International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 12 | Dec 2022 www.irjet.net p-ISSN: 2395-0072

Implementation of Steganographic Techniques and its Detection.

Amogh Amin[1], Vishal Mistry[2], Yogesh Choudhary[3]

[1,2,3]BE student, Dept. of Information Technology, Pillai College of Engineering, Navi Mumbai, India

---

Abstract - *There is a huge development in Computer technology in the past few decades and the question of information security rises. To solve this problem different methods have been used to cover the secret message with common media. Solutions such as Steganography and Cryptography are used to tackle this problem. The method of steganography is among the methods that have received attention in recent years. We have come up with a system for applying* ***steganographic techniques*** *to conceal (hide) and retrieve the provided information inside of digital files (primarily images and text files) and to create a classifier to detect if some information is hidden in digital images. Unlike cryptography, which works to obscure content so it can't be understood, steganography's goal is to hide the fact that content exists at all by embedding it in something else. The proposed system will include an interface to hide and retrieve messages in images and videos and documents. This way a steganographic image can be created and transported and then the secret information can be retrieved. The proposed system will also include a classifier trained to detect common techniques of steganography and hence can be used to detect if an image contains hidden information or not.*

Key Words: Hide, Steganography, image, text

1. INTRODUCTION

In the current world, there is a high need of a private peer to peer communication system. Here is where a place for Steganography comes into picture. A tool through which one can communicate by hiding a private secret message is a necessity in this monitored world. The method of steganography is a really popular method if concealing,

The main goal of steganography is to hide secret information in the other common forms of media so that anyone who does not know about this secret message cannot understand it or notice it. This is a major distinction between this method and the other methods like cryptography. In Cryptography, the user will notice the information by seeing the encrypted information but they will not be able to decode the information. Meanwhile in steganography, the existence of the information in the media is not noticed by the user.

The use case for such a system is primarily in digital watermarking for copyright and licencing protection by identifying the digital asset by its watermark and also to detect tampering. It could also be used for digital fingerprinting of media, so that its source can be tracked or verified, for example to find the culprit of film (movie) piracy, sensitive documents being leaked,etc. Other usage include covert (secret) communication, that is, it can be used to transport sensitive data from point A to point B such that the transfer of the data is unknown to evade any potential eavesdropper. It can also be used in combination with cryptography, for more protection. Other potential usage includes storing of secret information at a place.

1.1 OBJECTIVES

The objective of this project is to implement a system to apply steganographic techniques to an image / or other file types so as to hide information in them. This would achieve the following desired results

1. Information would be concealed in the image unknown to third parties.

2. The image can then be transferred to the desired recipient without anyone knowing about the secret communication taking place

3. The recipient can then extract the secret information from the received image.

2. LITERATURE SURVEY

Information concealing is the most important method of steganography. In computing general technique is to conceal a secret message in every nth bit of every place of a digital message. After the introduction of the Internet and all the different digital file formats that it has decreased in importance. Steganography is mainly implemented in Text, Images, Video or Audio forms of media. Below is a Diagram showing various methods of Steganography,

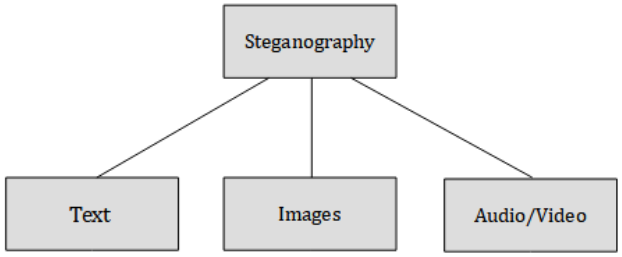

Fig -1: Methods of Steganography

Below is the summary of various research papers:

Digital Steganography and watermarking for digital images: a review of current research directions. (Oleg Evsutin, Anna Melman And Roman Meshcheryakov.) Issue-5, September, 2020.

This system shows various methods used in hiding and digital watermarking. It provides basic information about this field and the main applications. It focuses on contemporary works illustrating current research directions in the field of information embedding in digital images.

An Effective and Secure Digital Image Steganography scheme using two Random function and Chaotic Map. (Mohanand Najm Abdulwahed) Issue- 15, January 2020

The proposed system suggests a secure image steganographic system which is a key adaptive LSB system, which depends on four stages for the provision of better data-hiding algorithms in cover images by the volume, image quality, and security. In this paper a new adaptive of least significant bit substitution technique, merging two random functions, and chaotic technique.

Digital Steganography for preventing Cybercrime using Artificial Intelligence Technology. (Dr. R. Varalakshmi) Issue-8, February 2020.

It is observed that the proposed algorithm shows improvement than the existing algorithm. The cover image (RGB) using an embedding algorithm using Karhunen Loeve Transform for communication with the secret message taken as input. It converts an encoded image which hides the secret. This encoded image is decoded using a decoding algorithm (DES) to revert the original secret message.

3. EXISTING SYSTEM ARCHITECTURE

The main goal of this method is to hide information on the output image. This method can be used to send the image as a normal conversation or for announcing a secret message in a public place. Using a suitable Steganography algorithm the secret information is hidden within the normal data before sending.

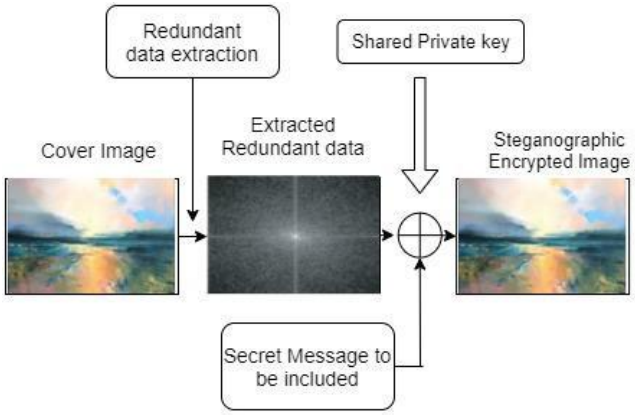

Fig -2: Implementation of Steganographic Encryption

Encrypt Data

The current system allows the user to select a cover image, and embed a secret message inside the cover image .

This operation uses the LSB Algorithm and embeds the binary data into different pixel value data of the cover image.

This uses an Encryption key and has a temp file which stores the data if the pixel bit value and the data bit value are same or different. Thus a steganographic image is created.

Extract Data

The current system allows the user to upload the Steganographic image and Decrypt the data out of the image using LSB and the temp values.

Disadvantages

One of the defects of the current system is that the user cannot choose which bit planes to embed the data in, there's no control in the hands of the user.

One more extra security protocol is to encrypt the data before embedding it with a private key so that even if the Steganography is detected and the data is extracted

there'll be an extra layer of security and the user won't be able to extract the information.

4. PROPOSED SYSTEM ARCHITECTURE

In our system we have fixed the two disadvantages mentioned above in the existing architecture.

Our system provides :

1. Encryption of data before Embedding data to add an extra layer of security for the user before LSB.

2. Giving the user choice to select the bit planes he wishes to embed the data in. The user can lower the distortion in image by embedding data into the lower bit planes.

3. An activity column to fetch all of the recent Steganographic operations by the user.

4. A Steganography Detection tool.

User Profile: Login/ Register

The Secure Login system logs the user into his profile which has the data of all of his Steganographic operation activities.

Each profile is assigned a unique private key which is used to encrypt and decrypt the data and can only be accessed by the user.

New Users can create new profiles to access these features.

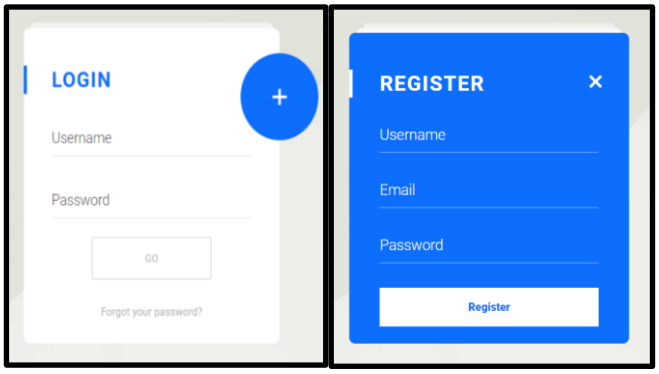

Fig -4: Login/Register system.

Dashboard

The Dashboard shows the basic operations of the Stegno tool Portal in an organized manner, It also shows the recent steganographic embedding activities of the current user logged in.

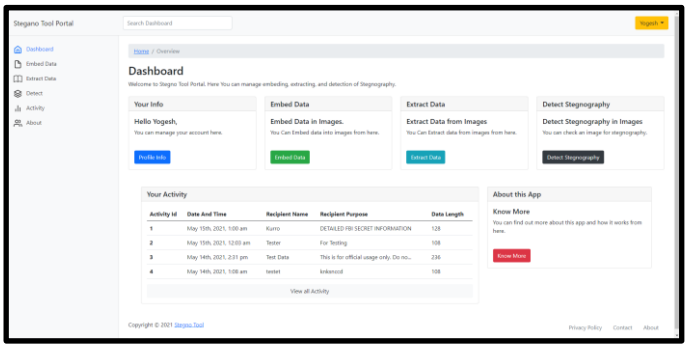

Fig -5: Dashboard

Embed Data

In embed data the sender can upload a file to generate a steganographic image with concealed data. Decided data is encrypted using AES 256 first, creating encrypted data which is then concealed into a file decided by the use of LSB algorithm and unique pattern of bit plane decided by user.

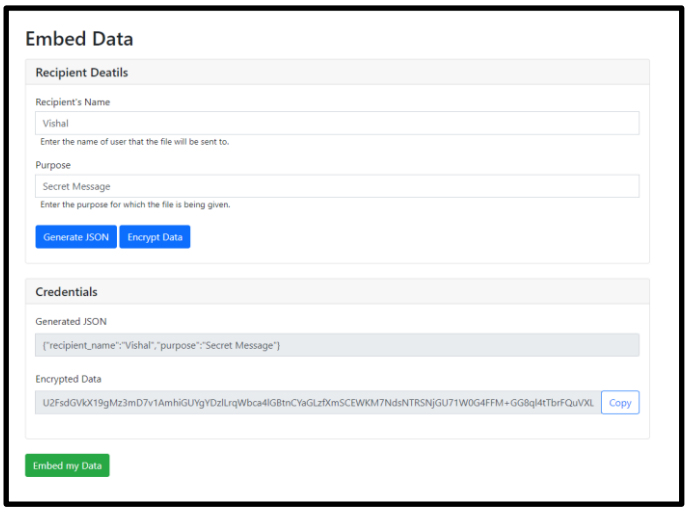

Fig -6: Creating Encrypted secret message

Here, the user can perform various operations with the image selected.

Some of the operations are :

Full Red/Green/Blue image

Inverted Image

Embed/ Extract Data

Embed B&W image

Show strings, RGBA values

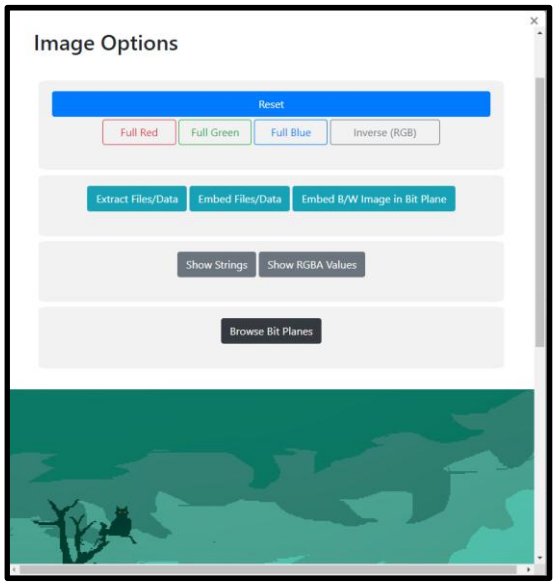

Fig -7: Available Image Options.

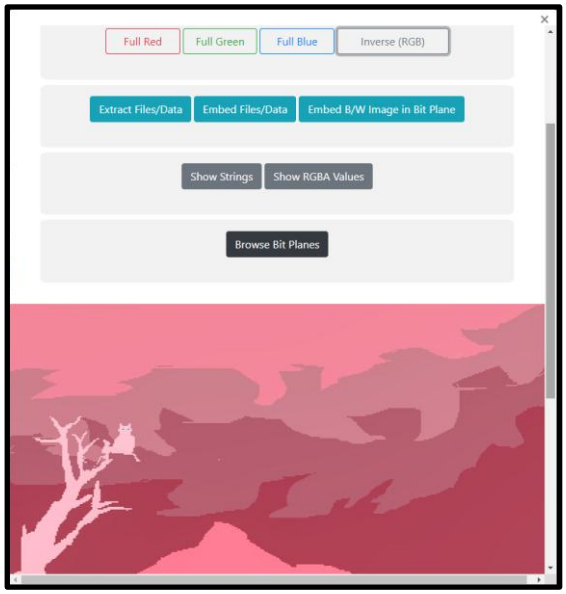

Fig -8: Full Red Option.

Here, the user can select which bit planes the data should be embedded in the image and paste the encrypted AES text in the data section and complete the embedding operation.

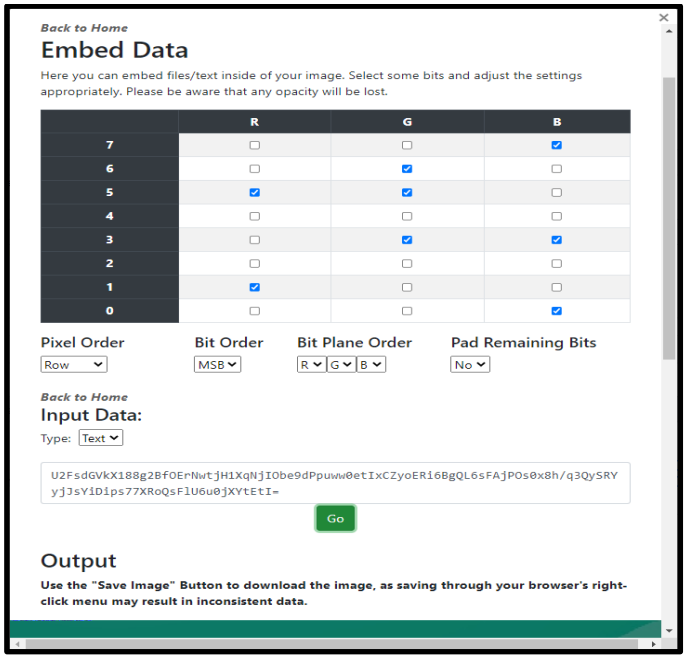

Fig -9: Embedding data into selected bit planes.

Extract Data

Here steganographic image with concealed data is extracted by firstly retrieving concealed encrypted data from streganaphic image. Then retrieved encrypted data is decrypted using a private key.

The user has to select the same bit planes he used for embedding the data.

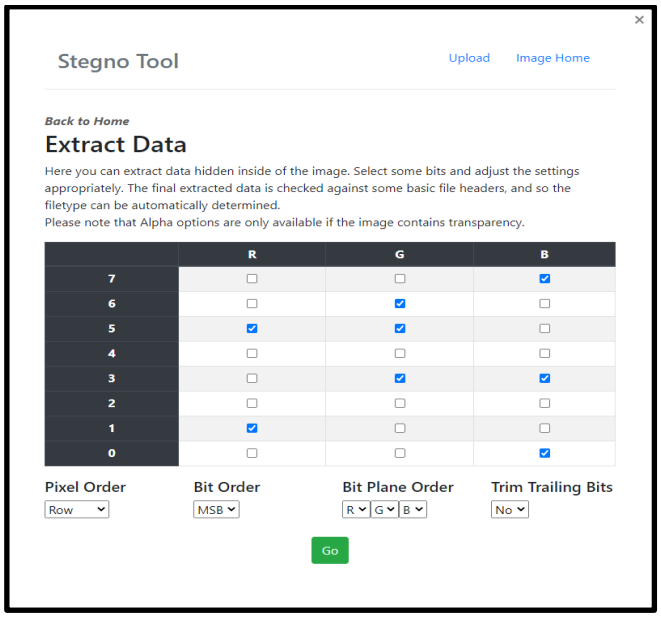

Fig -10: Selecting the bit planes to Extract data

The results are shown. The user now copies the ASCII value and decrypt the AES Encryption,

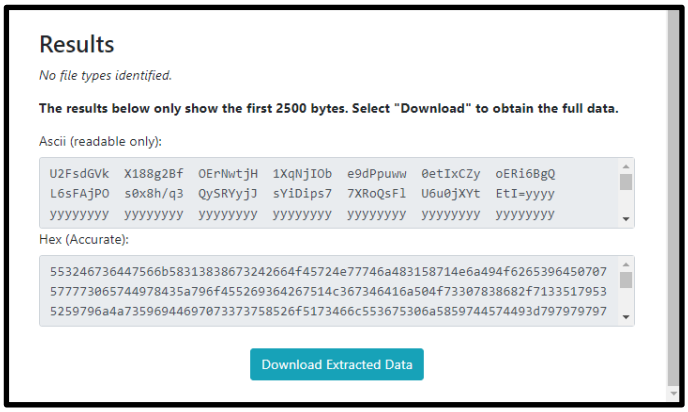

Fig -11: Results of Data Extraction

Once the user enters the ASCII value and decrypts he gets in return the original JSON value of the secret message. These operations are stored in the Activity tab.

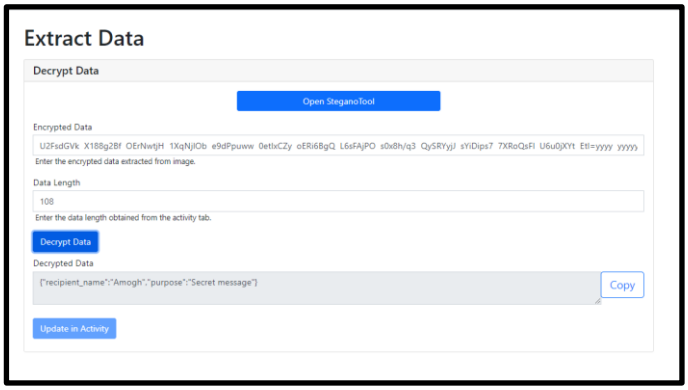

Fig -12: Embedding data into selected bit planes.

Activity

In the activity tab history of user activity is logged, it tracks the data sent thus it can be used to check if a file that belonged to the is tampered with. It's also used in detecting to which user the file belongs using respective hash. All the data is stored in a database.

Fig -13: Activity tab

About

In the about tab, the crux of the project is explained.

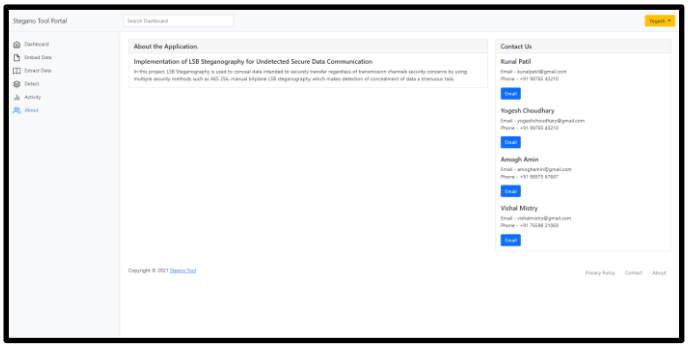

Fig -14: About tab

5. Algorithm

Step 1) User creates an account using the registration system.

Step 2) User logins with credentials user made .

Step 3) From dashboard user selects if he wants to embed data in file or extract data from encrypted file.

Step 4) To embed data in the data embed tab, the user generates a json using the recipient's name and purpose.

Step 5) User selects the encrypt feature.

Step 6) User uploads image to conceal data into image using unique bit plane.

Step 7) The user embeds the data and downloads the Steganographic image.

Step 8) To decrypt the image, the user enters encrypted data in the extract tab,after entering data length .

Step 9) User selects decrypt data button.

Step 10) Finish.

6. TECHNIQUE USED

LSB Algorithm

The LSB algorithm replaces the last bit which is the least significant bit of each pixel with the secret message's one data bit.

The Least Significant bit (LSB) has the lowest impact on image color or quality when it is changed. E.g. If the pixel is black and it's value is 1 and it is changed from 1 to 0, the

pixel color only changes from Black to a lighter version of black. The change in bytes is <0.000002%.

Working

Every pixel has a RGB value ranging from 0 to 255.

In LSB, if the user wants to insert a secret text message into an image, The secret message is first converted into Binary.

E.g. Secret message is "Steg" is converted to '01010011 01110100 01100101 01100111 '.

This binary value of the secret message is then embedded into the image data using LSB technique.

The Algorithm first takes the image data and converts it into pixel value.

The Algorithm then replaces the least significant bit of the 8-bit image RGB pixel with the first bit binary value of the secret message.

This continues till all of the bits are successfully embedded into the pixel value.

This is how Encryption of secret message into the cover image works and a Steganographic image is produced.

For the Decryption part, this algorithm reverses the process and decodes the secret message.

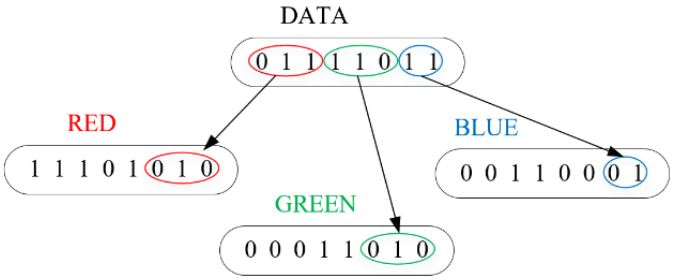

Fig -3: LSB Algorithm Data encrypting.

The current existing system uses the Embedding and Extracting data based on the above LSB algorithm.

7. CONCLUSIONS

The Project will demonstrate the application of steganographic techniques in real world scenarios. The system will provide the users with an easy to use interface for hiding and retrieving secret information in an image. It will be helpful in providing a secure communication medium and also the following applications.

This system will be primarily used in digital watermarking for copyright and licencing protection by identifying the digital asset by its watermark and also to detect tampering.

Other usage include covert (secret) communication, that is, it can be used to transport sensitive data from point A to point B such that the transfer of the data is unknown to evade any potential eavesdropper. It can also be used in combination with cryptography, for more protection.

8. ACKNOWLEDGEMENT

We would like to extend our deepest gratitude to our Project guide **Prof. Amol Kharat** for his exemplary guidance, monitoring and constant encouragement throughout this project which helped us improve our work.

We would also like to extend our gratitude to our Head of Information Technology Department **Dr. Satishkumar Varma** for providing us with an opportunity and platform to carry out this project.

We are also extremely grateful to our Principal **Dr. Sandeep Joshi** who provided us with this golden opportunity as well as all the facilities needed to carry out this project successfully.

9. REFERENCES

[1] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," in Computer, vol. 31, no. 2, pp. 26-34, Feb. 2018, doi: 10.1109/MC.1998.4655281. https://ieeexplore.ieee.org/abstract/document/4655281

[2] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "An overview of image steganography." ISSA. Vol. 1. No. 2. 2019.http://www.academia.edu/download/54323461/EN_-_Image_Steganography_Overview.pdf

[3] N. Provos and P. Honeyman, "Hide and seek: an introduction to steganography," in IEEE Security & Privacy, vol. 1, no. 3, pp. 32-44, May-June 2020, doi: 10.1109/MSECP.2003.1203220. https://ieeexplore.ieee.org/abstract/document/1203220

[4] Channalli, Shashikala, and Ajay Jadhav. "Steganography an art of hiding data." arXiv preprint arXiv:0912.2319 (2016). https://arxiv.org/pdf/0912.2319

[5] Evsutin et al 2017 J. Phys.: Conf. Ser. 803 012038 https://iopscience.iop.org/article/10.1088/1742-6596/803/1/012038/pdf