cryptography, covering its core principles, objectives, and the role it plays in securing data. It seeks to elucidate the cryptographic techniques employed, including symmetric and asymmetric encryption, and to underscore the necessity of robust keys and algorithms [1] [2]. Furthermore, the aim is to introduce the intriguing realm of artificial neural networks and their potential application in encryption and decryption processes.

1. **Explain Cryptographic Principles:** Clearly articulate the foundational principles of cryptography, including the use of cypher keys, encryption, and cryptanalysis.
2. **Emphasize Importance of Keys:** Highlight the essential characteristics that cypher keys must possess for effective encryption and decryption, ensuring the security of data.
3. **Explore Cryptanalysis:** Illuminate the purpose and methods of cryptanalysis, demonstrating its role in deciphering coded messages without the corresponding decryption key.
4. **Introduce Encryption Techniques:** Introduce symmetric and asymmetric encryption techniques, elucidating their mechanisms and applications in secure communication.
5. **Discuss Neural Networks:** Introduce artificial neural networks, exploring their structure, functionalities, and the potential role they can play in encryption and decryption processes.
6. **Showcase Advancements:** Showcase recent advancements, specifically the application of neural networks in cryptography through end-to-end adversarial training, highlighting its potential impact on secure communication.

III. RELATED WORKS

The research proposal aims to create artificial neural networks named Alice, Bob, and Eve for simulating a symmetrically encrypted conversation. Alice and Bob engage in encrypted communication, while Eve eavesdrops on the chat. Both Eve and the intended recipient have access to the ciphertext, but only the recipient possesses the corresponding n-bit key. Eve attempts to decipher the ciphertext without the key.

A. Dataset

The dataset comprises two randomly generated strings of equal length, with one serving as the plaintext and the other as the associated key. The strings are created using a uniform random distribution [6]. Both keys and texts are N bits long, with possible lengths of 16, 32, and 64 bits, randomly selected from these values.

B. Artificial Neural Networks

Artificial neural networks (ANNs) consist of interconnected processing units that communicate via weighted connections [7]. Key characteristics include:

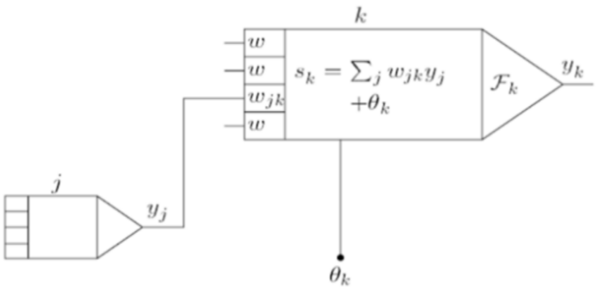

Fig. 1 Neural Network

DOI: 10.17148/IJARCCE.2024.13120

- Activation state (yk) of each unit, representing its output.
- Weights (wjk) specifying the relationships between units.
- External input propagation rule determining the effective input (sk) of the unit.
- Activation function (Fk) calculating the new activation level based on valid input and current activation.
- The external input of each unit, sometimes referred to as bias or offset, is denoted as θk.

The proposed model involves three neural networks: transmitter, receiver and adversary, structured with four layers resembling convolutional neural networks [8].

C. Convolutional Neural Networks

A Convolutional Neural Network (ConvNet/CNN) is a Deep Learning system designed for image processing, capable of assigning relevance to various aspects/objects in an image and distinguishing between them [5]. Unlike other classification methods, ConvNets require less pre-processing, as they can learn filters and characteristics with sufficient training [8]. While the research doesn't delve into CNN encryption's resilience against cryptographic attacks, it focuses on evaluating how well a specific neural network can be applied to symmetric cryptography [6].

For the demonstration in this context, three neural networks are considered:

Alice:
Responsible for generating the dataset, Alice employs a uniform random generator to create two strings of equal length: plaintext/message and its associated key (both n-bit).
These strings are passed to a fully connected layer, which converts them into a 2n-bit vector.
The output of the fully connected layer undergoes sigmoid convolutional layers and is then passed through a non-linear tanh layer, scaling it to n-bits within the range of -1 to 1.

Bob:
As the receiver, Bob's architecture mirrors Alice's, comprising a fully connected layer, three sigmoid convolutional layers, and a non-linear tanh layer.
Bob's input is the n-bit ciphertext generated by Alice and the key used for symmetric encryption.
The layers in Bob perform similar operations to Alice, producing deciphered text identical to the one input to Alice.

Eve:
Serving as the adversary in a man-in-the-middle attack scenario, Eve aims to crack the ciphertext without the secret key known only to Alice and Bob.
Eve's architecture is identical to Alice and Bob but takes only the ciphertext (along with an identity string) as input.
The primary purpose of Eve is to assess the viability of using ANNs for symmetric encryption, testing their strength and reliability [6].

D. Proposed Neural Network Architecture

1.Fully Connected Layer:
FCNNs represent a type of artificial neural network where all nodes (neurons) in one layer are connected to neurons in the subsequent layer.
While effective for certain data types, FCNNs have limitations in image identification and classification, demanding significant processing power and being susceptible to overfitting.
The complexity increases with the depth of the network (multiple layers), making it challenging for human comprehension.

2.Sigmoid Layer:
The sigmoid function, denoted as σ(x) or sig(x), is a logistic function defined as $\sigma(x) = 1/(1+\exp(-x))$.
Commonly used as an activation function in neural networks, the sigmoid function processes a weighted sum of inputs, producing an output between 0 and 1.
Neurons with sigmoid activation functions ensure outputs within this range, introducing nonlinearity to the weighted sum of inputs.

3.Tanh Layer:
The Tanh (hyperbolic tangent) function serves as another activation function.
Similar to the sigmoid function in appearance, Tanh returns values between -1 and 1.

DOI: 10.17148/IJARCCE.2024.13120

The calculation of the Tanh function is given by (e^x - e^(-x)) / (e^x + e^(-x)).
It maps larger inputs closer to 1.0 and smaller inputs closer to -1.0.

The proposed architecture incorporates these layers into the neural networks for Alice, Bob, and Eve. [8] The combination of fully connected, sigmoid, and tanh layers allows for complex transformations and nonlinearities, essential for the tasks of encryption, decryption, and adversarial decryption attempts in symmetric cryptography.

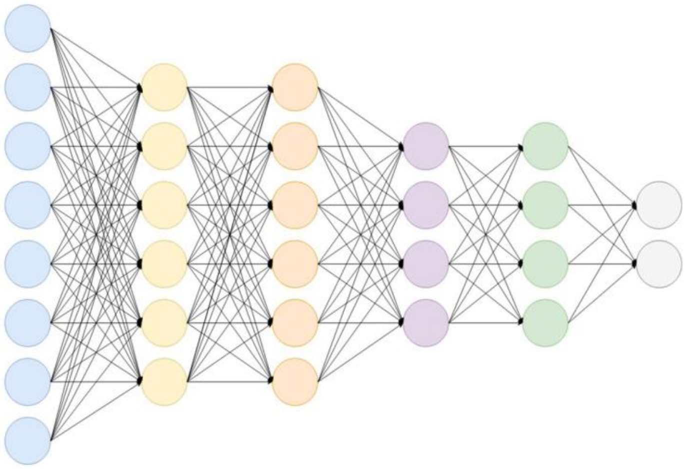

Fig. 2 Fully Connected Layer

IV. SYSTEM DESIGN

A. System Architecture

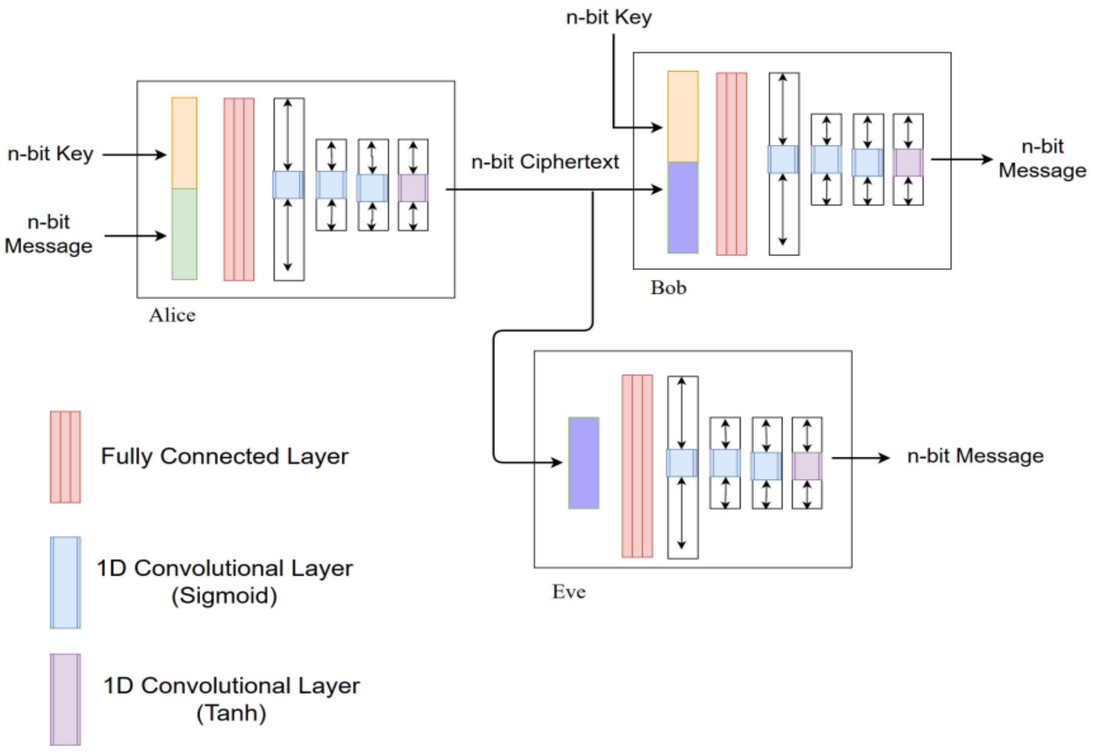

Fig. 3 System Architecture

DOI: 10.17148/IJARCCE.2024.13120

V. EXPECTED OUTCOME

Demonstration of Symmetric Encryption: Showcase the practical application of Neural Networks in achieving symmetric encryption, emphasizing their role in securing communication [6].

Enhanced Security: Illustrate how the integration of neural networks contributes to enhanced security by making brute-force attacks against the algorithm or key nearly insurmountable.

Innovation in Cryptography: Contribute to the advancement of cryptography by exploring innovative approaches, leveraging the capabilities of neural networks for robust encryption.

Insights into Adversarial Scenarios: Provide insights into the performance of Neural Networks in adversarial scenarios, particularly in the face of attempts to decipher encrypted messages without the corresponding key [8].

Application-Specific Networks: Explore the development of neural networks tailored specifically for cryptographic purposes, highlighting their adaptability and effectiveness in securing sensitive information.

Contribution to Research Domain: Contribute valuable insights to the broader research domain at the intersection of cryptography and neural networks, building upon previous works and paving the way for future advancements.

VI. LIMITATIONS

1. While machine learning demands extensive time for model training, the classic Diffie-Hillman technique offers time efficiency.

2. This system exhibits modest, yet potentially impactful limitations. It operates as a private key system where the network's weight and design serve as the key. Disruption of weights and architecture allows for encryption, but both mass and structure are necessary for both encryption and decryption. Possessing only one is insufficient for breaking the system.

3. The notable advantage of this system lies in its perceived robustness, challenging to circumvent without an understanding of its underlying approach.

4. Its implementation based on machine learning renders it noise-tolerant. Unlike standard encryption systems that resist any alteration in a single bit of the majority of transmissions, a neural network-based method allows variations in the encoded message while maintaining accuracy.

VII. CONCLUSION

In conclusion, cryptography stands as a pivotal element in safeguarding data and upholding privacy within the contemporary digital landscape. Various encryption techniques, encompassing both symmetric and asymmetric encryption, facilitate secure transmission of data and prevent unauthorized access.

It is imperative to counteract the progress of cryptanalysis, the discipline that seeks to decrypt messages without possessing the decryption key, to foster ongoing development and enhancement of cryptographic methods.

Moreover, the integration of artificial neural networks into encryption techniques underscores the potential for innovative and adaptable security solutions. Continued research in cryptography and cryptanalysis is essential to keep pace with technological advancements and the escalating demand for secure communication. This commitment ensures the provision of reliable and effective protection for sensitive data in an ever-evolving digital landscape.

REFERENCES

[1]. Grossi, Enzo & Buscema, Massimo. (2008). Introduction to artificial neural networks. European journal of gastroenterology & hepatology. 19. 1046-54. 10.1097/MEG.0b013e3282f198a0.
[2]. Zupan, Jure. (1994). Introduction to Artificial Neural Network (ANN) Methods: What They Are and How to Use Them. Acta Chimica Slovenica. 41.

DOI: 10.17148/IJARCCE.2024.13120

[3]. T. Dong and T. Huang, "Neural Cryptography Based on Complex-Valued Neural Network," in IEEE Transactions on Neural Networks and Learning Systems, vol. 31, no. 11, pp. 4999-5004, Nov. 2020, doi: 10.1109/TNNLS.2019.2955165.

[4]. Chandra, Sourabh & Bhattacharyya, Siddhartha & Paira, Smita & Alam, Sk. (2014). A Study and Analysis on Symmetric Cryptography. 10.1109/ICSEMR.2014.7043664. K. Elissa.

[5]. O'Shea, Keiron & Nash, Ryan. (2015). An Introduction to Convolutional Neural Networks. ArXiv e-print0s.

[6]. Volna, Eva & Kotyrba, Martin & Kocian, Vaclav & Janosek, Michal. (2012). Cryptography Based On Neural Network. 10.7148/2012-0386-0391.

[7]. Sooksatra, Korn & Rivas, Pablo. (2020). A Review of Machine Learning and Cryptography Applications. 591-597. 10.1109/CSCI51800.2020.00105.

[8]. Kalsi, Shruti & Kaur, Harleen & Chang, Victor. (2017). DNA Cryptography and Deep Learning using Genetic Algorithm with NW algorithm for Key Generation. Journal of Medical Systems. 42. 17. 10.1007/s10916-017-0851-z.