ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# SURVEY PAPER ON STEGANOGRAPHY

**Tejaswini Vyas*, Aditi Sharma**

* Computer science & engineering, acropolis institute of technology & research, (m.p.), india
Computer science & engineering, indore institute of science & technology, indore (m.p.), india

**DOI**: 10.5281/zenodo.218912

## ABSTRACT

Now a day's security is one of the prime factors while communicating on the network. Lakhs of peoples are actually using internet and share their information with each other. In such a scenario it becomes necessary that only intended person will fetch and read the confidential matter. Steganography is one of the way through which you can hide your data (Text form) into image or video. So that if any person has that image they cannot understand the information easily. In this paper, we will study about the steganography and cryptography.

**KEYWORDS:** Data hiding, steganography, cryptography.

## INTRODUCTION

Steganography is a Greek word which means concealed writing. The word "steganos" means "covered " and "graphical " means "writing" . Thus, steganography is not only the art of hiding data but also hiding the verity of transmission of secret data. Steganography hides the secret data in another file in such a way that only the recipient knows the existence of message. In ancient time, the data was protected by hiding it on the back of wax, writing tables, and stomach of rabbits or on the scalp of the slaves. But today's most of the people transmit the data in the form of text, images, video, and audio over the medium. In order to safely transmission of confidential data, the multimedia object like audio, video, images are used as a cover sources to hide the data [3].

Although steganography is an ancient subject, the modern formulation of it is often given in terms of the prisoner's problem proposed by Simmons [5], where two prisoners wish to communicate in secret to originate an escape plan. All of their communication passes through a warden who will throw them in solitary imprisonment should she suspect any covert communication [6]. The warden, who is free to examine all communication exchanged between the prisoners, can either be passive or active. A passive warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An active warden, on the other hand, will try to alter the communication with the suspected hidden information deliberately, in order to remove the information [4].

## LITRATURE SURVEY

In [7] this research paper, researchers have introduced a high capacity of hidden data utilizing the LSB (Least Significant Bit) and hybrid edge detection scheme. In this paper, he has used two types of canny and fuzzy computation edge detection method and with that the simple mechanism of substituting LSB to embed the hidden data. For edge computation two types of canny and fuzzy edges detection method applied and simple LSB substitution is used to embed the hidden data. This scheme is successful to embed data with higher peak signal to noise ratio (PSNR) with normal LSB based embedding. The proposed scheme is tested on limited images dataset. Madhuet al., in [8] proposed an image steganography method, based on LSB substitution and selection of random pixel of required image area. The method is firstly targeted to improve the security by adding password using LSB of pixels. By generating the random numbers set, it selects the region where we need to hidden the secret message. In [9] proposed an image steganography method of mapping pixels to alphabetic letters. It maps the 32 letters (26 for English alphabetic and other for special characters) with the pixel values. Five (5) bits are required to represent these 32 letters and authors have generated a table where 4 cases design to represent these 32 letters. According to that table, each letter can be represented in all 4 cases. It utilizes the image 7 MSB (Most Significant Bits) (27

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

= 128) bits for mapping. Proposed method maps each 4-case from the 7 MSB's of pixel to one of the 32 -cases in that table. These 4-cases increase the probability of matching. This algorithm keeps the matching pattern of cover-image which is then used for extracting data from the stego-image. Proposed method does not required any edge or smoothness computations but secret data should be in the form of text or letter for embedding.
In [10], authors have introduced a data hiding technique where it finds out the dark area of the image to hide the data using LSB. It converts it to binary image and labels each object using 8 pixel connectivity schemes for hiding data bits. This method required high computation to find dark region its connectivity and has not tested on high texture type of image. Its hiding capacity totally depends on texture of image. Babitaet al., in [11] uses 4 LSB of each RGB channel to embed data bits, apply median filtering to enhance the quality of the stego image and then encode the difference of cover and stego image as key data. In decoding phase the stego image is added with key data to extract the hidden data. It increases the complexity to applying filtering and also has to manage stego-key. Proposed scheme has high secret data hiding capacity.

## TYPES OF STEGANOGRAPHY

**Text Steganography:**
There are numerous methods by which to accomplish text based Steganography. I will introduce a few of the more popular encoding methods below.

**Line-shift encoding** involves actually shifting each line of text vertically up or down by as little as 3 centimeters. Depending on whether the line was up or down from the stationary line would equate to a value that would or could be encoded into a secret message.

**Word-shift encoding** works in much the same way that line-shift encoding works; only we use the horizontal spaces between words to equate a value for the hidden message. This method of encoding is less visible than line-shift encoding but requires that the text format support variable spacing.

**Feature specific encoding** involves encoding secret messages into formatted text by changing certain text attributes such as vertical/horizontal length of letters such as b, d, T, etc. This is by far the hardest text encoding method to intercept as each type of formatted text has a large amount of features that can be used for encoding the secret message.

**Image Steganography:**
Hiding the data by taking the cover object as image is referred as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital representation of an image. Coding secret messages in digital images is by far the most widely used of all methods in the digital world of today? This is because it can take advantage of the limited power of the human visual system (HVS). Almost any plaintext, cipher text, image and any other media that can be encoded into a bit stream can be hidden in a digital image. With the continued growth of strong graphics power in computers and the research being put into image based Steganography, this field will continue to grow at a very rapid pace.

**Audio Steganography:**
It involves hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography. These methods are i) Low Bit Encoding ii) Phase Coding iii) Spread Spectrum.

## APPLICATIONS OF STEGANOGRAPHY

1. Confidential Communication and Secret Data Storing
2. Protection of Data Alteration
3. Access Control System for Digital Content Distribution
4. E-Commerce
5. Media
6. Database Systems
7. Digital watermarking.

## CONCLUSION

This paper gave an overview of different steganography techniques its major types and classification of steganography which have been proposed in the literature during last few years. We have critical analyzed different proposed techniques which show that visual quality of the image is degraded when hidden data increased up to certain limit using LSB based methods. And many of them embedding techniques can be broken or shows indication of alteration of image by careful analysis of the statistical properties of noise or perceptually analysis.

## REFERENCES

[1] A.Joseph Raphael,Dr.V Sundaram, Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630
[2] I. Venkata Sai Manoj, "Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887), Volume 1 – No.12
[3] Jasleen Kour , Deepankar Verma , International Journal of Emerging Research in Management & Technology ISSN: 2278-9359 (Volume-3, Issue- 5)
[4] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998 Simmons, G., "The prisoners problem and the subliminal channel", CRYPTO, 1983
[5] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.
[6] W. J. Chen, C. C. Chang and T. H. N. Le, "High Payload Steganography Mechanism Using Hybrid Edge Detector", Expert Systems with Applications (ESWA 2010), vol. 37, pp. 3292-3301, (2010) April 4.
[7] V. MadhuViswanatham and J. Manikonda, "A Novel Technique for Embedding Data in Spatial Domain", International Journal on Computer Science and Engineering, IJCSE, vol. 2, (2010).
[8] M. A. Al-Husainy, "Image Steganography by Mapping Pixels to Letters", Journal of Computer Science, vol. 5, no. 1, (2009), pp. 33 -38.
[9] H. Motameni, M. Norouzi, M. Jahandar and A. Hatami, "Labeling Method in Steganography", World Academy of Science, Engineering and Technology, France, (2007).