TABLE OF CONTENTS

CHAPTER NO.	TABLE	PAGE NO.
	ABSTRACT	iv
	LIST OF FIGURES	vii
	LIST OF ABBREVIATIONS	viii
1	**INTRODUCTION**	1
	1.1 OVERVIEW	1
	1.2 OBJECTIVE	2
	1.3 PROBLEM STATEMENT	2
2	**LITERATURE SURVEY**	3
	2.1 AN ANDROID APPLICATION FOR IMAGE STEGANOGRAPHY	3
	2.2 ANDROID APPLICATION FOR IMAGE STEGANOGRAPHY USING ANDROID STUDIO	4
	2.3 AN ANDROID-BASED IMAGE STEGANOGRAPHY SYSTEM FOR CONCEALING DATA AND IMFORMATION TRANSMISSION USING ADAPTIVE IMAGE STEGANOGRAPHY	5
	2.4 IMAGE STEGANOGRAPHY ANDROID APPLICATION ANDROID BASED IMAGE STEGANOGRAPHY	5
	2.5 ANDROID BASED IMAGE STEGANO GRAPHY	6
3	**SYSTEM STUDY**	8
	3.1 EXISTING SYSTEM	8
	3.1.1 Disadvantages	8

	3.2 PROPOSED SYSTEM	9
	3.2.1 Advantages	9
4	**REQUIREMENT SPECIFICATION**	10
	3.3 HARDWARE REQUIREMENTS	10
	3.4 SOFTWARE REQUIREMENTS	10
5	**PROJECT DESCRIPTION**	11
	5.1 MODULE DESCRIPTION	11
	5.1.1 Load The Image	11
	5.1.2 Analysis of The Image	11
	5.1.3 Creating Stego Image	11
	5.1.4 Storing Image	12
6	**ARCHITECTURE DIAGRAMS**	13
	6.1 SYSTEM ARCHITECTURE	13
	6.2 STEGANOGRAPHY METHOD AND RETRIEVING OF SECRET DATA	13
7	**CONCLUSION AND FUTURE ENHANCEMENT**	14
	7.1 CONCLUSION	14
	7.2 FUTURE ENHANCEMENT	15
	APPENDICES	16-34
	Source Code	16
	Screen Shots	33
	REFERENCE	35
	LIST OF PUBLICATIONS	36

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE NO.
5.1	Module Description	11
6.1	System Architecture	13
6.2	Steganography Method and Retrieving of Secret Data	13

LIST OF ABBREVIATIONS

RAM - Random Access Memory

ROM - Read Only Memory

LSB - Least Significant Bit

MLEA - Multi-Level Encryption Algorithm

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

Recently, the cost of information exchange has reduced significantly due to modern and state-of-the-art communication technologies and infrastructure. As a result of this improvements, the interpersonal communication has become very easy. However, if information are not protected, then criminals may exploit it during transmission. Therefore, along with the convenience it provides, this also creates excessive demand for verification and security sources; therefore, stressing the role of information security. For example, let us take the example of information exchange between government institutions and military. If some confidential information is openly posted online, it could be easily deciphered and exploited by criminals, thereby Jeopardizing the national security. Therefore, promising information protecting technology is essentially needed in addition to cryptography and steganography. In fact, Steganography has become more relevant in this situation. Steganography is mostly used to conceal hidden messages that would otherwise be difficult to detect. Nobody will be able to surmise that a secret message has been sent.

However, the current development in digitization has urged the creation of a huge measure of data. Putting away, sending, and sharing this secret data over an open and uncertain correspondence channel is, in fact, yet a perplexing test. Therefore, the cover steganography comes into the art of science by conveying restricted information in a suitable interactive media transporter, e.g., image, sound, and video records. In fact, this is the game of embedding secret information in a manner that no one or attacker can detect and read the secret data or information. The spatial domain techniques adjust the gray level of the cover image for concealing confidential information. A high payload and better result in stego-images can be obtained in spatial area procedures.

1.2 OBJECTIVE

The primary objective of image steganography is to hide sensitive information within images, audio, or other data files. Information concealment in images can be achieved through spatial or frequency domain methods. The main advantage of steganography algorithm is because of its simple security mechanism. Because the steganographic message is integrated invisibly and covered inside other harmless sources, it is very difficult to detect the message without knowing the existence and the appropriate encoding scheme.

1.3 PROBLEM STATEMENT

- A problem statement in steganography refers to the specific challenge or requirement the steganographer is trying to solve. Some common problem statements include:
- Concealing the Existence of a Message: This is the basic problem statement in steganography, where the task is to hide a message in another piece of information (e.g., an image, audio file, etc.) without leaving any visible signs that the message is there.
- Concealing the Existence of a Message From Specific Individuals or Groups: This problem statement involves hiding a message so that it can only be deciphered by specific individuals or groups who possess the necessary key or knowledge to decrypt it.
- Concealing the Existence of a Message and Providing a Level of Security: This problem statement involves hiding a message so that it can only be read by authorized parties and providing a level of security to protect the message from being read by unauthorized parties.
- Hiding Multiple Messages in a Single File: This problem statement requires the steganographer to hide multiple messages in a single file so they can all be retrieved later.

CHAPTER 2

LITERATURE SURVEY

2.1 Prasenjit Kar, Rajiv Kumar, Pradeep Kumar Mishra, Diwakar Gautam, Department of Computer Science & Engineering, School of Engineering & Technology Sharda University, Uttar Pradesh, India. "An android application for image steganography"

Image Steganography is widely used for hiding a message image into a cover image. This research domain is deployed at the commercial level at both government and private sector to exhaust its opportunities. In this article, we discuss a special steganography approach carried at android platform. The prime objective of this research is to shorten the gap between existing steganography approaches and its deployment for android based applications. The bit level information of a cover image is modified to include the message bits to generate a steganographic image. The experimental outcome of this generated android application file is promising regarding accessing speed and steganography process.

Disadvantages

Steganography can be detected if a Person has the right tools and techniques, so it is not a foolproof method of securing communication.

2.2 Dr. K. Jayasakthi Velmurugan, Ganesh S, Daniel Alfred Visuvasam W , Akash K R 1Associate Professor, Department of Computer Science and Engineering, Jeppiaar Engineering College, Chennai-600119. "Android Application for Image Steganography using Android Studio".

A literature survey is a summary of a set of related research. It selects information from papers, and organizes and integrates it into a logical justification. This section aims to report a study of researchers' preferences in selecting information from cited papers to include review, and the kinds of transformations and editing applied to the selected information. G. Prashanti and K. Sandhyarani have done survey on recent

achievements of LSB based image steganography. In this survey, authors discuss the improvements that enhance the steganographic results such as high robustness, high embedding capacity and undetectability of hidden information. Along with this survey two new techniques are also proposed. First technique is used to embed data or secret messages into the cover image and in the second technique a secret gray scale image is embedded into another gray scale image. These techniques use four state table that produce pseudo random numbers. This is used for embedding the secret information. These two methods have greater security because secret information is hidden on random selected locations of LSBs of the image with the help of pseudo random numbers generated by the table.

Disadvantages

The quality of the media should not noticeably degrade upon addition of a secret data

2.3 Sarumi, J.A. (PhD) Department of Computer Science Lagos State Polytechnic Ikorodu, Lagos Nigeria. "An Android-Based Image Steganography System for Concealing Data and Information Transmission Using Adaptive Image Steganography"

Watermarking and fingerprinting are closely related technologies to steganography, which are primarily concerned with the protection of intellectual property rights. Watermarking marks all the instance of an object in the same way. Watermarking signature contains the information hidden in the watermark, created to suggest the originality or possession for the aim of copyright. Fingerprinting embeds different unique mask in distinct copies of the carrier object that are supplied to different customers. With this, the copyright owner identifies the consumer that breaks or violates their licensing agreement by supplying the property to third parties. Cryptography is a technique used in securing the secrecy of transmitted information. It is hard enough to keep the contents of a message secret. Various strategies are developed in encrypting and decrypting in order to keep the knowledge secret. It may even be necessary to

keep the existence of information secret. Steganography is the technique employed to keep the knowledge of the existence of the user's information secret. With the need to communicate sensitive information or personal messages secretly to a particular target destination without the fear of the message being breached or intercepted by a malicious third-party, considering the security challenges posed to users over the internet and possible identity thefts, we are forced to take matters into our own hands and protect ourselves from malicious people. These means of protection need to be fast, very accessible and handy. Different steganography systems have been built on computer systems, (desktops, laptop) but there is also a need to have this system built on handheld devices, for ease of use. With the recent advancement in hardware and software capabilities of smart devices, we can use their speed and processing power to create a steganography system on such devices. This would enable information hiding to be faster and more accessible to users.

Disadvantages

Susceptibility to Data Loss: The hidden message may be lost or distorted during the transmission or Processing of the image, resulting in a loss of data.

2.4 Saurabh Yadav, Computer Science And Engineering, School Of Computing Science & Engineering. "Image Steganography Android Application".

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.

Disadvantages

Misuse: Steganography can be misused for illegal activities, including hiding malicious code or malware within an image, making it difficult to detect and Prevent cybersecurity attacks.

2.5 Pawan Sharma, Srishanth Shetty, Om Kadam, Prof. Ritusharma, Electronics And Telecommunication Atharva College Of Engineering, Mumbai, India. "Android Based Image Steganography".

There are various other data hiding techniques for different purposes and applications. These techniques are collectively known as 'information hiding' techniques. Some of these are namely steganography, cryptography; watermarking and fingerprinting are inter-linked to each other as well. Steganography also called 'Covered Writing' conceals very existence of hidden secret data in cover object whereas cryptography scrambles the data to prevent the attacker from understanding the contents. Steganography also used where cryptography is either not allowed or not to be used. Steganography and cryptography are complementary and orthogonal to each other and both can be used in combined form provide higher level of security. Watermarking is the process of embedding watermark signal into multimedia data to generate watermarked object to protect authenticity of owner on that digital object and mainly focuses on the robustness of embedded message rather than capacity or concealment. Since increasing capacity and robustness at the same time is not possible therefore watermarking can be used for copyright protection and

tracking legitimate use of a particular software or media. In fingerprinting, on the other hand, separate marks are embedded in the copies of the object that are supplied to different customers such as hidden serial numbers which enables the intellectual property owner to identify individuals who break their license agreement and supply the property to third parties. Steganography provides an ultimate guarantee of authentication that no other security tool can ensure. The primary goal of steganography techniques is to maximize embedding rate and minimizing the detect ability of the resulting stego images.

Disadvantages

Susceptibility to Data Loss: The hidden message may be lost or distorted during the transmission or Processing of the image, resulting in a loss of data.

CHAPTER 3

SYSTEM STUDY

3.1 EXISTING SYSTEM

There have been many techniques for hiding messages in images in such a manner that the alterations made to the image are perceptually indiscernible. However, the question whether they result in images that are statistically indistinguishable from unhampered images has not been adequately explored. There are various algorithms used to hide a message in an image. But, mostly in all the places the old algorithms are used. Which is not a huge problem, but as the technology develops, the latest algorithm must be used to not question the privacy of users. In today's advanced technological world, keeping the integrity, authenticity, security and confidentiality of the secret information over the internet is hot issues. Different techniques are proposed, but they do not fulfill the need of secret data due to the advancement of technologies. So new treats focus us to develop new methods. Therefore, steganography is the best method used today for sending and receiving using any communication channels through internet. Because, it hides the secret message in a particular manner such that no one can detect the hidden information. In this paper, we are having a novel and significantly improved steganographic approach which is used in the RGB color space.

3.1.1 *Disadvantages*

- One of steganography's disadvantages is that there is large overhead to hide very tiny amounts of information. Hiding short messages within wide text is limited by the size of the extensive text. Text files cleanly aren't big enough to cover more complex data like images or audio files.
- The biggest risk is the clash between an original image without the secret message and the steganated image with the secret message. Also, you could make cruel degradation of an image trying to analyze it.

3.2 PROPOSED SYSTEM

We look at some specific image-based steganography techniques and show that an observer can indeed distinguish between images carrying a hidden message and images which do not carry a message. We derive a closed form expression of the probability of detection and false alarm in terms of the number of bits that are hidden. This leads us to the notion of steganographic capacity, that is, how many bits can we hide in a message without causing statistically significant modifications? Our results are able to provide an upper bound on the capacity. Our ongoing work relates to adaptive steganographic techniques that take explicit steps to foil the detection mechanisms. And a much stronger algorithm is used to ensure the safety of the encrypted text in the image.

3.2.1 Advantages

- The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal.
- Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.
- This method featured security, capacity, and robustness, the three needed aspects of steganography that makes it useful in hidden exchange of information through text documents and establishing secret communication.

CHAPTER 4

REQUIREMENT SPECIFICATION

4.1 HARDWARE REQUIREMENTS

- Laptop.
- 8 GB RAM or Higher.
- 256 GB ROM or Higher.
- Processor Intel I5/ AMD Ryzen5 or Higher.
- Graphics Card 4 GB/Higher

4.2 SOFTWARE REQUIREMENTS

- Windows Operating System.
- Android Studio.
- Java.
- XML.

CHAPTER 5

PROJECT DESCRIPTION

5.1 MODULES

The following are the modules designed for this project

- Load the image
- 6 the image
- Creating stegno Image
- Store the image

5.1.1 Load The Image

This particular module is responsible for getting the image from a storage device such as memory card, pendrive and internal storage etc….

5.1.2 Analysis The Image

It is responsible for processing the image, plain text and analysing it for choosing the best steganography scheme such as 1LSB, 2LSB AND 4LSB ETC..,, If the number of character in the plaintext is larger than steganography scheme such as 3LSB or 4LSB will be selected. If the number of character in the plain text is minimum and the number of pixels in the image is large enough then the steganography scheme such as 1LSB or 2LSB will be selected.

5.1.3 *Creating Stego Image*

This module takes the cover image and it will alter the least significant bits of every pixel based on the bits in the secret text. In the end of the secret bits the respective pixel's and its next 10 pixel's LSB will be altered as zero. The destination image is the stego image.

5.2.4 Storing Image

This particular module is responsible for storing the image from a storage device such as memory card, pendrive and internal storage etc.

CHAPTER 6

ARCHITECTURE DIAGRAMS

6.1 SYSTEM ARCHITECTURE

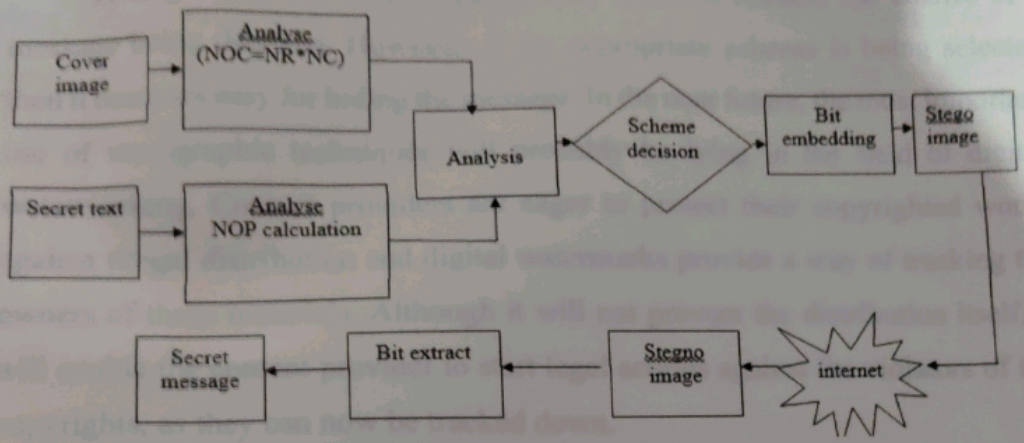


Figure 6.1: System Architecture

6.2 STEGANOGRAPHY METHOD AND RETRIEVING OF SECRET DATA

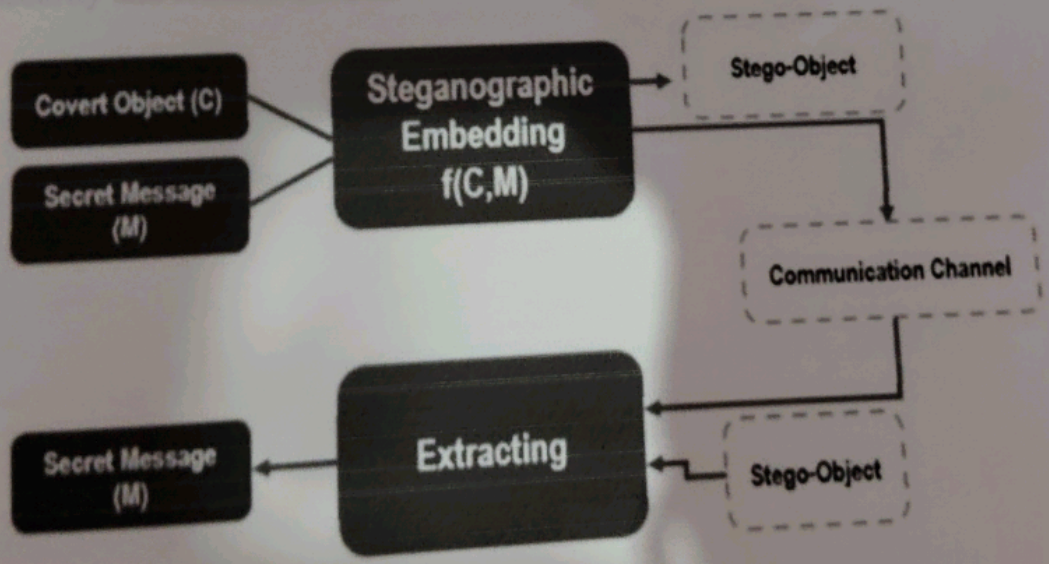


Figure 6.2: Steganography Method And Retrieving Of Secret Data

CHAPTER 7

CONCLUSION AND FUTURE ENHANCEMENT

7.1 CONCLUSION

Hiding a message with steganography methods reduces the chance of a message being detected. However, if the appropriate scheme is being selected then it becomes easy for hiding the message. In the near future, the most important use of stenographic techniques will probably be lying in the field of digital watermarking. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide a way of tracking the owners of these materials. Although it will not prevent the distribution itself, it will enable the content provider to start legal actions against the violators of the copyrights, as they can now be tracked down.

In this project we have discussed in detail about the steganography, security issues in computer networks and MPEG encryption. We have proposed a new scheme of selecting the suitable schemes which has many advantages. It improves the security and reduces the DD.

7.2 FUTURE ENHANCEMENT

The compression ratio of images can be improved. It can be extended to a level such that it can be used for the different types of image formats like bmp, jpeg, .tif etc. So other image formats also will come in use for Steganography. The security using least significant bit algorithm is good but in future it can be improved to a certain level by varying the carriers as well as using the different keys for encryption and decryption.

SOURCE CODE

Decode.java

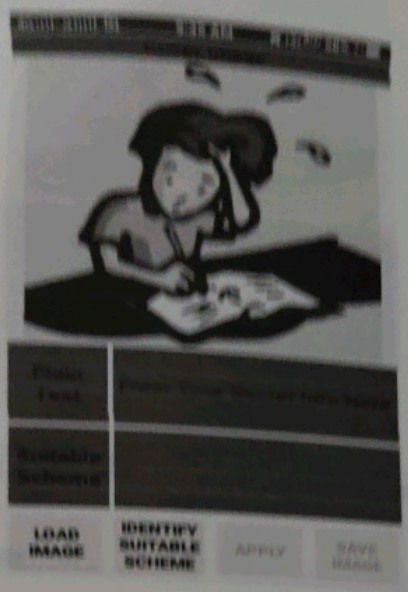
```
package com.ayush.steganography;

import android.content.Intent;
import android.graphics.Bitmap;
import android.net.Uri;
import android.os.Bundle;
import android.provider.MediaStore;
import android.support.v7.app.AppCompatActivity;
import android.util.Log;
import android.view.View;
import android.widget.Button;
import android.widget.EditText;
import android.widget.ImageView;
import android.widget.TextView;

import
com.ayush.imagesteganographylibrary.Text.AsyncTaskCallback.TextDecodingCallback;
import com.ayush.imagesteganographylibrary.Text.ImageSteganography;
import com.ayush.imagesteganographylibrary.Text.TextDecoding;

import java.io.IOException;
```

Cover Image



Scr No. 1: Cover Image

Secret Message

Scr No. 2: Secret Message

REFERENCES

[1] Amrutha C. V., Jyotsna C., & Amudha J, "Deep Learning Approach for Suspicious Activity Detection from Surveillance Video", 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), 2020.

[2] Amrutha C. V., Jyotsna C, "A Robust System for Video Classification: Identification and Tracking of suspicious Individuals from Surveillance Videos", International Conference On Soft Computing & Signal Processing, 2020.

[3] N. Krishnnan, S. Ahmed, T. Ganta and G. Jeyakumar," A Video Analytics Based Solution for Detecting the Attention Level of the Students in Class Rooms,"2020 10th International Conference on Cloud Computing, Data Science & Engineering, Noida, India, 2020.

[4] M. Awais et al., "Real-Time Surveillance Through Face Recognition Using HOG and Feedforward Neural Networks," in IEEE Access, vol. 7,2019.

[5] Nidhi Sharma, Manu Devi, "Improved Detection of Least Significant Bit

[6] Steganography Algorithms in Color and Gray Scale Images," Proceedings of 2014 RAECS UIET Panjab University Chandigarh,06- 08, March 2014.

[7] Padmini.K, Champakamala .B.S, Radhika .D. K Asst Professors, Department of TCE, Don Bosco Inst-itute of Technology, Bangalore, "Least Significant Bit algorithm for image steganography"India International Journal of Advanced Computer Technology(IJACT), Volume 3,Number 4.