SE EXTC (2020 - 2021) Python project report

Project member details

Name: Piyush Gupta	Roll number. 19014A0008
Name: Yajnesh Shetty	Roll number. 19104A0019
Name: Nikunj Tandan	Roll number. 19104A0031
Name: Vaibhav Kamble	Roll number. 19104A0038

Project title: DIGITAL STENOGRAPHY

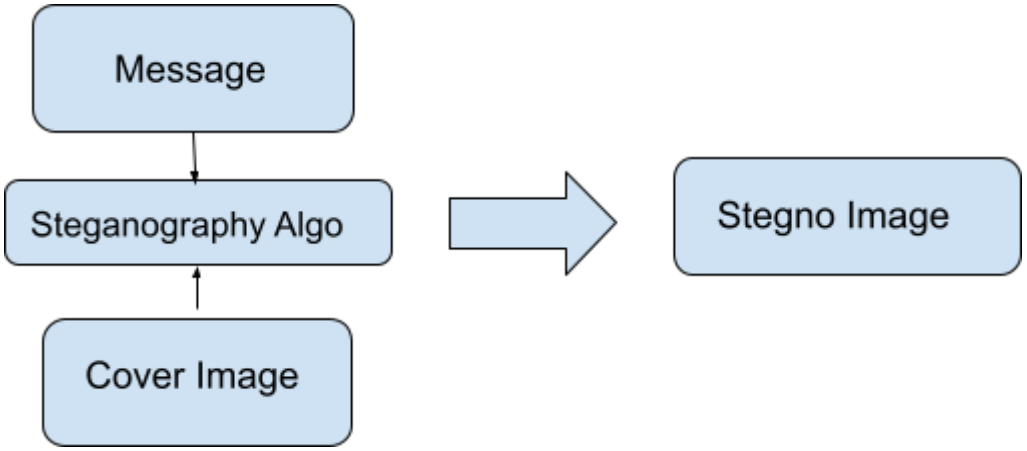
Abstract:

Steganograpy refers to data hiding. The main purpose of steganography is to hide the message into the image. Before these modern cryptography techniques, steganography was popular for secure communication. There are many techniques to hide information into the image, this project uses LSB hash technique. This technique embeds the bit of the message into the least significant bit of the image byte. LSB hash technique may change the properties of the original image, but there is no visual change in the image. This report also presents a method to decrypt the image and extract the secret data from the image.

Introduction:

Steganography is the art and science of hiding one type of information (eg, text message) into the image. It is a greek word which means concealed writing. The word steganos means covered and graphial means writing. This can be accomplished by changing the least significant bit of the image byte according to our need. As we all know, a digital image is made of pixels and every pixel has a certain value assigned to it, so by manipulating the last bit of that pixel value we can achieve our goal.
It had an advantage over cryptography as now the middle person does not come to know whether data is hidden in the image or not. The security and the reliability of data transmission also improved with the invention of steganography as now no other person could change the sent data.
The main application fields of steganography are:

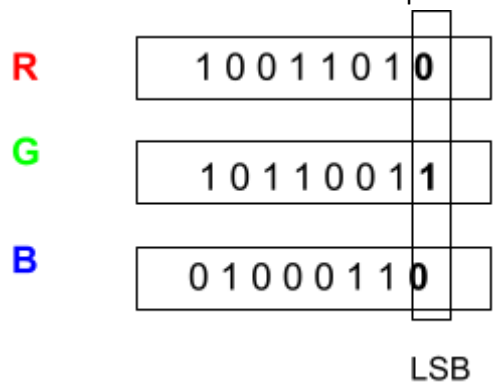
- Copyright Protection
- Feature Tagging
- Digital Watermarking



LSB Technique:
The advantage of changing the least significant bit is that it doesn't affect our image pixel value very much, there is just a unit change in the value.
For example:
Let's consider we want to conceal the alphabet “H ” into the image byte.
The Ascii value of the letter “H ” is 72. So, its binary representation is 0 1 0 0 1 0 0 0.

Consider, first pixel value of image is
R = 1 0 0 1 1 0 1 **1**
G = 1 0 1 1 0 0 1 **0**
B = 0 1 0 0 0 1 1 **0**

First bit of the letter H is ’0’, so we change the LSB of the red pixel from ‘1’ to ‘0’. Same for the second bit of letter H is ‘1’ so we will change the LSB of green pixel from ‘0’ to ‘1’. In case of a third bit of letter H is ‘0’ and LSB of blue pixel value is also ‘0’, so there will be no change.



This process is very lengthy, because converting every image pixel value into its binary, and after manipulating again converting it into decimal value, consumes a lot of processing power as well as time. So, to tackle this problem instead of manipulating every LSB of byte we will convert the value into even or odd.
For example:
If we want to change the LSB of the red pixel from ‘1’ to ‘0’, we will simply convert that pixel value from Odd to Even by adding 1 or subtracting 0 and vice versa. This will save our processing power as well as time.

Working:

This project uses LSB substitution. Modules used in this project are:

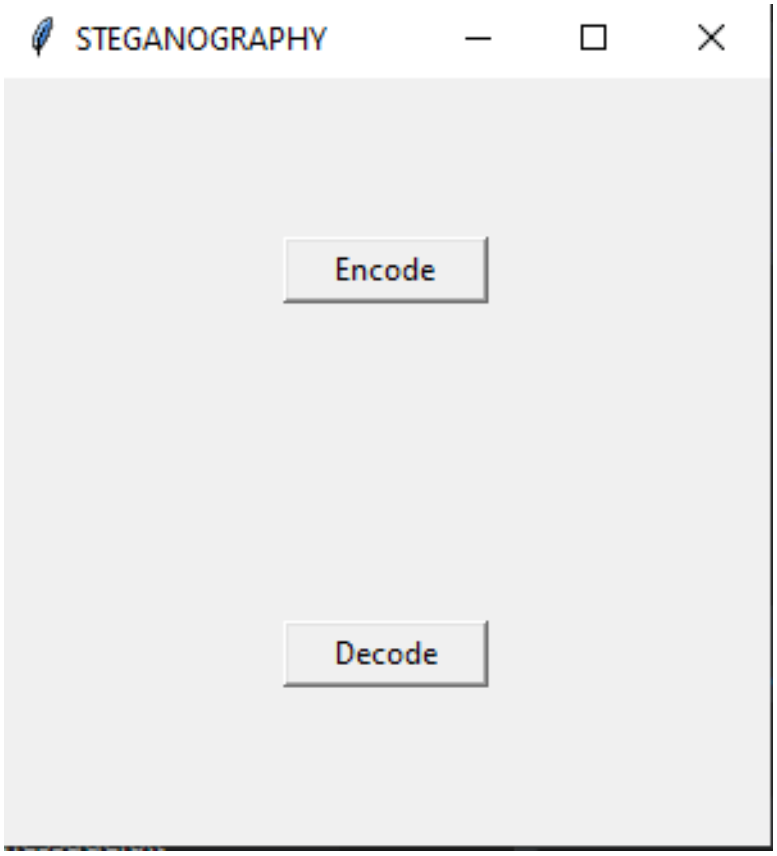
- tkinter
- PIL
- numpy
- cv2
- matplotlib
- os

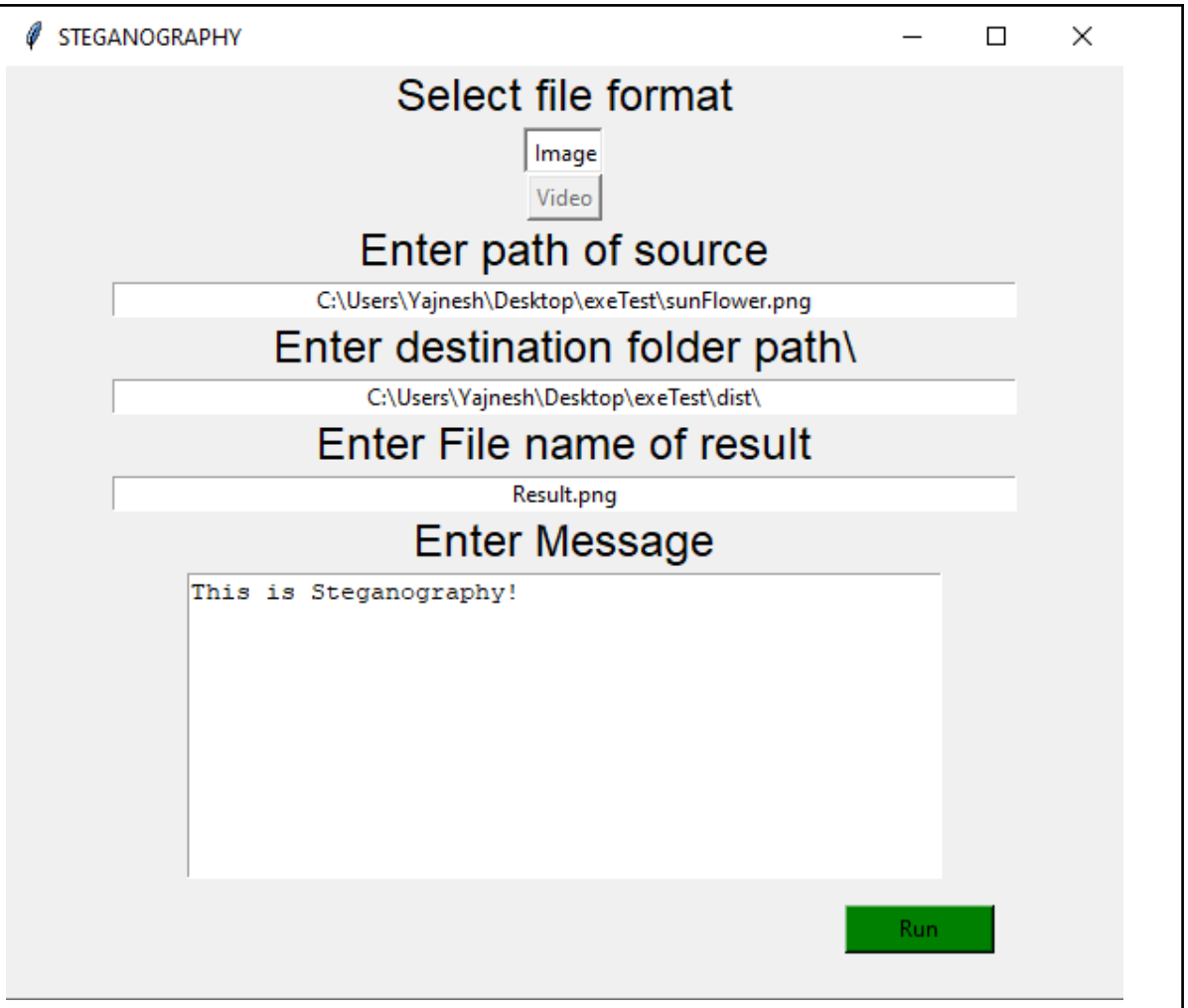
FIrst the user inputs the source image and that image is converted into an array depending upon the number of image channels and then it is converted into 1-D array with the help of imgData(image) function. After this, the user inputs the secret message for which she/he wants to encode into image, the message is converted into its binary value with the help of message(textFile) function. Further encode(imgData , messageData, shape) function is used to conceal the binary data of message into image pixel by using few for loops and IF conditions (refer below image).

After the encoding part, the user is asked for the path, to save the stegno image.

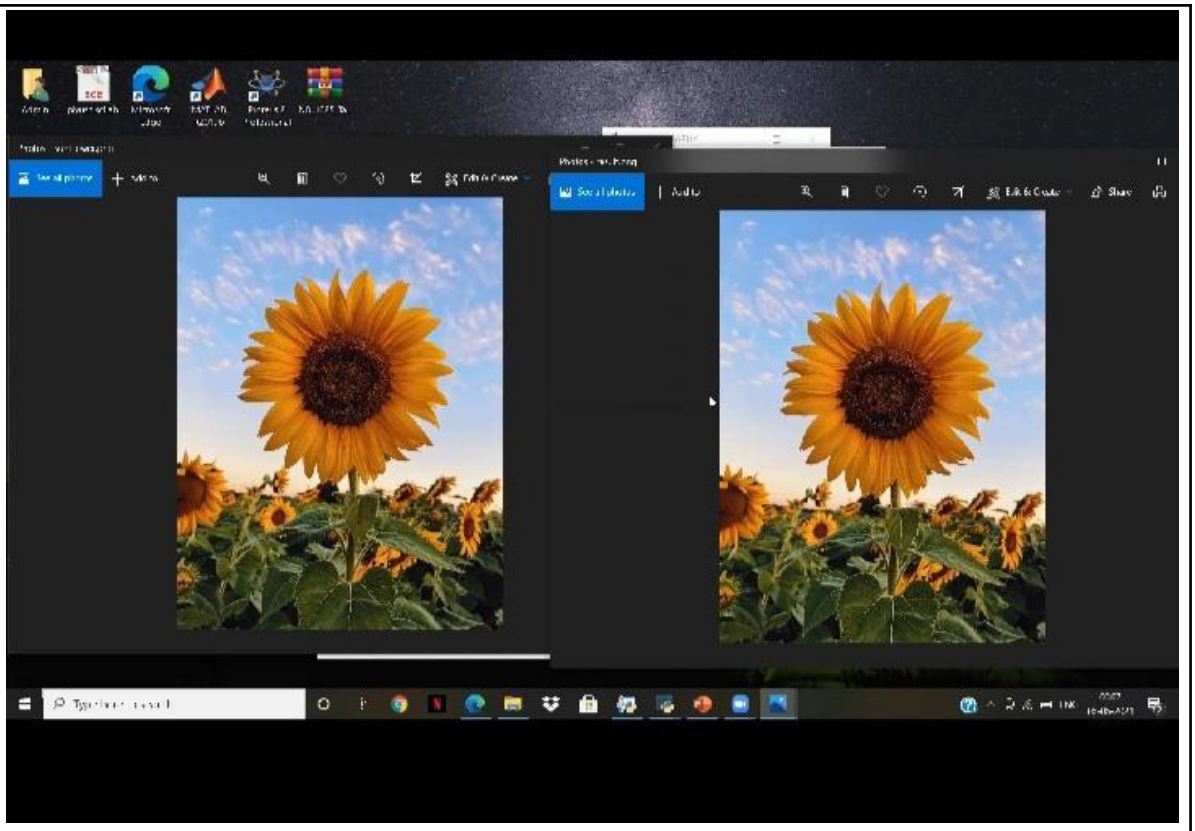
For decoding of the image and extracting secret data, the program uses decode(imgData) function, it first convert the input image into array and then into 1-D array, and then checking for weather the pixel value is Even or Odd it makes another array any appends the value '0' for Even and '1' for Odd. And then converting the list into its Ascii character and displaying it on the window. Program also creates one text file of secret messages inside the given directory.

Output: ENCODING

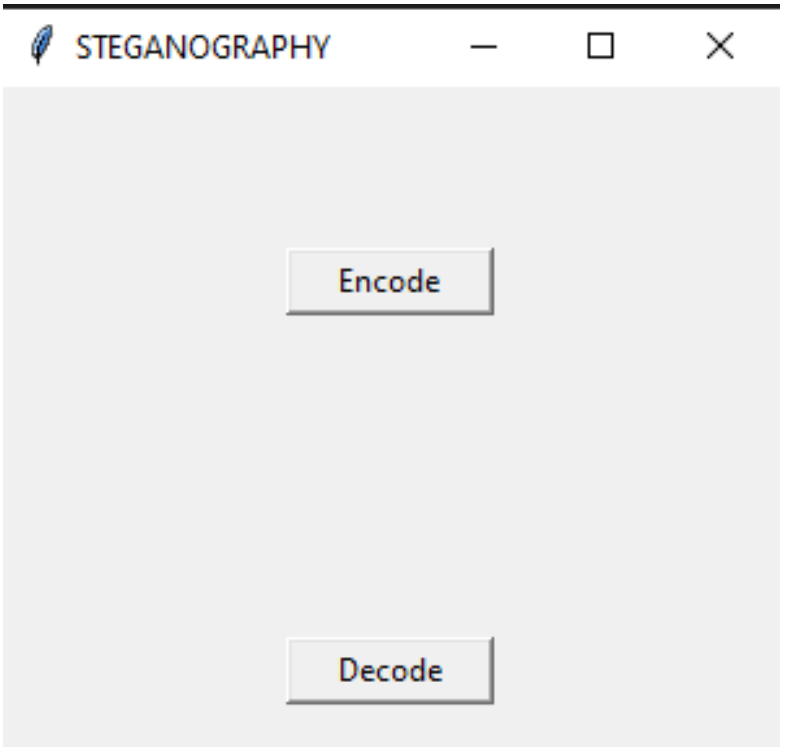


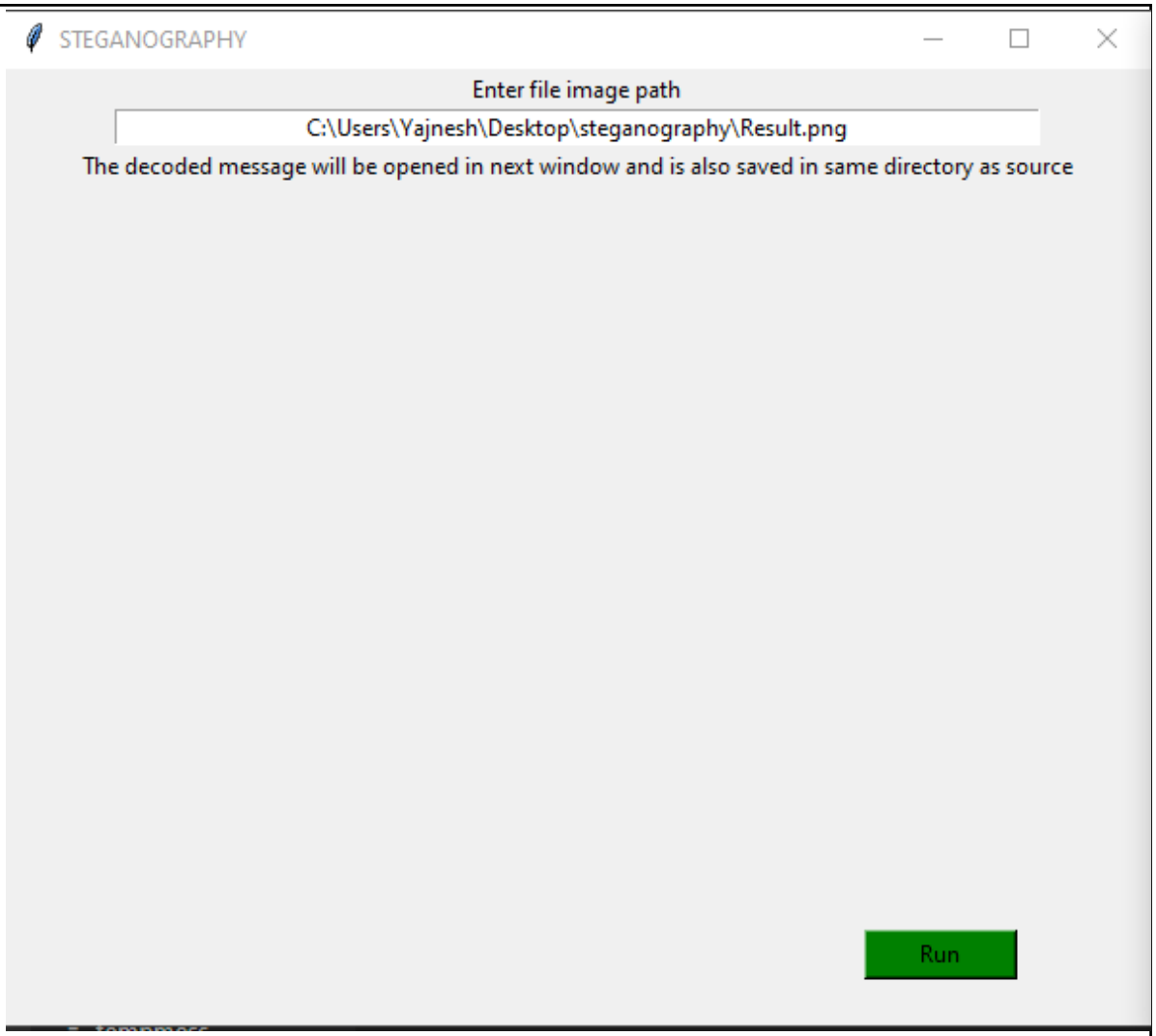


Comparison between source image and stegno image:



DECODING





Conclusion:

In this project we got to know that Stenography protects the data by hiding it and makes communication possible only for sender and authorized person. Though stenography is not implemented in wider ways but it can be the best security tool and is also a great tool for ethical

hackers too. Its been observed that through LSB substitution the data hiding is very impressive as it uses the simple algorithm and it can convert any image into a steganographic image.