VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology and Engineering

FALL Semester 2020-21

“IMAGE STEGANOGRAPHY”

PROJECT REPORT

Submitted in fulfilment for the JComponent of
Information And Security System (SWE3002)

M.Tech. – Software Engineering

by

17MIS1153-P.JYOSHNA

Under the guidance of

Dr. JAYASUDHA.M

TABLE OF CONTENTS

CHAPTER-1

ABSTRACT :-

Steganography is the process of hiding a text or a message within an image in such a way that someone cannot know the presence or contents of the hidden data. It means that it encrypts the text in the form of image. The steganography is done when the communication takes place between sender and receiver. The purpose of Steganography is to maintain secret communication between two different teams or parties. Now a day's in data transfer over the network, the security is the main issue concerned with this. There are many processes to hide the data in an image. In this paper we have implemented Least significant bit LSB to encrypt the message so that the message can be more secured. This paper will show how Steganography is used in a modern context while providing a practical understanding of what Steganography is and how to accomplish it. We have used LSB (Least Significant Bit).

CHAPTER-2

PROBLEM STATEMENT:-

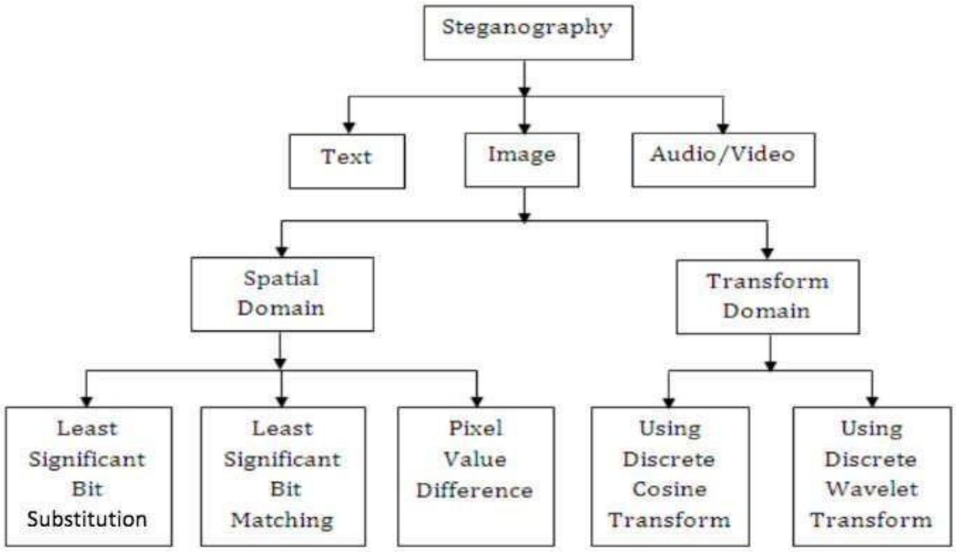
Data hiding is of importance in many applications. For hobbyists, secretive data transmission, for privacy of users etc. the basic methods are: Steganography and Cryptography. Steganography is a simple security method. Generally, there are three different methods used for hiding information: steganography, cryptography, watermarking.

In cryptography, the information to be hidden is encoded using certain techniques; this information is generally understood to be coded as the data appears nonsensical. Steganography is hiding information; this generally cannot be identified because the coded information doesn't appear to be abnormal i.e. its presence is undetectable by sight. Detection of steganography is called Steganalysis.

Steganography is of different types:

1. Text steganography
2. Image steganography
3. Audio steganography
4. Video steganography

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,


Steganography
Text
Image
Audio/Video
Spatial Domain
Transform Domain
Least Significant Bit Substitution
Least Significant Bit Matching
Pixel Value Difference
Using Discrete Cosine Transform
Using Discrete Wavelet Transform

therefore the person will not attempt to decrypt the information.

In all of these methods, the basic principle of steganography is that a secret message is to be embedded in another cover object which may not be of any significance in such a way that the encrypted data would finally display only the cover data. So it cannot be detected easily to be containing hidden information unless proper decryption is used.

As the above explanation goes, every steganography consists of three components:

1. Cover image
2. Message object
3. Resulting Steganographic image

In this project LSB substitution method is implemented and Fibonacci Encryption is used to encrypt the text message.

There are two different methods for image steganography:

1. Spatial methods
2. Transform methods

In spatial method, the most common method used is LSB substitution method.

Least significant bit (LSB):-

LSB method is a common, simple approach to embedding information in a cover file.

In steganography, LSB substitution method is used. i.e, since every image has three components (RGB). This pixel information is stored in encoded format in one byte. The first bits containing this information for every pixel can be modified to store the hidden text. For this, the preliminary condition is that the text to be stored has to be smaller or of equal size to the image used to hide the text.

LSB based method is a spatial domain method. But this is vulnerable to cropping and noise. In this method, the MSB (most significant bits) of the message image to be hidden are stored in the LSB (least significant bits) of the image used as the cover image. It is known that the pixels in an image are stored in the form of bits. In a grayscale image, the intensity of each pixel is stored in 8 bits (1byte). Similarly, for a color (RGB-red, green, blue) image, each pixel requires 24 bits (8bits for each layer).

The Human visual system (HVS) cannot detect changes in the color or intensity of a pixel when the LSB bit is modified. This is psycho-visual redundancy since this can be used as an advantage to store information in these bits and yet notice no major difference in the image.

CHAPTER-3

PLATFORM :-

Software Requirements

- Windows 10
- JAVA JDK 8
- NETBEANS

Language Used

- JAVA

TOOL

- NETBEANS

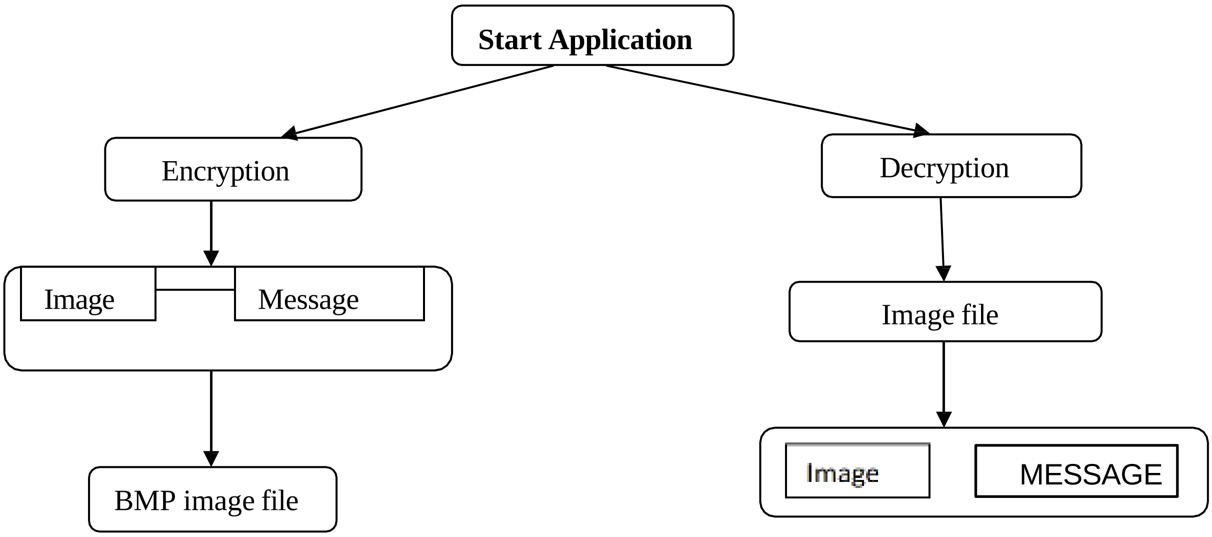
CHAPTER-4

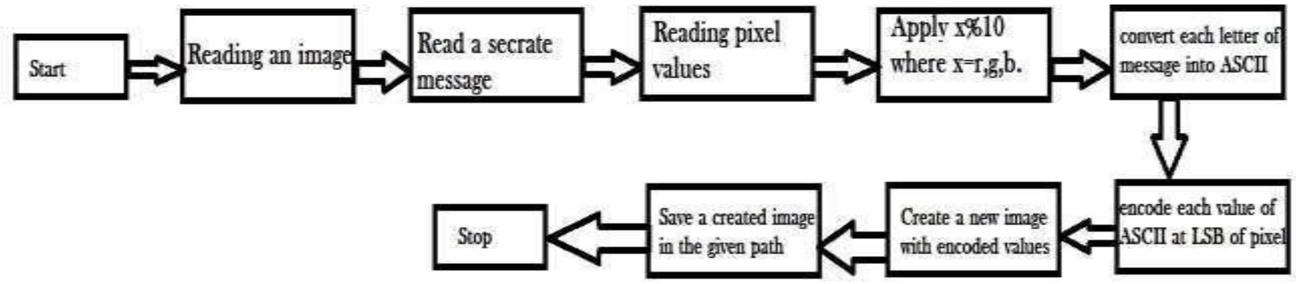
PROCESS IMPLEMENTATION

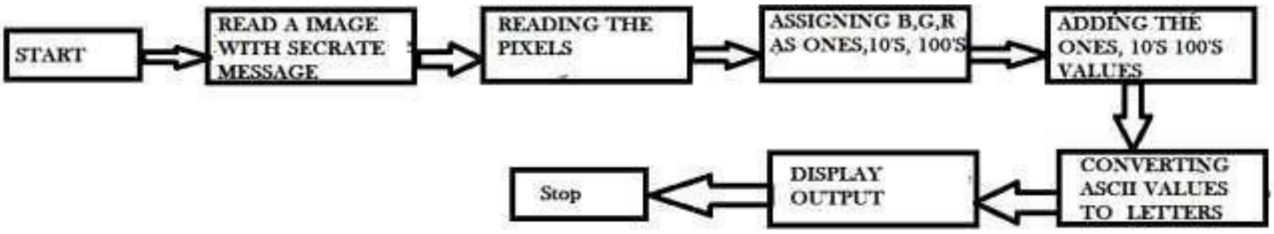
DIAGRAM:-

There are three important steps in steganography:

1. Select an image
2. Encrypt the data into an image
3. Decrypt the data from the image




Start
Reading an image
Read a secrate message
Reading pixel values
Apply x%10 where x=r,g,b.
convert each letter of message into ASCII
encode each value of ASCII at LSB of pixel
Create a new image with encoded values
Save a created image in the given path
Stop


START
READ A IMAGE WITH SECRATE MESSAGE
READING THE PIXELS
ASSIGNING B,G,R AS ONES,10'S, 100'S
ADDING THE ONES, 10'S 100'S VALUES
CONVERTING ASCII VALUES TO LETTERS
DISPLAY OUTPUT
Stop

CHAPTER-5

LITERATURE SURVEY:-

PAPER-1:-

Fibbonacci based text hiding using image cryptography

In digital word security is a most important issue and data hiding with image cryptography is one of the possible ways to ensure the security of the important message from outer world. In this paper we proposed a novel technique that encrypted the message such a ways that the message encoded as well as hidden in an image. The proposed solution is to use image cryptography to hide textual message. The proposed technique use of an encryption technique that is based on Fibonacci series & image encryption and a secret key generated from the image

PAPER-2:-

A Steganography Scheme on JPEG Compressed Cover Image with High Embedding Capacity

Joint Photographic Experts Group (JPEG) is one of the widely used lossy image compression standard and in general JPEG based compressed version images are commonly used during transmission over the public channel like the Internet. In this paper, the authors have proposed a steganography scheme where the secret message is considered for embedding into the JPEG version of a cover image. The steganography scheme initially employs block based Discrete Cosine Transformation (DCT) followed by some suitable quantization process on the cover image to produce the transformed coefficients. The obtained coefficients are considered for embedding the secret message bits. In general, most of the earlier works hide one bit message into each selected coefficient, where hiding is carried out either directly modifying the coefficients, like employing the LSB method or indirectly modifying the magnitude of the coefficients, like flipping the sign bit of the coefficients. In the proposed scheme, instead of embedding the secret message bits directly into the coefficients, a suitable indirect approach is adopted to hide two bits of the secret message into some selected DCT coefficients. As per the conventional approach, the modified coefficients are further compressed by entropy encoding. The scheme has been tested on several standard gray scale images and the obtained experimental results show the comparative performance with some existing related works

PAPER-3:-

Low-Tech Steganography for Covert Operations

Text steganography, the art of concealing a secret text inside another innocuous text called the cover, is usually performed by insertion of whitespace, punctuation marks, misspelling words, or by arbitrarily capitalizing words or inserting synonyms, changing font-sizes & colors, etc. All of these have the disadvantage that they either arouse suspicion or are easily noticeable; and even lost if manually copied, i.e. handwritten. Furthermore, they are easily detectable by automated checkers. Still there are other methods which require a stego-key in order to decrypt the message. In covert intelligence operations, transmission of the
stego-key may not be possible at all, more so when the message is urgent. Digital communications and Internet connectivity may also be lacking in certain situations, and the only mode of message passing available may be the exchange of handwritten text on paper; which effectively rules out text modifications like font-changes, whitespace insertion, etc. or any form of digital steganography like image/audio steganography. Finally, in almost all text- steganographic techniques, there is no provision to for the receiver to detect whether or not there is indeed any message embedded. This is very important in intelligence operations where a number of decoy text need to be sent with only one concealing the actual message. In this paper, we propose a new tool called STEGASSIST that can help the sender in generating the stego-text manually. It is a low-tech form of steganography that is especially suited to covert operations like espionage or undercover journalism. In this method, the generated cover and the stego-text are identical, or in other words, there is no cover-text.
Moreover, decryption does not require a stego-key, and the stego-text may be printed or even handwritten and sent via unreliable messengers, or published, without arousing any suspicion. Finally, the received stego-text can be checked by the receiver to detect whether or not there is any actual message embedded in it.

PAPER-4:-

A Comparative Study of Recent Steganography Techniques for Multiple Image Formats

Steganography is the technique for exchanging concealed secret information in a way to avoid suspicion. The aim of Steganography is to transfer secrete message to another party by hiding the data in a cover object, so that the imposter who monitors the traffic should not distinguish between genuine secret message and the cover object. This paper presents the comparative study and performance analysis of different image Steganography methods using various types of cover media ((like BMP/JPEG/PNG etc.) with the discussion of their file formats. We also discuss the embedding domains along with a discussion on salient technical properties, applications, limitations, and Steganalysis.

PAPER-5:-

A new encrypted method in image steganography

Steganography is data hiding technique in internet. Here we send CAPTCHA codes within a cover image using image steganography. CAPTCHA are the crazy codes. They are used in human response test. The word is actually acronym for: “Completely Automated Public Turning test to tell Computers and Humans Apart”. It is a type of challenge-response test used in computing to determine whether or not the user is human. Websites implement CAPTCHA codes into their registration process due to spam. This is the utility of CAPTCHA codes. Here we generate CAPTCHA codes are and later send them in an encrypted version. Actually CAPTCHA codes are embedded ASCII into cover image with an encrypted form resulting stego image and thus attackers can not fetch the actual CAPTCHA resulting in a secured transmission of confidential data via internet using image steganography

PAPER-6:-

IMAGE STEGANOGRAPHY BASED IMPROVING M-SECURITY

Endless supply of m-trade joined on new parts of online business, m-managing an account has raised most divisions of M-trade. Since the M-saving money gotten fine, it’s endless supply of grouped administrations bolstered totally unique frameworks with the assistance of arranged administrations like short electronic informing service (SMS).Be that it may, regardless of its endowments, embanking is confronting a few difficulties too. One in everything about difficulties is that the issue of security of this technique. This paper presents a procedure path system for expanding security of the information asked for clients with the usage of steganography strategy. Amid this method, instead of direct causation of the information, it is covered up in an exceedingly picture by the word and is set on a site. At that point the location of the picture is dispatched to the client. Once accepting the location of the picture through SMS, the client downloads the picture by a unique program. Once getting into the word, the client will observe the information extricated from the picture if the word is entered appropriately. This task is written in JavaEE dialect and has been upheld on new nokia cell phones

PAPER-7:-

Secure RGB Image Steganography based on Fused Distortion Measurement

Binary image Steganographic methods aim to generate stego images with good visual quality, while others focus more on the statistical security of the anti-steganalysis. This paper proposes a binary steganographic scheme that improves both of them by selecting more appropriate flipped pixels. First, a fused distortion measurement is developed that combines the advantages of flipping distortion measurement (FDM) and two data-carrying pixel location methods, including the edge adaptive grid method (EAG) and the
“Connectivity Preserving” criterion (CPc). The FDM measures the distortion score by statistical features and achieves high statistical security, while the EAG and CPc select pixels by analysing local texture structures based on visual quality. Then, to eliminate the interference brought by adjacent flipped pixels, a flipping position optimization strategy is proposed to find better positions for flipping pixels to further improve the steganographic performance.

PAPER-8:-

Digital image steganography using PVD and modulo operation

This paper proposes an image steganographic approach using the principle of pixel value differencing (PVD) and modulo operation (MO). The major contributions of the proposed approach are: (i) increase in peak signal-to-noise ratio (PSNR), (ii) increase in hiding capacity, and (iii) avoidance of fall off boundary problem (FOBP). At first, the image is partitioned into non-overlapping blocks consisting of three consecutive pixels. Then, the secret data is embedded in a block using two phases, (i) pixel difference modulo operation (PDMO) phase, and (ii) average PVD (APVD) readjustment phase. In the first phase, the difference between two consecutive pixels of a block is found and using an adaptive range table and modulo operation the secret data are embedded. In the second phase, the average of the first two stego-pixels of the block and the third pixel is considered for data embedding using PVD approach. The result of the proposed approach has been compared with existing approaches and found to be improved.

PAPER-9:-

Combining of Cryptography and Steganography for Improving of Security

To hide hidden data in digital images, a variety of techniques are available, some of which are more complex than others. Public key cryptography is very useful for applications, and the technique used depends on the requirements for encryption and encryption data.

Hiding is a kind of hiding method in which the host image is exactly retrievable. Presence lossless makes this technique suitable for medical and military applications. The image pixels are replaced with additional data into new values to embed several data pixels by S-block at multiple layers. From the original image, the embedded data can be extracted and the original image can be recovered from the decrypted image directly. Embedded data can be extracted directly from the encrypted domain. The decryption of the original plaintext

image doesn't affect the data embedding operation. With the combined technique, before decryption, a receiver may extract a part of embedded data, and recover the original plaintext image after decryption. A slight distortion is introduced due to the compatibility between the lossless and reversible schemes. The data embedding operations can be performed in the two manners simultaneously performed in an encrypted image and decrypted image. In this thesis, the design of Caesar cipher and Vigenere cipher is presented. Block 4 provides good encryption properties and software productivity. The proposed technique for the design of the S-box chain chaos provides a very secure level. The result of the implementation shows that the proposed method is suitable for lightweight cryptography due to the use of low resources using the C # .Net implementation tool.

PAPER-10:-

Digital image encryption algorithm based on pixels

A new image encryption algorithm based on pixels is proposed in this paper. All the strategies, programs, parameters, encryption and decryption steps and other key technologies are given in detail. First, scrambling the image pixels, then through the method of watermark increasing the difficulty of its decoded. At last, choose a camouflaged image to vision or the pixels of the true image, getting the final encryption image. The key parameters are encrypted by Elliptic Curve Cryptography (ECC). We verify and analyze the algorithm security, reliability and efficiency with an experiment. The experiment results and algorithm analyses indicate that the new provides a new access to satisfy high level security of interactive information requirements in the fields of aerospace, military, confidential, financial and economic, national security and so on.

CHAPTER-6

METHODOLOGY USED ALGORTIHM DESCRIPTION:-

METHODOLOGY:-

Here will show how Steganography is used in a modern context while providing a practical understanding of what Steganography is and how to accomplish it. We have used LSB (Least Significant Bit).

ALGORITHM DESCRIPTION:-

Encryption:-

1. START
2. Read a text message from user.
3. Read the input image that which the secrete message should be embedded
4. Enter the new file name after the image is encoded with the secrete message.
5. Convert Message to ASCII code
6. Add the ASCII values at the Units place of the r,g,b values.
7. Do this for every letter in the message
8. STOP

Decryption:-

1. START
2. Read the name of the file to be decoded
3. Read the pixel’s value from the image
4. Taking values from RGB.
5. Adding the values.
6. Convert the added value into ASCII values.
7. Do this for all the pixels.
8. Display output
9. STOP

CHAPTER-7

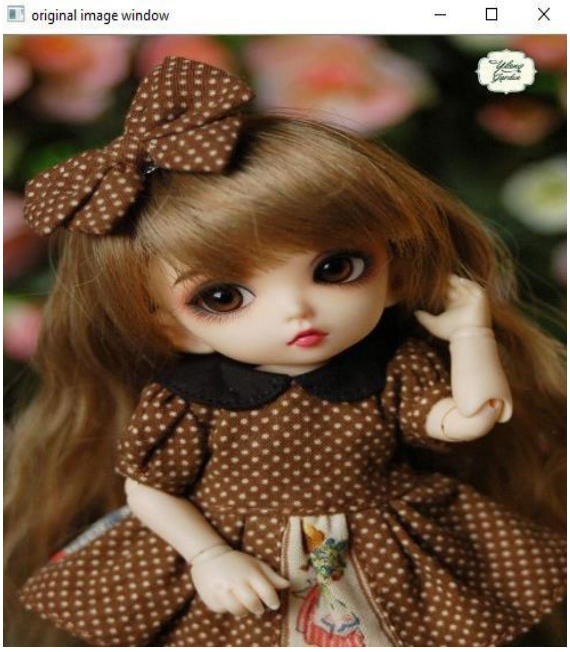
IMPLEMENTATION CODE:-

```
import cv2

import numpy as np

import types

import PIL


def messageToBinary(message):

  if type(message) == str:

    return ''.join([ format(ord(i), "08b") for i in message ])

  elif type(message) == bytes or type(message) == np.ndarray:

    return [ format(i, "08b") for i in message ]

  elif type(message) == int or type(message) == np.uint8:
    return format(message, "08b")
  else:
    raise TypeError("Input type not supported")



def hideData(image, secret_message):
  n_bytes = image.shape[0] * image.shape[1] * 3 // 8
  print("Maximum bytes to encode:", n_bytes)
  if len(secret_message) > n_bytes:
    raise ValueError("Error encountered insufficient bytes, need bigger image or less data !!")
  secret_message += "#####"
  data_index = 0
  binary_secret_msg = messageToBinary(secret_message)
  data_len = len(binary_secret_msg)
  for values in image:
    for pixel in values:
      r, g, b = messageToBinary(pixel)
      if data_index < data_len:
        pixel[0] = int(r[:-1] + binary_secret_msg[data_index], 2)
        data_index += 1
        if data_index < data_len

        pixel[1] = int(g[:-1] + binary_secret_msg[data_index], 2)

        data_index += 1

        if data_index < data_len:

          pixel[2] = int(b[:-1] + binary_secret_msg[data_index], 2)

          data_index += 1

          if data_index >= data_len:

            break

          return image


def showData(image):

  binary_data = ""

  for values in image:

    for pixel in values:

          r, g, b = messageToBinary(pixel)

          binary_data += r[-1]

          binary_data += g[-1]

          binary_data += b[-1]

          all_bytes = [ binary_data[i: i+8] for i in range(0, len(binary_data), 8) ]

          decoded_data = ""

          for byte in all_bytes:
            decoded_data += chr(int(byte, 2))
            if decoded_data[-5:] == "#####":
          break
        return  decoded_data[:-5]


def encode_text():
  image_name = input("Enter image name(with extension): ")
  image = cv2.imread(image_name)
  print("The shape of the image is: ",image.shape)
  print("The original image is as shown below: ")
  resized_image = cv2.resize(image, (500, 500))
  cv2.imshow('original img window',resized_image)
  data = input("Enter data to be encoded : ")
  if (len(data) == 0):
    raise ValueError('Data is empty')
  filename = input("Enter the name of new encoded image(with extension): ")
  encoded_image = hideData(image, data)
  cv2.imwrite(filename, encoded_image)



def decode_text():
  image_name = input("Enter the name of the steganographed image that you want to decode (with extension) :")
  image = cv2.imread(image_name)
  print("The Steganographed image is as shown below: ")
  resized_image = cv2.resize(image, (500, 500))
  cv2.imshow('new image',resized_image)
  text = showData(image)
  return text



def Steganography():
    a = input("Image Steganography \n 1. Encode the data \n 2. Decode the data \n Your input is: ")
    userinput = int(a)
    if (userinput == 1):
      print("\nEncoding....")
      encode_text()

    elif (userinput == 2):
      print("\nDecoding ... ")
      print("Decoded message is " + decode_text())
    else:
        raise Exception("Enter correct input")


Steganography()
#Steganography()
```

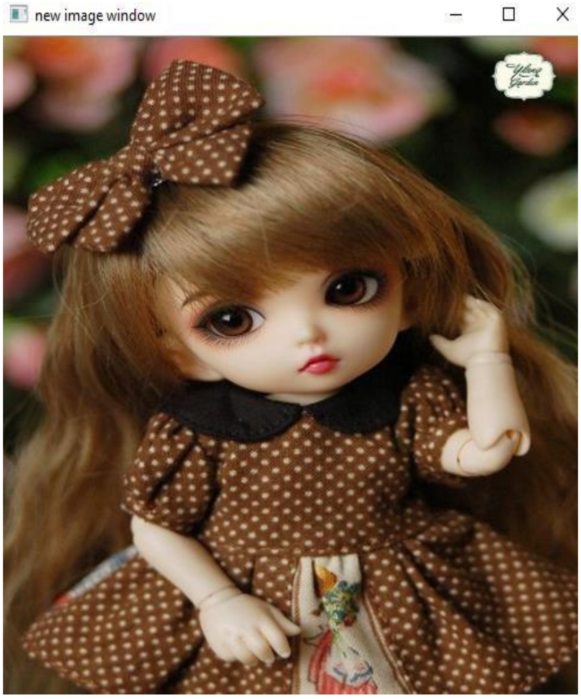
CHAPTER-8

EXPERIMENT RESULTS:-

INPUT IMAGE



OUTPUT IMAGE

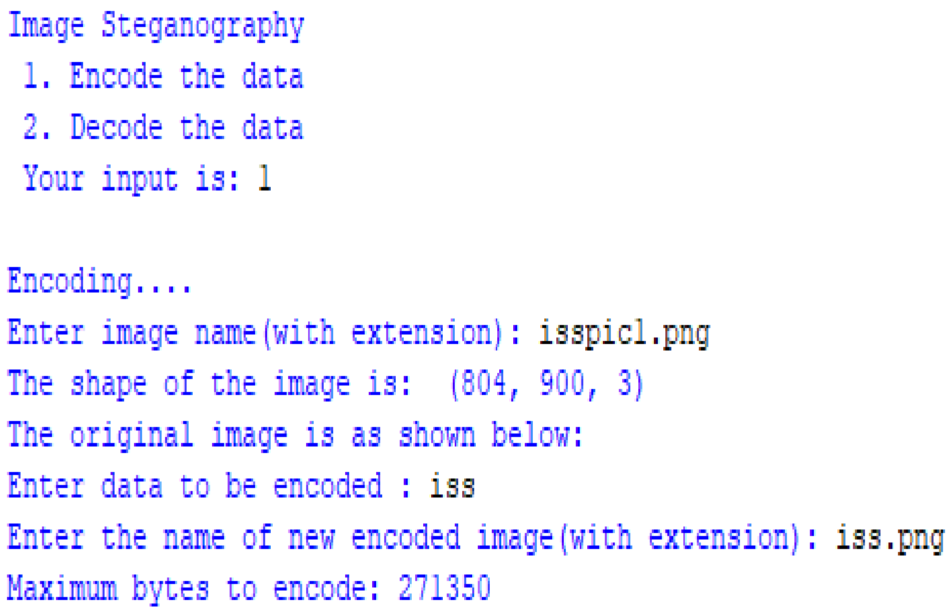


Here we cannot find any difference between because,

The Human visual system (HVS) cannot detect changes in the color or intensity of a pixel when the LSB bit is modified. This is psycho-visual redundancy since this can be used as an advantage to store information in these bits and yet notice no major difference in the image.

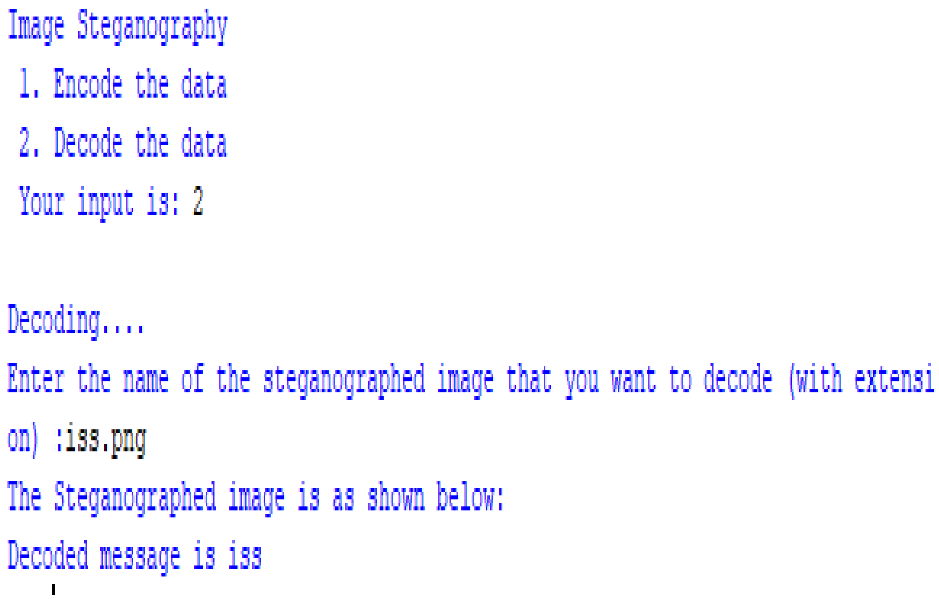
isspic1.png → input image
iss.png → output image

ENCODING:-



```
Image Steganography
 1. Encode the data
 2. Decode the data
 Your input is: 1

Encoding....
Enter image name(with extension): isspicl.png
The shape of the image is:  (804, 900, 3)
The original image is as shown below:
Enter data to be encoded : iss
Enter the name of new encoded image(with extension): iss.png
Maximum bytes to encode: 271350
```

DECODING:-



```
Image Steganography
 1. Encode the data
 2. Decode the data
 Your input is: 2

Decoding....
Enter the name of the steganographed image that you want to decode (with extensi
on) :iss.png
The Steganographed image is as shown below:
Decoded message is iss
```

CHAPTER-9

CONCLUSION:-

- Hiding a message with steganography methods reuces the chance of a message being detected
- In and Itself, steganography is not a good solution to secrecy , but neither is simple substitution and short block permutation for encryption. But if These methods are combained ,you have much stronger encryption routines

CHAPTER-10

REFERENCES:-

[1] Mukherjee, M., & Samanta, D. (2014). Fibonacci Based Text Hiding Using Image Cryptography. *Acharya Institute of Technology, Department of MCA, Bangalore, India*, *2*(2).

[2] A. Sinkov, Elementary Cryptanalysis: A Mathematical Approach,

Mathematical Association of America, 1966. [2] G. R. Blakely, “Safeguarding cryptographic keys,” in Proc. National Computer Conf., vol. 48, pp. 313–317.

[3] Z. G. Ma and S. S. Qiu, “An image cryptosystem based on general cat map,” J. China Inst. Commun., vol. 24, pp. 51-57, 2003.

[4] T. Kong and Z. Dan, “A new anti-arnold transform algorithm,” J. Software, vol. 15, pp. 1558-1564, 2004.

[5] C. Y. Hong and W. G. Zou, “Digital image scrambling technology based on three dimensions arnoldtransform and its period,” J. Nanchang Univ. Nat. Sci., vol. 29, pp. 619-621, 2005,

[6] Z. H, “On the period of 2D Random matrix scrambling transform

and its application in image hiding," Chinese J. Comput., vol. 29,

pp. 2218-2225, 2006.

[7] D. L. Yang, N. Cai, and G. Q. Ni, "Digital image scrambling technology based on the symmetry of arnold transform," J. Beijing Inst. Technol., vol. 15, pp. 216-220, 2006.