Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 2, April 2025, Page. 1017-1028
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.2.4423

Imperceptible Watermarking Using Discrete Wavelet Transform and Daisy Descriptor for Hiding Noisy Watermark

Abdussalam[*1], Chaerul Umam[2], Wellia Shinta Sari[3], Eko Hari Rachmawanto[4], Heru Lestiawan[5], Guruh Fajar Shidik[6], Pulung Nurtantio Andono[7], Hussain Md Mehedul Islam[8]

[1,2,4,5,6,7]Study Program in informatics Engineering, Universitas Dian Nuswantoro, Indonesia
[3]Study Program in Information System, Universitas Dian Nuswantoro, Indonesia
[8]Software Engineer, The Mathworks, Inc., United States

Email: [1]grey.salam@dsn.dinus.ac.id

Received : Feb 10, 2025; Revised : Mar 13, 2025; Accepted : May 07, 2025; Published : May 17, 2025

Abstract

This research aims at overcoming the challenge of improving security and robustness in digital image watermarking, a critical activity in protecting intellectual property against misuse and manipulation. In a move to overcome such a challenge, this work introduces a new form of watermarking that incorporates Discrete Wavelet Transform (DWT) and Daisy Descriptor, with a view to enhancing both durability and invisibility of the watermark. The proposed method embeds a noise-variant watermark into selected frequency sub-bands using DWT, while the Daisy Descriptor enhances resistance to noise-based attacks. Testing conducted with three grayscale images, namely Lena, Cameraman, and Lion, each with a resolution of 512 × 512 pixels, showed that the proposed DWT-Daisy Descriptor outperforms current methodologies, producing high Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) values. In fact, in Lena, a PSNR value of 63.71 dB and an SSIM value of 1 were attained, with Cameraman having a PSNR value of 68.33 dB and an SSIM value of 1. As for attack resistivity, a high PSNR value of 50.11 dB under Gaussian attack and 55.70 dB under Salt-and-Pepper attack, with SSIM values approaching 1, confirm the robustness of the proposed scheme. This study highlights the significance of an efficient and secure watermarking technique that not only preserves image quality but also withstands various distortions, making it highly relevant for digital content protection in modern multimedia applications.

Keywords : *Daisy Descriptor, Discrete Wavelet Transform, Gaussian Noise, Image Watermarking, Salt&Peppers Noise.*

1. INTRODUCTION

Watermarking in a digital format is a challenge in terms of its susceptibility to attack and its impact on source information quality, and most prominently, its potential to impair perceptibility of source information and cause perceptual distortions compromising information integrity and overall quality [1]. Complicating this problem is the fact that in inserting watermarks into high-resolution information, even small distortions can have a considerable impact on overall quality [2]. In addition, a challenge critical to a watermark is its survival under perturbations and attack types, such as JPEG compression, cropping, rotation, and added noise, prevalent in processing and information dissemination environments [3]. All such attack types have a potential for eroding, and in extreme cases, eradicating watermarks, and thus, a challenge in developing techniques strong enough to survive such adversity stands out in its formidability [4]. On the one hand, a constraint placed by a necessity for inserting additional marked images with no loss in source information integrity compels a narrow margin for watermarks with possibly deleterious secondary consequences. With an expansion of the use of digital information in a variety of industries, such as multimedia, finance, and medical, such a problem is

becoming increasingly acute [5], [6]. Thus, development of an efficient, sophisticated, and flexible mechanism for inserting watermarks stands out as an important necessity in resolving such complications, providing information integrity and security, and attack and degradation resistance in processing and dissemination environments [7], [8].

The issue at hand is widespread in the field of digital information; therefore, a successful resolution involves a mechanism capable of maintaining information integrity and at the same time embedding a watermark and withstanding a variety of attack types. One such mechanism that can be utilized entails the use of transform techniques in conjunction with feature descriptors for allowing secure and flexible embedding of watermarks. In such a case, use of Discrete Wavelet Transform (DWT) for embedding a watermark in the frequency domain constitutes a breakthrough in offering security for perturbations such as compression and rotation, with integrity in the original information not compromised in any way [9], [10], [11]. In addition, use of DAISY descriptors for counteracting perturbations in relation to noise promotes robustness, with DAISY having the capability of detecting and countering faint noise perturbations, including Gaussian and salt-and-pepper fluctuations [12]. In such a case, therefore, incorporation of DWT for watermark covertness in the frequency domain, in combination with use of DAISY for countering perturbances, effectively maximizes effectiveness in both techniques in use [13]. Consequently, a watermarked information scheme that is decidedly more robust, invisible, and resistant to a range of perturbations and manipulations, with integrity in the digital information not compromised, is produced.

Alzahrani et al. (2022) [10] proposed a digital watermarking system to address copyright issues, focusing on security, visibility, and robustness against attacks. The system combined Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to analyze and defend against various watermark attacks. The DWT was used to embed the host image across four levels, processed with SVD. Performance was evaluated using PSNR and SSIM for invisibility, and NC for robustness. Results showed that the DWT-SVD method provided superior invisibility and robustness against pixel-value modification attacks, outperforming existing systems and demonstrating its effectiveness in securing watermarked images. Awarayi et al. (2021) [14] proposed a digital image watermarking scheme for color images using Discrete Wavelet Transform (DWT) and Fractal Tromino encryption. The host image is first transformed into the frequency domain using DWT, then a binary watermark is encrypted with a fractal and a random key. The encrypted watermark is embedded into the host image to create the watermarked image. Performance was evaluated using Peak Signal-to-Noise Ratio (PSNR) for image quality and Structural Similarity Index Metric (SSIM) for perceptual similarity, showing the method's effectiveness in maintaining high image quality and watermark security. Also, Kumar (2020) [15] proposed a watermarking technique to protect digital rights using Discrete Wavelet Transform (DWT) and Least Significant Bit (LSB) methods. The approach aims to ensure the authenticity of documents, preventing unauthorized modifications or distribution. The cover image is first divided into frequency bands (HH, LH, LL, and HL) using DWT, allowing the watermark to be embedded into these frequency components. The extraction process works in reverse, based on the embedding algorithm. The method's performance is assessed in terms of its ability to maintain image quality while providing robustness against attacks such as JPEG compression and Gaussian noise, ensuring the security of intellectual property.

Based on related study above, this study introduces a new method in digital watermarking techniques through integration between the Discrete Wavelet Transform (DWT) and the DAISY descriptor with a view to improving security and degradation resistivity of watermarks in case of several types of degradation attacks. Unlike methodologies proposed in the past, including those proposed by Alzahrani et al. (2022) [10], who merged DWT with SVD; Awarayi et al. (2021) [14], who utilized Tromino fractal encryption with DWT; and Kumar (2020) [15], who used DWT with the Least

Significant Bit (LSB) algorithm, the present technique prioritizes use of the DAISY descriptor for embedding watermarks in a flexible and resistant manner in case of added noise. Integration of the DAISY descriptor maximizes watermarks' resistivity to degradation triggered through JPEG loss, added noise, and any form of degradation, with DWT allowing insertion of watermarks in the frequency domain, in a manner that integrity in an image is not compromised and detectability in watermarks is not hindered. The proposed mechanism seeks to develop an efficient, secure, and invisible watermarking system for protecting digital information against unauthorized access and distribution.

2. FUNDAMENTAL THEORY

In this section, the fundamental theories underlying the development of digital watermarking techniques will be discussed, along with the principles supporting this research, which include: 2.1 Noise Variant Attack, 2.2 DAISY Descriptor, 2.3 DWT, and 2.4 Quality Assessment (PSNR & SSIM).

2.1. Noisy Variant Attacks

Noise variant attack is a type of attack that involves injecting random perturbations in an image, with an intention to impair its quality and even remove a hidden watermark. Two common types of noise variant attacks include Gaussian noise and Salt-and-Pepper noise. Gaussian noise injects randomness in pixel values following a Gaussian distribution and can cause a degradation in image quality over a period, and in consequence, make detectability of a watermark even more challenging [16]. Salt-and-Pepper noise, in contrast, injects white and black pixels at arbitrary locations in an image, and in consequence, emulates extreme degradation with regard to loss of information [17]. Both types of noise attack can have a profound impact in terms of perceptibility of a concealed watermark and can threaten security of a watermarking scheme [18]. Thus, one must assess efficacy of a watermarking algorithm in terms of its resistivity towards such a noise variant attack, such that even when an image suffers such degradation, a hidden watermark not only survives but even tends to become detectable.

In image watermarking, noise addition is done through calculations which can be seen in equation (1) for Gaussian noise and equation (2) for salt & peppers noise.

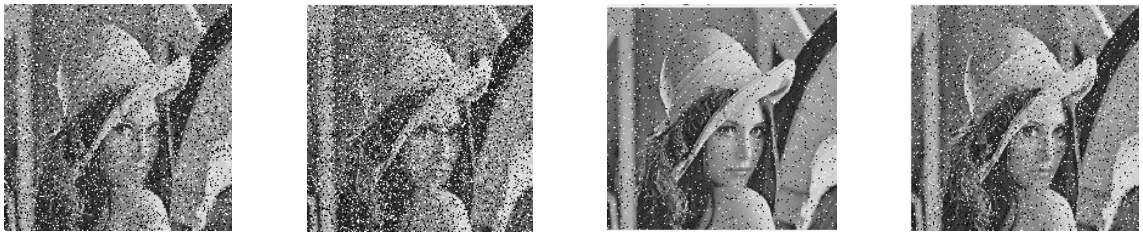
$$G\ (x,y) = W(x,y) + \ N(0,\sigma^2) \qquad (1)$$

Based on equation (1), the gaussian noise is generated by adding random values from a normal distribution to each pixel in an image. G\ \left(x,\ y\right) is the noisy pixel value at position (x,y), W\left(x,y\right) is the watermark pixel value at position (x,y), and N(0,\sigma^2) is the Gaussian noise with mean\ 0 and variance \sigma^2. The noise is sampled from a normal distribution N(0,\sigma^2), where \sigma controls the amount of noise.

$$S\&P\ (x,y) = \begin{cases} 0 & with\ probability\ S\&P_s \\ 255 & with\ probability\ S\&P_p \\ W(x,y) & otherwise \end{cases} \qquad (2)$$

Based on eqution (2), the salt and peppers noise involves randomly replacing pixels in an image with either black (0) or white (255) pixels. S&P\ \left(x,\ y\right) is the noisy pixel value at position (x,y), W\left(x,y\right) is he watermark pixel value at position (x,y), {S&P}_s is the probability of introducing a "salt" (white pixel), and {S&P}_p is the probability of introducing a "pepper" (black pixel). Salt and pepper noise is characterized by sporadic replacement of image pixels with extreme values (either 0 or 255), depending on the noise probability {S&P}_s and {S&P}_p. The results based on gaussian and salt&peppers noise can be seen in Figure 1.

Vol. 6, No. 2, April 2025, Page. 1017-1028
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.2.4423



(a) Gaussian Noise with 0.25 intensity (b) Gaussian Noise with 0.5 intensity (c) salt & peppers noise with 0.25 intensity (d) salt & peppers noise with 0.5 intensity

Figure 1. Pre-noise embedding at each intensity

2.2. Daisy Descriptor

DAISY descriptor is a feature extraction method primarily used for image analysis and pattern recognition, making it a useful tool in digital watermarking to enhance robustness and security [13]. In the context of image watermarking, DAISY can be utilized to encode watermark features in a way that makes them resilient against attacks such as noise addition, compression, and geometric distortions. The DAISY descriptor works by computing a dense set of descriptors across an image based on gradient orientations, allowing the extraction of distinctive patterns that can be used for embedding and later retrieval of watermark information. This enhances the watermark's imperceptibility while ensuring its robustness against distortions [19]. DAISY descriptor is computed using a weighted sum of convolved image gradients. The equation for the DAISY descriptor based on pixel location (x,y) can be seen in equation (3).

$$D\ (x,y) = \ \sum_{r=1}^{R} \sum_{\theta=1}^{T} W\ (r,\theta) \cdot\ G_{\sigma_r}\ \cdot I\ (x,y) \quad (3)$$

Where, $D\ (x,y)$ is the DAISY descriptor at pixel location (x,y), R is the number of concentric rings around the pixel, T is the number of gradient orientations, $W\ (r,\theta)$ is a weight function applied to the gradients at a specific radius r and orientation θ, G_{σ_r} is a Gaussian kernel with standard deviation σ_r applied at radius r, $I\ (x,y)$ represents the image intensity at position (x,y).

The DAISY descriptor operates using a circular grid structure, consisting of multiple concentric rings around a central pixel. Each ring contains several sampling points, which are strategically positioned to capture local gradient information. At each sampling point, a gradient orientation histogram is computed by analyzing the surrounding pixel intensities. As seen in Figure 2, the traversal goes through the position of the central pixel, with r_i as the radius of the $i-th$ circle and t_j as the $j-th$ sector of the circle. The histogram of gradient orientations for that sector is computed using Equation (4).

$$D\ (p) = \ \{H\ (p, r_i, t_j)\ |\ i = 1, \dots, R, j = 1, \dots, T \qquad (4)$$

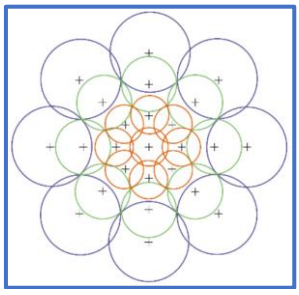


Figure 2. Feature Region of Daisy Derscriptor

Vol. 6, No. 2, April 2025, Page. 1017-1028
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.2.4423

2.3. Discrete Wavelet Transform (DWT)

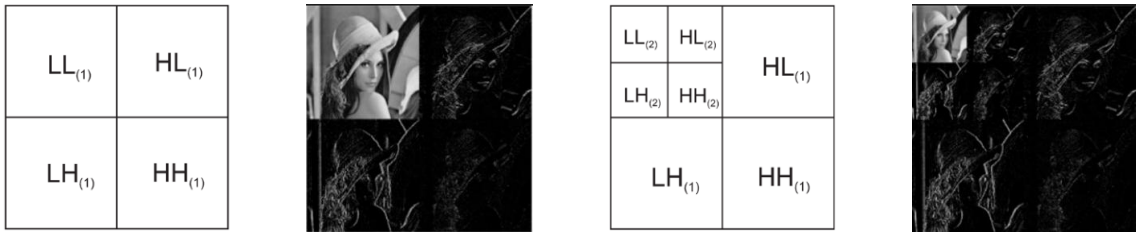
This algorithm is a powerful tool in the field of image watermarking, allowing for multi-resolution analysis through decomposition of an image into its individual frequency subbands [20]. In cases when a noised watermark is inserted in a host picture, DWT helps in attaining both perceptibility and robustness through insertion of the watermark in individual frequency bands in contrast to insertion in the spatial domain [21]. First, the host picture must be decomposed into four subbands: LL (approximation), LH (horizontal detail), HL (vertical detail), and HH (diagonal detail). Next, a pre-processed watermark, with additional added noise (e.g., Gaussian or salt-pepper noise), must be inserted into upper frequency subbands (LH, HL, HH) in a manner that its robustness is not compromised in general attacks such as filtering, shape transformation, and compression [22], [23]. Lastly, an inverse DWT (IDWT) is performed to produce a watermarked picture in which the concealed watermark cannot be detected but its robustness is preserved with regard to distortions. The decomposition of this algorithm can be seen in equation (5).

$$\begin{aligned} LL &= \sum\sum I\,(x,y)\phi\,(x)\phi\,(y) \\ LH &= \sum\sum I\,(x,y)\phi\,(x)\phi\,(y) \\ HL &= \sum\sum I\,(x,y)\phi\,(x)\phi\,(y) \\ HH &= \sum\sum I\,(x,y)\phi\,(x)\phi\,(y) \end{aligned} \tag{5}$$

Where, $I(x,y)$ represents the pixel intensity at coordinate (x,y), and $\phi(x)$ and $\psi(x)$ denote the scaling and wavelet functions, respectively. And to reconstruct the image after embedding the watermark, the Inverse DWT (IDWT) is applied by equation (6).

$$I\,(x,y) = LL \cdot \phi\,(x)\phi\,(y) + LH \cdot \phi\,(x)\phi\,(y) + HL \cdot \phi\,(x)\phi\,(y) + HH \cdot \phi\,(x)\phi\,(y) \tag{6}$$

This ensures that the noised watermark is seamlessly integrated while preserving image quality and robustness. The results of DWT processing each level can be seen in Figure 3.



(a) DWT level 1 (b)DWT level 2

Figure 3. DWT processing each level

2.4. PSNR and SSIM Assessment

Peak Signal to Noise Ratio (PSNR) and the Structural Similarity Index Measure (SSIM) have become universally acknowledged approaches for estimating watermarked image quality in terms of perceptibility and structural integrity [24], [25]. PSNR compares present distortion between a watermarked and its source counterpart through a calculation of the proportion between the value at its peak and added error. High PSNR values denote high-quality images with less distortion [26]. SSIM, on the other hand, compares perceptual image similarity through examination of factors such as luminance, contrast, and structure. Higher SSIM values, tending towards 1, denote a high level of maintenance of structural information [26]. These assessments are measured using respective calculations as shown in equation (7) for PSNR and equation (8) for SSIM.

Vol. 6, No. 2, April 2025, Page. 1017-1028
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.2.4423

$$PSNR = 10 \cdot Log_{10}\left(\frac{Max^2}{MSE}\right) \quad (7)$$

$$SSIM\ (x,y) = \frac{(\mu x2+\mu y2+c1)(\sigma x2+\sigma y2+c2)}{(2\mu x\mu y+c1)(2\sigma xy+c2)} \quad (8)$$

Both PSNR and SSIM play a crucial role in assessing the balance between watermark invisibility and robustness, ensuring that the watermark does not significantly degrade the image quality while remaining detectable under various attacks.

3. PROPOSED SCHEME

This chapter discusses the watermarking process, which consists of embedding and extraction stages. Section 3.1 Embedding Process explains how the pre-noised watermark is embedded into the host image using Discrete Wavelet Transform (DWT) and DAISY descriptor to ensure imperceptibility and robustness. Section 3.2 Extraction Process describes the retrieval of the watermark by reversing the embedding steps while preserving its integrity against attacks.

3.1. Embedding Process

Based on Figure 4, the diagram illustrates the process of embedding a watermark into an image using the DWT technique. The process begins with the host image undergoing DWT processing, which decomposes the image into sub-bands (LL, LH, HL, HH). Meanwhile, the watermark image is subjected to noise addition, such as Gaussian or salt-and-pepper noise, to generate a noised watermark image. This noisy watermark is then processed using the DAISY Feature Descriptor to extract local feature descriptors, D(x,y). These extracted features are embedded into the selected sub-band (typically LL or HL) of the host image through the DWT process. Finally, an Inverse DWT (IDWT) is applied to reconstruct the watermarked image, ensuring the watermark remains imperceptible to the human eye while preserving the image quality.

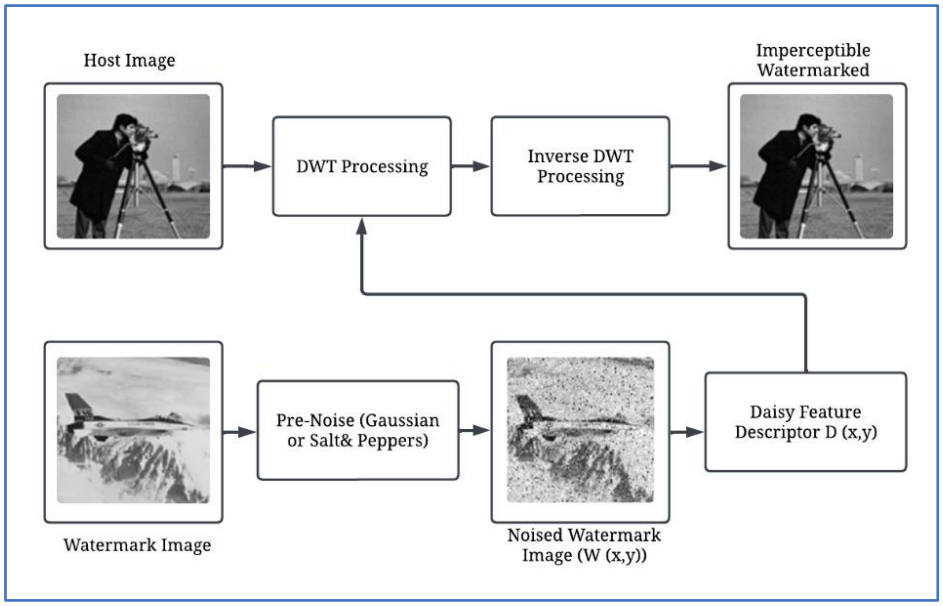


Figure 4. Proposed Embedding Process

3.2. Extracting Process

Based on Figure 5, the extraction process is the reverse of the embedding process. It begins with the watermarked image, which is first subjected to an IDWT to reconstruct the sub-bands. Next, the feature descriptors embedded using the DAISY descriptor are extracted from the relevant sub-bands,

Vol. 6, No. 2, April 2025, Page. 1017-1028
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.2.4423

typically the LL or HL sub-bands. These descriptors, D(x,y), are then processed to recover the noisy watermark. Finally, the extracted watermark is compared to the original one, ensuring that the watermark has been successfully retrieved while maintaining its integrity and robustness against various attacks.

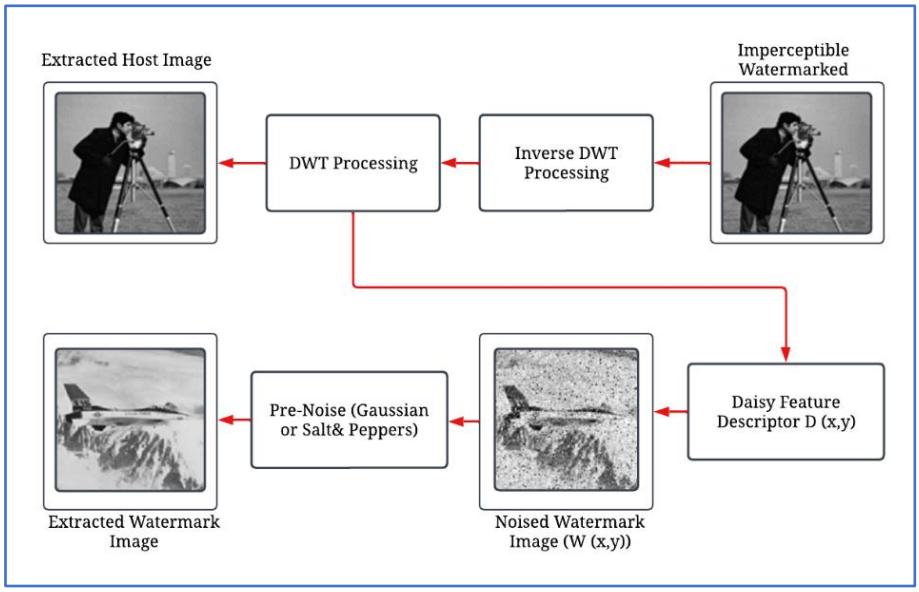


Figure 5. Proposed Extracting Process

4. RESULTS

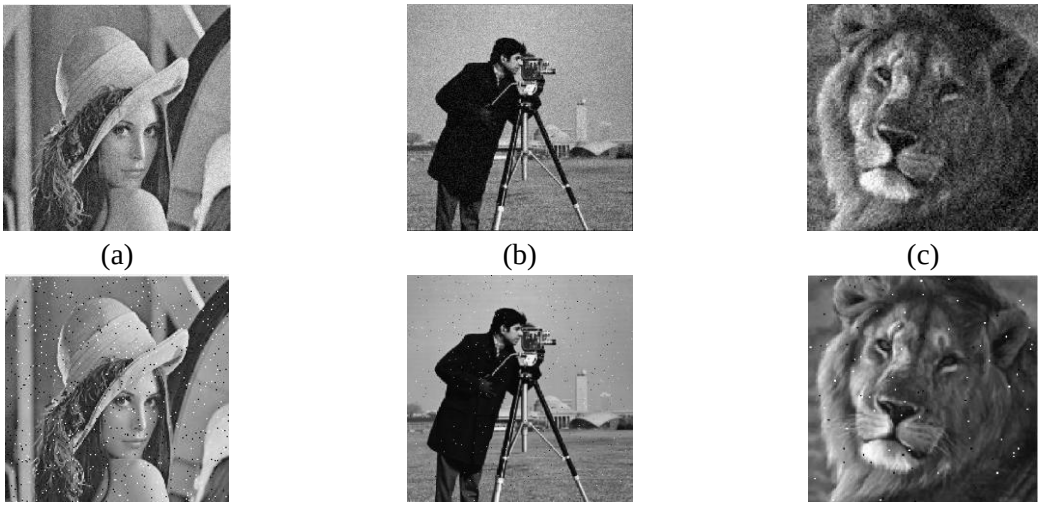
In this section, researcher introduce the performance of the proposed scheme for watermarking, together with an in-depth analysis of its efficiency. In testing, three sample images were incorporated, and these were then subsequently used as watermarks according to the embedding scheme. Lena, Cameraman, and Lion images, each in a resolution of 512 x 512 and in grayscale, were used. All three images underwent processing via the embedding scheme discussed in the preceding chapter, and performance of watermarked images was evaluated in terms of perceptibility, robustness, and extracted watermark quality. Proposed sample image host and watermark can be seen in Figure 6.

(a) Lena.jpg (b) Cameraman.jpg (c) Lion.jpg

Figure 6. Sample Host And Watermark Image

After initializing Figure 6, the next step involves embedding noise into the watermark images, followed by hiding the noised watermark using the DAISY descriptor, as shown in Figure 7. This process ensures that the watermark remains imperceptible while being securely embedded into the host image. The resulting images demonstrate the effectiveness of the embedding process and provide a basis for evaluating the quality and robustness of the watermarked images.

Vol. 6, No. 2, April 2025, Page. 1017-1028
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.2.4423

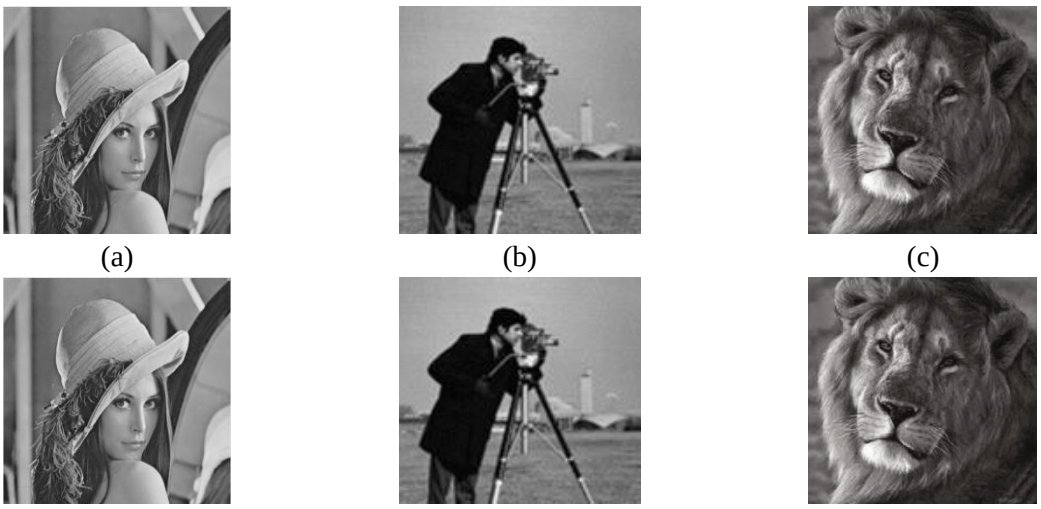


(a) (b) (c)

(d) (e) (f)

Figure 7. Pre-Processed Watermark Image. (A) – (C) Represents Gaussian Noise, (D) – (F) Represents Salt&Peppers Noise

The next step involves embedding the watermarked image, which has been subjected to noise addition and feature embedding using the DAISY descriptor, into the host image. This embedding process is carried out using the DWT technique, as shown in Figure 8. The result is a watermarked host image where the watermark remains imperceptible, ensuring both high-quality preservation of the host image and robust watermark embedding.



(a) (b) (c)

(d) (e) (f)

Figure 8. Embedded Watermark Image To Host Image. (A) – (C) Represents Gaussian Noise Attack, (D) – (F) Represents Salt&Peppers Noise Attack

The watermarked images, which have been embedded with added noise and hidden using the DAISY descriptor, were subjected to a performance evaluation to assess their imperceptibility and robustness. This evaluation is carried out using performance metrics such as PSNR and SSIM, which measure the quality of the watermarked images and their perceptual similarity to the original host images.

Vol. 6, No. 2, April 2025, Page. 1017-1028
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.2.4423

The results of this evaluation, which are displayed in Table 1 to table 3, provide a quantitative analysis of the effectiveness of the proposed watermarking method under different noise attacks, highlighting its robustness and the ability to maintain image quality.

Table 1. Comparison results by related study (No Attack)

Study by	Novelty	Watermarked	PSNR Results	SSIM Results
[10]	DWT-SVD	Lena	47.93 dB	0.9998
		Cameraman	N/A	N/A
		Lion	52.70 dB	0.9999
Our	DWT-Daisy Descriptor	Lena	63.71 dB	1
		Cameraman	68.33 dB	1
		Lion	66.89 dB	1

Table 2. Comparison results by related study (Gaussian Attack)

Study by	Novelty	Watermarked	PSNR Results	SSIM Results
[10]	DWT-SVD	Lena	29.92 dB	0.6940
		Cameraman	N/A	N/A
		Lion	29.95 dB	0.7053
Our	DWT-Daisy Descriptor	Lena	48.55 dB	0.9999
		Cameraman	50.11 dB	0.9999
		Lion	49.92 dB	0.9999

Table 3. Comparison results by related study (Salt&Peppers Attack)

Study by	Novelty	Watermarked	PSNR Results	SSIM Results
[10]	DWT-SVD	Lena	35.31 dB	0.9736
		Cameraman	N/A	N/A
		Lion	35.45 dB	0.9739
Our	DWT-Daisy Descriptor	Lena	52.69 dB	0.9999
		Cameraman	55.70 dB	0.9999
		Lion	53.62 dB	0.9999

5. DISCUSSIONS

The results shown in Table 1, which compare the performance of the proposed DWT-Daisy Descriptor watermarking method to that of the DWT-SVD method from related studies [10], demonstrate a significant improvement in both PSNR and SSIM for watermarked images with no attack applied. For all tested images (Lena, Cameraman, and Lion), the DWT-Daisy Descriptor method produced superior PSNR values, with scores reaching up to 68.33 dB for the Cameraman image and SSIM values of 1, indicating nearly perfect perceptual similarity to the original host images. These results highlight the effectiveness of the proposed approach in embedding watermarks that are both imperceptible and robust, as evidenced by the high PSNR and SSIM scores.

In Tables 2 and 3, the results under Gaussian and Salt-and-Pepper noise attacks further illustrate the robustness of the DWT-Daisy Descriptor method. For Gaussian noise, the PSNR values for the watermarked images remain significantly higher compared to the DWT-SVD method, with the Lena image showing a PSNR of 48.55 dB and SSIM of 0.9999, indicating minimal quality degradation even under such attacks. Similarly, under Salt-and-Pepper noise, the DWT-Daisy Descriptor method again outperforms the DWT-SVD method, with the Lena image achieving a PSNR of 52.69 dB and an SSIM of 0.9999. These results confirm that the proposed watermarking method maintains high robustness against various types of noise attacks, ensuring both the integrity and security of the watermarked images.

6. CONCLUSION

This study introduces a new scheme for digital image watermarking utilizing the Discrete Wavelet Transform (DWT) and Daisy Descriptor for enhancing security and robustness in watermarks. In its testing, three test images, Lena, Cameraman, and Lion, with a resolution of 512 x 512 pixels in grayscale, were utilized for evaluation in its scheme. In experimental testing, a high improvement in Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Metric (SSIM) for watermarked images was attained. For Lena, for example, PSNR attained 63.71 dB with an SSIM value of 1; for Cameraman, PSNR attained 68.33 dB with an SSIM value of 1; and for Lion, PSNR reached 66.89 dB with an SSIM value of 1, all of which represent high invisibility and high maintenance of quality in all cases. In its scheme, DWT-Daisy Descriptor showed high robustness under both Gaussian and Salt-and-Pepper attack cases. In cases of Gaussian attack, PSNR values for Lena, Cameraman, and Lion attained 48.55, 50.11, and 49.92, respectively, with SSIM values in all cases being near 1. In case of Salt-and-Pepper attack, PSNR values attained 52.69 for Lena, 55.70 for Cameraman, and 53.62 for Lion, with SSIM values in all cases approximating 1. Remarkably, Cameraman performed best in all cases of attack, with high PSNR and SSIM values, and therefore proving effective in terms of integrity and security of proposed watermarked images in its scheme.

ACKNOWLEDGEMENT

The authors sincerely appreciate the financial support provided by Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) Universitas Dian Nuswantoro (UDINUS) through the Internal Research Scheme within Grant Number 005/A.38-04/UDN-09/I/2025.

REFERENCES

[1] E. A. Sofyan, C. A. Sari, H. Rachmawanto, and R. D. Cahyo, "High-Quality Evaluation for Invisible Watermarking Based on Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD)," Advance Sustainable Science, Engineering and Technology (ASSET), vol. 6, no. 1, 2024, doi: 10.26877/asset.v6i1.17186.

[2] W. Alomoush et al., "Digital image watermarking using discrete cosine transformation based linear modulation," Journal of Cloud Computing, vol. 12, no. 1, Dec. 2023, doi: 10.1186/s13677-023-00468-w.

[3] N. R. D. Cahyo and M. M. I. Al-Ghiffary, "An Image Processing Study: Image Enhancement, Image Segmentation, and Image Classification using Milkfish Freshness Images," IJECAR) International Journal of Engineering Computing Advanced Research, vol. 1, no. 1, pp. 11–22, 2024.

[4] P. Aberna and L. Agilandeeswari, "Digital image and video watermarking: methodologies, attacks, applications, and future directions," Multimed Tools Appl, vol. 83, no. 2, pp. 5531–5591, Jan. 2024, doi: 10.1007/s11042-023-15806-y.

[5] A. K. Sahu et al., "A Study on Content Tampering in Multimedia Watermarking," SN Comput. Sci., vol. 4, no. 3, Feb. 2023, doi: 10.1007/s42979-022-01657-1.

[6] S. M. Darwish and L. D. S. Al-Khafaji, "Dual Watermarking for Color Images: A New Image Copyright Protection Model based on the Fusion of Successive and Segmented Watermarking," Multimed Tools Appl, vol. 79, no. 9–10, pp. 6503–6530, Mar. 2020, doi: 10.1007/s11042-019-08290-w.

[7] S. Gupta, K. Saluja, V. Solanki, K. Kaur, P. Singla, and M. Shahid, "Efficient methods for digital image watermarking and information embedding," Measurement: Sensors, vol. 24, p. 100520, Dec. 2022, doi: 10.1016/j.measen.2022.100520.

[8] E. Kartikadarma, E. D. Udayanti, C. A. Sari, and M. Doheir, "A Comparison of Non Blind Image Watermarking Using Transformation Domain," Scientific Journal of Informatics, vol. 8, no. 1, 2021, doi: 10.15294/sji.v8i1.28334.

[9] J. Khandelwal, V. K. Sharma, D. Singh, and A. Zaguia, "Dwt-svd based image steganography

using threshold value encryption method," Computers, Materials and Continua, vol. 72, no. 2, pp. 3299–3312, 2022, doi: 10.32604/cmc.2022.023116.

[10] A. Alzahrani, "Enhanced invisibility and robustness of digital image watermarking based on DWT-SVD," Appl Bionics Biomech, vol. 2022, 2022.

[11] F. Yasmeen and M. S. Uddin, "An Efficient Watermarking Approach Based on LL and HH Edges of DWT–SVD," SN Comput Sci, vol. 2, no. 2, pp. 1–16, Apr. 2021, doi: 10.1007/s42979-021-00478-y.

[12] C. A. Sari et al., "A Chaotic Image Encryption Based on Random Noise and Arnold Cat Maps," in 2024 International Seminar on Application for Technology of Information and Communication (iSemantic), IEEE, Sep. 2024, pp. 347–352. doi: 10.1109/iSemantic63362.2024.10762216.

[13] Y. Yuan, J. Li, U. A. Bhatti, M. Yang, and Q. Zhang, "Robust Color Images Zero-Watermarking Algorithm Based on Stationary Wavelet Transform and Daisy Descriptor," in Deep Learning for Multimedia Processing Applications, CRC Press, 2024, pp. 60–73.

[14] N. S. Awarayi, O. Appiah, B. A. Weyori, and C. B. Ninfaakang, "A Digital Image Watermarking Using Dwt and L-shaped Tromino Fractal Encryption," International Journal of Image, Graphics and Signal Processing, vol. 13, no. 3, pp. 33–43, Jun. 2021, doi: 10.5815/ijigsp.2021.03.03.

[15] A. Kumar, "A Review on Implementation of Digital Image Watermarking Techniques Using LSB and DWT," in ss, 2020, pp. 595–602. doi: 10.1007/978-981-13-7166-0_59.

[16] T. Badings et al., "Robust Control for Dynamical Systems with Non-Gaussian Noise via Formal Abstractions," Journal of Artificial Intelligence Research, vol. 76, pp. 341–391, Jan. 2023, doi: 10.1613/jair.1.14253.

[17] H. Zaini and Z. Alqadi, "High Salt and Pepper Noise Ratio Reduction," International Journal of Computer Science and Mobile Computing, vol. 10, no. 9, pp. 88–97, Sep. 2021, doi: 10.47760/ijcsmc.2021.v10i09.009.

[18] J. Ebrahimnejad and A. Naghsh, "Adaptive Removal of high-density salt-and-pepper noise (ARSPN) for robust ROI detection used in watermarking of MRI images of the brain," Comput Biol Med, vol. 137, p. 104831, Oct. 2021, doi: 10.1016/j.compbiomed.2021.104831.

[19] Y. Yuan, J. Li, U. A. Bhatti, M. Yang, and Q. Zhang, "Robust Color Images Zero-Watermarking Algorithm Based on Stationary Wavelet Transform and Daisy Descriptor," in Deep Learning for Multimedia Processing Applications, CRC Press, 2024, pp. 60–73.

[20] S. S. Rao, G. K. Narula, R. Sudhir, S. S, R. B, and B. B, "Video Codec IP using Discrete Wavelet Transform," in 2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), IEEE, Oct. 2021, pp. 1–7. doi: 10.1109/SMARTGENCON51891.2021.9645895.

[21] P. N. Andono and C. A. Sari, "Remove Blur Image Using Bi-Directional Akamatsu Transform and Discrete Wavelet Transform," Scientific Journal of Informatics, vol. 9, no. 2, pp. 179–188, Nov. 2022, doi: 10.15294/sji.v9i2.34173.

[22] W. W. Hu, R. G. Zhou, J. Luo, S. X. Jiang, and G. F. Luo, "Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms," Quantum Inf Process, vol. 19, no. 3, Mar. 2020, doi: 10.1007/s11128-020-2579-9.

[23] S. Pramanik, "An adaptive image steganography approach depending on integer wavelet transform and genetic algorithm," Multimed Tools Appl, vol. 82, no. 22, pp. 34287–34319, Sep. 2023, doi: 10.1007/s11042-023-14505-y.

[24] C. A. Sari, M. H. Dzaki, E. H. Rachmawanto, R. R. Ali, and M. Doheir, "High PSNR Using Fibonacci Sequences in Classical Cryptography and Steganography Using LSB," International Journal of Intelligent Engineering and Systems, vol. 16, no. 4, pp. 568–580, 2023, doi: 10.22266/ijies2023.0831.46.

[25] E. R. Pramudya et al., "Optimation of image encryption using fractal Tromino and polynomial Chebyshev based on chaotic matrix," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 22, no. 6, p. 1529, Aug. 2024, doi: 10.12928/telkomnika.v22i6.26080.

[26] U. Sara, M. Akter, and M. S. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," Journal of Computer and Communications, vol. 07, no. 03,

Vol. 6, No. 2, April 2025, Page. 1017-1028
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.2.4423

pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.