Name: C SAIKIRAN
SkillsBuild Email ID: chakalisaikiran10@gmail.com
College Name: Andhra University College of Engineering (A)
College State: Andhra Pradesh
Internship Domain: [Cyber Security]
Internship Start and End Date: [3rd June 2024 to 12th July 2024] - 6 weeks

IMAGE STEGANOGRAPHY

INTRODUCTION TO
IMAGE STEGANOGRAPHY

Image steganography is the practice of hiding secret information within digital images. This technique exploits the redundancy in image data, such as the least significant bits (LSBs) of pixel values, to embed hidden messages without noticeably altering the image's appearance.

AGENDA

The agenda of this project to send a secret text to higher officials using the steganography concept and RGB technique, ensuring that criminals or others cannot identify the image or its hidden content. Thos project will involve encoding the secret text into the least significant bits of the image’s pixels, making the alterations imperceptible to the human eye.

What is Image Steganography

- **Hiding Data**

Image steganography involves embedding secret data, such as text, images, or even files, within the pixels of a digital image.

- **Invisible to the Eye**

The hidden data is concealed in a way that it is undetectable to the casual observer, making the image appear normal and unaltered.

- **Secured Communication**

This technique allows for secure communication, as the existence of the hidden data is hidden from anyone who is not aware of its presence.

Least Significant Bit (LSB) Insertion : One of the most straightforward and widely used techniques in image steganography. This method involves modifying the least significant bits of the pixels in a digital image to encode hidden information.

Here’s a detailed look at how LSB steganography works:

1. **Image Pixels:**
   - Digital images are composed of pixels, each represented by bits.
   - In a grayscale image, each pixel can be represented by 8 bits.
   - In a color image (like RGB), each pixel is represented by 24 bits (8 bits for red, 8 bits for green, and 8 bits for blue).

2. **Least Significant Bit:**
   - The least significant bit is the lowest bit in a byte. For example, in the byte 10110101, the least significant bit is the rightmost one (1).

3. **Embedding Process:**
   - To hide information, the least significant bit of each pixel’s color value is altered to match the bits of the secret message.
   - Example: If a pixel's red value is 11001010, and the secret message bit is 1, the red value is changed to 11001011.

4. Extracting Process:

- The hidden information can be extracted by reading the least significant bits of the pixels in the same order they were modified.

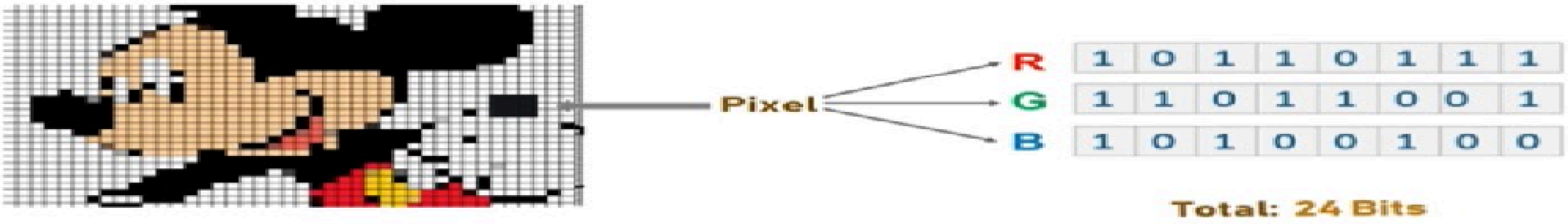


Photo credits to Edureka Steganography tutorial

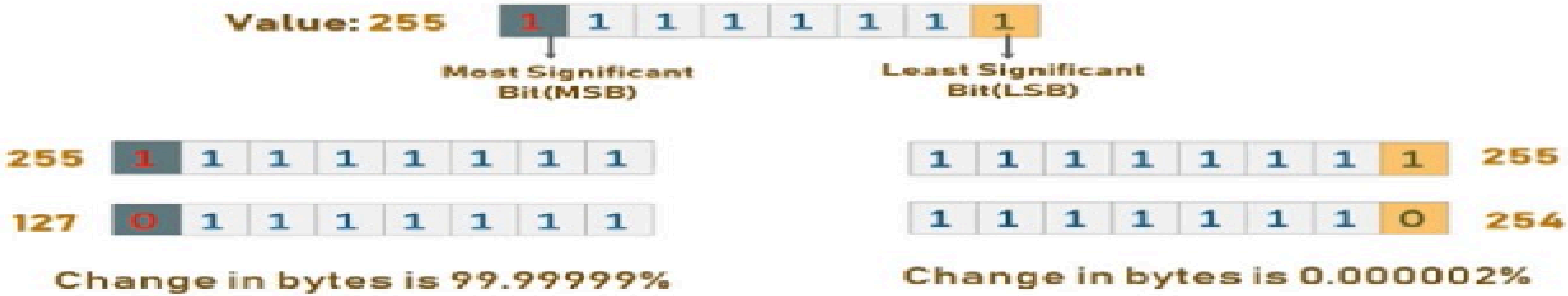

Value: 255
1 1 1 1 1 1 1 1
Most Significant Bit(MSB)
Least Significant Bit(LSB)
255 1 1 1 1 1 1 1 1
127 0 1 1 1 1 1 1 1
Change in bytes is 99.99999%
1 1 1 1 1 1 1 1 255
1 1 1 1 1 1 1 0 254
Change in bytes is 0.000002%

Photo by Edureka Steganography tutorial

WHO ARE THE END USERS OF THE PROJECT?

- The primary end users for this steganography project include government and military personnel secure communication, corporate executives protecting proprietary data, and journalists sharing sensitive information discreetly.
- IT and cyber security teams can integrate this technique to enhance organizational data security.
- Additionally, the person who wants to send any secret message other person in a hidden format then this project will helpful for them.

YOUR SOLUTION AND ITS VALUE PROPOSITION

- Steganography is the basic concept to hide the data inside other data.
- In this project RGB Mechanism is used for pixel manipulation.
- XOR operation is used for encryption and decryption of the test inside the image.
- The project reads an image and hides the secret text within the pixel values using the least significant bits (LSB) method.
- For security purpose that means to avoid unauthorized users taking the advantage of the message, a secret key used to hide and unhide the data.
- Finally, By using this project we can hide the data inside an image using secret key and for unhide the message secret is used.

```
heck_catch
k_catch(self):
Check if catch balls.
ball in self.overlappi
self.score.value += 10
self.score.right = games
ball.handle_caught()
""" Change game level. "
if self.score.value == 2
    self.level.value +
    self.level.left =
    """ Next level
    level_message
```

Implementing Image Steganography with Python

1

Image Manipulation

Using Python's image processing libraries, such as Pillow, you can read, manipulate, and save image files.

2

Data Embedding

Algorithms are used to encode the secret data into the image's pixels, ensuring it remains invisible.

3

Decoding and Extraction

Complementary algorithms are employed to extract the hidden data from the image, reverting the steganographic process.

Demonstrating the Project with Sample Images

Input Image

An image used to hide the secret data.

Hidden Data

The information that will be embedded within the image.

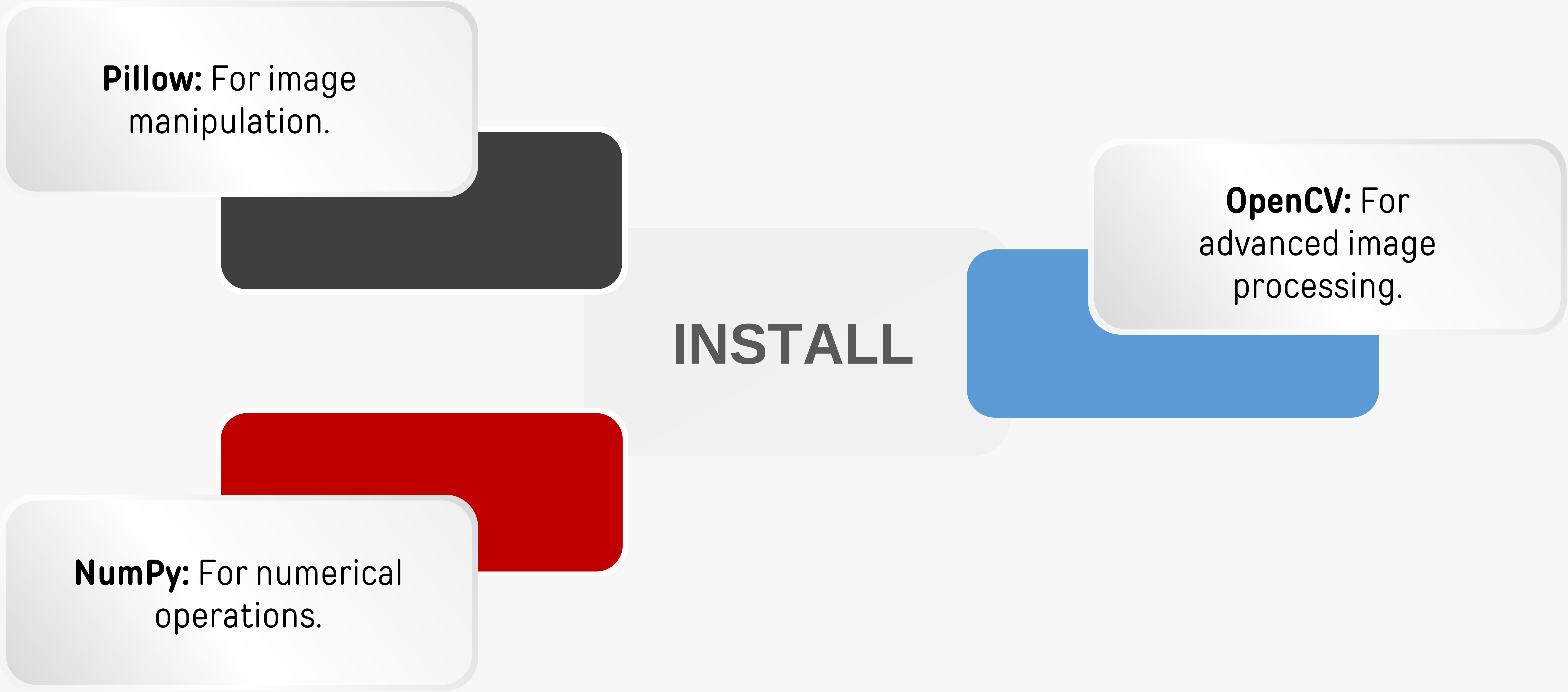
Output Image

The image with the hidden data, indistinguishable from the original.

Data Extraction

The process of retrieving the hidden data from the output image.

LIBRARIES



INSTALL

Pillow: For image manipulation.

OpenCV: For advanced image processing.

NumPy: For numerical operations.

MODELLING

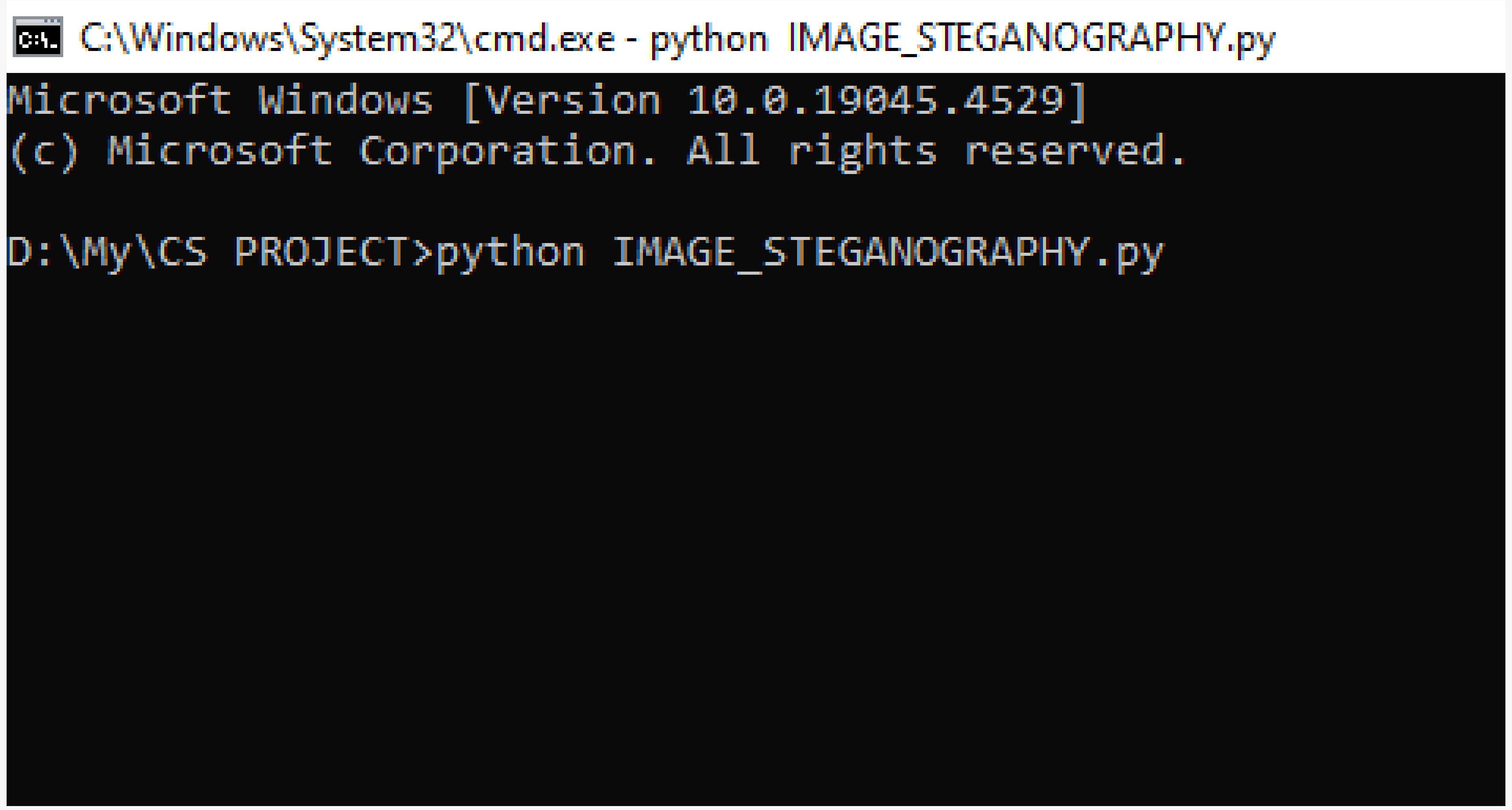
ENCODING PROCESS:

- Load the image.
- Convert the message into binary format.
- Modify the image's pixel values to encode the message.

DECODING PROCESS:

- Load the encoded image.
- Extract the binary data from pixel values.
- Convert binary data back to the original message.

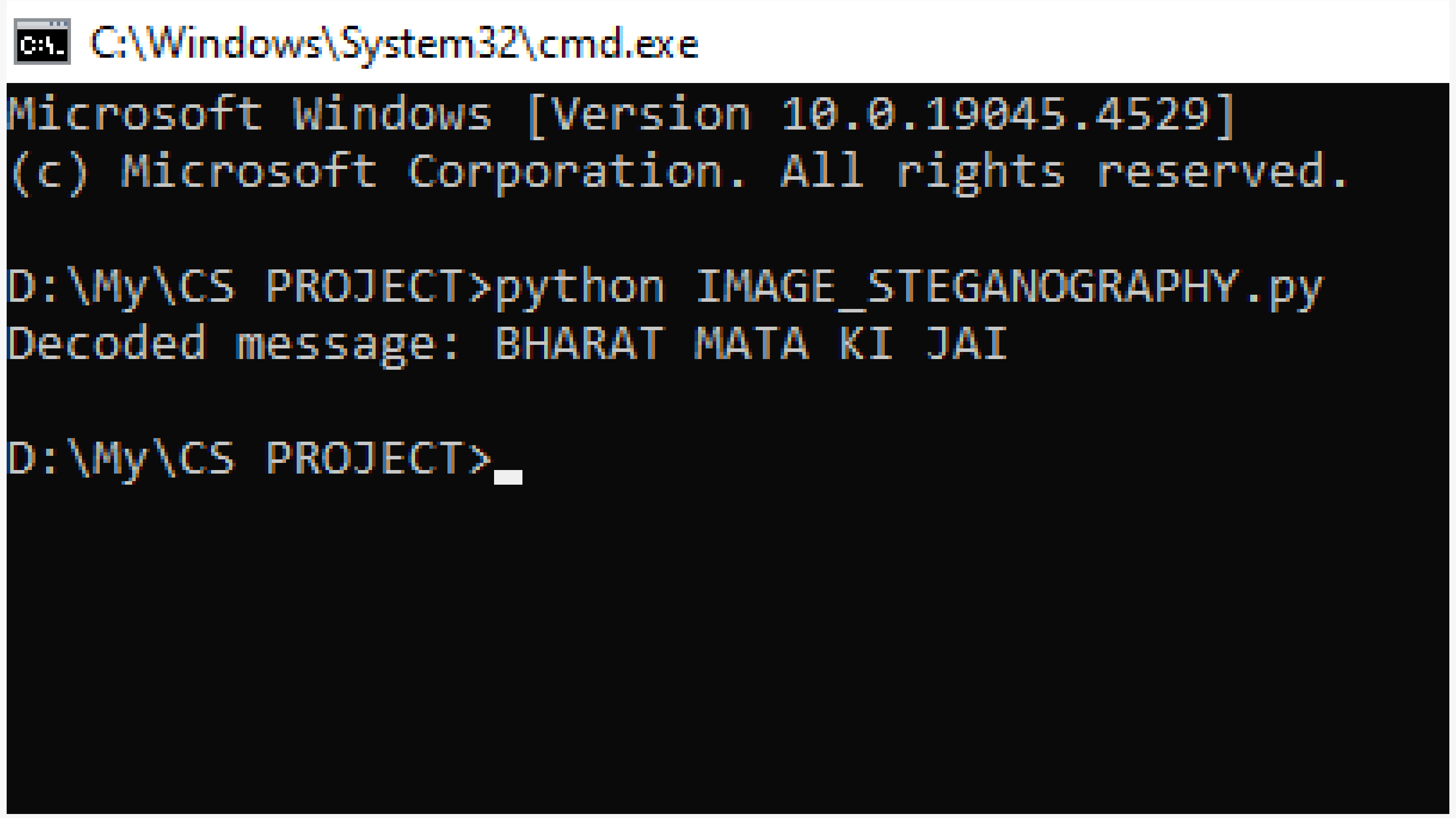
RESULT



C:\Windows\System32\cmd.exe - python IMAGE_STEGANOGRAPHY.py

```
Microsoft Windows [Version 10.0.19045.4529]
(c) Microsoft Corporation. All rights reserved.

D:\My\CS PROJECT>python IMAGE_STEGANOGRAPHY.py
```



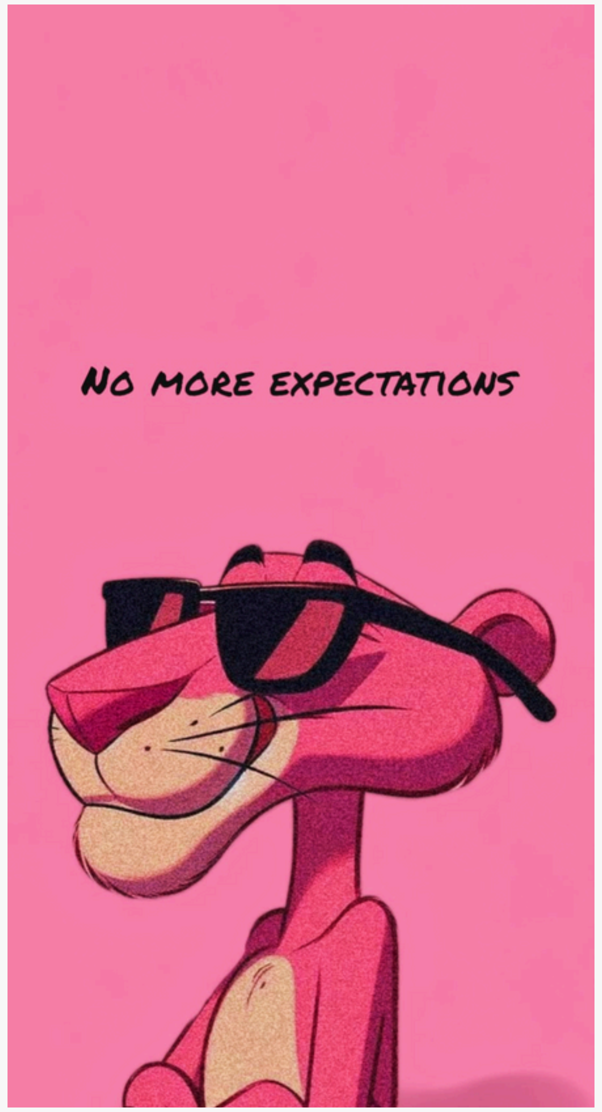
C:\Windows\System32\cmd.exe

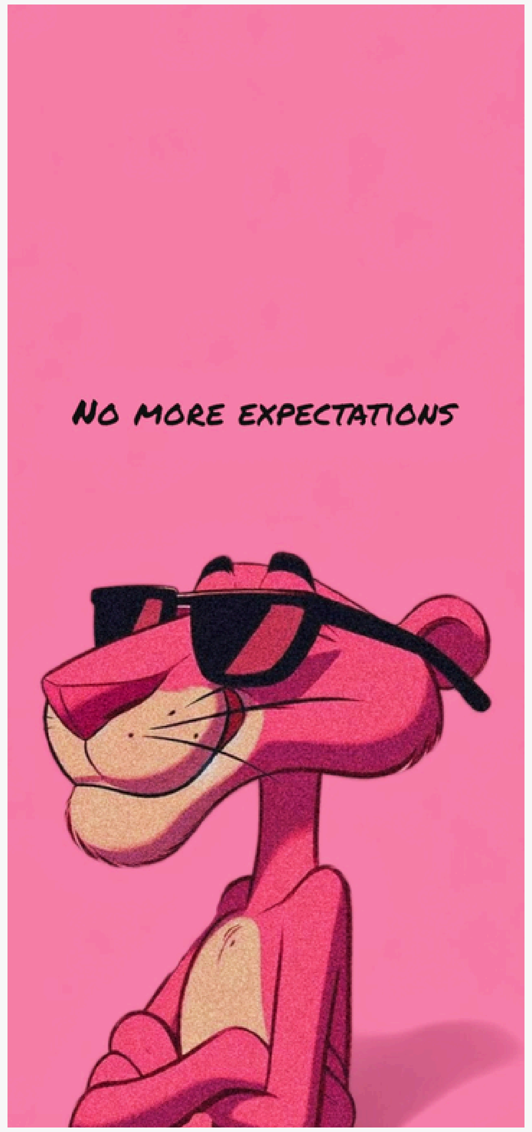
```
Microsoft Windows [Version 10.0.19045.4529]
(c) Microsoft Corporation. All rights reserved.

D:\My\CS PROJECT>python IMAGE_STEGANOGRAPHY.py
Decoded message: BHARAT MATA KI JAI

D:\My\CS PROJECT>_
```

- ORIGINAL IMAGE





- ENCODED IMAGE

- **DECODED MESSAGE** : **BHARAT MATA KI JAI** https://github.com/saikirancoder-159/Hiding-a-text-inside-an-image

THANK YOU