Digital Steganography

Dinesh Soni
Master student, Department of MCA, Jain Deemed-to-be University, Bengaluru, Karnataka, India

ABSTRACT

The mini project entitled "DIGATAL STEGANOGRAPHY" is explaining a technology of Steganography used to hide secret information within another file. In this project, we are hiding a secret file inside an image file. We are encrypting the text without using any secret code. The the Stegno-medium (picture with secret information) will be generated. This Stegno-medium is the final and expected output from the sender side. Anyone may get the picture (Stegno-medium) but only the intended person with the software can read the message. The main advantage of the project is that the user is not sharing any secret key to the receiver and hence is more safe option.

Keyword: - Steganography, Stegno-medium, Image Steganography, Secret Message, Cryptography, Encryption.

1. INTRODUCTION

Secrecy is very important in a large corporation. We have cryptography for transmitting secret data. Though cryptography is successful, and is helping to send secret information, it will attract hackers and it aims unintended users. The project is titled as Digital Steganography overcomes this drawback and provides a solution for sending secret data without affecting unintended users. We can include lengthy text information too. The project is developed using java as a programming language. It can be loaded through the command prompt. The application is simple and flexible and it also provides a user-friendly interface.
In this project, image file is used as Stegno-medium. In this project, we have two modules:

- Making Stegno-medium
- Getting secret information from Stegno-medium

2. STATEMENT OF PROBLEM

The problem statement of the project is to generate a solution to hide text in images. This can be done with both jpg and png images. The main aim is to send and receive secret messages without affecting unintended users.

3. SIGNIFICANCE

The project Digital Steganography gives a solution for transmitting secret information without affecting unintended users. Here we use pictures as covering medium. It may be received by anyone and it will not create any doubts for those who are not intended to receive.

4. REQUIREMENT SPECIFICATION

4.1 Hardware Requirements

- I7 Processor Based Computer
- 8GB - Ram
- 1TB GB Hard Disk

4.2 Software Requirements:

- Windows 10
- Java

5. PROPOSED SYSTEM

- The sender chooses an image file to hide a secret message.
- The sender can type a message in the text area provided.
- The message can be directly hidden into the image without using any secret key.
- This image can then be saved in desired location.
- The receiver can directly access the message with the help of the same software.

6. MODULES

In this project, we have two modules:

6.1 Making Stegno-medium

This module helps in hiding secret information within a multimedia file. Here, we are making use of an image file.

Fig: 1- Before Encoding

6.2 Getting secret information from Stegno-medium

This module helps in decoding the secret information from an encoded image file.

Fig: 2- After Encoding
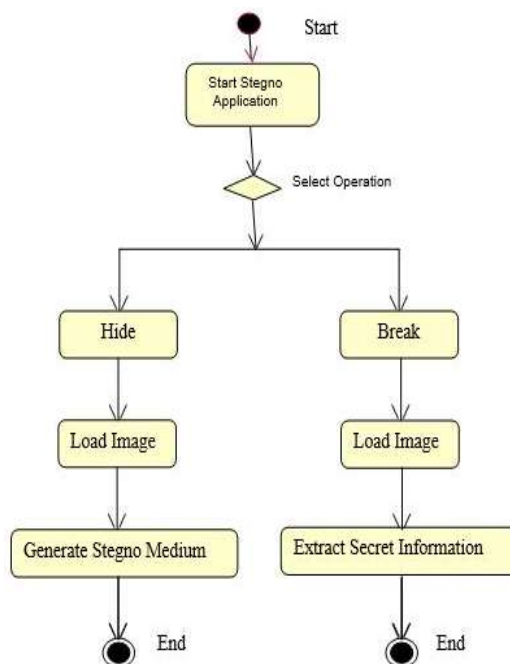
7. ACTIVITY DIAGRAM

Fig: 3- Activity Diagram

8. FUTURE ENHANCEMENTS

It can be enhanced so that it will support digital watermarking. Digital Watermarking is the concept of embedding some sort of information known as watermark within the digital data by its owner. Large variety of watermarking schemes are currently available.

Efforts can be done to make this project capable of escaping steganalysis. Steganography is the art of secret communication and steganalysis is the art of detecting the presence of hidden messages embedded in digital media using steganography.

9. CONCLUSION

To conclude, Mini Project "Digital Steganography" which has the Steganography concept is useful for hiding messages for transmission. The project is good in maintaining secrecy in communication of confidential and critical information. Here, image steganography is performed in which text can be hidden in picture. This is a fair technique that limits suspicion among unintended recipients. When properly implemented, steganography can be difficult to detect, but it is not impossible.

10. REFERENCES

[1] http://www.javaranch.com
[2] http://forum.java.sun.com
[3] http://java.sun.com
[4] http://www.javaworld.com