# Steganography Using Python

**Rajrishi Sengupta*[1], C. Umarani*[2]**

*[1,2]Department of MCA, Jain University, Bangalore, Karnataka, India.*

*[1]raj.rishi.581@gmail.com*

*[2]c.umarani@jainuniversity.ac.in*

***Abstract—****Steganography is the craft of concealing the way that correspondence is occurring, by concealing data in other data. A wide range of bearer record organizations can be utilized, yet computerized pictures are the most mainstream in light of their recurrence on the web. For concealing mystery data in pictures, there exists a huge assortment of steganography procedures some are more mind boggling than others and every one of them have individual solid and feeble focuses. Various applications may require outright imperceptibility of the mystery data, while others require an enormous mystery message to be covered up. This undertaking report means to give a review of picture steganography, its uses and strategies. It likewise endeavours to distinguish the necessities of a decent steganography calculation and quickly thinks about which steganographic methods are progressively reasonable for which applications.*

***Keyword—****Steganography, Techniques, Algorithm, Message, Calculation.*

## 1. INTRODUCTION

The point that is chosen is Steganography Using Python, one explanation that gatecrashers can be productive is most of the information they get from a system is in a construction that they can scrutinize and comprehend. Intruders may uncover the information to others, change it to misshape an individual or affiliation, or use it to dispatch an attack. One response for this issue is, utilizing steganography. Steganography is a technique for disguising information in modernized media. Rather than cryptography, it isn't to safeguard others from knowing the covered information yet it is to protect others from envisioning that the information even exists. Steganography become progressively significant as more individuals join the internet upheaval. Steganography is the craft of hiding data in manners that forestalls the identification of shrouded messages. Steganography incorporate a variety of mystery specialized strategies that conceal the message from being seen or found.

Due to propels in ICT, the vast majority of data is kept electronically. Therefore, the security of data has become a principal issue. Other than cryptography, steganography can be utilized to make sure about data. In cryptography, the message or encoded message is inserted in an advanced host before going it through the system, in this manner the presence of the message is obscure. Other than concealing information for privacy, this methodology of data stowing away can be reached out to copyright insurance for advanced media: sound, video and pictures.

This venture gives subtleties how to share information utilizing steganography.

The creating possibilities of current trades need the extraordinary strategies for security especially on PC mastermind. The framework security is getting dynamically huge as the amount of data being exchanged on the web increases. Thusly, the characterization and data decency are needing to guarantee against unapproved access and use. This has achieved a tricky improvement of the field of information concealing

Data concealing is a rising investigation region, which incorporates applications, for instance, copyright protection for cutting edge media, watermarking, fingerprinting, and steganography.

In watermarking applications, the message contains information, for instance, owner distinctive evidence and a modernized time stamp, which typically applied for copyright confirmation.

Unique mark, the owner of the enlightening record embeds a consecutive number that strikingly perceives the customer of the instructive file. This adds to copyright information to makes it possible to follow any unapproved utilized of the informational collection back to the client.

Steganography cover up the discharge message inside the host informational collection and nearness intangible and is to be dependably imparted to a collector. The host informational index is deliberately adulterated, however in an incognito way, intended to be imperceptible to a data examination.

## 2. ADVANTAGE OF STEGANOGRAPHY

Up to now, cryptography has reliably had its complete occupation in guaranteeing the secret between the sender and the arranged gatherer. Nevertheless, nowadays' steganography strategies are used continuously other than cryptography to add progressively guarded layers to the covered data. The advantage of using steganography over cryptography alone is that the arranged secret message doesn't stand apart to itself as an object of assessment. Clearly clear encoded messages, paying little mind to how tough they are, animate interest and may in themselves be embroiling in countries in which encryption is unlawful.

## 3. TYPES OF STEGANOGRAPHY

Steganography works have been completed on various transmission media like pictures, video, content, or sound

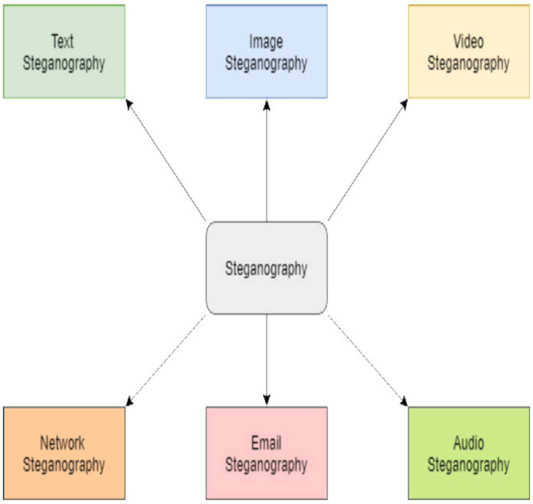


**Fig. 1 Types of Steganography**

## 4. BASIC STEGANOGRAPHIC MODEL

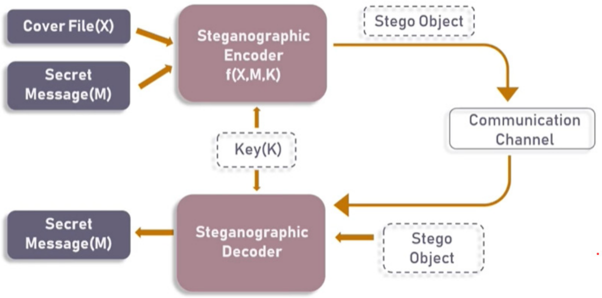


**Fig. 2 Steganographic Model**

As found in the above picture, both the first picture file(X) and mystery message (M) that should be covered up are taken care of into a steganographic encoder as info. Steganographic Encoder work, f(X,M,K) inserts the mystery message into a spread picture record by utilizing procedures like least critical piece encoding. The subsequent stego picture looks fundamentally the same as your spread picture record, with no obvious changes. This finishes encoding. To recover the mystery message, stego object is taken care of into Steganographic decoder.

This paper will assist you with implementing picture steganography utilizing Python. It will assist you with composing a Python code to conceal instant messages utilizing a procedure called Least Significant Bit

### 4.1 Least Steganographic Model

We can portray a computerized picture as a limited arrangement of advanced qualities, called pixels. Pixels are the littlest individual component of a picture, holding esteems that speak to the splendour of a given shading at a particular point. So we can think about a picture as a network (or a two-dimensional cluster) of pixels which contains a fixed number of lines and sections.

Least Significant Bit (LSB) is a strategy wherein the last piece of every pixel is changed and supplanted with the mystery message's information bit.

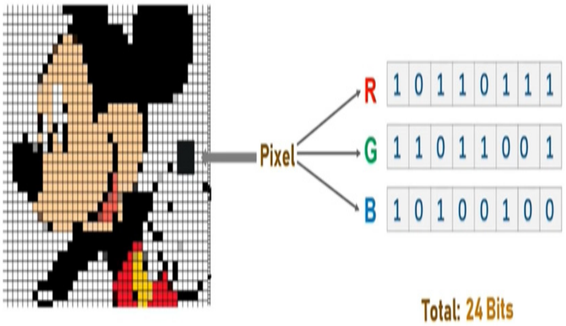


**Fig. 3 RGB Pixel**

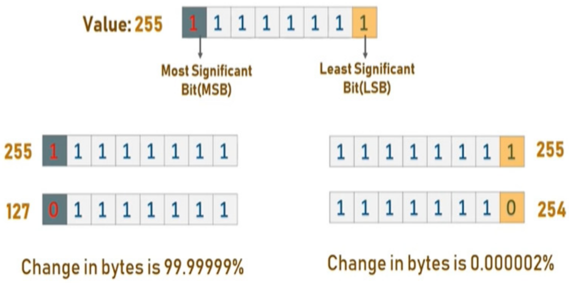

Value: 255 1 1 1 1 1 1 1 1
Most Significant Bit(MSB)
Least Significant Bit(LSB)
255 1 1 1 1 1 1 1 1
127 0 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 255
1 1 1 1 1 1 1 0 254
Change in bytes is 99.99999%
Change in bytes is 0.000002%

**Fig. 4 Bit Detail**

From the above image it is clear that, if we change MSB it will have a larger impact on the final value but if we change the LSB the impact on the final value is minimal, thus we use least significant bit steganography.

### 4.2 How LSB Techniques Work

Every pixel contains three qualities which are Red, Green, Blue, these qualities run from 0 to 255, at the end of the day, they are 8-piece esteems. Let's take a case of how this strategy functions, assume you need to shroud the message "howdy" into a 4x4 picture which has the accompanying pixel esteems:

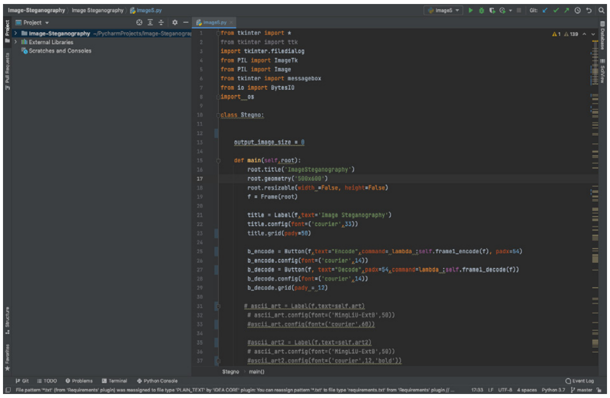
[(225, 12, 99), (155, 2, 50), (99, 51, 15), (15, 55, 22), (155, 61, 87), (63, 30, 17), (1, 55, 19), (99, 81, 66), (219, 77, 91), (69, 39, 50), (18, 200, 33), (25, 54, 190)]

Utilizing the ASCII Table, we can change over the mystery message into decimal qualities and afterward into parallel: 0110100 0110101.Now, we repeat over the pixel esteems individually, subsequent to changing over them to twofold, we supplant every least noteworthy piece with that message bits successively (e.g 225 is 11100001, we supplant the last piece, the bit morally justified (1) with the primary information bit (0) thus on).This will just adjust the pixel esteems by +1 or - 1 which isn't recognizable in any way. The subsequent pixel esteems in the wake of performing LSBS is as demonstrated as follows:

[(224, 13, 99), (154, 3, 50),(98, 50, 15),(15, 54, 23),(154, 61, 87),(63, 30, 17),(1, 55, 19),(99, 81, 66),(219, 77, 91),(69, 39, 50),(18, 200, 33),(25, 54, 190)]

## 5. HIDING TEXT IN IMAGE USING PYTHON

In this section, we can find a step-by-step of the hide and reveal process using Python code. You can upload the image(png) that you would like to use for steganography using the encode option.

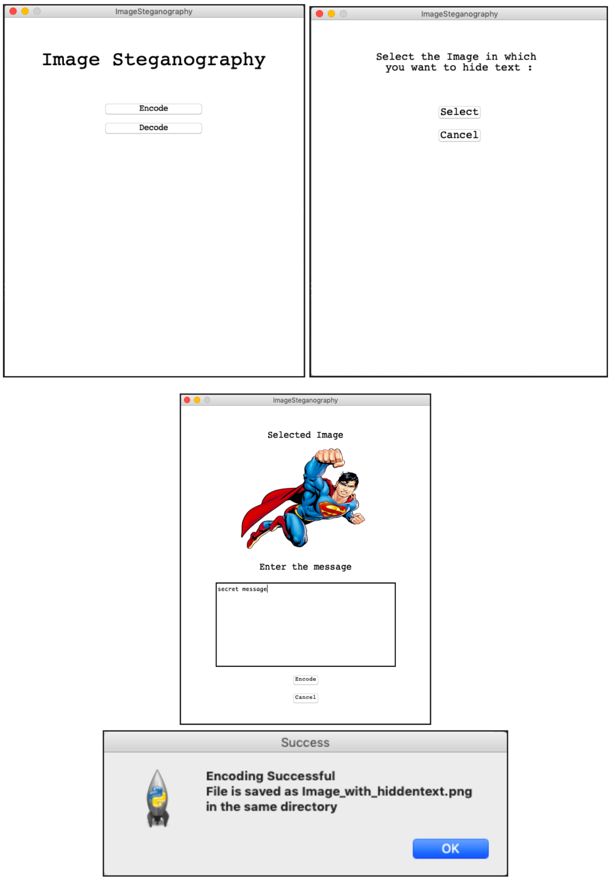


```
from tkinter import *
from tkinter import ttk
import tkinter.filedialog
from PIL import ImageTk
from PIL import Image
from tkinter import messagebox
from io import BytesIO
import  os

class Stegno:


    output_image_size = 0

    def main(self,root):
        root.title('ImageSteganography')
        root.geometry('500x600')
        root.resizable(width =False, height=False)
        f = Frame(root)

        title = Label(f,text='Image Steganography')
        title.config(font=('courier',33))
        title.grid(pady=50)

        b_encode = Button(f,text="Encode",command= lambda :self.frame1_encode(f), padx=54)
        b_encode.config(font=('courier',14))
        b_decode = Button(f, text="Decode",padx=54,command=lambda :self.frame1_decode(f))
        b_decode.config(font=('courier',14))
        b_decode.grid(pady = 12)

       # ascii_art = Label(f,text=self.art)
        # ascii_art.config(font=('MingLiU-ExtB',50))
        #ascii_art.config(font=('courier',60))

        #ascii_art2 = Label(f,text=self.art2)
        # ascii_art.config(font=('MingLiU-ExtB',50))
        #ascii_art2.config(font=('courier',12,'bold'))
```

Fig. 5 Python Interface

Import all the required python libraries.

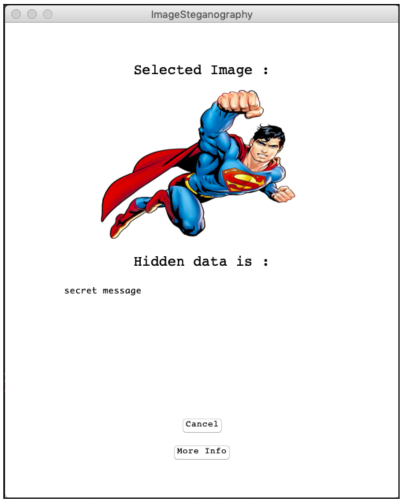
## 6. ENCODING THE MESSAGE



Encoding Successful
File is saved as Image_with_hiddentext.png
in the same directory

Fig. 7 Encoding the Message

## 7. DECODING THE MESSAGE



Hidden data is :

secret message

Fig. 8 Decoding the Message

## 8. CONCLUSIONS

To conclude, This Paper Steganography using python which has been developed using Python. This paper helps users to hide data inside another image file. Which provides Easy implementation. Thus, the paper entitled above should include all the above-mentioned features and it is confirmed that it is up to the specifications entitled for the project.

### *8.1 Key features of this application*

It can create another image file same as the original image file with different file name.

It provides:

Fast encoding of data

Fast decoding of data

Easy and efficient user experience.

## 9. REFERENCES

[1] https://securelist.com/steganography-in-contemporary-cyberattacks/79276/

[2] https://www.tutorialspoint.com/image-based-steganography-using-python

[3] https://www.tutorialspoint.com/python-image-based-steganography

[4] https://www.edureka.co/blog/steganography-tutorial

[5] https://www.techopedia.com/definition/4131/steganography

[6] http://webtorials.com/main/eduweb/security/tutorial/steg/steg.pdf

[7] https://www.cl.cam.ac.uk/teaching/0910/R08/work/essay-at443-steganography.pdf

[8] http://eeweb.poly.edu/~yao/EE4414/memon_F05_v2.pdf

[9] https://www.dreamincode.net/forums/topic/27950-steganography/

[10] https://www.ijcaonline.org/archives/volume133/number9/ 23816-2016908016