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 or patternizing the least significant bit (LSB) of the pixel values of an image. Modifying low bit planes of an image often overwrites visual structures that exist to some degree in all of the image's bit layers. Hidden messages within the low bit planes of an image can potentially be deciphered visually. Thus, stego systems modifying the LSB often exhibit vulnerability 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 the coefficients of the DFT magnitude. This

paper presents a similar idea, overcoming the shortcomings of old techniques by exploiting the spectral properties of Fourier Transformation. It improves three different aspects: capacity, 3-layer security, and robustness of hiding data.

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, in general, the hidden message 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 to color. This can be reasoned out because high-frequency information, i.e., fine details and edges, etc., mainly come from the brightness/luminance channels of an image. Most importantly, we use the color and brightness separation strategy and avoid altering the luminance channel. Experiments have revealed that altering the chrominance channels of an image has very few visible artifacts (almost not detectable by the human eye). Thus, we exploit not only the spectral properties of the image but also the chrominance and achromatic (luminance) properties of the image. In total, we embed the hidden message into the Fourier magnitude spectrum of the chrominance channels of the image.

Without significantly altering the visual quality of the image, the paper presents a technique of transforming the image into the L*a*b* space nonlinearly, following the color/brightness separation strategy. This transformation specifies the color of an image in a way that is independent of the characteristics of any particular imaging device. Let's call the image I=(R,G,B). The nonlinear operation converts the tuple (R,G,B) into the tuple (L,a,b), where L is the luminance channel and a and b are the two chrominance channels. Thus, this technique has almost double the hidden data carrying capacity than previous techniques. Now, we take the DFT of the chrominance channels a and b to embed the secret data. We separate the magnitude and phases in each of the chromatic channels. Most specifically, we embed the hidden message by replacing high-frequency areas of the chrominance channels of the Fourier magnitude of the chrominance channels. This type of embedding prevents aliasing of the hidden message when extracted. Aliasing refers to a phenomenon where high-frequency components in a signal are incorrectly represented or distorted in a reconstructed version of the signal due to insufficient sampling. In our case, high-frequency components appear as mirroring of parts of the hidden image from one side onto the opposite side and thus cause data loss. We partition the secret information into channel a and the rest in channel b. We hide the secret message through a for-loop which later acts as a security key for recovering the message. Without knowing the correct embedding loop, it becomes a guessing game for successfully recovering the hidden information. After modifying the Fourier magnitude of the a and b chrominance channels, we then combine them with their corresponding phases. We then apply the inverse FFT to the modified DFTs of the a and b channels to get the modified color/brightness separated image tuple (L,a',b'), where a' is the modified chromatic channel a and b' is the modified chromatic channel b. Then we transform (L,a',b') to the modified image tuple (R',G',B'). Here we get our stego image (image carrying the hidden information) S=(R',G',B').

Now let's look at how to recover the hidden information. The extraction of the secret message is just the process that is the reverse of hiding it. First, we convert (R',G',B') to (L,a',b') by the nonlinear transformation that was used during the hiding phase. Then we take the DFT of the chromatic channels a' and b'. Finally, we apply the security key for-loop 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, making sure that the for-loop used to extract the hidden images is the same for-loop that was used to embed these hidden images. Thus, we encode and decode the secret message, compromising the minor color artifacts in the stego image. The interesting fact about this technique is that it provides a 3-layered security measure because the resultant image has the effect of scattering the hidden image (info) three times across all pixels of the carrier image. The first scattering is when we multiply the modified chromatic channel Fourier magnitude with its unmodified phase. The second scattering is when we do the inverse FFT of the DFT of the chromatic channel, and the third scattering is when we convert (L,a',b') to (R',G',B'). This scattering leads to robustness to stego medium tampering. The most powerful fact about this technique is that because of the above scattering, as long as 40 or more of the stego image data remains intact, we can extract the hidden message image with reasonable integrity. The paper then demonstrates the robustness of this image-hiding technique to tampering (manipulating) degradations in the stego image by simulating different tampering effects like cutting parts of the image, repainting the image, rotating the stego image, etc., and still being able to recover the message in a legitimate, understandable amount.

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.