UOT:002.6:025.5/.6
DOI: https://doi.org/10.30546/09090.2025.01.2031

ROBUSTNESS EVALUATION OF DCT-DWT BASED INVISIBLE IMAGE WATERMARKING UNDER COMMON IMAGE ATTACKS

ABDURAHMAN VAGIFLI
avaqifli77@gmail.com
Azerbaijan Technical University
Baku, Azerbaijan

ARTICLE INFO

Article history:
Received:2025-03-26
Received in revised form:2025-04-02
Accepted:2025-04-16
Available online

Keywords: Digital watermarking, DCT-DWT, Invisible watermark, Image robustness, Image quality metrics

ABSTRACT

Invisible watermarking has become a vital technique in digital image security, allowing hidden data to be embedded without affecting visual quality. This study addresses the challenge of maintaining watermark imperceptibility while resisting common image distortions. The goal of this research is to assess the effectiveness of a hybrid watermarking method that combines Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). In the proposed approach, the watermark is embedded in the DCT coefficients of the low-frequency DWT sub-band. Experiments were conducted in both RGB and YCbCr color spaces, with varying strength factors (alpha). The method demonstrated high imperceptibility, with SSIM values above 0.998, but limited robustness against JPEG compression, Gaussian blur, and noise. These findings highlight the need for more resilient hybrid methods

12. Introduction

Digital watermarking is a crucial technology in multimedia security, enabling copyright protection, authentication, and content tracking [1]. Invisible watermarking methods embed information into digital media such that it is imperceptible to the human eye but can be retrieved algorithmically. Transform-domain techniques, such as DCT and DWT, are widely used for their robustness and frequency localization properties.

In this paper, we investigate a combined DCT-DWT approach for invisible watermark embedding and evaluate its quality and robustness under standard image attacks.

13. Related Work

2.1 Discrete Cosine Transform (DCT)

The Discrete Cosine Transform (DCT) expresses a finite sequence of data points as a sum of cosine functions oscillating at different frequencies. It is widely used in image compression and watermarking because it concentrates most of the signal energy into a few low-frequency components. The 2D DCT for an image block is defined as [2]:

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

Where $\alpha(u)=\begin{cases}\frac{1}{\sqrt{2}}, u=0\\ 1, u>0\end{cases}$

and $f(x,y)$ is the pixel intensity at position (x,y).

2.2 Discrete Wavelet Transform (DWT)

DWT provides a time-frequency representation of the signal by decomposing the image into sub-bands of different frequency resolutions. A single-level 2D DWT decomposes an image into four sub-bands: LL (approximation), LH (horizontal), HL (vertical), and HH (diagonal). The LL sub-band contains the most significant information and is commonly used for embedding watermarks. The inverse DWT reconstructs the image using these sub-bands [3].

2.3 Common Image Attacks

Watermarked images are subject to various distortions in real-world scenarios. JPEG compression introduces quantization errors, Gaussian blur reduces sharpness, and Gaussian noise adds pixel-level distortions. A robust watermarking technique must withstand these attacks while maintaining watermark recoverability [4].

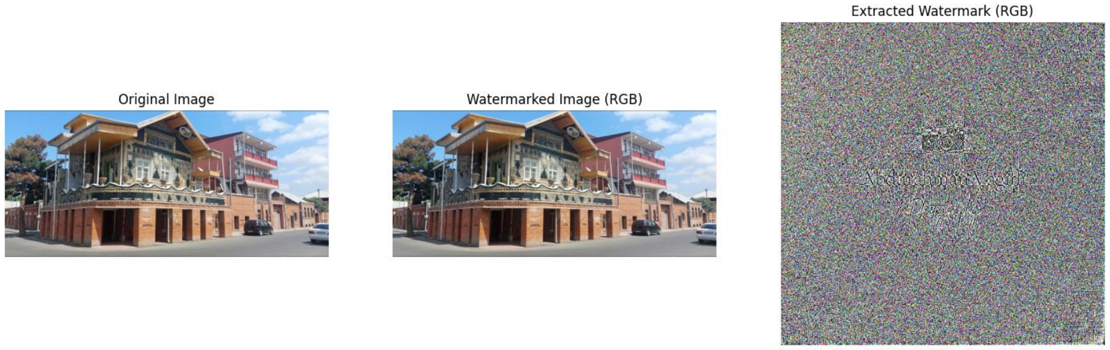
14. Research Methodology

We implemented a DCT-DWT-based invisible watermarking framework in Python using OpenCV and PyWavelets. The original image is first decomposed using a single-level Haar DWT. The LL sub-band is then transformed using DCT, and the watermark is added to the DCT coefficients using an embedding strength factor (alpha). The inverse DCT and inverse DWT reconstruct the watermarked image. This process was applied in both RGB and YCbCr color spaces, with a special focus on the Y channel in the latter for better perceptual embedding.

To evaluate quality, we used PSNR, SSIM [5] , and MSE between original and watermarked images. For robustness, we extracted the watermark after applying JPEG compression, Gaussian blur, and Gaussian noise, and evaluated similarity to the original watermark.

15. Experimental Results

The original image used in this experiment is a photograph of a decorative architectural structure located in a vibrant urban setting. This image was chosen for its rich color distribution, sharp edges, and varied texture regions, which make it an ideal candidate for evaluating the imperceptibility of watermarking methods. The watermark is a centered, minimalistic photography logo with a monochromatic color palette and a combination of serif and handwritten fonts, accompanied by a vintage camera icon. Its clean design and high contrast allow effective embedding and clearer visual assessment upon extraction. The watermark was embedded using the DCT-DWT technique at an alpha value of 0.1 to demonstrate the method's visual transparency. Figure 1 presents the original image, the corresponding watermarked image, and the extracted watermark before any attack.



Original Image

Watermarked Image (RGB)

Extracted Watermark (RGB)

Fig. 1. Original image, the corresponding watermarked image, and the extracted watermark before any attack

Before diving into attack resilience, it is important to first assess the baseline image quality after watermark embedding. The following tables present SSIM, PSNR, and MSE values comparing the original and watermarked images at different alpha values. These metrics confirm that the watermarking process introduces minimal visual distortion, providing a solid foundation for further analysis under attack conditions

Table 1. Image Quality Evaluation (Original vs Watermarked)

Alpha = 0.1

Metric	Value
SSIM (avg over R,G,B)	0.9985
PSNR(db)	49.92
MSE	0.66

Alpha=0.3

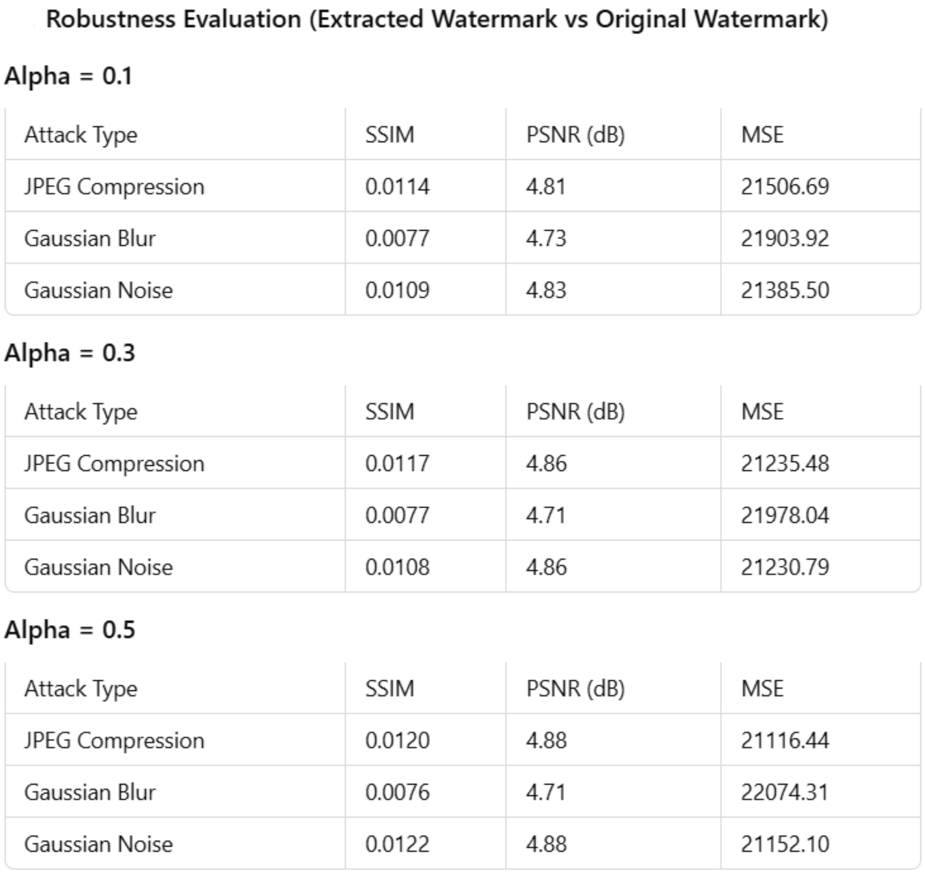
Metric	Value
SSIM (avg over R,G,B)	0.9983
PSNR(db)	50.21
MSE	0.62

Alpha=0.5

Metric	Value
SSIM (avg over R,G,B)	0.9982
PSNR(db)	50.38
MSE	0.60

The quality evaluation results presented in this section demonstrate that the proposed DCT-DWT watermarking method maintains a high level of imperceptibility. For all tested alpha values (0.1, 0.3, and 0.5), the SSIM values remain above 0.998, indicating nearly perfect structural similarity between the original and watermarked images. Additionally, PSNR values exceed 49 dB, which reflects excellent preservation of visual quality, as values above 40 dB are generally considered imperceptible to the human eye. The corresponding MSE values are all below 1, further confirming minimal pixel-level distortion introduced during embedding. These metrics collectively validate the effectiveness of the method in preserving image quality, which is critical for practical watermarking applications

Figure 2 shows a visual summary of the SSIM, PSNR, and MSE values for the extracted watermark after applying JPEG compression, Gaussian blur, and Gaussian noise across different alpha values. The results clearly illustrate that although the watermark is successfully embedded with minimal impact on the original image, its robustness against attacks remains limited. The SSIM values remain extremely low across all scenarios, indicating a significant degradation of structural similarity post-attack. Similarly, PSNR values are consistently below 5 dB, suggesting severe loss in signal fidelity. These visual metrics confirm the vulnerability of the DCT-DWT watermarking method to common image distortions and highlight the need for enhanced strategies in future work.



Robustness Evaluation (Extracted Watermark vs Original Watermark)

Alpha = 0.1

Attack Type	SSIM	PSNR (dB)	MSE
JPEG Compression	0.0114	4.81	21506.69
Gaussian Blur	0.0077	4.73	21903.92
Gaussian Noise	0.0109	4.83	21385.50

Alpha = 0.3

Attack Type	SSIM	PSNR (dB)	MSE
JPEG Compression	0.0117	4.86	21235.48
Gaussian Blur	0.0077	4.71	21978.04
Gaussian Noise	0.0108	4.86	21230.79

Alpha = 0.5

Attack Type	SSIM	PSNR (dB)	MSE
JPEG Compression	0.0120	4.88	21116.44
Gaussian Blur	0.0076	4.71	22074.31
Gaussian Noise	0.0122	4.88	21152.10

Fig.2. Summary of the SSIM, PSNR, and MSE values for the extracted watermark after applying JPEG compression, Gaussian blur, and Gaussian noise

5.Conclusion

The DCT-DWT watermarking method provides excellent invisibility but shows weak robustness under common attacks. Future work should explore hybrid methods such as DWT-SVD, block-based redundancy, or error-correction techniques to improve resilience. Additionally, CNN-based classifiers can be integrated to detect and adaptively adjust embedding strategies depending on content and predicted attack vulnerability

REFERENCES

[1] A. Astridefi, R. A.G. Gultom, Y. D. W, Asnar, H.A. D. Rimbawa, Audio, Text, Image, and Video Digital Watermarking Techniques for Security of Media Digital, International Journal of Progressive Sciences and Technologies (IJPSAT) ISSN: 2509-0119, Vol. 42 No. 1 December 2023, pp. 389-398

[2] https://www.mathworks.com/help/vision/ref/2ddct.html

[3] P. Vashist, R.Singh, Dr. R. R. Arora, Digital Watermarking Using DCT & DWT Technique, International Journal of Research, Volume 04, Issue 06, Ma y 2017

[4] C. Song, S. Sudirman, M. Merabti, D. Llewellyn-Jones, Analysis of Digital Image Watermark Attacks, 2010 7th IEEE Consumer Communications and Networking Conference

[5] A. Horé, D.Ziou, Image quality metrics: PSNR vs. SSIM, 2010 International Conference on Pattern Recognition