WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Image Steganography

Ankit Mahendra yadav

keraleeya Samajam dombivali's model college,
Email: yadavankit3237@gmail.com

Abstract

Steganography is the art of concealing the fact that communication is taking place by enclosing data in other data. to keep private information private, secure confidential information, and so forth. It is critical to securely exchange data across the internet network. So, there are numerous techniques of safely transferring data to the destination, such as cryptography and steganography.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. Multi Layer Security (MLS) is the art of concealing the fact that communication is taking place by encasing data in other data. Many other carrier file formats are available, but digital photos are the most used due to their widespread availability on the internet. There are several strategies for hiding secret information in photographs, some more intricate than others, and each has its own set of strengths and weaknesses. Depending on the application, perfect invisibility of the secret information may be required, while others may necessitate the hiding of a significant secret message.

1.Introduction

This is a template document. The conference website has an electronic copy available for download. Please contact the conference publications committee as mentioned on the conference website if you have any issues about the paper guidelines. The conference website has information on how to submit your final work. Steganography is defined as the science and art of hiding a hidden message in various sorts of media, such as digital photos, digital audio, digital video, and text files. The word steganography is made out of two Greek words: Stegano and Graphy. Stegano is a word that meaning "covered," and Graphy is a word that means "writing." As a result, the term "steganography" refers to "covered writing."

When steganography is compared to cryptography, the difference is that cryptography scrambles a message so that it cannot be deciphered, but steganography hides a message so that it cannot be seen. Steganography is a type of obscurity-based security approach that involves the science and art of concealing the existence of a message between the sender and the intended recipient. The goal of steganography, as demonstrated in Figure 1, is to hide the message under cover files, effectively hiding the fact that information is being exchanged. Indeed, image steganography is favoured among a number of file types since the altered image with minor color differences will be indistinguishable from the original image to the naked eye.

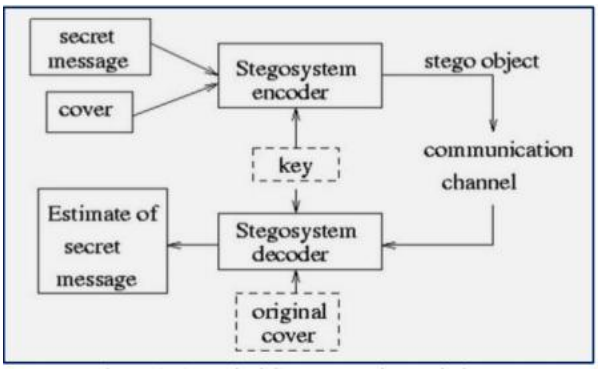

Figure 1: A Typical Steganography Technique

Steganography is divided into four categories in general [1]:
1. Image steganography: This is a technique for hiding a secret image inside a cover image in such a way that the secret image is hidden and the cover image appears to be genuine.
2. 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.
3. 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.
4. 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. Normally, Steganography requires three main components, namely carrier object, secret data, and steganographic .
algorithm. Steganography can be used for many useful applications, such as: secure transmission of top-secret data between national and international governments, online banking security, military and intelligent agencies security and safe circulation of secret documents among defense organizations].

2.REVIEW

Steganographic techniques are categorized into two broad domains as follows [1][20-22]:
1.
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 [1][20-22]:
i. 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) [1][23]. 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: 1111100**0** 1100100**1** 0000001**1**
Pixel 2: 1111100**0** 1100100**1** 0000001**1**
Pixel 3: 1111100**0** 1100100**1** 00000011

Least Significant Bit (LSB) algorithm hides (embeds) bits of letter 'A', which are **01000001**, into image pixels to
produce:
Pixel 1: 1111100**0** 1100100**1** 0000001**0**
Pixel 2: 1111100**0** 1100100**0** 0000001**0**
Pixel 3: 1111100**1** 1100100**1** 00000011

ii. Gray-Level Modification (GLM): Gray-Level Modification (GLM) is a technique for representing binary data in which the grey level values of picture pixels are adjusted according to a mathematical function. Each pixel has its own grey level value, which can be either odd or even. To represent binary data, the grey level's odd or even value is correctly changed [24].

iii. Pixel Value Differencing (PVD): The pixel-value differencing (PVD) scheme determines how many secret bits should be embedded by calculating the difference between two consecutive pixels in a block. It selects two consecutive pixels and creates a quantization range table to decide the payload based on the difference value between the successive pixels, giving the stego image excellent imperceptibility. Furthermore, it has the advantage of transporting a large number of payloads while yet maintaining visual integrity after data embedding.

3. Methods And Materials

The application must be run by the user. Encryption and decryption are the two tab options available to the user. If the user chooses to encrypt, the application will provide a screen with options to select an image file, information file, and save the image file. If the user selects decrypt, the application displays a screen that allows the user to select only an image file and asks where the secretive file should be saved. Encrypt and Decrypt are the two methods used in this project. The secret information is hidden in any type of image file under encryption. Decryption is the process of extracting secret information from an image file.

4.Categories Steganography Techniques

A research in [29] has proposed a modified image steganography method that is based on LSB technique in area of the spatial domain. Their introduced method expresses a secret data (message) in six bits of binary format by applying of LSBraille method rather than the American Standard Code for Information Interchange (ASCII) format. Their method veils three bits of a secret data (message) over one pixel of a true image that it composes of three coherent layers namely, red layer, green layer, and blue layer. In their method, two binary bits are hided on blue layer, while the last single bit is hided in green layer of a pixel. In addition, a secret data (message) is hided using second and the third LSB alongside with the least significant bit (LSB) of the blue layer.

Throughout hiding procedure or process, only one bit of the blue layer is manipulated and changed as well. Their research problem was to improve security of LSB steganographic technique. They dealt with the secret message and the cover image and the secret message as an input, and converted each byte in the secret message to its binary format through using LSBraille method so that a byte of the secret message is expressed in 6-bits only, as shown in Figure 2 below.

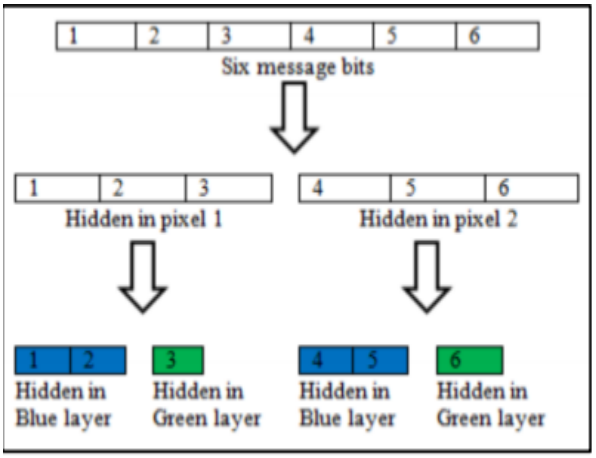

Figure 2: The Secret Message Bit

In a further detail, they converted a carrier (cover) image into three coherent layers; red layer, green layer, and blue layer. Then, each blue layer and green layer of the pixel is represented by its binary format through using of ASCII encoding format. In their method, they started with the blue layer, and then the green layer of the pixel, and so forth till the whole secret message is embedded. Two bits of the blue layer are utilized for embedding. Besides the message is hided using the second and the third LSB alongside with the least significant bit (LSB). Nonetheless, during each manipulate of hiding merely 1-bit of the blue layer that will be permitted to changed by manipulating last three binary bits of blue layer in the pixel through the next equations (1)(2):

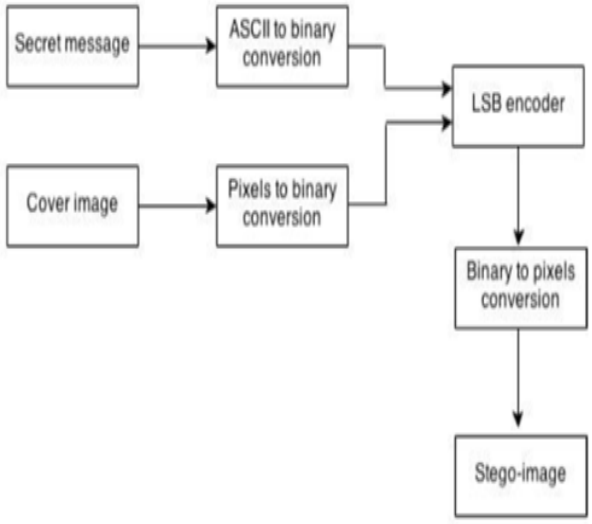

Figure 3: The Embedding Process

5. Discussion

Steganography is the practice of concealing confidential or sensitive information in something that appears to be ordinary. Steganography is frequently confused with cryptography since the two are used to protect sensitive information in similar ways. The distinction between the two is that steganography involves concealing data so that it looks that nothing is hidden at all.

The encoding of secret information is done in such a way that the existence of the information is hidden. Steganography can be used to carry out covert trades when combined with conventional communication mechanisms. The fundamental purpose of this project is to interact securely while being fully invisible, in order to avoid attracting suspicion to the transfer of hidden data. Steganography has seen a surge in popularity due to two factors: Techniques for disguising encrypted copyright marks and serial numbers in digital films, audio recordings, books, and multimedia items have piqued the interest of the publishing and broadcasting industries. 17 People are studying methods by which private messages can be buried in seemingly harmless cover messages as a result of moves by various governments to restrict the availability of encryption services. Carrier, Message, and Password are the three essential components of steganography. Carrier, also known as cover-object, is an object in which the message is embedded and which serves to mask the message's presence. The basic steganography model is depicted in the diagram below:

The data that the sender desires to keep private is referred to as a message. It could be plain text, ciphertext, another image, or anything else that can be embedded in a bit stream, like a copyright mark, covert communication, or a serial number. Only recipients who know the corresponding decoding key will be able to extract the message from a coverobject, which is known as stego-key. The Stego-object is the cover-object with the surreptitiously hidden message. If a stego -key was used during the encoding procedure, recovering a message from a stego -object requires the cover-object itself and a corresponding decoding key. In most applications, the original image may or may not be necessary to extract the message. There are numerous carriers that could be used as the cover-object listed below:

• TCP, IP, and UDP are examples of network protocols. • Audio files in digital formats including wav, midi, avi, mpeg, mpi, and voc

6.Conclusion

Steganography is a fascinating topic that lies outside of the usual realms of cryptography and system administration that most of us deal with on a daily basis. Steganography can be used to communicate invisibly. We've looked at the theoretical and practical constraints of steganography. To create a means of secure communication, we printed out the enhancement of the picture steganography system utilizing the LSB approach. During the embedding of the message into the cover image, a stego-key was applied to the system. This steganography program software demonstrates how to employ a variety of image formats to conceal any sort of file within them. This application's crowning achievement is its ability to support any type of image without the need to convert to bitmap format, as well as a reduced file size restriction for hiding due to the utilization of maximum memory space in photos. The ability to communicate discreetly has piqued man's interest since the dawn of time. Steganography isn't simply for military or espionage purposes, as evidenced by the current growth of research in watermarking to protect intellectual property.

Steganography, like cryptography, will play a bigger role in secure communication in the "digital world" in the future. In order to study and investigate a number of distinct methodologies, algorithms, and schemes in the image steganography sector, this research conducted a complete literature analysis. Following that, a table summarizing a comparative literature review for these studies is created. TABLE 1 is a summary table that presents a study title, a broad domain, a research technique, research benefits, research drawbacks, and the assessment method they utilized. Overall, as shown in TABLE 1, the studies are divided into two categories: spatial domain and transform domain.

Furthermore, each of these studies has pros and disadvantages. Finally, the table TABLE 1 shows how the research is assessed.

Reference

1.M. Kharinov, “Information quantity in a pixel of digital image,” arXiv1401.7517 [cs, math], no. 2, pp. 1–11, 2014.

2.. M. Studio, F. Digital, and M. Workshops, “digital image,” pp. 3–7, 2012.

3/. Hasan, “Computer Security,” 2010. [Online]. Available: http://www.contrib.andrew.cmu.edu/~aishah/Sec.html.

4. Talbot and D. Welsh, “Complexity and Cryptography,” pp. 1–9, 2006.

5.Sarciszewski, “Guide to Cryptography,” 2015.

6.E. R. Harold, “What is an Image,” 2006.