| DOI: 10.15680/IJIRCCE.2023.1105321 |

Multiple Image Steganography using DNNs

Prathamesh Yadav, Anandkumar Gupta, Prathamesh Shinde, Shubham Kothawade

UG Student, Dept. of Computer Engineering, Sinhgad Institute of Technology and Science, Pune, India

Mr. Nilesh Kamble

Faculty of Computer Engineering, Sinhgad Institute of Technology and Science, Pune, India

ABSTRACT: Deep Neural Network is a type of ANN that is composed of multiple layers of interconnected neurons, which can be trained using large amount of data to solve a complex task. The deep architecture of DNN allows us to solve complex problem in a simpler way. Steganography is the art of hiding information within other data in such a way which is not easily detectable by observer. It involves use of various techniques to embed data such as text, images etc, with seemingly innocuous cover data such as digital images, audio, video clips. We aim to utilize deep neural networks for the encoding and decoding of multiple secret images inside a single cover image of the same resolution.

KEYWORDS: Steganography, Cryptography, DNNs , ML, Tensor-flow , keras .

I.INTRODUCTION

The Deep architecture of DNNs allows them to learn hierarchical representation of input data, with each layer extracting increasingly abstract and high level features. This makes DNNs capable of achieving state-of-art performance in various domains, such as computer vision and speech recognition. Recent advancement in DNNs has led to development of techniques such as adversarial training , transfer learning ,which have led to performance abilities.

DNN’s has led to major impact on fields such as healthcare, finance and autonomous system.
Cryptography is study of techniques for secure communication in presence of third parties. It involves use of mathematical algorithms and protocols to ensure confidentiality , authenticity of information and to prevent unauthorized access , modification and disclosure of sensitive data. Steganography is the art and science of hiding information within other data in a way that is not easily detectable by an observer. The goal of steganography is to conceal the existence of secret message rather than to encrypt its content. This makes steganography the most powerful tool for covert communication and information exchange. History of Steganography is dated back to ancient times with example such as invisible ink and hidden art messages. In modern times Steganography has become more sophisticated and widely used With application fields such as intelligence gathering , personal privacy. Steganography also possess a significant challenge to digital forensics and security as it allows for covert transfer of sensitive data and can be used to avoid criminal and malicious activities .

Multiple Image Steganography (MIS) is a technique that involves embedding secret data into multiple cover images to increase the capacity and security of steganography. MIS is a relatively new area of research in steganography, and it has gained significant attention in recent years due to its potential to improve the security and robustness of covert communication. MIS algorithms involve splitting the secret message into multiple parts and embedding each part into a different cover image, which can be transmitted through different channels to reduce the risk of detection. MIS can also employ various embedding strategies, such as randomization, data partitioning, and error correction codes, to increase the capacity and robustness of the steganographic system.

II.PROBLEM

The traditional approach to data or message encryption cannot guarantee origin and authenticity of message since both sender and receiver use same key , messages cannot be verified to have come from a particular user , whereas cryptographic message can easily be hacked or the secret message can be easily decoded and hence anyone can decode messages which are secretive and sensitive such message are example of defence message , online transaction messages and messages which are highly sensitive .
Hence we need a more secure way to hide data which is more secure and hence we have used the technique of Multiple Image Steganography.

III.SOLUTION

Hence, we have tried to develop a technique which will be used for transaction of sensitive data from sender to receiver from in a more a secured way ; In this technique we are using the concept of Multiple Image Steganography using Deep Neural Networks .

In this technique we can hide or encrypt a number of images under a single cover image and this cover image will similar to that of the original images and the end user will have a special key to decode the original content .

IV.LITERATURE REVIEW

1. Multi-Image Steganography Using Deep Neural Networks Abhishek Das 1 Japsimar Singh Wahi 1 Mansi Anand 2 Yugant Rana Publication : January 2021. This paper is to provide a new technique that will provide better security for hiding data in an image and watermarked video. A new technique was proposed as security threats are growing day by day a new technique with high level of security is needed . This technique is moderately acceptable based because of high cost and time consuming process for message security.

2. “Improved Message Payload and Security of Image Steganography using 3-3-2 LSB and Dual Encryption.” Authors :PuteriAwaliatushShofro, Kiki Widia ; Publication : July 2021. It maintain the quality of stego- image with maximum message .To improve message security, dual encryption methods are used. Stegnographic technique was used to make sensitive data more secure using LSB . LSB algorithm is used whose execution time and computational cost is much more.

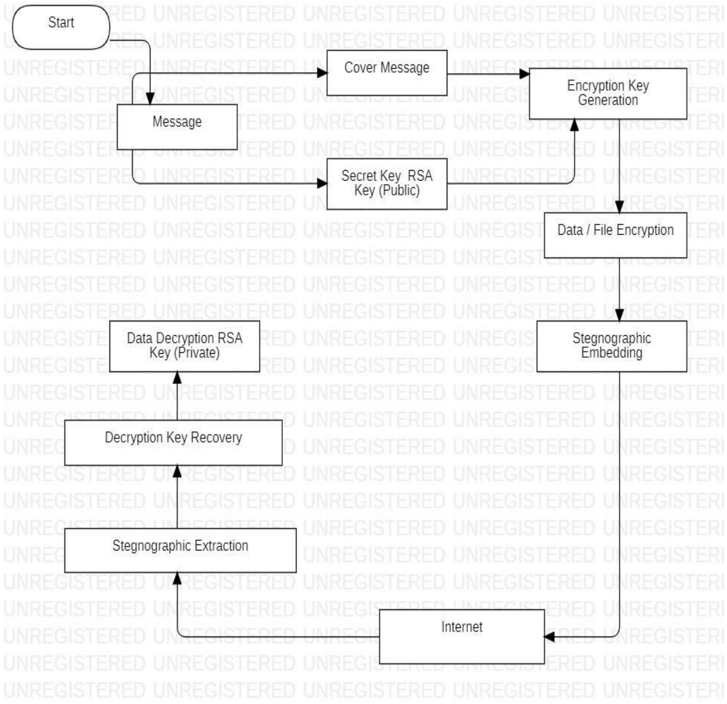
3. “Variance Analysis of Pixel-Value Differencing Steganography , “ Authors : Hao Zhang,TaoZhang,Huajin Chin Publication : December 2020. This paper introduces a novel method to study pixel-value difference (PVD) embedding scheme. Hence novel pixel value difference were studied using embedding scheme , It needs a vast amount of pixel value difference data hence is slow and costly .

4. “New Proposed Practise for Secure Image Stegnography on various Parameter :
Authors:- Rupesh Gupta ,Tanupreet Singh , Publication : July 2021. ,It maintain the quality of stego image with combinigStegnography and Cryptogrsphy using certain parameters , Stegnographic technique was used to make sensitive data more secure using PSNR , MSE , Watermarking , These techniques are more complex and complicated to used instead of other ones.

5. “Inivsible Backdoor attacks on networks via Steganography .” Authors : Benjamin Zhao , Haojin Zhu, Xinpeng Zhang. Publication : December 2020. This paper introduce scattered

Triggers for backdoor attacks .This work has found out that networks are sensitive for features imperceptible to human .It hard to recover Backdoor attacks for invisible triggers through algorithms of various types .

V.PROPOSED SYSTEM



In this above system architecture we are using taking image input and creating a cover image similar to that of images that we have input and the we have to encode these and send it to the receivers by generating the Steganographic Embedding is done and later via the internet we have to send this data to receivers end and at the receivers end and the receiver will have a key which will help the receiver to decode the sensitive data later we will be recovering it by the key . In , this technique we can encrypt multiple images in a single cover image which will be same as that of the data which is sensitive and it will be very difficult for the external threats to identify the real and the cover image difference .

VI.WORKING

Multi-image steganography refers to the technique of hiding secret information within multiple cover images simultaneously. It extends the concept of traditional steganography, which involves embedding information in a single image, to use multiple images as carriers for the hidden data. This technique offers increased security and capacity compared to single-image steganography.

Here is a general overview of how multi-image steganography works:
1. Image Selection: The first step is to select the cover images that will be used to hide the secret information. These cover images should be visually similar to prevent suspicion.

2. Secret Data Encoding: The secret data that needs to be concealed is encoded into a suitable format, typically binary or text. Encryption algorithms may also be applied to enhance the security of the hidden information.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105321 |

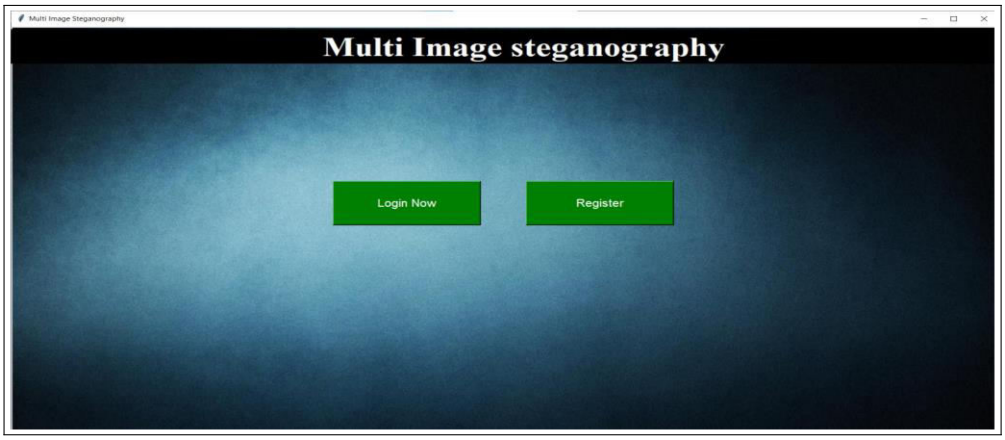
3. Data Distribution: The encoded secret data is divided into smaller chunks or fragments. Each fragment is assigned to a specific cover image in a predetermined manner. The distribution of data fragments across the cover images can be random or follow a specific pattern.

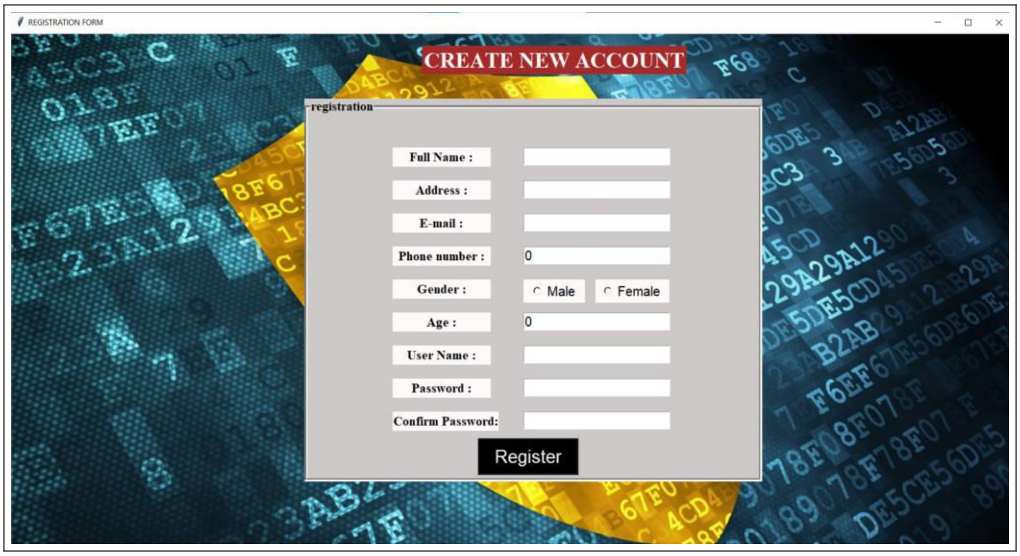
4. Embedding Process: In this step, each cover image undergoes modification to embed the assigned data fragments. Various steganographic techniques can be employed to embed the data, such as least significant bit (LSB) substitution, discrete cosine transform (DCT) modification, or spread spectrum modulation.

5. Extraction of Data: To retrieve the hidden information, the steganographic algorithm is applied to each cover image to extract the encoded fragments. These fragments are then reassembled to reconstruct the original secret data.

6. Decoding and Decryption: If encryption was applied during the encoding process, the extracted data fragments are decrypted using the appropriate decryption algorithm. The decrypted fragments are then combined to obtain the original secret information.

VII.RESULTS





Full Name :

Address :

E-mail :

Phone number : 0

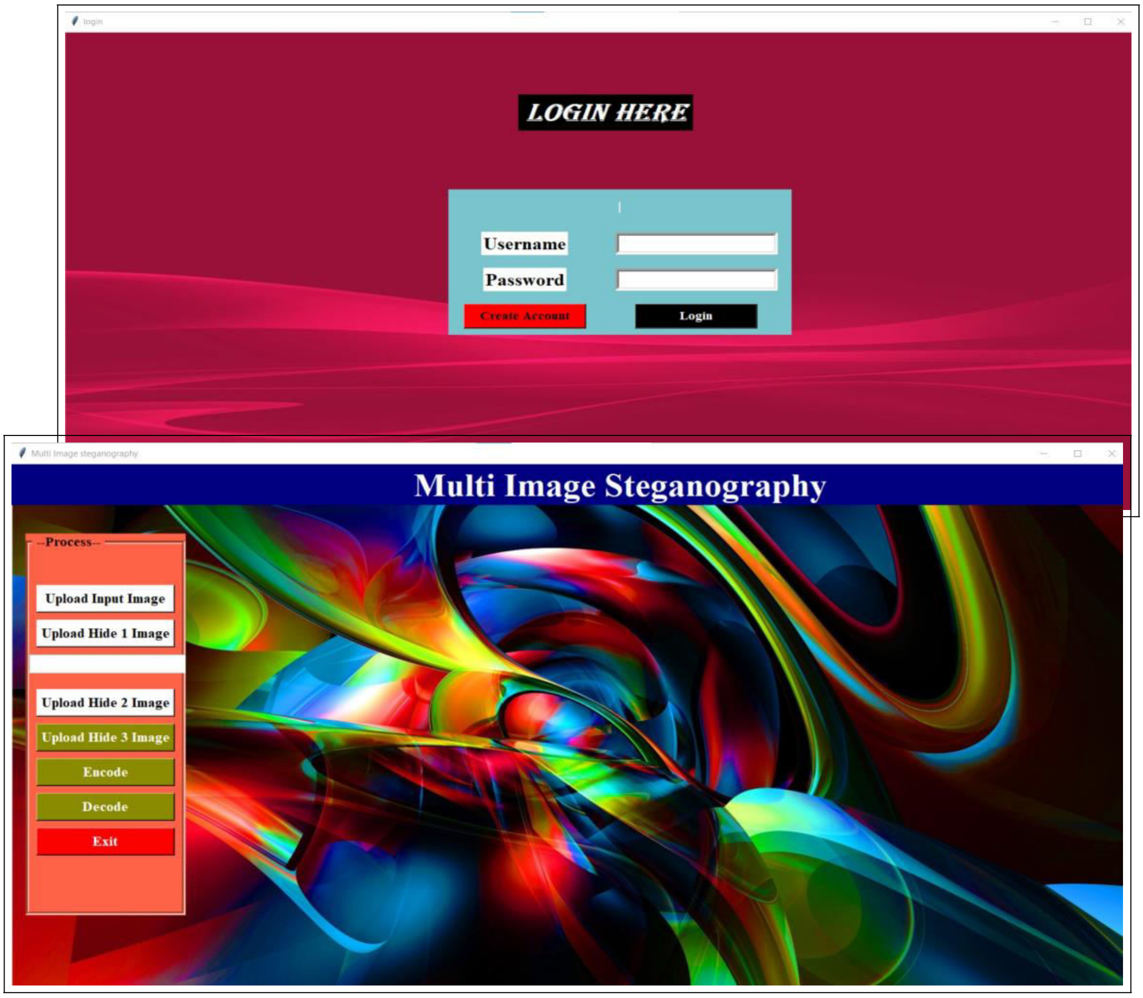
Gender : ○ Male ○ Female

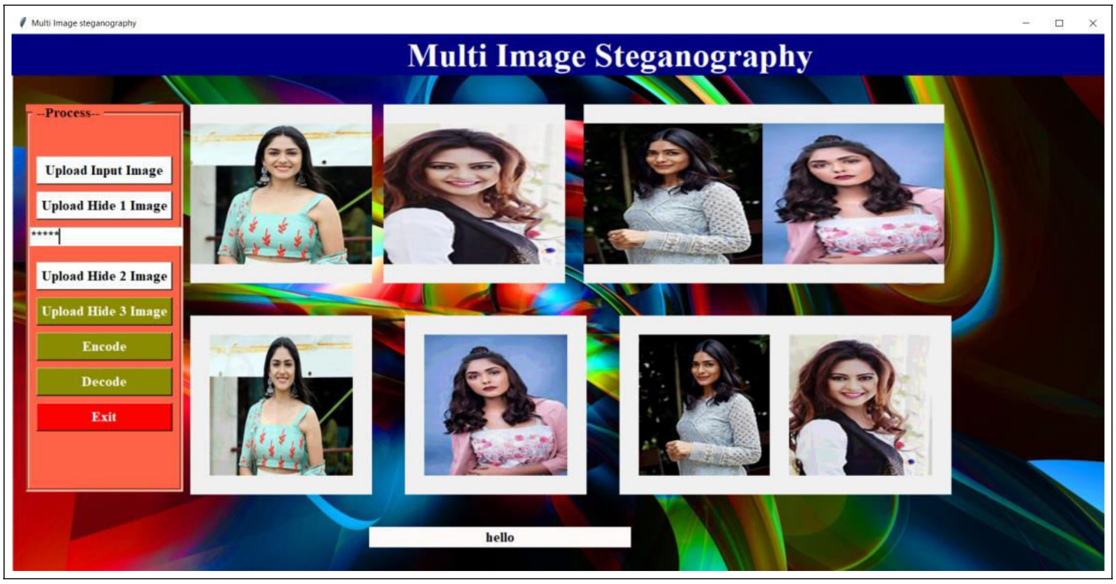
Age : 0

User Name :

Password :

Confirm Password:


login
LOGIN HERE
Username
Password
Create Account
Login
Multi Image steganography
Multi Image Steganography
--Process--
Upload Input Image
Upload Hide 1 Image
Upload Hide 2 Image
Upload Hide 3 Image
Encode
Decode
Exit


Multi Image steganography
Multi Image Steganography
--Process--
Upload Input Image
Upload Hide 1 Image
Upload Hide 2 Image
Upload Hide 3 Image
Encode
Decode
Exit

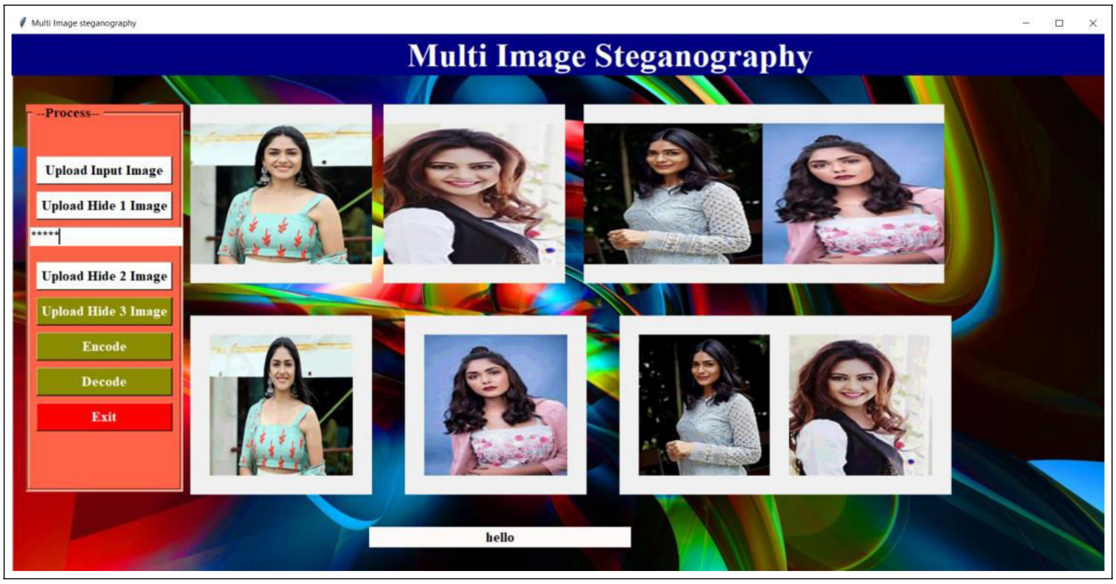
*****

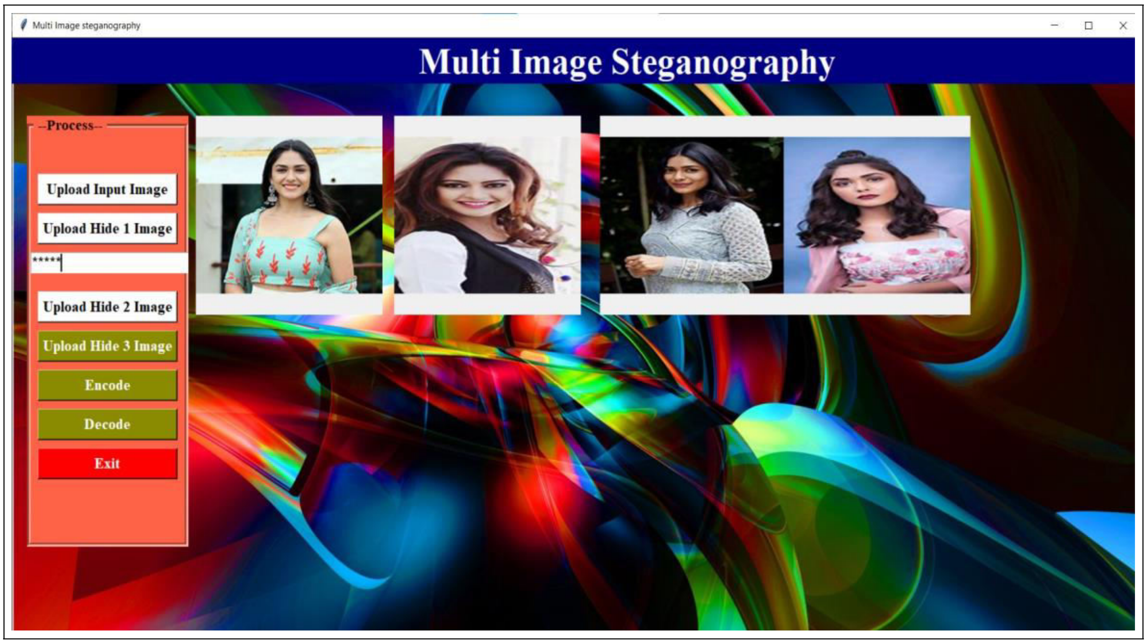
hello

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105321 |





VIII.CONCLUSION

To build this proposed system we have used the concept of Multiple Images Steganography using Deep Neural Network and in this process we have created different classes using Python Programming languages these classes are of Steganographic classes , Hiding Images classes , Cryptographic classes using concept of Advance Encryption algorithm , this paper helps us to understand the concept of multiple images steganography using deep neural network and showcases how we can use this concept so as to improve the security of sensitive data which may be shared in various fields such as defence , finance etc .We have tried to inculcate multiple sensitive images under a single cover images so as to reduce time and memory .This system aims to build an effective encryption and decryption system using Multiple Image Stegnography . The proposed system will be able to hide data in multiple images thus securing it from external threat and theft . It will hide sensitive data into images which will be completely different from our original data and the end user will be able to decrypt that data without much effort and thus protecting it from external threat .

REFERENCES

1. Rupesh Gupta ,Tanupreet Singh . "New Proposed Practice for Secure Image Combing Cryptography Stegnography". IEEE Explore .
2. K.Saranya, R.S.Reminaa, S.Subhitsha. "Modern Applications of QR-Code for Security ". IEEE Explore , .
3. PuteriAwaliatushShofro, Kiki Widia ,Dwi Dian Ayu Puji Astuti , Eko Hari Rachmawanto. "Improved Message Payload and Security of Image Steganography using 3-3-2 LSB and Dual Encryption" ,IEEE Explore, .
4. Byoungkoo Kim,Seoungyong Yoon,Yousung Kang,Dooho Choi. "Secure IoT Device Authentication Scheme using Key Hiding Technology" ,IEEE Explore.
5. ZhongliangYang, Xiaoqing Guo, Ziming Chen , Yongfeng Huang and Yu-Jin Zhang . "RNN-Stega: Linguistic Steganography Based on Recurrent Neural Network",IEEE Explore.
6. BehrouzA.Forouan, Debdeep Mukhopadhyay, 2nd edition Cryptography and network security, McGraw Hill Education.
7. Byoungkoo Kim,Seoungyong Yoon,Yousung Kang,Dooho Choi. "Secure IoT Device Authentication Scheme using Key Hiding Technology" ,IEEE Explore.
8. ZhongliangYang, Xiaoqing Guo, Ziming Chen , Yongfeng Huang and Yu-Jin Zhang . "RNN-Stega: Linguistic Steganography Based on Recurrent Neural Network",IEEE Explore.
9. M. M Amin, M. Salleh, S .Ibrahim, M.R.K atmin,andM.Z.I.Shamsuddin , Information Hiding using Steganography, National Conference on TelecommunicationTechnology Proceedings, Shah Alam, Malaysia.
10. Praveen Kumar, V Hemanth, MShareef, Securing Information Using Sterganoraphy, 2013 International Conference on Circuits, Power and ComputingTechnologies [ICCPCT-2017].
11. Ivan W. Selesniek "Wavelet Transforms A Quick Study", Physies Today magazine,¨uetober, 2016.