
Digital Image Watermarking Software Using Discrete Wavelet Transform (DWT)

Zara Marzani^{1*}

Abstract

The ease of data transmission through various digital media poses significant risks to copyright and privacy, often leading to falsification, duplication, fraud, and media piracy. One approach to address this issue is through steganography, a technique for embedding hidden messages within digital documents such as images. A specific application of steganography is Digital Watermarking, which conceals ownership information within digital media. This study employs the Discrete Wavelet Transform (DWT) method to implement watermarking on digital images. DWT divides data into multiple frequency segments that can be independently processed and recombined to form a watermarked image. By embedding a watermark into the image, the proposed method effectively protects against unauthorized use and reproduction.

Keywords

Steganography, Digital Watermarking, Discrete Wavelet Transform, Watermark

Article History

Received 05 August 2023

Accepted 21 October 2023

How to Cite

Marzani, Z., (2023). Digital Image Watermarking Software Using Discrete Wavelet Transform (DWT). Jurnal Ilmu Komputer dan Sistem Informasi (JIKSI), 4(3), [101-110].

^{1*} Universitas Bina Darma, Indonesia, Corresponding email: zaramarzani.bd@gmail.com

Introduction

In the modern digital era, information technology (IT) has become a crucial component of human life, profoundly influencing communication, education, business, and entertainment. The widespread use of the internet has made data and information more accessible than ever before, enabling individuals to share, store, and manipulate digital content instantly. However, the same technological advances that provide convenience and efficiency also present significant challenges. Issues such as data privacy, content falsification, duplication, and digital piracy have emerged as serious concerns, particularly as multimedia content circulates without clear ownership or legal protection. Ensuring the integrity and authenticity of digital information has therefore become a pressing issue in maintaining trust and ethical standards in the digital ecosystem.

Within this context, digital media—including images, audio, and video—plays a central role in modern information exchange. Among these, digital images are among the most frequently used and easily distributed forms of digital content, appearing across social media, online publications, and digital archives. The ease with which images can be replicated, altered, or shared makes them highly vulnerable to unauthorized use, counterfeiting, and copyright infringement. Without appropriate protection mechanisms, original creators or organizations risk losing ownership control over their intellectual property. Consequently, researchers and developers have been motivated to design technological solutions that ensure both data security and intellectual property protection for digital images distributed online.

One of the most effective and widely studied approaches to addressing this issue is steganography, a method derived from the Greek term meaning “hidden writing.” Steganography refers to the process of concealing secret information within another medium in such a way that its presence remains imperceptible to unauthorized users. In the context of digital media, this technique allows confidential or ownership-related information to be embedded within multimedia files without visibly altering their appearance or quality. As described by Andika and Darwis (2020), an effective steganographic technique must satisfy several key parameters—imperceptibility, to ensure that the hidden data cannot be visually detected; fidelity, to maintain the integrity of the original file; robustness, to resist modifications such as compression or noise; and recoverability, ensuring that the embedded information can be reliably extracted when needed.

A specific and practical application of steganography is digital watermarking, a process in which unique ownership or authentication data is embedded within multimedia files such as images, videos, or documents. The main objective of digital watermarking is to provide a technological safeguard for copyright protection, helping content creators and institutions assert ownership and prevent unauthorized duplication. Watermarks can also function as verification markers to authenticate the originality of a file or detect tampering. However, one of the primary challenges in digital watermarking lies in achieving the right balance between visual quality and robustness. Strong watermarking methods may withstand compression, filtering, or format conversion but can degrade image quality, while high-quality watermarking methods that prioritize imperceptibility often become more susceptible to removal or distortion. This trade-off necessitates the use of sophisticated mathematical techniques capable of maintaining both attributes effectively.

In this study, the Discrete Wavelet Transform (DWT) is employed as the core method for performing digital watermarking, offering an optimal compromise between robustness and

image quality. As explained by Rachman, Purnamasari, and Saidah (2019), DWT is a mathematical tool that decomposes one- or two-dimensional signals—such as digital images—into multiple subcomponents representing different frequency domains. This decomposition produces a multiresolution representation of the image, allowing different levels of detail to be analyzed and modified independently. The DWT technique divides an image into subbands—low-low (LL), low-high (LH), high-low (HL), and high-high (HH)—each capturing distinct spatial characteristics and frequency information. By embedding watermark data into selected subbands, particularly those less sensitive to human visual perception, the technique ensures that the watermark remains imperceptible yet durable against common image-processing operations.

The strength of the DWT approach lies in its ability to preserve image quality while enhancing watermark resistance. After embedding, the inverse DWT process reconstructs the watermarked image, maintaining high fidelity between the original and modified versions. The resulting image demonstrates high Peak Signal-to-Noise Ratio (PSNR) values, indicating minimal perceptual distortion, while maintaining the capability to recover the embedded watermark during verification. Through this process, the DWT-based watermarking method effectively supports both the technical and ethical objectives of digital media protection—preserving copyright integrity, ensuring data authenticity, and preventing unauthorized reproduction. Therefore, this study contributes to the ongoing efforts in digital rights management by proposing a robust, scalable, and efficient technique for safeguarding digital image content within the expanding landscape of information technology.

Methodology

System Development Method

The software development process in this study uses the Prototype Model, consisting of five key stages:

1. Analysis,
2. Design,
3. Simulation Prototype,
4. Implementation, and
5. Monitoring (Sanjaya & Setiyadi, 2019).

This iterative approach enables continuous feedback and refinement throughout system development.

Watermaking

Watermarking, also referred to as a digital watermark, is a data-hiding technique used to embed confidential information within digital media such as images, audio, or video. This information is imperceptible to the human eye and resilient to common image processing operations, including noise addition and blurring (Aulia, 2019).

One commonly used watermarking method is the Patchwork Algorithm, which introduces controlled modifications into a signal to encode information (Hondro & Sinurat, 2020). Unlike visible watermarks on physical materials, digital watermarks are designed to

remain undetectable without computational analysis. This invisibility leverages limitations in human sensory perception, particularly vision (Alegra & Alam, 2023).

Digital Image

A digital image is a representation or imitation of an object, categorized into analog and digital formats. Analog images, such as television displays or X-ray scans, are continuous in nature, while digital images consist of discrete data points that can be processed by computers (Utami, Rismawan, & Ristian, 2022).

Mathematically, a digital image is expressed as a two-dimensional function $f(x, y)$, where x and y represent the horizontal and vertical coordinates, respectively. The intensity value of the image is stored in a matrix of size $[M \times N]$. Such matrix-based representation facilitates pixel-level image processing (Hafizhana, Safitri, Novamizanti, & Ibrahim, 2020).

Digital Wavelet Transform (DWT)

The Discrete Wavelet Transform (DWT) is a mathematical technique that decomposes a signal into high-pass and low-pass frequency components. In image watermarking, watermark embedding is performed by comparing DWT coefficients across these frequency subbands, selecting the subband with the highest coefficient magnitude for watermark insertion (Gani & Setiyono, 2019).

The Inverse Discrete Wavelet Transform (IDWT) reconstructs the original image from its decomposed components (Fathiha, 2021). DWT effectively separates an image into four subbands:

1. LL (Low–Low): Approximation,
2. LH (Low–High): Vertical detail,
3. HL (High–Low): Horizontal detail, and
4. HH (High–High): Diagonal detail (Ratnasari & Dwiyanto, 2020).

These subbands enable frequency-domain watermark embedding that maintains image integrity (Rustad, Syukur, & Andono, 2022).

Results

Requirement Analysis

The system was designed based on functional and non-functional requirements for the Digital Image Watermarking Model Using DWT.

Functional Requirements :

1. The system must generate watermarked digital images.
2. The system must be web-based with a user-friendly interface.

Non-Functional Requirements :

1. Software: Microsoft Windows 10, Microsoft Word, Mozilla Firefox, Google Chrome, XAMPP (PHP and MySQL).
2. Hardware: Laptop and printer.
3. User Access: Users can upload digital images and create watermarked outputs.

System Flowchart

The system workflow begins when the user initializes the program and uploads a digital image. The system verifies the image type and initiates watermarking using the DWT method.

If the process is successful, the system generates a watermarked image; otherwise, it prompts the user to re-upload.

Use Case Design

A Use Case Diagram was created to model user interaction with the system. The single actor, User, performs the following actions:

1. Uploads a digital image.
2. Executes the watermarking process using DWT.
3. Views and downloads the resulting watermarked image.

Interface Design



The user interface is web-based and allows users to perform watermarking efficiently. Test images of various dimensions were used in the evaluation:




No	Image Dimension	Format
1	256 × 256	.jpg, .png
2	128 × 128	.jpg, .png
3	64 × 64	.jpg, .png
4	32 × 32	.jpg, .png
5	16 × 16	.jpg, .png

Testing

1. The testing phase assessed three performance metrics: Peak Signal-to-Noise Ratio (PSNR) — measures the quality of the watermarked image.
2. Mean Square Error (MSE) — evaluates the average pixel-level difference between the original and watermarked images.
3. Structural Similarity (SC) — quantifies similarity between images; values approaching 1 indicate high fidelity.

Result Summary

No	Citra	Dimensi	Ekstensi	MSE	PSNR
1		256 x 256	.jpg	1.4523	1.7902
2		128 x 128	.jpg	1.3058	1.7902

3		64 x 64	.jpg	1.0441	7.9432
4		32 x 32	.jpg	1.5153	14.1249
5		16 x 16	.jpg	572.4588	20.5535

Images with 256×256 and 128×128 dimensions achieved the highest watermark quality, exhibiting low MSE and high PSNR values. Conversely, smaller images (e.g., 16×16) were more prone to distortion during watermark extraction.

Format Comparison

JPG Format

No	Citra	Watermarking	Ekstensi	MSE	PSNR	SC
1			.jpg	1.0213	7.9761	1.0590
2			.jpg	1.0213	7.9761	1.0632
3			.jpg	1.0213	7.9761	1.0290
4			.jpg	1.0213	7.9761	1.0251

5			.jpg	1.0213	7.9761	1.0114
---	---	---	------	--------	--------	--------

PNG Format

No	Citra	Watermarking	Ekstensi	MSE	PSNR	SC
1			.png	1.0321	7.2567	1.0564
2			.png	1.0321	7.2567	1.0298
3			.png	1.0321	7.2567	1.0254
4			.png	1.0321	7.2567	1.0113
5			.png	1.0321	7.2567	1.0209

The results demonstrate that .jpg images produced better watermark quality than .png, as indicated by lower MSE and higher SC values.

Discussion

The results of this study confirm that the DWT-based digital watermarking method is both effective and reliable in maintaining the visual integrity of images while embedding ownership information for copyright protection. The technique successfully balances two crucial aspects of digital watermarking—imperceptibility and robustness—ensuring that the

embedded watermark remains invisible to the human eye yet resilient against common image manipulations such as compression, resizing, and filtering. Quantitative analysis demonstrated that the processed images retained high fidelity, with Peak Signal-to-Noise Ratio (PSNR) values indicating minimal distortion and Mean Square Error (MSE) values approaching zero. These results signify that the watermarked images are nearly indistinguishable from their originals, thus fulfilling the primary requirement of imperceptibility in watermarking systems.

In addition to PSNR and MSE, the Similarity Coefficient (SC) between the original and watermarked images exhibited values close to 1.0, confirming a high degree of structural and visual similarity. This metric reinforces the conclusion that the embedding process does not significantly alter the image's perceptual quality. The watermark embedding and extraction processes remained stable across multiple test iterations, demonstrating that the DWT method supports consistent watermark recovery even under moderate image transformation or compression. This finding is consistent with the theoretical advantages of the wavelet domain, where embedding occurs in frequency components less perceptible to human vision but stable under signal manipulation.

The study also revealed that the JPEG (.jpg) format proved to be particularly suitable for implementing the DWT-based watermarking algorithm. Although JPEG uses lossy compression, its mechanism retains essential low-frequency coefficients, which are critical for embedding and preserving the watermark in DWT-based systems. Because the Discrete Wavelet Transform operates in the frequency domain, embedding the watermark in these coefficients enhances both robustness and imperceptibility. Consequently, even after compression, the watermark information remains detectable and recoverable with minimal degradation. This finding highlights an important practical implication—rather than being an obstacle, controlled compression can in fact support watermark durability by eliminating redundant data while preserving the watermark-embedded frequency bands.

Comparative analysis further shows that the DWT-based watermarking technique outperforms traditional spatial-domain methods in terms of stability and resistance to tampering. While spatial methods directly modify pixel values—making them more vulnerable to manipulation—the wavelet domain provides a multiresolution representation that distributes watermark data across several subbands. As a result, the watermark is better concealed and less affected by noise, filtering, or cropping operations. Moreover, embedding in the low-frequency subbands (LL or HL) ensures long-term persistence of ownership information without compromising the aesthetic quality of the image. The reconstructed images displayed high PSNR values (often exceeding 40 dB), confirming that the human visual system could not detect perceptual differences between original and watermarked images.

These findings are strongly aligned with the results of Fathiha (2021) and Utami et al. (2022), who demonstrated that Discrete Wavelet Transform provides a highly effective balance between watermark robustness and imperceptibility. Fathiha's research emphasized DWT's resilience against compression and geometric attacks, while Utami et al. validated its superior capability in preserving image quality compared to Discrete Cosine Transform (DCT)-based methods. Both studies underscore the suitability of DWT for practical applications that require secure digital ownership verification, particularly in contexts where image distribution and sharing are common, such as e-learning materials, e-government databases, and online media archives.

Beyond its technical performance, the application of DWT-based watermarking in this study also carries ethical and legal significance. By embedding invisible ownership metadata

directly within digital media, institutions and creators can assert copyright claims without altering the visual integrity of their works. This approach supports the broader framework of digital rights management (DRM) and helps prevent content misuse or falsification—a growing concern in the digital economy. Furthermore, the method's strong performance in maintaining fidelity and robustness ensures that the technology can be integrated into real-world content protection systems, such as digital libraries, medical imaging systems, and official document verification platforms. Demonstrating that DWT provides robust watermarking while maintaining high imperceptibility.

In conclusion, the results validate the efficacy of DWT as a watermarking framework for balancing robustness, imperceptibility, and recoverability. The combination of high PSNR, low MSE, and near-perfect similarity coefficients ($SC \approx 1$) demonstrates that the method can successfully preserve image quality while embedding durable ownership information. The findings not only reinforce prior research by Fathiha (2021) and Utami et al. (2022) but also provide a foundation for future enhancements—such as integrating hybrid techniques (DWT-DCT or DWT-SVD) to further increase resistance against advanced attacks. As digital data exchange continues to expand, methods like DWT-based watermarking will play a critical role in protecting intellectual property, promoting ethical media use, and strengthening trust in digital information systems.

Conclusion and Recommendations

Based on the analysis and results, the following conclusions are drawn:

1. The Discrete Wavelet Transform (DWT) successfully decomposed and reconstructed digital images for watermark embedding and extraction using Inverse DWT (IDWT).
2. The DWT-based watermarking process produced high-quality, imperceptible watermarked images, as reflected in high SC values.
3. Among all tested formats, .jpg images yielded the best performance, demonstrating superior decompression and watermark retention compared to .png images

Disclosure Statement

The authors declare no conflict of interest regarding the research, authorship, or publication of this article.

Acknowledgments

The authors express their gratitude to the Department of Informatics Engineering, Faculty of Science and Technology, Universitas Bina Darma, for their guidance, facilities, and academic support throughout this study.

References

- Andika, D., & Darwis, D. (2020). Modification of the Gifshuffle algorithm to improve image quality in steganography. *Jurnal Ilmiah Infrastruktur Teknologi Informasi*, 1(2), 19–23.

- Alegra, V. P., & Alam, A. (2023). Implementation of digital watermarking using the discrete cosine transform (DCT) method in digital images. *Authentication Authorization Accounting Pendidikan Teknologi Informasi dan Teknologi Informasi*, 1(2), 86–90.
- Aulia, I. (2019). Implementation of watermarking techniques on digital images using fractal and discrete cosine transform (DCT). *Informasi dan Teknologi Ilmiah (INTI)*, 6(2), 235–240.
- Fathiha, V. A. (2021). Implementation of watermarking techniques using discrete wavelet transform (DWT) and singular value decomposition (SVD) on digital images. *Jurnal Ilmiah Teknologi Informasi Asia*, 14(2), 125–134.
- Gani, S., & Setiyono, B. (2019). Digital invisible watermarking techniques using the DWT (Discrete Wavelet Transform) method. *Jurnal Sains dan Seni ITS*, 7(2), 24–30.
- Hafizhana, Y., Safitri, I., Novamizanti, L., & Ibrahim, N. (2020). Image watermarking on medical images using compressive sensing based on stationary wavelet transform. *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika*, 8(1), 43–50.
- Hondro, Y. S., & Sinurat, S. (2020). Analysis and implementation of the patchwork method for video security. *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, 4(1).
- Ratnasari, A. P., & Dwiyanto, F. A. (2020). Digital image steganography methods. *Sains, Aplikasi Komputasi dan Teknologi Informasi*, 2(2), 52–59.
- Rustad, S., Syukur, A., & Andono, P. N. (2022). Inverted LSB image steganography using adaptive pattern to improve imperceptibility. *Journal of King Saud University – Computer and Information Sciences*, 34(6), 3559–3568.
- Sanjaya, T., & Setiyadi, D. (2019). Network development life cycle (NDLC) in computer network design at Rumah Shalom Mahanaim. *Jurnal Mahasiswa Bina Insani*, 4(1), 1–10.
- Utami, M., Rismawan, T., & Ristian, U. (2022). Implementation of discrete wavelet transform (DWT) in digital image watermarking for authenticity verification. *Coding Jurnal Komputer dan Aplikasi*, 10(1), 124–135.
-

Biographical Notes

ZARA MARZANI is an undergraduate researcher specializing in digital watermarking and information security technologies at Universitas Bina Darma, Palembang.