iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** V **Month of publication:** May 2020

DOI: http://doi.org/10.22214/ijraset.2020.5395

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

Digital Image Steganography

Divyansh Singh
Department of Computer Science and Engineering, Galgotias University, Uttar Pradesh, India

Abstract: ***Steganography is the practice of concealing the truth that communication is taking place. Intruders can easily attack information within a system if it is readily available. It can be read, modified, misused, and revealed to others. Therefore, the goal is to hide the existence of the secret data. Using steganography techniques, secret data can be concealed within an appropriate multimedia carrier, such as, image, audio, text files; among which digital image is the most widely used carrier format. Different steganography techniques are available, some are more advanced than the others, having strong and weak points respectively. The suitable technique can be selected as per the application requirement. The main objectives of steganography are undetectability, untraceable, robustness, and capacity of secret data. These are the factors that make it different from techniques such as cryptography. This paper analysis the uses of steganography and its techniques. It additionally aims to determine which steganography technique is more suitable for a certain application.***
Keywords: steganography; image steganography; digital steganography; lowest significant bit; LSB; data hiding

I. INTRODUCTION

The technology on the internet has improved drastically in the past two decades. The internet contains a huge amount of information- be it in any field. This improvisation allowed us to use the internet in most of our daily-use devices like mobile phones, tablets, computers, smart TVs, wristwatches, cars, etc. A large amount of data as text, image, audio, video, and animation is produced every day and is accelerating with the growth of the Internet of Things (IoT). Data security becomes a great concern where new developments are added in a fast-paced technical environment. Making copies of digital multimedia is breaking intellectual property rights more than before. Moreover, intruders can easily attack information within a system if it is readily available. The data is required to be kept safe and secure so that it could be retrieved by authorized personnel only. Two techniques are used for this purpose– Cryptography, and Steganography. Cryptography is used by the sender to send encoded texts to the receiver, where it is decoded. A cryptographic confidential key is used to decode the message. Whereas, using steganography techniques, secret data can be concealed within an appropriate multimedia carrier, without knowing the fact of its existence. Digital images are mostly used as a multimedia carrier due to their extensive usage. Its advantage over cryptography is that anyone viewing the image could not distinguish the initial (or carrier) image from the encrypted image. The security and reliability of data transmission also improved with steganography since now no other person could change the sent data. This can be achieved by storing the message with minor bites within the carrier file. Steganography can be accomplished either manually or with the employment of a steganography tool.

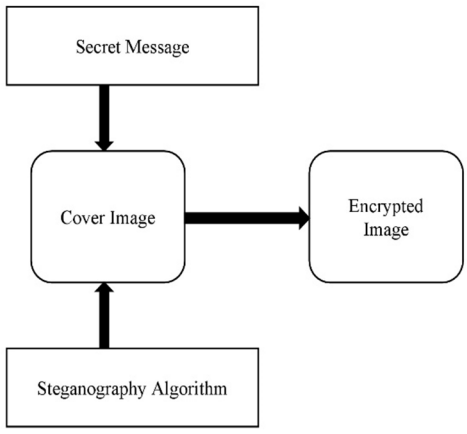


Figure 1: Principle of Steganography

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

II. STEGANOGRAPHY TECHNIQUES

Digital images are the most preferred and widely used cover objects for steganography, due to their availability and wide-ranging application. The steganography algorithm varies for different file formats.

An image is a collection of bytes, known as a pixel. Pixel, also known as pel, or picture element is the smallest element of an image. Each pixel represents any one value. The number of distinct colors that can be represented by a pixel depends on the number of bits per pixel (bpp). A 1 bpp image uses 1-bit for each pixel, so each pixel can be either on or off. Each additional bit doubles the number of colors available. So, a 2 bpp image can have 4 colors, and a 3 bpp image can have 8 colors:

1 bpp, 2^1 = 2 colors (Monochrome)
2 bpp, 2^2 = 4 colors
3 bpp, 2^3 = 8 colors
…
8 bpp, 2^8 = 256 colors
16 bpp, 2^{16} = 65,536 colors
24 bpp, 2^{24} = 16,777,216 colors

8 bpp and 24 bpp are the most typical carrier image formats. Both have their advantages and disadvantages. 8 bpp images are used due to their relatively small size but only 256 color combinations are available in total, which can prove to be a potential problem during encoding. 24 bpp images provide a lot more flexibility when used for steganography. More amount of secret data can be embedded into 24 bpp images in comparison to the 8 bpp images. The limitation of 24 bpp images is their high file size. More the number of colors (beyond 16-million), more it makes difficult for the human visual system (HVS) to detect the difference between the original image and the encoded image. Determining the type of message and the type of image, different algorithms are used.

A. Least Significant Bit Substitution

Least Significant Bit (LSB) substitution is one of the oldest and widely known steganography algorithms used for images. LSB replacement is the simplest technique in LSB steganography. As the name suggests, it involves the tempering of the LSB data value of the pixels. The message is stored in the LSB value of the pixels, which does not show any kind of distortion in the encrypted image.

Consider an 8 bpp grayscale bitmap image where an individual pixel is stored as a byte representing a grayscale value. Suppose the first eight pixels of the original image has the following grayscale values:

00010010
11111000
11010101
10100111
01100001
11000100
01011000
01111011

To hide the letter ‘D’ whose binary value is 01000100, we would replace the LSB’s of the original image with the value we need to hide. The new grayscale values are:

00010010
11111001
11010100
10100110
01100000
11000101
01011000
01111010

The value of LSB changes but this change is so minimal that it is not visible to the human eye. However, one of its major disadvantages is the small size of data which can be embedded by using only the least significant bits. Moreover, LSB’s can be vulnerable to attacks. LSB techniques applied to 24 bpp images are tough to detect and more data can be embedded contrary to 8 bpp file format.

B. Masking and Filtering

This technique works somewhat similar to the digital watermarking technique. Instead of hiding the data behind the image, it is appended on such a space which is safe and secure from attackers. The information is hidden in a manner like watermarks on an actual paper. Masking the image changes the image. Therefore, to make sure the changes cannot be detected, it is recommended to make changes in multiple small portions of the image. The masking and filtering technique is more robust than the LSB technique. Image compression is performed because data is embedded on a secured surface and visible to everyone. If the image is copied, then the information is also carried in the copy. Watermarks are integrated into the image; therefore, this technique can be applied without the fear of image destruction. This technique is mostly used for 24 bpp and grayscale images.

C. Redundant Pattern Encoding

Redundant Pattern Encoding (RPE) technique to a certain degree is similar to the spread spectrum technique. The message is dispersed throughout the cover image with the help of an algorithm. However, using this technique image cropping and rotation cannot be achieved. Multiple small cover images with redundancy increase the chance of recovering even when the stego-image is altered.

D. Distortion Technique

In this technique, the secret message is embedded by distorting the cover image. The receiver then decodes the encrypted image using an algorithm. A sequence of alterations is performed in the cover image. Then this sequence is applied to compare the encrypted message with the forwarded message. The decoder computes the differences between the original and the encrypted image to detect the sequence of alterations to recover the encrypted message. The data is encrypted behind random pixels. For the distortion technique, it is advised that a cover image should only be used once, or else it would be easy for intruders to attack and access the encrypted data.

E. Statistical Technique

Using the statistical technique, the message is encrypted by modifying the statistical properties of the cover image. To send multiple bits, the cover image is split into blocks, each corresponding to a single bit of the message. However, these images are vulnerable to scaling, cropping, and rotating attacks. To tackle these issues, the blocks should be selected based on picture elements, for instance, the faces in a crowd.

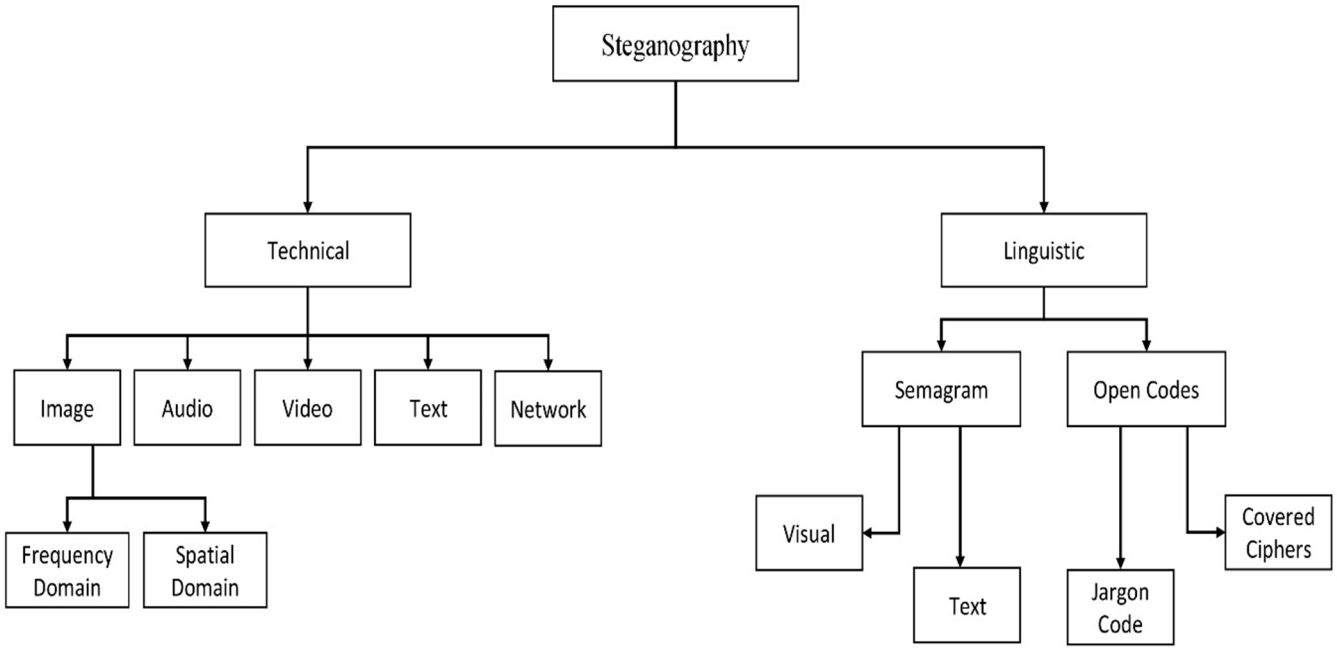


Figure 2: Types of Steganography

F. Transform Domain Technique

This technique is more complex to hide secret data in an image as compared to the other techniques. It can be defined as a domain of encrypting techniques for which several algorithms have been suggested. In this technique, the secret data is encrypted into the frequency domain of the cover image, which is much preferable than compared to the technique of embedding the data in the time domain. The benefit of this technique is that there is no need for data compression and the images are safe from attackers. It is worth saying that most of the strong steganographic systems today operate within the transform domain. Different methods of transforms used in steganography are–

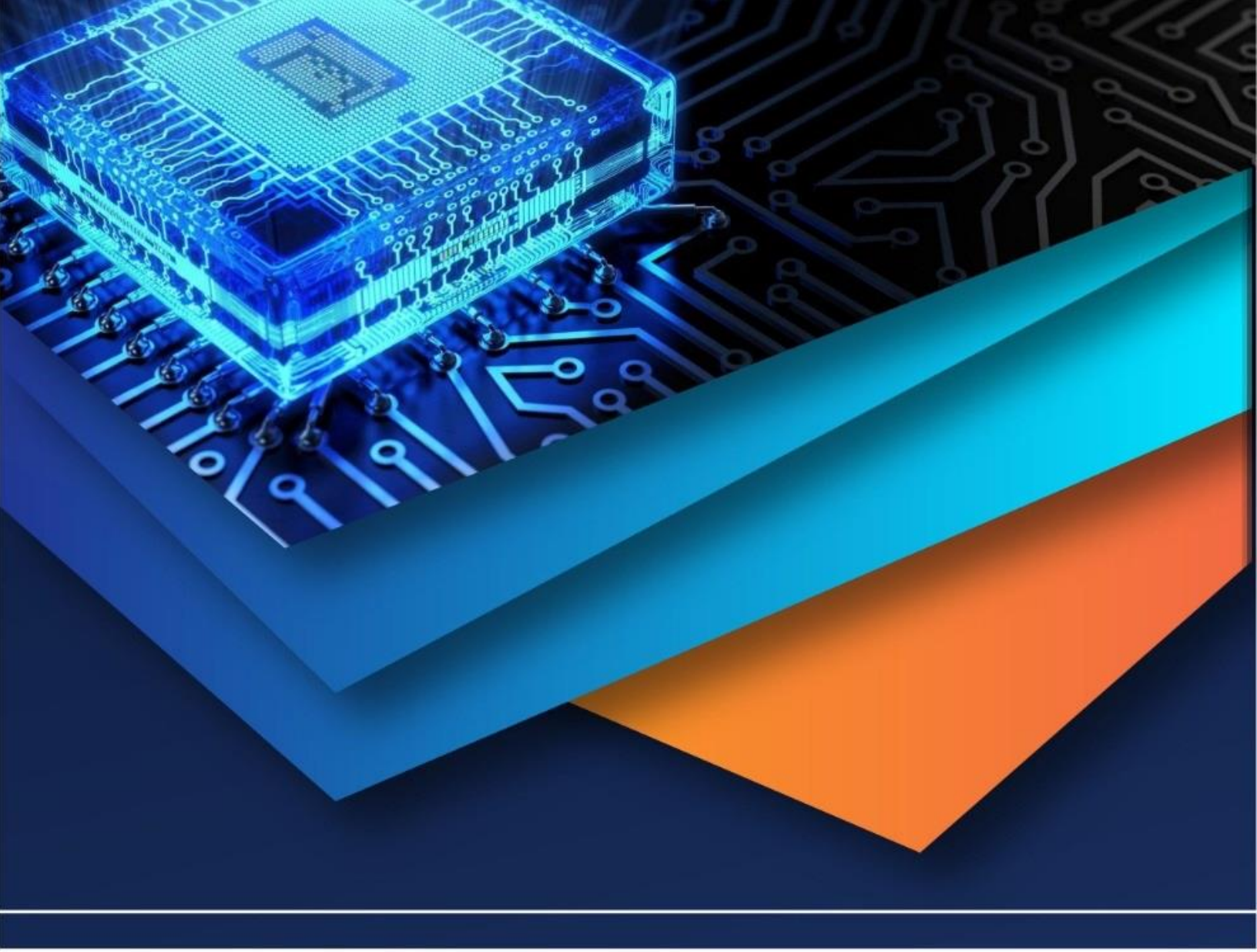
1) Fourier Transform (FT)
a) Discrete Fourier Transform (DFT)
b) Short Term Fourier Transform
2) Discrete Cosine Transform (DCT)
3) Wavelet Transform
a) Continuous Wavelet Transform
b) Discrete Wavelet Transform (DWT)
4) Graph Wavelet Transform

III. CONCLUSION

Steganography is the art of sharing encrypted information by concealing the fact that communication is even taking place. There are many steganography techniques already available and currently in use. This paper reviewed some of the most popular steganography techniques. Some of these techniques like LSB substitution is one of the oldest techniques but it is still preferred due to its simplicity. On the other hand, techniques like Transform Domain are complex but robust. We also learn that the message can also be embedded by using more than one technique together. For instance, the LSB substitution method can be modified with the RPE method to fill the gaps. Also, we can set a unique code to the already encrypted image so that if somehow someone gets to the encrypted image and decodes the message, then also that unique code would be needed to reveal the message. The most suitable technique depends on the user and the purpose it is required for.

REFERENCES

[1] Srishti Rajvanshi, Shrikrishna Sawant, Vedant Tiwari, Anurag Waghmare, Manjiri Gogate, “Image Steganography” International Journal for Research in Applied Science & Engineering Technology (IJRASET)- Volume 7, Issue XI, Nov 2019
[2] Ramadhan Mstafa, Christian Bach, “Information Hiding in Images Using Steganography Techniques” (2013) ASEE Northeast Section Conference
[3] Mustafa Cem Kasapbaşi, Wisam Elmasry, “New LSB-Based Colour Image Steganography Method to enhance the Efficiency in Payload Capacity, Security and Integrity Check” Sādhanā volume 43, Article number: 68 (2018)
[4] Aldi Wiliar Wira Permana, Silvester Dian Handy Permana, Yaddarabullah, “Modification of Least Significant Bit Method with Redundant Pattern Encoding for Protection of Message Integration from Image Modification” International Journal of Scientific & Technology Research, Volume 9, Issue 04, April 2020
[5] Mr. Jayesh Surana, Anirudh Sonsale, Bhavesh Joshi, Deepesh Sharma, Nilesh Choudhary, “Steganography Techniques” (2017) IJEDR, Volume 5, Issue 2, ISSN: 2321-9939
[6] Ashadeep Kaur, Rakesh Kumar, Kamaljeet Kainth, “Review Paper on Image Steganography” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 6, June 2016
[7] Ruchi, Umesh Ghanekar, “A Brief Review on Image Steganography Techniques” Proceedings of ICAEEC-2019, IIIT Allahabad India, 31st May - 1st June 2019
[8] The Types and Techniques Of Steganography Computer Science Essay https://www.ukessays.com/essays/computer-science/the-types-and-techniques-of-steganography-computer-science-essay.php
[9] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, “Digital Image Steganography: Survey and Analysis of Current Methods” (2009) Elsevier B.V
[10] Stuti Goel, Arun Rana, Manpreet Kaur, “A Review of Comparison Techniques of Image Steganography” Global Journal of Computer Science and Technology Graphics & Vision, Volume 13, Issue 4, Version 1.0, Year 2013
[11] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, “A Survey on Image Steganography and Steganalysis” Journal of Information Hiding and Multimedia Signal Processing, Volume 2, Number 2, April 2011



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY