A Transform-Domain Robust Watermarking Model Using Discrete Wavelet Transform for Image Copyright Security

Randi Rizal[1]*, Nazwa Auliarahman[1], Siti Rahayu Selamat[2], Mae B. Lodana[3]

[1]Department of Informatics, Siliwangi University, Tasikmalaya (Indonesia)
[2]Faculty of Artificial Intelligence and Cyber Security, Universiti Teknikal Malaysia Melaka (Malaysia)
[3]College of Information and Communication Technology, STI West Negros University (Philippines)

* Corresponding author: randirizal@unsil.ac.id

International Journal of Informatics and Computing

Received 6 October 2025 | Accepted 5 November 2025 | Early Access 30 November 2025

Abstract

This research investigates the application of the Discrete Wavelet Transform (DWT) for digital image copyright protection in JPG and PNG formats. Specifically, a level 1 two-dimensional DWT decomposition using the Haar wavelet is employed to embed and evaluate digital watermarks. The experimental framework compares original (raw) images and watermarked images to assess imperceptibility and robustness. Image quality degradation is quantitatively analyzed using Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) metrics. The results demonstrate that, under non-attacked conditions, the proposed DWT-based watermarking approach achieves high visual fidelity, with an average PSNR of 57 dB and an MSE of 0.1. These values indicate minimal perceptual distortion and confirm that watermark embedding preserves the structural and visual authenticity of the host image. The Haar wavelet decomposition effectively distributes watermark information within frequency sub-bands while maintaining image quality. However, robustness evaluation under common image manipulation attacks reveals notable limitations. When subjected to noise addition, object removal, image tagging, scaling, flipping, format conversion to PNG, and compression, the method exhibits significant performance degradation. The average PSNR decreases to approximately 30 dB, while the MSE increases to around 5, reflecting reduced resilience against signal processing and geometric distortions. Overall, while the DWT-Haar approach ensures strong imperceptibility in controlled environments, its robustness against diverse attacks remains insufficient. These findings highlight the need for integrating advanced multi-level DWT schemes, hybrid transforms, or adaptive embedding strategies to enhance watermark durability in real-world scenarios.

Keywords

Discrete Wavelet Transform (DWT), Digital Watermarking, Haar Wavelet, Peak Signal-to-Noise Ratio (PSNR), Image Robustness.

I. Introduction

Digital legality is a crucial aspect of today's creative industry, particularly in safeguarding against the illegal use and distribution of digital media [1]. Digital signature protection for image-based media, such as JPG and PNG, requires an effective and efficient method to ensure original artwork can be recognized and protected from infringement [2]. One method used to achieve this goal is the application of the Discrete Wavelet Transform (DWT) method, which can increase the strength security of digital work protection [3].

Discrete Wavelet Transform (DWT) is used to convert a sine wave or bar graph into variable frequency components, allowing it to capture important information in both the time and frequency domains [4]. Denoising, pattern recognition, image compression, and various image processing applications have been widely used with DWT methods. In the context of digital signature protection, DWT can be used to apply digital watermarks to images that are not readily visible to the human eye but can still be detected and verified [5].

One important aspect of watermarking techniques is how image quality changes when a watermark is applied [6]. Peak Signal-to-Noise Ratio (PSNR) is often used as an evaluation metric to determine image quality degradation after watermarking. PSNR provides a distance of a few millimetres between the original image and the watermarked image. This is crucial to ensure that the watermark does not significantly degrade the visual quality of the image [7],[8].

Some of the advantages gained from using DWT in the watermarking process, the most prominent is its ability to utilize multi-resolution wavelet transform data. This means that the watermark can be applied at various resolution settings, thus allowing flexibility in comparing the strength of the watermark with image quality [9],[10]. In addition, by using DWT, the watermark can be applied to more sensitive image content. This makes watermark detection more difficult and requires attention from disadvantaged parties [11].

Please cite this article as: Rizal, R., Auliarahman, N., Rahayu Selamat, Siti., & B. Lodana, Mae. (2025). A Transform-Domain Robust Watermarking Model Using Discrete Wavelet Transform for Image Copyright Security. International Journal of Informatics and Computing, 1(2), 72-81.

The use of PSNR in post-watermarking image quality analysis provides important information regarding the impact of the watermarking process on image quality. A higher PSNR indicates that the image quality after watermarking is almost the same as the original image, this is the main goal of any effective watermarking technique [12]. Combining DWT with PSNR analysis allows the development of a digital signature protection system that is not only secure but also improves the visual integrity of graphic media [13], [14].

Therefore, this research will concentrate on the use of the Discrete Wavelet Transform (DWT) method for legal protection in JPG and PNG image formats, as well as assessing the quality of previously watermarked images using PSNR measurements. The main objective of this research is to develop an efficient and effective watermarking technique that can protect digital works without reducing the visual quality of the protected images.

II. Related Work

The rapid growth of digital media distribution has intensified concerns regarding copyright protection, data integrity, and unauthorized image manipulation [15]. Consequently, numerous studies have explored robust and imperceptible watermarking techniques to safeguard digital images against misuse. Prior research has primarily focused on transform-domain approaches, particularly those leveraging frequency-based methods due to their superior balance between imperceptibility and robustness [16]. Among these, the Discrete Wavelet Transform (DWT) has emerged as a widely adopted technique because of its multi-resolution characteristics [17].

A. Digital Image

A visual representation of an object or work produced through a digitization process. In this process, analog (continuous) graphics are converted into digital (discrete) graphics using digital image processing software or a digital camera sensor [6]. Digital imagery consists of individual image fragments, or pixels, each of which has a different intensity or value represented by a different binary code. Digital media can be structured in a two-dimensional matrix format, where each matrix element (pixel) has a value representing an intensity or value. For example, grayscale has only one intensity value per image, while RGB has three values for each image corresponding to three color values red, green, and blue [7]. In this experiment, digital images were used as watermarked image files. An example of a digital image can be seen in Figure 1.

Fig. 1. Digital Image

B. Watermarking

In the digital watermarking process, a watermark is applied to the digital signature, also known as encoding. Encoding is responsible for storing the media and the watermark itself. The image below shows the insertion process in digital media, as shown in Figure 2.

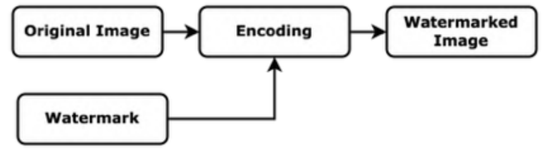


Fig. 2. Insertion Flow Process

After the encoding process, a watermarked image is obtained. Decoding information is also involved in the watermarking process. Decoding is an extraction process applied to a watermarked document with the aim of recovering the original digital document and the watermark that was previously removed from the watermarked document. Essentially, extraction is the process of comparing the original digital signature with the watermarked signature to obtain an approved watermark. This depends on the method used in developing the watermarking, in terms of its relative strength compared to other processes. Below is a diagram of the extraction process flow for a watermarked image using the DWT method, as shown in Figure 3.

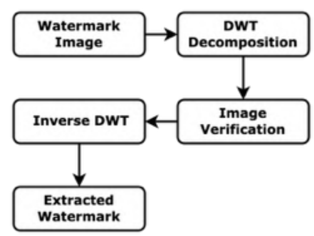


Fig. 3. Extraction Process with DWT

C. Discrete Wavelet Transform (DWT)

The Wavelet Transform (DWT) is a fast and gentle transformation technique that converts an image from the spatial domain to the frequency domain. Wavelets are functions integrated over the upper and lower x-axis. Wavelets are used as substitutes for sine and cosine in the Fourier transform. They serve as basic functions for graphical and symbolic representation. In general, DWT refers to the decomposition of an image into appropriate frequency sub bands. The sub band components of the wavelet transform are achieved by decreasing the decomposition level. One method of implementing DWT is to use low-pass and high-pass filters to extract the signal. The filters themselves are functions applied to the signal. Average and difference decompositions play a crucial role in understanding the wavelet transform. Smoothing is achieved by calculating the average value of two data pairs using the equation below.

$$p = \frac{x+y}{2}, \quad p = \frac{x-y}{2} \tag{1}$$

Description:

p = pixel in the digital image.
x = first digit of the obtained decimal value.
y = second digit of the obtained decimal value.

The level 1 decomposition process produces four sub-images created from the image transformation process: LL (Low-Low), LH (Low-High), HL (High-Low), and HH (High-High). The sub image that is the average of the original image is the LL sub image. On the other hand, HL, LH, and HH have high frame rates so they can be called basic versions of the original image [8], as shown in Figure 4.

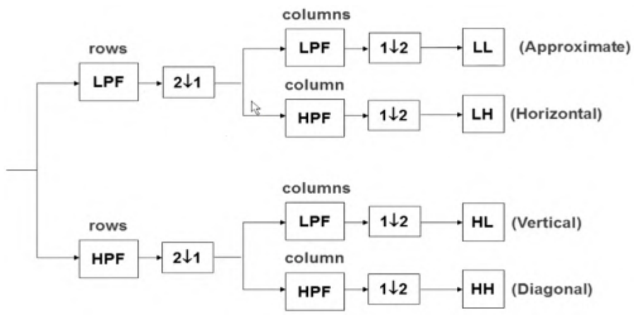


Fig. 4. Haar Wavelet Level 1 Results

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

The Peak Signal-to-Noise Ratio (PSNR) is a metric used to measure the quality of a reconstructed compressed image or video compared to the original. PSNR is often used in image processing and image compression to assess how closely the compressed or transformed image resembles the original image. PSNR is measured in decibels (dB), by comparing the mean squared error (MSE) between the pixels of the original image and the processed image.

To calculate the MSE value, there is an equation formula that needs to be done, namely:

$$MSE = \frac{\sum[F(i,j) - f(i,j)]^2}{N^2} \quad (2)$$

Description:

N^2 = the result of length and width in pixels.
F (i, j) = original image.
f (i, j) = reconstructed image.

Based on the MSE equation, the PSNR value can be calculated. The value of 255 in the formula below is the upper limit of a pixel for PSNR analysis.

$$PSNR = 10 \log_{10}\left(\frac{MAXi}{MSE}\right) \quad (3)$$

Description:

MSE = calculated Mean Squared Error value.
MAX_i = maximum possible pixel value of the image used.

The PSNR value to determine the image quality after being watermarked is shown in Table 1.

TABLE I. Image Quality Classification Criteria

No	PSNR (dB)	Image Quality
1.	60	Excellent
2.	50	Good
3.	40	Acceptable
4.	30	Poor
5.	20	Unusable

III. METHODOLOGY

To ensure methodological rigor and achieve the objectives of the proposed watermarking scheme, this study was conducted through a systematic and structured sequence of experimental stages. The research workflow encompasses image acquisition, watermark preparation, DWT-based embedding using Haar wavelet decomposition, reconstruction through inverse DWT, and quantitative performance evaluation. Each stage was designed to assess both imperceptibility and robustness under controlled and attack scenarios. The overall procedure is summarized in the flowchart below, which illustrates the sequential framework of the proposed watermarking methodology.

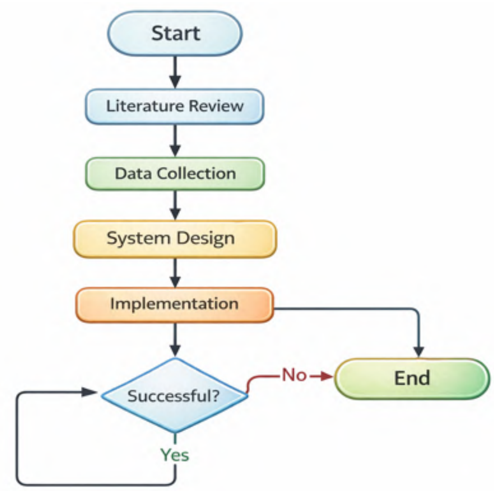


Fig. 5. Research Methodology

A. Literature Review

At this stage, the author conducted a series of observations regarding the workings of the method to be used, namely the Discrete Wavelet Transform (DWT), on 2-dimensional objects. This is done by filtering with a wavelet filter horizontally (rows) and then vertically (columns). The types of wavelets used are Low Pass Filters (LPF) and High Pass Filters (HPF). The results of wavelet filtering produce four sub-bands containing wavelet coefficient values. It works by comparing vertical (column) data with horizontal (row) data. The principle is that combining Low and Low data will produce a small average value, resulting in an insignificant image. However, combining High and High data will also produce a high-pixel image, burdening the system [9]. Therefore, it can be concluded that in the Discrete Wavelet Transform (DWT) workings, a good principle is that combining Low and High data will produce a balanced value. This is done by considering the analysis aspect of the PSNR generated from the MSE value.

B. Data Collection

In this study, we have provided several images and logos that have been customized to meet the needs of the desired results in the watermarking process. The author has also prepared several images that have undergone manipulations such as adding noise, adding objects, cropping images, resizing, transforming, flipping, converting, and converting.

C. System Design

To simplify the system design, the author illustrates the connection to the database using a flowchart.

D. Implementation

In this stage, a system will be developed based on existing research. The implementation method includes creating a desktop application using C#, implementing the evaluated methods, and providing user-friendly interfaces. The watermarking application will function as a tool for protecting digital rights on images using the Discrete Wavelet Transform (DWT) method. The DWT method allows for the efficient and effective application of watermarks to many types of graphics or image manipulation. This application will allow users to edit images and add watermark text. With an intuitive user interface, users can easily complete the watermarking process without requiring complex technical knowledge.

E. Testing

The final stage is testing, to verify the application's feasibility based on the applied method. The author used the Haar Wavelet method to compare system calculations with raw data and watermarked data. The results were analyzed using the PSNR (Regressive Real-Time Regression Regression) to determine the quality of the watermarked image, which is a derivative of the level 1 decomposition of the DWT method in two dimensions. The testing was illustrated with a flowchart to facilitate understanding.

IV. Result and Discussion

The following section presents the implementation results of the proposed Discrete Wavelet Transform (DWT)-based watermarking scheme. The algorithm operates by decomposing pixel intensity values of the host image into frequency-domain components, enabling watermark embedding within selected sub-bands. This transformation facilitates controlled modification of image coefficients while preserving perceptual quality.

In this study, a level 1 two-dimensional DWT decomposition is employed, producing four sub-bands: Low-Low (LL), Low-High (LH), High-Low (HL), and High-High (HH). Among these, the LH and HL sub-bands are primarily utilized for PSNR-based imperceptibility analysis, as they capture significant edge and texture information while maintaining a balanced trade-off between robustness and visual fidelity [10]. Embedding within these mid-frequency components reduces visible distortion compared to spatial-domain approaches and enhances resistance to minor signal processing operations.

Prior to conducting robustness evaluation through controlled attack simulations, it is essential to outline the watermark embedding workflow implemented in the proposed system. This workflow includes image preprocessing, DWT decomposition, coefficient modification for watermark insertion, inverse DWT reconstruction, and quantitative quality assessment using MSE and PSNR metrics. Understanding this structured insertion mechanism provides a clear foundation for interpreting the robustness and performance results discussed in the subsequent sections.

A. Image Processing

It should be noted that image processing, such as using the DWT algorithm, requires pixel adjustments for each dimension. Since the author conducted the research in 2 dimensions, the pixels will be equalized at 3760 x 2144 px. Next, a decomposition calculation will be performed for each media section. The final step is embedding to produce the watermarked media. As shown in the image, the process will be carried out according to the flowchart below in Figure 6.

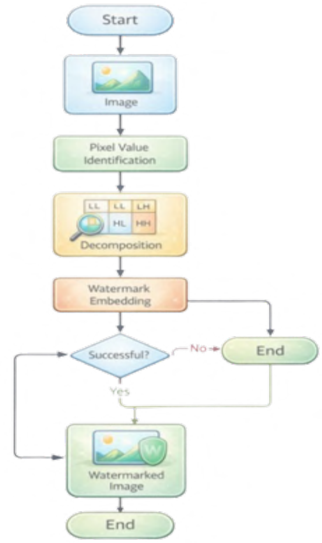


Fig. 6. Image Processing Process

B. Logo Encryption Process in the Watermarking Process

Our experiment involved encrypting a previously grayscale logo. This was done to normalize the color ratio and ensure stability. Furthermore, pixel values at 3760 x 2144 px were also aligned. Next, we performed a decomposition calculation for each part of the logo. The final step was to embed the logo into the image to produce the watermarked media. The image will be processed according to the flowchart below as shown in Figure 7.

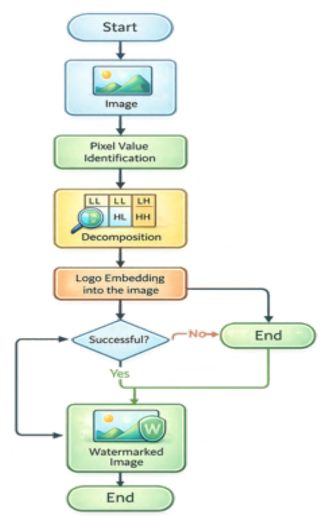


Fig. 7. Logo Processing Process

C. Decomposition Process in Images and Logos

The image below represents a flowchart of the image and logo decomposition process, where the pixels of the resized image and logo will go through two decomposition processes: row decomposition and column decomposition. Therefore, it produces a signal with a pattern and combines all existing sub bands: LL, HL, LH, and HH. This can be seen in the flowchart below as shown in Figure 8.

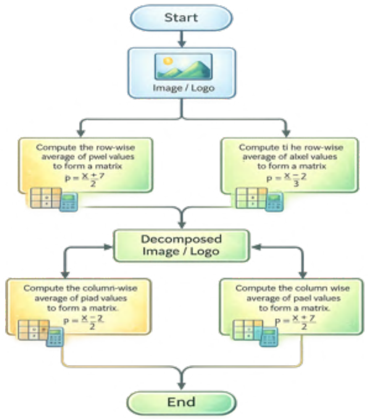


Fig. 8. Decomposition Flow

The first step of calculating the decomposition on each existing row will produce the L and H sub bands when the row direction decomposition calculation process is used. The results of the row decomposition can be seen in the table below as shown in Table II.

TABLE II. Row Decomposition Results

L				H			
36	6.5	3.5	13.5	30	45	2	14
17.5	15.5	4.5	15.5	41	36	32	17
19.5	7.5	10	10	27	29	34.5	46
30	29	27	27	37	15	16	15
12	64	17.5	18	59	38	24	33.5
7	12	24	37	48	55	37	63
14	17	28	5	12	32	41	37
6	3	40	38	10	26	27	53.5

The second step in calculating the decomposition of each existing column will produce 4 sub bands, namely LL, HL, LH, and HH sub bands when the column direction decomposition calculation process is used. The results of the decomposition calculated vertically produce calculations as in the Table III.

TABLE III. Column Decomposition Results

	L				H			
L	260	164.5	94.5	101	-54.5	45	35	33
	135	109.5	133.5	266	-41.5	-17	-32	21
	89.5	98	129	192	32	19	34.5	16
	117	93	106	131	19	15	16	-21
H	-5	25	13	26	13.5	21	-11	24.5
	-9	-12	-31	42	-22	-18	19	-10
	11	-27	22	-51	10.5	7	18.5	-15
	4	9	19	-13	-12	8	23	43

D. Sniffing the Logo into the Watermark

This process involves inserting the logo into the original image by taking the LL pixel values from the image and the LL pixel values from the logo. The next step involves inserting the LL pixel values from the logo and image using a shift method. After successful insertion, the resulting image is watermarked. The process is as shown in Figure 9.

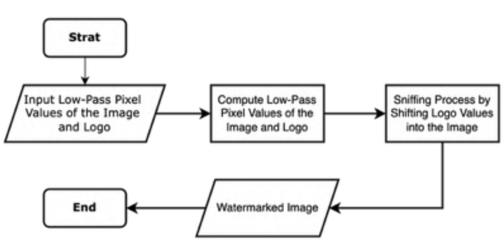


Fig. 9. The sniffing processes logo into a watermarked image

E. Image Reconstruction Process

This process involves two important aspects: row reconstruction and column reconstruction. The two are then mathematically multiplied to produce the coefficient variables for the image to be encrypted. The image reconstruction process is illustrated in Figure 10.

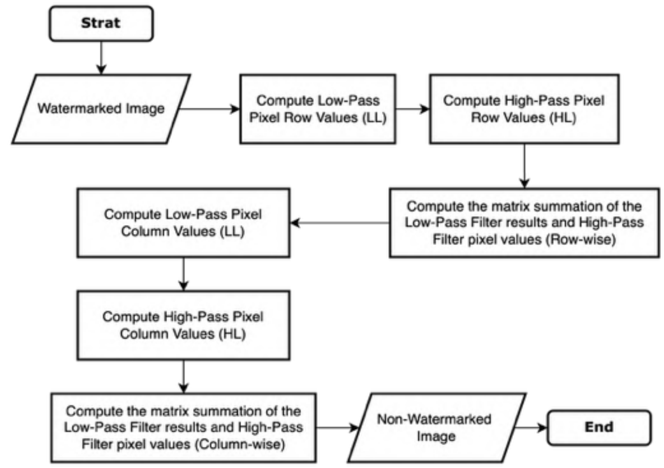


Fig. 10. Image Reconstruction Process

This reconstruction process is essentially a balancing act of the decomposition process, adhering to the parameters established in the decomposition process. It is possible to see the matrix rules for the Low and High filters.

TABLE IV. Low Pass

C1	C2	C3	C4
1	0	0	0
1	0	0	0
0	1	0	0
0	1	0	0
0	0	1	0
0	0	1	0
0	0	0	1
0	0	0	1

TABLE V. High Pass

C1	C2	C3	C4
1	**0**	**0**	**0**
-1	0	0	0
0	1	0	0
0	-1	0	0
0	0	1	0
0	0	-1	0
0	0	0	1
0	0	0	-1

The first step is to reconstruct the calculation first on the row by multiplying the row in the LL sub band matrix with the low-pass filter matrix. The next step is to multiply the row in the HL sub band matrix with the high-pass filter matrix. The results of the rows in the LL sub band and HL sub band are then added together, resulting in a full reconstruction of the entire row. The results of the row reconstruction are as shown in the table below.

Table VI. Row Reconstruction Matrix

L_1	L_2	L_3	L_4	H_1	H_2	H_3	H_4
44	66	53	85	13	17	29	27
87	71	83	56	-15	43	-7	43
12	38	10	13	23	20	23	32
39	78	56	45	32	44	-38	-30

L_1	L_2	L_3	L_4	H_1	H_2	H_3	H_4
44	66	53	85	13	17	29	27
52	34	17	38	44	-32	30	-33
99	48	35	51	67	-55	-44	31
37	26	46	48	28	30	31	-28
41	64	42	71	19	-35	42	-30

After the row reconstruction process is successful, the next step is column reconstruction. This column reconstruction process is almost the same as the row reconstruction process. The first step is to match the coefficients of the LL sub band matrix with the low-pass filter matrix. Next, a high-pass filter is applied to the curve in the HL sub band. The results of the LL and HL sub bands are then combined, resulting in a reconstructed column. This procedure is performed on each LL sub band column and each HL sub band column so that each column is constructed independently. The results of the column reconstruction are as shown in the table below.

Table VII. Column Reconstruction Results

L_1	L_2	L_3	L_4	H_1	H_2	H_3	H_4
11	66	42	85	57	107	29	27
95	71	50	71	121	43	28	43
54	90	44	39	166	20	28	32
40	152	56	75	130	44	30	55
49	163	68	116	36	85	30	35
152	117	33	129	34	130	31	28
163	34	64	95	82	30	31	30
117	59	57	32	169	29	27	39

F. Watermark Extraction Process

The process shown in the image below illustrates the steps required to recover a watermark from its original form. The first step in the reconstruction process is to perform a low-pass filter matrix analysis on the rows and columns. Once the results are obtained, the next step is to analyze the rows and columns using a high-pass filter. The output of this reconstruction process is a watermark-free image.

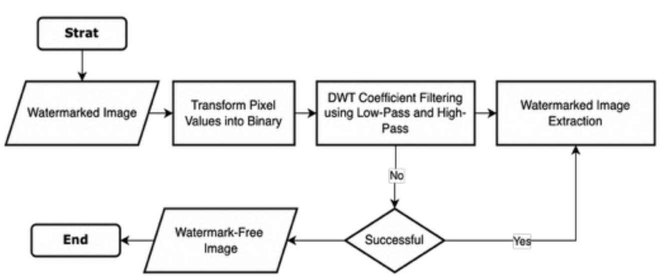


Fig. 11. Watermark Extraction Process

G. PNSR Analysis Process

The final step in assessing watermarking performance involves calculating the Mean Squared Error (MSE) to measure the average squared difference between the original and watermarked images at the pixel level. A lower MSE value indicates minimal distortion and higher structural fidelity. Correspondingly, the Peak Signal-to-Noise Ratio (PSNR), which is inversely related to MSE, provides a logarithmic measure of perceptual quality; thus, higher PSNR values signify better image preservation and imperceptibility of the embedded watermark.

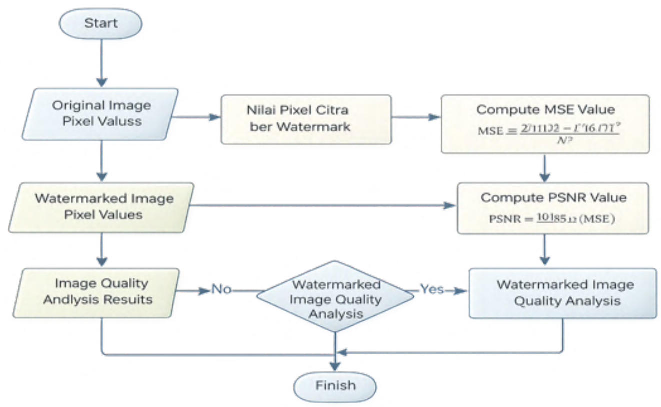
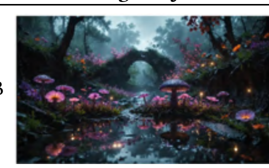


Fig. 12. PSNR Analysis Process

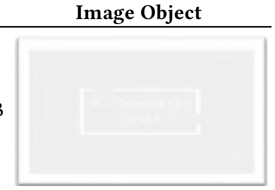
The MSE value will assist PSNR analysis in deciding whether the image is suitable for embedding. The process is illustrated in the flowchart below. This research aims to identify image manipulation using the Discrete Wavelet Transform (DWT) detection method as a preventative measure. The focus of this research is a copyright infringement simulation where digital images have been modified. This study covers various scenarios to understand potential cases. DWT is used as a method to strengthen security features in the image manipulation detection process.

Table VIII. Cover Image Identification

File Name	Dimensions	Format	Size	Image Object
Image3	3760×2144px	JPEG	750 KB	

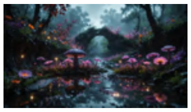
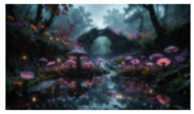
The cover page and watermark page were the objects of the study. To optimize research efficiency, the research scenario was adjusted to the predetermined final assignment duration and can be seen in Tables 8 and 9. Table 9 presents the digital images that were the focus of the analysis as cover images in .jpeg format, while Table 9 contains all digital images that were used as the object of analysis as watermarks in .jpg format.

Table IX. Digital Image Identification

File Name	Dimensions	Format	Size	Image Object
Watermark	3760×2144px	.png	64 KB	

The next step is to apply a digital watermark to the image using the DWT technique. Once this process is complete, the watermarked image (or something similar) will be generated. This procedure is performed using a C# application created in Visual Studio. At this point, several requirements must be met for the process to run smoothly. These requirements include the watermark and cover image must have the same resolution. For example, if the watermark cover resolution is 3760x2144 pixels, then the watermark resolution must also be the same, as shown in Table 10.

Table X. Image Alignment

Cover Image	Image Watermarked	Image Object
		
(a)	(b)	(c)

Analysis of the quality of watermarked images using MSE and PSNR testing, the results of the PSNR and MSE value analysis. The MSE value is close to zero and the PSNR value is more than 30 indicating that the watermark insertion process does not significantly affect the image quality so that the watermarked image still has good quality. The analysis presented in Table 11 demonstrates that the MSE values remain close to zero, while the PSNR values consistently exceed 30dB. These results confirm that the watermark embedding process introduces negligible distortion. Consequently, the visual integrity and perceptual quality of the watermarked images are effectively preserved.

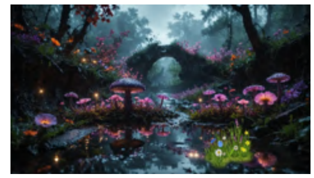
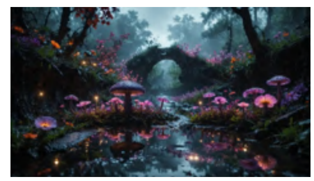
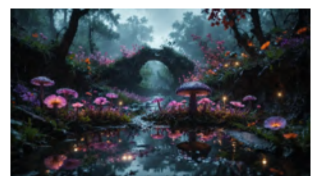
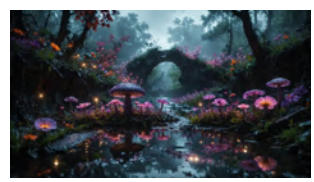
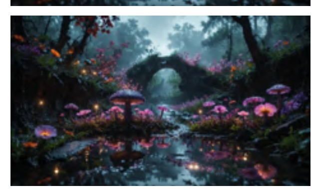
Table XI. PSNR Analysis Results on High Paas Images

Nama File	Nilai MSE	Nilai PSNR
Watermarked3_HighRes	0.110963177779453795	57.679014751776776 dB

Watermark resistance testing will be conducted by modifying or manipulating the watermarked image. Several watermark resistance testing methods include adding noise to the watermarked image, object manipulation, and adding new objects to the watermarked image. Other transformation methods include image cropping and flip transformation, as well as testing the format conversion to PNG and compression of 12.66%. The test results are presented in Table 12, which shows various types of image modifications. After this stage, the watermarked image that has undergone the modification process will be extracted and compared with the original watermarked image to determine the differences and effects of the modification or manipulation on the watermarked image. This allows for the watermarking resistance using the DWT method to be determined.

The robustness evaluation is designed to simulate realistic signal processing and geometric attacks that commonly occur during image transmission and redistribution. Additive noise, object removal, and object insertion assess resistance against content-level manipulation, while cropping and flipping evaluate geometric transformation resilience. Following each attack scenario, the modified watermarked image is subjected to the extraction process using the inverse DWT procedure. The extracted watermark is then quantitatively compared with the originally embedded watermark to measure degradation effects. Variations in PSNR, MSE, and visual similarity provide objective indicators of robustness. Through this comparative analysis, the resilience of the proposed DWT-based watermarking scheme can be rigorously determined in terms of its ability to withstand intentional and unintentional distortions.

Table XII. Image Modification as a Form of Attack

Modification/Manipulation	Image Object
(a) Add Noise	
(b) Add Object	
(c) Crop Image	
(d) Resize (1080x615px)	
(e) Transform flip	
(f) Convert to PNG	
(g) Compressed 12,66_	

After the watermarked image has gone through the modification process, the watermark will be extracted from the modified image and then compared with the results of the watermark extraction from the original image that has not gone through the modification process. The results of the watermark extraction from the original image that has not gone through the modification process can be seen in Figure 13.

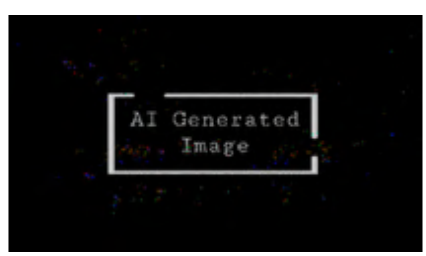


Fig. 13. Original Image Extraction Results

In Figure 13, it can be seen that the image that has been watermarked and has not gone through the modification process produces a complete watermark extraction and there is no damage to the watermark, while the image that has been watermarked and has gone through the modification or manipulation process is presented in Table 13 for further analysis using MSE and PSNR tests.

Table XIII. Modified Image Extraction Results

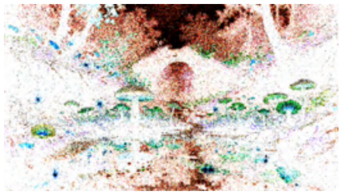
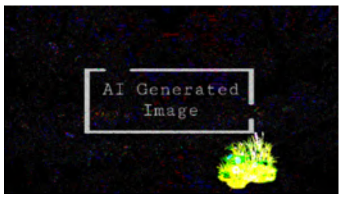
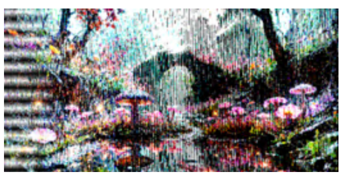
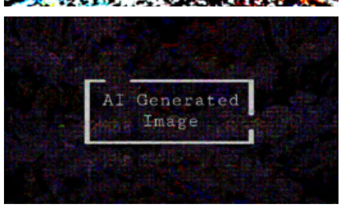
Modification/Manipulation		Image Object
(a)	Add Noise	
(b)	Add Object	
(c)	Crop Image	
(d)	Resize (1080x615px)	
(e)	Transform flip	
(f)	Convert to PNG	
(g)	Compressed 12,66_	

Table 13 shows the results of watermark extraction from the modified image. The quality of the extracted watermark will then be assessed using the MSE and PSNR parameters to obtain conclusions from the watermark extraction results on the modified image. The test results using the MSE and PSNR parameters are presented in Table 14, which shows the assessment of the watermark extraction results on the modified image. The MSE and PSNR calculations in Table 14 indicate that the watermarked image that has undergone the modified process exhibits significant changes compared to the watermark extraction results from the original image that has not undergone the modified process. This is based on the MSE calculation results not approaching zero and the PSNR calculation results being less than 30.

Table XIV. PSNR Analysis on Modified Images

Modification	MSE	PSNR
Add Noise	50636.34486071967	1.086180118860885 dB
Add Object	2457.527583533463	14.225819597720196 dB
Crop Image	28723.77719439703	3.5483881155039114 dB
Resize 1080x615px	35806.39446550492	2.5911976905372907 dB
Transform Flip	30146.91788923567	3.33837442803652 dB
Convert to PNG	1638.3260742497619	15.986800176840712 dB
Compressed 12,66_	7688.053332655208	9.272639734606052 dB

The test results presented in Table 14 show that images that have been watermarked and gone through a modification or manipulation process can have a significant impact on the results of watermark extraction from the modified image, thus the DWT method has weaknesses against image modification or manipulation because it cannot maintain the quality of the watermark on images that have undergone a modification process.

V. Conclusion

The experimental evaluation of the proposed DWT-based digital copyright protection scheme on JPG and PNG image formats reveals two principal findings. Under non-attack conditions, the watermarked images achieved a Peak Signal-to-Noise Ratio (PSNR) of 57 dB, indicating excellent perceptual quality and minimal distortion relative to the original image. This high PSNR value, combined with a Mean Squared Error (MSE) of 0.1, confirms that the watermark embedding process preserves structural fidelity and visual authenticity. These results demonstrate that the Discrete Wavelet Transform (DWT), particularly in the transform domain, provides strong imperceptibility and maintains the integrity of the host image when no external interference is introduced. However, robustness evaluation under various manipulation attacks reveals significant performance degradation. The watermarking scheme was tested against common signal processing and geometric distortions, including additive noise, object insertion, image cropping, resizing (1080 × 615 px), horizontal and vertical flipping, format conversion to PNG, and compression (12.66 quality level). Under these attack scenarios, the average PSNR dropped below 30 dB, while the average MSE increased to approximately 5. These metrics indicate substantial distortion and reduced watermark resilience. Consequently, although the proposed DWT-based approach demonstrates strong imperceptibility in controlled environments, it exhibits limited robustness against diverse manipulation attacks. This finding highlights the necessity of integrating more advanced embedding, multi decomposition, or hybrid transform-domain techniques to enhance resistance against real-world adversarial modifications.

References

[1] K. Anam, 'Legal Protection of Intellectual Property Rights in the Digital Industry: A Review of Legal Developments and Implementation Challenges', *West Science Law and Human Rights*, vol. 2, no. 04, pp. 358–366, Oct. 2024. DOI: 10.58812/wslhr.v2i04.1155

[2] J. Xu, J. Zhang, and J. Wang, 'Digital Image Copyright Protection and Management Approach—Based on Artificial Intelligence and Blockchain Technology', *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 20, no. 2, p. 76, Apr. 2025. DOI: 10.3390/jtaer20020076

[3] M. Begum *et al.*, 'Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition for Enhanced Imperceptibility and Robustness', *Algorithms*, vol. 17, no. 1, p. 32, Jan. 2024. DOI: 10.3390/a17010032

[4] E. Ghaderpour, S. D. Pagiatakis, and Q. K. Hassan, 'A Survey on Change Detection and Time Series Analysis with Applications', *Applied Sciences*, vol. 11, no. 13, p. 6141, Jul. 2021. DOI: 10.3390/app11136141

[5] M. Begum and M. S. Uddin, 'Digital Image Watermarking Techniques: A Review', *Information*, vol. 11, no. 2, p. 110, Feb. 2020. DOI: 10.3390/info11020110

[6] A. A. R. Bsoul and A. B. Ismail, 'Optimizing Image Watermarking with Dual-Tree Complex Wavelet Transform and Particle Swarm Intelligence for Secure and High-Quality Protection', *Applied Sciences*, vol. 15, no. 3, p. 1315, Jan. 2025. DOI: 10.3390/app15031315

[7] C. Zhan, L. Leng, C.-C. Chang, and J.-H. Horng, 'Reversible Image Fragile Watermarking with Dual Tampering Detection', *Electronics*, vol. 13, no. 10, p. 1884, May 2024. DOI: 10.3390/electronics13101884

[8] M. Rai and A. Kesarwani, 'Image Watermarking in the Digital Era: A Review of Transform, ML-Based, and Evolutionary Methods', *Circuits, Systems, and Signal Processing*, Dec. 2025. DOI: 10.1007/s00034-025-03437-7

[9] A. Alrammahi and H. Sajedi, 'A Robust Image Watermarking Based on DWT and RDWT Combined with Möbius Transformations', *Computers, Materials & Continua*, vol. 84, no. 1, pp. 887–918, 2025. DOI: 10.32604/cmc.2025.063866

[10] K. Hebbache, B. Khaldi, O. Aiadi, and A. Benziane, 'A DWT-Based Approach with Gradient Analysis for Robust and Blind Medical Image Watermarking', *Applied Sciences*, vol. 14, no. 14, p. 6199, Jul. 2024. DOI: 10.3390/app14146199

[11] A. Benyoucef, A. Goudjil, M. Hamadouche, M. C. Boutalbi, M. Ammar, and M. El Habib Daho, 'High-capacity DWT-SVD watermarking for MRI images embedding MITR medical information', *Results in Engineering*, vol. 27, p. 105795, Sep. 2025. DOI: 10.1016/j.rineng.2025.105795

[12] M. Bistroń, J. M. Żurada, and Z. Piotrowski, 'Deep Learning for Image Watermarking: A Comprehensive Review and Analysis of Techniques, Challenges, and Applications', *Sensors*, vol. 26, no. 2, p. 444, Jan. 2026. DOI: 10.3390/s26020444

[13] T. K. Araghi and D. Megías, 'Analysis and effectiveness of deeper levels of SVD on performance of hybrid DWT and SVD watermarking', *Multimedia Tools and Applications*, vol. 83, no. 2, pp. 3895–3916, Jan. 2024. DOI: 10.1007/s11042-023-15554-z

[14] A. K. Patel and P. Patel, 'Enhanced Security and Robustness in Color Image Watermarking Using DWT-HD and Quaternion SVD under Hybrid Attacks', *Traitement du Signal*, vol. 41, no. 5, Oct. 2024. DOI: 10.18280/ts.410507

[15] V. Kadha, S. Bakshi, and S. K. Das, 'Unravelling Digital Forgeries: A Systematic Survey on Image Manipulation Detection and Localization', *ACM Computing Surveys*, vol. 57, no. 12, pp. 1–36, Dec. 2025. DOI: 10.1145/3731243

[16] A. S. Beggari, A. Wali, A. Khaldi, M. R. Kafi, and A. K. Sahu, 'Secure and imperceptible medical image watermarking via multiscale QR embedding and attention-based optimization', *Engineering Science and Technology, an International Journal*, vol. 73, p. 102250, Jan. 2026. DOI: 10.1016/j.jestch.2025.102250

[17] X. Guan, R. He, L. Wang, H. Zhou, Y. Liu, and H. Xiong, 'DWTMA-Net: Discrete Wavelet Transform and Multi-Dimensional Attention Network for Remote Sensing Image Dehazing', *Remote Sensing*, vol. 17, no. 12, p. 2033, Jun. 2025. DOI: 10.3390/rs17122033

Randi Rizal

He was born in Tasikmalaya, West Java, Indonesia. He earned his Ph.D. from the Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Malaysia. He is currently a lecturer in the Department of Informatics, Faculty of Engineering, Siliwangi University, Indonesia. His research interests focus on cybersecurity, digital forensics, artificial intelligence, and intelligent systems. He has authored and co-authored numerous scholarly publications in reputable national and international journals and conferences. In addition to his research activities, he serves as the Managing Editor of Innovation in Research of Informatics (INNOVATICS) and as the Editor-in-Chief of the International Journal of Informatics and Computing (JICO), published by the Institute of Advanced Informatics and Computing, Indonesia. His research interests include information security, cryptography, and artificial intelligence for digital forensics, with a particular focus on secure data protection, post-quantum cryptographic mechanisms, intelligent threat detection, and AI-driven forensic investigation frameworks.

Nazwa Auliarahman

She is a researcher in the Forensic and Security Research Group at Siliwangi University, Indonesia. Her research focuses on cryptography, information security, digital forensics, and secure multimedia protection. She is actively involved in studies related to digital watermarking, secure data transmission, and cybersecurity frameworks for image and multimedia systems. Her academic interests also include post-quantum cryptographic mechanisms, intelligent threat detection, and applied security models for digital copyright protection. Through her research activities, she contributes to the development of robust and secure digital information systems in emerging technology environments.

Siti Rahayu Selamat

She is currently an associate professor at the Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Malaysia. She received her Doctor of Philosophy in Computer Science, specializing in Digital Forensics. Her research interests encompass network forensic, cyber terrorism, cyber violence extremism, intrusion detection, network security, and penetration testing. Additionally, she is a dedicated member of the Information Security, Forensics, and Networking (INSFORNET) research group. Her ongoing research includes malware analysis, profiling criminal behavior, and addressing the complexities of cyber violence extremism, contributing significantly to the advancement of cybersecurity and digital forensics fields. She frequently collaborates with international experts, presents her findings at global conferences, and publishes extensively in renowned journals, thereby impacting both academic and professional communities.

Mae B. Lodana

She is affiliated with the College of Information and Communication Technology, STI West Negros University, Philippines. She is engaged in academic and research activities in the areas of information technology, digital technology management, and applied computing.