HIDING TEXT INTO IMAGE,AUDIO AND VIDEO USING STEGANOGRAPHY

A PROJECT REPORT

GALGOTIAS UNIVERSITY

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

Submitted by

Vishesh Gupta – 18021011814
Saima Imroz Khan - 18021011413

in partial fulfilment for the award of the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE

UNDER THE SUPERVISION OF
Dr. J.N. Singh
PROFESSOR

GALGOTIAS UNIVERSITY
GREATER NOIDA

December 2021

BONAFIDE CERTIFICATE

Certified that this project report **"HIDING TEXT INTO IMAGE,AUDIO AND VIDEO USING STEGANOGRAPHY "**is the bonafide work of "**VISHESH GUPTA & SAIMA IMROZ KHAN"** who carried out the project work under my supervision.

SIGNATURE
Dr. J.N. Singh

PROFESSOR
GALGOTIAS UNIVERSITY
GREATER NOIDA

SIGNATURE
Mr. HARDESH KUMAR

ASSISTANT PROFESSOR
GALGOTIAS UNIVERSITY
GREATER NOIDA

ABSTRACT

The objective of our research project is to convert the text into image, audio and video using steganography. Steganography is the art of hiding message. The goal of steganography is to hide the message in such a way that it cannot be interpreted by the intruder.BMP image format has been used for image steganography.The reason for using this image format is that the size and quality of the BMP image is very high so it is easy to hide the information in these type of image format. But Audio Steganography and Video Steganography can be performed on any type of audio file and video file without any problem of space complexity as the size of audio file is large enough for information hiding.The problem of the research project is that the size of the resulted image ,audio and video must not be increased after the text insertion.This problem has been removed by using L.S.B METHOD for Steganography.Thus ,the space complexity problem has been solved under this project of steganography.The quality of the stego may be deflated but it cannot be interpreted by the naked eyes and by hearing the audio.Future prospects of this project is the stego cannot be used further for steganography as by further performing the steganography on the stego object result in loss of information of the previous message.In addition to this, other future propect is that the large amount information hiding in the small size of object.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF SYMBOLS

f_E: steganographic function "embedding"

f_E^{-1}: steganographic function "extracting"

cover: cover data in which *emb* will be hidden

emb: message to be hidden

key: parameter of f_E

stego: cover data with the hidden message

wav: wave audio format

bmp: Bitmap image format

(1) INTRODUCTION

As long as there has been written communication, humans had the desire to conceal their messages from the curious eyes of others. The method of hiding one piece of information within another is called steganography. The meaning of this Greek term is ‘covered writing’.

Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication-to hide the existence of a message from a third party.

Steganography is the hiding of information within a more obvious kind of communication. Although not widely used, digital steganography involves the hiding of data inside a sound or image file.

The goal of Steganography

The goal of steganography is to avoid drawing attention to the transmission of a hidden message. If suspicion is raised, then this goal is defeated.
A steganographic message generally appears to be something else, like an article or a picture, or some other "cover" message. Drawings have often been used to conceal information since it is easy to encode a message by varying lines, colors or other elements in pictures.

Steganography was booming in World War II. Another method was to camouflage secret messages through null ciphers contained in innocent messages, which passed the enemy’s mail filters. Because these methods became more and more insecure due to increasing detection efforts, the Germans developed the microdot technology. Microdots are photographs the size of a printed period having the clarity of standard-sized typewritten pages. The first microdots were discovered masquerading as a period on a typed envelope carried by a German agent in 1941. The message was neither hidden nor encrypted, but

was too small to attract attention – at least for a while.

Unfortunately steganography can also be used for illegitimate purposes. For example, if someone was trying to steal data, they could conceal it in files and send it out in an innocent looking email or file transfer.

The purpose of steganography is covert communication to hide a message from a third party. This differs from cryptography, the art of secret writing, which is intended to make a message unreadable by a third party but does not hide the existence of the secret communication. Although steganography is separate and distinct from cryptography, there are many analogies between the two, and some authors categorize steganography as a form of cryptography since hidden communication is a form of secret writing.

This paper is intended as a high-level technical introduction to steganography for those unfamiliar with the field.

1.1STEGANOGRAPHY: THE HISTORY

1.1.1 Steganography In Second World War

Steganography dates back to ancient Greece when etching messages or images in wooden tablets and covering them with wax, and tattooing a shaved messenger's head, letting the hair grow back, and then shaving the head again to read the message were common practices.

Early in WWII steganographic technology consisted almost exclusively of **invisible inks**. Sources for invisible inks include milk, vinegar, fruit juices and urine that darken when heated. The following message was sent by a German spy during WWII :

1.1.2. Usage of Null Ciphers and Microdots

Usage of Null Ciphers

Historically, null ciphers are a way to hide a message in another without the use of a complicated algorithm. One of the simplest null ciphers is shown in the classic examples below:

When invisible inks became easy to decode through improved technology, **null ciphers** were used. Null ciphers are unencrypted messages that are indiscernible in innocent sounding messages.

Usage of Microdots

The Germans developed the microdot technology during WWII. **Microdots** are text or photographic images that are shrunk down to the size and shape of a period or the dot of an i or j. Microdots were usually sent by writing a letter containing periods, i's, or j's, and the intended recipient could read the messages using a microscope. Because of the extremely small size of the microdots the messages typically went unnoticed by inspectors.

1.2 STEGANOGRAPHY: THE BASICS

Steganography is a branch of cryptography. While most cryptography applications are used to encrypt information so that only the sender and recipient can understand it, steganography hides information that only the sender and recipient know it exist. The secret message is hidden in plain sight. The public may see the data, unaware that a hidden message is present.

Steganography is used not only to digital images but also to other media such as voice, text and binary files, and communication channels.

. Steganography provides some very useful and commercially important functions in the digital world, most notably digital watermarking. In this application, an author can embed a hidden message in a file so that ownership of intellectual property can later be asserted and/or to ensure the integrity of the content. An artist, for example, could post original artwork on a Website. If someone else steals the file and claims the work as his or her own, the artist can later prove ownership because only he/she can recover the watermark. Although conceptually similar to steganography, digital watermarking usually has different technical goals. Generally only a small amount of repetitive information is inserted into the carrier, it is not necessary to hide the watermarking information, and it is useful for the watermark to be able to be removed while maintaining the integrity of the carrier.

Steganography has a number of nefarious applications; most notably hiding records of illegal activity, financial fraud, industrial espionage, and communication among members of criminal or terrorist organizations.

1.2.1Basic Principles

The basic principles of Stegnography are as follows:

Digital files can be altered to a certain degree without losing functionality.

The senses of human beings are not acute enough to distinguish minor changes in altered files.

BMP contain unused areas, to hide the things, inserting data in those areas.

1.2.2Covert channel

In information theory, a covert channel is a communications channel that does a writing-between-the-lines form of communication. Typically a covert channel is parasitic to its host channel; it reduces bandwidth of the host channel by reducing the signal-to-noise ratio in the host channel. Observers are unaware that a covert message is being communicated. Only the sender and recipient of the message notice it.

For example, in steganography hidden messages are encoded within pictures or other data in such a way that the picture does not appear to be altered. To an outside observer the picture would appear innocuous, but the recipient is able to extract the message from within the image.

A covert channel could be defined as a communications channel that transfers some kind of information using a method originally not intended to transfer this kind of information. The term is used in the TCSEC specifically to refer to ways of transferring information from a higher classification compartment to a lower classification. There are two kinds of covert channels: storage channels, which communicate by modifying a stored object; and timing channels, which transmit information by affecting the relative timing of events

1.2.3Cryptography Vs Steganography

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this is in contrast to cryptography, where the existence of the message is clear, but the meaning is obscured. Notice that there is a difference between concealing and disguising a message. In the first case, the message is made invisible (ie via the old lemon trick), whereas in the second case the message is visible, however, it is enciphered and has to be deciphered.

The purpose of steganography is covert communication to hide a message from a third party. This differs from cryptography, the art of secret writing, which is intended to make a message unreadable by a third party but does not hide the existence of the secret communication. The following are the differences between Cryptology and Stegnography

Cryptography

Messages are not hidden.

Enemy can intercept the messages.

Enemy can decrypt the messages.

Steganography

Message is hidden.

Enemy must discover the medium.

Although steganography is separate and distinct from cryptography, there are many analogies between the two, and some authors categorize steganography as a form of cryptography since hidden communication is a form of secret writing.

1.3 STEGANOGRAPHY TAXONOMY

Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuries-for fun by children and students and for serious espionage by spies and terrorists. Microdots and microfilm, a staple of war and spy movies, came about after the invention of photography (Arnold et al. 2003; Johnson et al. 2001; Kahn 1996; Wayner 2002).

Steganography hides the covert message but not the fact that two parties are communicating with each other. The steganography process generally involves placing a hidden message in some transport medium, called the carrier. The secret message is embedded in the carrier to form the steganography medium. The use of a steganography key may be employed for encryption of the hidden message and/or for randomization in the steganography scheme. In summary:

steganography_medium = hidden_message + carrier + steganography_key

Figure 1 shows a common taxonomy of steganographic techniques.

• Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size-reduction methods.

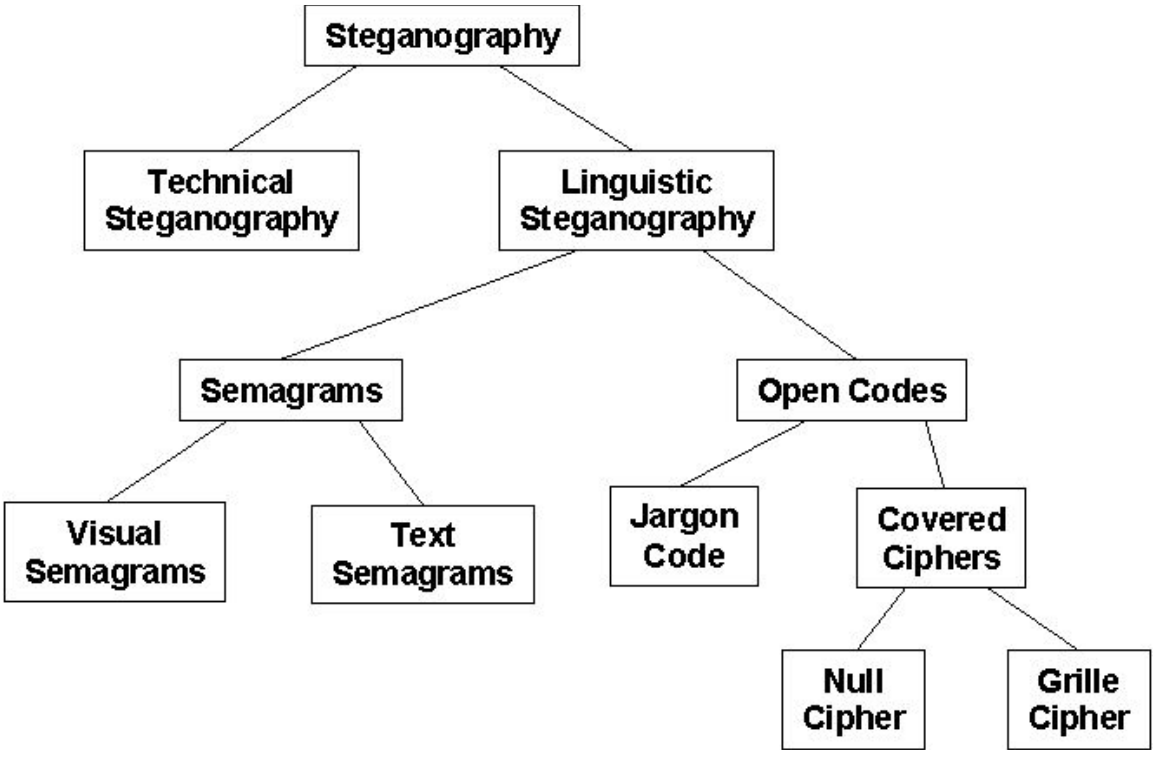
• Linguistic steganography hides the message in the carrier in some no obvious ways and is further categorized as semagrams or open codes.

• Semagrams hide information by the use of symbols or signs. A visual semagram uses innocent-looking or everyday physical objects to convey a message, such as doodles or the positioning of items on a desk or Website. A text semagram hides a message by modifying the appearance of the carrier text, such as subtle changes in font size or type, adding extra spaces, or different flourishes in letters or handwritten text.

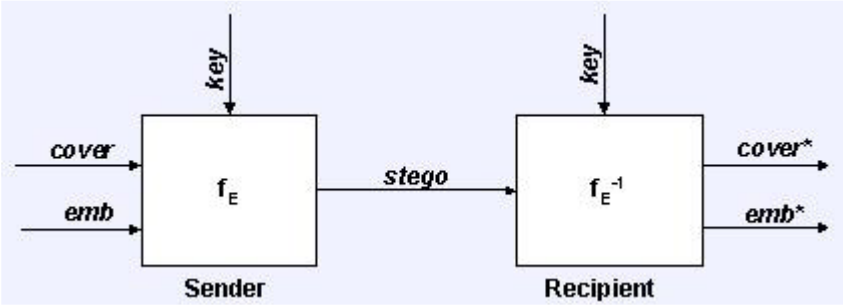
• Open codes hide a message in a legitimate carrier message in ways that are not obvious to an unsuspecting observer. The carrier message is sometimes called the overt communication whereas the hidden message is the covert communication. This category is subdivided into jargon codes and covered ciphers.

• Jargon code, as the name suggests, uses language that is understood by a group of people but is meaningless to others. Jargon codes include warchalking (symbols used to indicate the presence and type of wireless network signal, underground terminology, or an innocent conversation that conveys special meaning because of facts known only to the speakers. A subset of jargon codes is cue codes, where certain prearranged phrases convey meaning.

• Covered or concealment ciphers hide a message openly in the carrier medium so that it can be recovered by anyone who knows the secret for how it was concealed. A grille cipher employs a template that is used to cover the carrier message. The words that appear in the openings of the template are the hidden message. A null cipher hides the message according to some prearranged set of rules, such as "read every fifth word" or "look at the third character in every word."



1.4. STEGANOGRAPHY SYSTEM



f_E: steganographic function "embedding"

f_E^{-1}: steganographic function "extracting"

cover: cover data in which *emb* will be hidden

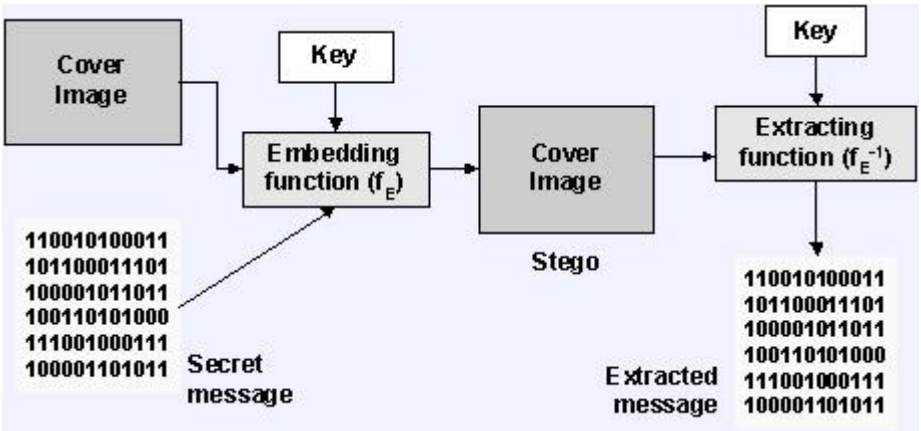
emb: message to be hidden

key: parameter of f_E

stego: cover data with the hidden message

A Graphical Version of the Steganographic System

Modern steganography refers to hiding information in digital picture files and audio files. It works by replacing bits of unused data in regular digital files with bits of invisible information. To embed hidden information into an image requires two files - the cover image file that will hold the hidden data and the secret message file. A message may be plain text, cypher text (or another image). When combined, the cover image and the hidden message makes a stego image. A stego-key or password may be used to hide and decode the message.



1.5 STEGANALYSIS

Steganalysis is "the process of detecting steganography by looking at variances between bit patterns and t of discovering and rendering useless covert messages. Steganalysis is a relatively new research discipline with few articles appearing before the late-1990s. The challenge of steganalysis is that: • The suspect information stream, such as a signal or a file, may or may not have hidden data The hidden data, if any, may have been encrypted before inserted into the signal or file. suspect information stream and cannot be sure that it *is* being used for transporting secret **analysis Vs cryptanalysis** t of suspect information streams to a subset of most likely altered information streams. This is usually done with statistical analysis using advanced statistics techniques. The problem is generally handled with statistical analysis. A set of unmodified files of the same type, and ideally from the same source (for example, the same model of digital camera, or if possible, the *same* digital camera; digital audio from a CD MP3 files have been "ripped" from; etc.) as the set being inspected, are analyzed for various statistics. Some of these are as simple as spectrum analysis, but since most image and audio files these days are compressed with lossy compression algorithms, such as JPEG unusually large file sizes". It is the ar

Goal and challenges of Steganalysis The goal of steganalysis is to identify suspected information streams, determine whether or not they have hidden messages encoded into them, and, if possible, recover the hidden information.

encoded into them. •

•Some of the suspect signal or file may have noise or irrelevant data encoded into them (which can make analysis very time consuming).

• Unless it is possible to fully recover, decrypt and inspect the hidden data, often one has only a information.

1.6 STEGANOGRAPHY USED

1.6.1IMAGE STEGANOGRAPHY

When hiding information inside images the LSB (Least Significant Byte) method is usually used.To a computer an image file is simply a file that shows different colors and intensities of light ondifferent areas of an image.

The best type of image file to hide information inside of is a 24 Bit BMP (Bitmap) image.

The reason being is this is the largest type of file and it normally is of the highest quality. When an image is of high quality and resolution it is a lot easier to hide and mask information inside of.

Although 24 Bit images are best for hiding information inside of due to their size some people may choose to use 8 Bit BMP's or possibly another image format such as GIF, the reason being is that posting of large images on the internet may arouse suspicion.

It is important to remember that if you hide information inside of an image file and that file is converted to another image format, it is most likely the hidden information inside will be lost.

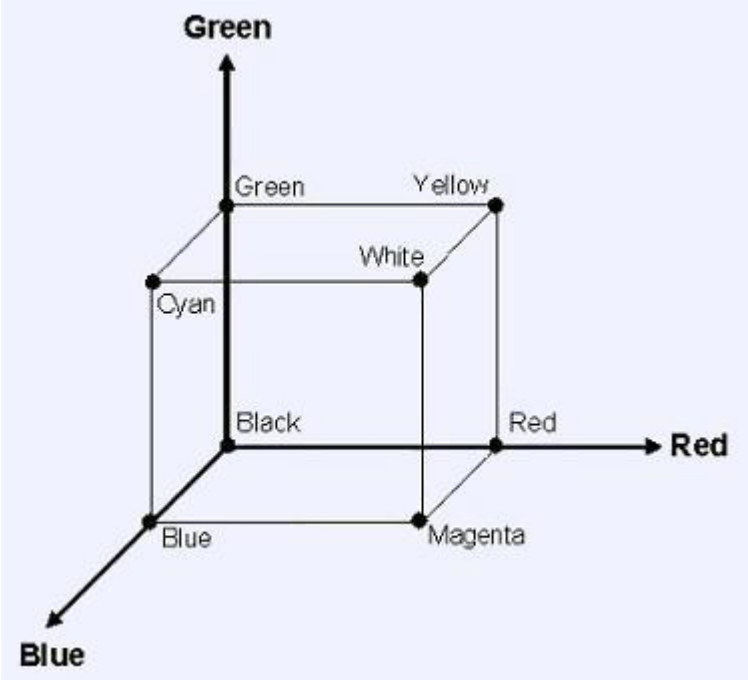
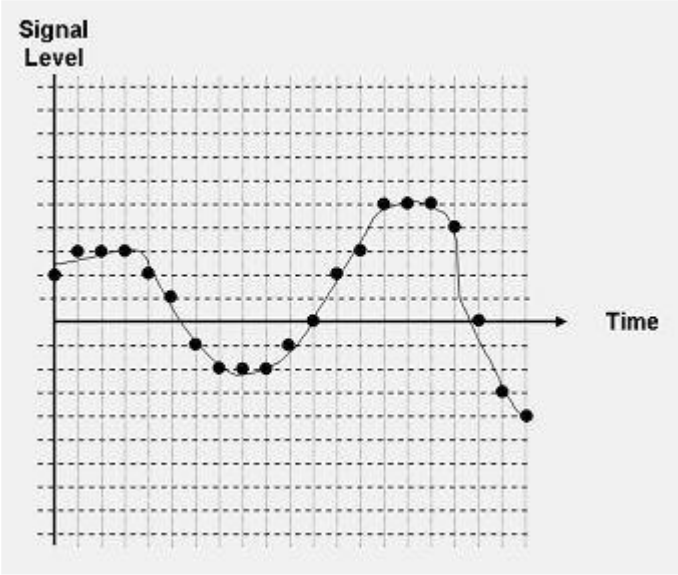


IMAGE REPRESENTATION IN 3D SPACE

1.6.2 AUDIO STEGANOGRAPHY

When hiding information inside Audio files the technique usually used is low bit encoding which is some what similar to LSB that is generally used in Images.
The problem with low bit encoding is that it is usually noticeable to the human ear, so it is a rather risky method for someone to use if they are trying to mask information inside of an audio file.
Spread Spectrum is another method used to conceal information inside of an audio file.
This method works by adding random noises to the signal the information is conceal inside a carrier and spread across the frequency spectrum.

Echo data hiding is yet another method of hiding information inside an audio file.
This method uses the echoes in sound files in order to try and hide information.
By simply adding extra sound to an echo inside an audio file, information can be concealed. The thing that makes this method of concealing information inside of audio files better than other methods is that it can actually improve the sound of the audio inside an audio file.



WAVE REPRESENTATION OF AUDIO FILE

1.6.4 VIDEO STEGANOGRAPHY

When information is hidden inside video the program or person hiding the information will usually use the DCT (Discrete Cosine Transform) method.
DCT works by slightly changing the each of the images in the video, only so much though so it's isn't noticeable by the human eye. To be more precise about how DCT works, DCT alters values of certain parts of the images, it usually rounds them up.

For example if part of an image has a value of 6.667 it will round it up to 7.
Steganography in Videos is similar to that of Steganography in Images, apart from information is hidden in each frame of video.

When only a small amount of information is hidden inside of video it generally isn't noticeable at all, however the more information that is hidden the more noticeable it will become.

2 LITERATURE REVIEW

A *bitmap* is a graphical object used to create, manipulate (scale, scroll, rotate, and paint), and store images as files on a disk. A Bitmap image has two parts

- Information Header
- Image Content

The BITMAP FILE HEADER structure contains information about the type, size, and layout of a file that contains a DIB.

Size of BITMAPFILEHEADER is 14 Bytes.

bfOffBits specifies the offset, in bytes, from the BITMAPFILEHEADER structure to the bitmap bits.

(2.1) PROGRAM LOGIC

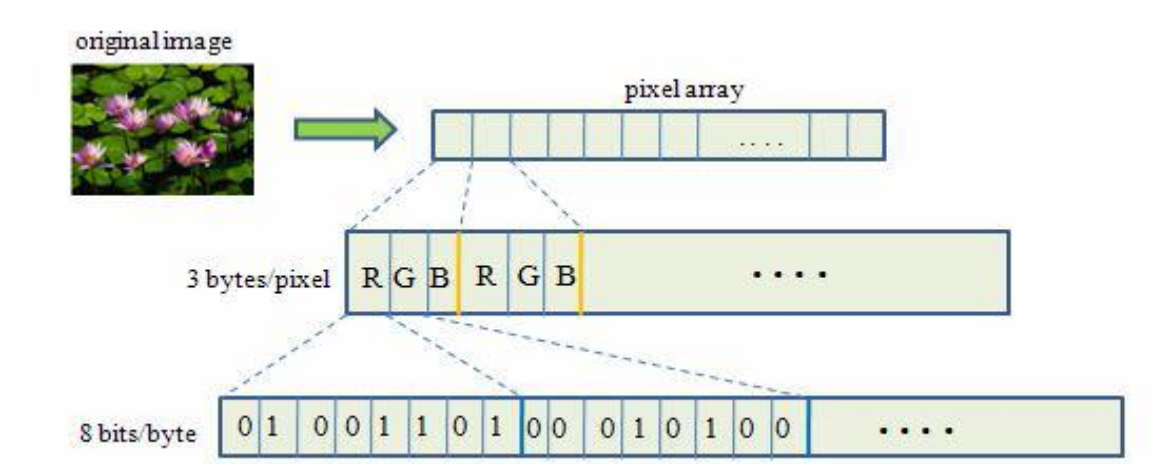
(LEAST SIGNIFICANT BIT SUBSTITUTION)

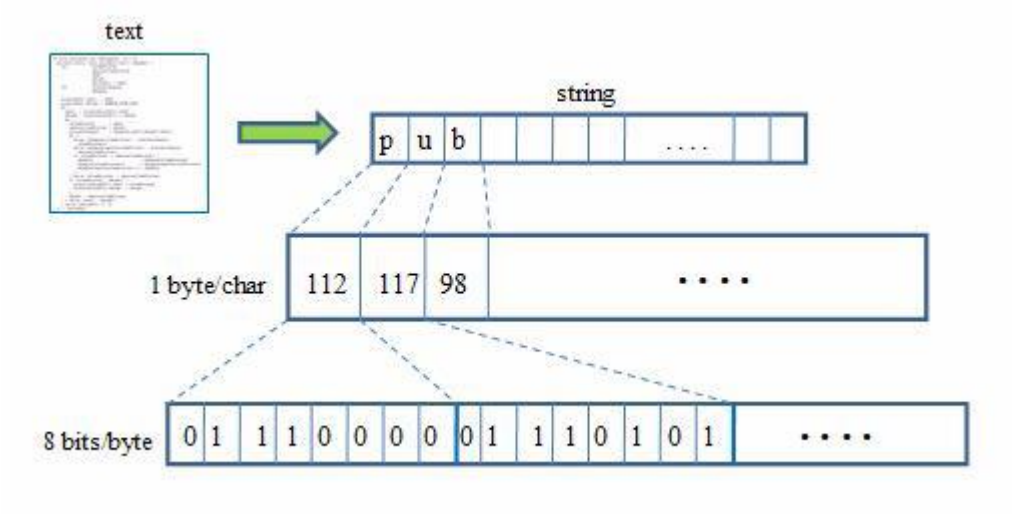
Least significant bit insertion Data Hiding in Image

LSB insertion is the easiest and one of the most commonly used techniques to implement Data hiding in Image. It makes use of the fact that any change in the LSB of the data field of an image is not detected by the human eye without any distinction. The LSB insertion technique can similarly be applied to audio files also.

Following steps are implemented for the LSB insertion:-

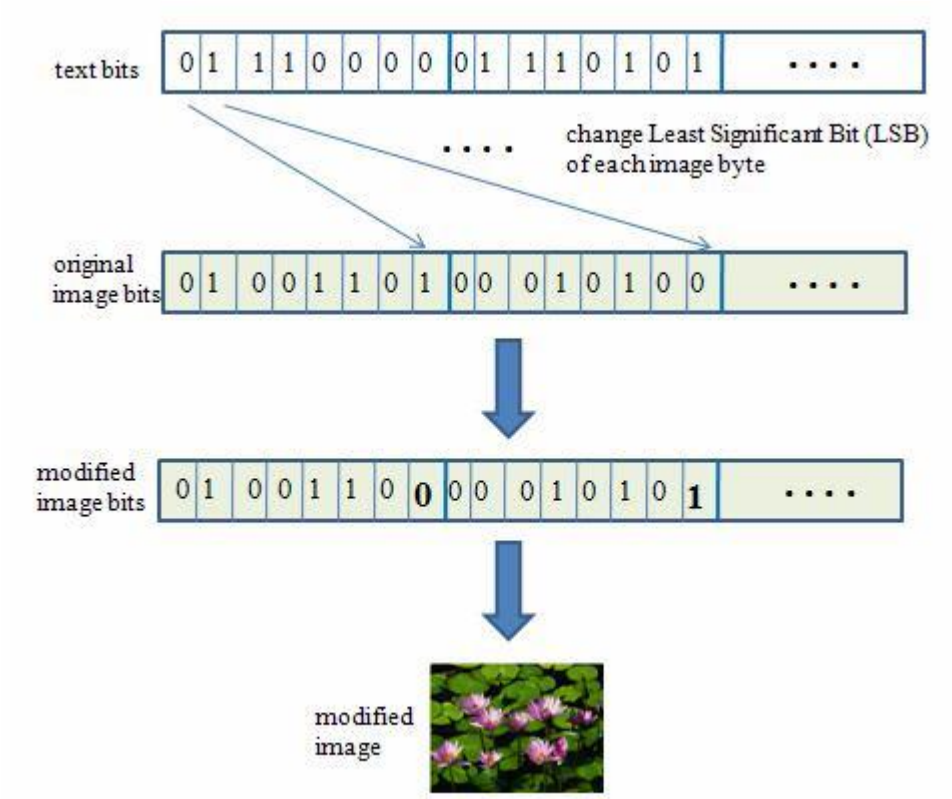
1. Read the container file and the text byte to byte.





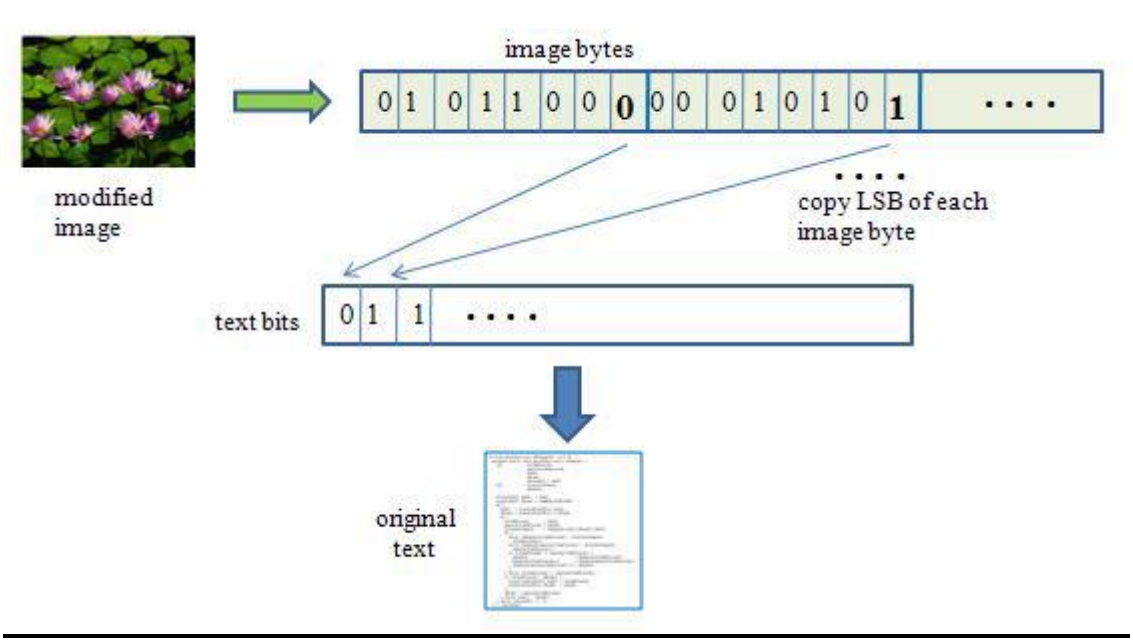
2. Replace the LSB of the source file with the text bit.

3. Store the resultant byte in the Image file.



Following steps are implemented for the retrieval of data from a file:-

1. Read the source file byte to byte.
2. Collect the LSB of every byte.
3. Combine the LSB to retrieve back the hidden data.



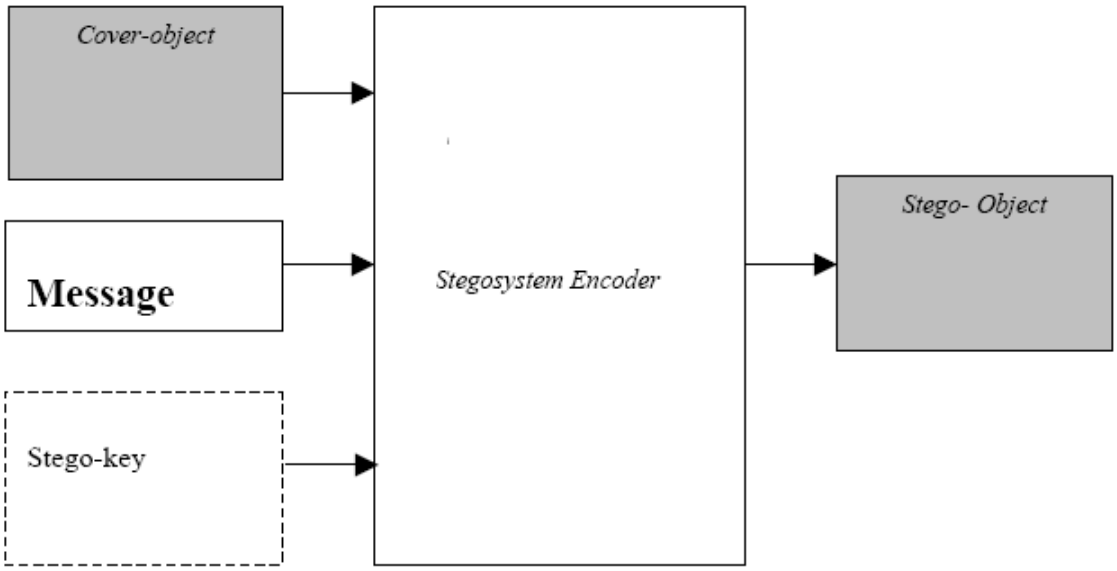
ADVANTAGES OF LSB INSERTION TECHNIQUE

- **ENCRYPTION**: The data to be embedded is first encrypted and then embedded in to the image. There are many algorithms which are used for the encryption hence at the time of retrieval user can get the meaningful data if he knows the algorithm applied and the key used for encryption.
- **SELECTIVE INSERTION**: In this only the selected bytes of the container file are modified. In this case the amount of the data stored in an image would decrease but it is fairly acceptable from the security point of view.

- **HIGH LEVEL LSB INSERTION**: We hide the data in more than one bit of a byte taking in to account that there is no distortion in the final file. This has two advantages:-

- More data is stored in the image file.

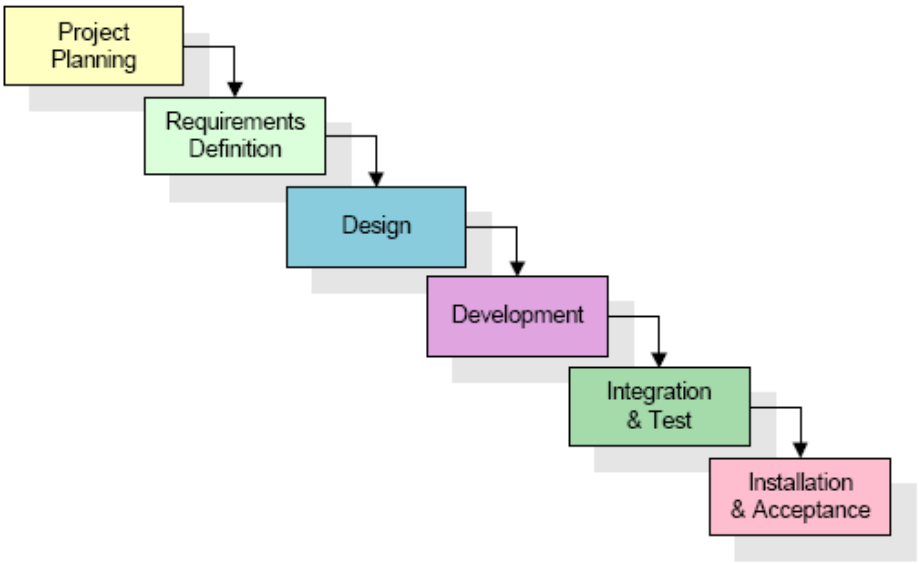
- Any intruder might not be able to retrieve the data as he will only look for single bit from a file.



Basic Model of Steganography

2.2 RESEARCH DEVELOPMENT LIFE CYCLE

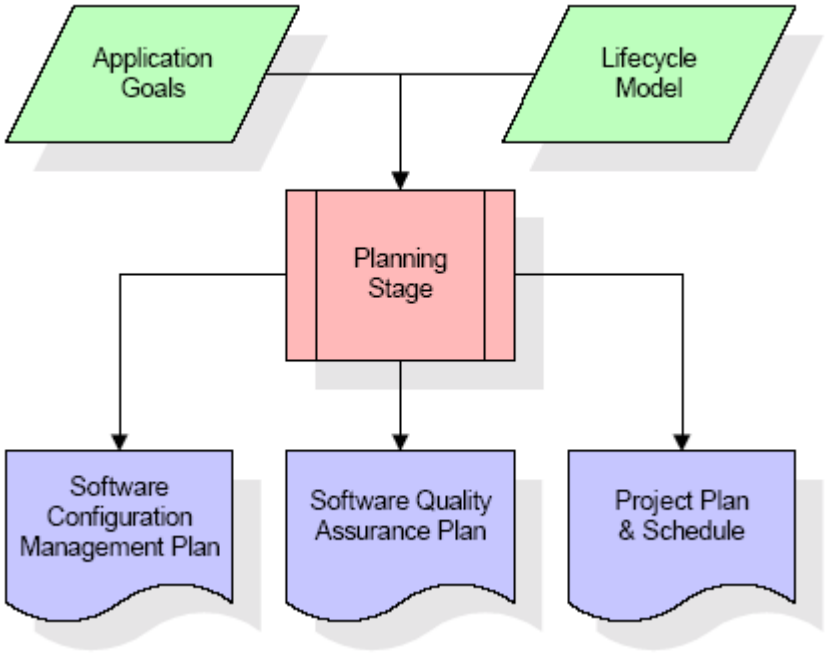
Research projects are generally broken down into six main stages as shown in the below diagram:



The six stages of the SDLC or RDLC are designed to build on one another, taking the outputs from the previous stage that serve as the initial inputs for the following stage.

During each stage, additional information is gathered or developed, combined with the inputs, and used to produce the results that leverage the previous effort and are directly traceable to the previous stages. This project is implemented using Waterfall model.

PLANNING STAGE



The most critical section of the project plan is a listing of high-level product requirements, also referred to as goals. All of the software product requirements to be developed during the requirements definition stage flow from one or more of these goals. The minimum information for each goal consists of a title and textual description.

Information is rapidly available through the Internet. Companies have the ability to communicate with a worldwide audience through the World Wide Web. So Information hiding techniques are received increasing attention due to:

a. The availability of multimedia and digital form objects.

b. The need to present solutions to criminal copying.

The Internet as a whole does not use secure links, thus information in transit may be vulnerable to interception as well. The important of reducing a chance of the information being detected during the transmission is being an issue now days. One solution is how to pass information in a manner that the very existence of the message is unknown in order to repel attention of the potential attacker.

In this project, we clarify what Steganography is, the definition, the importance as well as the technique used in implementing Steganography.

REQUIREMENTS DEFINITION STAGE

This is a high-level requirements section of the project plan. Each goal will be refined into a set of one or more requirements. These requirements define the major functions of the intended application, define operational data areas and reference data areas, and define the initial data entities.

Major functions include critical processes to be managed, as well as mission critical inputs, outputs and reports. A user class hierarchy is developed and associated with these major functions, data areas, and data entities.

Each of these definitions is termed a Requirement. Requirements are identified by unique requirement identifiers and, at minimum, contain a requirement title and textual description.

Steganography can be implemented by using three different approaches:

1. Least significant bit
2. Masking and filtering

3. Algorithms and transformation.

We focus on the Least Significant Bit (LSB) technique in hiding messages in an image. The system enhanced the LSB technique by randomly dispersing the bits of the message in the image and thus making it harder for unauthorized people to extract the original message. We are using Symmetric key encryption aprroach.

RESOURCE REQUIREMENTS

Minimum Hardware Requirements

- Intel Pentium 66 Mhz or equivalent processor
- 8 MB RAM.
- 20 GB Hard disk Storage Device

Recommended Hardware Requirements

- Intel Pentium 233 Mhz or above equivalent processor
- 32 MB RAM
- 20 GB Hard disk Storage Device

Software Resource Requirements:

- Dos 5.x or above.
- Windows 9.x operating system running DOS based application.
- TURBOC C compiler

2.3.3 DESIGN STAGE

The design stage takes as its initial input the requirements identified in the approved requirements document. For each requirement, a set of one or more design elements will be produced as a result of interviews, workshops, and/or prototype efforts.

Design elements describe the desired software features in detail, and generally include functional hierarchy diagrams, screen layout diagrams, tables of business rules, business process diagrams, pseudocode, and a complete entity-relationship diagram with a full data dictionary. These design elements are intended to describe the software in sufficient detail that skilled programmers may develop the software with minimal additional input.

The project is implemented using C programming language. It is based on modular design approach using three modules:

1..Main Module

2. Hide Image Module

3.Retrieve Image Module

Following steps are implemented for the LSB insertion:-

1. Read the container file and the text byte to byte.
2. Replace the LSB of the source file with the text bit.

3. Store the resultant byte in the Image file.

Following steps are implemented for the retrieval of data from a file:-

1. Read the source file byte to byte.
2. Collect the LSB of every byte.
3. Combine the LSB to retrieve back the hidden data.

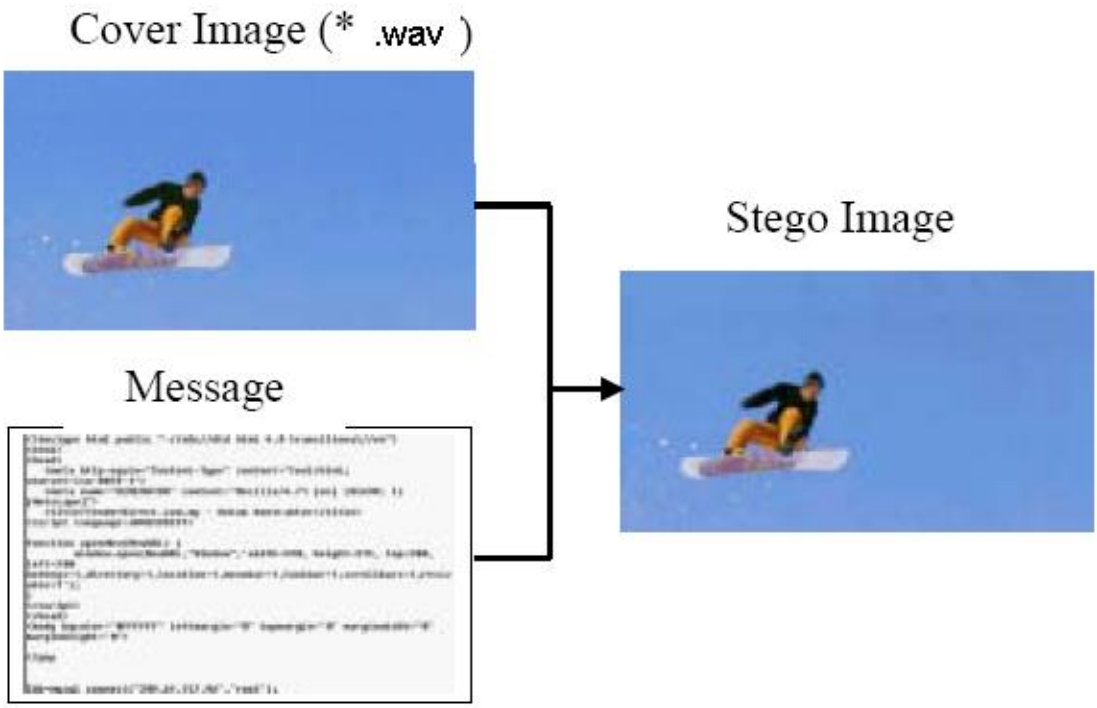


IMAGE BEFORE AND AFTER IMAGE STEGANOGRAPHY

DEVELOPMENT STAGE

The development stage takes as its primary input the design elements described in the approved design document. For each design element, a set of one or more software artifacts will be produced. Software artifacts include but are not limited to menus, dialogs, data management forms, data reporting formats, and specialized procedures and functions. Appropriate test cases will be developed for each set of functionally related software artifacts, and an online help system will be developed to guide users in their interactions with the software.

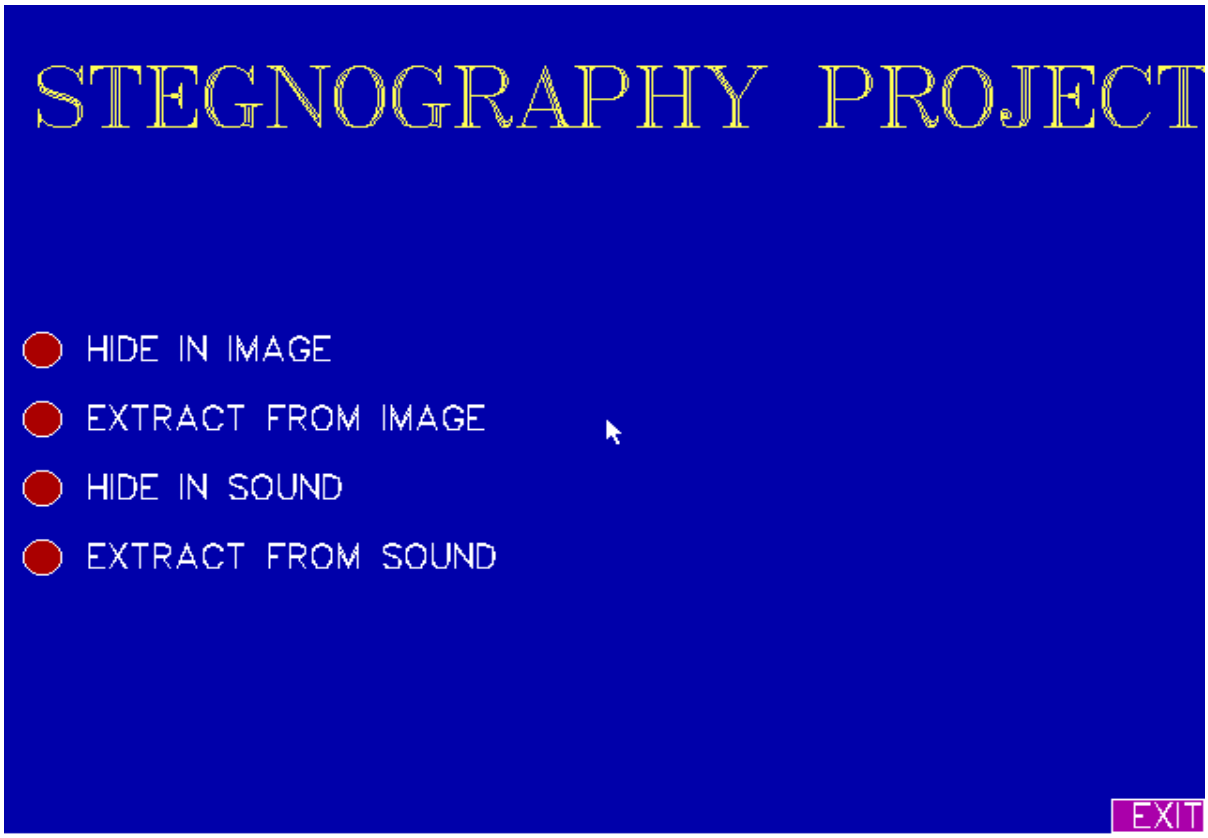
The outputs of the development stage include a fully functional set of software that satisfies the requirements and design elements previously documented, an online help system that describes the operation of the software, an implementation map that identifies the primary code entry points for all major system functions, a test plan that describes the test cases to be used to validate the correctness and completeness of the software, an updated RTM, and an updated project plan.

The Project Development include FIVE main modules (description) as:

.

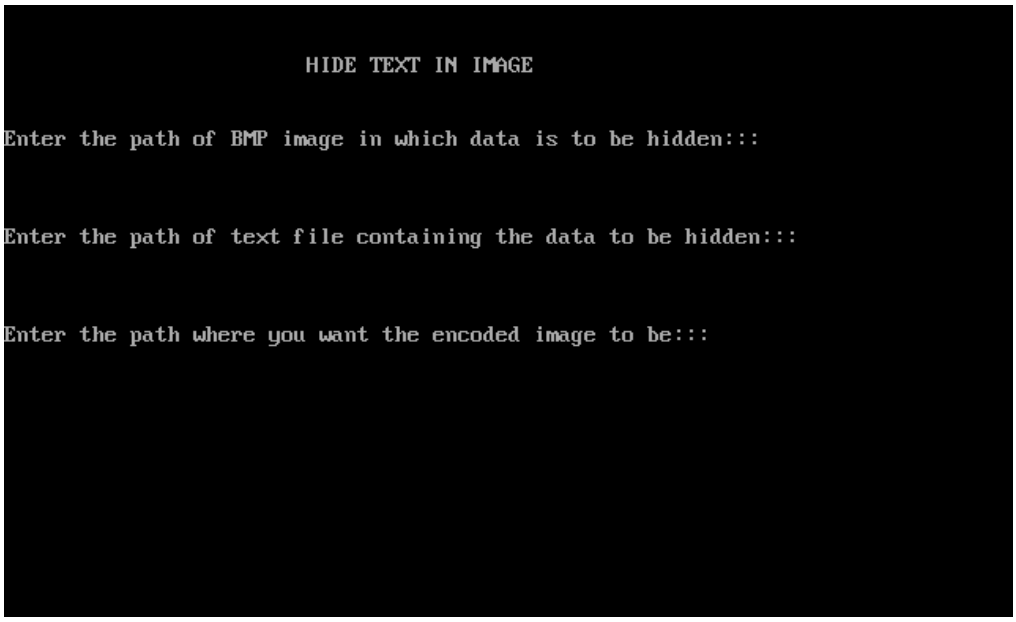
MODULE 1-MAIN MODULE

Main module is providing an interface among all other modules.



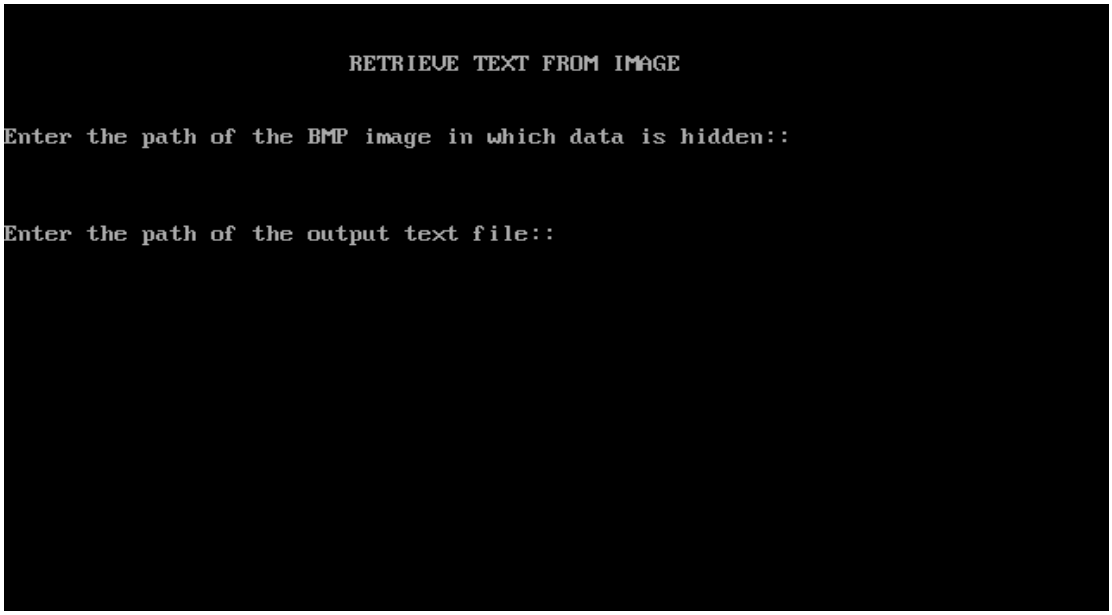
MODULE 2-HIDE IMAGE

This image hide message ‘TEXT File’ in ‘BMP File’ and produce as output a new BMP file the encrypted image.



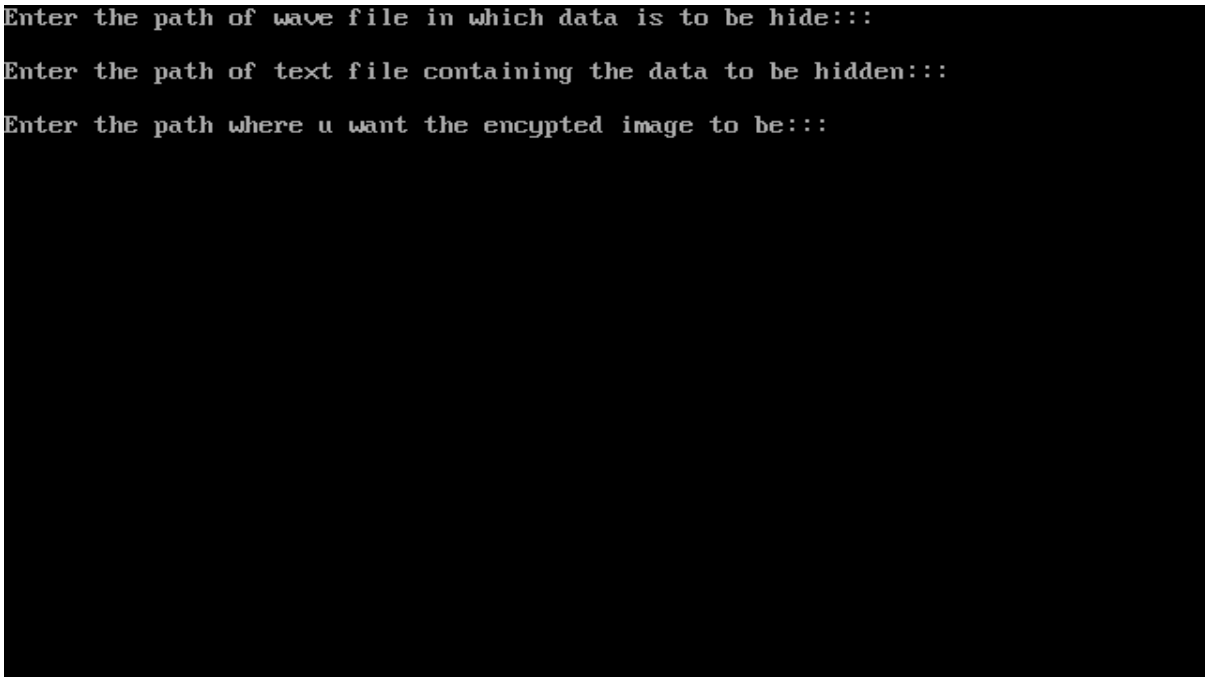
MODULE 3-RETIMAGE

RETRIVE IMAGE is the module which will retrieve the text message by creating a new text file as output in the specified path using the encrypted Image file.



MODULE 4-HIDSOUND

HIDE SOUND is the module which hide the text message in .wav audio file format.



MODULE 5-RETSOUND

RETRIEVE SOUND is the module which extract the text message from the audio file and generates the .txt file of the message.

2.3.5 INTEGRATION & TEST STAGE

During the integration and test stage, the software programs, online help, and test data are migrated from the development environment to a separate test environment. At this point, all test cases are run to verify the correctness and completeness of the software. Successful execution of the test suite confirms a robust and complete migration capability.

During this stage, Individual C programs are tested and integrated together to get the final results as:

- Encrypted BMP files using message(text file) picture
- Decrypted text file(message) from Encrypted file (BMP file)

The final reference data (or links to reference data source files) and production user list are compiled into the Production Initiation Plan.

The outputs of the integration and test stage include an integrated set of software, i.e. how Main program can be interfaced to all the other file.

INSTALLATION & ACCEPTANCE STAGE

During the installation and acceptance stage, the software programs, online help, and initial production data are loaded onto the production server. At this point, all test cases are run to verify the correctness and completeness of the software.

Successful execution of the test suite is a prerequisite to acceptance of the software by the customer.

After customer personnel have verified that the initial production data load is correct and the test suite has been executed with satisfactory results, the customer formally accepts the delivery of the software .

The primary outputs of the installation and acceptance stage include a production

application, a completed acceptance test suite, and a memorandum of customer acceptance of the software.

2.2 LIMITATIONS

The maximum size which can be encrypted depends on size of image.

Our Project is not compatible to other image file formats like JPEG, TIFF, and JPG.

Many intermediate files are used for processing data that require system memory.

It does not provide authentication of sender and receiver.

Project is not showing source and target image in dialog windows. User has to see it in separate image viewing software like “Paint Brush”, “Imaging”, “Iran View”.

2.3FUTURE SCOPE

Our project can handle only BMP imagess. They take more space. The project should be compatible with other file formats like JPEG, PNG, PPM, DIP and TIFF.

The project uses symmetric key encryption which is vulnerable to attack. The project can be extended to asymmetric key encryption.

2.4 CONCLUSIONS

Is Steganography a good or a bad technology?

Like other security tools, as encryption, it depends on the purpose. Unfortunately Steganography can also be used for illegitimate reasons. For instance, if someone was trying to steal data, they could conceal it in another file or files and send it out in an innocent looking email or file transfer. And, as was pointed out in the concern for terrorist purposes, it can be used as a means of covert communication. Of course, this can be both a legitimate and an illegitimate application. Steganography is a fascinating and effective method hiding data that has been used throughout history. Methods that can be

employed to uncover such devious tactics, but the first step are awareness that such methods even exist. There are many good reasons as well to use this type of data hiding, including watermarking or a more secure central storage method for such things as passwords, or key processes.One of the main advantages of steganography, which has been undermined is that the data can be transferred in a more efficient way as the space used to send multiple messages in an encrypted file is very less. Regardless, the technology is easy to use and difficult to detect. The more that you know about its features and functionality, the more ahead you will be in the game

2.5. REFERENCES

1) www.securityfocus.com/infocus/1684

2) http://google.com