Karnataka Law Society's

GOGTE INSTITUTE OF TECHNOLOGY

Udyambag Belagavi -590008

(An Autonomous Institution under Visvesvaraya Technological University, Belagavi)

(APPROVED BY AICTE, NEW DELHI)

Department of Information Science and Engineering

Course Activity Report

CYBER SECURITY (18IS756)

Submitted in the partial fulfilment for the academic requirement of

Seventh Semester BE

TITLE: **"IMAGE STEGANOGRAPHY"**

Submitted by

SL No.	Batch Members Names	USN
1.	Megha Magadumakar	2GI19IS024
2.	Sanjana Sunadholi	2GI19IS047
3	Shweta Naik	2GI19IS050
4	Tejaswini Naganur	2GI19IS055

Under the guidance of

Prof. R.J.Kadkol

Prof., Dept. of ISE

Academic Year 2022-2023 (Odd semester)

Karnataka Law Society's
GOGTE INSTITUTE OF TECHNOLOGY
Udyambag Belagavi -590008
(An Autonomous Institution under Visvesvaraya Technological University, Belagavi)
(APPROVED BY AICTE, NEW DELHI)

Department of Information Science and Engineering

CERTIFICATE

This is to certify that Megha Magadumakar, Sanjana Sunadholi, Shweta Naik, Tejaswini Naganur bearing **USNs:2GI19IS024, 2GI19IS047, 2GI19IS050, 2GI19IS055** has satisfactorily completed the course project in Cyber Security. It can be considered as a bonafide work carried out for partial fulfilment of the academic requirement of 7th Semester B.E.(Information Science & Engineering) prescribed by KLS Gogte Institute of Technology Belagavi, during the academic year 2022- 2023. The report has been approved as it satisfies the academic requirements prescribed for the said degree.

Signature of Faculty Member: **Signature of HOD:**

Date:

Course Project report

Marks allocation:

	Batch No:8					
	Project Title: **Image Steganography**	Marks Range	USN			
			2GI19IS024	**2GI19IS047**	**2GI19IS050**	**2GI19IS055**
1.	Technical knowledge and awareness related to the project	5				
2.	Use of methadologies and results	5				
6.	Queries answered	5				
7.	Report and Oral presentation skill	5				
	Total	20				

*** 20 marks is converted to 10 marks for CGPA calculation**

1. Engineering Knowledge: Apply the knowledge of mathematics, science, engineering fundamentals and an engineering specialization to the solution of complex engineering problems.

2. Problem Analysis: Identify, formulate, review research literature, and analyse complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences and Engineering sciences.

3. Design/Development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

4. Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

5. Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering.

6. **The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
7. **Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. **Individual and team work:** Function effectively as an individual and as a member or leader in diverse teams, and in multidisciplinary settings.
10. **Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
11. **Project management and finance:** Demonstrate knowledge and understanding of the engineering management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. **Life-long learning:** Recognize the need for and have the preparation and ability to engage in independent and lifelong learning in the broadest context of technological change.

CONTENTS

1. Problem statement---06

2. Abstract---06

3. Objective--06

4. Introduction--06

5. Functional and Non-Functional Requirements -----------------------07

6. Steganography

    6.1. What Is Steganography? ------------------------------------07

    6.2. Steganography Vs. Cryptography ---------------------------08

    6.3. Image steganography--08

    6.4. Least significant bit method---------------------------------09

7. Methodology--10

8. Output---10

8. Conclusion---12

9. References---12

I. PROBLEM STATEMENT:

In todays scenario security is the very big challenge in any communication. The image steganography is the science of hiding secrete information in any transmission medium. Implement image steganography using Least Significant Bit method to hide secrete message inside a image.

II. ABSTRACT

Image Steganography is the process of hiding information which can be text, image or video inside a cover image. The secret information is hidden in a way that it not visible to the human eyes. Deep learning technology, which has emerged as a powerful tool in various applications including image steganography, has received increased attention recently. Steganography is a form of security technique through obscurity, the science and art of hiding the existence of a message between sender and intended recipient. Steganography has been used to hide secret messages in various types of files, including digital images, audio and video. The three most important parameters for audio steganography are imperceptibility, payload, and robustness. Different applications have different requirements of the steganography technique used.

III. OBJECTIVES:

To hide a secret ssmessage within a cover-media in such a way that others cannot discern the presence of the hidden message. The goal is to avoid drawing suspicion to the existence of a hidden message.

IV. INTRODUCTION:

Data. In essence, the modern computing world revolves around this word. But just what is so intriguing about it? In today’s world, businesses have started realizing that data is power as it can potentially predict customer trends, increase sales, and push the organization to newer heights. With the fast pace advancement in technology and use of data for continuous innovation it has become our topmost priority to secure data. Data sharing is increasing as thousands of messages and data are being transmitted on the internet every day from one place to another. The protection of data is the primary concern of the sender and it is really important that we encrypt our message in a secret way that only the receiver is able to understand.

Given the amount of data that is being generated and transmitted electronically in the world today , it’s no surprise that numerous methods of protecting data have evolved. Today’s security-conscious environment is the ideal place for trying out new techniques for hiding sensitive information. After all, we need to stay one step ahead of hackers and would-be data thieves! One of the rapidly growing security methods is Steganography.

V. FUNCTIONAL AND NONFUNCTIONAL REQUIREMENTS:

➢ Functional Requirements

- The system shall embed the secrete message inside image. This is done using LSB encryption method.
- . The output image should be same as the original image.

➢ Non-Functional Requirements/Performance Requirements

- For smooth & efficient encryption, image size must be less than 5MB.
- Decryption should not take more than 10 seconds.
- Safety and Security Requirements
- If the decryption takes more than 10 seconds, then discard the message (because the message might have been corrupted during transmission) and ask sender to re-send it.

VI. STEGANOGRAPHY:

➢ WHAT IS STEGANOGRAPHY?

The word **Steganography** is derived from two Greek words- ‘stegos’ meaning ‘to cover’ and ‘grayfia’, meaning ‘writing’, thus translating to ‘covered writing’, or ‘hidden writing’.
Steganography is a means of concealing secret information within (or even on top of) an otherwise mundane, non-secret document or other media to avoid detection. A The sensitive information will then be extracted from the ordinary file or message at its destination, thus avoiding detection. Steganography is an additional step that can be used in conjunction with encryption in order to conceal or protect data.

Steganography can be used to conceal almost any type of digital content, including text, image, video or audio content; the data to be hidden can be hidden inside almost any other type of digital content. The content to be concealed through steganography -- called hidden text -- is often encrypted before being incorporated into the innocuous-seeming cover text file or data stream. If not encrypted, the hidden text is commonly processed in some way in order to increase the difficulty of detecting the secret content.

➢ STEGANOGRAPHY VS. CRYPTOGRAPHY

It's fair to say that steganography and cryptography aim to shield messages and data from prying eyes at their most fundamental level However, they differ in the respect that cryptography makes the data unreadable, or hides the *meaning* of the data, while steganography hides the *existence* of the data.

The most important difference between Steganography and Cryptography is that the structure of data remains unchanged in steganography, which is not the case in cryptography. There aren't many mathematical transformations in steganography, whereas cryptography uses number theory, mathematics, and other techniques to alter the data.

➢ IMAGE STEGANOGRAPHY

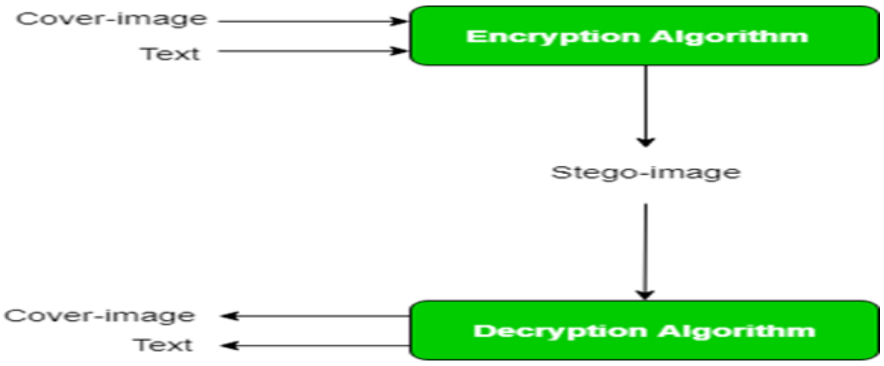
Image steganography, is a type of steganography which entails concealing data by using an image of a different object as a cover. Pixel intensities are the key to data concealment in image steganography.

The various terms used to describe image steganography include:

Cover-Image - Unique picture that can conceal data.

Message - Real data that you can mask within pictures. The message may be in the form of standard text or an image.

Stego-Image − A stego image is an image with a hidden message.



➢ LEAST SIGNIFICANT BIT METHOD FOR IMAGE STAGENOGRAPHY

We can describe a **digital image** as a finite set of digital values, called pixels. Pixels are the smallest individual element of an image, holding values that represent the brightness of a given color at any specific point. So we can think of an image as a matrix (or a two-dimensional array) of pixels which contains a fixed number of rows and columns.

Least Significant Bit (LSB) is a technique in which the last bit of each pixel is modified and replaced with the secret message’s data bit.

- Each pixel contains three values which are Red, Green, Blue, these values range from **0 to 255**, in other words, they are 8-bit values.
- Let’s take an example of how this technique works, suppose you want to hide the message “**hi**” into a **4x4** image which has the following pixel values: [(225, 12, 99), (155, 2, 50), (99, 51, 15), (15, 55, 22),(155, 61, 87), (63, 30, 17), (1, 55, 19), (99, 81, 66),(219, 77, 91), (69, 39, 50), (18, 200, 33), (25, 54, 190)].

Using ASCII table we can convert the secret message into decimal values and then into binary: **0110100 0110101.**Now, we iterate over the pixel values one by one, after converting them to binary, we replace each least significant bit with that message bits sequentially (e.g 225 is 11100001, we replace the last bit, the bit in the right (1) with the first data bit (0) and so on).This will only modify the pixel values by +1 or -1 which is not noticeable at all.

The resulting pixel values after performing LSBS is as shown below:
[(224, 13, 99),(154, 3, 50),(98, 50, 15),(15, 54, 23),(154, 61, 87),(63, 30, 17),(1, 55, 19),(99, 81, 66),(219, 77, 91),(69, 39, 50),(18, 200, 33),(25, 54, 190)]

VII. METHADOLOGY/ ALGORITHM:

Step 1: Import all the required libraries

Step 2: Define a function to convert any type of data into binary, we will use this to convert the secret data and pixel values to binary in the encoding and decoding phase.

Step 3: Write a function to hide secret message into the image by altering the LSB

Step 4: Define a function to decode the hidden message from the stego image

Step 5: Function that takes the input image name and secret message as input from user and calls hideData() to encode the message

Step 6: Create a function to ask user to enter the name of the image that needs to be decoded and call the showData() function to return the decoded message.

Step 7: Main Function()

VIII. OUTPUT:

Home Page:

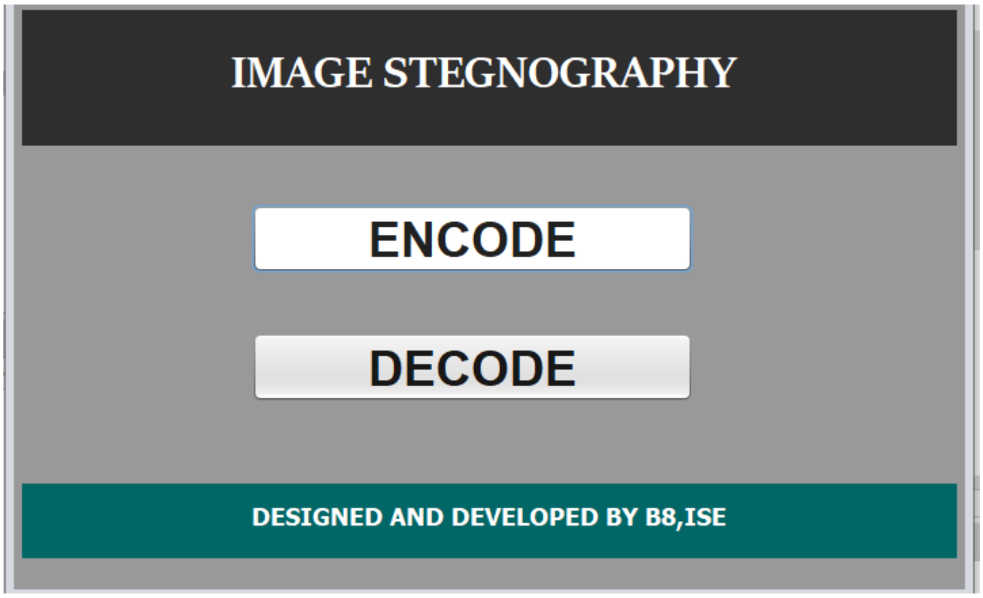
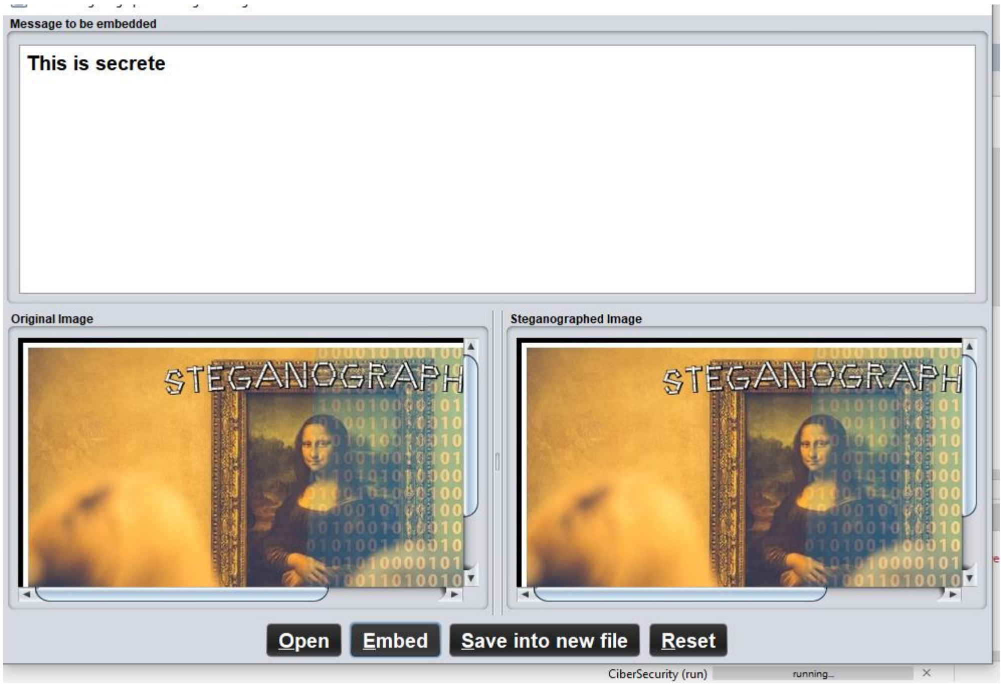


IMAGE STEGNOGRAPHY

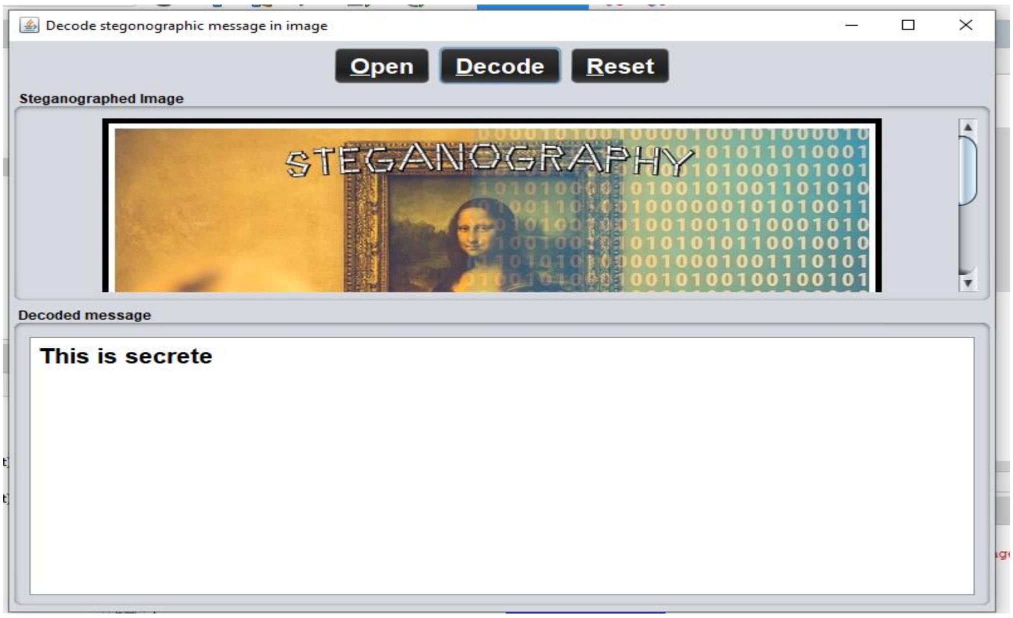
DESIGNED AND DEVELOPED BY B8,ISE

Encryption:



This is secrete

Decryption:



This is secrete

IX. CONCLUSION:

In todays scenario security is the very big challenge in any communication.The image steganography is the science of hiding secrete information in any transmission medium.In this project we mainly concentrated on embedding the data into image.We have developed a software program using java which embedded the data into the image.

X. REFERENCES:

1) https://towardsdatascience.com/steganography-hiding-an-image-inside-another-77ca66b2acb1

2) https://www.edureka.co/blog/steganography-tutorial

3) https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#191d0b0160ba