ISSN 2347 - 3983

Volume 8. No. 7, July 2020

International Journal of Emerging Trends in Engineering Research

Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter146872020.pdf

https://doi.org/10.30534/ijeter/2020/146872020

Exploring Artificial Neural Networks in Cryptography – A Deep Insight

Manikandan.N[1], Abirami.K[2], Muralidharan.D[3], Muthaiah.R[4]

[1]Research Assistant, School of Computing, SASTRA Deemed to be University, India, manikandan_phd@outlook.com

[2]PG Scholar, School of Computing, SASTRA Deemed to be University, India, abivlsi2018@gmail.com

[3]Assistant Professor, School of Computing, SASTRA Deemed to be University, India, murali@core.sastra.edu

[4]Professor, School of Computing, SASTRA Deemed to be University, India, muthaiah66@gmail.com

ABSTRACT

In today's digital world, cryptography became indispensable in almost all trending technologies. For ensuring a completely secure system with limited computational complexity involved in the generation of randomness, secret key and other aspects, researchers employed various techniques to the cryptosystems. Despite the considerable number of strategies, applications of Artificial neural networks (ANN) for cryptographic problems appeared to be more remarkable. Owing to this fact, this work has been devoted to reveal the applications of different kinds of artificial neural networks for different categories in cryptosystems. Artificial Neural Networks are stepping stones in search of artificial intelligence. ANNs are chosen because they are good at generalization, adaptive decision making and unknown pattern recognition. This plethora of information regarding how each neural network was used in different types of cryptosystems is mainly contributed to future researchers to aid their novel works in this discipline. Also, application of Neural networks for cryptography related problems yielded positive results in almost all the applied fields. Therefore, this work is done with the intention of highlighting the novel combination of neural networks and cryptography.

Key words: Artificial Intelligence (AI), Artificial Neural Networks (ANN), Cryptography, Cryptanalysis.

1. INTRODUCTION

Cryptography-Greek word refers to "Secret Writing''. This secret writing dates back to 2000 B.C. as it is evident from Hieroglyphics of Egyptians, Scytale of Spartans and Caesar cipher of Romans. Academic research of cryptography was started in 1970.Until then, Cryptography was used only for diplomatic, military and Government purposes [1]. Since 1970 researchers find this discipline more fascinating, because of its application in daily life. For instance, unlocking a car using a remote-control system, making calls via voice-over-IP, installing a software update, e-health, car telematics, smart buildings and the applications goes on. These practical cryptographic implementations make the cryptology discipline omni-present. Cryptology is categorized as cryptography and cryptanalysis. Cryptography deals with securing data/message communication of any cryptosystem. Cryptanalysis is the art of breaking the security of that cryptosystem [1]. Cryptanalysis might sound controversial, but it has its importance, since security property of any cryptosystems is only empirical and hard to measure. Strength and efficiency of cryptosystems are directly proportional to the difficulties it involves in breaking the algorithm or retrieving the secret key [2]. Researches over recent years have proved that many cryptographic algorithms are still vulnerable to cryptanalytic attacks. From [3] the idea of using artificial neural networks for providing security to the cryptographic protocols appears to be the right solution as they reduce the complex computations in secret key generations. Briefly, Neural networks are designed from the inspiration of how a human brain perceives the world. Perception is one more attracting concept-in the eye of the beholder. Perceptual recognition task of a human brain happens within100-200ms, whereas the same task by a powerful and faster computer takes too long time [4]. This delay is due to the controversial nature of a human brain's computation and a conventional computer. These computations are possible by the brain because of the basic functional units named "neurons" from where the idea behind the design of an artificial neural network emerged. By nature from the birth of human, a brain has considerable structure and the ability to build up its own rules of behavior through what we usually refer to as "experience". So, to design an artificial neural network to yield the desired output in the applications of interest, the network needs to be trained to acquire experience or knowledge. This training is also called as the learning process of a neural network. Once the training is done neural networks are ready to anticipate the output for a given new input other than inputs given to training them. This article explores what will happen when the intelligence of artificial neural networks (ANN) through their massive-parallel structure is combined with cryptosystems to provide more security. This article surveys different cryptosystems that use various aspects of artificial neural networks viz., its learning process, non-linear approximation, pattern recognition. Survey also includes different ways to ensure security from various cryptanalytic attacks. This treatise restricts itself to the niche use of ANNs for cryptographic domain and does not intend to discuss the basic architecture of neural networks in depth. This paper is structured as following five sections. Section 2 narrates steganography and steganalysis along with the use of ANN in steganalysis technique. Section 3 discusses the digital watermarking techniques and different works proposed by various researchers that explains the use of ANN for providing robustness to the watermarked images. Section 4 explains about PRNGs and related works that use different types of neural networks (NN) for producing randomness in PRNGs. This section also briefs the use of an ANN for predicting the next bit of a random sequence. In section 5, describes the works related to neural key exchange protocols and the survey is summarized and concluded in section 6.

2. STEGANALYSIS - PERCEIVING THE IMPERCEPTIBLE

Steganography is the word derived from the Greek word 'Steganos' meaning 'concealed writing'. Steganography is the concept of masking a confidential message with another file or image. Steganography is one of the leaves of cryptography and sounds to be same. But they have different security goals. The goal of cryptography is to encrypt the contents of the message while steganography's goal is to hide the fact that the secret message even exists. Steganography was used in countries where cryptography was considered illegal and banned. Earlier sources of steganography were invisible ink, wax tables, microdots, vinegar and fruit juices. Messengers intending to hide secret messages were shaved their head and tattooed information in their head and grown hair. So, it is discernible that steganography is an old technique that existed back in centuries. This technique has taken a giant stride forward from the 1990s because of the growth of free software applications for data hiding process into the forms of video, audio or image formats [87-88]. This growth is well and good until it was being used by the terrorists and other cybercriminals for hiding secret information against the Government. Therefore, there exists a need to detect these hidden messages which opens the door for a new discipline named Steganalysis. Steganalysis is analogous to cryptanalysis. Steganalysis technique is to detect the hidden message from the concealed cover. This cover maybe in the form of any digital formats like image, audio, video file that acts as a carrier of the secret message called stego-medium or stego carrier. Stego-message is the final product that needs to be detected by steganalysis method. Following are the reasons for the use of artificial neural networks for steganalysis

- Artificial neural networks can meticulously predict unpredictable patterns
- Steganography often involves hiding of data in a non-linear pattern. ANN is optimum for non-linear classification [5].
- ANN's learning process is an added advantage for the steganalysis process.
- Feature extraction of high-dimensional statistical images is another advantage of ANN. In recent years, the steganography algorithm is developed with more sophisticated statistical characteristics of images. Steganalysis methods with low-dimensional statistical features might yield unfavorable results in this aspect. Therefore, ANN is preferred as it provides feature extraction of high-dimensional statistical images [6],[89].

Table 1 discusses the pioneered work for steganalysis using ANN during the year 2003-2004.The results obtained were more positive to attract the researchers towards this field. Later during the year 2014 to 2018, many researchers showed interest in this field and published surplus amounts of publications using CNN and DNN for steganalysis and steganography. Traditional steganalysis method involved feature extraction and applying a classifier to detect the stego-images as evident from table1. From 2014, researchers combined these two tasks as a single automated steganalysis process by using deep neural networks thereby reducing the complexity in manual feature extraction. Tan Li et al [80] proposed this method first in his work using Convolutional Neural Network (CNN) with unsupervised learning from a stack of auto-encoders. Following his work, many researchers published similar works from 2014. Table 2 describes the review works proposed by various researchers for steganalysis applied along with deep neural networks. It is observed from the table that these review articles reduce the burden of future researchers from surveying about steganalysis using ANN.

Chaumont [8] clearly explained the architecture of CNN with each of its block functions and the resulting feature maps. This work helps one in getting familiarity with the CNN architecture. He mentioned all the contemporary works published from the year 2015 to 2018 along with their architectures. The author claims to minimize the classification error in his work and also, he justified how CNN is best suitable for image steganalysis process. Thanks to Reinel et al [9] as they presented a systematic review article that distinctly explains the past and recent works of CNN based image steganalysis along with different kinds of CNNs. Authors reviewed 14 biblical works in which they analysed neural networks' architecture used in each work and conferred the percentage of error in a clear-cut way. This work aids in clear insight of which domain (Spatial, JPEG) and steganographic algorithm are used for particular CNN architecture in the steganalysis process. Another review article enabling the blooming researchers in this field to get more familiar about Deep Neural Networks (DNN) and CNN for steganalysis was proposed by Ruan, F et al [10]. Initially, the authors described in short about four types of image steganography since the image is the prominent cover source preferred more compared to other forms of cover source. This article also assists readers with previously published works that convey how DNNs are applied in different fields of steganalysis such as audio, video and how it has improved the detection process in an efficient way. Like other works, this survey also justifies that CNN is best suited for image steganalysis than other neural networks. Authors in addition to real-time image steganalysis with neural networks also

Table1: Pioneer works for Steganalysis

Biblical work	**Published year**	**Techniques used for data hiding/embedding**	**Types of classifiers (ANN) for performing steganalysis**	**Limitations Addressed**	**Results obtained**
Liu Shaohui et al [5]	` 2003	Statistical feature extraction of images-DCT, DWT, DFT. Data hiding method-Brain Chen's quantization index modulation method.	Backpropagation neural network used to classify secret information hidden images and non-hidden images. Hidden layer-1	Slow convergence of backpropagation neural network	85.4 % correct detection of hidden images and 75 % correct detection of non-hidden images
Yun et al [7]	2004	Statistical Feature -Moments of characteristic function along with wavelet sub bands.	Feed Forward Neural network with backpropagation training algorithm. Hiddenlayer-4	--	98.7 % accuracy obtained which is 3-4% increase than Bayes classifier.

suggested about edge computing and fog computing of real time images to be considered by future researchers to meet certain criteria like network traffic. In 2020, Israr Hussain et al [19] proposed one more review article about deep learning for image steganalysis. Authors provided readers with a surplus knowledge by differentiating the previous works based on two domains- Spatial and JPEG steganalysis with the pros and cons of each work. Previous works that are related to steganography based on deep learning was also surveyed along with the challenges faced by steganalysis and steganography in detail.

Therefore, the future research scope from this analysis of previous works are as follows:

- Future researchers should design new neural networks other than CNN and previously mentioned networks for the steganalysis process which takes arbitrary size input image rather than fixed input image size.
- Stego-mismatch and cover-source mismatch are other important challenges that should be addressed.
- Database is significant for training a neural network. Previous works use only one set of databases for one network training. Future researchers can use the large scale of a database from benchmarked sources for the training.
- There are various algorithms available for steganography. One can train the existing CNN with one algorithm and test with others to get a clear insight of how the transfer is possible between one algorithm to another.

3. NEURAL NETWORKS FOR DIGITAL WATERMARKING

Watermarking is another old technique that existed back in the thirteenth century. Initially, watermarking was used in the papermaking industry. When water was squeezed out from a wet fibre, it made impressions differentiating watermarked areas and non-watermarked areas. This idea forms the basis of watermarking technology [20]. Earlier it was used to represent the brand and manufacturer of the paper mill and later it was used to authorize the context of paper also. This traditional watermarking has now grown well and become prominent in the digital world since all the data in the present world are in digital forms. The widespread applications of digital watermarking schemes are copyright assurance, tamper proofing and authentication of data. Through digital watermarking counterfeiting of currencies, postage stamps and other intellectual properties are avoided. The relation between steganography and watermarking is that steganography conceals the secret message and it has no relation with the covering source or carrier while watermarking gives authentication to the cover source or carrier. Cryptography provides encryption to the plain text or secret message while watermarking provides security to unencrypted multimedia content. Information pertaining to the legal owner (it may be a logo or electronic signatures known as watermark) is injected in the target media (called host media) in the form of random bits and transmitted over the network. The ultimate aim of watermarking is providing robustness to the host media without degrading its quality at the time of media enhancing process like image processing, video and audio processing.

Table 2: Review works contributed by various Researchers for Steganalysis

Biblical review works	Published year	Techniques discussed	Types of ANN discussed	Research scope addressed
Chaumont [8]	2019	Spatial steganalysis (Side-channel-informed), Spatial steganalysis (not-side-channel aware), JPEG steganalysis, mismatch phenomenon	CNN along with its major blocks and operations.	Cover-source mismatch and stego-mismatch should be sought in upcoming research works. Clever networks other than CNN should be used in future.
Reinel, Tabares-Soto, Ramos-Pollan Raul, and Isaza Gustavo [9]	2019	Steganographic algorithms namely HUGO [11], WOW [15], S-UNIWARD [14], J-UNIWARD [14], HILL [12], F5[16], MiPOD [13], UERD [18], UED [17] using JPEG and Spatial domain.	Different types of CNN namely YeNet, XuNet, ZhuNet, YedroudjNet, QianNet or GNCNN.	New CNN for correct detection with deeper architecture. Training of CNN with images of large size along with largescale database is essential.
Ruan,F., hang, X., Zhu, D.et al [10]	2019	Review of CNN and DNN based steganalysis, real-time image steganalysis in edge and fog-computing.	Different DNN networks for audio steganalysis and CNN network-MCNN (multi-column CNN network) image steganalysis	Fog computing and edge computing for real time image steganalysis
Israr Hussain, Jishen Zeng, Xinhong, Shunquan Tan [19]	2020	Spatial and JPEG image based steganalysis, Generative Adversary Network (GAN) based steganography.	CNN with algorithms namely Tan-Net, Qian-Net, Xu-Net-V1, Xu-Net-V2, Ye-Net, Sedighi-Net, ReSt-Net, Zeng-Net, Chen-Net, Xu-Net-V3, Yang-Net, SR-Net, Zhu-Net,Wu-Net, Yedroudj-Net, Pitfalls-Net, Mo-Chen-Net, WISER-Net.	Steganalysis method should be designed with neural networks that accept arbitrary input image, and dataset should be quantitative and from different benchmarked sources. Cover-source and stego-mismatch should be reduced.

Any degradation to the quality of the host image will make watermark perceptible to the adversaries who might involve in the copyright infringement [21]. Watermark techniques are of different types which are outlined in figure 1. Past research works of digital watermarking especially image watermarking are based on different types of neural networks. In [30]-[34], neural networks' application in image preprocessing techniques, feature extraction and data reduction are explained. It is evident that neural networks became central importance to the researchers when it comes to image classification and other processes like noise removal. Neural networks' adaptive decision-making ability, learning and generalization, unknown pattern recognition made it to be used for the watermarking technology. Neural networks are widely utilized for watermark embedding in the target image, video or audio once the host media co-efficient are decomposed using DCT, DWT, DFT, FFT transforms. Also, for watermark removal without degrading the quality of host image and watermarked image. Besides capacity estimation, tampering detection, error-rate prediction, safe region location are other uses of ANN in watermarking technique [29]. Table.3. describes the works contributed to the various utilization of ANN for digital watermarking scheme.

Following are the general quality assessment of the watermarking scheme.

PSNR - Peak Signal to Noise ratio is the quality assessment of a good watermark embedding process. High PSNR indicates the good visual quality of the watermarked image.

BER – Bit Error Rate is the assessment for the watermark extraction process. If BER is near to 0, it indicates great recuperation of the watermark.

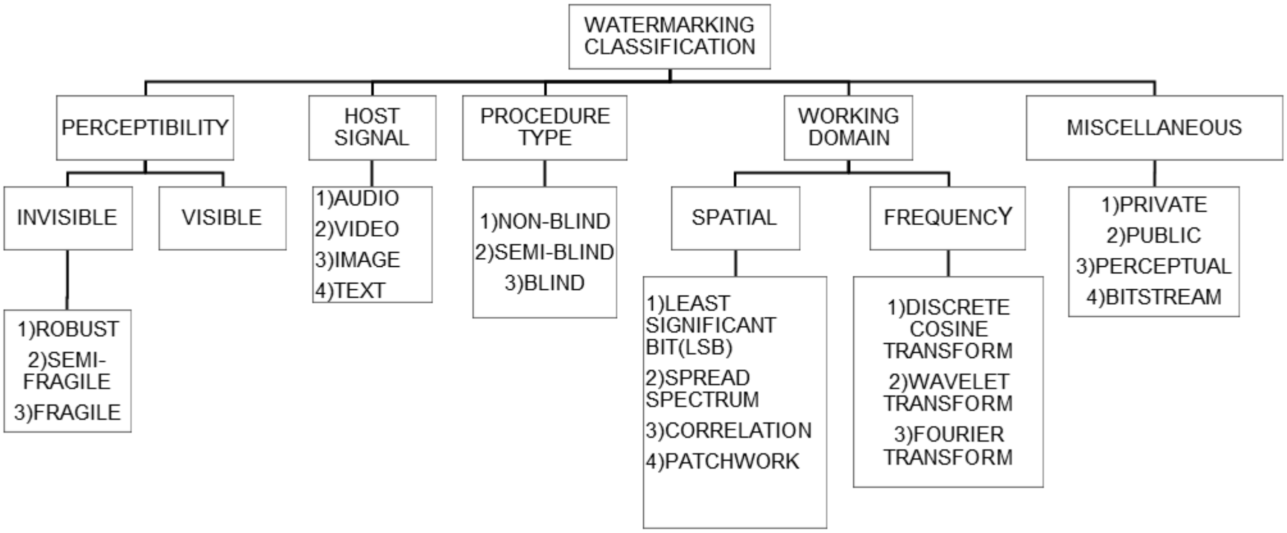

Figure 1: Classification of Digital Watermarking techniques

MSE - Mean Square Error indicates the rising squared error between the watermarked image and the original image. If MSE is lower, then the error is lower.

NC – Normalized cross correlation to indicate a correlation between the actual and the retrieved watermark. If NC is 1 it denotes perfect correlation.

In 2001, the novel usage of neural networks for the digital watermarking technique was proposed by Pao-Ta Yu et al. [22]. Authors used 9-5-1 (Input layer with 9 nodes, hidden layer with 5 nodes and output layer with 1 node) Multi-Layer Perceptron with backpropagation algorithm to remove the signature watermark from the target image. Neural network's adaptive learning is used in this extraction process and it greatly reduced false recovery for color image. Authors claimed that this approach of using neural networks in watermarking technique aids in preventing the host image from many image processing attacks. Thanks to Bibi Isac et al as they contributed a review article [24] and reduced the burden for future researchers from searching related works back from 2001 to 2011.Authors provided survey about the works related to image and video watermarking using Back propagation Network (BPN),Counter Propagation Network (CPN), Full Counter Propagation Network and Cellular Neural Networks (FCNN) along with pros and cons. Their research work covered the use of NN in the watermark embedding and recuperation.

Also, N. Mohananthini et al [25] contributed similar work along with domains (Spatial and frequency transform) and described the related works till 2014. They detailed the use of ANN in embedding and extraction of watermarking for achieving robustness, imperceptibility, authenticity. Haribabu Kandi et al proposed a new approach of using auto encoder CNN for image watermarking [27]. Authors justified their use of CNN with the following reasons: (i) Auto-encoder CNN has learning feature of the given input image samples which have systematic discerning power. (ii)Incrementing the input dimension of the watermarked image will increase buffer size which in turn requires more interconnections for performing the watermarking. This is the case of a general feedforward neural network. Owing to this fact, auto-encoder CNN has the advantage of weight sharing mechanism with the help of convolution and pooling operations thus reducing the intricated connectivity of interconnection layers for the watermarking purpose. (iii)Even if the input images have small distortions and scale changes, those are handled efficiently by the CNN. (iv)Previous works are mostly based on frequency domain whereas this approach is based on a spatial domain. PSNR achieved was 58.91 dB. Owing to the highest PSNR, high imperceptibility is achieved between the watermarked image and the host image. (v)Authors also claimed that this approach is suited for real-time applications. This approach discusses about non-blind type of watermarking distinctly and proved to be secure against the image processing attacks. A Semi-blind digital watermarking technique [28] in the frequency domain was proposed by Ankit Rajpal et al. Authors proposed a new neural network known as fast single-layer feed- forward neural network. This neural network is also called as Online Sequential Extreme Learning Machine (OS-ELM). From the results of this approach, it is apparently visible that the work served the purpose of twin requirement-visual quality and robustness of a digital watermarking technique. The Author used OS-ELM network for its attributes such as fast computation, good generalization capability and accuracy. The PSNR result obtained was 43dB as an evident for good visual quality and BER (Bit Error Rate) obtained was 0.0029 denoting a good extraction process by the neural networks. All the training, embedding and extraction process was done in milliseconds which is why authors stated that this approach is applicable for real-time applications such as video watermarking.

Table 3: Works contributed to the various utilization of ANN for Digital Watermarking Scheme

Applications	Contributions	Type of ANN used	Results obtained
Detecting strength of the watermark	Shi-Chun et al., (2002) [81]	Feed Forward Neural Network	Robustness and watermarking strength of DCT co-efficient enhanced.
	Ming et al, (2003) [82]	Radial Basis Function (RBF) neural network	RBF aided in achieving the watermark strength also robustness against destructive signal processing and JPEG compression attacks.
	Fang and Zhang (2005) [83]	Hopfield neural network	Restricted the bounds of the watermark capacity as watermark was viewed as a noise.
	Jin and Wang (2007) [84]	Feed Forward Multi-layer network	Good imperceptibility and high robustness.
Error rate prediction	Naoe and Takefuji et al. (2008) [85]	Multi-layered Perceptron Model	Low error rate in prediction of the watermark without any damage to the target content. Robustness to high pass filtering.
Tamper detection	Fan, Y. C., Mao, W. L., & Tsao, H. W. (2003) [26]	ANN with backpropagation model	89-99% recognition rate of image processing attacks. Tampering was detected and located. Also, analyzed what kind of changes occurred in fragile watermarking scheme.
Location of safe region (place where watermark is hidden)	Olanrewaju et al., 2010 [86]	Complex Valued Neural Network (CVNN)	CVNN used to locate safe region without degrading the content. Also, imperceptibility is achieved.
	Pao-Ta Yu et al., (2001) [22]	Multi-layer Perceptron with backpropagation algorithm	MSE 1.597 and PSNR 46.097dB. Robustness against single and multiple image processing attacks.
Embedding and extraction of watermark	Lu, W., Lu, H., & Shen, R. (2004) [23]	Multi-layer Perceptron with backpropagation algorithm	NC obtained 0.98 (normal), 0.86 (with attacks). Withstand signal processing and geometric attacks.
	Ankit Rajpal et al., (2016) [28]	Online Sequential Extreme Learning Machine (OS-ELM)	PSNR 43 dB, BER 0.0029
	Haribabu Kandi et al., (2016) [27]	Auto-encoder Convolutional neural network	PSNR 58.91dB (without noise), PSNR 36-55.10dB (with noise)
	A. Loganathan et al., (2016) [36]	Bidirectional Associative Memory (BAM) Neural Network	PSNR 60.97dB. Robustness against video frame filtering, cropping, noising, dropping, Gamma correction, Histogram attack and other video processing attacks.
	Farah Deeba et al., (2020) [35]	Deep Neural Network (DNN)	Accuracy for the watermark content test 51.6 with standard benchmarked dataset.

In 2016, A. Loganathan et al [36], proposed video watermarking technique with Bidirectional Associative Memory (BAM) Neural Network. This approach proposed multiple watermarks to provide robustness against various geometric and video processing attacks. Authors presented a distinct work on video watermarking and claim that their work is best suited for medical videos in security aspects with better embedding capacity. Authors left a hint to future researchers stating that their proposal is not suitable for fast motion videos and researches should be made such that the contributed technique is available for live multimedia content.

Another more innovative approach of using NN for embedding and extracting watermark was proposed by

Rashidah Funke Olanweraju et al [29] in 2020. This approach is said to be damage less due to the fact that the host image is not affected physically. One may wonder how is it possible to embed the watermark with this condition but the novel idea proposed by the authors serves as the answer. Authors proposed a complex-valued neural network (CVNN). This network is composed of complex-valued neurons and synaptic weights that gets complex values (real and imaginary) as their training inputs. This input is taken as a result of the conversion of real domain data into complex domain data through Fast Fourier Transform strategy. Unlike other works, this proposal doesn't involve physical addition hence named their technique as damage less. CVNN also have the property of fast convergence which is proved in this work. This novel work should be considered by future researchers to further develop this work against image processing attacks.

The identified future research scope from the outcome of previous works are as follows:

- Many works are related to the use of NN in embedding and extraction of the watermarking scheme. Thus, future works should concentrate on more novel works for strength detection, safe region location and tamper detection.
- Researchers should attempt to do video and audio watermarking rather than image watermarking alone.
- Most of the works are done with Lenna and baboon image or some other binary images. Other images rather than these greyscale images should be preferred for watermarking. More payload of watermark also affects the watermarked image quality. So, this trade-off should be addressed in future works.
- Real-time image watermarking and fast motion video water marking are the techniques to be explored still.

4. PSEUDO-RANDOM NUMBER GENERATORS (PRNGS)

Pseudorandom number generators are the implementation that involves the generation of randomness and nonce in the form of numbers called pseudo random numbers by a background algorithm. These random numbers have widespread usage in VLSI technology, Cryptography, Information theory, Game theory, Pattern recognition, Statistics and Probability theory [37]. The idea behind the usage of this random numbers dates back to 19th century where people found numbers on dice to be more superior form of randomness creation in statistical experiments than shuffled cards, marked balls [38] and many researches were proposed in this context as it is evident from [39]. Owing to the advent of technologies many PRNGs were found in recent times. A good PRNG should be efficient in statistical, uniform distribution and non-predictability terms. From the results obtained from certain statistical tests explained clearly in [40,41,42,58] it is evident that newly designed PRNG is always found to be superior to the previously designed one. PRNGs are predominantly distinguished into three categories depending on the source of randomness. First category Linear Congruential (LCG) based generators which had linear modulo recurrences of a prime number as a source of pseudo-randomness. It was first designed by Lehmer in [43]. Linear Feedback Shift Register (LFSR) based generators initially used by Tausworthe [44] that had linear recurrences of a modulo 2 operators as a source of randomness. The third category is based on randomness from Cellular automaton (CA) introduced by Wolfram [45]. PRNGs are very important in the field of cryptography since it provides the obscurity through randomness and makes any cryptosystem exhibit scrambled nature. Thus, a PRNG is a vital part of a cryptosystem.

The ANNs possess a property called overfitting when they imitate the "training data" exorbitantly [47]. Overfitting occurs when a neural network learns the features and noise in the training data to a degree that it contrarily effects the performance of the network on new pattern. So, it often refers to the inability of the generalization property of ANN. Although overfitting is undesirable in conventional functions of the neural networks, this is exploited in the pseudo random number generations. Use of ANN for PRNGs in this context proved to be a good solution as the PRNGs yield good statistical performance [60] and also their patterns are non-predictable to the cryptanalysts to make an attack.

4.1. Neural Networks based PRNG approaches

A. **PRNGs based on HNN and MLP**: In 2003, D.A. Karras et al [46] proposed PRNG based on two factors. One is the direct utilization of overfitting property of Multilayer Perceptron (MLP) neural network. another one is the use of Hopfield type neural network (HNN) by uncorrelating the network's recurrent recall scheme so that the output patterns are unpredictable favoring the generation of pseudo-random numbers. This kind of manipulation in HNN yielded good results while evaluation for non-predictability and statistical tests. Similar works using HNN are done in [48] [57]. Along with addressing the convergence problem of HNN, Kayvan Tirdad et al [48] proposed fuzzy- based HNN for PRNG in 2010.In the same year Wang Y. et al presented PRNG using Hopfield neural network and ensured the unpredictability property with SHA-512 in their work [49].

B. **PRNGs based on Recurrent Neural Network with LSTM**: Young-Seob Jeong et al [50] proposed PRNG based on Long Short-Term Memory of recurrent neural networks along with an iterative generator. This generator is the key of this design that is designed in such a way as to not repeat the LSTM's sequence pattern. In 2020, same authors published their work along with NIST test suite [51].

*C.***PRNGs based on Generative Adversarial Networks (GAN)*:*** PRNG based on the generative adversarial neural network was proposed by Rajvardhan Oak et al. in [52]. This

Table 4: Contributions of various researchers for Neural Key Exchange Protocols

Contributions	Year	Cryptographic scheme	Secret key Exchanged	Type of NN used	Tolerance obtained
Guo et al.,[71]	1999	Symmetric key encryption	Permutation operation of neural synaptic matrix	Hopfield neural network (HNN) for its chaotic classifying property	Withstand probabilistic attack.
Scott Su et al., [72]	2000	Encryption /decryption of digital signal	--	Chaotic neural network along with its VLSI architecture	High computation speed and high security
Guerreiro et al.,[78]	2006	Symmetric block cipher	Stronger Key scheduling process	Spike Neural Network (SNN)	Withstand brute force attack
Prabakaran.N et al., [74]	2008	Key exchange protocol	Wight vectors	Tree Parity Machine with Feedback mechanism	Withstand geometric attack (Major flipping attack)
Ahmed M. Allam et al.., [75]	2013	Key exchange protocol	Pre-shared key as reflecting boundary	Tree Parity Machine (TPM)	Withstand genetic attack
Anikin et al.,[69]	2016	Symmetric key encryption	Weight vectors	Multi-layered feed forward neural network -Tree Parity Machine (TPM)	Difficult to break this key-exchange protocol.
Pattanayak et al., [76]	2018	Symmetric key encryption	Random keys padded with decimal values	Feed Forward Neural network with backpropagation algorithm.	Withstand brute force attack
Dong et al.,[79]	2019	Symmetric key encryption	Two group keys (real and imaginary parts) in one synchronization process	Complex Valued Tree Parity Machine Network (CVTPM)	Better security than TPM
Smruti Chourasia et al., [77]	2019	Key exchange protocol	Larger keys authenticated by HMAC (Hash based message authentication code) and SHA-512	Vectorized Tree Parity Machine(vTPM)	Withstand Birthday attack, man-in-the-middle attack

design passed 97% by NIST (National Institute of Standards and Technology) test suite and authors claimed that they have exploited the property of neural network with the supervision of a discriminator. Similar work was done in [53] and proved that the generator passed 98% of NIST test suite.

D. **PRNGs based on Other Neural Networks:** PRNG based on Chaotic and Random Neural Network (CRNN) which has four neurons in the discrete-time system was presented by Hitoaki Yoshida et al [54] and it is used for the chaos generation. Authors claimed that random output of this CRNN was not predictable with asymmetric piecewise linear function 3 (APLF3) and their future work will be the design of a new PRNG with a novel design for data security applications for IoT devices. This application may not assist floating-point arithmetic and GPU furnished smartphones.

In 2011, V.V. Desai et al [55] proposed PRNG based on Elman Neural network. This is a two-layer network in which the output from the first layer is feedbacked to the to the input in the first layer. This feedback states forms as the basis for the generation of different outputs. Authors claimed that this neural network based PRNG used in their work was simple, fast and easy for implementation.

E. **PRNGs Evaluation with Neural Networks:** Neural networks are used for the evaluation of PRNG also Related works are discussed in this section briefly. Multi-Layer Neural network for anticipating the next bit in the output of a pseudo-random number sequence was done by Yuki Taketa et al [56]. The difficulty of prediction is based on linear complexity. PRNG's randomness cannot be assessed only by the linear complexity of a sequence. Authors claim that statistical aspects are required for future work. The prediction on next bit is an important aspect for the evaluation of a good PRNG.

Hayato Kimura proposed PRNG evaluation tool based on the LSTM neural network that detected the statistical biases of RC4 (Rivest Cipher 4) and LCG[59].LSTM networks are used here as they are good at handling continuous values like time series and also they are used for finding the linearity of LCG, which is association between bytes. Authors proved that the proposed system detected the linearity of LCG, which cannot be detected by NIST SP 800-22. Therefore, they claimed that the proposed design can detect multiple biases.

5. NEURAL CRYPTOGRAPHY

Cryptography is categorized as symmetric and asymmetric key cryptography. Symmetric key cryptography involves the same private key for encryption and decryption whereas asymmetric key cryptography involves public and a private key. The secret key generated involves complex computations in order to withstand the adversary attacks. In 2002 [61], researchers were attracted towards neural cryptography, the concept of exchanging a secret key over an unsecured public channel using neural network. To be precise, with the help of synchronization by mutual learning of neural networks, key exchange was done. This concept aids in reducing the computational complexity of the secret key and outperforms the traditional number theory method in secret key generations [62-68]. Synchronization by mutual learning widely use Tree Parity Machine (TPM). It is a tree shaped graph. In TPM, each party has tree parity machine. It is a unique kind of multi-layer feed-forward neural network. The TPM neural network forms the backbone of neural cryptography. One important aspect of TPM is that they converge to the same state of weight even if they are distributed randomly [70]. TPM network without feedback mechanism cannot withstand genetic attack [73], probabilistic attack and geometric attack [74] which are made on a key exchange protocol by the adversaries while TPM with feedback mechanism [65] can withstand these attacks. The learning rule for this TPM is three types namely Hebbian learning rule, Anti-Hebbian learning rule, Random-walk learning rule. TPM training is also three types. One is by changing the weights alone, second training is by changing the inputs alone and the third one is by changing both the weights and inputs. In [69] authors proved that it is difficult to crack a key-exchange protocol that uses TPM synchronization [63]. Table 4 lists the contributions of neural key exchange protocols.

From all the above literary works, in our view the inferences and gapes to be addressed are presented below.

- More research works are based on symmetric key encryption and key exchange protocols only. Future scope exists for asymmetric key based encryption.
- TPM forms the backbone of neural cryptography yet more neural network architectures should be exploited in order to withstand genetic, probabilistic and geometric attacks.
- Secret key length and its generation should be more effective rather than always preferring synaptic weights of the TPM model.
- Key generation with the help of neural networks remains to be center of attraction for all the researchers as it reduces computational complexity and outperforms the number theory method. Therefore, this field needs to be well explored.

6. CONCLUSION

Artificial Neural networks are boons for modern world whereas cryptography on the other hand vital for network security. It is evident from this review that when both massive fields are combined, various cryptographic applications are benefitted. This work has discussed how and what type of neural networks were used for steganalysis, digital watermarking, pseudo-random number generators and neural key exchange. Also, this article presented why neural networks were preferred for each of the above said applications. These are only a handful applications of cryptography. Future works should concentrate on many unsolved cryptographic problems like protection of secret keys with more key length and its life-span, mutual-authentication, secured public channel communication, real-time multimedia security in the medical field and diplomatic field. Also, it is witnessed from this work that with the help of neural networks, computational complexity was reduced and more favorable results were achieved in almost all the applications of cryptography where ANNs are used. Yet there are many unsolved cryptographic problems like Diffie-Hellman Mapping Problem (DHMP), Discrete Logarithm Problem (DLP), approximation and factorization problems. It is recommended that along with these problems, many other cryptographic related problems should be solved using artificial neural networks Thus, future researches need to address more innovative neural cryptographic applications.

REFERENCES

1. Paar, Christof, and Jan Pelzl**. *Understanding cryptography: a textbook for students and practitioners*,** Springer Science & Business Media, 2009**.**
2. Schmidt, T., H. Rahnama, and A. Sadeghian. **A review of applications of artificial neural networks in cryptosystems,** *World Automation Congress*. IEEE, 2008.
3. Kinzel, Wolfgang, and Ido Kanter. **Interacting neural networks and cryptography,** *Advances in solid state physics*. Springer, Berlin, Heidelberg, 2002. 383-391.
4. Haykin, Simon S.**Neural networks and learning machines/Simon Haykin**. (2009).
5. Shaohui, Liu, Yao Hongxun, and Gao Wen.**Neural**

network based steganalysis in still images,*2003 International Conference on Multimedia and Expo. ICME'03. Proceedings (Cat. No. 03TH8698)*. Vol. 2. IEEE, 2003.

6. Tang, Yong-He, et al. **A review on deep learning-based image steganalysis,***2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*. IEEE, 2018.
7. Shi, Y. Q., Xuan, G., Zou, D., Gao, J., Yang, C.,Zhang, Z., Chai, P., Chen, W., & Chen, C. (2005). **Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network**,*IEEE International Conference on Multimedia and Expo, ICME 2005*, *2005*, 269–272. https://doi.org/10.1109/ICME.2005.1521412
8. Chaumont, Marc.**Deep Learning in steganography and steganalysis from 2015 to 2018** (2019).
9. Reinel, Tabares-Soto, Ramos-Pollan Raul, and Isaza Gustavo.**Deep learning applied to steganalysis of digital images: a systematic review**, *IEEE Access* 7 (2019): 68970-68990.
10. Ruan, Feng, et al. **Deep learning for real-time image steganalysis: a survey**, *Journal of Real-Time Image Processing* 17.1 (2020): 149-160.
11. Pevný, Tomáš, Tomáš Filler, and Patrick Bas.**Using high-dimensional image models to perform highly undetectable steganography**,In *International Workshop on Information Hiding*, pp. 161-177. Springer, Berlin, Heidelberg, 2010.
12. Li, Bin, Ming Wang, Jiwu Huang, and Xiaolong Li.**A new cost function for spatial image steganography**,*IEEE International Conference on Image Processing (ICIP)*, pp. 4206-4210. IEEE, 2014.
13. Sedighi, Vahid, Rémi Cogranne, and Jessica Fridrich. **Content-adaptive steganography by minimizing statistical detectability**,*IEEE Transactions on Information Forensics and Security* 11.2 (2015): 221-234.
14. Holub, Vojtěch, Jessica Fridrich, and Tomáš Denemark.**Universal distortion function for steganography in an arbitrary domain,** *EURASIP Journal on Information Security* 2014.1 (2014): 1.
15. Holub, Vojtěch, and Jessica Fridrich**. Designing steganographic distortion using directional filters**, *2012 IEEE International workshop on information forensics and security (WIFS)*. IEEE, 2012.
16. Westfeld, A.**F5: A steganographic algorithm. Proceedings of the 4th international workshop information hiding**, *Lect. Notes Comput. Sci* 2137.1 (2001): 289-302.
17. Guo, Linjie, Jiangqun Ni, and Yun Qing Shi.**Uniform embedding for efficient JPEG steganography**,*IEEE transactions on Information Forensics and Security* 9.5 (2014): 814-825.
18. Guo, Linjie, et al. **Using statistical image model for JPEG steganography: uniform embedding revisited,***IEEE Transactions on Information Forensics and Security* 10.12 (2015): 2669-2680.
19. Hussain, Israr, Jishen Zeng, and Shunquan Tan**. A Survey on Deep Convolutional Neural Networks for Image Steganography and Steganalysis**,*KSII Transactions on Internet & Information Systems* 14.3 (2020).
20. Shih, Frank Y**. *Digital watermarking and steganography: fundamentals and techniques***,CRC press, 2017.
21. Cox, I. J., M. L. Miller, and J. A. Bloom. J. Fridrich, T. Kalker**, Digital Watermarking and Steganography**, (2008).
22. Yu, Pao-Ta, Hung-Hsu Tsai, and Jyh-Shyan Lin. **Digital watermarking based on neural networks for color images**,*Signal processing* 81.3 (2001): 663-671.
23. Lu, Wei, Hongtao Lu, and Ruiming Shen**. Color image watermarking based on neural networks**,*International symposium on neural networks*. Springer, Berlin, Heidelberg, 2004.
24. Isac, Bibi, and V. Santhi. **A study on digital image and video watermarking schemes using neural networks,** *International Journal of Computer Applications* 12.9 (2011): 1-6.
25. Karim, Akram Jalal.**The indispensable styles, characteristics and skills for charismatic leadership in times of crisis**,*International Journal of advanced engineering, management and science* 2.5 (2016): 239445.
26. Fan, Yu-Cheng, Wei-Lung Mao, and Hen-Wai Tsao.**An artificial neural network-based scheme for fragile watermarking,***2003 IEEE International Conference on Consumer Electronics, 2003. ICCE*. IEEE, 2003.
27. Kandi, Haribabu, Deepak Mishra, and Subrahmanyam RK Sai Gorthi.**Exploring the learning capabilities of convolutional neural networks for robust image watermarking,***Computers & Security* 65 (2017): 247-268.
28. Rajpal, Ankit, Anurag Mishra, and Rajni Bala. **Multiple scaling factors based Semi-Blind watermarking of grayscale images using OS-ELM neural network,***2016 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*. IEEE, 2016.
29. Ali, Nor'ashikin, Othman Khalifa, and Azizah Abd Manaf**. ICT in telemedicine: Conquering privacy and security issues in health care services,***Electronic Journal of Computer Science and Information Technology: eJCIST* 4.1 (2013).
30. Shih, Frank Y., Jenlong Moh, and Fu-Chun Chang. **A new ART-based neural architecture for pattern classification and image enhancement without prior knowledge**, *Pattern Recognition* 25.5 (1992): 533-542.
31. Figueiredo, Mário AT, and José MN Leitão. **Sequential and parallel image restoration: neural**

network implementations, *IEEE transactions on image processing* 3.6 (1994): 789-801.

32. Zhang, Zeeman Z., and Nirwan Ansari.**Structure and properties of generalized adaptive neural filters for signal enhancement,***IEEE transactions on neural networks* 7.4 (1996): 857-868.
33. Lee, Chi-Chien, and Jose Pineda de Gyvez.**Color image processing in a cellular neural-network environment**, *IEEE Transactions on neural networks* 7.5 (1996): 1086-1098.
34. Chandrasekaran, V., Marimuthu Palaniswami, and Terry M. Caelli.**Range image segmentation by dynamic neural network architecture,** *Pattern Recognition* 29.2 (1996): 315-329.
35. Deeba, Farah, et al.**Digital Watermarking Using Deep Neural Network**,*International Journal of Machine Learning and Computing* 10.2 (2020).
36. Loganathan, Agilandeeswari, and Ganesan Kaliyaperumal. **An adaptive HVS based video watermarking scheme for multiple watermarks using BAM neural networks and fuzzy inference system**,*Expert Systems with Applications* 63 (2016): 412-434.
37. Bhattacharjee, Kamalika, Krishnendu Maity, and Sukanta Das.**A Search for Good Pseudo-random Number Generators: Survey and Empirical Studies,** *arXiv preprint arXiv:1811.04035* (2018).
38. Galton, Francis. **Dice for statistical experiments**, (1890): 13-14.
39. Von Neumann, John. **various techniques used in connection with random digits,** *Appl. Math Ser* 12.36-38 (1951): 5.
40. Marsaglia, George.**DIEHARD: a battery of tests of randomness**.,*http://stat. fsu. edu/geo* (1996).
41. L'Ecuyer, Pierre, and Richard Simard. **TestU01: AC library for empirical testing of random number generators,***ACM Transactions on Mathematical Software (TOMS)* 33.4 (2007): 1-40.
42. Rukhin, Andrew, et al. ***A statistical test suite for random and pseudorandom number generators for cryptographic applications*.** Booz-allen and hamilton inc mclean va, 2001.
43. Harvard University. **Computation Laboratory**. *Annals of the Computation Laboratory of Harvard University*. Vol. 26. Harvard University Press, 1951.
44. Tausworthe, Robert C. **Random numbers generated by linear recurrence modulo two,***Mathematics of computation* 19.90 (1965): 201-209.
45. Wolfram, Stephen.**Cryptography with cellular automata**,*Conference on the Theory and Application of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 1985.
46. Karras, D. A., and V. Zorkadis.**Improving pseudorandom bit sequence generation and evaluation for secure Internet communications using neural network techniques**,*Proceedings of the International Joint Conference on Neural Networks, 2003.*. Vol. 2. IEEE, 2003.
47. Patterson, Dan W**. *Artificial neural networks: theory and applications***. Prentice Hall PTR, 1998.
48. Tirdad, Kayvan, and Alireza Sadeghian. **Hopfield neural networks as pseudo random number generators**, *2010 Annual Meeting of the North American Fuzzy Information Processing Society*. IEEE, 2010.
49. Wang, Yuhua, Guoyin Wang, and Huanguo Zhang.**Random number generator based on Hopfield neural network and sha-2 (512),** *Advancing Computing, Communication, Control and Management*. Springer, Berlin, Heidelberg, 2010. 198-205.
50. Jeong, Young-Seob, et al.**Pseudo random number generation using LSTMs and irrational numbers**, *2018 IEEE International Conference on Big Data and Smart Computing (BigComp)*. IEEE, 2018.
51. Jeong, Young-Seob, et al. **Pseudo-random number generation using LSTMs**, *The Journal of Supercomputing* (2020): 1-19.
52. Oak, Rajvardhan, Chaitanya Rahalkar, and Dhaval Gujar.**Poster: Using Generative Adversarial Networks for Secure Pseudorandom Number Generation**,*Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2019.
53. Marcello De Bernardi, M. H. R., and Pasquale Malacaria.**Pseudo-random number generation using generative adversarial networks**, *Workshop Proceedings*.
54. Yoshida, Hitoaki, Haruka Fukuchi, and Takeshi Murakami. **Implementation of High-Speed Pseudo-Random-Number Generator with Chaotic and Random Neural Networks,** *Proceedings of the 53rd Hawaii International Conference on System Sciences*. 2020.
55. Desai, V. V., V. B. Deshmukh, and D. H. Rao. **Pseudo random number generator using Elman neural network**, *2011 IEEE Recent Advances in Intelligent Computational Systems*. IEEE, 2011.
56. Taketa, Yuki, et al**. Mutual Relationship between the Neural Network Model and Linear Complexity for Pseudorandom Binary Number Sequence**, *2019 Seventh International Symposium on Computing and Networking Workshops (CANDARW)*. IEEE, 2019.
57. Hameed, Sarab M., and Layla M. Mohammed Ali**. Utilizing Hopfield Neural Network for Pseudo-Random Number Generator**,*2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*. IEEE, 2018.
58. Freeth, Adam, Krzysztof Pawlikowski, and Donald McNickle. **Pseudo-random number generators for massively parallel discrete-event simulation**, (2012).
59. Kimura, Hayato, Takanori Isobe, and Toshihiro Ohigashi.**Neural-Network-Based Pseudo-Random Number Generator Evaluation Tool for Stream Ciphers**,*2019 Seventh International Symposium on*

Computing and Networking Workshops (CANDARW). IEEE, 2019.

60. Maksutov, Artem A., et al. **PRNG assessment tests based on neural networks**,*2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. IEEE, 2018.
61. Kinzel, Wolfgang. **9 Theory of interacting neural networks,** *Handbook of Graphs and Networks* (2003): 199.
62. Kinzel, Wolfgang, and Ido Kanter.**Neural cryptography**, *Proceedings of the 9th International Conference on Neural Information Processing, 2002. ICONIP'02.* Vol. 3. IEEE, 2002.
63. Klein, Einat, et al. **Synchronization of neural networks by mutual learning and its application to cryptography**, *Advances in Neural Information Processing Systems*. 2005.
64. Klimov, Alexander, Anton Mityagin, and Adi Shamir. **Analysis of neural cryptography**, *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, Berlin, Heidelberg, 2002.
65. Ruttor, Andreas, et al. **Neural cryptography with feedback**, *Physical Review E* 69.4 (2004): 046110.
66. Ruttor,Andreas et al.,**Synchronization of random walks wth reflecting boundaries**,*Journal of Physics A:Mathematical and Genera*l 37.36 (2004):8609
67. Mislovaty, Rachel, et al. **Security of neural cryptography**, *Proceedings of the 2004 11th IEEE International Conference on Electronics, Circuits and Systems, 2004. ICECS 2004.*. IEEE, 2004.
68. Ruttor, Andreas. **Neural Synchronization and Cryptography**, *arXiv preprint arXiv:0711.2411* (2007).
69. Anikin, I. V., A. Z. Makhmutova, and O. E. Gadelshin.**Symmetric encryption with key distribution based on neural networks,***2016 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*. IEEE, 2016.
70. Tezcan, Zahir. **Public Key Exchange by Neural Networks**. (2005).
71. Guo, Donghui, Lee-Ming Cheng, and L. L. Cheng.**A new symmetric probabilistic encryption scheme based on chaotic attractors of neural networks**,*Applied Intelligence* 10.1 (1999): 71-84.
72. Su, Scott, Alvin Lin, and Jui-Cheng Yen. **Design and realization of a new chaotic neural encryption/decryption network**, *IEEE APCCAS 2000. 2000 IEEE Asia-Pacific Conference on Circuits and Systems. Electronic Communication Systems.(Cat. No. 00EX394)*. IEEE, 2000.
73. Ruttor, Andreas, et al. **Genetic attack on neural cryptography**, *Physical Review E* 73.3 (2006): 036121.
74. Prabakaran, N., P. Loganathan, and P. Vivekanandan. **Neural cryptography with multiple transfers functions and multiple learning rule**,*International Journal of soft computing* 3.3 (2008): 177-181.
75. Allam, Ahmed M., Hazem M. Abbas, and M. Watheq El-Kharashi. **Authenticated key exchange protocol using neural cryptography with secret boundaries**,*The 2013 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 2013.
76. Pattanayak, Sayantica, and Simone A. Ludwig.**Encryption based on neural cryptography**, *International Conference on Health Information Science*. Springer, Cham, 2017.
77. Chourasia, Smruti, et al**. VECTORIZED NEURAL KEY EXCHANGE USING TREE PARITY MACHINE**,*Compusoft* 8.5 (2019): 3140-3145.
78. Guerreiro, Ana Maria G., and Carlos Paz de Araujo**. A Neural Key Generator for a Public Block Cipher**, *2006 Ninth Brazilian Symposium on Neural Networks (SBRN'06)*. IEEE, 2006.
79. Dong, Tao, and Tingwen Huang. **Neural cryptography based on complex-valued neural network**, *IEEE Transactions on Neural Networks and Learning Systems* (2019).
80. Tan, Shunquan, and Bin Li. **Stacked convolutional auto-encoders for steganalysis of digital images**, *Signal and Information Processing Association Annual Summit and Conference (APSIPA), 2014 Asia-Pacific*. IEEE, 2014.
81. Mei, Shi-chun, et al. **Decision of image watermarking strength based on artificial neural-networks**,*Proceedings of the 9th International Conference on Neural Information Processing, 2002. ICONIP'02.*. Vol. 5. IEEE, 2002.
82. Zhi-Ming, Zhang, Li Rong-Yan, and Wang Lei. **Adaptive watermark scheme with RBF neural networks**,*International Conference on Neural Networks and Signal Processing, 2003. Proceedings of the 2003*. Vol. 2. IEEE, 2003.
83. Zhang, Fan, and Hongbin Zhang. **Applications of a neural network to watermarking capacity of digital image**, *Neurocomputing* 67 (2005): 345-349.
84. Jin, Cong, and Shihui Wang.**Applications of a neural network to estimate watermark embedding strength**,*Eighth International Workshop on Image Analysis for Multimedia Interactive Services (WIAMIS'07)*. IEEE, 2007.
85. Naoe, Kensuke, and Yoshiyasu Takefuji. **Damageless information hiding using neural network on YCbCr domain**,*International Journal of Computer Sciences and Network Security* 8.9 (2008): 81-86.
86. Olanrewaju, R. F., et al. **Watermarking in safe region of frequency domain using complex-valued neural network**, *International Conference on Computer and Communication Engineering (ICCCE'10)*. IEEE, 2010.
87. Gustilo, Reggie.C. **Android-based Image and Video Steganography System**, *International Journal of Emerging Trends in Engineering Research*. 346-352. 2019 10.30534/ijeter/2019/19792019.

88. B, Kusuma et al, **A Systematic Approach for Data Hiding Using Cryptography and Steganography**, *International Journal of Emerging Trends in Engineering Research*. 8. 1326-1332. 2020 10.30534/ijeter/2020/63842020.
89. N. Manikandan et al, **Approximation Computing Techniques to Accelerate CNN Based Image Processing Applications – A Survey in Hardware/Software Perspective**. *International Journal of Advanced Trends in Computer Science and Engineering*. 9. 3828-3846. 2020 10.30534/ijatcse/2020/202932020.