ENCRYPTION AND DECRYPTION ALGORITHM BASED ON NEURAL NETWORKS

A.A.Narasimham (Ph.D) , Associate Professor, Dept.of Computer Science and Engineering, Raghu Engineering College, Visakhapatnam, narasimham.aa@raghuenggcollege.in
Duddu Srinivasa Pavan Kumar,Gandi Sowdhamini,Guttula Ramya, 4th B. Tech Students, Dept. of Computer Science and Engineering, Raghu Engineering College, Visakhapatnam
19981a0541@raghuenggcollege.in, 20985a0507@raghuenggcollege.in, 19981a0556@raghuenggcollege.in

ABSTRACT

The project describing neural networks, their numerous properties, and practical uses. A machine called a neural network is created to function similarly to the brain. It can easily carry out complicated calculations. Data exchange between users without data leakage to others is called cryptography. Many public key cryptography exist that are based on numerical theory, but they are constrained by the lack of powerful analytical tools, trigonometry, and time requirements for key generation. We constructed neural network as the ideal method to build a secret key in order to get around these restrictions. We used the ideal strategy for the study of cryptography in this. Neural networks are being used to explore cryptography. We included training strategies and knowledge of numerous additional neural network topologies in our article. To convey information securely through a communication network, we combine the self-associative neural network principle with encryption technology. The fundamental principle of cryptography is to protect data from unauthorised users who might abuse it.

Keywords: Cryptography , Encryption , Decryption , Neural Network

INTRODUCTION

The need for safe channels for data transmission has always increased as communication technology continues to advance. Building such channels has always been successful thanks to cryptography. These channels are utilized by numerous devices, including mobile phones, the internet, digital watermarking, and private communication protocols. For a safe data transfer, a number of encryption-decryption techniques, such as public and private key cryptosystems, may be improvised. Nonetheless, there is still a significant chance that an intruder may attack. Here, a novel method has been used to apply neural networks to cryptography. As a result, if the key is made public, the message transfer in the case of shift cyphers would not be secure. As a result, if the key is made public, the message transfer in the case of shift cyphers would not be secure. Sending it across a neural network ensures that the transfer is secure by keeping the key secret. Also, The RSA cryptosystem makes use of neural networks as a useful technique, which entails two keys that can be quickly found by figuring out the factor issue.

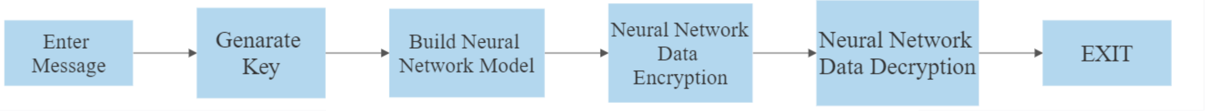

Enter Message
Genarate Key
Build Neural Network Model
Neural Network Data Encryption
Neural Network Data Decryption
EXIT

Fig: Building Blocks of the Suggested System

LITERATURE REVIEW

Recently, numerous studies using neural networks in cryptography have been conducted by numerous scholars. Hence, the following literatures are discussed:

Artificial neural networks have been discussed by Zurada [1] in relation to various learning strategies and network characteristics. In-depth explanations of supervised and unsupervised learning have been provided with the use of network design. It is demonstrated how to use parameters for training. The backpropagation algorithm has been used to describe how error functions in multilayer feedforward networks are minimized.

Koshy [2] has placed emphasis on problem-solving strategies and how to use them. We might discover the least residues with the aid of Fermat's Small Theorem. The various encryption-decryption algorithms are illustrated through various cryptosystems. The cryptosystem has been split and thoroughly discussed based on the key usage.

By synchronising neural networks for the safe transmission of secret messages, Kanter and Kinzel [3] introduced the theory of neural networks and cryptography. The encryption approach is based on synchronising neural networks through reciprocal learning, which entails creating two neural networks and synchronising their synaptic weights through the exchange and learning of shared outputs for certain inputs. One's output could instruct the other's network. When the outputs disagree, the Hebbian learning rule is applied to update and change the weights. The time it takes for those two networks to synchronise tends to get shorter as the amount of the inputs gets bigger. The author focuses on reducing the number of time steps in the synchronisation process from hundreds to the fewest number while simultaneously preserving network security.

[4] Laskari et al. looked examined how artificial neural networks performed on cryptography-related challenges based on several kinds of computationally challenging cryptosystems. They have provided examples of several approaches for employing artificial neural networks to tackle these issues and find better answers. The computational intractability of a cryptosystem can be used to assess its effectiveness. The discrete logarithmic problem, the Diffie-Hellman key exchange protocol, and the factorization problem are the three topics covered in this essay. Artificial neural networks have been used to train feedforward networks for plain and ciphered text using the backpropagation technique. It seeks to minimise the discrepancy between the actual and planned output by properly weighting the network. The network is fed with the normalised data, and its performance is then assessed. The close measure and the trained data percentage are assessed.

The vulnerability of RSA cryptography to several attacks has been examined by Meletiou et al. [5]. As the author computed the euler totient function using an artificial neural network to determine the decoding key, RSA cryptography is vulnerable to being readily faked. The data set is trained using a multilayer feedforward network with backpropagation of mistakes. Although the learning rate of the network may not be optimal, it is asymptotically feasible. The complete and close measure of errors are used to gauge network performance. Additionally, the outcome has been confirmed for prime numbers with a range of high to low values.

METHOD

CNN Algorithm: CRYPTOGRAPHY

Asymmetric cryptography is used in this system, which uses a public key for encryption [2]. The public key is referred to as a "shared key" since it is used to encrypt plain text and is known by all users of the network [1]. The message can be decrypted as long as the recipient has access to the secret key [3, 4]. A sort of encryption key that is only visible to the specific individuals who possess it is referred to as a "Private Key."

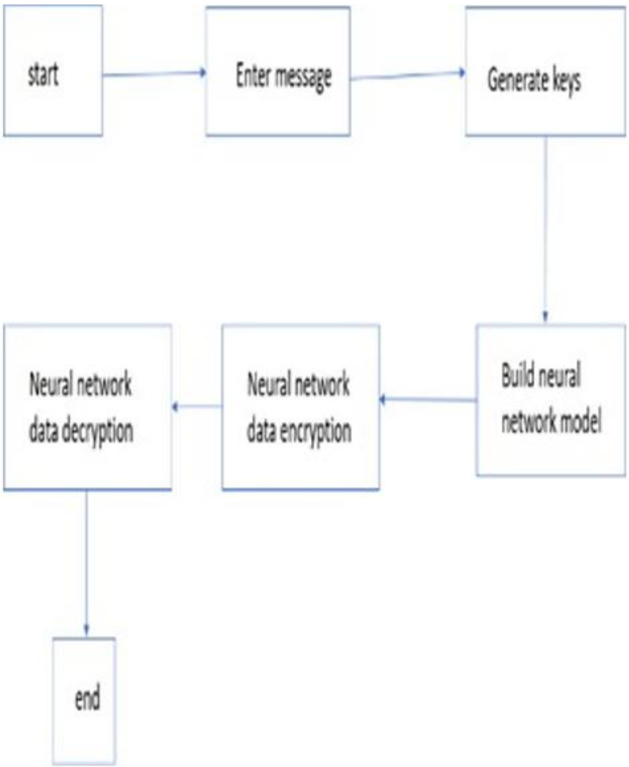
Single-Key Symmetric Cryptography: This system uses the symmetric cryptography model. This private secret key is used to encrypt and decrypt cypher text as well as plain text [5]. The phrase "shared secret key" has gained popularity as a result of the fact that a single key is utilised for both encryption and decryption. In this situation, only the sender and recipient have access to the shared key [6, 7].

Networks of neurons:

Artificial intelligence, machine learning, and deep learning all benefit from neural networks' ability to mimic the functions of the human brain. A crucial element of deep learning techniques are neural networks, commonly referred to as artificial neural networks (ANNs) or simulated neural networks (SNNs). Due to the fact that they replicate how real neurons actually communicate with one another, its name and structure are also inspired by the human brain.

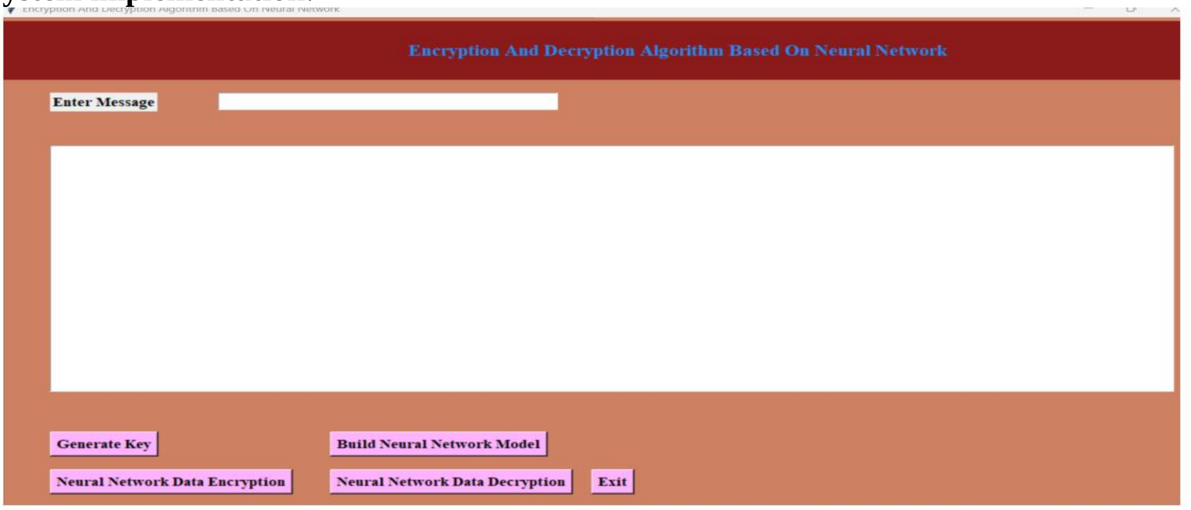
Information processing models called artificial neural networks are inspired by biological nerve systems like the brain (ANNs). The layout of the information processing system is a crucial component of this paradigm. To handle certain problems, it is made up of a lot of closely coupled processing components (called neurons). Similar to how people learn, artificial neural networks (ANNs) imitate other things to develop new skills. An ANN is tailored for a specific purpose, such as pattern recognition or data classification, using a learning process. In biological processes, learning modifies the synaptic connections between neurons.

Flow chart:


start
Enter message
Generate keys
Build neural network model
Neural network data encryption
Neural network data decryption
end

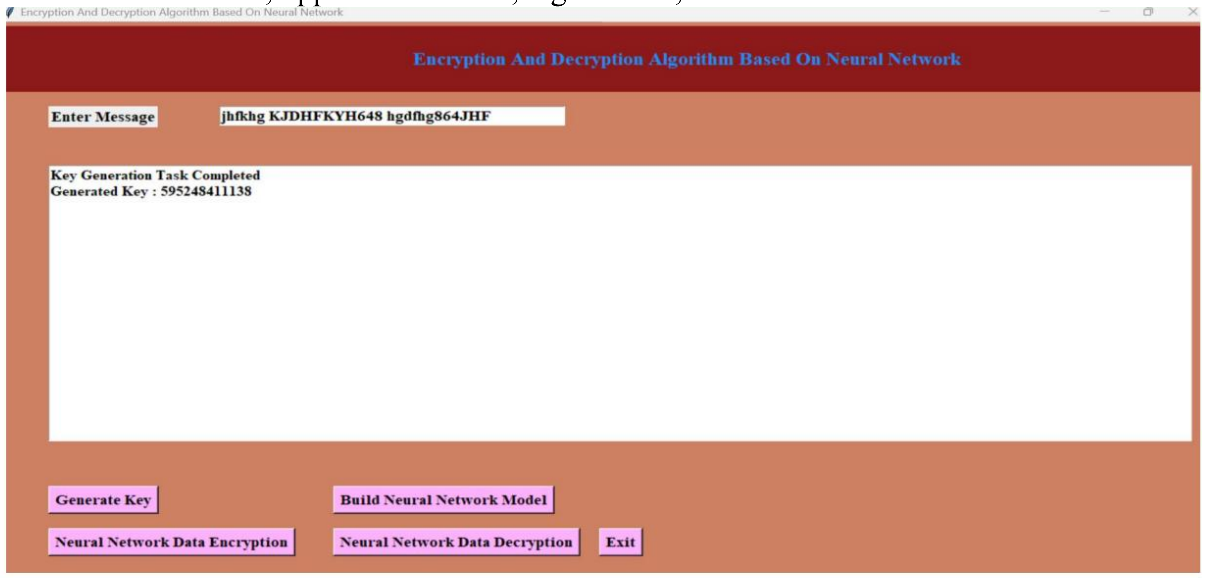
Flow chart of proposed system

System implementation:


Encryption And Decryption Algorithm Based On Neural Network
Encryption And Decryption Algorithm Based On Neural Network
Enter Message
Generate Key
Build Neural Network Model
Neural Network Data Encryption
Neural Network Data Decryption
Exit

GUI of Encryption and Decryption Algorithm

Step1-Enter Message: Message is nothing but plain text . Plain text is usually ordinary readable text. Ex: lowercase letters , upper case letters , digits etc…,

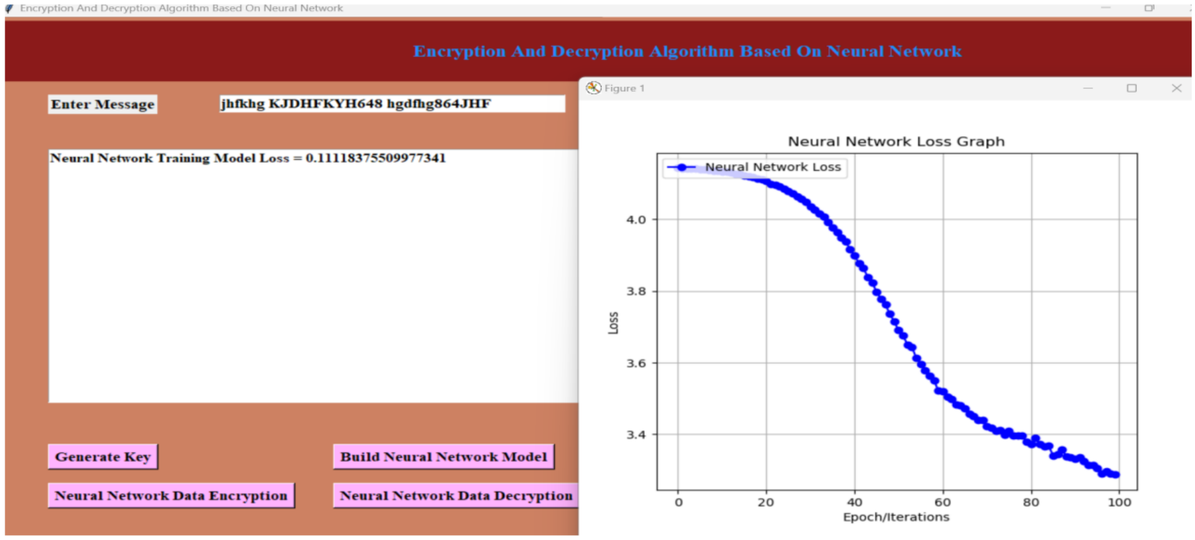

Encryption And Decryption Algorithm Based On Neural Network
Encryption And Decryption Algorithm Based On Neural Network
Enter Message

jhfkhg KJDHFKYH648 hgdfhg864JHF

Key Generation Task Completed
Generated Key : 595248411138

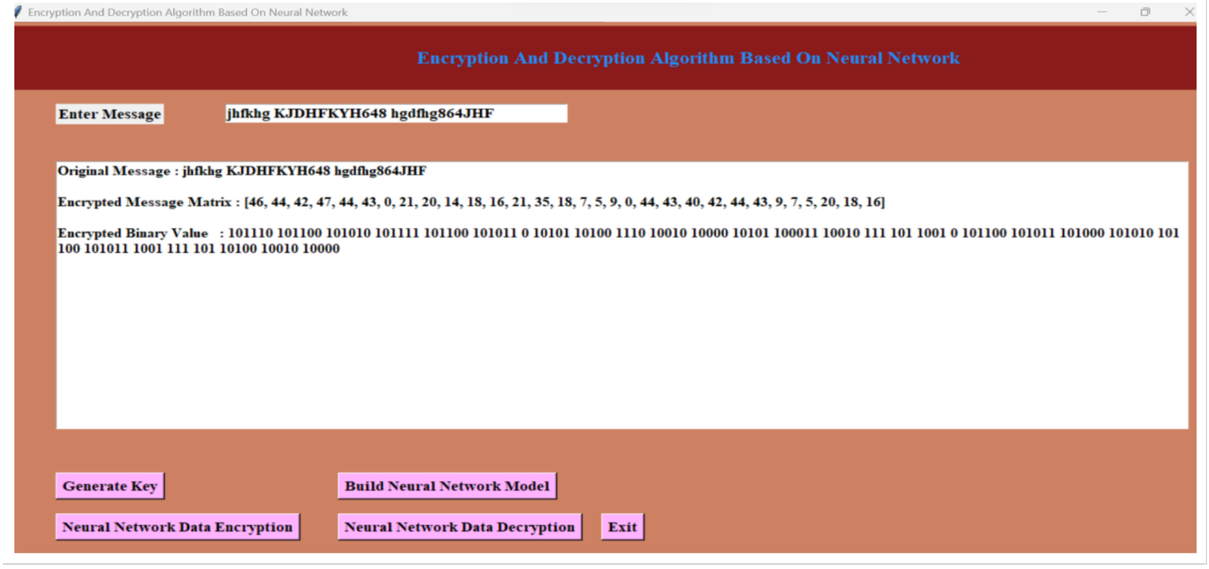
Generate Key
Build Neural Network Model
Neural Network Data Encryption
Neural Network Data Decryption
Exit

Step2- Generation of Key: In this step we will generate random keys for Encryption and Decryption algorithm based on neural networks.


Encryption And Decryption Algorithm Based On Neural Network
Encryption And Decryption Algorithm Based On Neural Network
Enter Message
jhfkhg KJDHFKYH648 hgdfhg864JHF
Generate Key
Build Neural Network Model
Neural Network Data Encryption
Neural Network Data Decryption
Figure 1
Neural Network Loss Graph
Neural Network Loss
Loss
4.0
3.8
3.6
3.4
0
20
40
60
80
100
Epoch/Iterations

Neural Network Training Model Loss = 0.11118375509977341

Step3- Build Neural Network Model: Keys and a straightforward test are used to construct a neural network model, and we observe a reduction in model loss from 5.0 to 0.11. The graph's y-axis represents loss value, and the x-axis represents epoch. The graph above shows that the loss value drops from 5 to 0.1 with each subsequent increasing epoch, and if a neural network's loss value falls to zero, it can be said to be dependable.

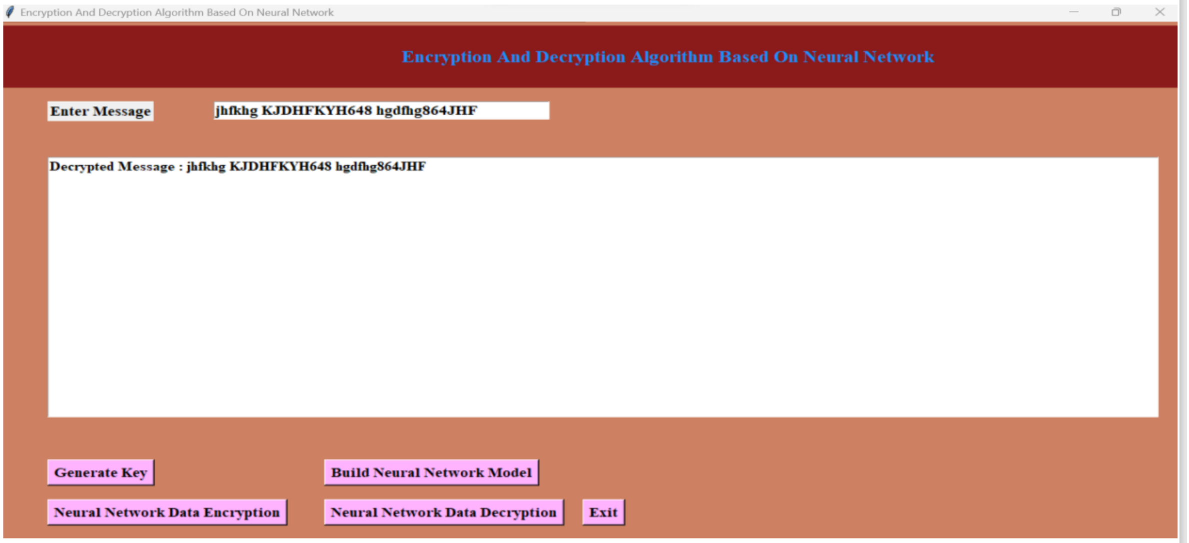

Encryption And Decryption Algorithm Based On Neural Network
Encryption And Decryption Algorithm Based On Neural Network
Enter Message
jhfkhg KJDHFKYH648 hgdfhg864JHF
Generate Key
Build Neural Network Model
Neural Network Data Encryption
Neural Network Data Decryption
Exit

```
Original Message : jhfkhg KJDHFKYH648 hgdfhg864JHF

Encrypted Message Matrix : [46, 44, 42, 47, 44, 43, 0, 21, 20, 14, 18, 16, 21, 35, 18, 7, 5, 9, 0, 44, 43, 40, 42, 44, 43, 9, 7, 5, 20, 18, 16]

Encrypted Binary Value   : 101110 101100 101010 101111 101100 101011 0 10101 10100 1110 10010 10000 10101 100011 10010 111 101 1001 0 101100 101011 101000 101010 101
100 101011 1001 111 101 10100 10010 10000
```

Step4- Neural Network Data Encryption : To encrypt the message, select the "Neural Network Data Encryption" button now. Binary digits and an encrypted matrix were then presented to us.



Encryption And Decryption Algorithm Based On Neural Network

Enter Message: jhfkhg KJDHFKYH648 hgdfhg864JHF

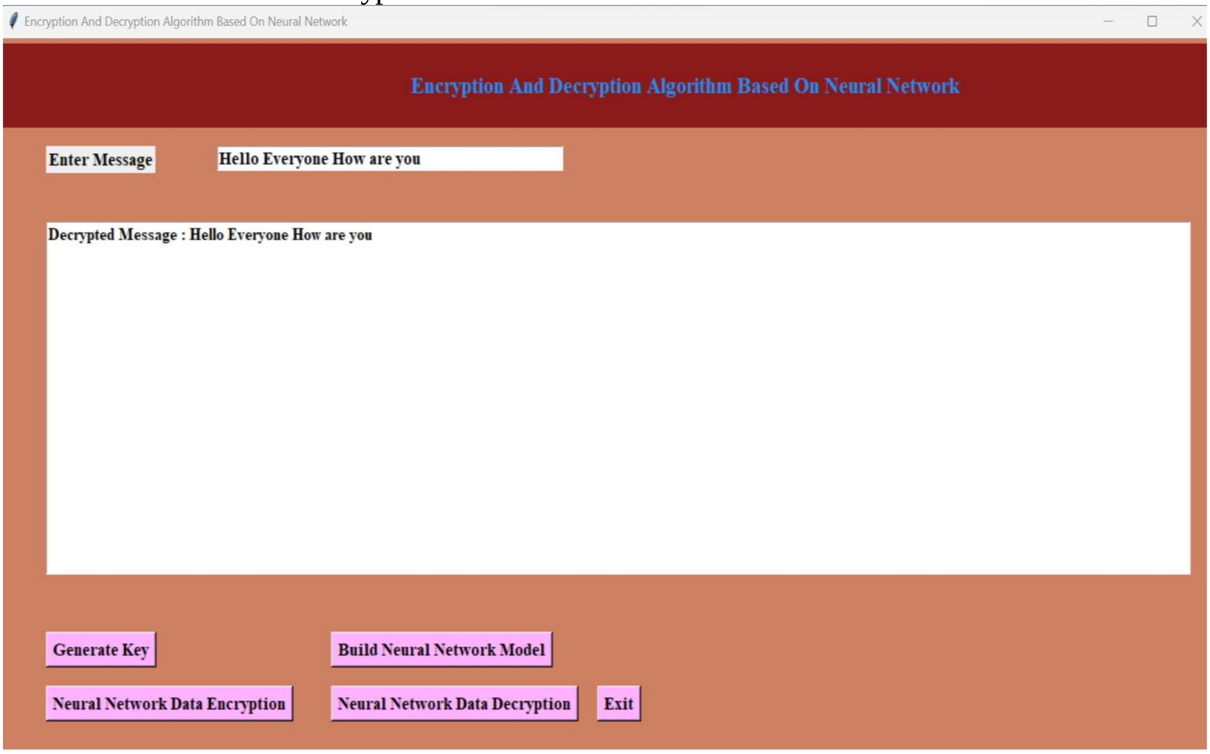
Decrypted Message : jhfkhg KJDHFKYH648 hgdfhg864JHF

Encryption And Decryption Algorithm Based On Neural Network
Generate Key
Build Neural Network Model
Neural Network Data Encryption
Neural Network Data Decryption
Exit

Step5- Neural Network Data Decryption : To decrypt the message, select the "Neural Network Data Decryption" button now. After that, the message was properly decrypted. In a similar manner, you can encrypt and decrypt any communication.

RESULTS

Case1: Initially you enter some message in message box , the same message have came after clicking on neural network data decryption box.



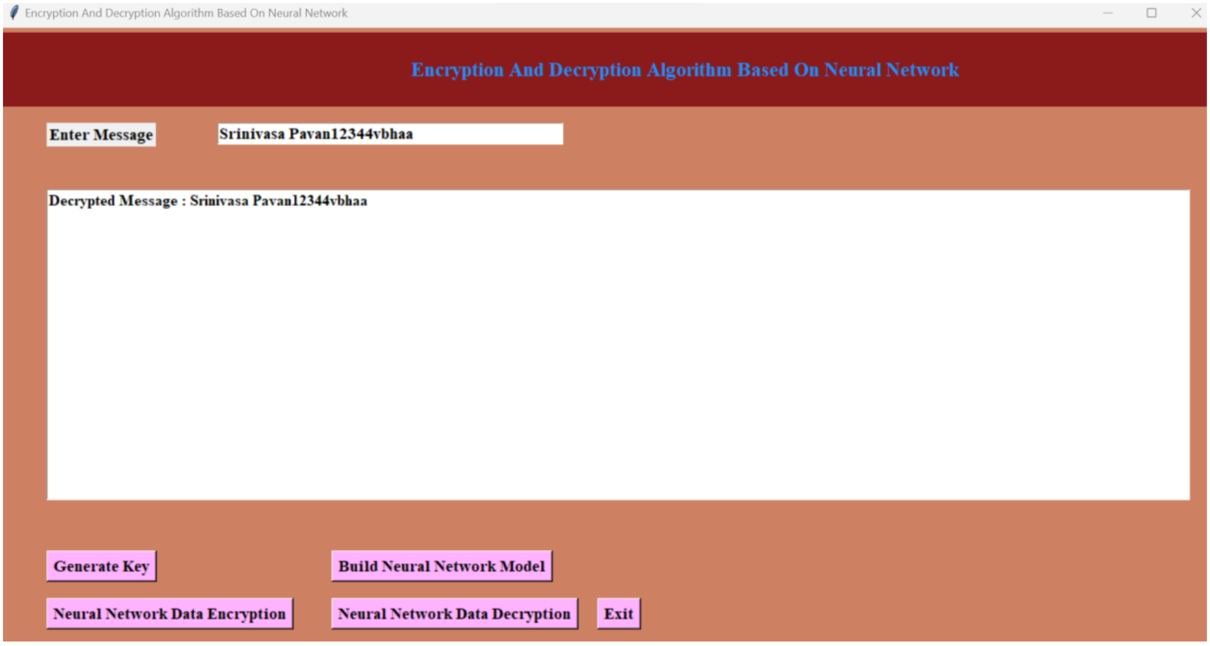
Encryption And Decryption Algorithm Based On Neural Network

Enter Message: Hello Everyone How are you

Decrypted Message : Hello Everyone How are you

Encryption And Decryption Algorithm Based On Neural Network
Generate Key
Build Neural Network Model
Neural Network Data Encryption
Neural Network Data Decryption
Exit

Case2: Initially you enter some message in message box , the same message have came after clicking on neural network data decryption box.



Encryption And Decryption Algorithm Based On Neural Network

Encryption And Decryption Algorithm Based On Neural Network

Enter Message: Srinivasa Pavan12344vbhaa

Decrypted Message : Srinivasa Pavan12344vbhaa

Generate Key
Build Neural Network Model
Neural Network Data Encryption
Neural Network Data Decryption
Exit

DISCUSSION

The proposal of utilising neural networks in the field of cryptography is rapidly gaining ground. Several neuro-crypto algorithms have been put out by academics in the literature. However, the majority of them are restricted to cryptanalysis and key creation. Auto associative memory networks are used in the study to encrypt plain text and convert it into a form that is entirely distinct from the original. The formula has a quicker coding and deciphering pace and is fairly simple to use. Since the algorithm employs a symmetric key scheme, key leakage is a possibility. This can be prevented by limiting the parties involved in correspondence, or by using a specified third party as an associate authority to halt the key run.

REFERENCES

[1]. 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.

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

[3]. 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.

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

[5]. Nakano,Kaoru.”Association-a model of associative memor”.Systems,Man and cybernetics,IEEE Transactions on 3(1972):380-388.

[6]. Amari,S-I.”Neural theory of association and concept formation.”Biological cybernatics 26.3(1997):175-185.

[7]. 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.

[8]. 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.

[9]. Valentin,Dominique.Herve Abdi,and Alice J.O’TOOLE.”Categorization and identification of human face images by neural networks:A review of the linear auto associative and principal component approaches.”Journal of biological systems 2.03(1994):413-429.

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

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

[12]. L.P.Yee and L.C.D.Silva.Application of multilayer perceptron networks in public key cryptography.Proceedings of IJCNN02,2(Honolulu,HI,USA):1439- 1443,May 2002.