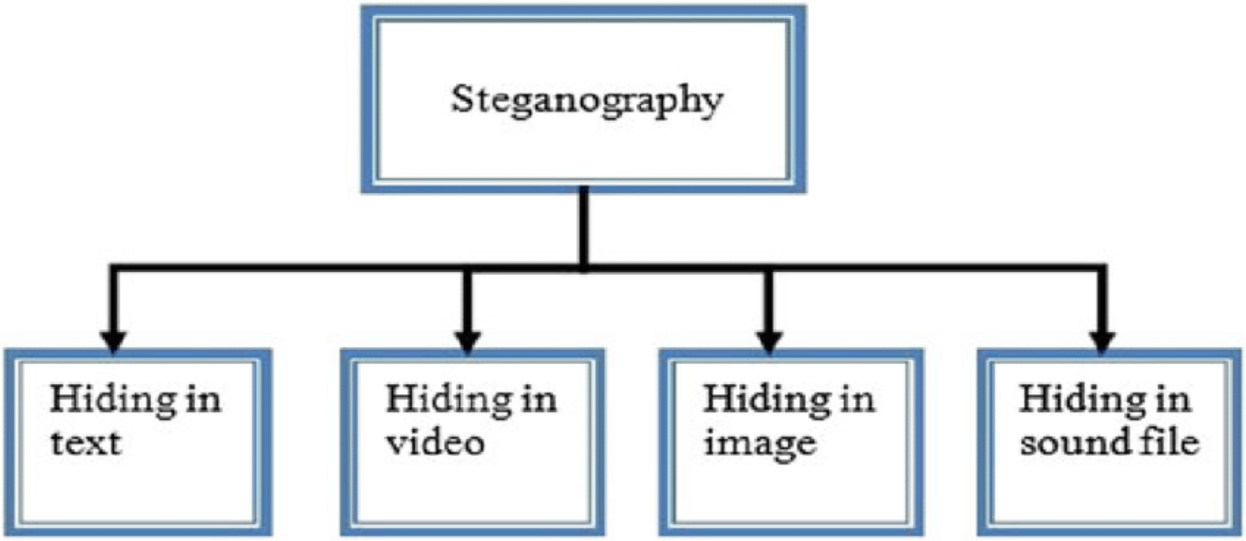
1. Introduction

Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out to the usual. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between two is that steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information.

What steganography essentially does is exploit human perception, human senses are not trained to look for files that have information inside of them, although this software is available that can do what is called Steganography. The most common use of steganography is to hide a file inside another file.



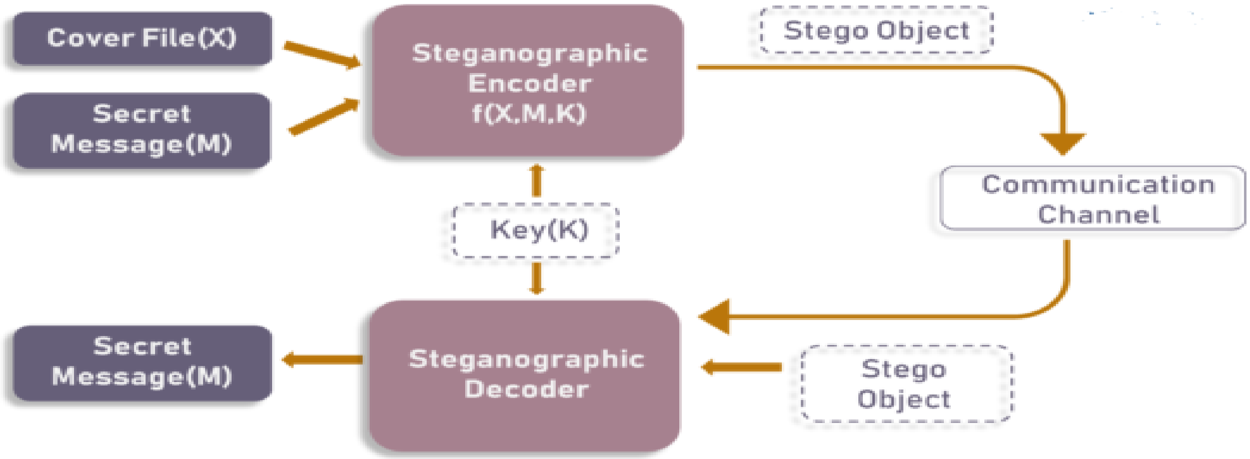
1.1 Project Scope:

This project is developed for hiding information in any image file. The scope of the project is implementation of steganography tools for hiding information includes any type of information file and image files and the path where the user wants to save Image and extruded file.

2. Methodology

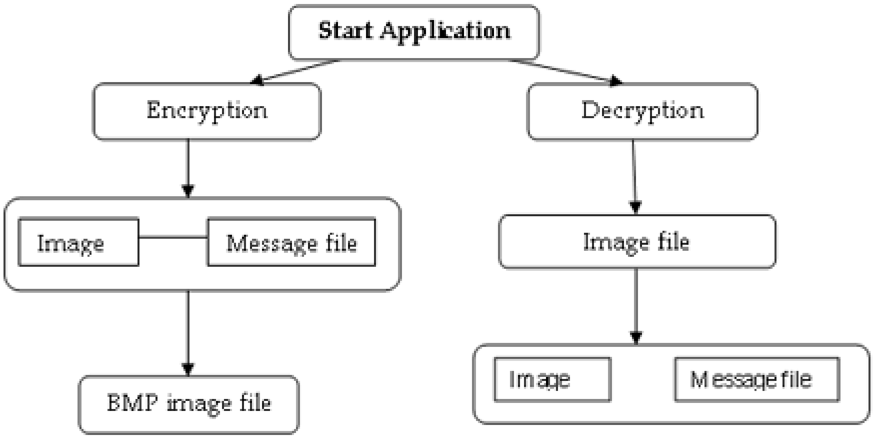
The user needs to run the application. The user has two tab options – encrypt and decrypt. If the user select encrypt, the application gives the screen to select an image file, information file, and option to save the image file. If the user select decrypt, the application gives the screen to select the image file and ask the path where the user wants to save the secrete file.

2.1. Proposed Model



2.2 Graphical Representation:

The graphical representation of Steganography system is as follows:



Encoding

There are a lot of algorithms that can be used to encode data into the image, and in fact, you can also make one yourself. The one being used in this blog is easy to understand and implement, as well.

The algorithm is as follows:

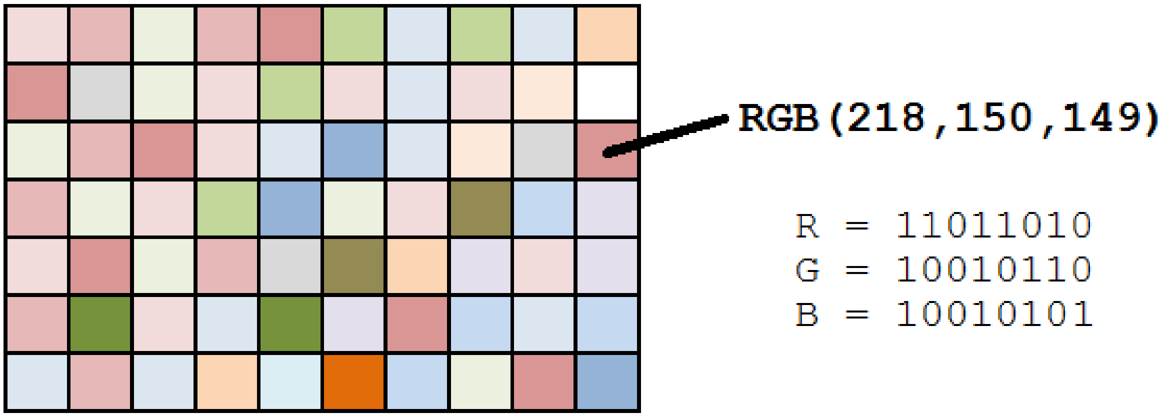
1) For each character in the data, its ASCII value is taken and converted into an 8-bit binary [1].

2) Three pixels are read at a time having a total of 3*3=9 RGB values. The first eight RGB values are used to store one character that is converted into an 8-bit binary.

3) The corresponding RGB value and binary data are compared. If the binary digit is 1 then the RGB value is converted to odd and, otherwise, even.

4) The ninth value determines if more pixels should be read or not. If there is more data to be read, i.e. encoded or decoded, then the ninth-pixel changes to even. Otherwise, if we want to stop reading pixels further, then make it odd.

5) Repeat this process until all the data is encoded into the image.



Decoding

For decoding, we shall try to *reverse* the previous algorithm that we used to encode data.

The algorithm is as follows:

1) Again, three pixels are read at a time. The first 8 RGB values give us information about the secret data, and the ninth value tells us whether to move forward or not.

2) For the first eight values, if the value is odd, then the binary bit is 1, otherwise it is 0.

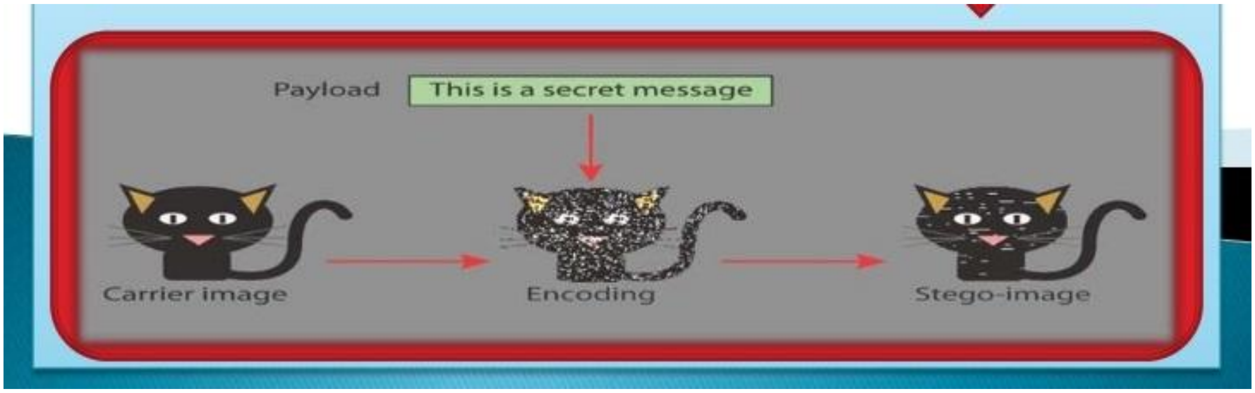
3) The bits are concatenated to a string, and with every three pixels, we get a byte of secret data, which means one character.

4) Now, if the ninth value is even then we keep reading pixels.

2.3 Example

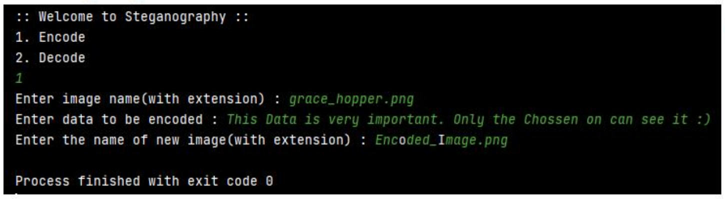
There are many ways to conceal information using Steganography. The most common method is by embedding information into digital images.

We all know that digital images say, a JPEG image, contains several megabytes of data in the form of pixels.



3. Implementation

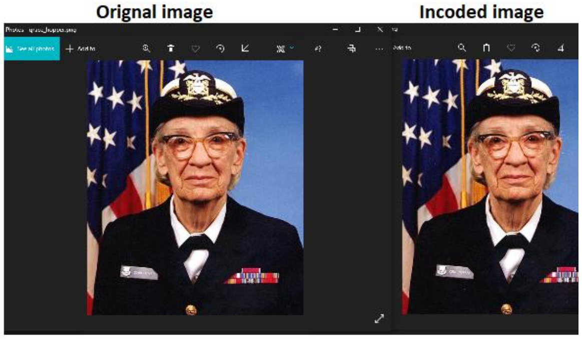
Encodeing Image



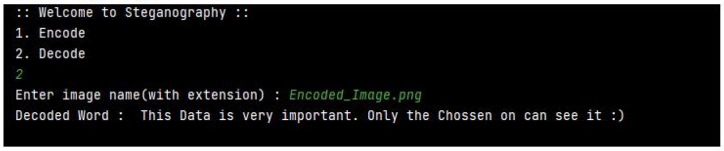
```
:: Welcome to Steganography ::
1. Encode
2. Decode
1
Enter image name(with extension) : grace_hopper.png
Enter data to be encoded : This Data is very important. Only the Chossen on can see it :)
Enter the name of new image(with extension) : Encoded_Image.png

Process finished with exit code 0
```

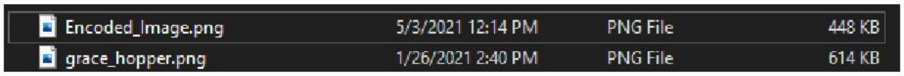
Orignal image Incoded image



Decodeing Image



```
:: Welcome to Steganography ::
1. Encode
2. Decode
2
Enter image name(with extension) : Encoded_Image.png
Decoded Word :  This Data is very important. Only the Chossen on can see it :)
```



Encoded_Image.png	5/3/2021 12:14 PM	PNG File	448 KB
grace_hopper.png	1/26/2021 2:40 PM	PNG File	614 KB

The **encrypt module** is used to hide information into the image; no one can see that information or file. This module requires any type of image and message and gives the only one image file in destination.

The **decrypt module** is used to get the hidden information in an image file. It take the image file as an output, and give two file at destination folder, one is the same image file and another is the message file that is hidden it that.

3.1. Advantage

- Difficult to Detect
- Only Receiver can Detect
- It can done faster through large no. of softwares
- Important communication exchange
- Provides better security through LAN, MAN, WAN
- Can be applied differently with audio, video and Image.
- Hide data over encryption is that it helps obscure the fact that there is sensitive data hidden in the file or other content carrying the hidden text.

3.2 Disadvantage

- Only Small size of photos can conceal
- Breaking down of software or server can replicate the Data
- Suspicious Activity Inclusion
- Invalidate Signatures
- Invalidate Hashing

3.3 Applications:

a) Used in modern printers.

b) Alleged use by terrorists.

c) Alleged use by intelligence department.

d) Privacy and anonymity is a concern on the internet.

e) Allows for two parties to communicate secretly and covertly.

f) It allows for some morally-conscious people to safely whistle blow on internal actions.

g) It allows for copyright protection on digital files using the message as a digital watermark.

h) One of the other main uses for Image Steganography is for the transportation of high-level or top-secret documents between international governments.

4. Conclusion

This Software will be Harder and more complex, Any Shape and Size Image will Hide and Carry Message, Less Data Reduction, Image Communication with less time and space complexity, Active and passive attacks will not easily able to break down the system. The new image(encoded image) looks exactly the same as the original image(original image) to the human eyes. The slight change in the pixel values is unnoticeable to the human eyes. It is impossible for a human to distinguish between the two images. Even for a computer, it will be very difficult to detect the image as a Steganography image if it does not have access to the original image, to compare the two against each other.