Steganography with Google Recognizer

Shailja Dubey[1] Shivani Porwal[2] Vartika Khaddar[3] Prof. Kavita Namdev[4] Prof. Deepika Jain[5]
[4]Project coordinator [5]Project Guide
[1,2,3,4,5]Acropolis Institute of Technology and Research, Indore, MP, India

Abstract— The main aim of this research paper is to contribute our knowledge and services to the society. The steganography with google recognizer will help the person by providing more convenient means of life. the goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present." Steganography includes a vast array of techniques for hiding messages in a variety of media. Among these methods are invisible inks, microdots, digital signatures, covert channels and spread-spectrum communications. Today, thanks to modern technology, steganography is used on text, images, sound& signals. The advantage of steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered. Often, using encryption might identify the sender or receiver as somebody with something to hide. For example, that picture of your cat could conceal the plans for your company's latest technical innovation.

Keywords: Least significant algorithm, secret key, image processing, data retrieval, image steganography, security, visual quality

I. INTRODUCTION

Data hiding is of importance in many applications. For hobbyists, secretive data transmission, for privacy of users etc. the basic methods are: Steganography and Cryptography. Steganography is a simple security method.

Generally, there are three different methods used for hiding information: steganography, cryptography, watermarking. In cryptography, the information to be hidden is encoded using certain techniques; this information is generally understood to be coded as the data appears nonsensical.

Steganography is hiding information; this generally cannot be identified because the coded information doesn't appear to be abnormal i.e. its presence is undetectable by sight. Detection of steganography is called Steganalysis.
Steganography is of different types:

- Textsteganography
- Imagesteganography
- Audiosteganography
- Videosteganography

In all of these methods, the basic principle of steganography is that a secret message is to be embedded in another cover object which may not be of any significance in such a way that the encrypted data would finally display only the cover data. So, it cannot be detected easily to be containing hidden information unless proper decryption is used.

II. LITERATURE SURVEY

Johnson, N. and Jajodia S. [34] This article explores the different methods of steganography such as LSB, Masking and Filtering and also explains about different software tools present in the market for Steganography, such as Stego Dos, White Noise Storm, S-tool etc.

Marvel et al. [38] It is proposed that (Spread Spectrum Image Steganography) SSIS is a blind scheme where the original image is not needed to extract the hidden information unless the receiver possesses the secret key to extract the secret message, otherwise it is virtually undetectable. Thus, making this technique reliable and secure.

Jessica Fridrich et al.[32] This paper proposes a highly accurate steganalysis technique which can even estimate the length of secret message embedded in LSB method. In this method, the test image is divided into groups of n consecutive or disjoint pixels. This method exploits the modified pixel values to determine the content of secret message.

Tseng, Y.C et al. [63] This paper presents a secure steganographic scheme which makes sure that if any modified bit in the cover image should be adjacent to another bit that has the same value as the former's new value. By this way the detection becomes extremely difficult. But for achieving this, data hiding space has to be reduced.

Da-Chun Wu, and Wen-Hsiang Tsai [23] proposed a differencing steganographic method that uses the difference between two consecutive pixels in the same block to determine the number of secret bits to be stuffed. In this method a range table is used which ranges from 0-255. The difference value is subsequently adjusted to the difference in the same range to embed the secret bits, and the difference between the original difference value and the new one is shared between the two pixels. Extraction scheme in this method is quite simple and it do not require cover image.

Sorina Dumitrescu et al.[55] This paper proposes a new steganalysis technique to detect LSB steganography in digital signals such as image and audio. This technique is based on statistical analysis of sample pairs. By this technique the length of hidden message embedded via LSB steganography can be estimated with high precision.

III. RESEARCH METHODOLOGY

Basically, we divide our project in four significant parts. Every part of this this project is connected to each other.

A. Image Steganography

Image Steganography refers to the process of hiding data within an image file. The image selected for this purpose is called the cover-image and the image obtained after steganography is called the stego-image.

In image steganography, a message is embedded into an image by altering the values of some pixels, which are chosen by an encryption algorithm. The recipient of the image must be aware of the same algorithm in order to

known which pixels he or she must select to extract the message.

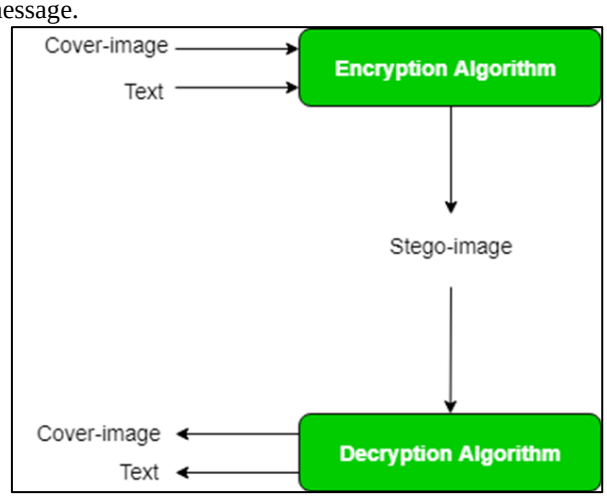

Fig. 1: process of image steganography

B. *Audio Steganography*

Audio Steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner. It is the science of hiding some secret text or audio information in a host message. The host message before steganography and stego message after steganography have the same characteristics.

C. *Video Steganography*

Video Steganography is a technique to hide any kind of files into a cover Video file. The use of the video-based Steganography can be more secure than other multimedia files, because of its size and complexity.

D. *Text Steganography*

Text steganography is a mechanism of hiding secret text message inside another text as a covering message or generating a cover message related with the original secret message.

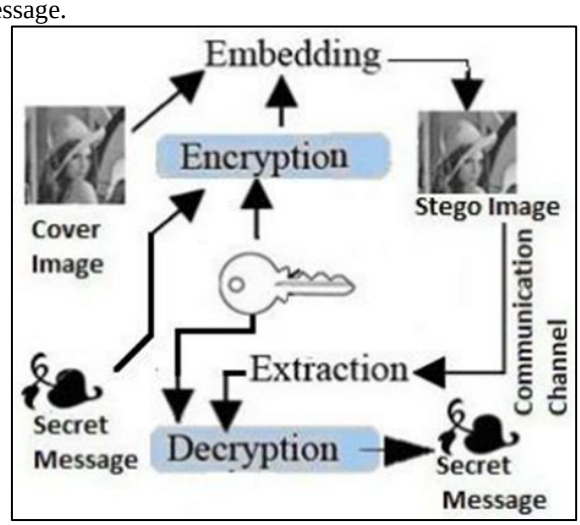

Fig. 2: process flow diagram

IV. Results

The image steganography is one which helps its dwellers in making their day to day life easier. By our application, we can attain the following features:

- To provide better and efficient service.
- To Reduce the threat of information transmission.
- To encode the confidential message into image.
- To decode the message from image.
- Implemented video and audio steganography.

V. Conclusion

Our proposed work investigates that steganography enhancement by combining text and image through least significant bit (LSB) falls into several categories viz. the strict way to choose the secret message such as text, cipher text, text-image and biometrics data to be embedded into the media content. The proposed system uses LSB technique which is employed for the data embedding, which doesn't change the content of the media. Then the reversible data hiding algorithms have been further studied so as to perform the extraction without information loss for the purpose of security and robustness. The robustness of the system has been evaluated through various attacks on Stango-object such as compression, cropping, filtering, and noisy transmission… etc., cause the original information to belost.

References

[1] Fundamentals of Android by L.Morphey.
[2] School of Computer & Software, Nanjing University of Information Science & Technology, Nanjing210044.
[3] Key Laboratory of Meteorological Disaster of Ministry of Education Nanjing University of Information Science & Technology, Nanjing210044.
[4] Krithi P1, Dr M Ramakrishna2 ,PG Student1, Professor 2,1,2 Computer Science and Engineering, Vemana Institute of Technology,Bangalore-34.
[5] Mona Institute of Applied Science, University of West Indies, Kingston, Jamaica salbogleprogmer@gmail.com 2Computing & Information Applications, Institute Technology Brunei, Brunei 3Department of Computing, University of West Indies, Kingston,Jamaica.
[6] Review on Android and Smartphone Security Tiwari Mohini, Srivastava Ashish Kumar and Gupta Nitesh NRI Institute of Information Science and Technology, Bhopal,Madhya Pradesh,INDIA.
[7] "Programming Android Java Programming for the New Generation of Mobile Devices" by Zigurd Mennieks , Laird Dornin , G. Blake Meike ,& Mausmi Nakamura.
[8] "Hello, Android Introducing Google's Mobile Development Platform" by Ed Burnette.
[9] "Learning Android Building Applications for the Android Market" byMarko.

