JES
Journal of Engineering Sciences

Vol 13, Issue 03, MARCH /2022

ISSN NO:0377-9254

ENCRYPTION AND DECRYPTION ALGORITHM BASED ON NEURAL NETWORK

Dr.Amarnadh S, Assistant Professor, Ph.d, Department of CSE, asurada@gitam.edu

D.Prudhvi raju, BTech, Department of CSE, dprudhviraju007@gmail.com

N.Santosh Kumar, BTech, Department of CSE, santoshnagireddi1983@gmail.com

N.Sai charan,B.Tech, Department of CSE, charannagamalla52701@gmail.com

ABSTRACT: In order to prevent a cipher's plain text from being decoded without the corresponding key, cryptography is used. In network communication, security is a top priority. Encryption and decryption are the two main components of cryptography, which makes it possible to transfer private and secret information through an insecure network. Data must be hidden from unauthenticated users so that they cannot misuse it. This is the fundamental principle of cryptography. It is nearly impossible to break the algorithm or the key using brute force if you use good cryptography. Good cryptography relies on extremely long keys and encryption algorithms that are resistant to other forms of attack. Good cryptography's next step is represented by the neural net application. When it comes to cryptography, neural networks can be a useful tool. This paper discusses using neural networks for this purpose. Using neural networks to encrypt and decrypt, the neural network will be trained with keys and plain text in this study. An experimental demonstration is also included in this publication.

Cryptography, encryption, and decryption are all terms used here.

1. INTRODUCTION

Kryptos, from the Greek kryptos meaning hidden or secret, is the root of the term "cryptography." Communication in the presence of an untrustworthy third party can be secured using this method. This discipline of mathematics and computer science focuses on the art and science of encrypting and decrypting information. Data is encrypted and decrypted during the process. It also makes it possible to communicate data over an unsafe network safely. A key is used to plain text to transform it into ciphertext, and the process of decryption is the opposite. The basic model of cryptography is as follows.

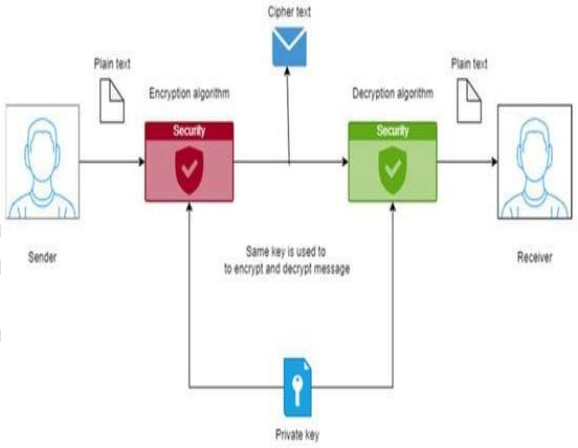

Fig.1: Image encryption decryption

The field of cryptography is concerned with devising news-storage security mechanisms that prevent unauthorised readers from accessing confidential information. The cypher systems are the systems that protect data. The cypher key is a set of principles used to encrypt every piece of news. The process of converting plain text, such as a message, into cypher text by applying rules is known as encryption. It is a reverse process: the cypher is deciphered by the recipient, and the original text is deciphered by the recipient. One of the most important parts of the encryption process is the cypher key. Singularity in encryption and cryptanalysis is the greatest option. For the most part, the open text is formed of characters from the international alphabet, numbers, and punctuation. The cypher text is identical to the open text in composition. International alphabet characters and/or numerals are frequently found. The reason for this is the ease with which information may be transported via various media. Next on the list of cypher systems are transposition cyphers,

substitution cyphers, and cypher tables and codes, all of which can be traced back in time. The inclination to read cypher news without knowing the cypher key developed at the same time as information secrecy. The use of cypher keys was rigorously monitored. It is the primary purpose of cryptology to guess the cypher news and to reconstruct the used keys with the help of effective cypher news analysis. It also makes use of well-known cipher-related blunders, such as those in statistics, algebra, and mathematical linguistics. Every cypher system reflects the legality of the open text and the used cypher key. This legality can be reduced by enhancing the cypher key. The cypher system is safe since it is impervious to deciphering.

2. LITERATURE REVIEW

2.1 Key-insulated symmetric key cryptography and mitigating attacks against cryptographic cloud software [7] :

Cryptographic software is vulnerable to software-based assaults (e.g., malware) since the associated cryptographic keys can be compromised in their entirety. To lessen the impact of repeated attacks on cryptographic software, we look into key-insulated symmetric key cryptography in this study. Our proof-of-concept implementation in a Kernel-based Vir-tual Machine (KVM) environment shows that key-insulated symmetric key cryptography is feasible.

Associative memory learning in a recurrent neural network is governed by the following:

We provide a new rule for neural network learning that applies to intralayer connections. The rule is derived from information theoretic considerations and is based on Hebbian learning principles. The associative memory-like features of a basic network trained using this rule have been demonstrated. The network builds connections between data points that are related to each other, but only if certain conditions are met.

Learning and generalisation of linearly separable Boolean functions through the Hebb rule

An arbitrary linearly separable Boolean function defined on the hypercube of size N is investigated using the Hebb solution. In the N limit, we calculate the learning and generalisation rates. P/N = P/N can be used as an analogy to indicate how many learnt patterns there are.

[10] A New Steganographic Method employing Neural Networks.

The information, or a string of characters containing the information, is concealed in a carrier image using the steganographic approach. The data is encoded into the carrier's constituent primary rows. This method makes use of a neural network to find the hidden message within the carrier image's individual rows and to obtain the message's contents. The visual quality of the carrier picture can be maintained using this method. The PSNR and MSE values of the unmodified carrier and the steganographic image were found to be much lower using this technique.

It's a model of associative memory called the "Associatron" [11].

The human brain's ability to think relies heavily on systems of association that can also be used to artificial intelligence. The "Associatron," an associative memory device, has been proposed. In the Associatron, entities are stored in a dispersed fashion and can be retrieved from a single bit pattern. In large parts, the recalled entities will be accurate; on the other hand, in minor parts the recalled entities will be confusing. However, the recall accuracy declines exponentially with an increase in stored entities. Each cell is connected just to its neighbours and all cells run in parallel in the Associatron, which is considered a simplified form of the neural network. Some aspects of its systems are likely to be used for human-like information processing. A computer simulation of an Associatron, which deals with entities with less than 180 bits, is run after these features have been examined. Concept creation and game-playing examples are shown, and the chain of associations used to think is explained.

Neuronal theory of connection and concept formation: 2.6

These high-level brain functions, such as association and concept creation, are investigated in this research for potential neural mechanisms. Associative and conceptual concepts are provided as primitive neural models in order to explain how knowledge is stored in the brain. Orthogonal and covariance learning principles govern the self-organization of synaptic weights in the models. Self-organization is shown to be converging, and the properties of these learning principles are demonstrated. The association net and concept-formation net's performances, in particular their noise immunity, are examined.

Associative neural networks can be used to monitor the wear of on-the-spot tools.

In this paper, an auto associative neural network-based tool wear monitoring approach is presented. The model's key advantage is that it can be developed using simply the data under regular cutting conditions. As a result, the tool wear status training samples are no longer required during the training process, making it easier to apply in a real industrial scenario than other neural network models. Other methods Tool wear can be indicated by an averaged distance indicator, which can also indicate how severe it is. For better auto associative neural network convergence accuracy, the Levenberg–Marquardt (LM) training procedure is included. An online tool condition monitoring framework is illustrated and cutting force data under different tool wear statuses are gathered to simulate the online modelling and monitoring process for rough and finish milling, respectively, in accordance with the proposed approach This study's findings suggest that the proposed indicator is more accurate than gradient descent approaches at reflecting tool wear evolution. Consequently, it sheds light on how neural networks can be used practically for on-line tool status monitoring.

2.8 A search engine for computer- and network-located images and photographs based on cognitive memory and auto-associative neural networks [14]:

Input data, images, or patterns can be saved in cognitive memory systems, which can then retrieve them without knowing where they were stored in response to a query pattern that is related to the previously stored pattern in question. For the cognitive memory's retrieval system, neural networks and techniques for pre-processing query patterns are used to build a relationship between the query patterns and the sought-after patterns, locate the sought-after patterns, and retrieve them and associated data. computational architecture that can be applied to navigation, location, and recognition of objects in images, character recognition, facial recognition, medical analysis, and video image analysis is introduced when cognitive memory is connected to a computer or information appliance. When prompted with a query photograph containing faces and objects, photographic search engines can retrieve related photographs stored in a computer or other in-memory device.

Linear autoassociative and principal component approaches to categorization and identification of human face images using neural networks

Recent statistical and neural network models of face processing propose that the eigendecomposition of a matrix encoding pixel-based descriptions of a collection of face photos can efficiently describe faces. The research given here shows that basic linear models (linear autoassociator or principle component analysis) and pixel-based coding of the faces can describe the information useful for addressing seemingly complex tasks such as face categorization or identification.

3. IMPLEMENTATION

For cryptanalysis, the ultimate goal is to make it possible for a coded message to be deciphered without the use of a key. Encryption uses two main techniques: symmetric and asymmetric. In symmetric encryption, the encryption and decryption keys are shared by both parties. P stands for plain text, while K stands for the secret key used by the sender to construct C stands for encrypted, or cypher text, i.e.

$$C = \text{Encrypt}(K, P) \quad (1)$$

It is possible to communicate the cypher text after it has been generated. Once received, the cypher text can be decrypted using the same key that was used for encryption to return to the original plain text, as follows:

$$P = \text{Dencrypt}(K, C) \quad (2)$$

One key is used for encryption, and the other is utilised for decryption in asymmetric encryption. A cryptographic key's length is often expressed in bits. Each new key is an opportunity to improve security, and this is true regardless of which cryptographic algorithm allows for additional bits to be included in the key in a given key.

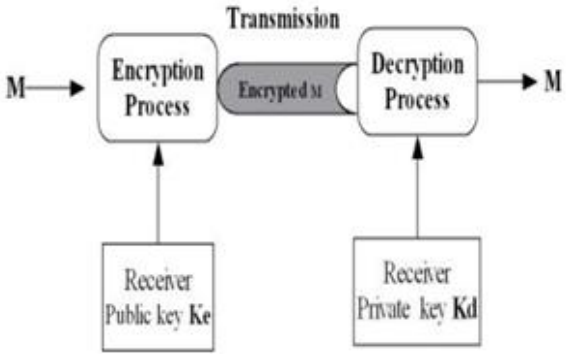

Fig.2: System architecture

CRYPTOGRAPHY:

Encryption and decryption are the two processes that are used to hide sensitive information from prying eyes while it travels over an insecure network.

Cryptography Using a Public Key:

It is an asymmetric cryptography model that is employed in this system [2]. Because the public key is known to all the network's users for encryption of plain text, it is referred to as a "shared key" [1]. As long as the receiver has access to the private key, they can decrypt the message [3, 4]. The term "Private Key" refers to a type of encryption key that is only visible to the individual people that have it.

Cryptography Using a Single Key:

The symmetric cryptography model is employed in this system. This secret key, which is a private key, is used both for encrypting plain text and decrypting cypher text [5]. Because a single key is used for both encryption and decryption, the term "shared secret key" has become popular. The sender and receiver are the only ones who have access to the shared key in this instance [6, 7].

Networks of neurons:

Artificial intelligence, machine learning, and deep learning all benefit from neural networks' ability to mimic the human brain's functioning. Deep learning methods rely on neural networks, often known as artificial neural networks (ANNs) or simulated neural networks (SNNs). Because they replicate the way biological neurons communicate with one another, their name and structure are derived from the human brain as well.

Information processing paradigms inspired by biological nervous systems, such as the brain, are known as Artificial Neural Networks (ANNs). The information processing system's architecture is a critical component of this paradigm. In order to tackle certain problems, it is made up of a vast number of intricately coupled processing parts (called neurons). As with human beings, artificial neural networks (ANNs) learn by mimicry. A learning process is used to customise an ANN for a particular application, such as pattern recognition or data classification. Synaptic connections between neurones are altered during learning in biological systems. This is also true for ANNs.

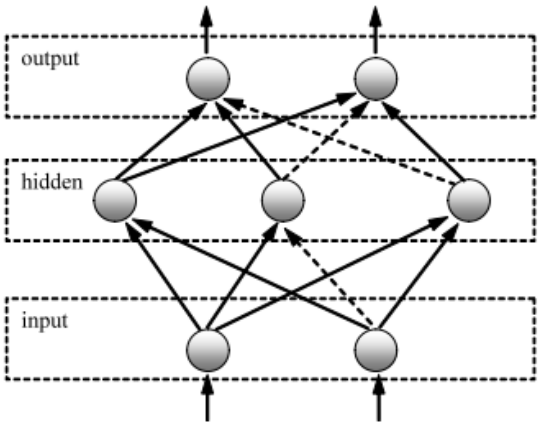

Fig.3: A general three layer neural network

This neural network is one of the most complex for supervised learning. Multilayer feedforward neural networks are the topology of the network.

In our experimental study, the following are the parameters of both ANNs:

There are six nodes in each input layer, each representing a 6-bit block;

• There are a total of six nodes in each concealed layer;

The decrypted output message is defined by six nodes in each output layer.

Full network connectivity;

An activating function of the sigmoid;

• A learning rate is equivalent to 0.03.

Encryption and decryption algorithms using neural networks have proven to be effective. Keys for cryptography were created using parameters from both modified neural networks. Backpropagation was used to adjust multilayer neural networks. Each neural network's topology is determined by the data it has been trained with (see Table 1). The input message is separated into 6-bit data sets throughout the encryption process, and 6-bit data sets are also produced following the encryption process. This means that each system was built as follows: Six units on the input layer and six units on the output layer are available. In the buried layer, there is no prescribed number of units, but we used six. Binary symbol representations were used to train both networks. This means that each training set has

chains of numbers and letters equivalent to binary values of their ASCII code, and each chain of punctuation symbols (e.g. 32) is equivalent to a binary value for the ASCII code of space. This random string of six bits becomes the encryption text. A cryptographic key is the foundation of all encryption and decryption systems. For both encryption and decryption, SIMPLE systems rely on a single, unique key. There are two keys in the best systems. Only the second key can decrypt a message encrypted with the first. In order to use the neural network as an encryption and decryption algorithm, the keys must be configured in accordance with both the topologies (architecture) and the configurations of the neural networks themselves (weight values on connections in the given order).

5. ALGORITHMS

1) Encryption:

• The 0s in the key matrix's principal columns should be replaced with bits of plain text, and the new matrix should be called S.

The weight matrix W can now be found as follows:"

$$W = S^T * S$$

•This weight matrix W is the cipher text.

• Send the weight matrix to the receiver.

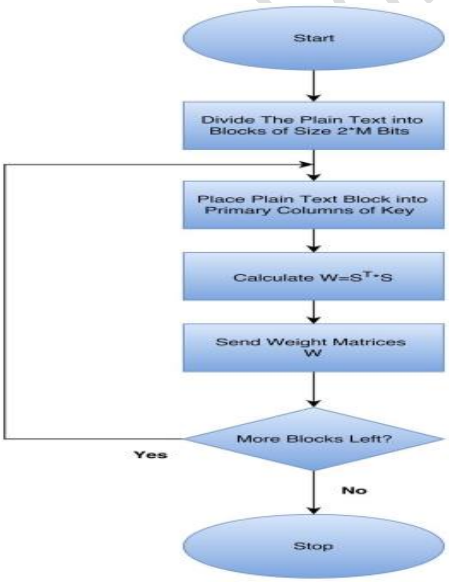

Fig.4: Encryption process

2) Decryption:

The weight matrix W can be used to calculate the matrix C in the following manner:

$$C=K*W$$

• Apply activation function of auto associative memory network on matrix C which is-

$$C[i,j] = \begin{cases} +1 if C[i,j] > 0 \\ -1 if C[i,j] \leq 0 \end{cases}$$

• The plain text will be displayed in the primary columns or even columns of the matrix C when the activation function is applied.

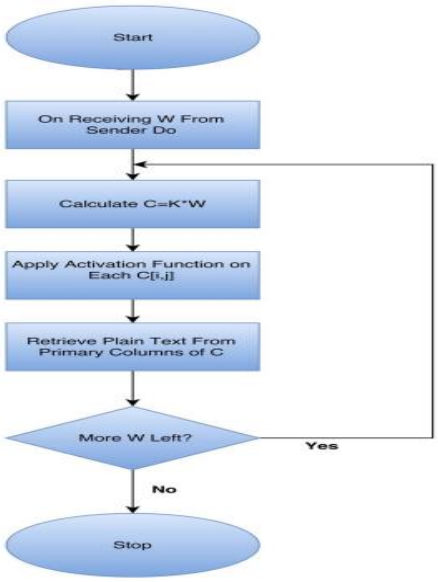

Fig.5: Decryption process

5. EXPERIMENTAL RESULTS

1) Using neural networks to encrypt and decrypt, the neural network will be trained with keys and plain text in this study. In order to train neural networks, weights are calculated between the keys and the neural networks, and this weight is treated as encrypted data. To decrypt the text, simply deliver it to the recipient and have them follow the steps outlined below.
2) Accept a weight matrix for encrypted data.

3) You can decrypt a binary weight value by applying an activation function.
4) By mapping the index to the actual character, the index value is transformed into plain text.
5) The following modules were created specifically for the purpose of carrying out this project:
6) This module will be used to generate keys using random integers.
7) Using this module, we'll design a neural network by computing the weight of each key and each character in the text.
8) Third, we'll employ neural networks to recalculate the weights between the keys and the user's message before encrypting it. When you do the math, you'll get an encrypted matrix.
9) We'll use this module to decrypt encrypted weight values, and then apply an activation function to turn the weight values into binary indexes, which will subsequently be mapped to plain text in the original message in order to decrypt it.

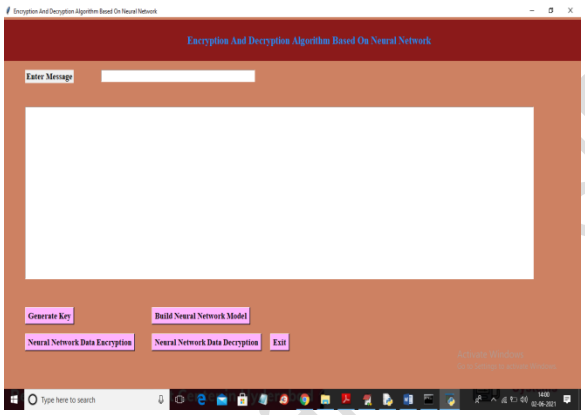

Fig.6: Home screen

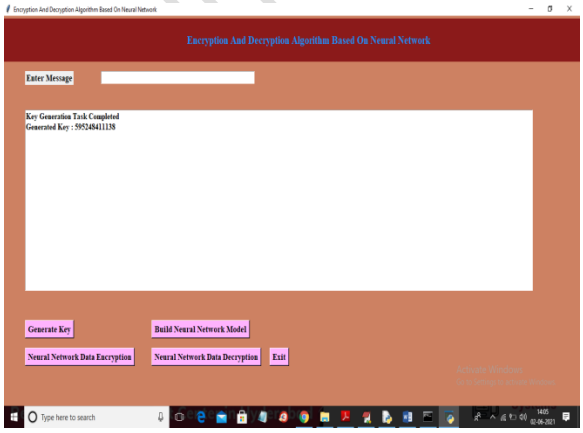

Fig.7: Generate key

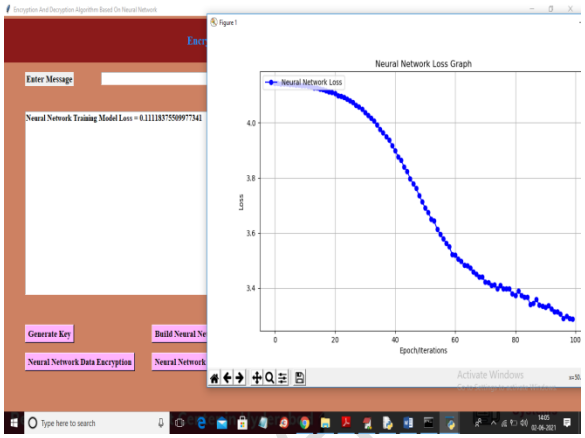

Fig.8: Build neural network model

We can see a reduction in loss from 5.0 to 0.11 in the neural network model shown above, which was constructed using keys and a simple test. The x-axis shows the epoch, while the y-axis shows the loss value. As can be seen in the graph, loss value decreases from 5.0 to 0.1 with each increasing epoch. Now that the model has been created, you can write a message in the text box.

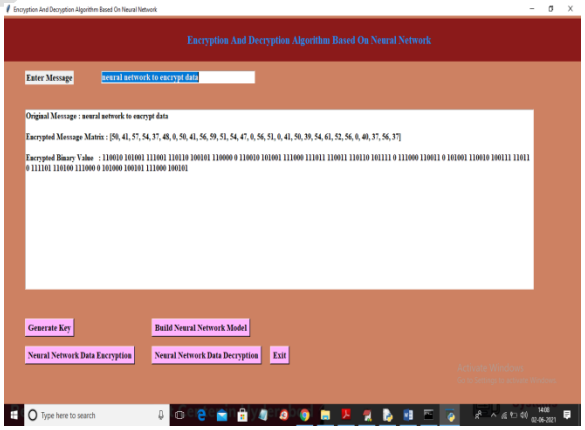

Fig.9: Message screen

To encrypt my message, I typed "neural network to encrypt data" in the text field above and then clicked the "Neural Network Data Encryption" button.

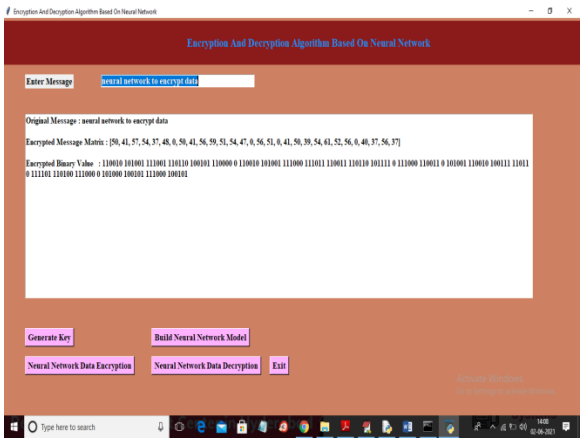

Fig.10: Neural network data encryption

Encrypted binary and matrix numbers are displayed in the above screen. To decode the message, click the "Neural Network Data Decryption" button.

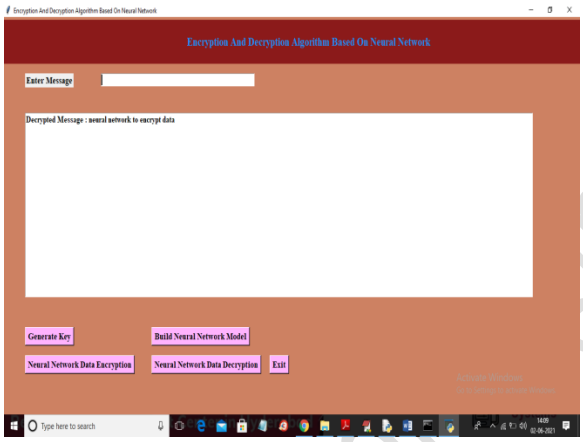

Fig.13: Neural network data decryption

Decryption of the message can be seen in the text box on the right-hand side of the screen. If you have a message to encrypt or decrypt, you can do so by entering it into the application.

Note that the key generation and neural network model button must be clicked just once when the application is activated, and then you can execute encryption and decryption any number of times.

6. CONCLUSION

However, we might still raise concerns about the neural net application as a potential next step in the evolution of secure encryption. What are the system's limitations? This type of technology has only a few drawbacks, but those drawbacks could have severe consequences. This is a secret-key system, with the key being the network's weights and design. Breaking the encryption is now a piece of cake because to the weights and the design. Encryption and decryption, on the other hand, necessitate both weights and architecture. The only way to break it is to know both. What are the benefits of using this method? For example, if you don't know how the system works, it appears to be extremely tough to break it. Besides that, it can handle a lot of noise. Standard encryption schemes prevent most messages from being altered by even a single bit. The encoded message can fluctuate and yet be correct thanks to the neural network-based approach.

REFERENCES

[1] M. Hellman, "An overview of public key cryptography", IEEE CommunicationsMagazine, 2002, 40(5): 42-49.

[2] Diffie W, Hellman M., "New Directions in Cryptography". IEEE Transactions on Information Theory. 1976, 22(6):644-654.

[3] L. P. Yee and L. C. D. Silva. Application of multilayer per- ceptron networks in public key cryptography. Proceedings ofIJCNN02,2(Honolulu,HI,USA):1439–1443, May2002.

[4] Salomaa, Arto. Public-key cryptography. Springer Science & Business Media, 2013.

[5] Law, Laurie, et al. "An efficient protocol for authenticated key agreement."Designs, Codes and Cryptography 28.2 (2003): 119-134.

[6] McInnes, James L., and Benny Pinkas. "On the impossibility of private key cryptography with weakly random keys." Advances in CryptologyCRYPT0'90. Springer Berlin Heidelberg, 1991. 421-435.

[7] Dodis, Yevgeniy, et al. "Key-insulated symmetric key cryptography and mitigating attacks against cryptographic cloud software." Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. ACM, 2012.

[8] Jacob, Theju, and Wesley Snyder. "Learning rule for associative memory in recurrent neural networks." Neural Networks (IJCNN), 2015 International Joint Conference on. IEEE, 2015.

[9] Vallet, F. "The Hebb rule for learning linearly separable Boolean functions: learning and generalization." EPL (Europhysics Letters) 8.8 (1989): 747.

[10] Phadke, Akshay, and Aditi Mayekar. "New Steganographic Technique using Neural Network." International Journal of Computer Applications 82.7 (2013): 39-42.

[11] Nakano, Kaoru. "Associatron-a model of associative memory." Systems, Man and Cybernetics, IEEE Transactions on 3 (1972): 380-388.

[12] Amari, S-I. "Neural theory of association and conceptformation." Biological cybernetics 26.3 (1977): 175-185.

[13] Wang, Guofeng, and Yinhu Cui. "On line tool wear monitoring based on auto associative neural network." Journal of Intelligent Manufacturing 24.6 (2013): 1085-1094.

[14] Widrow, Bernard, Juan Carlos Aragon, and Brian Mitchell Percival. "Cognitive memory and auto-associative neural network based search engine for computer and network located images and photographs." U.S. Patent No. 7,991,714. 2 Aug. 2011.

[15] Valentin, Dominique, Hervé Abdi, and Alice J. O'TOOLE. "Categorization and identification of human face images by neural networks: A review of the linear autoassociative and principal component approaches." Journal of biological systems 2.03 (1994): 413- 429.