iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XII **Month of publication:** December 2023

DOI: https://doi.org/10.22214/ijraset.2023.57655

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: 7.538
Volume 11 Issue XII Dec 2023- Available at www.ijraset.com

Image Steganography: A Review

Rahul[1], Jyoti[2]
[1]*Department of Computer Science South Point Institute of Technology & Management (SITM), Deenbandhu Chhotu Ram University of Science & Technology (DCRUST), Sonepat*

Abstract: ***An image steganographic scheme is one kind of steganographic systems, where the secret message is hidden in a digital image with some hiding method. Someone can then use a proper embedding procedure to recover the hidden message from the image. The original image is called a cover image in steganography, and the message-embedded image is called a stego image. This Steganography technique is more popular in recent year than other steganography possibly because of the flood of electronic image information available with the advent of digital cameras and high-speed internet distribution. It can involve hiding information in the naturally occurred noise within the image. In this paper we provide a review on various image steganography techniques.***

Keywords: Spatial Domain, Frequency Domain, Patchwork, Spread Spectrum

I. INTRODUCTION

The rise of internet plays an important role in information technology. Nowadays use of internet has been increasing day by day. Providing security has also become important issue due to the use of internet. Cryptography [1] and Steganography are the ways to provide the security to the information. Cryptography is used to encrypt the message so that it is protected from any third parties. Steganography is a method that is used to hide information in a cover so that nobody can guess it. The cover can be any image, text, audio or video. Steganography [2] defines from Greek word 'Stegnos' means secret and 'Graphy' means writing so overall means secret writing. The goal of Steganography is to hide the information whereas cryptography is used to protect the information from intruder or hacker. Due to the availability image file has been popularly used as the carrier.

Embedding data which is to be hidden requires two files first is innocent-looking image that will hold the hidden information, called the cover image. The second file is the message the information to be hidden [3]. Firstly the cover image and hidden message are combined to form stego image. A stego key is used to hide the message and then to extract the message. Most Steganography software use lossless 24 bit images such as BMP rather than JPEG. Each pixel is represented as a single byte in 8 bit GIF files. Pixel value is between 0 and 255.Pixel. Data is index to the color palette with 256 possible colors.

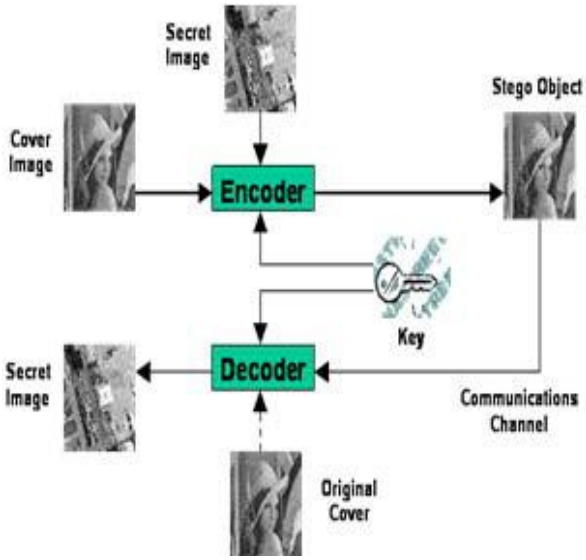


Figure 1: Encoding and Decoding process

In this paper we provide a review on various image steganography techniques.

©IJRASET: All Rights are Reserved

II. IMAGE STEGANOGRAPHY TECHNIQUES

Image Steganography techniques can be classified into two broad categories [4]:

1) Image Domain
2) Transform Domain

Image domain also known as spatial domain techniques embed messages in the intensity of the pixels directly, while for transform domain also known as frequency domain, images are first transformed and then the message is embedded in the image

A. Image Domain

Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterized as "simple systems". The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format.

1) *Least Significant Bit*: Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. For example a grid for 3 pixels of a 24-bit image can be as follows [6]:

Pixels: (00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

A: 10000001
Result: (00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100110 11101001)

2) *LSB and Palette Based Images:* Palette based images, for example GIF images, are another popular image file format commonly used on the Internet. By definition a GIF image cannot have a bit depth greater than 8, thus the maximum number of colours that a GIF can store is 256. GIF images are indexed images where the colours used in the image are stored in a palette, sometimes referred to as a colour lookup table. Each pixel is represented as a single byte and the pixel data is an index to the colour palette. The colours of the palette are typically ordered from the most used colour to the least used colours to reduce lookup time.

GIF images can also be used for LSB steganography, although extra care should be taken. The problem with the palette approach used with GIF images is that should one change the least significant bit of a pixel, it can result in a completely different colour since the index to the colour palette is changed. If adjacent palette entries are similar, there might be little or no noticeable change, but should the adjacent palette entries be very dissimilar, the change would be evident. One possible solution is to sort the palette so that the colour differences between consecutive colours are minimized. Another solution is to add new colours which are visually similar to the existing colours in the palette. This requires the original image to have less unique colours than the maximum number of colours (this value depends on the bit depth used).

Using this approach, one should thus carefully choose the right cover image. Unfortunately any tampering with the palette of an indexed image leaves a very clear signature, making it easier to detect. A final solution to the problem is to use greyscale images. In an 8-bit greyscale GIF image, there are 256 different shades of grey. The changes between the colours are very gradual, making it harder to detect.

B. Transform Domain

Steganography in the transform domain involves the manipulation of algorithms and image transforms .These methods hide messages in more significant areas of the cover image, making it more robust Many transform domain methods are independent of the image format and the embedded message may survive conversion between lossy and lossless compression.

1) *JPEG steganography*: Originally it was thought that steganography would not be possible to use with JPEG images, since they use lossy compression which results in parts of the image data being altered. One of the major characteristics of steganography is the fact that information is hidden in the redundant bits of an object and since redundant bits are left out when using JPEG it was feared that the hidden message would be destroyed. Even if one could somehow keep the message intact it would be difficult to embed the message without the changes being noticeable because of the harsh compression applied. However, properties of the compression algorithm have been exploited in order to develop a steganographic algorithm for JPEGs [7].

One of these properties of JPEG is exploited to make the changes to the image invisible to the human eye. During the DCT transformation phase of the compression algorithm, rounding errors occur in the coefficient data that are not noticeable. Although this property is what classifies the algorithm as being lossy, this property can also be used to hide messages. It is neither feasible nor possible to embed information in an image that uses lossy compression, since the compression would destroy all information in the process. Thus it is important to recognize that the JPEG compression algorithm is actually divided into lossy and lossless stages. The DCT and the quantization phase form part of the lossy stage, while the Huffman encoding used to further compress the data is lossless. Steganography can take place between these two stages. Using the same principles of LSB insertion the message can be embedded into the least significant bits of the coefficients before applying the Huffman encoding. By embedding the information at this stage, in the transform domain, it is extremely difficult to detect, since it is not in the visual domain.

In level of steganography some steganographic algorithms can either be categorized as being in the image domain or in the transform domain depending on the implementation.

C. Patchwork

Patchwork is a statistical technique that uses redundant pattern encoding to embed a message in an image. The algorithm adds redundancy to the hidden information and then scatters it throughout the image. A pseudorandom generator is used to select two areas of the image (or patches) patch A and patch B. All the pixels in patch A is lightened while the pixels in patch B are darkened. In other words the intensities of the pixels in the one patch are increased by a constant value, while the pixels of the other patch are decreased with the same constant value. The contrast changes in this patch subset encodes one bit and the changes are typically small and imperceptible, while not changing the average luminosity.

A disadvantage of the patchwork approach is that only one bit is embedded. One can embed more bits by first dividing the image into sub-images and applying the embedding to each of them. The advantage of using this technique is that the secret message is distributed over the entire image, so should one patch be destroyed, the others may still survive. This however, depends on the message size, since the message can only be repeated throughout the image if it is small enough. If the message is too big, it can only be embedded once.

The patchwork approach is used independent of the host image and proves to be quite robust as the hidden message can survive conversion between lossy and lossless compression [8].

D. Spread Spectrum

In spread spectrum techniques, hidden data is spread throughout the cover-image making it harder to detect. A system proposed by Marvel et al. combines spread spectrum communication, error control coding and image processing to hide information in images.

Spread spectrum communication can be defined as the process of spreading the bandwidth of a narrowband signal across a wide band of frequencies. This can be accomplished by adjusting the narrowband waveform with a wideband waveform, such as white noise. After spreading, the energy of the narrowband signal in any one frequency band is low and therefore difficult to detect. In spread spectrum image steganography the message is embedded in noise and then combined with the cover image to produce the stego image. Since the power of the embedded signal is much lower than the power of the cover image, the embedded image is not perceptible to the human eye or by computer analysis without access to the original image.

III. EVALUATION OF DIFFERENT TECHNIQUES

All the above mentioned algorithms for image steganography have different strong and weak points and it is important to ensure that one uses the most suitable algorithm for an application. All steganographic algorithms have to comply with a few basic requirements. The most important requirement is that a steganographic algorithm has to be imperceptible. The authors propose a set of criteria to further define the imperceptibility of an algorithm [8].

These requirements are as follows:

1) *Invisibility* – The invisibility of a steganographic algorithm is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised
2) *Payload capacity* – Unlike watermarking, which needs to embed only a small amount of copyright information, steganography aims at hidden communication and therefore requires sufficient embedding capacity.
3) *Robustness against statistical attacks* – Statistical steganalys is is the practice of detecting hidden information through applying statistical tests on image data. Many steganographic algorithms leave a "signature" when embedding information that can be easily detected through statistical analysis. To be able to pass by a warden without being detected, a steganographic algorithm must not leave such a mark in the image as be statistically significant.
4) *Robustness against image manipulation* – In the communication of a stego image by trusted systems, the image may undergo changes by an active warden in an attempt to remove hidden information. Image manipulation, such as cropping or rotating, can be performed on the image before it reaches its destination. Depending on the manner in which the message is embedded, these manipulations may destroy the hidden message. It is preferable for steganographic algorithms to be robust against either malicious or unintentional changes to the image.
5) *Independent of file format* – With many different image file formats used on the Internet, it might seem suspicious that only one type of file format is continuously communicated between two parties. The most powerful steganographic algorithms thus possess the ability to embed information in any type of file. This also solves the problem of not always being able to find a suitable image at the right moment, in the right format to use as a cover image.
6) *Unsuspicious files* – This requirement includes all characteristics of a steganographic algorithm that may result in images that are not used normally and may cause suspicion. Abnormal file size, for example, is one property of an image that can result in further investigation of the image by a warden.

The following table 1 compares least significant bit (LSB) insertion in BMP and in GIF files, JPEG compression steganography, the patchwork approach and spread spectrum techniques as discussed in previous section.

Table 1: Comparison of Image Steganography Algorithms

	LSB in BMP	LSB in GIF	JPEG compression	Patch work	Spread spectrum
Invisibility	High	Medium	High	High	High
Payload capacity	High	Medium	Medium	Low	Medium
Robustness against statistical attacks	Low	Low	Medium	High	High
Robustness against image manipulation	Low	Low	Medium	High	Medium
Independent of file format	Low	Low	Low	High	High
Unsuspicious file	Low	Low	High	High	High

IV. CONCLUSION

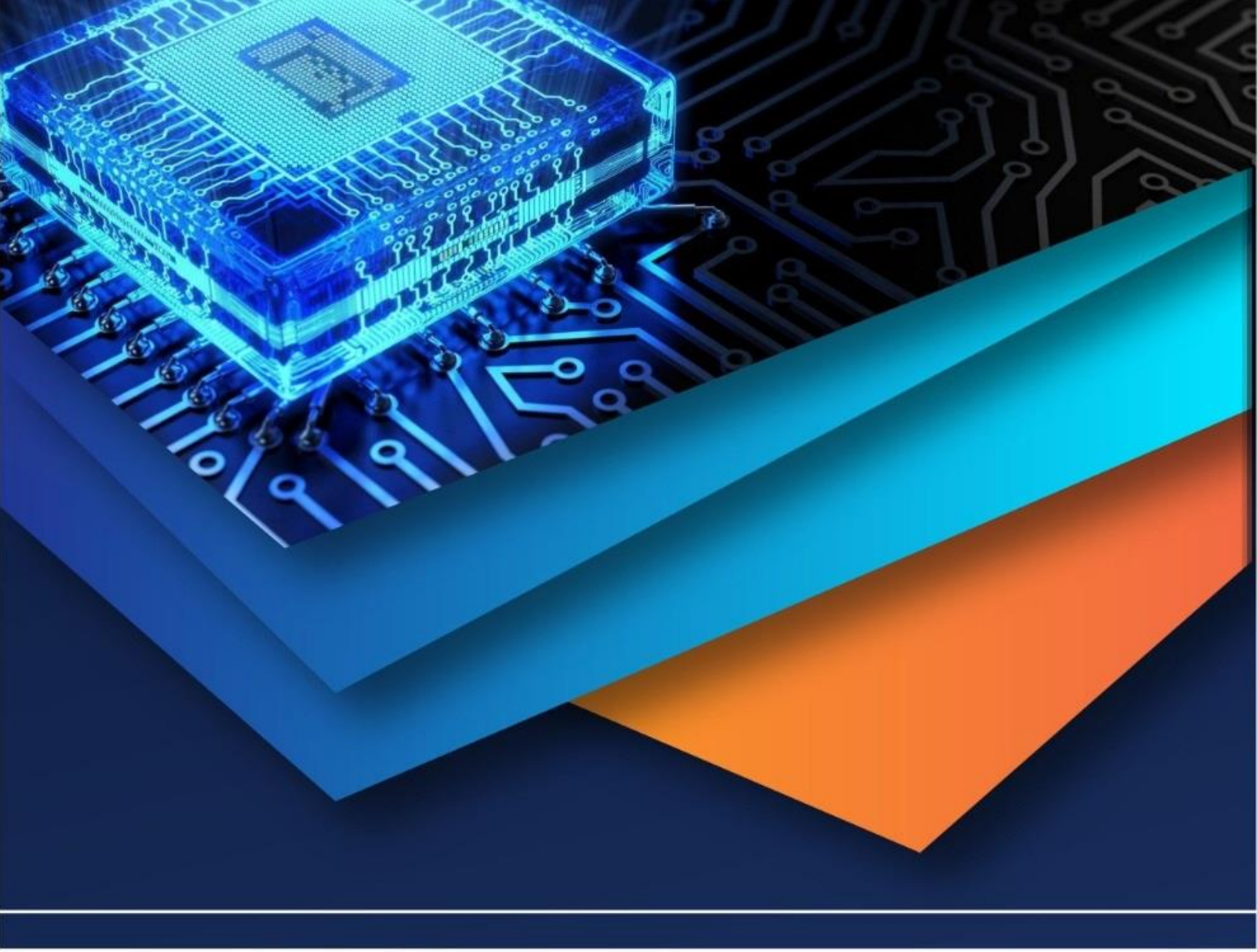
The rise of internet plays an important role in information technology. Nowadays use of internet has been increasing day by day. Providing security has also become important issue due to the use of internet. An image steganographic scheme is one kind of steganographic systems, where the secret message is hidden in a digital image with some hiding method.

Someone can then use a proper embedding procedure to recover the hidden message from the image. The original image is called a cover image in steganography, and the message-embedded image is called a stego image. In this paper we studied a review on various image steganography techniques.

REFERENCES

[1] K. Pachghare, Cryptography & Information Security, Prentice-hall of India Pvt Ltd
[2] Eric Cole, Hiding in Plain Text, Wiley Publishing, Inc. :2003
[3] Stefan Katzenbeisser and Fabien A. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Inc., Norwood, MA, USA, 2000.
[4] Brainos II, A. C. A Study of Steganography and the Art of Hiding Information, East Carolina University, November 13, 2003.
[5] Artz, D. Digital Steganography: Hiding Data within Data. IEEE Internet Computing, May 2001. IEEE.
[6] T. Morkel , J.H.P. Eloff, M.S. Olivier, “An overview of image steganography” Information and Computer Security Architecture (ICSA), 2010
[7] Neil F. Jonhson and S. Jajodia, “Exploring Steganography: Seeing the Unseen”, pp 26-34, IEEE 1998.
[8] A. Cheddad, J. Condell, K. Curran and P.M. Kevitt, "Digital image steganography: survey and analysis of current methods." Signal Processing Journal, 2010..
[9] K B Raja, Venugopal K R and L M Patnaik, "A Secure Stegonographic Algorithm using LSB, DCT and Image Compression on Raw Images", Technical Report, Department of Computer Science and Engineering, December 2004.
[10] P. Kruus, C. Scace,M. Heyman, and M. Mundy. (2003), "A survey of steganography techniques for image files.", Advanced Security Research Journal, 2003.
[11] E Lin, E Delp, “A Review of Data Hiding in Digital Images”, Center for Education and Research Information Assurance and Security, 2011.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)