Digital Image Steganography: A Frequency Domain Approach

Shreyas Wankhede
ai21btech11028@iith.ac.in

Abhishek Kumar
ai21btech11003@iith.ac.in

Pradeep Mundlik
ai21btech11022@iith.ac.in

Sathvika Marri
ai21btech11020@iith.ac.in

Jacky Meena
ee21btech11025@iith.ac.in

Abstract

This project delves into digital image steganography, a vital component of secure communication in today's digital landscape. Steganography conceals sensitive information within seemingly innocuous cover media, offering a covert alternative to encryption. Focusing on the frequency domain approach, mainly using techniques like the Discrete Fourier Transform (DFT), this study explores embedding secret data within digital images. By manipulating the frequency components, imperceptible alterations are made to the digital images, ensuring the confidentiality and integrity of the hidden information. The paper provides a comprehensive overview of digital image steganography, discussing its methodologies and applications.

1. Introduction

In today's digital age, the importance of secure communication and data transmission cannot be overstated. With the proliferation of digital platforms and the vast exchange of information over networks, ensuring the confidentiality and integrity of sensitive data has become paramount. This has led to the emergence of various techniques and methodologies aimed at concealing information within digital media, one of which is steganography.

Steganography, derived from the Greek words "steganos" (meaning covered or concealed) and "graphein" (meaning writing or drawing), is the art and science of hiding secret information within innocuous cover media in such a way that the existence of the hidden message remains undetectable to unintended recipients. Unlike cryptography, which focuses on encrypting the content of a message to render it unintelligible to unauthorized parties, steganography ensures that the existence of the hidden information itself is not apparent.

Steganography techniques can be broadly categorized into various types based on the cover media, such as text, audio, video, and images. In this project, we specifically focus on digital image steganography, leveraging the frequency domain approach facilitated by techniques like Discrete Fourier Transform (DFT).

Digital image steganography involves embedding secret data into digital images, exploiting the imperceptible alterations that can be made to the pixel values or the frequency components of the image. By utilizing transformations like DFT, which represent images in terms of their frequency components, we can embed information in a manner that is robust against typical image processing operations while minimizing perceptual distortion.

By employing the frequency domain approach, we aim to achieve efficient and imperceptible hiding of information within images, thereby ensuring both the secrecy and integrity of the concealed data.

2. Problem Statement

Developing a robust digital image steganography method that enhances the imperceptibility and capacity of hidden information within images. By leveraging the Fourier Transform, this technique will seek to embed data without compromising the image's visual integrity, ensuring that the embedded message remains undetectable to both visual and algorithmic detection methods while maintaining resistance to common image processing operations.

3. Literature Review

Old popular data hiding techniques have generally revolved around modifying the least significant bit (LSB) of the pixel values of an image, which often overwrites visual structures and makes the hidden messages vulnerable to visual detection methods. The importance of Fourier Transformation in data hiding techniques has been seen rarely in the literature. In early work, researchers have used it by encoding the hidden message in coefficients of the Discrete Fourier Transform (DFT) magnitude. This approach overcomes the shortcomings of old techniques by exploiting the spectral properties of Fourier Transformation, improving capacity, security, and robustness.

An important fact that the paper builds on is that as long as the Fourier phase of an image remains intact, the original appearance remains intact with very minute visible artifacts if the Fourier magnitude of the image is slightly modified. Experimental results show that the hidden message image may be as large as half the size of the carrier image for an unnoticeable amount of noise artifacts in the stego image.

Experimental evidence has established that the human visual system is much more sensitive to brightness than color. Therefore, the color and brightness separation strategy is used, avoiding altering the luminance channel. Altering the chrominance channels of an image has very few visible artifacts, almost not detectable by the human eye. Thus, the hidden message is embedded into the Fourier magnitude spectrum of the chrominance channels of the image.

The paper presents a method of transforming the image into the Lab* space non-linearly, following the color/brightness separation strategy. This transformation specifies the color of an image into human perception independently of any particular imaging device. The non-linear operation converts the RGB tuple into the Lab tuple, where L is the luminance channel, and a and b are the chrominance channels. This technique has almost double the hidden data carrying capacity than previous techniques. The DFT of the chrominance channels a and b is taken to embed the secret data, separating magnitude and phases in each of the chromatic channels. The hidden message is embedded by replacing high-frequency areas of chrominance channels in the Fourier magnitude of the chrominance channels, preventing aliasing when extracted. After modifying the Fourier magnitude of a and b chrominance channels and combining them with their corresponding phases, the Inverse Discrete Fourier Transform (IDFT) is applied to get the modified color/brightness-separated image tuple (L ,a' ,b'). Then, this tuple is transformed into the modified image tuple (R',G',B'), resulting in the stego image S = (R',G',B').

To recover the hidden information, the process is reversed. First, the stego image is converted into the Lab* space by the non-linear transformation used during the hiding phase. Then, the DFT of the chromatic channels a' and b' is taken, and the security key for-loop is applied to recover the hidden message. The first part of the hidden message is extracted from the high-frequency areas in the Fourier chrominance-a magnitude spectrum, and the second hidden image is extracted from the high-frequency areas in the Fourier chrominance-b magnitude spectrum. The technique provides a 3-layered security measure because the resultant image scatters the hidden image three times across all pixels of the carrier image. This scattering leads to robustness to stego medium tampering. As long as 40% or more of the stego image data remains intact, the hidden message image can be extracted with reasonable integrity.

The paper demonstrates the robustness of this image hiding technique to various tampering effects, such as cutting parts of the image, repainting the image, and rotating the stego image, while still being able to recover the message.

In general, a technique qualifies as a steganography technique broadly based on:

1. Transparency: How much information you can hide in the cover image (stego hidden) without distorting the original appearance of the image much so that it is undetectable by any visual attacks.
2. Robustness/Tamper resistance: The ability of the hidden message to remain undamaged even if the stego image undergoes some sort of transformation like filtering (linear and blurring), blurring, cropping, repainting.

We can see clearly that the technique mentioned in the paper satisfies the above properties. In total, the paper presents a very secure, high-capacity, tamper-resistant technique to hide some secrecy exploiting the color/brightness of the image and spectral properties of the Fourier-transformed image.

References

[1] Sos S. Agaian, Khaled M. Mstafa, and Khaled Elleithy. Frequency domain approach of image steganography. https://www.researchgate.net/publication/309425281_Frequency_Domain_Approach_of_Image_Steganography, 2016.

[2] CIE Commission. Cie homepage. http://www.cie.co.at, 2021.

[3] Tamer Rabie. Digital image steganography: An fft approach. https://www.researchgate.net/publication/269705199_Digital_Image_Steganography_An_FFT_Approach, 2018.

[4] Wikipedia. Discrete fourier transform. https://en.wikipedia.org/wiki/Discrete_Fourier_transform, 2021.

[5] Wikipedia. Fast fourier transform. https://en.wikipedia.org/wiki/Fast_Fourier_transform, 2021.

[6] Wikipedia. Steganography. https://en.wikipedia.org/wiki/Steganography, 2021.

[7] YouTube. Digital image steganography. https://www.youtube.com/watch?v=u_luy52v7z4, 2021.