Neural Network-Based Cryptography: A Primary Study on the Performances and Techniques

Jia-Lin Foo, Kok-Why Ng(✉), and Palanichamy Naveen

Faculty of Computing and Informatics, Multimedia University, Persiaran Multimedia, 63100
Cyberjaya, Selangor, Malaysia
kwng@mmu.edu.my

Abstract. Cybersecurity is getting more and more important in this big data era. Neural Network-based cryptosystem which is a complex system and deserve more research study for improvement. This article will discuss and analyse existing neural network-based cryptography performance and techniques. The in-depth analysis will examine the effectiveness of older structure as well as the effects initiated against them. Several advanced techniques will be discussed that reliant on generative adversarial networks (GANs) to contend with one another in pursuit of a common goal such as efficient encryption for communication. At the end of the paper, it will review a few decent neural network methods best applied on cryptography.

Keywords: Neural Network · Cryptograph · Generative Adversarial Networks

1 Introduction

Cryptography is an essential technology for safeguarding data in computer systems. It is the analysis of encrypted communication pathways that limit access to the information of a message to only the recipient and the desired receiver [1]. Cyber-attacks could adversely impact information security. As both the rate of data and internet traffic keeps increasing, awareness of cyber-security is becoming more crucial and vital. Establishing an advanced and stable medium is currently among the most complex and challenging subject matters for communication system development. There are innumerable types of public key cryptography, but somehow it requires more detailed procedures as well as greater computer capacity [2].

Artificial Neural Networks (ANNs) are computing systems inspired by the biological neural networks derived from animal brains. Artificial neurons are a set of linked nodes or units in an ANN that loosely reconstruct the synapses in a biological brain [3, 4].

There are various technological devices and automated items available in the twenty-first century, including tablet devices, cell phones, and other comparable IoT devices. The systems perform vital services such as data storage and multimedia information interchange, among others. The proliferation of digital images and videos can be attributed to

S.-C. Haw and K. Sonai Muthu (Eds.): CITIC 2022, 10, pp. 68–78, 2022.
https://doi.org/10.2991/978-94-6463-094-7_6

the development of multimedia technology. It is more necessary than the usual methods of converting digital and digital imagery. It is crucial to retain the confidentiality and security of the digital information during the flow of data, which means it genuinely requires a strong protection of end-user protection [5]. As a result, protecting the multimedia information and data is becoming essential. To keep the data private, a variety of strategies are deployed. No one can simply access or hack the database. Data is sent from one location to another without viewing or comprehending it in the process. Technologies are rising rapidly in wireless communication i.e. cyberspace demands considerable data security and protective measures for everyone. Security is a major concern with the latest advancements in computing information and technology process optimization [6]. Many issues arise in relation to network security and digital sharing. Even now, there is a significant problem with cyber hacking, thus it is essential to keep data protected. Embedding data is one way to safeguard sensitive files while it is being transmitted from one location to another via an unencrypted connection. Encryption is used in different applications to meet needs such as privacy and anonymity.

Every firm now recognises the need of data protection. In other words, the parties-involved must be certain that the content can only be accessed by the sender and recipient. The fundamental requirement for establishing a secure is the use of cryptography.

Encryption systems have emerged as an instant solution for protecting information from other sources. The skills usually required information and data be encrypted using some form of cryptographic formula which only the person who shared the data could decipher in order to use it. Encryption is a way of transforming transmitted data into a structure that cannot be viewed without being decrypted [7]. To cryptographic confidential material, a cryptographic signature and a decryption key are required. The private key is used for encryption and decode data. The key is utilized by the sender and receiver of the encrypted sensitive material. The private key, also known as symmetric cryptography, is shared by both sides, whereas the public key is known as asymmetric cryptography. Private key cryptography is significantly quicker than public-key encryption [8]. A private key can only be shared between two parties, whereas a public key can be used by anybody.

1.1 Neural Network

ANN is a densely interconnected framework of Artificial Neurons with an inherent tendency for storing and retrieving large amounts of experience data. Data-driven neural networks (NN) are well-suited for non-linear applications. An ANN is a simple primitive technique for attempting to imitate the brain electrically using software or hardware. There are two considerations to be made: the acquisition of knowledge through learning and the storage of knowledge in weights, i.e. coefficients [9]. These are the two parts of the AI neural network that describe the brain. ANN may be used to build powerful complex algorithms that mimic the human brain's capacity to comprehend. When developing first-principles network equations is complicated, an ANN is used. Non-linear Regressions, Clustering, and Classification are all done with ANN [10]. It has the capability of learning from examples. The data collection step for Neural Network design must be meticulously planned to guarantee that there is sufficient data, that it reflects the underlying principles at operation, so the data is as clean of noise as possible. Neural networks have a variety

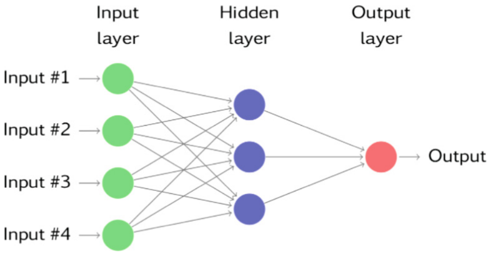

Fig. 1. An ANN with 4 inputs and 1 output layer, and with 3 hidden neurons/inputs.

of features [11]. Neural Networks are capable of recognising complicated patterns and modelling non-linear systems by themselves. Because of the great degree of structural parallelism, it can respond quickly.

Neural networks are frequently utilised data modelling and statistical analysis, where they are viewed as an alternative to traditional non-linear regression and cluster analytic methods. They are frequently used in situations that can be contextualised in terms of classification or prediction [12].

Deep learning is a new term or method for an approach to artificial intelligence which could be known as neural networks. It aims to discover relationship between two sets of data by mimicking how the human brain processes. It has the capability to perform multiplex calculation with simplicity. Because of its amazing ability to analyse information from complicated data, it could be used to discover patterns and detect trends that would be too hard for users or other computer systems to grasp on their own [13].

1.2 Network Architecture

Neural Network is build-up from 3 type of layers and is illustrated in Fig. 1.

- Input layers – initial data
- Hidden layers – intermediate or second layer between inputs and output layers
- Output layers – generate the result based on the given inputs data.

The fundamental types of network architectures are shown below.

1.2.1 Single Layer Feed Forward Networks/Single-Layer Perceptrons

The neurons of a layered neural network are grouped into layers. In the most basic form of a layered network, a number of neurons of source nodes projects upon an output layer of neurons, and not the other way round. The system is primarily of the feed forward variety (Fig. 2). Single-layer perceptron requires only one input and one output layer. As it has no algorithm, the input layer is not classified a layer.

1.2.2 Multilayer Feed Forward Networks/Multi-layer Perceptrons

The number of hidden layers distinguishes the second type of feed forward neural network. The hidden neuron's purpose is to meaningfully influence with the outputs and

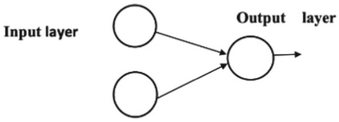

Fig. 2. Single layer Feed-forward network/Single layer perceptrons

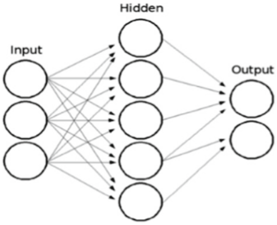

Fig. 3. Multi layers Feed-forward Network/Multi-layer perceptrons

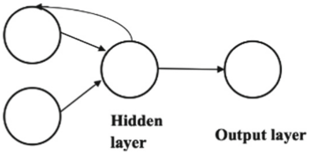

Fig. 4. Recurrent Network

inputs. By integrating more hidden layers, the network can obtain the maximum accuracy of data. The second layer's neurons receive the incoming signal (Fig. 3). The output signal is used as an entry to the third layer, and so on throughout the system hierarchy.

1.2.3 Recurrent Networks

A recurrent neural network should have at minimum one feedback mechanism, also known as a feedback loop. A recurrent network can have a single layer of neurons, with each neuron transmitting its output signal along to the inputs of all the other neurons. Self-feedback describes a circumstance in which a neuron's output is fed back itself into input. The inclusion of feedback loops has a substantial impact on a network's learning capabilities as well as its protection and dependability (Fig. 4).

1.3 Learning Process

A learning rule is a mechanism for calculating the weighted and prejudices of a network while it is being trained. A learning rule's purpose is to educate the network on how to fulfil its unique responsibilities. They can be classified into three groups.

1.3.1 Supervised Learning

The learning algorithm generates a set of important training data that exhibits proper network behaviour. The network outputs are examined in regard to the objectives since the inputs are transferred to the network. As a result, the training rule develops a habit of modifying the network's weights and biases to bring its output closer to the objectives.

1.3.2 Reinforcement Learning

It is similar to supervised learning, however the algorithm is still not provided the proper output for the input nodes; instead, it is guaranteed a rating for how well it performed. The rating may be used as a baseline for the network's effectiveness over a set of inputs in some instances.

1.3.3 Unsupervised Learning

Only network inputs have an effect on the weights and biases of the model. There is no target output available. The majority of the algorithms perform some type of clustering operation, which can be of various types. They learn how to categorise the input recognised patterns into a number of finite classes.

2 Literature Review on GNNS-Related Work

Khaled et al. [14] presented a generalized regression neural network (GRNN) encryption system that is fixed to the secret keys. Many training iterations were tested in the proposed system. The researchers also tested the system with different numbers of input data and hidden neurons. The obtained results were more accurate and better performance than the traditional encryption methods.

Natvita et al. [15] used a back propagation recurrent network for implementing a finite state sequential machine. Different sequential machines are acting important role to cultivate the neural network. The key is representing the complexity and the level of security can do this. The obtained results are promising and opening a new research direction. Other than that, Navita raise two ANNs for cryptography. The model is identical to the model presented by Nitin [16]. The demonstrated results showed that the two networks are safe and reliable, which as of now without any results about promptitude [15].

MuriloCountinho et al. [17] protected communication with Adversarial Neural Cryptography (ANC) by using secure cryptography. The researchers showed that in the right circumstances a perfectly secure cryptosystem can be improved and ameliorated by neural network. In addition, the obtained results demonstrated that the original adversarial neural cryptography methodology is time-consuming to accomplish the goal [18]. Moreover, the researchers showed a new CPA-ANC methodology (Chosen-Plaintext Attack) for the purpose of enhancing the function and the learned model. In the investigations, they used simple neural networks to improve and raise the understand the learned model. The obtained results showed the dominant position of proposed CPA-ANC over the original ANC methodology, as in CPA-ANC almost all the learned models were

Table 1. Summary of GANs-Related work.

Method	Techniques discussed	Types of ANN discussed	Pros	Cons
Data Security Based on Neural Network	A variation to radial basis neural networks. Mostly used on regression, prediction and classification	General Regression Neural Network	Single-Pass Learning	No optimal method to improve it
Use of Artificial Neural Network in the Field of Security	Computes the gradient of the los function for a single weight by the chain rule	Back Propagation Recurrent Network	No parameters to tune apart from the numbers of inputs	Actual Performance of backpropagation on a specific problem is dependant on the input data [28]
Learning perfectly secure cryptography to protect communication with Adversarial neural cryptography	Provided with primitive data to produce fake data. The fake data is then passed to the discriminator network	Adversarial Neural Cryptography	Proceed into detail of data and can easily interpret into several versions so it is advantageous in machine learning work	Difficult to train as required to provide several types of data in order to check if it works meticulously as it intended

secure one-time password (OTP). The researchers concluded that in order to force the solution into a formidable cryptosystem [19], the adversary must be very strong. In this case the standalone CPA-ANC methodology is not good enough to guarantee security [20], the key is to devise a very powerful adversarial capable of breaking cryptosystems. In their model, the researchers showed that it was achievable. In conclusion, Table 1 shows the summary of the GANs-related work.

3 Literature Review on Cryptography

Prabakaran et al. [21] developed a secret key [22] based on neural network cryptography and the reciprocal learning of Tree Parity Machines (TPMs). The network consists of two dynamical systems, each of which starts with a different set of beginning circumstances and is linked by common input values that are shared across the two systems. After computing their responses, the networks arrive at a shared input vector and their weight vectors are changed depending on the fit between their respective outputs at each step. The input and output connectors do not interflow across a public channel until their weight vectors are identical that can be used as a secret key for encrypting and decrypting secret communications [23]. The weight vectors of the two neural networks are created using PRNG-generated random numbers.

Wenwu et al. [24] proposed a model, which Jiyun Yang [25] dissected. It is difficult to obtain the secret of Wenwu et al.'s cryptosystem using traditional methods. However, because every encryption operation uses the same key stream, it may be easily obtained using a chosen plaintext attack involving two pairings of plaintext and cipher-texts [26]. The results of the demonstration show that chaotic cryptography is unreliable.

Karam et al. [27] demonstrated an Artificial Neural Network-based stream cypher scheme based on Pseudo Random Number Generator (PRNG). For key sequences employing ANN, the Pseudo Random Number Generator (PRNG) model provides unforeseeable statistical randomness qualities. The two stages of the presented neural Pseudo Random Number generator are as follows: the very first phase generates a tremendous and lengthy set of trends from an ideal equation and initial value. As a result, these patterns have inexplicable features. The entire number of equations and initial values is defined by the amount of bits acting as the initial value. The phase two is an ANN that receives the previous phase's outputs and groups them as input to the NN [29].

The generation progress of back propagation neural network contains of three phases. The first phase is the feed-forward NN, the second phase is a back-propagation and the third phase is associated with weights adjustments. Demonstration results presented that the ANN cryptosystem is very reliable, and can be applied on hardware application.

Ilker et al. [30] demonstrated chaotic cryptosystems using synchronised chaotic generators and artificial neural networks. The ANN model generates chaotic dynamics with many Chua's circuit solutions. Three input variables and a time variable are used as inputs, with two hidden layers and three chaotic dynamics are used as outputs. The majority of the demonstrations are based on the neurons on the hidden nodes in order to find the optimum ANN structure with chaotic dynamics. Encryption and decryption processes rely heavily on chaotic dynamics [31]. The chaotic ANN generator's substantial disparity between chaotic dynamics can be viewed as an advantage. The provided approach eliminates the fundamental shortcomings and weaknesses of analogue circuits, as well as the various chaotic circuit solutions. The approach is efficient in terms of synchronization, is trustworthy and safe, and can be employed in real world applications, according to the demonstrated findings. The associated cryptographic work is summarised in Table 2.

Figure 5 shows the number of journal papers reviewed in this work and the methods used by the researchers in neural network and cryptography field.

4 Conclusion

In this paper, we discuss the current research on applying neural networks into the cryptography field. The Neural network-based cryptosystem is a brilliant and interesting idea that builds perplexed cryptosystems [6], in which the crypto analyst or hacker needs to know not only the algorithm of the Neural Network and the key to access the system [33], but also the numerous adaptive iterations and final weights for the encryption and decryption systems. Using a Neural Network-based cryptosystem with a higher number of plain-txt/cipher-text pairs can reduce mistake as much as possible [34, 35].

Table 2. Summary Table of Cryptography works.

Title	Techniques discussed	Types of ANN discussed	Pros	Cons
New Security on Neural Cryptography with Queries	The resolution is based on a mapping process that map the mutual learning in TPM into learning in noisy perceptrons	Mutual Learning Tree Parity Machines	Producing a secret key is a simple perception of the TPM	Hardware dependency
Cryptanalysis if a cryptographic scheme based on delayed chaotic neural networks	The techniques that used to transfer the information securely with the presence of a third-party	Chaotic Cryptography	High sensitivity to initial conditions and control parameter	Insecure [32]
Implementation of neural–cryptographic system using FPGA	Algorithm for generating a series of data whose properties estimate the properties of sequence of random data	Pseudo Random Number Generator	Very efficiency and can be applied on hardware application	Could be correlation of successive values
Artificial neural network based chaotic generator for cryptology	Generated the chaotic dynamics by the several kinds of solution of Chua's circuit	Chaotic cryptosystems/chaotic generator synchronization	Reliable and able to built into real time application	Could be lack of uniformity of distribution for large quantities of generated numbers

Finally, based on the finding in this study, it is believed that the future trend in the usage of ANNs in cryptography field will be mostly focused on convolutional neural network (CNNs), Layer Recurrent Neural Network (LRNNs), Tree Parity Machine (TPM) and some other neural-networks related work.

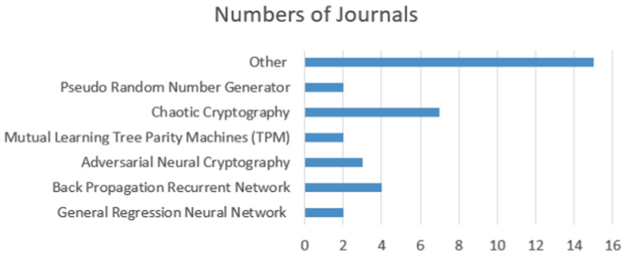

Fig. 5. Numbers of Journal Reviewed

Authors' Contributions. Jia-Lin Foo: Original draft preparation, Conceptualization.
Kok-Why Ng: Supervision, Reviewing and Editing.
Palanichamy Naveen: Supervision, Reviewing and Editing.

References

1. Rakhim S. Nakhushevm, Natalia V.Sukhanova, "Application of the Neural Networks for Cryptographic Information Security", 2020. DOI: https://doi.org/10.1109/ITQMIS51053.2020.9322981
2. T.Godhavari, N.R. Alamelu, R.Soundararajan, "Cryptography Using Neural Network", IEE Indicon 2005 Conference, Chennai, India, 11–13 Dec. 2005, 2005. DOI: https://doi.org/10.1109/INDCON.2005.1590168
3. Halenar Igor, Juhasova Bohuslava, Juhas Martin, Nesticky Martim, "Application of Neural Networks in Computer Security", 24th DAAAM International Symposium on Intelligent Manufacturing Automation, 2013. DOI:https://doi.org/10.1016/j.proeng.2014.03.111
4. Denis Roenko, "Evaluating Efficiency of Artificial Neural Networks for Solving Symmetric Cryptography Issues", ITMO University, 49 Kronversksky Pr, Saint Petersburg, 197101, Russian Federation, 2020
5. Shweta B. Suryawanshi, Devesh D. Nawgaje, —A triple-key Chaotic neural network for cryptography in image processing, International Journal of Engineering Sciences & Emerging Technologies, Vol. 2, Issue. 1, 46–50, 2012. DOI: https://doi.org/10.1109/ICCSP.2011.5739316
6. Wenwu Yu, Jinde Cao, "Cryptography based on delayed chaotic neural network", Physics Letters A, Vol. 356, (4) Elsevier, 333–338, 2006. DOI:https://doi.org/10.1016/j.physleta.2006.03.069
7. Jonathan Blackledge, Napo Mosoloa, "Applications of Artificial Intelligence to Cryptography", School of Electrical and Electronic Engineering, 2020. DOI: https://doi.org/10.14738/tmlai.83.8219
8. Wolfgang Kinzel, IdoKanter, "Neural Cryptography", Proceedings TH2002 Supplement, Vol. 4, 147–153, 2003
9. Manikandan. N, Abirami. K, Muralidharan. D, Muthaiah. R, "Exploring Artificial Neural Networks in Cryptography – A Deep Insight", International Journal of Emerging Trends in Engineering Research, 2020. DOI: https://doi.org/10.30534/ijeter/2020/146872020
10. Chia-Hung Lin, Jian-Xing Wu, Pi-Yun Chen, Chien-Ming Li, Neng-Sheng Pai, Chao-Lin Kuo, "Symmetric Cryptography With a Chaotic Map and a Multilayer Machine Learning Network for Physiological Signal Infosecurity: Case Study in Electrocadiogram", 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), 2021. DOI: https://doi.org/10.1109/ACCESS.2021.3057586

11. InadyuttiDutt, Soumya Pail and Dipayan Band yopadyay, “Security in All-Optical Network using Artificial Neural Netowrk”, International Journal of Advanced Research in Computer Science, 2012. https://doi.org/10.26483/ijarcs.v3i2.1093
12. Khalil Shihab, “A Backpropagation Neural Network for Computer Network Security,” Department of Computer Science, SQU, Box 36, A1-Khod.123, Oman, 2006. DOI: https://doi.org/10.3844/jcssp.2006.710.715
13. B. Geetha vani, E. V. Prasad, —A Hybrid Model for Secure Data Transfer in Audio Signals using HCNN and DD DWT, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No.7, 202–208, 2013
14. Khaled M.G. Noaman and Hamid Abdullah Jalab, “Data Security Based on Neural Network”, Task Quarterly 9.4 (2005): 409–414
15. Navita Agarwal,Prachi Argawal, “Use of Artificial Neural Network in the Field of Security”, MIT International Journal of Computer Science & Information Technology, 2013. DOI:https://doi.org/10.1016/j.proeng.2014.03.111
16. Nitin Shukla, Abhinav Tiwari, “An Empirical Investigation of Using ANN Based N-State Sequential Machine and Chaotic Neural Network in the Field of Cryptography”, Global Journal of Computer Science and Technology Neural & Artificial Intelligence, Vol. 12, Issue. 10, No 1,17–26, 2012
17. MuriloCountinho, Robson de Oliveira Albuquerque, Fabio Borges, Luis Javier GarciaVillalba and Tai Hoon Kim,” Learning perfectly secure cryptography to protect communication with Adversarial neural cryptography”, MPBI, sensors 2018. DOI: https://doi.org/10.3390/s18051306
18. Amr H.Yassin, Hany Hamdy, “Survey Report on Cryptography Based on Neural Network”, December 2013
19. Ajit Singh, Aartinandal, “Neural Cryptography for Secret Key Exchange and Encryption with AES”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue. 5, 376–381, 2013
20. Vasyl Lytvyn, Roman Peleshchak, Ivan Paleshchak, Victoria Vysotska, “Information Encryption Based on the Synthesis of a Neural Network and AES Algorithm”, 2019. DOI: https://doi.org/10.1109/AIACT.2019.8847896
21. Prabakaran, N., Vivekanandan, P. “A New Security on Neural Cryptography with Queries”, Int. J. of Advanced Networking and Application, Vol 2, Issue, 1, 437–444, 2010
22. Marcin Niemiec, “Error correction in quantum cryptography based on artificial neural networks”, Quantum Information Prcessing(2019) 18:174, 2019
23. Karthik Nandakumar, Nalini Ratha, Sharath Pankanti, Shai Halevi, “Towards Deep Neural Network Training on Encrypted Data”. DOI: https://doi.org/10.1109/CVPRW.2019.00011
24. Riccardo Cantoro, Nikolas I. Deligiannis, Matteo Sonza Reorda, Marcello Traiola, Emanuele Valea, “Evaluating Data Encryption Effects on the Resilience of an Artificial Neural Network”, 2020. DOI: https://doi.org/10.1109/DFT50435.2020.9250869
25. Jiyun Yang, Xiaofeng Liao, Wenwu Yu, Kwok-wo Wong, Jun Wei, “Cryptanalysis of a cryptographic scheme based on delayed chaotic neural networks”, Choas, Solitions & Fractals, Vol 40, Issue. 2, 821–825, 2009. Doi: https://doi.org/10.1016/j.chaos.2007.08.029
26. Linfei Chen, Boyan Peng, Wenwen Gan, Yuanqian Liu, “Plaintext attack on joint transform correlation encryption system by convolutional neural network”, The School of Science, Hangzhou Dianzi University, Hangzhou Zhejiang 310018, China, 2020. Doi:https://doi.org/10.1364/OE.402958
27. Karam M.Z. Othman, Mohammed H.AL Jammas, “Implementation of neural – cryptographic system using FPGA”, Journal of Engineering Science and Technology, Vol. 6, No. 4, 411–428, 2011

28. Maha Mahmood, Belal AI-Khateeb, WisamMakki Alwash, “Review of Neural Networks Contribution in Network Security”, Jour of Adv Research in Dynamical & Control Systems, Vol 10, 13 Special Issue, 2018
29. Muhammad Imran Tariq, Nisar Ahmed Memon, Shakeel Ahmed, Shahzadi Tayyaba, Muhammad Tahir Mushtaq, Natash Ali Mian, Muhammad Imran, Muhammad W.Ashraf, “A Review of Deep Learning Security and Privacy Defensive Techniques”, Department of Computer Science, Superior University, Lahore, Pakistan, 2020. Doi: https://doi.org/10.1155/2020/6535834
30. Ilker Dalkiran, Kenan Danis, “Artificial neural network based chaotic generator for cryptology”, Turk J Elec Eng& Comp Sci, Vol.18, No.2, 240–255, 2010. DOI:https://doi.org/10.3906/elk-0907-140
31. Harpreet Kaur, Tripatjot Singh Panag, “Cryptography Using Chaotic Neural Network”, International Journal of Information Technology and Knowledge Management, July–December 2011, Volume 4, No. 2, pp. 417–422, 2011. DOI: https://doi.org/10.13140/RG.2.2.33027.63525
32. Suhrid Das, Sudip Mandap, Shankha Shubra Murkherjee, “Application of Chaotic Neural Network in Cryptography”, 2021. DOI: https://doi.org/10.13140/RG.2.2.33027.63525
33. Rafaek Valencia-Ramos, Luis Zhinin-Vera, Gissela E.Pilliza, Oscar Chang, “An Asymetric-key Cryptosystem based on Artificial Neural Network”, School of Mathematical and Computational Science, Yachay Tech University, 100650, Urcuqui, Ecuador, 2022
34. S Taransenko, N A Andriyannow, A A Gladkikh, “Analysis of the applicability of artificial neural networks for the post-quantum cryptography algorithms development”, Russia FSS Academy, Oryol, Russia, 2021. DOI: https://doi.org/10.1088/1742-6596/2032/1/012026
35. Ong, K., Haw, S. C., Ng, K. W., “Deep Learning Based-Recommendation System: An Overview on Models, Datasets, Evaluation Metrics, and Future Trends”, In Proceedings of the 2019 2nd International Conference on Computational Intelligence and Intelligent Systems (pp. 6–11). DOI: https://doi.org/10.1145/3372422.3372444