The Dichotomy of Neural Networks and Cryptography

Subjects: Computer Science, Artificial Intelligence | Computer Science, Interdisciplinary Applications
Contributor: Behrouz Zolfaghari , Takeshi Koshiba

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.

neural network cryptography cryptanalysis survey

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.

2. War: Neural Computing against Cryptography

2.1. 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 [11]. 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.

2.1.1. 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 [12]. 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 [13] 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. [12] 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. [12] speculate that better accuracy could be achieved by changing the preprocessing and classification models to consider non-sequential execution of code.

2.2. 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 [14]. 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 [14].

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 [15], 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 [16].

Danziger and Henriques studied how effective NNs could be at cryptanalyzing S-DES ciphers [17]. 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 [18]. 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 [19]. 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 [20].

2.3. 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) [21]. More specifically FNNs are being used to model out attack scenarios against the Challenge Response Pairs (CRPs) of the PUFs [21]. 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 [21]. 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 [21].

2.4. 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) [22].

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) [23].

3. Peace: Coexistence and Alliance

3.1. 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.

3.1.1. 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 [24]. 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 [25].

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 [26]. Similarly Nandakumar et al. developed a method of training a NN on fully homomorphicaly encrypted data [27]. 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.

3.2. 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.

3.2.1. 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 [28], while others have researched the use of NN's using tree parity machines as a way to distribute keys of a symmetric encryption system [29]. 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 [30]. This method provides no need for key exchange [30]. 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 [30]. 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 [31][32].

- **Random Number Generation:** Neural cryptography has guided the verification of Pseudo Random Number Generators (PRNGs) by picking up on statistical biases unknown to humans [33]. This is achieved using neural cryptography to detect the difference between actual output and desired ideal random numbers [33].

The use of neural cryptography for encryption [34] and decryption [35] has received a focus from the research community in recent decades [36][37][38]. Different security models have been proposed based on neural cryptography [39] and different kinds of NNs [40] have been used for design and implementation of cryptosystems [41]. This effort has led to the development of different types of neural cryptosystems [41][42]. In the following, researchers 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 [43]. Particularly both the scrambling and diffusion are performed independently meaning an attacker can attack each separately [43]. 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 [43]. This allows not only for the protection from the aforementioned independent cracking of the scrambling and diffusion steps, but also resists chosen plaintext attacks [43]. 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 [44]. 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 [45]. It is important to note that this method uses asymmetric RSA for key exchanges [45]. This can pose an issue since the security of the model relies then on the RSA key and not the Neural Cryptography system [46]. 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 [46]. Finally, Wavelet Chaotic NNs (WCNN) and chaotic NNs have also been used for secure encryption and decryption of images [47]. However, research has shown that WCNN provides stronger ciphertext [47]. Furthermore, during transmission the only data that would need to be sent is approximation coefficients, reducing the size of the ciphertext drastically [47].

* **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 [48]. This model transmits data via the Orthogonal Frequency Division Multiplexing (OFDM) modulation technique and controls the bit rate and quality of the decrypted video [48]. 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) [49]. AENN is a NN meant to provide the least possible distortion to the resulting ciphertext, this allows ciphertext normalization to still appear as ascii [49]. 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 [50]. The application of delayed Chaotic NNs to generate binary sequences has also been researched in text encryption [51]. The binary sequence is used to create the key for the first level of encryption [51]. Then used in conjunction with DNA cryptography to create a secure ciphertext [51].

- **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, researchers 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 [52].

* **Authentication:** While issues with WiMAX have been thoroughly documented [53]. Neural Cryptography proposes solutions to authentication and authorization by creating neural synchronized key pairs [53]. To achieve this neural synchronization two NNs are created with the same weight changing algorithm and passed the same input [54]. 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 [54]. RFID has seen many problems due to having no international standards and posses security risk, one proposed solution [55]. Involves using a tree parity NN in order to perform key generation [55]. Biometric recognition for authentication has also seen support from deep recurrent NNs in order to increase accuracy and performance of models [56].

* **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 [57]. Then using a Deep NN this message is embedded into a host image [57]. Other groups have achieved similar results of image using Self-Organizing Map (SMO) NNs with 26 clusters for every letter of the alphabet [58]. Research has also been conducted to hide messages within sound [59]. 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 [59].

* **Visual Cryptography:** One drawback of visual cryptography is its lack of evaluation criteria [60]. One group proposed a method of evaluating the desirable results of visual cryptography would be encryption-inconsistency and decryption-consistency [60]. 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 [61][62]. Other types of NNs used for visual cryptography includes Pi-Sigma NNs, which is a double layered feed forward network [63]. Allowing for fewer communications between sender and receiver with higher security [63].

- **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 [55][64][65]. After proof of its security was published [66]. 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 [64][67][68]. 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 [69][70]. Finally, chaotic NNs has seem many applications as well [71]

[72][73]. 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 [72][73].

* **Applications in Medical Technologies:** Applications of neural cryptography in the field of medicine have come from the requirement of keeping patient images confidential [74]. 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 [75]. Other methods of security proposed involve using the Region of Non-Interest in the image in order to watermark the image [74].

- **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 [76]. 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 [77]. Achieved postquantum key exchange protocols by using NNs in order to augment Diffie–Hellman key exchange protocols by using multivariate cryptosystems [78]. Explored the relationship between cryptographic functions and the learning abilities of RNN [79][80]. Used Principle Component Analysis NNs to generate random numbers for a chaos encryption system [81]. Other groups have experimented with cellular NNs with iterative interchangeability to produce encryption that allows flat historgrams for randomness and bias [82]. Back-propogating NNs in order to provide strong image compression-encryption using a fractional-order hyperchaotic system [83]. unbounded inertia NNs with input saturation in order to obtain good cryptographic properties [84]. Memristive bidirectional associative memory NNs for colored image encryption [85]. 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 [86][87]. 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 [88].

- **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 [89]. 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 [89]. Further ways to disallow NNs to learn from challenge responses of PUF's is to use analog NNs [90]. Moving on to hardware purposes, researches have created a 1-bit PUF with a 2

neuron CNN with good metrics for robustness [91]. Other uses for NNs in the space of PUF's involve Error Coding Correction for keys which provides more efficient corrections than standard models [92]. Finally, Tests have been conducted to show there is feasibility in using NN based PUF's for authentication purposes [93].

- **Security Evaluation:** Here researchers discuss attacks on previously mentioned cryptographic systems [94] [95]. First researchers note a majority attack on neural synchronization via NN to provide secret keys, this attack is possible due to many cooperating attackers [94]. Then researchers 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 [95]. Finally, researchers 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 [96]. Although NNs are susceptible to the aforementioned attacks, it also provides resistances to the more commonly known vectors of classical cryptography [97].

- **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 [98]. There has also been study into the generalization of synchronization by using Discrete Time-Array Equations [99]. Other papers investigate the use of lag within the neuron activation functions of a network of NNs in order to provide secure synchronization [100]. Papers have also tested different reaction-diffusion technique of Lyapunov time-dependent impulses within NNs to see its applicability to encrypting images [101]. Synchronization for arrays in a network system can also be achieved by using master-slave synchronization of a delayed NN [102]. The use of memristor-based models and its chaotic properties have also been studied in regards to its image encryption capabilities [103]. Other memristive models using lyapunov functions have also been used for image encryption [104].

- **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 [105]. Produce a chaotic time series using a chaotic NN and use that to encrypt plaintext [105], while the method does have its errors the proposed encryption scheme to use in conjunction, a one-time pad, does alleviate those problems [105].

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.
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.

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.
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.
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.
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.
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.
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.
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.
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.
11. 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.
12. 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.
13. 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.
14. 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.

15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.

26. 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.
27. 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.
28. Kim, T.; Youn, T.Y.; Choi, D. Deep Neural Networks Based Key Concealment Scheme. IEEE Access 2020, 8, 204214–204225.
29. 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.
30. 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.
31. Jin, J.; Kim, K. 3D CUBE Algorithm for the Key Generation Method: Applying Deep Neural Network Learning-Based. IEEE Access 2020, 8, 33689–33702.
32. 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.
33. 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.
34. 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.
35. 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.
36. Kinzel, W.; Kanter, I. Neural cryptography. In Proceedings of the 9th International Conference on Neural Information Processing, Vancouver, BC, Canada, 9–14 December 2002.
37. 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 December 2011.

38. 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.
39. 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.
40. 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.
41. 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.
42. 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.
43. 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.
44. 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.
45. 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.
46. 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.
47. 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.
48. 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.

49. 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.
50. 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.
51. 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.
52. 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.
53. 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.
54. 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.
55. 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.
56. 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.
57. 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.
58. 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.

59. 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.
60. 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.
61. 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.
62. 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.
63. 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.
64. 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.
65. 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.
66. 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.
67. 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.
68. 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.
69. 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.

70. 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.
71. 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.
72. 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.
73. 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.
74. 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.
75. 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.
76. 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.
77. Dong, T.; Huang, T. Neural Cryptography Based on Complex-Valued Neural Network. IEEE Trans. Neural Netw. Learn. Syst. 2020, 31, 4999–5004.
78. 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.
79. 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.
80. 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.
81. 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.

82. 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.
83. 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.
84. 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.
85. 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.
86. 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.
87. 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.
88. 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.
89. 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.
90. 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.
91. 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.
92. 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.

93. 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.
94. 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.
95. 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.
96. 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.
97. 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.
98. 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.
99. 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.
100. 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.
101. 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.
102. 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.
103. 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.

104. 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.

105. 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.