Comparison of DCT and DWT-Based Invisible Watermarking Techniques

Abdurahman Vagifli
Doctoral Student, Azerbaijan Technical University
Baku, Azerbaijan
avaqifli77@gmail.com

***Abstract*— This paper investigates the effectiveness of Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) for invisible watermarking in digital images. The study compares their embedding quality using Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), and Structural Similarity Index Measure (SSIM), and evaluates their robustness against common attacks, including Gaussian noise, Gaussian blur, and JPEG compression. Experimental results indicate that DCT achieves significantly higher image quality retention, whereas DWT exhibits better resilience to distortions. However, both methods struggle with robustness against strong attacks. These findings suggest that while DCT is preferable for quality preservation, DWT may be more suitable for applications requiring resilience to distortions. A hybrid approach combining both methods may offer a balanced solution.**

Keywords*— Digital watermarking, Discrete Cosine Transform, Discrete Wavelet Transform, robustness, image quality

I. Introduction

Digital watermarking is a widely used technique for embedding information into images for authentication, copyright protection, and tamper detection [1]. Among various approaches, transform domain methods such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) have gained popularity due to their ability to embed watermarks in a visually imperceptible manner.

While DCT is known for its high-quality watermark embedding, it is vulnerable to attacks, particularly compression techniques like JPEG. On the other hand, DWT provides multi-resolution analysis, potentially offering better robustness against distortions. This study compares these two techniques by analyzing their imperceptibility and robustness through objective metrics such as PSNR, MSE, and SSIM. Furthermore, their ability to withstand common attacks, including Gaussian noise, Gaussian blur, and JPEG compression, is evaluated by measuring extraction rates and robustness values.

The results demonstrate that while DCT offers superior image quality retention, DWT exhibits some resilience to distortions. The findings highlight the need for a hybrid approach that leverages the strengths of both methods for optimal performance in watermarking applications.

II. Description of the Processing System

To begin with, a more detailed explanation of the operational stages of the developed watermarking system is provided. The input images (fig .1), which serve as the host for embedding watermarks (fig .2), are processed through a series of steps to ensure the watermark is successfully embedded and remains robust under various conditions. The process flow is divided into two main parts: watermark embedding and evaluation metrics, followed by robustness testing. Below, the key stages of the system are outlined [2], [3]:

A. **Watermark Embedding**
B. **Evaluation Metrics**
C. **Robustness Testing**

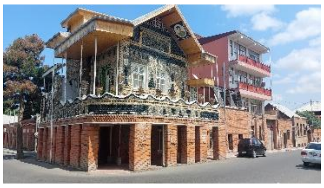

Fig. 1. Input image

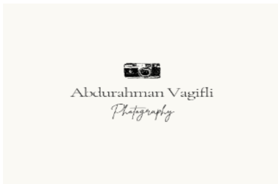

Fig.2.Watermark

A. Watermark Embedding

DCT Watermarking (Discrete Cosine Transform)

1. Divide the Image into 8x8 Blocks: DCT is typically applied to small blocks of the image (usually 8x8 pixels).
2. Apply DCT: Each 8x8 block is transformed from the spatial domain (pixel values) to the frequency domain (DCT coefficients).
3. Select DCT Coefficients: After the transformation, you select certain DCT coefficients (mid- or high-frequency components) to modify. These coefficients are more suitable for embedding the watermark while being imperceptible to the human eye.
4. Embed the Watermark: The watermark is embedded by slightly altering the selected DCT coefficients. This could be done by adding or modifying values in a pattern that represents the watermark data.
5. Apply Inverse DCT (IDCT): Once the watermark is embedded in the DCT coefficients, the Inverse DCT is applied to return the image to the spatial domain, creating the watermarked image. (fig .3) [4], [5]

Fig. 3 . DCT watermarked image

DWT Watermarking (Discrete Wavelet Transform)

1. Apply DWT: The image is decomposed into multiple frequency subbands using DWT. These subbands include:
   - Approximation (low-frequency components)
   - Details (high-frequency components in horizontal, vertical, and diagonal directions)
2. Select Subbands for Embedding: The watermark is typically embedded in the high-frequency subbands (horizontal, vertical, diagonal) because they are less noticeable to the human eye and more resilient to attacks like compression.
3. Embed the Watermark: The watermark is embedded by modifying the selected high-frequency coefficients in the subbands. Small changes are made to these coefficients to encode the watermark information.
4. Apply Inverse DWT (IDWT): After embedding the watermark, the Inverse DWT is applied to reconstruct the image, combining all modified subbands into the final watermarked image. (fig.4)[6]

Fig.4.DWT watermarked image

B. Evaluation Metrics

The evaluation process in watermarking refers to the set of techniques and metrics used to assess the effectiveness of a watermarking algorithm. The goal is to ensure that the watermark is successfully embedded in the image without significantly degrading its quality, and that it remains detectable and extractable even after the image undergoes transformations or attacks (like compression or noise) [7].

The evaluation process typically involves:

1. Assessing Image Quality: Ensuring that the watermarking process does not noticeably degrade the visual quality of the image.
2. Evaluating Watermark Detection: Checking whether the watermark can still be extracted correctly after the image is modified.
3. Testing Robustness: Evaluating how well the watermark survives attacks like compression, noise addition, or cropping.

1. Structural Similarity Index (SSIM)

Purpose: SSIM measures the perceptual quality of the watermarked image by comparing the structural information between the original and the watermarked image. It assesses luminance, contrast, and structure [8].

Formula: SSIM compares the local patterns of pixel intensities between the original and watermarked images. The formula for SSIM is:

$$\text{SSIM}=\frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)}$$

Where:

- μ_x *and* μ_y are the mean pixel values of the original (x) and watermarked (y) images, respectively.
- σ_x^2 and σ_y^2 are the variances of the original and watermarked images.
- σ_{xy} is the covariance between the original and watermarked images.
- C_1 and C_2 are constants to stabilize the division with weak denominators (usually small values like $C1=0.01^2$and $C2=0.03^2$)

Interpretation: SSIM returns a value between -1 and 1, where 1 indicates that the two images are identical in terms of structure, and 0 indicates no similarity. A high SSIM value means that the watermarked image is perceptually very similar to the original image.

2. Mean Squared Error (MSE)

Purpose: MSE measures the average squared difference between corresponding pixel values of the original and watermarked images. It is a simple method to quantify the error or distortion introduced by the watermarking process.

Formula:

$$\text{MSE}=\frac{1}{N}\sum_{i=1}^{N}(I_{original}(i)-I_{watermarked}(i))^2$$

Where:

- $I_{original}(i)$ and $I_{watermarked}(i)$ are the pixel values of the original and watermarked images, respectively.
- N is the total number of pixels in the image.

Interpretation: A lower MSE indicates better image quality (less distortion), as it means the difference between the original and watermarked images is minimal.

3. Peak Signal-to-Noise Ratio (PSNR)

Purpose: PSNR is a metric used to measure the quality of the watermarked image in terms of pixel-level differences. It compares the original and watermarked images based on the maximum possible pixel value (usually 255 for an 8-bit image) and the MSE (Mean Squared Error) [8].

Formula:

$$\text{PSNR}= 10\text{x}\log_{10}(\frac{R^2}{MSE})$$

Where:

- R is the maximum pixel value of the image (typically 255 for an 8-bit image).
- MSE is the Mean Squared Error between the original and watermarked images.

Interpretation: A higher PSNR indicates better quality (less distortion), meaning the watermarked image is more similar to the original. Typical PSNR values are in the range of 30-50 dB, where higher values (closer to 50) generally indicate better quality.

TABLE I. Evaluation Metrics for DCT and DWT Watermarked Images

Metric	DCT Watermarked Image	DWT Watermarked Image
PSNR(dB)	45.29	26.26
MSE	0.85	153.79
SSIM	0.997	0.523

DCT exhibited significantly higher PSNR and SSIM values, indicating better preservation of image quality compared to DWT.

C. Robustness Testing

There are three main categories of attacks applied to watermarked images. Natural Distortions occur during regular image processing or transmission, such as compression, noise, or blurring, which can degrade image quality without intent to remove the watermark. Intentional Attacks are specifically designed to remove or degrade the watermark, including cropping, rotation, or filtering operations. Signal Processing Attacks involve technical modifications to the image's signal, such as compression or noise, which affect the image's structure and can disrupt watermark detection

We selected Gaussian Blur**,** Gaussian Noise, and JPEG Compression as representative attacks for evaluating the robustness of watermarking techniques due to their relevance in real-world applications and their distinct effects on image integrity. Gaussian Blur simulates blurring caused by focus issues or motion, testing the watermark's resilience against typical distortions encountered in practical scenarios. Gaussian Noise introduces random pixel variations, mimicking environmental disturbances such as transmission errors, and allows us to assess the watermark's ability to withstand random interference. JPEG Compression is widely used for image storage and transmission, and its lossy nature poses significant challenges to watermark robustness, particularly in terms of loss of high-frequency components, making it an essential test for evaluating watermark stability under real-world image compression conditions [9], [10].

TABLE I. Watermark Extraction Rate After Attacks (DCT in Percentage, DWT in dB)

Attacks	DCT Extraction Rate(%)	DWT Extraction Rate
Gaussian Noise	0.00%	0.26 dB
Gaussian Blur	0.00%	0.30 dB
JPEG Compression	0.00%	Not computable due to errors

While DWT showed some resilience against Gaussian noise and blur, both methods struggled under JPEG compression..

Fig.1.Extracted Watermark before attacks

III. Performance Improvement

In this study, we evaluated the performance of DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform) watermarking techniques, focusing on visual quality**,** robustness**,** and extraction accuracy under various attacks.

a) Visual Quality of DCT Watermarking

The DCT watermarking method shows superior visual quality compared to DWT. The watermark is invisible or minimally perceptible, as indicated by high SSIM (Structural Similarity Index) scores and low MSE (Mean Squared Error) values. These results confirm that DCT watermarking is highly effective in maintaining the aesthetic quality of the watermarked image while embedding the watermark in a way that is not noticeable to the human eye.

b) Robustness and Extraction Rate in DCT Watermarking

However, the DCT watermarking method demonstrates poor robustness to attacks. After applying attacks like JPEG compression, Gaussian noise, and Gaussian blur, the watermark extraction rate drops to zero. This result highlights that while DCT is excellent for maintaining visual quality, it is highly susceptible to distortions caused by compression and noise, making it ineffective for applications where the watermark must survive under various conditions.

c) DWT Watermarking – Robustness and Extraction Accuracy

The DWT watermarking method, though also not immune to attacks, shows better robustness than DCT. After subjecting the watermarked images to the same attacks, DWT extraction rates were measured at 0.26 dB and 0.30 dB. Although these values are low and indicate some vulnerability to attacks, they are still non-zero, showing that DWT performs better than DCT in terms of attack resilience. However, the extraction accuracy of DWT is still compromised under significant distortions, suggesting that even multi-scale approaches like DWT need further refinement to improve robustness against various types of attacks.

d) Comparison of DCT and DWT

Comparing DCT and DWT, we find that while DCT excels in visual quality, it offers no resilience against attacks, as evidenced by the zero extraction rate after distortion. On the other hand, DWT provides some level of robustness (with extraction rates of 0.26 dB and 0.30 dB) but at the cost of reduced visual quality. This indicates that DWT is more robust than DCT, but neither method is entirely immune to the distortions caused by common image attacks.

IV. Conclusion

In conclusion, the study reveals a trade-off between visual quality and robustness in both watermarking methods. DCT watermarking offers better visual imperceptibility but fails to withstand common attacks, as shown by the zero extraction rate. DWT watermarking offers better robustness, but the extraction rate still drops significantly under attack, suggesting that further improvements are necessary to enhance resilience without compromising visual quality. These findings indicate that both methods have limitations, and future research should focus on improving robustness without sacrificing visual quality, or consider exploring hybrid watermarking methods that combine the advantages of both DCT and DWT

References

[1] Ayu Astridefi, Rudy A.G. Gultom,Yudistira Dwi Wardhana Asnar and H.A. Danang Rimbawa "Audio,Text,Image,and Video Digital Watermarking Techniques for Security of Media Digital." International Journal of Progressive Sciences and Technologies Vol.42, No.1, 1 Dec 2023,pp 389-398

[2] Sanghyun Joo,Youngho Suh, Jaeho Shin and Hisakazu Kikuchi, "A New Robust Watermark Embedding into Wavelet DC Components," ETRI Journal, Vol 24, Num 5, Oct 2002.

[3] Brian Chen "Design and Analysis of Digital Watermarking,Information Embedding, and Data Hiding Systems "Massachusetts Institute of Tecnology,Thesis, 2000.

[4] Krishna Kumar Bohra and Vinod Kumar Soni, "Invisible watermarking using Discrete Cosine Transform(DCT):A comprehensive exploration," World Journal of Advanced Research and Reviews, 2024,24(02),2639-2645.

[5] Haiming Li and Xiaoyun Guo . "Embedding and Extracting Digital Watermark Based on DCT algorithm," Journal of Computer and Communications, 2018, 6, 287-298.

[6] Priyanka Vashist, Roop Singh, and Dr.Rajeev Ratan Arora, "Digital Watermarking Using DCT&DWT Technique," International Journal of Research, May. 2017, Vol. 4 Iss. 6,.

[7] Dujan B.Taha ,and Taha B.Taha. "Towards a New Metric for Watermarked Image Assesment ," 2nd International Conference on Electrical, Communication, Computer, Power and Control Engineering, 2019,.

[8] Alain Hore, and Djemel Dizou, "Image Quality metrics; PSNR VS SSIM," 2010 Second International Conference on Pattern Recognition

[9] Mohammad Rizwan Khan and Ankur Goyal , "Gaussian Noise attack Analysis of Non Blind Multiplicative Watermarking using 2D-DWT ," International Journal of Computer Science and Information Technologies, Vol. 7 (6) , 2016, 2481-2486.

[10] Yuepeng Hu,Zhengyuan Jiang,Moyang Guo,Neil Gong "A Transfer Attack to Image Watermark"