

DIGITAL IMAGE WATERMARKING

A

Minor Project Report

Submitted in Partial fulfillment for the award of
Bachelor of Engineering Degree in Computer Science & Engineering

Submitted

To

**RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA
BHOPAL (M.P)**



Submitted by

Abhay Lunkad [0157CS131002] Akansha Raghuvanshi [0157CS131008]
Deepali Shandilya[0157CS131031] Durgesh Prasad Jaiswal[0157CS131033]

Under the Supervision of
Mr. Atul Gupta



**DEPARTMENT OF COMPUTER SCIENCE& ENGINEERING
LAKSHMI NARAIN COLLEGE OF TECHNOLOGY & SCIENCE
BHOPAL (M.P.)
SESSION 2013-17**

LAKSHMI NARAIN COLLEGE OF TECHNOLOGY & SCIENCE

BHOPAL (M.P.)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING



CERTIFICATE

This is to certify that the Major Project work entitled “ **DIGITAL IMAGE WATERMARKING**” has been satisfactorily completed by **Abhay Lunkad (0157CS131002), Akansha Raghuvanshi (0157CS131008), Deepali Shandilya (0157CS131031), Durgesh Prasad Jaiswal (0157CS131033)** .It is a bonafide piece of work, carried out under my guidance in the **Department of Computer Science & Engineering, Lakshmi Narain College of Technology&science, Bhopal** for the partial fulfilment of the award of Bachelor of Engineering degree in Computer Science & Engineering during the academic year 2013-17.

Mr. Atul Gupta

Assistant Professor (CSE)

Guide

Approved By

Head of the Department

Forwarded By

Principal

Lakshmi Narain College of Technology & Science, Bhopal

LAKSHMI NARAIN COLLEGE OF TECHNOLOGY & SCIENCE
BHOPAL (M.P.)
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING



CERTIFICATE OF APPROVAL

This foregoing project work is hereby approved as a creditable study of Engineering carried out and presented in a manner satisfactory to warranty its acceptance as a prerequisite to the degree for which it has been submitted. It is understood that by this approval the undersigned do not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein, but approve the project only for the purpose for which it has been submitted.

(Internal Examiner)

Date:

(External Examiner)

Date:

LAKSHMI NARAIN COLLEGE OF TECHNOLOGY & SCIENCE

BHOPAL (M.P.)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING



DECLARATION

We Abhay Lunkad (0157CS131002), Akansha Raghuvanshi (0157CS131008), Deepali Shandilya (0157CS131031), Durgesh Prasad Jaiswal (0157CS131033) .

The student of Bachelor of **Computer Science&Engineering, Lakshmi Narain College of Technology & Science, Bhopal** hereby declare that the work presented in this Minor Project is outcome of our own work, is bona fide, correct to the best of our knowledge and the work has been carried out taking care of Engineering Ethics.

Abhay Lunkad
(0157CS131002)

Akansha Raghuvanshi
(0157CS131008)

Deepali Shandilya
(0157CS131031)

Durgesh Prasad Jaiswal
(0157CS131033)

Date:

LAKSHMI NARAIN COLLEGE OF TECHNOLOGY& SCIENCE
BHOPAL
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING



ACKNOWLEDGEMENT

We express our deep sense of gratitude to **Mr. Atul gupta (Assistant Professor)Department of Computer Science & Engineering, Lakshmi Narain College of Technology & Science, Bhopal** ,whose kindness, valuable guidance and timely help encouraged us to complete this project.

A special thank goes to **Dr. Sadhna Mishra (Head of the Department)Department of Computer Science & Engineering, Lakshmi Narain College of Technology & Science, Bhopal**,who helped us in completing this project work. He exchanged his interesting ideas &thoughts which made this project work successfully.

We should also thank our institution and all the faculty members without whom this project work would have been a distant reality.

Abhay Lunkad
(0157CS131002)

Akansha Raghuvanshi
(0157CS131008)

Deepali Shandilya
(0157CS131031)

Durgesh Prasad Jaiswal
(0157CS131033)

Date:

ABSTRACT

Main aim of the project is to provide copyright protection of images. Any or all of our original content could easily be copied and displayed To overcome this type of problem copyright protection is needed.

Watermark is a message which is embedded into digital content (audio, video, images or text) that can be detected or extracted later. Such messages mostly carry copyright information of the content. Watermarking has been revealed to be an efficient technique to cope with the problem of intellectual property rights (IPR) protection of multimedia data. This technology embeds into the data an unperceivable digital code, namely the watermark, carrying information about the copyright status of the work to be protected.

To our best Knowledge, upto now there is no research that addresses the issue of desktop application watermarking. In this project we propose a new watermarking scheme for Desktop applications. It has both Invisible and visible watermarked image.

List of Figures

TITLE	PAGE NO.
Figure 1: a) The first marks were simple objects.....	3
b) This mark of "foolscap" for a certain size paper.....	3
Figure 2: Applications of Digital Watermarking	5
Figure 3: a) Original image.....	9
b) Watermark image.....	9
Figure 4: Visible watermark image	10
Figure 5: Invisible watermark image.....	10
Figure 6: System development life cycle.....	19
Figure 7: Organization of pixel under ARGB system.....	22
Figure 8: a) Watermark embedding process	23
b) Watermark extraction process	23
Figure 9: a) System flow chart for insertion	26
b) System flow chart for extraction	27
Figure 10: a) Use case diagram for insertion	28
b) Use case diagram for extraction	29
Figure 11: a) Data flow diagram level 0.....	31
b) Data flow diagram level 1	32
c) Data flow diagram level 2	33

INDEX

Title	Page no.
ABSTRATACT	[v]
LIST OF FIGURES.....	[vi]
LIST OF TABLE.....	- -
Chapter 1 Introduction	1-2
1.1 Introduction	1
1.2 Scope & Objectives	1
1.3 Overview	2
Chapter 2 General Description.....	3-12
2.1 About Watermarking.....	3
2.1.1 History	3
2.1.2 Problem Definition	5
2.2 Applications of Digital Watermarking.....	5
2.3 User characteristics	12
Chapter 3 System Design & Analysis	12-15
3.1 Software Requirements Specifications.....	13
3.2 User Requirements	13
3.3 Problem Definition.....	14
3.4 Solution Provided	14
Chapter 4 System planning	16-18
4.1 Selection of Technology	16
4.2 Development of Modules.....	17
Chapter 5 System Implementation	19-23
5.1 Software Development Lifecycle	19
5.2 Hardware Specification	20
5.3 Software Specification.....	20
5.4 Watermark insertion & extraction	23
Chapter 6 Cost Benefits	24
Chapter 7 System Life Cycle.....	25-33
7.1Description.....	25
7.1.1 Flow Chart Diagram	26
7.1.2 Use Case Diagram	26
7.1.3 Data Flow Diagram	27

7.2 Diagram	28
7.2.1 Flow Chart	28
7.2.2 Use Case Diagram	30
7.2.3 Data Flow Diagram	32
Chapter 8 Testing	34-37
8.1 Levels of testing	34
8.2 Test plan & test case specification	36
Chapter 9 Implementation	38-59
9.1 Snapshots	38
Chapter 10 Conclusion & Future Scope	60
10.1 Conclusion	60
10.2 Limits of the project	60
10.3 Future Enhancement	60
References	61

CHAPTER 1

INTRODUCTION

1.1 Introduction

Data security is the essential in the today's world of internet and networking. In any organization information is critical. In today's world people are ready to spent thousands and lacks of money in order to ensure high level of information security. In spite of spending such a huge amount, still the objective of securing the information is not achieved as the data some how gets in the hands of hacker. As the technology for securing the data is advancing, hackers are also keeping pace with this technology. Hackers now make use of certain algorithm or other techniques to decode the data encoded by the senders. One of the ways to ensure security is to ensure that data is not visible to the hacker. This can be done by hiding the message itself behind some other objects. Here we are achieving this data security concept through the technique of Watermarking (By Steganography).

1.2 Objective and scope of the project

Objective:

The main objective for developing this application is that, it can provide the user with security of data. Only the authorized user and administrator can access the application.

Scope:

The project "Digital Watermarking" will basically deal with data security. It will provide security of data by mechanism which is popularly known as "Steganography" in the world of internet security.

In this project, the focus is on image watermarking **visible** as well as **invisible**.

Visible Watermarking involves only insertion of the watermark. Whereas Invisible Watermarking involves insertion of the watermark and extraction of a Watermark.

- It will embed any text data,image into any other suitable file such as image, audio, video, text file, without actually changing the content of the carrier file.

- Consequently will also retrieve the information from file in which information is embedded.
- It will also provide a mechanism for embedding a whole text file in other files.
- It will provide the mechanism to retrieve the text file as it was embedded without changing the format or look of the file in which it was embedded.

1.3 Overview

This project will basically implement the Steganographic technique of hiding the data or information behind the image file. The main aim of this project will be the data security aspect.

Watermark is a message which is embedded into digital content (audio, video, images or text) that can be detected or extracted later. Such messages mostly carry copyright information of the content. Watermarking has been revealed to be an efficient technique to cope with the problem of intellectual property rights (IPR) protection of multimedia data. This technology embeds into the data an unperceivable digital code, namely the watermark, carrying information about the copyright status of the work to be protected.

CHAPTER 2

GENERAL DESCRIPTION

2.1 About Watermarking:

2.1.1 History of Watermarking:

Watermarks are identification marks produced during the paper making process. The first watermarks appeared in Italy during the 13th century, but their use rapidly spread across Europe. They were used as a means to identify the papermaker or the trade guild that manufactured the paper. The marks shown here were created by a wire sewn onto the paper mold. Watermarks continue to be used today as manufacturer's marks and to prevent forgery.



- a) The first marks were simple objects. b) This mark is the source of the term "foolscap" for a certain size of paper.

Fig. 1 Example of old Watermark paper

During the Seventeenth and Eighteenth Centuries, British papermakers began to use certain symbols to designate the paper's intended size. According to Dard Hunter, it would not be reasonable to assume that prior to that time the different watermarks would have denoted the various sizes of paper, because every different size of paper would have required a special pair of

moulds. Marks such as the foolscap, hand, post and pott came into use in the 1400s (for example, the foolscap mark can be traced to the year 1479).

This first watermark to be utilized in the making of paper in the colonies stood for the partnership that Rittenhouse entered into with William Bradford, the first printer in the Province of Pennsylvania and two other gentlemen. In 1704, Bradford dropped out of the partnership, and two years later Rittenhouse became the sole owner of the papermill. After 1706 Rittenhouse employed two watermarks, the one being just the letters "W" and "R" joined together, and the other being the image of a clover leaf inside a crowned shield with the word "Pensilvania" below it. The initial letters watermark was positioned on one half of the sheet of paper, while the other watermark was positioned on the opposite half of the sheet.

In 1790 an Englishman by the name of John Phipps patented a method of teaching writing in which ruled lines were embedded in the paper by means of watermarking. The nearly invisible lines would help pupils to write straighter and more uniformly.

The next major step in the history of watermarks came in the late Eighteenth and early Nineteenth Centuries with the introduction of finer mesh brass screens. The finer mesh allowed more detail to be captured when a shape was pressed into it. And that is exactly what papermakers began to do. They continued to shape and bend wire to form images, but instead of attaching the shaped wire to the screen, they pressed the shaped wire into the screen itself.

Digital watermarking is a technique which allows an individual to add hidden copyright notices or other verification messages to digital audio, video, or image signals and documents. Such a message is a group of bits describing information pertaining to the signal or to the author of the signal (name, place, etc.). The technique takes its name from watermarking of paper or money as a security measure. Digital watermarking can be a form of steganography, in which data is hidden in the message without the end user's knowledge.

A simple example of a digital watermark would be a visible "seal" placed over an image to identify the copyright. However the watermark might contain additional information including the identity of the purchaser of a particular copy of the material.

According to the human perception, **the digital watermarks can be divided into two different types as follows:**

1. Visible Watermarking

2. Invisible Watermarking

2.1.2 Problem Definition:

Digital watermarking is the process of inserting a digital signal or pattern into digital content. The signal, known as a watermark, can be used to identify the owner of the work, to authenticate the content, and to trace illegal copies of the work. A watermark is a form, image or text that is impressed onto paper, which provides evidence of its authenticity. Digital watermarking is an extension of this concept in the digital world.

Techniques that use to watermark a digital image is LSB (Least Significant Bit) Algorithm. The system implements both visible as well as invisible watermarking. The digital content could be a still image, an audio clip, video clip, a text document, or some form of digital data that the creator or owner would like to protect.

The main purpose of the watermark is to identify who the owner of the digital data is, but it can also identify the intended recipient. This project focuses on still digital image watermarking.

2.2 Applications of Digital Watermarking:

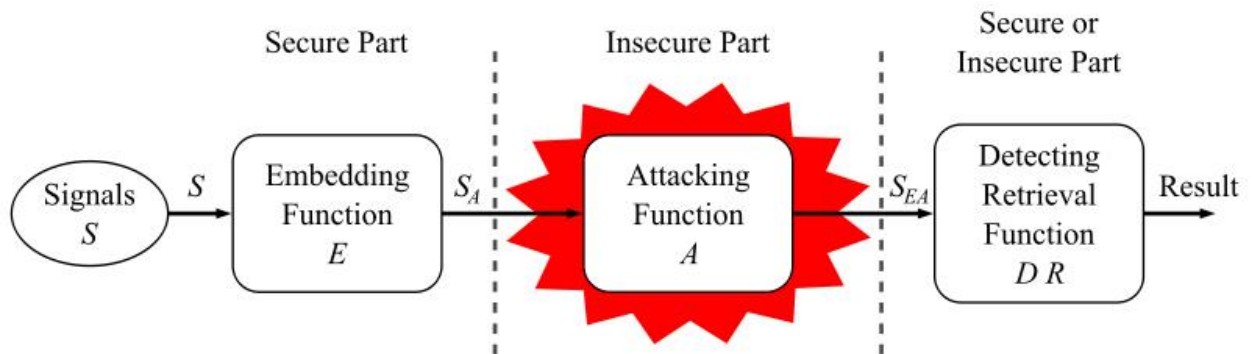


Figure 2: Applications of Digital Watermarking

Very frequently there is a need to associate some additional information with a digital content, such as music, image or video. For example, copyright notice may need to be associated with an image to identify a legal owner of that image. Or a serial number may need to be associated with a video to identify a legitimate user of that video. Or some kind of identifier may need to be associated with a song to help find a database where more information about it can be obtained from. This additional information can be associated with a digital content by placing it in the header of a digital file, or for images, it can be encoded as a visible notice. Storing information in the header of a digital file has a couple of disadvantages. First, it may not survive a file format conversion, and second, once an image is displayed or printed, its association with the header file and information stored in it is lost. Adding a visible notice to an image may not be

acceptable if it negatively affects the esthetics of the image. This could be corrected to some extent by making the notice as small as possible and/or moving it to a visually insignificant portion of the image, such as the edge. However, once on the edge, this additional information can easily be cropped off, either intentionally or unintentionally.

The Lena image used as a test image on the left, and the cropped part of the original image which identifies the copyright owner, Playboy Enterprises, Inc. on the right. This is exactly what happened with an image of Lena Soderberg after its copyright notice was cropped off. The image was originally published as a Playboy centerfold in November 1972. After the image has been scanned for use as the test image, most of it has been cropped including the copyright notice which was printed on the edge of the image. The "Lena" image became probably the most frequently used test image in image processing research, and appeared in a number of journal articles without any reference to its rightful owner, Playboy Enterprises, Inc. Digital watermarking seems to be the suitable method for associating this additional information, the metadata, with a digital work. The metadata is imperceptibly embedded as a watermark in a digital content, the cover work, and it becomes inseparable from it.

Classification of Digital Watermarking Applications:

There are a number of different watermarking application scenarios, and they can be classified in a number of different ways. The following classification is based on the type of information conveyed by the watermark. In the following section we will provide a more detailed explanation of possible application scenarios involving watermarking.

- **Digital Watermarking for Copyright Protection:**

Copyright protection appears to be one of the first applications digital watermarking was targeted for. The metadata in this case contains information about the copyright owner. It is imperceptibly embedded as a watermark in the cover work to be protected. If users of digital content (music, images, and video) have an easy access to watermark detectors, they should be able to recognize and interpret the embedded watermark and identify the copyright owner of the watermarked content.

- **Digital Watermarking for Copy Protection:**

The objective of a copy protection application is to control access to and prevent illegal copying of copyrighted content. It is an important application, especially for digital content, because digital copies can be easily made, they are perfect reproductions of the original, and they can easily and inexpensively be distributed over the Internet with no quality degradation. There are a number of technical and legal issues that need to be addressed and resolved in order to create a working copy protection solution. Those issues are difficult to resolve in open systems, and we are not aware of the existence of an open system copy protection solution. Copy protection is feasible in closed, proprietary systems, and we will describe one proprietary solution, the Digital Versatile Disk (DVD) copy.

- **Digital Watermarking for Fingerprinting:**

There are some applications where the additional information associated with a digital content should contain information about the end user, rather than about the owner of a digital content. For example, consider what happens in a film making environment. During the course of

film production, the incremental results of work are usually distributed each day to a number of people involved in a movie making activity. Those distributions are known as film dailies, and they are confidential. If a version is leaked out, the studio would like to be able to identify the source of the leak. The problem of identifying the source of a leak can be solved by distributing slightly different copies to each recipient, thus uniquely associating each copy with a person receiving it.

1. Digital Watermarking for Content Authentication:

Multimedia editing software makes it easy to alter digital content. For example, The left one is the original, authentic image. The middle one is the modified version of the original image, and the right one shows the image region which has been tampered. Since it is so easy to interfere with a digital content, there is a need to be able to verify integrity and authenticity of the content.

A solution to this problem could be borrowed from cryptography, where digital signature has been studied as a message authentication method. Digital signature essentially represents some kind of summary of the content. If any part of the content is modified, its summary, the signature, will change making it possible to detect that some kind of tampering has taken place. One example of digital signature technology being used for image authentication is the trustworthy digital camera.

Visible watermarks can be used in following cases:

- Visible watermarking for enhanced copyright protection.

In such situations, where images are made available through Internet and the content owner is concerned that the images will be used commercially (e.g. imprinting coffee mugs) without payment of royalties. Here the content owner desires an ownership mark, that is visually apparent, but which does not prevent image being used for other purposes (e.g. scholarly research).

- Visible watermarking used to indicate ownership originals.

In this case images are made available through the Internet and the content owner desires to indicate the ownership of the underlying materials (library manuscript), so an observer might be encouraged to patronize the institutions that own the material.

Invisible watermarks do not change the signal to a perceptually great extent, i.e., there are only minor variations in the output signal. An example of an invisible watermark is when some bits are added to an image modifying only its least significant bit. Invisible watermarks that are unknown to the end user are steganography. While the addition of the hidden message to the signal does not restrict that signal's use, it provides a mechanism to track the signal to the original owner.

- To protect digital media by fingerprinting.

Another application is to protect digital media by fingerprinting each copy with the purchaser's information. If the purchaser makes illegitimate copies, these will contain his name. Fingerprints are an extension to watermarking principle and can be both visible and invisible.

- Copyright protection

This is the most prominent application of Digital watermarking. It embeds the information about the owner to prevent others from claiming copyright. It Requires very high level of robustness.

- Copy protection

It embeds watermark to disallow unauthorized copying of the cover. For example, compliant DVD players will not playback or copy data that carries a "copy never" watermark.

- Content Authentication

It embeds a watermark to detect modifications to the cover. The watermark in this case has low robustness, "fragile".

- Transaction Tracking

It embeds a watermark to convey information about the legal recipient of the cover. This is useful to monitor or trace back illegally produced copies of the cover. This is usually referred to as "fingerprinting".

- Broadcast Monitoring

It embeds a watermark in the cover and use automatic monitoring to verify whether cover was broadcasted as agreed requirements.

➤ **About Steganography**

Steganography is a technology that hides a message within an object, a text, or a picture. It is often confused with cryptography, not in name but in appearance and usage. The easiest way to differentiate the two is to remember Steganography conceals not only the contents of the message but also the mere existence of a message. Steganography is a Greek word meaning covered writing, which is as old as cryptography itself and can be as simple as writing with invisible ink made from vinegar or lemon juice. Computerized applications of Steganography have truly breathtaking implications, including hiding large data files inside digital graphic or audio files or even on ordinary- looking and sounding CD-ROMs and digital audio tapes.

The first steganographic technique was developed in ancient Greece around 440 B.C... Herodotus's Histories describes two types of the earliest steganography. The first type involved the shaving of a slave's head, and then a tattoo was inscribed on the scalp. When the slave's hair had grown back and hidden the message, the slave was sent to warn of the Persians' impending invasion. The recipient once again shaved the slave's head and retrieved the important warning. Another method was to modify ancient writing tablets. The layer of wax covering the tablets was the surface upon which messages were written. However Demeratus, a Greek exiled into Persia, devised a plan to hide a message by removing the layer of wax and writing directly on the underlying wood a warning to Sparta that the Persians were planning an invasion. The tablets were then covered again with wax and appeared unused to the examiners of the shipment.

Example of visible watermark :-

Original Image :-



Figure 3(a): original imag

Watermark Image:-



Figure 3(b): watermark image

Visible watermark Image :-



Figure 4: visible watermark image

Example of Invisible watermark :-

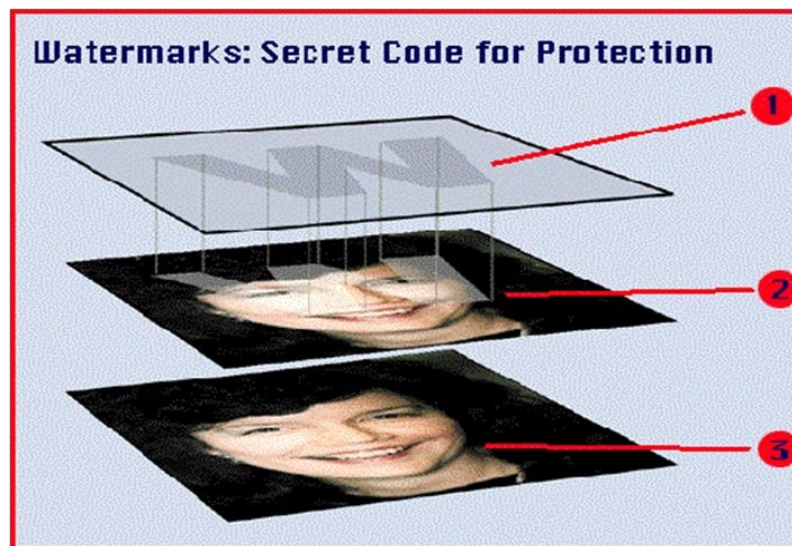


Figure 5: Invisible watermark image

Image Formats:

There are many types of image formats, but with respect to our project we consider following three popular image formats:

- JPEG (Joint Photographic Experts Group)

Format name: JPEG (Joint Photographic Experts Group)

Extension: jpg, jpeg, jfif, jfl

Type: bitmapped

Compression algorithm: JPEG (lossy)

Color depth: 24 bits

Platforms: all

JPEG format was designed to transfer graphic data and images via digital telecommunication networking and was generally used to hold and transfer full color photo realistic images. Before JPEG, there were very few formats, which supported 24 bit halftone images. TIFF and BMP formats allowed holding 24 bit data, but they failed to perform a lossless compression of the data, which contained thousand colors from the real world. Jpeg compresses photos though with quality loss. Compression algorithm is that data are deleted for deallocation (it allows to raise the compression degree). Data are hold as pixel block in a certain color with intensity information save (the matter is that a human eye discerns disintensity better than discoloration).

- Bitmap (Microsoft Windows Bitmap)

Format name: Bitmap (Microsoft Windows Bitmap)

Extension: bmp, dib, rle

Type: bitmapped

Compression algorithm: RLE (lossless), without compression

Color depth: up to 32 bits

Platforms: Windows, OS/2

Bitmap is a home Windows raster format, which is used practically for all possible raster data storage. All BMP versions were designed for computers with Intel processors. The current format version is device undependable (that means that Bitmap determines the pixel's color without reference to display device) and makes possible to record images of a different quality level (to the point of 32 bits). After revising, the format was used to hold color and black and white images, so it became general. The main advantage of the format is considered to be its usability and wide software support.

All BMP versions were designed for computers with Intel processors. The current format version is device undependable.

- PNG (Portable Network Graphic)

Format name: PNG (Portable Network Graphic)

Extension: png

Type: bitmapped

Compression algorithm: Deflate (lossless)

Color depth: up to 48 bits

Platforms: all

PNG file format is a comparatively new progressive format originally designed to replace dated Gif. PNG format has got a set of new features that Gif lacks. PNG also performs a lossless compression with the help of Deflate algorithm (read more about Deflate algorithm [here](#)) and supports interlaced mode. The format handles 256 transparency levels (that means that images might be partially transparent). The fact, that the format supports color depth up to 48 bits and performs a lossless compression, makes possible to hold photo realistic images. They won't lose its quality while compressing and decompressing. PNG format is used specially for networking.

2.3 User Characteristics

Data security and data transfer is the main functionality provided by this application. The user of this application needs to be conscious about the data security and its importance. However any user who is aware of or has basic knowledge of computer can use it. The user need to have little basic knowledge of what the Watermarking is for using the data security functionality provided by this application. However this application can be independently be used for transferring the files from one machine to other machine.

CHAPTER 3

SYSTEM ANALYSIS AND DESIGN

3.1 SRS (Software Requirements Specifications)

SRS is a document that completely describes what the proposed software should do without describing how the software should do it. SRS describes the complete external behavior of the proposed software.

Title: Digital Watermarking

Aim: The main aim of this project or application is to provide high quality of data security and transfer of data from source to destination.

3.2 User Requirements

The software which will be developed should have the following capabilities:

- It should be capable of identifying the authorized and un-authorized users.
- It should be capable of embedding text message into image file, audio file and video file.
- Before embedding the message, the message should be first encrypted.
- On embedding the message, the format and look of the image should not be distorted.
- Reverse to embedding the message, it should also retrieve the message from image file as it was embedded.
- After embedding the message, it should retrieve the message from the file in the same format in which the message was previously embedded.
- It should also decrypt the message which was encrypted by the sender.
- After retrieving the message from the file, the look and the format of the image should not change.
- It should be capable of embedding the whole text file into the image file so that user could be able to embed large message in the form of text file.
- The format of data in file should not change during the process of transfer.
- When the file is embedded in the image file, look of the file holding the file should not change.
- Before embedding the file, the data of the file should be encrypted.
- It should also decrypt the content of the file which was encrypted by the sender.

3.3 Problem statement

The problem statements are as follows:

- For some applications User-Id and password are not protected. As a result any one who is interested in using the application can access it.
- Sending a plain text of data to the receiver is not secure. Since the data is readable any one can get the information.
- Even if the message is encoded before sending the message, it can be decoded by the hacker by making use of certain algorithm.
- Some times the systems may not be connected properly. As a result the data which is transferred may not reach the destination in proper format.
- It is very difficult to maintain reliability of the software. The reliability comes with the cost.
- When the message falls in the hand of the hacker then the hacker can insert, delete or modify the content of the original message.
- Confidentiality of the message is lost if the message is not protected properly.
- A hacker can pose as sender and can misguide the receiver. Thus hacker can violate the authentication.
- In some cases hacker are not able to get the content of the original message. Thus they perform the exponential attack. Exponential attack is the attack where the hacker destroys the content of the original message.

3.4 Solution provided

- The software should be provided proper user id and password, so that no one can misuse it.
- The user id and the password should be protected from the internal and the external hacker.
- The message will be encoded using Steganography technique so that if it falls in the hand of the hacker then hacker will not be able to detect it.

- Since in Invisible watermarking technique the message is not visible the hacker gets fooled. Thus hacker can not make use of any kind of algorithm to get the original content of the message.
- Software will be reliable enough to handle exceptional conditions; it will provide operability on different platforms.
- In Stenography, as the message is not visible the hacker can not perform any kind of modification.
- Confidentiality level is very high in this technique.
- Authentication of the user can be done using user id and password. This ensures that interception is avoided.
- Receiver can easily rely on the Steganography.
- Steganography is the technique where sender can hide the original message behind the image and send it to receiver. Receiver at opposite end can retrieve the message by using the same technique.

CHAPTER 4

SYSTEM PLANNING

System Planning:

System Planning is an important for any successful project. With out proper planning the project is doomed. Good planning can be done after the requirements for the project are available. The input to the project planning activity is the requirement specification. The output of this phase is the project plan, which is the document describing the different aspects of the plan. The project plan is instrumental in driving the development process through the remaining phases. The major issues the project plan addresses are:

- Selection of technology.
- Development of modules.
- Cost Estimation
- Average Duration Estimation
- Gantt Chart

Various models have been proposed for the software planning. E.g. COCOMO (COConstructive COSt MOdel) developed by Boehm. The model fits the large scale projects and can be implemented with few modifications for the small projects.

4.1 Selection of Technology

The system planning also includes the selection of technology for the development of the modules and the application. The technology which will be used in this project is Java Standard Edition. The JAVA technology will be used for providing platform independency to the application and for doing the bit level calculations in the modules.

The application which we will be developing is a stand alone application. This application, apart from providing data security communicates with other machines for file transfer. The machines which will be communicating might not have same platform. So the application needs to be platform independent. For embedding the files and the message the image files need to be rendered at bit level. So a very secure technique is required for dealing at bit level.

System Development Model

This project deals with the secure transfer of data from one machine to another machine via any Network. The development of such software would really be complex task. It is more of a technical project. Although the requirements and the concepts of the project are clear at the initial stage but would require some advancement at the later stage. This advancement can not be detected initially. So it would be better to develop those modules that are clear at the current stage. As the development proceeds the further features can be added into the system as per the requirement of the user. The project development also requires the coverage of technical risks.

Since the development of the system can be done and advanced features can be added at the regular interval of time, for this system *Incremental model* is recommended. In incremental model, iterative development can be done i.e. system can be developed in number of phases. First that module is developed whose requirement is clear. If the user is satisfied with that module then work is done on other iteration. Also incremental model helps us to cover risk for our project.

About Java

Java is an Object Oriented Programming language which can be used for developing platform independent applications. The platform independency means that the application developed on one platform can also be executed on other platforms. Also Java provides strong support for file handling mechanism. It has a very good exception handling mechanism which can be used for detecting the various file errors while performing operations on them. It has a wide range of bitwise operators for supporting operations at bit level. Java also has classes for socket programming which can be used for communication between the machines. Also object oriented techniques helps in development of applications which can be re-used.

Reason for using Java :

Following are the reasons for using the JavaSE:

- ✓ Java will help in doing the operations at the bit level in embedding the message/data file in the image file
- ✓ Since our application is standalone and need communication between different platform machines, Java can be used for platform independent application development.
- ✓ The Object-Oriented concept can be used for reusability of the application and is very good for Incremental Model of software development which we will be used.
- ✓ Java provides various streams for handling files; it also has classes rendering images
- ✓ Java provides wide range of predefine Methods so it is very easy to implement the various things
- ✓ Java support Graphical User Interface(GUI), So it provide very easy and user friendly environment to work on Desktop application of JAVA.

4.2 Development of Modules

This project will contain mainly five major modules:

1. User interface Module
2. Invisible and Visible option
3. Insertion of Invisible Watermark
4. Extraction of Invisible Watermark
5. Insertion of Visible Watermark.

1) User Interface Module :

This module will basically provide the main frame for accessing the functionality of the application. Since the application will be implemented in the form of MDI parent child property for user interface, this module will work as a parent form for other child forms.

2) Invisible and Visible option:

This module will basically provide the option of which Watermark can apply whether it is visible watermark or it can be Invisible watermark. It all depends on the user's choice or need of the user. Different Watermark can be used for different purposes.

3) Insertion of Invisible Watermark

This module will basically provide the functionality of embedding the message and the text or data file in the image files. It will also have a sub module named 'Encrypt' which will be responsible for encrypting the message and the data file. The embed module will make use of this encrypt module for encryption purposes. It will be invisible to normal human eyes. It can be only retrieved by software.

4) Extraction of Invisible Watermark

This module will basically provide the functionality of retrieving the message and the text or data file from the image files. It will also have a sub module named 'Decrypt' which will be responsible for decrypting the message and the data file. The retrieve module will make use of this decrypt module for decryption purposes.

5) Insertion of Visible Watermark

This module will basically provide the functionality of embedding the message and the text or image file in the image files. It will also have a sub module named 'Encrypt' which will be responsible for encrypting the message and the data file. The embed module will make use of this encrypt module for encryption purposes. It will be visible to normal human eyes.

CHAPTER 5

SYSTEM IMPLEMENTATION

5.1 System Development Life Cycle:-

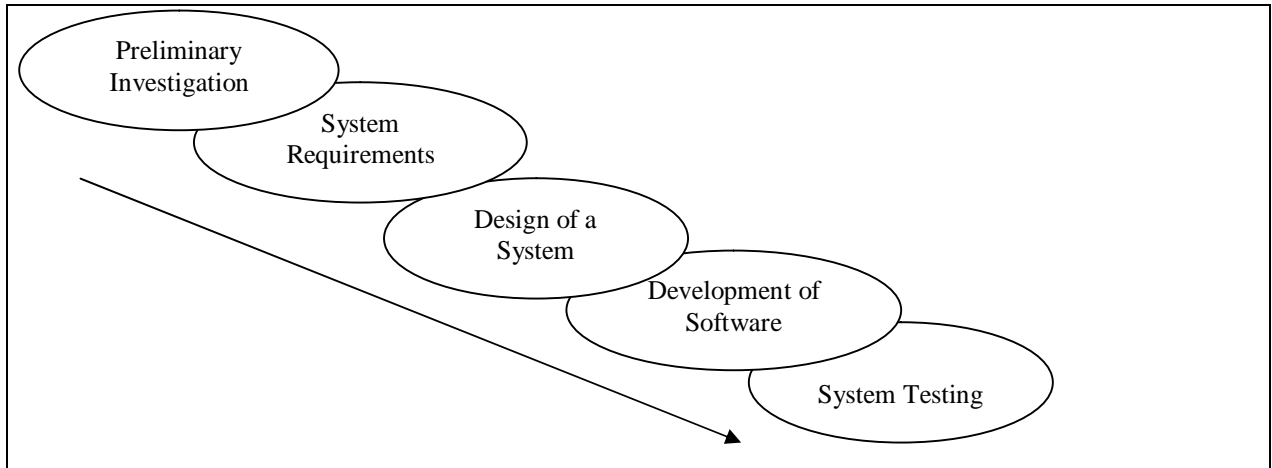


Figure 6: Syetem development life cycle

Preliminary Investigation:-

The First step is to identify a need for the new system. This will include determine whether a business problem or opportunity exists, conducting a feasibility study to determine if the proposed solution is cost effective, and developing a project plan. This process may involve end users who come up with an idea for improving their work. Ideally the process occurs in tandem with a view of the organization strategy.

System Requirements:-

Requirements analysis is the process of analyzing the information needs of the end users, the organizational environment and any systems presently being used thereby developing the functional requirements of a system that can meet the needs of the users. Also, the requirements should be recorded in a document, email, user interface. The requirements documentation should be referred to throughout the rest of the system development process to ensure the developing project aligns with the needs and requirements.

Design of a System:-

After the requirements have been determined, the necessary specification for the hardware, software, people, data resources, and the information products that will satisfy the functional requirements of the proposed system can be determined. The design will serve as a blue print for the systems and helps to detect these problems before these errors or problems are built into the final system.

Development of Software:-

Coding and debugging is the act of creating the final system. Software developed may use purchased software or they may create new custom designed programs depending upon the cost and time available. Documentation is essential to test the program and carry out maintenance.

System Testing:-

The system must be tested to evaluate its actual functionality. In relation to expected or intended functionality. Some other issues to consider during this stage would be converting old data into the new system and training employees to use the new system. End users will be key in determining whether developed system meets the intended requirements, and the extent to which the system is actually used.

5.2 Hardware Requirement

- Display drive that should support 32-bit color scheme.
- Display resolution that should be 1024 x 768 pixels..
- Minimum of 128 MB RAM is required
- 20 Gb HDD or more.
- The processor preferably should be Pentium III or above /its equivalent.

Justification

- The screen resolution of 1024 x 768 pixels must be used for the better vision and clarity of the system.
- Minimum 128 MB RAM must be used for faster access of the system.
- Processor of Pentium III or equivalent must be used for faster access of the system.

5.3 Software Requirement

- JDK 1.5 and above.
- Any Version OS of Windows, Macintosh, UNIX and Solaris.

Justification

- Since this application is developed using Java and full care is taken while coding to keep it platform independent.

Design issues of the procedure & algorithms:

The following considerations were made during the project.

- The data structure used to store the image data & encoding data is integer arrays.
- The image after it is watermarked is saved as the format with the same as the host image.
- The watermark insertion algorithm is minimally implemented with the least resistance to any attack.
- The watermark extraction algorithm is the reversal of the insertion algorithm.
- A simple spatial watermarking algorithm LSB is used.

The LSB Technique:

The LSB technique is the simplest technique of watermark insertion. If we specifically consider still images, each pixel of color image has four components -alpha, red, green & blue. Let us assume we allocate 4 bytes for each pixel. Thus, each color has 1 byte, or 8 bits, in which the intensity of that color can be specified on a scale of 0 to 255.

So a pixel that is bright purple in color would have full intensities of red & blue, but no green. Thus, that pixel can be shown as

$X_0 = \{R=255, G=255, B=255\}$

Now, let's have a look at another pixel.

$X_0 = \{R=254, G=254, B=254\}$

Now, since each color is stored in a separate byte, the last bit in each byte stores this difference in one. That is, the difference between values 255 & 254 is stored in the last bit, called Least Significant Bit.

Even after changing the value of RGB here, the difference is not noticeable to a human eye. For the eye, detecting a difference of 1 on a color scale of 256 is almost impossible.

Modified LSB algorithm:

A modification of the above method would be to use a secret key to choose a random location & replace the last bit with the watermark information. This technique of watermarking is invisible, as changes are made to the LSB only, but is not robust. Image manipulations, such as resembing, format conversion & cropping will in most cases result in watermarking information being lost. Let W be watermarking information.

For every random pixel in the image, X_i

FORMAT OF IMAGE DATA:

Images are constructed using tiny dots named pixels. Each pixel has got its own attributes for displaying colour and transparency. There are several systems available for representing colour in image pixel. The most common system for representing colour is the ARGB system which stores pixel data in the form of red, green, blue and alpha (transparency). The code shown in this article uses ARGB system for storing and manipulating pixel data.

Under ARGB system, first 8 bits (0 to 7) of the pixel belong to Alpha value or the transparency value. The second 8 bits (8 to 15) represent red colour, third 8 bits (16 to 23) represent green colour and the last 8 bits (24 to 31) represent blue colour.

Now that the pixel level organization of ARGB system is clear, we should understand that that the maximum value for each parameter of ARGB system is 2^8 , i.e., 256.



Figure 7: Organization of pixel under ARGB system

5.4 Watermark Insertion and Extraction:

1. Blind (oblivious or public) Watermarking.

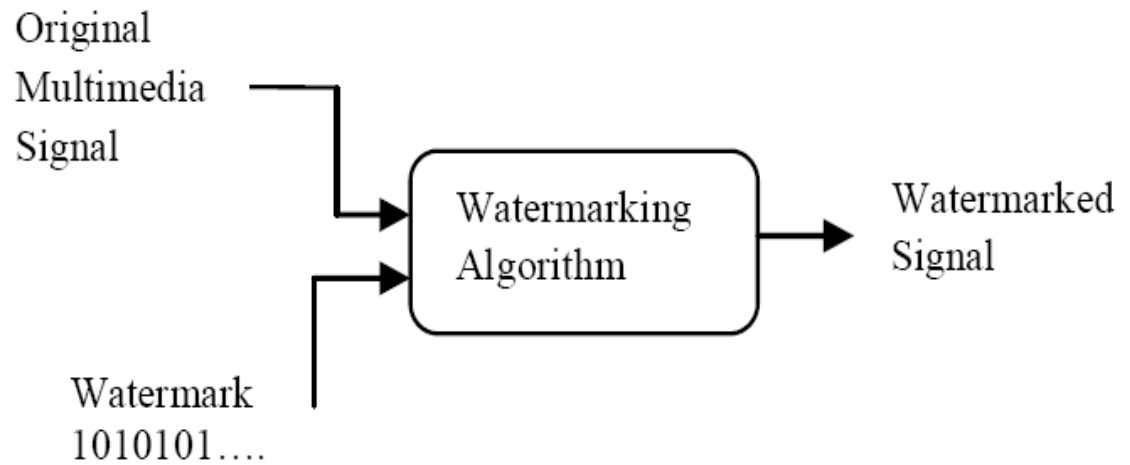


Figure 8: a) Watermark embedding process

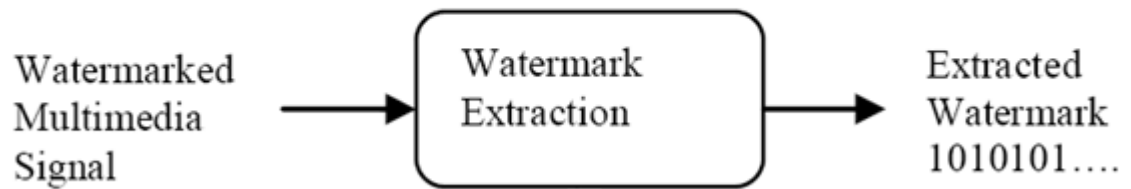


Figure 8: b) Watermark extraction process

CHAPTER 6

COST BENEFIT ANALYSIS

Cost Benefit Analysis

For any given set of requirements by the user it is essential to know how much it will cost to develop the software to satisfy the given requirements, and how much time will be taken in the development process. These all estimates are required before development is initiated. The primary reason for cost and schedule estimation is to enable the client or developer to perform a cost-benefit analysis and for project monitoring and control.

The cost estimates are made at the planning phase of the project. Here in the planning phase we calculated the cost of this project using the COCOMO model. As per the calculations the total cost of the project is 8.0 persons month (PM).

6.1 Benefit Analysis

- The system provides a very good user-friendly interface to enhance the communication between the user and the software.
- The system is platform independent, thus allows the user to deploy on any operating system.
- The information security provided by this application is very valuable as any organization cannot compromise on this aspect.
- This application also provides the feature of transferring the files from one machine to another machine which is also the valuable aspect when combined with the security.
- This application also provide a very good help support for the application.

CHAPTER 7


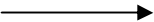
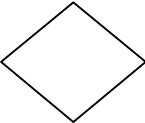

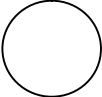


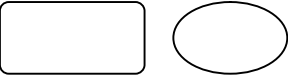
SYSTEM LIFE CYCLE

7.1 Description:

1) System Flow Chart

A flowchart is a picture of the separate steps of a process in sequential order. Elements that may be included are: sequence of actions, materials or services entering or leaving the process (inputs and outputs), decisions that must be made, people who become involved, time involved at each step and/or process measurements.

Table of Commonly used symbols for flow chart are:

	One step in the process; the step is written inside the box. Usually, only one arrow goes out of the box.
	Direction of flow from one step or decision to another.
	Decision based on a question. The question is written in the diamond. More than one arrow goes out of the diamond, each one showing the direction the process takes for a given answer to the question. (Often the answers are <i>õ yes</i> and <i>õ no</i> .)
	Delay or wait
	Link to another page or another flowchart. The same symbol on the other page indicates that the flow continues there.
	Input or output
	Document
	Alternate symbols for start and end points.

SYSTEM FLOW CHART:

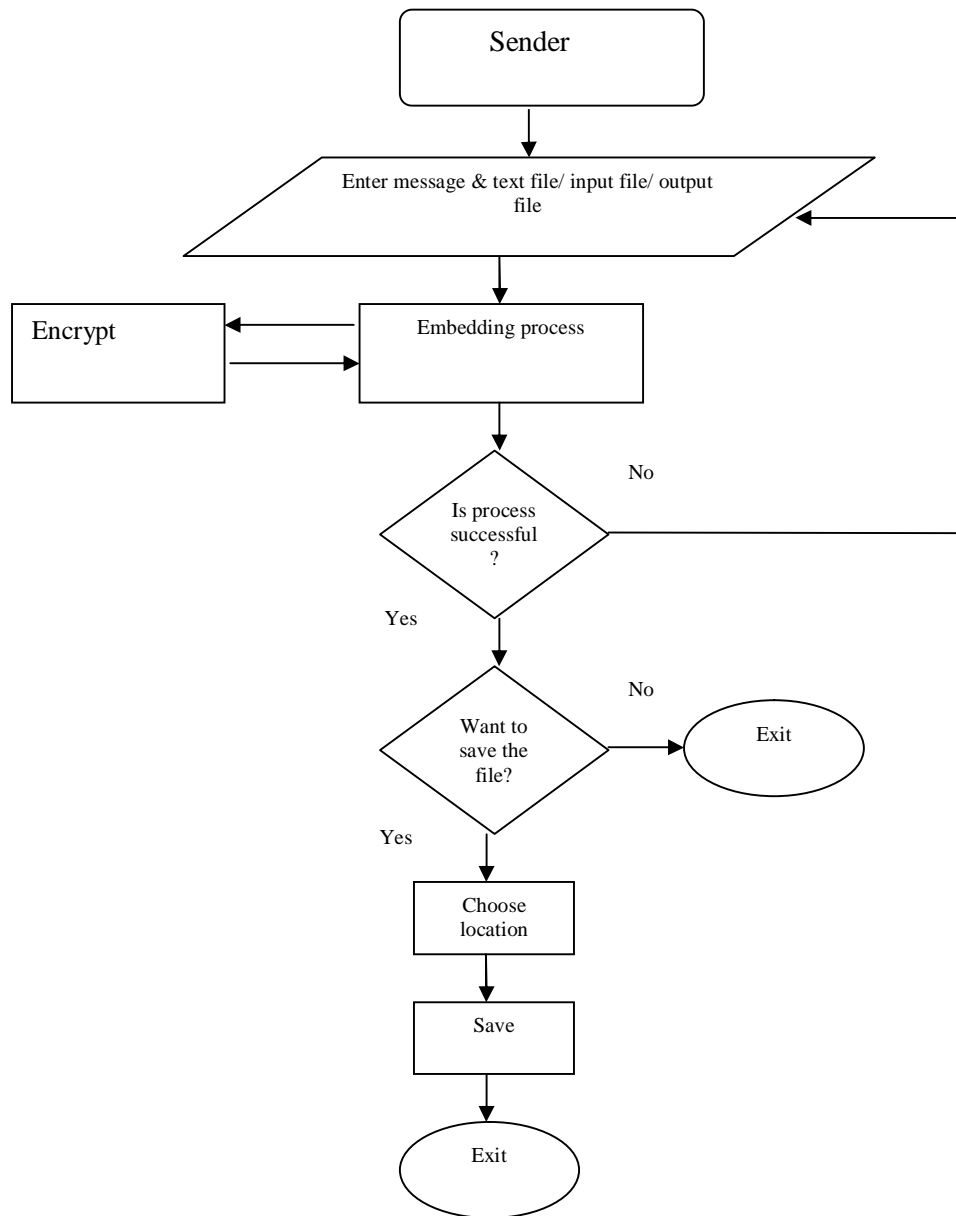


Figure 9: a) System flow chart for Insertion

SYSTEM FLOW CHART:

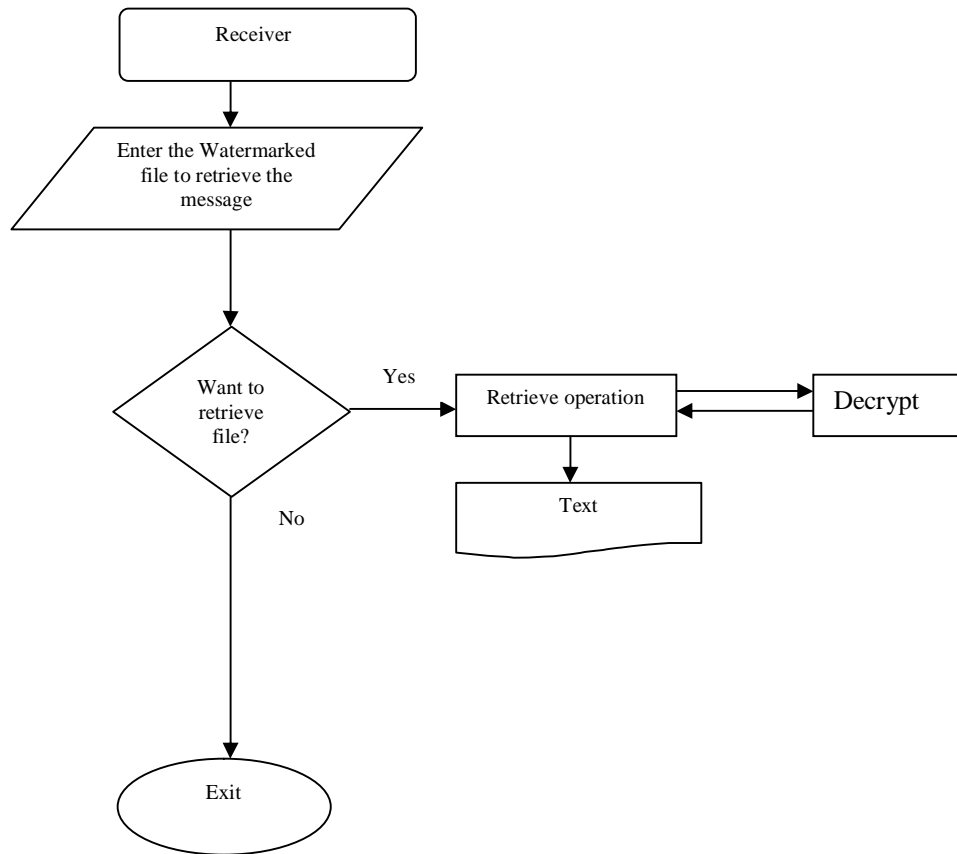


Figure 9: b)System flow chart for Extraction

2)Use case Diagram:

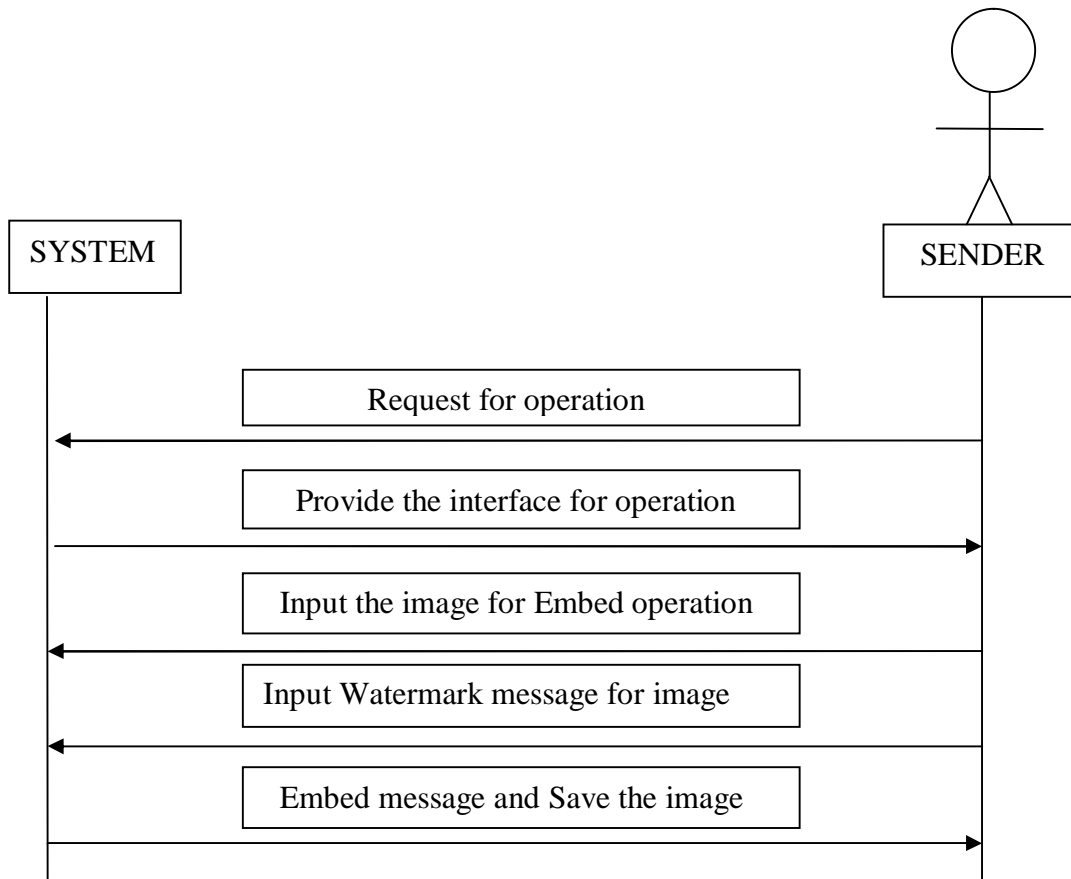


Figure 10 a) : Use case diagram For Sender

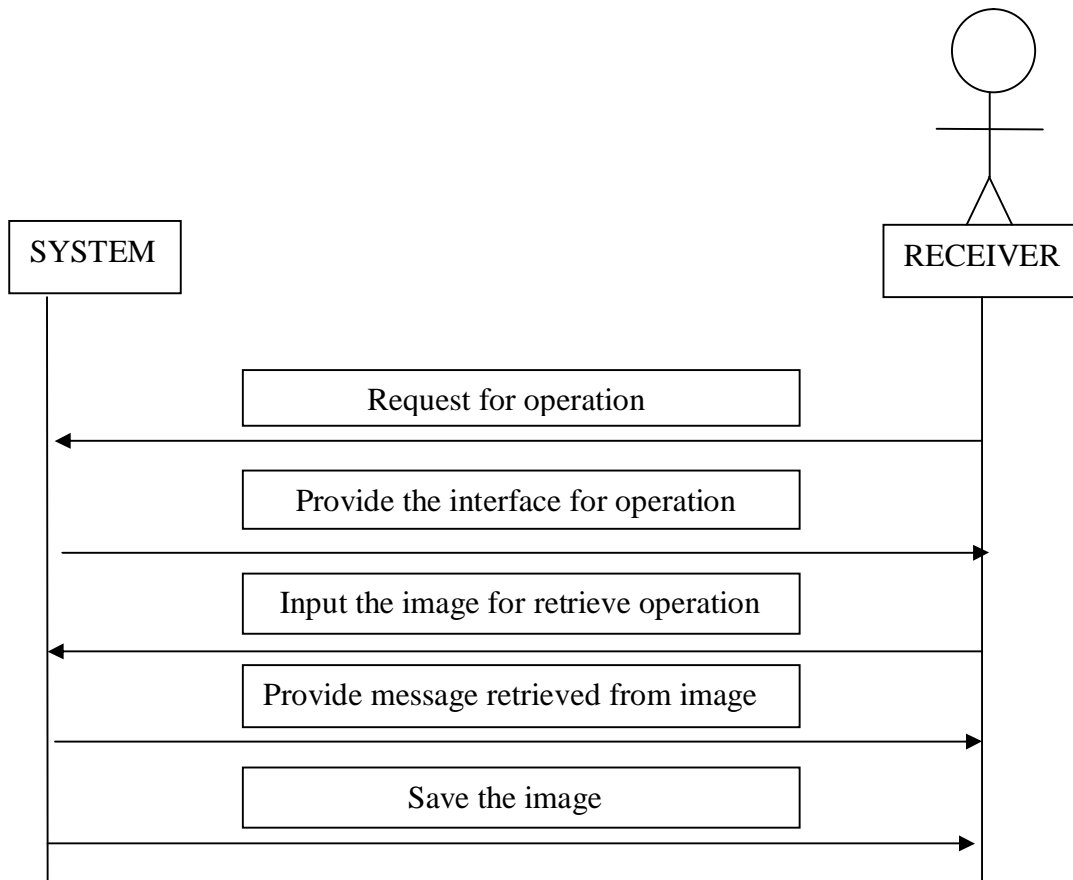


Figure 10 b) : Use case diagram For Receiver

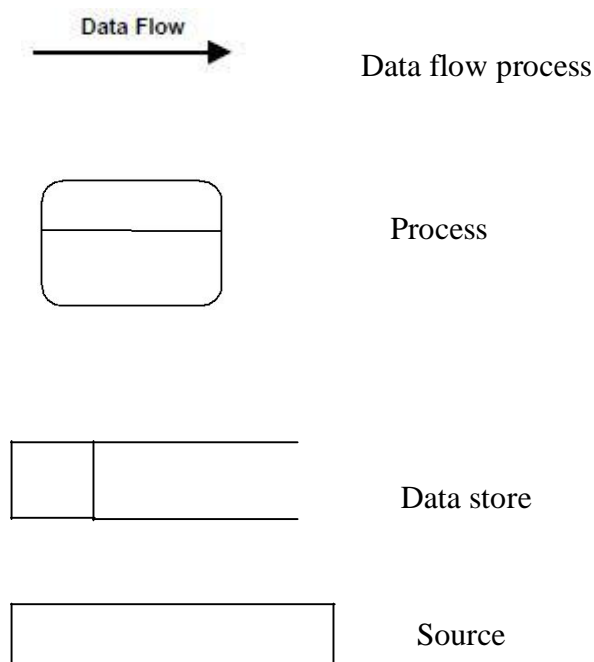
7.1.3 DATA FLOW DIAGRAMS:

Data flow diagrams are the basic building blocks that define the flow of data in a system to the particular destination and difference in the flow when any transformation happens. It makes whole procedure like a good document and makes simpler and easy to understand for both programmers and non-programmers by dividing into the sub process.

The data flow diagrams are the simple blocks that reveal the relationship between various components of the system and provide high level overview, boundaries of particular system as well as provide detailed overview of system elements

The data flow diagrams start from source and ends at the destination level i.e., it decomposes from high level to lower levels. The important things to remember about data flow diagrams are: it indicates the data flow for one way but not for loop structures and it doesn't indicate the time factors.

The general notations for constructing a block diagram in this project are



Data flow processes:

It will define the direction i.e., the data flow from one entity to another entity.

Process:

Process defines the source from where the output is generated for the specified input. It states the actions performed on data such that they are transformed, stored or distributed.

Data store:

It is the place or physical location where the data is stored after extraction from the data source.

Source:

It is the starting point or destination point of the data, starting point from where the external entity acts as a cause to flow the data towards destination.

Data Flow Diagram Level 0 :

DFD level 0 is the highest level view of the system, contains only one process which represents whole function of the system. It doesn't contain any data stores and the data is stored within the process.

For constructing DFD level 0 diagram for the proposed approach we need two sources one is for source and another is for destination and a process.



Figure 11: a) Data flow diagram level 0

DFD level 0 is the basic data flow process, the main objective is to transfer the data from sender to receiver after encryption.

Data Flow Diagram Level 1:

For constructing ŠDFD level 1 , we need to identify and draw the process that make the level 0 process. In the project for transferring the personal data from source to destination, the personal data is first encrypted and processed and latter decrypted.

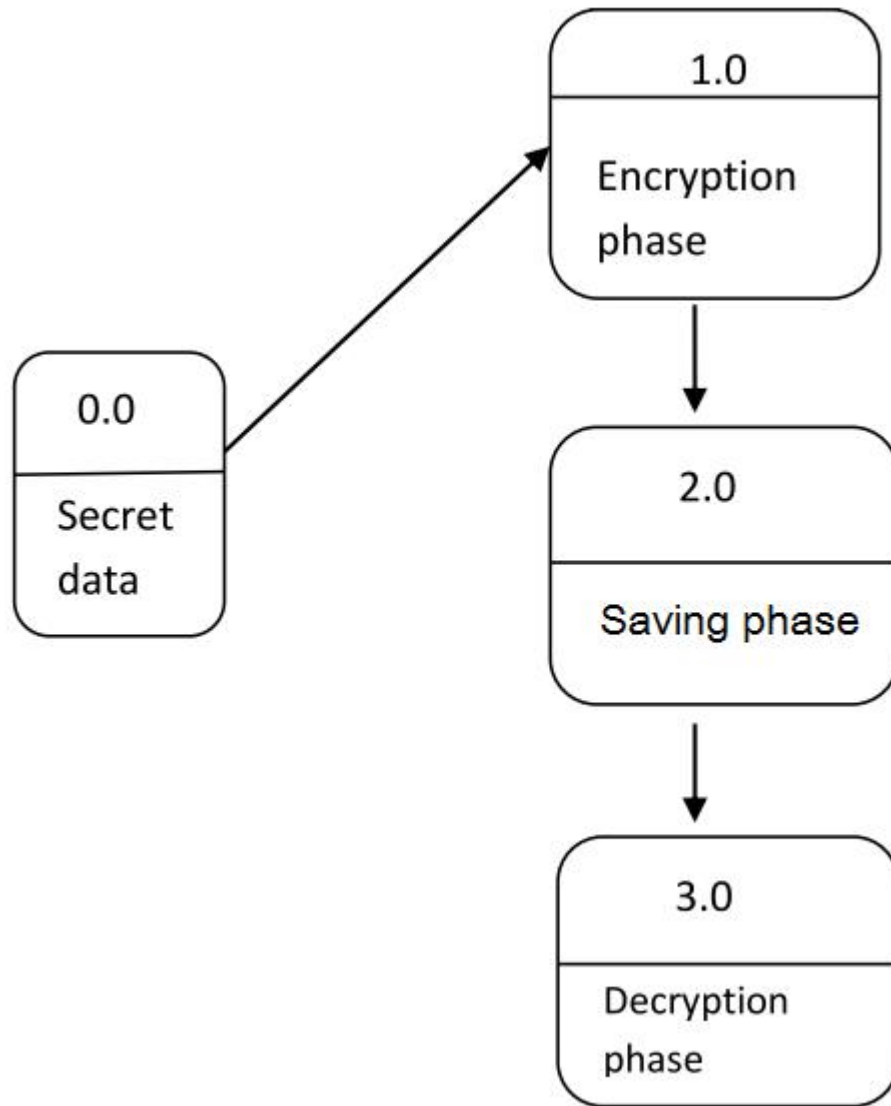


Figure 11: b) Data flow diagram level 1

In this data flow diagram, the secret data is sent to the encryption phase for embedding the data into the image for generating the Watermarked image. In the next phase the Watermarked image is sent to the decryption phase through the Saving phase. The final phase is the decryption phase where the data is extracted from the image and displays the original message.

Data Flow Diagram Level 2 :

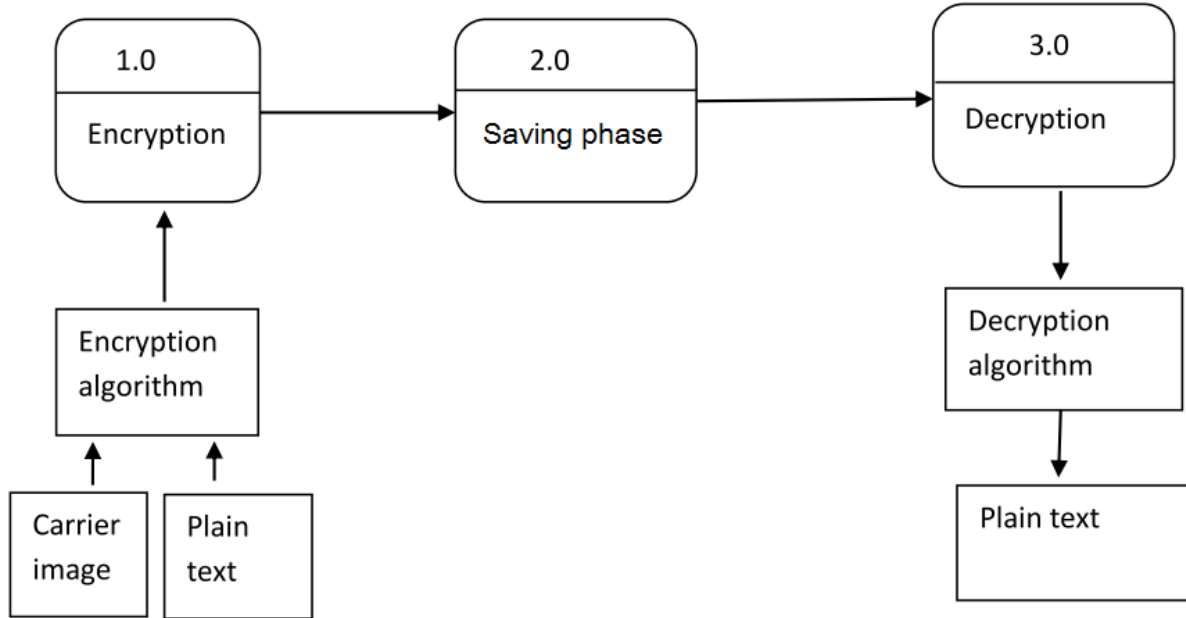


Figure 11: c) Data flow diagram level 2

The image and the text document are given to the encryption phase. The encryption algorithm is used for embedding the data into the image.

The resultant image acting as a Watermarked image is saved to the decryption. For extracting the message from the Watermarked image, it is sent to the decryption section. The plain text is extracted from the Watermarked image using the decryption algorithm.

CHAPTER 8

TESTING

Testing:-

The basic goal of software development process is to produce the software that has very few or no errors. In an effort to detect errors soon after they are introduced each phase ends with verification activity such as reviews. However most of these verification activities in the early phase of the software development are based on human evaluation and cannot detect all the errors. Testing plays an important role in quality assurance for the software. It is a dynamic method for the verification and validation, where the system to be tested is executed and the behavior of the system is observed.

8.1 Levels of testing

The programs are tested at various levels:

Unit testing

The first level of testing is called unit testing. In this different modules are tested against the specifications produced during design for the modules. Unit testing is essentially for verification of code produced during the coding phase and hence the goal is to test internal logic of the modules. Each of the modules is tested independently.

Integration testing

The next level of testing is often called integration testing. In this many unit tested modules are combined into sub systems which are then tested. The goal here is to see if the modules can be integrated properly.

System testing

This is the next levels of testing. Here the entire software is tested. The reference document for this process is the requirements document and the goal is to see if the software meets its requirements. This is essentially a validation exercise and in this situation it is the only validation activity.

8.2 Test Plan

A test plan is a general document for the entire project that defines the scope, approach to be taken, and the schedule of testing as well as identifies the test items for the entire testing process and the personnel responsible for the different activities of testing.

The test planning can be done well before the actual testing commences and can be done in parallel in the design and coding phase.

The input for the test plan is:

- 1) Project Plan
- 2) Requirement Document and
- 3) System Design Document.

The project plan is needed to make sure that the test plan can be consistent with the overall plan for the project and the testing schedule matches that of the project plan.

The requirement documents and the design document are the basic documents used for selecting the test unit and the deciding the approaches to be used during testing.

A test plan should contain following:

- 1) Test Unit Specification.
- 2) Features to be tested.
- 3) Approach for testing.

1) Test Unit

A test unit is a set of one or more modules, together with associated data, that are from single computer program and that are the object of testing.

A test unit can occur at any level and can contain from a single module to entire system.

2) Features to be tested.

All functional features specified in the requirement document will be tested. The features to be tested are:

- 1) Embed Message
- 2) Embed File
- 3) Retrieve Message
- 4) Retrieve File
- 5) Help

3) Approach for testing.

There are two approaches to testing:

1. Functional (Black Box) Testing

In functional testing the internal logic of the system is not considered and the test cases are decided from the specifications or the requirements. It is often called "Black Box" testing.

Test case 1: Embed Message

- User can embed the message behind the image. For that user has to enter the Input file and the message which is to be embedded.

- If the Embed process is successful then it will show message, "Embed file on screen". If at all the embed process do not complete successfully, then it will generate an alert.
- As soon as the embed process complete successfully, the send button will get enabled and then the user can send the message to the desired destination.
- Either of the fields should not be left blank. If any of the field is left blank then it will show an alert message.

Test case 2: Embed File

- User can embed the entire file behind the image. For that user has to enter the Input file and the file that contains the data which is to be embedded.
- If the Embed process is successful then it will show message, "Embed Process completed Successfully". If at all the embed process do not complete successfully, then it will generate an alert.
- As soon as the embed process complete successfully, the send button will get enabled and then the user can send the message to the desired destination.
- Either of the fields should not be left blank. If any of the field is left blank then it will show an alert message.

Test case 3: Retrieve Message

- User can retrieve the entire message from the image. For that user has to enter the Input file in which the message has been embedded. Then user has to click on retrieve button to get the content.
- If the Retrieve process is successful then it will show message, "Retrieve Process completed Successfully". If at all the retrieve process do not complete successfully, then it will generate an alert.
- If the retrieve process completes successfully, then the message, which was embedded, will get visible in the text area provided for displaying the message.
- As soon as the retrieve process complete successfully, the save button will get enabled and then the user can save the message to the desired location.
- Either of the fields should not be left blank. If any of the field is left blank then it will show an alert message.

Test Case 4: Help File

- User when goes to the Help menu and clicks on "Watermark info" button then Help window get open.
- Clicking on the back hyperlink on the help page main help menu is displayed

2. Structural (White Box) Testing

In structural testing, the test cases are decided entirely on the internal logic of the program or module being tested. The external specifications are not considered.

In white box testing we check

- Whether all the methods are implemented and working properly.
- All the conditional statement is giving right output or not.
- Whether the variable that is declared is reserved or not and also checked the scope of variable.
- Whether all the control properties are used appropriately.
- Proper validation of various fields is done or not.

Test case 1:

- Whether all the buttons become enabled after the successful open application. Some of the buttons which are required for accessing the application will get enabled after open application.

Test case 2:

- Whether the message is entered in text area or not. If message is not provided in text area, then it will ask user to enter the message.

Test case 3:

- Whether the selected input file is valid or not. That is, the input file which is selected should be present in the system and also it should be valid.

Test case 4:

- Whether the embed process complete successfully or not. If the embed process do not complete successfully then it will show error message. If the embed process complete successfully then it will then it will give message that the embed process has been completed successfully.

Test case 5:

- Whether the retrieve operation can fetch the message or file or not. If the retrieve operation fail to retrieve the message or file then it will display the message. If the retrieve operation complete successfully the then it will ask the receiver to set the location for the file to be saved. Similarly the message which is retrieved can also be saved.

Test case 6:

- Whether the input file from which the user is trying to fetch result contain embedded message or not. If the input file do not contain embedded message then it will show error message.

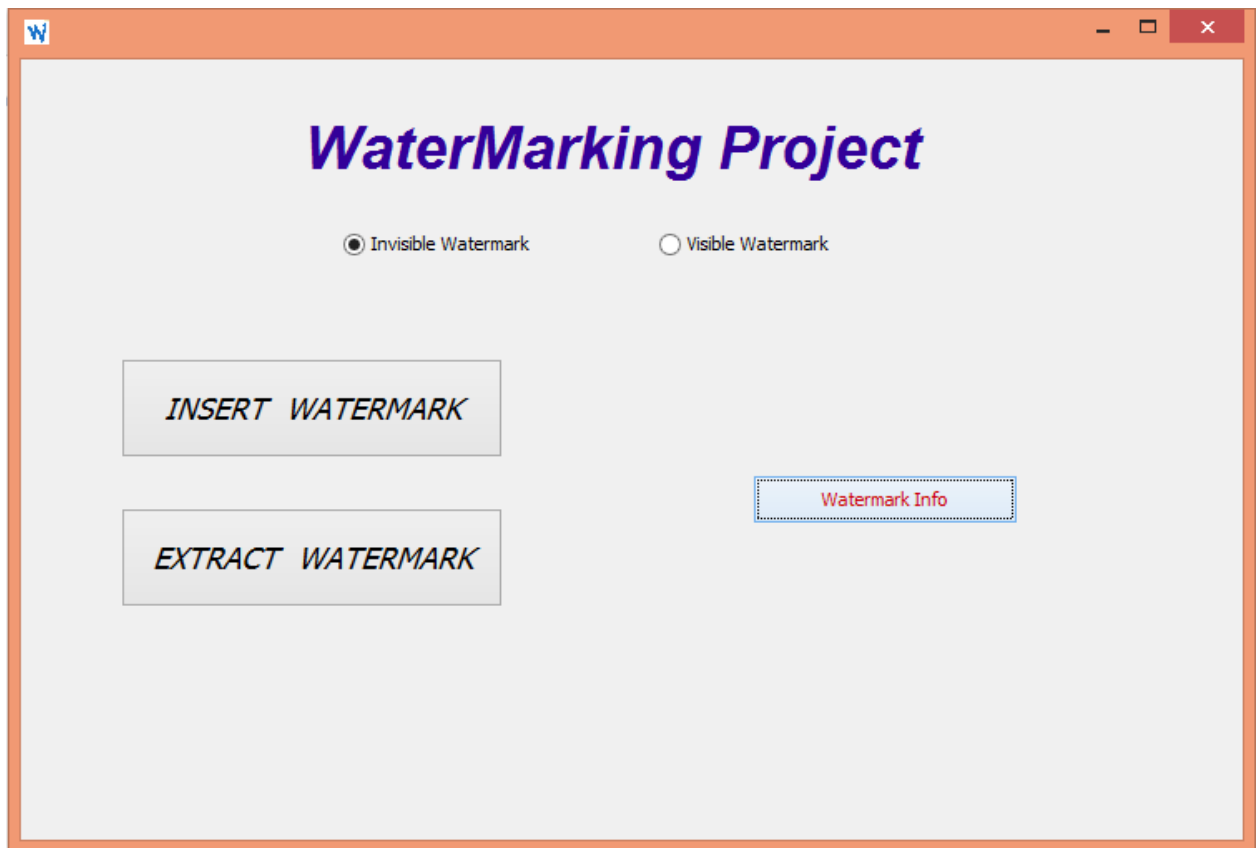
CHAPTER 9

IMPLIMENTATION

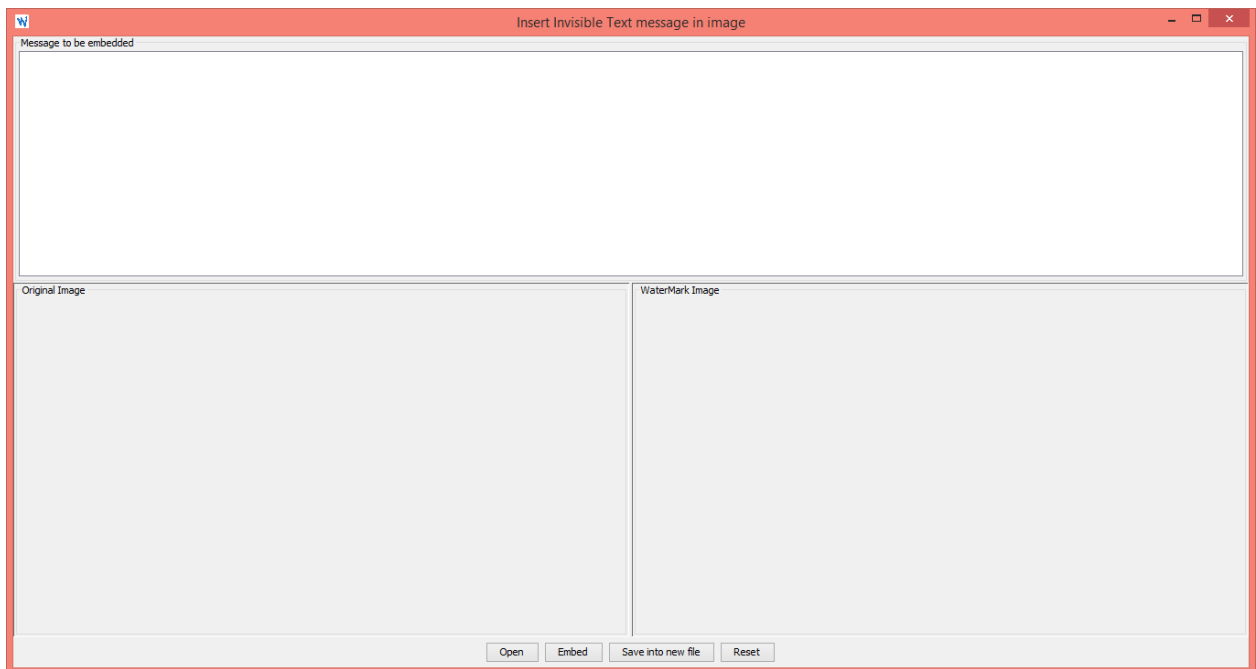
9.1 Snap Shot of Project:

INVISIBLE WATERMARK INSERTION :

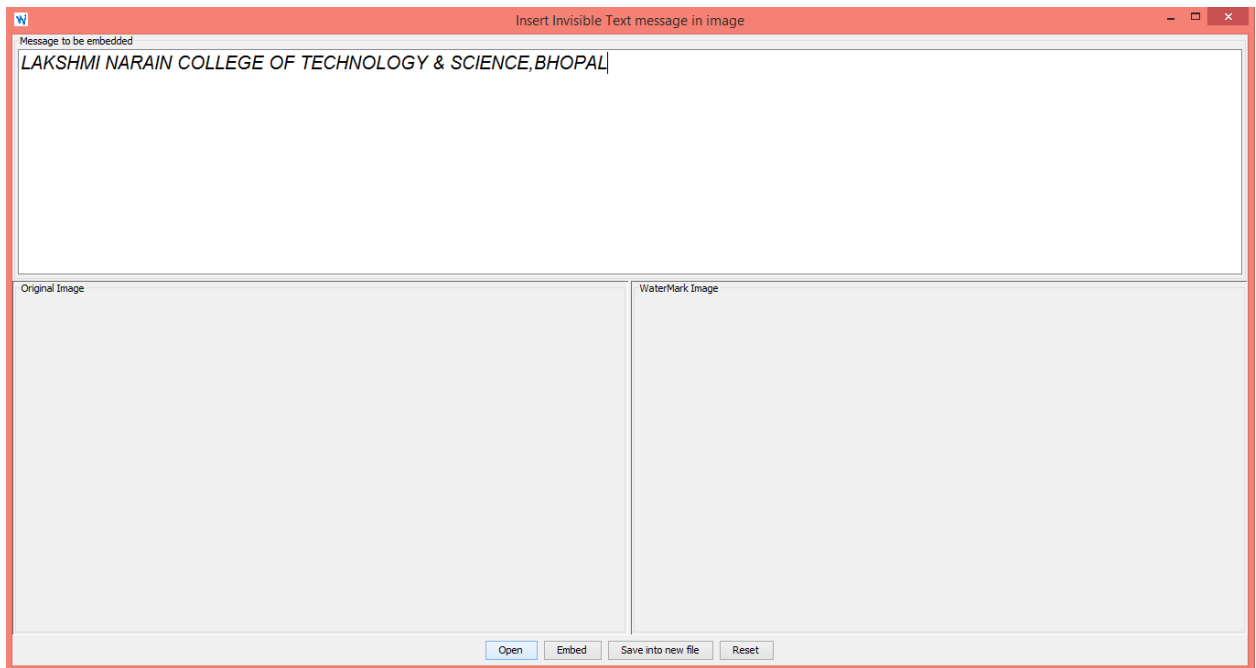
INITIAL PAGE :



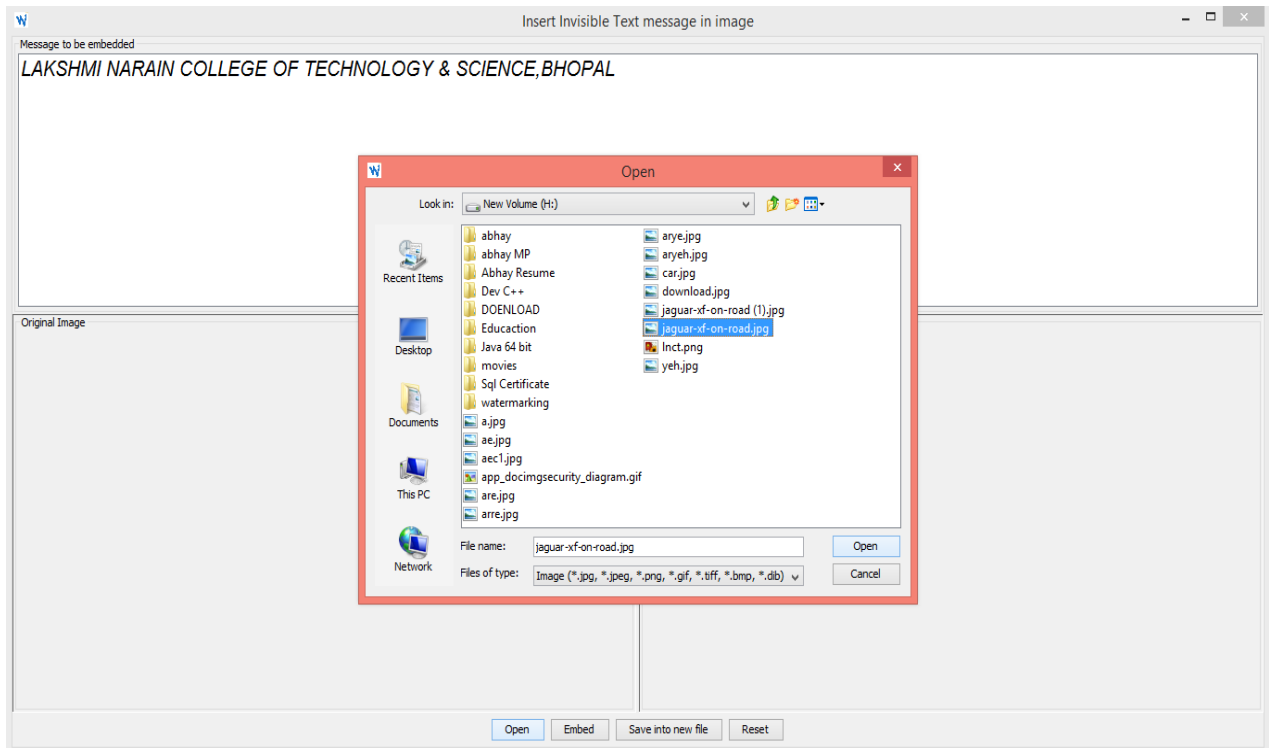
INSERTION WINDOW FOR INVISIBLE WATERMARK



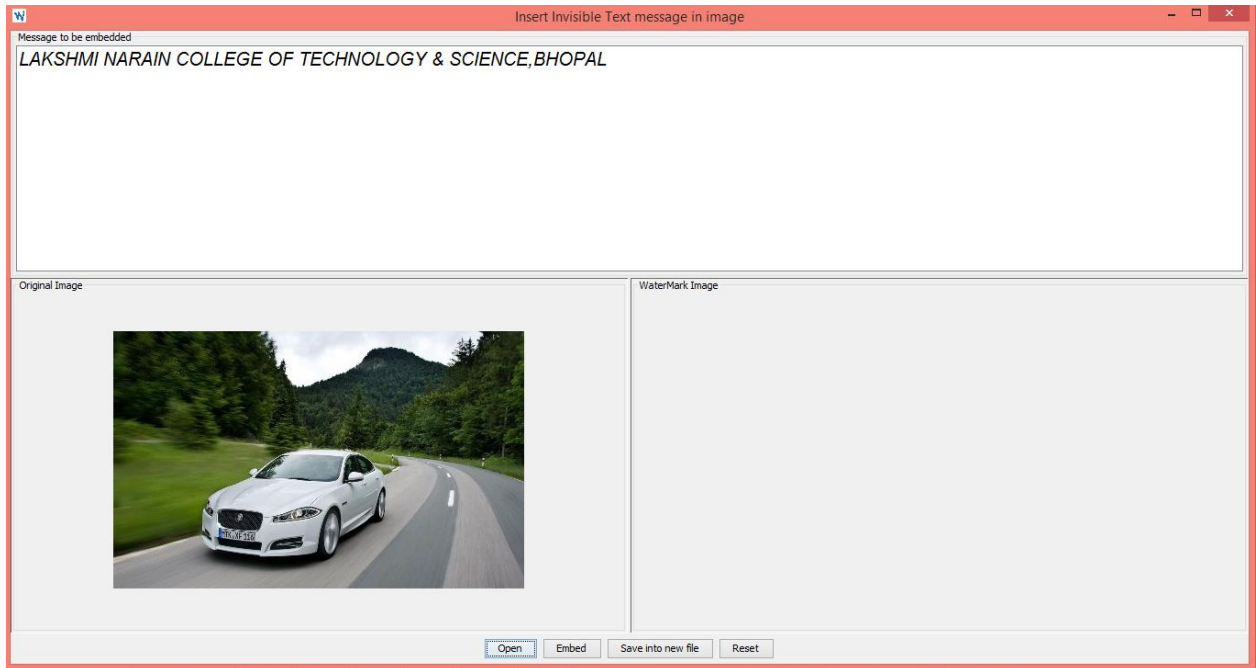
TEXT TO BE WATERMARKED



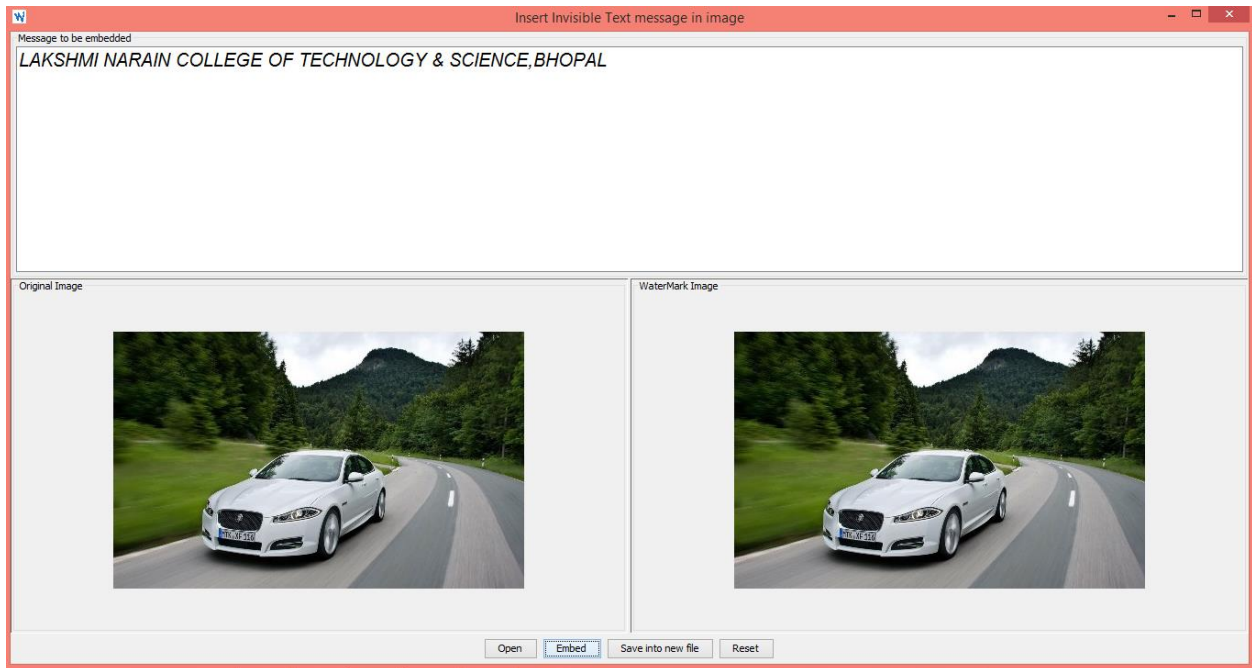
CHOOSING IMAGE FOR WATERMARKING



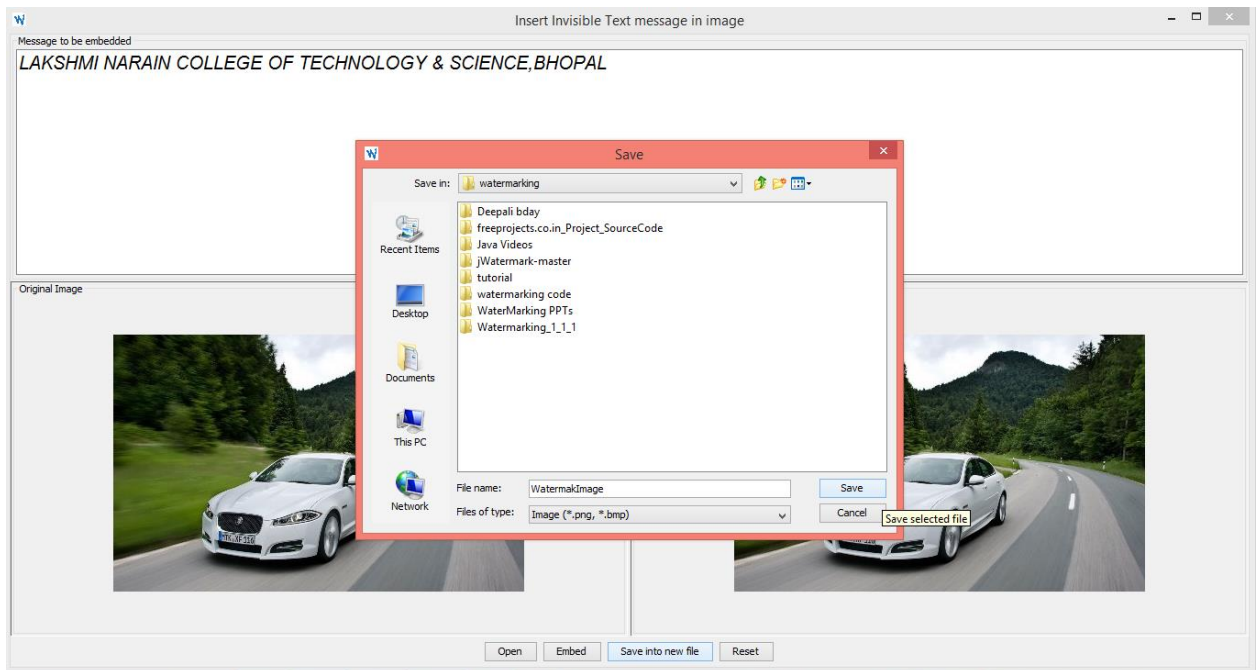
ORIGINAL IMAGE OPENED



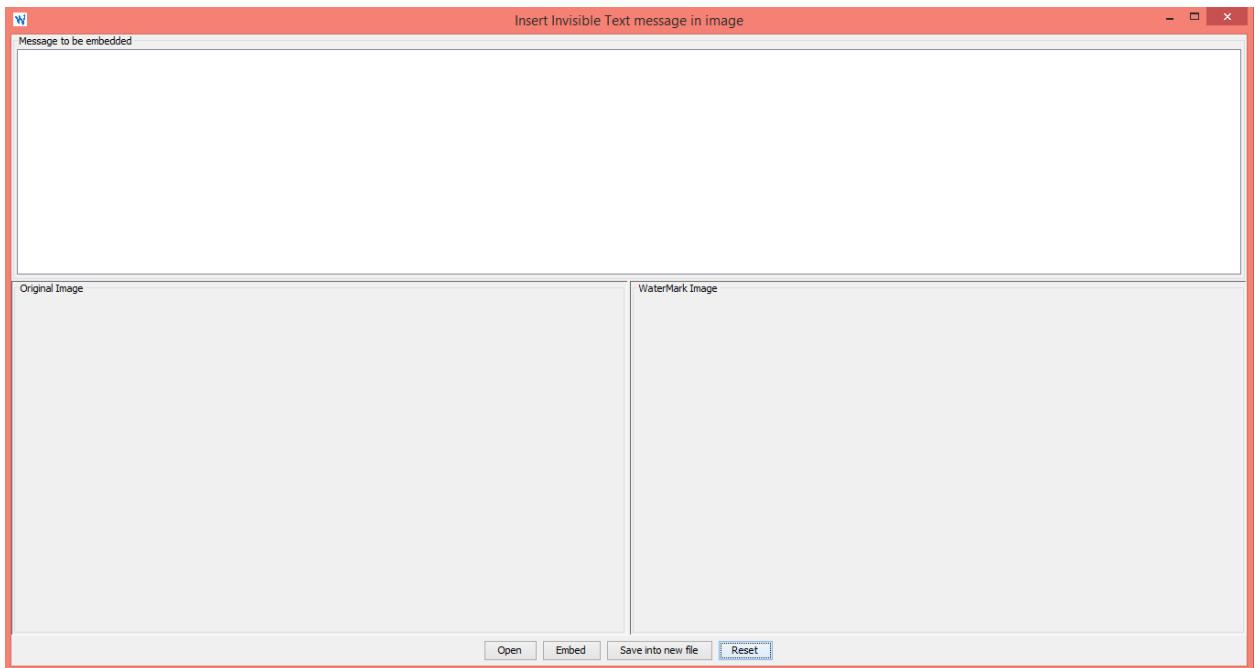
ON EMBEDDING WATERMARKED IMAGE IS GENERATED



SAVING WATERMARKED IMAGE

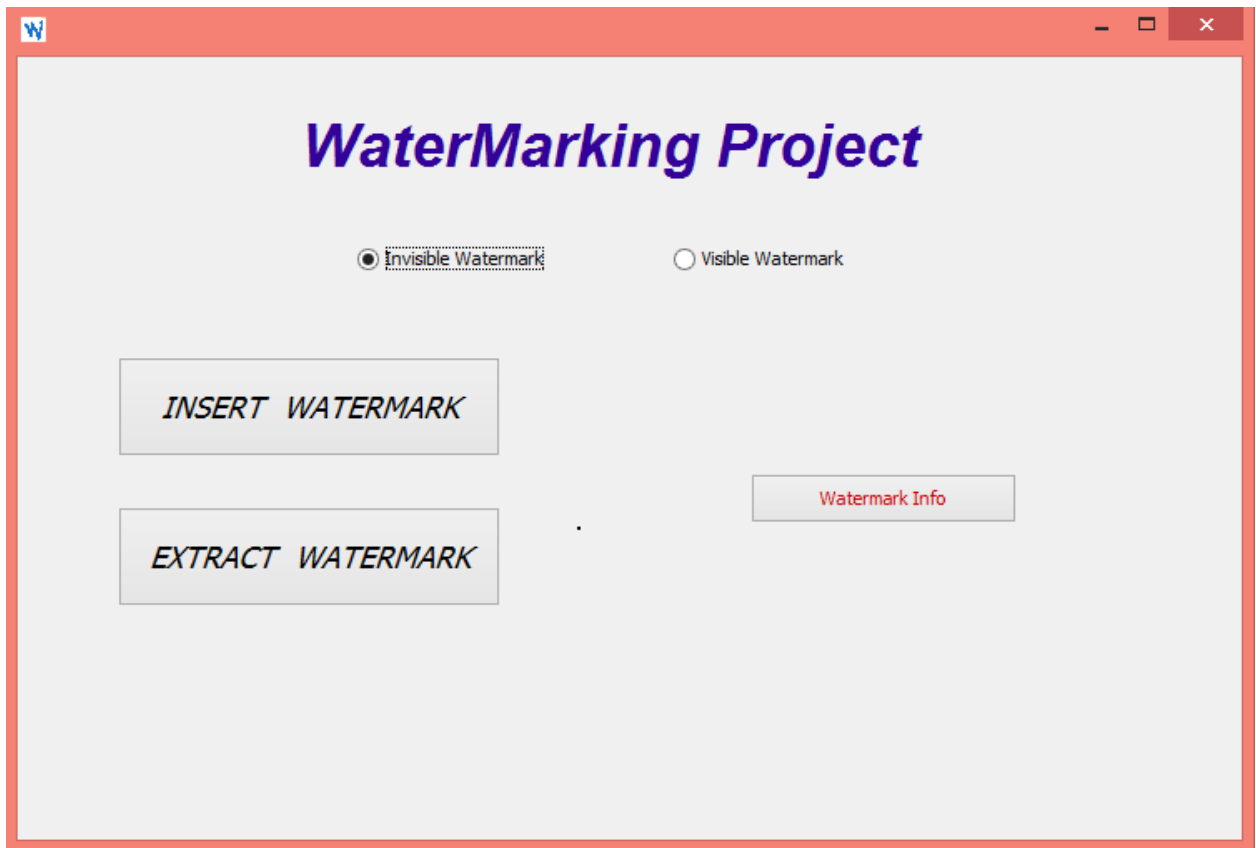


WINDOW RESET

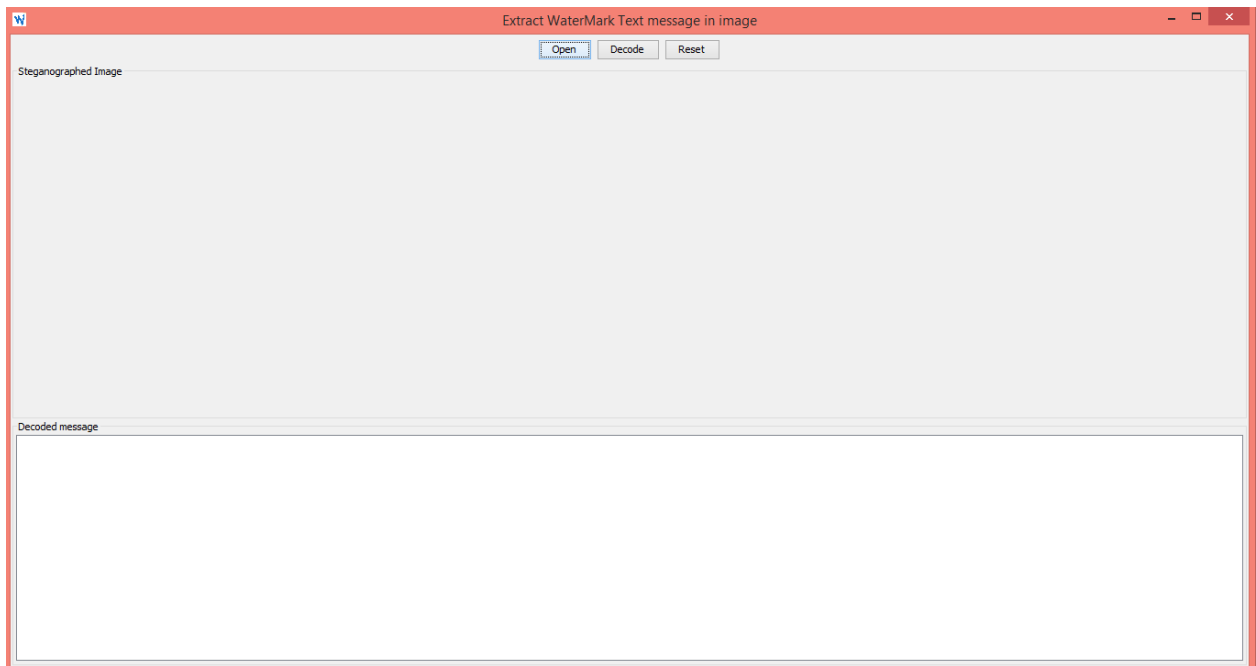


INVISIBLE WATERMARK EXTRACTION

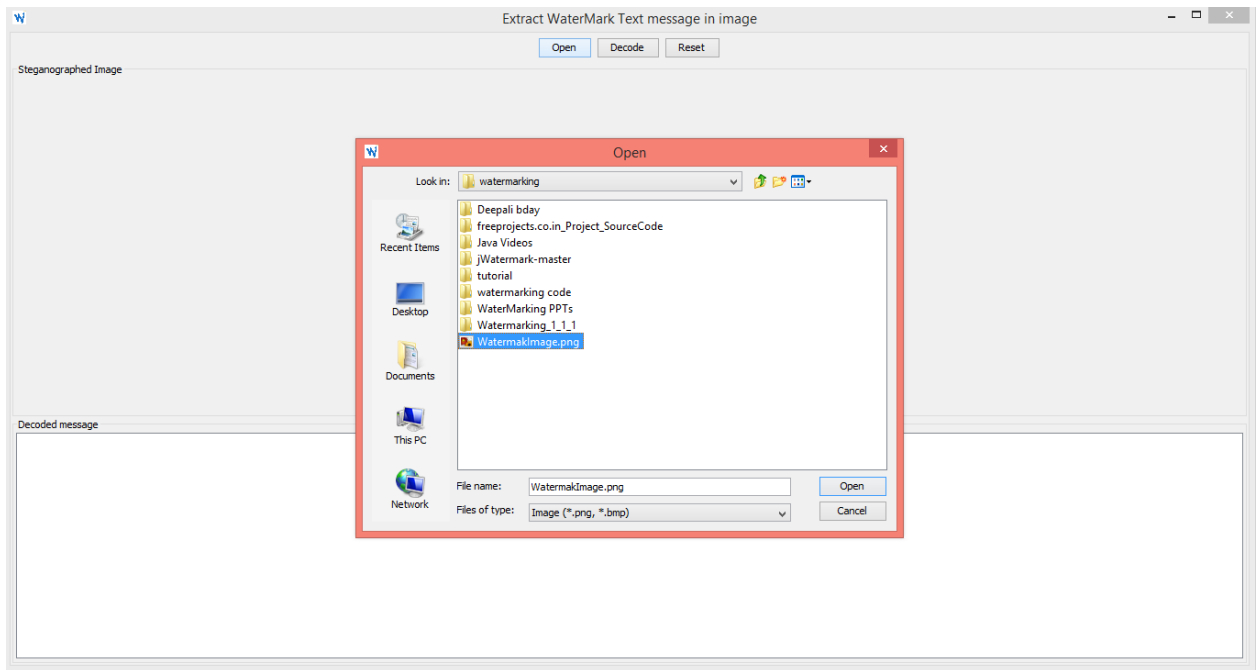
INITIAL PAGE:



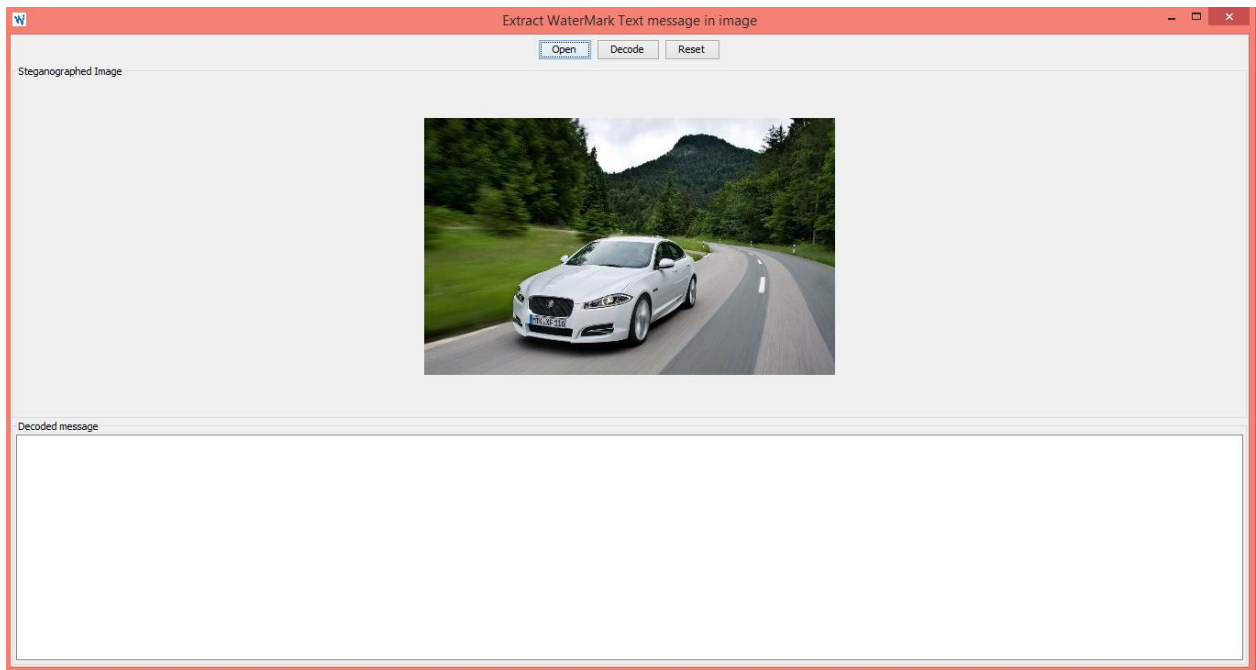
EXTRACTION WINDOW



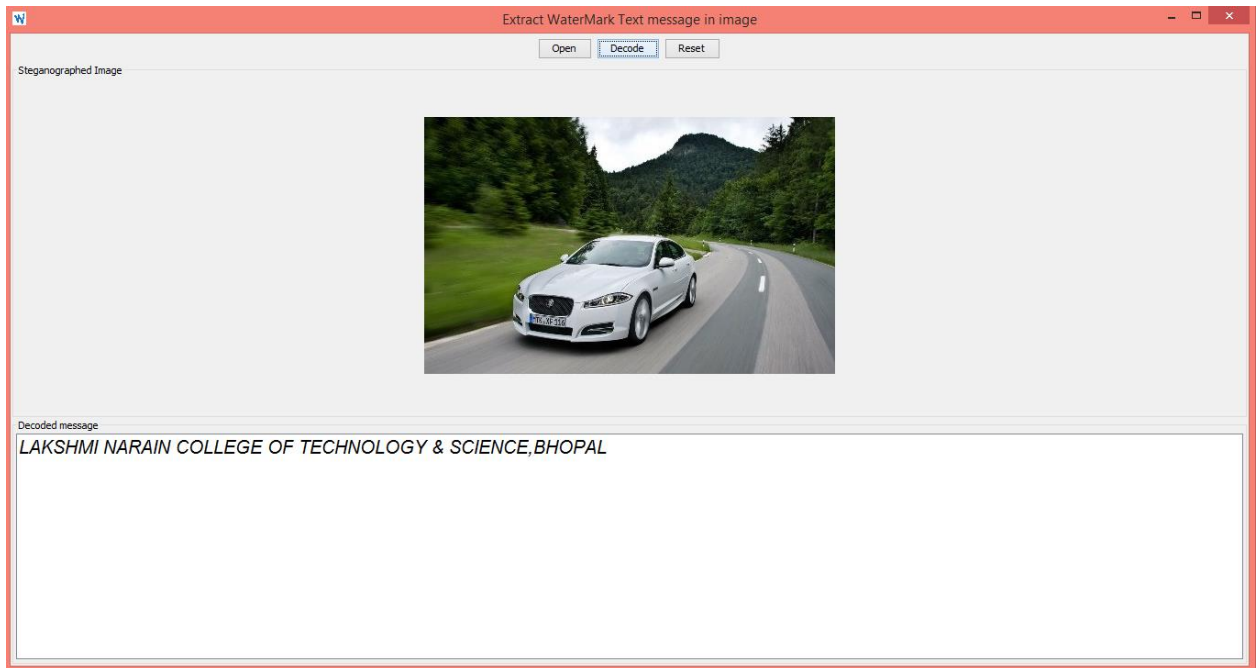
CHOOSING WATERMARKED IMAGE



WATERMARKED IMAGE OPENED



ON DECODING WATERMARKED TEXT IS EXTRACTED



VISIBLE WATERMARKING :

INITIAL PAGE

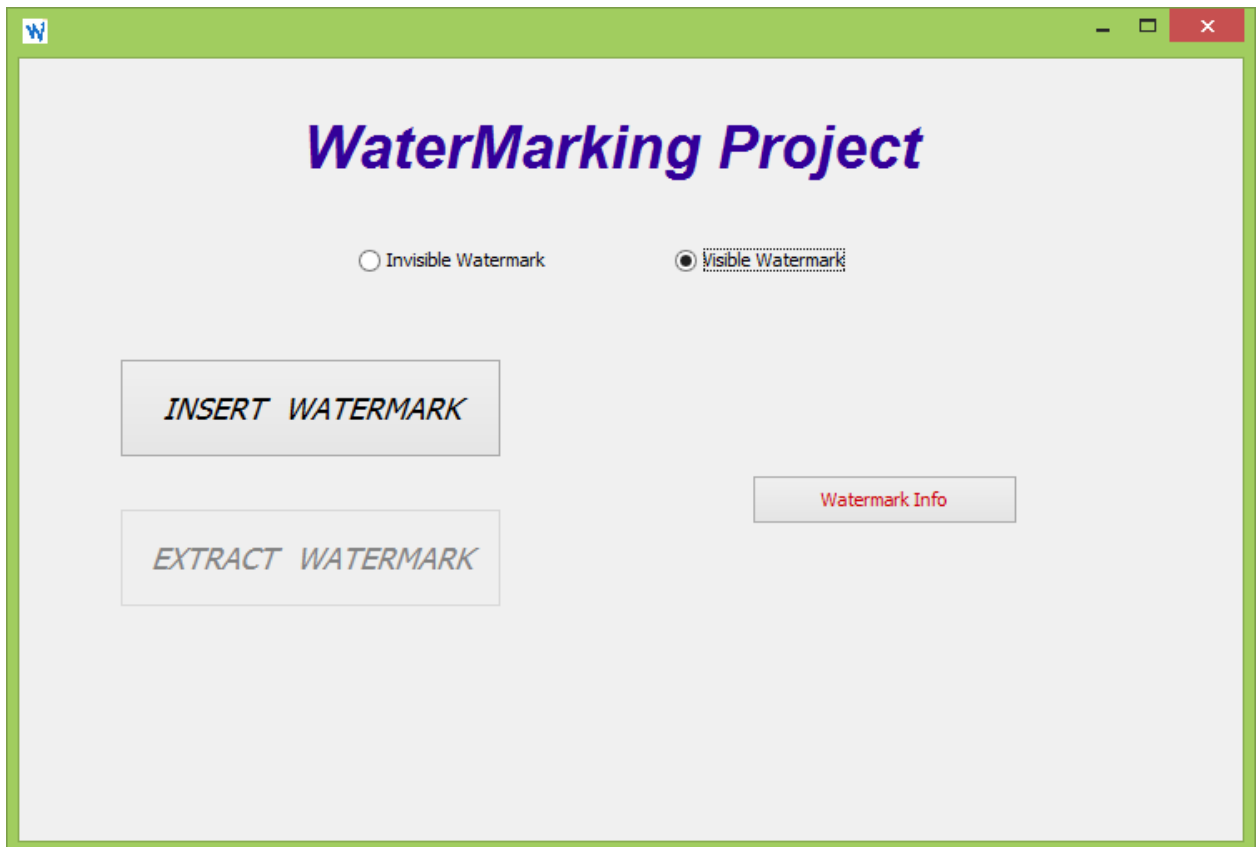


IMAGE INFORMATION WINDOW FOR WATERMARK INSERTION

The image shows a software window titled "IMAGE INFORMATION WINDOW FOR WATERMARK INSERTION". The window has a light gray background and an orange border. At the top left, there is a small icon of a circle with a left-pointing arrow. Below this, the text "IMAGE INFO" is displayed in a bold, italicized font. Underneath, the label "SOURCE IMAGE :" is followed by a text input field and a "Browse..." button. In the center, the text "WATERMARK TEXT / IMAGE" is displayed in a bold, italicized font. Below this, there are two radio buttons: "Text" (which is selected) and "Image". Below the radio buttons is a text input field and a "Browse..." button. At the bottom center of the window, there is a large button labeled "INSERT".

IMAGE INFO

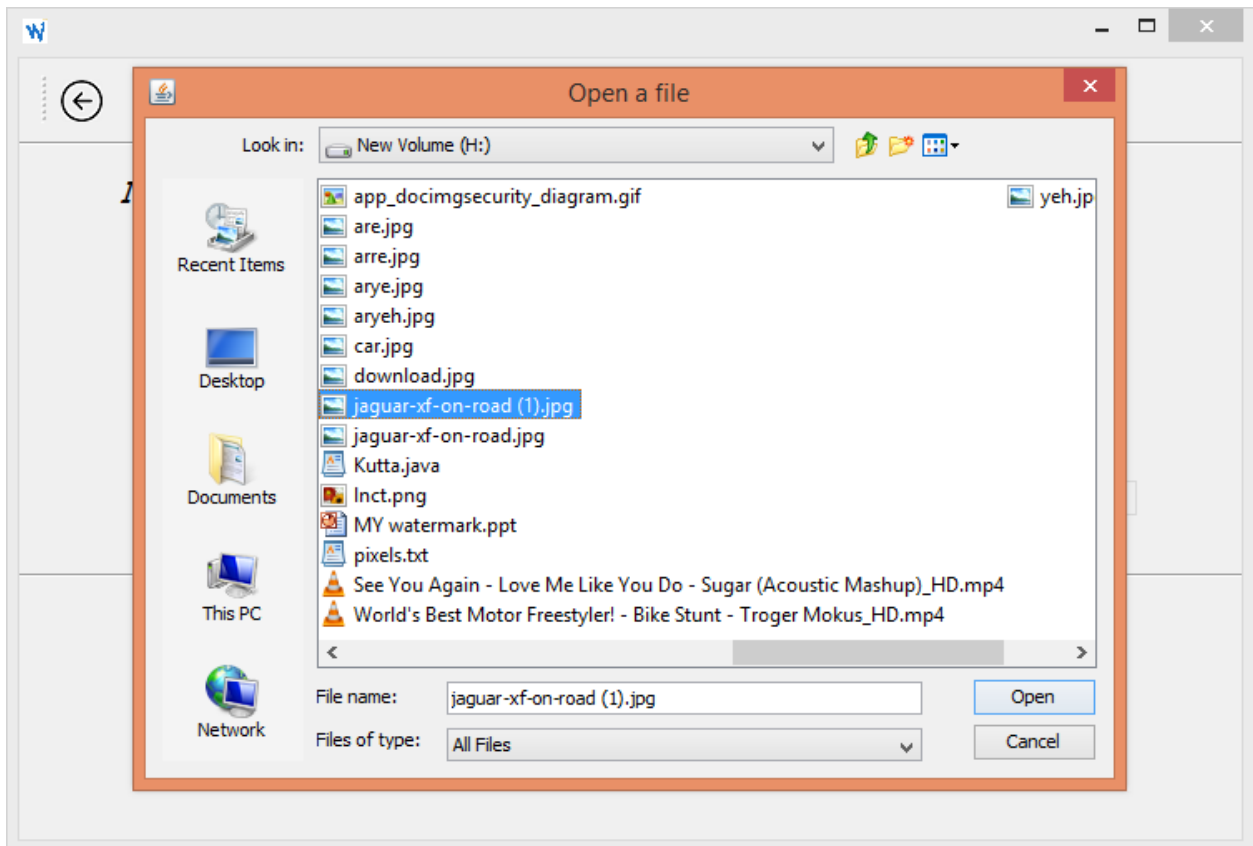
SOURCE IMAGE :

WATERMARK TEXT / IMAGE

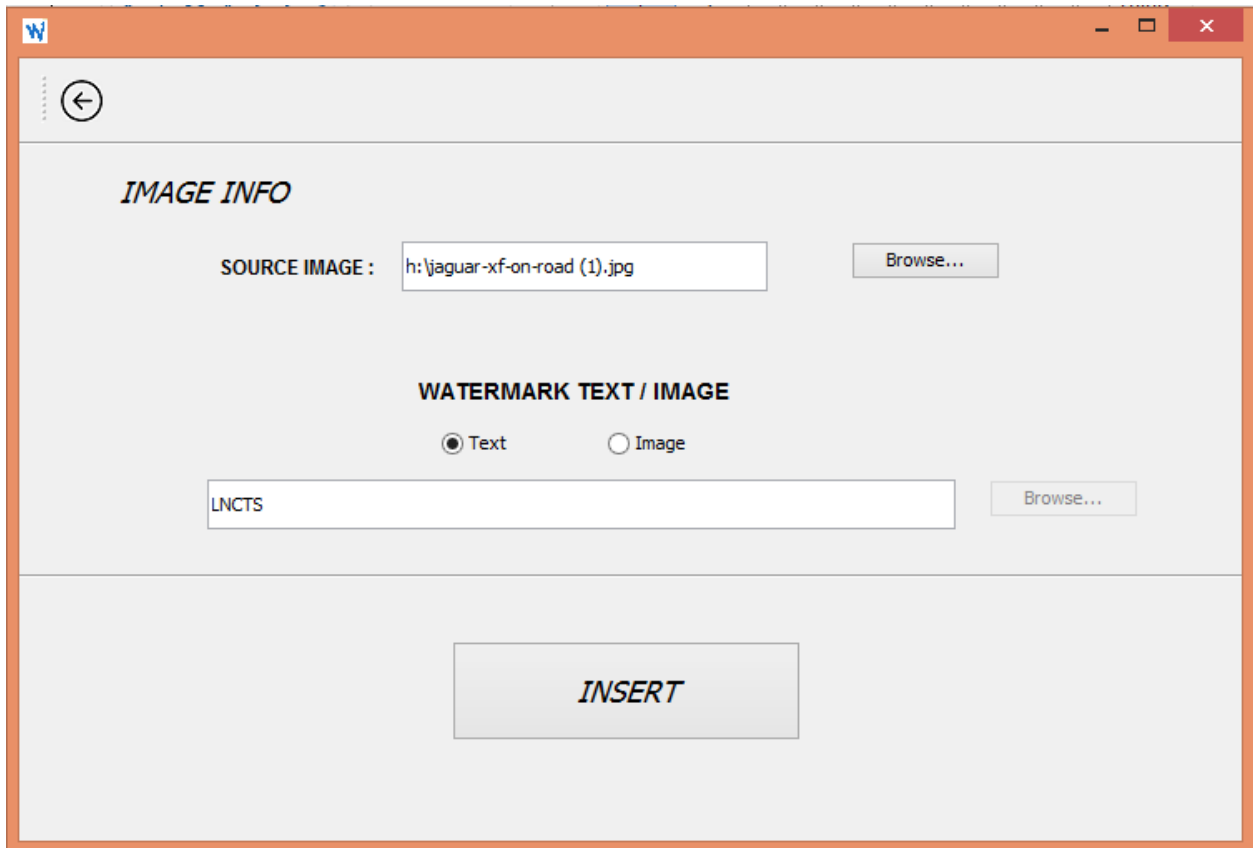
☒ Text ☐ Image

INSERT

CHOOSING IMAGE

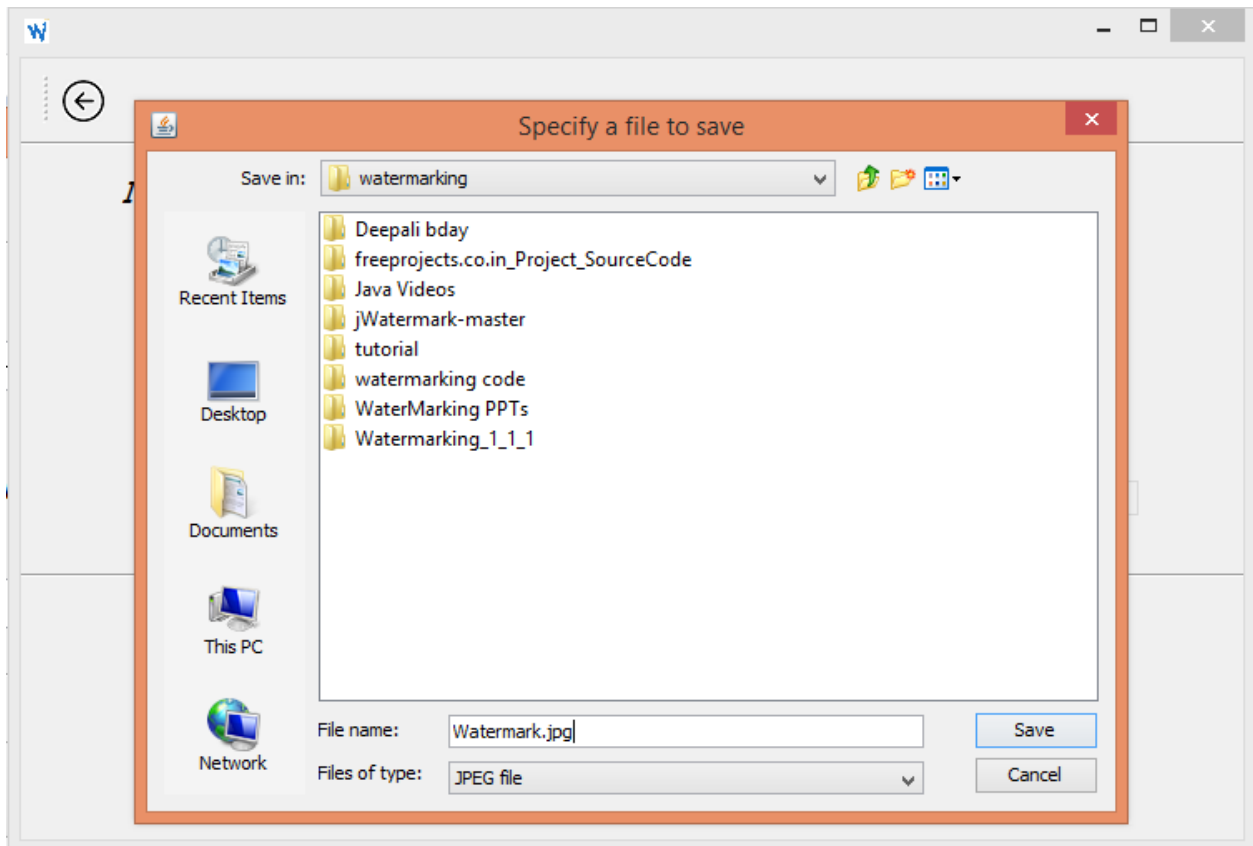


WRITE A TEXT TO BE WATERMARKED



The image shows a screenshot of a watermarking application window. The window has an orange title bar with a Windows logo icon on the left and standard minimize, maximize, and close buttons on the right. Inside the window, there is a light gray background. At the top left, there is a circular icon with a left-pointing arrow. Below this, the text *IMAGE INFO* is displayed. Underneath, the label "SOURCE IMAGE :" is followed by a text box containing the path "h:\jaguar-xf-on-road (1).jpg". To the right of this text box is a "Browse..." button. Below the source image section, the text **WATERMARK TEXT / IMAGE** is centered. Underneath this, there are two radio buttons: "Text" (which is selected) and "Image". Below the radio buttons is a text box containing the text "LNCTS". To the right of this text box is another "Browse..." button. At the bottom center of the window is a large button labeled *INSERT*.

SAVE THE WATERMARKED IMAGE



ORIGINAL IMAGE & WATERMARKED IMAGE



SELECTION OF ORIGINAL IMAGE & IMAGE TO BE WATERMARKED

W

←

IMAGE INFO

SOURCE IMAGE : h:\jaguar-xf-on-road (1).jpg Browse...

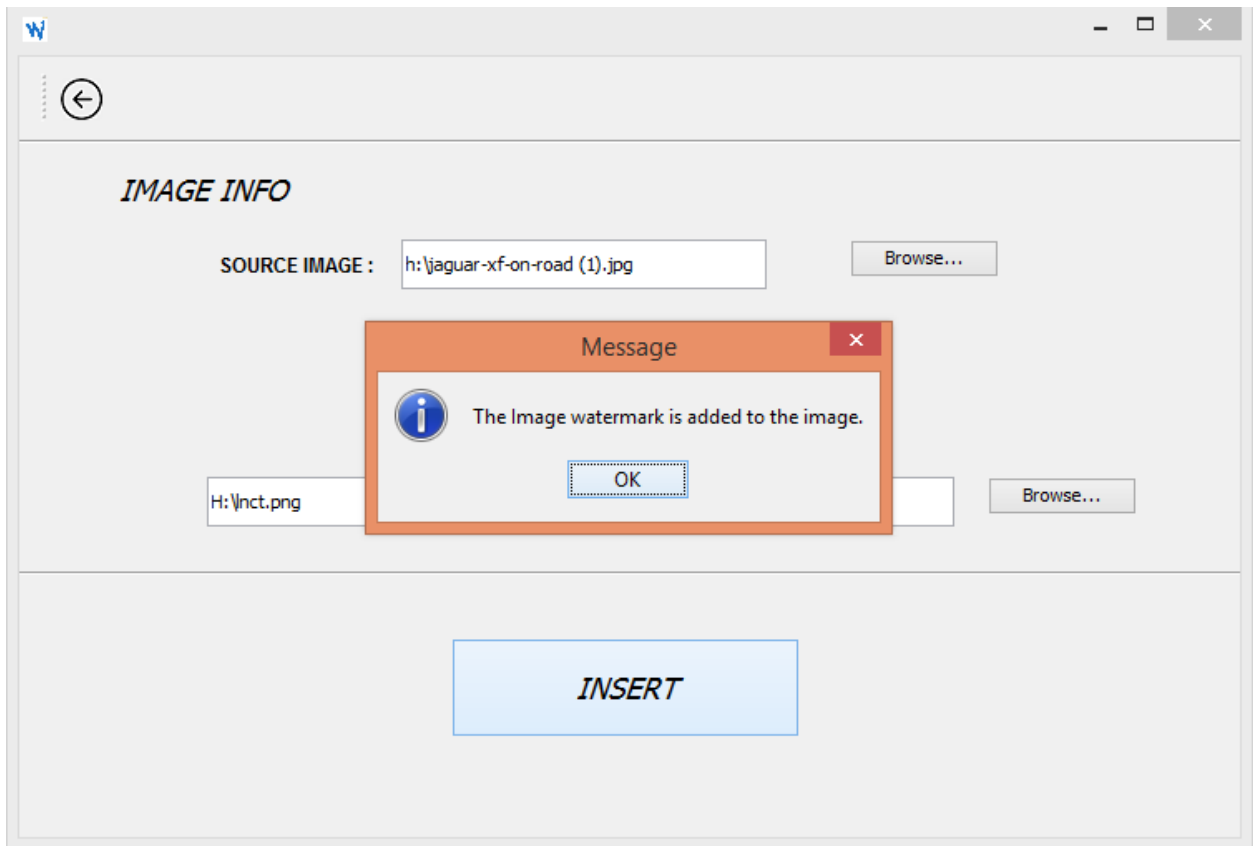
WATERMARK TEXT / IMAGE

☐ Text ☒ Image

H:\hct.png Browse...

INSERT

CONFIRMATION MESSAGE



ORIGINAL IMAGE WITH WATERMARKED IMAGE



CHAPTER 10

CONCLUSION

10.1 Conclusion

Watermark is a message which is embedded into digital content (,images or text) that can be detected or extracted later. Such messages mostly carry copyright information of the content. Watermarking has been revealed to be an efficient technique to cope with the problem of intellectual property rights (IPR) protection of multimedia data. This technology embeds into the data an unperceivable digital code, namely the watermark, carrying information about the copyright status of the work to be protected.

10.2 Limitation of the project:

1. If any one makes changes in Watermark file then it security is lost.
2. The application cannot embed message in text file. If it tries to embed message in text file then it will show distorted text file.
3. Only text file can be embedded in image file. No other files can be embedded.
4. The message cannot be transferred to any other device such as mobile.
5. The message can be transferred in intranet environment and not in Internet environment.

10.3 Future Enhancement:

1. The application can have multiple login id and password.
2. Security will not lose by any mean.
3. The application can embed message in text file.
4. Not only text file but also any other file can be embedded in image, audio and video file.
5. The message can be transferred in intranet and in Internet environment.
6. The message can be transferred to any other device such as mobile.
7. The content of the file can be seen in the text area provided for displaying the messages.

References:

- [1] G. Rafael, C. Gonzalez and R. E. Woods, "Digital Image Processing", Third Edition, (2008).
- [2] N. Tiwari, M. k. Ramaiya and Monika Sharma, "Digital watermarking using DWT and DES", IEEE (2013).
- [3] D. Zhang, S. Xu, Y. Wang, J. Zhang and Y. Li, "A Digital Fingerprinting Scheme of Digital Image", International Conference on Computational Intelligence and Software Engineering (CISE) (2010).
- [4] S. Emmanuel, A. P. Vinod, D. Rajan and C.K. Heng, "An Authentication Watermarking Scheme with Transaction Tracking Enabled", Digital Ecosystem and Technologies Conference, 2007. DEST 07 Inaugural IEEE-IES.
- [5] L. Robert and T. Shanmugapriya, "A Study on Digital Watermarking Techniques", International Journal of Recent Trends in Engineering, vol. 1, no. 2, (2009) May.