DIP COURSE PROJECT

UE17EC316

SAHIL F - PES1201701653
BHUVAN M R - PES1201701823

Title

Image steganography

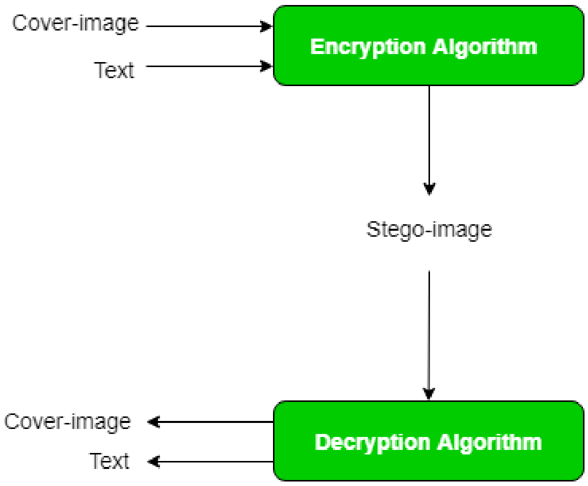
Introduction

The objective of this project is data security using digital image processing. Steganography is a mode of invisible communication.Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word *steganography* combines the Greek words *stegano*, meaning "covered or concealed", and *graphe* meaning "writing". Image steganography is used to encrypt the data in an image. We are restricting the medium to image hence the name Image Steganography. The image used for this purpose is called the cover-image and image obtained after steganography is called stego-image.

Problem Statement

Steganography hides the very existence of a message so that if successful it generally attracts no suspicion at all. Using steganography, information can be hidden in carriers such as images, audio files, text files, videos and data transmissions. In this study, we proposed a new framework of an image steganography system to hide a digital text of a secret message.So given an information in the form of text or an image, encrypt the data in an image from sender end, and decrypt the data from the image at the receiver end.

Methodology - block diagram



Implementation

Encryption Algorithm:

In the beginning, an image and a text file(which has the data) will be given as input. Convert all characters present in the text file to its ASCII value, which is then converted to binary value(8 bits). The given input image is split into its RGB components. Assuming that image is of the dimension mxnx3,individual component will be represented by a matrix(which contains intensity values) which will be of the dimension mxn. Next step of the algorithm is the encryption part. Take the R-component matrix and convert all the intensity values present in it to binary value(8 bits). Then take the first character's binary value. First two bits of the character's binary value will replace the last two bits of the first value in R-component matrix. Next two bits will replace the last two bits of the second value in the matrix. So in this way first character will take four values in the matrix. Similarly do the same thing for next character. Once the R-component matrix has no more values to be replaced ,take the G-component matrix and repeat the same thing that was done R. Go to the Blue-component matrix if still there are characters left in the text file. Once all the characters are done, concatenate all the three matrices to form a new image. The new image created will be called as Stego-image(Encrypted image).

Decryption Algorithm:

For the decryption algorithm input will be the Stego-image. Along with the Stego-image there will be one more input .Second input in the decryption part is called as Key. Key specifies till which pixel we have to traverse to get all the characters of the required data. First step of decryption is to split the input image into its RGB component matrices. Take the R-component matrix and convert all the intensity values to binary value(8 bits). Acquire the last two bits of the first value in R-component matrix. Go to the second value acquire the last two bits. Once eight bits is acquired convert it into decimal value. Corresponding to that decimal value whatever character is obtained store it in a string. Repeat the same thing until the Key condition is satisfied. Once the Key condition is satisfied, write that string into a new file. That file will contain the required data.

Saving the Stego-image

The Stego-image has to be saved in order to use it in the near future for decryption. In which format or extension the new image has to be saved? .We will be comparing only JPEG and PNG format here. JPEG format is a lossy algorithm which compresses the intensity values in order to reduce the size of the image while storing. If the Stego-image is saved in JPEG format and it is passed on as input to the decryption algorithm we will get garbage data instead of the original data as output. PNG format is a lossless algorithm which does not do any compression while storing the image. If the Stego-image is saved in PNG format and it is passed on as input to the decryption algorithm we will the original data itself as the output. Though the size of the Stego-image may be bigger in PNG format but in order to recover the stored data it is better to save the image in PNG format.

Comparison of Original image and Stego-image

Will the Original image and Stego-image be different? Or else Stego-image will be same as Original image itself? Since we are replacing only the LSB of the image with each character's bits the new image will be the same as the original image. It is almost impossible to identify the difference between both the images from naked eye. So we will use a parameter called psnr (peak signal to noise ratio)value to identify the difference. What psnr does is that it will compute signal to noise ratio of the new image with reference to the original image. If the output of psnr function is more than 45 we can easily infer that new image is a very good image and it does not have much noise compared to the original image. If the psnr function returns a value less than 40 it means that new image is corrupted with noise

Extension

Considering the data security, encryption algorithm can be modified. Instead of just replacing the last two bits of the pixel, a threshold can be set for the intensity values. If the intensity values are more than the threshold different encryption pattern can be employed.

Is it possible to encrypt an image in an image? Yes, it is definitely possible. The complexity of encryption algorithm will be slightly more compared to the former case.

Applications

This technique can be used to increase the security of the communication. Sensitive data can be transferred from one person to another person such that transfer of data is unknown.

THANK YOU