A Minor Project Proposal Report On

**Data Hiding: Image Steganography by Using LSB Replacement Algorithm**

Submitted in Partial Fulfillment of Requirements for the Degree of **Bachelors of Engineering in Information Technology**

Under Pokhara University

Submitted by:

**Atit Kunwar, 191508**

**Utsab Maharjan, 191549**

**Sagar Nemkul, 191535**

Date:

17 May, 2023

**Department of Information Technology**



**NEPAL COLLEGE OF**

**INFORMATION TECHNOLOGY**

**Balkumari Lalitpur, Nep****al**

# 1. Abstract

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 because of their frequency on the internet. For hiding secret information in images, there exist a large variety of steganography techniques some are more complex than other and all of them have respective strong and weak points. Different application has different requirement of the steganography technique used.

For example, some application may require absolute invisibility of the information, while others require a larger secret message to be hidden. This project hides the message within the image. Sender select the cover image with the secret text or text file and hide it in to the image with the bit replacement choice, it helps to generate the secure stego-image. The stego image is sent to the destination with the help of private or public communication network. On the other side, Receiver download the stego-image and using the software retrieve the secret text hidden in the stego image.

Here, we use the Least Significant Bit (LSB) algorithm to embed the Cipher text, to be transferred in an image and indistinguishable from original image and cannot detect the presence of original data. The secret data is converted to cipher text through cryptography using AES algorithm.

**Keyword:** encryption, decryption, receiver, steganography, data security

[1. Abstract 3](#_Toc115018757)

[2. Introduction 4](#_Toc115018758)

[3. Problem of Statement 5](#_Toc115018759)

[4. Project Objective 6](#_Toc115018760)

[5. Scope and Importance of the Project 7](#_Toc115018761)

[6. Literature Review 8](#_Toc115018762)

[7 .METHODOLOGY 9](#_Toc115018763)

[8. Deliverables 13](#_Toc115018764)

[9. Task and Time Schedule 14](#_Toc115018765)

[10. Bibliography 15](#_Toc115018766)

# 2. Introduction

Image steganography is a technique of concealing secret information within digital images. The primary goal of steganography is to hide the existence of the secret data in such a way that it is undetectable by any observer. Steganography has been used for centuries, and the practice has changed to take advantage of technology.

In today's world, where digital communication is required, image steganography is becoming more and more important. Steganography differs from cryptography, which focuses on hiding the meaning of the data, rather than its existence. Cryptography uses mathematical algorithms to convert the data into a code that can be decrypted only by authorized users. In contrast, steganography involves embedding the secret data in a digital image, audio, or video file.

In conclusion, image steganography is an important field with applications in various areas, including security, privacy, and digital forensics. Ongoing research is focused on enhancing the capacity and robustness of stenographic algorithms while ensuring they are secure and difficult to detect.

# 3. Problem of Statement

In this digital era, everything has been digitalized, lots data has been losing daily through different medium. In this project we attempt to hide the data using encryption and steganography to maintain the privacy. While sharing the files, user is able to send through that image file without being noticed by any noticeable changes.

The primary challenge in image steganography is to embed secret data in an image without altering the image's quality. The goal is to ensure that the existence of the hidden data is undetectable by any observer. The challenge is to find a balance between the amount of secret data that can be hidden in an image and the extent to which the image's quality is degraded.

Finally, the ethical use of steganography is a challenge. Steganography can be used for wrong intentions, such as hiding critical data during cyberattacks or acts of terrorism. Therefore, it is essential to use steganography ethically and lawfully to prevent any misuse of the technique.

Main problems are as follows:

* Unethical use of steganography
* Altering image’s quality
* Altering size of the image

# 4. Project Objective

Objectives of image steganography includes:

* To create a tool that to hide confidential data inside a 24-bit color image and

encrypt the message produce cipher text.

* To display the hidden message successfully from the cover image if and only if private key is matched.

# 5. Scope and Importance of the Project

The concept intends to secure the confidential information that may occur in digital data.

* The scope of the project is to limit unauthorized access and provide better security during message transmission.
* In this project, the proposed approach finds the suitable algorithm for embedding the data in an image using steganography which provides the better security pattern for sending messages through a network.
* The data is converted to cipher-text incase, if attacker knew the data is driven.
* The goal of this study is to conceal / hide data in image.
* Reveal the stego image's hidden message when the symmetric key is used.

# 6. Literature Review

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 because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points.

Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This project intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.

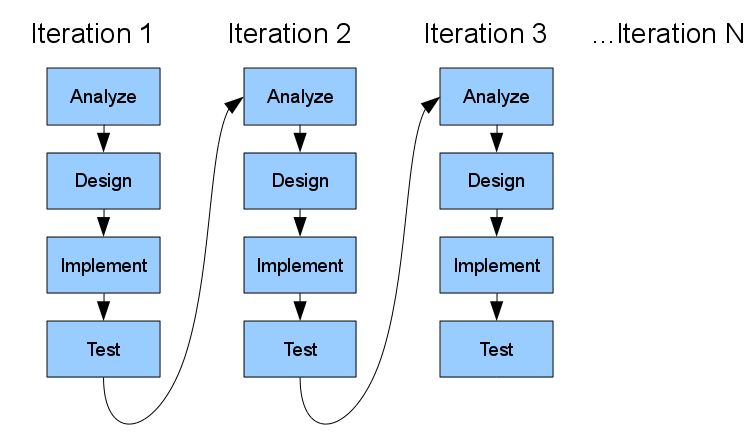
1. In Ancient Greece, they used to select messengers and shave their head, they would then write a message on their head. Once the message had been written the hair was allowed to grow back. After the hair grew back the messenger was sent to deliver the message, the recipient would shave off the messenger’s hair to see the secrete message.
2. During World War 2, invisible ink was used to write information on pieces of paper so that the paper appeared to the average person as just being blank pieces of paper. Liquids such as milk, vinegar and fruit juices were used, because when each one of these substances were heated, they darken and become visible to the human eye. Invisible ink has been in use for centuries for fun by children and students and for serious espionage by spies and terrorists.
3. Cryptography became very common place in the middle ages. Secret writing was employed by the Catholic Church in its various struggles down the ages and by the major governments of the time. Steganography was normally used in conjunction with cryptography to further hide secret information.

# 7. METHODOLOGY

To complete our project, we have planned to work in accordance with these methodologies for the application of knowledge, skills, and techniques to a variety of activities.

**7.1. Software Development Lifecycle**

The framework we will be used for developing this project is an iterative model of software development life cycle. In this model, a simple and primitive implementation of very small set of software requirement is done at first, which is followed by the iterative enhancement in the primitive model until all requirements are fulfilled and the software is ready for deployed. The following sub section briefly describe various phase in iterative model of SDLC that was applied in the development of system.



**Fig**: Iterative methodology

**7.1.1. REQUIREMENT ANALYSIS:**

In this phase, analysis will be performed in order to find out the requirements of the system. The outcome of this phase would be a SRS which is an acronym for “system requirement specifications”

**7.1.2. DESIGN PHASE:**

In this phase the SRS would be translated into the system design. Context diagram DFD ED diagram, use case diagram, sequence diagram and class diagram will be developed.

**7.1.3. CODING PHASE:**

In this phase coding will be done according for the design and a working system will be developed by the end of the process.

**7.1.4. TESTING PHASE:**

In this phase the system will be tested with each testing list of changes to the system developed, is suggested and the change will be applied to the software and the software would be delivered as a successive increment until a satisfying system is achieved.

**TOOLS USED**

1. VS Code: Integrated Development Environment (IDE)
2. GitHub: Manage source code
3. Libre Office: Design

# 8. DELIVERABLES

The system proposed mainly aims to provide privacy and security during the data transfer. In case of any cyber attack in any company or any government institution, there won’t be any loss of data as the important confidential data are first cipher texted and further encrypted as well as they are hidden using steganography which will make the attacker to detect the data and decrypt those confidential data.

# 9. PROJECT TASK AND TIME SCHEDULE

The project schedule has been designed as per requirements and constraints involved. This project is scheduled to be completed in about 4-5 months. Requirement analysis have been given more emphasis. Research is to be done first and well documented. Debugging and Testing is to be done prior to the completion of the project.

|  |  |  |  |
| --- | --- | --- | --- |
| Task | ImagePicker Feature | Encrypt Decrypt Feature | Steganography |
| Requirement Analysis | 2d | 2d | 3d |
| Analysis of  System | 3d | 3d | 3d |
| Design System | 2d | 3d | 3d |
| Implementation | 5d | 3d | 1w |
| Testing and Debugging | 2d | 2d | 4d |
| Develop Dccumentation | 5d | 4d | 4d |

**Use case Diagram**

A use case diagram represents the relationship between the user and the different use cases in which the user is involved. The actors for our system are: Sender and Receiver.

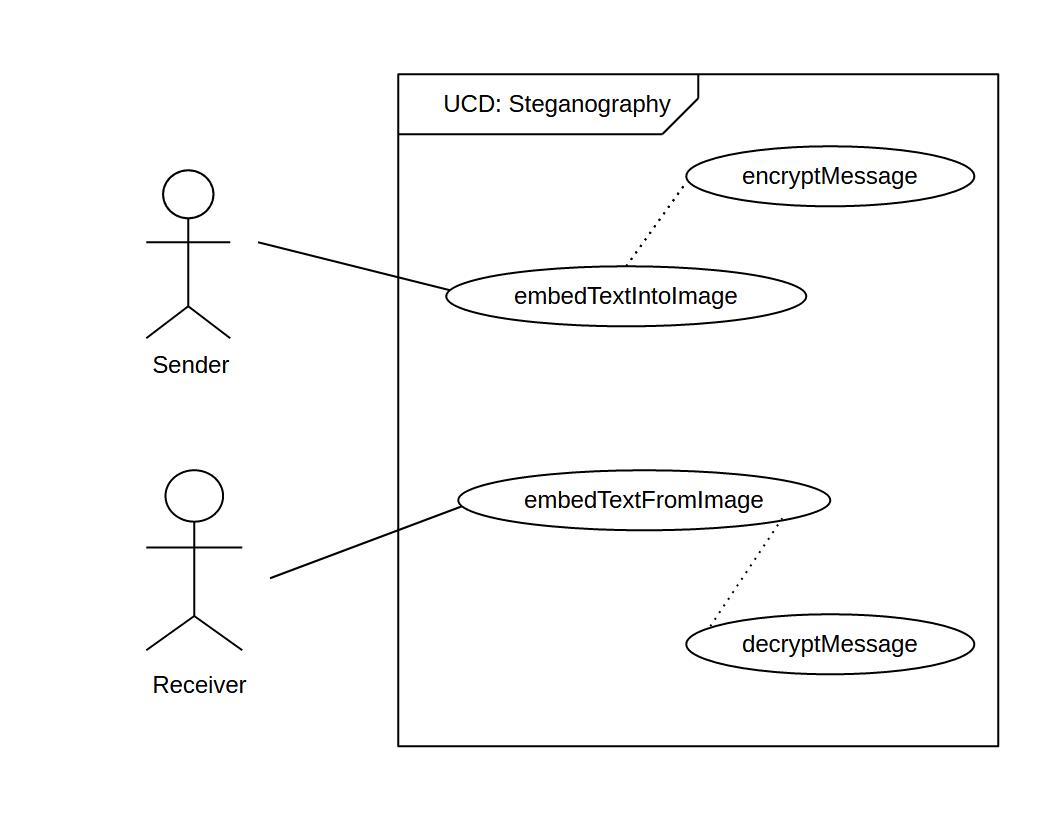
****

Fig: use case diagram

**Use case UC1: EmbedTextIntoImage:**

**Primary Actor:** Sender

**Cross References:** Steganography

**Secondary Actor:** none

**Stakeholder:**

Sender: Select the image, insert message and key

**Preconditions:**

24 bit color image

**Post conditions:**

CryptText instance creation

Image source attribute modification

Cipher text creation

**Use case UC1: EmbedTextIntoImage:**

**Primary Actor:** Receiver

**Cross References:** Steganoanalysis

**Secondary Actor:** none

**Stakeholder:**

Receiver: Select the image, insert message key

**Preconditions:**

24 bit color image

**Post conditions:**

CryptText instance creation

Image source attribute modification

Cipher text creation

**Bibliography**

* Sree Lakshmi Sree; Nov 9,2015. Image Steganography using LSB [https://www.slideshare.net/SreelekshmiSree1/image-steganography-using35

lsb]

* [https://www.matecconferences.org/articles/matecconf/pdf/2016/20/matecconf

\_icaet2016\_02003.pdf]

* [https://www.slideshare.net/AnimeshShawRana/cryptographysteganography].