Analysis of Image Steganographic techniques

Madhu R[1], Shammi L[2]

[1] Assistant Professor, Computer Science and Engineering, SJC Institute of Technology, Karnataka, India
[2] Assistant Professor, Computer Science and Engineering, East Point College of Engineering and Technology, Karnataka, India

ABSTRACT

Computer-based communications are on the verge of simplifying life for everyone in the globe today, whether it's through information sharing, interpersonal conversation, the exchange of electronic documents, or checking bank balances and paying bills. To maintain secure connections, information security is a crucial component that must be taken into account. Since the expanding usage of the internet and multimedia has increased interest in picture steganography to secure and safeguard them, there is significant interest in security approaches that aim to protect information and digital data. In order to analyse and explore the many approaches, algorithms, and schemes used in image steganography, a thorough literature survey on the subject is done in this paper. Also, this study summarised a review of related literature for these studies and presented it in a table with the research's name, broad domain, research technique, benefits, and drawbacks, as well as the evaluation method.

Keywords : *Data Embedding and Extracting, Image Steganography, Data Hiding, and Image Steganography Methods etc….*

1. INTRODUCTION

Steganography is the science and art of hiding a hidden message in many file types, such as text files, digital pictures, digital audio, and digital video files. The words "steganography" are made from of the Greek words "stegano" and "graphy." Stegano denotes a covered object, whereas Graphy denotes writing. Steganography is therefore a Covered Writing.

In contrast to cryptography, which scrambles messages so they cannot be deciphered, steganography conceals messages so they cannot be seen. Steganography, which is the science and art of concealing a message's existence between a sender and its intended recipient, is a type of security technique through obscurity. Steganography's goal is to hide the message within cover files, hence hiding the flow of information itself. Moreover, among the many file types, image steganography is chosen since the altered image will be virtually indistinguishable from the original image to the human eye with just minor colour alterations.

2. TYPES OF STEGANOGRAPHY

Text Steganography: It consists of hiding information inside the text files. The secret data is concealed using this technique behind every nth letter of every text message word. There are numerous ways to hide data in text files. The first strategy is format-based, the second is random and statistical, and the third is linguistics-based.

Image steganography: It is the practise of concealing data by using a cover object as a picture. In image steganography, the data is concealed using pixel intensities. Images are a common cover source in digital steganography since the digital representation of an image contains a number of bits.

Audio steganography: Data is concealed within audio files using audio steganography. With this technique, data in WAV, AU, and MP3 sound files is concealed. Several techniques exist for audio steganography. Some techniques include phase coding, low bit encoding and Spread spectrum.

Video steganography: Steganography for video is a method of encrypting any kind of data or file into a digital video format. In this instance, the data is concealed via video (a mixture of images). The data in each of the images in the video is typically hidden using discrete cosine transform (DCT), which typically modifies the values

(e.g., 8.667 to 9) in a way that is invisible to the human eye. Video steganography uses the file types H.264, Mp4, MPEG, and AVI.

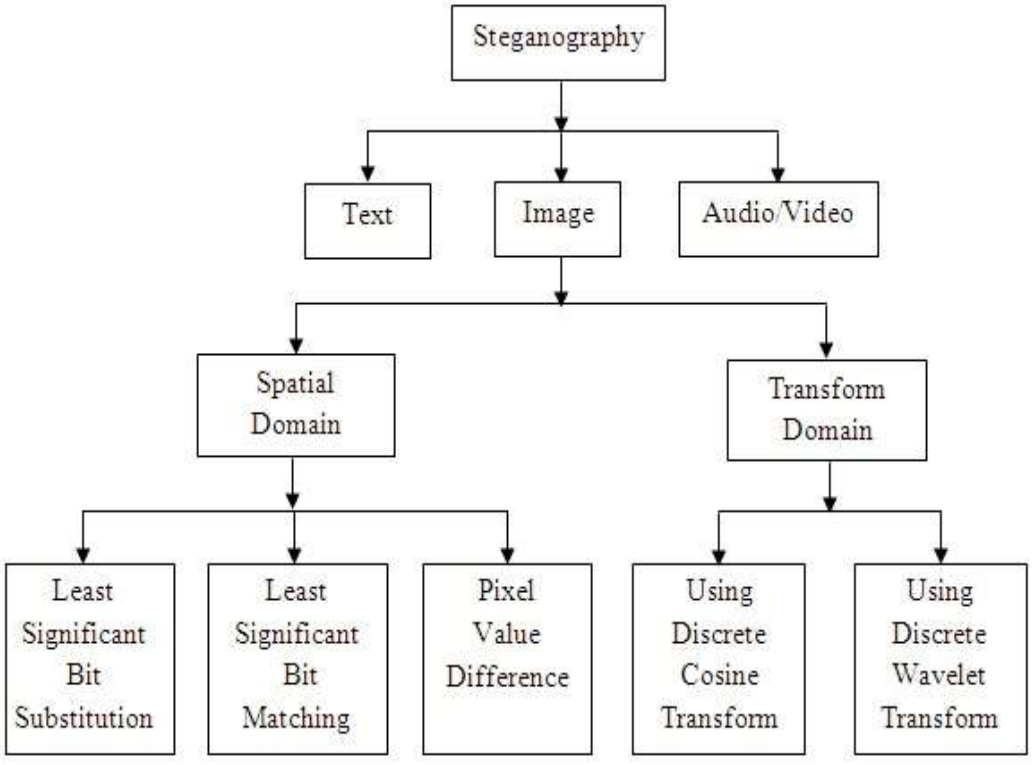

Fig-1 Types of Steganography

Protocol or network Steganography: This technique includes concealing information by using a network protocol as a cover object, such as TCP, UDP, ICMP, or IP. There are covert channels in the OSI layer network model where steganography can be applied.

3. STEGANOGRAPHY TECHNIQUES

1. Spatial Domain Methods: In this technique, the secret information is immediately included into the pixel intensities. That implies that portions of the image's pixel values are directly altered during data concealment. The following categories are used to classify spatial domain techniques: I The least important bit (LSB) ii) Pixel value comparison (PVD) Edges-based data embedding technique (iii) (EBE) iv) Random-picture-loop-embedding technique (RPE) v) Pixel to hidden data mapping technique Labeling or connection techniques vii) Based on pixel intensity.

i) LSB: The most typical application of this technique is data concealing. By swapping out the least important image pixel bits for the secret data bits, this approach embeds the data. Because the change in the LSB of an image pixel does not significantly alter the image, the image obtained after embedding is essentially identical to the original image.

ii) BPCP: Measurements of the image's complexity are employed in this segmentation. The noisy block is identified using the complexity. This method maps binary patterns from a secret data to replace noisy bit plan blocks.

iii) PVD: This technique chooses two adjacent pixels to put the data in. In order to establish whether two consecutive pixels belong to an edge area or a smooth area, the payload is calculated by comparing the differences between two successive pixels.

2. Spread Spectrum Technique : This method makes use of the spread spectrum notion. The secret data is dispersed over a large frequency spectrum in this manner. Every frequency band's signal-to-noise ratio must be so low that it is challenging to detect the presence of data. There would still be enough information available in other bands to recover the data, even if portions of the data were removed from a few bands. As a result, it is challenging to totally delete the data without also completely ruining the cover. It is a fairly reliable method that is mostly employed in military communication.

3. Statistical Technique: Using a technology, the message is embedded by altering a number of the cover's attributes. One message bit is embedded in each block once the cover is divided into segments. Only when the size of the message bit is one does the cover block need to be updated; otherwise, there is no need.

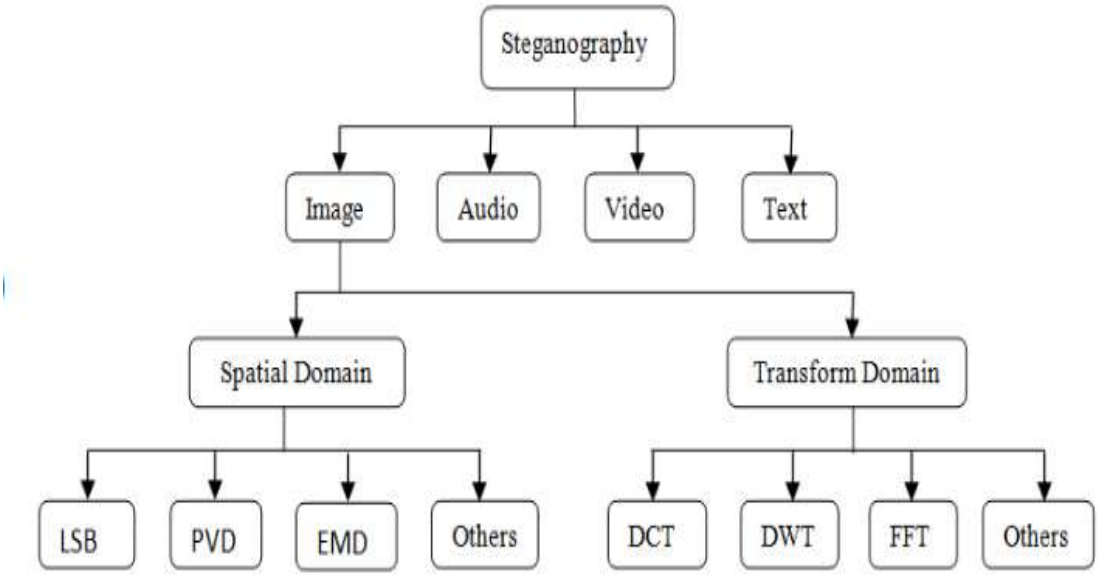

Fig-2 Image Steganography Techniques

4. Transform Domain Technique: In this method, the cover's transform or frequency domain contains the hidden message. This is a trickier approach to conceal a message in an image. The image is subjected to several algorithms and changes in order to conceal the message. Discrete Fourier transformation technique (DFT), Discrete Cosine transformation technique (DCT), Discrete Wavelet transformation technique (DWT), Lossless or reversible approach (DCT), and Embedding in coefficient bits are some examples of the various transform domain techniques.

5. Distortion Techniques: With this method, the signal is distorted in order to store the hidden message. The cover is modified in a series of steps by the encoder. In order to identify the order of modifications and subsequently recover the hidden message, the decoder compares the discrepancies between the original cover and the distorted cover.

6. Masking and Filtering: These methods label an image to conceal information. Watermarks become a portion of the image, whereas steganography just conceals the information. Instead of burying the information in the background noise, these strategies embed it in the parts that are more important. When they are more integrated into the image, watermarking techniques can be used without worrying that lossy compression will result in image damage. Essentially, this technique is used to 24-bit and grayscale photos.

4. CONCLUSION

In this study, we examined a wide range of literature on steganography methods. These studies are adequate and have a broad potential application. We discovered that the majority of the steganography work has been completed by reading these articles. These days, the most used steganography method is called LSB. Other researchers have also used techniques including water marking, distortion, spatial, ISB, and MSB in their study and have offered a potent way of transmitting encrypted information. Using LSB, ISB, and MLSB, various security and data concealment techniques are employed to perform steganography. In subsequent research, we'll combine more sophisticated techniques like steganography with a hybrid cryptographic method to improve data security.

5. REFERENCES

[1]. Banerjee, & Indradip. (2011). A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier. Journal of Global Research in Computer Science, 2(4), 116..
[2]. Bhagat, A., & Dhembhare, A. (2015). An efficient and secure data hiding techniqueSteganography. International Journal of Innovative Research in Computer and Communications Engineering, 3(2), 944-949.
[3]. Kumari, S. (2017). A research paper on cryptography encryption and compression techniques. International Journal of Engineering snd Computer Science, 6(4), 20915-20919.
[4]. Bhattacharyya, S., Banerjee, I., & Sanyal, G. (2011). A Survey of steganography and steganalysis Technique in image, text, audio and video as cover carrier. Journal of Global Research in Computer Science, 2(4), 1-16.
[5]. Patel, S. K. J., & Tahilraman, N. V. (2016). Information hiding techniques: Watermarking, steganography. International Journal of Innovational Research in Electrical, Electronics, Instrumentation and Control Engineering, 4(4), 168-173.