STEGANOGRAPHY

For the course of

IT352 : Information Assurance and Security

Submitted by:

PRITHVI RAJ PATIL (18IT234)

GAGANDEEP KN (18IT215)

ATHARV BELAGALI (18IT208)

Under the guidance of

Dr. Bhawana Rudra

Information Technology , NITK Surathkal

in partial fulfillment for the award of the degree of

Bachelor of Technology

In

Information Technology

at

National Institute of Technology Karnataka, Surathkal.

March 2021

ABSTARCT:

Steganography is basically the art of hiding a message inside another message. In the digital form (computers), a text,audio or an image maybe even a video is concealed within another file.
It is better when compared to cryptography because the third party doesn't really know that there exists an hidden message inside a file.Whereas in case of cryptography the content is kinda blended in and is plainly visible but in a puzzling format but nevertheless arises interest to whoever is looking at the file
Looking into digital steganography, e-communications consists of steganographic coding within a layer usually the transport one,for instance a document/image file. To accommodate lager file for better steganographic transmission media files are used. An instance for it is:Let's say a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.

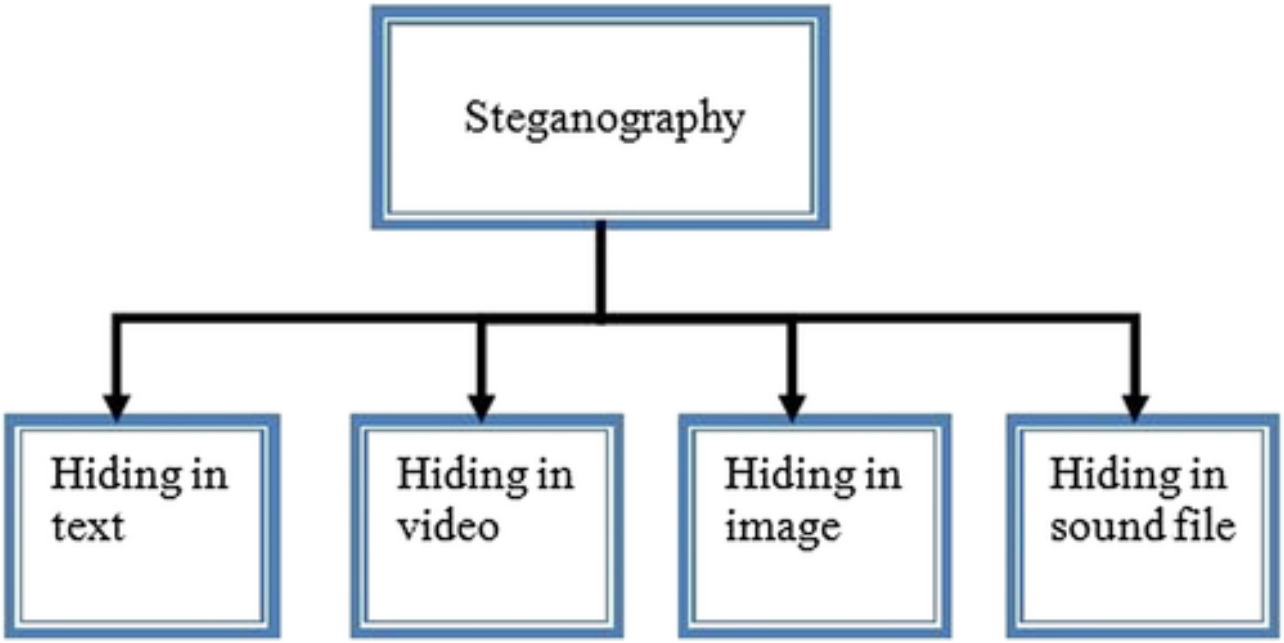
In our paper we try to implement the three major parts of Steganography namely:

1. ***Text***
2. ***Image***
3. ***Audio***

The Ultimate goal is to be able to conceal data in the above three given formats and be able to reveal them by the recipient.

INTRODUCTION:

In the modern era, the data transmission has reached a paramount pinnacle in terms of speed but what about the security of it? The result has made it taht much easier for the data to be interrupted by a third party whose intentions maybe malicious.The data can be altered destroyed ,etc.. , by anonymous users or for unauthorized access by eavesdropper, attacker, and etc. Therefore, secure and safety of data transmission has gained so much relevance in the modern era. Information security has 2 major techniques:Data encryption and data hiding to avoid the above mentioned circumstances.
Encryption basically converts the data into a cypher text during the data transmission phase, which is tough to comprehend unless presented with a decryption key. Data hiding basically consists of hiding a secret data into some random data . The random data are usually digital media like text, audio, image, video, and multimedia and called the cover for secret data. Data hiding has two main branches, steganography and watermarking. We will be looking specifically at steganography in this paper.



In this paper we are focusing only on the text , image and audio format.

Image Steganography:

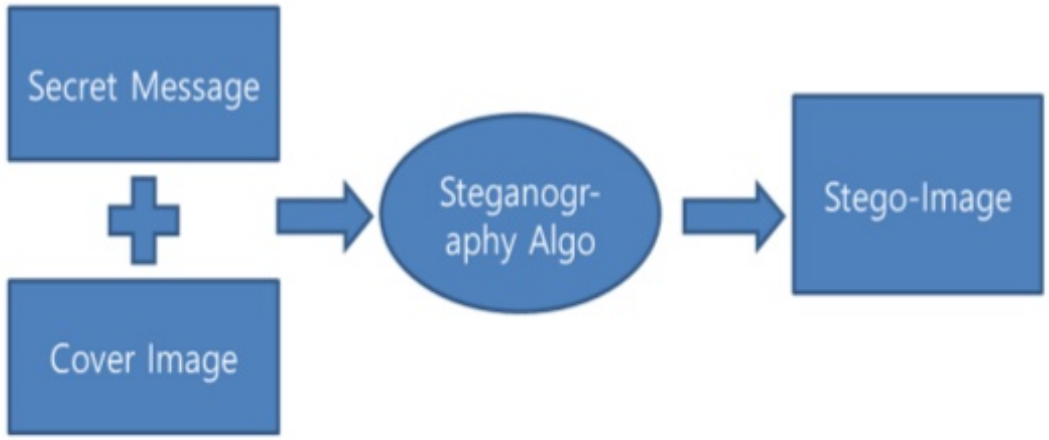


Figure 1.1: **PORCESS OF STEGANOGRAPHY**

to sender and receiver only. The message cannot be accessed by anyone without using the encryption key. However, the transmission of encrypted message may easily arouse attackers suspicion, and the encrypted message may thus be intercepted, attacked or decrypted violently. In order to overcome the shortcomings of cryptographic techniques, steganography techniques have been developed. Steganography is the art and science of communicating in such a way that it hides the existence of the communication. Thus, steganography hides the existence of data so that no one can detect its presence. In steganography the process of hiding information content inside any multimedia content like image , audio, video referred as a Embedding. For increasing confidentiality of communicating data both techniques may combined. Application of Steganeography:

i)Confidential Communication

ii) Protection of Data Alteration

iii) Access Control System for Digital Content Distribution

iv) E-Commerce

v) Media

vi) Database Systems.

This technique is used for hiding data inside the image. Hiding the data in an image file causes a slight alteration to the image such as: the bit quality will be changed (e.g., resolution or color),pixels also change when compared to the original image . On the other hand, the limitations on the binary string length, size, and number of pixels in the image, which each pixel hides one bit in it using one of the image steganography algorithms. The simplest method is to append the message to the end of the image. So the image is viewed by some image viewer application and the text at the EOF(end of file) is generally ignored.The image steganography can be classified as spatial domain steganography and transform domain steganography.

Text Steganography:

Text steganography is a mechanism of hiding secret text message inside another text as a covering message or generating a cover message related with the original secret message.

There are three main categories used to hide text-in-text messages:

1.format based

2. random and statistical generations

3.linguistic method.

Audio Steganography:

Here a secret message is embedded into a digitized audio signal which results in slight altering of binary sequence of the corresponding audio file. There are several methods available for audio steganography. It involves hiding data in audio files. This

method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography which are listed below:

i) Low Bit Encoding

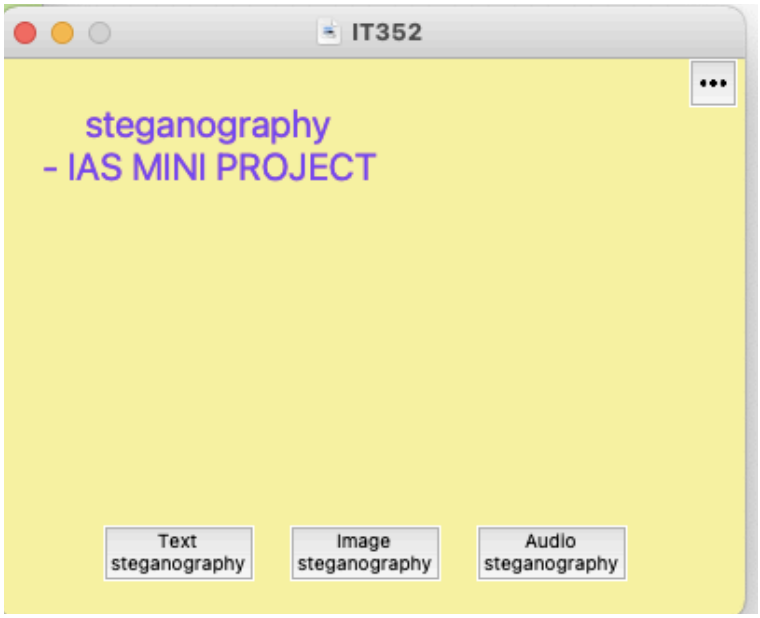
ii) Phase Coding

iii) Spread Spectrum.

Progress:

Main driver part of the project is implemented

UI of the main page is completed

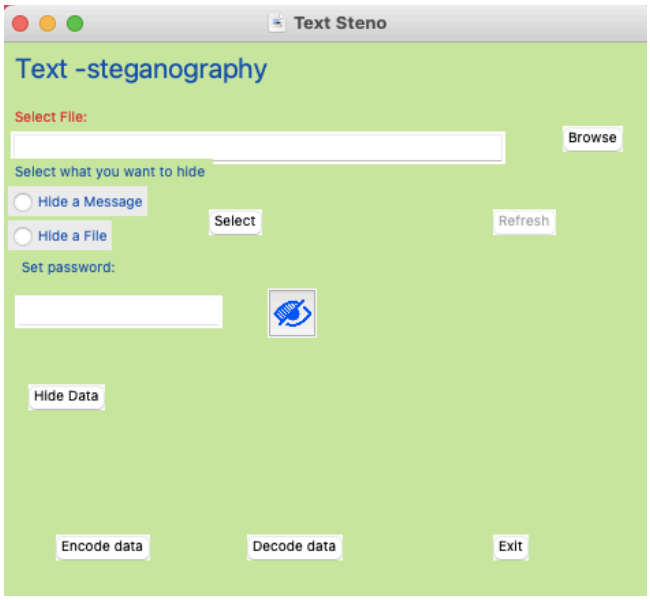


Text Steganography :

Python script of this part is completed,

```
def encode(passwd: str, infile: str, outfile: str, file: str = None, message: str = None):
    if message is not None:
        command = 'snow -C -Q -p "{}" -m "{}" {} {}'.format(passwd, message, infile, outfile)
        os.system('cmd /c' + command)
        db.format_txt(outfile, passwd)
    elif file is not None:
        command = 'snow -C -Q -p "{}" -f {} {} {}'.format(passwd, file, infile, outfile)
        os.system('cmd /c' + command)
        db.format_txt(outfile, passwd)
```

UI design part of text steganography is completed



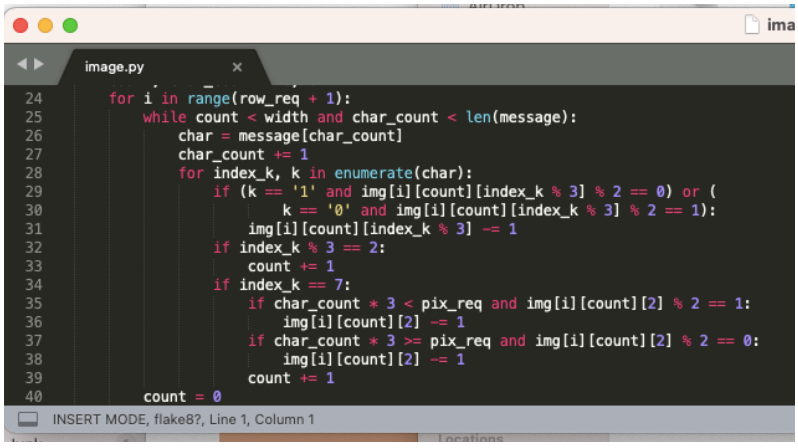
Output:
There is some error in saving the text file after embedding the secret message

Work left:

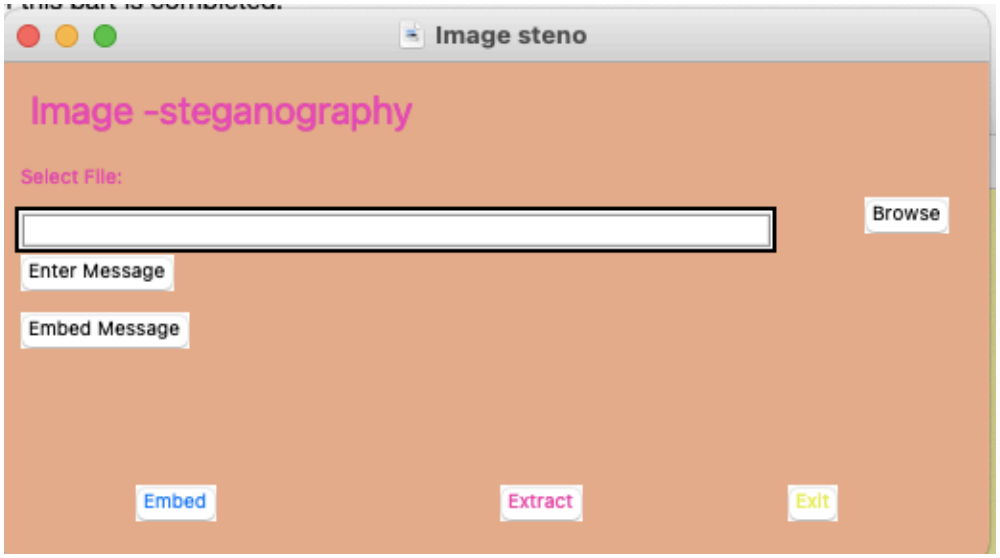
Debug the error and make sure the hidden text is saved as text file with the cover text file

Image steganography:

Python script of this part is completed



UI design is successfully implemented



Output:
Desired output is obtained

Result: Image steganography part is successfully implemented

Audio steganography:
Working on the python script of the audio part
And UI is yet to be designed

Overall:
Image steganography is 100% implemented
Text steganography has debugging left
Audio steganography is in progress