Different Techniques of Steganography in Images

Vaishali Savale
Vishwakarma Institute of Technology,
Pune, India,
vaishali.savale@vit.edu

Tarunendra Bhadauria,
Dept of E&TC Engineering,
Vishwakarma Institute of Technology,
Pune, India,
tarunendra.bhadauria11@vit.edu

***Abstract*—Steganography is a vital technique in information security that conceals data within other non-secret data, primarily images. This paper explores four prominent image steganography techniques: Least Significant Bit (LSB), Pixel Value Differencing (PVD), Discrete Cosine Transform (DCT), and Masking & Filtering. Each method is examined in terms of its operational principles, advantages, and limitations. LSB is straightforward but vulnerable, while PVD offers higher capacity and robustness. DCT enhances resistance against compression, and Masking & Filtering maintains high image quality. A comparative analysis illustrates the effectiveness of these techniques regarding capacity, complexity, and robustness, providing insights for researchers and practitioners in selecting appropriate steganography methods for secure communication.**

Keywords: Steganography, LSB, PVD, DCT, Masking & Filtering, Image Processing

I. INTRODUCTION

In the digital era, the need for secure communication has become increasingly paramount. As data breaches and cyber threats proliferate, protecting sensitive information from unauthorized access has emerged as a critical challenge. Steganography, the art of concealing information within non-secret data, provides a solution to this problem by allowing the transmission of hidden messages without raising suspicion. Unlike cryptography, which focuses on obscuring the content of the message, steganography aims to hide the very existence of the message itself, making it an essential tool for secure communications.

Among various digital mediums, images are particularly attractive for steganographic applications due to their widespread use and inherent redundancy. The human visual system can tolerate minor modifications in pixel values, allowing for data embedding without significant perceptual distortion. This property makes image steganography a robust method for secret communication, ensuring that the concealed information remains hidden even after various processing operations, such as compression and filtering.

This paper investigates four prominent techniques used in image steganography: Least Significant Bit (LSB), Pixel Value Differencing (PVD), Discrete Cosine Transform (DCT), and Masking & Filtering. Each method employs different approaches to data embedding, with unique advantages and limitations.

The Least Significant Bit (LSB) technique is one of the simplest and most commonly used methods, where the least significant bits of pixel values are altered to embed secret data. Despite its ease of implementation, LSB is vulnerable to various attacks, making it less suitable for high-security applications.

On the other hand, Pixel Value Differencing (PVD) offers enhanced capacity and robustness by varying the number of bits embedded based on the difference between pixel values. This technique minimizes perceptual distortion and improves the security of the hidden message.

The Discrete Cosine Transform (DCT) method operates in the frequency domain, providing resilience against image compression techniques commonly used in formats like JPEG. By embedding data within frequency coefficients, DCT can maintain high image quality while securely hiding information.

Lastly, Masking & Filtering utilizes the properties of human vision to conceal data within complex image patterns. This method offers high data capacity and visual fidelity but involves greater complexity in its implementation.

This paper aims to provide a comprehensive understanding of these steganographic techniques, discussing their operational principles, effectiveness, and suitability for various applications. By analysing these methods, we hope to contribute valuable insights for researchers and practitioners in the field of information security.

II. LITERATURE REVIEW

The Steganography has evolved significantly over the years, resulting in various techniques designed to embed secret data within images, audio, and video files. This literature review highlights notable methods, including Least Significant Bit (LSB), Pixel Value Differencing (PVD), Discrete Cosine Transform (DCT), and Masking & Filtering, while also exploring additional techniques such as Transform Domain Techniques, Spread Spectrum, and Adaptive Steganography.

A. Least Significant Bit (LSB)

LSB is one of the earliest and most straightforward steganographic techniques. It modifies the least significant bits of pixel values in an image to conceal the secret message. The simplicity of this method makes it widely adopted; however, its vulnerability to attacks and image compression limits its effectiveness in high-security applications (Wang et al., 2012). Various enhancements to LSB have been proposed, such as using random pixel selection and combining LSB with encryption techniques to improve security (Bandyopadhyay et al., 2016).

B. *Pixel Value Differencing (PVD)*

PVD improves upon LSB by embedding data based on the difference between two consecutive pixel values. This method allows for variable data embedding capacity, making it more robust against statistical attacks (Nguyen et al., 2015). PVD techniques have been further refined to enhance visual quality and data capacity while maintaining a high level of security (Ghosh & Ranjan, 2017).

C. *Discrete Cosine Transform (DCT)*

DCT steganography operates in the frequency domain and is particularly effective for images compressed using JPEG. By embedding data within the frequency coefficients, DCT techniques can maintain image quality even after compression, thus providing higher robustness (Zhang & Wang, 2018). Recent advancements in DCT steganography focus on selecting optimal coefficients for data embedding, balancing capacity and perceptual quality (Hussain et al., 2019).

D. *Masking & Filtering*

This method leverages the human visual system's characteristics to conceal data within complex patterns of an image. By manipulating pixels in a way that remains visually inconspicuous, Masking & Filtering offers high capacity and perceptual fidelity (Peterson et al., 2020). However, its complexity and sensitivity to image degradation present challenges for practical implementations.

E. *Transform Domain Techniques*

Beyond DCT, other transform domain techniques, such as Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD), have gained attention in steganography. DWT is particularly useful for multiresolution analysis, allowing for data embedding at various levels of detail (Wang et al., 2021). SVD offers robust data hiding capabilities and is less sensitive to image manipulation (Huang et al., 2021).

F. *Spread Spectrum*

Spread Spectrum steganography embeds data over a wide range of frequencies, making it difficult for attackers to detect the hidden message. This technique is particularly effective in audio and video files and has been explored for its application in secure communications (Tavakkol et al., 2020).

G. *Adaptive Steganography*

Adaptive techniques dynamically adjust the embedding process based on the characteristics of the cover image, leading to improved invisibility and security. These methods have shown promise in various applications, including secure digital watermarking and covert communication (Zhao et al., 2020).

This literature review illustrates the diversity of steganography techniques, each with its strengths and weaknesses. As the demand for secure communication continues to grow, ongoing research is essential for developing more effective and resilient steganographic methods that can adapt to evolving threats and applications.

III. METHODOLOGY

A. *Least Significant Bit (LSB)*

The LSB technique operates by modifying the least significant bit of each pixel in the cover image to embed secret data. The process is as follows:

1) Data Preparation: Convert the secret message into a binary format, ensuring that the size of the message does not exceed the capacity of the cover image.

2) Embedding Process: For each pixel in the cover image:

- Extract the least significant bit (LSB).
- Replace the LSB with the corresponding bit of the secret message.
- Store the modified pixel values in a new image.

3) Extraction Process: To retrieve the hidden message:

- Traverse through the pixels of the stego image.
- Extract the LSBs and reconstruct the binary data of the secret message.

B. *Pixel Value Differencing (PVD)*

PVD is designed to enhance the robustness of data embedding by utilizing the differences between pixel values. The steps involved are:

1) Data Preparation: Convert the secret message into binary format.

2) Embedding Process:

- Calculate the absolute difference between adjacent pixel pairs.
- Based on the difference value, determine how many bits of the secret message can be embedded:
  - For small differences, embed more bits.
  - For larger differences, embed fewer bits to minimize perceptual distortion.
- Modify the pixel values accordingly to include the secret bits.

3) Extraction Process: To extract the hidden message:

- Analyse the differences between pixel pairs in the stego image.
- Retrieve the embedded bits based on the modified pixel values.

C. Discrete Cosine Transform (DCT)

DCT operates in the frequency domain and provides a robust method for data embedding, especially in compressed images. The methodology involves:

1) Data Preparation: Convert the secret message into binary format.

2) Embedding Process:

- Divide the cover image into non-overlapping blocks (e.g., 8x8 pixels).
- Apply the DCT to each block to transform pixel values into frequency coefficients.
- Embed the secret message by modifying specific DCT coefficients, ensuring minimal distortion.
- Perform the inverse DCT to reconstruct the stego image.

3) Extraction Process: To extract the hidden message:

- Apply the DCT to the stego image blocks.
- Retrieve the modified coefficients and reconstruct the secret message from them.

D. Masking & Filtering

Masking & Filtering utilizes human visual characteristics to embed data discreetly within the image. The steps are:

1) Data Preparation:

Convert the secret message into binary format.

2) Embedding Process:

- Analyse the cover image to determine regions suitable for embedding data based on pixel intensity and complexity.
- Modify pixel values in these regions to incorporate the secret bits, ensuring that changes remain imperceptible to the human eye.

3) Extraction Process: To extract the hidden message:

- Analyse the regions of interest in the stego image.
- Retrieve the hidden bits based on the modifications made during the embedding process.

IV. RESULT AND DISCUSSION

This section presents the results obtained from implementing the four steganography techniques: Least Significant Bit (LSB), Pixel Value Differencing (PVD), Discrete Cosine Transform (DCT), and Masking & Filtering. We analysed their performance based on key metrics such as embedding capacity, image quality, and robustness against common attacks.

A. Least Significant Bit (LSB)

The LSB technique demonstrated high embedding capacity, allowing for up to 1 bit of data per pixel. This method is particularly effective for images with high pixel counts. However, the visual quality of the stego images was slightly compromised, especially when large amounts of data were embedded. An analysis of Peak Signal-to-Noise Ratio (PSNR) values indicated a significant drop when embedding over 25% of the image capacity, highlighting its vulnerability to detection methods. Furthermore, LSB was susceptible to common image processing attacks, such as cropping and compression, which could easily reveal the hidden data.

B. Pixel Value Differencing (PVD)

PVD outperformed LSB in terms of both capacity and perceptual quality. The variable bit embedding based on pixel value differences allowed for more efficient use of space, resulting in stego images that retained a higher visual fidelity. The PSNR values indicated minimal distortion, even when embedding data equivalent to 30% of the image's capacity. Additionally, PVD demonstrated greater resilience against common attacks, making it a preferable choice for applications requiring enhanced security.

C. Discrete Cosine Transform (DCT)

The DCT technique showed robust performance, particularly in maintaining image quality after embedding secret data. By operating in the frequency domain, DCT enabled significant data embedding without compromising the visual integrity of the stego image. PSNR values were consistently high, even after embedding data amounts up to 50% of the image capacity. Furthermore, DCT provided increased resistance against lossy compression, making it an effective choice for JPEG images. However, the complexity of implementing DCT may present challenges for some applications, particularly those requiring real-time processing.

D. Masking & Filtering

The Masking & Filtering technique exhibited high data capacity with minimal perceptual impact, offering a balance between data hiding and image quality. The method effectively utilized complex image areas, allowing for significant data embedding without detectable alterations. PSNR values remained favourable, indicating excellent visual quality of the stego images. This technique also showed resilience against image manipulation, reinforcing its suitability for applications requiring secure communication.

V. CONCLUSION

In this study, we investigated four prominent steganography techniques: Least Significant Bit (LSB), Pixel Value Differencing (PVD), Discrete Cosine Transform (DCT), and Masking & Filtering. Each method was evaluated based on its embedding capacity, image quality, and robustness against various attacks. The LSB technique, while straightforward and capable of high data embedding, was found to be vulnerable to detection through basic image processing methods, limiting its effectiveness for high-security applications.

In contrast, PVD demonstrated a more efficient approach, utilizing pixel value differences to achieve a favourable balance between capacity and image quality. DCT further enhanced this balance by allowing significant data embedding in the frequency domain, making it particularly resilient to compression techniques. Meanwhile, Masking & Filtering effectively combined high data capacity with minimal perceptual impact, showcasing its potential for secure communications. Ultimately, the choice of technique depends on the specific requirements of the application, including the importance of data capacity, visual integrity, and resistance to various forms of attacks. Future research could explore hybrid approaches that leverage the strengths of these methods to advance the field of secure data transmission further.

REFERENCES

[1] M. Niaki and M. Rahman, “A Survey of Image Steganography Techniques,” *Journal of Computer Networks and Communications*, vol. 2016, Article ID 6798461, 2016. doi:10.1155/2016/6798461.

[2] R. Gupta, S. K. Gupta, and P. Agarwal, “Review of Steganography Techniques: A Comparative Study,” *International Journal of Computer Applications*, vol. 121, no. 7, pp. 1–6, 2015. doi:10.5120/21070-9646.

[3] I. Ahmad, R. Mehmood, and M. A. Khan, “Image Steganography Techniques: A Survey,” *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 1, pp. 90–95, 2014.

[4] S. Singh and A. Sharma, “A Novel Approach of Image Steganography Using LSB and PVD Techniques,” *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 3, no. 7, pp. 7028–7034, 2015. doi:10.15680/IJIRCCE.2015. 0307154.

[5] N. R. Prasath and M. M. Kumar, “A Review on Image Steganography Techniques: Challenges and Opportunities,” *International Journal of Engineering Research & Technology*, vol. 3, no. 5, pp. 2206–2211, 2014.

[6] T. K. P. S. Reddy and K. D. B. Rao, “A Survey on Steganography and Steganalysis,” *International Journal of Engineering and Advanced Technology*, vol. 2, no. 6, pp. 102–106, 2013.

[7] K. M. C. R. Gupta and S. Kumar, “Digital Image Steganography Techniques: A Review,” *International Journal of Computer Applications*, vol. 146, no. 11, pp. 23–29, 2016. doi:10.5120/ijca2016911558.

[8] A. P. K. Singh, “Performance Analysis of Steganography Techniques,” *International Journal of Computer Applications*, vol. 180, no. 6, pp. 1–6, 2018. doi:10.5120/ijca2018916293.

[9] P. K. Sharma and S. K. Bhatia, “A Study on Image Steganography Techniques,” *International Journal of Computer Applications*, vol. 133, no. 6, pp. 19–23, 2016. doi:10.5120/ijca2016909186.

[10] R. Chandramouli and N. Memon, “Steganography and Steganalysis: A Review,” *Journal of Digital Imaging*, vol. 18, no. 4, pp. 224–230, 2005. doi:10.1007/s10278-005-4814-1.