# ACKNOWLEDGEMENT

Firstly, we would like to thank Himalaya College of Engineering for providing us this platform to gain knowledge about different aspects of Computer Science and Information Technology.

We would also like to thank our Head of Department Er. Himal Chand Thapa who played an important role in providing us advice and suggestion towards the selection of our project topic as well as for providing us with necessary content and classes regarding the project. We are also grateful for the care and support from our supervisor Mr. Bhupendra Luhar and for providing us all necessary suggestions and corrections he provided, for our project.

In addition, we also want to thank our friends and classmates for helping us with the guidelines we needed during the completion of our project.

# ABSTRACT

Steganography refers to information or a file that has been concealed inside a digital picture, video or audio file. If a person views the object in which the information is hidden inside, he or she will have no indication that there is any hidden information. So the person will not try to decrypt the information. Steganography can be divided into Text Steganography, Image Steganography, Audio/Video Steganography. Image Steganography is one of the common methods used for hiding the information in the cover image. LSB is very efficient algorithm used to embed the information in a cover file. This paper presents the detail knowledge about the LSB based image steganography and its applications to various file formats. In this paper we also analyze the available image-based steganography along with cryptography technique to achieve security.

Table of Contents

[ACKNOWLEDGEMENT 1](#_Toc12379113)

[ABSTRACT 2](#_Toc12379114)

[List of Figures 5](#_Toc12379115)

[Abbreviations 6](#_Toc12379116)

[Chapter 1: Introduction 7](#_Toc12379117)

[1.1 Introduction to Image Steganography 7](#_Toc12379118)

[1.2 Problem Statement 8](#_Toc12379119)

[1.3 Objective 8](#_Toc12379120)

[1.4 Scope and Limitations 9](#_Toc12379121)

[1.5 Report Organization 9](#_Toc12379122)

[Chapter 2: Literature Review 10](#_Toc12379123)

[Chapter 3: System Analysis and Feasibility Study 11](#_Toc12379124)

[3.1 Requirement Analysis 11](#_Toc12379125)

[3.1.1 Functional Requirements 11](#_Toc12379126)

[3.1.2 Non-Functional Requirements 12](#_Toc12379127)

[3.2 Feasibility Study 13](#_Toc12379128)

[3.2.1 Economical Feasibility 13](#_Toc12379129)

[3.2.2 Technical Feasibility 13](#_Toc12379130)

[3.2.3 Operational Feasibility 13](#_Toc12379131)

[3.3 Process Model 14](#_Toc12379132)

[3.3.1 DFD Diagram 14](#_Toc12379133)

[Chapter 4: System Design 15](#_Toc12379134)

[4.1 System Design 15](#_Toc12379135)

[4.2 Class Diagram 16](#_Toc12379136)

[4.3 Activity Diagram 16](#_Toc12379137)

[4.4 Algorithm used 17](#_Toc12379138)

[Chapter 5: Implementation and Testing 19](#_Toc12379139)

[5.1 Tools Used 19](#_Toc12379140)

[5.2 Testing 20](#_Toc12379141)

[5.2.1 Unit Testing 20](#_Toc12379142)

[5.2.2 Integration Testing 20](#_Toc12379143)

[5.2.3 System Testing 20](#_Toc12379144)

[Chapter 6: Conclusion and Future Enhancement 21](#_Toc12379145)

[6.1 Conclusion 21](#_Toc12379146)

[6.2 Future Enhancement 21](#_Toc12379147)

[References 22](#_Toc12379148)

# List of Figures

[**Figure 1: Use-Case Diagram** 11](file:///E:\Project\Documentation\Final.docx#_Toc12369357)

[**Figure 2: Activity Diagram** 16](file:///E:\Project\Documentation\Final.docx#_Toc12369358)

# Abbreviations

AES: Advanced Encryption Standard 10

ICT: Information and Communication Technology 7

LSB: Least Significant Bit 10

# 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 [1]. 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.

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. 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.

## 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 in 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 had been used. The program first encrypts the message data using AES algorithm and embeds the result of encrypted data in the provided image file using steganography technique for sending over the network. The system also provides 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 system program provides a way to hide text data into a cover image file, it is limited only to data of the mentioned types i.e., text data onto image data.

## 1.5 Report Organization

# Chapter 2: Literature Review

The word steganography is derived from the Greek words stegos meaning cover and grafia meaning writing [2]. Image steganography the information is hidden exclusively in images. Steganography is the art and science of secret communication. It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The actual files can be referred to as cover text, the cover image, or cover audio message. After inserting the secret message, it is referred to as stegomedium. A stego-key has been used for hiding encoding process to restrict detection or extraction of the embedded data [3].

# 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

The system is economically feasible as all the tools and resources required are either cheap or free.

### 3.2.2 Technical Feasibility

The technical requirements for the project are easily available and the system can be operated by users with simple knowledge regarding the required technologies.

### 3.2.3 Operational Feasibility

The system is user friendly as it is easy to use and operating the system doesn’t require too complex skills.

## 3.3 Process Model

### 3.3.1 DFD Diagram

# Chapter 4: System Design

## 4.1 System Design

## 4.2 Class Diagram

## 4.3 Activity Diagram

**Figure 2: 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 are many techniques for hiding information or messages in images such that alteration made to the image is perceptually indiscernible. Commonly used approaches include LSB, Masking and filtering and Transform techniques.

LSB based technique is simple approach in which message bits are embed in the least significant bits of cover image [4]. In this technique, the least significant bit of cover image is used to hide the secret message. This is method for embedding data into cover image. The least significant bit of each pixel of an image is altered to a bit of a message that is to be hidden [5].

**Message embedding procedure:**

1. Read the cover image and secret text information which is to be embedded into the image.
2. Convert the secret information into encrypted text by using AES algorithm and secret key shared by receiver and sender.
3. Convert encrypted text message into binary form – which will give the text message’s bits.
4. Find LSBs of each RGB pixels of the cover image.
5. Embed the bits obtained on step 3 into LSBs of RGB pixels of step 4.
6. Continue the procedure until the secret information is fully hidden in cover image file.

**Message extraction procedure:**

1. Read the stego image and secret key.
2. Retrieve LSBs of each RGB pixels 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 and AES decryption, decrypt secret information obtained on step 4 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

|  |  |
| --- | --- |
| [1] | S. Singh, Literature Review On Digital Image Steganography and Cryptography Algorithms, 2015/07/01. |
| [2] | A. Soni, J. Jain and R. Roshan, "Image steganography using discrete fractional Fourier transform," *Intelligent Systems and Signal Processing (ISSP),* 2013. |
| [3] | N. Akhtar, P. Johri and S. Khan, "Enhancing the Security and Quality of LSB Based Image Steganography," *Computational Intelligence and Communication Networks (CICN),* 2013. |
| [4] | M. R. Garg, "Comparison Of Lsb & Msb Based Steganography In Gray-Scale Images," *International Journal of Engineering Research and Technology (IJERT),* vol. 1, no. 8, 2012. |
| [5] | P. J. N. Dr. Ekta Walia, "“An Analysis of LSB & DCT based Steganography," *Global Journal of Computer Science and Technology,* vol. 10, no. 1, 2010. |