AAVARTAN'13

DIGITAL MEDIA STEGANOGRAPHY

STEGANOGRAPHY

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Generally, messages will appear to be something else: images, articles, or any other media file like audio or video file.

The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

INDEX

1. Introduction

2. Abstract & working model

3. Installing the Software

4. Introduction to digital security system

5. Image Steganography

    Embedding of text file with image file . . .

6. Digital Media Steganography

    Embedding of doc/pdf file with other media file . . .
    Embedding of audio/image with media file . . .

7. Sending over LAN

8. Add-on Features

9. Bibliography

Abstract

It is important to have secured communication channels as we often need to share our secret information. Encryption is one of the widely used techniques to ensure secure communication, however, sending encrypted messages often draw eavesdropper's attention to intercept the messages and reveal the original message. The concept of 'image steganography' focuses on embedding secret information into the digital images without drawing any attention of eavesdropper to think that such information is embedded. In this paper, a novel approach is proposed in information hiding, by using a common framework that will generate the digital stegano medium. As a proof of concept, we propose a module that will support this framework, using different algorithms and an optimized approach for message compression on RTF documents (Rich Text Format). Level of security is further enhanced by supporting encryption and diffusion, before applying the Steganography.

CRC : Cyclic redundancy check is done for a data and a checksum value is generated to verify weather the information received is same as sent or not.

Compression : The encrypted file will be compressed to a '.cmp extension' file. This is very important feature as generally image files are already large in size so for the ease of sending the file we need to compress the information.

Embedding : The compressed file containing the information will be attached to the image file.

Sending the file : Main task of Steganography is to share the information. Accomplishing the main task of sending the file to another computer the user has to enter the address of the computer and the file will be sent.

Notification : Each process will be accompanied with a notification after the completion of task given to the software and the result will be displayed.

De-emed, decompress and de-encrypt : Receiver has to just click though the options to get the hidden message.

User-friendly: One of the **most important features** will be the user friendliness of the software. It will be very easy to handle and use. User has to just run a batch file for software execution and then has to just roll over his mouse and click the options available to accomplish his task. Also, a help will be there for further assistance.

Results: There will be an image file with the embedded message which is to be hidden from the sender side and at the receiver side recovery of the

INSTALLING THE SOFTWARE

(1) Install software

- JAVA, Java Development Kit with Java Virtual Machine 1.7.0 compiler.
- Set corresponding path in your system.

(2) Install the project in both sender system as well as in receiver system

(3) In receiver system's click the batch file i.e. Server1.bat

(4) Open the project folder

- Run the batch file Stego.bat in sender system.

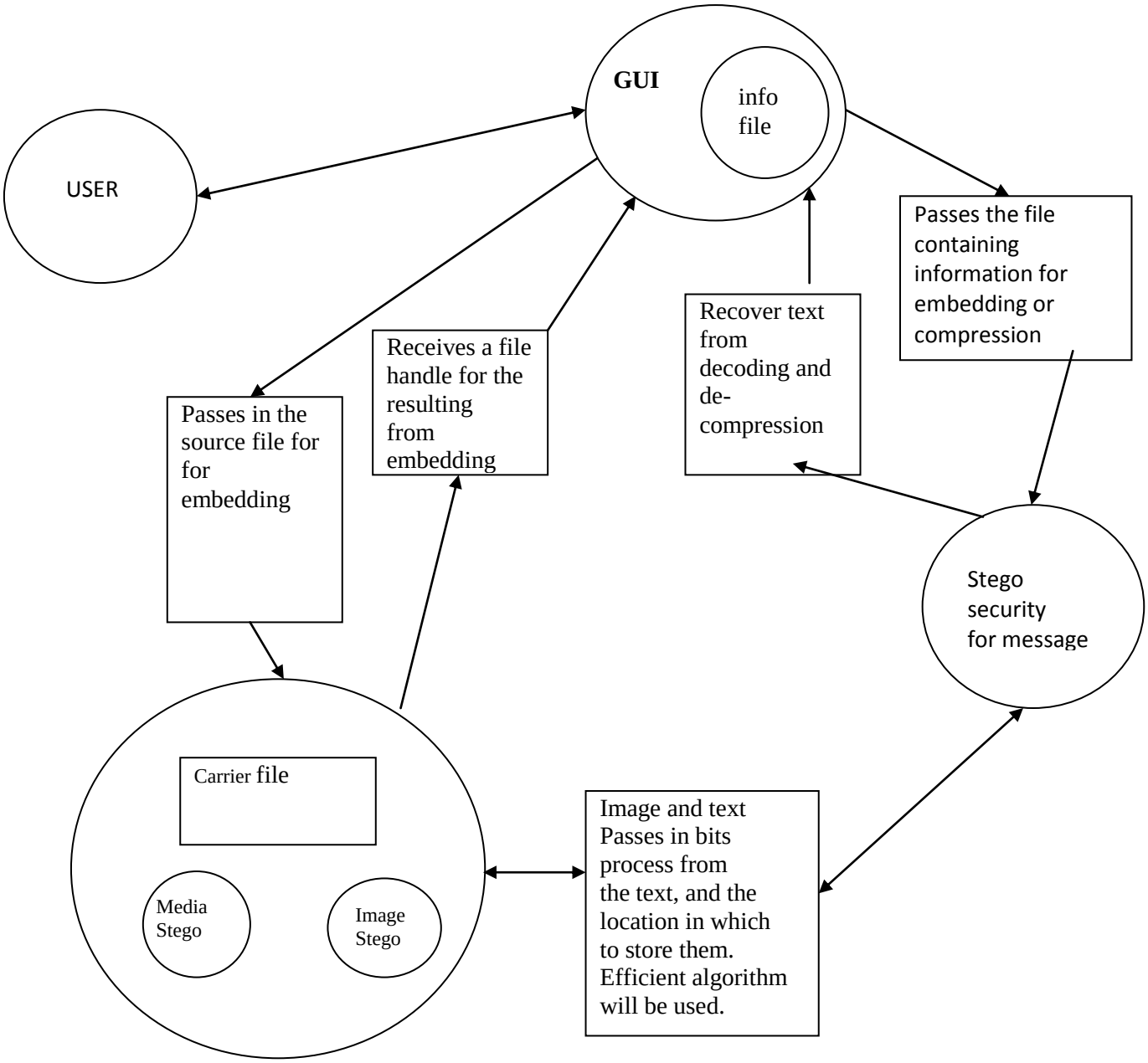
(5) Keep the message file and Carrier file ready in the project folder
This is mandatory.

(6) Check hostname(or *IP* address) of the receiver by typing as follows in the command Promt of receiver system

- ipconfig

Systems IP Address will be displayed.

WORKING MODEL



INTRODUCTION TO DIGITAL SECURITY SYSTEM

The system deals with security during transmission of secret message. This system deals with implementing security using Stegnography. In this end user identifies an image which is going to act as the carrier of data. The data file is also selected and then to achieve greater speed of transmission the data file and image file are compressed and sent. Prior to this the data is embedded into the image and then sent. The image if hacked or interpreted by a third party user will open up in any image previewed but not displaying the data. This protectsthe data from being invisible and hence be secure during transmission. The user in the receiving end uses another piece of code to retrieve the data from the image.

This project is developed using graphics in 'JAVA' language. The options available are displayed in a
menu format, like in an online editor. Clicking on any particular menu item through mouse or through
keyboard a dropdown menu is displayed, listing all the options available under that menu item and the user can select the needed actions according to their wish.

The Menu Bar consists of the following contents

- Data
- Utility
- Help
- Exit

Data
This menu consists of the following submenu content.

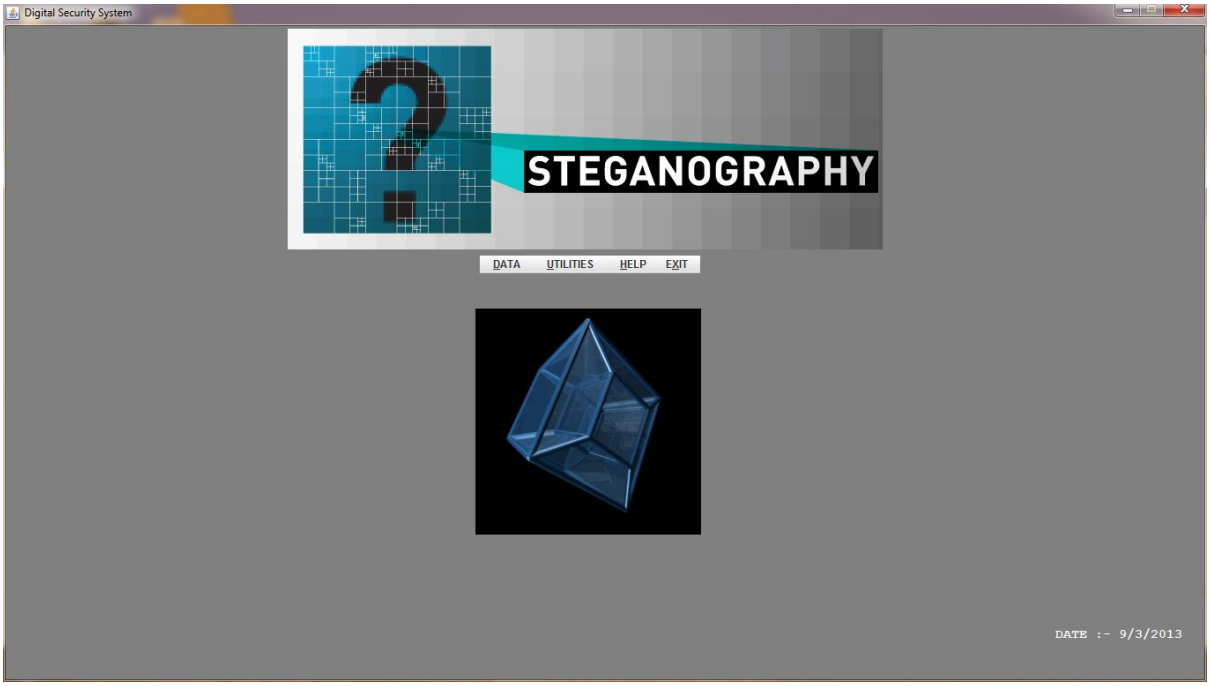
- CRC
- Embed
- De-embed

Utility
This menu consists of the following submenus

- Compression
- De Compression
- Send

Help
This menu consists of the following submenus

- About
- Contents
- Information



The software supports the embedding of the secret message with the carrier file. Secret message can be :

- Text File(.txt)
- Document File(.doc/.docx)
- Image File(.jpg/.gif/.png/.bmp etc)
- Pdf File(.pdf)

Carrier File can be :

- Image File(.jpg/.gif/.png/.bmp etc)
  preferably png
- Audio File(.mp3/.m4a/.wav etc)
- Video File(.wmv/.mp4/.avi etc)

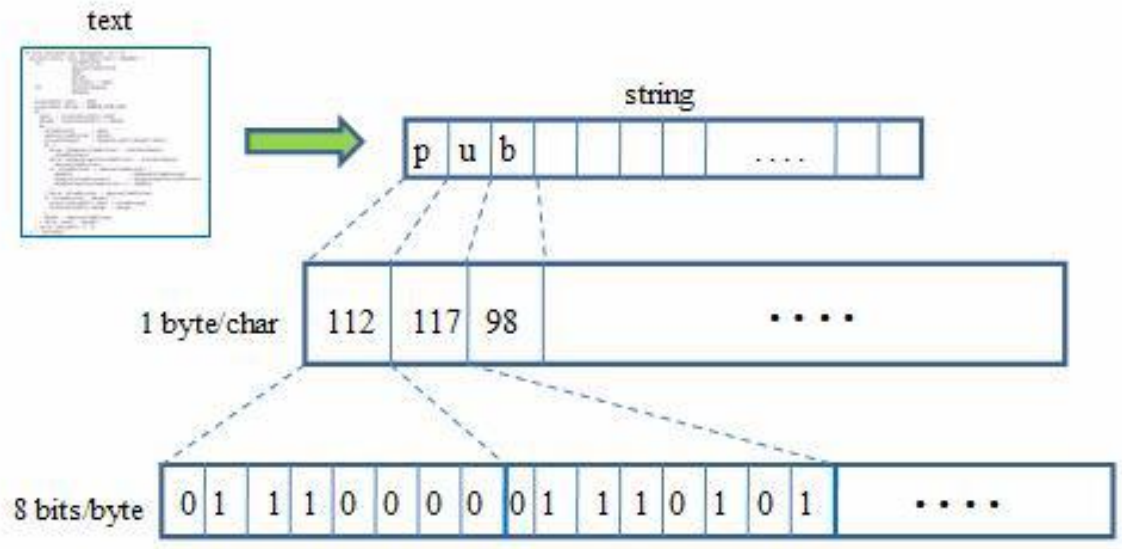
IMAGE STEGANOGRAPHY

EMBEDDING OF TEXT FILE WITH IMAGE FILE

For Image Steganography, the message file is embedded with the image file. Pre-Defined classes in JAVA is used for converting image formats like jpeg,gif,bmp etc into png format. Image file used for embedding is of png format because compression of png is lossless and it size of png files is generally small.
.

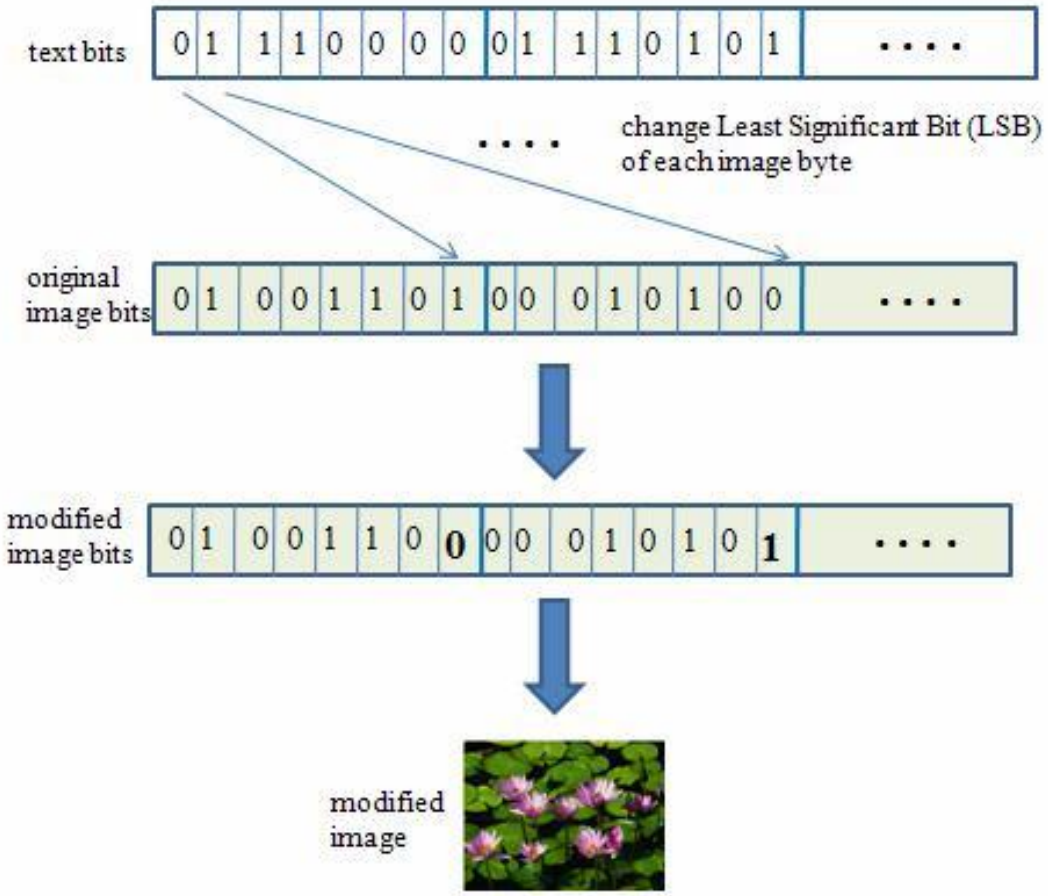
- Here we implemented LSB insertion (Changing in least significant bit of bytes) algorithm which enhances security and detection of message is very difficult . Splitting up of message into multiple pieces.

- In this algorithm compression of embedded file is occurring simultaneously.



The information is converted into byte form. Simultaneously the pixels of the image are accessed. Embedding is done traversing through each bit of the bytes of the information file and pixels of the image file.

EMBED

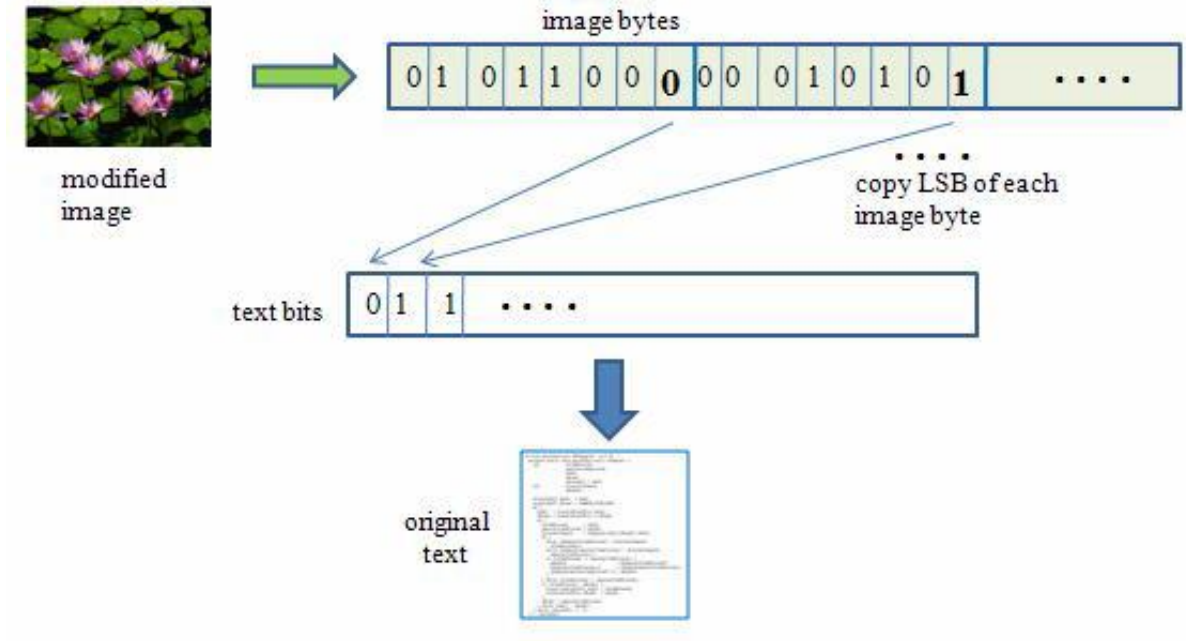


Least Significant Bit(LSB) of the image bytes of the pixel is changed according to each bit of the information file. Mask and Insert operation is used for this process. Thus the embedding of information with the image is done by the LSB Algorithm.
Process

Steps to be followed for embedding text file :

(1) Select the embed option under the Data menu.
(2) Select the carrier and text information file.
(3) Press the embed button.

DE-EMBED



Just the reverse process is followed for retrieving the information i.e. the least significant bits of the image file are extracted and grouped back together generating the hidden information.

For de-embedding :

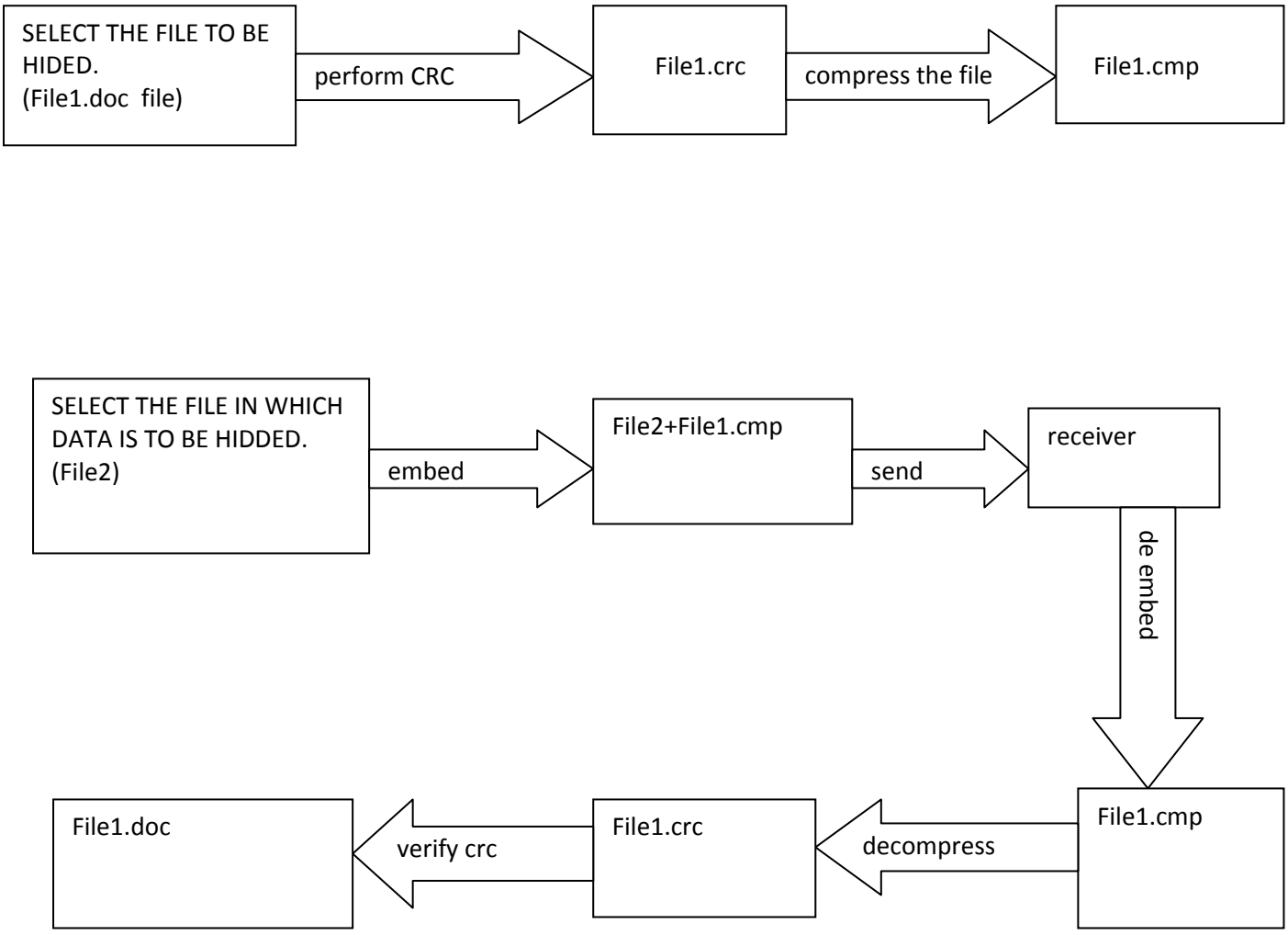
(1) Select the de-embed option under the data tab.
(2) Select the png image file from the filedialog that will appear.
(3) Press the de-embed button.

LSB Algorithm supports simultaneous compression of the carrier which is advantageous for sending. There are no visible significant changes in the image file before and after embedding the information.

DIGITAL MEDIA STEGANOGRAPHY

Software supports hiding of a media information file with any other media file. There can be many instances where a person may want to hide any information like any designs or business plans for which he/she will need media steganography.

EMBEDDING OF DOCUMENT/PDF FILE WITH OTHER MEDIA FILE

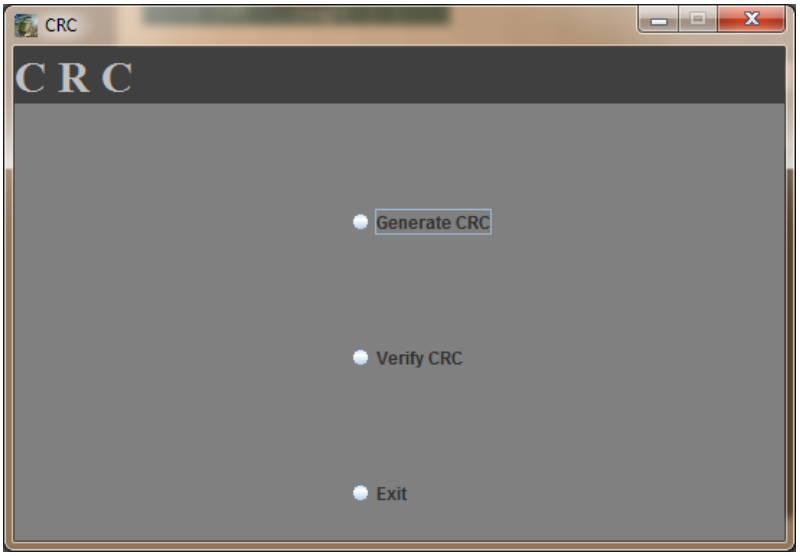


Process to be followed for embedding doc or pdf file with media files :

1.CRC

This embedding process has the feature of verifying the message at the receiver end, for this a Cyclic redundancy check is performed on the message file and a 64-bit checksum value is generated and is attached to data.
This acts as identification and tells whether the information is same that was sent or not.
In the menu bar under the data option, select 'generate crc'.

- 'Generate CRC' accepts the file from the user and automatically generates the CRC value and attach them to the Data .

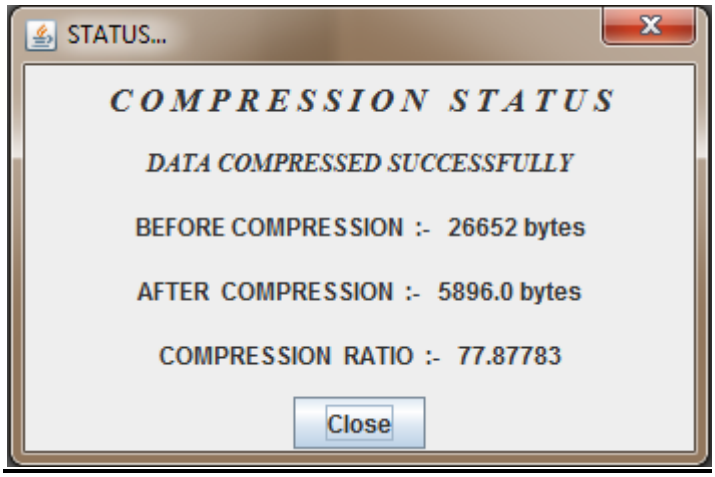


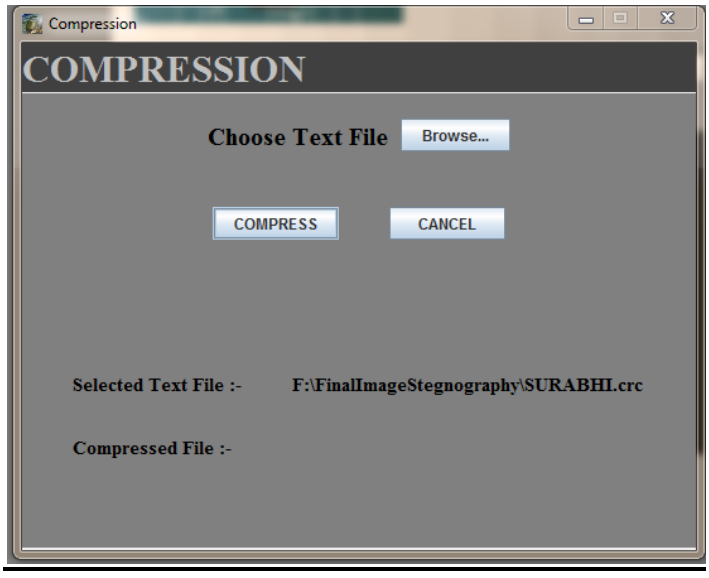
.

2.COMPRESSION

Embedding of large files will increase the size of carrier file which posses a threat to detection of message. As we see, media files are large in size. So, compression of message reduces the risk of detection of message also, increasing the rate of transfer of files between the networks.
In the menu bar, under the utilities, select 'compress'.

- 'Compress' It accepts the text file name from the user and compresses it with a ratio about 15%. The compressed file will have the same name of the text file with the '.CMP' extension. This process is also accompanied with a notification which shows the compression ratio, and size of file before and after compression.

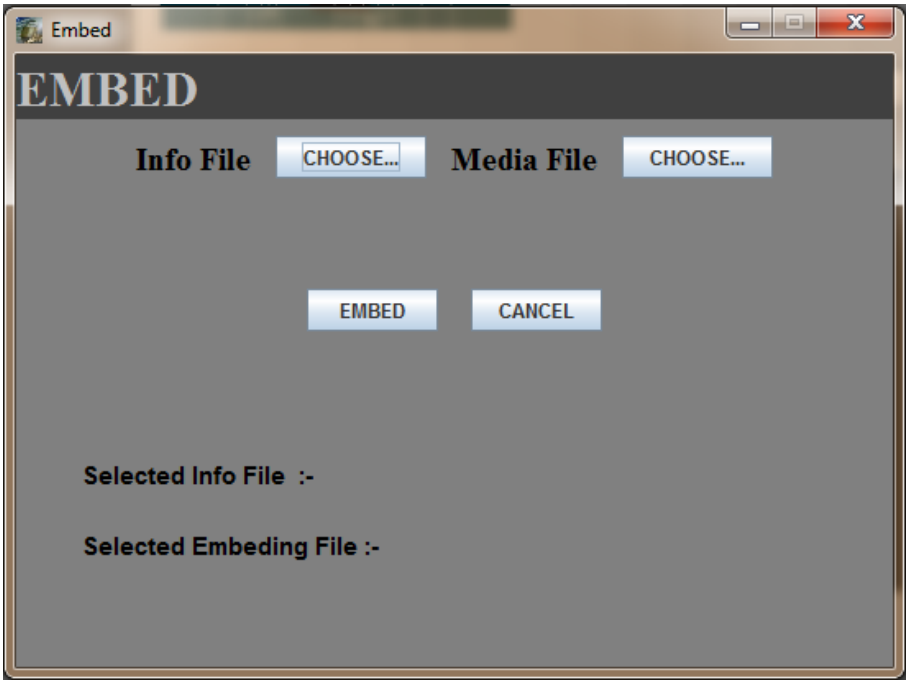




3.EMBED

This module deals with identifying the data and the image to embed the data into the image before it can be transmitted.

The module opens by prompting the user to identify the file that need to be transmitted across the network. The file is then selected using the GUI interface provided through JAVA. The module then prompts to identify the image file, which needs to house the data file. The data is then embedded into the image file in such a way that the image file is not corrupted at the same time the data is secure. The file if hacked or interrupted by a third party can be viewed in any browser or played in any system without actually displaying the hidden data.



4.DE-EMEBED

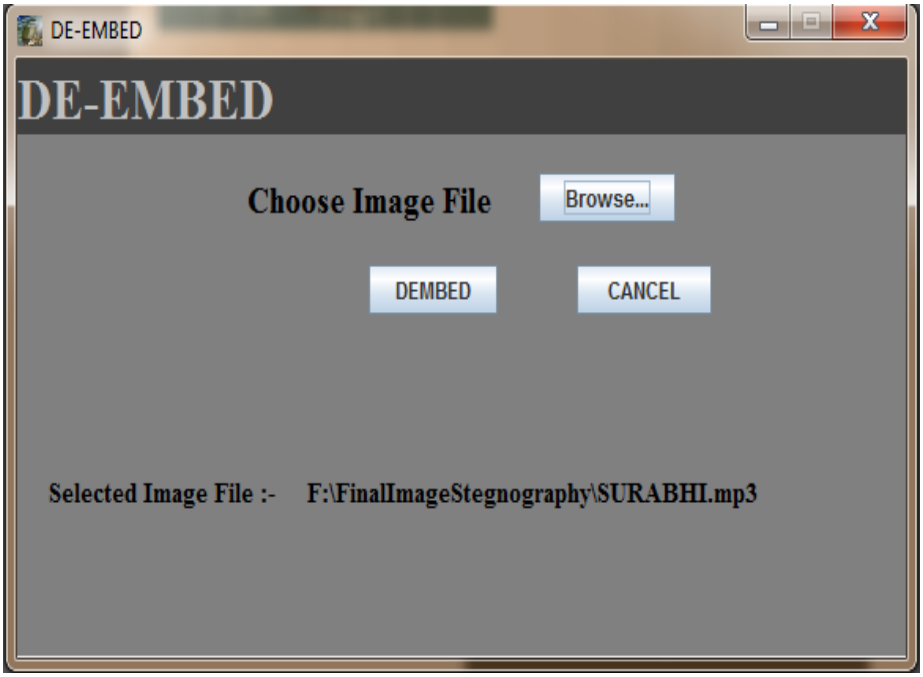
The data on the receivers end is isolated and removed from the image. The module deals with identifying the hidden data in the image. The module receives the media file from the user. The file is then browsed to remove the associated data. The data is then removed from the media file.

This process plays the vital role in the Steganography part. Here the package accepts the media file name and Data file name from the user and generates first the compressed data file which was embedded.
In the menu bar,

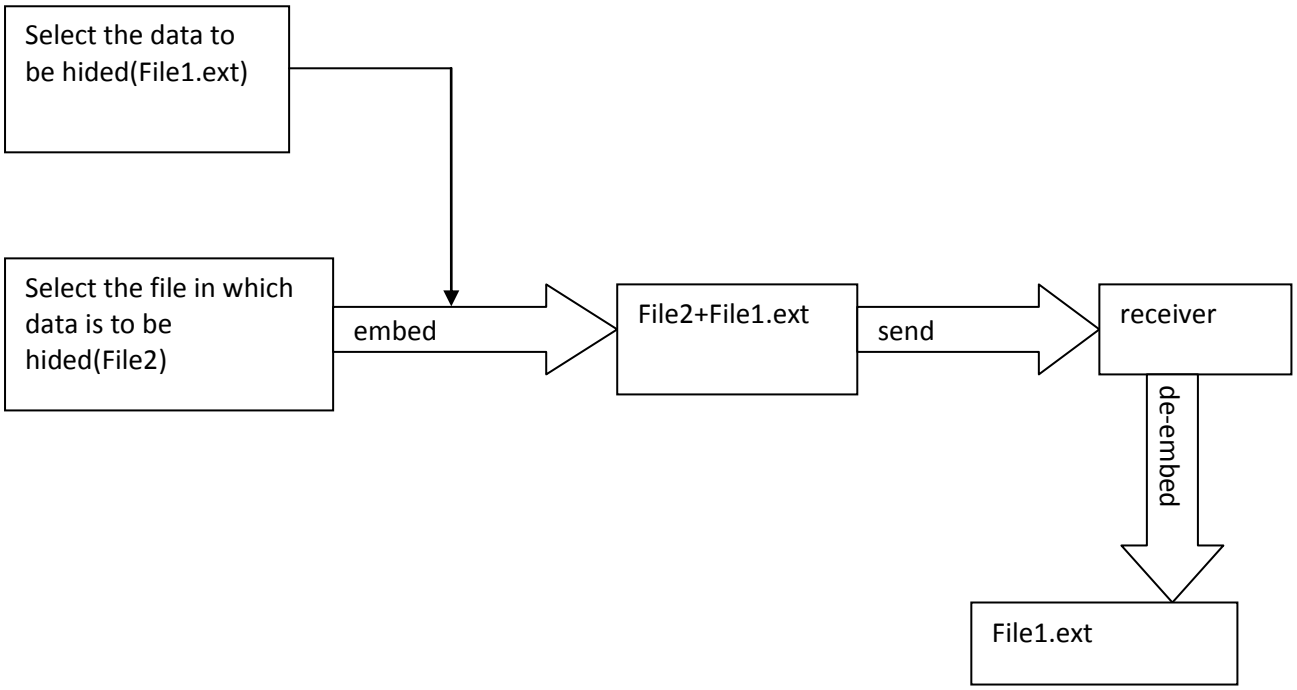
Under the data ,
1. Select the decompress option, which will decompress the compressed data file with '.crc' extension.

Under the data,

1.Select the 'verify crc' option, which will verify the value of checksum and ensures that the data file which was sent has been received without any manipulation and hence the data file is de-embedded.



EMBEDDING OF AUDIO/IMAGE WITH MEDIA FILE



Most of the image types suffer from lossy compression .So compression is not suitable for those types therefore they have to be embedded directly. In this embedding process the image/audio file is directly embedded with the media fie.

1.EMBED

Under the data option in the menu bar, select 'embed'.From the dialogue box, select the audio/image file and the carrier media file in which it has to be embedded,it will be .

2.DE-EMBED

Under the data option in the menu bar, select 'de-embed'.

SENDING OVER LAN

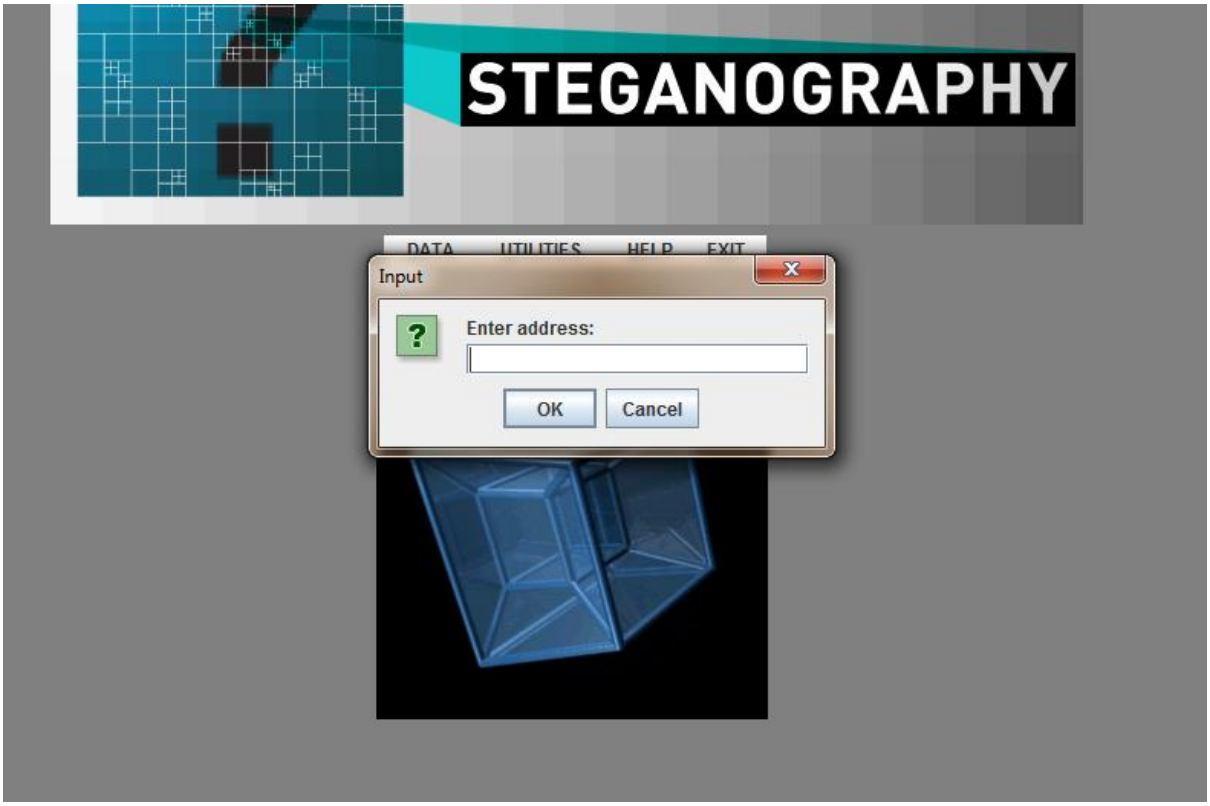
Objective of steganography is to share a information. And if it has to be done with a person connected over the network, it can be achieved with the help of the software only..

To enhance security and so that any third party except the desired receiver does not receive the file, two separate classes have been created to achieve the purpose.

The send option has been included in the software and is placed under the utilities tab.

To make the receiver active a batch file with name server.bat has been placed in the project folder.
As soon as the batch file is run the receiver becomes active and the accept method of the client socket returns true indicating that a connection has been established.

Now, if the client sends any file it will be saved automatically in the directory where the batch file exists with a default name. Then the receiver has to run the software and can regenerate the hidden information from the de-embed option under the data tab.



BIBLIOGRAPHY

(1) Java The Complete Reference, Seventh Edition by Hebert Schildt

(2) www.docs.oracle.com

(3) www.wikipedia.com

(4) www.stackoverflow.com

(5) www.tutorialspoint.com

(6) www.webreference.com