Image Steganography Android Application

A Report for the Evaluation 3 of Project 2

Submitted by

SAURABH YADAV

(16SCSE101583/1613101653)

in partial fulfillment for the award of the degree of

Bachelor of Technology

In

Computer Science and Engineering

SCHOOL OF COMPUTING SCIENCE & ENGINEERING

Under the Supervision of

Ms. Varsha Sisaudia
Asst. Professor

APRIL/MAY 2020

SCHOOL OF COMPUTING AND SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

Certified that this project report **"IMAGE STEGANOGRAPHY ANDROID APPLICATION"** is the bonafide work of "**SAURABH YADAV(1613101653)"** who carried out the project work under my supervision.

SIGNATURE OF HEAD
Dr. MUNISH SHABARWAL,
PhD (Management), PhD (CS)
Professor & Dean,
School of Computing Science & Engineering

SIGNATURE OF SUPERVISOR
Ms. VARSHA SISAUDIA,
Mtech
Asst. Professor,
School of Computing Science & Engineering

TABLE OF CONTENTS

1. ABSTRACT

Steganography is the art of hiding information in some other. There can be various file formats which can be used for this technique, but images are the most popular because of their use. For hiding the secret message or information different techniques are used some are easy and some are complex. Also the techniques are chosen according to the fact that different applications have different requirements. For example, some applications require large secret message to be hidden while some require absolute invisibility.

This project hides the secret message within the image and also hides an image inside other image. The message to be embedded inside the image is in .txt format. The application generates a secure and less distorted stego image.

At sender side, sender encodes the message into the image using the application's encode button, as an output senders get a stego image. This stego image is send to the receiver who retrieves the secret information. For the process to happen the receiver must have the same application for retrieval.

INTRODUCTION

Data and information hiding is very important as far as security is concerned and as the data transmission is increasing rapidly so does the attacks over the network. In such scenarios it is must to have some algorithms or techniques that can make sure that the secret data sent over the network is secure. Through data hiding we can secure our data from hackers or intruders.

There are various ways of hiding data from unauthorized users like Cryptography, Watermarking and Steganography. These techniques ensure that embedded information into digital content cannot be easily detected. Cryptography is a technique with some protocol between sender and receiver where both of the parties agree on some encryption keys to communicate. These keys can be private or public. There are five primary functions of cryptography- Key exchange, Integrity, non-repudiation, authentication and confidentiality. The unauthorized users can see the coded data but they cannot derive any meaningful information by just seeing that coded data. In this cryptography we start with plain text. Plain text is changed to cipher text using encryption algorithms. And finally decryption is done to get back the same plain text. The types include – secret key cryptography, public key cryptography and hash functions.

Watermarking is a process in which the information is hidden into image or signals (videos or audios). This hidden information verifies the owner. There are two types of watermarking performed – visible and invisible watermarking. Watermarking can be performed on text, images, audio and videos

Steganography is a Greek word which means concealed writing. The word steganos means covered and graphia means writing. Thus, steganography is not only the art of hiding data but also hiding the fact of transmission of secret data over a network. Steganography hides the secret data in another file in such a way that only the recipient knows the existence of message.

Today's most of the people transmit the data in the form of text, images, video, and audio over the medium. Steganography usually deals with the way of hiding the secret data inside other data file. These other data files may be anything like, image, audio, video etc. It maintains secrecy between the communicating parties. Specifically talking about image steganography, secrecy is achieved by embedding data into the cover image and generating a stego-image. There are different types of steganography techniques each having their own merits and demerits.

Steganography main aim is to hide information inside a cover data in such a way that intruders are not able to detect the presence of the information. Unlike watermarking, steganography is not intended to prevent the hidden information by opponents or changing the hidden message, but it emphasizes on making the secret information undetectable.

There are various types of steganography that are used to hide the secret information into another information or signal. These are -:

A. Image Steganography

In this steganography technique image is used as cover image to hide the secret message. There are various image formats that are used like BMP, JPEG, TIFF, GIF, etc. and techniques used are LSB, spread spectrum, these techniques come under spatial domain techniques.
Another category is Transform domain which hides message in significant area of the cover image. DFT, DWT, DCT, etc. are some of the techniques used under transform domain.

B. Audio Steganography

The sender implants hidden information of any kind utilizing a key in a cover file to create a stego file, in such a way, that an intruder can't distinguish the presence of the hidden message. In many schemes strategy for audio steganography is performed by modifying the LSB. Along with LSB some more techniques are used like error diffusion, minimum error replacement and temporal masking effect.

C. Video Steganography

Videos are commonly an assortment of pictures and sounds, so the greater part of the introduced methods on image and audio can be applied to videos as well. The favorable circumstances of video are the amount of information that can be covered up inside is very large and also the way that it is a moving stream of images and audios. The video steganography is combination of image and audio steganography.

A digital image is described using a 2-D matrix of the color intestines at each grid point (i.e. pixel). Typically gray images use 8 bits, whereas colored utilizes 24 bits to describe the color model, such as RGB model. Bytes of pixels are sufficient to hold one message byte. And the remaining bits in the pixel remain the same. Steganography plays a crucial role in securing a secret message from unauthorized access by the changing the least significant bits in the pixel. This approach of modifying the least significant bits is known as LSB technique.
The LSB technique falls under spatial domain techniques, as they are simple and easy to implement. The Least Significant Bit (LSB) is one of the main techniques in spatial domain image Steganography. The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many

image formats is far greater than that perceivable by average human vision. Therefore, a modified image with some small variations in its colors will be indistinguishable from the actual one by a human being. In conventional LSB technique, this requires eight bytes of pixels to store 1byte of secret data.

EXISTING SYSTEM

The existing system in Image steganography, technique of hiding the data within the image called as cover image. It is done to prevent the secret message from unauthorized user. These cover images are called as Stego image which carry the confidential or secret message. The terminologies used in image steganography are:

a) Secret Message: This is the message which is to be hidden into the cover image.

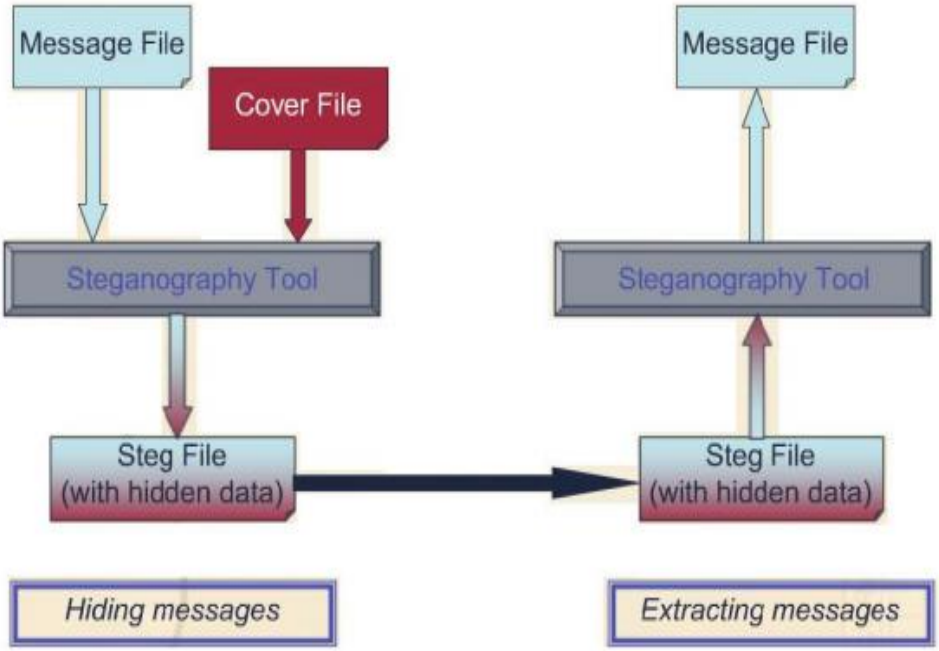
b) Cover Image: This is the image which is going to contain the secret message.

c) Embedding Algorithm: This is the actual technique which is used to hide the secret message into the cover image.

d) Stego Image: This is the output image when the embedding algorithm is applied. This is the image which is sent by sender.

Firstly, in encoding part (or hiding messages part), the secret message is encrypted with secret key, and then the encoding of the secret message takes place using various image steganography techniques. The output of the encoding part is taken, and is sent to the receiver.

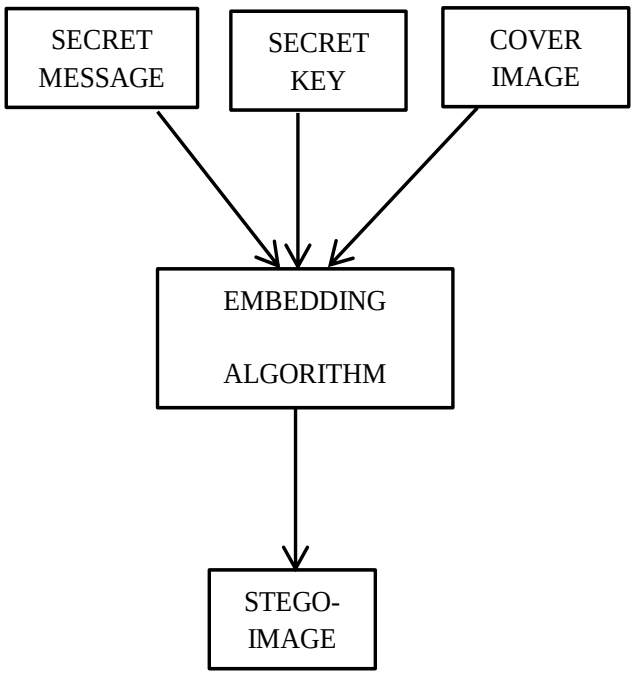
Decoding process (extracting message part) is performed at receiver side. In decoding part, message from the encrypted image (called as Stego image) is obtained by performing reverse of the technique used for encoding and then, the message is decrypted to obtain the original message using the secret key. The secret key used here must be same as the one which was used to encode the message.


Message File
Cover File
Steganography Tool
Steg File
(with hidden data)
Hiding messages
Message File
Steganography Tool
Steg File
(with hidden data)
Extracting messages

PROPOSED SYSTEM

The Proposed System here is Object Oriented Analysis. Object Oriented Analysis is basically the decomposition of the problem into its component parts and establishing a logical model to describe the system functions.
The proposed method is to develop an android application for image steganography which uses LSB technique to hide the secret message within the cover image. And the reverse of the algorithm is applied to extract the secret message. Most of the applications developed only hide the text inside the images. Moreover, in those applications, the text size allowed is not more than few words.
In this proposed work we can hide long text messages inside the cover images, and can also hide image inside another image. Also using these two features we can embed the secret message inside an image and then again hide that stego image inside a cover image. Some features of the application are as follows:

- Less distorted stego image
- Use of secret key
- Hiding text inside cover image
- Hiding image inside cover image

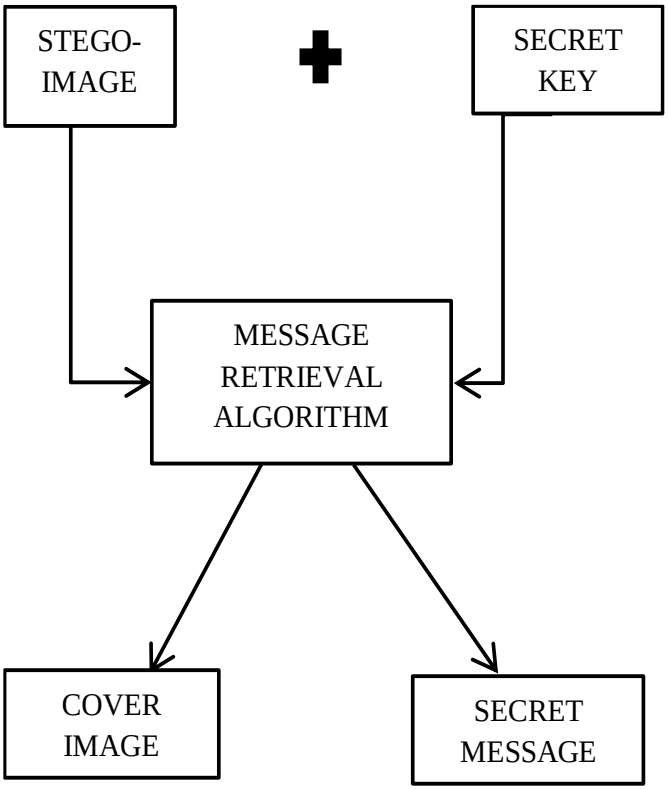


This above figure shows the process which takes place at sender side. Here the embedding of the message takes place. Along with the secret message we can also take an image to hide into a cover image. The output of the embedding

process gives image known to be stego image. The secret key used here plays an important role in the whole process.

The format of the stego image is same as that of the cover image used. And also the stego image generated here has less distortion due to which it is not very easy to detect just by seeing the stego image.

After the embedding process, the message retrieval phase takes place. Firstly, the image, called the stego image is sent to the receiver. The receiver uses the same key which was used to encrypt the message. The key used here works as condition checking. If the key used in the decoding part matches with the key used in the encoding part then the secret message or secret image, hidden inside the cover image will be retrieved otherwise not. The below figure shows the decoding phase:



IMPLEMENTATION

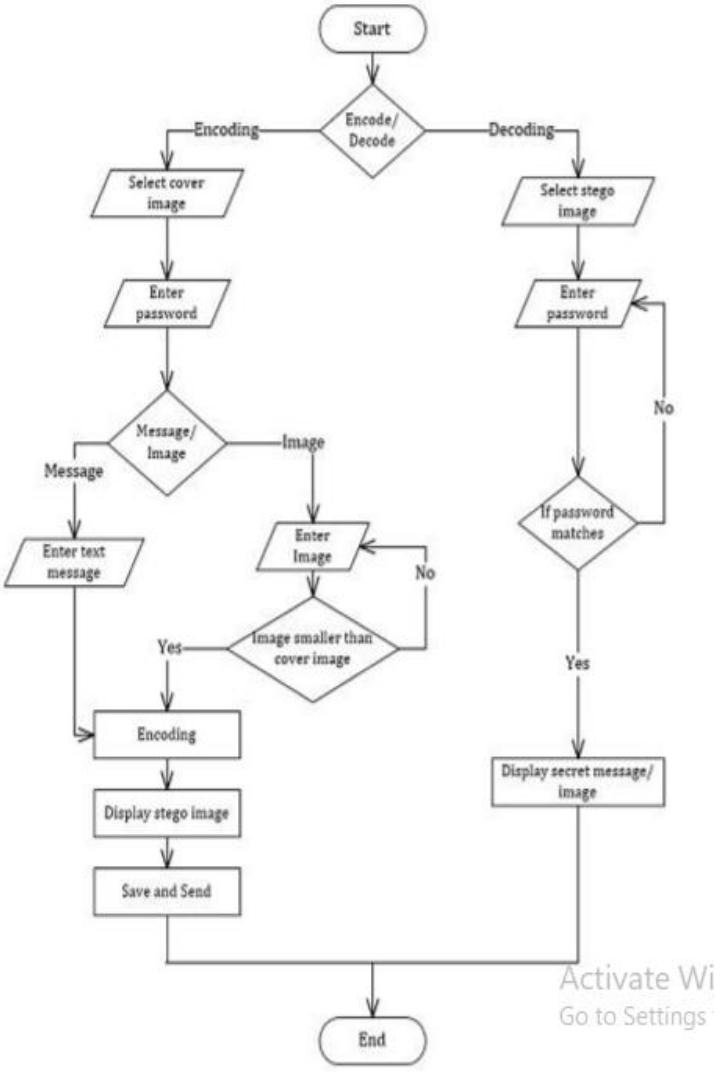
For implementation, the IDE used is:

- Android Studio

For testing the application, devices used are:

- Vivo V3 (Android version 5.1.1 lollipop)
- Redmi Note 7 Pro (Android version 9.0 Pie)

Design of the Application consists of two phases: Encoding phase and Decoding phase.



Brief Algorithm Implementation (working): The LSB is the most common used method in image steganography as it is easy to implement and generates a less

distorted images. The imperceptibility is high when LSB is used. Since every image has basically three components in it, i.e, RGB. This information about the pixel is stored in one byte in encoded format. The least significant bit which is having RGB information can be modified to hide the secret message.

The very first condition while hiding the text inside the cover image is that the text size should either be less or equal to the size of the cover image used. And same for the image i.e, the image to be hidden inside the cover image must be either less or equal to the size of the cover image used.

The embedding procedure:
Step 1: All Pixels of the cover image are extracted and are stored in some array.
Step 2: From the given text, extract all the characeters and store it in some another array.
Step 3: From the given secret key, which is in text format, extract characters and store it in other array.
Step 4 (If performing image encryption): Take the second image, extract all the pixels and store it in array.
Step 5: Take the pixel and characters from the secret key and put it in the least significant bit of the cover image.
Step 6: Use any symbol so as to indicate the end of the secret key.
Step 7: Take the message array put it in each pixel one by one by replacing it.
Step 8: Keep repeating step 6 till all the characters of the secret message have been placed inside the cover image.
Step 9: Put some symbol so as to detect the end of the data.

The decoding procedure:
Step 1: The secret key used during encryption will be used as a condition checking. If the key matches with the secret key already stored then the further process takes place else the application terminates.
Step 2: If the key matches, then the message retrieval algorithm will execute.
Step 3: The text embedded inside the image will be extracted. (Secret Image is also extracted if Image encryption option is chosen while encoding process.)

How the Application Works:

The first page has two options -:
- Encode
- Decode

1) ENCODE: Encoding has further three options
- Select Image to Encode: Fetches Cover image from Gallery of the phone.

And displays the selected image on the top.

- Text Encryption: This option allows writing the secret message or text along with the secret key
- Image Encryption: This option allows the sender to select another image which he/she wants to hide inside the cover image. Along with this selected image there are two more options, the secret key and the secret text. (The size of this image must be less or equal to cover image size).

2) DECODE: This options opens the page having stego images. The desired stego image is selected and right secret key is given to extract the message or message along with secret image.

OUTPUT

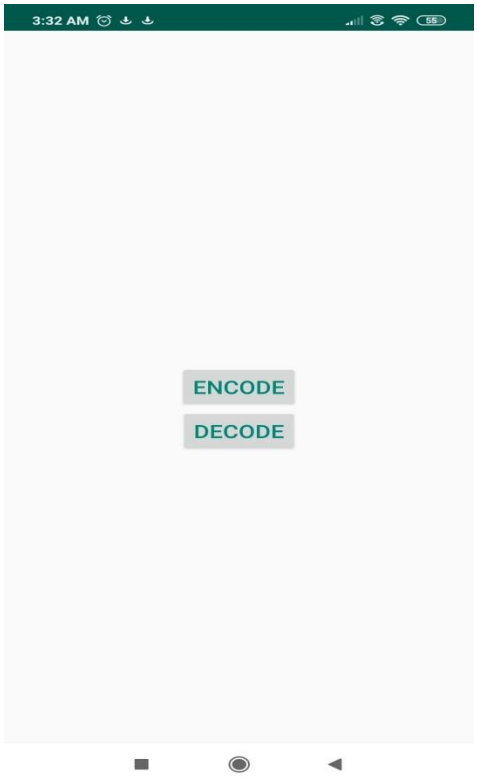


Figure1. Front Page of Application

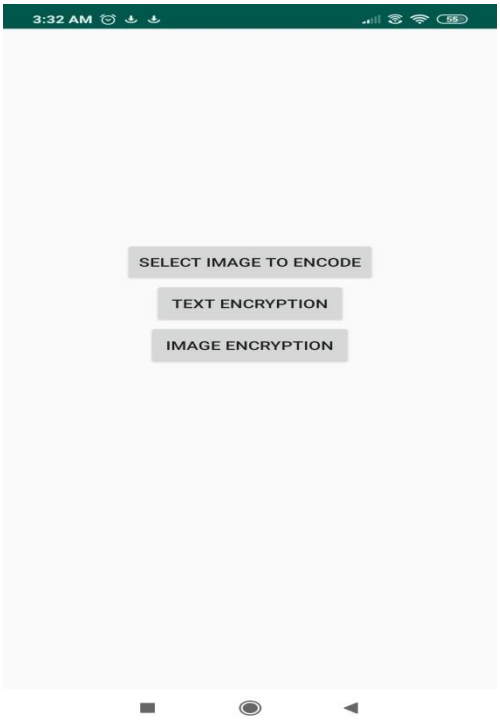


Figure2. Encode Options

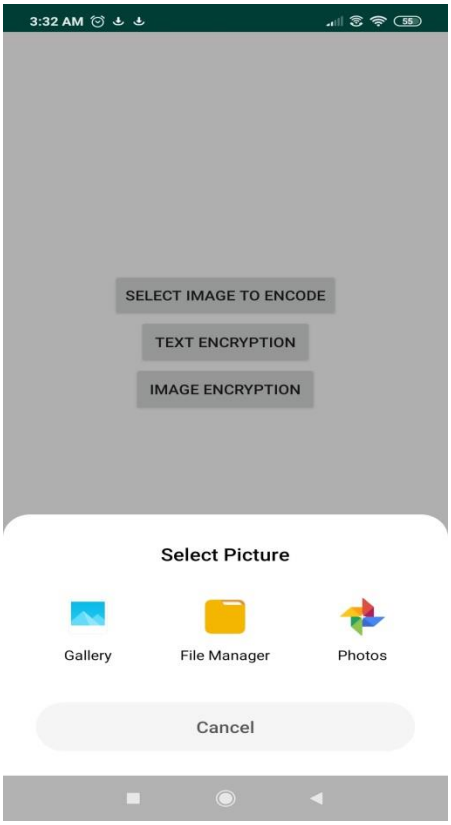


Figure3. Cover image selection choice

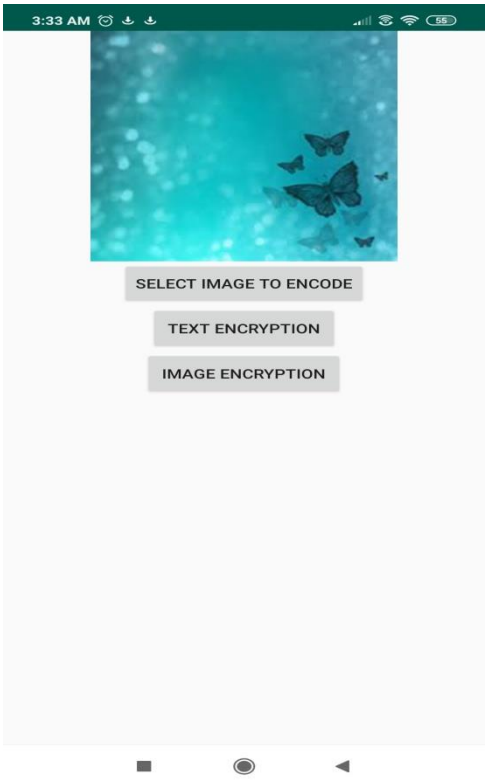


Figure4. Selected Cover Image

Figure5. Text Encryption page

Figure6. Secret Text with Secret Key

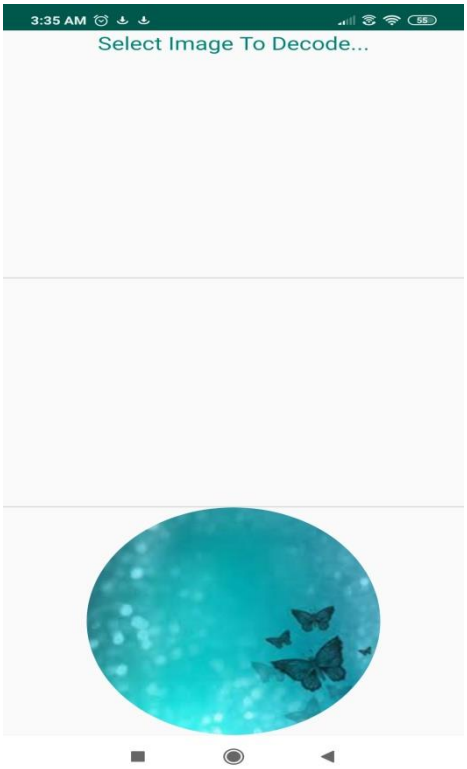


Figure7. Decode Page for selecting the stego image

Figure8. Secret key Request for message Retrieval

Figure9. Hidden message Retrieval of text encryption process

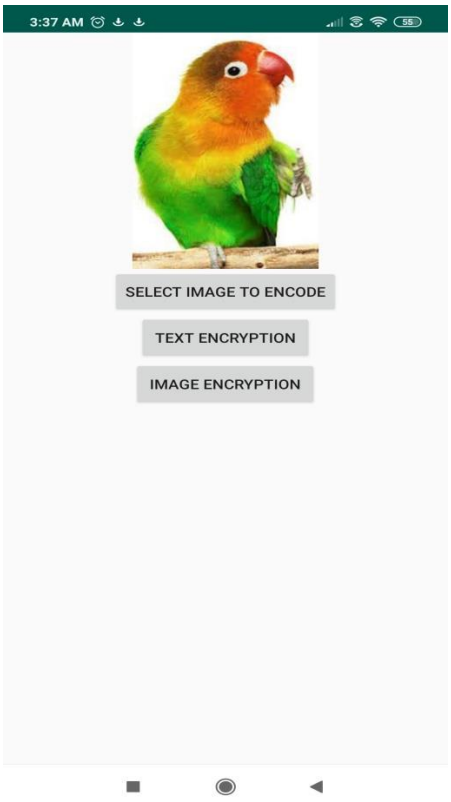


Figure10. Encode option with selected cover image

Figure11. Image Encryption Page

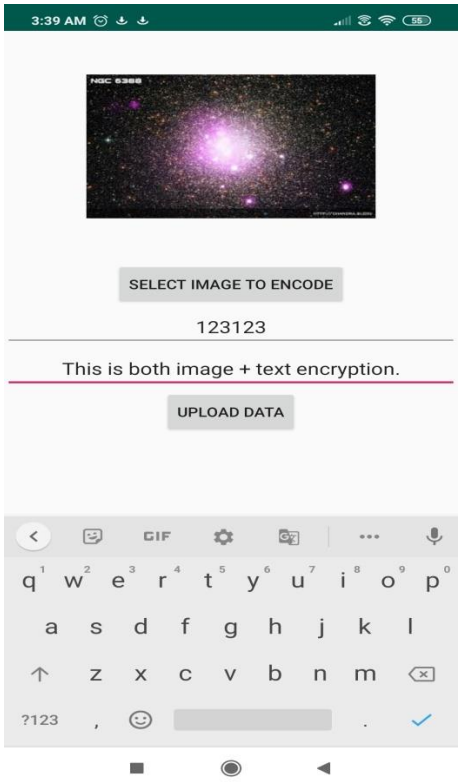


Figure12. Image selected to be hidden inside cover image along with key and secret text

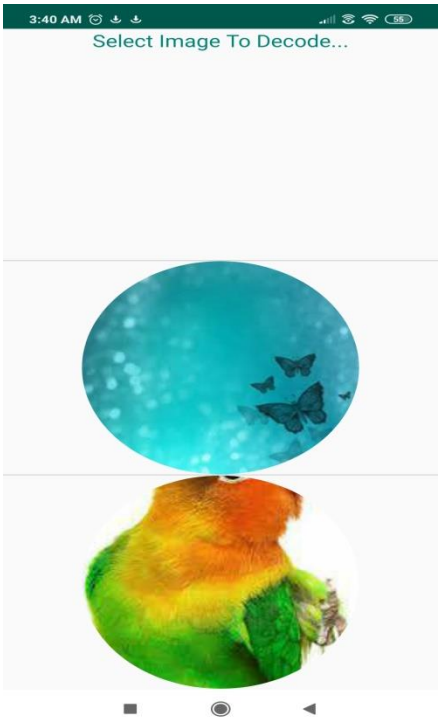


Figure13. Decode page for stego image selection after image + text encryption

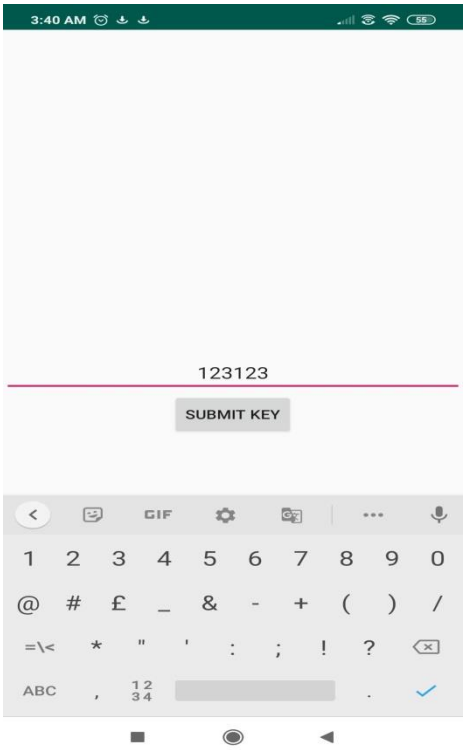


Figure14. Secret key request for both image + text decryption

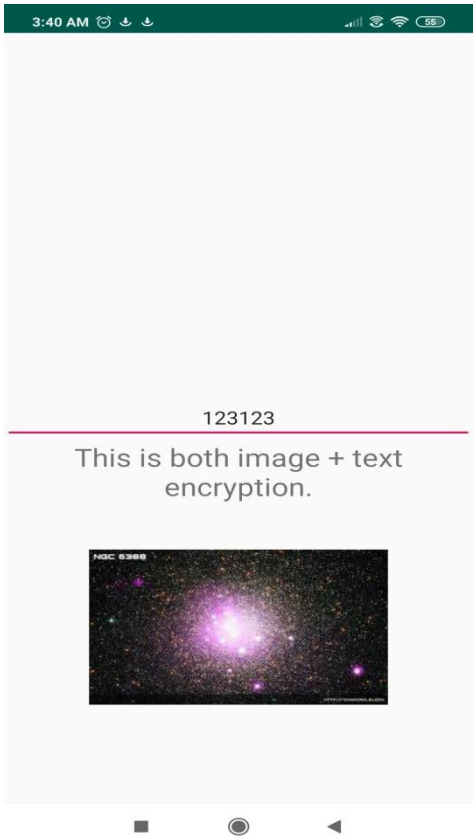


Figure15. Retrieval of both image and text with secret key

CONCLUSION

At the end, I would like to conclude that Image Steganography for hiding the secret information can be very useful in private conversation so that the secret information cannot be easily detected. The developed app adds more feature to the LSB technique used, making the proposed work more robust and allowing high imperceptibility to the stego image. The distortion in image is also negligible which shows the stego image is undetectable. Some of the Advantages of the proposed work are:

- Execution time is fast.
- Cover image can hold large size text.
- Image can be hidden inside cover image along with the text.
- Works smoothly on different android versions.

REFERENCES

1. Parmar Ajit Kumar Maganbhai, Prof. Krishna Chouhan, “A Study and literature Review on Image Steganography”, 2015, IJCSIT.
2. S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, “A New Approach for LSB Based Image Steganography using Secret Key”, (2011), ICCIT
3. S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, “A New Approach for LSB Based Image Steganography using Secret Key”, (2011), ICCIT
4. Ozcan Çataltaş, Kemal Tütüncu, “Improvement Of Lsb Based Image Steganography” (2017),
5. Odai M. Al-Shatanawi1 and Nameer N. El. Emam, “A New Image Steganography Algorithm Based On Mlsb Method With Random Pixels Selection” (2015), IJNSA
6. Rosziati Ibrahim and Teoh Suk Kuan, “Steganography Algorithm to Hide Secret Message inside an Image”, (2011),
7. Win Win Maw, San San Lwin, “Text Embedded System using LSB Method” (2019), IJTSRD