International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT228642

Steganography Techniques - An Overview

Amitava Podder*[1], Piyal Roy[2], Smaranika Roy[3]

*[1]Department of Computer Science & Engineering, Brainware University, Barasat, West Bengal, India

[2]Department of Computer Science & Engineering, Brainware University, Barasat, West Bengal, India

[3]Department of Computer Science, Sarada Ma Girls' College, Barasat, West Bengal, India

Article Info

Publication Issue :
Volume 8, Issue 6
November-December-2022
Page Number : 300-304

Article History
Accepted: 12 Nov 2022
Published: 28 Nov 2022

ABSTRACT

Cryptography, or the use of code, has a sinister relative called steganography. Steganography is supposed to offer confidentiality whereas encryption is said to provide privacy. A method of concealed communication is steganography. The process of steganography involves hiding a message in a suitable carrier, such as an image or audio file, which can then be transported to the receiver without anybody being aware that it contains a hidden message. This is a method that civil rights organizations in oppressive states, for instance, might utilize to propagate their message without the knowledge of their own government. This paper aims to discuss different techniques for implementing steganography to multimedia files (text, still images, audio, and video).

Keywords: Digital Image Steganography, Spatial Domain, Frequency Domain, Adaptive Steganography, Security

I. INTRODUCTION

Steganography is a Greek word that means "secret or hidden writing." It is the science of information hiding. Steganography is used to hide data from third parties, whereas encryption is used to make data unreadable to them. Information can be concealed via steganography in carriers like photos, audio files, text files, videos, and data transmissions [1]. When a message is concealed within a carrier, a stego-carrier is created (e.g. a stego-image). Human senses interpret as being as similar to the original carrier or cover image as feasible.

Cryptography and steganography go hand in hand. The communication is scrambled via encryption, which makes it difficult to decipher. On the other hand, steganography conceals the message such that its presence is not known beforehand. Information is concealed in computer files using steganography. In digital steganography, transport layers like as document files, image files, applications, or protocols may contain steganographic encoding [5].

II. HISTORY OF STEGANOGRAPHY

Since ancient times, steganographic methods have been employed. Before the creation of cryptography technologies, steganography was often used. The first known use dates back to ancient Greece, when messengers tattooed messages on their shaved heads and grew their hair so that the messages were not

visible. Wax wood tablets were also employed. The message was coated with fresh wax once the message had been written on the underlying wood [3]. The tablet appeared to be empty, thus it was accepted without a problem after inspection. Invisible ink was used to write information on paper during World War II, giving the impression that the paper was blank to the regular person.

III.RESULTS AND DISCUSSION

Steganography conceals information in an invisible way. The most commonly used method is called LSB (Least Significant Bit) steganography. In this type of steganography, the least important parts of media files are used to hide secret information. For instance, each pixel in an image file has 3 bytes of data, or the red, green, and blue hues, and some image formats have an additional 4 bytes for transparency that is alpha [7]. To conceal data bits, LSB steganography alters the final bit of each of these bytes. Therefore, an 8 megabyte image file is required to conceal 1 megabyte of data in this manner. A person viewing the original image and the steganographically modified image cannot detect the difference since altering the last piece of pixel value does not result in a visually noticeable change in the image.

Figure 1. Least Significant Bit Steganography.

Example: -

1) In 11001101 bytes, the first "1" on the left has the most weight and the "1" on the right has the least weight. (When converting from binary to decimal, multiply the "1" on the left by 128, and multiply the "1" on the right by 1) Therefore, manipulating the rightmost bit of a sequence has little effect. There is none. Of course, the pixels will have different colors, but the change is imperceptible to the human eye.

2) Images usually use 8-bit or 24-bit color. With 8-bit color, there are up to 256 color definitions that make up the image's palette, each identified by an 8-bit value. A 24-bit color scheme, as the term suggests, uses 24 bits per pixel and provides a much better set of colors. In this case, each image is represented by 3 bytes, each representing the intensity of the three primary colors red, green, and blue (RGB). Hypertext Markup Language (HTML) formats for displaying colors in web pages often use a 24-bit format of 6 hexadecimal digits, each pair representing the amount of red, blue, and green respectively. increase. For example, orange is displayed at 100% red (255 decimal, FF hex), 50% green (127 decimal, 7F hex), and no blue (0). HTML.

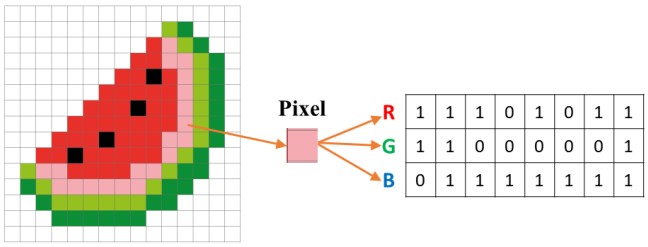

Figure 2. Pixel size of different color.

The size of an image file, then, is directly related to the number of pixels and the granularity of the color definition. A typical 640╳480 pixel image using a palette of 256 colors would require a file about 307 KB in size (640╳480 bytes), whereas a 1024╳768 pixel high-resolution 24-bit color image would result in a 2.36 MB file (1024╳768╳3 bytes).

To avoid sending files of this enormous size, a number of compression schemes have been developed over time, notably Bitmap (BMP), Graphic Interchange Format (GIF), and Joint Photographic Experts Group (JPEG) file types. Not all are equally suited to steganography, however.

The lossless compression method used by GIF and 8-bit BMP files enables software to precisely rebuild the original image. Contrarily, JPEG employs lossy compression, which results in an extended image that is very similar to the original but not an exact replica. While both techniques enable computers to reduce their storage requirements, lossless compression is far more appropriate for applications like steganography where the original data's integrity must be preserved. Despite the fact that JPEG can be utilised for stego applications, data is typically included in GIF or BMP files.

IV.TECHNIQUES OF STEGANOGRAPHY

Depending on the nature of the cover object (the real object with the sensitive data embedded), steganography can be divided into five types:

1. Text Steganography
2. Image Steganography
3. Video Steganography
4. Audio Steganography
5. Network Steganography

Let's explore each of them in detail –

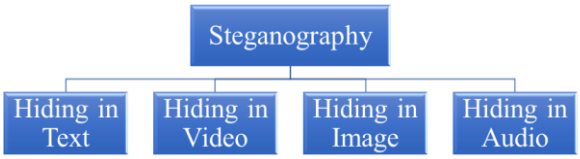

Figure 3. Types of Steganography.

A. Text Steganography

Text steganography hides information in text files. This includes modifying the formatting of already written text, altering individual words, creating random strings, and creating understandable text using context-free grammars. There are several methods for hiding data in text, including:

- Format Based Method
- Random and Statistical Generation
- Linguistic Method

B. Image Steganography

Image steganography is the practice of concealing data by utilizing a cover object that is an image. Images are frequently employed as the cover source in digital steganography because of the high bit depth of the digital representation of the images. Information can be concealed in images in a variety of ways. A typical strategy is:

- Least Significant Bit Insertion
- Masking and Filtering
- Redundant Pattern Encoding
- Encrypt and Scatter
- Coding and Cosine Transformation

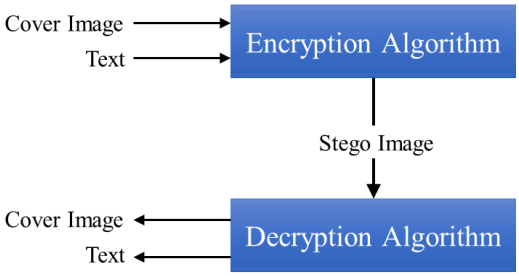

Figure 4. Image steganography.

C. Audio Steganography

In audio steganography, hidden messages are inserted into audio signals and the binary sequences of the accompanying audio files are altered. Image steganography, which is far more challenging to use in order to cover up secret messages with digital sound. There are several types of audio steganography, including:

- Least Significant Bit Encoding
- Parity Encoding
- Phase Coding
- Spread Spectrum

This method hides the data in WAV, AU, and even MP3 sound files.

Figure 5. Audio Steganography.

D. Video Steganography

Information can be concealed in a digital video format using video steganography. This type has the benefit that a lot of data can be concealed in it and that it is a moving stream of images and sounds. It can be compared to a fusion of audio and visual steganography. Two major classes in video steganography are:

- Embedding data in uncompressed raw video and compressing it later
- Embedding data directly into the compressed data stream

E. Network Steganography (Protocol Steganography)

It is a method of incorporating data into network control protocols like TCP, UDP, and ICMP that are used for data transport. Some covert channels that can be found in the OSI model can be used with steganography [4]. For instance, you can conceal information in a few TCP/IP packets' optional header fields. Different software tools for steganography are accessible in today's digital environment [8].

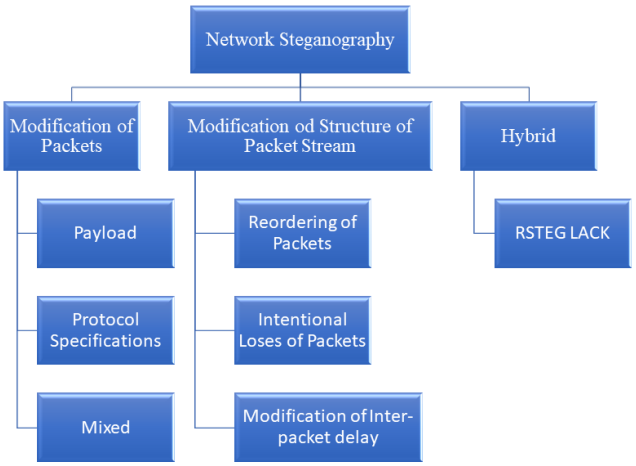

Figure 5. Network Steganography Types.

V. STEGANOGRAPHY DETECTION

Identifying the strategies, methods, and procedures (TTPs) used by attackers and pentesters is the job of security analysts. They have utilized steganography software throughout time to recognize common signatures [2]. So, for instance, a steganography application's typical steps can be recognized by an antivirus program. In order to avoid discovery, intruders and attackers alter and tweak their methods. Security analysts are continuously searching for new signatures and approaches because attackers are continually updating their tools and methodologies.

VI.CRYPTOGRAPHY VS STEGANOGRAPHY

Both steganography and cryptography are techniques used to conceal or protect secret data. However, they differ in that steganography conceals the existence of the data, whereas cryptography renders the data unreadable or hides the meaning of the data [6]. The primary benefit of steganography over encryption for data concealment is that it makes it appear as though no sensitive information is concealed within files or other content that contains hidden text. Steganography techniques can be used to mask the presence of a secure channel even when the payload of an encrypted file, communication, or network packet is uniquely marked and traceable.

VII. APPLICATIONS

There are various reasons to hide data, but ultimately it is done to stop anyone from figuring out that a message even exists. Hidden messages are no longer recognizable from white noise. There is no proof of the message's existence, even if it is suspected. Steganography can be used in business to cover up confidential chemical formulas and blueprints for brand-new inventions. Steganography can be used to leak trade secrets without anyone in the firm knowing, which is another form of industrial espionage. Steganography is another tool that terrorists might employ to conceal communications and plan attacks. All of this sounds quite sinister, yet intelligence gathering is a clear application of steganography.

VIII. CONCLUSION

Steganography is an intriguing and successful method of data hiding that has been utilized for centuries. Such cunning strategies can be exposed using certain techniques, but acknowledging their existence is the first step. This type of data hiding is also used for many legitimate reasons, such as secured storage techniques. In either case, the technology is both straightforward to use and scarce. The further you may proceed in the game, the more you will understand about its features and functionalities. This paper outlines numerous methods for including data as cover media in text, pictures, and audio and video signals. I provided you a succinct summary of the computer security sector, which is very fascinating and developing quickly.

IX. REFERENCES

[1] Johnson, N. F. and Jajodia, S. (1998). Exploring steganography: Seeing the unseen. Computer, 31(2):26–34.

[2] Souvik Bhattacharyya. and Gautam Sanyal. An image based steganography model for promoting global cyber security. In, 2009 Proceedings of International Conference on Systemics, Cybernetics and Informatics, Hyderabad, India.

[3] Niels Provos, Peter Honeyman, Hide and Seek: Introduction to Steganography (2003).

[4] Biswas, S.K., Podder, A. (2022). "Path Minimization Planning and Cost Estimation of Passive Optical Network Using Algorithm for Sub-optimal Deployment of Optical Fiber Cable". In: Mitra, M., Nasipuri, M., Kanjilal, M.R. (eds) Computational Advancement in Communication, Circuits and Systems. Lecture Notes in Electrical Engineering, vol 786. Springer, Singapore. https://doi.org/10.1007/978-981-16-4035-3_7.

[5] Silman, J., “Steganography and Steganalysis: An Overview”, 2001 SANS Institute.

[6] Westfeld, A. (2001). F5-a steganographic algorithm: High capacity despite better steganalysis. In Proc. 4th Int’l Workshop Information Hiding, pages 289–302.

[7] Nasir Memon R. Chandramouli. Analysis of lsb based image steganography techniques. In, 2001 Proceedings of IEEE ICIP.

[8] Amitava Podder, Satyaki Kumar Biswas. "Energy-Efficient Passive Optical Network (PON) Planning with Wavelength Allocation Scheme based on User Behaviors and Bit Error Rate (BER) Performance Evaluation", International Journal of Engineering Science Invention (IJESI) ISSN (Online): 2319-6734, ISSN (Print): 2319-6726 www.ijesi.org ||Volume 10 Issue 2 Series I || February 2021 || PP 01-11 || Journal DOI-10.35629/6734.

Cite this article as :

Amitava Podder, Piyal Roy, Smaranika Roy, "Steganography Techniques - An Overview", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 6, pp. 323-327, November-December 2022. Available at doi : https://doi.org/10.32628/CSEIT228642

Journal URL : https://ijsrcseit.com/CSEIT228642