International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 795-798 www.ijaem.net ISSN: 2395-5252

Encryption and Decryption Algorithm Based on Neural Network

Dr.M.Malyadri[1],C.Raghavi[2],P.Saivardhan Reddy[3], G.Shravan Kumar[4]

[1]*Associate Professor,Dept of CSE,CMR Technical campus,Kandlakoya,Medchal-501401.*
[2]*B.Tech Student,Dept of CSE,CMR Technical campus,Kandlakoya,Medchal-501401.*
[3]*B.Tech Student,Dept of CSE,CMR Technical campus,Kandlakoya,Medchal-501401.*
[4]*B.Tech Student,Dept of CSE,CMR Technical campus,Kandlakoya,Medchal-501401.*

Submitted: 01-06-2022 Revised: 10-06-2022 Accepted: 15-06-2022

ABSTRACT: The project elaborating Neural Network, its various characteristics and business applications. A Neural Network is a machine which is designed to work like brain. It has the capability to execute complex calculations easily. Cryptography is the interchange of data between the users without seep of data to others. Many public key cryptography are there which are based on numerical theory but it has the limitation of availability of large analytical power, trignometric and time utilization during creation of key. To overcome these limitations, we prepared neural network is the perfect way to create secret key. In this, we implemented a perfect approach in the study of cryptography. We are utilizing neural networks in the study of cryptography. In our article, we had knowledge of many other neural network architectures along with training algorithms. we use self associative neural network concept of soft computing in coordination with encryption technique to send information securely on communication network. The ground idea of cryptography is concealing of the information from unauthenticated users as they can misuse the data.

KEYWORDS: Keysgeneration,NeuralNetworkModel,Encryption,Decryption.

I. INTRODUCTION

This paper aims at removing the necessity for the coding to follow a general rule by employing a neural network for cryptography the cipher text. Thus introducing the randomness in secret writing creating it most harder to decrypt. We've conjointly introduced the thought of as well as lies with in the data transmitted to misguide any listener who manages to decipher the ciphetext.

Security is one among the foremost vital desires in network communication. Cryptography may be a science that involves two techniques secret writing and decipherment and it essentially permits to send sensitive and confidential information over the unsecure network.

II. LITERATURE REVIEW

Key-insulated symmetric key cryptography and mitigating attacks against cryptographic cloud software. **[1] Dodis, Yevgeniy, et al** Software-based attacks (e.g., malware) pose a big threat to cryptographic software because they can compromise the as-sociated cryptographic keys in their entirety. In this paper, we have a tendency to investigate key-insulated radially symmetrical key cryptography, which may mitigate the harm caused by perennial attacks against scientific discipline package.For example,the feasibleness of key-insulated radially symmetrical key cryptography, we have a tendency to additionally report a proof-of-concept implementation within the Kernel-based Vir-tual Machine (KVM) atmosphere.

An efficient protocol for authenticated key agreement. **[2] Law, Laurie, et al**, Authentication and key establishment are fundamental building blocks for securing electronic communication. Cryptographic rule for coding and integrity cannot perform their perform unless secure keys are established and therefore the users grasp that parties share such keys. It's essential that protocols for providing and key institution area unit fit their purpose. This paper proposes a replacement and economical key institution protocol with in the uneven (public key) setting that's supported MTI (Matsumoto, Takashima and Imai)-two pass key agreement protocol which consists of three phases; The Transfer and Verification Phase, and The Key

Generation Phase. This potential attacks(Known-Key Security, Forward (Perfect)Secrecy,Key-Compromise Impersonation, Unknown Key-Share Attack, Small Subgroup Attack, and Man-in-the-Middle Attack) with low complexity (complexity is 4), also it provide authentication between the two entities before exchanging the session keys. On the impossibility of private key cryptography with weakly random keys. **[3] McInnes, James L., and Benny Pinkas**, The properties of weak sources of randomness have been investigated in many contexts and using several models of weakly random behaviour. For two such models, developed by Santha and Vazirani, and Chor and Goldreich, it is known that the output from one such source cannot be "compressed" to produce nearly random bits. At the sametime, however, a single source is sufficient to solve problems in the randomized complexity classes BPP and RP. It is natural to raise precisely that tasks is employing a single, weak supply of randomness and that cannot. This work begins to answer this question by establishing that one frail random supply of either model can not be accoustomed acquire a secure "one-time-pad" kind of cryptosystem. New Steganographic Technique using Neural Network. **[4] Phadke, Akshay, and Aditi Mayekar**, Steganographic technique is used to hide the information,a string of characters information, in a carrier image. The information is coded into individual rows of the constituent primaries of the carrier. Victimisation this system the neural network is utilized to find the presence of the message within the individual rows of the carrier image and to retrieve the contents of the message hidden in the carrier. This technique is able to maintain good visual quality of the carrier image. The results of this technique revealed high PSNR values and significantly less MSE values for the unmodified carrier and the steganographic image.

III. PROPOSED SYSTEM

In this paper author is using neural network to encrypt and decrypt and this neural network will be trained with keys and plain text. While training neural network application calculate weight between keys and neural network and this weight will be consider as encrypted data.This encrypted data can be send to any receiver and then receiver willperform below steps to decrypt text .

1.1 PROJECT ARCHITECTURE

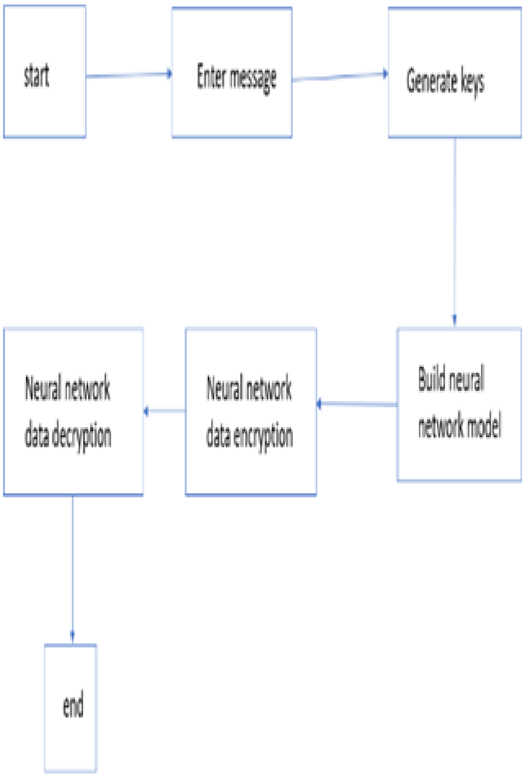

start
Enter message
Generate keys
Build neural network model
Neural network data encryption
Neural network data decryption
end

Fig 1. Architecture diagram of Encryption and decryption algorithm based on neural network

1.2 DATA FLOW DIAGRAM

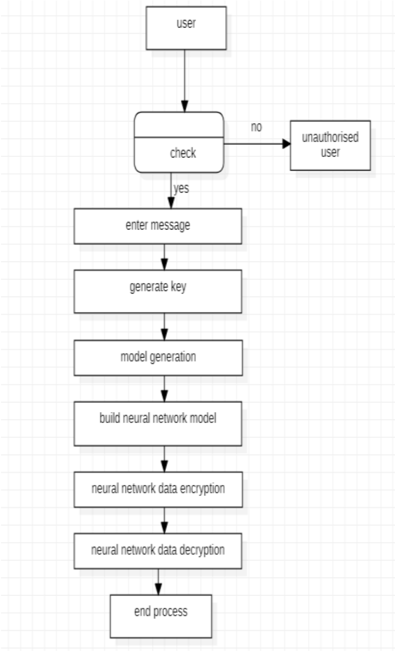
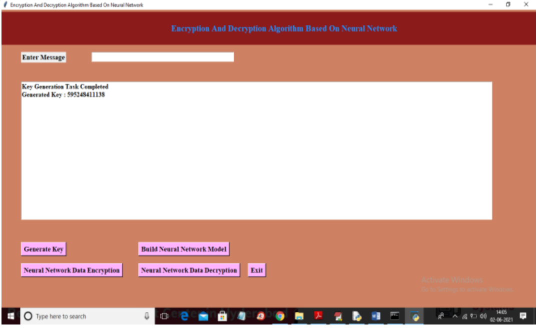

user
check
no
unauthorised user
yes
enter message
generate key
model generation
build neural network model
neural network data encryption
neural network data decryption
end process

Fig 2. Dataflow diagram of Encryption and Decryption alogorithm based on neural network

IV. RESULTS AND DISCUSSION

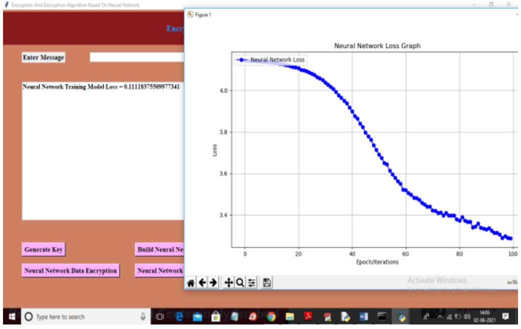
In below screen click on ‘Generate Key’ button to generate keys.


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
Type here to search
14:05
02-06-2021

Key Generation Task Completed
Generated Key : 595248411138

Fig 3. Generation of keys for Encryption and Decryption alogorithm based on neural networks

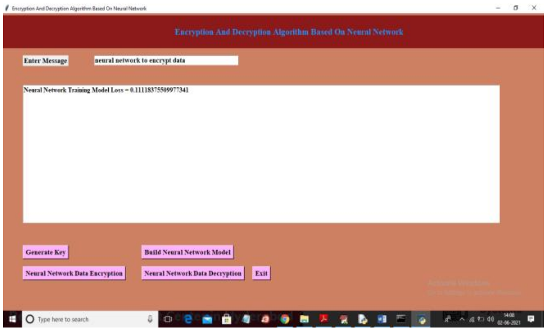
In above screen random key is generated and now click on ‘Build Neural Network Model’ button to generate neural network for encryption and decryption.



Neural Network Training Model Loss = 0.11118375509977341

Fig 4. Neural Network Model for Encryption and Decryption alogorithm based on neural networks

In above screen neural network model is built using keys and plain test and we can see model loss reduce from 5.0 to 0.11 and in graph we can see x-axis represents EPOCH and y-axis represents loss value and we can see in above graph at each increasing epoch loss value is getting decreased and we can see loss value decrease from 5 to 0.1 and in any neural network can be consider as reliable if its loss value decrease to 0. Now model is build and enter some message in text field.

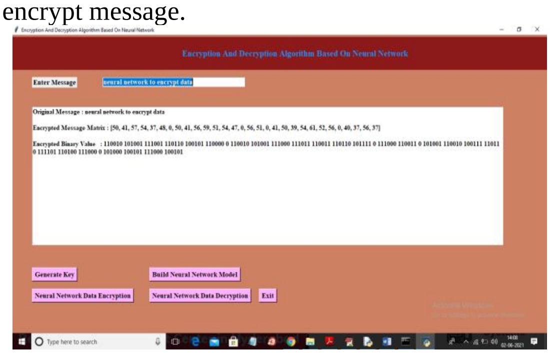

Encryption And Decryption Algorithm Based On Neural Network
Encryption And Decryption Algorithm Based On Neural Network
Enter Message
Generate Key
Build Neural Network Model
Neural Network Data Encryption
Neural Network Data Decryption
Exit
Type here to search

Enter Message: neural network to encrypt data

Neural Network Training Model Loss = 0.11118375509977341

Fig 5..Web page showing Model with zero loss for Encryption and Decryption alogorithm based on neural networks

In above screen in text field I entered message as ‘neural network to encrypt data’ and now click on ‘Neural Network Data Encryption’ button to encrypt message.


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
Type here to search

Enter Message: neural network to encrypt data

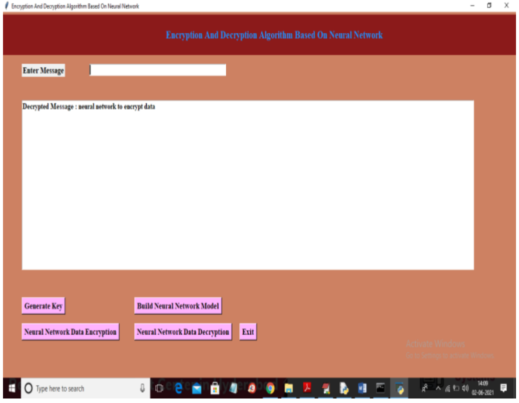
Original Message : neural network to encrypt data

Encrypted Message Matrix : [50, 41, 57, 54, 37, 48, 0, 50, 41, 56, 59, 51, 54, 47, 0, 56, 51, 0, 41, 50, 39, 54, 61, 52, 56, 0, 40, 37, 56, 37]

Encrypted Binary Value : 110010 101001 111001 110110 100101 110000 0 110010 101001 111000 111011 110011 110110 101111 0 111000 110011 0 101001 110010 100111 11011 0 111101 110100 111000 0 101000 100101 111000 100101

Fig 6. Encrypted matrix for Encryption and Decryption alogorithm based on neural networks

In above screen message is encrypted and we got encrypted matrix and binary numbers and now click on ‘Neural Network Data Decryption’ button to decrypt message.


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
Type here to search

Decrypted Message : neural network to encrypt data

Fig 7. Decrypted message for Encryption and Decryption alogorithm based on neural networks

In above screen in text area we can see message is decrypted successfully. Similarly you can enter any message and perform encryption and decryption.

Note: key generation and build neural network model button has to click only one time when application started and then u can perform encryption and decryption any number of times.

V. CONCLUSION

The concept of using neural networks in the field of cryptography is growing at a rapid pace. Various neuro- crypto algorithms planned by researchers are offered in literature. But most of them are limited to the key generation and cryptanalysis. In the research work auto associative memory network is utilized to encrypt the plain text into the form which is totally independent from the previous one. The formula is pretty easy to implement and has quicker coding and decipherment speed. The algorithm is following the symmetric key system which makes it vulnerable to leakage of key. To overcome this, solely sure parties ought to be concerned in communication or a sure third party will be used as associate authority to forestall the key run.

VI. ACKNOWLEDGEMENT

The success of this project includes help from our guide as well.We are grateful tour guide,Mr.M.Malyadri,Associate Professor,CMR Technical Campus,for his expertise that guided us in our research.

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.