DAYANANDA SAGAR UNIVERSITY

A Pattern Recognition Synopsis

ON

“STEGANOGRAPHY”

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE & ENGINEERING

Submitted by

DEVANSH AWASTHI (ENG17CS0065)

VII Semester, 2020

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

SCHOOL OF ENGINEERING

DAYANANDA SAGAR UNIVERSITY
KUDLU GATE BANGLORE-560068

DAYANANDA SAGAR UNIVERSITY
School of Engineering, Kudlu Gate, Bangalore-560068

CERTIFICATE

This is to certify that Mr. Chethan N USN ENG17CS0058, Mr. Ashfaq Ahmed A bearing USN ENG17CS0041 and Mr. Adithya srinivas bearing bearing USN ENG17CS0011 has satisfactorily completed their Pattern Recognition Project Report as prescribed by the University for the Seventh semester B.Tech. Program in Computer Science & Engineering during the year 2020 at the School of Engineering, Dayananda Sagar University, Bangalore.

Date:

Signature of the faculty in charge

Signature of the Chairman

Abstract:

Traffic control and vehicle owner identification has become major problem in every country. Sometimes it becomes difficult to identify vehicle owner who violates traffic rules and drives too fast. Therefore, it is not possible to catch and punish those kinds of people because the traffic person might not be able to retrieve vehicle number from the moving vehicle because of the speed of the vehicle. Therefore, there is a need to develop Automatic Number Plate Recognition system as a one of the solutions to this problem. There are numerous Automatic Number Plate Recognition systems available today. These systems are based on different methodologies but still it is really challenging task as some of the factors like high speed of vehicle, non-uniform vehicle number plate, language of vehicle number and different lighting conditions can affect a lot in the overall recognition rate. Most of the systems work under these limitations.

Aknowledgement

The satisfaction that accompanies the successful completion of task would be incomplete without the mention of the people who made it possible and whose constant guidance and encouragement crown all the efforts with success.

We are especially thankful to our **Chairman, Dr. Sanjay Chitnis**, for providing necessary depatmental facilities, moral support and encouragement.

We are very much thankful to our **Guide, Prof. Lavanya B Koppal** for providing help and suggestions in completion of this pattern recognition project completely.

We have received a great deal of guidance and co-operation from our friends and we wish to thank all that have directy or indirectly helped us in the successful completion of this project work.

Table Of Contents

1. Introduction

Image files are also used to hide data for communication. An image file is an array of numbers that constitutes light intensities. In this approach, the data can be hidden in a color image or a gray scale image. Gray-scale images were given more importance because of theirvariation in shades. This will increase the scope for hiding information. In the process of embedding the image file, the confidential data that should be hidden in the image file is first embedded using a cryptographic algorithm. Then the embedded data is embedded into the image file, which in turn results in a stego-image. Then a stego-key is used during the hiding process to send the image securely to the receiver.

After the image is received at the other end, the receiver will extract the data from the image. In order to extract the message, the receiver requires a shared secret key. The extraction process detailed is a cryptographic algorithm or a stego-key approach. To improve this process, message compression can be applied, so that data security is maintained at a higher degree When hiding information inside images the LSB (Least Significant Byte) method is usually used. When hiding information inside Audio files the technique usually used is low bit encoding which is somewhat similar to LSB that is generally used in Images. The problem with low bit encoding is that it is usually noticeable to the human ear, so it is a rather risky method for someone to use if they are trying to mask information inside of an audio file.

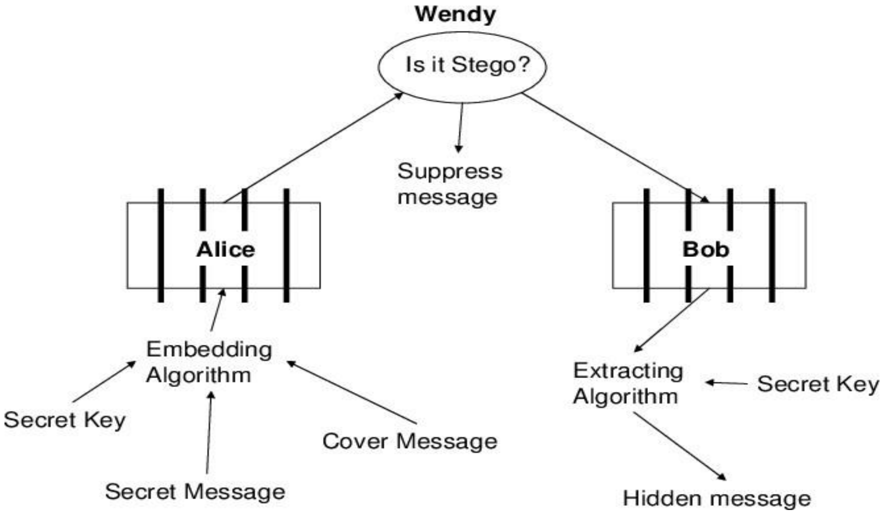
1.1Project Scope:

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. Problem Statement

To design and implementation of Steganography using python

3.Block Diagram



4. **Implementation**

4.1 Algorithm

Step 1: Actual image and the data to be hidden were read. Step 2: n
bits shift operation was performed.

Step 3: Shift operation was performed for the cover image with 11110000 so that MSB's were set to 0.

Step 4: After the shift operation both are bitored.

5. REQUIREMENTS

5.1 HARDWARE AND SOFTWARE REQUIREMENTS

Hardware

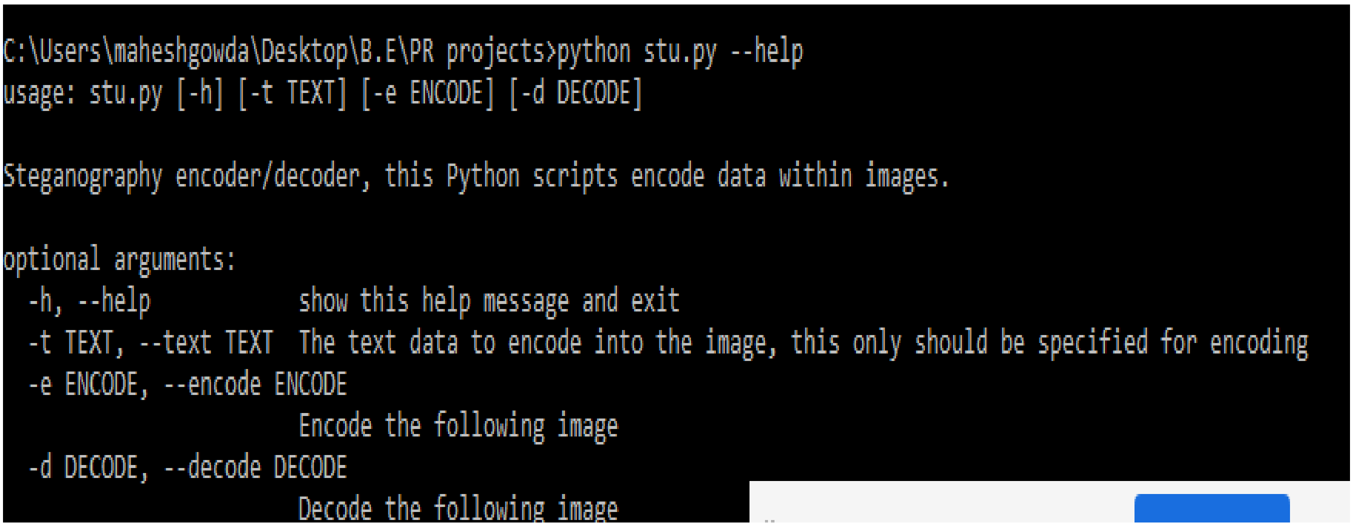
- RAM : 128MB (Minimum)
- Processor : Pentium 2 and above
- Processor speed: Above 500MHz

Software

- Language : python
- Platform : IntelliJ IDE
- Tool : IDLE (python 3.8 64-bit)

6. OUTPUT SCREENSHOT:

Syntax for Encoding and decoding :

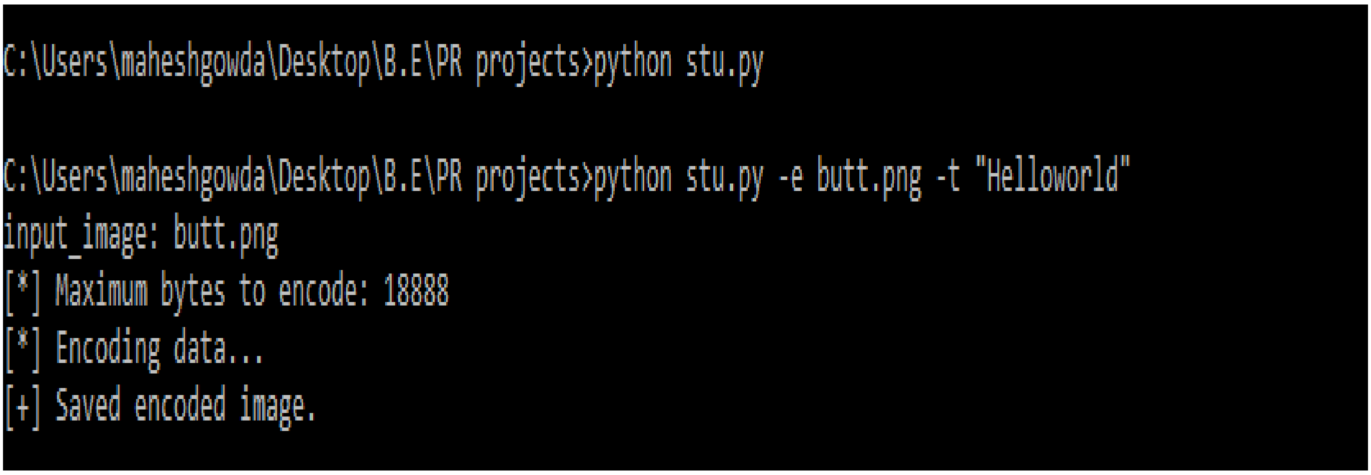


```
C:\Users\maheshgowda\Desktop\B.E\PR projects>python stu.py --help
usage: stu.py [-h] [-t TEXT] [-e ENCODE] [-d DECODE]

Steganography encoder/decoder, this Python scripts encode data within images.

optional arguments:
  -h, --help            show this help message and exit
  -t TEXT, --text TEXT  The text data to encode into the image, this only should be specified for encoding
  -e ENCODE, --encode ENCODE
                        Encode the following image
  -d DECODE, --decode DECODE
                        Decode the following image
```

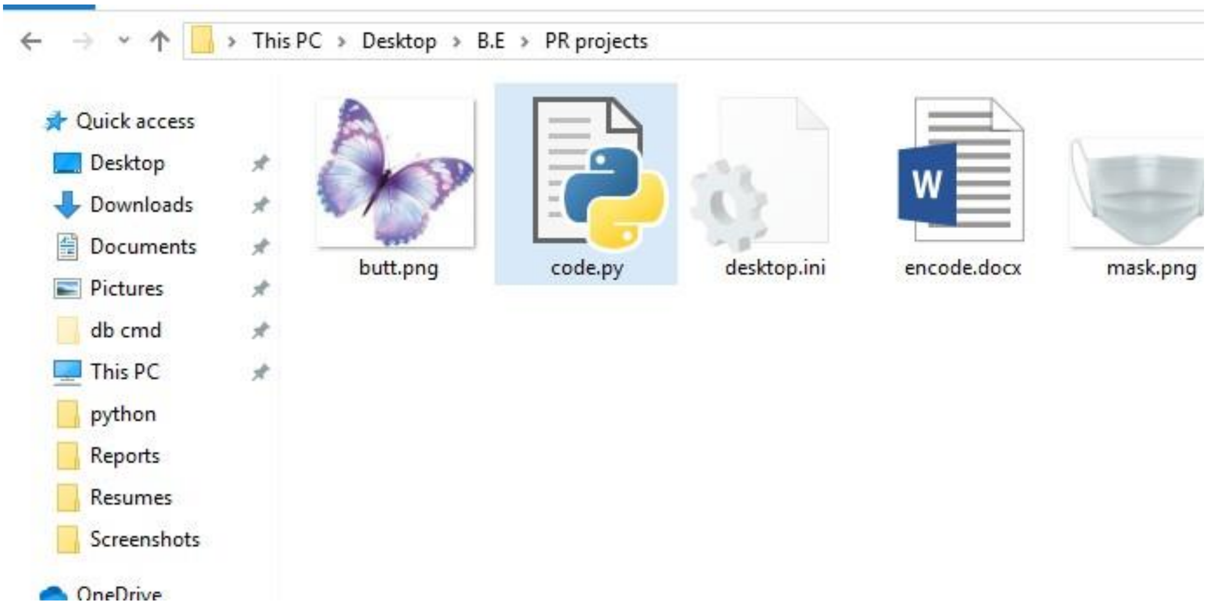
Encoding Part:



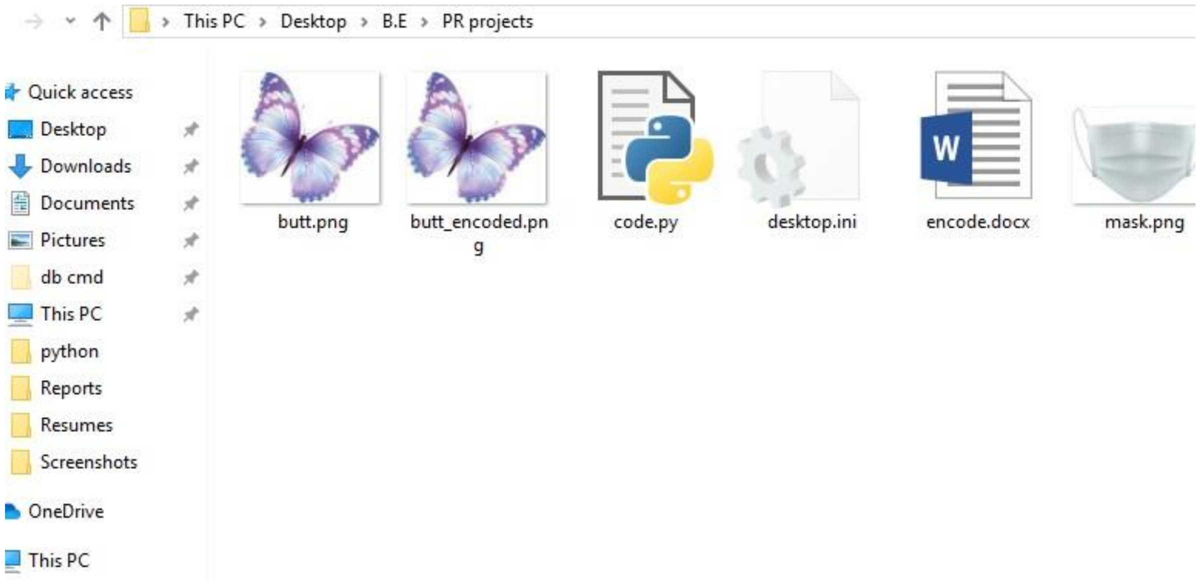
```
C:\Users\maheshgowda\Desktop\B.E\PR projects>python stu.py

C:\Users\maheshgowda\Desktop\B.E\PR projects>python stu.py -e butt.png -t "Helloworld"
input_image: butt.png
[*] Maximum bytes to encode: 18888
[*] Encoding data...
[+] Saved encoded image.
```

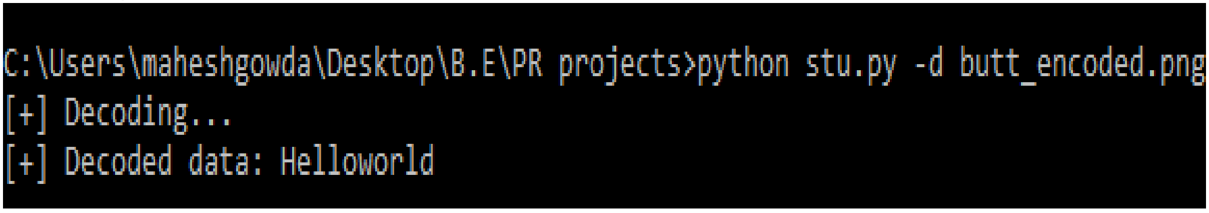
You can see the image filename as butt.png were the data has been stored inside the image.above image you can see the how to encode the image



After encoding the image ,you can see the encoded image has ”butt_encoded.png” in the below image .



Decoding the data:



```
C:\Users\maheshgowda\Desktop\B.E\PR projects>python stu.py -d butt_encoded.png
[+] Decoding...
[+] Decoded data: Helloworld
```

You can see te decoded data .

Conclusion:

Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day.

Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice. We printed out the enhancement of the image steganography system using LSB approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover image.

This steganography application software provided for the purpose to how to use any type of image formats to hiding any type of files inside their. The master work of this application is in supporting any type of pictures without need to convert to bitmap, and lower limitation on file size to hide, because of using maximum memory space in pictures to hide the file.

Since ancient times, man has found a desire in the ability to communicate covertly. The recent explosion of research in watermarking to protect intellectual property is evidence that steganography is not just limited to military or espionage applications. Steganography, like cryptography, will play an increasing role in the future of secure communication in the “digital world”.

References:

Following websites are referring to create this project reports.

- http://www.google.com
- http://www.microsoft.com
- http://www.programmer2programmer.net
- http://www.codeproject.com
- http://www.asp.net
- http://www.asp123.com
- http://www.wikipedia.org