Digital Image Processing

UE18EC317

Steganography - Project Report

By -
Vaishnavi C K
PES1201800605
B.Tech 5th sem

INTRODUCTION:

- Steganography is the process of concealing a file, message, image or video within another file, image or video.

- It is one of the methods employed to protect secret or sensitive data from malicious attacks.

- In this case we use an image which has been digitally altered to carry a hidden message.

- The aim here is to encrypt text into an image by varying intensity values of individual pixels according to the ASCII values of individual characters and decrypt the image.

- The steps involved in doing so are:
  Text -> Encryption algorithm -> Encrypted Image -> Decryption Algorithm -> Text transmitted

ALGORITHM:

- Encryption :
  1. Read the text and convert it into equivalent ASCII Values.
  2. Fetch the image.
  3. Vary the intensity of the image according to the ASCII Values.
  4. Generate the Encrypted Image.

- Decryption :
  1. Fetch the Encrypted Image.
  2. Having the initial image as the reference, get the encrypted ASCII values.
  3. Generate the decrypted text using the ASCII values.

CONCEPTS:

- Grayscale Image Intensity: Each image intensity value of a pixel in grayscale mode has intensity values 0 to 255. Each pixel intensity is represented using 8 bit.

- ASCII: Abbreviated from American Standard Code for Information Interchange, is a character encoding standard for electronic communication. ASCII codes represent text in computers, telecommunications equipment, and other devices. The ASCII table has 128 characters, with values from 0 through 127. Thus, 7 bits are sufficient to represent a character in ASCII; however, most computers typically reserve 1 byte, (8 bits), for an ASCII character.

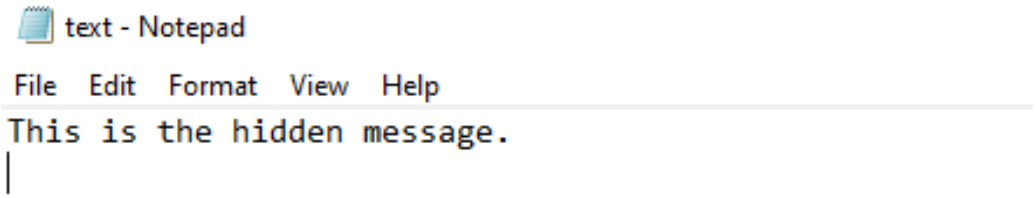
PROCEDURE:

- Encryption:
  1. Read the text file which contains the text to be encrypted.
  2. Get the length of the text file.
  3. Convert the characters into unsigned 16/8 bit characters.
  4. Add the ASCII Values to the intensities of individual pixels. If the values is exceeding 255, then keep the value (Intensity + Value)-256
  5. Write the encrypted image.

- Decryption:
  1. Fetch the encrypted image.
  2. Get individual intensity values of the pixels. Compare the values with the original image value.
  3. If the value is less than the original value, then it says that the value has exceeded 255 and hence we can calculate proper values.
  4. Else the difference if the ASCII value itself.
  5. Decrypted Text file is generated from the ASCII Values.

RESULTS:

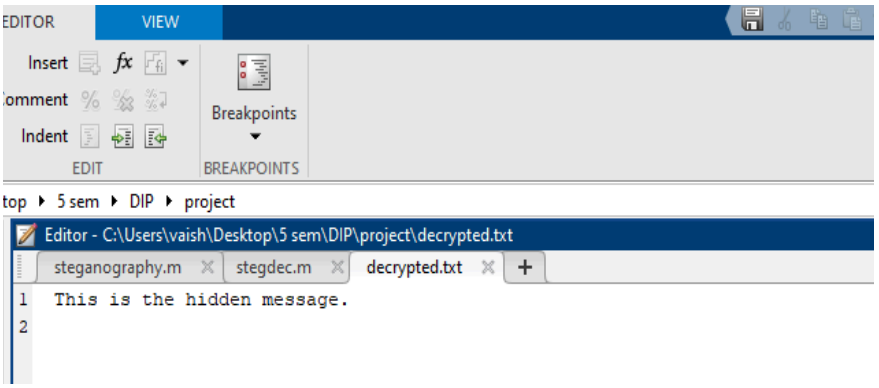
- Text to be hidden:

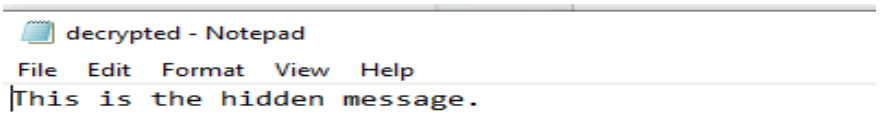


- Original Image:

- Encrypted Image:

- Decrypted text from the image:





APPLICATIONS

Steganography is applicable to, but not limited to, the following areas.

1. Confidential communication and secret data storing
2. Protection of data alteration
3. Access control system for digital content distribution
4. Media Database systems

Permits safe data transfer with minor changes to the original image.

LIMITATIONS

Though this process of data transfer is secure, it has its limitations.

1. Large amounts of data i.e image files must be transmitted to convey a message of small size. i.e it is strenuous on the resources the program can use for transmission and reception.
2. Image is susceptible to noise and hence alteration of the input message in some cases.
3. Large text files heavily distort the image giving it an appearance very different from its original form.