The National Institute of Engineering

(An Autonomous Institution under Visvesvaraya Technological University, Belagavi)

Mysuru-570008

PROJECT REPORT ON

"IMAGE STEGANOGRAPHY, A GUI BASED PROGRAM USING PYTHON"

Submitted in partial fulfilment for the award of

BACHELOR OF ENGINEERING

IN

"ELECTRONICS AND COMMUNICATION"

For the academic year 2020-2021

Submitted by:

MANOJ N G	**4NI18EC039**
SOHAIL MAIDARGI	**4NI18EC088**

Under the guidance of

Mr. RAJARAM K G

Associate Professor, Dept. of ECE

THE NATIONAL INSTITUTE OF ENGINEERING

Department of Electronics and Communication

Mysuru -570008.

ESTD : 1946

CERTIFICATE

This is to certify that the project entitled **"IMAGE STEGANOGRAPHY, A GUI BASED PROGRAM USING PYTHON"** has been successfully completed by **MANOJ N G (4NI18EC039) AND SOHAIL MAIDARGI (4NI18EC088),** of 6th semester B.E. who carried out the project work under guidance of "**Mr. RAJARAM K G"** in the Partial fulfilment for the award of degree of Bachelor Engineering in Electronics and Communication Engineering of Visvesvaraya Technological University, Belagavi during the year 2020-21. It is certified that all corrections/suggestions indicated during internal assessment have been incorporated in the report. The project has been approved in partial fulfillment for the award of the said degree as per academic regulations of the National Institute of Engineering (An Autonomous Institution under Visvesvaraya Technological University, Belagavi).

Mr. Rajaram K G	**Dr. Narasimha Kaulgud**	**Dr. N V Raghavendra**
Project Guide	Head of the Department	Principal
Department of ECE	Department of ECE	NIE Mysuru

Name of the Examiner	**Signature with date**
1.	
2.	

THE NATIONAL INSTITUTE OF ENGINEERING

Department of Electronics and Communication

Mysuru -570008.

ACKNOWLEDGEMENT

We would take this opportunity to express our sincere gratitude and respect to lot of eminent personalities. Without whose constant encouragement and gratitude, the project of ours would not become reality.

We are grateful for the cooperation and constant encouragement from our honourable Head of the Department **Dr. Narasimha Kaulgud** for his support and encouragement.

We sincerely extend our thanks to our guide **Mr. RAJARAM K G**, Associate Professor, Department of Electronics and Communication Engineering, NIE Mysuru for his valuable guidance, constant assistance, and support for the betterment of this project.

MANOJ N G

SOHAIL MAIDARGI

CONTENTS

ABSTRACT

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. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This project hides the message with in the image. For a more secure approach, the project it allows user to choose the bits for replacement instead of LSB replacement from the image. sender select the cover image with the secret text or text file and hide it in to the image with the bit replacement choice, it help to generate the secure stego image .the stego image is sent to the destination with the help of private or public communication network . On the other side i.e. receiver. download the stego image and using the software retrieve the secret text hidden in the stego image .

INDEX OF FIGURE

CHAPTER 1

1.1 INTRODUCTION

1.1.1 Motivation and Theoretical overview

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

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.

1.1.2 Problem Statement

Today the world is witnessing a data explosion like never before. The amount of data we produce every day is truly mind-boggling. The Forbes article ***"How Much Data Do We Create Every Day?"*** states that there are about 2.5 quintillion bytes of data created each day at our current pace, but that pace is only accelerating with the growth of the Internet of Things (IoT). Over the last two years alone 90 percent of the data in the world was generated.

With the fast pace advancement in technology and use of data for continuous innovation it has become our topmost priority to secure data. The protection of data is the primary concern of the sender and it is really important that we encrypt our message in a secret way that only the receiver is able to understand.

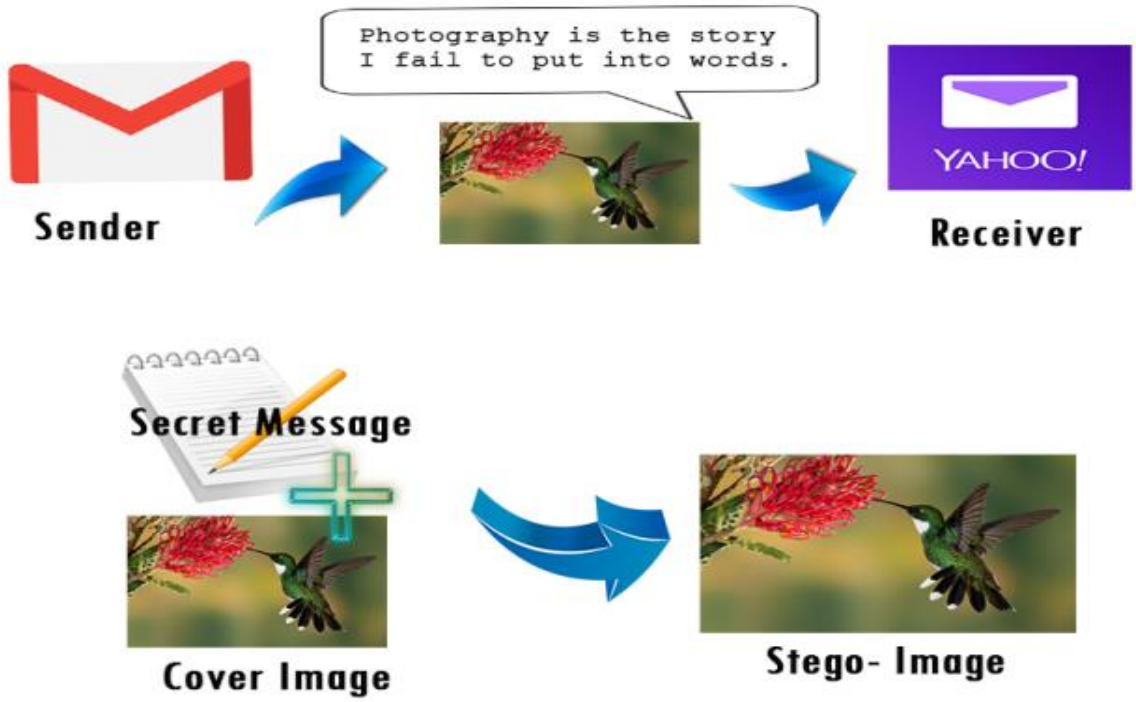

Figure 1.1.2: COMMUNICATION THROUGH IMAGE STEGANOGRAPHY

1.1.3 Literature survey

Authors	Title	Summary
Nannpaneni Manoj kumar M.Praveen kumar M.Srinivasa Roa .	"***Data hiding using Image Steganography"*** -available online at ***www.ijarnd.com***	**Keywords** Steganography, Encryption, Decryption, LSB Array
Hyder Yahya	***"Hide and encryption fingerprint image by using LSB and transposition pixel by spiral method"*** - Published in IJCSMC, vol. 3, pg.624-632, December 2014.	This research paper is about encryption and decryption of fingerprint image using transposition pixel
Yildiray Murat Karabatak.	***"A stenography application for hiding student information into an image"***.	It is aimed to strengthen the LSB technique which is one of the steganography methods.

1.1.4 Methodology

We can describe a digital image as a finite set of digital values, called pixels. Pixels are the smallest individual element of an image, holding values that represent the brightness of a given colour at any specific point. So we can think of an image as a matrix (or a two-dimensional array) of pixels which contains a fixed number of rows and columns.

Least Significant Bit (LSB) is a technique in which the last bit of each pixel is modified and replaced with the secret message's data bit.

- **Stegit**, a graphical user interface.
- **Sqlite3**, a C library that provides a lightweight disk-based database.
- **LSB algorithm**, an algorithm for encoding and decoding images.

1.1.5 Scope of study

This includes

• Image steganography using LSB algorithm.

• A program using PYTHON language.

• Encryption and decryption of images and their access on site.

• Accessing PYTHON library files like Tkinter, stegano, sqlite3.

CHAPTER 2

2.1 DESCRIPTION

2.1.1 What Is Steganography?

Steganography is a Greek word which means concealed writing. The word steganos means covered and graphial means writing. Thus, steganography is not only the art of hiding data but also hiding the fact of transmission of secret data. Steganography hides the secret data in another file in such a way that only the recipient knows the existence of message. In ancient time, the data was protected by hiding it on the back of wax, writing tables, and stomach of rabbits or on the scalp of the slaves. But today's most of the people transmit the data in the form of text, images, video, and audio over the medium. In order to safely transmission of confidential data, the multimedia object like audio, video, images are used as a cover sources to hide the data. Steganography is defined as the study of invisible communication. Steganography usually deals with the ways of hiding the existence of the communicated data in such a way that it remains confidential. It maintains secrecy between two communicating parties. In image steganography, secrecy is achieved by embedding data into cover image and generating a stego-image. There are different types of steganography techniques each have their strengths and weaknesses. In this paper, we review the different security and data hiding techniques that are used to implement a steganography such as LSB, ISB, and MLSB etc.

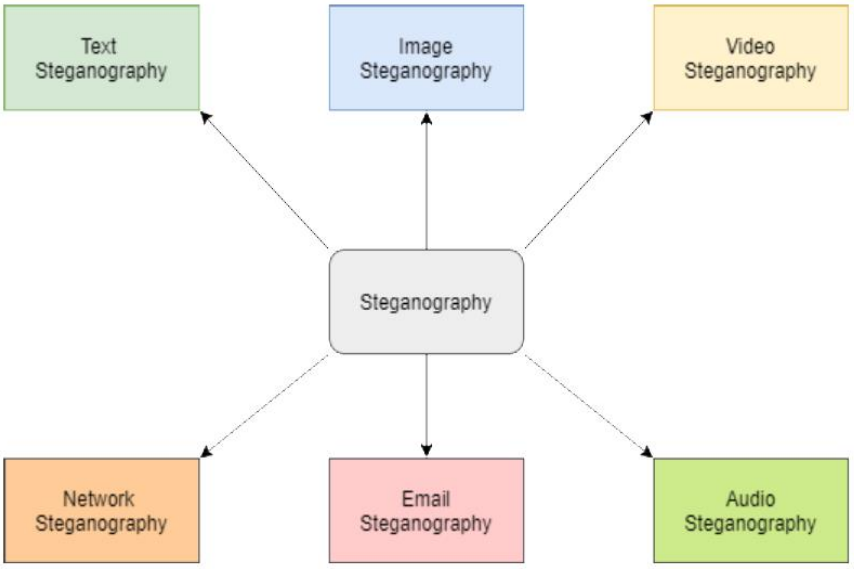

Figure 2.1.1: TYPES OF STEGANOGRAPHY

In today's world, the communication is the basic necessity of every growing area. Everyone wants the secrecy and safety of their communicating data. In our daily life, we use many secure Pathways like internet or telephone for transferring and sharing information, but it's not safe at a certain level. In order to share the information in a concealed manner two techniques could be used. These mechanisms are cryptography and steganography. . In cryptography, the message is modified in an encrypted form with the help of encryption key which is known to sender and receiver only. The message cannot be accessed by anyone without using the encryption key. However, the transmission of encrypted message may easily arouse attacker's suspicion, and the encrypted message may thus be intercepted, attacked or decrypted violently. In order to overcome the shortcomings of cryptographic techniques, steganography techniques have been developed. Steganography is the art and science of communicating in such a way that it hides the existence of the communication. Thus, steganography hides the existence of data so that no one can detect its presence. In steganography the process of hiding information content inside any multimedia content like image, audio, video referred as an Embedding. For increasing confidentiality of communicating data both techniques may combined. Application of Steganeography:

- Confidential Communication
- Protection of Data Alteration
- Access Control System for Digital Content Distribution
- E-Commerce
- Media
- Database Systems.
- Digital watermarking.
- Secret Data Storing

2.1.2 History

The first recorded uses of steganography can be traced back to 440 BC when Herodotus mentions two examples in his Histories.Histiaeus sent a message to his vassal, Aristagoras, by shaving the head of his most trusted servant,"marking" the message onto his scalp, then sending him on his way once his hair had regrown, with the instruction, When thou art come to Miletus, bid Aristagoras shave thy head, and look thereon." Additionally, Demaratus sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax surface. Wax tablets were in common use then as reusable writing surfaces, sometimes used for shorthand. Steganography has been widely used for centuries. Here

are some examples Hidden messages within a wax tablet: in ancient Greece, people wrote messages on wood and covered it with wax that bore an innocent covering message. Hidden messages on messenger's body were also used in ancient Greece. Herodotus tells the story of a message tattooed on the shaved head of a slave of Histiaeus, hidden by the hair that afterwards grew over it, and exposed by shaving the head. The message allegedly carried a warning to Greece about Persian invasion plans. The method has obvious drawbacks, such as delayed transmission while waiting for the slave's hair to grow and restrictions on the number and the size of messages that can be encoded on one person's scalp.

Figure 2.1.2: ANCIENT USE OF STEGANOGRAPHY

Hidden messages on paper written in secret inks, under other messages or on the blank parts of other messages Messages written in Morse code on yarn and then knitted into a piece of clothing worn by a courier. Messages written on envelopes in the area covered by postage stamps. In the early days of the printing press, it was common to mix different typefaces on a printed page because the printer did not have enough copies of some letters in one typeface. Thus, a message could be hidden by using two or more different typefaces, such as normal or italic. During both world wars, female spies used knitted codes so new knitted patterns were banned during both wars.During and after World War II, espionage agents used photographically produced microdots to send information back and forth. Microdots were typically minute (less than the size of the period produced by a typewriter). World War II microdots were embedded in the paper and covered with an adhesive, such as collodion. That was reflective and so was detectable by viewing against glancing light. Alternative techniques included inserting microdots into slits cut into the edge of postcards.

During World War II, Velvalee Dickinson, a spy for Japan in New York City, sent information to accommodation addresses in neutral South America. She was a dealer in dolls, and her letters discussed the quantity and type of doll to ship. The stegotext was the doll orders, and the concealed"plaintext" was itself encoded and gave information about ship movements, etc. Her case became somewhat famous and she became known as the Doll Woman. During World War II, photosensitive glass was declared secret, and used for transmitting information to Allied armies. Jeremiah Denton repeatedly blinked his eyes in Morse code during the 1966 televised press conference that he was forced into as an American prisoner-of-war by his North Vietnamese captors, spelling out "T-O-R-T-U-R-E". That confirmed for the first time to the US Naval Intelligence and other Americans that the North Vietnamese were torturing American prisoners-of-war. In 1968, crew members of the USS Pueblo intelligence ship, held as prisoners by North Korea, communicated in sign language during staged photo opportunities, to inform the United States that they were not defectors but captives of the North Koreans. In other photos presented to the US, crew members gave "the finger" to the unsuspecting North Koreans, in an attempt to discredit photos that showed them smiling and comfortable.

2.2 Types of Steganography

2.2.1 Text Steganography

It consists of hiding information inside the text files. In this method, the secret data is hidden behind every nth letter of every words of text message. Numbers of methods are available for hiding data in text file. These methods are:

i) Format Based Method
ii) Random and Statistical Method
iii) Linguistics Method

Text steganography can be achieved by altering the text formatting, or by altering certain characteristics of textual elements (e.g., characters). The goal in the design of coding methods is to develop alterations that are reliably decodable (even in the presence of noise) yet largely indiscernible to the reader. These criteria, reliable decoding and minimum visible change, are somewhat conflicting; herein lies the challenge in designing document marking techniques. The three coding techniques that we propose illustrate different approaches rather than form an exhaustive list of document marking techniques. The techniques can be used either separately or jointly. These are following:

1. Line-Shift Coding: This is a method of altering a document by vertically shifting the locations of text lines to encode the document uniquely.

2. Word-Shift Coding: This is a method of altering a document by horizontally shifting the locations of words within text lines to encode the document uniquely.

3. Feature Coding: This is a coding method that is applied either to a format file or to a bitmap image of a document.

2.2.2 Image Steganography

Hiding the data by taking the cover object as image is referred as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital representation of an image.

2.2.3 Audio Steganography

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods are available for audio steganography. We are going to have a brief introduction on some of them. It involves hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography. These methods are

i) Low Bit Encoding

ii) Phase Coding

iii) Spread Spectrum.

2.2.4 Video Steganography

It is a technique of hiding any kind of files or data into digital video format. In this case video (combination of pictures) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography.

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.

CHAPTER 3

3.1 TECHNICAL DISCUSSION

In the current project image steganography is dealt with using data hiding.

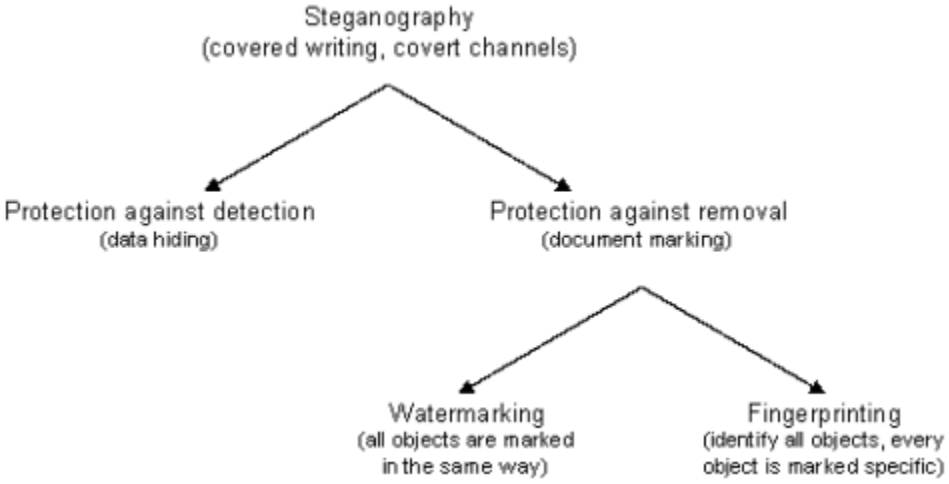

Figure 3.1: VARIOUS USE OF STEGANOGRAPHY

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.

3.1.1 Least significant bit (LSB) method

This 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 colour (RGB-red, green, blue) image, each pixel requires 24 bits (8bits for each layer).

The Human visual system (HVS) cannot detect changes in the colour 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

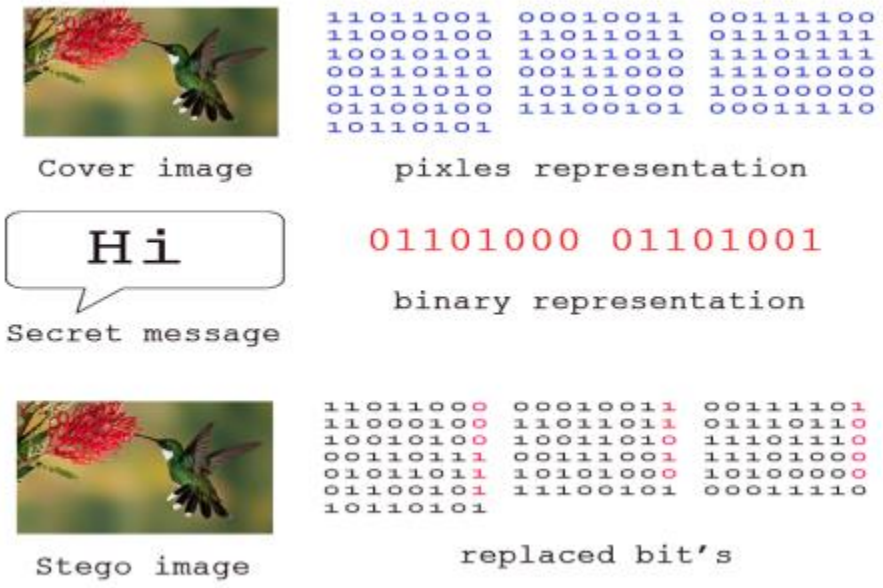

Figure 3.1.1: LSB ALGORITHM AND PROCESS

Steps used in LSB steganography:

a. Steps for hiding message image:

1. Read the image to be used as cover image. Noise is added to make it easier to disguise changes due to embedding the message image.

2. Read the image to be sued as message image.

3. Separate the bit planes of each image.

As it is known that the LSB (least significant bit) plane contains the least information associated with any image, and the MSB (most significant bit) plane contains most of the shape, colour information of an image. It is generally ideal to replace up to 4 least bitplanes of the cover image, with the upper 4 biplanes without revealing changes in the resultant image. Lesser number of

biplanes from the message image could be used, but the retrieved image would become distorted and loses information.

4. Replace the least 4 biplanes of cover image with the 4 most significant biplanes from message image.

5. Get the resultant Steganographic image by recombining these bitplanes.

b. Retrieving message image:

1. Read the Steganographic image.
2. Extract the required number of bitplanes of the image.
3. Recombining the lower four bitplanes would give the retrieved message image.

3.1.2 Discrete Cosine Transform (DCT) method:

When information is embedded in spatial domain, losses can occur such as when the image is cropped etc. To overcome this problem the information is embedded in frequency domain in such a way that we embed the secret information in the significant frequency values and omit the higher frequency part. First the required transformations are applied and then accordingly to hide the secret message, the transform coefficients are changed.

Like in other transforms, decorrelation of the image data is required after applying discrete cosine transform (DCT). And encoding can be then done independently for each coefficient. Hence, compression efficiency is not lost.

In blocking method, blocks of the image are considered and DCT (discrete cosine transform) is done in order to break them. Each block is then subdivided into 64 parts (DCT coefficients). These coefficients are modified i.e. the colour gets modified a little by storing some text or another image in it. Embedding the secret data in the carrier image is generally done for the DCT coefficients that are lower than the chosen threshold value. But embedding information in DCT coefficient value 0 is avoided as this may lead to visual distortion of the cover image.

CHAPTER 4

4.1 SYSTEM DESIGN

4.1.1 Working process of the model:

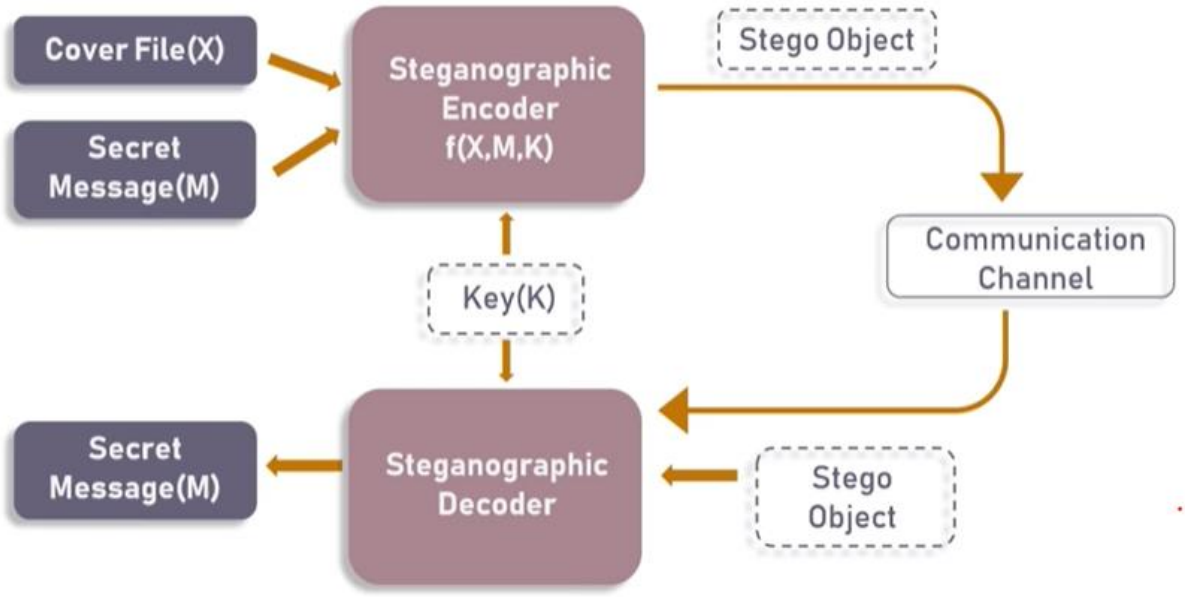

Figure 4.1.1: WORKING MODEL OF IMAGE STEGANOGRAPHY

A Use Case Diagram at its simplest is a representation of a user's interaction with the system. First user writes secret text then he selects cover image and data gets hidden inside image, then user sends stego image to receiver through image. At the receiver side, user selects the stego image and applies decryption on stego image. After that he can get text hidden in the text.

4.1.2 Activity Diagram

Purpose: An example of UML activity diagram describing behaviour of the Stego System for Secure Communication.

Summary: Activity is started by opening stegit software. Stegit software asks for authentication by entering username and passwords. If username and passwords are correct Stegit software authenticates user. Three options get available front of user as

1. Encode 2. Decode 3.Share

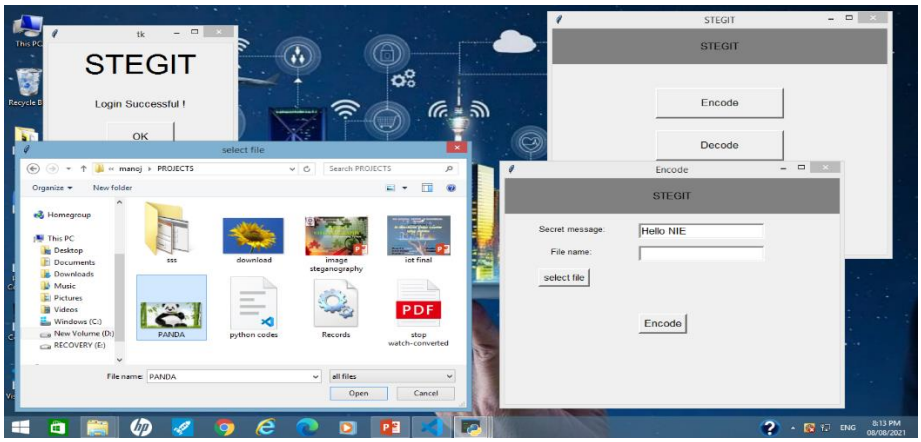

Figure 4.1.2(A): SYSTEM IMPLEMENTATION OF PROGRAM

• User can generate stegit image by hiding secret data in it

• User can get his secret code by decoding image.

• User can send stegit image to another user by share option.

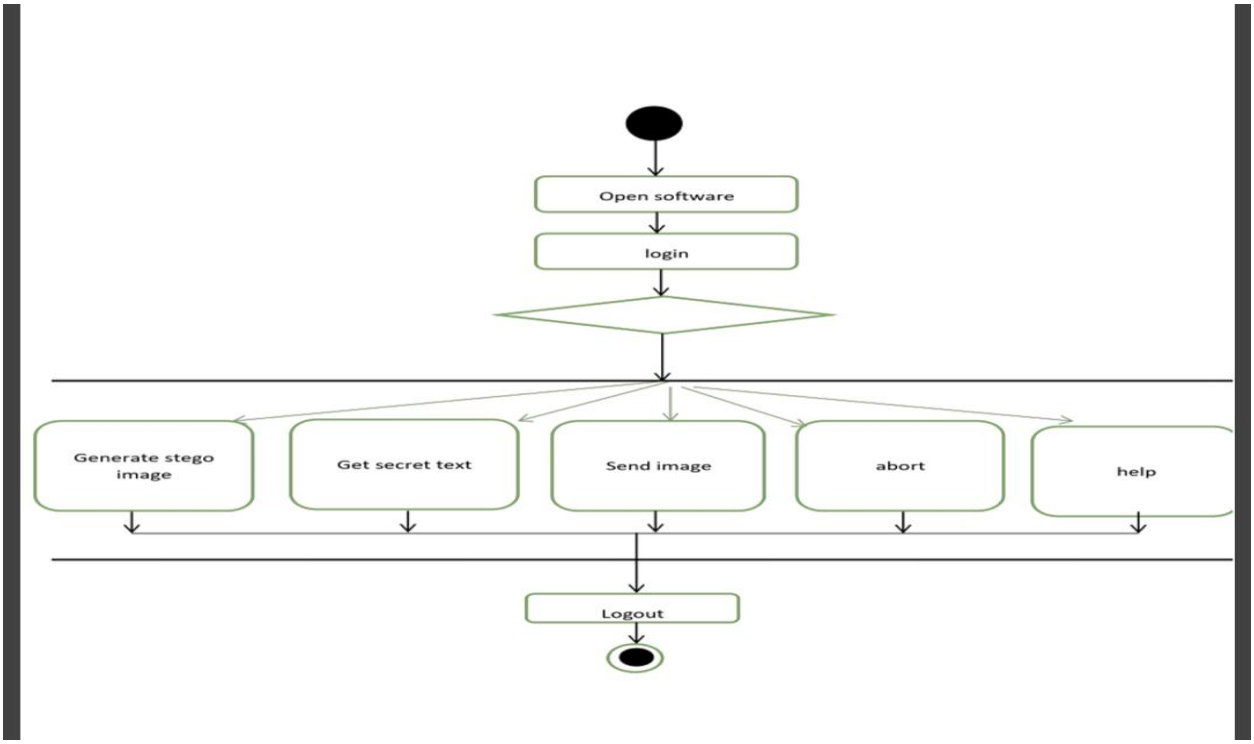

Figure 4.1.2(B): ACTIVITY DIAGRAM

CHAPTER 5

5.1 APPLICATION OF SYSTEM

5.1.1 Advantages

- The main advantages of this system is Security that it provides security to your messages without knowing to third party.
- Number of bits have been replaced according to user or sender, therefore third party cannot quess password.
- Normal network user can't guess image.
- In steganography anyone can't jump on suspect by looking images.
- It is Reliable.
- Easy to use.
- Easy Maintenance.
- System have been secured by password authentication.

5.1.2 Disadvantages

- Images can have attacks like diluting, nosing, contrast changes and so on.
- Number bits of pixel should be replaced by equal bits of message.
- If someone is eavesdropping then then there is probability of message get unfold.
- If more than two people having same steganography software then hidden massage can acquire.
- This software has been implemented by python, which is open source, therefore code is readable so anyone with bad mentality can make software perform inverse operation.
- Only unintended user may know the actual working of software.
- Intruder may penetrate suspecting images to get hidden data.

5.1.3 Application

- Confidential Communication and Secret Data Storing.
- Protection of Data Alteration.
- Access Control System for Digital Content Distribution.
- E-Commerce.
- Media.
- Database Systems.
- Digital Watermarking.

CHAPTER 6

6.1 ANALYSIS

6.1.1 Result

After the encryption and decryption, the images and the final results looks like:

There will be no change in resolution or clarity of the pic but the encrypted image contains the secret message for the secured communication.

Figure 6.1.1(a): IMAGE PANDA

Figure 6.1.1(b): ENCYPTED IMAGE PANDA

6.1.2 CONCLUSION

It is observed that through LSB Substitution Steganographic method, the results obtained in data hiding are pretty impressive as it utilizes the simple fact that any image could be broken up to individual bit-planes each consisting of different levels of information. It is to be noted that as discussed earlier, this method is only effective for bitmap images as these involve lossless compression techniques. Also, in this project grey-scale images have been used for demonstration. But this process can also be extended to be used for colour images where, bit plane slicing is to be done individually for the top four bit-planes for each of R, G, B of the message image, which are again to be placed in the R, G, B planes of the cover image, and extraction is done similarly.

It is also important to discuss that though steganography was once undetected, with the various methods currently used, it is not only easy to detect the presence but also retrieving them is easier. For instance, without having to use a software or complex tools for detection, simple methods to observe if an image file has been manipulated are:

1. **Size of the image:** A Steganographic image has a huge storage size when compared to a regular image of the same dimensions. I.e. if the original image storage size would be few KBs, the Steganographic image could be several MBs in size. This again varies with the resolution and type of image used.

2. **Noise in image:** A Steganographic image has noise when compared to a regular image. This is the reason why initially little noise is added to the cover image, so that the Steganographic image doesn't appear very noisy when compared to the original cover image.

Though this project focusses on LSB and spatial domain steganography, few details about transform domain methods have also been researched, basics of which have been discussed. So through the various articles and theory available, it is observed that transform domain methods perform better in comparison with spatial domain methods.

6.1.3 FUTURE SCOPE

Steganography, though is still a fairly new idea. There are constant advancements in the computer field, suggesting advancements in the field of steganography as well. It is likely that there will soon be more efficient and more advanced techniques for Steganalysis. A hopeful advancement is the improved sensitivity to small messages. Knowing how difficult it is to detect the presence of a fairly large text file within an image, imagine how difficult it is to detect even one or two sentences embedded in an image! It is like finding a microscopic needle in the ultimate haystack. What is scary is that such a small file of only one or two sentences may be all that is needed to commence a terrorist attack. In the future, it is hoped that the technique of Steganalysis will advance such that it will become much easier to detect even small messages within an image. In this work it explores only a small part of the science of steganography. As a new discipline, there is a great deal more research and development to do. The following section describe areas for research which were offshoots of, or tangential to, our main objectives.

1. **Detecting Steganography in Image Files:** Can steganography be detected in images files? This is difficult question. It may be possible to detect a simple Steganographic technique by simple analysing the low order bits of the image bytes. If the Steganographic algorithm is more complex, however, and spreads the embedded data over the image is random way or encrypts the data before embedding, it may be nearly impossible to detect.

2. **Steganography on the World Wide Web:** The world wide web (www) makes extensive use of inline images.There are literally millions of images on various web pages worldwide. It may be possible to develop an application to serve as a web browser to retrieve

data embedded in web page images. This stego-web could operate on top of the existing WWW and be a means of covertly disseminating information.

3. **Steganography in printed media:** If the data is embedded in an image, the image printed, then scanned and stored in a file can the embedded data be recovered? This would require a special form of a steganography to which could allow for in accuracies in the printing and scanning equipment

6.1.4 REFERENCES

1. Johnson, Neil F. "Steganography." Http://www.jjtc.com/pub/tr_95_11_nfj/sec101.html. N.p., Nov. 1995. Web.

2. Shikha, and Vidhu Kiran Dutt. "International Journal of Advanced Research in Computer Science and Software Engineering." Http://www.ijarcsse.com/. N.p., Sept. 2014. Web.

3. Niels Provos, and Peter Honeyman. “Hide and Seek: An Introduction to Steganography.” IEEE Security & Privacy Magazine, May-June 2013. Web.

4. Nick Nabavian. “Image steganography” Nov. 28, 2007. http://www1.chapman.edu/~nabav100/ImgStegano/download/ImageSteganography.p df

5. Dr Ekta Walia, Payal Jain and Navdeep. “An analysis of LSB & DCT based Steganography.” Global Journal of Computer Science and Technology, April2010. https://globaljournals.org/GJCST_Volume10/gjcst_vol10_issue_1_paper8.pdf

6. Deepak Singla, and Rupali Syal. "International Journal of Computational Engineering Research." Citeseerx.ist.psu.edu. N.p., Mar-Apr. 2012. Web.

7. Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, Information Hiding-A Survey, IEEE, special issue on protection of multimedia content, Jul 1999, 1062-1078.