IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

SECRETE COMMUNICATION SYSTEM FOR MILITARY BY USING MACHINE LEARNING & STEGANOGRAPHY

[1]Aishwarya More, [2]Namrata Gawade, [3]Sagar Ingole , [4]Swati Dange, [5]Shubhra Mathaur

[1,2,3,4] U.G Student Department of Computer Engineering, Shree Ramchandra College of Engineering, Pune, India.
[5] Professor Department of Computer Engineering, Shree Ramchandra College of Engineering, Pune, India.

Abstract: Information security is an important factor during transmitting secret information between two objects. Generally, we use cryptography for information hiding and sending secret message in the form of text. Nowadays, there are several techniques used for hiding information in any medium. One of such technique is steganography. In this technique, digital images are used for hiding information and the information is in the form of text, digital image, video or audio file may be used as secret message. Using LSB Steganography Technique we can implement high level if information security without any damage to cover image. In this system we are using the hybrid approach i.e. cryptography and steganography. So, our system have higher security level than existing systems.

***Index Terms* - AES cryptography, Face Recognition, Machine Learning CNN technique, Image data hiding, LSB Steganography**

I. Introduction

Information security is an important factor during transmitting secret information between two objects. As early as in ancient Greece there were attempts to hide a message in trusted media to deliver it across the enemy territory. Generally, we use cryptography for information hiding and sending secret messages in the form of text. In the modern world of digital communication, there are several techniques used for hiding information in any medium. One of such technique is steganography. In which digital media mainly digital images are used as a medium for hiding information and the information in the form text, digital image, video or audio file may be used as secret message. The word steganography derived from two Greek words: steganos means covered and graphos means writing and often refers to secret writing or data hiding. With the development of machine learning, face recognition technology based on CNN (Convolutional Neural Network) has become the main method adopted in the field of face recognition security system securely access the confidential system. Information security plays a major role in any data transfer security can be obtained by information hiding that focuses on hiding the existence of secrete information. In this project we use to provide security and hide information.

- ➢ In this project we use to provide security and hide information:
  1. Cryptography
  2. Steganography
- ➢ Using LSB Steganography Technique.

II. Problem Statement

In today's scenario of data security is a very big challenge in any communication. The technique Cryptography and steganography is the science of hiding sensitive information in another transmission medium and by enhancing more security to it by using machine learning.

III. PROJECT OBJECTIVE

The main objectives of this project are

- ➢ Requirement of the steganography system is that the Hidden message carried by stego-media should not be sensible to human beings.
- ➢ This approach of information hiding technique has recently become important in a number of application area.
- ➢ Secure the data transfer system with high security login methods.

IV. TOOLS AND TECHNIQUES USED DURING THE PROJECT

In this project we use to provide security and hide information

1. Machine Learning.
2. Cryptography.
3. Steganography.
4. Using CNN machine learning technique.
5. AES cryptography technique.
6. LSB Steganography Technique.

V. SOFTWARE & HARDWARE REQUIREMENTS

- Software Requirements:
  1. Operating system: Windows 7/8/10
  2. Coding Language: Python
  3. IDE: Visual Studio Code
- Hardware Requirements:
  1. Processor - Intel i3 core
  2. Speed - 1.1 GHz
  3. Ram - 4 GB
  4. Hard Disk -500 GB & Above
  5. Monitor – SVGA

VI. Mathematical Model

Mathematical Model of hiding secret data (the embedding algorithm) and the steps for retrieving secret data (the extracting algorithm).

- In the following, a description of the image used in the proposed method is given. – Assume I is any gray image, and consists of set of pixels I = P1, P N.
- Every pixel composed of 8 bits: $|P_i|$ = 8 bits, Pi = b1, b8, b_j =1, 0 4 – The image size is computed as N = H ∗ W. – Where H, W is the height and width of the image respectively.
- Assume M and n are the secret data bits and its length respectively, M = m1, m2, m n, where mi 1, 0 . – And h is the maximum hiding capacity in the image I and computed in terms of bits as $1 \leq h \leq (N * 8)$. Finally, make a division for the results and embed the new results into the cover image to obtain the stego image.
- The results show that the proposed method gives high capacity and good imperceptibility in comparison with the previous methods.

VII. SYSTEM ARCHITECTURE

In this system, User give secret data as input. After receiving secret data system will encrypt secret data and divide cipher text into two parts. After that two cipher text embedded with cover images i.e. take from user /apply default images and create stego images for respective cipher text. Then send that images to receiver. At the receiver end, user will un steg the stego images. After unstegoing images decrypt the cipher text and merge plain text. We get secret data then display the secret data.

- In LSB Steganography, hidden information is stored at a specific position of the LSB of image.
- Take the binary representation of the hidden information and overwrite the LSB of each byte within the cover image
- Formula: cover image + secret key + hidden message = stego image [2]
- Improved LSB method for hiding secret information written in text file into colour image.
- Each character of the secret image is converted into its equivalent ASCII value and then each code is converted into 8 bit binary, and each bit is inserted into the last LSB of each pixel of the cover image.

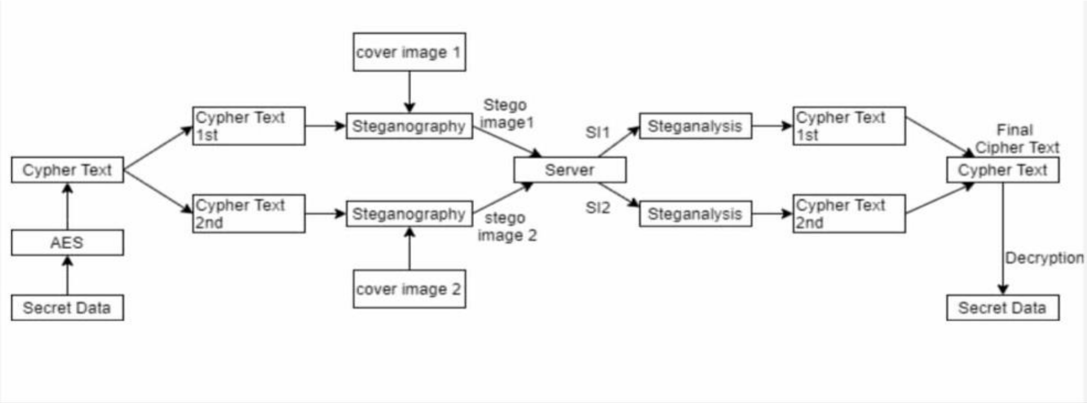


Fig. 1 System Architecture

VIII. CLASS DIAGRAM

The class diagram is the main building block of object-oriented modelling. It is used for general conceptual modelling of the structure of the application, and for detailed modelling, translating the models into programming code.

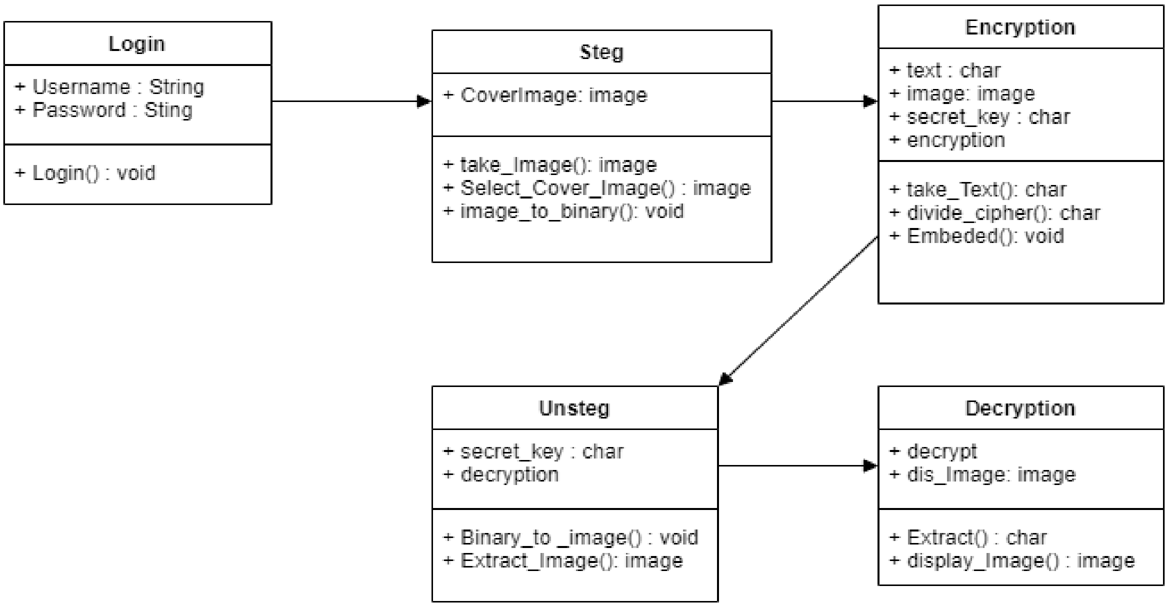


Fig. 2 Class Diagram

IX. ACTIVITY DIAGRAM

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modelling Language, activity diagrams are intended to model both computational and organizational processes (i.e., workflows), as well as the data flows intersecting with the related activities. Although activity diagrams primarily show the overall flow of control, they can also include elements showing the flow of data between activities through one or more data stores.

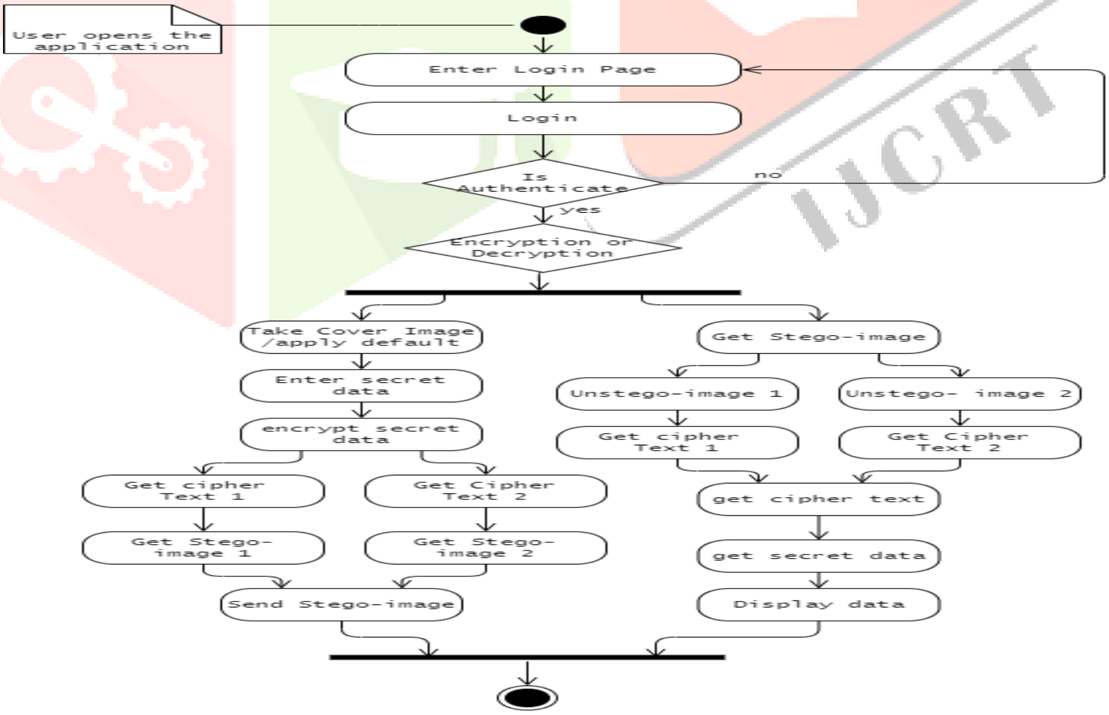


Fig. 3 Activity Diagram

X. STATE DIAGRAM

A state diagram is a type of diagram used in computer science and related fields to describe the behavior of systems. State diagrams require that the system described is composed of a finite number of states; sometimes, this is indeed the case, while at other times this is a reasonable abstraction.

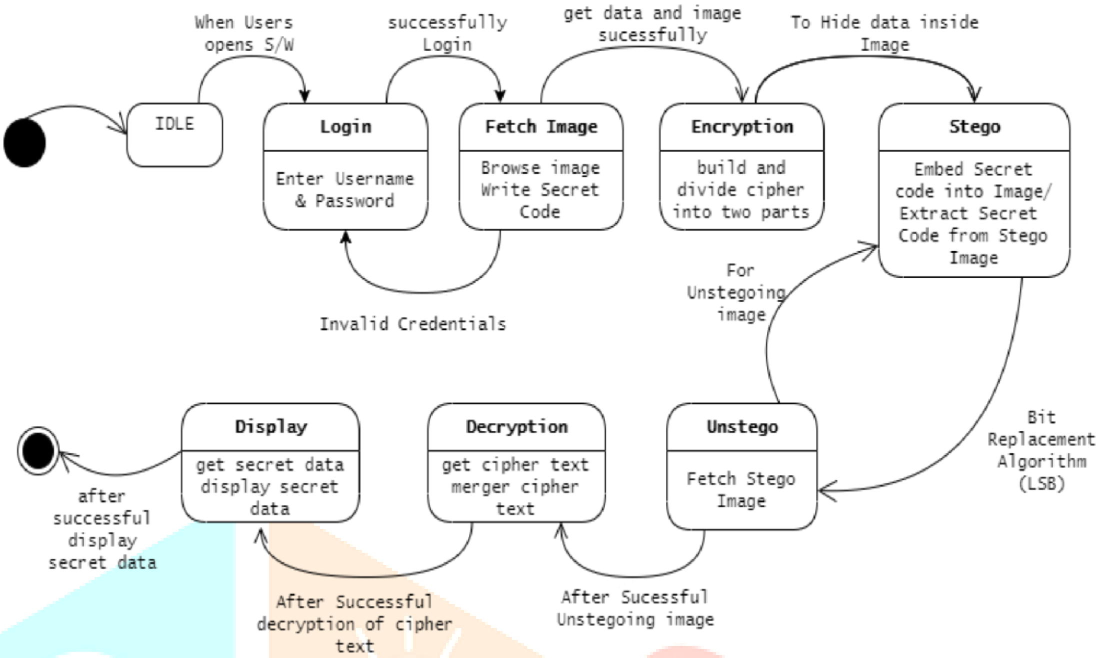
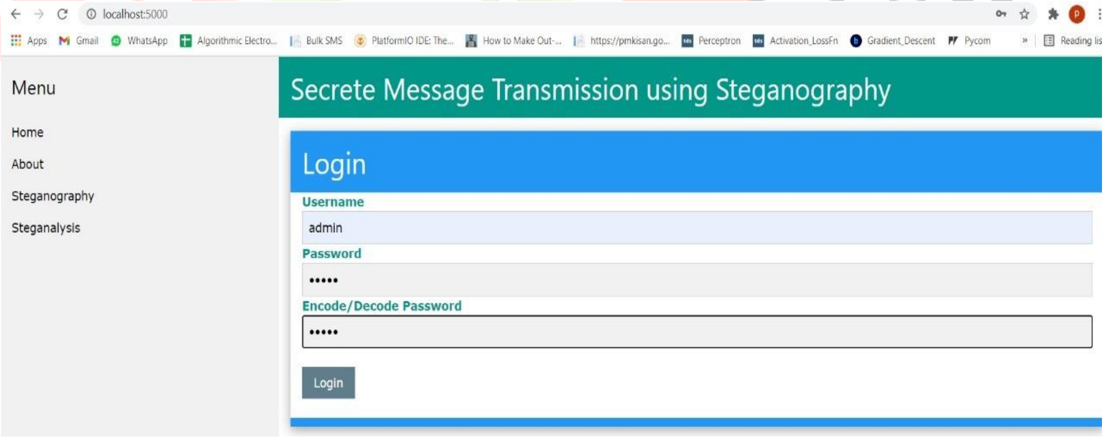

When Users opens S/W
successfully Login
get data and image sucessfully
To Hide data inside Image
IDLE
Login
Enter Username & Password
Fetch Image
Browse image Write Secret Code
Encryption
build and divide cipher into two parts
Stego
Embed Secret code into Image/ Extract Secret Code from Stego Image
Invalid Credentials
For Unstegoing image
Bit Replacement Algorithm (LSB)
Display
get secret data display secret data
Decryption
get cipher text merger cipher text
Unstego
Fetch Stego Image
after successful display secret data
After Successful decryption of cipher text
After Sucessful Unstegoing image

Fig. 4 State Diagram

XI. OUTCOMES

- Using LSB Technique we can implement high level of information security without any damage to cover image.
- LSB Steganography has very less MSE value (Mean square error) as compared to DWT & Other techniques
- LSB steganography has high PSNR value as compared with DCT & DWT steganography.
- As LSB has good performance in terms of MSE & PSNR, it becomes very difficult for hackers to hack the information.

1) LOGIN PAGE



Secrete Message Transmission using Steganography

Login

Username

admin

Password

•••••

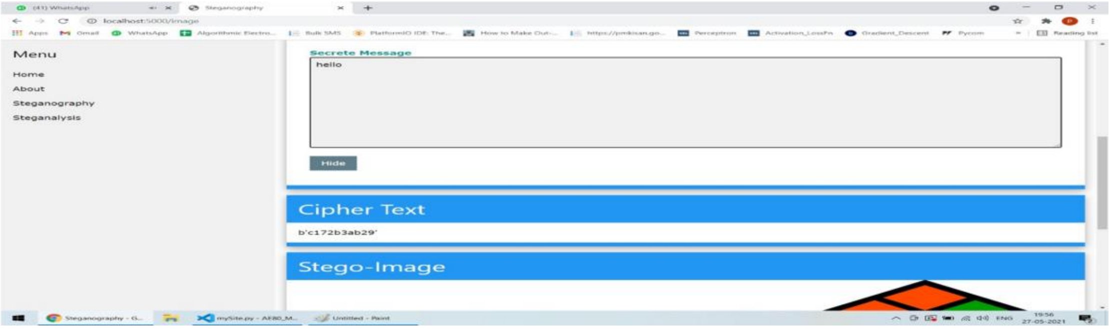
Encode/Decode Password

•••••

Login

Fig. 5 Login Page

2) STEGNOGRAPHY



Secrete Message

hello

Hide

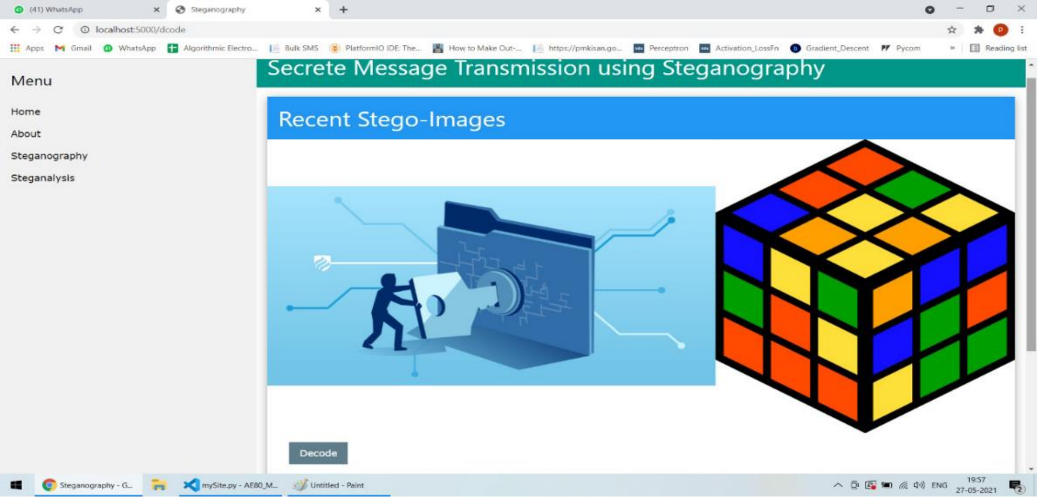
Cipher Text

b'c172b3ab29'

Stego-Image

Fig. 6 Stegnography

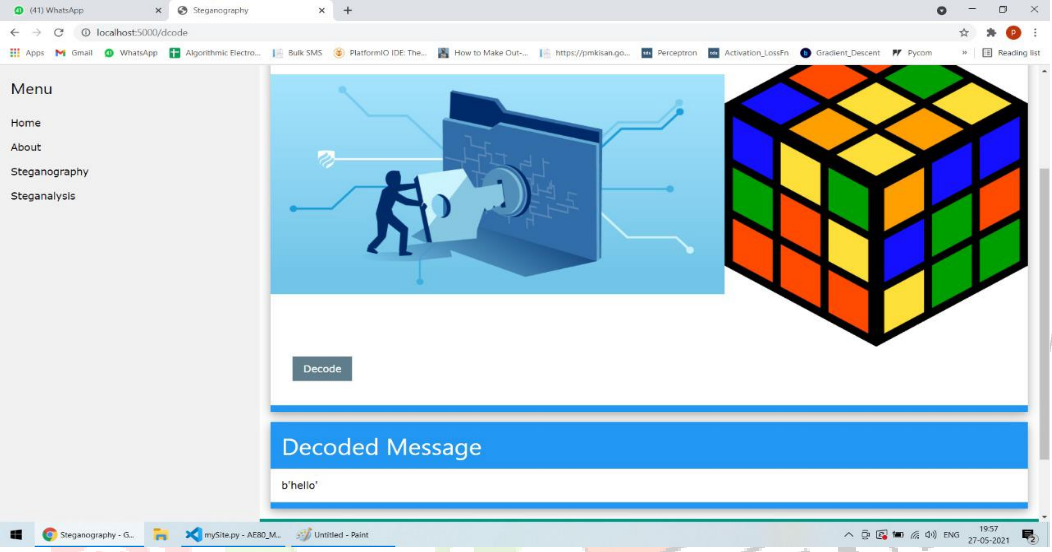
3) STEGANALYSIS



Secrete Message Transmission using Steganography

Recent Stego-Images

Fig. 7 Steganalysis



Decoded Message

b'hello'

Fig. 8 Steganalysis Decoded Message

XII. CONCLUSION

- Using face recognition technology based on CNN (Convolutional Neural Network) to ensure high security to access the secret communication system securely.
- Using LSB Technique we can implement high level of information security without any damage to cover image.
- It will be almost impossible for hackers to attack the stego Image as cover image and stego image looks similar.
- Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day.
- Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice. We printed out the enhancement of the image steganography system using LSB approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover image.

XIII. GENERALIZE APPLICATIONS

- Confidential communication and secret data storing
- Protection of data alteration
- Access control system for digital content distribution
- Media Database systems
- To Maintain Secrecy in Storage
- Reliability in Transmission
- Authentication of Identity

XIV. Acknowledgment

We thank the Management, Principal, Head of Computer Science Department and the Professors of Shree Ramchandra College of Engineering for providing the opportunity. A special thanks to our project Guide and Counsellors for extending a helping hand throughout the process. We would also like to thank our parents and friends for their help and Motivation throughout this project.

References

[1] G. Prashanti, K. Sandhyarani, “A New Approach for Data Hiding with LSB Steganography”, Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI, Springer 2021, pp. 423- 430.

[2] S. Goel, S. Gupta, N. Kaushik, “Image Steganography – Least Significant Bit with Multiple Progressions”, Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), Springer 2020, pp. 105-112S.

[3] D. Baby, J. Thomas, G. Augustine, E. George, Arseev and L. Mestetsky, "Handwritten Text Recognition Using Reconstructed Pen Trace with Medial Representation," 2020 International Conference on Information Technology and Nanotechnology (ITNT), 2020, pp. 1-4, doi: 10.1109/ITNT49337.2020.9253330.

[4] B. Feng, W. Lu, and W. Sun, “Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture”, IEEE transactions on Information Forensics and Security, Feb. 2020.

[5] M. Nusrati, A. Hanani and R. Karimi, “Steganography in Image Segments Using Genetic Algorithm”, 5th IEEE International Conference on Advanced Computing & Communication Technologies (ACCT), Feb 2019 pp. 102-107.

[6] N. A. Al-Otaibi, and A. A. Gutub, “2-Leyer Security System for Hiding Sensitive Text Data on Personal Computers”, Lecture Notes on Information Theory, June 2019, pp. 151-157.

[7] M. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal and M. D. Hossain, “An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography”, IEEE International Conference on Informatics, Electronics & Vision (ICIEV), May 2019, pp. 1-6.

[8] K. Qazanfari and R. Safabakhsh, “A new Steganography Method which Preserves Histogram: Generalization of LSB++”, Elsevier International Journal of Information Sciences, Sept. 2019, pp. 90-101.48