

INFORMATION HIDING IN IMAGES USING STEGANOGRAPHY TECHNIQUES

TANZILA AKTER

This Project Report submitted in fulfilment of the requirements for the award of
the degree of
Masters of Engineering Information and Communication Engineering

**MASTERS OF ENGINEERING INFORMATION AND
COMMUNICATION ENGINEERING**

NOAKHALI SCIENCE AND TECHNOLOGY UNIVERSITY

ABSTRACT

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Steganography is a method of hiding secret data by embedding it into an audio, video, image and text file. It is one of the methods employed to protect secret or sensitive data from malicious attack. 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 exist a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. This project report intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which steganography techniques are more suitable for which applications.

TABLE OF CONTENTS

Contents

ABSTRACT

CHAPTER 1 INTRODUCTION

- 1.1 Problem Statement
- 1.2 Objectives
- 1.3 Project scope

CHAPTER 2 LITERATURE REVIEW

CHAPTER 3 METHODOLOGY

- 3.1 Steganography technique
- 3.2 Image and bitmap pictures
- 3.3 Bitmap steganography
- 3.4 System design and analysis
- 3.5 Data Flow Diagram

CHAPTER 4 RESULT AND DISCUSSION

- 4.1 outcomes

CHAPTER 5 CONCLUSION

REFERENCES

CHAPTER 1

INTRODUCTION

Steganography has been derived from two greek words firstly Steganos (covered) and Graptos (Writing) that means “covered writing” which basically mean to hide data and information into a plain sight. In today’s world everyone is sharing data and information with one another, the development in electronic information and data sharing gadgets and with their increased use, the data security issue has become essential. For this information and data security there have been different methods available such as Steganography, cryptography etc. People often gets confused between steganography and cryptography because both these methods are used for data and information hiding, but there is difference between these two, Steganography is a way of data and information hiding, in this method a person is not able to known that whether there is a hidden data or information is available or not, steganography basically exploits the perception of humans. The hidden data and information are not visible directly. Steganography is mainly done to hide files inside other files whereas cryptography is the way of protecting data, which can be known through decryption, the message in cryptography is given in an encrypted form, and there are encryption key which is shared between the authorized persons, by knowing this encryption key anyone can get the data and information, in cryptography there is nothing like hiding up of data it’s just a way of protecting the data, no human exploitation of human sense are done in cryptography as people know that there is some information available the only trick is to get the encryption key, so as to overcome this issues steganography is introduced. Steganography involves audio, video, image, text, etc.

1.1 Problem statement

The former consists of linguistic or language forms of hidden writing. The later, such as invisible ink, try of hide messages physically. One disadvantage of linguistic steganography is that users must equip themselves to have a good knowledge of linguistry. 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 exist 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 more simple and user friendly.

1.2 Objectives

The goal of steganography is covert communication. So, a fundamental requirement of this steganography system is that the hider message carried by stego-media should not be sensible to human beings. The other goad of steganography is to avoid drawing suspicion to the existence of a hidden message. This approach of information hiding technique has recently become important in a number of application area.

This project has following objectives:

- To product security tool based on steganography techniques.
- Providing more security for image communication
- To achieve transparency, authority and high capacity of the hidden data.

- To avoid drawing suspicion to the existence of a hidden message.
- To explore techniques of hiding data using encryption module of this project
- To extract techniques of getting secret data using decryption module.

1.3 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.

- The scope of the project is to limit unauthorized access and provide better security during message transmission.
- In this project, the proposed approach finds the suitable algorithm for embedding the data in an image using steganography which provides the better security pattern for sending message through a network.

CHAPTER 2

LITERATURE REVIEW

A literature review discusses the published information in a particular subject area, and sometimes information in a particular subject area within a certain time period. It can be just a simple summary of the sources, but it usually has an organizational pattern and combines both summary and synthesis.

Ritu Sindhu proposed information hiding using steganography shows the amount of hidden information that the cover image can implant in it. The rate of implantation is given in complete amount such as the secret message length. Without the prior permission of main user who have the password, hidden data should not release [1]

Ashees Tiwari implemented, In this paper, stenographic solution to strengthen the security and confidentiality of data concealed in the RGB picture cover. They used an LSB insertion which hides the bits of hidden message of red plane of the pixels within an enclosing image. Random number generator helps in choosing the pixels.

Ramadhan Mstafa proposed the information hiding within the image this paper shows the steganography and digital watermarking provide methods that users can hide and mix their information within other information that make them difficult to recognize by attackers. In this paper, we review some techniques of steganography and digital watermarking in both spatial and frequency domains. Also we explain types of host documents and we focused on types of images.

Aishwarya Talekar implemented Steganography technique for hiding secret audio in an image this shows Information security is one of the most important factor which is to be considered when secret information has to be communicated between two parties. Cryptography and

steganography are the two techniques used for this purpose. Cryptography scrambles the information, but it reveals the existence of information. Steganography hides the actual existence of information so that anyone else other than the sender and recipient cannot recognize the transmission. In steganography the secret information to be communicated is hidden in some carrier such a way that the secret information is invisible. In our paper an image steganography technique is proposed. Audio signal is hidden in the transform domain of a cover image using wavelet transform. The audio signal in any format (MP3 or WAV) is encrypted and carried by the image without revealing the existence to anybody.

Ms. Pratidnya Sapate proposed video hiding within image file due to which it is possible to transfer data from one place to another place with very high speed. But it is very risky to transfer data over internet. Hence to maintain privacy and to prevent an unauthorized person from extracting information steganography technique is used. Steganography is the science of hiding secret information. The secret information is in the form of text, image, audio and video. This secret information can be hidden in the text, image, audio and video. Hiding secret information in video file is called as video steganography. In this paper, review on various video steganography techniques is presented.

Ranganatha H R proposed information hiding using audio steganography this paper shows, steganography does not alter the structure of the secret message, but hides it inside a cover image so that it cannot be seen. A message in a cipher text, for instance, might arouse suspicion on the part of the recipient while an invisible message created with steganography methods will not. In other word, steganography prevents an unintended recipient from suspecting that the data exists. In addition, the security of classical steganography system relies on secrecy of the data encoding system.

CHAPTER 3

METHODOLOGY

3.1 Steganography technique

The basic model of steganography consists of Carrier, message and password. Carrier is also known as cover-object, which the message is embedded and serves to hide the presence of the message. 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. Commonly approaches are include LSB, masking and filtering and transform techniques. Least significant bit (LSB) insertion is a simple approach to embedding information in 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 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 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.

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

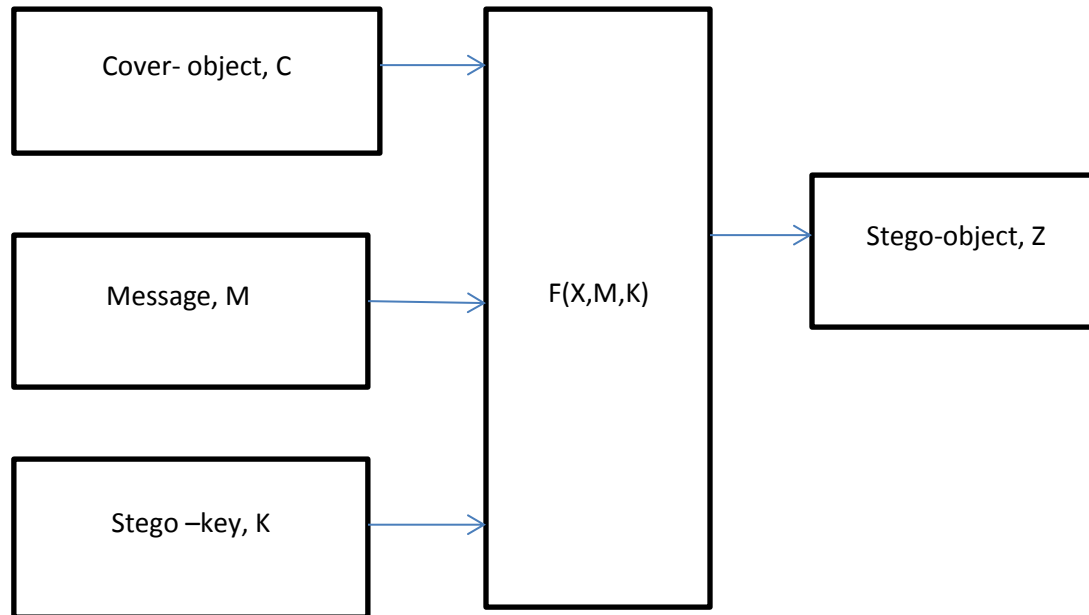


Figure 3.1 steganography model

Message is the data that the sender wishes to remain it confidential. It can be plain text, cipher-text, 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-object which ensures that only recipient who known 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 message from a stego-object requires the cover-object 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.

3.2 Image steganography and bitmap pictures

Using bitmap pictures for hiding secret information is one of most popular choices for Steganography. Many types of software built for this purpose, some of these software use password protection to encrypting information on picture. To use these software you must have a BMP format of a pictures to use it, but using other type of pictures like JPEG, GIF or any other types is rather or never used, because of algorithm of BMP pictures for Steganography is simple. Also we know that in the web most popular of image types are JPEG and other types not 'BPM' so we should have a solution for this problem. This software provide the solution of this problem, it can accept any type of image to hide information file, but finally it give the only 'BMP' image as an output that has hidden file inside it.

3.3 Bitmap steganography

Bitmap type is the simplest type of picture because that it doesn't have any technology for decreasing file size. Structure of these files is that a bitmap image created from pixels that any pixel created from three colors (red, green and blue said RGB) each color of a pixel is one byte information that shows the density of that color. Merging these three color makes every color that we see in these pictures. We know that every byte in computer science is created from 8 bit that first bit is Most-Significant-Bit (MSB) and last bit Least-Significant-Bit (LSB), the idea of using Steganography science is in this place; we use LSB bit for writing our security information inside BMP pictures. So if we just use last layer (8st layer) of information, we should change the last bit of pixels, in other hands we have 3 bits in each pixel so we have $3 \times \text{height} \times \text{width}$ bits memory to write our information. But before writing our data we must write name of data size of name of data & size of data. We can do this by assigning some first bits of memory.

(00101101	0001110 <u>1</u>	11011100)
(10100110	1100010 <u>1</u>	00001100)
(11010010	1010110 <u>0</u>	01100011)

Using each 3 pixel of picture to save a byte of data.

3.4 System Analysis and design

Steganography system requires any type of image file and the information or message that is to be hidden. It has two modules encrypt and decrypt. Microsoft .Net framework prepares a huge amount of tool and options for programmers that they simplify programming. One of .Net tools for pictures and images is auto-converting most types of pictures to BMP format. I used this tool in this software called “Steganography” that is written in C#.Net language and you can use this software to hide your information in any type of pictures without any converting its format to BMP. The algorithm used for Encryption and Decryption in this application provides using several layers instead of using only LSB layer of image. Writing data starts from last layer (8th or LSB layer); because significant of this layer is least and every upper layer has doubled significant from its down layer. So every step we go to upper layer image quality decreases and image retouching transpires.

The encrypt module is used to hide information into the image; no one can see that information or file. This module requires any type of image and message and gives the only one image file in destination.

The decrypt module is used to get the hidden information in an image file. It takes the image file as an input, and gives two files at destination folder, one is the same image file and another is the message file that is hidden in it.

Before encrypting file inside image we must save name and size of file in a definite place of image. We could save file name before file information in LSB layer and save file size and file name size in most right-down pixels of image. Writing this information is needed to retrieve file from encrypted image in decryption state.

The graphical representation of this system is as follows:

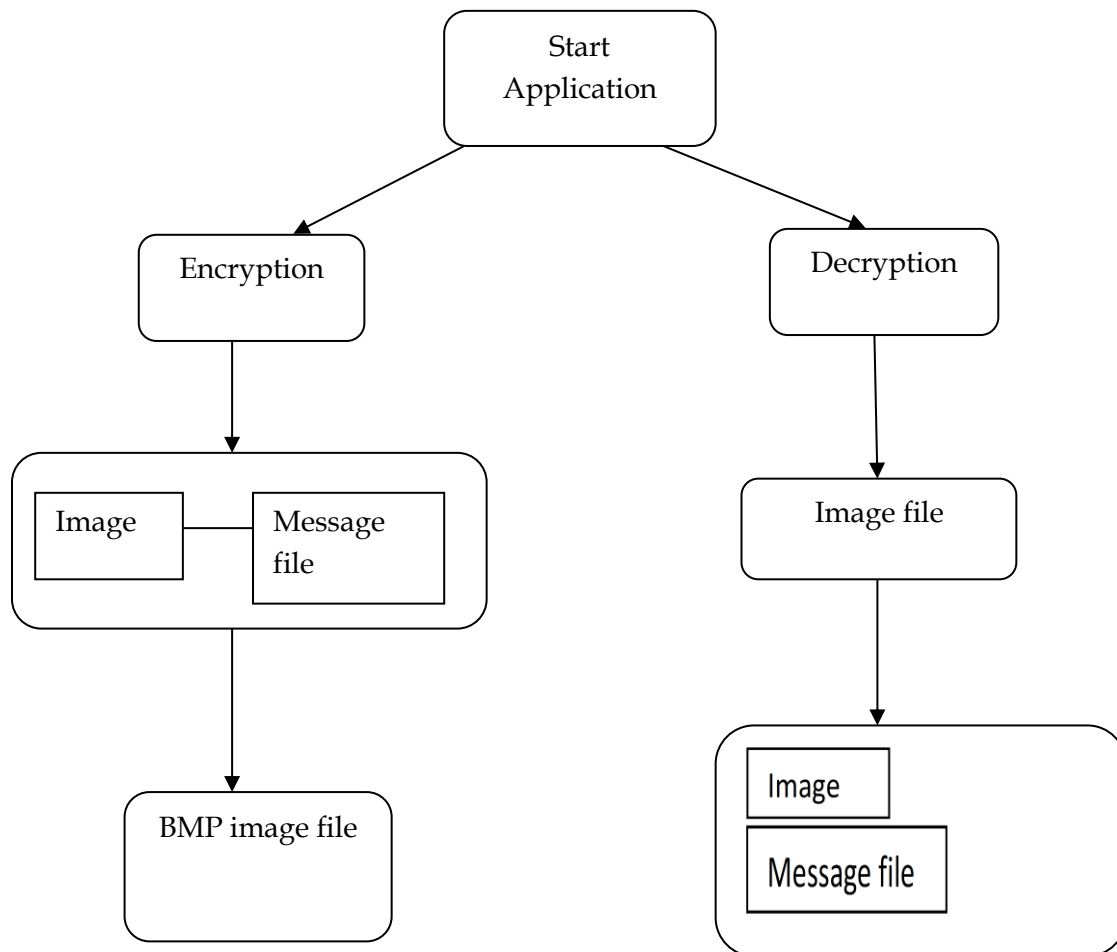


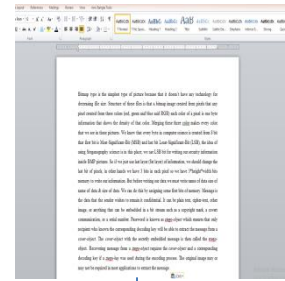
Figure 3.2 system design

Encryption Process

Image file



Information file



BMP file



Figure 3.3 Encryption process

Decryption Process

BMP file



Information file

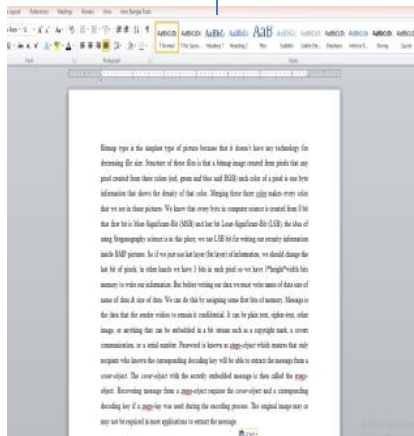


Image file



Figure 3.4 Decryption process

3.5 Entity Relationship diagram

An entity-relationship model describes interrelated things of interest in a specific domain of knowledge. A basic ER model is composed of entity types which classify the things of interest and specifies relationships that can exist between entities. The ER diagram represents the model of image steganography system. Figure (3.2) shows a simple ER diagram for image steganography system.

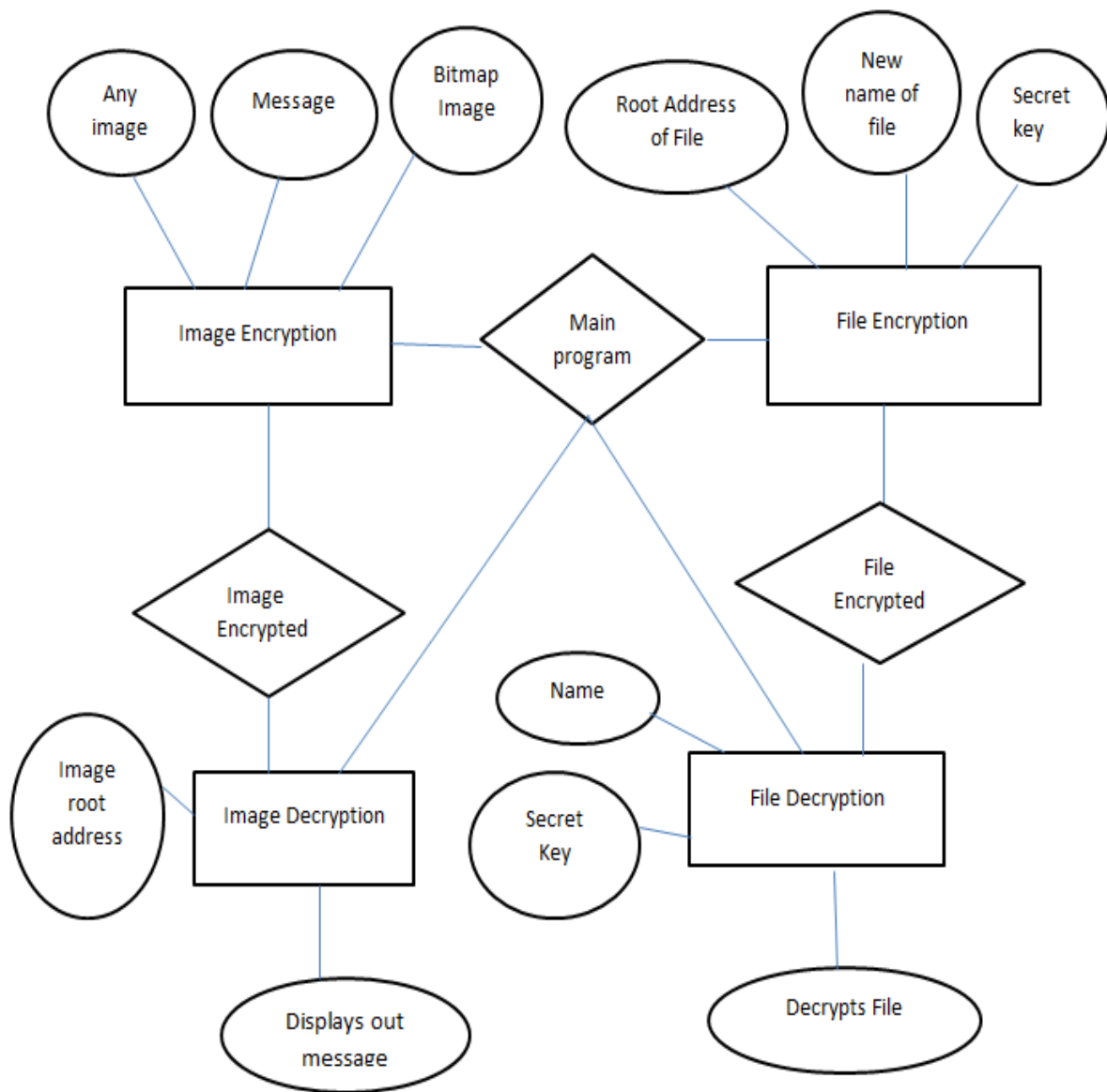


Figure 3.5 Entity Relationship Diagram

3.6 Use case diagram

A Use Case diagram at its simplest is a representation of a user's interaction with the system and depicting the specifications of a use case. A use case diagram can portray the different types of users of a system and the various ways that they interact with the system. This type of diagram is typically used in conjunction with the textual use case and will often be accompanied by other types of diagrams as well.

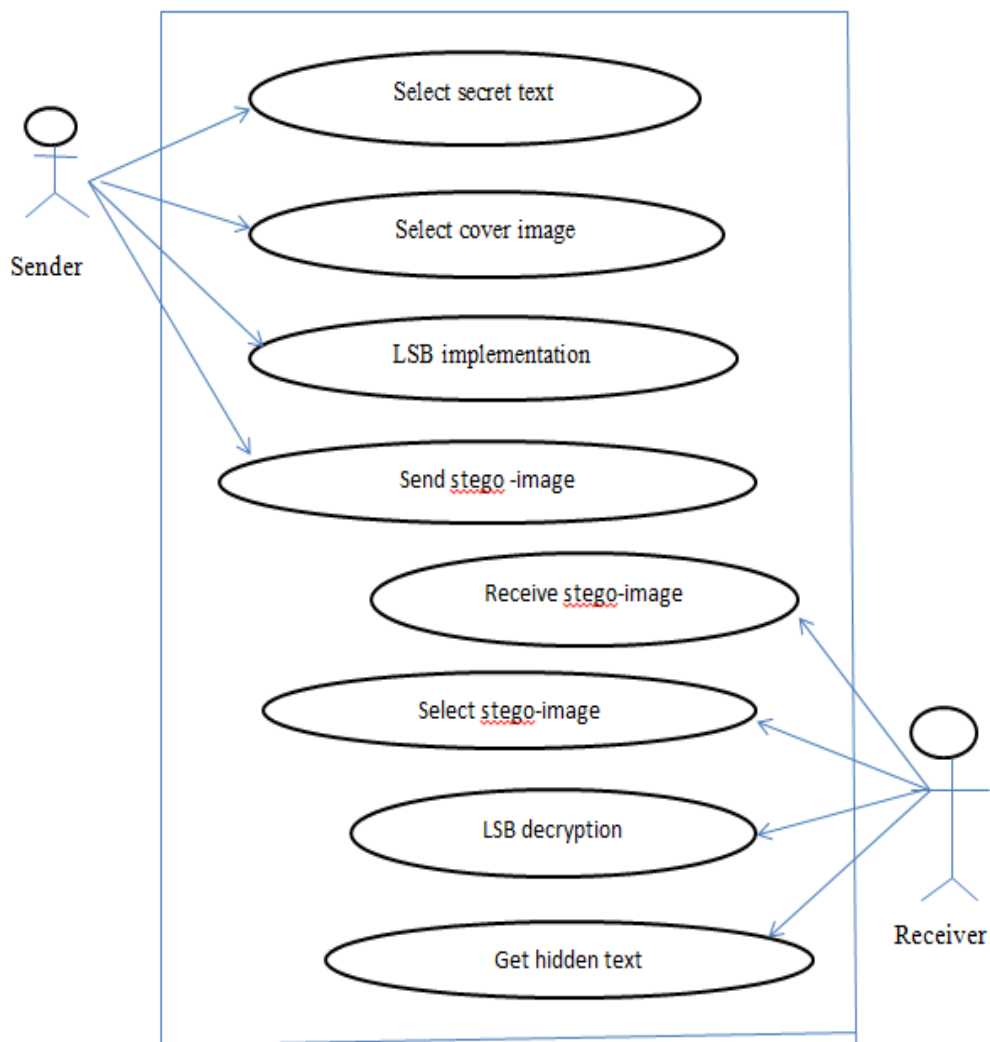


Figure 3.6 Use Case Diagram

3.7 Data flow diagram

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system, modelling its process aspects. A DFD is often used as a preliminary step to create an overview of the system without going into great detail, which can later be elaborated. DFDs can also be used for the visualization of data processing. A DFD shows what kind of information will be input to and output from the system, how the data is advance through the system, and where the data is stored.

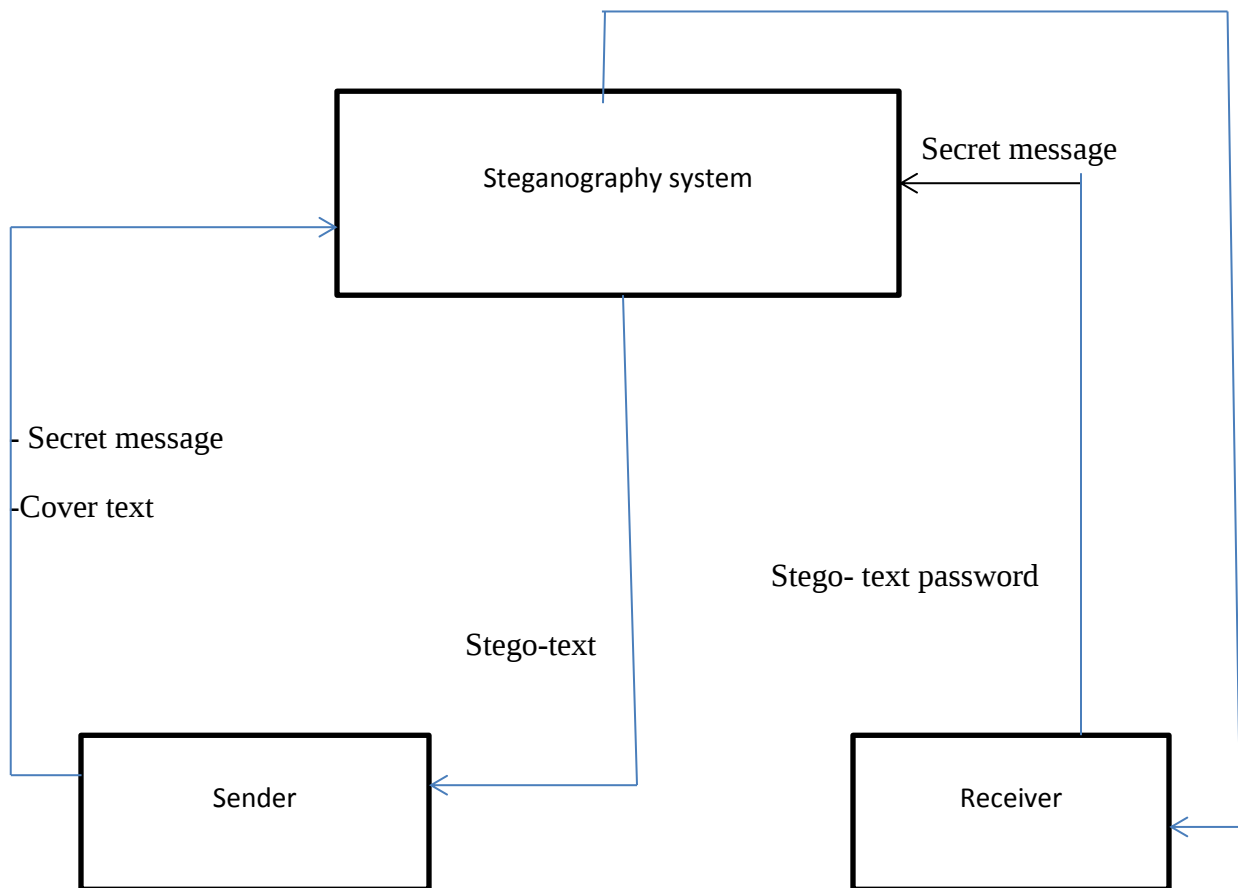


Figure 3.7 Data Flow Diagram

CHAPTER 4

RESULT AND DISCUSSION

4.1 Outcomes

This steganography application software provided for the purpose to how to use any type of image formats to hiding any type of files inside their. 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.

User Manual

This is the first screen which has two tab options – one is Encrypt Image for encryption and another is Decrypt image for decryption. In right – top panel is displays the information about the image such as size, height and width.

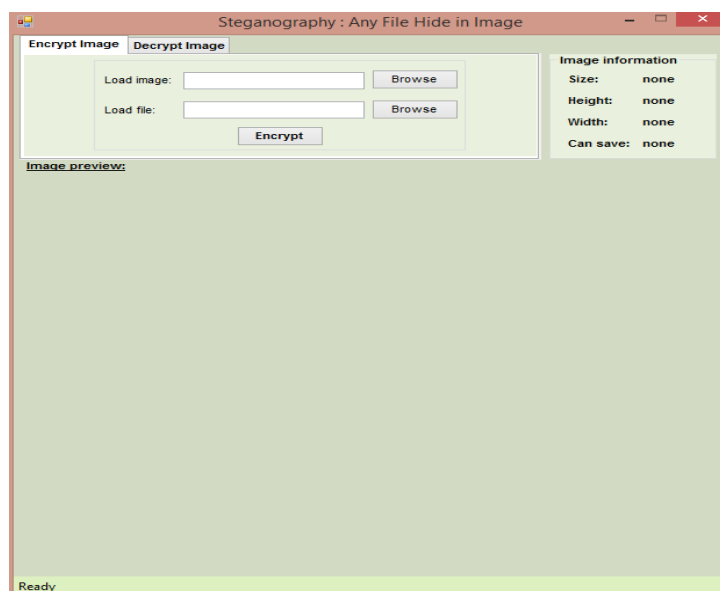


Figure 4.1 user manual

Encryption

For Encryption select Encrypt Image tab option. For load image click on button Browse that is next to the Load Image textbox. The file open dialog box will displays as follows, select the Image file, which you want to use hide information and click on Open button.

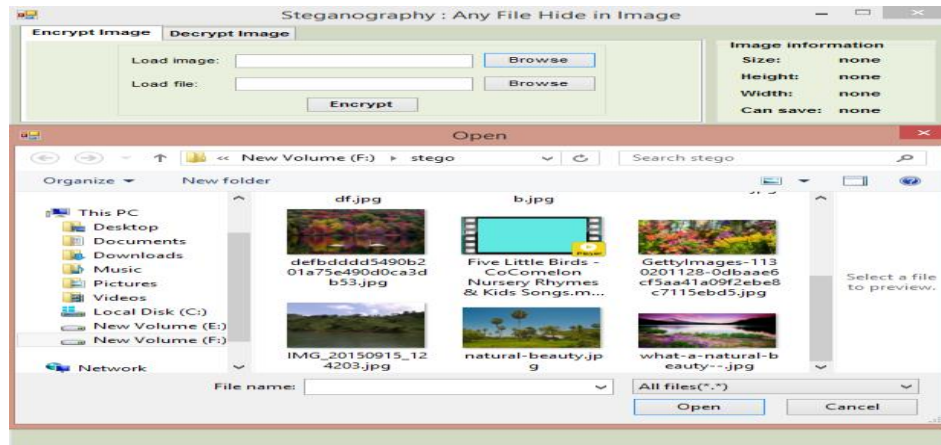


Figure 4.2 Load image textbox

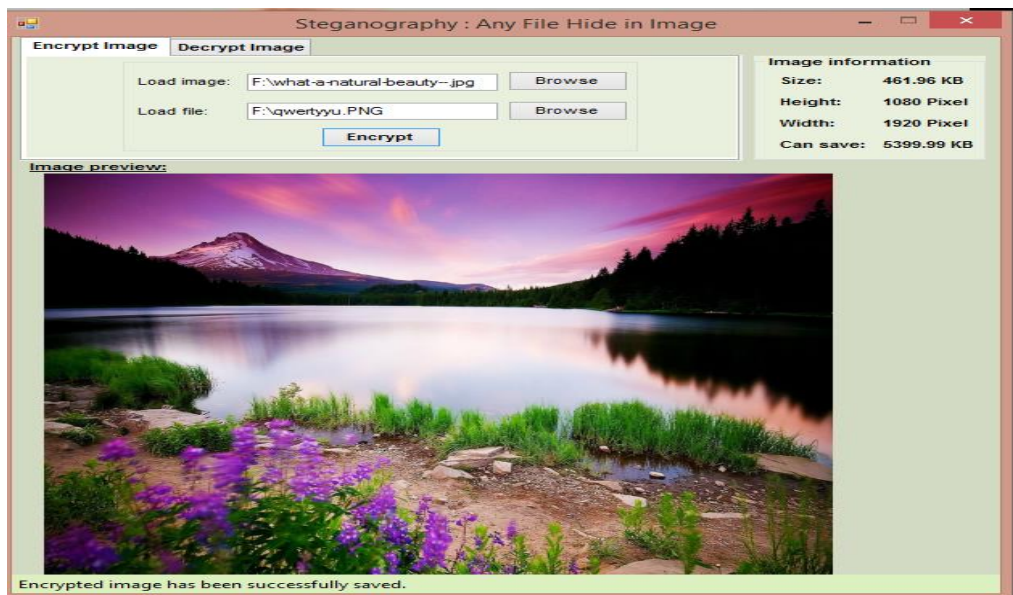


Figure 4.3 Encryption process

Decryption

Select the Decryption Image tab option. Next click on the Browse button, which open the Open file dialog box, here you have to select the image which is Encrypted and has hidden information file. Select the image file and click on Open button. Now click on browse button which is next to save file to textbox. It will open a dialog box that is browse for folder. Select the path or folder, where you want to extract the hidden file. Select the folder and click on Ok button.

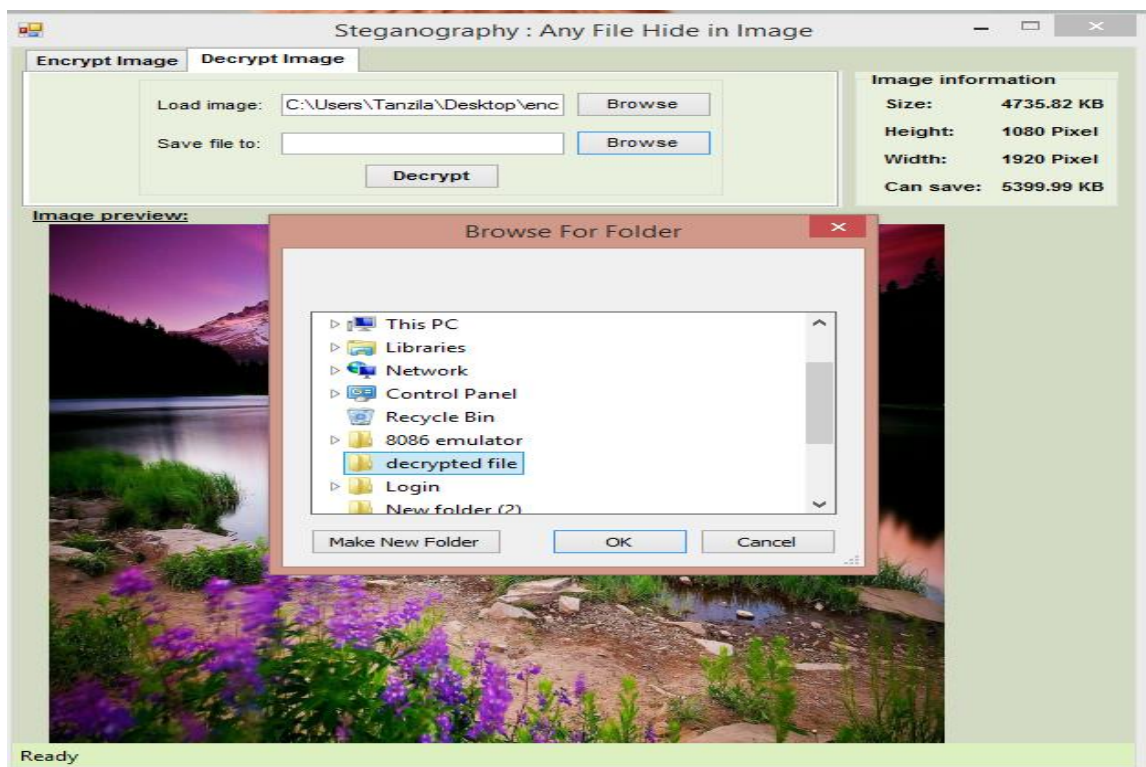


Figure 4.4 Encrypted file

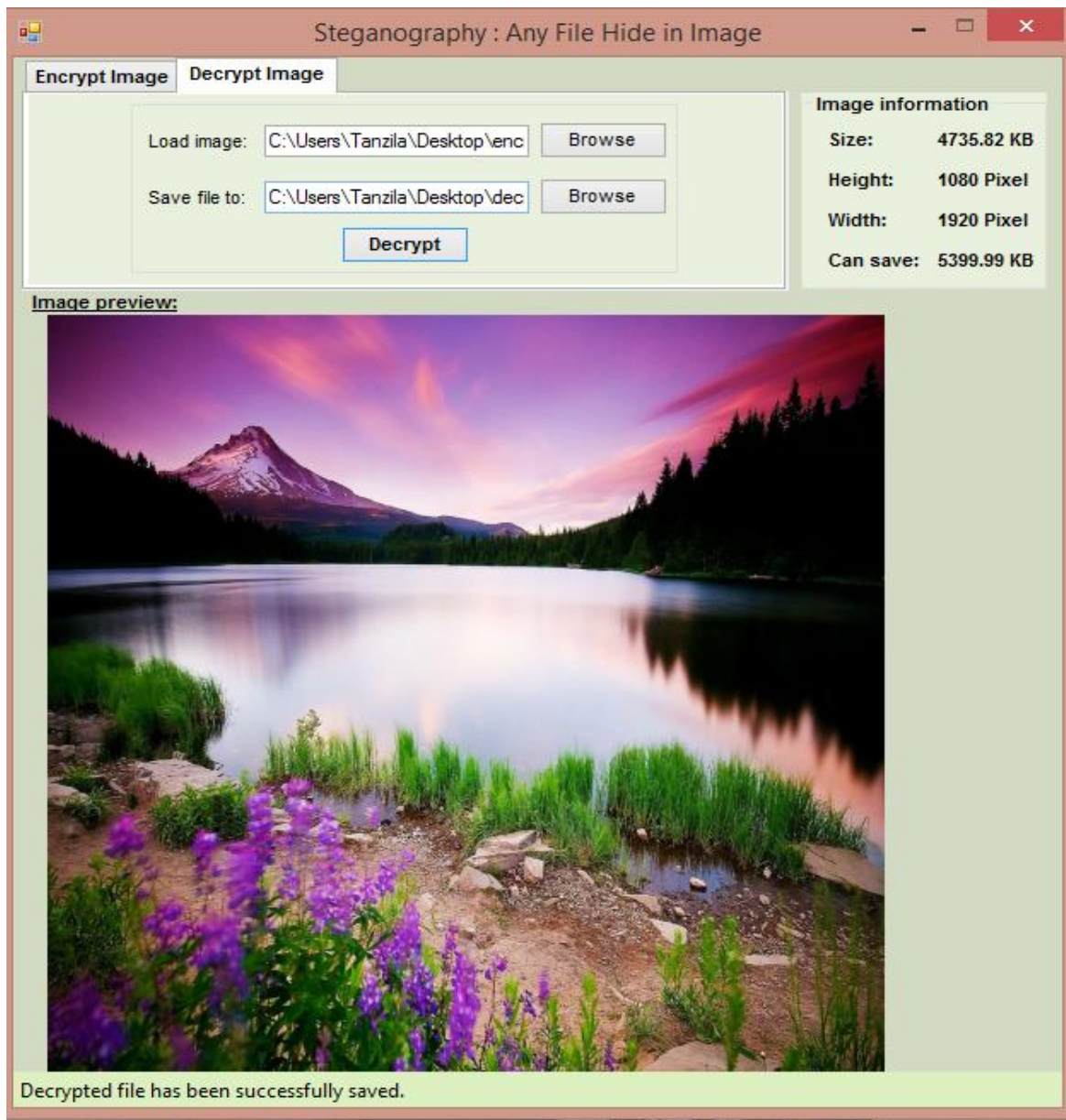


Figure 4.5 Decryption process

CHAPTER 5

CONCLUSION

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 steganography key has been applied to the system during embedment of the message into the cover image. This steganography application software provided for the purpose to how to use any type of image formats to hiding any type of files inside their. 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.

REFERENCES

- [1] Ritu Sindhu, Pragati sing, “Information hiding using steganography”, International journal of engineering and advanced technology.
- [2] Ashees Tiwari “Information hiding using LSB technique”, 3rd International Conference on System Modeling and advancement.
- [3] Ramadhan Mstafa “Information hiding within the image”, International journal of multimedia and its application (IJMA)
- [4] Aishwarya Talekar” Steganography technique for hiding secret audio in an image” 4th ICCCNT 2013, Tiruchengode, India No.6, July 2013. IEEE –31661.
- [5] Ms. Pratidnya Sapate, Arjun nischal “Video hiding within image file”, international advanced journal in science & engineering and technology.
- [6] Ranganatha H R, jayaram P “Information hiding using audio steganography” the international journal of multimedia and its application, vol.3 August 2011.
- [7] Shivendra Katiyar, Kullai Reddy Meka, Ferdous A.Barbhuiya, Sukumar Nandi, ” Information hiding within an image “Powered By Biometric Security Using Steganography” Second International Conference on Emerging Applications of Information Technology, 2011.
- [8] Ms Jambudiya Aarti P, Ms Topiya Dipa C, Ms Paneliya Bhumi R, “Audio file hide in an image”, Shree M. & N. Science College.
- [9] kedar Nath Choudry, Aaksh Wanjari, “ Video steganography”, International journal of computer science and information technologies vol. 6 (3) .
- [10] Bhagyashri Rahangdale, P.R. Deshmukh, “Data hiding using video steganography”, International journal of engineering research & technology (IJERT).

