



Image And Audio Steganography

A Report for the Evaluation 3 of Project 2

Submitted by

SHOBHIT MEHTA

(1613114046/16SCSE114013)

in partial fulfilment for the award of the degree

of

BACHELOR OF TECHNOLOGY

IN

**COMPUTER SCIENCE AND ENGINEERING WITH SPECIALIZATION
OF**

COMPUTER NETWORK AND CYBER SECURITY

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING

**Under the Supervision of
Dr. S. RAKESH KUMAR
ASSISTANT Professor**

APRIL / MAY- 2020



**SCHOOL OF COMPUTING AND SCIENCE AND
ENGINEERING**

BONAFIDE CERTIFICATE

Certified that this project report “Image And Audio Steganography” is the bonafide work of “SHOBHIT MEHTA(16SCSE114013)” who carried out the project work under my supervision.

SIGNATURE OF HEAD

**Dr. MUNISH SHABARWAL,
PhD (Management), PhD (CS)
Professor & Dean,
School of Computing Science &
Engineering**

SIGNATURE OF SUPERVISOR

**Mr. S. RAKESH KUMAR,
M.Tech.,
Assistant Professor
School of Computing Science &
Engineering**

ABSTRACT

Security of data is of real importance in today's world. Innovation of technology and having fast internet make information to distribute over the world easily and economically. This has made people to worry about their data and privacy. Thus there is need to develop a way for secure transmission of data so that the data which is transferred from one point reaches to another point without any compromise. In order to address this problem various methods are developed one of them is Steganography. For highly secure, hidden communication and sharing of data Steganography is used. Steganography is basically communication of secret data in an appropriate multimedia carrier like image, audio and video files. It comes under the assumption that if feature is visible the point of attack is evident, thus the goal here is always to conceal the very existence of embedded data. In this paper the main emphasis is given to educate the people about various steganography techniques, their application and the latest advancement in the field keeping in view the security aspect also.

Table Of Contents

<u>1</u>	<u>INTRODUCTION</u>	1
<u>1.1</u>	What Is Steganography?	1
<u>1.2</u>	History	3
<u>2</u>	<u>LITERATURE REVIEW</u>	5
<u>2.1</u>	Cryptography Basics	5
<u>2.2</u>	Basics Of Steganography	7
<u>2.3</u>	Steganography With LSB Algorithm	7
<u>3</u>	<u>REQUIREMENTS ANALYSIS</u>	8
<u>3.1</u>	Functional Requirements	8
<u>3.2</u>	Non-Functional Requirements	8
<u>3.3</u>	System Requirements	9
3.3.1	Software Requirements	9
3.3.2	Hardware Requirements	9
<u>4</u>	<u>IMAGE STEGANOGRAPHY</u>	10
<u>4.1</u>	Types of Steganography	10
4.1.1	Text Steganography	10
4.1.2	Image Steganography	11
4.1.3	Audio Steganography	11
4.1.4	Video Steganography	11
<u>4.2</u>	STEGANOGRAPHY IN IMAGE	11
<u>5</u>	<u>HOW IT WORKS?</u>	14
<u>5.1</u>	Implementation	14
5.1.1	Technical Details	14
5.1.2	The Encoding Process	14

5.1.3 Creation of User Space	14
5.1.4 The Decoding Process	15
6 BRIEF ALGORITHM IMPLEMENTATION	16
<u>6.1</u> LSB(Least Signi cant Bit)	16
6.1.1 Spatial Method	16
6.1.2 Masking and ltering	20
7 <u>SYSTEM DESIGN</u>	21
<u>7.1</u> Usecase Diagram	21
<u>7.2</u> Activity Diagram	23
<u>7.3</u> Class Diagram	25
<u>7.4</u> State Chart Diagram	26
<u>7.5</u> Sequence Diagram	27
8 <u>SYSTEM IMPLEMENTATION</u>	28
9 <u>APPLICATION OF SYSTEM</u>	34
<u>9.1</u> Advantages	34
<u>9.2</u> Disadvantages_.....	34
<u>9.3</u> Application	35
<u>10 FUTURE SCOPE</u>	36

List of Figures

1.1 PORCESS OF STEGANOGRAPHY	2
4.1 COMMUNICATION THROUGH STEGANOGRAPHY	12
5.1 LSB Operation	15
6.1 Encryption Diagram	19
6.2 Decryption Diagram	20
7.1 Usecase Diagram	21
7.2 Activity Diagram	23
7.3 Class Diagram	25
7.4 State Chart Diagram	26
7.5 Sequence Diagram	27
8.1 REQUIREMENTS	29
8.2 MENU	30
8.3 A.TXT	31
8.4 ENCODE	32
8.5 DECODE	33

Chapter 1

INTRODUCTION

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, 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, MLSB etc.

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 attackers suspicion, and the encrypted message may thus be intercepted, attacked or decrypted violently.

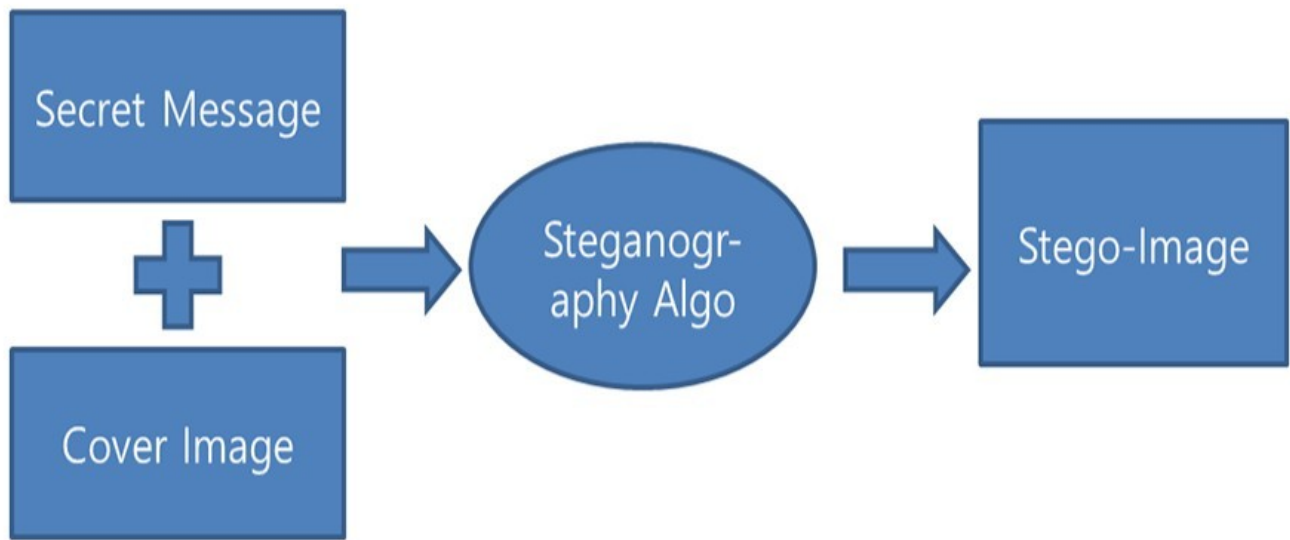


Figure 1.1: PORCESS OF STEGANOGRAPHY

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 a Embedding. For increasing con dentiality of communicating data both techniques may combined. Application of Steganeography:

- i)Con dential Communication
- ii) Protection of Data Alteration
- iii) Access Control System for Digital Content Distribution
- iv) E-Commerce
- v) Media
- vi) Database Systems
- vii) Digital watermarking
- viii) Secret Data Storing

1.2 History

The 1st 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.

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.

Chapter 2

LITERATURE REVIEW

Electronic communication is the lifeblood of many organizations.

Much of the information communicated on a daily basis must be kept confidential. Information such as financial reports, employee data and medical records needs to be communicated in a way that ensures confidentiality and integrity. This makes good business sense and may even be regulated by legislation like the Health Insurance Portability and Accountability Act (HIPAA). The problem of unsecure communication is compounded by the fact that much of this information is sent over the public Internet and may be processed by third parties, as in e-mail or instant messaging (IM).

2.1 Cryptography Basics

Cryptography can be used to provide message confidentiality and integrity and sender verification. The basic functions of cryptography are encryption, decryption and cryptographic hashing. In order to encrypt and decrypt messages, the sender and recipient need to share a secret. Typically this is a key, like a password, that is used by the cryptographic algorithm. The key is used by the sender to encrypt the message (transform it into cipher text) and by the recipient to decrypt the message (reverse the cipher text back to clear text). This process can be done on a fixed message, such as an e-mail, or a communications stream, such as a TCP/IP connection. Cryptographic hashing is the process of generating a fixed-length string from a message of arbitrary length. If the sender provides a cryptographic hash with the message, the recipient can verify its integrity. Modern cryptographic systems are based on complex mathematical relationships and processes. Let's focus on the common cryptography standards used to secure computer communications and how they are used. The three basic types of cryptography in common use are symmetric key, asymmetric (public) key systems and cryptographic hash functions. Typically, the strength of a crypto system is directly related to the length of the key.

The three basic types of cryptography in common use are symmetric key, asymmetric (public) key systems and cryptographic hash functions. Typically, the strength of a crypto system is directly related to the length of the key. This assumes that there is no inherent weakness in the algorithm and that the keys are chosen in a way that fully utilizes the key space (the number of possible keys). There are many kinds of attacks that can be used against crypto systems, but these are beyond our scope here. That said, if you use public algorithms with no known vulnerabilities, use reasonable key lengths (most defaults are ne) and choose good keys (which are normally chosen for you), your communications will be very secure. Cryptography Drawbacks

Apart from the four fundamental elements of information security, there are other issues that affect the effective use of information:

A strongly encrypted, authentic, and digitally signed information can be difficult to access even for a legitimate user at a crucial time of decision-making. The network or the computer system can be attacked and rendered non-functional by an intruder.

High availability, one of the fundamental aspects of information security, cannot be ensured through the use of cryptography. Other methods are needed to guard against the threats such as denial of service or complete breakdown of information system.

Another fundamental need of information security of selective access control also cannot be realized through the use of cryptography. Administrative controls and procedures are required to be exercised for the same.

Cryptography does not guard against the vulnerabilities and threats that emerge from the poor design of systems, protocols, and procedures. These need to be fixed through proper design and setting up of a defensive infrastructure.

Cryptography comes at cost. The cost is in terms of time and money

1. Addition of cryptographic techniques in the information processing leads to delay.
2. The use of public key cryptography requires setting up and maintenance of public key infrastructure requiring the handsome nancial budget.

The security of cryptographic technique is based on the computational difficulty of mathematical problems. Any breakthrough in solving such mathematical problems or increasing the computing power can render a cryptographic technique vulnerable.

2.2 Basics Of Steganography

Steganography aims to hiding information in a cover data in such a way that non-participating persons are not able to detect the presence of this information by analyzing the information detection. Unlike watermarking, steganography does not intended to prevent the hidden information by opponents of removing or changing the hidden message, which is embedded in the cover data but it emphasizes on remains it undetectable. Steganography is particularly interesting for applications in which the encryption can not used to protect the communication of confidential information.

2.3 Steganography With LSB Algorithm

bytes of pixels are sufficient to hold one message byte. Rest of the bits in the pixels remains the same. Steganography is the art and science of communicating in a way which hides the existence of the communication. Steganography plays an important role in information security. It is the art of invisible communication by concealing information inside other information. The term steganography is derived from Greek and literally means covered writing. A Steganography system consists of three elements: coverimage (which hides the secret message), the secret message and the stegano-image (which is the cover object with message embedded inside it). A digital image is described using a 2-D matrix of the color intensities at each grid point (i.e. pixel). Typically gray images use 8 bits, whereas colored utilizes 24 bits to describe the color model, such as RGB model. The Steganography system which uses an image as the cover, there are several techniques to conceal information inside cover-image. The spatial domain techniques manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. Consequently, the spatial domain techniques are simple and easy to implement. The Least Significant Bit (LSB) is one of the main techniques in spatial domain image Steganography.

The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision. Therefore, an altered image with slight variations in its colors will be indistinguishable from the original by a human being, just by looking at it. In conventional LSB technique, which requires eight bytes of pixels to store 1 byte of secret data but in proposed LSB technique.

Chapter 3

REQUIREMENTS ANALYSIS

3.1 Functional Requirements

Functional requirements are the requirements that that define specific behavior or function of the system.

Login: Login function will authenticate the sender if username and password are correct. Otherwise it will exit the system.

Secret Text Message File: In this file you will have to write secret message to hide or you can select any text file of secret message.

Cover Image: Cover Image is the image is to be selected in which secret text message can be hidden.

Stego Encryption LSB implementation is performed on cover image to hide secret text message by replacing bits of cover image by the bits of message.

Sender In this Sender send this stego image file to intended recipient to which he does want to communicate.

Receiver In this receiver receives the stego image and opens in decryption option for getting hidden text message inside that image.

3.2 Non-Functional Requirements

Safety Requirements:

Sender and Receiver should make sure that only they are having the same software to encrypt and decrypt data inside image. Both should take care of eavesdropping.

Security Requirements:

We are going to develop a software in which embedding secret text data in image. Only sender and receiver should be aware of encrypted le. User should not unfold the message regarding sent image as well as receiver information.

Software Quality Attributes:

The Quality of the software is maintained in such a way that only sender and receiver can communicate through image. There is no probability of knowing secret image.

3.3 System Requirements

3.3.1 Software Requirements

Operating System: Linux Debian

based OS.

Front End :Python.

Tool:Python3.0

PhotoshopCC.

3.3.2 Hardware Requirements

INTEL I5 2.50 GHZ 4 GB RAM

Minimum Hardware Requirement:

Pentium 3 166 MHZ Or Higher 128 mb RAM

Chapter 4

IMAGE STEGANOGRAPHY

4.1 Types of Steganography

4.1.1 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 word of text message. Numbers of methods are available for hiding data in text files. 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 text file or to a bitmap image of a document.

4.1.2 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.

4.1.3 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.

4.1.4 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 normally display only the cover data. So it cannot be detected easily to be containing hidden information unless proper decryption is used.

4.2 STEGANOGRAPHY IN IMAGE

Hiding information inside images is a popular technique nowadays. An image with a secret message inside can easily be spread over the World Wide Web or in newsgroups. The use of steganography in newsgroups has been researched by German steganographic expert Niels

Provos, who created a scanning cluster which detects the presence of hidden messages inside images that were posted on the net. However, after checking one million images, no hidden messages were found, so the practical use of steganography still seems to be limited. Image Steganography is the technique of hiding the data within the image in such a way that prevents the unintended user from the detection of the hidden messages or data.

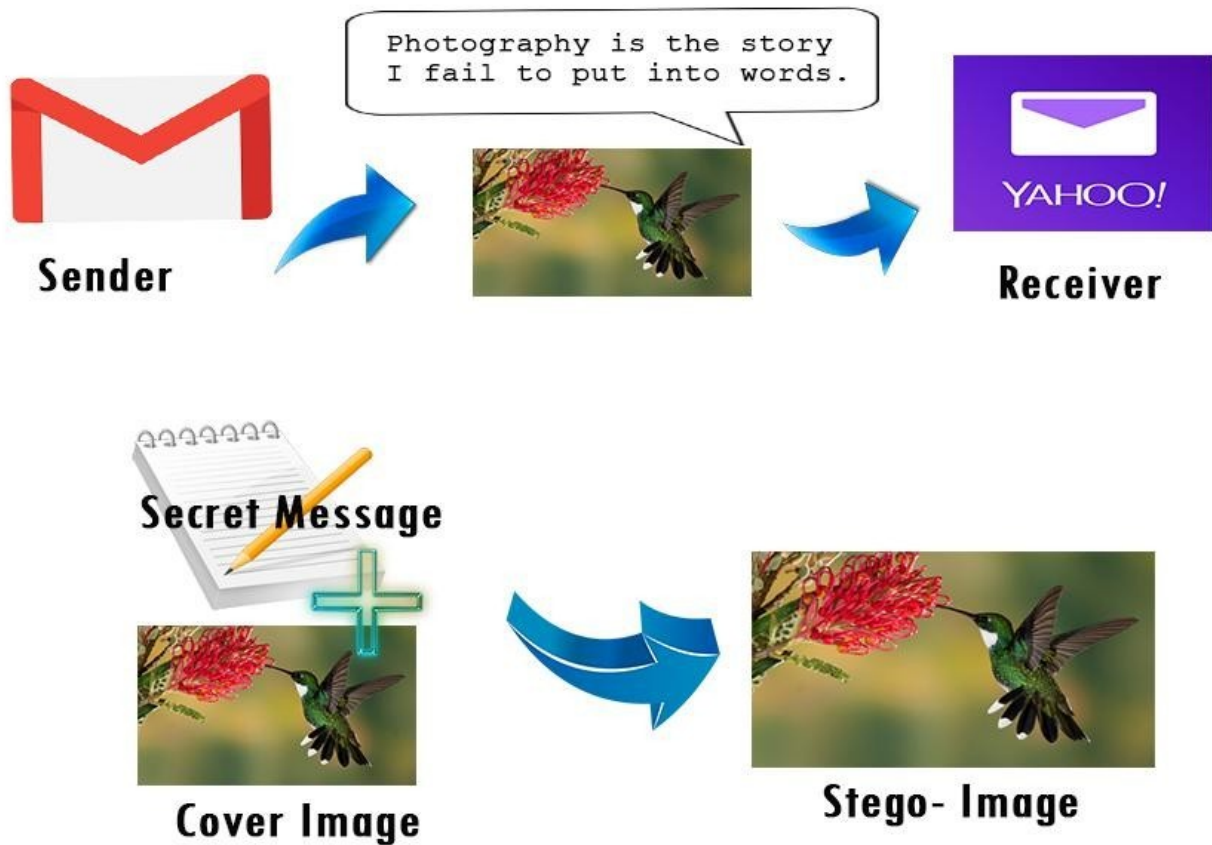


Figure 4.1: COMMUNICATION THROUGH STEGANOGRAPHY

To hide a message inside an image without changing its visible properties, the cover source can be altered in noisy areas with many color variations, so less attention will be drawn to the modifications. The most common methods to make these alterations involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image. These techniques can be used with varying degrees of success on different types of images. The project deals with learning about the various types of steganography available. Image steganography is performed for images and the concerning data is also decrypted to retrieve the message image. Since this can be done in several ways, image steganography is studied and one of the methods is used to demonstrate it. Image steganography refers to hiding information i.e. text, images or audio files in another image or video files. The current project aims to use

steganography for an image with another image using spatial domain technique. This hidden information can be retrieved only through proper decoding technique. This encryption and decryption of the images is done using java codes.

Chapter 5

HOW IT WORKS?

5.1 Implementation

5.1.1 Technical Details

- o Using `java.awt.Image`, `ImageIO`
- o The package contains all the necessary classes and methods along with interfaces that are necessary for the manipulation of the images.

5.1.2 The Encoding Process

The steganography technique used is LSB coding. The offset of the image is retrieved from its header. That offset is left as it is to preserve the integrity of the header, and from the next byte, we start our encoding process. For encoding, we first take the input carrier file i.e. an image file and then direct the user to the selection of the text file.

5.1.3 Creation of User Space

- o User Space is created for preserving the original file, so that all the modifications are done in the user space.
- o In the object of `Bu eredImage`, using `ImageIO.read` method we take the original image.
- o Using `createGraphics` and `drawRenderedImage` method of `Graphics` class, we create our user space in `Bu eredImage` object.

The text file is taken as input and separated in stream of bytes. Now, each bit of these bytes is encoded in the LSB of each next pixel. And, finally we get the final image that contains the encoded message and it is saved, at the specified path given by user, in PNG format using



Figure 5.1: LSB Operation

ImageIO.write method. This completes the encoding process.

5.1.4 The Decoding Process

The color set of the image is retrieved from its header. Create the user space using the same process as in the Encoding. Using getRaster() and getDataBuffer() methods of Writable Raster and DataBufferByte classes. The data of image is taken into byte array. Using above byte array, the bit stream of original text file is retrieved into the another byte array. And above byte array is written into the decoded text file, which leads to the original message.

Chapter 6

BRIEF ALGORITHM IMPLEMENTATION

6.1 LSB(Least Significant Bit)

There are two different methods for image steganography:

1. Spatial methods
2. Transform methods

But we are using Spatial Methods.

6.1.1 Spatial Method

In spatial method, the most common method used is LSB substitution method. Least significant bit (LSB) method is a common, simple approach to embedding information in a cover image. 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.

Algorithm of LSB method of steganography. There might be two different phases of LSB method, embedding phase and extracting phase. Algorithms of both of the phases are given below:

A. Embedding phase Procedure:

Step 1: Extract all the pixels from the given image and store them in some array named (imagearray).

Step 2: Extract all the characters from the given text (message) and store it in the array called (messagearray).

Step 3: Retrieve the characters from the Stego key and store them in an array called Keyarray. A stego-key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data.

Step 4: Take first pixel and characters from Key-array and place it in first component of pixel. If there are more characters in Key array, then place rest in the first component of next pixels.

Step 5: Place some terminating symbol to indicate end of the key. 0 has been used as a terminating symbol in this algorithm.

Step 6: Place characters of message Array in each component of next pixels by replacing it.

Step 7: Repeat step 6 till all the characters have been embedded.

Step 8: Again place some terminating symbol to indicate end of data.

Step 9: Obtained image will hide all the characters that input.

The simplest steganography techniques embed the bits of the message directly into the 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. To hide a secret message inside an image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel. For example, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

When the character A, which binary value equals 10000001, is inserted, the following grid results:

(00100111 11101000 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)

In this case, only three bits needed to be changed to insert the character successfully. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximal cover size. The result changes that are made to the least significant bits are too small to be recognized by the human visual system (HVS), so the message is effectively hidden. As you see, the least significant bit of third color is remained without any changes. It can be used for checking the correctness of 8 bits which are embedded in these 3 pixels. In other words, it could be used as parity bit.

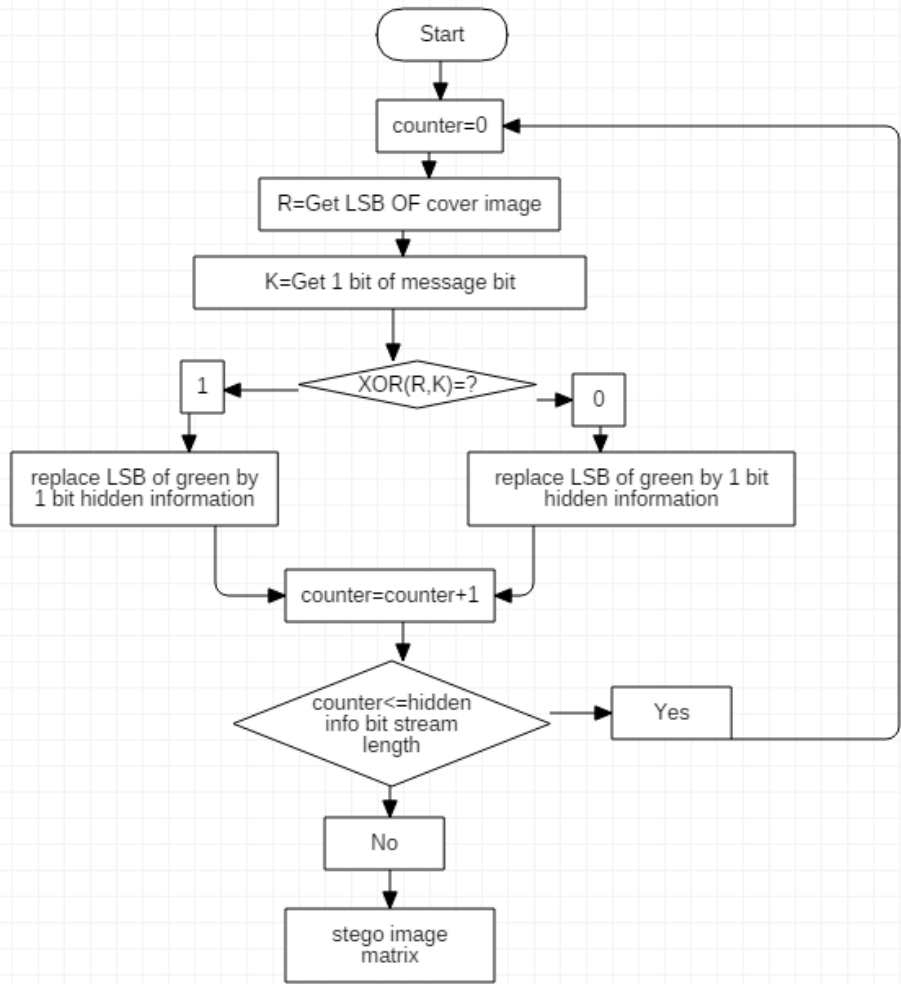


Figure 6.1: Encryption Diagram

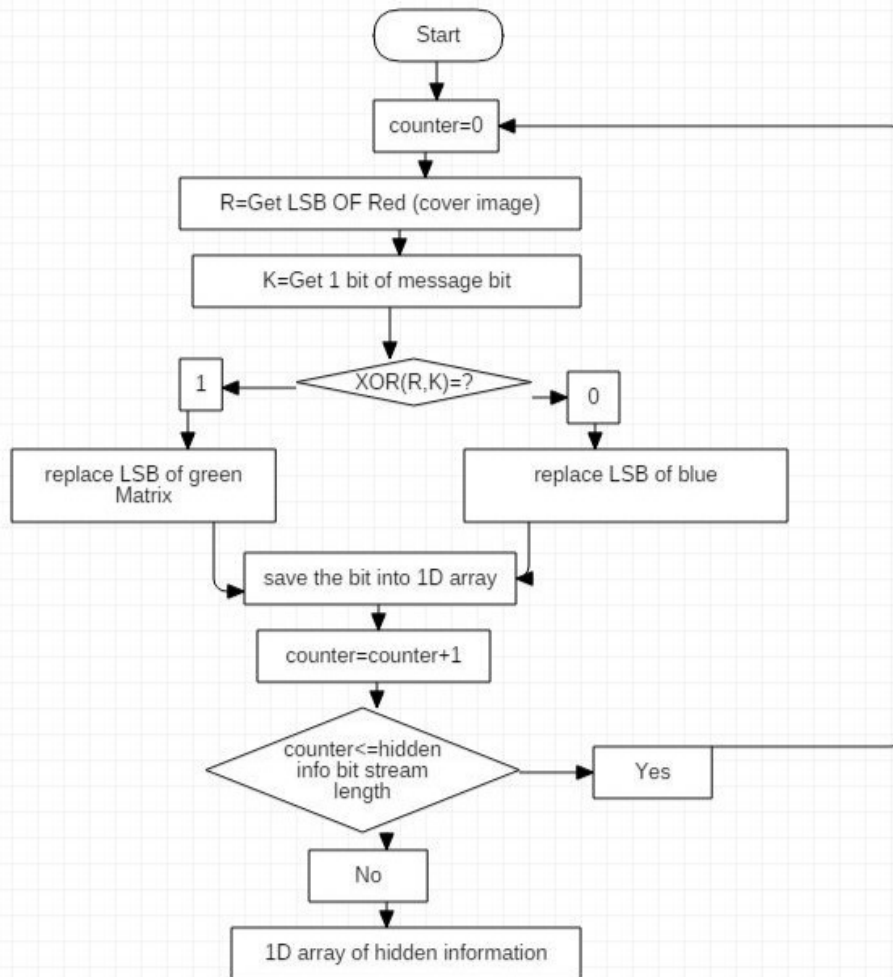


Figure 6.2: Decryption Diagram

6.1.2 Masking and Itering

Masking and Itering techniques, usually restricted to 24 bits or grayscale images, take a different approach to hiding a message. These methods are effectively similar to paper watermarks, creating markings in an image. This can be achieved for example by modifying the luminance of parts of the image. While masking does change the visible properties of an image, it can be done in such a way that the human eye will not notice the anomalies. Since masking uses visible aspects of the image, it is more robust than LSB modification with respect to compression, cropping and different kinds of image processing. The information is not hidden at the noise level but is inside the visible part of the image, which makes it more suitable than LSB modifications in case a lossy compression algorithm like JPEG is being used.

Chapter 7

SYSTEM DESIGN

7.1 Usecase Diagram

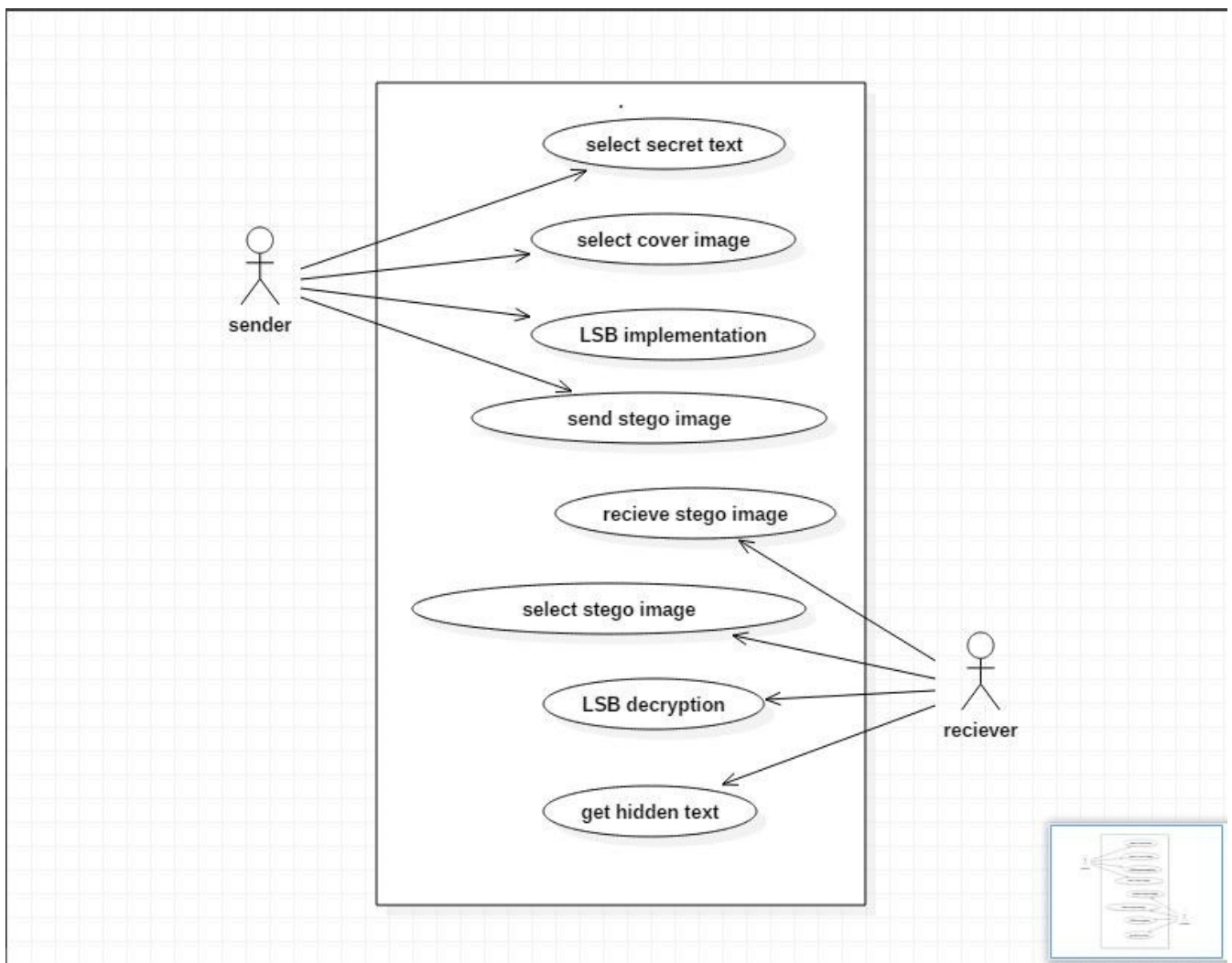


Figure 7.1: Usecase Diagram

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.

7.2 Activity Diagram

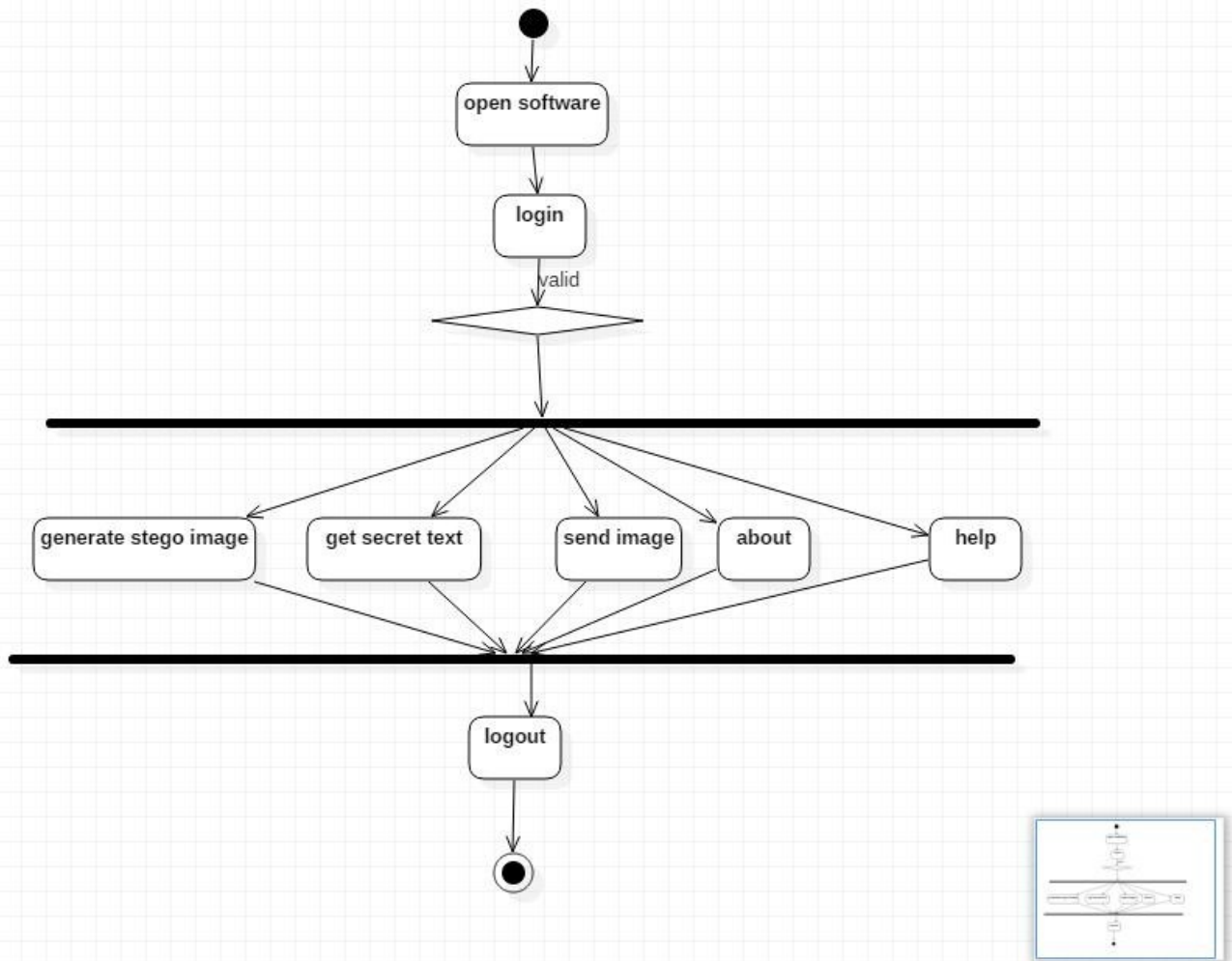


Figure 7.2: Activity Diagram

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

Summary: Activity is started by opening stego software. Stego software asks for authentication by entering username and passwords. If username and passwords are correct Stego software authenticates user. Four options get available front of user as 1. Generate stego image. 2. Get secret code. 3. Send image 4. About 5. Help.

User can generate stego image by hiding secret data in it.

User can get his secret code by decoding image.

User can send stego image to another user by send image option. User can know about software by clicking on about option.

User can look for help in case he needs it.

User can terminate stego software by clicking on log out.

7.3 Class Diagram

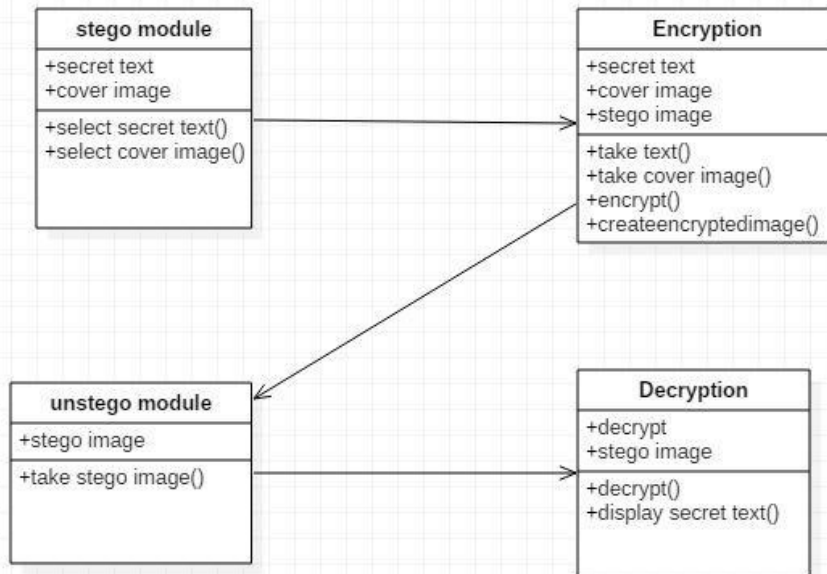


Figure 7.3: Class Diagram

There are four following classes:

1. Stego module
2. Encryption
3. Unstego module
4. Decryption

Stego module: secret module consists of two attributes secret text and cover image as well as two operations as select secret text() and select cover image().

Encryption: Encryption is the process of hiding secret text into cover image.

Ustego Module: It takes input from stego image that is stego image.

Decryption: It separates the secret text from the image.

7.4 State Chart Diagram

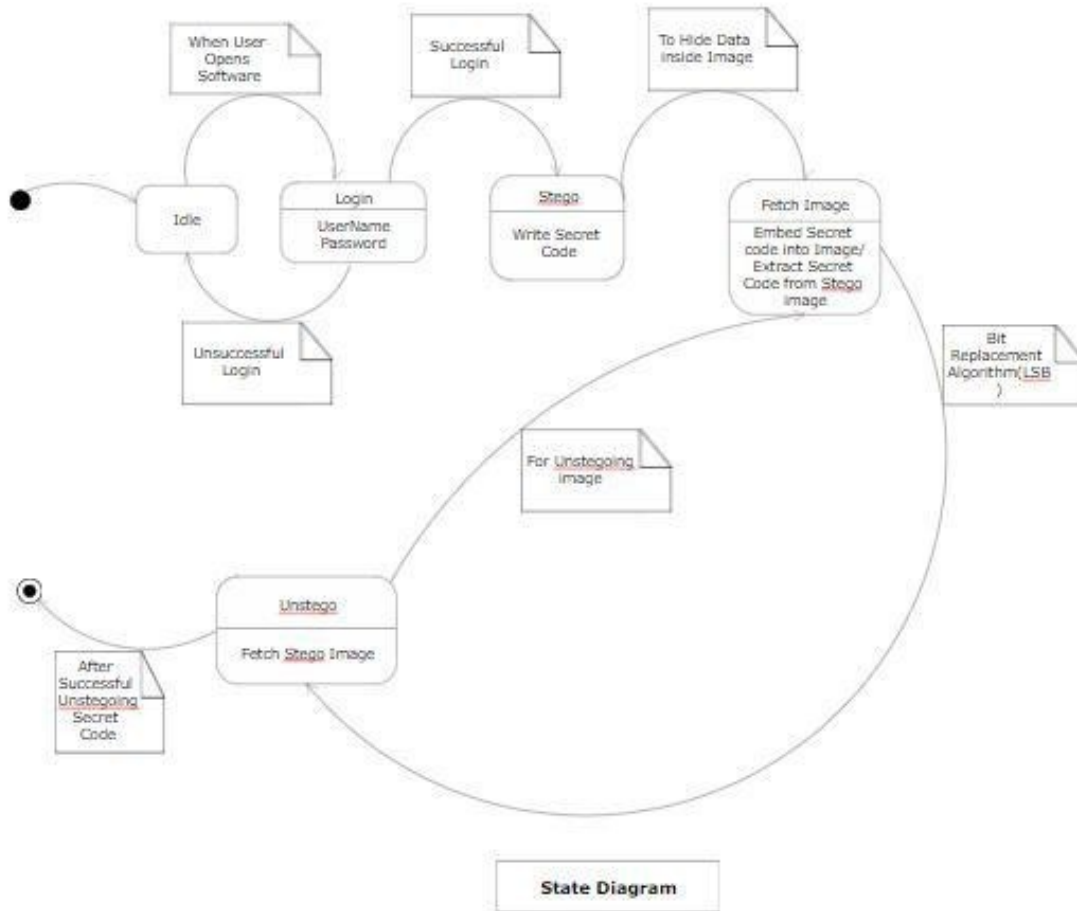


Figure 7.4: State Chart Diagram

System is in the Idle state, when user open it, After login correctly state changes from login to stego module where user writes secret code. After writing secret code state passes to Fetch Image in which secret code is embedded inside image. For decoding image state changes from Fetch image to Unstego module. User can exit system successfully after decryption of image.

7.5 Sequence Diagram

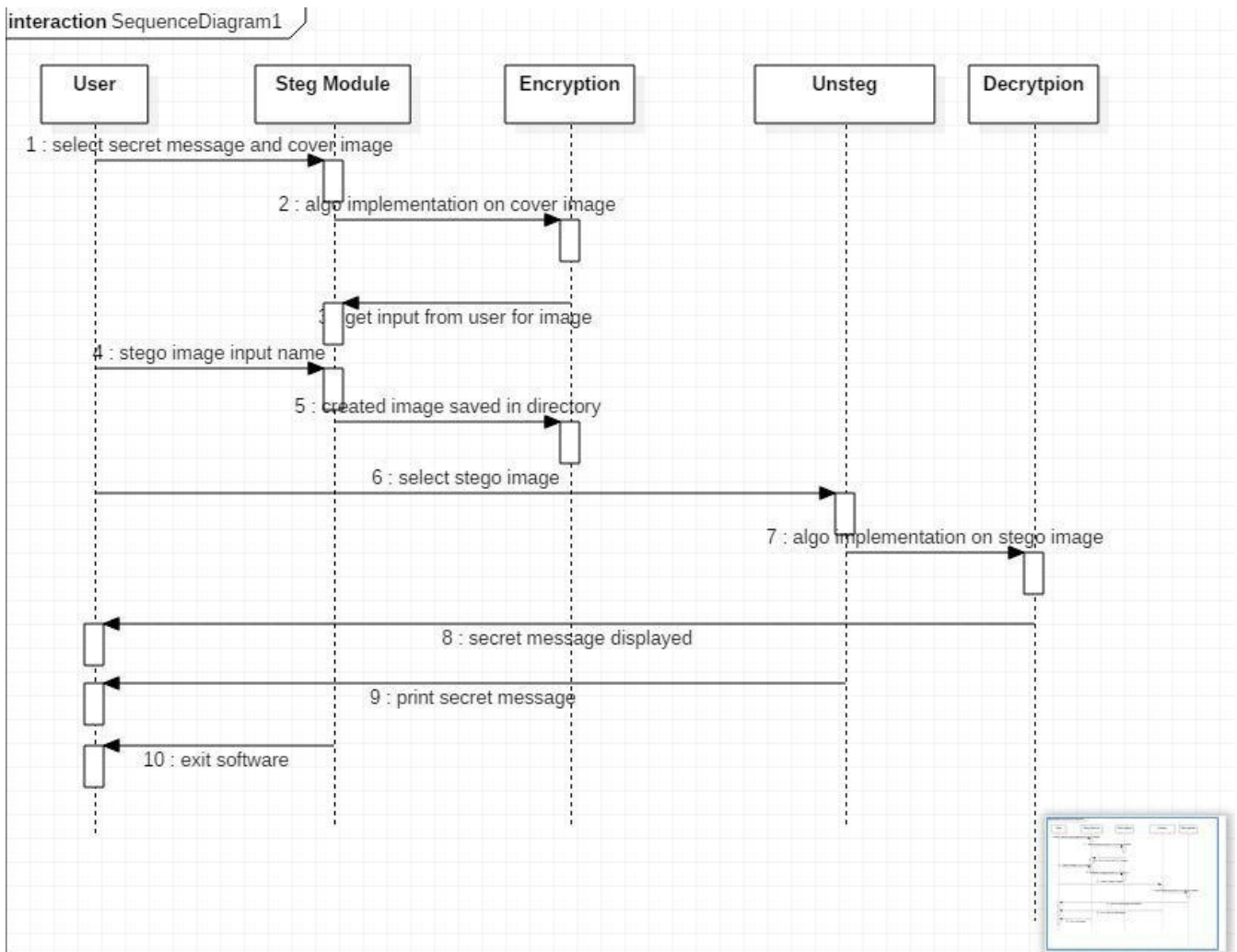


Figure 7.5: Sequence Diagram

Sequence diagrams are a popular dynamic modeling solution in UML because they specifically focus on lifelines, or the processes and objects that live simultaneously, and the messages exchanged between them to perform a function before the lifeline ends in which there are five lifelines :

1. User
2. Steg Module
3. Encryption
4. Unsteg
5. Decryption.

The user selects cover image and text to be hidden by LSB algorithm.

In which algorithm is implemented on that cover image and hides the secret text.

After completion of process the system takes input for newly generated image. As user gives input, image is saved in respective directory.

Saved image in directory is opened and Unsteg operation is performed on the image and original message is obtained.

Chapter 8

SYSTEM IMPLEMENTATION

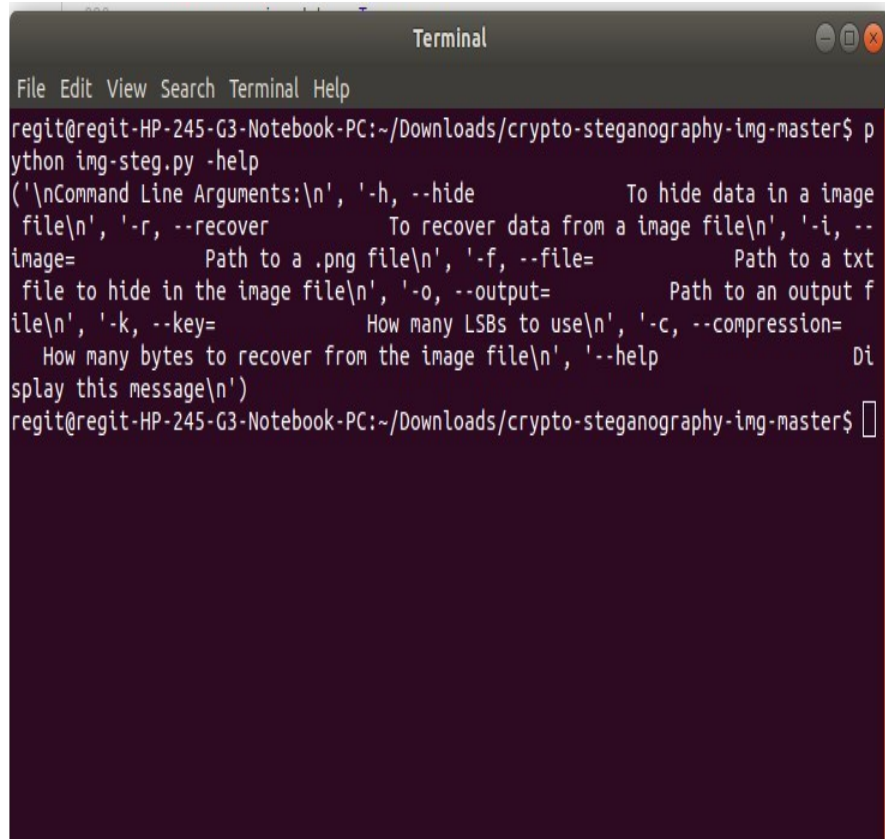
```
olefile==0.44
Pillow==6.2.0
pycipher==0.5.2
```

Figure 8.1: REQUIREMENTS

First of all the user needs to download some specific files which are required during the successful operation of the software.

You can install it by following commands in your Linux OS:

```
$ sudo apt install <package name>.
```



```

Terminal
File Edit View Search Terminal Help
regit@regit-HP-245-G3-Notebook-PC:~/Downloads/crypto-steganography-img-master$ p
python img-steg.py -help
('\nCommand Line Arguments:\n', '-h, --hide          To hide data in a image
file\n', '-r, --recover          To recover data from a image file\n', '-i, --
image=          Path to a .png file\n', '-f, --file=          Path to a txt
file to hide in the image file\n', '-o, --output=          Path to an output f
ile\n', '-k, --key=          How many LSBs to use\n', '-c, --compression=
          How many bytes to recover from the image file\n', '--help          Di
splay this message\n')
regit@regit-HP-245-G3-Notebook-PC:~/Downloads/crypto-steganography-img-master$ █

```

Figure 8.2: MENU

After installing the requirements you can navigate to help section by the command:

```
$ python img-steg.py -help
```

Here you get the complete list of commands and what function it performs like

- h = hide data in a image
- r = recover data from an image
- i = image path to the .png file
- f = file path to the text file to hide inside the image
- o = output path of the file
- k = key how many lsb algorithm to use
- c = compression of the image file
- help = to get the help menu



Figure 8.3: A.TXT FILE

You can edit the a.txt file inside the folder for the message that you like to encrypt. Also you can select any image and paste it in the folder so that you can use the image for encryption.

```
C:\Users\super\Documents\GitHub\crypto-steganography-img>py img-steg.py -h -i pic.png -f a.txt -o steg.png
-k MSW -c 1
  Hiding 23 bytes
  Runtime: 1.42 s
C:\Users\super\Documents\GitHub\crypto-steganography-img>py img-steg.py -r -i steg.png -o b.txt -k MSW -c 1
  Looking to recover 23 bytes
  Runtime: 0.67 s
```

Figure 8.4: ENCODE

For Encrypting following code is used:

```
$ python img-steg.py -h -i pic.png -f a.txt -o steg.png -k MSW -c 1
```

The command will run the img-steg.py code and encrypt the text file in image and will give you an output file as steg.png

```
C:\Users\super\Documents\GitHub\crypto-steganography-img> python img-steg.py -h -i pic.png -f a.txt -o steg.png  
-k MSW -c 1  
Hiding 23 bytes  
Runtime: 1.42 s  
C:\Users\super\Documents\GitHub\crypto-steganography-img> python img-steg.py -r -i steg.png -o b.txt -k MSW -c 1  
Looking to recover 23 bytes  
Runtime: 0.67 s
```

Figure 8.5: DECODE

For Decrypting following code is used:

```
$ python img-steg.py -r -i steg.png -o b.txt -k MSW -c 1
```

The command will run `img-steg.py` again to recover the text file from the Encrypted image.

Chapter 9

APPLICATION OF SYSTEM

9.1 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 can not guess password.

Normal network user cant guess image.

In steganography anyone cant jump on suspect by looking images. It is Reliable.

Easy to use.

Easy Maintenance.

System have been secured by password authentication.

9.2 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 message can acquire.

This software has been implemented by java, 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.

9.3 Application

- i) Confidential Communication and Secret Data Storing.
- ii) Protection of Data Alteration.
- iii) Access Control System for Digital Content Distribution.
- iv) E-Commerce.
- v) Media.
- vi) Database Systems.
- vii) Digital Watermarking.

Chapter 10

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 analyzing the low order bits of the image bytes. If the Steganographic algorithm is more complex, however, and spreads the embedded data over the image in 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.

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. But this process can also be extended to be used for color images where, bitplane slicing is to be done individually for the top four bit-planes for each of R, G, B of the message image.

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 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.

REFERENCES

[1] Literature Survey,

<http://www.ijetajournal.org/volume-2/issue-5>.

[2] Design Realated Research,

https://www.researchgate.net/publication/314116270_imagesteganography:ImageSteaga http :
==repository:root me:org=Stganoraphy

[3] Programming Tutorial

www.dreamincode.net