applied system innovation

MDPI

Review

The Dichotomy of Neural Networks and Cryptography: War and Peace

Behrouz Zolfaghari [1,*] and Takeshi Koshiba [2]

[1] CyberScienceLab, University of Guelph, Guelph, ON N1G 2W1, Canada
[2] Department of Integrated Arts and Sciences, Waseda University, Tokyo 169-8050, Japan; tkoshiba@waseda.jp
* Correspondence: behrouz@cybersciencelab.org

Abstract: In recent years, neural networks and cryptographic schemes have come together in war and peace; a cross-impact that forms a dichotomy deserving a comprehensive review study. Neural networks can be used against cryptosystems; they can play roles in cryptanalysis and attacks against encryption algorithms and encrypted data. This side of the dichotomy can be interpreted as a war declared by neural networks. On the other hand, neural networks and cryptographic algorithms can mutually support each other. Neural networks can help improve the performance and the security of cryptosystems, and encryption techniques can support the confidentiality of neural networks. The latter side of the dichotomy can be referred to as the peace. There are, to the best of our knowledge, no current surveys that take a comprehensive look at the many ways neural networks are currently interacting with cryptography. This survey aims to fill that niche by providing an overview on the state of the cross-impact between neural networks and cryptography systems. To this end, this paper will highlight the current areas where progress is being made as well as the aspects where there is room for future research to be conducted.

Keywords: neural network; cryptography; cryptanalysis; survey

Citation: Zolfaghari, B.; Koshiba, T. The Dichotomy of Neural Networks and Cryptography: War and Peace. *Appl. Syst. Innov.* **2022**, *5*, 61. https://doi.org/10.3390/asi5040061

Academic Editor: Andrey Chernov

Received: 23 May 2022
Accepted: 21 June 2022
Published: 24 June 2022

1. Introduction

In recent years, artificial neural networks (ANNs), simply referred to as neural networks (NNs) have been of great interest to the research community. They consist of layered networks of nodes meant to mimic a human brain, where the nodes represent biological neurons and the connections between them represent the synapses. Neural computing, as technology and a field of research has a wide ecosystem. It is in close interaction with many scientific and technological fields. NNs support a range of technological fields including medical technology [1] as well as image processing [2], cloud computing [3], aerospace technology [4], meteorology [5], and especially in security-related technologies [6,7]. Moreover, several technologies and sciences such as chaos theory [8], frequency-domain transforms [9], genetic algorithms [10] and Digital Signal Processing (DSP) [1] are supporting neural networks as enablers.

In this paper, we focus on the intersection of neural computing with cryptography. Cryptography is the study of mathematical techniques as a means of securing data communication and storage. Like the case of neural computing, cryptography has a broad ecosystem consisting of different scientific and technological fields. It supports a variety of technologies including Internet of Things (IoT) [11], cloud computing [12], Fog computing [13], etc. [14]. It also serves to security-related scenarios such as information hiding [15], authentication [16,17], privacy [18], etc. Furthermore, cryptography is supported by a variety of enabling technologies and sciences including radix 2^n [19] and modular arithmetics [20], quantum computing [21,22], coding and information theory [23,24], Very Large Scale Integration [25], chaos theory [26], and error management techniques [27] are used to support cryptography.

Neural computing and cryptography frequently appear in the ecosystems of each other. They come together, in war and peace, in many ways; NNs can play adversarial roles against cryptosystems while they can support and be supported by cryptography at the same time. This tight interaction forms a dichotomy. Figure 1 illustrates the two sides of this war-and-peace dichotomy.

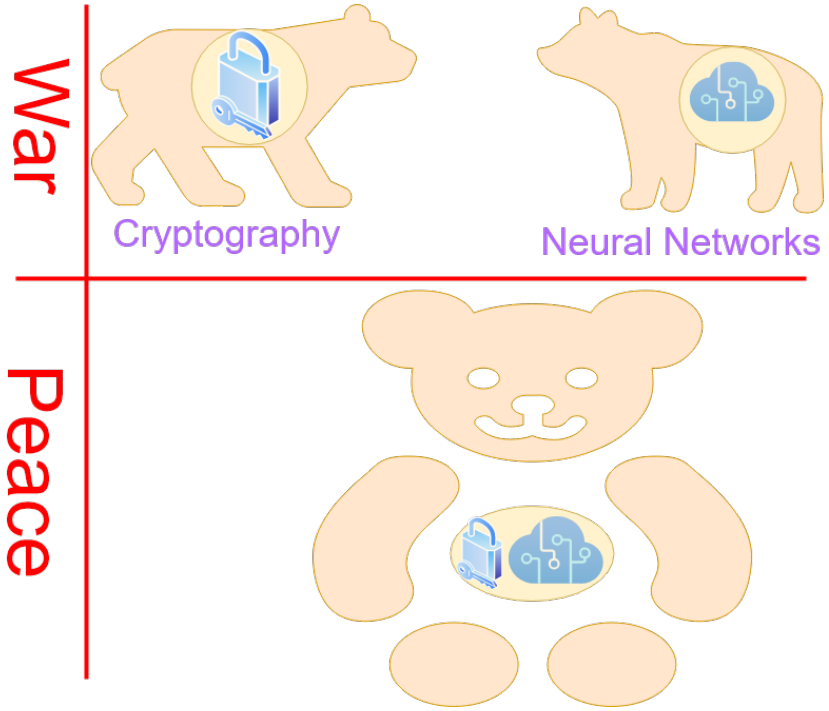

Figure 1. The war-and-peace dichotomy of neural networks and cryptography.

In Figure 1, the two bears facing each other represent the war or the adversarial role of NNs in breaking cryptographic systems. The teddy bear represents the peaceful give and take between the two technologies including the use of cryptography to secure NNs or the use of NNs in order to improve cryptosystems.

A comprehensive survey on the war-and-peace dichotomy shown in Figure 1 can pave the way for future research. In this paper, we first summarize some existing relevant surveys. We highlight the shortcomings of these surveys to motivate this research. We will then discuss the current state of the war; the ways in which NNs are being used to break cryptogrphic systems. We will then study the state-of-the-art in the peace side; how the two technologies work in concert with each other, cryptography providing confidentiality and privacy guarantees for NNs, and NNs adding to the functionality and the security of cryptographic systems. Lastly, we will discuss how quantum computing might fit into the future of this dichotomy. We briefly discuss what the future may hold for the war-and-peace dichotomy under the impact of quantum computing.

1.1. Contributions

This survey aims to highlight the current state of the dichotomy described above, with the goal of highlighting areas for future research where the two technologies intersect. This research is unique in the broadness of it's scope. Our goal is to cover as many of the interactions between cryptography and NNs as possible. There are some surveys that cover limited aspects of this dichotomy, some covering out of date research, and others failing to look to the future of the field. We aim to address these niches via providing a broad study on different aspects of the of NN-crypto dichotomy, and using that for a look into the future.

The contributions of this paper can be listed as follows.

1. Our paper is the first of its kind to analyze the cross-impact between neural networks and cryptography and decompose it into two opposite sides.
    - **War:** In this side, we study the aggressive activities assisted by neural networks against cryptography. We investigate the role of NNs in cryptanalysis and attacks against cryptographic systems.
    - **Peace:** This side consists of the ways cryptography and NNs mutually support each other. We study this mutual support in the following lines.
        - Cryptographic techniques, mechanisms and devices can be used to provide confidentiality for NNs and their processed data.
        - Neural networks can be applied in the design of cryptosystems aiming at improved security and efficiency.
2. In addition to shedding light on the current state in the dichotomy of NNs and cryptography, we establish a future roadmap for further research in this area. This roadmap is developed in consideration of future computing paradigms and expected advancements.

1.2. Organization

The rest of this paper is organized as follows. Section 2 studies existing surveys. Section 3 reviews research works focusing on the use of NNs against cryptography. Section 4 shows how neural computing and cryptography can coexist, cooperate and support each other. Section 5 provides directions for future research on the interaction between neural computing and cryptography. Lastly, Section 6 concludes the paper.

2. Existing Surveys and Motivations

Although there might be some related surveys, their shortcomings motivate the work of this paper. These shortcomings can be itemized as follows.

- There are a few reviews on the role of artificial intelligence (AI), and especially NNs in cryptography. However, to the best of our knowledge, there is no comprehensive survey on the roles of cryptography in secure neural networks. Moreover, there is no survey on the role of neural networks in aggressive activities against cryptography.
- Some existing surveys are too outdated for such a dynamic research area [28–30].
- Most of them fail to develop directions for future research in this area [31,32].

The above shortcomings highlight the importance of our work in this paper with the contributions mentioned in Section 1.

In the following, some relevant surveys are briefly discussed ordered by their publication year.

There have been several past surveys studying the relationship of AI and cryptography. Figure 1 shows the general relationship between the two technologies, in places they are adversaries and others they combine to create a benevolent system. Some older surveys study technology which is no longer relevant to the current discussion. Many of the newer surveys take too narrow field to garner insight into the future of the field.

Vandewalle et al. looked at the current state of cryptography by defining the goals of security systems and discussing possible solutions [28]. Concerning NNs this study mentions the application of cellular NNs (CeNNs) too implement Boolean mappings and the application of cellular automata (CeA) to encrypt data.

Ten years later Schmidt et al. summarized uses of NNs in private key systems, an image encryption scheme, pseudo random number generation, the analysis and generation of digital watermarks [29]. That same year Hu and Wang proposed using a specific NN model for 802.16 to share private keys over a public channel through training synchronization [30].

Hadke and Kale provided another broad review of NN's ability to improve on current cryptographic techniques [31]. This paper fails to mention any techniques that the the 2008 review did not mention, but it gives an overview of some attacks on NN-improved cryptography systems.

Sharma and Sharma compared key exchange schemes using NNs and quantum computers as means to improve on current key management systems in 2016 [32]. This paper concluded that NN Key exchange is more practical but has yet to be practically implemented and the theory needs hardening against unconventional attacks.

ÖzÇakmak et al. published a paper in 2019 referencing the work of Sharma and Sharma also comparing NNs and quantum computers ability to improve key exchange systems [33]. This paper also come to the conclusion that current quantum solutions cannot be broadly implemented and NNs could be used but it does not bring up any specific implementations or steps needed to further research.

Su et al. studied current image encryption techniques using NN to propose a possible architecture for encrypting medical images [34].

Meraouche et al. [35] published a comprehensive survey documenting various NN cryptography techniques along with verified attacks and some published solutions for the attacks. Through this survey Meraouche et al. found that cryptographic NN systems are trending in two directions, providing a low computation cost encryption solution and being a viable post-quantum encryption primitive.

Table 1 provides a summary of existing surveys in order to make it easy to see their shortcomings and compare them with our survey.

Table 1. Summary of existing surveys.

Survey	Year	NN-Peace-Crypto	Crypto-Pace-NN	NN-War-Crypto	Future Roadmap
[28]	1998	yes	no	no	no
[29]	2008	yes	no	no	no
[30]	2008	yes	no	no	no
[31]	2016	yes	no	no	no
[32]	2016	yes	no	no	yes
[33]	2019	yes	no	no	no
[34]	2020	yes	no	no	yes
[35]	2021	yes	no	no	yes

In Table 1, each entry in the first column contains one of the surveys studied in this section. The second column indicates the publication year of the related survey. Outdated surveys can be identified using this column. The next three columns indicate the aspects of the NN-crypto dichotomy (partially) covered by each survey. The third column indicates whether or not the survey discusses the roles of NN in improvement of cryptosystems. The fourth column contains "yes" if the survey studies the roles of cryptography in protection of NNs. It contains "no" otherwise. Surveys focusing on the adversarial role of NN against cryptography are designated by a "yes" in the fifth column. Lastly, the sixth column demonstrates whether or not the related survey builds a future roadmap.

3. War: Neural Computing against Cryptography

There is no research work focusing on the activity of cryptography against NNs. However, NNs are used against cryptography in different ways.

Cryptography schemes are designed so that it is hard to garner information from their output. If implemented correctly many cryptography schemes should be secure against analysis. However there are several proposed methods to use neural computing to break or otherwise perform cryptanalysis on different encryption schemes.

3.1. Detecting Malicious Encryption

Detecting and locating malicious encrypted data can help detecting ransomware and other kinds of malware. Some researchers have focused on the applications of NNs in this area [36]. Some research works focusing on malicious encryption detection in software code and network traffic are briefly reviewed in the following.

Cryptography can be used to hide malicious data until it is needed. When encrypted data is detected and it cannot be decrypted, there is normally no way to tell if it is malicious or not. It has been proposed to use machine learning models to identify encrypted files and network traffic as malicious.

3.1.1. Software Code

Cryptography is a tool that can protect the confidentiality of data, while often used to the benefit of users it can be used by attackers to hide malware on a system until it is needed or obfuscate network traffic. It can be difficult to identify malware that is able to encrypt data as it might require reverse engineering the suspicious program and applying a thorough understanding of many encryption methods [37]. It has been found that NNs could simplify the process of detecting encryption in obfuscated programs. This section will discuss some researchers applying NNs to detecting encrypted malicious code.

Wright and Manic [38] built a NN system trained with error back propagation that analyzes the ratio of certain opcodes that are commonly used by cryptographic algorithms. Trained on functions in OpenBSD it was found this system could identify most typical encryption functions regardless of compiler optimization or specific implementation, but failed to detect methods that operate sufficiently different from typical encryption methods such as elliptical curve cryptography and public key encryption.

Jia et al. [37] propose solving this issue with a NN model called K-max-CNN-Attention that looks for common instruction patterns rather than relative instruction density. The improvements this model brings is in the move to a convolutional NN (CNN), which interpret blocks of data maintaining the original structure and a better preprocessing scheme which simplifies the input enough to be meaningful to the NN but leaving more information to be interpreted, while these changes improve on performance and accuracy of existing techniques Jia et al. [37] speculate that better accuracy could be achieved by changing the preprocessing and classification models to consider non-sequential execution of code.

3.1.2. Network Traffic

Due to the increase in VPN usage by average users, companies have begun looking for solutions and security models in order to distinguish between a legitimate connection and a malicious connection [39]. One group has used flow-based statistics to classify TCP layer traffic as VPN or Non VPN connections. These flow statistics are TCP flows taken as time-based statistics and other key features found using Pearson's correlation coefficient algorithm [39]. Using a multilayered perceptron NN trained from the features selected, the model was successfully able to distinguish 92% of the data given during the validation phase making it feasible to tell whether a connection is using a VPN or not [39]. What this model of VPN identifying does not consider is the identification of non VPN traffic that may be malicious and encrypted. However, other models that use a combination of encryption and abnormality detection can solve this problem [40]. In order to provide high performance and data integrity, this model will use clustering and feature vector expansion to improve the quality of their data [40], while this model does seem provide better performance and classification rates that traditional methods, it is subject to the data imbalance problem due to the diversity of encrypted malicious attacks.

3.2. Cryptanalysis

Cryptanalysis is the processes of finding vulnerabilities in ciphers by studying their operation. This is usually completed with knowledge of some combination of the cipher text, plain text, and key. Though it is often associated with attacks on cryptogrphic systems,

cryptanalysis can be used to audit current systems to improve them. In some cases, cryptanalysis can be considered as an aggressive activity against cryptosystems, because it can be conducted in an initial stage of an attack. There have been some attempts at creating cryptanalysis attacks to directly decrypting cipher text using NNs. Apolinhrio Jr. et al. found an early cryptanalysis application for NNs reordering blocks of audio data scrambled with time segment permutation scrambler [41]. Their Hopfield network, trained with simulated annealing with a "genetic algorithm" approach on a small set of words, was able to meet the performance of exhaustively searching for a solution [41].

Ruzhentsev et al. attempted to apply neural nets to decrypt 8 bit cipher texts from a substitution permutation cipher using the same key for the training set and the test set [42], while they did not find complete success decrypting cipher texts this way, they found it possible to decrypt 232 out of the 256 possible cipher texts with the average number of wrong bits in each erroneous decryption being 1.3.

Other papers focused on applying NNs to determine some amounts of the key used to encrypt a cipher text, possibly reducing the amount of time needed to guess the correct key. Abassal and Wahdan propose an attack specific to Feistel block ciphers using NNs to determine the key but was limited to only the cipher the neural net is designed for [43].

Danziger and Henriques studied how effective NNs could be at cryptanalyzing S-DES ciphers [44]. In particular they attempted to determine key bits based on a given plain text and it's corresponding cipher text. Their test found that certain bits of the key were more easily determined due to problems with the substitution box being used by the cipher.

Xiao et al., utilized NNs to quantify the strength of ciphers by predicting cipher text based on the plain text [45]. Using this approach only ciphers as strong as DES-3 were successfully mimicked, though the researchers suggested that using a neural net architecture that more closely reflected that of the cipher being analyzed would be more capable.

NNs have also been used to analyze cipher operation in order to encrypt data. Khan et al. tested the application of neural nets to directly replicate the functionality of a cipher by training some models on cipher, plain text pairs with and without knowledge of the key [46]. Hsiao et al. proposed a different system, training a NN to analyze the output of multiple time-delay chaotic system in order to approximate its output and synchronize a second multiple time-delay chaotic system as a means for establishing an encrypted communication over a public channel [47].

3.3. Vulnerability Analysis

Vulnerability analysis is the act of evaluating threats to security or cryptographic systems and networks. This process will identify and assess these systems and networks for flaws that could lead to exploitation by malicious actors.

Like the case of cryptanalysis, vulnerability analysis can help an adversary design the attack scenario against a cryptosystem. There are a few research works where NNs have been used to analyze the vulnerabilities of cryptosystems. The use of feed-forward NNs FNNs has been applied to the vulnerability analysis of Physical Unclonable Functions (PUFs) [48]. More specifically FNNs are being used to model out attack scenarios against the Challenge Response Pairs (CRPs) of the PUFs [48]. It was found that given very few CRPs as a baseline, an FNN using the Dragonfly Algorithm(DA) was able to accurately predict more challenge–response pairs with a 85.2% accuracy attacking the Configurable Ring Oscillator PUF and 71.3% against the XOR-inverter Ring Oscillator PUF [48]. DA works by moving neurons as dragonflies, moving them closer to the goal (food sources) and away from bad predictions (enemies) by using the neurons as dragonflies on a dimensional grid with speed and velocity [48].

3.4. Attack

Some researchers have been able to develop attacks on cryptogrphic systems leveraging the features of NNs. In some research works, NNs have been directly used to attack

cryptosystems. It has been shown that symmetric ciphers can be broken by using Real-time Recurrent NNs (RRNN) with Chosen Plaintext Attack (CPA) [49].

As another example, UFnet, a NN using ReLU activation functions and Xavier initialization techniques, can predict the responses of double-arbiter physically unclonable functions (PUFs) [50].

4. Peace: Coexistence and Alliance

NNs have also been integrated with cryptography systems. Section 4.1 will discuss NNs trained on encrypted data and Section 4.2 will discuss encryption schemes that make use of NNs on some level.

4.1. Coexistence

It has been proposed to use NNs trained on encrypted data. Since there is a noticeable performance drop when using encrypt data, either in processing time accuracy or both. The methods to address this are twofold, developing infrastructure that can better support using encrypted data or tailoring the encryption scheme and the Neural net to improve accuracy and reduce training and processing time.

4.1.1. NNs Adapted to Encrypted Data

Researchers are working on the design of NNs capable of being applied on encrypted data. To this end, NNs need to be able to be trained over encrypted datasets, and process encrypted input data. Training NNs on normal data can be computationally expensive. However training on encrypted data can be even more expensive. To reduce the extra cost of using encrypted data researchers have proposed several efficiency increasing methods.

NNs Trained over Encrypted Datasets

To train NNs on encrypted data, very large and diverse datasets are needed. Instead of coming up with individual training datasets for each new model it is common to create a database of standard training data.

Xu et al. proposed a framework to securely share encrypted data sets from multiple sources, comparing the model training time and accuracy to that of MINST data sets [51]. Xu et al. proposed another different framework which applies functional encryption scheme to cloud AI service architectures where user supplied data is processed by the service provider [52].

Another consideration is the extra complexity of creating a model to understand information that is not meant to be readable as would be the case creating a model which can process encrypted data. In order to train a NN on data that has to be permuted to maintain privacy, Molek and Hurtik proposed using a fully connected auto encoder as a preprocessor for a convolutional NN to make the encoded data more readable [53]. Similarly Nandakumar et al. developed a method of training a NN on fully homomorphicaly encrypted data [54]. By making some optimizations in training a small drop in accuracy is traded to reduce the time needed to train on encrypted data from 6.5 h to 40 min.

NNs Capable of Processing Encrypted Input Data

This section will list many of the ways that NNs are being implemented to use encrypted data. In the following, we study some types of neural computing processes possible to applied on encrypted data.

1. **Classification:** Different kinds of input data can be classified in their encrypted form by special types of NNs. Some of these types are discussed below. Similar to identifying encrypted malicious data, NNs have been trained to classify other kinds of encrypted data to protect the confidentiality of the contents while still providing useful classification.
    - **Encrypted Network Traffic:** This type of input data can be classified by NNs for anomaly detection [55] or application identification [56,57] purposes. Some

papers focused on improving the classification of TLS/SSL traffic since it is commonly used to protect web traffic. Zhang et al. designed a NN combining, stereo transform, and convolutional NNs to classify TLS/SSL traffic with up to 95% accuracy [58]. Yang et al. proposed using a Bayesian NN system that observes non-encrypted handshake packets, the specific cipher being used and the compression method to classify TLS connections [59]. Zhou and Cui improved upon the Alexnet deep NN by developing multi-scale convolution, a deconvolution operation, and batch standardization in order to reduce training time [60]. Other papers focused their efforts further on classifying encrypted VPN traffic. Song et al. applied a text convolutional NN system to classifying VPN traffic [61]. In order to avoid imbalances in class identification caused during training a loss function and class weighing method were implemented. Zou et al. proposed a novel deep NN that takes series of three packets as input so that features of packets that are continuous between packets can be considered by the system [62]. He and Li method interprets encrypted packets as greyscale images [63]. The images are classifies the by a convolutional NN. In implementation a convolutional NN was trained on VPN traffic and was able to classify similar traffic with 97.3% accuracy. Wang et al. [64] on the other hand evaluated their novel NN's ability to classify mobile data sourced from 80 different mobile applications. The novel design combines long short-term memory recurrent networks with convolutional NNs, for pattern and signature recognition, respectively. Some researchers designed systems focusing on factors external to the specifics of one encryption method. Wang and Zhu made an early attempt in 2017 at end-to-end encrypted traffic classification using a 1D convolution NN [65]. While many approaches rely on deep learning which require a lot of training Cheng et al. propose using lighter weight system utilizing multi-headed attention and 1D convolutional NN which has to consider far less parameters and halves the training time of comparable systems [66]. In order to perform classification using information provided by observing feature attributes Cui et al. propose an improvement to CapsNet which weighs effective traffic more and now considers the spacing of features [67]. Yang et al. developed a classification method using an auto encoder and convolutional NNs taking packet length and arrival time into account [68]. More recently Wang et al. proposed a similar method using the combination of stacked autoencoder and convolutional NN but raising the number of parameters to 26, including both statistical data and information from the raw packets, to supply high level classification features [69].

- **Encrypted Image:** In order to efficient perform ITS image evaluation, images need to be secured. This group of researchers proposes using a convolutional NN to classify encrypted images based on partially decrypting them to reveal only nonsensitive information [70].
- **Encrypted Speech:** In order to retrieve encrypted speech, a deep NN using deep hashing is proposed with two different models: both convolutions and convolutional recurrent. With their high quality deep hashing capabilities, a two stage retrieval strategy is proposed [71].
- **Encrypted Application:** Uses an end-to-end encryption application for encrypting network traffic based on a 1 dimensional convolutional NN using spatial and temporal features [72].

2. **Other Processes:** In addition to classification, researchers have proposed NNs for applying other processes such as compression [73] or visual quality assessment [74] on encrypted input data.

4.1.2. Cryptographic Technology Adapted to Neural Computing

Cryptosystems are being adapted to neural computing. They are trying to encrypt data in a way that the encrypted data can be efficiently processed by NNs. Homomorphic

encryption is the most common attempt made towards achieving this goal. While classification can be performed on normal encryption data, researchers have proposed some systems which use specially designed encryption schemes which obfuscate the data in a way that better allows processing. Homomorphic encryption is a form of encryption that allows a user to perform valid computations with the ciphertext. Upon decryption of the ciphertext the plaintext will have the same computations applied.

In order to maintain privacy in the current world filled with powerful data mining techniques and massive networks of data gathering sensor it is becoming increasingly obvious that Fully Homomorphic Encryption (FHE) will be needed for end-to-end encryption [75].

As this field has been growing rapidly we have seen many changes, as recently as 2018 it was shown that current homomorphic systems were too slow for large amounts of data and NNs were not yet secure enough to work with encrypted data [76]. The same year it was thought a possible solution would be to perform the homomorphic encryptions as a part of a cloud environment using multiple parties [60].

However, this too showed to be too slow, but brought to light possibilities of using GPU's to increase efficiency [60]. The authors of [77] have taken into consideration the space-efficiency problems with FHE functions and have begun work on a method named DOReN. Their method is used to instantly evaluate multiple quantized ReLU-activated neurons in the NN which are processing encrypted data. This considerably cuts down on the space needed to perform these neuron activations.

Other research groups have tackled FHE's time efficiency problem by transforming all the operations into bit-wise functions and transforming the input encrypted data into binary format; this technique roughly equates to a 6.3 times increase in the speed of CNN's [78].

More recent work has shown that the security of NNs lead to Fully Homomorphic Encryption over Torus (TFHE), which is a scheme that uses NN's to effectively evaluate encrypted input data [75]. TFHE along with the protection against backdoor attacks into NNs has provided NNs with security against some forms of malicious attacks [79].

While optimizations of how we use FHE are still in production, some groups have already begun applying these systems to facial recognition and English to Arabic translation [79,80].

Although the translation time for even small words still has a massive run-time to provide adequate accuracy, facial recognition on ciphertext using CNN's provides real-time usage for high accuracy verification [79,80].

4.2. Alliance

Aside from training NNs on encrypted data, NNs have also shown to be useful to improve the functionality of cryptographic systems and vice versa.

4.2.1. The Role of NNs in Cryptography

NNs have been applied to improving several aspects of cryptographic systems from encrypting several data types to key management and generally securing different aspects of cryptographic systems.

Neural Cryptography:

Neural cryptography refers to the application of mutual learning, self learning, and stochastic behavior of neural networks as well as similar algorithms in the design, implementation, or evaluation of any cryptographic algorithm, device, system, or scenario. Particularly, neural networks have been used as enablers in the design of several cryptographic mechanisms, which are implemented as individual modules in cryptosystems. This should be considered an important aspect of neural cryptography.

- **Key Management:** Neural Cryptography has been applied to key management in many different ways, some have researched its use in concealing keys in Deep NNs [81], while others have researched the use of NN's using tree parity machines as a way to distribute keys of a symmetric encryption system [82]. A more novel

approach uses Artificial Spiking NNs (ASNNs) to create keys for a symmetric block cipher algorithm with the ability to use any block size [83]. This method provides no need for key exchange [83]. The environment systems itself uses a semblance of public key cryptography where the public key is the seed used to generate the private key on both sides [83]. Additional approaches to neural cryptography symmetric key exchanges involve using a 3D cube algorithm in order to induce secrets on the receiver side or search guided gravitational neural keys [84,85].

- **Random Number Generation:** Neural cryptography has guided the verification of Pseudo Random Number Generators (PRNGs) by picking up on statistical biases unknown to humans [86]. This is achieved using neural cryptography to detect the difference between actual output and desired ideal random numbers [86].

The use of neural cryptography for encryption [87] and decryption [88] has received a focus from the research community in recent decades [89–91]. Different security models have been proposed based on neural cryptography [92] and different kinds of NNs [93] have been used for design and implementation of cryptosystems [94]. This effort has led to the development of different types of neural cryptosystems [94,95]. In the following, we use the research literature to establish an ecosystem for neural cryptography. This ecosystem consists of applications, enablers, and challenges.

- **Applications:** The applications of neural cryptography can be studied in the following lines.
  - **Encrypting Different Content Types:** Neural cryptography has been successfully tested on different content types, among which one may refer to the following.
    - **Image:** Regular scrambling-diffusion image encryption suffers from many vulnerabilities [96]. Particularly both the scrambling and diffusion are performed independently meaning an attacker can attack each separately [96]. With neural cryptography this vulnerability can be resolved. More specifically using an algorithm that performs the initial scrambling and diffusion in parallel then a second diffusion from a Hopfield chaotic NN trained [96]. This allows not only for the protection from the aforementioned independent cracking of the scrambling and diffusion steps, but also resists chosen plaintext attacks [96]. Other groups have also implemented parallelization in their neural cryptography encryption algorithms, electing instead to perform these operations using cellular NNs and block encryption to create an algorithm based on the feistel framework [97]. Cellular NNs are being used in all kinds of Image Encryption software, including an encryption scheme that uses the hyper chaotic system sequences of a cellular NN to shuffle around the bit of an image before performing a bit-wise XOR [98]. It is important to note that this method uses asymmetric RSA for key exchanges [98]. This can pose an issue since the security of the model relies then on the RSA key and not the Neural Cryptography system [99]. To resolve this issue a NN at the receiver end and a stochastic encryption method at the senders end can be used to eliminate the need for key exchanges all together [99]. Finally, Wavelet Chaotic NNs (WCNN) and chaotic NNs have also been used for secure encryption and decryption of images [100]. However, research has shown that WCNN provides stronger ciphertext [100]. Furthermore,during transmission the only data that would need to be sent is approximation coefficients , reducing the size of the ciphertext drastically [100].
    - **Video:** For video encryption of the MPEG-2 video code, research has shown that using Chaotic NNs to encrypt the bitstream results in high entropy and high key sensitivity, both desirable results for security [101]. This model transmits data via the Orthogonal Frequency Division Multiplexing (OFDM) modulation technique and controls the bit rate and quality of the decrypted

video [101]. A hybrid chaos and NN cipher encryption algorithm for compressed video signal transmission over wireless channel.

* **Text:** While image and video encryption introduces new types of encryption, some approaches taken for text encryption have been to improve upon existing systems to provide new cryptographic schemes. Some groups have used Neural cryptography to encrypt plaintext , generating both a secret key and a hash using the Auto Encoder NNs (AENN) [102]. AENN is a NN meant to provide the least possible distortion to the resulting ciphertext, this allows ciphertext normalization to still appear as ascii [102]. Another improvement of schemes is the use of secret dimensions of a NN model as key instead of relying on asymmetric keys and trapdoor functions [103]. The application of delayed Chaotic NNs to generate binary sequences has also been researched in text encryption [104]. The binary sequence is used to create the key for the first level of encryption [104]. Then used in conjunction with DNA cryptography to create a secure ciphertext [104].

– **Applications in Security-Related Scenarios:** There are some security-related scenarios, which depend on cryptography. Neural networks have been used by researchers in many of these scenarios. To mention a few, we may refer to the following.

  * **Privacy:** The security of ubiquitous computing has seen great improvement due to Neural cryptography. The idea of neural synchronization to generate shared keys is currently one that provides real-time security for systems already in place [105].
  * **Authentication:** While issues with WiMAX have been thoroughly documented [106]. Neural Cryptography proposes solutions to authentication and authorization by creating neural synchronized key pairs [106]. To achieve this neural synchronization two NNs are created with the same weight changing algorithm and passed the same input [107]. To achieve neural synchronization boundary conditions are set, whenever both weights shift to the same direction and one of the networks touches the boundary, the boundaries close tighter eventually leading to neural synchronization [107]. RFID has seen many problems due to having no international standards and posses security risk, one proposed solution [108]. Involves using a tree parity NN in order to perform key generation [108]. Biometric recognition for authentication has also seen support from deep recurrent NNs in order to increase accuracy and performance of models [109].
  * **Steganography:** Stenography is the study of hiding messages within something that is not a message, in some cases an image. One way to achieve this using neural cryptography is to first perform Discrete Cosine similarity Transform and Elliptic Curve Cryptography to first encrypt the image you would like to hide [110]. Then using a Deep NN this message is embedded into a host image [110]. Other groups have achieved similar results of image using Self-Organizing Map (SMO) NNs with 26 clusters for every letter of the alphabet [111]. Research has also been conducted to hide messages within sound [112]. To accomplish sound stenography, SMO's are used again with 27 clusters , 1 for every letter in the alphabet and then a cluster for the space between words [112].
  * **Visual Cryptography:** One drawback of visual cryptography is its lack of evaluation criteria [113]. One group proposed a method of evaluating the desirable results of visual cryptography would be encryption-inconsistency and decryption-consistency [113]. Visual cryptography via NNs can be achieved by passing a Q'tron NN a set of greyscale images and the output be a set of binary images [114,115]. Other types of NNs used for visual cryptography includes Pi-Sigma NNs, which is a double layered feed forward

network [116]. Allowing for fewer communications between sender and receiver with higher security [116].

- **Technological Applications:** The recent literature comes with several successful applications of neural cryptography in the technology. Some of these applications are studied below.
  - **Applications in Industry:** A large contribution to NN in technology comes from its applications for secure wireless communication [108,117,118]. After proof of its security was published [119]. Particularly, NN have been used with Fast Handover Protocol in place of MIPv6 to replace its short comings, allow the encryption of large scale satellite images for secure transmission and decryption efficiently and lightweight implementation for key systems in an IoT environment [117,120,121]. Other applications of Neural Cryptography has allowed for homomorphic encrpytion to be applied to cloud services for secure communication and noise compression, as well as intelligent transportation systems to allow confidentiality of personal information [122,123]. Finally, chaotic NNs has seem many applications as well [124–126]. To note, hyper chaotic systems and chaotic Feistel transform and time synchronization with multiple dimensions have allowed the resistance of plain text attacks and brute force attacks within the physical layer [125,126].
  - **Applications in Medical Technologies:** Applications of neural cryptography in the field of medicine have come from the requirement of keeping patient images confidential [127]. One approach uses a Hermite Chaotic NN in two rounds , first a chaotic sequence is generated from a logical mapping and used to train the NN, then the image is passed into the network to generate a key for encryption [128]. Other methods of security proposed involve using the Region of Non-Interest in the image in order to watermark the image [127].

- **Challenges:**
  - **NN Type Selection:** A look at the literature shows that different kinds of NNs are useful for different applications. NN type selection is critical to the ability of neural cryptography to be successful, one group has even used NNs to effectively create new cryptography based off NN training [129]. Investigated the use of Complex-valued tree parity machines in order to perform key synchronizations and how CVTPM's can be seen as more secured to create key synchronizations than using simple tree parity machines [130]. Achieved postquantum key exchange protocols by using NNs in order to augment Diffie–Hellman key exchange protocols by using multivariate cryptosystems [131]. Explored the relationship between cryptographic functions and the learning abilities of RNN [132,133]. Used Principle Component Analysis NNs to generate random numbers for a chaos encryption system [134]. Other groups have experimented with cellular NNs with iterative interchangeability to produce encryption that allows flat historgrams for randomness and bias [135]. Back-propogating NNs in order to provide strong image compression-encryption using a fractional-order hyperchaotic system [136]. unbounded inertia NNs with input saturation in order to obtain good cryptographic properties [137]. Memristive bidirectional associative memory NNs for colored image encryption [138]. Uses recurrent NNs parallel processing speed to increase the performance of encryption, also proposes a symmetric encryption scheme allowing for variable message and block sizes for data integrity and data encryption [139,140]. A look at the literature shows that different kinds of NNs are useful for different applications.
  - **Hardware Implementation:** A successful implementation of Izhikevich's neural model has been created using SIMECK block cryptography to allow the spiking NN to perform authentication [141].

- **Neural Physically Unclonable Function (PUF):** A Physically Unclonable Function is a physical device that when provided with challenges provides a response that acts as a digital finger print. The uniqueness of these fingerprints relies on the physical variations created during manufacturing of the device. Neural PUF are PUFs with NNs embedded into the hardware in an attempt to make them resistant against attacks from NNs learning the outcome of challenge response pairs [142]. It is well known that Strong PUF's can have their pattern recognized by NNs, thus it is suggested to used a WiSARD NN in order to add machine learning resistance to strong PUF'S [142]. Further ways to disallow NNs to learn from challenge responses of PUF's is to use analog NNs [143]. Moving on to hardware purposes, researches have created a 1-bit PUF with a 2 neuron CNN with good metrics for robustness [144]. Other uses for NNs in the space of PUF's involve Error Coding Correction for keys which provides more efficient corrections than standard models [145]. Finally, Tests have been conducted to show there is feasibility in using NN based PUF's for authentication purposes [146].
- **Security Evaluation:** Here we discuss attacks on previously mentioned cryptographic systems [147,148]. First we note a majority attack on neural synchronization via NN to provide secret keys, this attack is possible due to many cooperating attackers [147]. Then we view the lack of side-channel resistance in tree parity machine NNs and how you can obtain the secret weight vector via this side channel attack [148]. Finally, we look at a power analysis attack on NNs in order to discover their secret information and then propose resistances against these types of side channel attacks [149]. Although NNs are susceptible to the aforementioned attacks, it also provides resistances to the more commonly known vectors of classical cryptography [150].
- **Synchronization:** Synchronization of NNs is when a client and network exchange output of NN's with the goal of having identical weights for synapses. Following with the derivation of a shared key using these keys. Researchers use Period Self-Triggered Impulses to attempt synchronization of NNs and then applied the NN to encrypted images [151]. There has also been study into the generalization of synchronization by using Discrete Time-Array Equations [152]. Other papers investigate the use of lag within the neuron activation functions of a network of NNs in order to provide secure synchronization [153]. Papers have also tested different reaction-diffusion technique of Lyapunov time-dependent impulses within NNs to see its applicability to encrypting images [154]. Synchronization for arrays in a network system can also be achieved by using master-slave synchronization of a delayed NN [155]. The use of memristor-based models and its chaotic properties have also been studied in regards to its image encryption capabilities [156]. Other memristive models using lyapunov functions have also been used for image encryption [157].
- **Asynchronous Neural Cryptography:** Asynchronours Neural cryptography is neural cryptography where synchronization of the sender and receiver model need not be conducted, in fact they can calculate their weights separately based on information passed to each other via encryption schemes such as one time pad [158]. Produce a chaotic time series using a chaotic NN and use that to encrypt plaintext [158], while the method does have its errors the proposed encryption scheme to use in conjunction, a one-time pad, does alleviate those problems [158].

- **Enablers:** By "Enablers", we mean technologies sciences and techniques used to support the design of neural cryptography systems. Some of these enablers are discussed below.
  - **Chaos Theory:** Chaos theory is a branch of mathematics that aims to understand and accurately describe systems which are highly sensitive to their initial conditions [159]. In image encryption, three separate chaotic functions are used

for each rgb color in order to allow image encryption via Hopfield NNs [160]. Other uses of Hopfield NNs include using creating asymmetric cryptography by using the semblances of the NN with the human body to do synchronization [161]. Other uses for Hopfield NNs and its human-like similarities is using it in conjunction with DNA cryptography [104]. Signal encryption using the chaotic nature of some NNs have been explored to create digital envelopes [162]. Signal encryption has also been achieved using VLSI architecture for chaotic NNs [163]. Further broad-brand signal encryption utilize Chain Chaotic NNs [164]. Other uses for Chaos NNs is pseudo random number generations using a peice wise linear chaotic map [165,166]. Besides using chaotic maps for pseudo random generation, it is also being used in research in conjunction with S-boxes in order to improve upon public key cryptography [167,168], while encryption via NNs may be possible, a comparison with AES shows it provides better performance at the cost of security for larger files [169].

- **Genetic Algorithms:** Genetic algorithms are heuristics based of the theory of evolution where the best performing individuals will be used to create the next generation of individuals for further optimization in the hopes to converge to an optimization. A version of genetic synchronization has been used to create a key where the hidden weights of both NNs acts as a key between parties where weights are taken as the distance between chromozones of the NN [170]. Other symmetric key applications use Genetic algorithms with error back propogating NNs to instead create the key to be used for other encryption schemes [171]. Some encryption schemes have also seen improvement, by using AES with a GA algorithm in a NN, the SP-Box portion of AES can be greatly improved [172]. Public Key cryptography enhancements via genetic algorithms have also been of interest to some researchers, in fact it has been used for key generation here as well [173].
- **Error Management Codes:** Error management codes such as Cyclic Redundancy Check (CRC) have been used by some researchers in the design of neural cryptosystems. CRC is a type of checksum which is primarily used to verify there are no errors in a message. It accomplishes this by executing some polynomial operations on the body of a message, the result of the operations can then be used to verify the messages integrity [174]. One way researchers have augmented the security of neural cryptography is using the DTMP algorithm to produce erroneous bits into the bits transferred between NNs during the synchronization phase [175]. However it was found this two allows potential attacks [176]. The researchers continued by finding three algorithms to build upon the original idea of DTMP [176].
- **Frequency-Domain Transforms:** Frequency-Domain transforms methematical algorithms which can be used to obtain a description of a function in the frequency domain as opposed to the time domain [177]. Researchers created a data transmission method using classification of speech patterns via NNs to leave no speech signals available on the phone line [178].
- **Blockchain:** A blockchain is collection of data organized into blocks which are connected to each other by a chain of cryptographic hash digests, commonly implemented in a way such that modifications to the blockchain need to be made through a peer to peer network [179]. To aid in the authentication of users performing key synchronization, researchers have proposed using a second secret value for implicit identity authentication based on block chain technologies [180].
- **Combinatorics:** Combinatorics is the study of arranging discrete structures, and can expand into other fields including enumeration, graph theory and algorithms [181]. With the power of cellular NNs and its chaotic sequences along with 5 distinct latin squares are used for greyscale image encryption [182].

– **Existing Cryptographic Algorithms:** In existing cryptography some researchers propose using the synaptic connections of a NN and an input image in order to generate the secret key for an AES encryption [183]. Other researchers propose the use of a variety of AES encryptions for files using the same NN key structure [184].

According to the above discussions, the ecosystem of neural cryptography is illustrated by Figure 2.

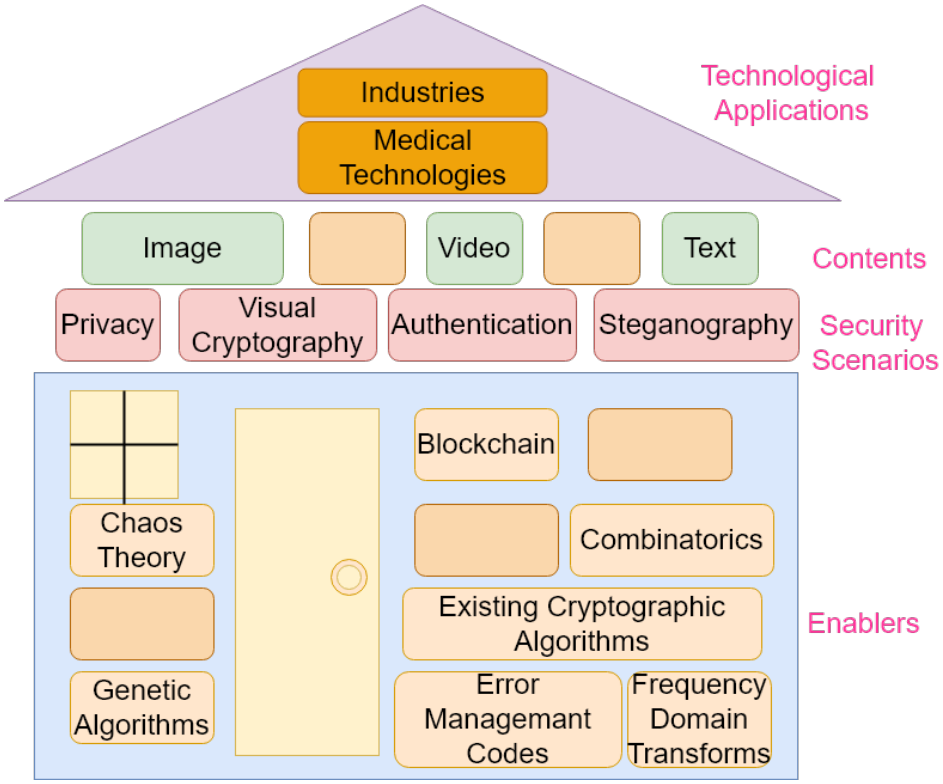

Figure 2. The ecosystem of neural cryptography.

NN-Improved Cryptography:

Researchers have shown that NNs can be used in conjunction with colored image encryption schemes to reduce the noise leftover after decryption [185].

Cryptography Using Neural-like Methods:

Neural-like methods are the application of neural functions and methodology without the use of a NN. For example, the neural-like method proposed by the authors of [186] is capable of using a hardware neural-like data decryption/encryption system based on a geometric transformations model.

4.2.2. The Role of Cryptography in Secure Neural Computing

Cryptography has also been used to ensure the confidentiality of NN data. The following subsection will discuss different approaches to encrypting the data that NNs use.

Encrypted NNs

Architectures for encrypted NNs have been proposed in order to preserve the privacy of data being processed through integrating some kind of cipher, usually homomorphic, into the normal operation of the system. This section will discuss some proposed methods to work on data sets that have been processed to protect the privacy of it's subjects.

Li and Han propose a framework for a federated learning scheme which protects the data sets of clients contributing to a central server [187]. This is performed by encoding the

calculated gradient before it is sent by the client. The gradient update is decoded while being combined with the gradients from other clients, effectively preventing interception as well breaches from server.

Other approaches focused more heavily on working on encrypted data.

Choi et al. designed, implemented and tested a convolutional NN ASIC system with integrated AES functionality [188].

Emmanuel et al. propose a system similar to Li and Han's [187] scheme, which only sends data in the form of encoded gradients. This system however never decodes the data as it is encrypted homomorphicaly [189].

Mefta et al. also designed a hardware solution, but this system differs as it is based on a deep NN that is working on homomorphicaly encrypted data [77].

Crypto-Enabled NNs

Another vector for compromising the confidentiality of NNs is through the data stored in memory [190]. A solution could be encrypting any data needed for operating the NN until it is used. This would protect the data but would introduce a significant loss in performance. There are however a few specialized cryptographic techniques the enable NNs to maintain the confidentiality of their data without much loss of performance [190].

Enabling In-Memory NNs Using Cryptography

Cai et al. proposed an encryption scheme that only encrypts a small number of weights in memory called sparse fast gradient encryption [190]. Encrypting only a few of the weights has far less overhead compared to encrypting all of the weights, and in tests it was still enough to protect the model. The same group of researchers also extended sparse fast gradient encryption to the storage level when non-volatile memory is used [191].

Data Encryption for Securing NNs

Considering the large overhead that comes with using encrypted data, Hu et al. proposed a deep NN system processing homomorphicaly encrypted data with the goal of achieving real-time [192]. The proposed changes are to use the NN blocks whichcan be hardware accelerated.

Cantoro et al. take a different approach, they proposed using encrypted weights not only as a method for protecting the training data set and operation of the NN for highly sensitive systems but also as a fault detection mechanism [193].

Image Encryption for Privacy-Preserving NNs

Dealing with text data that is encrypted come with performance challenges as the patterns in the data are harder to recognize. encrypted image data compounds the issue, as images can be far larger in size.

Sirichotedumrong et al. present pixel-based image encryption, an image encryption scheme that obfuscates image data while maintaining a deep NNs ability to analyze it after a little preprocessing [194]. Sirichotedumrong et al. then propose a cipher-text only attack on images that have been encrypted with pixel-based image encryption when a victim uses the same key [195].

Sirichotedumrong et al. propose encryption scheme that is resistant to the known cipher-text only attack involving using another novel image encryption algorithm and training NN models on encrypted images that use unique keys [196]. Sirichotedumrong et al. published another paper building on the cipher-text only attack resistant scheme. They trained models on encrypted images as well as non encrypted images extending their models ability to classify encrypted images, to also classifying plain images as well [197].

5. Future Roadmap: The Promise of Secure AI

As quantum computing becomes a more mature technology, viable applications will become more clear. A possible field quantum computing could move into is cryptography

and neural computing. Thus, we anticipate that the war and peace will be between quantum NN and quantum-inspired NN-assisted cryptography in the future. Our reason for such an anticipation is the existence of the trends discussed in Sections 5.1–5.3.

5.1. Quantum NNs in Cryptography

Some researchers are looking at the application of fractional-order quantum cellular NNs (QCNN) in an attempt to solve the nonlinearities that exist in image cryptography [198]. On the other hand, researchers have instead proposed multilayer quantum NNs trained with synchronization to create a new cryptosystem [199]. Continuing the trend of developing quantum cryptosystems with NN, one group proposes a multivariate cryptosystem for a post cryptography world [200].

5.2. NNs in Quantum Cryptography

In Quantum Cryptography, the use of artificial NNs provide good security and efficiency for error correction provided the model meets necessary requirements [201]. Other groups have introduced the idea of noise diffusion using Chaotic Recurrent NNs by using chaotic keys from NNs with quantum noise [202].

5.3. Quantum-Inspired AI

Quantum computing is finding its applications in a variety of technological areas ranging from navigation [203] to channel coding [204] and IoT [205]. Quantum-inspired AI is a recent research trend dealing with the applications of quantum computing in artificial intelligence. In the following, we review some research works focusing on quantum-inspired AI.

Some researchers have proposed a quantum inspired reinforcement learning (QiRL) solution in the application of trajectory planning for unmanned aerial vessels(uavs) in order to create a greedy AI [206]. QiRL has also been studied in the used of Markov chains in order to utilize collapse phenomenon and amplitude amplification in Robotic navigation [207]. In contrast, some groups have developed AI frameworks based on 're-experiencing' based events (inputs) using quantum technology in order to further develop sophisticated models [208]. Quantum inspired multi directional associative memory has also been proposed using a model suited for self-convergence and iterative learning [209]. Finally, a model for Fuzzy based NNs in two-class classification has been proposed using using iterative learning by integrating fuzzy clustering techniques with quantum computing [210].

Figure 3 shows a possible future for the neural network–cryptography dichotomy.

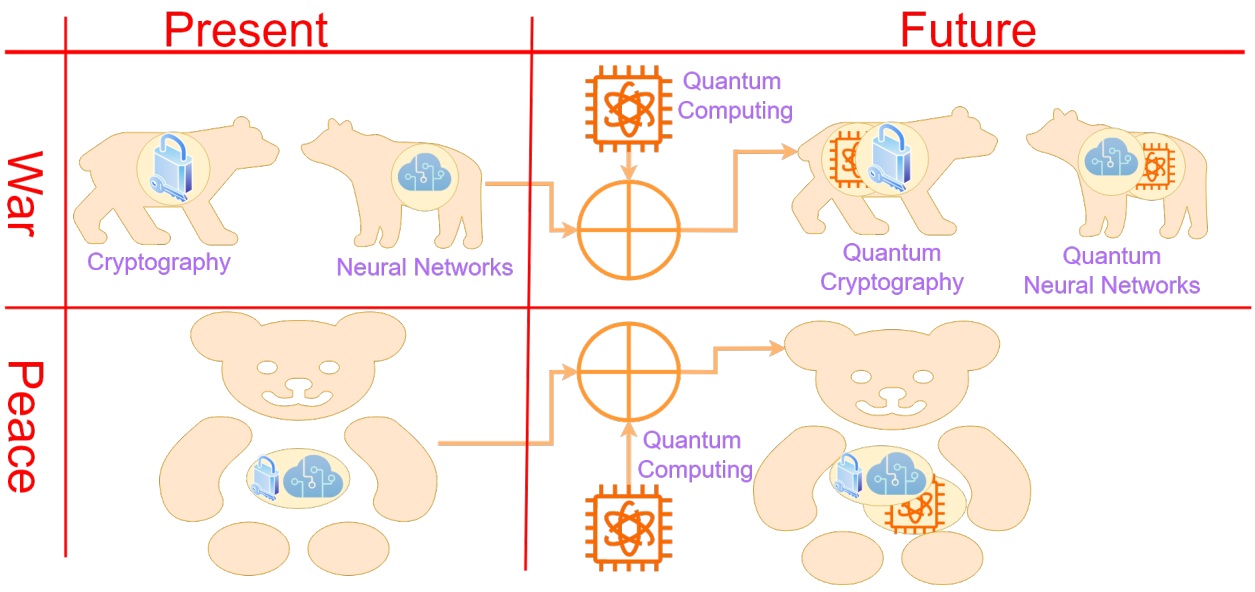

Figure 3. The future of the neural network–cryptography dichotomy.

6. Concluding Remarks

As the relationship between NNs and cryptography grows more matured, the cross-impact between them is growing more and more complex. Spanning over a decade makes it pertinent to study this dichotomy. This paper has been a look at the many ways NN and cryptographic technologies have come together as well as the future of both given recent computing paradigms and related advancements. This paper can be concluded in the following lines.

6.1. State-of-the-Art: War and Peace

The recent literature suggests the following aspects for the war-and-peace dichotomy of neural networks and cryptography.

- The application of neural networks in the cryptanalysis of cryptographic schemes and attacks against them (War);
- The application of neural networks towards improving the security as well as the efficiency of cryptosystems (Peace);
- The application of cryptography towards the confidentiality of neural networks (Peace).

6.2. At the Horizon: Quantum Advancements

Quantum computing stands in a position to create a similar dichotomy. Once quantum computing finds its way into cryptographic and neural computing schemes, it will inherit the problem of balancing data confidentiality with computational efficiency. It will remain a key concern protecting legitimate confidential data from analysis techniques, while still being able to defend against malicious data being hidden through similar means. Thus, quantum computing will need to bring cryptography and neural computing together in ware and peace again. In the era of quantum computing, the war-and-peace dichotomy of neural networks and cryptography will lead to another dichotomy; quantum neural networks and quantum cryptography.

6.3. Contributions

This paper aimed to highlight areas where current research is going on as well as related topics in need for future research. The authors hope that this survey will provide some insight for those looking to do further work in the field.

6.4. Further Research

In this paper, we have not covered the adversarial role of cryptography against neural networks. The reason is the lack of adequate research in this area. This gap is shown by the red box in Figure 4. To address this gap researchers can continue the work of this paper, when the literature comes with adequate relevant works, via studying the ways cryptanalysis and cryptographic attacks can be conducted against encrypted neural networks. Moreover, we would recommend future research investigating defensive provisions for cryptography schemes against neural attacks.

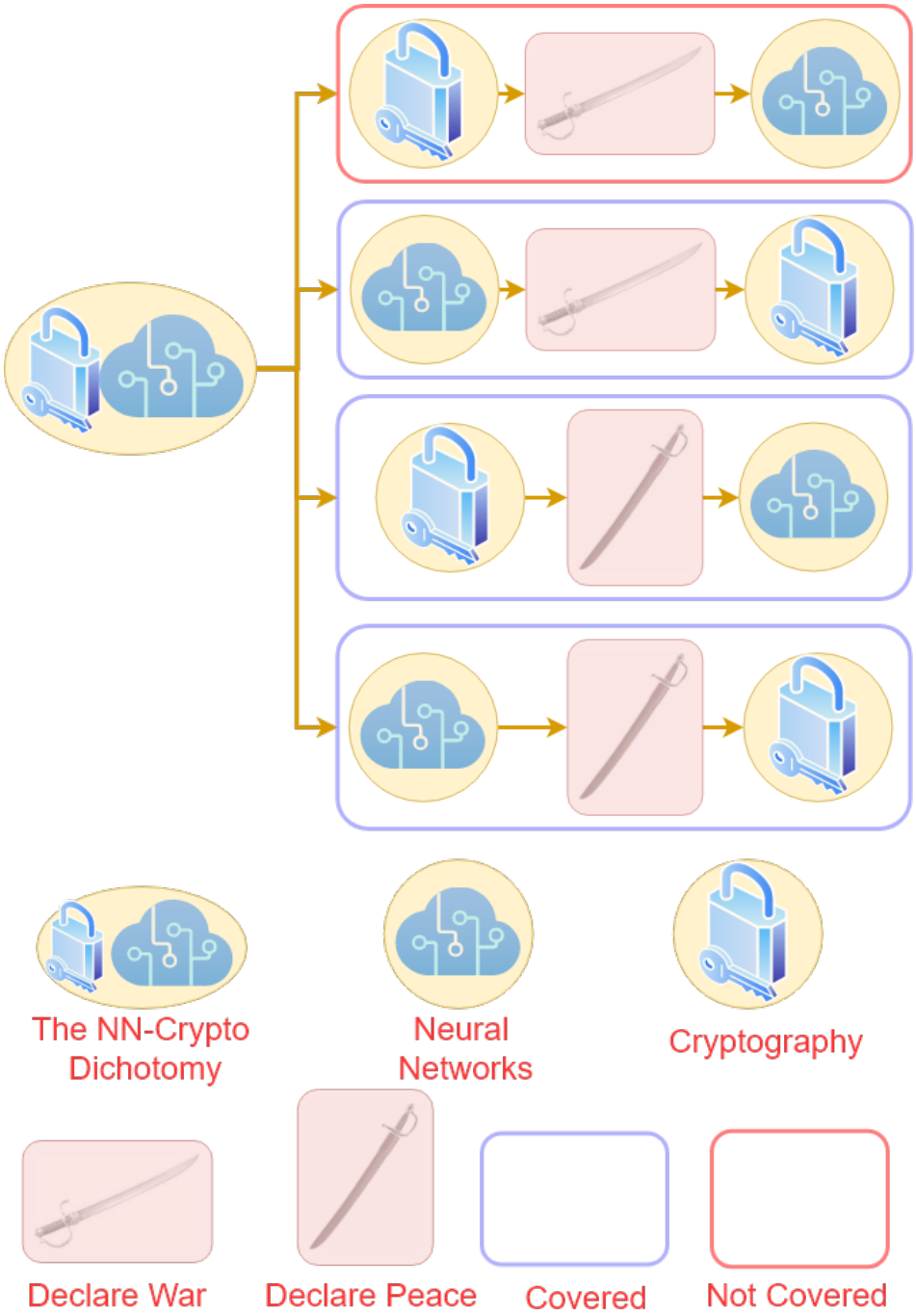

Figure 4. The covered and uncovered aspects in the war-and-peace dichotomy of neural networks and cryptography.

Author Contributions: T.K. has contributed to the review. B.Z. has contributed in review, writing and preparation. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Si, J.; Li, G.; Cheng, Y.; Zhang, R.; Enemali, G.; Liu, C. Hierarchical Temperature Imaging Using Pseudo-Inversed Convolutional Neural Network Aided TDLAS Tomography. *IEEE Trans. Instrum. Meas.* **2021**, *70*, 4506711. [CrossRef]
2. Wang, Y.; Cheng, J.; Zhou, Y.; Zhang, F.; Yin, Q. A Multichannel Fusion Convolutional Neural Network Based on Scattering Mechanism for PolSAR Image Classification. *IEEE Geosci. Remote Sens. Lett.* **2021**, *19*, 4007805. [CrossRef]
3. Huang, Y.; Qiao, X.; Ren, P.; Liu, L.; Pu, C.; Dustdar, S.; Chen, J. A Lightweight Collaborative Deep Neural Network for the Mobile Web in Edge Cloud. *IEEE Trans. Mob. Comput.* **2021**, *21*, 2289–2305. [CrossRef]
4. Liu, Y.; Chen, X.; Wu, Y.; Cai, H.; Yokoi, H. Adaptive Neural Network Control of a Flexible Spacecraft Subject to Input Nonlinearity and Asymmetric Output Constraint. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**, *in press*. [CrossRef]
5. Zhang, Z.; Chen, G.; Yang, S. Ensemble Support Vector Recurrent Neural Network for Brain Signal Detection. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**, *in press*. [CrossRef] [PubMed]
6. Nandy, S.; Adhikari, M.; Khan, M.A.; Menon, V.G.; Verma, S. An Intrusion Detection Mechanism for Secured IoMT framework based on Swarm-Neural Network. *IEEE J. Biomed. Health Inform.* **2021**, *26*, 1969–1976. [CrossRef]
7. Alladi, T.; Gera, B.; Agrawal, A.; Chamola, V.; Yu, R. DeepADV: A Deep Neural Network Framework for Anomaly Detection in VANETs. *IEEE Trans. Veh. Technol.* **2021**, *70*, 12013–12023. [CrossRef]
8. Zhang, C.; Yu, Y.; Wang, Y.; Han, Z.; Zhou, M. Chaotic Neural Network-Based Hysteresis Modeling With Dynamic Operator for Magnetic Shape Memory Alloy Actuator. *IEEE Trans. Magn.* **2021**, *57*, 2501004. [CrossRef]
9. Wang, M.H.; Lu, S.D.; Liao, R.M. Fault Diagnosis for Power Cables Based on Convolutional Neural Network with Chaotic System and Discrete Wavelet Transform. *IEEE Trans. Power Deliv.* **2021**, *37*, 582–590. [CrossRef]
10. Zhou, M.; Long, Y.; Zhang, W.; Pu, Q.; Wang, Y.; Nie, W.; He, W. Adaptive Genetic Algorithm-aided Neural Network with Channel State Information Tensor Decomposition for Indoor Localization. *IEEE Trans. Evol. Comput.* **2021**, *25*, 913–927. [CrossRef]
11. Liu, Z.; Seo, H. IoT-NUMS: Evaluating NUMS Elliptic Curve Cryptography for IoT Platforms. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 720–729. [CrossRef]
12. Gao, X.; Yu, J.; Chang, Y.; Wang, H.; Fan, J. Checking Only When It Is Necessary: Enabling Integrity Auditing Based on the Keyword with Sensitive Information Privacy for Encrypted Cloud Data. *IEEE Trans. Dependable Secur. Comput.* **2021**, *in press*. [CrossRef]
13. Zhang, X.; Tang, W.; Gu, D.; Zhang, Y.; Xue, J.; Wang, X. Lightweight Multidimensional Encrypted Data Aggregation Scheme With Fault Tolerance for Fog-Assisted Smart Grids. *IEEE Syst. J.* **2022**, *in press*. [CrossRef]
14. Zolfaghari, B.; Singh, V.; Rai, B.K.; Bibak, K.; Koshiba, T. Cryptography in Hierarchical Coded Caching: System Model and Cost Analysis. *Entropy* **2021**, *23*, 1459. [CrossRef]
15. Xiong, L.; Han, X.; Yang, C.N.; Shi, Y.Q. Robust Reversible Watermarking in Encrypted Image with Secure Multi-party based on Lightweight Cryptography. *IEEE Trans. Circuits Syst. Video Technol.* **2021**, *32*, 75–91. [CrossRef]
16. Parida, P.; Pradhan, C.; Gao, X.Z.; Roy, D.S.; Barik, R.K. Image Encryption and Authentication With Elliptic Curve Cryptography and Multidimensional Chaotic Maps. *IEEE Access* **2021**, *9*, 76191–76204. [CrossRef]
17. He, D.; Zeadally, S.; Kumar, N.; Wu, W. Efficient and Anonymous Mobile User Authentication Protocol Using Self-Certified Public Key Cryptography for Multi-Server Architectures. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2052–2064. [CrossRef]
18. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Khalil, A.; Hasbullah, I.H. Security and Privacy Schemes in Vehicular Ad-Hoc Network With Identity-Based Cryptography Approach: A Survey. *IEEE Access* **2021**, *9*, 121522–121531. [CrossRef]
19. Oudjida, A.K.; Liacha, A. Radix-2w Arithmetic for Scalar Multiplication in Elliptic Curve Cryptography. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2021**, *68*, 1979–1989. [CrossRef]
20. Tian, J.; Lin, J.; Wang, Z. Fast Modular Multipliers for Supersingular Isogeny-Based Post-Quantum Cryptography. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2021**, *29*, 359–371. [CrossRef]
21. Xie, J.; He, P.; Wang, X.M.; Imana, J.L. Efficient Hardware Implementation of Finite Field Arithmetic AB + C over Hybrid Fields for Post-Quantum Cryptography. *IEEE Trans. Emerg. Top. Comput.* **2021**, *10*, 1222–1228.
22. Bibak, K.; Ritchie, R.; Zolfaghari, B. Everlasting security of quantum key distribution with 1K-DWCDM and quadratic hash. *Quantum Inf. Comput.* **2021**, *21*, 181–202. [CrossRef]
23. Cohen, A.; D'Oliveira, R.G.L.; Salamatian, S.; Médard, M. Network Coding-Based Post-Quantum Cryptography. *IEEE J. Sel. Areas Inf. Theory* **2021**, *2*, 49–64. [CrossRef]
24. Zolfaghari, B.; Bibak, K.; Koshiba, T. The Odyssey of Entropy: Cryptography. *Entropy* **2022**, *24*, 266. [CrossRef]
25. Zolfaghari, B.; Bibak, K.; Nemati, H.R.; Koshiba, T.; Mitra, P. *Statistical Trend Analysis on Physically Unclonable Functions: An Approach via Text Mining*; CRC Press: Boca Raton, FL, USA, 2021.
26. Lin, C.H.; Wu, J.X.; Chen, P.Y.; Li, C.M.; Pai, N.S.; Kuo, C.L. Symmetric Cryptography With a Chaotic Map and a Multilayer Machine Learning Network for Physiological Signal Infosecurity: Case Study in Electrocardiogram. *IEEE Access* **2021**, *9*, 26451–26467. [CrossRef]
27. Canto, A.C.; Mozaffari-Kermani, M.; Azarderakhsh, R. Reliable CRC-Based Error Detection Constructions for Finite Field Multipliers With Applications in Cryptography. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2021**, *29*, 232–236. [CrossRef]
28. Vandewalle, J.; Preneel, B.; Csapodi, M. Data security issues, cryptographic protection methods, and the use of cellular neural networks and cellular automata. In Proceedings of the Fifth IEEE International Workshop on Cellular Neural Networks and their Applications, Proceedings (Cat. No.98TH8359), London, UK, 14–17 April 1998.

29. Schmidt, T.; Rahnama, H.; Sadeghian, A. A review of applications of artificial neural networks in cryptosystems. In Proceedings of the World Automation Congress, Waikoloa, HI, USA, 28 September–2 October 2008.
30. Hu, D.; Wang, Y. Security Research on WiMAX with Neural Cryptography. In Proceedings of the International Conference on Information Security and Assurance, Busan, Korea, 24–26 April 2008.
31. Hadke, P.P.; Kale, S.G. Use of Neural Networks in cryptography: A review. In Proceedings of the World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, India, 29 February–1 March 2016.
32. Sharma, A.; Sharma, D. Big data protection via neural and quantum cryptography. In Proceedings of the 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 16–18 March 2016.
33. ÖzÇakmak, B.; Özbİlen, A.; YavanoĞlu, U.; CİN, K. Neural and Quantum Cryptography in Big Data: A Review. In Proceedings of the IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019.
34. Su, J.; Kankani, A.; Zajko, G.; Elchouemi, A.; Kurniawan, H. Review of Image encryption techniques using neural network for optical security in the healthcare sector—PNO System. In Proceedings of the 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA), Sydney, Australia, 25–27 November 2020.
35. Meraouche, I.; Dutta, S.; Tan, H.; Sakurai, K. Neural Networks-Based Cryptography: A Survey. *IEEE Access* **2021**, *9*, 124727–24740. [CrossRef]
36. Wright, J.L.; Manic, M. Neural network architecture selection analysis with application to cryptography location. In Proceedings of the International Joint Conference on Neural Networks (IJCNN), Barcelona, Spain, 18–23 July 2010.
37. Jia, L.; Zhou, A.; Jia, P.; Liu, L.; Wang, Y.; Liu, L. A Neural Network-Based Approach for Cryptographic Function Detection in Malware. *IEEE Access* **2020**, *8*, 23506–23521. [CrossRef]
38. Wright, J.L.; Manic, M. Neural network approach to locating cryptography in object code. In Proceedings of the IEEE Conference on Emerging Technologies & Factory Automation, Palma de Mallorca, Spain, 22–25 September 2009.
39. Miller, S.; Curran, K.; Lunney, T. Multilayer perceptron neural network for detection of encrypted VPN network traffic. In Proceedings of the International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Glasgow, UK, 11–12 June 2018.
40. Yu, T.; Zou, F.; Li, L.; Yi, P. An encrypted malicious traffic detection system based on neural network. In Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Guilin, China, 17–19 October 2019.
41. Apolinario, J.; Mendonca, P.; Chaves, R.; Caloba, L. Cryptanalysis of speech signals ciphered by TSP using annealed Hopfield neural network and genetic algorithms. In Proceedings of the 39th Midwest Symposium on Circuits and Systems, Ames, IA, USA, 18–21 August 1996.
42. Ruzhentsev, V.; Levchenko, R.; Fediushyn, O. Cryptanalysis of Simple Substitution-Permutation Cipher Using Artificial Neural Network. In Proceedings of the IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 6–9 October 2020.
43. Albassal, A.; Wahdan, A.M. Neural network based cryptanalysis of a feistel type block cipher. In Proceedings of the International Conference on Electrical, Electronic and Computer Engineering, Cairo, Egypt, 5–7 September 2004.
44. Danziger, M.; Henriques, M.A.A. Improved cryptanalysis combining differential and artificial neural network schemes. In Proceedings of the International Telecommunications Symposium (ITS), Sao Paulo, Brazil, 17–20 August 2014.
45. Xiao, Y.; Hao, Q.; Yao, D.D. Neural cryptanalysis: Metrics, methodology, and applications in CPS ciphers. In Proceedings of the IEEE Conference on Dependable and Secure Computing (DSC), Hangzhou, China, 18–20 November 2019.
46. Khan, A.N.; Fan, M.Y.; Malik, A.; Husain, M.A. Cryptanalyzing merkle-hellman public key cryptosystem with artificial neural networks. In Proceedings of the IEEE 5th International Conference for Convergence in Technology (I2CT), Pune, India, 28–31 March 2019.
47. Hsiao, F.H.; Hsieh, K.P.; Lin, Z.H. Exponential optimal synchronization of chaotic cryptosystems: Neural-network-based approach. In Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Shanghai, China, 10–12 October 2014.
48. Oun, A.; Niamat, M. Defense mechanism vulnerability analysis of ring oscillator PUFs against neural network modeling attacks using the dragonfly algorithm. In Proceedings of the IEEE International Conference on Electro Information Technology (EIT), Chicago, IL, USA, 31 July–1 August 2020.
49. Arvandi, M.; Sadeghian, A. Chosen Plaintext attack against neural network-based symmetric cipher. In Proceedings of the International Joint Conference on Neural Networks, Orlando, FL, USA, 12–17 August 2007.
50. Awano, H.; Iizuka, T.; Ikeda, M. PUFNet: A deep neural network based modeling attack for physically unclonable function. In Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), Sapporo, Japan, 26–29 May 2019.
51. Xu, R.; Joshi, J.; Li, C. NN-EMD: Efficiently Training Neural Networks using Encrypted Multi-sourced Datasets. *IEEE Trans. Dependable Secur. Comput.* **2021**, *in press*. [CrossRef]
52. Xu, R.; Joshi, J.B.; Li, C. CryptoNN: Training neural networks over encrypted data. In Proceedings of the IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–10 July 2019.
53. Molek, V.; Hurtik, P. Training neural network over encrypted data. In Proceedings of the IEEE Third International Conference on Data Stream Mining & Processing (DSMP), Lviv, Ukraine, 21–25 August 2020.

54. Nandakumar, K.; Ratha, N.; Pankanti, S.; Halevi, S. Towards deep neural network training on encrypted data. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Long Beach, CA, USA, 16–17 June 2019.
55. Bazuhair, W.; Lee, W. Detecting malign encrypted network traffic using perlin noise and convolutional neural network. In Proceedings of the 10th Annual Computing and Communication Workshop and Conference (CCWC), Vegas, NV, USA, 6–8 January 2020.
56. Shen, M.; Zhang, J.; Zhu, L.; Xu, K.; Du, X. Accurate Decentralized Application Identification via Encrypted Traffic Analysis Using Graph Neural Networks. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 2367–2380. [CrossRef]
57. Wang, X.; Chen, S.; Su, J. Automatic Mobile App Identification From Encrypted Traffic With Hybrid Neural Networks. *IEEE Access* **2020**, *8*, 182065–182077. [CrossRef]
58. Zhang, Y.; Zhao, S.; Zhang, J.; Ma, X.; Huang, F. STNN: A novel TLS/SSL encrypted traffic classification system based on stereo transform neural network. In Proceedings of the IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS), Tianjin, China, 4–6 December 2019.
59. Yang, J.; Narantuya, J.; Lim, H. Bayesian neural network based encrypted traffic classification using initial handshake packets. In Proceedings of the 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks—Supplemental Volume (DSN-S), Valencia, Spain, 29 June–2 July 2019.
60. Zhou, Y.; Cui, J. Research and improvement of encrypted traffic classification based on convolutional neural network. In Proceedings of the IEEE 8th International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, 20–22 November 2020.
61. Song, M.; Ran, J.; Li, S. Encrypted traffic classification based on text convolution neural networks. In Proceedings of the IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, 19–20 October 2019.
62. Zou, Z.; Ge, J.; Zheng, H.; Wu, Y.; Han, C.; Yao, Z. Encrypted traffic classification with a convolutional long short-term memory neural network. In Proceedings of the IEEE 20th International Conference on High Performance Computing and Communications and IEEE 16th International Conference on Smart City and IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Exeter, UK, 28–30 June 2018.
63. He, Y.; Li, W. Image-based encrypted traffic classification with convolution neural networks. In Proceedings of the IEEE Fifth International Conference on Data Science in Cyberspace (DSC), Hong Kong, China, 27–29 July 2020.
64. Wang, X.; Chen, S.; Su, J. App-net: A hybrid neural network for encrypted mobile traffic classification. In Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020.
65. Wang, W.; Zhu, M.; Wang, J.; Zeng, X.; Yang, Z. End-to-end encrypted traffic classification with one-dimensional convolution neural networks. In Proceedings of the IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, China, 22–24 July 2017.
66. Cheng, J.; He, R.; Yuepeng, E.; Wu, Y.; You, J.; Li, T. Real-Time encrypted traffic classification via lightweight neural networks. In Proceedings of the IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020.
67. Cui, S.; Jiang, B.; Cai, Z.; Lu, Z.; Liu, S.; Liu, J. A session-packets-based encrypted traffic classification using capsule neural networks. In Proceedings of the IEEE 21st International Conference on High Performance Computing and Communications and IEEE 17th International Conference on Smart City and IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Zhangjiajie, China, 10–12 August 2019.
68. Yang, Y.; Kang, C.; Gou, G.; Li, Z.; Xiong, G. TLS/SSL encrypted traffic classification with autoencoder and convolutional neural network. In Proceedings of the IEEE 20th International Conference on High Performance Computing and Communications and IEEE 16th International Conference on Smart City and IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Exeter, UK, 28–30 June 2018.
69. Wang, M.; Zheng, K.; Luo, D.; Yang, Y.; Wang, X. An encrypted traffic classification framework based on convolutional neural networks and stacked autoencoders. In Proceedings of the IEEE 6th International Conference on Computer and Communications (ICCC), Chengdu, China, 11–14 December 2020.
70. Lidkea, V.M.; Muresan, R.; Al-Dweik, A. Convolutional Neural Network Framework for Encrypted Image Classification in Cloud-Based ITS. *IEEE Open J. Intell. Transp. Syst.* **2020**, *1*, 35–50. [CrossRef]
71. Zhang, Q.; Zhao, X.; Hu, Y. A Classification Retrieval Method for Encrypted Speech Based on Deep Neural Network and Deep Hashing. *IEEE Access* **2020**, *8*, 202469–202482. [CrossRef]
72. Yang, K.; Xu, L.; Xu, Y.; Chao, J. Encrypted application classification with convolutional neural network. In Proceedings of the IFIP Networking Conference (Networking), Paris, France, 22–26 June 2020.
73. Shortt, A.E.; Naughton, T.J.; Javidi, B. Compression of Optically Encrypted Digital Holograms Using Artificial Neural Networks. *J. Disp. Technol.* **2006**, *2*, 401–410. [CrossRef]
74. Fezza, S.A.; Keita, M.; Hamidouche, W. Visual quality and security assessment of perceptually encrypted images based on multi-output deep neural network. In Proceedings of the 9th European Workshop on Visual Information Processing (EUVIP), Paris, France, 23–25 June 2021.
75. Novotný, J.K. WTFHE: Neural-network-ready torus fully homomorphic encryption. In Proceedings of the 9th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 8–11 June 2020.

76. Ghimes, A.M.; Vladuta, V.A.; Patriciu, V.V.; Ioniţă, A. Applying neural network approach to homomorphic encrypted data. In Proceedings of the 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, 28–30 June 2018.
77. Meftah, S.; Tan, B.H.M.; Mun, C.F.; Aung, K.M.M.; Veeravalli, B.; Chandrasekhar, V. DOReN: Toward Efficient Deep Convolutional Neural Networks with Fully Homomorphic Encryption. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 3740–752. [CrossRef]
78. Zhou, J.; Li, J.; Panaousis, E.; Liang, K. Deep binarized convolutional neural network inferences over encrypted data. In Proceedings of the 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), New York, NY, USA, 1–3 August 2020.
79. Ma, Y.; Wu, L.; Gu, X.; He, J.; Yang, Z. A Secure Face-Verification Scheme Based on Homomorphic Encryption and Deep Neural Networks. *IEEE Access* **2017**, *5*, 16532–16538. [CrossRef]
80. Gaid, M.L.; Fakhr, M.W.; Selim, G.I. Secure translation using fully homomorphic encryption and sequence-to-sequence neural networks. In Proceedings of the 28th International Conference on Computer Theory and Applications (ICCTA), Alexandria, Egypt, 30 October–1 November 2018.
81. Kim, T.; Youn, T.Y.; Choi, D. Deep Neural Networks Based Key Concealment Scheme. *IEEE Access* **2020**, *8*, 204214–204225. [CrossRef]
82. Allam, A.M.; Abbas, H.M. Group key exchange using neural cryptography with binary trees. In Proceedings of the 24th Canadian Conference on Electrical and Computer Engineering (CCECE), Niagara Falls, ON, Canada, 8–11 May 2011.
83. Guerreiro, A.M.G.; de Araujo, C.P. A Neural Key Generator for a Public Block Cipher. In Proceedings of the Ninth Brazilian Symposium on Neural Networks, Ribeirao Preto, Brazil, 26–27 October 2006.
84. Jin, J.; Kim, K. 3D CUBE Algorithm for the Key Generation Method: Applying Deep Neural Network Learning-Based. *IEEE Access* **2020**, *8*, 33689–33702. [CrossRef]
85. Sarkar, A.; Singh, M.M.; Khan, M.Z.; Alhazmi, O.H. Nature-Inspired Gravitational Search-Guided Artificial Neural Key Exchange for IoT Security Enhancement. *IEEE Access* **2021**, *9*, 76780–76795. [CrossRef]
86. Kimura, H.; Isobe, T.; Ohigashi, T. Neural-Network-Based Pseudo-Random Number Generator Evaluation Tool for Stream Ciphers. In Proceedings of the Seventh International Symposium on Computing and Networking Workshops (CANDARW), Nagasaki, Japan, 26–29 November 2019.
87. Saraswat, P.; Garg, K.; Tripathi, R.; Agarwal, A. Encryption algorithm based on neural network. In Proceedings of the 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 18–19 April 2019.
88. Munukur, R.K.; Gnanam, V. Neural network based decryption for random encryption algorithms. In Proceedings of the 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication, Hong Kong, China, 20–22 August 2009.
89. Kinzel, W.; Kanter, I. Neural cryptography. In Proceedings of the 9th International Conference on Neural Information Processing, Vancouver, BC, Canada, 9–14 December 2002.
90. Liu, C.Y.; Woungang, I.; Chao, H.C.; Dhurandher, S.K.; Chi, T.Y.; Obaidat, M.S. Message security in multi-path ad hoc networks using a neural network-based cipher. In Proceedings of the IEEE Global Telecommunications Conference—GLOBECOM, Houston, TX, USA, 5–9 Decmber 2011.
91. Tsmots, I.; Rabyk, V.; Lukaschuk, Y.; Teslyuk, V.; Liubun, Z. Neural Network Technology for Protecting Cryptographic Data. In Proceedings of the IEEE 12th International Conference on Electronics and Information Technologies (ELIT), Lviv, Ukraine, 19–21 May 2021.
92. Hu, D. A New Service-Based Computing Security Model with Neural Cryptography. In Proceedings of the Second Pacific-Asia Conference on Web Mining and Web-based Application, Wuhan, China, 6–7 June 2009.
93. Forgáč, R.; Očkay, M. Contribution to symmetric cryptography by convolutional neural networks. In Proceedings of the Communication and Information Technologies (KIT), Vysoke Tatry, Slovakia, 9–11 October 2019.
94. Noura, H.; Samhat, A.E.; Harkouss, Y.; Yahiya, T.A. Design and realization of a new neural block cipher. In Proceedings of the International Conference on Applied Research in Computer Science and Engineering, Beirut, Lebanon, 8–9 October 2015.
95. Rabyk, V.; Tsmots, I.; Lyubun, Z.; Skorokhoda, O. Method and means of symmetric real-time neural network data encryption. In Proceedings of the IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT), Zbarazh, Ukraine, 23–26 September 2020.
96. Liu, L.; Zhang, L.; Jiang, D.; Guan, Y.; Zhang, Z. A Simultaneous Scrambling and Diffusion Color Image Encryption Algorithm Based on Hopfield Chaotic Neural Network. *IEEE Access* **2019**, *7*, 185796–185810. [CrossRef]
97. Zhou, S. Image encryption technology research based on neural network. In Proceedings of the International Conference on Intelligent Transportation, Big Data and Smart City, Halong Bay, Vietnam, 19–20 December 2015.
98. Hu, G.; Kou, W.; Dong, J.; Peng, J. A novel image encryption algorithm based on cellular neural networks hyper chaotic system. In Proceedings of the IEEE 4th International Conference on Computer and Communications (ICCC), Chengdu, China, 7–10 December 2018.
99. Joshi, S.D.; Udupi, V.R.; Joshi, D.R. A novel neural network approach for digital image data encryption/decryption. In Proceedings of the International Conference on Power, Signals, Controls and Computation, Thrissur, India, 3–6 January 2012.
100. Kumar, S.; Aid, R. Image encryption using wavelet based chaotic neural network. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, India, 21–24 September 2016.

101. Fadil, T.A.; Yaakob, S.N.; Ahmad, B. A hybrid chaos and neural network cipher encryption algorithm for compressed video signal transmission over wireless channel. In Proceedings of the 2nd International Conference on Electronic Design (ICED), Penang, Malaysia, 19–21 August 2014.
102. Gaffar, A.F.O.; Putra, A.B.W.; Malani, R. The Multi Layer Auto Encoder Neural Network (ML-AENN) for Encryption and Decryption of Text Message. In Proceedings of the 5th International Conference on Science in Information Technology (ICSITech), Jogjakarta, Indonesia, 23–24 October 2019.
103. Wang, H.; Lursinsap, C. Neural Cryptosystem for Textual Message with Plasticity and Secret Dimensions. In Proceedings of the 18th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Chiang Mai, Thailand, 19–22 May 2021.
104. Roy, S.S.; Shahriyar, S.A.; Asaf-Uddowla, M.; Alam, K.M.R.; Morimoto, Y. A novel encryption model for text messages using delayed chaotic neural network and DNA cryptography. In Proceedings of the 20th International Conference of Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 22–24 December 2017.
105. Hu, D.; Lao, H. Privacy research on ubicomp computing with neural cryptography. In Proceedings of the 3rd International Conference on Grid and Pervasive Computing—Workshops, Kunming, China, 25–28 May 2008.
106. Hu, D.; Wang, Y. Secure Authentication on WiMAX with Neural Cryptography. In Proceedings of the International Conference on Information Security and Assurance, Busan, Korea, 24–26 April 2008.
107. Allam, A.M.; Abbas, H.M.; El-Kharashi, M.W. Authenticated key exchange protocol using neural cryptography with secret boundaries. In Proceedings of the International Joint Conference on Neural Networks (IJCNN), Dallas, TX, USA, 4–9 August 2013.
108. Firmino, M.; Brandão, G.B.; Guerreiro, A.M.G.; de Valentim, R.A.M. Neural cryptography applied to key management protocol with mutual authentication in RFID systems. In Proceedings of the International Conference for Internet Technology and Secured Transactions, London, UK, 9–12 November 2009.
109. Arora, A.; Miri, R. Taylor-Grey Rider based Deep Recurrent Neural Network using Feature Level Fusion for Cryptography Enabled Biometric System. In Proceedings of the 3rd International Conference on Intelligent Sustainable Systems (ICISS), Palladam, India, 3–5 December 2020.
110. Duan, X.; Guo, D.; Liu, N.; Li, B.; Gou, M.; Qin, C. A New High Capacity Image Steganography Method Combined With Image Elliptic Curve Cryptography and Deep Neural Network. *IEEE Access* **2020**, *8*, 25777–25788. [CrossRef]
111. Petkov, T.; Sotirova, E.; Ahmed, S.; Sotirov, S. Encrypting message in a sound using self organizing map neural network described by a generalized net. In Proceedings of the IEEE 8th International Conference on Intelligent Systems (IS), Sofia, Bulgaria, 4–6 September 2016.
112. Petkov, T.; Panayotova, K.; Sotirov, S. Generalized net model of encrypting message in an image using self organizing map neural network. In Proceedings of the 19th International Symposium on Electrical Apparatus and Technologies (SIELA), Bourgas, Bulgaria, 29 May–1 June 2016.
113. Wang, Y.; Li, Y.; Lu, X.N. Evaluation criteria for visual cryptography schemes via neural networks. In Proceedings of the International Conference on Cyberworlds (CW), Caen, France, 29 September–1 October 2020.
114. Yue, T.W.; Chiang, S. A neural network approach for visual cryptography. In Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks—IJCNN 2000—Neural Computing: New Challenges and Perspectives for the New Millennium, Como, Italy, 27 July 2000.
115. Yue, T.W.; Chiang, S. A known-energy neural network approach for visual cryptography. In Proceedings of the International Joint Conference on Neural Networks, Washington, DC, USA, 15–19 July 2001.
116. Ge, S.; Changgen, P.; Xuelan, M. Visual cryptography scheme using pi-sigma neural networks. In Proceedings of the International Symposium on Information Science and Engineering, Shanghai, China, 20–22 December 2008.
117. Hu, D. Secure mobile network handover with neural cryptography. In Proceedings of the International Symposium on Communications and Information Technologies, Sydney, Australia, 17–19 October 2007.
118. Mandal, J.K.; Sarkar, A. An adaptive neural network guided random block length based cryptosystem for online wireless communication (ANNRBLC). In Proceedings of the International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), Chennai, India, 28 February–3 March 2011.
119. Karas, D.S.; Karagiannidis, G.K.; Schober, R. Neural network based PHY-layer key exchange for wireless communications. In Proceedings of the IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications, Toronto, ON, Canada, 11–14 September 2011.
120. Sun, Y.; Lo, F.P.W.; Lo, B. Light-weight Internet-of-Things Device Authentication, Encryption and Key Distribution using End-to-End Neural Cryptosystems. *IEEE Internet Things J.* **2021**, *in press*. [CrossRef]
121. Ismail, I.A.; Galal-Edeen, G.H.; Khattab, S.; Bahtity, M.A.E.M.E. Satellite image encryption using neural networks backpropagation. In Proceedings of the 22nd International Conference on Computer Theory and Applications (ICCTA), Alexandria, Egypt, 13–15 October 2012.
122. Yelina, T.N.; Bezzateev, S.V.; Mylnikov, V.A. The homomorphic encryption in pipelines accident prediction by using cloud-based neural network. In Proceedings of the Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), Saint-Petersburg, Russia, 3–7 June 2019.
123. Thoms, G.R.W.; Muresan, R.; Al-Dweik, A. Chaotic Encryption Algorithm With Key Controlled Neural Networks for Intelligent Transportation Systems. *IEEE Access* **2019**, *7*, 158697–158709. [CrossRef]

124. Kumar, C.N.S.V.; Suhasini, A. Improved secure three-tier architecture for WSN using hopfield chaotic neural network with two stage encryption. In Proceedings of the International Conference on Computer, Electrical & Communication Engineering (ICCECE), Kolkata, India, 16–17 December 2016.
125. Bi, M.; Zhuo, X.; Fu, X.; Yang, X.; Hu, W. Cellular Neural Network Encryption Scheme for Time Synchronization and CPAs Resistance in OFDM-PON. *IEEE Access* **2019**, *7*, 57129–57137. [CrossRef]
126. Zhou, Y.; Bi, M.; Zhuo, X.; Lv, Y.; Yang, X.; Hu, W. Physical Layer Dynamic Key Encryption in OFDM-PON System Based on Cellular Neural Network. *IEEE Photonics J.* **2021**, *13*, 7200314. [CrossRef]
127. Preethi, P.; Asokan, R. Neural Network oriented RONI prediction for embedding process with hex code encryption in DICOM images. In Proceedings of the 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, 18–19 December 2020.
128. Han, B.; Jia, Y.; Huang, G.; Cai, L. A medical image encryption algorithm based on hermite chaotic neural network. In Proceedings of the IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 12–14 June 2020.
129. Zhu, Y.; Vargas, D.V.; Sakurai, K. Neural cryptography based on the topology evolving neural networks. In Proceedings of the Sixth International Symposium on Computing and Networking Workshops (CANDARW), Takayama, Japan, 27–30 November 2018.
130. Dong, T.; Huang, T. Neural Cryptography Based on Complex-Valued Neural Network. *IEEE Trans. Neural Netw. Learn. Syst.* **2020**, *31*, 4999–5004. [CrossRef]
131. Wang, J.; Cheng, L.M.; Su, T. Multivariate Cryptography Based on Clipped Hopfield Neural Network. *IEEE Trans. Neural Netw. Learn. Syst.* **2018**, *29*, 353–363. [CrossRef]
132. Srivastava, S.; Bhatia, A. On the learning capabilities of recurrent neural networks: A cryptographic perspective. In Proceedings of the IEEE International Conference on Big Knowledge (ICBK), Singapore, 17 November 2018.
133. Zhou, K.; Kang, Y.; Huang, Y.; Feng, E. Encrypting algorithm based on RBF neural network. In Proceedings of the Third International Conference on Natural Computation, Haikou, China, 24–27 October 2007.
134. Fei, X.; Liu, G.; Zheng, B. A chaotic encryption system using PCA neural networks. In Proceedings of the IEEE Conference on Cybernetics and Intelligent Systems, Chengdu, China, 21–24 September 2008.
135. Lin, J.; Luo, Y.; Liu, J.; Bi, J.; Qiu, S.; Cen, M.; Liao, Z. An image compression-encryption algorithm based on cellular neural network and compressive sensing. In Proceedings of the IEEE 3rd International Conference on Image, Vision and Computing (ICIVC), Chongqing, China, 27–29 June 2018.
136. Yang, F.; Mou, J.; Cao, Y.; Chu, R. An image encryption algorithm based on BP neural network and hyperchaotic system. *China Commun.* **2020**, *17*, 21–28. [CrossRef]
137. Li, H.; Li, C.; Ouyang, D.; Nguang, S.K. Impulsive synchronization of unbounded delayed inertial neural networks with actuator saturation and sampled-data control and its application to image encryption. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**, *32*, 1460–1473. [CrossRef]
138. Xiao, J.; Wang, W.; Wang, M. Image encryption algorithm based on memristive BAM neural networks. In Proceedings of the IEEE Third International Conference on Data Science in Cyberspace (DSC), Guangzhou, China, 18–21 June 2018.
139. Arvandi, M.; Wu, S.; Sadeghian, A.; Melek, W.; Woungang, I. Symmetric cipher design using recurrent neural networks. In Proceedings of the IEEE International Joint Conference on Neural Network, Vancouver, BC, Canada, 16–21 July 2006.
140. Arvandi, M.; Wu, S.; Sadeghian, A. On the use of recurrent neural networks to design symmetric ciphers. *IEEE Comput. Intell. Mag.* **2008**, *3*, 42–53. [CrossRef]
141. Feizi, S.; Nemati, A.; Haghiri, S.; Ahmadi, A.; Seif, M. Digital hardware implementation of lightweight cryptography algorithm using neural networks. In Proceedings of the 28th Iranian Conference on Electrical Engineering (ICEE), Tabriz, Iran, 4–6 August 2020.
142. Santiago, L.; Patil, V.C.; Prado, C.B.; Alves, T.A.O.; Marzulo, L.A.J.; França, F.M.G.; Kundu, S. Realizing strong PUF from weak PUF via neural computing. In Proceedings of the IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Cambridge, UK, 23–25 October 2017.
143. Takalo, H.; Ahmadi, A.; Mirhassani, M.; Ahmadi, M. Analog cellular neural network for application in physical unclonable functions. In Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), Montreal, QC, Canada, 22–25 May 2016.
144. Addabbo, T.; Fort, A.; Marco, M.D.; Pancioni, L.; Vignoli, V. Physically Unclonable Functions Derived From Cellular Neural Networks. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2013**, *60*, 3205–3214. [CrossRef]
145. Alimohammadi, N.; Shokouhi, S.B. Secure hardware key based on physically unclonable functions and artificial neural network. In Proceedings of the 8th International Symposium on Telecommunications (IST), Tehran, Iran, 27–28 September 2016.
146. Shibagaki, K.; Umeda, T.; Nozaki, Y.; Yoshikawa, M. Feasibility evaluation of neural network physical unclonable function. In Proceedings of the IEEE 7th Global Conference on Consumer Electronics (GCCE), Nara, Japan, 9–12 October 2018.
147. Mislovaty, R.; Klein, E.; Kanter, I.; Kinzel, W. Security of neural cryptography. In Proceedings of the 11th IEEE International Conference on Electronics, Circuits and Systems, Tel Aviv, Israel, 13–15 December 2004.

148. Stöttinger, M.; Huss, S.A.; Mühlbach, S.; Koch, A. Side-channel resistance evaluation of a neural network based lightweight cryptography scheme. In Proceedings of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Hong Kong, China, 11–13 December 2010.
149. Liu, N.; Guo, D. Security analysis of public-key encryption scheme based on neural networks and its implementing. In Proceedings of the International Conference on Computational Intelligence and Security, Chengdu, China, 19–21 November 2006.
150. Allam, A.M.; Abbas, H.M.; El-Kharashi, M.W. Security analysis of neural cryptography implementation. In Proceedings of the IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), Victoria, BC, Canada, 27–29 August 2013.
151. Tan, X.; Xiang, C.; Cao, J.; Xu, W.; Wen, G.; Rutkowski, L. Synchronization of Neural Networks via Periodic Self-Triggered Impulsive Control and Its Application in Image Encryption. *IEEE Trans. Cybern.* **2021**, *in press*. [CrossRef] [PubMed]
152. Zang, H.; Min, L. Generalized synchronization theorems for a kind of Neural Network with application in data encryption. In Proceedings of the 3rd IEEE Conference on Industrial Electronics and Applications, Singapore, 3–5 June 2008.
153. Wen, S.; Zeng, Z.; Huang, T.; Meng, Q.; Yao, W. Lag Synchronization of Switched Neural Networks via Neural Activation Function and Applications in Image Encryption. *IEEE Trans. Neural Netw. Learn. Syst.* **2015**, *26*, 1493–1502. [CrossRef] [PubMed]
154. Chen, W.H.; Luo, S.; Zheng, W.X. Impulsive Synchronization of Reaction–Diffusion Neural Networks With Mixed Delays and Its Application to Image Encryption. *IEEE Trans. Neural Netw. Learn. Syst.* **2016**, *27*, 2696–2710. [CrossRef]
155. Zhang, X.; Sheng, S.; Lu, G.; Zheng, Y. Synchronization for arrays of coupled jumping delayed neural networks and its application to image encryption. In Proceedings of the IEEE 56th Annual Conference on Decision and Control (CDC), Melbourne, Australia, 12–15 December 2017.
156. Wang, W.; Wang, X.; Luo, X.; Yuan, M. Finite-Time Projective Synchronization of Memristor-Based BAM Neural Networks and Applications in Image Encryption. *IEEE Access* **2018**, *6*, 56457–56476. [CrossRef]
157. Wang, W.; Yu, X.; Luo, X.; Kurths, J. Finite-Time Synchronization of Chaotic Memristive Multidirectional Associative Memory Neural Networks and Applications in Image Encryption. *IEEE Access* **2018**, *6*, 35764–35779. [CrossRef]
158. Zou, A.; Xiao, X. An asynchronous encryption arithmetic based on laguerre chaotic neural networks. In Proceedings of the WRI Global Congress on Intelligent Systems, Xiamen, China, 19–21 May 2009.
159. Chaos. Available online: https://mathworld.wolfram.com/Chaos.html (accessed on 18 May 2022).
160. Bharadwaj, G.V.S.E.; Vijaya, K.; Balaga, S.K.; Thanikaiselvan, V. Image encryption based on neural network architecture and chaotic systems. In Proceedings of the Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 29–31 March 2018.
161. de Almeida Ramos, E.; Filho, J.C.B.; Reis, R. Cryptography by synchronization of hopfield neural networks that simulate chaotic signals generated by the human body. In Proceedings of the 17th IEEE International New Circuits and Systems Conference (NEWCAS), Munich, Germany, 23–26 June 2019.
162. Chatzidakis, S.; Forsberg, P.; Tsoukalas, L.H. Chaotic neural networks for intelligent signal encryption. In Proceedings of the 5th International Conference on Information, Intelligence, Systems and Applications, Chania, Greece, 7–9 July 2014.
163. Su, S.; Lin, A.; Yen, J.C. Design and realization of a new chaotic neural encryption/decryption network. In Proceedings of the IEEE Asia-Pacific Conference on Circuits and Systems. Electronic Communication Systems. (Cat. No.00EX394), Tianjin, China, 4–6 December 2000.
164. Dogaru, R.; Murgan, A.; Ioan, D. Chains of discrete-time chaotic neural networks for generation of broadband signals with applications in improved ciphering systems. In Proceedings of the 8th Mediterranean Electrotechnical Conference on Industrial Applications in Power Systems, Computer Science and Telecommunications, Bari, Italy, 16 May 1996.
165. Singla, P.; Sachdeva, P.; Ahmad, M. A chaotic neural network based cryptographic pseudo-random sequence design. In Proceedings of the Fourth International Conference on Advanced Computing & Communication Technologies, Rohtak, India, 8–9 February 2014.
166. Lokesh, S.; Kounte, M.R. Chaotic neural network based pseudo-random sequence generator for cryptographic applications. In Proceedings of the International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Davangere, India, 29–31 October 2015.
167. Zhang, Y.; Xue, T.; Zhai, Z.; Ma, C.; Cai, X. The improvement of public key cryptography based on chaotic neural networks. In Proceedings of the Eighth International Conference on Intelligent Systems Design and Applications, Kaohsiung, Taiwan, 26–28 November 2008.
168. Ahmad, M.; Malik, M. Design of chaotic neural network based method for cryptographic substitution box. In Proceedings of the International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 3–5 March 2016.
169. Skovajsová, L. Comparison of cryptography by chaotic neural network and by AES. In Proceedings of the IEEE 19th International Symposium on Computational Intelligence and Informatics and 7th IEEE International Conference on Recent Achievements in Mechatronics, Automation, Computer Sciences and Robotics (CINTI-MACRo), Szeged, Hungary, 14–16 November 2019.
170. Mandal, J.K.; Sarkar, A. An adaptive genetic key based neural encryption for online wireless communication (AGKNE). In Proceedings of the International Conference on Recent Trends in Information Systems, Kolkata, India, 21–23 December 2011.
171. Sagar, V.; Kumar, K. A symmetric key cryptography using genetic algorithm and error back propagation neural network. In Proceedings of the 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 11–13 March 2015.

172. Kalaiselvi, K.; Kumar, A. Enhanced AES cryptosystem by using genetic algorithm and neural network in S-box. In Proceedings of the IEEE International Conference on Current Trends in Advanced Computing (ICCTAC), Bangalore, India, 10–11 March 2016.
173. Jhajharia, S.; Mishra, S.; Bali, S. Public key cryptography using neural networks and genetic algorithms. In Proceedings of the Sixth International Conference on Contemporary Computing (IC3), Noida, India, 8–10 August 2013.
174. Checksum and Cyclic Redundancy Check Mechanism. Available online: https://link.springer.com/referenceworkentry/10.1007/978-0-387-39940-9_1474 (accessed on 18 May 2022).
175. Allam, A.M.; Abbas, H.M. Improved security of neural cryptography using don't-trust-my-partner and error prediction. In Proceedings of the International Joint Conference on Neural Networks, Atlanta, GA, USA, 14–19 June 2009.
176. Allam, A.M.; Abbas, H.M. On the Improvement of Neural Cryptography Using Erroneous Transmitted Information with Error Prediction. *IEEE Trans. Neural Netw.* **2011**, *21*, 1915–1924. [CrossRef]
177. Fourier Transform. Available online: https://docs.opencv.org/3.4/de/dbc/tutorial_py_fourier_transform.html (accessed on 18 May 2022).
178. Ashtiyani, M.; Behbahani, S.; Asadi, S.; Birgani, P.M. Transmitting Encrypted Data by Wavelet Transform and Neural Network. In Proceedings of the IEEE International Symposium on Signal Processing and Information Technology, Giza, Egypt, 15–18 December 2007.
179. What Is a Blockchain? Available online: https://www.investopedia.com/terms/b/blockchain.asp (accessed on 18 May 2022).
180. Noh, S.; Rhee, K.H. Implicit authentication in neural key exchange based on the randomization of the Public Blockchain. In Proceedings of the IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2–6 November 2020.
181. Combinatorics. Available online: https://www.cs.uleth.ca/~morris/Combinatorics/Combinatorics.pdf (accessed on 18 May 2022).
182. Lin, M.; Long, F.; Guo, L. Grayscale image encryption based on Latin square and cellular neural network. In Proceedings of the Chinese Control and Decision Conference (CCDC), Yinchuan, China, 28–30 May 2016.
183. Lytvyn, V.; Peleshchak, I.; Peleshchak, R.; Vysotska, V. Information encryption based on the synthesis of a neural network and AES algorithm. In Proceedings of the 3rd International Conference on Advanced Information and Communications Technologies (AICT), Lviv, Ukraine, 2–6 July 2019.
184. Husein, A.M.; Harahap, M.; Dharma, A.; Simarmata, A.M. Hybrid-AES-Blowfish algorithm: Key exchange using neural network. In Proceedings of the International Conference of Computer Science and Information Technology (ICoSNIKOM), Medan, Indonesia, 28–29 November 2019.
185. Liu, Y.; Zhang, J.; Tang, W. Noise removal using Cohen-Grossberg neural network for improving the quality of the decrypted image in color encryption. In Proceedings of the IEEE 3rd International Conference on Communication Software and Networks, Xi'an, China, 27–29 May 2011.
186. Tsmots, I.; Tsymbal, Y.; Skorokhoda, O.; Tkachenko, R. Neural-like methods and hardware structures for real-time data encryption and decryption. In Proceedings of the IEEE 14th International Conference on Computer Sciences and Information Technologies (CSIT), Lviv, Ukraine, 17–20 September 2019.
187. Li, H.; Han, T. An end-to-end encrypted neural network for gradient updates transmission in federated learning. In Proceedings of the Data Compression Conference (DCC), Snowbird, UT, USA, 26–29 March 2019.
188. Choi, Y.; Sim, J.; Kim, L.S. CREMON: Cryptography Embedded on the Convolutional Neural Network Accelerator. *IEEE Trans. Circuits Syst. II Express Briefs* **2020**, *67*, 3337–3341. [CrossRef]
189. Emmanuel, A.B.; Zhou, S.; Liao, Y.; Liu, Q. Privacy-preservation in distributed deep neural networks via encryption of selected gradients. In Proceedings of the IEEE 22nd International Conference on High Performance Computing and Communications and IEEE 18th International Conference on Smart City and IEEE 6th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Cuvu, Fiji, 14–16 December 2020.
190. Cai, Y.; Chen, X.; Tian, L.; Wang, Y.; Yang, H. Enabling secure in-memory neural network computing by sparse fast gradient encryption. In Proceedings of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Austin, TX, USA, 2–6 November 2019.
191. Cai, Y.; Chen, X.; Tian, L.; Wang, Y.; Yang, H. Enabling Secure NVM-Based in-Memory Neural Network Computing by Sparse Fast Gradient Encryption. *IEEE Trans. Comput.* **2020**, *69*, 1596–1610. [CrossRef]
192. Cantoro, R.; Deligiannis, N.I.; Reorda, M.S.; Traiola, M.; Valea, E. Evaluating data encryption effects on the resilience of an artificial neural network. In Proceedings of the IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Frascati, Italy, 19–21 October 2020.
193. Hu, X.; Tian, J.; Wang, Z. Fast permutation architecture on encrypted data for secure neural network inference. In Proceedings of the IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Ha Long, Vietnam, 8–10 December 2020.
194. Sirichotedumrong, W.; Maekawa, T.; Kinoshita, Y.; Kiya, H. Privacy-preserving deep neural networks with pixel-based image encryption considering data augmentation in the encrypted domain. In Proceedings of the IEEE International Conference on Image Processing (ICIP), Taipei, Taiwan, 22–25 September 2019.
195. Sirichotedumrong, W.; Kinoshita, Y.; Kiya, H. On the security of pixel-based image encryption for privacy-preserving deep neural networks. In Proceedings of the IEEE 8th Global Conference on Consumer Electronics (GCCE), Osaka, Japan, 15–18 October 2019.

196. Sirichotedumrong, W.; Kinoshita, Y.; Kiya, H. Privacy-Preserving deep neural networks using pixel-based image encryption without common security keys. In Proceedings of the Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), Lanzhou, China, 18–21 November 2019.
197. Sirichotedumrong, W.; Kinoshita, Y.; Kiya, H. Pixel-Based Image Encryption Without Key Management for Privacy-Preserving Deep Neural Networks. *IEEE Access* **2019**, *7*, 177844–177855. [CrossRef]
198. Liu, X.; Jin, X.; Zhao, Y. Optical image encryption using fractional-order quantum cellular neural networks in a fractional fourier domain. In Proceedings of the 14th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), Huangshan, China, 28–30 July 2018.
199. Anh, T.T.; Thanh, N.V.; Luong, T.D. A construction of cryptography system based on quantum neural network. In Proceedings of the Eighth International Conference on Knowledge and Systems Engineering (KSE), Hanoi, Vietnam, 6–8 October 2016.
200. Dai, S. Quantum Cryptanalysis on a Multivariate Cryptosystem Based on Clipped Hopfield Neural Network. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**, *in press*. [CrossRef]
201. Niemiec, M.; Mehic, M.; Voznak, M. Security Verification of artificial neural networks used to error correction in quantum cryptography. In Proceedings of the 26th Telecommunications Forum (TELFOR), Belgrade, Serbia, 20–21 November 2018.
202. Wang, B.; Li, Y.; Lei, C.; Zhao, Y.; Zhang, J.; Wang, X. Quantum noise diffusion mapping based on chaotic recurrent neural network in quantum noise cipher. In Proceedings of the Asia Communications and Photonics Conference (ACP) and International Conference on Information Photonics and Optical Communications (IPOC), Beijing, China, 24–27 October 2020.
203. Zamani, H.; Nadimi-Shahraki, M.H.; Gandomic, A.H. QANA: Quantum-based avian navigation optimizer algorithm. *Eng. Appl. Artif. Intell.* **2021**, *104*, 104314. [CrossRef]
204. Cheng, H.C.; Hanson, E.P.; Datta, N.; Hsieh, M.H. Duality between source coding with quantum side information and classical-quantum channel coding. *IEEE Trans. Inf. Theory* **2022**, *in press*. [CrossRef]
205. Lee, W.K.; Hwang, S.O. High Throughput Implementation of Post-quantum Key Encapsulation and Decapsulation on GPU for Internet of Things Applications. *IEEE Trans. Serv. Comput.* **2021**, *in press*. [CrossRef]
206. Li, Y.; Aghvami, A.H.; Dong, D. Intelligent Trajectory Planning in UAV-Mounted Wireless Networks: A Quantum-Inspired Reinforcement Learning Perspective. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 1994–1998. [CrossRef]
207. Dong, D.; Chen, C.; Chu, J.; Tarn, T.J. Robust Quantum-Inspired Reinforcement Learning for Robot Navigation. *IEEE/ASME Trans. Mechatron.* **2012**, *17*, 86–97. [CrossRef]
208. Wei, Q.; Ma, H.; Chen, C.; Dong, D. Deep Reinforcement Learning with Quantum-Inspired Experience Replay. *IEEE Trans. Cybern.* **2021**, *in press*. [CrossRef]
209. Masuyama, N.; Loo, C.K.; Seera, M.; Kubota, N. Quantum-Inspired Multidirectional Associative Memory With a Self-Convergent Iterative Learning. *IEEE Trans. Neural Netw. Learn. Syst.* **2018**, *29*, 1058–1068. [CrossRef]
210. Patel, O.P.; Bharill, N.; Tiwari, A.; Prasad, M. A Novel Quantum-Inspired Fuzzy Based Neural Network for Data Classification. *IEEE Trans. Emerg. Top. Comput.* **2021**, *9*, 1031–1044. [CrossRef]