Proceedings of the 5th International Conference on Computing and Data Science
DOI: 10.54254/2755-2721/14/20230798

A research on applications of neural network-based cryptography

Yuheng Liang

School of Intelligent Manufacturing, Zhanjiang University of Science and Technology, Zhanjiang, 524003, China

1811000127@mail.sit.edu.cn

Abstract. With the rapid development of neural networks, they have been integrated into more and more fields, and cryptography is no exception. Research on the combination of neural networks and cryptography is developing rapidly, and numerous scholars have made significant progress in these fields. Neural network-based cryptography is a complex system that deserves an in-depth study. This paper will first introduce the foundation types of neural networks, some of the other types of neural network , and cryptographic techniques. Immediately after, this paper will introduce the scheme of Generative Adversarial Neural Networks (GANs) generating cryptography and the scheme of combining GANs and Convolutional Neural Networks (CNNs) generating cryptography and analyze their differences and advantage and disadvantages. This paper will then introduce the application of neural networks in blockchain, key exchange technology, and the combination of neural networks and Advanced Encryption Standard (AES). As well as at the end of this paper will show some views of combining neural networks and cryptography in the future.

Keywords: cryptography, application, neural networks.

1. Introduction

As more and more applications based on neural networks emerge, neural networks have become an increasingly hot topic of discussion. It is made up of linked nodes or neurons that work together to categorize and group data, uncover correlations and patterns in it, and become better over time. Neural network is a subset of machine learning. And the foundation of deep learning is neural network. Neural networks are used in various applications such as image recognition, cryptography, natural langue processing, and speech recognition.

Cryptography is the study and practice of techniques for secure communication in the midst of malevolent activity. Cryptography combines rule-based procedures and secure information and communication techniques created from mathematics. Messages are also transformed using ideas into an unintelligible format that can only be decrypted by individuals with the proper authorization and the unlocking key. In the presence of malevolent outsiders or adversaries, cryptography enables safe communication. Whereas decryption reverses the process to recover the original plaintext, encryption employs an algorithm and a key to convert plaintext into ciphertext.

Nowadays the applications of cryptography and neural networks combined with neural networks are increasing with the development of neural networks, but there are few surveys based on cryptography

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/14/20230798

and neural networks. This paper provides an in-depth survey of neural network-based cryptography, it introduces, discusses, and analyses the application of neural based cryptography. And give some views of future direction in the last. This paper divides neural networks into foundation types and other types. Foundation types it has Single layer feed forward neural networks (SLFNNs), Multilayer feed forward neural networks (MLFNNs), recurrent neural networks (RNNs), and other types it as Convolutional Neural Networks (CNNs), Generative Adversarial Neural Networks (GANs) which will appear in literature reviews. And this paper also introduces some cryptography technologies such as Chosen-plaintext Attacks (CPA), One Time Pad (OTP), and Advanced Encryption Standard (AES).

The following sections make up the remaining portions of this essay. In section 2, this paper introduced several types of neural and several cryptography technologies. In section 3, this paper discusses and analyzes the application based neural network cryptography. And, in section 4, this paper provides a summary of the survey results as well as potential directions for further study.

2. Preliminary

2.1. Neural models

The neural network is build-up from 3 types of layers, hidden layer, input layer, and output layer. Between the input and output layers lies a layer called the hidden layer. It gives the weights of the input and, as the output, directs them using an activation function. The input layer, which is the initial layer of the neural network. The data is received in the input layer and sent to be processed in the second layer. The neural network's output layer is the last layer. Before deriving the final output, it applies its own set of weights and biases. The type of problem being handled determines how many nodes are present in the output layer [1]. The foundation types of network architectures are shown in Table 1.

Table 1. The foundation types of network architectures.

Types	Contents	Advantages	Disadvantages
SLFNNs	input and output nodes are both on a single layer, and no hidden layers.	1. relatively simple 2. computationally efficient.	may not be able to capture complex nonlinear relationships in the data [1].
MLFNNs	multiple layers of interconnected nodes (neurons) arranged in a feedforward fashion [1].	1. handle complicated tasks. 2. have high performance. 3. widely used in various fields.	1. being computationally expensive 2. requiring a large amount of data for training. 3. having difficulty with overfitting.
RNNs	process sequential or time series data.	1. model time-dependent 2. sequential data problems 3. can model sequence data.	Training is very difficult.

2.1.1. Single layer feed forward networks (SLFNNs). The nodes accept data for the input layer, and the data is transmitted over the network to the output layer, where it is used to create the final output. Depicted in Figure 1. The SLFNNs architecture is often used in classification problems where the goal is to assign an input to one of several possible categories. The node with the highest output value is chosen as the classification result from the output layer, which contains nodes representing each potential category [1].

DOI: 10.54254/2755-2721/14/20230798

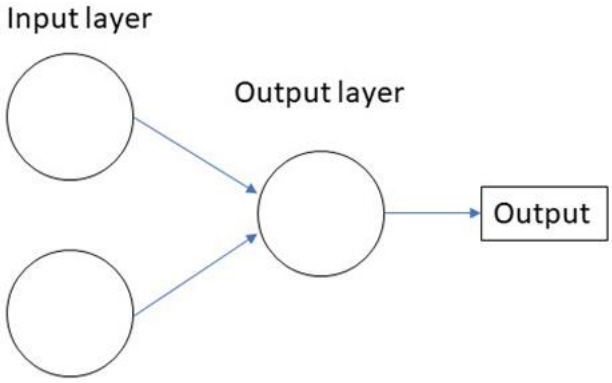


Figure 1. SLFNNs.

2.1.2. Multilayer feed forward neural networks (MLFFNNs). The nodes accept data for the input layer. The output of each node in one layer serves as an input to the nodes in the next layer, as shown in Figure 2 until the output layer generates the final output. The weights of the connections between neurons are adjusted during the training of MLFFNNs using supervised learning algorithms like back-propagation to reduce the discrepancy between the desired and actual output [1].

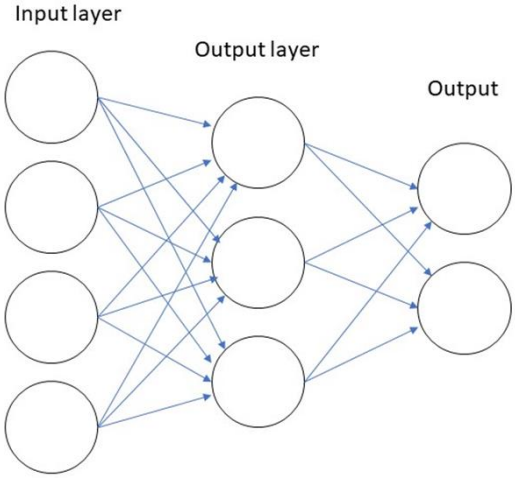


Figure 2. MLFFNNs.

2.1.3. Recurrent neural networks (RNNs). As depicted in Figure 3, Unlike feedforward neural networks, RNNs have connections between nodes that create a cycle, allowing output from some nodes to be used as input for others in the next step of the sequence. This makes them useful for modelling and predicting patterns in sequential data such as speech recognition and natural language processing [1].

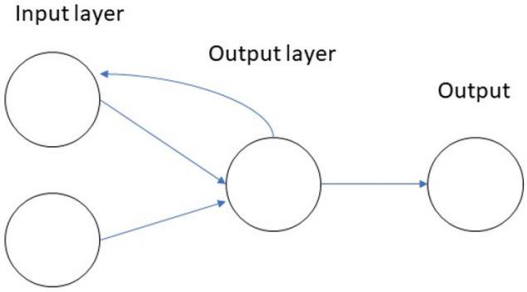


Figure 3. RNNs.

DOI: 10.54254/2755-2721/14/20230798

2.2. Others neural network types

2.2.1. Convolutional Neural Networks (CNNs). Convolutional neural networks are a kind of Deep Learning algorithm that is frequently utilized in the processing of visual information. It is composed of several layers, including a convolutional layer, which is the fundamental component of a CNNs and the location of most of the computation. CNNs can assign importance to various features in an image using learnable weights and biases, making them particularly helpful for image identification and classification problems. Convolution neural networks are a subclass of feedforward neural networks. Convolutional architecture is a technique used by CNNs to extract characteristics from data. CNNs does not require manually extracting features, in contrast to data using conventional feature extraction techniques [2] [3].

2.2.2. Generative adversarial neural networks (GANs). The use of generative adversarial networks is growing for both semi-supervised and unsupervised learning. They accomplish this by modelling high dimensions implicitly [4]. It was proposed in 2014[5], which uses two neural networks competing using deep learning methods. One network creates fresh data samples, and the other network determines if the generated samples are authentic or fraudulent. The two networks continue to learn from each other until the generator network can produce realistic samples that can fool the discriminator network. GANs have been used for various applications, for example, image, video, and music generation.

2.3. Crypto techniques

2.3.1. Chosen-plaintext attacks （CPA). The capacity of an adversary to exert (partial) influence over what the truthful parties encrypt is captured by chosen-plaintext attacks. The attacker can select any plaintext data to be encrypted during this attack, and they will subsequently obtain the associated ciphertext. The attacker can choose plain texts and view their corresponding encryptions. In other words, the attacker is given the corresponding ciphertext after selecting some plaintext. An attacker using a chosen-plaintext attack can obtain a plaintext message of their choice that has been encrypted using the key to the target and has access to the decrypted text.

2.3.2. One time pad (OTP). One-time pad encryption encrypts data using a pre-shared key that can only be used once, and the intended receiver must also have the key to decrypt the data. The key must be at least if the message is being encrypted and is produced randomly. OTP is regarded as an impenetrable cipher; however, it has requirements that must be met.

2.3.3. Advanced encryption standard (AES). The substitution-permutation network is the foundation for AES, which is effective in both hardware and software. As a symmetric-key technique, AES uses same key for both encryption and decryption. There are three key lengths supported in AES encryption, which are 128,192,256-bit lengths. And standard data size of 128 bites the variable number of encryptions rounds of each block to be ciphered [6].

3. Literature review

Neural networks are not very good at cryptography, so most of the research on neural networks has been on key sharing. Abadi M et al [7] proposed that neural networks can learn to protect their information from other neural networks without learning specific algorithms using GANs. After their study, many researchers improved on them and found that neural networks can learn more secure encryption schemes. This section displays a ciphertext produced using the neural network model Abadi M et al [7] proposed. The security of the Abadi M et al [7] model is then examined using a security study by Coutinho M et al [8], and the model's improvements as determined by Coutinho M et al [8] and Li Z et al [9] are then shown. In 3.2, this paper shows some applications of the combination of cryptography and neural networks.

DOI: 10.54254/2755-2721/14/20230798

3.1. Crypto techniques

The first search initiative on using adversarial neural cryptography (ANC) to learn how to protect communications was made by Abadi M et al [7]. It tries to develop neural networks that can pick up on how to encryption algorithm. Based on generative adversarial networks, this technology.

As depicted in Figure 4, the sender and receiver share the same secret key. The original text is input into the sender. After the sender processes this input, it outputs a text which is encrypted. The receiver and attacker all will receive C, and they all will process it, and attempt to recover the original text. The goal for the attacker is to recover the original text, and the goal for the sender and receiver is to communicate clearly and hide the communication from the attacker.

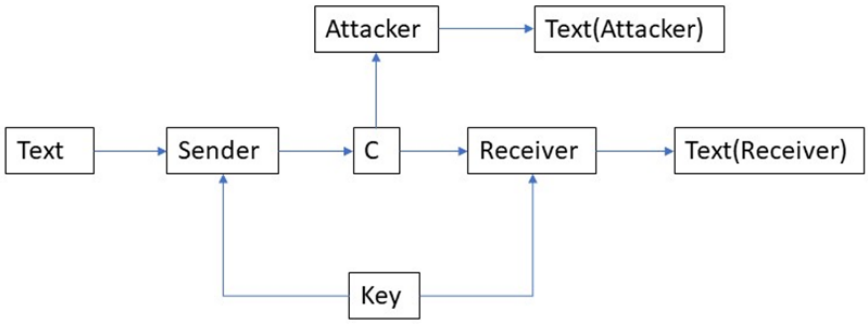


Figure 4. Sender, receiver, attacker, with a symmetric cryptosystem.

In the neural network design, Abadi M et al [7] choose to engineer a neural architecture that can learn to safely communicate. They chose the following "mix&transform" architecture. It has a first fully connected layer and a sequence of convolution layers. In the training process, the accuracy of the receiver will be trained until the text decrypts as the original text, and for the attacker, it will be trained by about 50%.

According to research by Abadi M et al [7], neural networks may learn different encryption and decryption techniques as well as apply them selectively to achieve secrecy goals. However, through experiments by Coutinho M et al [8], they found that the encryption in ANC is not secure, because serval plaintext bits were encrypted with the same key, and some of the cryptosystems are Vigenère, which means it can be broken. But the crypto net thinks it was successful because the attacker and receiver can success communication.

And Coutinho M et al [8] improve the model based on ANC, which is called CPA-ANC Coutinho M et al [8]. In CPA-ANC, Coutinho M et al [8] adding Chosen-Plaintext-Attack (CPA) to ANC. As depicted in Figure 5, compared to the general ANC system, the attacker in the CPA-ANC system does not try to crack the cipher text, the attacker selects two messages for the sender to choose one at random and send it with NN encryption, and the attacker goes to the attacker determines that the cipher-text belongs to the original encrypted message.

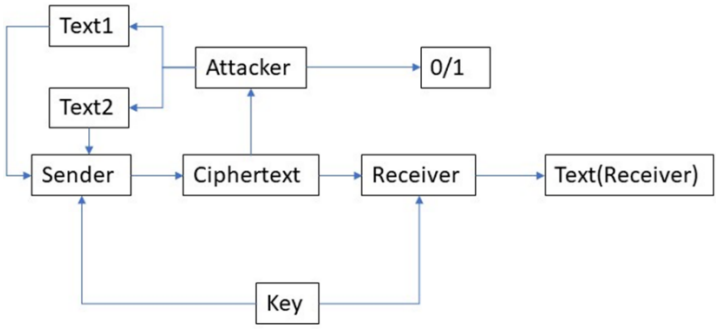


Figure 5. Sender, Receiver, Attacker, and the CPA-ANC setup.

DOI: 10.54254/2755-2721/14/20230798

In the experiments [8], they found the CPA-ANC which they proposed, can learn OTP with high probability. However, in this system only having CPA-ANC is not enough to make sure secure, in other words, it needs a stronger attacker to train the system. Li Z et al [9] proposed a new system that has a stronger adversary than CPA-ANC that can break the crypto-system and it was called Adversary Network Encryption System (ANES).

As depicted in Figure 6, ANES is compared to the usual adversarial network in that it is not one-to-one, but one-to-three. In which, the sender, receiver, and attacker are constructed by the CNNs model. During the transmission, the sender encrypts two segments of the original text P and text K into C to send to the common channel, and the receiver receives C and tries to decrypt them. And three attackers listen to the public channel.

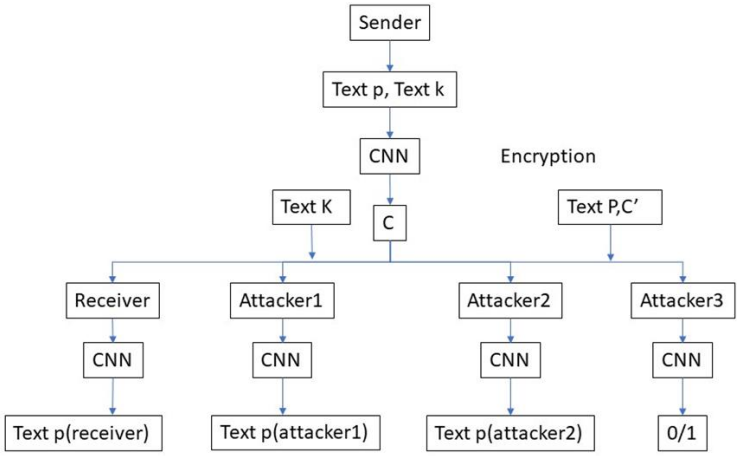


Figure 6. Architecture for ANES.

The three attackers differ in that the first attacker has access to the ciphertext C and the original K and tries to output another original P. The second attacker has access to the encrypted message and tries to brute-force break it. The third attacker simulates a chosen cipher-text attack, where it receives the original P, the encrypted cipher-text C, and a random cipher-text C', and it uses machine learning to decide which cipher-text is randomly generated and which is the real cipher-text corresponding to P. The attacker is also learning how to decrypt while the sender and recipient are practicing encryption and decryption.

Through constant practice, the ANES system has a very high possibility of mastering the OTP [9]. Also, in the experiments, Li Z et al [9] compare the probability of ANES mastering the OTP in different numbers and intensities of the attacker. The experiment data [9] shows that the stronger attacker they have, the higher probability ANES can master the OTP. In other words, a powerful attacker can get a more secure system. In this point, Li Z et al [9] and Coutinho M et al [8] have a very similar conclusion.

3.2. Some applications of the combination of cryptography and neural networks

To address issues with the blockchain's low security, difficult recovering a lost key, and poor communication efficiency, Zhang W et al [10] introduce a key secret-sharing technique based on the GANs. The main concept behind this technique is to treat the plaintext during the secret-sharing procedure like an image. They divide the original image into several original sub-images, and then they DNA code each original sub-image. Afterward, train the suggested network to produce the result for secret sharing. This technique resolves the issue of recovering secret key lost in blockchain transactions.

Jin J et al [11] present a 3D-CUBE algorithm to generate the same secret key. The sender and receiver use ANN to shuffle and solve the 3D-CUBE to get the same secret key. This algorithm solves the problem of breaking asymmetric encryption algorithms that have emerged because of the advent of quantum computers.

DOI: 10.54254/2755-2721/14/20230798

Lytvyn V et al. [12] developed a unique cryptosystem based on the synthesis of a neural network with the AES algorithm. This system, based on the diagonalized matrix of synaptic weight coefficients based on vectors of input photographs, can generate a new asymmetric key for each input image. The cryptographic stability of the algorithm is increased by this system.

4. Conclusion

This paper introduces the current research on the neural network in the cryptography field, and observed Abadi M et al [8], Coutinho M et al [9], and Li Z et al [10]. that GANs can learn encryption methods to protect communication by themselves, and through the process and experiments can know that the stronger GANs it makes, the more secure system it has. This effects of Zheng W et al [11], Jin J et al [12], and Lytvyn V et al [13] are also presented in this study. These researchers combined cryptography and used them to blockchains, and key exchange, and to increase the stability of cryptography.

A lot of interest has been paid to neural network-based cryptography in the hope that it would one day offer a more effective encryption technique. However, there are still few studies and research in this field. Currently, more research in this area is on the use of neural networks for key sharing, and it is believed that newer neural network-based models for key sharing will emerge in the future.

In addition, another research is that of secure communication systems generated with GANs, and more and more researchers will propose more powerful models of GANs to obtain more powerful encryption schemes, and perhaps other more secure encryption schemes will be generated in the future without human intervention.

References

[1] Sharkawy A N 2020 Principle of neural network and its main types vol 7 pp 8-19
[2] Albawi S, Mohammed T A, Al-Zawi S 2017 *International Conference on Engineering and Technology* Understanding of a convolutional neural network pp 1-6
[3] Li Z, Liu F, Yang W, Peng W, Zhou J 2021 A survey of convolutional neural networks: analysis, applications, and prospects vol 33 pp 6999-7019
[4] Creswell, A., White, T., Dumoulin, V., Arulkumaran, K., Sengupta, B., and Bharath, A. A 2018 Generative adversarial networks: An overview vol 35 pp 53-65
[5] Goodfellow I, Pouget-Abadie J, Mirza M, Xu B 2014 Generative adversarial nets in advances in neural information processing systems pp 2672-2680
[6] Hamza A, Kumar B 2020 *9th International Conference System Modeling and Advancement in Research Trends* A review paper on DES, AES, RSA encryption standards pp 333-338
[7] Abadi M, Andersen D G 2016 Learning to protect communications with adversarial neural cryptography pp 1-15
[8] Coutinho M, de Oliveira Albuquerque R, Borges F, Garcia Villalba L. J., and Kim T. H. 2018 Learning perfectly secure cryptography to protect communications with adversarial neural cryptography vol 18 p 1306
[9] Li Z, Yang X, Shen K, Zhu R, Jiang J 2020 Information encryption communication system based on the adversarial networks Foundation. Neurocomputing vol 415 pp.347-357
[10] Zheng W, Wang K, Wang F Y 2020 Gan-based key secret-sharing scheme in blockchain vol 51 pp 393-404
[11] Jin J, Kim K 2020 3D CUBE algorithm for the key generation method: applying deep neural network learning-based vol 9 pp 33689-33702
[12] Lytvyn V, Peleshchak I, Peleshchak R, and Vysotska V 2019 Information encryption based on the synthesis of a neural network and AES algorithm pp 447-460