Innovative Assignment Report

Fundamentals of Image and Video Processing (2ECOE04)

Topic :

Steganography Using Image Processing

Submitted By :
Rushi Patel, 18BCE201
Sanket Cheladiya, 18BCE042

INDEX

Sr.	Topic
1.	Introduction
2.	History of Steganography
3.	Why This Steganography?
4.	Scope
5.	Methodology
6.	Limitations of the software
7.	Detecting Steganography
8.	Problem Statement
9.	Objectives
10.	Overview
11.	Steganography Techniques
12.	Graphical Representation
13.	Encryption
14.	Decryption
15.	Code snippet
16.	Summary

Introduction :

- Steganography is one technique of hiding private or sensitive information within something here we use images that appear to be nothing out of the ordinary.
- 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 the 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, therefore the person will not attempt to decrypt the information.
- What steganography essentially does is exploit human perception, human senses are not trained to look for files that have information inside of them, although this software is available that can do what is called Steganography. The most common use of steganography is to hide a file inside another file.

History of Steganography:

- Steganography is used to secretly communicate information between people.

1. During World War 2 invisible ink was used to write information on pieces of paper so that the paper appeared to the average person as just being blank pieces of paper. Liquids such as milk, vinegar and fruit juices were used, because when each one of these substances are heated they darken and become visible to the human eye.
2. In Ancient Greece they used to select messengers and shave their head, they would then write a message on their head. Once the message had been written the hair was allowed to grow back. After the hair grew back the messenger was sent to deliver the message, the recipient would shave off the messenger's hair to see the secret message.
3. Another method used in Greece was where someone would peel wax off a tablet that was

Why This Steganography?

- This technique is chosen, because this system includes not only imperceptibility but also un-delectability by any steganalysis tool.

Project Scope :

- This project is developed for hiding information in any image file. The scope of the project is implementation of steganography tools for hiding information includes any type of information file and image files and the path where the user wants to save Image and extruded file.

Methodology:

- User needs to run the application. The user has two tab options – encrypt and decrypt.
- If the user selects, the application gives the screen to select the image file, information file and option to save the image file.
- If the user selects decrypt, the application gives the screen to select only the image file and asks the user where the user wants to save the secret file.
- This project has two methods – Encrypt and Decrypt.

In encryption the secret information is hiding in with any type of image file.

Decryption is getting the secret information from an image file.

Limitations of the Software:

- This project has an assumption that both the sender and receiver must have shared some secret information before imprisonment.
- Pure steganography means that there is none prior information shared by two communication parties.

Detecting Steganography:

- The art of detecting Steganography is referred to as **Steganalysis.**

- To put is simply Steganalysis involves detecting the use of Steganography inside of a file. Steganalysis does not deal with trying to decrypt the hidden information inside of a file, just discovering it.

- There are many methods that can be used to detect Steganography such as:

- “Viewing the file and comparing it to another copy of the file found on the Internet (Picture file). There are usually multiple copies of images on the internet, so you may want to look for several of them and try and compare the suspect file to them.

- For example if you download a JPED and your suspect file is also a JPED and the two files look almost identical apart from the fact that one is larger than the other, it is most probable you suspect the file has hidden information inside of it.

Problem Statement :

- The former consists of linguistic or language forms of hidden writing. The later, such as invisible ink, try to hide messages physically.

- One disadvantage of linguistic steganography is that users must equip themselves to have a good knowledge of linguistics.

- In recent years, everything is trending toward digitization. And with the development of the internet technology, digital media can be transmitted conveniently over the network.

- Therefore, messages can be secretly carried by digital media by using the steganography techniques, and then be transmitted through the internet rapidly

- Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats

can be used, but digital images are the most popular because of their frequency on the internet.

- For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points.

- So we prepare this application, to make the information hiding simpler and user friendly.

Objective :

- The goal of steganography is covert communication. So, a fundamental requirement of this steganography system is that the higher message carried by stego-media should not be sensible to human beings.

- The other goal of steganography is to avoid drawing suspicion to the existence of a hidden message. This approach of information hiding technique has recently became important in a number of application area

- This project has following objectives:
  - To produce a security tool based on steganography techniques.
  - To explore techniques of hiding data using encryption module of this project
  - To extract techniques of getting secret data using a decryption module.
- Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption.

- An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen

Overview :

- The word steganography comes from the Greek “Seganos”, which means covered or secret and – “graphy” means writing or drawing.

- Therefore, steganography means, literally, covered writing. It is the art and science of hiding information such that its presence cannot be detected and communication is happening.

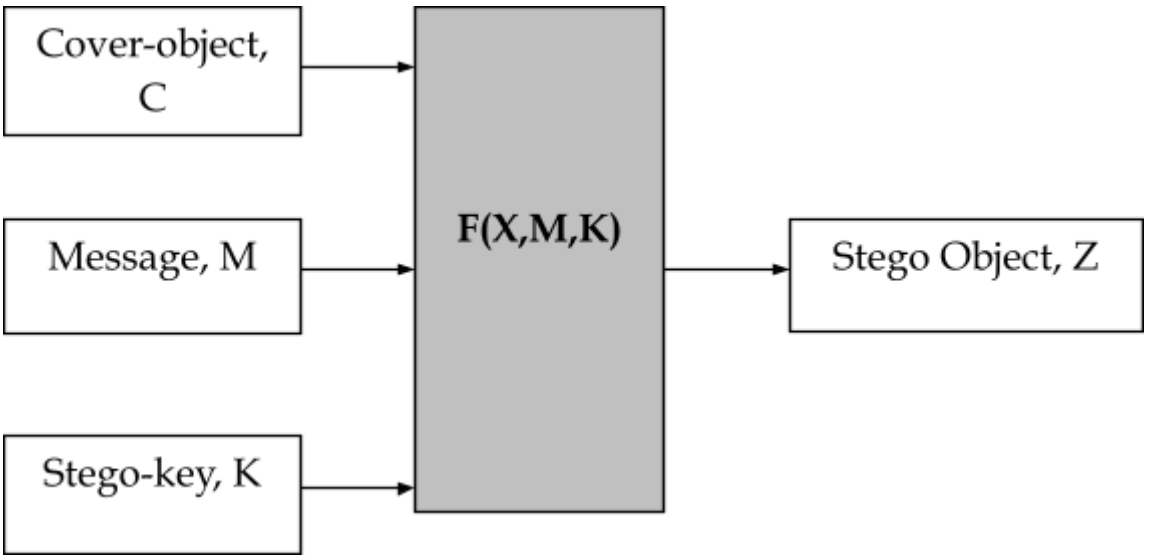
- A secret information is encoding in a manner such that the very existence of the information is concealed. Paired with existing communication methods, steganography can be used to carry out hidden exchanges.

- The main goal of this project is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hider data. There has been a rapid growth of interest in steganography for two reasons:
- The publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products

- Moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages.

- The basic model of steganography consists of Carrier, Message and password. Carrier is also known as cover-object, in which the message is embedded and serves to hide the presence of the message.

Basically, the model for steganography is shown on following figure:



- ✶ Message is the data that the sender wishes to remain confidential. It can be plain text, ciphertext, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number.
- ✶ Password is known as *stego-key*, which ensures that only recipients who know the corresponding decoding key will be able to extract the message from a *cover-object*. The *cover-object* with the secretly embedded message is then called the *Stego-object*.

- ✶ Recovering a message from a *stego-object* requires the *cover-object* itself and a corresponding decoding key if a *stego-key* was used during the encoding process. The original image may or may not be required in most applications to extract the message.

- ✶ There are several suitable carriers below to be the *cover-object:*
    - Network protocols such as TCP, IP and UDP
    - Audio that using digital audio formats such as wav, midi, avi, mpeg, mpi and voc
    - File and Disk that can hides and append files by using the slack space
    - Text such as null characters, just alike morse code including html and java
    - Images file such as bmp, gif and jpg, where they can be both color and gray-scale.

✶ In general, the information hiding process extracts redundant bits from *cover-object.* The process consists of two steps:

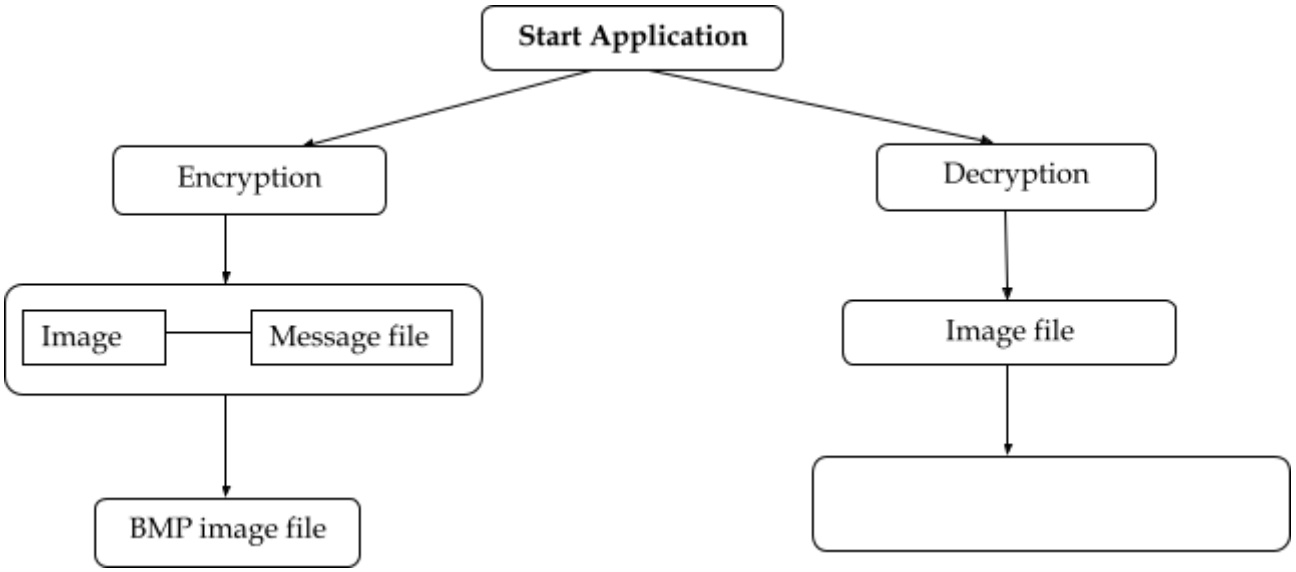
- Identification of redundant bits in a *cover-object.* Redundant bits are those bits that can be modified without corrupting the quality or destroying the integrity of the *cover-object.*
- Embedding process then selects the subset of the redundant bits to be replaced with data from a secret message. The *stego-object* is created by replacing the selected redundant bits with message bits

Steganography Techniques:

- Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed. There have been many techniques for hiding information or messages in images in such a manner that alteration made to the image is perceptually indiscernible. Common approaches include LSB, Masking and filtering and Transform techniques.
- Least significant bit (LSB) insertion is a simple approach to embedding information in an image file. The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover-image in a
- Deterministic sequence. Modulating the least significant bit does not result in human perceptible difference because the amplitude of the change is small. In this technique, the embedding capacity can be increased by using two or more least significant bits. At the same time, not only the risk of making the embedded message statistically detectable increase but also the image fidelity degrades. Hence a variable size LSB embedding schema is presented, in which the number of LSBs used for message embedding/extracting depends on the local characteristics of the pixel. The advantage of LSB-based method is easy to implement and high message pay-load.
- Although LSB hides the message in such a way that the humans do not perceive it, it is still possible for the opponent to retrieve the message due to the simplicity of the technique. Therefore, malicious people can easily try to extract the message from the beginning of the image if they are suspicious that there exists secret information that was embedded in the image.

- Therefore, a system named Secure Information Hiding System (SIHS) is proposed to improve the LSB scheme. It overcomes the sequence-mapping problem by embedding the massage into a set of random pixels, which are scattered on the cover-image.
- Masking and filtering techniques, usually restricted to 24 bits and gray scale images, hide information by marking an image, in a manner similar to paper watermarks. The technique performs analysis of the image, thus embedding the information in significant areas so that the hidden message is more integral to cover the image than just hiding it in the noise level.
- Transform techniques embed the message by modulating coefficient in a transform domain, such as the Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other variant.

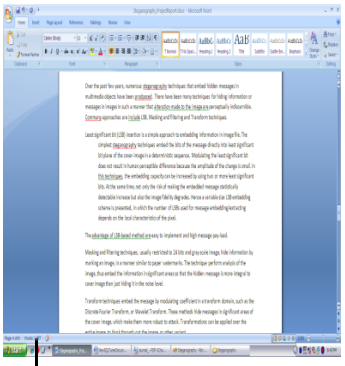
❖ The **graphical representation** of this system is as follows:



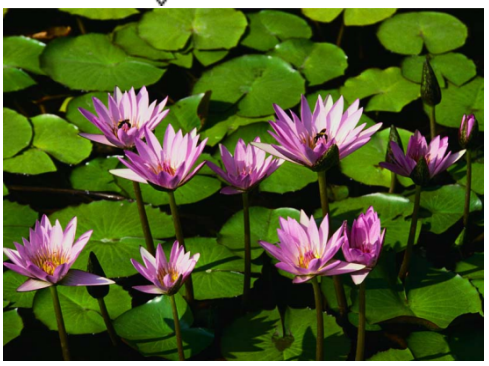
Encryption Process :

IMAGE FILE

INFORMATION FILE

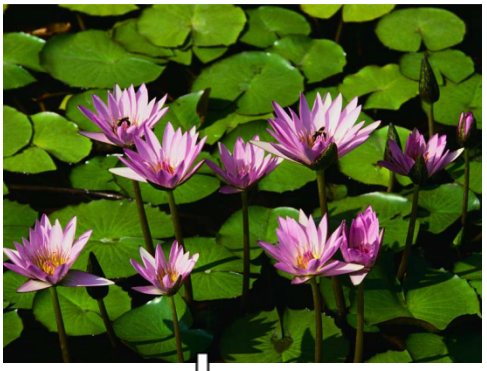


BMP FILE



Decryption Process :

BMP FILE



INFORMATION FILE

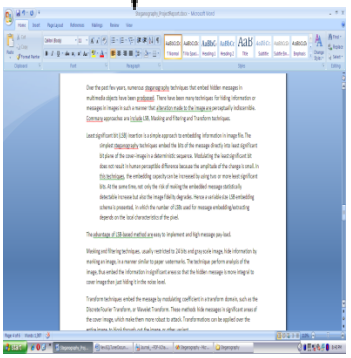
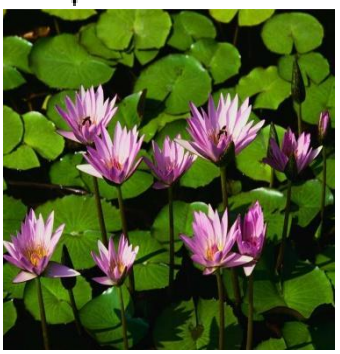


IMAGE FILE



Code Snippet

Part 1

```
import cv2
import string
import os
d={}
c={}

for i in range(255):
    d[chr(i)]=i
    c[i]=chr(i)


#print(c)

x=cv2.imread("2.jpg")

i=x.shape[0]
j=x.shape[1]
print(i,j)

key=input("Enter key to edit(Security Key) : ")
text=input("Enter text to hide : ")

kl=0
tln=len(text)
z=0 #decides plane
n=0 #number of row
m=0 #number of column

l=len(text)

for i in range(l):
    x[n,m,z]=d[text[i]]^d[key[kl]]
```

```
    n=n+1
    m=m+1
    m=(m+1)%3 #this is for every value of z , remainder will
be between 0,1,2 . i.e G,R,B planes will be set
automatically.

#whatever be the value of z , z=(z+1)%3 will always be
between 0,1,2 . The same concept is used for random numbers
in dice and card games.

    kl=(kl+1)%len(key)


cv2.imwrite("encrypted_img_2.jpg",x)
os.startfile("encrypted_img_2.jpg")
print("Data Hiding in Image completed
successfully.",end="\n\n-----------------\n\n")
#x=cv2.imread("encrypted_img.jpg")
```

Part 2

```
kl=0
tln=len(text)
z=0 #decides plane
n=0 #number of row
m=0 #number of column

ch = int(input("\nEnter 1 to extract data from Image : "))

if ch == 1:
    key1=input("\n\nRe enter key to extract text : ")
    decrypt=""

    if key == key1 :
```

```
        for i in range(l):
            decrypt += c[x[n,m,z]^d[key[kl]]]
            n=n+1
            m=m+1
            m=(m+1)%3
            kl=(kl+1)%len(key)
        print("Encrypted text was :
",decrypt,end="\n\n-----------------\n\n")
    else:
        print("Key doesn't
matched.",end="\n\n-----------------\n\n")
else:
    print("Thank you.
EXITING.",end="\n\n-----------------\n\n")
```

Summary

- Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day.

- Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice. We printed out the enhancement of the image steganography system using LSB approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover image.

- This steganography application software provided for the purpose of how to use any type of image formats to hide any type of files inside there. The master work of this application is in supporting any type of pictures without need to convert to bitmap, and lower limitation on file size to hide, because of using maximum memory space in pictures to hide the file.

- Since ancient times, man has found a desire in the ability to communicate covertly. The recent explosion of research in watermarking to protect intellectual property is evidence that steganography is not just limited to military or espionage applications. Steganography, like cryptography, will play an increasing role in the future of secure communication in the “digital world”.

~~~~~~~~~~~~~~~~ Thank You ~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~