



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

Information Theory and Coding

ECE4007

Class Number - VL2019205005058

Final Project Report

IMAGE STEGANOGRAPHY USING LSB
ALGORITHM

Submitted By:

Name: Kartik Gupta

Reg. No.: 17BEC0548

Slot: B2+TB2

Submitted To:

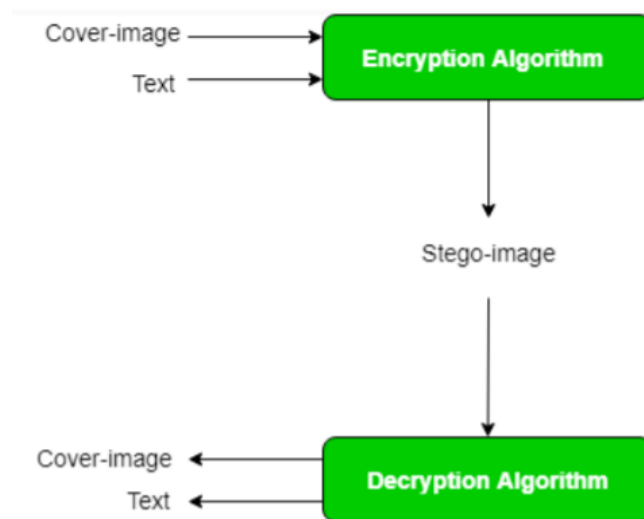
Prof. K.S. Preetha

Problem Statement:

Sometimes there is a need to keep our data safe and as at many places there is private data which needs to be secured. For this reason, we propose steganography here as a technique that can be applied for keeping the data safe. Also, we can add data in the image for the ease of access of sending information. Steganography is using the DWT technique and LSB steganography. The data to be steganographed is encrypted using AES algorithm to enhance the security.

Abstract:

As the internet has become the primary medium for the transfer of information, the security of the transferred information has become the subject of utmost importance. Image steganography has emerged out as the eminent tool of information hiding that ensures the security of the transferred data. Image files provide high capacity and their frequency of availability over the internet is high. The data to be transmitted is encrypted on the image and is transmitted. The encrypted image is decoded at the receiver by making use of the original image. The original image serves as the key for decryption. On decoding, we obtain the original information that was encoded.



Introduction:

Since the rise of the Internet one of the most significant components of data technology and communication has been the security of data. Cryptography was made as a technique for securing the secrecy of communication and a wide range of techniques have been created to encrypt and decrypt information so as to keep the message secret. Unfortunately, it is once in a while insufficient to keep the contents of a message secret, it might likewise be important to keep the existence of the message secret. The method used to actualize this, is called steganography.

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. In image steganography the information is hidden exclusively in images.

An image that is defined in the “real world” is considered to be a function of two real variables, e.g. $a(x, y)$ with a as the amplitude (e.g. brightness) of an image at real coordinate position (x, y) . An image may be considered to contain sub images also called as regions-of-interest or regions. Image is a collection of objects. The amplitude of a given image will always be either real number or integer number.

Steganography is a branch of information hiding. It allows the people to communicate secretly. As increasingly more material becomes available electronically, the influence of steganography on our lives will continue to grow. Many confidential information was leaked to a rival firm using steganographic tools that hid the information in music and picture files. The application of steganography is an important motivation for feature selection.

The main perspective of steganography is to communicate securely in a completely undetectable manner and to avoid any drawing suspicion to the transmission of a hidden data. It is not to let others from knowing the hidden information, but it is to keep others from thinking that the information even exists somewhere. The data can be hidden in basic formats like:

Audio, Video, Text and Images etc.

The various kinds of steganography include:

1. Image Steganography: The image steganography is the process in which we hide the data within an image to protect the data so that there will not be any perceived visible change in the original image. The conventional image steganography algorithm is LSB embedding algorithm.
2. Audio Steganography: Steganography can also be applied to audio files i.e., we can hide information in an audio file, it can be called Audio Steganography. The audio file should not be detectable.
3. Video Steganography: Steganography can be applied to video files also. If we hide information in a video file, it can be called Video Steganography. The video file should be undetectable by any attacker.
4. Text files Steganography: Steganography can be applied to text files also. If we hide information in a text file, it is called Text Steganography.

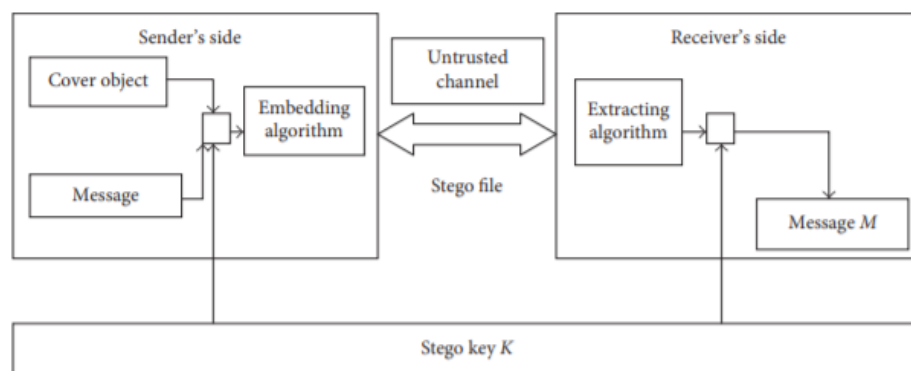


FIGURE 1: Steganography system.

Literature Survey:

The word steganography is derived from the Greek word “Seganos”, means covered or secret and – “graphy” meaning writing or drawing. Therefore, literally, the meaning of steganography is covered writing. It is the technique of making information invisible such that its presence cannot be sensed by a third party that communication is going on. A secret message is encoded such that even the presence of the data is hidden. Along with other communication techniques, steganography can be used to transmit secret messages.

The main target of the presented technique is to transmit message securely in a completely unnoticeable way and to avoid any kind of suspicion to the transmission of a hidden information. In the modern world, the interest in steganography has been increased very rapidly primarily because of two reasons:

- The publishing & broadcasting sector needs steganography technique for hiding copyright related pieces of information and serial numbers in digital films, audio, and video recordings, books, articles and multimedia products.
- Due to rapidly increasing cases of data theft throughout the whole world, people have been self-motivated to study and implement methods by which personal information can be hidden secretly within the cover images.

The basic steganography model has Carrier Image, Secret Message and Encryption Key. Carrier Images are also known as cover-image, inside which the secret data is hidden. Thus, it serves the purpose to hide the very existence of the secret messages.

Secret Information is the message that the sender wants to transmit with confidentiality. It is of many types like plain text, cipher-text, or anything that can be embedded in a stream of bits such as a copyright logo, a secret communication, or any kind of serial number. Encryption Key ensures that only the intended receiver who knows the decoding technique will be able to retrieve the message from a cover-image. The cover-image with the embedded secret information is called the Stego-image.

Retrieving the secret information from a stego-image needs the cover-image itself and the Encryption Key which was used during the process of encoding. The best part is that the original image is not even required in the presented method to retrieve the hidden data.

Tool to be Used:

- MATLAB Software
(Matrix Laboratory)

It is a multi-paradigm numerical computing environment and proprietary programming language developed by MathWorks. It allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages.

- Image for hiding text

Image is a function of two real variables, e.g. $a(x, y)$ with a as the amplitude (e.g. brightness) of an image at real coordinate position (x, y) . An image may be considered to contain sub images also called as regions-of-interest or regions. Image is a collection of objects.

- Hidden text file

Block Diagram:

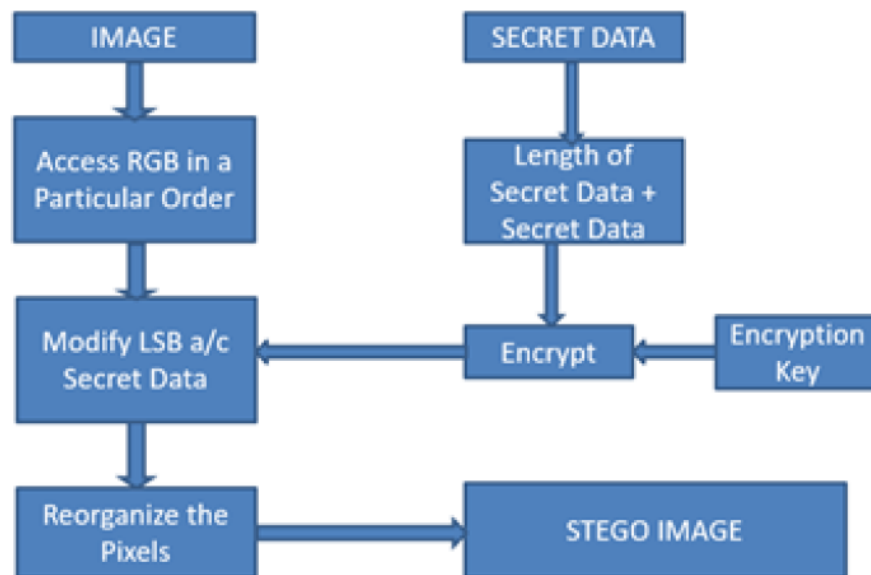


Fig -1: Block Diagram of Encoding

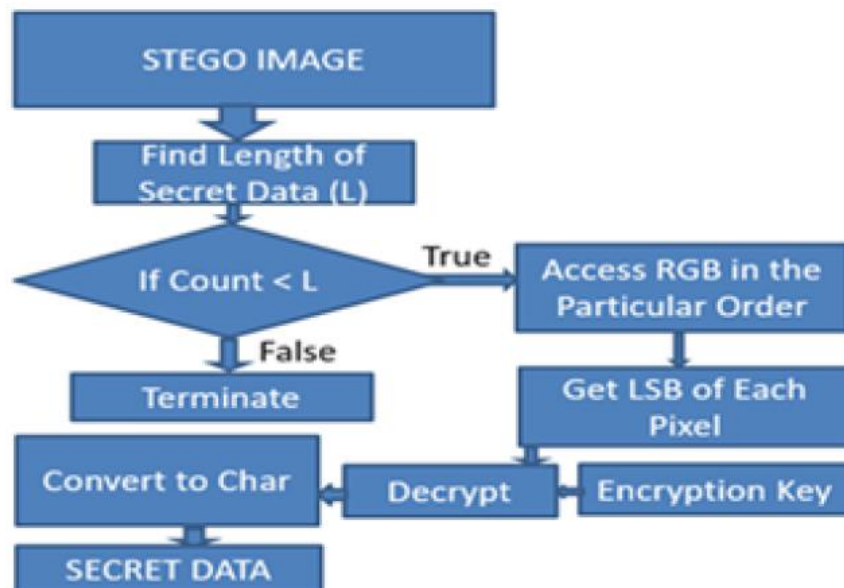


Fig -2: Block Diagram of Decoding

Methodology:

LSB Algorithm is being used to steganograph an image.

Least significant bit (LSB) insertion is a simple but still efficient approach for embedding data into a digital image. The simplest steganography technique inserts the bits of the data directly into the least significant bits of the image, i.e. LSB of the cover-image in a particular sequence.

Digital images are used as the cover images. They are mainly of two types- 24-bit images and 8-bit images. In 24-bit images, we can insert up to three bits of data into each pixel. In 8-bit images, one bit of data can be hidden into each pixel. After applying the LSB method, the output image within which the secret message is embedded is called as the stego-image. LSB technique, as the name suggests replaces the least significant bit of each pixel with the data that is to be hidden. Since LSB is replaced, there is no major or any noticeable effect on the cover image and hence third-party users will not be able to even suspect or find that any information is embedded inside the cover-image. However, obviously, there will be a minor unnoticeable change in the intensity level of original and stego image, but it is impossible to detect any change in the image by naked eyes.

Following example shows how the letter A is embedded into the 3 pixels, i.e. 8 bytes of a 24-bit image.

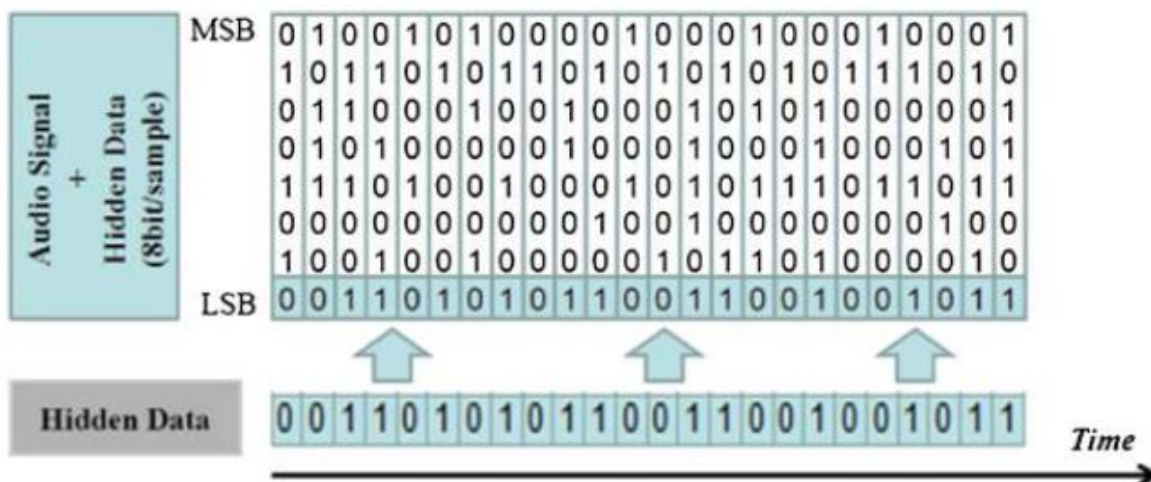
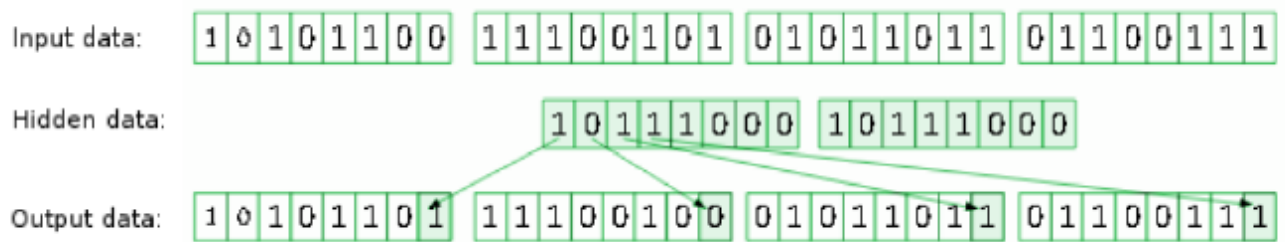
Pixels: (00100111 11101011 11001010)
(00100111 11011000 10101001)
(11001000 00110111 11011001)

A: 01010011

Result: (0010011**0** 11101011 11001010)
(00100111 11011000 101010**00**)
(1100100**1** 00110111 11011001)

One of the best advantages of this LSB technique is that it is easy to implement and has large message capacity. Also, there is very small chance of change in the quality of the cover image.

In the presented method, the hiding capacity can be increased, as per need by using two or three least significant bits.



Pseudocode:

Encryption:

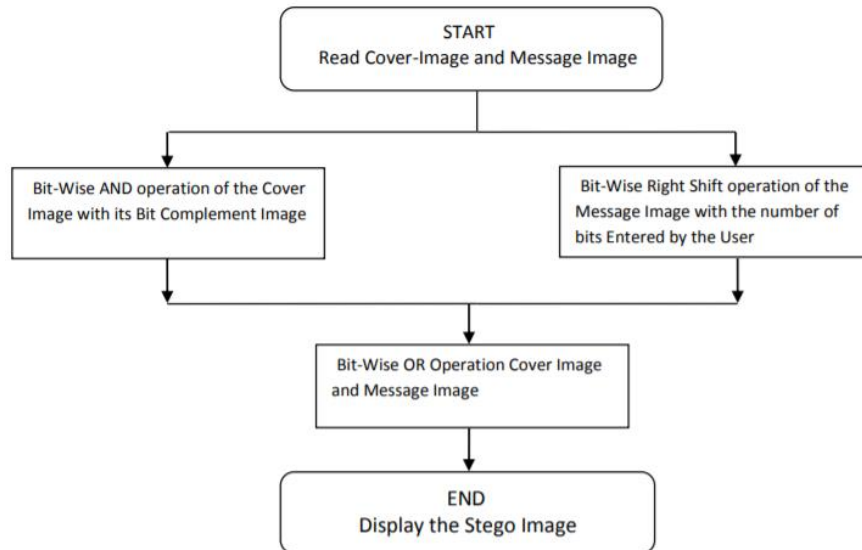
1. Open the text and image file.
2. loop while (character count <= total characters)
 - i. character=convert to 16-bit integer(character) //by default the pixels and characters will be 8-bit in MATLAB. This caused me a lot of problems
 - ii. pixel=convert to 16-bit integer(pixel)
 - iii. encrypted_pixel= (pixel) bitwise_xor (character)
 - iv. pixel=next pixel
 - v. character=next character.
 - vi. character count= character count + 1
3. end loop
4. rest of encrypted_pixels = pixels of original image

Decryption:

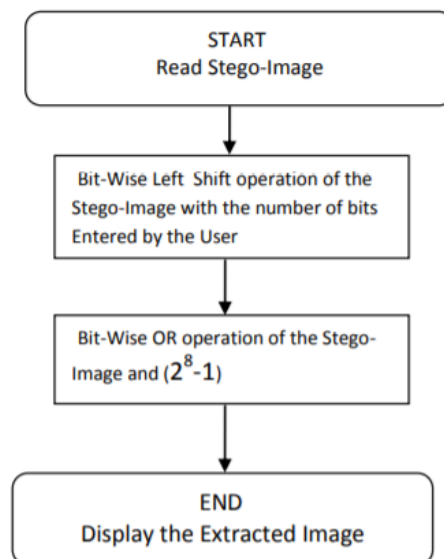
1. Open the original image and encrypted image.
2. loop while (pixel count <= total pixel)
 - i. original pixel=convert to 16-bit integer (original pixel)
 - ii. encrypted_pixel=convert to 16-bit integer(encrypted_pixel)
 - iii. a= (original pixel) bitwise_xor (encrypted_pixel)
 - iv. if a=0 then break else decrypted_text=a
 - v. original pixel=next original pixel
 - vi. encrypted_pixel=next encrypted_pixel.
3. end loop

Flow Chart:

Embedding Algorithm

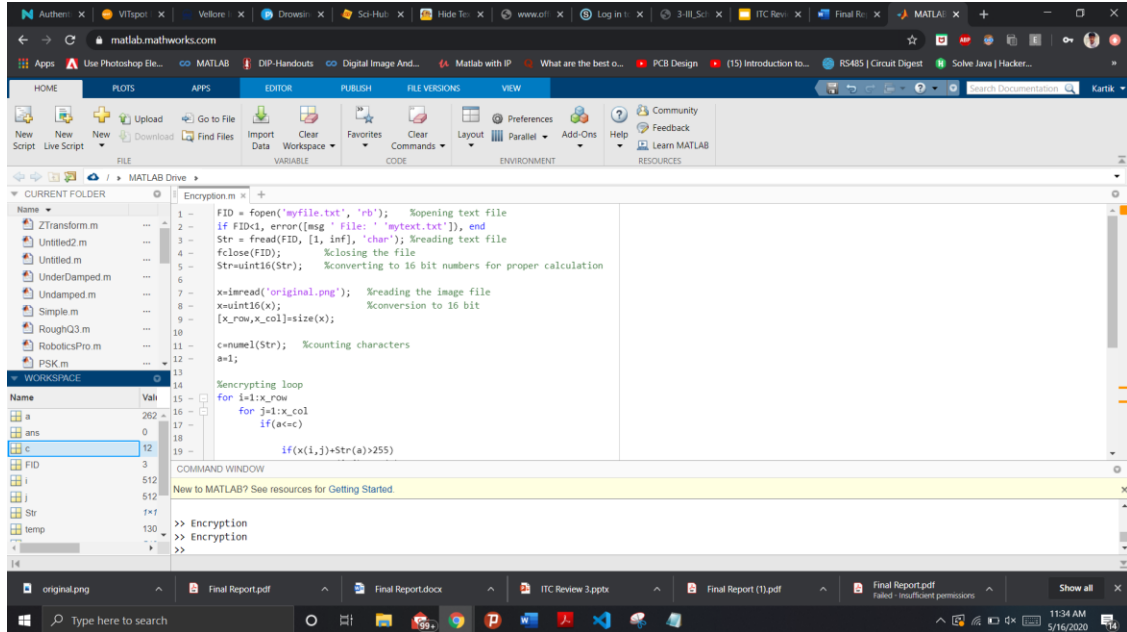


Extraction Algorithm



Results:

Encryption



The screenshot shows the MATLAB environment with the following code in the editor:

```
1 FID = fopen('myfile.txt', 'rb'); %Opening text file
2 if FID<1, error(['File: ' 'mytext.txt']), end
3 Str = fread(FID, [1, inf], 'char'); %reading text file
4 fclose(FID); %closing the file
5 Str=uint16(Str); %converting to 16 bit numbers for proper calculation
6
7 x=imread('original.png'); %reading the image file
8 x=uint16(x); %conversion to 16 bit
9 [x_row,x_col]=size(x);
10
11 c=numel(Str); %counting characters
12 a=1;
13
14 %encrypting loop
15 for i=1:x_row
16     for j=1:x_col
17         if(a<c)
18             if(x(i,j)+Str(a)>255)
```

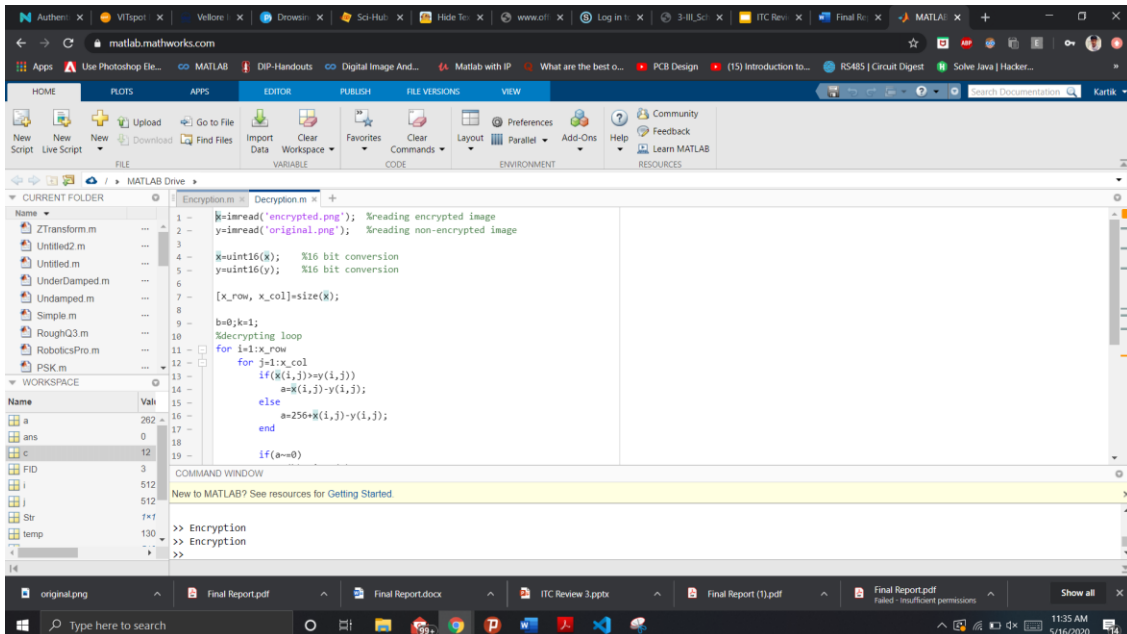
The workspace shows the following variables:

Name	Value
a	262
ans	0
c	12
FID	3
i	512
j	512
Str	1x1
temp	130

The command window shows the following output:

```
>> Encryption
>> Encryption
```

Decryption



The screenshot shows the MATLAB environment with the following code in the editor:

```
1 x=imread('encrypted.png'); %reading encrypted image
2 y=imread('original.png'); %reading non-encrypted image
3
4 x=uint16(x); %16 bit conversion
5 y=uint16(y); %16 bit conversion
6 [x_row,x_col]=size(x);
7
8 b=0;k=1;
9 %decrypting loop
10 for i=1:x_row
11     for j=1:x_col
12         if(x(i,j)>y(i,j))
13             a=x(i,j)-y(i,j);
14         else
15             a=256+x(i,j)-y(i,j);
16         end
17         if(a==0)
```

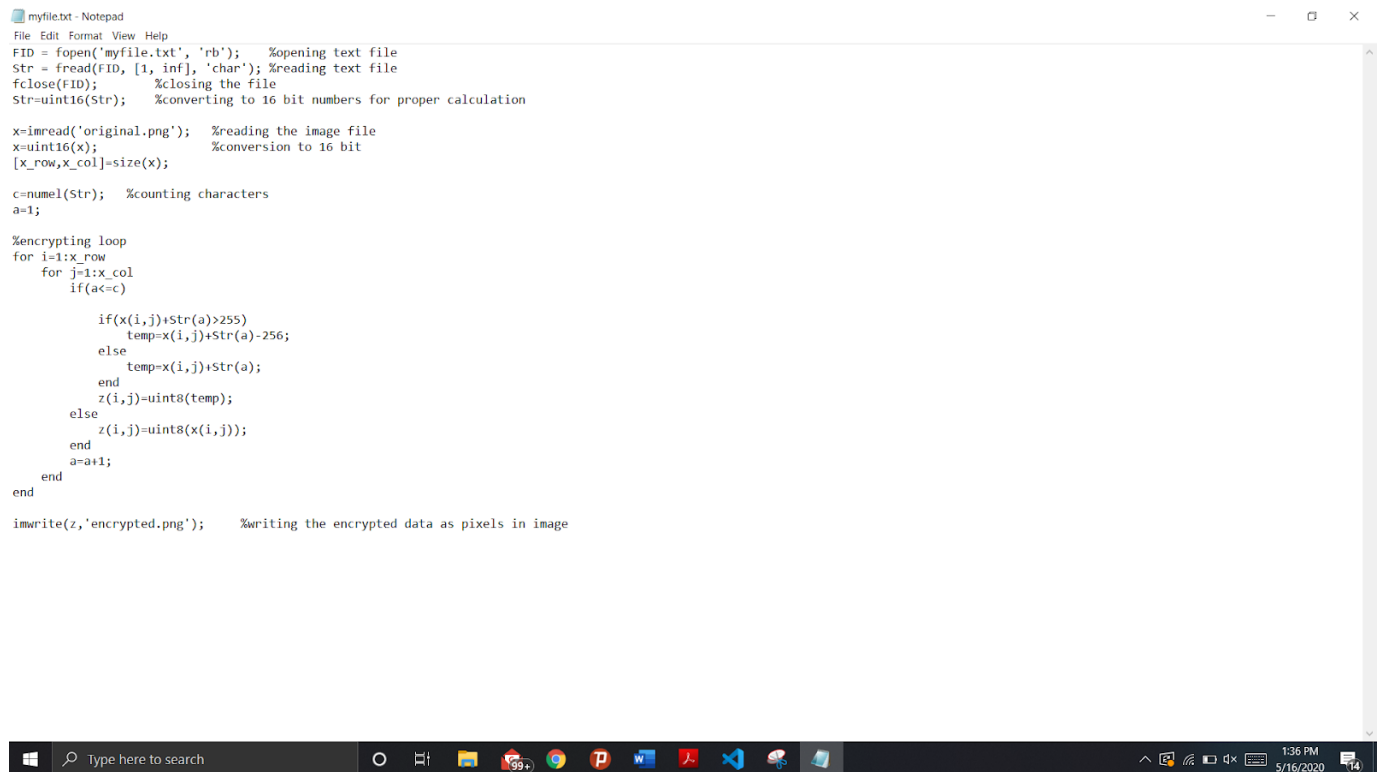
The workspace shows the following variables:

Name	Value
a	262
ans	0
c	12
FID	3
i	512
j	512
Str	1x1
temp	130

The command window shows the following output:

```
>> Encryption
>> Encryption
```

Text to be Encrypted



```
myfile.txt - Notepad
File Edit Format View Help
FID = fopen('myfile.txt', 'rb'); %opening text file
Str = fread(FID, [1, inf], 'char'); %reading text file
fclose(FID); %closing the file
Str=uint16(Str); %converting to 16 bit numbers for proper calculation

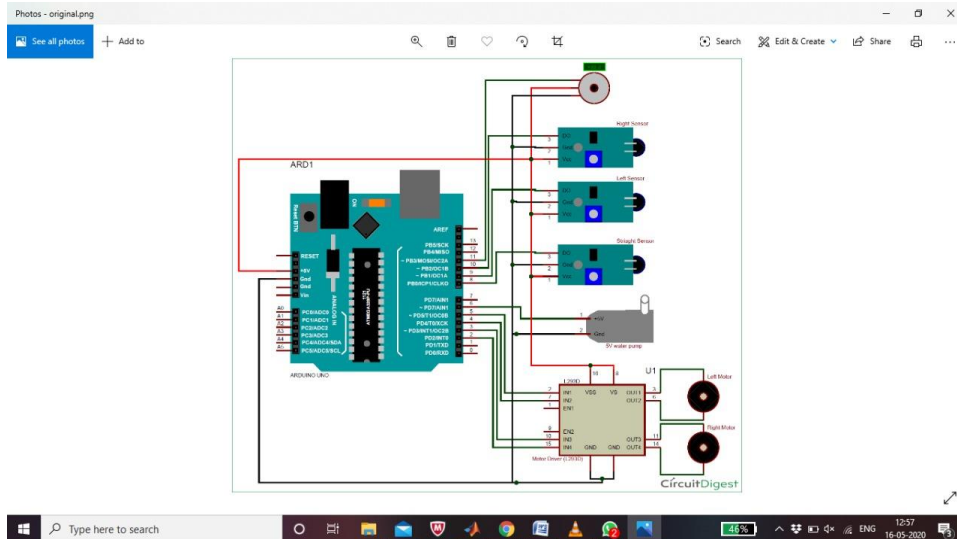
x=imread('original.png'); %reading the image file
x=uint16(x); %conversion to 16 bit
[X_row,X_col]=size(x);

c=numel(Str); %counting characters
a=1;

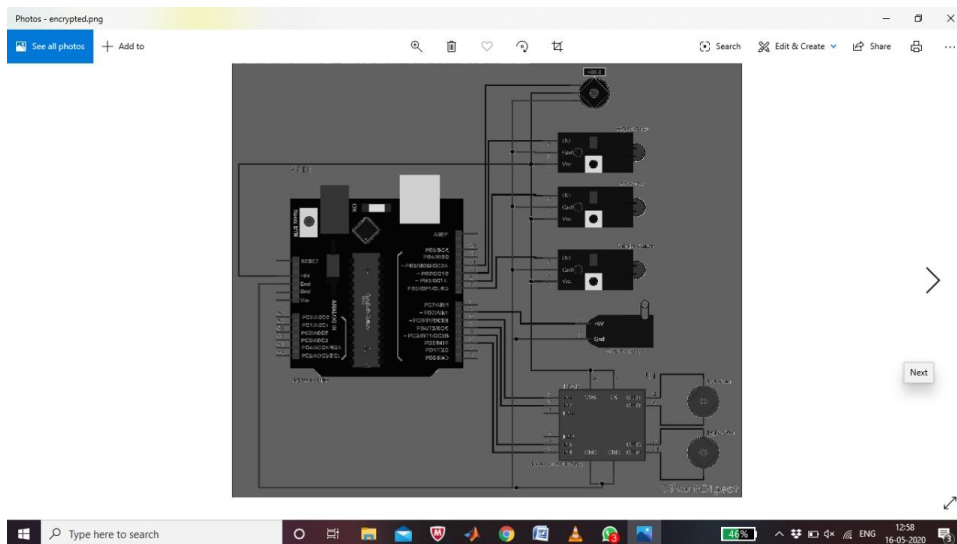
%encrypting loop
for i=1:X_row
    for j=1:X_col
        if(a<=c)
            if(x(i,j)+Str(a)>255)
                temp=x(i,j)+Str(a)-256;
            else
                temp=x(i,j)+Str(a);
            end
            z(i,j)=uint8(temp);
        else
            z(i,j)=uint8(x(i,j));
        end
        a=a+1;
    end
end

imwrite(z,'encrypted.png'); %writing the encrypted data as pixels in image
```

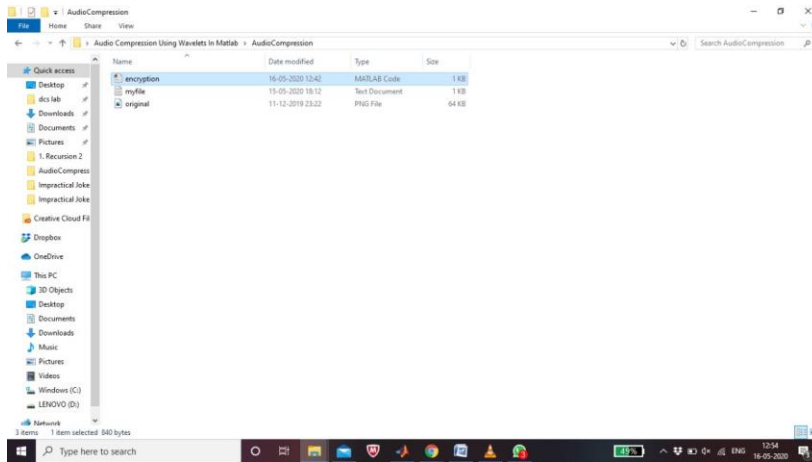
Original Image



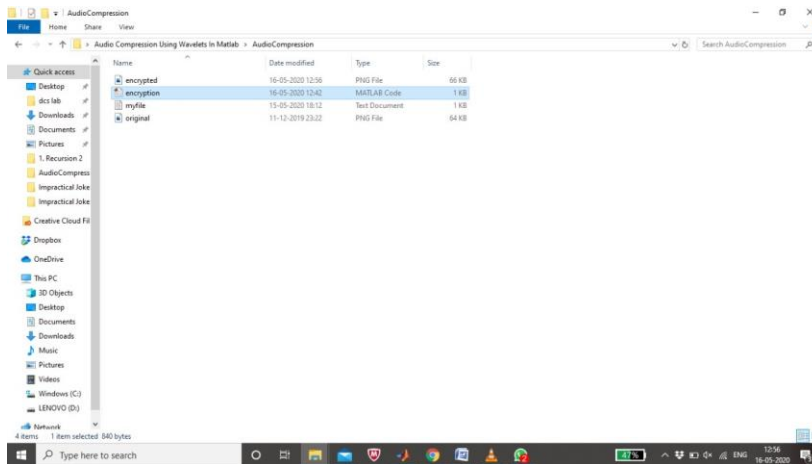
Encrypted Image



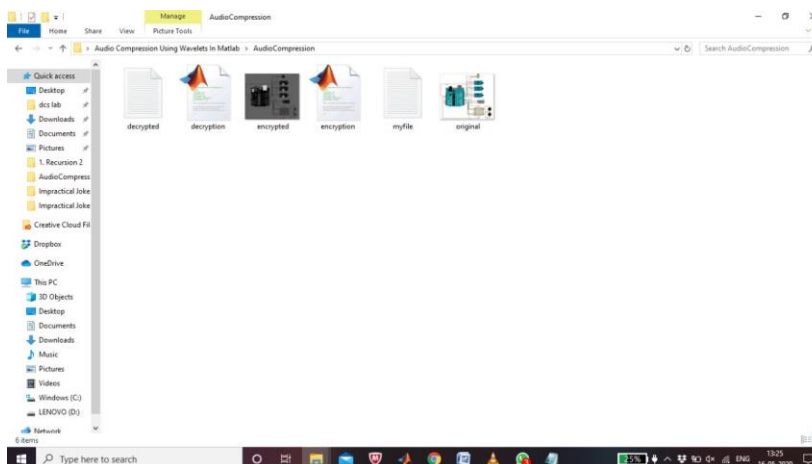
Before



After Encryption



After Decryption



Conclusion:

The advantage of LSB technique lies in its simple structure and ease of implementation. LSB method also allows high embedding capacity. The LSB technique uses encryption key and thus it is more secure. Hiding secret data using Steganography method lowers the chances of secret data being detected. LSB technique for digital image Steganography works smoothly for 8 bits and 24 bits BMP, GIF and PNG image formats.

Using this encoding and decoding algorithms, one can retrieve the secret message exactly as original data without altering the cover image.

We can also say that if LSB Bit substitution is increased the Cover Images also changes accordingly.

References:

- <https://www.hindawi.com/journals/jcnc/2018/9475142/>
- V. Potdar and E. Chang, "Gray level modification steganography for the secret communication," in Proceedings of the IEEE International Conference on Industrial Informatics, Berlin, Germany, 2004
- W. Bender, "Techniques for data hiding," IBM Systems Journal, vol. 35, no. 3-4, pp. 313-336, 1996.
- D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613-1626, 2003.
- Z. Y. Al-Omari and A. T. Al-Taani, "Secure LSB steganography for coloured images using character-colour mapping," 2017 8th International Conference on Information and Communication Systems (ICICS), 2017, pp. 104-110.
- Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999.
- https://www.academia.edu/40316220/IMAGE_STEGANOGRAPHY_USING_MODIFIED_LSB
- K B Raja, Venugopal K R and L M Patnaik, "A Secure Stegonographic Algorithm using LSB, DCT and Image Compression on Raw Images", Technical Report, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, December 2004.
- Emam, M.M., Aly, A.A. and Omara, F.A., 2016. An improved image steganography method based on lsb technique with random pixel selection. International Journal of Advanced Computer Science and Applications, 7(3), pp.361-366.

Reference Paper:

- https://www.academia.edu/40316220/IMAGE_STEGANOGRAPHY_USING_MODIFIED_LSB

IMAGE STEGANOGRAPHY USING MODIFIED LSB

Abhijeet Bhaskar

abhijha6@gmail.com

Student (B.Tech.), Department of ECE
Galgotia's College of Engineering & Technology
Gr. Noida, UP-201306

Under the supervision of

Mr. Upendra Kumar Acharya

Upendra.acharya@galgotiacollege.edu

Asst. Prof., Dept. of ECE,
Galgotia's College of Engineering & Technology
Gr. Noida, UP-201306

ABSTRACT

The proposed method is a quite useful technique for secure communication over the web. In steganography, the hidden message is invisible. This paper depicts methods to implement encryption and decryption techniques on the secret information to be hidden into other images, this will provide confidentiality to the secret information. The sender and the receiver only know the techniques to hide and retrieve the secret message. No third party person will even suspect that there is a hidden message inside the image file. The sender and the receiver only have the knowledge of the instructions to hide and retrieve.

Keywords— *Steganography; Data-hiding; Cover Image; Stego Image; LSB; PSNR; Encryption Key; MSE; UIQI; SSIM;*

1. INTRODUCTION

Steganography is the art of concealing the fact that communication is going on, by hiding secret message into other files. Many types of carrier files are used, but the most popular are digital images because of their massive usages on the internet. To hide data in digital images, there are a number of steganography methods. Each one of them has their strong and weak points. Many applications require complete confidentiality of the secret data, while others may need a large text message to be hidden. Presented method intends to provide a new technique of image steganography and its uses.

Steganography is more important as many people are engaging with the internet. Steganography means hiding secret data in such a way that no third party can detect the hidden data. The difference between steganography and cryptography is that the information is visible in cryptography but is still undeciphered but in steganography, the information is hidden.

2. LITERATURE SURVEY

The word steganography is derived from the Greek word "Seganos", means covered or secret and - "graphy" meaning writing or drawing. Therefore, literally, the meaning of steganography is covered writing. It is the technique of making information invisible such that its

presence cannot be sensed by a third party that communication is going on. A secret message is encoded such that even the presence of the data is hidden. Along with other communication techniques, steganography can be used to transmit secret messages.

The main target of the presented technique is to transmit message securely in a completely unnoticeable way and to avoid any kind of suspicion to the transmission of a hidden information. In the modern world, the interest in steganography has been increased very rapidly primarily because of two reasons:

- The publishing & broadcasting sector needs steganography technique for hiding copyright related pieces of informations and serial numbers in digital films, audio, and video recordings, books, articles and multimedia products.
- Due to rapidly increasing cases of data theft throughout the whole world, people have been self-motivated to study and implement methods by which personal information can be hidden secretly within the cover images.

The basic steganography model have Carrier Image, Secret Message and Encryption Key. Carrier Images are also known as cover-image, inside which the secret data is hidden. Thus it serves the purpose to hide the very existence of the secret messages.

Secret Information is the message that the sender wants to transmit with confidentiality. It is of many types like plain text, cipher-text, or anything that can be embedded in a stream of bits such as a copyright logo, a secret communication, or any kind of serial number. Encryption Key ensures that only the intended receiver who knows the decoding technique will be able to retrieve the message from a cover-image. The cover-image with the embedded secret information is called the Stego-image.

Retrieving the secret information from a stego-image needs the cover-image itself and the Encryption Key which was used during the process of encoding. The best part is that the original image is not even required in the presented method to retrieve the hidden data.