Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

A Study and Implementation of Image Steganography using DCT and DWT Techniques

Komal Vasant Utane

Student, Computer Science & Engineering, Guru Nanak Institute of Engineering & Technology

Abstract

Image steganography is a technique used to hide confidential information within digital images to ensure secure communication. With the rapid growth of digital communication, protecting sensitive data from unauthorized access has become a major concern. This research focuses on various image steganography techniques such as Least Significant Bit (LSB), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT).

The study analyzes both spatial and frequency domain techniques for embedding secret data into images. The proposed approach combines DCT and DWT methods to enhance security and robustness. Performance evaluation is carried out using parameters such as Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE).

The results demonstrate that the combined DCT-DWT approach provides better imperceptibility and resistance against attacks compared to traditional methods.

Keywords: Image Steganography, Data Hiding, DCT, DWT, LSB, PSNR, Security

1. Introduction

In today's digital era, communication over the internet has become essential. However, ensuring the security and privacy of transmitted data remains a significant challenge. Traditional encryption techniques protect the content of communication but do not hide its existence.

Steganography, on the other hand, provides a solution by concealing the presence of communication itself. Image steganography is widely used because images contain a large amount of redundant data, making them suitable for hiding information.

A steganographic system consists of three main components:

- Cover Image
- Secret Message
- Stego Image

Techniques used in image steganography are broadly classified into:

- Spatial Domain Techniques (e.g., LSB)
- Frequency Domain Techniques (e.g., DCT, DWT)

2. Literature Review

Steganography is the art of hiding secret information within a medium such that its existence is not detectable. It has been used historically for secure communication and is now widely applied in digital media.

2.1 Types of Steganography

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography

2.2 Techniques

- **LSB (Least Significant Bit):** Simple and widely used but less secure
- **DCT:** Used in JPEG compression, provides better robustness
- **DWT:** Provides multi-resolution analysis and improved security

2.3 Limitations of Existing Systems

- Low resistance to attacks in spatial domain
- Data loss in lossy compression
- Limited capacity

3. Methodology

3.1 Proposed System

The proposed system uses a hybrid approach combining DCT and DWT for secure data embedding.

3.2 Steps of Algorithm

[01] Select cover image
[02] Convert image into RGB planes
[03] Apply DWT on selected plane
[04] Divide image into sub-bands (LL, HL, LH, HH)
[05] Apply DCT on HH band
[06] Convert secret message into binary
[07] Embed data using LSB technique
[08] Apply inverse DCT and inverse DWT
[09] Generate stego image

4. Implementation

The system is implemented using Python with libraries:

- Tkinter (GUI)
- PIL (Image Processing)

Steps:

- Load image
- Encode secret message
- Save stego image
- Decode message

5. Results & Analysis

The performance of the system is evaluated using:

5.1 PSNR (Peak Signal to Noise Ratio)

Measures quality of stego image

5.2 MSE (Mean Square Error)

Measures error between original and stego image

5.3 Observations

- DCT-DWT method shows higher PSNR
- Less distortion in image
- Better security compared to LSB

6. Conclusion

Image steganography is an effective technique for secure communication. The combination of DCT and DWT provides improved security, better image quality, and resistance against attacks.

The proposed system successfully hides data without noticeable changes in the image, making it suitable for secure data transmission.

7. Future Scope

- Use of Deep Learning for better security
- Real-time steganography systems
- Improved resistance against steganalysis
- Application in video steganography
- Add captions/headings for figures and table using their “caption” option/setting.

References

1. R. Vijayrajeswari et al., “Image Steganography Techniques”
2. N. Saxena and G. Agarwal, “DCT based Steganography”
3. Various IEEE papers on DWT and Image Processing