CMPE 362

Introduction to Signals for Computer Engineers

Term Project

Image Watermarking

Students:

Hatice Kübra AKSU
Umut DEMİR

Instructor:

Fatih ALAGÖZ

Teaching Assistant:

Özdeniz DOLU

I. Introduction

The rapidly advancing digital landscape has transformed the way we interact with and manipulate data. The representation, analysis, and processing of signals – in particular, the transformation of these signals from one form to another – form a cornerstone of digital technologies. In the realm of Computer Engineering, signal processing plays a crucial role, opening a vista of applications ranging from image and data compression, pattern recognition, to security such as in digital watermarking. This document aims to provide a comprehensive examination of digital watermarking, a dynamic field of signal processing that encompasses both the necessity for copyright protection and the innovative technical solutions it provides.

Digital watermarking refers to the process of embedding a specific pattern or set of bits, known as a watermark, within a digital signal which can be an image, audio, video, text, or 3D data. The objectives of watermark embedding range from the assertion of copyright ownership, detection of unauthorized alterations in content, to managing digital rights by prescribing permitted operations on the digital content. The goal, regardless of the application, remains to embed the watermark in such a manner that it is both imperceptible to human senses and robust against typical signal processing operations and malicious attacks.

Signal processing context:

In the signal processing context, two transformative techniques form the backbone of most watermarking systems: Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). Each of these techniques features unique strengths and applications, leading to distinct performance characteristics in the watermarking domain.

DCT-based watermarking:

DCT-based watermarking operates by transforming the host signal from the spatial domain to the frequency domain. The watermark is then inserted into the mid-frequency components of the transformed signal. This method leverages the energy compaction property of DCT to make the watermark less perceptible and more resistant to common signal processing techniques.

DWT-based watermarking:

On the other hand, DWT-based watermarking involves hierarchical decomposition of the signal using wavelet transforms, followed by watermark embedding into the high-frequency sub-bands. This method benefits from the multi-resolution characteristics of wavelets, allowing for a better trade-off between the perceptibility and robustness of the watermark.

This report provides a detailed comparative study between DCT and DWT-based watermarking techniques, as implemented in a project undertaken as part of a signal processing course for computer engineering. The discussion delves into the nuances of the mathematical foundations, algorithmic implementations, and the experimental results associated with both these techniques, thereby laying the groundwork for a more profound understanding of the theoretical and practical aspects of digital watermarking. This project analysis is not only critical for assessing the performance of the implemented techniques but also for setting a robust foundation for future research and development in this field.

II. Discrete Cosine Transform (DCT) Based Watermarking

Digital watermarking harnesses the power of various signal processing techniques to achieve its goal of embedding information subtly and robustly within digital content. Among these techniques, the Discrete Cosine Transform (DCT) holds a pivotal role owing to its excellent energy compaction properties and its high compatibility with the human visual system. This section aims to delve deeper into the underlying concepts of DCT-based watermarking, its mathematical formulations, and the algorithmic implementation.

II.I. Understanding the Discrete Cosine Transform (DCT)

The Discrete Cosine Transform, in essence, is a technique that transforms a signal from the spatial domain (where each pixel is considered individually) into the frequency domain (where groups of pixels form patterns). This transformation facilitates the representation of the signal in terms of its frequency components, thereby segregating the image data into different spectral sub-bands. Each of these spectral bands varies in their perceptual significance to the overall image quality.

The mathematical formulation of the 2D DCT for an image block is given by:

$$X(u,v) = \frac{1}{4}C(u)C(v)\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}x(i,j)cos\left[\frac{(2i+1)u\pi}{2N}\right]cos\left[\frac{(2j+1)v\pi}{2N}\right]$$

where:

x(i, j) denotes the pixel value at the i-th row and j-th column of the image block.
X(u, v) signifies the DCT coefficient at the u-th row and v-th column of the DCT matrix.
N represents the size of the image block, and α(u) and α(v) are normalizing constants.

The transformation segregates the DCT coefficients into different frequencies. The top-left corner of the DCT matrix corresponds to the lowest frequency, often referred to as the DC component. It represents the average intensity of the pixels in the block. As we move towards the bottom-right corner of the matrix, the frequency increases, corresponding to the changes or details in the image block.

II.II. Algorithm Description

The algorithm for DCT-based watermarking follows these steps:

Load the source image and the watermark image.
Normalize the source image and watermark image to the range [0, 1].
If the watermark image is in color, convert the source image to grayscale.
Apply the block-wise DCT operation on the source image.
Create a binary mask indicating the areas where the watermark will be embedded.
Resize the watermark image to match the size of the binary mask.
For each block in the DCT-transformed image:
- If the corresponding location in the binary mask is 1, modify the DCT coefficient by adding the product of the watermark and the embedding strength.
Reconstruct the watermarked image by applying the inverse DCT operation.
Extract the watermark from the watermarked image.
Display the original image, watermarked image, and extracted watermark.
Calculate the root mean square error (RMSE) values to evaluate the quality of the watermark extraction.
Plot the RMSE values.

II.III. DCT Functionality

The algorithm utilizes the following DCT-related functions:

dct2(): Performs a 2D Discrete Cosine Transform on an image block.
idct2(): Performs the inverse 2D Discrete Cosine Transform to reconstruct the image block from DCT coefficients.

The DCT operation is applied block-wise on the image using the dct2() function. Each block is transformed into its frequency domain representation. The DCT coefficients are modified according to the watermark pattern and the embedding strength. The inverse DCT (idct2()) is then applied to reconstruct the watermarked image.

II.IV. Embedding Process in DCT-Based Watermarking

The uniqueness of DCT-based watermarking lies in the fact that the watermark is embedded into the mid-frequency components of the DCT-transformed image. Mid-frequency components are chosen as they strike a balance between robustness and imperceptibility. These components are less prone to typical signal processing attacks than high-frequency components and less perceptible to the human eye than low-frequency components.

The process of watermark embedding modifies the DCT coefficients according to the watermark signal, and this can be mathematically represented as:

$$X_{wm}(u, v) = X(u, v) + \gamma \cdot W(u, v)$$

where:

$X_{wm}(u, v)$ is the watermarked DCT coefficient
$X(u, v)$ is the original DCT coefficient
$W(u, v)$ is the watermark pattern, and
γ represents the watermarking strength, determining the robustness and perceptibility of the watermark.
In a DCT-based watermarking algorithm, we firstly conduct a block-wise DCT operation on the host image. Then, the watermark embedding operation adjusts the DCT coefficients of the selected blocks in the middle frequencies.

The watermark embedding operation can also be depicted in the form of the following pseudo-code:

```
for each block in the DCT_image:
    if mask[block_index] == 1:  # binary mask indicating where the watermark should be embedded
        DCT_image[block_index] += γ * watermark[block_index]  # watermark is the watermark pattern
```

In the above pseudo-code, DCT_image is the DCT-transformed host image. mask is a binary mask indicating where the watermark should be embedded, γ is the watermarking strength determining the degree of the DCT coefficient modification, and watermark is the watermark pattern that needs to be embedded. The block_index corresponds to the indices of the DCT coefficients in the mid-frequency bands of each block in the DCT-transformed host image.

II.V. Advantages and Strengths of DCT-Based Watermarking

DCT-based watermarking offers several advantages and strengths that make it a popular choice for embedding watermarks in digital images. These advantages are as follows:

Energy compaction: One of the key strengths of DCT-based watermarking is its ability to compact the majority of an image's energy into a small number of low-frequency DCT coefficients. The energy compaction property allows for the embedding of watermarks in perceptually insignificant components of the image. By focusing on these coefficients, DCT-based watermarking minimizes the visibility of the watermark, ensuring that it remains subtle and unobtrusive to the human visual system. This results in a watermarked image that closely resembles the original image, maintaining its quality and visual appearance.

Robustness against common attacks: DCT-based watermarking exhibits robustness against common attacks and image processing operations. Watermarks embedded in mid-frequency DCT coefficients are inherently resilient to various attacks such as compression, noise addition, and filtering. The information contained in these coefficients is less affected by such operations, allowing the watermark to remain intact even when the watermarked image undergoes typical digital manipulation. This robustness ensures that the watermark persists and remains detectable, even in the presence of unintended modifications or intentional attacks.

Imperceptibility: DCT-based watermarking strikes a balance between watermark invisibility and robustness. By embedding the watermark in mid-frequency bands, the modifications made to the image are often imperceptible to the human visual system. This means that the watermarked image appears visually close to the original image, maintaining its quality and perceptual integrity. The imperceptibility of the watermark is a crucial factor in watermarking applications, as it ensures that the presence of the watermark does not interfere with the overall visual experience or usability of the image.

Compatibility: DCT is a widely used and well-established transform technique in image and signal processing. It is supported by numerous software libraries, tools, and platforms, making DCT-based watermarking easily implementable and compatible with various applications. The availability of DCT functions and algorithms simplifies the integration of DCT-based watermarking into existing software systems and workflows. This compatibility enhances the practicality and versatility of DCT-based watermarking, enabling its adoption in a wide range of digital media applications.

In summary, DCT-based watermarking offers several advantages and strengths, including energy compaction, robustness against common attacks, imperceptibility, compatibility, high embedding capacity, and computational efficiency. These advantages contribute to the effectiveness and popularity of DCT-based watermarking in digital media applications, providing a robust and efficient solution for protecting the integrity, authenticity, and ownership of digital images.

II.VI. Limitations of DCT-Based Watermarking

While DCT-based watermarking offers numerous advantages, it is important to consider its limitations. These limitations include:

Lack of geometric robustness: DCT-based watermarking is sensitive to geometric attacks such as rotation, scaling, and cropping. Since DCT is applied block-wise to the image, any geometric modification can disrupt the block membership, affecting the integrity and extraction of the watermark. Geometric transformations can alter the positions of the image blocks, causing misalignment between the embedded watermark and the corresponding blocks during watermark extraction. This limitation restricts the effectiveness of DCT-based watermarking in scenarios where geometric distortions are a concern, such as when the watermarked image needs to be resized or undergoes transformations in different orientations.

Limited resistance to advanced attacks: While DCT-based watermarking demonstrates robustness against common attacks, it may be susceptible to sophisticated attacks specifically designed to remove or manipulate the watermark. Advanced attackers with knowledge of the watermarking algorithm and access to the watermarked image can employ targeted attacks to undermine the integrity and effectiveness of the watermark. These attacks may involve carefully designed image manipulations or intentional removal of specific DCT coefficients associated with the watermark. To enhance the security of DCT-based watermarking, additional measures such as encryption, authentication mechanisms, or the use of multiple watermarking techniques can be considered.

Sensitivity to image content: DCT-based watermarking can be sensitive to the content of the image being watermarked. Images with high-frequency details or complex textures may result in less effective watermark embedding due to the distribution of energy across a wider range of DCT coefficients. In such cases, the watermark may become more visible or susceptible to attacks, compromising its robustness. It is important to consider the characteristics of the image content and adapt the watermarking technique accordingly to maintain the desired level of imperceptibility and robustness.

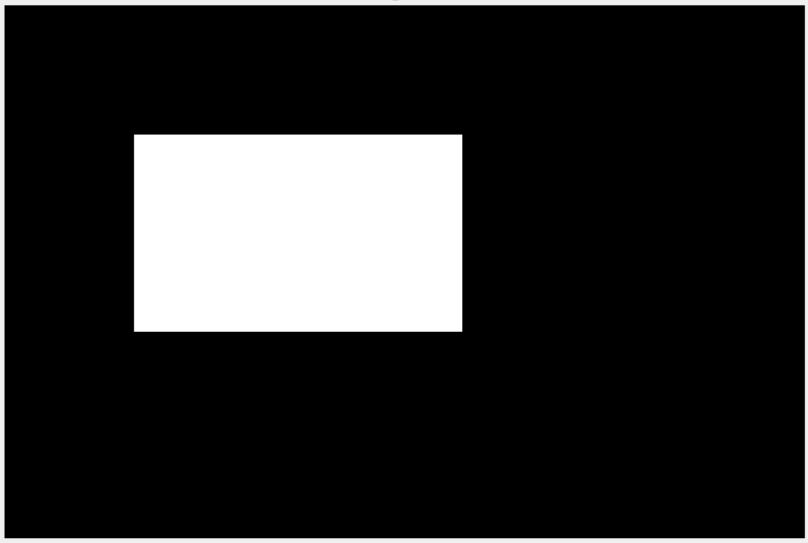
Trade-off between robustness and imperceptibility: DCT-based watermarking involves a trade-off between the robustness of the watermark and its perceptual invisibility. While embedding the watermark in mid-frequency bands enhances its robustness against common attacks, it may introduce visible artifacts or distortions that affect the image quality. Striking a balance between robustness and imperceptibility is crucial to ensure that the watermarked image remains visually pleasing while maintaining the watermark's detectability.

Vulnerability to collusion attacks: DCT-based watermarking can be vulnerable to collusion attacks, where multiple watermarked images are combined to remove or weaken the watermark. Attackers can use statistical analysis and techniques such as averaging or filtering to exploit the common components across multiple watermarked images and diminish the visibility of the watermark. This vulnerability highlights the importance of incorporating secure watermarking techniques, such as using unique watermarks for each image or employing spread spectrum techniques, to mitigate the risk of collusion attacks.

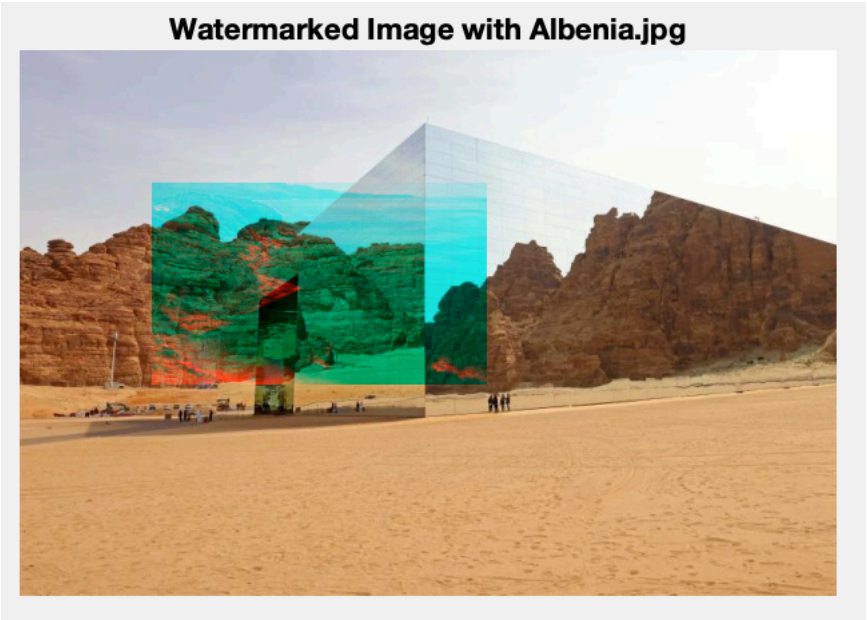
In conclusion, while DCT-based watermarking offers several advantages, it is important to consider its limitations. The lack of geometric robustness, vulnerability to advanced attacks, sensitivity to image content, trade-off between robustness and imperceptibility, and vulnerability to collusion attacks necessitate careful consideration and additional measures to address these limitations.

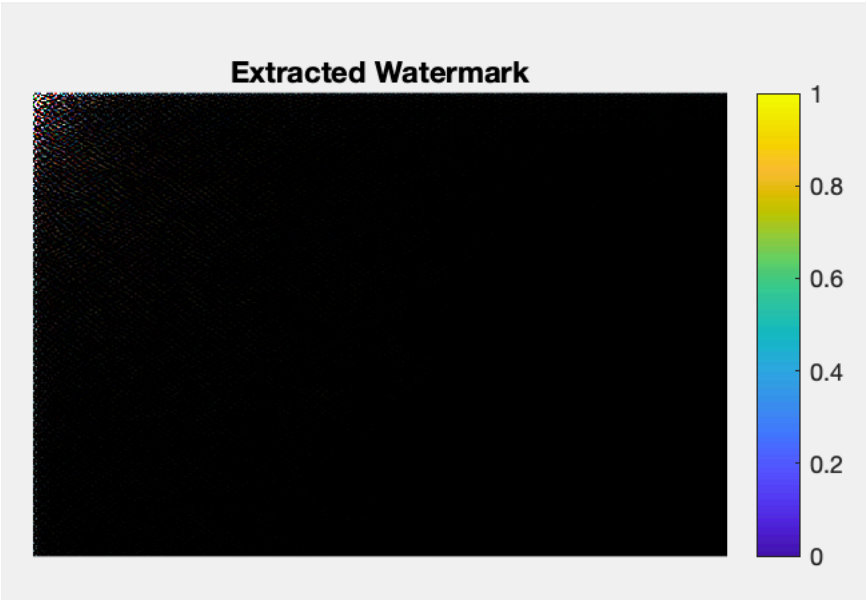
Original Image

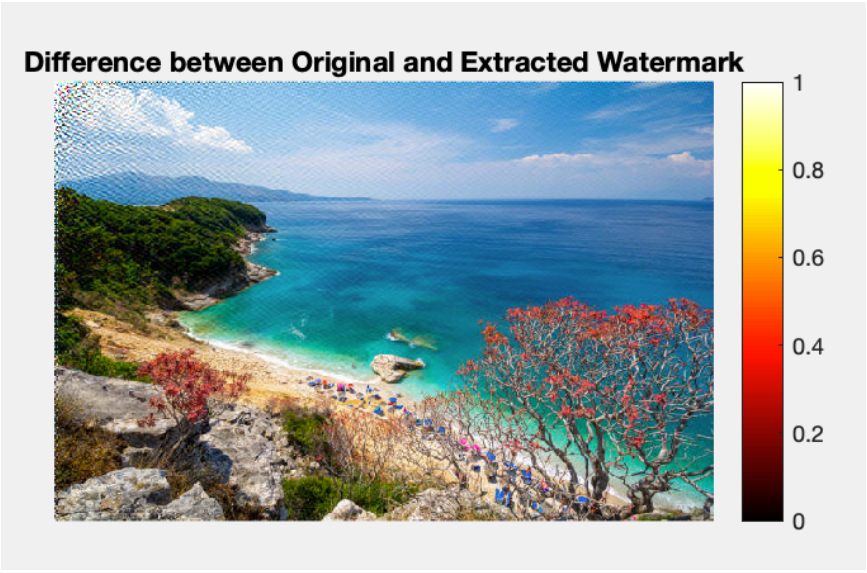
Binary Mask



Watermark Image


Watermarked Image with Albenia.jpg


Extracted Watermark
1
0.8
0.6
0.4
0.2
0


Difference between Original and Extracted Watermark
1
0.8
0.6
0.4
0.2
0

III. Discrete Wavelet Transform (DWT) Based Watermarking

III.I. Algorithm Description

The algorithm follows the following steps:

Define the image to be watermarked and the watermark image.
Convert the image to grayscale using the rgb2gray() function if necessary.
Perform the DWT operation on the image using the dwt2() function to obtain the approximation and detail coefficients.
Resize the watermark image to match the size of the image.
Embed the watermark into the appropriate DWT coefficients by modifying the coefficients in specific frequency sub-bands.
Reconstruct the watermarked image by applying the inverse DWT using the idwt2() function.
Extract the watermark from the watermarked image by subtracting the original image from the watermarked image and scaling the result.
Display the original image, watermarked image, and extracted watermark.Calculate the root mean square error (RMSE) values to evaluate the quality of the watermark extraction.
Plot the RMSE values for each color channel.

III.II. DWT Functionality

The algorithm heavily relies on two MATLAB functions: dwt2() and idwt2().

dwt2() Function:

The dwt2() function performs a 2D discrete wavelet transform (DWT) on an input image or signal.
It takes two input arguments: the input data and the wavelet name.
The wavelet name specifies the type of wavelet to be used for the decomposition, such as 'haar', 'db1', 'db2', etc.
The function returns four output arguments: the approximation coefficients (LL), horizontal detail coefficients (LH), vertical detail coefficients (HL), and diagonal detail coefficients (HH).
The DWT is implemented using the separable property of wavelets, allowing for the application of a 1D DWT along each dimension of the input data.
The wavelet filters used in the DWT are designed to be orthogonal, ensuring that the wavelet coefficients are uncorrelated.
Although the DWT is a lossy transform, the amount of information lost during the decomposition is typically small.

idwt2() Function:
The idwt2() function performs the inverse discrete wavelet transform (IDWT) on the wavelet coefficients obtained from a 2D DWT.

It reconstructs the original image or signal from the wavelet coefficients.
The function takes the wavelet coefficients and size information obtained from the DWT as input.
The IDWT involves applying the inverse of the wavelet filters used in the DWT to the wavelet coefficients.
The reconstruction process combines the approximation (LL) and detail (LH, HL, HH) coefficients using synthesis filters associated with the chosen wavelet.
The synthesis filters perform upsampling and filtering operations to upsample the coefficients and reconstruct the original data.
The reconstructed image or signal is obtained by iteratively applying the synthesis filters and upsampling to the wavelet coefficients, starting from the coarsest scale (LL subband) and proceeding to finer scales.
The resulting reconstructed data is stored in a matrix representing the original image or signal.

III.III. Introduction and Mathematical Representation of DWT

The Discrete Wavelet Transform (DWT) is another powerful transform technique extensively applied in the hierarchical decomposition of images. It decomposes an image into a lower resolution approximation image (LL) along with the horizontal (HL), vertical (LH), and diagonal (HH) detail components. These components each represent a distinct frequency domain within the image, providing a multi-resolution representation of the original image.

The 2D-DWT of an image is a mathematical transformation that can be formally expressed with the following equation:

$$[LL, LH, HL, HH] = \mathrm{dwt2}(x_1, \text{'haar'})$$

In the above formula, dwt2(.) is the 2D DWT function, x_1 is the input image, and 'haar' specifies the Haar wavelet as the mother wavelet. The function returns four outputs corresponding to the LL, LH, HL, and HH sub-bands of the decomposed image.

III.IV. Embedding Process in DWT-based Watermarking

The watermarking embedding primarily takes place in the HL, LH, and HH components of the DWT transformed image. These components are selected due to their ability to handle modifications without significantly degrading the perceptual quality of the original image. On the contrary, the LL component, which contains the most significant part of the image's energy and contains low-frequency elements, is typically avoided.

The watermark embedding process in DWT-based watermarking is mathematically represented by the following equation:

$$LH_1[\text{logical}(a_{\text{resized}})] = LH_1[\text{logical}(a_{\text{resized}})] + g \times \text{watermark\_red}[\text{logical}(a_{\text{resized}})]$$

In this equation, LH_1 is the LH sub-band of the DWT transformed image, $a_{resized}$ is a binary mask indicating the embedding locations, g is the watermark strength, and watermark_red is the watermark image's red channel and this applies to all three RGB channel separately.

The algorithm embeds the watermark by modifying the appropriate DWT coefficients based on a chosen embedding factor. The inverse process is used to extract the watermark from the watermarked image. Here are the steps involved:

Embedding:
Load the source image and the watermark image.
If the watermark image is in color, convert the source image to grayscale using the rgb2gray() function.
Perform the DWT on each color channel of the source image using the dwt2() function with the 'haar' wavelet.
Create a binary mask indicating the area where the watermark will be applied.
Resize the watermark image to match the size of the binary mask.
Split the image and the watermark into color channels.
Resize the binary mask to match the size of the DWT coefficients.
Define the coefficient of watermark strength.
Embed the watermark into the appropriate DWT coefficients by adding the product of the watermark and the strength coefficient.
Apply the inverse DWT using the idwt2() function to reconstruct the watermarked image.
Combine the color channels back into an image.

Extraction:
Create the watermarked image by replacing the corresponding pixels in the source image with the resized watermark.
Display the watermarked image.
Extract the watermark by subtracting the original image from the watermarked image and scaling the result.
Display the extracted watermark.

III.V. Evaluation Metrics

To evaluate the quality of the watermark extraction, the algorithm calculates the root mean square error (RMSE) values for each color channel. A lower RMSE indicates that the extracted watermark is closer to the original watermark. The algorithm also plots the RMSE values for visualization.

III.VI. Advantages of DWT-Based Watermarking

DWT-based watermarking using the dwt2() and idwt2() functions offers several advantages:

Robustness: DWT-based watermarking techniques tend to be robust against common image processing operations and attacks, such as compression, noise addition, cropping, and filtering.

Localization: DWT provides both spatial and frequency localization of image content, allowing for precise placement of the watermark within specific frequency sub-bands or image regions.

Imperceptibility: DWT-based watermarking techniques can achieve a good balance between watermark invisibility and robustness. By embedding the watermark in less perceptually significant frequency sub-bands, the modifications made to the image are often imperceptible to the human visual system.

Security: DWT-based watermarking techniques can provide a certain level of security by incorporating encryption and authentication mechanisms.

Compatibility: DWT is a widely used transform in image and signal processing, supported by many software libraries and tools like the dwt2() function in MATLAB. This makes DWT-based watermarking techniques easily implementable and compatible with various platforms and applications.

III.VII. Limitations of DWT-Based Watermarking

Despite its advantages, DWT-based watermarking has some limitations:

Sensitivity to image modifications: While DWT-based watermarking can be robust against certain types of image processing operations, it may be sensitive to certain modifications that significantly alter the image.

Limited embedding capacity: DWT-based watermarking has a limited capacity to embed large amounts of data within an image, determined by the available coefficients in the chosen frequency sub-bands.

Vulnerability to collusion attacks: DWT-based watermarking techniques can be vulnerable to collusion attacks, especially when the same sub-band coefficients are used for embedding different watermarks.

Sensitivity to synchronization errors: In some cases, watermark extraction may be affected by synchronization errors.

Lack of standardized algorithms: Unlike some other watermarking techniques, DWT-based watermarking does not have widely adopted standardized algorithms. This can lead to variations in implementation approaches and make it challenging to compare and evaluate different DWT-based watermarking methods.

III.VIII. Conclusions on DWT-Based Watermarking

In conclusion, the algorithm presented in this report utilizes Discrete Wavelet Transform (DWT) for image watermarking. The algorithm applies the DWT to the image and embeds the watermark into specific frequency sub-bands using the dwt2() function in MATLAB. The watermark can be extracted from the watermarked image using the inverse DWT, performed by the idwt2() function. DWT-based watermarking offers advantages such as robustness, localization, imperceptibility, security, and compatibility.

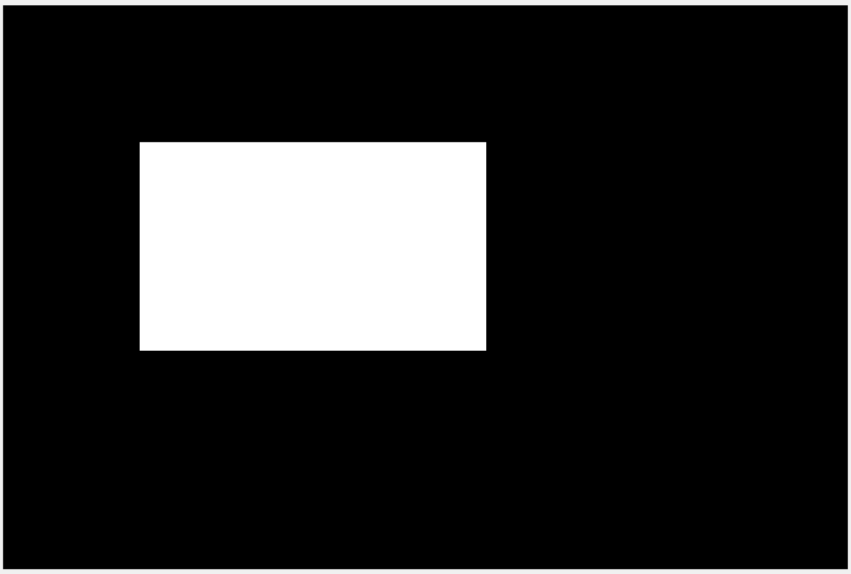
By exploiting the frequency domain properties of the image, DWT-based watermarking provides robustness against common image processing operations and attacks, such as compression, noise addition, cropping, and filtering. The ability to localize the watermark within specific frequency sub-bands or image regions allows for precise placement and improves the robustness of the watermark. The imperceptibility of the modifications made to the image ensures that the watermarked image appears visually close to the original. The compatibility of DWT with various platforms and applications, supported by functions like dwt2() and idwt2() in MATLAB, facilitates easy implementation.

However, DWT-based watermarking also has limitations. It may be sensitive to certain image modifications that significantly alter the image, and the embedding capacity is limited by the available coefficients in the chosen frequency sub-bands. Collusion attacks pose a risk when multiple watermarked copies are combined, especially if the same sub-band coefficients are used for embedding different watermarks. Synchronization errors can affect watermark extraction, and the lack of standardized algorithms makes it challenging to compare and evaluate different DWT-based watermarking methods. Furthermore, while DWT-based watermarking is robust against common attacks, it may be susceptible to sophisticated attacks designed to remove or manipulate the watermark.

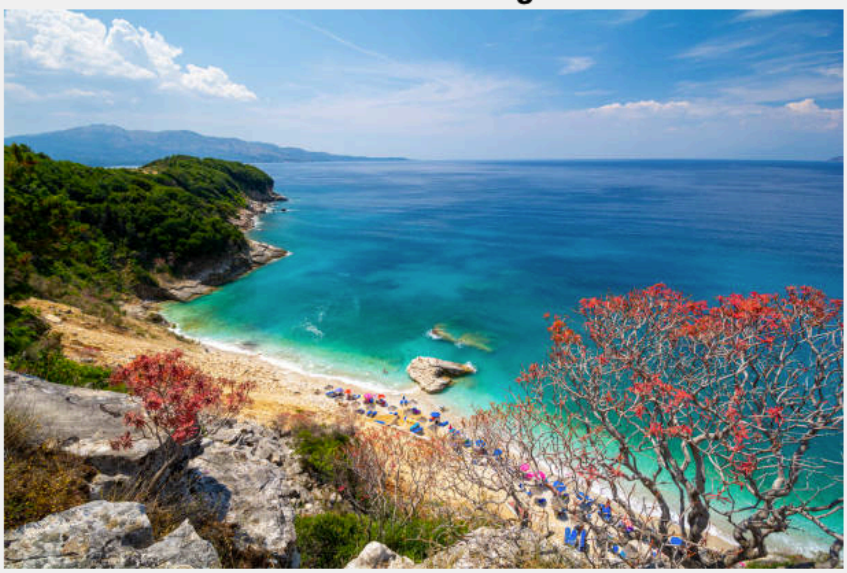
Despite these limitations, DWT-based watermarking using the dwt2() and idwt2() functions provides a viable approach for embedding and extracting watermarks in images. Further research and advancements in watermarking algorithms can address the limitations and enhance the robustness and security of DWT-based watermarking methods. DWT-based watermarking is particularly useful when resilience against compression is required, as the watermark can be hidden in the frequency components that are least affected by the compression process.

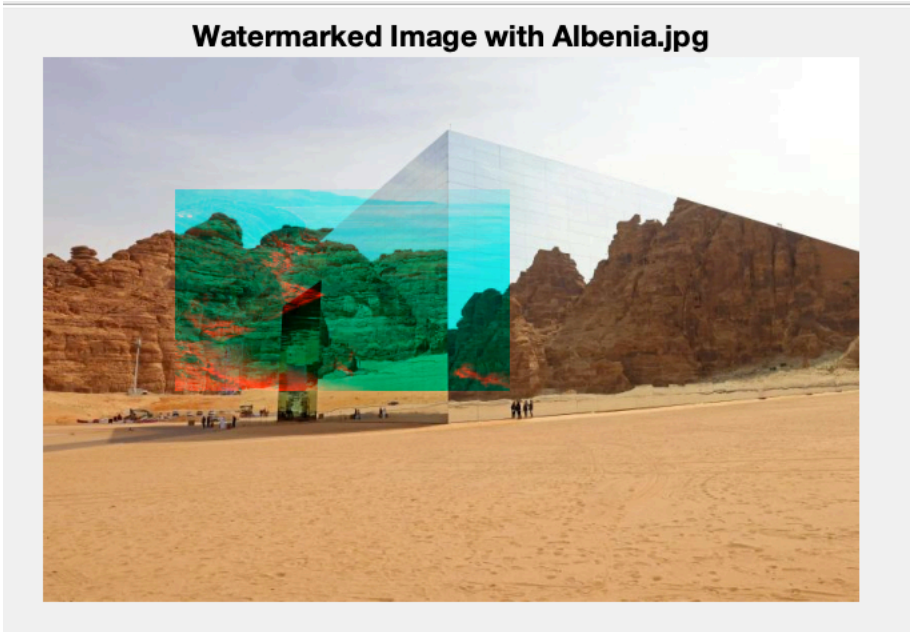
Original Image

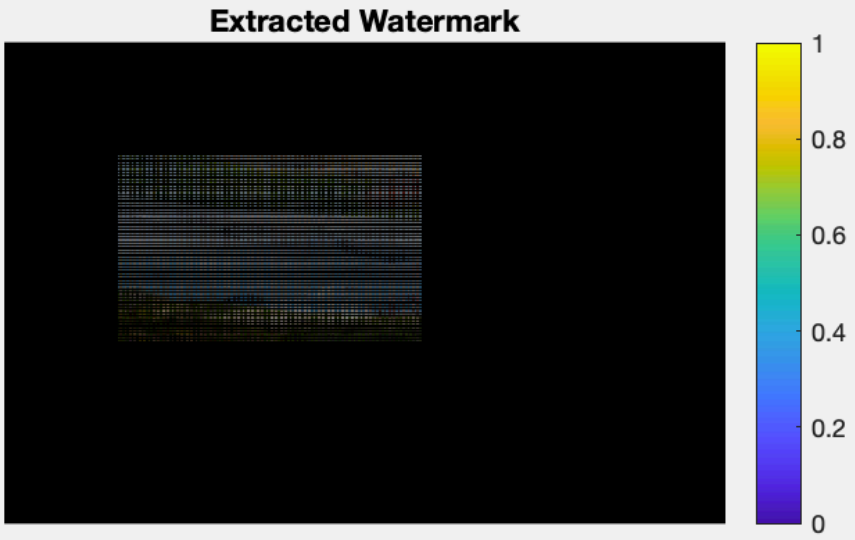
Binary Mask

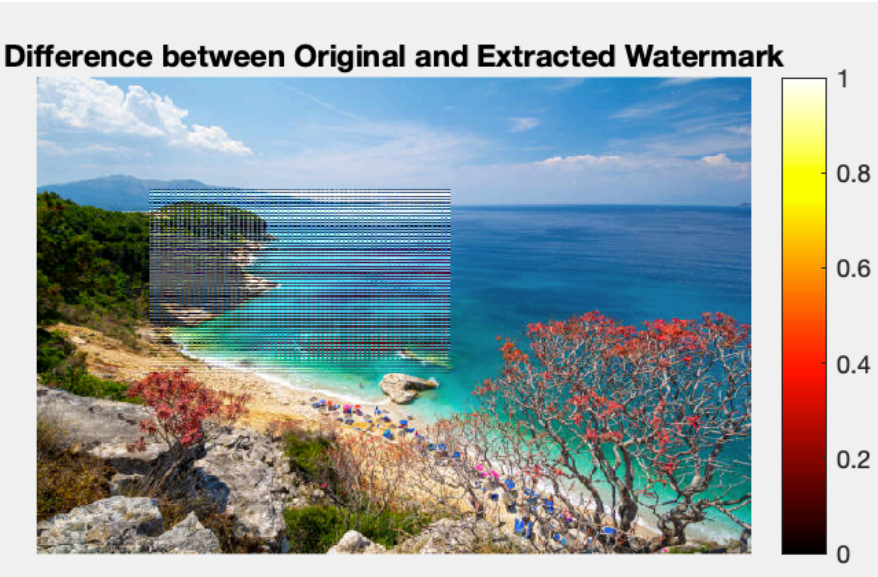


Watermark Image




Watermarked Image with Albenia.jpg


Extracted Watermark
1
0.8
0.6
0.4
0.2
0


Difference between Original and Extracted Watermark
1
0.8
0.6
0.4
0.2
0

IV. Comparative Analysis and Discussion

A. Discrete Cosine Transform (DCT) vs Discrete Wavelet Transform (DWT)
Both DCT and DWT are highly valuable techniques in the realm of digital watermarking. They owe their popularity to their distinct abilities to separate an image into its high and low-frequency components. Despite this common trait, their practical implementations differ and lead to different results. This section provides a detailed analysis of the outcomes produced by DCT and DWT-based watermarking methods, focusing on two major metrics: robustness and imperceptibility, and quality preservation.

IV.I. Robustness and Imperceptibility
i. The Concept of Robustness and Imperceptibility
Robustness and imperceptibility are two of the most sought-after properties in digital watermarking. Robustness refers to the resilience of the watermark against various attacks or alterations. A robust watermark can withstand common image processing operations such as rotation, scaling, and cropping, and more nefarious attempts to remove it like compression and noise addition.
On the other hand, imperceptibility pertains to the watermark's invisibility or unnoticeability. A good watermark should not degrade the quality of the host image or be perceptible by viewers. In other words, the presence of the watermark should not be obvious to the naked eye.

The challenge in digital watermarking is to balance these two characteristics – a more robust watermark might be easier to detect, whereas a more imperceptible watermark might be fragile.

ii. DWT Superiority in Robustness and Imperceptibility
DWT-based watermarking schemes are generally favored due to their superior performance in maintaining both robustness and imperceptibility. The main reason for this is DWT's ability to capture both frequency and spatial information about the image. In other words, DWT provides a time-frequency representation of the image, which is not possible with DCT.

Furthermore, the multi-resolution analysis intrinsic to DWT gives a more granular view of the image structure. This feature is particularly useful in digital watermarking since it spatially localizes the watermark within the image. By doing this, the watermark becomes more resilient to common image processing operations like rotation, scaling, and cropping.

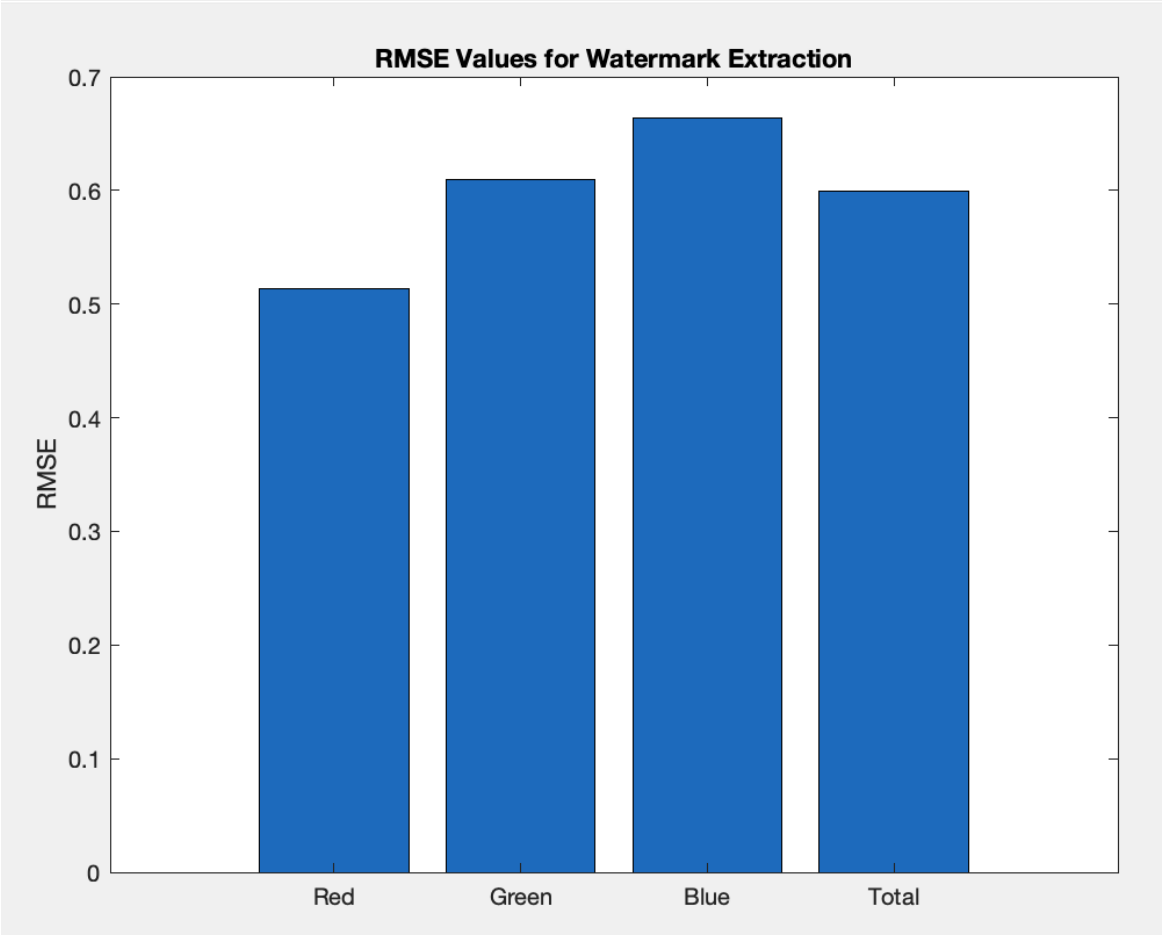
IV.II. Quality Preservation
i. The Importance of Quality Preservation
The concept of quality preservation in digital watermarking refers to the algorithm's ability to embed a watermark into the host image without significantly degrading the image's quality. This is crucial as, in most applications, the utility of the watermarked image should not be compromised by the watermarking process.

Quality preservation can be quantitatively measured using the Root Mean Square Error (RMSE) between the original and watermarked images. The RMSE is a standard measure that calculates the square root of the average squared differences between the actual (original image) and predicted (watermarked image) values. Consequently, a lower RMSE value signifies a minor difference between the original and watermarked image, reflecting a higher quality preservation post-watermarking.

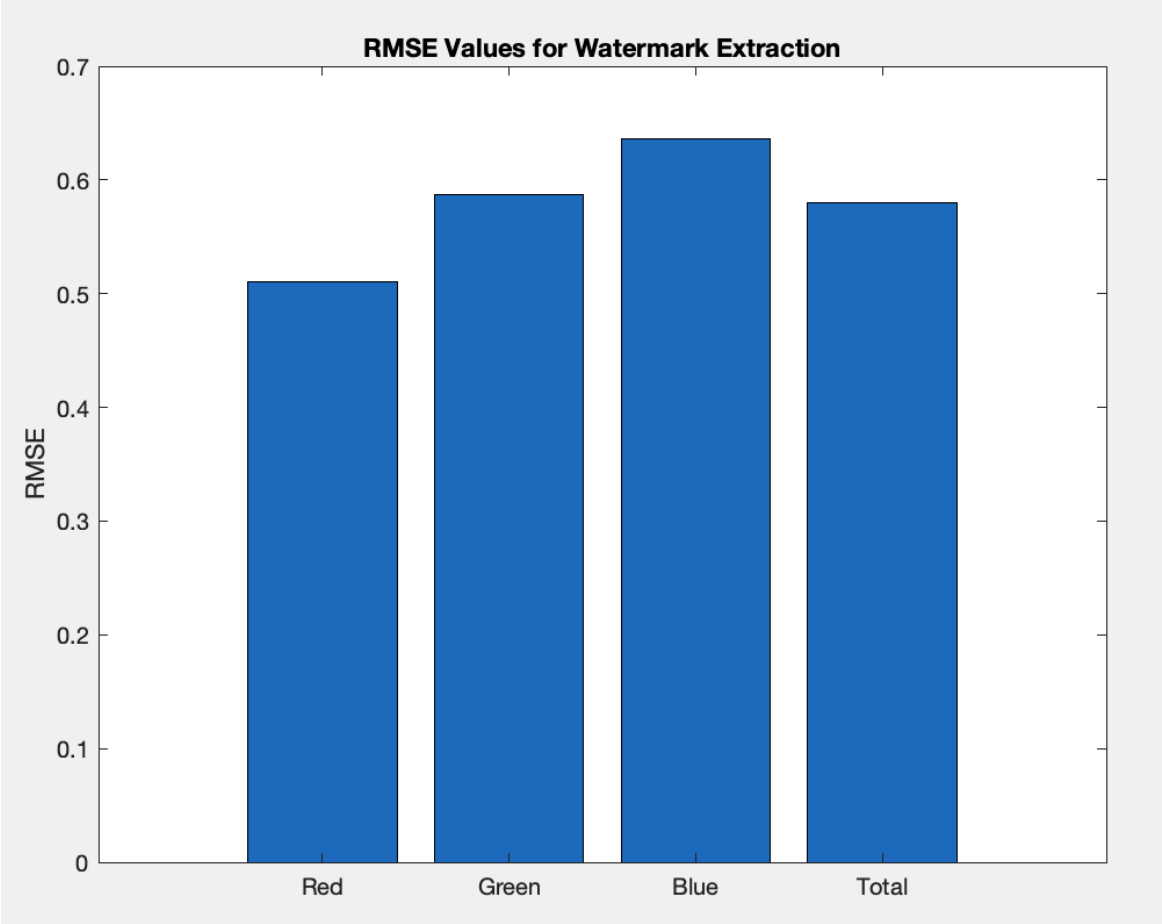
ii. DWT Dominance in Quality Preservation
Based on the acquired RMSE values, it has been observed that the DWT-based watermarking algorithm yields a lower total RMSE. This suggests that when employing DWT, the differences between the original and watermarked image are minimal, demonstrating superior quality preservation.

In comparison, while DCT is capable of effective watermarking, the resulting RMSE values are generally higher, which signifies that the watermarked image strays more from the original when DCT is used. This evidence, thus, further underscores DWT's dominance in preserving the quality of the original image during the watermarking process.

For DCT:



For DWT:



DCT RMSE VALUES

```
RMSE (Red): 0.51324
RMSE (Green): 0.60994
RMSE (Blue): 0.66404
Total RMSE: 0.599
```

DWT RMSE VALUES

```
RMSE (Red): 0.51077
RMSE (Green): 0.587
RMSE (Blue): 0.6361
Total RMSE: 0.58025
```

V. Conclusion

Having thoroughly examined both the Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) as methods for digital watermarking, it can be affirmed that each possesses unique strengths and drawbacks. While both methods effectively enable watermarking, their performance and the outcome significantly depend on the specific requirements of the application.

The DWT-based watermarking approach excels in several areas. It maintains superior performance in robustness and imperceptibility due to its ability to capture both the frequency and spatial localization of the image data. Furthermore, the multi-resolution characteristic intrinsic to DWT ensures greater resilience against common image processing operations such as rotation, scaling, and cropping.

In terms of image quality preservation, as demonstrated by the RMSE values, DWT also outperforms DCT. Lower RMSE values imply that the DWT-based watermarked image adheres more closely to the original, consequently preserving the quality of the image more efficiently.

In contrast, the DCT-based method, while being effective, does not quite match the performance levels of the DWT method. Although it can successfully embed watermarks, it is comparatively less robust and produces watermarked images that vary more from the original, as evidenced by higher RMSE values.

Despite these observations, it is essential to emphasize that the choice between DCT and DWT should be made considering the application's unique demands. Factors such as the importance of image fidelity, robustness against specific types of image processing operations or attacks, the nature of the data contained in the image, and computational resources can influence this choice.

Overall, while this study provides valuable insights into the comparative performance of DCT and DWT-based watermarking, it also underscores the complexity of the field of digital watermarking. It invites further exploration into the development of hybrid or new watermarking techniques to continue enhancing robustness, imperceptibility, and quality preservation.

Resources:

https://www.wikipedia.org/

https://www.mathworks.com/

https://core.ac.uk/download/pdf/234676913.pdf

MaTlaB Project Codes YouTube channel
MaTlaB Adda YouTube channel