Performance Analysis of Image Steganography Techniques

Dhruv Chaudhary, LSS Jyotiraditya
Manipal University Jaipur, (MUJ), Rajasthan, India.
dhruv.209303197@muj.manipal.edu
lss.209303292@muj.manipal.edu

Abstract

Image steganography is a technique of hiding secret information inside an image, without altering its visual quality. Various image steganography techniques have been developed to achieve this objective, and their performance varies in terms of the level of security and the amount of information that can be hidden. In this research article, we present a comprehensive performance analysis of various image steganography techniques, including Least Significant Bit (LSB), Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) essentially providing us with the analysis of Spatial Domain technique vs Transform Domain technique. The performance analysis metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE) are discussed. We also analyze the trade-offs between security, capacity, and computational complexity for each of these techniques.

Keywords: *Image steganography, performance analysis, Least Significant Bit (LSB), Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), security, capacity, computational complexity, metrics, Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE)*

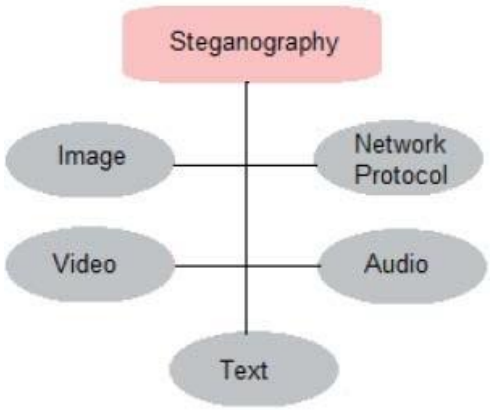
1. Introduction

The term "cover writing" (steganography) derives from the Greek words "steganós" (covered) and "graptos" (writing) [6]. Steganography is frequently referred to as "invisible" communication. Steganography is the practice of hiding the existence of communications in other media (audio, video, image, communication). Multimedia assets including photographs, audio, and videos are often used as cover media in modern steganography systems since they are frequently shared via email and other internet communication tools. That is distinct from securing a message's real content. In plain English, it would be similar to that—information would be concealed within information.

Steganography involves concealing a secret subject within a cover-object without changing the message's structure (carrier object). Cover objects and stego-objects (containing hidden information objects) are comparable subsequent to the steganography procedure. Steganography (the art of hiding information) and cryptography (the science of protecting information) are thus entirely dissimilar. It is challenging to recover information in steganography without following an established technique due to invisibility or hidden factors. Steganalysis is a method of steganography detection.

1.1. Steganography in Various Forms [6]

There are multiple steganographic techniques that are used depending on the kind of cover object to be used. It is depicted in figure below [6].



1.1.1. Image Steganography: Image steganography is the method used to conceal information in images. In this technique, a cover image is utilised as a carrier to hide a secret information. The pixel intensities of the cover image are used to hide the message, which means that the message is embedded in the least significant bits (LSBs) of the pixel values. This technique is widely used because images are easily available and can be easily shared over the internet. The main advantage of image steganography is that it provides high capacity for information hiding, which means that a large quantity of information can be concealed in just a single image.

1.1.2. Video Steganography: Video steganography is a technique used to hide information in digital videos. In this technique, a video is used as a carrier to hide the secret message or information. Generally, discrete cosine transform (DCT) is used to alter the values of the pixels in the video frames to hide the message. The altered values are not noticeable by the human eye, which means that the hidden message remains undetectable. Video steganography is widely used because videos are very popular and are easily accessible on the internet.

1.1.3. Audio Steganography: Audio steganography is a method used to hide information in digital audio files. In this technique, a digital audio format such as WAV, MIDI, MP3, etc. is used as a carrier to conceal the secret message or information. The main advantage of audio steganography is that it provides high security, as the audio files are already compressed, making it difficult for attackers to detect the hidden message.

1.1.4. Network Steganography: Network steganography is a method used to hide information in network protocols such as IP, UDP, TCP etc. This technique utilizes the unused header bits of the network protocols to hide the secret message or information. Primary advantage of network steganography is that it provides high security, as the communication channel is already encrypted, making it difficult for attackers to detect the hidden message.

1.1.5. Text Steganography: Text steganography is a technique used to hide information in text. In this technique, various methods like the white spaces, capital letters, morse code, tab spaces, etc. are used to hide the secret message or information. Text steganography is widely used because it is simple and easy to use. However, the main disadvantage of text steganography is that it provides low capacity for information hiding, which means that only a small amount of information can be hidden in a text file.

1.2. Terminologies related to Image Steganography

Here are some basic terminologies used in Image Steganography: -

- **Cover Image**: A cover image is used as a carrier to hide the secret message or information. The cover image can be any image such as a JPEG, PNG, BMP, etc.
- **Message**: A secret message is the message or information that is hidden inside the cover image using image steganography techniques.
- **Stego-Image**: Once the information is hidden/embedded inside the cover image it is then called the stego-image.
- **Stego-Key**: A key value is utilized for embedding or extracting the hidden content from the stego-images and is called the stego-key.

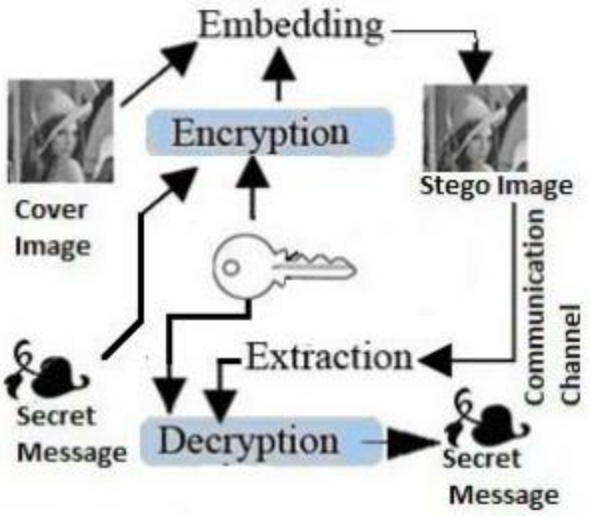


Figure – 2: Image Steganography Working

Generally, image steganography method is used for embedding information inside cover images and creating stego images. Next, using a communication medium, this stego-image is sent to the other user, who is not told of the secret message. Depending on the technique employed, the recipient can fairly readily decipher the image's secret message. Without a stego-key, a basic picture steganography diagram is presented in Figure 2, where a cover image with a message is necessary for the embedding procedure. The result of the embedding approach is a stego-image. This stego-image is then sent to the extraction algorithm, which extracts the message from it.

1.4 Image Steganographic Techniques

The following categories can be used to group image steganography techniques:

1.4.1 Spatial Domain Methods: Multiple variations of spatial steganography methods are present, which directly change some image pixel values to hide data. Least significant bit (LSB)-based steganography is one of the most straightforward techniques for concealing a secret message in the LSBs of pixel values without introducing many observable distortions. LSB value changes are not visible or noticeable to the naked eye. Spatial domain techniques can be classified into the following types[6]:

1. Least significant bit (LSB)
2. Edges based data embedding method (EBE)
3. Pixel value differencing (PVD)
4. Random pixel embedding method (RPE)
5. Pixel intensity-based method
6. Texture based method
7. Histogram shifting methods
8. Mapping pixel to hidden data method
9. Labeling or connectivity method

Least Significant bit (LSB) Method:

The Least Significant Bit (LSB) method is a steganographic technique that involves hiding a secret message in the least significant bits of an image pixel values. In this particular method, the original image is first divided into small blocks of pixels, and then the least significant bit of each pixel in the block is replaced with a bit of the secret message. Since the least significant bit only contains minimal information about the pixel, this modification is typically imperceptible to the human eye. This method is often used for covert communication and can be vulnerable to detection by steganalysis techniques.

Some advantages of spatial domain LSB technique can be:

1. Low chance for reduction in image quality.
2. Capacity for storing information is larger.

Some weaknesses, on the other hand, of LSB technique are:

1. The hidden data might get lost with image manipulation making it less robust.
2. Concealed data can be damaged rather easily by attacks.

1.4.2 Transform Domain Technique: This is a trickier approach to conceal data in an image. The image is subjected to several algorithms and changes to conceal information. A variety of algorithms have been proposed for the embedding approach known as transform domain embedding. The method of embedding data into a signal's frequency domain is far more powerful than the concepts of time-domain embedding. Nowadays, the transform domain is where the majority of powerful steganographic systems operate. Compared to spatial domain techniques, transform domain techniques are more advantageous because they conceal information in portions of the image that are less susceptible to compression, cropping, and image processing. Certain transform domain techniques may outperform lossless and lossy format conversions since they do not appear to be dependent on the image format. Transform domain techniques are broadly classified into[6]:

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).
4. Lossless or reversible method (DCT)
5. Embedding in coefficient bits

Discrete Wavelet Transform (DWT):
The Discrete Wavelet Transform (DWT) is another mathematical technique used in signal processing. It decomposes a signal into a set of wavelet functions, which are used to represent the signal in a multi-resolution fashion. In image processing, the DWT can be used to analyze the spatial frequencies of an image at different scales. This technique is particularly useful for image denoising, compression, and feature extraction.

Discrete Cosine Transform (DCT):
The Discrete Cosine Transform (DCT) is a mathematical technique used to analyze signals such as images, videos, and audio. In image processing, the DCT is applied to a block of pixels in an image to transform it into the frequency domain. The resulting coefficients represent the frequency components of the image in a way that enables compression and other signal processing operations. The DCT is widely used in image and video compression algorithms such as JPEG and MPEG.

1.4.3 Distortion Techniques: In order to recover the hidden message, distortion techniques require knowledge of the original cover image during the decoding phase, when the decoder functions to look for discrepancies between the original cover image and the distorted cover image. To the cover image, the encoder adds a series of modifications. Signal distortion is therefore used to explain the storage of information. With this method, the cover image is modified in a series of ways to produce a stego object. This series of adjustments is used to match the encoded message that must be transmitted. In pixels selected in a pseudo-random manner, the message is encoded. The message bit is a "1" if the stego-image at the

specified message pixel differs from the cover picture; otherwise, it is a "0." The "1" value pixels can be altered by the encoder without affecting the image's statistical characteristics. The advantages of this method are nonetheless constrained by the requirement for supplying the cover image. The cover image should never be used more than once in any steganographic method. The receiver can quickly identify any cropping, scaling, or rotational manipulation of the stego-image. In some circumstances, the modification can even be undone and the original message can be recovered provided the message is encoded with error-correcting information.

1.4.4 Masking and Filtering: Like paper watermarks, these techniques mark an image to conceal information. These methods embed the information in locations that are more important than just blending it into the background noise. The cover image is more crucial to the hidden message. As watermarking techniques are better integrated into the image, there is no need to worry about lossy compression destroying the image when using them.

Advantages of Masking and filtering Techniques:

1. As the information is concealed in the viewable portions of the image, this approach is far more robust than LSB replacement in terms of compression.

Disadvantages of Masking and filtering Techniques:

1. Techniques can be applied only to gray scale images and restricted to 24 bits.

2. Performance Measure Parameters

The most important feature of a steganographic system is the stego picture's good visual quality because detectors have a difficult time detecting distortion between the stego image and the cover image (PSNR). This is a common method of evaluating the quality of an image, and it quantifies how much corrupting noise there is in relation to the maximum strength that a signal can have without impairing the representation's accuracy.

PSNR is measured as per [2,3].

$$\text{PSNR} = 10\frac{\log_{10}(255)^2}{\text{MSE}}\ \text{dB}$$

Where MSE stands for mean-square error, defined as [2,3]

$$\text{MSE} = \frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}(C_{j,k} - I_{j,k})^2$$

Here, $C_{j,k}$ and $I_{j,k}$ represent the pixel location of jth row and Kth column of cover image (C) and stego image (I), respectively, of size $M \times N$. It is hard to distinguish between two similar images (i.e., cover image and stego image) by human eyes when the PSNR is superior to 30 dB [3].

After secret image embedding process, the similarity of original cover images and stego images was measured by the standard normalized cross-correlation (NCC) coefficient as [2]

$$\mathrm{NCC} = \sum_{j=1}^{M}\sum_{k=1}^{N}(C_{j,k} \times I_{j,k})\frac{1}{\sum_{j=1}^{M}\sum_{k=1}^{N}(C_{j,k})^2}$$

The NCC denotes the correlation between two images (i.e. C and I). If NCC (C, I) is closer to 1, then C and I images are highly correlated. NCC = 1 indicates that images compared are 100% similar.
The other image quality measurements parameters are the average difference (AD), the maximum difference (MD) and structural content (SC) have taken for detailed experimental analysis.

Bit Error Rate: Bit error rate (BER) can be calculated as the actual number of bit positions which are changed in the stego-image compared with CVR.

Performance Analysis parameters as per [1].

3. Evaluation of Different techniques

Regarding image steganography, all of the aforementioned methods have both strong and weak features. It is crucial to choose the best strategy to use as a result. As previously said, there are several parameters to gauge the effectiveness of the steganographic technique.

The parameters are [5]: -

- Robustness: This second characteristic gauges how well the steganographic approach can withstand attempts to decrypt the information being concealed. These efforts include data compression, image filtering, and image manipulation (such as cropping or rotation). A reliable steganographic method (outside the purview of this work) is the use of watermarks.
- Payload Capacity: It indicates the most amount of data that may be properly buried and retrieved. Steganography is thought to conceal communication, in contrast to watermarking, which only needs a tiny amount of copyright information embedded; as a result, a substantial embedding capacity is needed. Little bits of data could therefore be concealed using this parameter without being seen by the human eye. On the other side, more data may allow the HVS or statistical tests to find artefacts.
- Imperceptibility: This metric refers to the capacity to evade detection, i.e., where the human eye fails to see it. While not altering the image in a way that can be seen by the human eye, some techniques may nonetheless do so in a way that can be seen by statistical testing. Genuinely secure steganographic methods ought to be imperceptible to statistical and visual inspection.

Now we will discuss previously mentioned techniques on basis of the parameters just discussed.

- Although the LSB technique in the spatial domain is a useful method of information concealment, it is also susceptible to minute alterations brought on by lossy compression or picture processing. Although LSB approaches have a high payload capacity (the ability to conceal huge amounts of information), they frequently adjust for the statistical characteristics of the image, indicating a low level of robustness against statistical attacks and image manipulation [5].

- When the hidden message is small, promising approaches like DCT, DWT, and adaptive steganography are less vulnerable to attacks. This can be explained in terms of how they alter the transform domain coefficients, which minimizes image distortion. Comparing such methods to the spatial domain algorithms, it can be said that they often have a smaller payload. After presenting some encouraging findings, the studies on the discrete cosine transform (DCT) coefficients shifted the researchers' focus to JPEG images. When steganography operates at a level akin to DCT, it becomes significantly more robust and resistant to statistical attacks. In certain ways, embedding in the DWT domain is more effective than DCT embedding, particularly in terms of compression survivability [5].

	LSB	**DCT**	**DWT**
Imperceptibility	High	Medium	Medium
Robustness	Low	Medium	High
Payload Capacity	High	Low	Low

Table: Comparison of Image Steganography techniques

4. Conclusion

This article provided a summary of the various image steganographic techniques, key categories, and classifications that have been put forth in recent years in the literature. As hidden data is raised up to a specific limit utilizing LSB based approaches, the visual quality of the image degrades, according to our careful analysis of several proposed methodologies. And a lot of these embedding approaches can be broken or reveal signs of image change with careful statistical noise analysis or perceptual analysis.

The primary steganographic methods for lossy and lossless picture formats, including JPEG and BMP, were examined in this work. The effects are described using a taxonomy that focuses on the three main steganographic methods used to encrypt image files with information. These methods involve changing the image's spatial properties, transform properties, and file formatting properties. Each of these methods aims to satisfy the three key steganographic design tenets of capacity, resilience, and imperceptibility or undetectability.

Table shows that although one technique may not have enough payload capacity, another may not be sufficiently resilient. For instance, file formatting techniques

can store a lot of data, but they are simple to find and compromise. Similar to LSB approaches, spatial LSB techniques have a large payload capacity but frequently fail to thwart statistical attacks, making them visible. It is significant to note that the LSB technique's hiding capacity is dependent on the cover image being used.

5. References

[1] Sharma, V.K., Srivastava, D.K. and Mathur, P. (2018), Efficient image steganography using graph signal processing. IET Image Processing, 12: 1065-1071. https://doi.org/10.1049/iet-ipr.2017.0965

[2] Khalili M., and Asatryan D.: 'Colour spaces effects on improved discrete wavelet transform-based digital image watermarking using Arnold transform map', *IET Signal Process.*, 2013, **7**, pp. 177–187

[3] Prabakaran G., and Bhavani R.: 'A modified secure digital image steganography based on discrete wavelet transform'. Int. Conf. Computing, Electronics and Electrical Technologies, March 2012, pp. 1096–1100

[4] Ms. Shubhangi Hiwe, Prof. S. I. Nipanikar, 2014, An Analysis of Image Steganography Methods, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 03, Issue 02 (February 2014),

[5] Hamid, Nagham, et al. "Image steganography techniques: an overview." *International Journal of Computer Science and Security (IJCSS)* 6.3 (2012): 168-187.

[6] Hussain, Mehdi, 2013, A Survey of Image Steganography Techniques. *International Journal of Advanced Science and Technology. (2013):* 113-125