

# Table of Content

# Chapter no. Title Page Numbers

# Table of Content 2

# Abstract 3

# Keywords 3

# Introduction 3

# Image Steganography 4

# Audio Steganography 4

# Video Steganography 4

# Text Steganography 5

# Literature Survey 5

# Spatial Domain Techniques 5

# Transform Domain Techniques 6

# Problem Statement 7

# Conclusion 7

# References 8

# Abstract:

Nowadays, computer-based communications are at the threshold of making life easier for everyone in the world; from sharing information, to communicating with each other, to exchanging electronic documents, and to checking bank balances and paying bills. Nonetheless, information security is an essential factor, which must be taken into consideration to ensure secure communications. There are significant interests in security approaches that aim to protect information and digital data, since the growing increase in uses of the internet and multimedia, have raised the interests in image steganography in order to secure and protect them. In this paper, a detailed literature review on a variety of different methods, algorithms, and schemes in image steganography is conducted in order to analyse and investigate them. In addition, this research summarized a comparative literature review for these researches and presented into a table, which involves a research name, broad domain, research methodology, advantages, disadvantages, and the evaluation method.

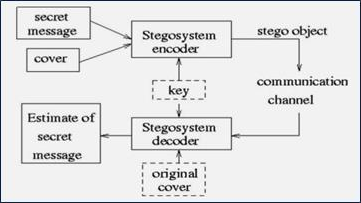
# Keywords:

Image Steganography, Data Hiding, Image Steganography Techniques, Data Embedding and Extracting.

# Introduction:

Steganography is defined as the science and art of concealing a secret message in different files types, for instance: digital images files, digital audio files, digital video files, and text files. Steganography

word is composed of two Greek words, namely: Stegano and Graphy. The word Stegano means a Covered, whereas Graphy means Writing. Therefore, steganography means a Covered Writing. Steganography is compared to Cryptography is that Cryptography scrambles a message so it cannot be understood, while steganography hides the message so it cannot be seen. Steganography is a form of security technique through obscurity, the science and art of hiding the existence of a message between sender and intended recipient.



Steganography is classified into four types as follows:

# Image steganography:

It is a process of concealing the secret image inside the cover image in such a way that the existence of the secret image is disappeared and the cover image seems to be original.

# Audio steganography:

Digital sound files are used to hide a secret message by vaguely changing the binary sequence of a sound file, which is known as audio steganography.

# Video steganography:

Video files can be defined as a collection of images and sounds combined together, thus, most of the introduced images and audio

can be used and applied to the digital video files. In fact, large amount of secret data that can be embedded inside the video files, since the video file is a moving stream of images and sounds.

# Text steganography:

Text steganography basically refers to the information that is hidden in text files. The text steganography includes everything from manipulating and changing text formatting, word changing within the text, producing and generating random sequences or using context-free language grammars to generate readable texts.

# Literature survey:

Steganographic techniques are categorized into two broad domains as follows:

# Spatial Domain Techniques:

In spatial domain techniques, carrier object pixels, like image and video objects, are directly manipulated and changed in order to hide secret data inside it. The following techniques belong to spatial domain:

# Least Significant Bit (LSB):

Least Significant Bit (LSB) is a simple strategy for implementing steganography. Such as all steganographic methods, it embeds the data into the cover, so that it cannot be detected by a casual observer. The technique works by replacing some of the information in a given pixel with information from the data in the image. Normally, An LSB algorithm replaces the most-right bits of a cover files bytes. In case a bit of the cover image C(i,j) is equal to the bit of a secret massage (SM) that to be embedded, C(i,j) stay untouched, otherwise C(i, j) is set to bit of a secret massage (SM). For instance, the letter 'C' is an ASCII code of 67 in decimal, which is 01000011 in binary, and bits of the image pixels before the hiding(embedding) a secret message are:

Pixel 1: 11111000 11001001 00000011

Pixel 2: 11111000 11001001 00000011

Pixel 3: 11111000 11001001 00000011

Least Significant Bit (LSB) algorithm hides (embeds) bits of letter 'A', which are 01000001, into image pixels to produce: Pixel 1: 11111000 11001001 00000010

Pixel 2: 11111000 11001000 00000010

Pixel 3: 11111001 11001001 00000011

# Gray-Level Modification (GLM):

Gray level Modification (GLM) is defined as a technique in which the grey level values of the image pixels are modified in accordance with a mathematical function to represent binary data. Each pixel has a distinct grey level value which can have an odd or even value. This odd or even value of the grey level is appropriately modified to represent binary data.

# Pixel Value Differencing (PVD):

Pixel-value differencing (PVD) scheme uses the difference value between two consecutive pixels in a block to determine how many secret bits should be embedded. It provides high imperceptibility to the stego image by selecting two consecutive pixels and designs a quantization range table to determine the payload by the difference value between the consecutive pixels. Besides, it offers the advantage of conveying a large number of payloads, while still maintaining the consistency of an image characteristic after data embedding.

# Transform Domain Techniques:

In transform domain techniques, the carrier object is first transformed from spatial domain to transform domain, and then its frequencies are used to hide the secret data. After embedding the secret data, the object is again transformed into spatial

domain. These techniques have lower payload but are robust against statistical attacks:

# Discrete Wavelet Transform (DWT):

The DWT transform is defined as accomplishment of the wavelet transform that utilizes translations following defined rules and a discrete set of the wavelet scales.

# Discrete Fourier Transform (DFT):

This transform is considered the most important discrete transform used to carry out Fourier analysis in numerous practical applications. The samples can be the values of pixels along a row or column of a raster image in image processing.

# Discrete Cosine Transform (DCT):

This transform articulates a fixed sequence of data points in sense of a sum of cosine functions that are fluctuating at several frequencies. DCTs are important to various applications in engineering and science such as, lossy audio compression like MP3 files, and images like JPEG files wherever little high- frequency components are rejected. In fact, uses of cosine instead of sine functions is significant for compression, since smaller amount of cosine functions are required to estimate a normal signal.

# Problem Statement:

Steganography hides the very existence of a message so that if successful it generally attracts no suspicion at all. Using steganography, information can be hidden in carriers such as images, audio files, text files, videos and data transmissions.

# Conclusion:

This paper presented a detailed literature review on a variety of different methods, algorithms, and schemes in image steganography area in order to analyze and investigate them.

# REFERENCES:

* + S. Kurane, H. Harke, and S. Kulkarni, “TEXT AND AUDIO DATA HIDING USING LSB AND DCT A REVIEW APPROACH,” Natl. Conf. “Internet Things Towar. a Smart Futur. “Recent Trends Electron. Commun., 2016.
  + E. Nandhini, M. Nivetha, S. Nirmala, and R. Poornima,

“MLSB Technique Based 3D Image Steganography Using AES Algorithm,” J. Recent Res. Eng. Technol. ISSN, vol. 3, no. 1, p. 2936, 2016.

* + A. Hasan, “Computer Security,” 2010. [Online]. Available: [http://www.contrib.andrew.cmu.edu/~aishah/Sec.html.](http://www.contrib.andrew.cmu.edu/~aishah/Sec.html)
  + J. Talbot and D. Welsh, “Complexity and Cryptography,” pp. 1–9, 2006.
  + Sarciszewski, “Guide to Cryptography,” 2015.