ATMIYAUNIVERSITY

RAJKOT

A

ReportOn

STEGANOGRAPHY

Undersubjectof

PROJECT

B.TECH,Semester– VII

(ComputerEngineering)

Submitted by:

1. JAY R. VORA 190002124
2. VIVEK J. VADODARIYA 190002114

Prof. Nirali Borad

(FacultyGuide)

Prof. Tosal M.Bhalodia

(Head of the Department)

Academic Year

(2022-23)

CANDIDATE'S DECLARATION

We hereby declare that the work presented in this project entitled "**STEGANOGRAPHY"** submitted towards completion of project in **7th Semester** of B.Tech. (Computer Engineering) is an authentic record of our original work carried out under the guidance of "**Prof. Nirali Borad".**

We have not submitted the matter embodied in this project for the award of any other degree.

Semester: 7th

Place: Rajkot

Signature:

Jay R. Vora (190002124)

Vivek J. Vadodariya (190002114)

ATMIYA

UNIVERSITYRAJKOT

CERTIFICATE

Date:

This is to certify that the "**STEGANOGRAPHY**" has been carried out by **Jay R. Vora** under my guidance in fulfillment of the subject Project in COMPUTER ENGINEERING (7thSemester) of Atmiya University, Rajkot during the academic year 2022.

Prof. Nirali Borad — **(Project Guide)**

Prof.Tosal M.Bhalodia — **(Head of the Department)**

ATMIYA

UNIVERSITYRAJKOT

CERTIFICATE

Date:

This is to certify that the "**STEGANOGRAPHY**" has been carried out by **Vivek J. Vadodariya** under my guidance in fulfillment of the subject Project in COMPUTER ENGINEERING (7th Semester) of Atmiya University, Rajkot during the academic year 2022.

Prof. Nirali Borad — **(Project Guide)**

Prof.Tosal M.Bhalodia — **(Head of the Department)**

ACKNOWLEDGEMENT

We have taken many efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. We would like to extend our sincere thanks to all of them.

We are highly indebted to Prof. Nirali Borad for their guidance and constant supervision as well as for providing necessary information regarding the Major Project titled **"STEGANOGRAPHY".** We would like to express our gratitude towards staff members of Computer Engineering Department, Atmiya University for their kind co-operation and encouragement which helped us in completion of this project.

We even thank and appreciate to our colleague in developing the project and people who have willingly helped us out with their abilities.

Jay R. Vora (190002124)

Vivek J. Vadodariya (190002114)

ABSTRACT

Steganography is the art of hiding the fact that communication is taking place, by hiding information in the 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 large variety of steganographic 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 application may require absolute invisibility of the secret message to be hidden. This project intends to give an overview of image steganography, its uses and techniques. It also supports steganography in Audio Files. For a more secure approach, the project encrypts the message using secret key and then sends it to the receiver. The receiver than decrypts the message to get the original one

INDEX

LIST OF FIGURES

LIST OF TABLES

INTODUCTION

1.1 What Is Steganography?

Steganography is a Greek word which means concealed writing. The word stegmos means covered and graphial mats 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 wc writing tables, stomach of rabbits or on the scalp of the slaves. But today most of the people transmit the data in the form of text. images, video, and audio over the modium. In order to safely transmission of confidential data, the multimedia object like audio, video, images are wind 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-intings. There are different types of steganography techniques each have their strengths and weakness. 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 world, the communication is the bani city 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.

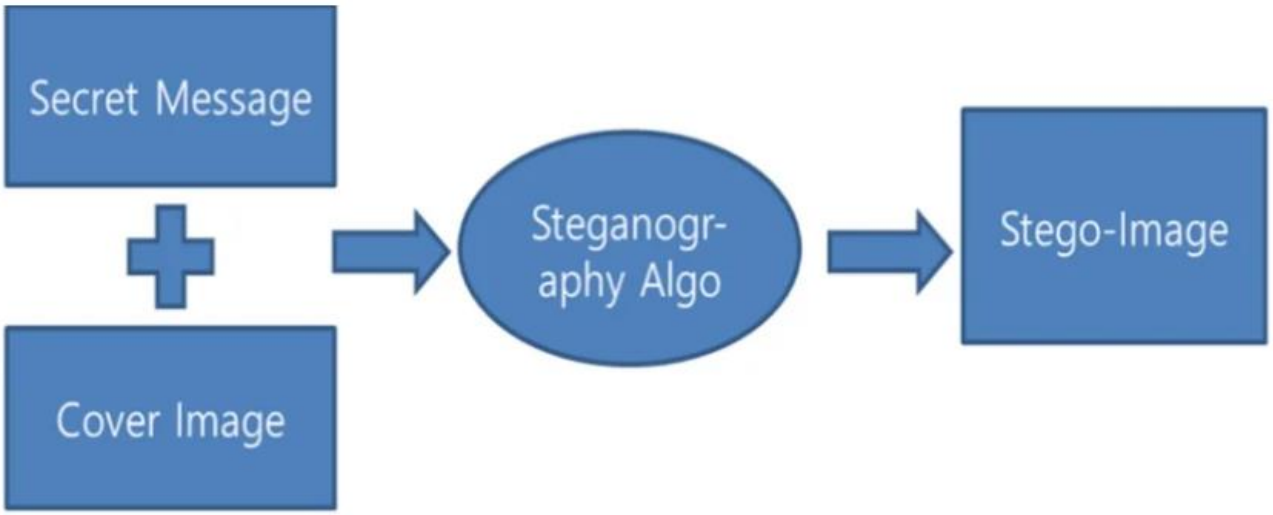

Figure 1.1: **PORCESS OF STEGANOGRAPHY**

The message cannot be accessed by anyone without using the encryption key. However, the transmission of encrypted message may easily arose attackers spicion, 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 hide 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 maitimedia content like image audio, video referred as a Embedding For increasing confidentiality of communicating data both techniques may combined. Application

of Steganography:

i)Confidential 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 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.

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 address 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 coded and gave information about ship movements, etc. Her case became somewhat fans 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 forturing 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 Korea. 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**.**

1.3 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 in formation les 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 cannot wed to protect the communication of confidential information

1.4 STEGANOGRAPHY WITH LSB ALGORITHM

bytes of peels are sufficient to hold one message byte. Rest of the bits in the pixels remains the same. Steganography is the set and science of communicating in a way which hides the ex-istence of the communication. Steganography plays an important role in information security. It is the art of invisible communication by canceling information inside other information. The term steganography is derived from Greek and literally means covered writing A Steganogra-phy system consists of three elements cover image (which hides the secret mage) Aber secret message and the stegano-image(which is the cover object with me embedded inside it). A digital image is described using a 2-D matrix of the color intestines at each grid point (ie) pixel). Typically gray images use 8 bits, whereas colored utilizes 24 bits to describe the color model, much as RGB model The Steganography system which uses an image as the cover, there are several techniques to conceal information de coverage. The spatial domain techniques manipulate the ever unge pixel bit values to ended the secret information. The secret bits are written directly to the cover image pixel bytes. Consequently, the spatial domain techniques are simple and eary to implement. The Let Significant Hit (LSB) one of the main techniques in spatial domain image Steganography

The court of LSB Embedding is simple. It exploits the fact that the level of precision is 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 label, just by looking at it. In conventional LSB technique, which required eight bytes of pois to store byte of secs data but in proposed LSB technique.

CHAPTER 2 :

SOFTWARE REQUIREMENTS SPECIFICATION

2.1 Hardware Requirements

Table 2.1.1 Hardware Requirements

Number	Description
1	INTEL I5 2.50 GHZ 4 GB RAM
2	Pentium 3 166 MHZ Or Higher 128 mb RAM

2.2 Software Requirements

Table 2.2.2 Software Requirements

Number	Description	Type
1	Operating System	Windows XP, 7, 8, 10, 11
2	Language	JAVA
3	Database	
4	IDE	Android Studio

CHAPTER 3
IMAGE STEGANOGRAPHY

3.1 Type of Steganography

3.1.1 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 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 (eg, 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 documentmarking 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

3.1.2 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

3.1.3 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**.**

3.1.4 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 cosinetransform (DCT) alter the values (eg.,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. Soit cannot be detected easily to be containing hidden information unless proper decryption is used.

3.2 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 Proves, 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.

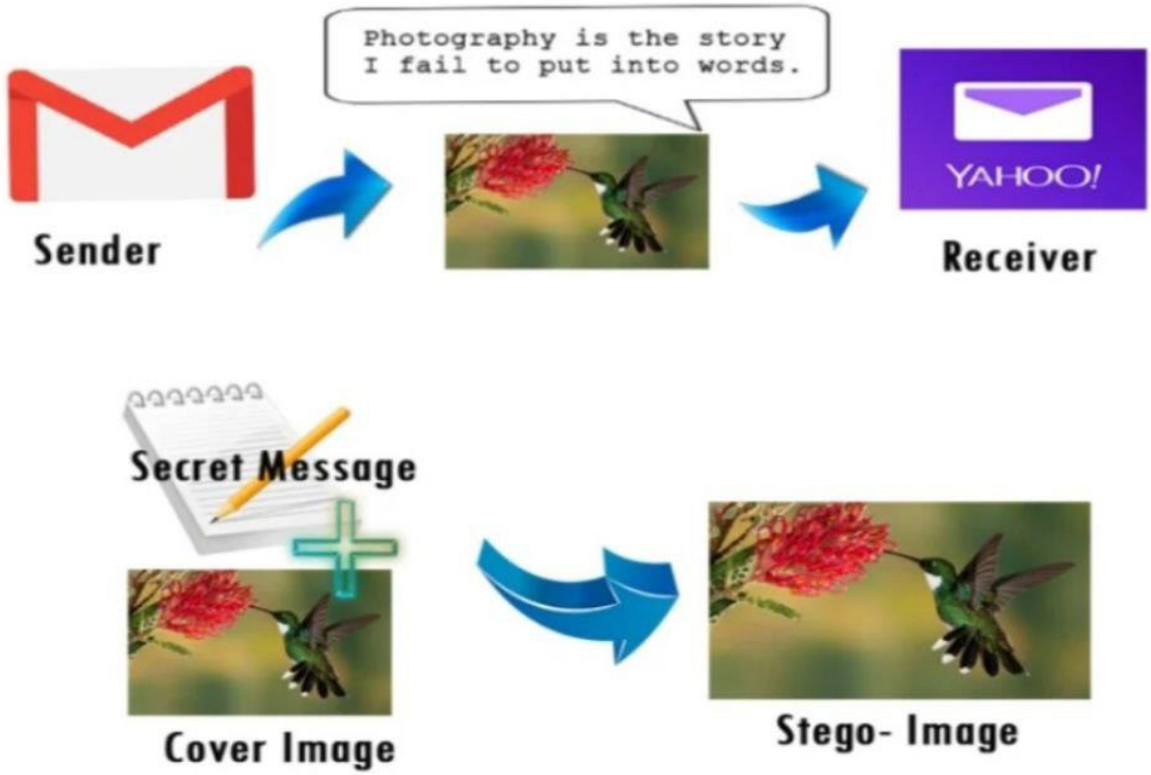

Fig.3.2: Communication Through Steganography

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 image files 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 Le, 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 4

HOW IT WORKS ?

4.1 Implementation

4.1.1 Technical Details

Using java.awt.Image. ImageI0
The package contains all the necessary classes and methods along with interfaces that are necessary for the manipulation of the images**.**

4.1.2 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 Le. An Image file and then direct the user to the selection of the text file.

4.1.3 Creation of User Space

User Space is created for preserving the original file, so that all the modifications are done in the user space.
In the object of Buffered image, using Image10.read method we take the original image.
Using create Graphics and draw Rendered image method of Graphics class, we create our user space in Buffered Image 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
4..444

Figure 4.1.3: LSB Operation

ImageIO.write method. This completes the encoding process

4.1.4 The Decoding Process

The offset of the image is retrieved from its header. Create the user space using the same pro-cess as in the Encoding. Using get Haster() and get Data Buffer() methods of Writable Raster and Data Buffer Byte classes. The data of image is taken into byte array. Using above byte array, the bit stream of original text file is retrieved into theanother byte array. And above byte array is written into the decoded text file, which leads to the original message

CHAPTER 5

IMPLEMENTATION

5.1 LSB (Least Significant Bit)

There are two different methods for image steganography:
1. Spatial methods
2. Transform methods
But we are using Spatial Methods

5.1.1 Spatial Method

In spatial method, the most common method used is LSB substitution method. Lest significant bit (LSB) method is a common, simple approach to embedding information in a cover file. In steganography, LSB substitution method is used. Le 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 med 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 (byte). Similarly for a color (RGB-red, green, blue) image, each pixel requires 24 bits (8bits for each layer). The Human visual system (HVS) cannot detect changes in the color 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 (image array).
Step 2: Extract all the characters from the given text file (message file) and store it in the array called (message array)
Step 3: Retrieve the characters from the Stego-key and store them in a array called Key array. 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. O 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 has 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 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 com pression 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.

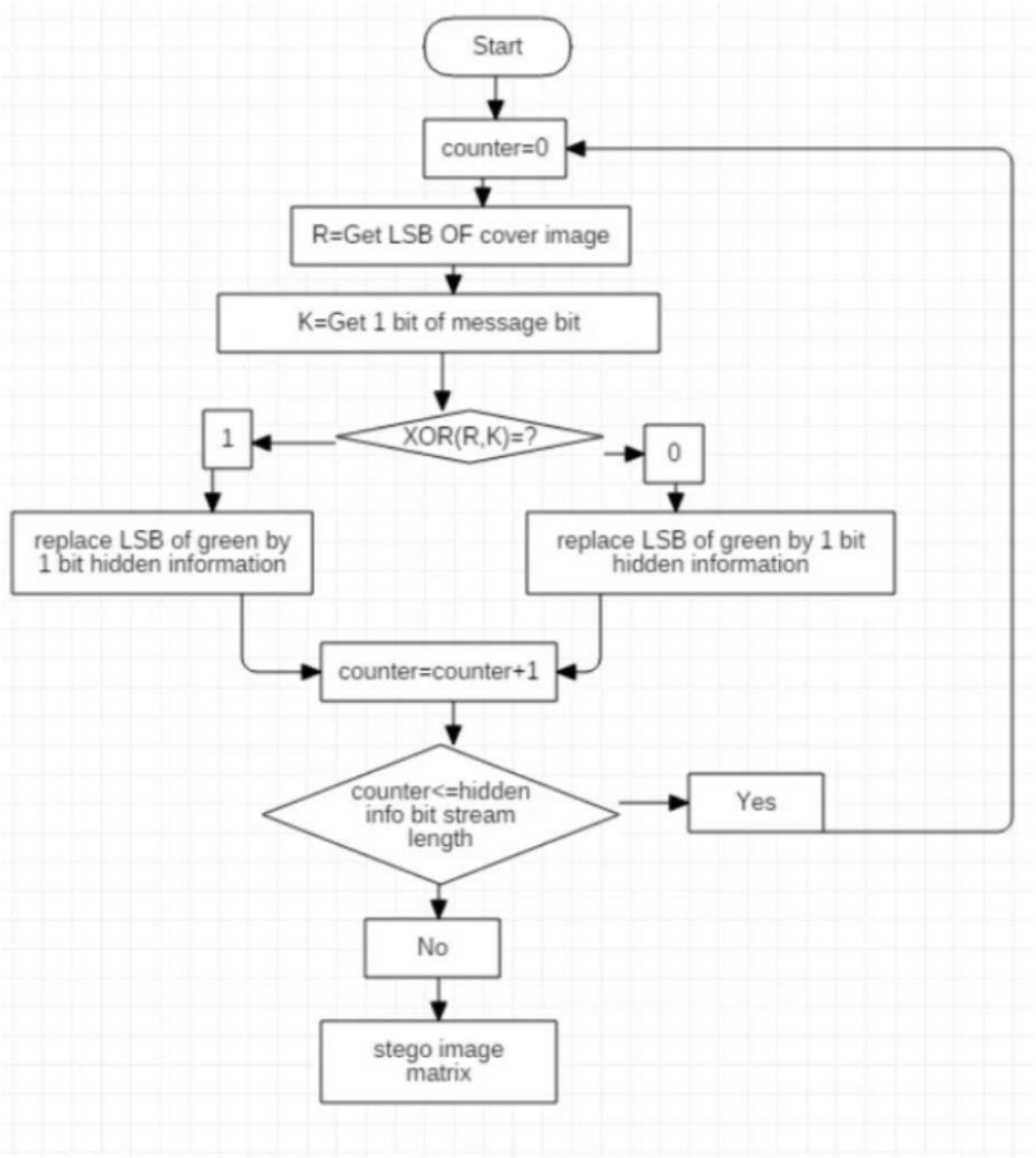

Figure 5.1: Encryption Diagram

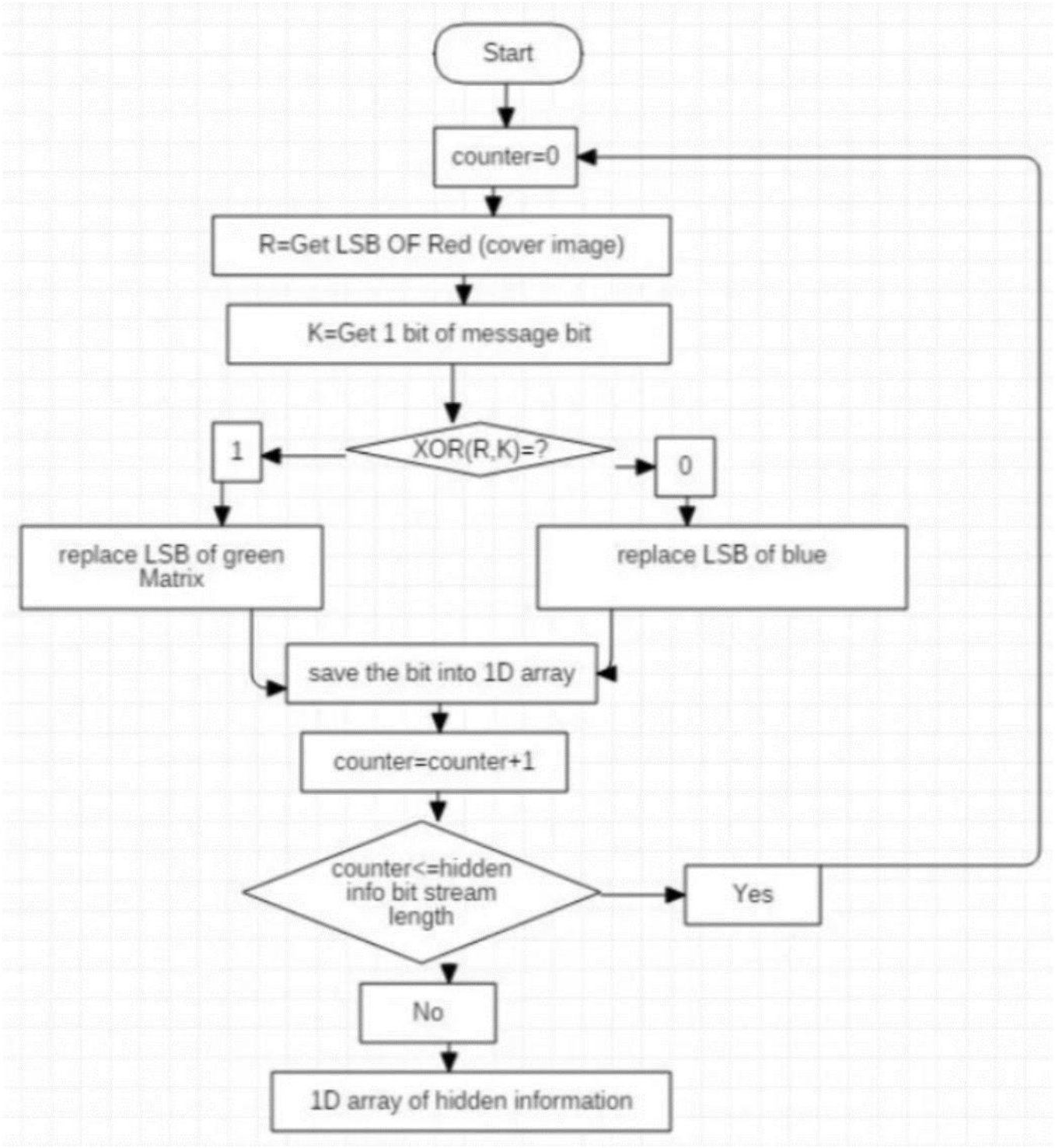

Figure 5.2: Decryption Diagram

5.1.2 Masking and Filtering

Masking and filtering 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 6

SYSTEM DESIGN

6.1 DFD Diagram

6.1.1 DFD level 0

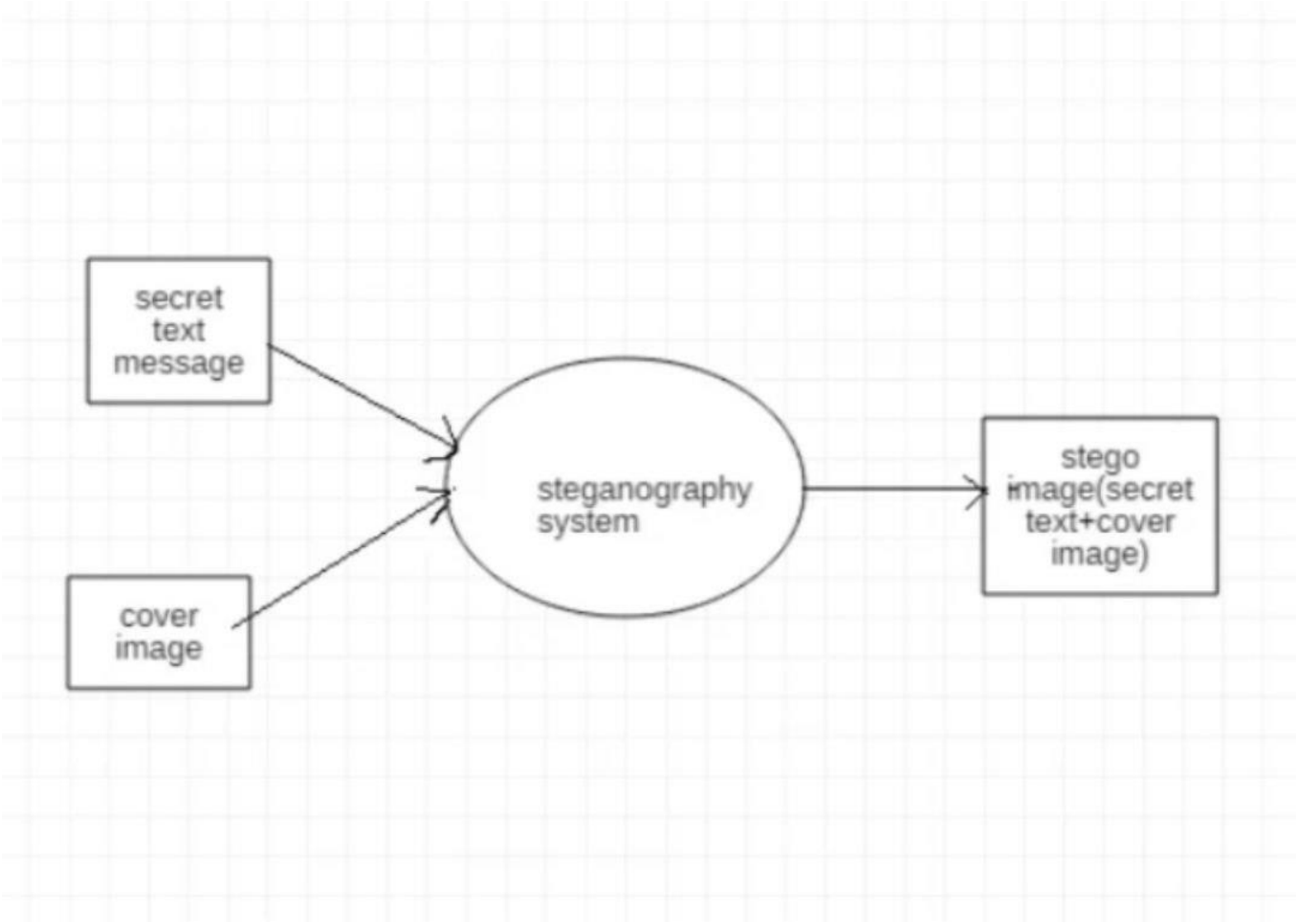

Figure6.1.1: Level 0 Diagram

6.1.2 DFD level 1

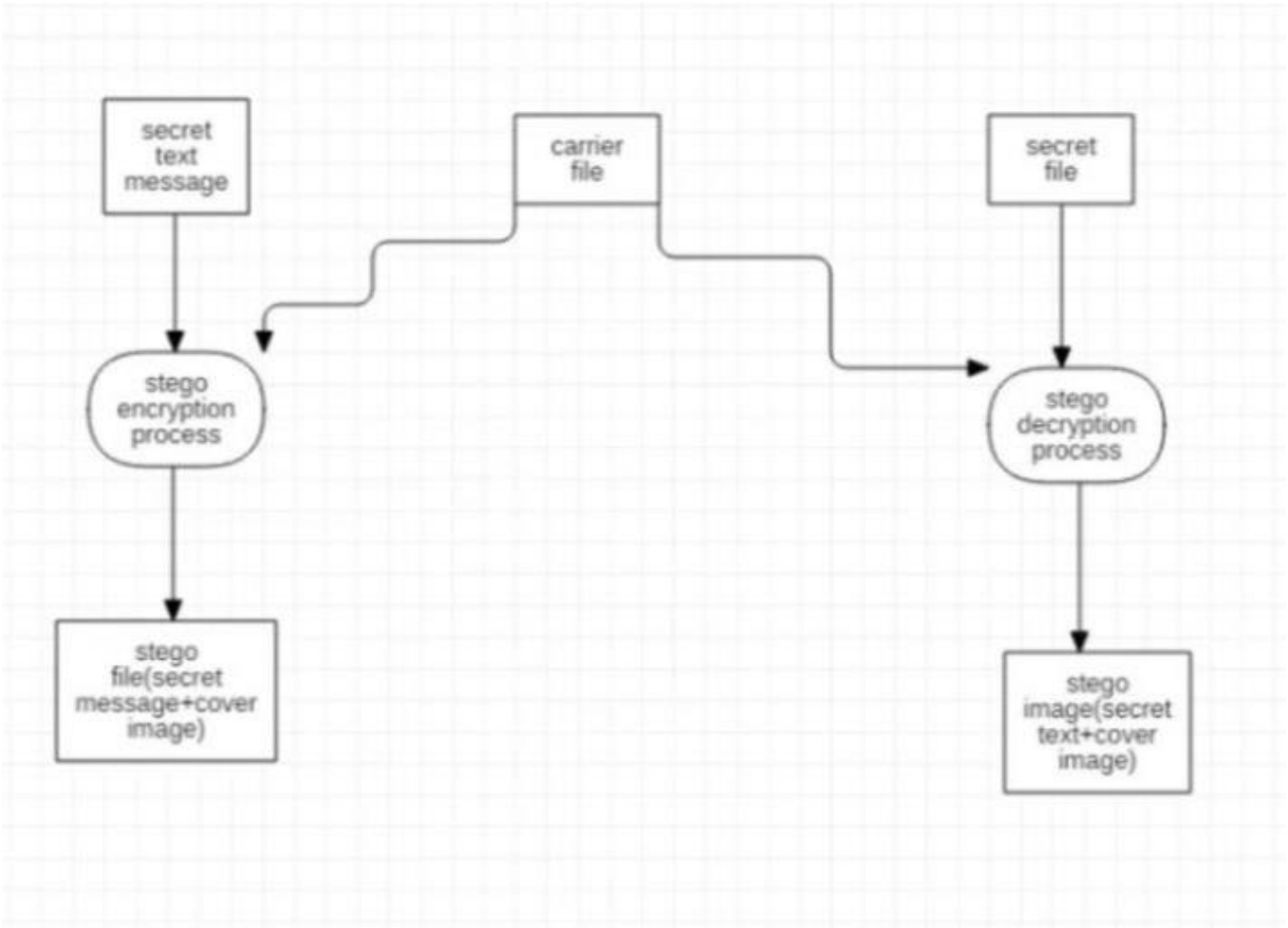

Figure6.1.2: Level 1 Diagram

6.1.3 DFD level 2

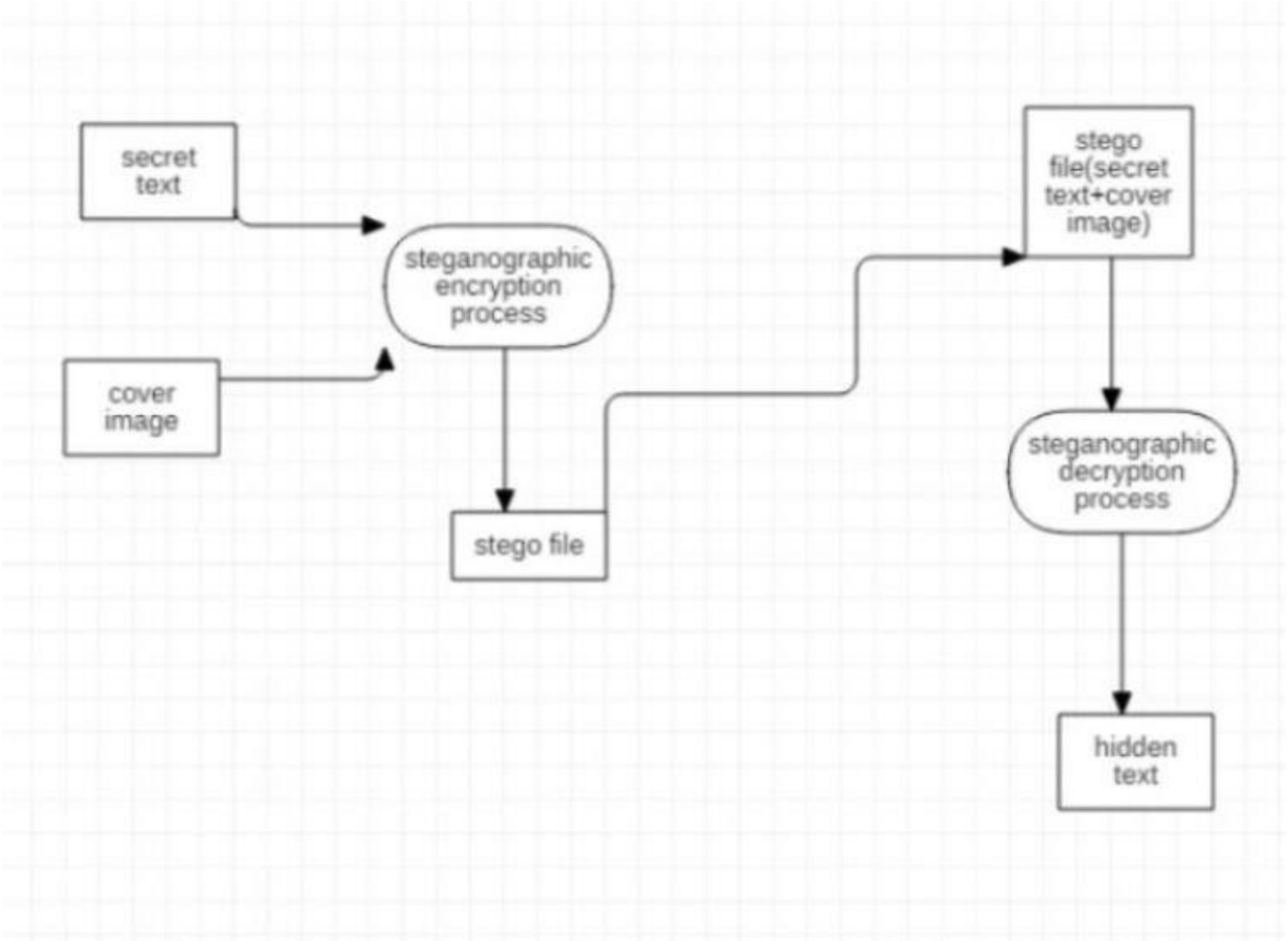

Figure6.1.3: Level 2 Diagram

6.2 Use case Diagram

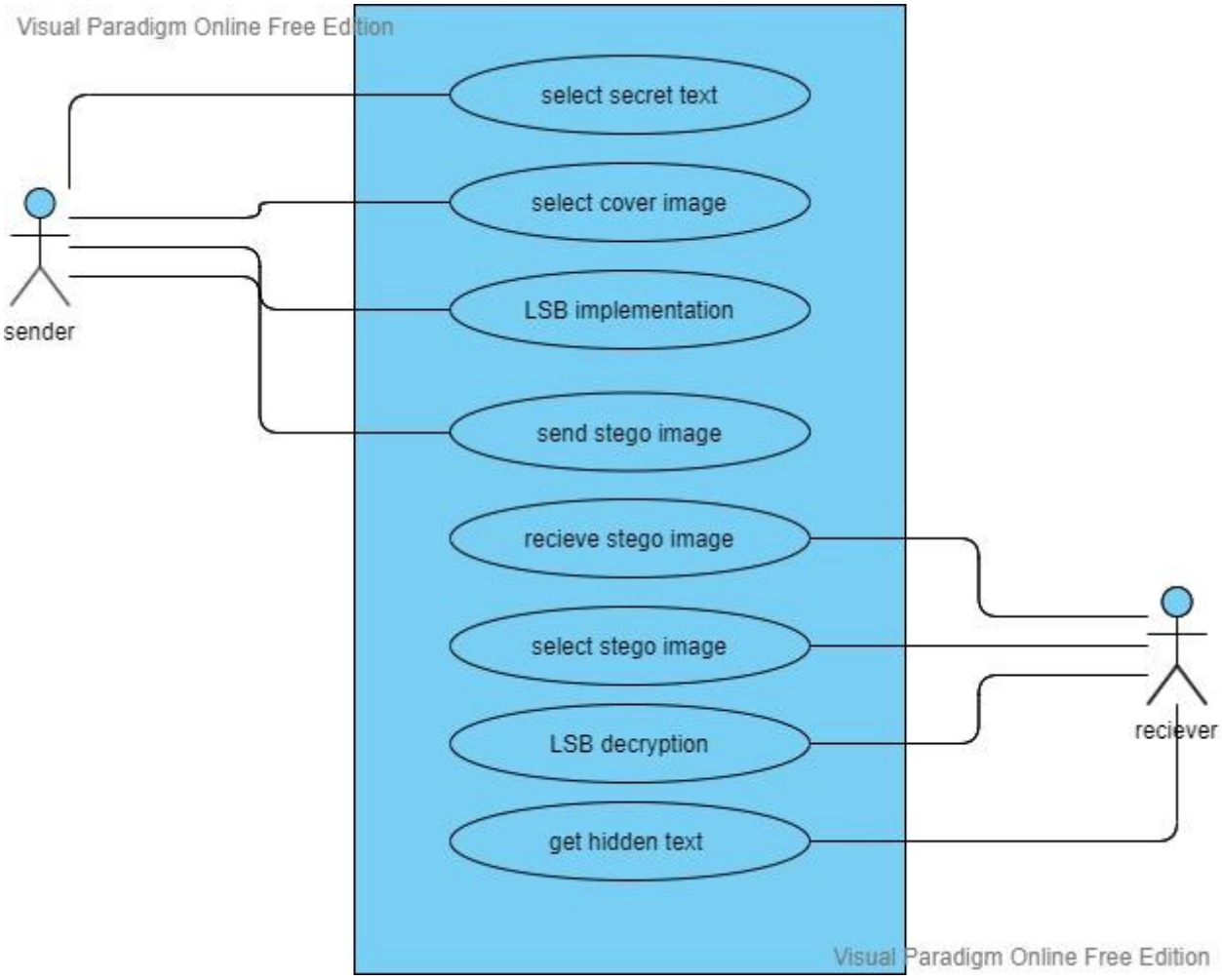

Figure6.2: Use case Diagram

6.3 Activity Diagram

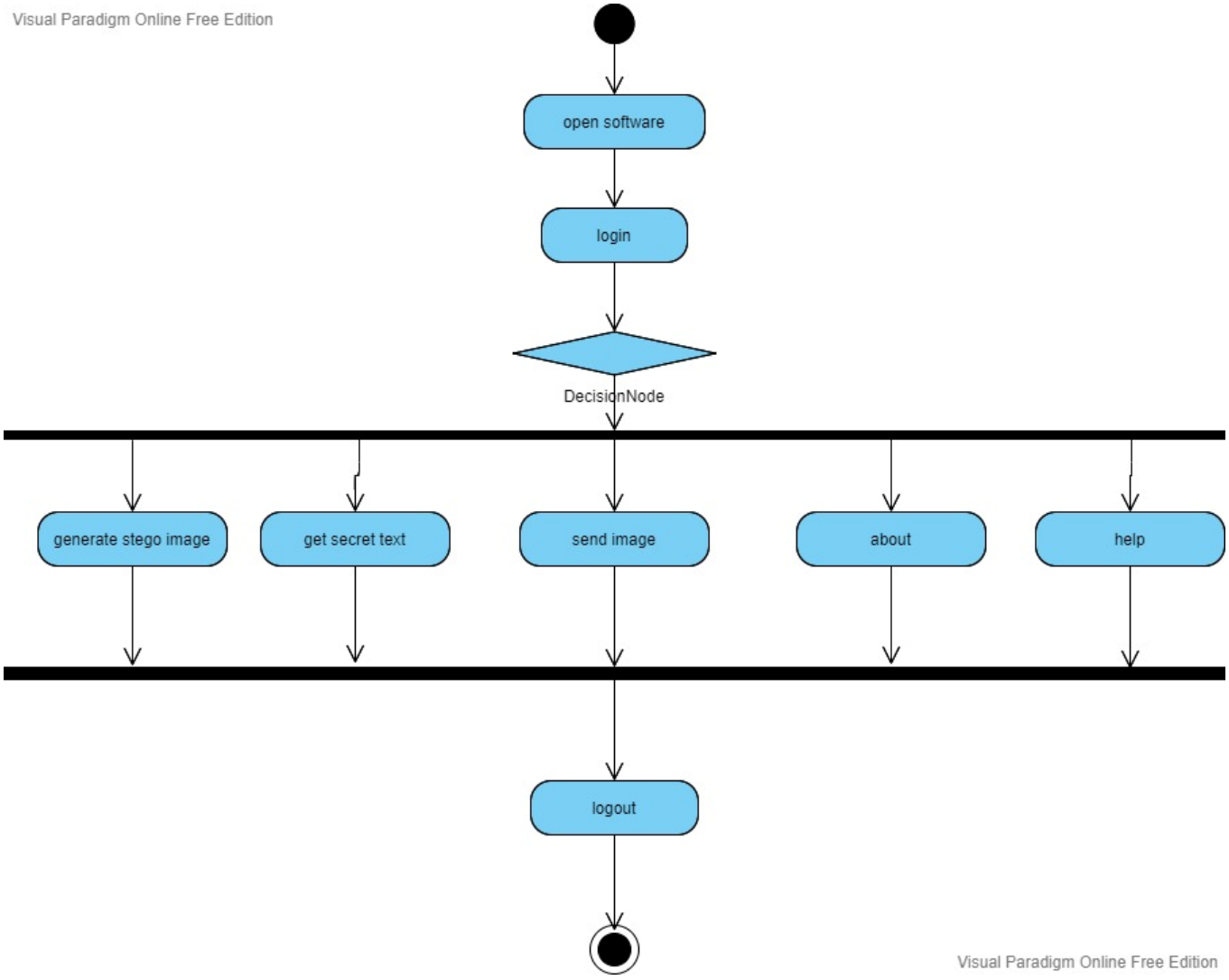

Figure6.3: Activity Diagram

6.4 Class Diagram

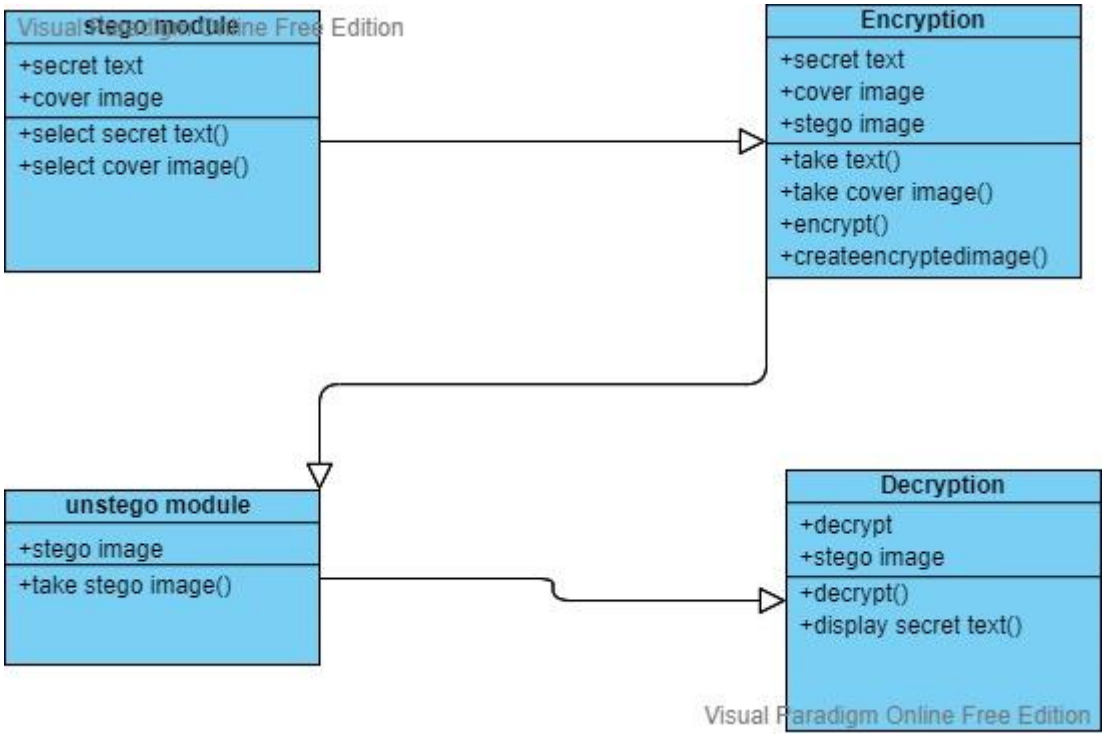

Figure6.4: Class Diagram

CHAPTER 7

SYSTEM IMPLEMENTATION

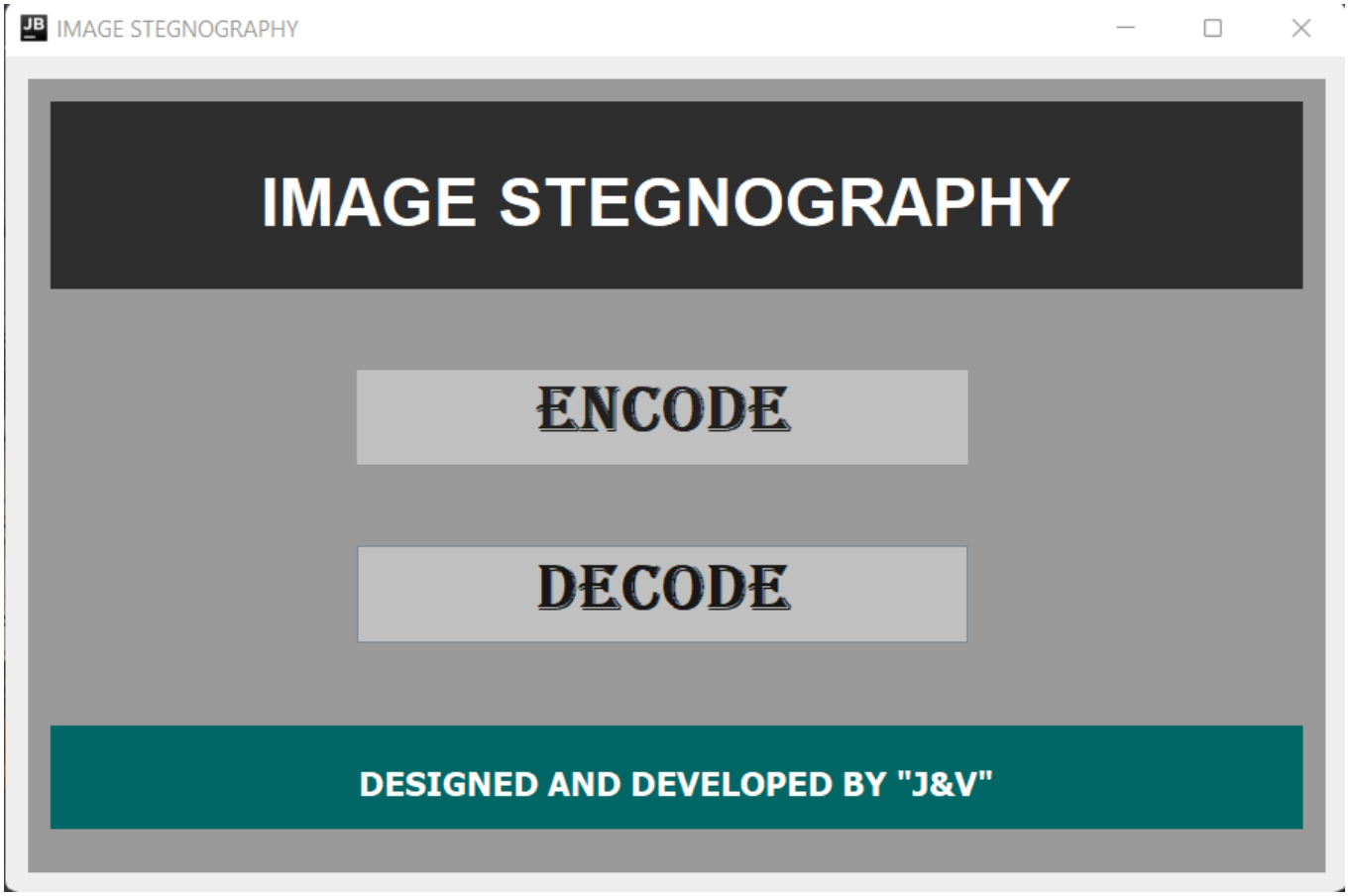

Figure7.1 Home Page

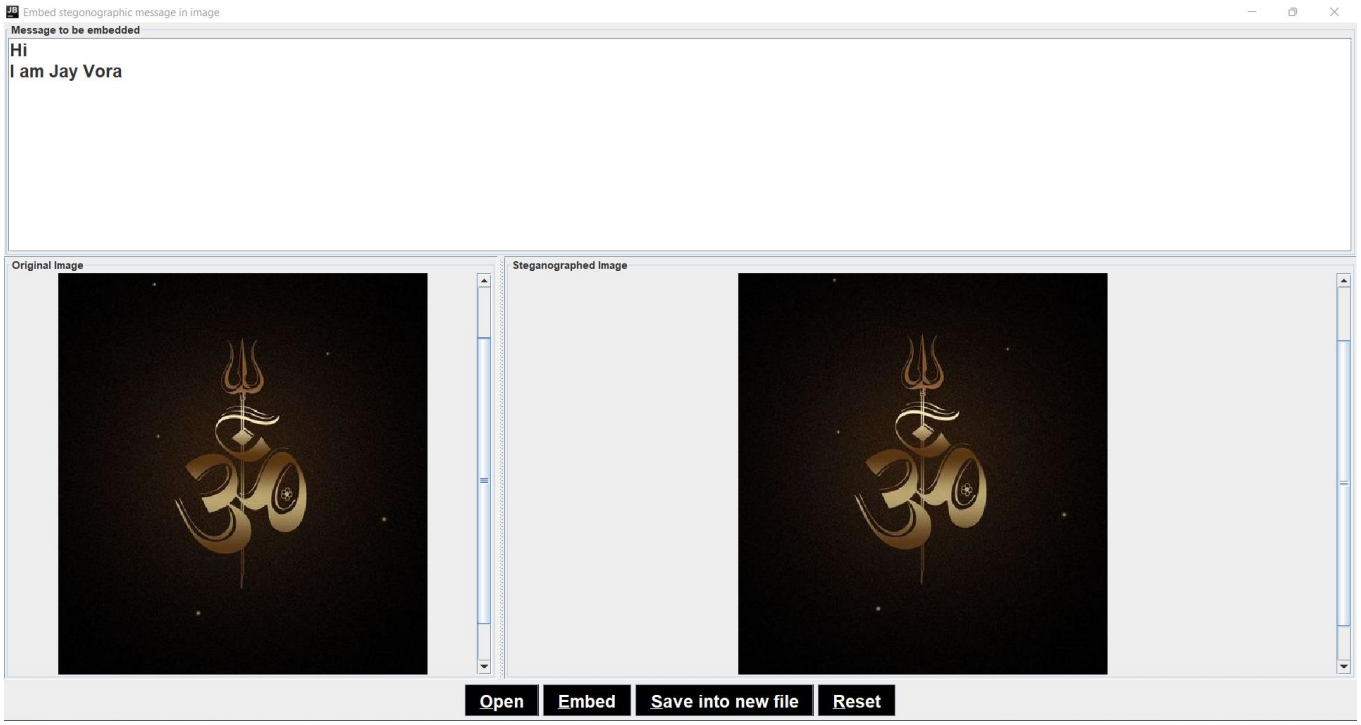

Figure7.2 Encode

This frame prompts you to enter secret message or secret file and the cover image to hide secret code or secret code file.

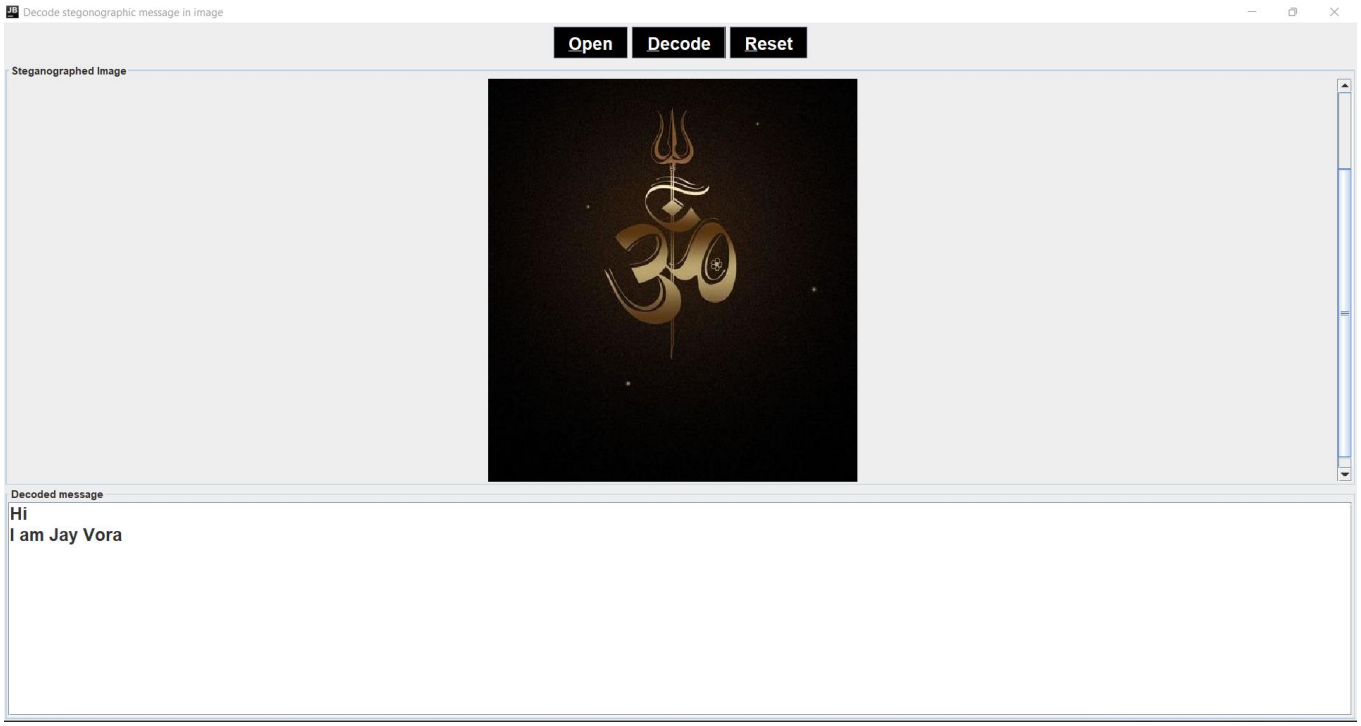

Figure7.3 Decode

This Window is about to decrypt image by choosing secret code file or secret code.

CHAPTER 8

LIMITATIONS

8.1 Advantage

- 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 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.

8.2 Disadvantage

- 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 mas
- sage can acquire.
- This software has been implemented by java, which is open source, therefore
- code is readable so anyone with bad mentality can made software perform inverse operation.
- Only unintended wer may know the actual working of software.
- Intruder may penetrate suspecting images to get hidden data

CHAPTER 9

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 nooded to commence a terrorist attack In the future, it is hoped that the technique of Steg analysis 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 displine, 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 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.

CONCLUSION

It is observed that through LSB Sulistitution 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, bit plane slicing is to be done individually for the top four bit-planes for each of R, G, B of the message

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. Le 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 does not appear very noisy when compared to the original cover image.