# ACKNOWLEDGEMENT

# ABSTRACT

Table of Contents

[ACKNOWLEDGEMENT 1](#_Toc12119380)

[ABSTRACT 2](#_Toc12119381)

[List of Figures 5](#_Toc12119382)

[Abbreviations 6](#_Toc12119383)

[Chapter 1: Introduction 7](#_Toc12119384)

[1.1 Introduction to Image Steganography 7](#_Toc12119385)

[1.2 Problem Statement 8](#_Toc12119386)

[1.3 Objective 8](#_Toc12119387)

[1.4 Scope and Limitations 9](#_Toc12119388)

[1.5 Report Organization 9](#_Toc12119389)

[Chapter 2: Literature Review 10](#_Toc12119390)

[Chapter 3: System Analysis and Feasibility Study 11](#_Toc12119391)

[3.1 Requirement Analysis 11](#_Toc12119392)

[3.1.1 Functional Requirements 11](#_Toc12119393)

[3.1.2 Non-Functional Requirements 12](#_Toc12119394)

[3.2 Feasibility Study 13](#_Toc12119395)

[3.2.1 Economical Feasibility 13](#_Toc12119396)

[3.2.2 Technical Feasibility 13](#_Toc12119397)

[3.2.3 Operational Feasibility 13](#_Toc12119398)

[3.3 Process Model 14](#_Toc12119399)

[3.3.1 DFD Diagram 14](#_Toc12119400)

[Chapter 4: System Design 15](#_Toc12119401)

[4.1 Architectural Design 15](#_Toc12119402)

[4.2 Class Diagram 15](#_Toc12119403)

[4.3 Activity Diagram 15](#_Toc12119404)

[4.4 Algorithm used 15](#_Toc12119405)

[Chapter 5: Implementation and Testing 16](#_Toc12119406)

[5.1 Tools Used 16](#_Toc12119407)

[5.2 Testing 17](#_Toc12119408)

[5.2.1 Unit Testing 17](#_Toc12119409)

[5.2.2 Integration Testing 17](#_Toc12119410)

[5.2.3 System Testing 17](#_Toc12119411)

[Chapter 6: Conclusion and Future Enhancement 18](#_Toc12119412)

[6.1 Conclusion 18](#_Toc12119413)

[6.2 Future Enhancement 18](#_Toc12119414)

[References 19](#_Toc12119415)

# List of Figures

[**Figure 1: Use-Case Diagram** 11](file:///E:\Project\Documentation\Final.docx#_Toc12117281)

# Abbreviations

# Chapter 1: Introduction

## 1.1 Introduction to Image Steganography

Due to advances in ICT, most information is kept electronically. Consequently, the security of information has become a fundamental issue. Maintaining the integrity and confidentiality of sensitive information, blocking the access of sophisticated hackers is very important. Steganography is a technique of hiding information in digital media. Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular ones because of their frequency on the internet. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists.

The growing possibilities of modern communications need the special means of security especially on computer network. With the increment in exchange of data over in internet, the network security is becoming more important. Therefore, the confidentiality and data integrity require protection against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding.

Steganography is the art of concealing information in ways that prevent the detection of hidden messages. Similarly, Cryptography is a technique associated with the process of converting ordinary plain text into unintelligible text and vice-versa. Together cryptography and steganography can provide a powerful basis for data security. These techniques become more important as more people join the cyberspace revolution.

Steganography hides the secrete message within the host data set and presence imperceptible and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an information analysis.

## 1.2 Problem Statement

No matter how large or small a company is, there is a need to have a plan to ensure the security of the information assets. With growing digitization in every field, digital security has become a fundamental aspect. Also, because of development in the internet technology, digital media can be transmitted conveniently over the network. This calls for security over the internet.

Throughout history Steganography and cryptography have been used to secretly communicate information between people. In the past, means of cryptography and steganography were carried out using traditional methods of pen and paper, using invisible ink, etc.

But, as mentioned earlier, with the increasing use of communication of information over digital medium, security for digital methods are to be developed.

Furthermore, the data hidden inside the stego medium needs to be encrypted rather than its original form. This ensures even more data security.

## 1.3 Objective

The main objectives of this project are:

* To produce security tool based on steganography and cryptography techniques combined.
* To avoid drawing suspicion to the existence of a hidden message.
* For the hidden message to be insensible to human beings.

## 1.4 Scope and Limitations

The scope of this project is to limit unauthorized access and provide better security during message transmission. To meet the requirements, simple and basic LSB approach of steganography will be used. In this project, the proposed system will first encrypt the message data using suitable algorithm and embed the result of encrypted data in an image file using steganography technique for sending over the network. The system will also provide the feature for extracting the hidden data from the corresponding image file and decrypting the extracted data for eventually finding the original message.

Steganography means hiding data into another data. It can be used to hide data such as text, image, audio, video etc. within a cover image, video etc. While our project will provide a way to hide text data into a cover image file, it will be limited only to data of the mentioned types i.e., text data onto image data.

## 1.5 Report Organization

# Chapter 2: Literature Review

# Chapter 3: System Analysis and Feasibility Study

## 3.1 Requirement Analysis

### 3.1.1 Functional Requirements

**Figure 1: Use-Case Diagram**

Functional requirements are the requirements that deﬁne speciﬁc behavior or function of the system.

* Cover Image: Cover Image is the image to be selected in which secret text message will be hidden.
* Secret Text Message: The sender will have to write secret message to hide or can select any text ﬁle containing the secret message.
* Sender: The sender will encrypt and embed the message onto an image and send the Stego image ﬁle to the intended recipient.
* Receiver: The receiver will receive the Stego image, extract and decrypt the same to find out the intended secret message.

### 3.1.2 Non-Functional Requirements

## 3.2 Feasibility Study

Feasibility Study is a test of the system according to its workability, impact of the organization, ability to meet user needs and effective use of the resources. A Feasibility Study is generic in nature and can be applied to any type of project, be it for systems and software development, making an acquisition, or any other project. We can test our system by different type of the feasibilities.

### 3.2.1 Economical Feasibility

This system will be economically feasible as all the tools and resources required are either open source or free.

### 3.2.2 Technical Feasibility

Technical feasibility is a study of resources availability that may affect the ability to achieve an acceptable system. This evaluation determines whether the technology needed for the proposed system is available or not.

### 3.2.3 Operational Feasibility

This system will be user friendly and will also provide easy ways to add new features as per new requirements.

## 3.3 Process Model

### 3.3.1 DFD Diagram

# Chapter 4: System Design

## 4.1 Architectural Design

## 4.2 Class Diagram

## 4.3 Activity Diagram

## 4.4 Algorithm used

**Least Significant Bit (LSB) Method**

Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed. There have been many techniques for hiding information or messages in images in such a manner that alteration made to the image is perceptually indiscernible. Commonly used approaches include LSB, Masking and filtering and Transform techniques.

Least significant bit (LSB) insertion is a simple approach for embedding information in image file. A digital image consists of a matrix of color and intensity values. In a gray scale image, there are 8 bits per pixel are used. In a full-color image there are 24 bits per pixel, and 8 bits assigned to each color components that means red, green and blue. This technique embeds the bits of the message directly into the least-significant bit of the cover image in a deterministic sequence.

**Message embedding procedure:**

1. Read the cover image and secret text information which is to be embedded in to the cover image.
2. Convert the secret information into cipher text by using secret key shared by receiver and sender.
3. Convert encrypted text message into binary form.
4. Find LSBs of each RGB pixels of the cover image.
5. Embed the bits of the secret information into bits of LSB of RGB pixels of the cover image.
6. Continue the procedure until the secret information is fully hidden into cover file.

**Message extraction procedure:**

1. Read the stego image.
2. Retrieve the LSBs of each RGB pixel of the stego image.
3. Convert binary strings formed by every 8 RGB pixels of step 2 to character and append the characters to a string builder.
4. Continue the process until the data is fully extracted from stego image to the string builder.
5. Using shared key, decrypt secret information to get original information.

# Chapter 5: Implementation and Testing

## 5.1 Tools Used

## 5.2 Testing

### 5.2.1 Unit Testing

### 5.2.2 Integration Testing

### 5.2.3 System Testing

# Chapter 6: Conclusion and Future Enhancement

## 6.1 Conclusion

## 6.2 Future Enhancement

# References

**There are no sources in the current document.**

## 