AN OVERVIEW OF IMAGE STEGANOGRAPHY TECHNIQUES

[1]Vaibhav Singh Shekhawat, [2]Dr. Manish Tiwari and [3]Dr. Mayank Patel

[1]M.Tech Student, Department of CSE, GITS, Udaipur (Raj), India
[2]Assistant professor, Department of CSE, GITS, Udaipur (Raj), India
[3]Associate Professor, Department of CSE, GITS, Udaipur (Raj), India.

Abstract: Hiding information is one of the techniques used to change hidden facts and can be defined as the study of invisible communication that generally offers with strategies of concealing the presence of a dispatched message. In this way, if the message is accessed, the message does not appeal to the attention of eavesdroppers or attackers. With Hide Information, records can be hidden in unique embed media, called arguments. These media can be images, audio files, video files, and textual content files. In this paper, we present the overview of data or image hiding that called stenography. In this paper an image file is used as support, and therefore a classification of current information masking techniques for image files has been provided. These techniques are analyzed and discussed not only in terms of the ability to hide information in image files, but also in terms of the amount of information that can be withheld and the power of various image processing attacks.

Keywords: Steganography, Text, Information Hiding, Data Security, Steganalysis, Secrete Image, Cover Image.

I. INTRODUCTION

The idea of hiding information is not new in the story. Early in ancient Greece, attempts to hide a message in the authoritative media had tried to get it across enemy territory. In the modern digital communications world, quite a few methods are used to conceal data on any medium. One of these methods is to hide records in which digital pictures are primarily used as media to disguise information; information in the structure of text, digital images, video files, or audio can be used as confidential messages. Hide facts are derived from two Greek words: the staginess covered word and graphs mean writing and often refer to secret writing or data hiding [2]. Since the advent of the Internet, information security has been one of the most important factors of communication. Hide information is the art and science of invisible communication. This is done by hiding the information in other information and hiding the existence of this information. Anonymity is derived from the Greek words "stegos" which means "cover" and "grafia" which means "writing", known as "covered writing" [3].

II. OVERVIEW OF STEGANOGRAPHY

The three key terms used in Steganography systems are: cover massage, confidential data message and embedding algorithm. Secret key terms can also be entered to provide a more secure connection. The cover message is the medium of the message, for example a picture, video, sound, text, or other digital medium [4-5]. A confidential message is information that must be hidden in the appropriate digital medium. The secret key is generally used to merge the message according to masking algorithms. An integration algorithm is the idea or method used to include confidential information in a cover message.

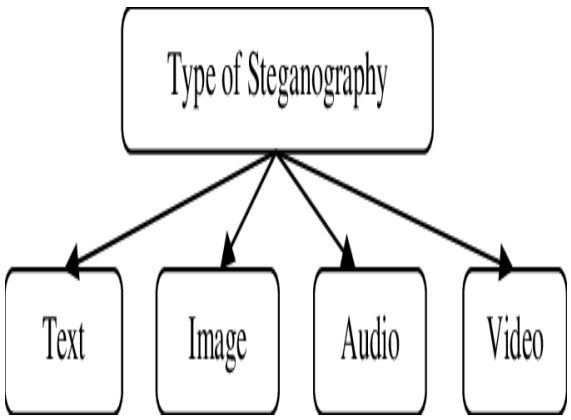

Figure 1: Types of Steganography

Text Steganography: Managing text or Text Steganography Hiding information in text is the most common method of hiding information or

Steganography. The way was to hide a secret message in a text message. After the advent of the Internet and various types of digital file formats, their importance diminished. Text stenos are with digital files is often not used because text files contain very little excess data.

Image Steganography: In Image Steganography the pictures are used as the simplest way to hide the concealment coverage. A message is embedded during a exceedingly in a digital image using an integration algorithmic rule, victimization the key. The ensuing stego image is shipped to the recipient. On the opposite hand, it's processed by the extraction algorithmic rule using a similar key. After you send associate degree unregistered photograph, solely unauthenticated individuals will notice the photograph move, however they can't see the hidden message.

Audio Steganography: Hide voice information aims to integrate secure and powerful information into a harmless cover story. the protection and confidentiality of communications and transmission is critical to transmit very important info to the meant sources whereas prohibiting access to unauthorized persons. An audible sound may be inaudible with a louder sound. This property is employed to spot the channel to cover info [3].The present voice information hiding software can merge messages into WAV and MP3 audio files. The list of strategies normally wont to hide audio info is listed and mentioned below.

- LSB coding
- Parity coding
- Phase coding
- Spread spectrum
- Echo hiding

Video Steganography: Video Steganography could be a technique to cover any sort of extension enters a video file. Concealing or embedding a message within the video is comparable to the art of hiding info, as a result of the sender doesn't hide it, however this message is prevented from being opened by anyone except the recipient. Concealing a message within the video is a component of the art of hiding info, which avoids revealing hidden messages. Video-based info masking techniques are similar to those supported the image, and are classified within the field and frequency field strategies [8].

Retention and disadvantages in hiding video information are important to use to evaluate performance. The results have a bonus over the power to cover info once exploitation the abstraction domain. The algorithmic program can integrate info directly into the supported image, while not dynamic visual or sensible quality. the sector conversion algorithmic program contains hint within the conversion area, and also the advantage of this algorithmic program is its sensible stability, however low capability.

Steganography of digital info from pictures may be a confidential communication tool designed to transmit an outsized quantity of confidential information relating to the size of cover image between continuous parties. Additionally, the goal is to avoid suspicion of this sort of unrelated parties. Thus, this study discusses and proposes some ways that to enhance these basic aspects of cryptography. Thus, some characteristics and characteristics of digital pictures were accustomed increase the flexibility to cover info and improve image quality.

III. IMAGE STEGANOGRAPHIC TECHNIQUES

There are several Steganography techniques for image file format which are as follow:

A. Spatial Domain Technique

There are many versions of spatial Steganography, all of that directly modification some bits in constituent values within the image once knowledge is hidden. LSB is one amongst the only ways that to cover secret messages in low-value bits of constituent values while not noticeable distortion. In our human read, changes within the LSB price don't seem to be visible. Message bits will be dead either merely or willy-nilly. Replacement the smallest amount necessary matrix (LSB), as well as the matrix is a few of the spatial domain strategies.

- **Advantages of spatial domain LSB technique are:**

1. Degradation of the original image is not easy.

2. Hiding capacity is more i.e. more information can be stored in an image.

➢ **Disadvantages of LSB technique are:**

1. Robustness is low
2. Hidden data can be destroyed by simple attacks.

B. Masking and Filtering

Masking and filtering is an info masking technique which will be used on grayscale pictures. The mask and muck agree the watermark of a written image. These strategies embrace info in areas that are additional necessary than merely concealing them at the amplitude. Watermark strategies is applied without worrying of damaging the image because of missing compression, because it is additional integrated into the image.

➢ **Advantages of Masking and filtering technology:**

This methodology is additional reliable than replacement LSB in terms of pressure.

➢ **Disadvantages of Masking and filtering technology:**

Strategies will solely be applied to grayscale pictures and are restricted up to twenty four bits.

C. Transform Domain Technique

The frequency target that the message is entered within the reborn image coefficients, providing a lot of data, activity power, and bigger purpose resistance. The inclusion of a reborn domain could also be observed because the field of modulation strategies during which a range of algorithms are projected. Today, powerful data concealment systems operate within the field of transformation. Space switch strategies take precedence over LSB methods as a result of they mask data in image areas that are less prone to compression, cropping, and image process. Some vary conversion strategies are freelance of image format and may transcend lost and lost conversions.

➢ **Transform domain techniques are of different types:**

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).

D. Distortion Techniques

In this technique, store the signal distortion info and live the deviation from the first coverage throughout decryption. Distortion ways need information of the first cowl image throughout the coding method, because the decoder works to see for variations between the first cowl image and also the distorted cover image to recover a confidential message. During this approach, a stego image is formed by applying a series of changes to the duvet image. This sequence of modifications is employed to match the key message needed for transmission. The message is encrypted in willy-nilly designated pixels. If the stego image is completely different from the duvet image in a very given element of the message, the message bit is one. Otherwise, the message bit is zero. The encoders will modification the pixels at one so the applied math properties of the image don't seem to be detected. If the assaulter interferes with a stego image by cropping, scaling, or rotating it, the receiver will simply sight it.

IV. APPLICATION OF STEGNOGRAPHY

1. **Secret Communications:** The use of Steganography anonymity does not advertise confidential communication and, thus, avoids checking the sender, message and recipient. Trade secrets, schemes or different counsel could also be sent abruptly potential attackers.

2. **Feature Tagging:** Elements are often embedded within the image, for instance, individual names on the image or places on the map. Repeating a stego additionally copies all the intrinsic functions, and solely people who have a coding key will retrieve and examine functions.

3. **Copyright Protection:** Copy protection mechanisms that stop the repeating of information, typically digital knowledge, and also the inclusion and analysis of watermarks to safeguard proprietary materials are liable for the recent increase in interest out of sight and consolidating digital info.

V. CONCLUSION

Steganography transmits secrets through seemingly harmless covers to conceal the existence of a secret. Hide digital information, images and their derivatives is increasingly used and applied. In this paper we presented the

different techniques of Steganography like Spatial Domain Technique, Masking and Filtering, Transform Domain Technique and Distortion Techniques. We discussed the application of stenography. This paper give us the overview the different stenography techniques, data or information hiding and application of stenography.

REFERENCES

[1]. Nagham Hamid, Abid Yahya, R. Badlishah Ahmad and Osamah M. Al-Qershi, "Image Steganography Techniques: An Overview", International Journal of Computer Science and Security (IJCSS), Volume-6, Issue-3, PP-168-187, 2012.

[2]. Deepesh Rawat and Vijaya Bhandari, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image", International Journal of Computer Applications, Volume-64,No-20, PP-15-19,February 2013.

[3]. R. BharathiPriya and Dr. E. Karthikeyan, "A Comparative Study on Secured Image Transmission Using Steganography Techniques", Proceedings of the UGC Sponsored National Conference on Advanced Networking and Applications, 27th March 2015, Special Issue Published in Int. Jnl. of Advanced Networking and Applications (IJANA), PP-198-201, 2015.

[4]. Gary C. Kessler, "Hiding Data in Data", Windows & .NET Magazine, 2002.

[5]. Nidhi Menon and Vaithiyanathan, "A Survey on Image Steganography", 2017 IEEE International Conference on Technological Advancements in Power and Energy (TAP Energy), PP-1-5, 2017.

[6]. Eakbodin Gedkhaw, Nantinee Soodtoetong and Mahasak Ketcham, "The Performance of Cover Image Steganography for Hidden Information within Image File using Least Significant bit algorithm", IEEE The 18th International Symposium on Communications and Information Technologies (ISCIT 2018), PP- 504-508, 2018.

[7]. N. Gopalakrishna Kini, Vishwas G. Kini and Gautam, "A Secured Steganography Algorithm for Hiding an Image in an Image", Springer Nature Singapore Pte Ltd., Integrated Intelligent Computing, Communication and Security, Studies in Computational Intelligence 771, PP-539-546, 2019.

[8]. Aryfandy Febryan, Tito Waluyo Purboyo and Randy Erfa Saputra, "Steganography Methods on Text, Audio, Image and Video: A Survey", International Journal of Applied Engineering Research, Volume-12, Number-21, PP-10485-10490, 2017.