JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Wavelet-Based Chaotic Neural Network for Secure Cryptography: A Study on the Effects of Wavelet Function and Chaotic Map Selection

[1]Aviral Srivastava
[1]Student
[1]Amity school of engineering and technology
[1]Amity University Rajasthan, Jaipur, India

Abstract : In recent years, there has been a growing interest in using chaotic neural networks for secure cryptography. One of the recent developments in this field is the use of wavelet-based chaotic neural networks, which add an additional layer of complexity to the system. In this paper, we present a study on the use of wavelet-based chaotic neural networks for secure cryptography, with a focus on the effects of wavelet function and chaotic map selection. We demonstrate that careful selection of these parameters can significantly enhance the security of the system. Our results show that the proposed system provides a high level of security and can be a promising approach for secure data encryption.

Keywords **– Cryptography, Wavelet-Based Chaotic Neural Network, secure communication**

I. INTRODUCTION

The rapid development of the internet and other communication technologies has led to a growing need for secure data encryption. One of the promising approaches for secure cryptography is the use of chaotic neural networks. Chaotic neural networks exhibit complex and unpredictable behaviour, which can be used to produce secure cryptographic keys. One of the recent developments in this field is the use of wavelet-based chaotic neural networks, which have shown promising results in providing high levels of security.
In this paper, we present a study on the use of wavelet-based chaotic neural networks for secure cryptography. We focus on the effects of wavelet function and chaotic map selection on the security of the system. We begin by introducing the concept of chaotic neural networks and their applications in secure cryptography. We then describe the wavelet-based chaotic neural network and its components, including the wavelet transform, neural network architecture, and chaotic map.
Next, we present the results of our study, which demonstrate the effects of wavelet function and chaotic map selection on the security of the system. We show that careful selection of these parameters can significantly enhance the security of the system. Finally, we conclude with a discussion of the implications of our study and the potential applications of wavelet-based chaotic neural networks in secure data encryption.
In the first section of our paper, we provide a brief introduction to chaotic neural networks and their applications in cryptography. We discuss the advantages of chaotic systems in providing secure encryption, including the unpredictability of the system's behaviour and the potential for producing high-quality cryptographic keys.
In the second section, we introduce the wavelet-based chaotic neural network and its components. We describe the wavelet transform, which converts the input data into a set of wavelet coefficients, and the neural network architecture, which uses these coefficients as inputs to produce encrypted output data. We also discuss the selection of the chaotic map, which determines the behaviour of the system and influences the security of the encryption.
In the third section, we present the results of our study, which investigated the effects of different wavelet functions and chaotic maps on the security of the system. We evaluated the performance of the system using standard metrics for secure encryption, including key space, correlation, and entropy. Our results demonstrate that careful selection of the wavelet function and chaotic map can significantly improve the security of the system.
Finally, in the conclusion section, we summarize the main findings of our study and discuss the potential applications of wavelet-based chaotic neural networks in secure data encryption. We suggest that the wavelet-based chaotic neural network can be a promising approach for secure data encryption and can be used in a variety of applications, including secure communication, data storage, and financial transactions.

II. WAVELET-BASED CHAOTIC NEURAL NETWORK

The wavelet-based chaotic neural network consists of a wavelet transform, which converts the input data into a set of wavelet coefficients, and a neural network architecture, which uses these coefficients as inputs to produce encrypted output data. The chaotic map determines the behavior of the system and influences the security of the encryption.
The wavelet-based chaotic neural network is a type of neural network architecture that uses wavelet transforms and chaotic maps to provide secure encryption for data. Here's an elaboration of its key components:

1. Wavelet Transform: The wavelet transform is a mathematical tool that can be used to decompose signals into a series of wavelets at different scales. In the context of the wavelet-based chaotic neural network, it is used to decompose the input data into a set of wavelet coefficients. These coefficients are then used as inputs to the neural network, which performs the encryption.
2. Neural Network Architecture: The neural network architecture of the wavelet-based chaotic neural network consists of several layers of neurons. These layers can be organized into an encoder and a decoder. The encoder takes the wavelet coefficients as input and performs a series of nonlinear transformations to produce an encrypted output. The decoder takes the encrypted output as input and performs a series of inverse transformations to reconstruct the original input data.
3. Chaotic Map Selection: The chaotic map selection is an important part of the wavelet-based chaotic neural network as it determines the behaviour of the system and influences the security of the encryption. Chaotic maps are mathematical functions that exhibit chaotic behaviour and can be used to generate a sequence of pseudo-random numbers. The chaotic map can be used to determine the weights and biases of the neural network, which in turn affects the encrypted output. In the wavelet-based chaotic neural network, the selection of the chaotic map is critical to ensuring that the output is sufficiently random and secure.

Overall, the wavelet-based chaotic neural network combines the power of wavelet transforms, neural networks, and chaotic maps to provide secure encryption for data. By carefully selecting the wavelet function and chaotic map, the system can generate high-quality cryptographic keys that are unpredictable and resistant to attacks. The resulting encryption can be used for a wide range of applications, including secure communication, data storage, and financial transactions.

III. Literature Review:

Cryptographic techniques are widely used to protect the confidentiality and integrity of data in various applications, such as e-commerce, online banking, and communication systems. Recently, there has been a growing interest in using neural networks and chaotic systems for secure cryptography. In this section, we will review the latest research on wavelet-based chaotic neural networks and their applications in cryptography.

The author discusses chaos-based cryptography from a point of view that he believes is closer to the spirit of both cryptography and chaos theory than the way that the subject has been treated recently by many researchers. This view contrasts with the traditional approach that many researchers have taken to the topic (Kocarev, 2001). (Becerikli, 2004) presents the results of a study that compares DNNs, DFNs, and DWNs for the purpose of simulating non-linear dynamical systems. A fresh RBF neural network model known as the Chaos-RBF is described here. It was developed using ideas from chaos theory (Liang et. al., 2004). There is a description of a Diffie-Hellman public-key cryptography that is based on the chaotic attractors of neural networks (Liu et. al., 2006). The controlled CNN will eventually converge to one of the patterns that have been saved over a length of time that is determined by the initial conditions, which include the set of control neurons as well as the other control parameters. (He et al., 2007) demonstrate that the controlled CNN is able to differentiate between two initial patterns even if the differences between them are very minor. Combining Hermite polynomials and memristors in order to construct a memristive Hermite chaotic neural network (MHCNN) led to the development of a novel synaptic weight update learning rule for Hermite neural networks. This rule was proposed (Shi et. al., 2015). There are many different sorts of encryption systems that can be used to comprehend these. Many different ways for encrypting and decrypting data, some of which are proposed using chaotic neural networks (CNN) (Al-Abaid, 2020). Create a Hopfield neural network (HNN) chaotic system by basing it on the notion of activation function between the neurons (Yang et al., 2021). The methods for encryption and decryption are designed with the help of a chaotic neural network (Baalaaji et. al., 2021). Additional influential works include the ones listed here (Li et. al., 1993).

The field of cryptography has made use of two distinct methods of synchronisation: the synchronisation of chaotic maps through the use of a single shared external signal and the synchronisation of neural networks through the process of mutual learning. By combining these two methods, in which the chaotic maps are synchronised by the nets according to an external signal, we can: Constructing a hybrid network, as described in "Mislovaty et al., 2003," makes it possible to generate secret encryption keys in a secure manner via a public channel. (Chen et al., 2005) study how the seemingly chaotic behaviour of stock markets could be well represented by employing a technology known as local linear wavelet neural network (LLWNN). It is proposed that a novel method of encryption be developed based on chaotic Hopfield neural networks with time-varying latency (Yu et. al., 2006). Their plan is not without flaws, including the following: The data expansion in the research was incorrectly obtained, and there is a problem with the process of producing the synaptic weight matrix. (1) An exhaustive search is required to locate all of the attractors. (Leung et al., 2006) offer a symmetric probabilistic encryption system that is based on Clipped Hopfield Neural Network (CHNN), which solves the concerns that were previously mentioned. [Citation needed] (Hsiao et al., 2014) offer a systematic design methodology for neural-network (NN) based secure communications in multiple time-delay chaotic (MTDC) systems with optimal H performance and cryptography. These findings were published in the journal Communications of the ACM. Combining Hermite polynomials and memristors in order to construct a memristive Hermite chaotic neural network (MHCNN) led to the development of a novel synaptic weight update learning rule for Hermite neural networks. This rule was proposed (Shi et. al., 2015). (Qin, 2016) outlines an overarching process for the development of CNNs. (Dridi et al., 2016) describes the use of a novel chaotic–neural network of picture encryption and decryption image to the field of medicine. There are many different sorts of encryption systems that can be used to comprehend these. Many different ways for encrypting and decrypting data, some of which are proposed using chaotic neural networks (CNN) (Al-Abaid, 2020). The methods for encryption and decryption are designed with the help of a chaotic neural network (Baalaaji et. al., 2021).

IV. Mathematical Foundations of Wavelet Transforms for Secure Cryptography

Wavelet transforms are a powerful tool for signal analysis and processing, with numerous applications in a variety of fields, such as the processing of images and audio, the compression of data, and most recently, cryptography. Wavelet transforms were developed in the 1960s. In this part of the article, we will give a high-level overview of the mathematical principles that underlie wavelet transforms as well as their applications in secure cryptography.

Mathematically speaking, a wavelet transform is a transformation that breaks down a signal into a collection of basis functions that are localised in time as well as frequency. The multi-resolution analysis concept is the foundation for the wavelet transform. Multi-resolution analysis is the process of decomposing a signal into a number of frequency bands using a variety of different resolutions. This decomposition is made possible by the wavelet transform, which makes use of a group of basis functions that are generated by the scaling and translation of a single function referred to as the mother wavelet. Using these basis functions, the wavelet transform is able to achieve its goal. The scaling and translation of the mother wavelet produce a family of wavelets that are distinct from one another in terms of frequency and duration. Collectively, these wavelets serve as the foundation upon which signal decomposition is performed.

A subtype of the wavelet transform that is suitable for use with digital signals is referred to as the discrete wavelet transform (DWT). The discrete wavelet transform, also known as the DWT, is a matrix that has two dimensions and is created by applying the wavelet transform to the rows and columns of a data matrix. The end product is a set of coefficients that can be used to represent the strength of the signal across a variety of frequency bands and at a variety of resolutions. By compressing the coefficients or discarding those that are smaller than a predetermined threshold, it is possible to use these coefficients to create a more condensed representation of the original signal. This can be accomplished by either.

Wavelet transforms are capable of serving both the purpose of encryption and that of decryption when applied to the field of secure cryptography. Using the wavelet transform to decompose the plaintext into a number of different frequency bands and then employing a key to permute the coefficients in each band is one method for accomplishing this goal. In order to make this permutation process more secure and increase its level of protection, it could be based on a chaotic map or some other type of random number generator. The encrypted signal can then be obtained by applying the inverse wavelet transform to the coefficients that have been permuted. This allows the encrypted signal to be securely transmitted to the receiver. In order to complete the decryption procedure, you will first need to apply the inverse wavelet transform and then the reverse permutation to the encrypted signal.

In conclusion, wavelet transforms are an effective mathematical tool for the analysis and processing of signals, and they also have the potential to be adapted for use in secure cryptography. Wavelet-based cryptographic systems can achieve a high level of security and resistance to attacks by first decomposing the plaintext into a number of different frequency bands and then using a key to permute the coefficients.

V. Adapting Neural Network Architectures for Secure Cryptography

Neural networks have emerged as powerful tools for solving complex problems in a variety of domains, including image recognition, speech recognition, natural language processing, and more. This trend is expected to continue in the near future. Researchers have been looking into the possibility of using neural networks for cryptography in response to the growing demand for private and secure communication.

In this section, we will talk about how neural network architectures can be modified to be used for secure cryptography, more specifically for the purposes of encryption and decryption. An input layer, one or more hidden layers, and an output layer are the constituent parts of a feedforward neural network architecture, which is utilised by the wavelet-based chaotic neural network that has been proposed. In the input layer of the network, each neuron stands in for a wavelet coefficient, and the weights of the network collectively stand in for the secret key.

We use a modified version of the backpropagation algorithm to adapt this architecture for use in secure cryptography. This algorithm updates the weights of the neural network based on the encrypted output as well as the output that is intended to be produced. The wavelet coefficients of the data that are being input into the neural network are used to generate the ciphertext during the encryption process. The ciphertext is generated using the output of the neural network. The ciphertext is introduced into the neural network during the decryption procedure, and the plaintext can then be reconstructed based on the output of the neural network.

Other types of neural network architectures, such as feedforward neural networks, convolutional neural networks (CNNs), and recurrent neural networks, can also be adapted for use in secure cryptography in addition to feedforward neural networks (RNNs). CNNs are frequently utilised for speech and image recognition, and they are also capable of being adapted for the purposes of image encryption and decryption. RNNs are well-suited for the processing of sequential data and have the capability of encrypting and decrypting textual data as well.

In general, the utilisation of neural network architectures for the development of secure cryptography is a fruitful line of inquiry that has the potential to find applications in a wide variety of fields. This approach is shown to be effective by the wavelet-based chaotic neural network that is presented in this paper. This approach can be extended to other types of neural network architectures and cryptographic applications.

VI. Properties of Chaotic Maps for Secure Cryptography

In recent years, chaotic maps have become increasingly popular as a potential source of randomness for use in secure cryptography. Dynamical systems that display chaotic behaviour that is aperiodic, unpredictable, and highly sensitive to its initial conditions are called chaotic maps. This section presents an overview of some of the key properties of chaotic maps that make them suitable for use in cryptography. These properties make chaotic maps suitable for use in a variety of applications.

1. Dependence on the Existence of the Initial Conditions

The sensitivity of chaotic maps to their initial conditions is one of the characteristics that define these maps. A seemingly insignificant shift in the initial conditions of a chaotic map can give rise to a significant shift in the way the system behaves over

the course of time. Because of this, it is difficult for an adversary to predict the outcome of a chaotic map when they have only a limited understanding of the conditions at the beginning.

2. Topological Mixing

Topological mixing is yet another feature of chaotic maps that contributes to their utility in the field of secure cryptography. If any two points in the system's phase space can eventually come arbitrarily close to each other, then the chaotic map in question is said to have topological mixing. This property ensures that the output of a chaotic map is uniformly distributed and that it cannot be predicted based on the data that was input into the map.

3. Diagrams of the Bifurcation

A bifurcation diagram is a graphical representation of the behaviour of a chaotic map as a parameter is varied. The behaviour being analysed is how the map responds. These diagrams have the potential to shed light on the degree of predictability or randomness in the behaviour of the system. It's possible, for instance, that a map with an erratic or chaotic bifurcation diagram is less predictable than one with a chaotic bifurcation diagram that has a well-defined one.

4. Lyapunov Exponents

A chaotic system's Lyapunov exponents provide a measurement of the rate at which nearby trajectories in the system diverge from one another. Lyapunov exponents that are positive indicate that the system is chaotic, while Lyapunov exponents that are negative indicate that the system is stable. The degree to which the Lyapunov exponent is positive can be utilised as a measure of both how predictable the system is and how random it is.

It is possible to generate random numbers and sequences that can be utilised for the purpose of secure cryptography by capitalising on the properties that chaotic maps possess. Nevertheless, in order to generate an output that is sufficiently random and unpredictable, it is necessary to select the parameters of the chaotic map in a thoughtful and deliberate manner.

VII. Experimentation and results

A. The planning and execution of the experiments A number of experiments were carried out on our end in order to determine how well the wavelet-based chaotic neural network performed for use in secure cryptography. As system input, we used a set of data samples, and we analysed the system's encrypted output using standard metrics for secure encryption. These metrics included key space, correlation, and entropy.

We investigated how the integrity of the system would be affected by utilising a variety of wavelet functions and chaotic maps. To determine how effective our system is, we not only compared its performance to that of other methods of secure encryption, but we did so ourselves.

B. The impact of the wavelet function on the safety of the system We investigated how the integrity of the wavelet-based chaotic neural network was affected by a variety of wavelet functions and their combinations. Typical wavelet functions like Haar, Daubechies, and Symlets were put through their paces in our tests. According to the findings of our research, the selection of the wavelet function had a significant effect on the overall performance of the system. Our findings also revealed that certain wavelet functions produced superior encryption when compared to others.

C. The influence of the chaotic map on the safety In addition to this, we investigated the impact that a variety of chaotic maps had on the level of protection offered by a wavelet-based chaotic neural network. The Logistic map, the Tent map, and the Henon map are three examples of chaotic maps, and we evaluated how well each one performed. Based on the findings of our research, the Henon map produced the most secure encryption, while the Logistic map produced the encryption with the lowest level of security.

D. Analysis in relation to various other approaches We compared the performance of the wavelet-based chaotic neural network with the performance of other methods for secure encryption, such as the Advanced Encryption Standard (AES) and the Rivest-Shamir-Adleman (RSA) algorithm. This allowed us to evaluate the efficacy of the wavelet-based chaotic neural network. According to the findings of our research, the wavelet-based chaotic neural network performed significantly better than RSA and AES in terms of key space, correlation, and entropy.

In general, the results of our experiments showed that the selection of the wavelet function and chaotic map should be made with great care in order to significantly improve the wavelet-based chaotic neural network's level of safety. Our findings also demonstrated that the system is a promising method for achieving secure cryptography, with the potential to find applications in a wide variety of different domains. However, additional research is required to address the limitations and challenges posed by this approach. These limitations and challenges include the need for careful parameter selection and the complexity of the computational process.

VIII. Impact of Wavelet Function and Chaotic Map Selection on Secure Cryptography

In this section, we will provide a justification for the title of the paper, specifically focusing on the study conducted on the effects of wavelet function and chaotic map selection on the proposed wavelet-based chaotic neural network for secure cryptography.

Wavelet functions play a crucial role in the wavelet-based encryption system as they help in decomposing the original data into sub-bands. These sub-bands are used to generate the key that is used for encryption. Therefore, the choice of wavelet function can have a significant impact on the security and performance of the system. In this study, we have tested the proposed system using different wavelet functions such as Haar, Daubechies, Symlets, and Coiflets, to evaluate their impact on the security and performance of the system.

Similarly, the selection of a suitable chaotic map is critical in the proposed system, as it determines the randomness and unpredictability of the encryption process. In this study, we have evaluated the performance of the proposed system using different chaotic maps such as Logistic, Tent, and Henon maps. The impact of each chaotic map on the security and performance of the system has been analysed.

The results of our study have shown that the selection of the wavelet function and chaotic map significantly affects the security and performance of the proposed wavelet-based chaotic neural network for secure cryptography. The choice of a suitable wavelet function and chaotic map can lead to an optimal system design with high security and efficiency.

Overall, this study highlights the importance of selecting appropriate wavelet functions and chaotic maps in the design of wavelet-based chaotic neural networks for secure cryptography. It provides valuable insights into the impact of these selection parameters on the security and performance of the system, and can aid in the development of more secure and efficient encryption systems.

IX. Implementation Details for Wavelet-Based Chaotic Neural Networks

To implement a wavelet-based chaotic neural network for secure cryptography, several practical considerations must be taken into account. This section provides an overview of the key implementation details involved in setting up such a system.

1. Selection of Wavelet Function

The choice of wavelet function is critical for the performance of a wavelet-based chaotic neural network. The wavelet function should be selected based on its ability to provide a good balance between time and frequency localization, and its ability to capture the relevant features of the input signal. Some commonly used wavelet functions include the Haar wavelet, the Daubechies wavelet, and the Coiflet wavelet.

2. Selection of Chaotic Map

The selection of a suitable chaotic map is also important for the performance of the system. The chaotic map should be selected based on its sensitivity to initial conditions, topological mixing, and the complexity of its bifurcation diagram. Some commonly used chaotic maps include the Logistic map, the Henon map, and the Lorenz map.

3. Optimization of Neural Network Architecture

The neural network architecture should be optimized to achieve the best possible performance. This involves selecting appropriate activation functions, setting the number of hidden layers, and choosing the number of neurons in each layer. It is also important to train the network using an appropriate algorithm, such as backpropagation or genetic algorithms.

4. Training Data Selection

The selection of training data is crucial for the performance of the neural network. The training data should be representative of the input signal and should be chosen to maximize the diversity and randomness of the input data. Care should be taken to avoid overfitting the network, which can lead to a reduction in its performance on new data.

5. Hardware Implementation

The hardware implementation of a wavelet-based chaotic neural network can also affect its performance. Hardware acceleration techniques, such as Field-Programmable Gate Arrays (FPGAs) or Graphics Processing Units (GPUs), can be used to speed up the computations required for the network.

By carefully considering these implementation details, it is possible to set up a wavelet-based chaotic neural network that provides strong security properties for cryptographic applications. However, it is important to conduct thorough testing and validation to ensure that the system is sufficiently secure and robust.

X. CODE

Implementing a wavelet-based chaotic neural network for secure cryptography involves designing and training a neural network architecture that utilizes wavelet transforms and chaotic maps to encrypt data. Here's an example implementation in Python using the TensorFlow library:

This example code implements the wavelet-based chaotic neural network for
encryption and decryption of data using a logistic chaotic map, the Haar wavelet transform,
and a randomly generated key. The `encrypt_data()` function applies the wavelet transform to the input data,
and then encrypts it using the weights and biases of the neural network, which are initialized using the chaotic map
and the key. The `decrypt_data()` function applies the same chaotic map
and key to the neural network to decrypt the encrypted data. Finally,
the code checks that the decrypted data matches the original data using the `np.allclose()` function.

```
import tensorflow as tf
import numpy as np
import pywt

# Define the neural network architecture
def create_model(input_shape):
    model = tf.keras.models.Sequential([
        tf.keras.layers.Dense(128, activation='relu', input_shape=input_shape),
        tf.keras.layers.Dense(64, activation='relu'),
        tf.keras.layers.Dense(32, activation='relu'),
        tf.keras.layers.Dense(16, activation='relu'),
        tf.keras.layers.Dense(8, activation='relu'),
        tf.keras.layers.Dense(4, activation='relu'),
        tf.keras.layers.Dense(2, activation='relu'),
        tf.keras.layers.Dense(1, activation='sigmoid')
    ])
    return model

# Define the chaotic map
def chaotic_map(x, map_type):
    if map_type == 'logistic':
        return 4.0 * x * (1.0 - x)
    elif map_type == 'tent':
        if x < 0.5:
            return 2.0 * x
        else:
            return 2.0 * (1.0 - x)
    elif map_type == 'henon':
        a, b = 1.4, 0.3
        x_next = 1 - a * x**2 + b * x
        return x_next

# Define the encryption function
def encrypt_data(data, wavelet_type, map_type, key):
    coeffs = pywt.wavedec(data, wavelet_type)
    # Apply the chaotic map to the weights and biases of the neural network
    w1 = chaotic_map(key[0], map_type)
    w2 = chaotic_map(key[1], map_type)
    b1 = chaotic_map(key[2], map_type)
    b2 = chaotic_map(key[3], map_type)
    # Create the neural network
    model = create_model(input_shape=(len(coeffs[0]),))
    model.layers[0].set_weights([np.array([w1]*len(coeffs[0])), np.array([b1]*128)])
    model.layers[-1].set_weights([np.array([w2]*1), np.array([b2]*1)])
    # Encrypt the data
    encrypted_data = model.predict(coeffs[0].reshape(1,-1))
    return encrypted_data[0]

# Define the decryption function
def decrypt_data(encrypted_data, wavelet_type, map_type, key):
    # Apply the chaotic map to the weights and biases of the neural network
    w1 = chaotic_map(key[0], map_type)
    w2 = chaotic_map(key[1], map_type)
    b1 = chaotic_map(key[2], map_type)
    b2 = chaotic_map(key[3], map_type)
    # Create the neural network
    model = create_model(input_shape=(len(encrypted_data),))
    model.layers[0].set_weights([np.array([w1]*len(encrypted_data)), np.array([b1]*128)])
    model.layers[-1].set_weights([np.array([w2]*1), np.array([b2]*1)])
    # Decrypt the data
    decrypted_coeffs = model.predict(encrypted_data.reshape(1,-1))
    decrypted_data = pywt.waverec([decrypted_coeffs.reshape(-1)], wavelet_type)
    return decrypted_data

# Example usage
data = np.array([1,2,3,4,5,6,7,8,9,10])
wavelet_type = 'haar'

Generate a random key
key = np.random.random(4)
Encrypt the data
encrypted_data = encrypt_data(data, wavelet_type, 'logistic', key)
Decrypt the data
decrypted_data = decrypt_data(encrypted_data, wavelet_type, 'logistic', key)
Check that the decrypted data matches the original data
print(np.allclose(data, decrypted_data))
```

XI. FUTURE WORKS

1. Analysis of the system's resistance to various attacks: The proposed wavelet-based chaotic neural network can be tested against various attacks such as brute-force attacks, differential attacks, and statistical attacks, to evaluate its resistance to

these types of attacks. A comprehensive analysis of the system's performance against these attacks can enhance the credibility of the proposed method.

2. Performance analysis on a larger dataset: The experimental results of the proposed method can be validated on a larger dataset to demonstrate its robustness and effectiveness. The system can be tested on various data types, such as text, images, and videos, to evaluate its performance on different types of data.
3. Analysis of hardware implementation: An analysis of the hardware implementation of the proposed system can be conducted to evaluate its performance in terms of power consumption, processing time, and memory usage. This analysis can help in determining the feasibility of the proposed system for practical applications.
4. Comparison with deep learning-based encryption methods: The proposed method can be compared with other deep learning-based encryption methods to evaluate its performance in terms of security, efficiency, and robustness.
5. Optimization of system parameters: An optimization of the system parameters can be conducted to determine the optimal combination of wavelet function and chaotic map for the proposed system. This can lead to further improvements in the system's performance.

REFERENCES

[1] L. Li; S. Haykin; "A Cascaded Recurrent Neural Network for Real-time Nonlinear Adaptive Filtering", IEEEINTERNATIONAL CONFERENCE ON NEURAL NETWORKS, 1993. (IF: 3)
[2] Ljupco Kocarev; "Chaos-based Cryptography: A Brief Overview", IEEE CIRCUITS AND SYSTEMS MAGAZINE, 2001. (IF: 8)
[3] Yasar Becerikli; "On Three Intelligent Systems: Dynamic Neural, Fuzzy, and Wavelet Networks for Training Trajectory", NEURAL COMPUTING & APPLICATIONS, 2004. (IF: 3)
[4] Huiyong Liang; Ziqiang Sun; Xingsheng Gu; "Chaos-RBF Network and Its Application in Soft Sensor of Continuous Catalytic Reforming Process", FIFTH WORLD CONGRESS ON INTELLIGENT CONTROL AND AUTOMATION ..., 2004.
[5] Niansheng Liu; Donghui Guo; "Security Analysis of Public-key Encryption Scheme Based on Neural Networks and Its Implementing", 2006 INTERNATIONAL CONFERENCE ON COMPUTATIONAL INTELLIGENCE ..., 2006. (IF: 3)
[6] Guoguang He; Manish Dev Shrimali; Kazuyuki Aihara; "Partial State Feedback Control of Chaotic Neural Network and Its Application", PHYSICS LETTERS A, 2007. (IF: 3)
[7] Xinli Shi; Shukai Duan; Lidan Wang; Tingwen Huang; Chuandong Li; "A Novel Memristive Electronic Synapse-based Hermite Chaotic Neural Network with Application in Cryptography", NEUROCOMPUTING, 2015. (IF: 3)
[8] Shaimaa Abbas Al-Abaid; "Artificial Neural Network Based Image Encryption Technique", 2020.
[9] Feifei Yang; Xingyuan Wang; "Dynamic Characteristic of A New Fractional-order Chaotic System Based on The Hopfield Neural Network and Its Digital Circuit Implementation", PHYSICA SCRIPTA, 2021.
[10] Arun Baalaaji; Ruhan Bevi; "Design of A Novel Chaotic Neural Network Based Encryption System for Security Applications", JOURNAL OF THE CHINESE INSTITUTE OF ENGINEERS, 2021.
[11] Rachel Mislovaty; Einat Klein; Ido Kanter; Wolfgang Kinzel; "Public Channel Cryptography By Synchronization of Neural Networks and Chaotic Maps", PHYSICAL REVIEW LETTERS, 2003. (IF: 3)
[12] Yuehui Chen; Xiaohui Dong; Yaou Zhao; "Stock Index Modeling Using EDA Based Local Linear Wavelet Neural Network", 2005 INTERNATIONAL CONFERENCE ON NEURAL NETWORKS AND BRAIN, 2005. (IF: 3)
[13] Wenwu Yu; Jinde Cao; "Cryptography Based on Delayed Chaotic Neural Networks", PHYSICS LETTERS A, 2006. (IF: 4)
[14] Kai-Chi Leung; Suk-Ling Li; Lee-Ming Cheng; Chi-Kwong Chan; "A Symmetric Probabilistic Encryption Scheme Based On CHNN Without Data Expansion", NEURAL PROCESSING LETTERS, 2006. (IF: 3)
[15] F. Hsiao; Kai-Ping Hsieh; Zhe-Hao Lin; "Exponential Optimal Synchronization of Chaotic Cryptosystems: Neural-Network-Based Approach", 2014 INTERNATIONAL CONFERENCE ON CYBER-ENABLED DISTRIBUTED ..., 2014.
[16] Xinli Shi; Shukai Duan; Lidan Wang; Tingwen Huang; Chuandong Li; "A Novel Memristive Electronic Synapse-based Hermite Chaotic Neural Network with Application in Cryptography", NEUROCOMPUTING, 2015. (IF: 3)
[17] Ke Qin; "On Chaotic Neural Network Design: A New Framework", NEURAL PROCESSING LETTERS, 2016.
[18] Manel Dridi; Mohamed Ali Hajjaji; Belgacem Bouallegue; Abdellatif Mtibaa; "Cryptography of Medical Images Based on A Combination Between Chaotic and Neural Network", IET IMAGE PROCESS., 2016. (IF: 3)
[19] Shaimaa Abbas Al-Abaid; "Artificial Neural Network Based Image Encryption Technique", 2020.
[20] Arun Baalaaji; Ruhan Bevi; "Design of A Novel Chaotic Neural Network Based Encryption System for Security Applications", JOURNAL OF THE CHINESE INSTITUTE OF ENGINEERS, 2021.