JAYPEE INSTITUTE OF INFORMATION TECHNOLOGY

SOFTWARE ENGINEERING LAB

PROJECT-BASED LEARNING

TITLE: CRYPTOGRAPHY AND IMAGE STEGANOGRAPHY

GROUP MEMBERS:

Name	Enrollment No.
Mukund Sarda	21103105
Akash Sharma	21103093
Karanjot Singh	21103096
Mannat	21103109

TABLE OF CONTENTS

PROBLEM STATEMENT

As more people join the new technological revolution, steganography becomes increasingly significant.

The purpose of steganography is to eliminate the possibility of a hidden message being discovered.

This method of information concealment has recently gained popularity in a variety of fields. Digital music, video, and images are becoming increasingly marked with distinct but undetectable marks that may convey a concealed notice or serial number or even directly aid to prevent unauthorized duplication.

There are several hacking cases in today's world. Many businesses, including banking and business, are concerned that unauthorized people will access all of their personal and industry data.

Domain tools or basic systems such as least significant bit (LSB) insertion and noise manipulation, transform domain that involves manipulation algorithms, and picture modification such as discrete cosine transformation and wavelet transformation are some of the techniques utilized in steganography.

The goal of this project is to use steganographic techniques to encrypt or hide data over an image, as well as to understand the algorithms in terms of concealment quality and functionality in data security.

INTRODUCTION

In the proposed system, we implement two important n/w security concepts namely STEGANOGRAPHY and ENCRYPTION(CRYPTOGRAPHY). Steganography is the science of hiding data. A steganography process normally involves a cover medium, secret information, and a stego-key. Together combined, they form the Stego-medium. Encryption is often confused with Steganography. Encryption is the process of converting a plaintext message into an unrecognizable form known as the ciphertext.

Various algorithms are used in Encryption but in this project, no standard algorithm has been used due to time consumption. In this project, a text file containing the secret information is created. An image file in PNG format is chosen as the cover medium. Since the contents of the image file and text file are different, a function is written to convert the text file into the bitstream. Then the text data is converted to an unrecognizable form. This process is known as Encryption. The encrypted file is then taken and embedded into the image file.

Care is taken throughout the project so that the image file does not suffer from any corruption. On the receiver side, the image file is taken and the encrypted file is recovered by De-Steganography. Then the encrypted file is decrypted to reveal the secret information. The contents of the image file are listened to before and after the techniques have been implemented with the aid of a speaker.

GOAL OF THE PROJECT

The goal of this project is to use steganographic techniques to encrypt or hide data over an image, as well as to understand the algorithms in terms of concealment quality and functionality in data security.

There are several hacking cases in today's world. Many businesses, including banking and business, are concerned that unauthorized people will access all of their personal and industry data.

Domain tools or basic systems such as least significant bit (LSB) insertion and noise manipulation, transform domain that involves manipulation algorithms, and picture modification such as discrete cosine transformation and wavelet transformation are some of the techniques utilized in steganography.

USER STORY

1. As a user,

   I must be able to encrypt data

   So that I can send it easily to my colleague
2. As a customer,

   I must be able to decrypt data

   So that I can understand my friend's message
3. As a developer,
   I have to create efficient software

   So that users can communicate without privacy issues.

FUNCTIONAL REQUIREMENTS

1. Users should be able to choose an image for steganography.
2. If the image file is not in.png format, it is converted to.png format.
3. A bitstream is created from the encrypted text file.
4. The user selects an encryption algorithm for cryptography.
5. User will input the data to be encrypted.
6. The bitstream, together with the key, is then embedded into the picture file using the chosen technique.
7. The key must match the receiving end. If the key matches, a reverse algorithmic method is used to de-steganography the data.
8. To acquire the concealed message, the received bitstream is transformed into a text file and then decrypted.

NON-FUNCTIONAL REQUIREMENTS

1. Performance

   The embedded image file generated should not contain any unwanted pixels. Also, the application should be secure for statistical and comparison reanalysis. The time taken by the designed system is very less. The majority of the time is taken from the client/user side. The software gives almost instantaneous results.

2. Reliability

   The product should not crash under any circumstance such as a user entering invalid values, a user trying to load unsupported files, etc. It should show appropriate messages for every user-generated message.

3. Ease of Access

   Our product will be easy to use and self-explanatory as well. The user will be asked to do everything step by step and thus will not face any problems. Any user will be able to use our product from scratch and thus can easily encrypt and decrypt data.

4. Language

   The software will be in the English Language. As it is a universal language, so anyone can use and understand it.

5. User Interface

   The user interface will be intuitive and visually appealing, with clear instructions and prompts guiding users through the steganography and cryptography processes.

6. Compatibility

   The application will be compatible with multiple operating systems, including Windows, macOS, and Linux, to accommodate a wide range of users.

7. Scalability

   The software architecture will be designed to scale seamlessly as the user base and data volume grow over time.

8. Data Integrity

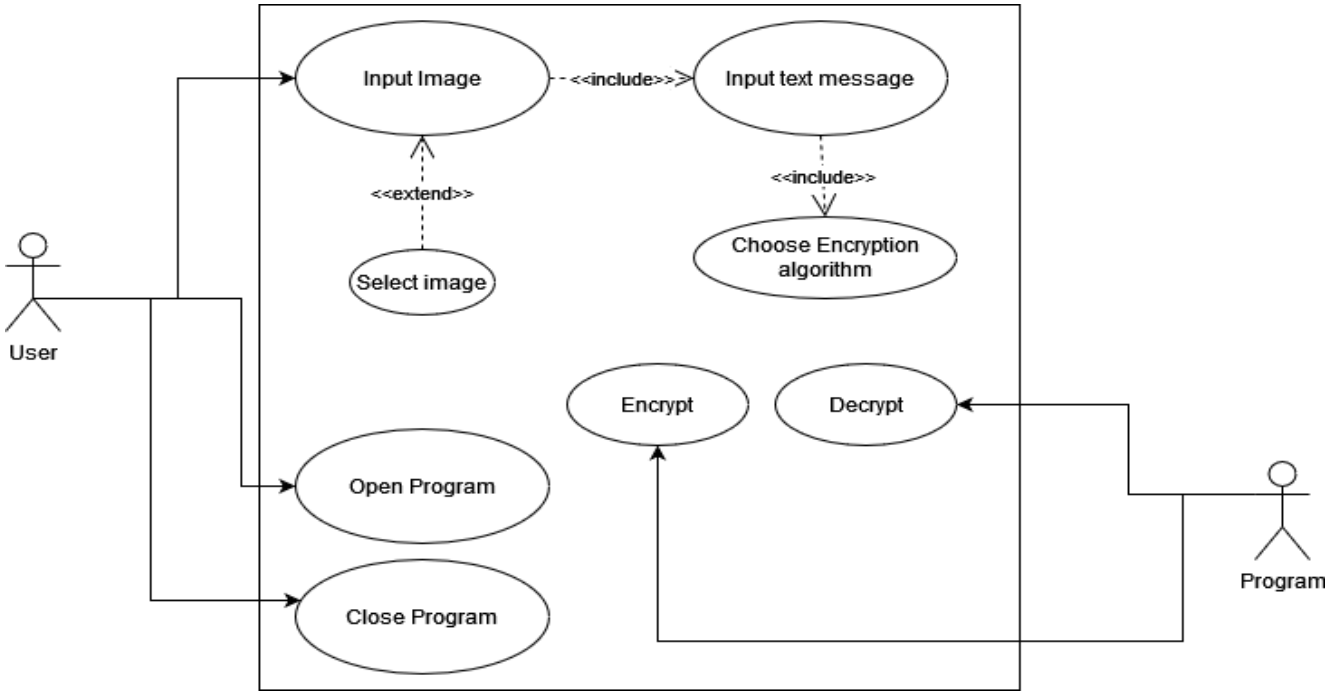
   The application ensures the integrity and accuracy of the concealed data during the embedding and extraction processes.

9. Privacy and Security

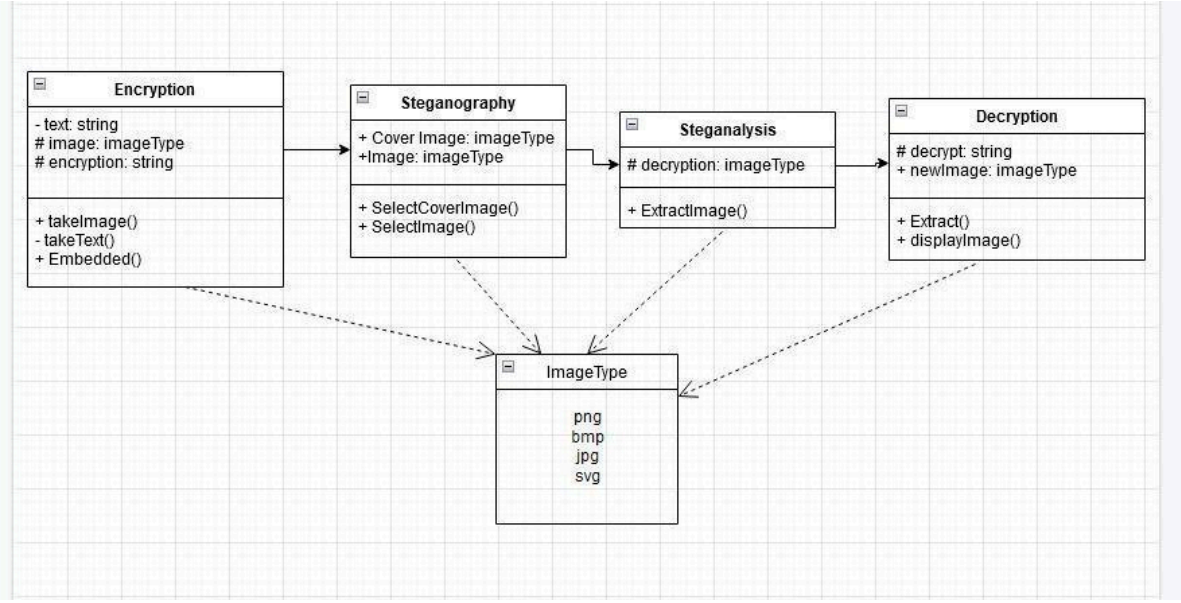
   The software adheres to industry-standard security practices and encryption protocols to protect sensitive information from unauthorized access or interception.

UML DIAGRAMS

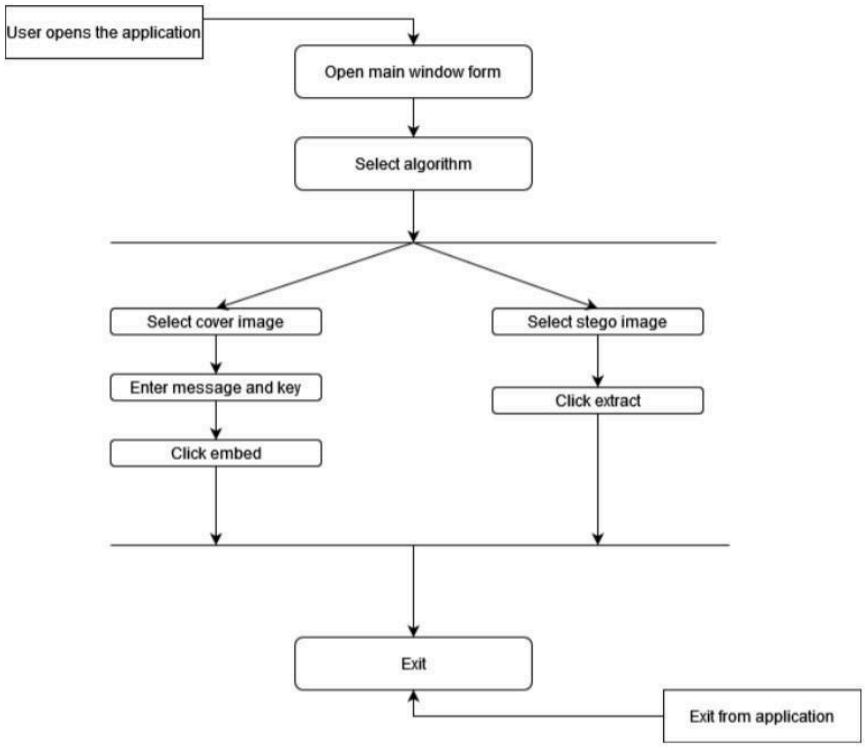
1. USE CASE DIAGRAM



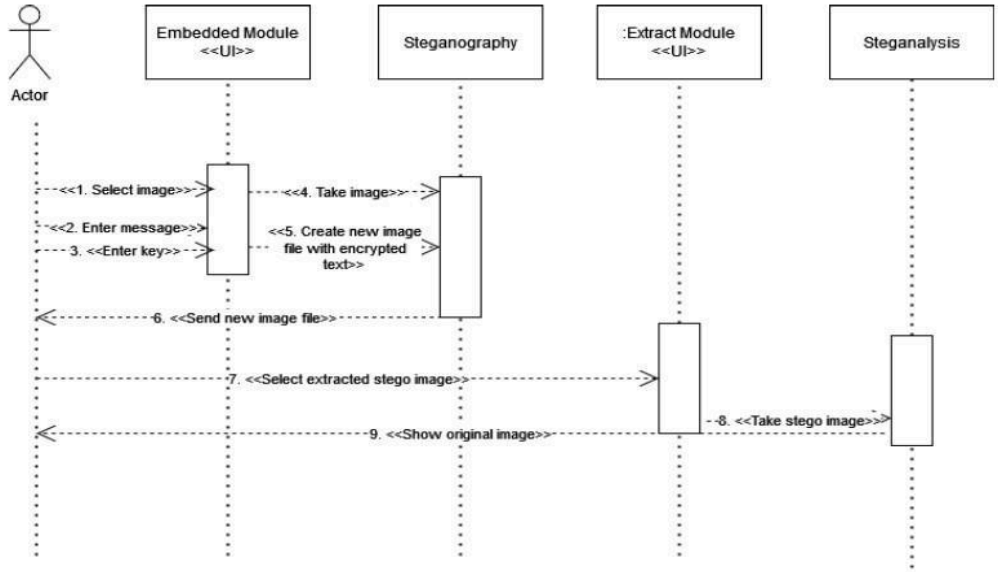
2. CLASS DIAGRAM



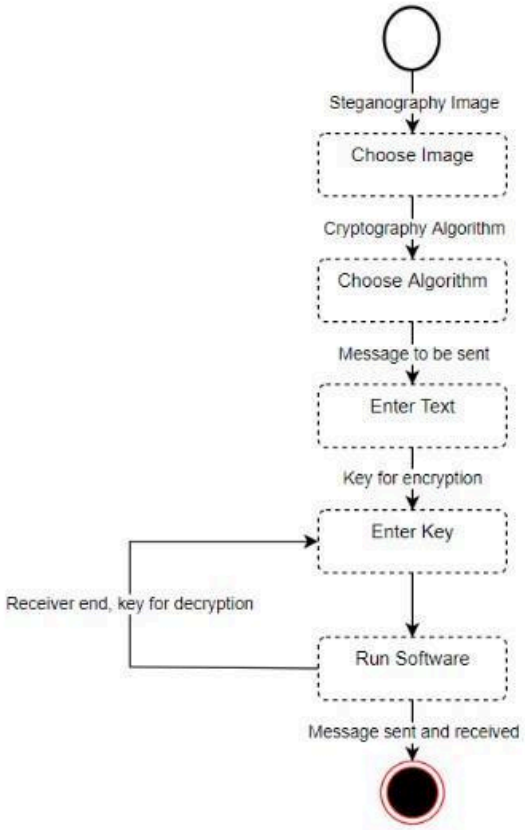
3. ACTIVITY DIAGRAM



4. SEQUENCE DIAGRAM



5. STATE DIAGRAM



IMPLEMENTATION

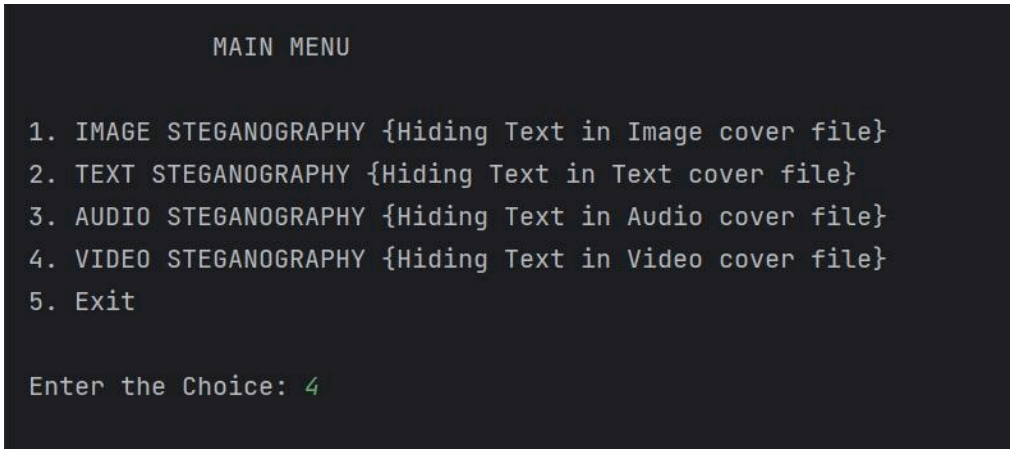
The user is given choices to select a steganography method among the four which are: -

- Image Steganography
- Text Steganography
- Audio Steganography
- Video Steganography

On selecting one of the above methods the user is then asked whether he wants to encrypt, decrypt the data.

If the user wants to encrypt the data then firstly he needs to provide the file name and then the text which has to be encrypted and the given text is stored in the file name provided.

If the decryption is selected then the key has to be provided by the user to ensure if the user is reliable and the file name that has to be decrypted and the embedded text is returned by the program.



```
        VIDEO STEGANOGRAPHY OPERATIONS
1. Encode the Text message
2. Decode the Text message
3. Exit
Enter the Choice:1
Total number of Frame in selected Video : 172
Enter the frame number where you want to embed data :
100

Enter the data to be Encoded in Video :wertyui
Enter the key :
123
The encrypted data is :  $ÍöÍöm

Encoded the data successfully in the video file.
```

```
        VIDEO STEGANOGRAPHY OPERATIONS
1. Encode the Text message
2. Decode the Text message
3. Exit
Enter the Choice:2
Total number of Frame in selected Video : 172
Enter the secret frame number from where you want to extract data
100
Enter the key :
123

The Encoded data which was hidden in the Video was :--
 wertyui
```

TEST CASE REPORT

- **VIDEO STEGANOGRAPHY**

CASE 1: - PASS

```
        VIDEO STEGANOGRAPHY OPERATIONS
1. Encode the Text message
2. Decode the Text message
3. Exit
Enter the Choice:1
Total number of Frame in selected Video : 172
Enter the frame number where you want to embed data :
100

Enter the data to be Encoded in Video :wertyui
Enter the key :
123
The encrypted data is :  $ØÍöØ▫m

Encoded the data successfully in the video file.
```

CASE 2: - FAIL

```
        VIDEO STEGANOGRAPHY OPERATIONS
1. Encode the Text message
2. Decode the Text message
3. Exit
Enter the Choice:1
Total number of Frame in selected Video : 172
Enter the frame number where you want to embed data :
500
Invalid Frame Number Selected
```

- **TEXT STEGANOGRAPHY**

CASE 1: - PASS

```
Maximum number of words that can be inserted :-  879

Enter data to be encoded:- 1

Inputed message can be hidden in the cover file

The string after binary conversion appyling all the transformation :- 001111001011111111111111
Length of binary after conversion:-  24

Enter the name of the Stego file after Encoding(with extension):- 1245.txt

Stego file has successfully generated
```

CASE 2: -FAIL

```
        TEXT STEGANOGRAPHY OPERATIONS
1. Encode the Text message
2. Decode the Text message
3. Exit
Enter the Choice:1
Maximum number of words that can be inserted :-  879

Enter data to be encoded:- qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq

String is too big please reduce string size
Maximum number of words that can be inserted :-  879
```

- **IMAGE STEGANOGRAPHY**

CASE 1: -PASS

```
        IMAGE STEGANOGRAPHY OPERATIONS

1. Encode the Text message
2. Decode the Text message
3. Exit
Enter the Choice: 2
Enter the Image you need to Decode to get the Secret message :  se.png


The Encoded data which was hidden in the Image was :--   Software Engineering
```

CASE 2: -FAIL

```
        IMAGE STEGANOGRAPHY OPERATIONS

1. Encode the Text message
2. Decode the Text message
3. Exit
Enter the Choice: 2
Enter the Image you need to Decode to get the Secret message :  rk.jpeg
File Format Not Supported
```