A

PROJECT Report

on

File Camouflage

Submitted for partial fulfilment of award of

BACHELOR OF TECHNOLOGY

Degree

In

Information Technology

By

STUDENTS

Nikhil Saini -1900300130064

Naveen Kumar Varshney-1900300130063

Md Sadique Rashid-1900300130057

Arun Kumar-1900300130018

Under the Supervision of

Ms. Jasneet Kaur

INDERPRASTHA ENGINEERING COLLEGE, GHAZIABAD,

Dr. A P J ABDUL KALAM TECHNICAL UNIVERSITY

LUCKNOW, UTTAR PRADESH

(SESSION:2022-23)

Certificate

This is to certify that the Project Report entitled "…… File Camouflauge....." which is submitted by Naveen Kumar Varshney, Nikhil Saini, Arun Kumar, Md Sadique Rashid…in partial fulfillment of the requirement for the award of degree B. Tech. in Department of ....Information Technology..... of Dr. A.P.J. Abdul Kalam Technical University, Lucknow, is a record of the candidate's own work carried out by him under my supervision. The matter embodied in this thesis is original and has not been submitted for the award of any other degree.

(Ms. Jasneet kaur)

Designation: Assistant Professor

Date: 22-12-2023

Address: IPEC, Ghaziabad

Acknowledgement

We take this opportunity to thank our teachers and friends who helped us throughout the project.

First and foremost, I would like to thank my guide for the project (**Ms. Jasneet kaur, Assistant professor, Information Technology Department**) for her/his valuable advice and time during development of project.

We would also like to thank **Dr. Pooja Tripathi** (**HOD, Information Technology Department**) for his constant support during the development of the project.

Name: Naveen Kumar Varshney

Roll No. 1900300130063

Signature

Name: Nikhil Saini

Roll No. 1900300130064

Signature

Name: Md Sadique Rashid

Roll No. 1900300130057

Signature

Name: Arun Kumar

Roll No. 1900300130018

Signature

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text.

Name: Naveen Kumar Varshney
Roll No. 1900300130063
Signature

Name: Nikhil Saini
Roll No. 1900300130064
Signature

Name: Md Sadique Rashid
Roll No. 1900300130057
Signature

Name: Arun Kumar
Roll No. 1900300130018
Signature

Abstract

The word steganography means" covered in hidden writing". The object of steganography is to send a message through some innocuous carrier (to a receiver while preventing anyone else from knowing that a message is being sent to all. Computer based steganography allows changes to be made to what are known as digital carriers such as images or sounds.

The changes represent the hidden message, but result if successful in no discernible change to the carrier. The information may be nothing to do with the carrier sound or image or it might be information about the carrier such as the author or a digital watermarking or fingerprint.

In steganography information can be hidden in carriers such as images, audio files, text files, and video and data transmissions. When message is hidden in the carrier a stego carrier is formed for example a stego-image. Hopefully it will be perceived to be as close as possible to the original carrier or cover image by the human senses.

Images are the most widespread carrier medium. The are used for steganography in the following way. The message may firstly be encrypted. They are used for steganography in the following way. The message may firstly be encrypted. The sender embeds the secret message to be sent into a graphic file. This results in the production of what is called stego-image. Additional secret data may be needed in the hiding process e.g. a stegokey etc. This stego-image is then transmitted to the recipient.

KEYWORDS:

Stegnography, Images, Hiding, Web application, Online, Text Files, Message, Encryption, Extraction.

Role and Responsibility:

The growing use of the Internet has led to a continuous increase in the amount of data that is being exchanged and storage in various digital media. This has led to some unexpected cases involving both benevolent and malevolent usage of digital data.

With the ever increasing amount and variety of data to be stored and transmitted in various mediums, the specification of security which has to be established at various levels of medium access and the accompanying issues of authentication and authorization has become a critical factor.

Various stenographic, watermarking and data-embedding algorithms have usually manipulated the actual data in order to either hide any coveted information or to provide some level of access control over the medium. The mediums are usually images, video, audio etc., wherein specific portions or the overall space is usually ‗corrupted' with ‗significant' data. This paper is an attempt to bring out the significance of the steganographic techniques that are employed in information processing algorithms for data security. It deals with the problem of data security, focusing mainly on images, and tries to state the various properties and characteristics that the steganographic algorithms should possess.

Scope: This Application is used to secure online privacy—the method of securing secret information in carriers such as a video, audio, digital image, text .

TABLE OF CONTENTS

Table of Figures

INTRODUCTION

INTRODUCTION

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data.

1.1 Background

The term steganography refers to a technique that aims to hide communication between two interlocutors**.** The term is composed precisely of the Greek words στεγανός (covered) and γραφία (writing). Unlike encryption, which allows you to encrypt a message so as to make it incomprehensible if you do not have a key to decipher it, steganography aims to keep the very existence of the message away from prying eyes**,** by hiding it.

Traces of steganography already existed in ancient Greece, when Herodotus narrated two examples in his Stories, but the first recorded use of the term was in 1499 by Johannes Trithemius in his *Steganographia,* a treatise on cryptography and steganography, disguised as a book about magic. Initially the author decided not to print it and even destroyed large parts of it, believing that they should never have seen the light of day, but the text continued to circulate in the form of a provisional draft and was published posthumously in 1606.

Since then, many throughout history have used this technique to deliver messages safely. For example, it is known that during both world wars, female spies used knitting to send messages, perhaps making an irregular stitch or leaving an intentional hole in the fabric.

1.2 Objective

In this project we primarily concentrated on the data security issues when sending the data over the network using steganographic techniques. The main objectives of our project are to product security tool based on steganography techniques to hider message carried by stego-media which should not be sensible to human beings and avoid drawing suspicion to the existence of hidden message.

1.3 Purpose, Scope and Applicability

Purpose

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination.

Scope

Our project scope is developed for hiding information in any image file to ensure the safety of exchange the data between different parties and provide better security during message transmission.

Applicability

This application can be used for data hiding purpose in government sector, sports, education, IT industry etc.

1.4 Achievement

The benefit after completing this project is we can hide data inside an image and it can be shared to any organisation as well as any person, while maintaining the confidentiality.

SURVEY OF THE TECHNOLOGY

LITERATURE SURVEY

Now we will provide an overview of steganography using LSB to hide the files inside images using the JavaScript technical computing language, it is development environment is used in a variety of domains, such as image and signal processing, C# offers many "toolboxes", and a simple interface to high-performance libraries, one of the most advantages is a large user community with lots of free code and knowledge sharing and the ability to process both still images and video. It is popular because of its ease and simplicity. Also, we will mention some programs that have the same approach it is using an encryption. Then, we will give the recommendation that help to develop our program. In this project, use a method of encrypting any data file in an image file. This process of hiding the data helps to sharing the information with others over the internet network without any potential risk. The proposed system will help to hide the content within the image and encryption of data file within the image will help to make the document much securer. In this research, developed the proposed system by using steganographic algorithm which is LSB and a technique for hiding capacity and efficiency of hiding the message within an image.

Existing System:

White Noise Storm is a DOS based tool that could easily embed secret messages in cover images without any degradation. However, the integrity of the cover image could be severely affected by noise. The tool uses LSB steganography technique to embed secret messages in PCX files. The main disadvantage of this tool is the loss of many bits that can be used to hold information. Additionally, it uses large cover images to store information that it could be stored in a smaller cover image using other tools.

Proposed System:

After studying similar tools to our proposed system LSB substitution is used to embed the message into an image. It works by adjusting the LSB of the carrier image's pixels whereas, the last bit of each byte in the image is changed to a bit of the secret message that is known standard LSB (1-LSB). Also, use 2-LSB method that differs from the standard LSB method by allowing more data to be hidden into the cover image. The idea of this method is almost like the standard LSB, except that it replaces the

Functions and features will be followed as:

- For user interfaces we take in consideration that they should has a standard look and being user friendly at the same time to make sure that users' attention will not be distracted and interface to provide more flexibility and scalability.
- The program will be in the English language
- The program must be fast in processing
- The program must hide the image within the image and then extract image from the image properly.
- All function must be works well then system will be a high quality.

[1]: G. Prashanti and K. Sandhyarani have done survey on recent achievements of LSB based image steganography. In this survey authors discuss the improvements that enhance the steganographic results such as high robustness, high embedding capacity and un-detectability of hidden information. Along with this survey two new techniques are also proposed. First technique is used to embed data or secret messages into the cover image and in the second technique a secret gray scale image is embedded into another gray scale image. These techniques use four state table that produce pseudo random numbers. This is used for embedding the secret information. These two methods have greater security because secret information is hidden on random selected locations of LSBs of the image with the help of pseudo random numbers generated by the table.

[2]: Savita Goel et al. in proposed a new method of embedding secret messages in cover image using LSB method using different progressions. Authors compare the quality of stego image with respect to cover image using number of image quality parameters such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), histograms and CPU time, Structure Similarity (SSIM) index and Feature Similarity Index Measure (FSIM). Their study and experimental results shows that their proposed method is fast and highly efficient as compared to basic LSB methods.

[3]: Della Baby et al. proposed a "Novel DWT based Image Securing method using Steganography". In their work new steganography technique is prosed in which multiple RGB images are embedded into single RGB image using DWT steganographic technique. The cover image is divided into 3 colors i.e. Red, Green and Blue color space. These three color spaces are utilized to hide secret information. Experimental results obtained using 2 this system has good robustness.

Value of PSNR and SSIM index have been used by authors to compare the quality of stego image and original cover image. Proposed method has good level of PSNR and SSIM index values. Authors have found that their experimental results are better than existing approaches and have increased embedding capacity because of data compression. So overall security of their approach is high with less perceptible changes in stego image.

[4]: Bingwen Feng, Wei Lu, and Wei Sun in their paper "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture" purposed a stateof-the-art approach of binary image steganography. This technique is proposed to minimize the distortion on the texture. In this method of steganography firstly the rotation, complement and mirroring invariant texture patterns are extracted from the binary image. They also proposed a measurement and based on this proposed measurement this approach is practically implemented. Practical results show that proposed steganographic approach has high statistical security with high stego image quality and high embedding capacity.

[5]: M. Nusrati et al. have done study on heuristic genetic algorithm based steganographic method for hiding secret information in a cover image. This method optimally find the appropriate locations in cover image to embed the secret information by focusing on the "before embedding hiding techniques". It tries to make least changes in the bits which lead to minimal modifications in image histogram. To covert the LSBs and secret message to set of blocks, segmentation is done in this genetic algorithm. After this algorithm finds the appropriate locations for embedding, the secret blocks are embedded and it generates the key file which is used during message extraction process. Experimental results show that this genetic based method is more efficient than basic LSB algorithm with high stego image quality.

[6]: Kazem Qazanfari and Reza Safabakhsh proposed an improved version of LSB++ approach. In this improved LSB++ they make distinction between sensitive pixels and allow protecting them from embedding of extra bits, which results in lower distortion in the cooccurrence matrices. They also extend this method to preserve DCT coefficients of JPEG 3 format images. This improved method results in fewer traces in the co-occurrence matrices then old LSB++ technique. This method is also secure against histogram based attacks because this method does not make any changes in the histogram and hence histograms of both cover image as well as stego image will be same. The quality of stego images is also high because of elimination of extra bit embedding.

[7]: On the based on Huffman Coding, Amitava Nag et al. present a novel steganographic technique of LSB substitution. Their technique basically focuses on high security, larger embedding capacity and acceptable level of stego image quality. Firstly Huffman tree is produced to encode every 8 bits of secret image. After encoding, they divide the encoded bits into four parts and have 0 to 3 decimal values. Location of embedding a message in cover image is determined by these decimal values. Experimental results show that it is very difficult for attacker to extract the secret information because Huffman table decrease the size of the cover image. Purposed techniques just have acceptable level of PSNR values and lie between 30 dB to 31 dB.

[8]: N. Akhtar et al. in present and implement the improved version of traditional LSB image steganography technique. Their work enhances the quality of stego image using bit inversion method. They propose and implement two approaches of bit inversion techniques. These both techniques resolves around bit inversion techniques in which LSBs of pixels of carrier image are inverted only and only if they arise with specific pattern of pixel's bits. This leads to lesser modification in pixels is compared to traditional LSB method. For correct retrieval of secret message, inverted bits need to be embedded somewhere within

the stego image. Experimental results demonstrate that PSNR value of stego image is improved; hence stego image quality is improved.

[9]: P. U. Deshmuk et al. also present the edge adaptive steganography based on LSB substitution. They embed secret information in sharp (edges) regions of the carrier image using adaptive scheme and difference between two adjacent pixels of carrier image. Their technique performs well than other LSB and Pixel difference based techniques and maintains the quality of stego image.

[10]: E. Dagar and S. Dagar present the steganography technique for color RGB images to improve the security level of data transfer through the internet. 24 bit RGB image is utilized as cover image to embed secret data in red, green and blue pixels. X-Box mapping is used and several boxes contain 16 different values. Here "X" represent any integer number from 0 to 9. After this values saved in X-Boxes are mapped with LSBs of carrier image. It is very difficult for the attacker to extract the secret information because they make use of mapping. Thus this mapping provides high level of security to hidden information. PSNR value is also calculated and it has high PSNR value which leads to greater stego image quality.

REQUIREMENT AND ANALYSIS

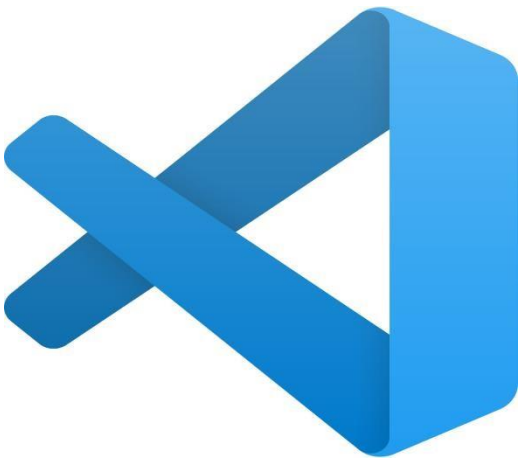
Requirement and Analysis

Problem definition

In this section, we define problems. The problem is that, when elections are to be conducted, lot of money, physical space, man power is required. And there are so many people who are qualified for voting like old ones, but due to age factor or medical illness they are not able to visit voting venue. Another problem is that, voting machine could be manipulated by some bad people which can result in fake voting or one sided voting.

Applications requirements

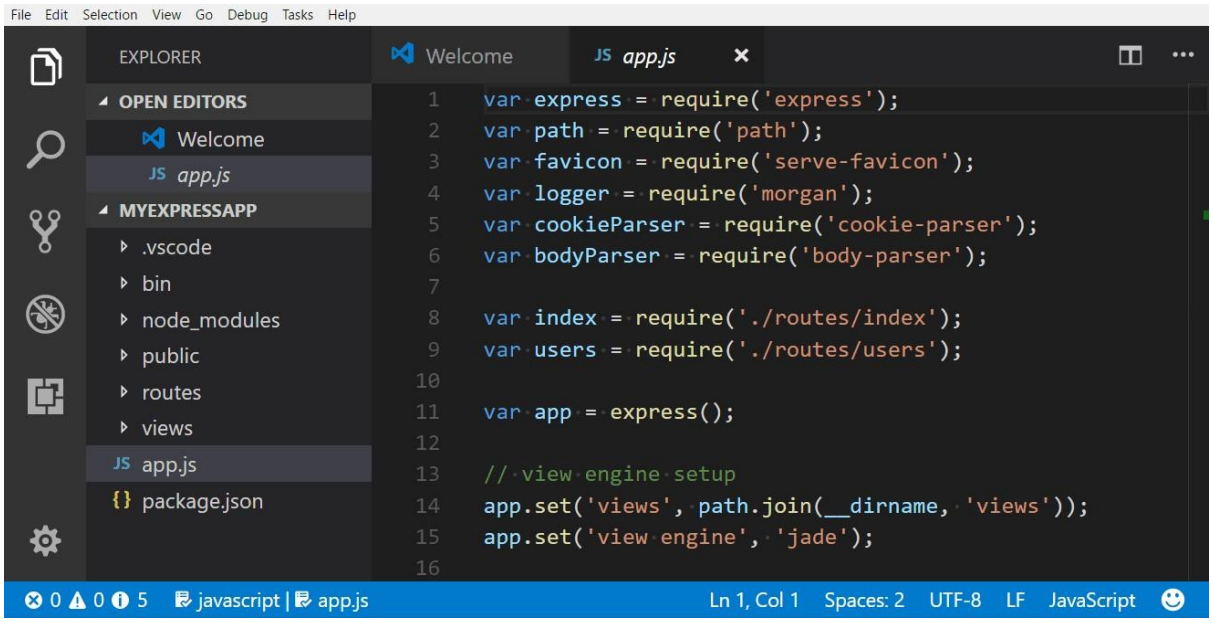
Visual Studio Code



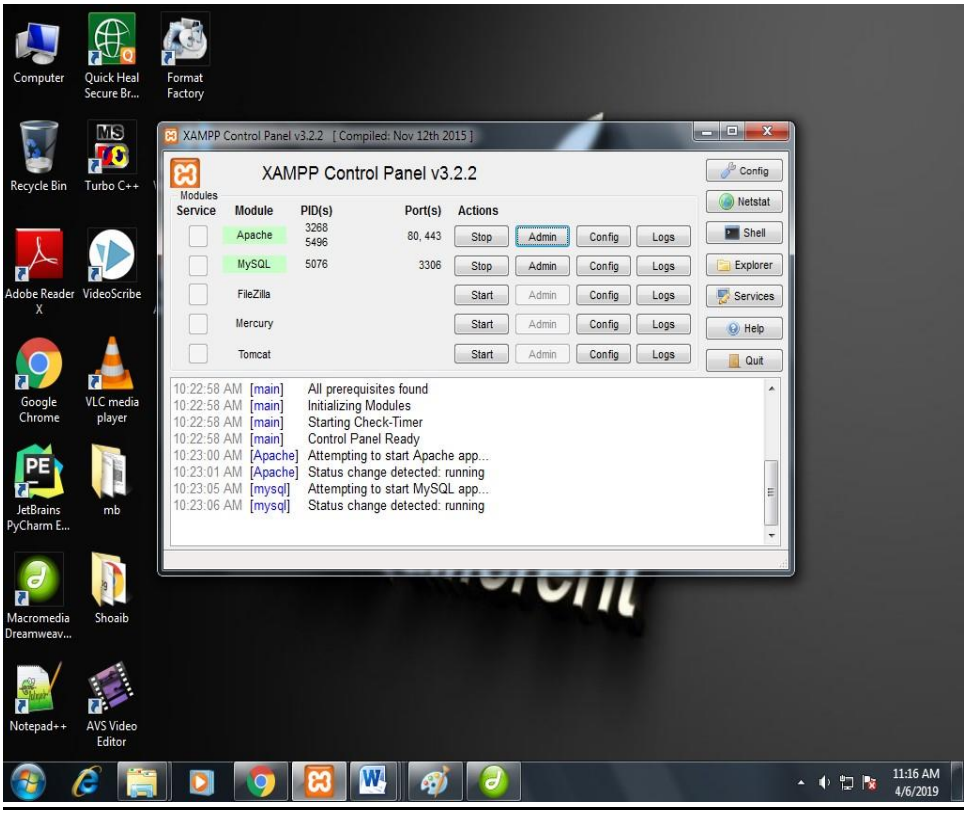
Visual Studio Code is an integrated development environment made by Microsoft for Windows, Linux and macOS. Features include support for debugging, syntax highlighting, intelligent code completion, snippets, code refactoring, and embedded Git. Users can change the theme, keyboard shortcuts, preferences, and install extensions that add

additional functionality. Microsoft has released most of Visual Studio Code's source code on GitHub under the permissive MIT License, while the releases by Microsoft are proprietary freeware.

In the Stack Overflow 2021 Developer Survey, Visual Studio Code was ranked the most popular developer environment tool, with 70% of 82,000 respondents reporting that they use it. Visual Studio Code was first announced on April 29, 2015, by Microsoft at the 2015 Build conference. A preview build was released shortly thereafter. On November 18, 2015, the source of Visual Studio Code was released under the MIT License, and made available on GitHub.
Extension support was also announced.[13] On April 14, 2016, Visual Studio Code graduated from the public preview stage and was released to the Web.



XAMPP



The full form of XAMPP is X stands for Cross-platform, (A) Apache server, (M) MariaDB, (P) PHP and (P) Perl. XAMPP is open source free software developed by Apache friends. XAMPP software package contains Apache distributions for Apache server, MariaDB, PHP, and Perl. And it is basically a local host or a local server. This local server works on your own desktop or laptop computer. You can just install this software on your laptop or desktop and test the clients or your website before uploading it to the remote web server or computer. This XAMPP server software gives you suitable environment for testing MYSQL, PHP, Apache and Perl projects on the local computer.

The Cross-platform usually means that it can run on any computer with any operating system. Next MariaDB is the most famous

database server and it is developed by MYSQL team. PHP usually provides a space for web development. PHP is a server-side scripting language. And the last Perl is a programming language and is used to develop a web application.

What are the Main Tools of XAMPP and its definition?

XAMPP contains tools such as Apache, MYSQL, PHP, and Perl. We will see these tools.

Apache

Apache server is an open source free software which is initially developed by a group of software developers and now it is maintained by Apache software foundation. Apache HTTP is a remote server(computer) if someone request files, images or documents using their browser they will serve those files to clients using HTTP servers. Mainly hosting companies use this application to create a VPS server and shared hosting for their clients.

MYSQL

MYSQL is an open source software. It is actually a relational database management system(RDBMS). This SQL stands for Structured Query Language.It is the most popular and best RDBMS used for developing a variety of web-based software applications. With the help of MYSQL, it is possible to organize the information, manage, retrieve and update the data whenever you wish to do.

PHP

The full form of PHP is Hypertext Preprocessor. It is a server-side scripting language that helps you to create dynamic websites. This language is mainly used to build web-based software applications. It is an open source software and works fine with MYSQL. What actually happens is, the PHP code will be executed on the server and at the browser side its HTML code will be displayed.

Perl

Perl is usually said to be general purpose programming language. This Perl language is interpreted and highly dynamic. Actually, this language is used for web development, GUI development, system administration etc. Perl is capable of working with HTML, XML and other markup languages.

In the latest version of XAMPP, there are additional tools such as Mail server Mercury, OpenSSL, phpMyAdmin etc. With the above tools, you can create a full-fledged desktop server.

Programming technology requirements

HTML

- HTML (HyperText Markup Language) is the most basic building block of the Web. It defines the meaning and structure of web content. Other technologies besides HTML are generally used to describe a web page's appearance/presentation (CSS) or functionality/behavior (JavaScript).
- "Hypertext" refers to links that connect web pages to one another, either within a single website or between websites. Links are a fundamental aspect of the Web. By uploading content to the Internet and linking it to pages created by other people, you become an active participant in the World Wide Web.

- HTML uses "markup" to annotate text, images, and other content for display in a Web browser. HTML markup includes special "elements" such as <head>, <title>, <body>, <header>, <footer>, <article>, <secti on>, <p>, , , <img>, <aside>, <audio>, <canvas>, <da talist>, <details>, <embed>, <nav>, <output>, <progress>, <vide o>, <ul>, <ol>, <li> and many others.

- An HTML element is set off from other text in a document by "tags", which consist of the element name surrounded by "<" and ">". The name of an element inside a tag is case insensitive. That is, it can be written in uppercase, lowercase, or a mixture. For example, the <title> tag can be written as <Title>, <TITLE>, or in any other way.

CSS

- Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation of a document written in a markup language such as HTML.[1] CSS is a cornerstone technology of the World Wide Web, alongside HTML and JavaScript.[2]
- CSS is designed to enable the separation of presentation and content, including layout, colors, and fonts.[3] This separation can improve content accessibility, provide more flexibility and control in the specification of presentation characteristics, enable multiple web pages to share formatting by specifying the relevant CSS in a separate .css file which reduces complexity and repetition in the structural content as well as enabling the .css file to be cached to improve the page load speed between the pages that share the file and its formatting.
- Separation of formatting and content also makes it feasible to present the same markup page in different styles for different rendering methods, such as on-screen, in print, by voice (via speech-based browser or screen reader), and on Braille-based tactile devices. CSS also has rules for alternate formatting if the content is accessed on a mobile device.[4]
- The name cascading comes from the specified priority scheme to determine which style rule applies if more than one rule matches a particular element. This cascading priority scheme is predictable.

- The CSS specifications are maintained by the World Wide Web Consortium (W3C). Internet media type (MIME type) is registered for use with CSS by RFC 2318 (March 1998). The W3C operates a free CSS validation service for CSS documents.[5] `text/css`
- In addition to HTML, other markup languages support the use of CSS including XHTML, plain XML, SVG, and XUL.

JavaScript

- JavaScript (/ˈdʒɑːvəˌskrɪpt/),[6] often abbreviated as JS, is a programming language that conforms to the ECMAScript specification.[7] JavaScript is high-level, often just-in-time compiled, and multi-paradigm. It has curlybracket syntax, dynamic typing, prototype-based objectorientation, and first-class functions.
- Alongside HTML and CSS, JavaScript is one of the core technologies of the World Wide Web.[8] JavaScript enables interactive web pages and is an essential part of web applications. The vast majority of websites use it for clientside page behavior,[9] and all major web browsers have a dedicated JavaScript engine to execute it.
- As a multi-paradigm language, JavaScript supports eventdriven, functional, and imperative programming styles. It has application programming interfaces (APIs) for working with text, dates, regular expressions, standard data structures, and the Document Object Model (DOM). However, the language itself does not include any input/output (I/O), such as networking, storage, or graphics facilities, as the host environment (usually a web browser) provides those APIs.
- JavaScript engines were originally used only in web browsers, but they are now embedded in some servers, usually

via Node.js. They are also embedded in a variety of applications created with frameworks such as Electron and Cordova.

- Although there are similarities between JavaScript and Java, including language name, syntax, and respective standard libraries, the two languages are distinct and differ greatly in design.

JavaScript Advantages

Following are the advantages of JavaScript −

- **Simple** − JavaScript is simple to comprehend and pick up. Both users and developers will find the structure to be straightforward. Additionally, it is very doable to implement, saving web developers a tonne of money when creating dynamic content.
- **Speed** − JavaScript is a "interpreted" language, it cuts down on the time needed for compilation in other programming languages like Java. Another client-side script is JavaScript, which accelerates programme execution by eliminating the wait time for server connections.
  No matter where JavaScript is hosted, it is always run in a client environment to reduce bandwidth usage and speed up execution.
- **Interoperability** − Because JavaScript seamlessly integrates with other programming languages, many developers favour using it to create a variety of applications. Any webpage or the script of another programming language can contain it.
- **Server Load** − Data validation can be done within the browser itself rather than being forwarded to the server because JavaScript is client-side. The entire website does not need to be reloaded in the event of any discrepancy. Only the chosen area of the page is updated by the browser.

How does JavaScript work?

JavaScript is what is known as a client-side script. Most Web applications, such as a search engine, work because of an interaction between the user's device (e.g. computer, phone or tablet) and a remote server. The software on the remote server sends information to the client (i.e. the user's machine) and the software on the client side reads the information and renders a Web page on screen.

A client-side script is a programming language that performs its tasks entirely on the client's machine and does not need to interact with the server to function. For instance, if you have a Web page loaded on your computer and your Internet service provider goes down, you are still able to interact with the Web pages already loaded on your browser. You will not, however, be able to navigate to new Web pages or access any data located remotely.

Some of the dynamic website enhancements performed by JavaScript are:

- Autocomplete
- Loading new content or data onto the page without reloading the page
- Rollover effects and dropdown menus
- Animating page elements such as fading, resizing or relocating
- Playing audio and video
- Validating input from Web forms
- Repairing browser compatibility issues

While JavaScript is a client-side language, some of its most powerful features involve asynchronous interaction with a remote server. Asynchronous simply means that JavaScript is able to communicate with the server in the background without interrupting the user interaction taking place in the foreground.

Take a search engine for example. Today, search engines almost all have an autocomplete function. The user begins typing a word into the

search box and a list of possible search terms or phrases appears below. The experience is seamless. Suggested search terms appear without reloading the page.

In the background, JavaScript reads the letters as the user types, sends those letters to a remote server and the server sends suggestions back.

The software on the server side analyzes the words and runs algorithms to anticipate the user's search term. Such programs are diabolically large and complex. The JavaScript on the client's machine is as simple and small as possible so as not to slow down the user's interaction. The communication between JavaScript and the server-side program is limited by the user's bandwidth. This is why developers prioritize efficiency in JavaScript functions and make the amount of data communicated between the programs as small as possible.

Only once the user selects a search term does the entire page reload and produce the search results. Engines such as Google have reduced or eliminated the need to reload, even for that step. They simply produce results using the same asynchronous process.

Bootstrap

- Bootstrap is a free and open-source CSS framework directed at responsive, mobile-first front-end web development. It contains CSS- and (optionally) JavaScript-based design templates for typography, forms, buttons, navigation, and other interface components.

- Bootstrap is a web framework that focuses on simplifying the development of informative web pages (as opposed to web apps). The primary purpose of adding it to a web project is to apply Bootstrap's choices of color, size, font and layout to that project.

As such, the primary factor is whether the developers in charge find those choices to their liking. Once added to a project, Bootstrap provides basic style definitions for all HTML elements. The result is a uniform appearance for prose, tables and form elements across web browsers. In addition, developers can take advantage of CSS classes defined in Bootstrap to further customize the appearance of their contents. For example, Bootstrap has provisioned for light- and dark-colored tables, page headings, more prominent pull quotes, and text with a highlight.

- Bootstrap also comes with several JavaScript components in the form of jQuery plugins. They provide additional user interface elements such as dialog boxes, tooltips, and carousels. Each Bootstrap component consists of an HTML structure, CSS declarations, and in some cases accompanying JavaScript code. They also extend the functionality of some existing interface elements, including for example an auto-complete function for input fields.

- Example of a webpage using Bootstrap framework rendered in Firefox

- The most prominent components of Bootstrap are its layout components, as they affect an entire web page. The basic layout component is called "Container", as every other element in the page is placed in it. Developers can choose between a fixedwidth container and a fluid-width container. While the latter always fills the width of the web page, the former uses one of the four predefined fixed widths, depending on the size of the screen showing the page:

- Smaller than 576 pixels
- 576–768 pixels
- 768–992 pixels
- 992–1200 pixels

- Larger than 1200 pixels
- Once a container is in place, other Bootstrap layout components implement a CSS Flexbox layout through defining rows and columns.
- A precompiled version of Bootstrap is available in the form of one CSS file and three JavaScript files that can be readily added to any project. The raw form of Bootstrap, however, enables developers to implement further customization and size optimizations. This raw form is modular, meaning that the developer can remove unneeded components, apply a theme and modify the uncompiled Sass files.

System minimum requirements

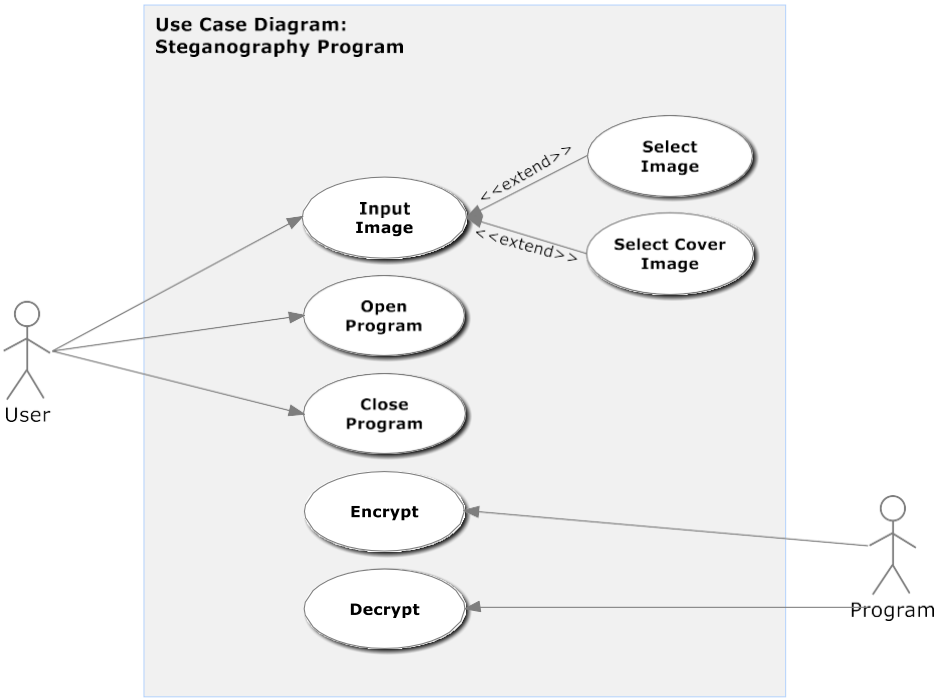
Hardware System Configuration:-

- Processor - Dual Core/ Pentium/ i3 Intel Processor
- RAM - 2 GB
- Hard Disk - 512MB
- Keyboard - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse • Monitor - Any

Software System Configuration: -

- Operating System - Windows XP/7/8/10/11
- Server-side Script - JavaScript

General Use Case Diagram



Actors

An actor in the Unified Modeling Language (UML) "specifies a role played by a user or any other system that interacts with the subject." "An Actor models a type of roleplayed by an entity that interacts with the subject (e.g., by exchanging signals and data), but which is external to the subject."

There are two actors in our application:

1. User
2. Program

A use case is a set of scenarios that describing an interaction between a user and asystem. A use case diagram displays the relationship among actors and use cases.

SYSTEM DESIGN

SYSTEM DESIGN

INTRODUCTION

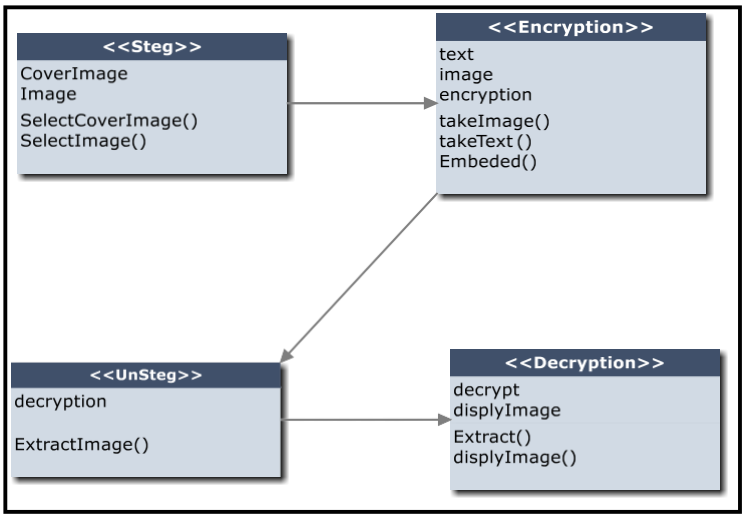
Software design is a process of problem-solving and planning for a softwaresolution. After the purpose and specifications of software is determined, software developers will design or employ designers to develop a plan for a solution. It includes construction component and algorithm implementation issues which shown in as thearchitectural view. During this chapter we will introduce some principles that areconsidered through the Software design.

STRUCTURAL VIEW

Structural diagrams are used to describe the relationships between classes. Structuralview can be described using class diagram.

Class Diagram

A class diagram is a picture for describing generic descriptions of possible systems.Class diagrams and collaboration diagrams are alternate representations of object models. Class diagrams contain classes and object diagrams contain objects, but it is possible to mix classes and objects when dealing with various kinds of metadata, so the separation is not rigid.



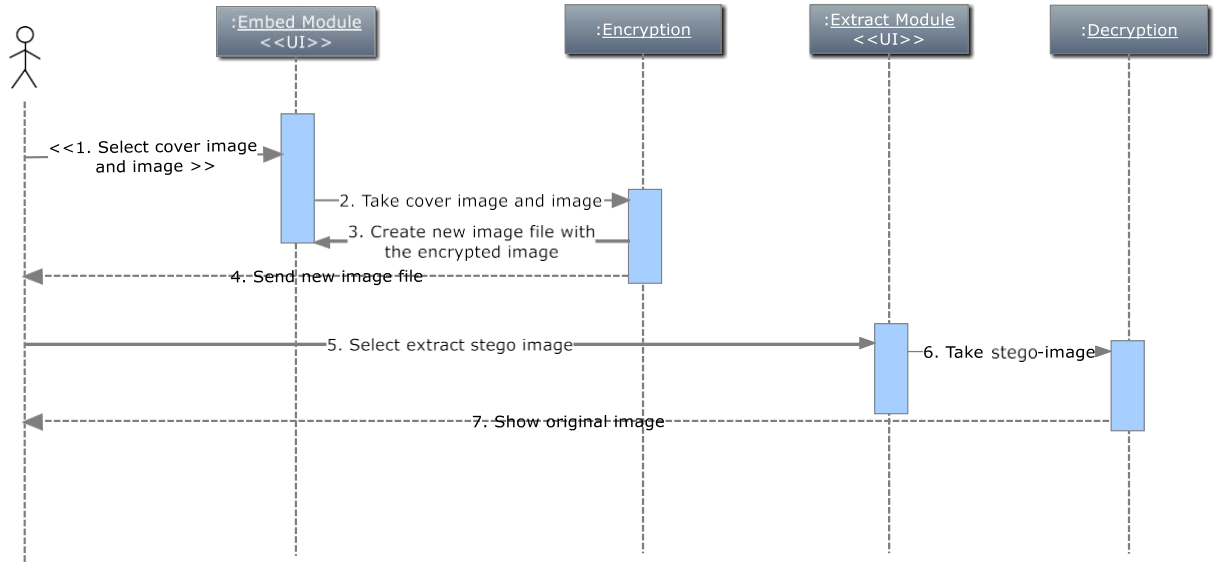
Class diagrams are more prevalent than object diagrams. Normally you will build class diagrams plus occasional object diagrams illustrating complicated data structures or message-passing structures.

BEHAVIORAL VIEW

As we mentioned previously that activity diagram, and sequence diagram provide the behavioral view for our project. Behavioral diagrams are used to describe the interaction between the actors and the system. All the activities that are performed by the actors and the system are introduced in some way.

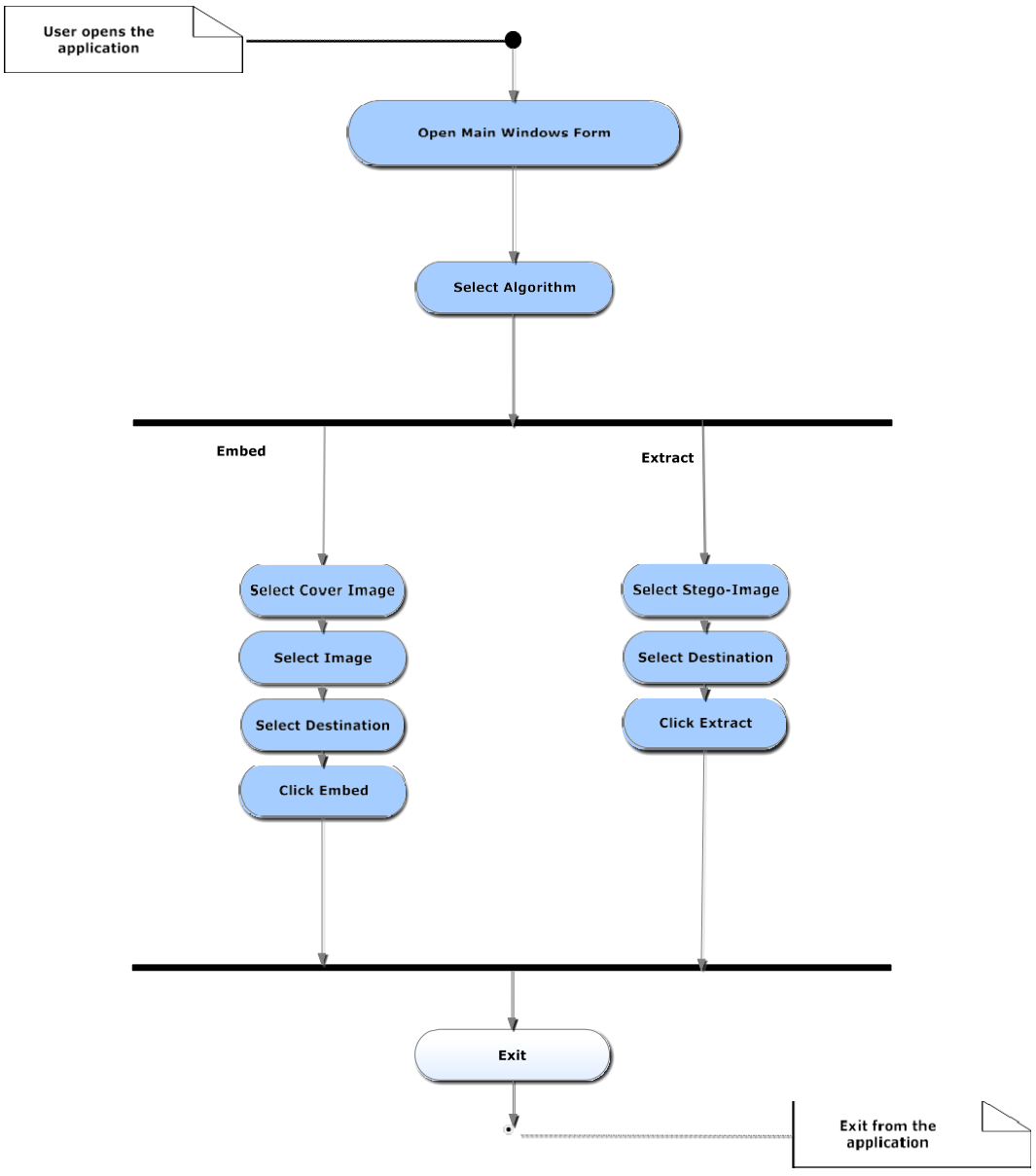
Sequence Diagram

A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario.



Activity Diagram

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modelling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of processes.



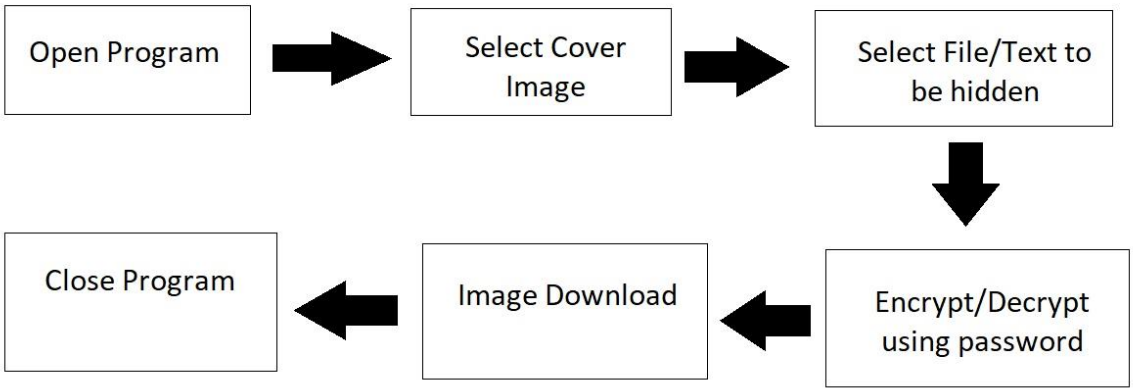
Data Flow Diagram

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system, modeling its process aspects. Often they are a preliminary step used to create an overview of the system which can later be elaborated. DFDs can also be used for the visualization of data processing (structured design).

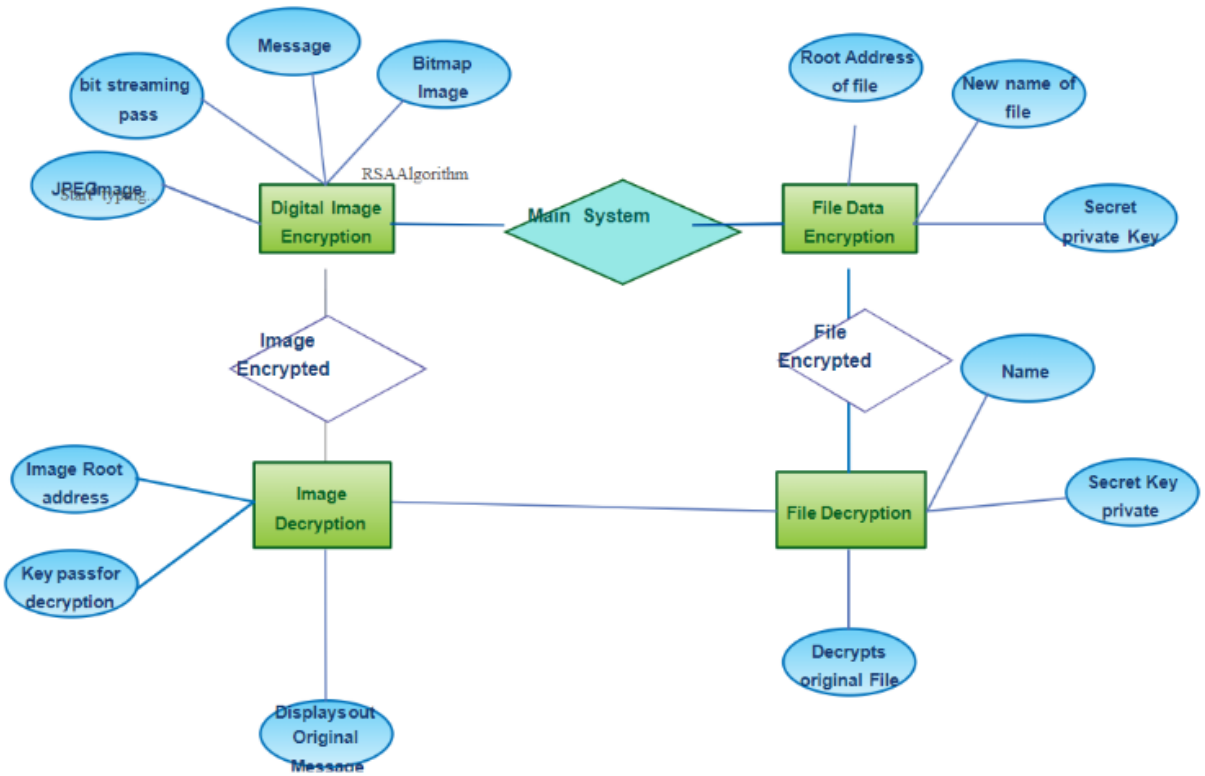
A DFD shows what kinds of information will be input to and output from the system, where the data will come from and go to, and where the data will be stored.

It does not show information about the timing of processes, or information about whether processes will operate in sequence or in parallel.

Flow Chart


Open Program
Select Cover Image
Select File/Text to be hidden
Encrypt/Decrypt using password
Image Download
Close Program

ER Diagram


Message
bit streaming pass
Bitmap Image
JPEGmage
RSAAlgorithm
Digital Image Encryption
Main System
Root Address of file
New name of file
File Data Encryption
Secret private Key
Image Encrypted
File Encrypted
Name
Image Root address
Key passfor decryption
Image Decryption
File Decryption
Secret Key private
Decrypts original File
Displays out Original Message

APPLICATIONS

APPLICATIONS

This system is applicable in below fields for data hiding purpose:

➢ School ➢ College ➢ Industry ➢ Corporate ➢ Government ➢ Hospital ➢ Food and Restaurant ➢ Tourism ➢ Sports ➢ Entertainment ➢ Production ➢ Investment ➢ News and Media ➢ Technology ➢ Army ➢ Intelligence Department

CONCLUSIONS

Conclusion and Future work

Conclusion

Although only some of the main image steganographic techniques were discussed in this document, one can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness. For example, the patchwork approach has a very high level of robustness against most type of attacks, but can hide only a very small amount of information.
Least significant bit (LSB) in both BMP and GIF makes up for this, but both approaches result in suspicious files that increase the probability of detection when in the presence of a warden.
The proposed approach in this project uses a new steganographic approach called image steganography. The application creates a stego image in which the personal data is embedded inside the cover file image.

Used the Least Significant Bit algorithm in this project for developing the application which is faster and reliable and compression ratio is moderate compared to other algorithms.

Limitations of the system

The major limitation of the application is designed for images cover files. It accepts only images as a carrier file.

Future enhancements

The future work on this project is to improve the compression ratio of the image to the text. This project can be extended to a level such that it can be used for the different types of multimedia files.

REFERENCES

Programming languages

- https://www.w3schools.com
- https://www.javapoint.com
- https://www.youtube.com
- https://www.wikipedia.com

[1] G. Prashanti, K. Sandhyarani, "A New Approach for Data Hiding with LSB Steganography", Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI, Springer 2015, pp. 423- 430.

[2] S. Goel, S. Gupta, N. Kaushik, "Image Steganography – Least Significant Bit with Multiple Progressions", Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), Springer 2014-2015, pp. 105-112.

[3] D. Baby, J. Thomas, G. Augustine, E. George, N.R. Michael, " A Novel DWT based Image Securing method using Steganography", International Conference on Information and Communication Technologies (ICICT), Procedia Computer Science, April 2015, pp. 612-618.

[4] B. Feng, W. Lu, and W. Sun, "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture", IEEE transactions on Information Forensics and Security, Feb. 2015.

[5] M. Nusrati, A. Hanani and R. Karimi, "Steganography in Image Segments Using Genetic Algorithm", 5th IEEE International Conference on Advanced Computing & Communication Technologies (ACCT), Feb 2015, pp. 102-107.

[6] N. A. Al-Otaibi, and A. A. Gutub, "2-Leyer Security System for Hiding Sensitive Text Data on Personal Computers", Lecture Notes on Information Theory, June 2014, pp. 151-157.
[7] M. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal and M. D. Hossain, "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography", IEEE International Conference on Informatics, Electronics & Vision (ICIEV), May 2014, pp.1-6.
[8] K. Qazanfari and R. Safabakhsh, "A new Steganography Method which Preserves Histogram: Generalization of LSB++", Elsevier International Journal of Information Sciences, Sept. 2014, pp. 90-101. 18
[9] A. Nag, J.P. Singh, S. Biswas, D. Sarkar, and P.P. Sarkar, "A Huffman Code Based Image Steganography Technique", 1st International Conference on Applied Algorithm (ICAA) , Jan. 2014, pp. 257-265.
[10] N. Akhtar, S. Khan and P. Johri, "An Improved Inverted LSB Image Steganography", IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), Feb. 2014, pp. 749-755.
[11] P.U. Deshmukh and T.M. Pattewar, "A Novel Approach for Edge Adaptive Steganography on LSB Insertion Technique" IEEE International Conference on Information Communication and Embedded Systems (ICICES), Feb. 2014, pp. 1-5.
[12] E. Dagar and S. Dagar, "LSB based Image Steganography using X-Box Mapping", IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), Sept. 2014, pp. 351-355.
[13] Youssef Bassil , A Simulation Model for the Waterfall Software Development Life Cycle, 2011 http://arxiv.org/ftp/arxiv/papers/1205/1205.6904.pdf
[14] ANALYSIS MODEL WATERFALL MODEL http://www.scribd.com/doc/87322736/Analysis-Model-Waterfall-Model
[15] Data Flow Diagram Symbols http://www.idi.ntnu.no/~sif8035/pdf/flesn/notation.pdf

[16] Donald S. Le Vie, Jr., Understanding Data Flow Diagrams http://ratandon.mysite.syr.edu/cis453/notes/DFD_over_Flowcharts.pdf