Available online at website: https://jurnal.iaii.or.id/index.php/RESTI

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 9 No. 6 (2025) 1451 - 1462 e-ISSN: 2580-0760

Securing NFT Copyright with Robust DWT-Hessenberg-SVD Watermarking and RSA Signatures

Muhammad Romadhona Kusuma[1], Efri Syamsul Bahri[2]
[1]Doctoral Program in Informatics, Universitas Nusa Mandiri, Depok, Indonesia
[2]Asia e University, Selangor, Malaysia

[1]m.romadhona.kusuma@gmail.com, [2]efrisb@gmail.com

Abstract

In the digital era, protecting visual content from misuse and forgery is essential. This study proposes a robust image watermarking method by integrating Discrete Wavelet Transform (DWT), Hessenberg Decomposition (HD), and Singular Value Decomposition (SVD), aiming to enhance watermark imperceptibility and resilience against common image attacks. Additionally, the system incorporates RSA digital signatures within the watermark metadata to ensure verifiable authenticity in NFT (Non-Fungible Token) applications. The method was implemented using Python and tested on multiple grayscale images across various attack scenarios, including noise addition and compression. Experimental results demonstrate high SSIM and PSNR values, confirming the method's effectiveness in maintaining both visual fidelity and embedded watermark integrity. These findings support the potential of this approach for secure and scalable NFT copyright protection.

Keywords: DWT-Hessenberg-SVD; Image Watermarking; NFT Copyright Protection; RSA Digital Signature; Robustness

How to Cite: M. R. Kusuma and E. S. Bahri, "Securing NFT Copyright with Robust DWT-Hessenberg-SVD Watermarking and RSA Signatures", *J. RESTI (Rekayasa Sist. Teknol. Inf.)* , vol. 9, no. 6, pp. 1451 - 1462, Jan. 2026.
Permalink/DOI: https://doi.org/10.29207/resti.v9i6.6747

Received: June 9, 2025
Accepted: December 16, 2025
Available Online: January 11, 2026

This is an open-access article under the CC BY 4.0 License
Published by Ikatan Ahli Informatika Indonesia

1. Introduction

In today's digital era, the circulation and distribution of digital content have increased rapidly, bringing significant benefits in terms of accessibility and dissemination while simultaneously raising serious concerns related to copyright infringement, unauthorized duplication, and content manipulation [1]. As digital images become core assets in creative industries, scientific communication, and blockchain-based ecosystems, ensuring their integrity, authenticity, and ownership protection has become an increasingly critical challenge.

One widely adopted approach to address these issues is digital watermarking, which embeds imperceptible information such as logos, signatures, or authentication codes into digital images [2]. The primary objectives of watermarking include authenticity verification, traceability, and protection against illegal copying or tampering [3], [4]. To be effective, watermarking techniques must balance two often conflicting requirements: robustness against various signal processing attacks and preservation of high visual quality in the host image [5].

To enhance robustness, numerous studies have explored transform-domain watermarking techniques. Among them, the Discrete Wavelet Transform (DWT) has been extensively utilized due to its ability to represent both spatial and frequency information effectively [6]. However, DWT-based watermarking schemes remain vulnerable to common attacks such as compression, filtering, and geometric manipulation, which may degrade or destroy the embedded watermark [7], [8]. These limitations have motivated researchers to integrate DWT with additional mathematical decompositions to improve resistance while maintaining imperceptibility.

Singular Value Decomposition (SVD) has emerged as a widely used technique due to its numerical stability and resistance to minor perturbations. Several studies have demonstrated that combining DWT and SVD significantly improves watermark invisibility and robustness against common image processing attacks. Narima Zermi et al. [9] and Gaur et al. [10] confirmed strong imperceptibility and robustness using DWT–SVD integration, while Sourabh Sharma et al. [11] further enhanced robustness in color images by

applying RDWT–SVD combined with Artificial Bee Colony optimization.

Beyond conventional DWT–SVD schemes, various hybrid and adaptive watermarking strategies have been proposed. Junxiu Liu et al. [12] introduced a hybrid watermarking method that balances robustness and invisibility, while Zhenyu Li et al. [13] developed an algorithm resilient to rotation and other geometric attacks. Application-specific approaches were explored by Reem A. et al. [14] for Arabic text images and by Asha Durafe et al. [15], who emphasized minimal image degradation even with large secret image sizes. Additionally, Hwai-Tsu Hu et al. [16] presented a scheme with strong resistance to signal processing attacks and high payload capacity, and Wafa' Hamdan et al. [17] combined DWT and SVD with chaos-based embedding to enhance resilience.

Further advancements have shown that extending SVD-based watermarking to multi-transform hybrid domains can improve robustness and imperceptibility. Lingzhuang Meng et al. [18] proposed adaptive embedding strategies to improve visual quality, while E. Najafi et al. [19] and S. Arunkumar et al. [20] demonstrated that combining SVD with other transforms enhances security in image transmission. Beyond image watermarking, Hwai-Tsu Hu et al. [21] validated DWT-based watermarking in the audio domain, and Liya Zhu et al. [22] introduced block compressive sensing combined with SVD for effective image encryption. More recently, hybrid schemes integrating Integer Wavelet Transform (IWT), Discrete Cosine Transform (DCT), and SVD with multi-block embedding strategies have demonstrated strong resistance to common signal processing and geometric attacks while maintaining high visual quality, as measured by PSNR and SSIM [23].

More recent developments have incorporated Hessenberg Decomposition (HD) into DWT–SVD frameworks to further enhance robustness and transparency. Junxiu Liu et al. [24] demonstrated that integrating HD and SVD within the DWT domain improves resistance to various attacks while preserving perceptual quality. Complementary studies confirm that robust watermarking based on DWT, Hessenberg decomposition, and SVD can effectively protect visual content from misuse, unauthorized copying, and forgery in increasingly complex digital environments [25].

Alongside these technical advancements, the emergence of Non-Fungible Tokens (NFTs) has introduced a blockchain-based paradigm for certifying ownership and provenance of digital assets through immutable metadata and cryptographic signatures. However, NFTs alone do not provide intrinsic visual protection, allowing associated media to be copied or redistributed independently of the token [26]. This limitation highlights the need to embed ownership information directly into visual content through watermarking mechanisms that are complemented by cryptographic authentication.

Motivated by the above challenges and research gaps, the objectives of this study are to analyze the strengths and limitations of existing digital watermarking techniques to identify recent advancements and unresolved issues, to propose and evaluate a novel hybrid watermarking framework based on the integration of Discrete Wavelet Transform (DWT), Hessenberg Decomposition (HD), and Singular Value Decomposition (SVD) with improved robustness and visual quality, and to incorporate RSA-based cryptographic signature generation into the watermark metadata to support reliable NFT-oriented copyright protection.

2. Methods

This study was implemented using Python and conducted on grayscale digital images, with watermark inputs primarily in JPEG format and additional support for PNG and BMP formats. The proposed approach embeds watermark metadata within the Discrete Wavelet Transform (DWT) domain by integrating Hessenberg Decomposition (HD) and Singular Value Decomposition (SVD) to enhance robustness and imperceptibility. Furthermore, RSA-based digital signature generation is incorporated into the watermark metadata to provide cryptographic authentication and verifiable ownership, particularly in NFT-oriented copyright protection environments.

2.1 Digital Image

In the proposed watermarking framework, digital images are treated as structured pixel-based data in which each pixel carries numerical values representing brightness or color intensity. Such images can be acquired through devices such as digital cameras or scanners and further processed using digital image processing techniques, including filtering, enhancement, segmentation, and merging, to improve visual quality, extract features, or embed hidden information [27].

Within the context of digital watermarking, digital images function as the host medium for imperceptible embedding of authentication data, such as logos, signatures, or cryptographic identifiers, through controlled pixel or transform-domain modifications to ensure authenticity, traceability, and copyright protection [28]. This pixel-based representation enables systematic transform-domain decomposition, which is essential for applying the proposed DWT–HD–SVD watermarking method while preserving visual fidelity and maintaining robustness against common image manipulations.

2.2 Discrete Integer Wavelet Transform (DWT)

The Discrete Wavelet Transform (DWT) is employed in this study as a transform-domain technique that analyzes image signals in both spatial and frequency

domains by decomposing an image into four sub-bands, namely LL, LH, HL, and HH. The LL sub-band represents coarse image information, whereas the remaining sub-bands capture directional and high-frequency details. In digital watermarking applications, embedding is commonly performed in selected sub-bands, particularly LL or HL, to achieve an effective balance between robustness and imperceptibility. Unlike the Integer Wavelet Transform (IWT), DWT operates in the real-number domain, which may introduce minor rounding errors but offers greater flexibility for robust watermark embedding under common signal processing attacks [29].

Within the proposed framework, DWT functions as the initial decomposition stage that enables stable integration with Hessenberg Decomposition (HD) and Singular Value Decomposition (SVD), followed by image reconstruction through inverse DWT, as illustrated in Figure 1.

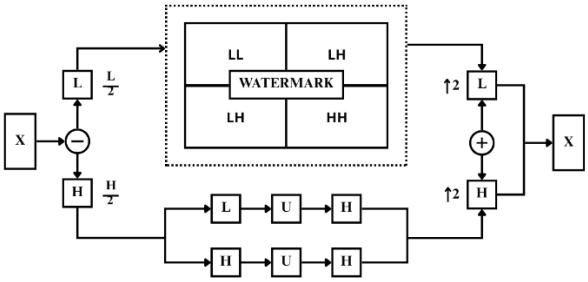


Figure 1. Discrete Wavelet Transform

2.3 Hessenberg Decomposition (HD)

Hessenberg Decomposition (HD) is applied in this study as a matrix transformation technique that converts a square matrix into an upper Hessenberg form, in which all elements below the second sub-diagonal are zero, thereby simplifying matrix structure while preserving essential information [30]. This transformation facilitates more efficient and numerically stable computations, particularly in operations such as matrix multiplication and eigenvalue analysis, which are critical in transform-domain watermarking.

Within the proposed framework, the image matrix Aobtained from the DWT sub-band is decomposed as $A = QHQ^T$, where $Q$is an orthogonal matrix and $H$is an upper Hessenberg matrix. The watermark embedding process is performed by modifying the Hessenberg matrix as $H' = H + \alpha W$, where Wrepresents the watermark and αcontrols the embedding strength. The watermarked image is then reconstructed as $A' = QH'Q^T$, enabling robust watermark insertion while maintaining visual quality. This role of HD as an intermediate decomposition stage enhances numerical stability and supports seamless integration with Singular Value Decomposition (SVD), as illustrated in Figure 2.

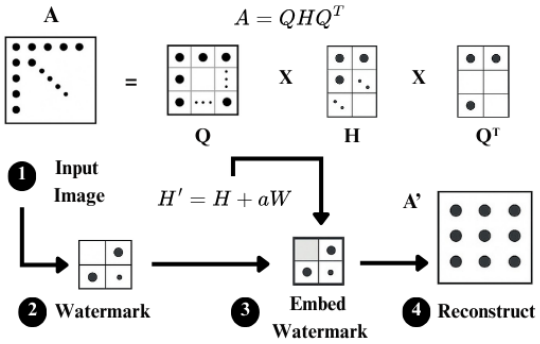


Figure 2. Watermark Embedding Process Using Hessenberg Decomposition

2.4 Singular Value Decomposition (SVD)

Singular Value Decomposition (SVD) is employed in this study as a matrix factorization technique that decomposes an image matrix into three components, namely an orthogonal matrix representing the left singular vectors, a diagonal matrix containing non-negative singular values in descending order, and an orthogonal matrix representing the transposed right singular vectors [31], [32]. In image processing and digital watermarking, SVD is particularly advantageous due to the stability of its singular values, where small perturbations in the image result in minimal variation, thereby enabling watermark embedding without significant degradation of visual quality [33]. Within the proposed framework, an image matrix $A$is decomposed as $A = U\Sigma V^T$, where $U$and V^Tdescribe the structural characteristics of the image and Σcontains singular values corresponding to the energy distribution of each component. Watermark embedding is performed by modifying selected singular values, after which the image is reconstructed using inverse SVD to preserve visual fidelity while maintaining robustness against common signal processing attacks. The overall decomposition and reconstruction process using SVD is illustrated in Figure 3.

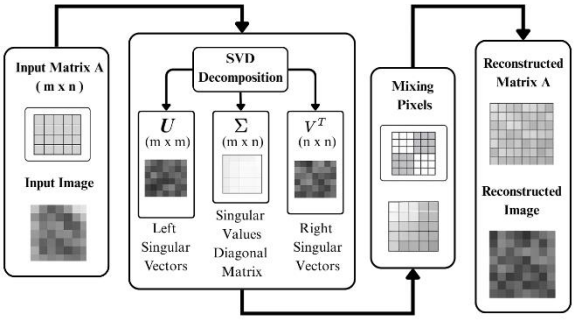


Figure 3. Step-by-Step Illustration of Image Decomposition and Reconstruction Using SVD

2.5 Watermark

Digital watermarking refers to the process of embedding imperceptible information, known as a watermark, into a digital signal or image to support purposes such as authentication, copyright protection, ownership identification, and content tracking [34], [35]. In image watermarking, the embedded watermark

is designed to remain visually invisible while being robust against common signal processing operations and intentional attacks.

Within the proposed framework, the watermark functions as protected metadata that is embedded in the transform domain using a hybrid DWT–HD–SVD approach, enabling a balance between imperceptibility and robustness. By integrating the watermark into selected transform coefficients rather than directly modifying pixel values, the proposed method enhances resistance to image manipulation while preserving visual quality, which is essential for reliable copyright protection in NFT-oriented environments.

2.6 Image Quality and Robustness Evaluation

Imperceptibility in digital watermarking refers to the ability of a watermarking method to preserve the original visual quality of an image after watermark embedding, such that the presence of the watermark is imperceptible to the human visual system [36]. In this study, imperceptibility and image quality are quantitatively evaluated using Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index Metric (SSIM), which are widely adopted evaluation metrics in digital image watermarking [37], [38]. Among these metrics, MSE measures the average squared difference between the original image $o$and the watermarked image w, and it is mathematically defined in Equation 1.

$$\mathrm{MSE}(o,w) = \frac{1}{W \times H} \sum_{x=1}^{W} \sum_{y=1}^{H} (o_{xy} - w_{xy})^2 \quad (1)$$

$o_{xy}$and w_{xy}denote the pixel intensity values of the original and watermarked images at position (x, y), respectively, and $W \times H$represents the image dimensions. Based on the obtained MSE value, the Peak Signal-to-Noise Ratio (PSNR) is then calculated to evaluate the level of distortion introduced by the watermarking process. PSNR is defined in Equation 2.

$$\mathrm{PSNR}(o,w) = 10\log_{10}\left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}(o,w)}\right) \quad (2)$$

MAX denotes the maximum possible pixel intensity value (e.g., 255 for 8-bit grayscale images). Higher PSNR values indicate lower distortion and better imperceptibility of the embedded watermark.

In addition to pixel-based distortion metrics, perceptual image quality is further evaluated using the Structural Similarity Index Metric (SSIM), which assesses luminance, contrast, and structural similarity between the original and watermarked images [38]. SSIM is defined in Equation 3.

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (3)$$

$\mu_x$and $\mu_y$represent the mean intensities, $\sigma_x^2$and σ_y^2denote the variances, $\sigma_{xy}$is the covariance between the two images, and $C_1$and $C_2$are constants used to stabilize the division. SSIM values range from 0 to 1, with values closer to 1 indicating higher structural similarity.

Furthermore, the robustness of the proposed watermarking method is evaluated by subjecting the watermarked images to various common image processing attacks, including filtering, noise addition, and compression. The ability of the embedded watermark to remain detectable under such distortions reflects the robustness of the proposed DWT–HD–SVD watermarking framework, which is quantitatively assessed using PSNR and SSIM metrics under post-attack conditions [39], [40].

2.7 Integration of RSA Digital Signatures into Watermarking Metadata

To ensure authenticity, integrity, and verifiability of the embedded watermark, RSA digital signatures are integrated into the proposed watermarking framework as part of NFT-oriented metadata creation. As illustrated in Figure 4, the process begins with watermark preprocessing, in which the watermark image is converted to grayscale to ensure consistency prior to hashing and embedding. The watermark is then embedded into the host image using the proposed DWT–HD–SVD framework by modifying selected singular values, followed by image reconstruction through inverse transformations. Subsequently, a SHA-256 hash of the watermark is generated and incorporated into structured JSON metadata together with essential attributes such as creator identification, timestamp, and copyright information. The metadata is digitally signed using the creator's private RSA key to ensure data integrity and authenticity, while the corresponding public key enables third-party verification, allowing any unauthorized modification to be reliably detected. This integration effectively combines robust transform-domain watermarking with cryptographic assurance to support secure and verifiable protection of digital assets in NFT ecosystems

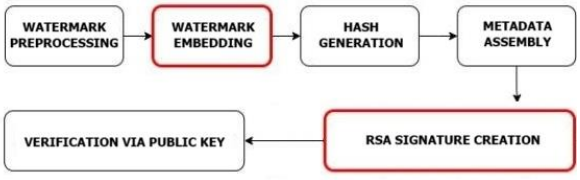


Figure 4. Proposed Integration of RSA Digital Signatures into Watermarking Metadata Procedure

3. Results and Discussions

3.1 Watermark Implantation Procedure

The watermark implantation procedure represents a key stage in protecting copyright and verifying the authenticity of digital content through the embedding of watermark information into a host image. The overall workflow of the proposed implantation process is illustrated in Figure 5.

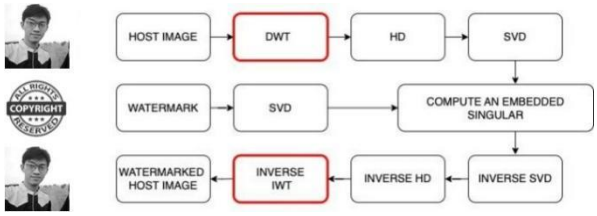


Figure 5. Proposed Watermark Embedding Procedure

As shown in Figure 5, the process begins with the preparation of the host image, which serves as the primary medium for watermark insertion, along with the definition of the watermark content such as a logo, text, or digital signature. The host image is subsequently transformed using the Discrete Wavelet Transform (DWT) to decompose it into multiple frequency sub-bands, enabling selective and robust embedding. Hessenberg Decomposition (HD) is then applied to simplify the matrix structure and enhance numerical stability, followed by Singular Value Decomposition (SVD), where the watermark information is embedded by modifying selected singular values to minimize visual distortion. After the embedding stage, the image is reconstructed through inverse SVD and inverse DWT operations, producing a watermarked image that remains visually similar to the original. During the verification phase, the same sequence of transformations is applied to accurately extract and validate the embedded watermark, demonstrating the effectiveness and reliability of the proposed watermarking framework.

3.2 Watermark Extraction Procedure

The watermark extraction procedure represents the process of retrieving the embedded watermark from the watermarked image to verify authenticity and ownership, as illustrated in Figure 6.

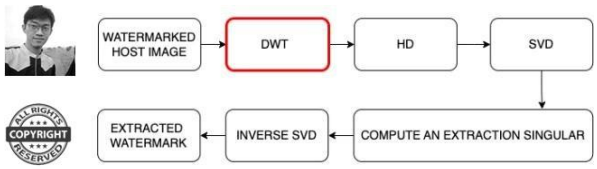


Figure 6. Proposed Watermark Extraction Procedure

As shown in Figure 6, the extraction process begins with the watermarked host image, which serves as the input for watermark recovery. The image is first transformed using the Discrete Wavelet Transform (DWT) to decompose it into multiple frequency sub-bands, enabling multi-resolution analysis consistent with the embedding stage. Hessenberg Decomposition (HD) is then applied to simplify the matrix structure and enhance numerical stability, followed by Singular Value Decomposition (SVD) to isolate the singular values that contain the embedded watermark information. The relevant singular components are subsequently extracted, and inverse SVD is applied to reconstruct the corresponding matrix representation. Finally, the watermark is recovered from the reconstructed singular matrix, completing the extraction process using the integrated DWT–HD–SVD framework. This procedure ensures accurate and reliable watermark retrieval while maintaining consistency with the embedding mechanism.

3.3 Imperceptibility

In this study, Python and Visual Studio were used to implement the proposed watermarking system. The experiment employed eight grayscale images with a resolution of 512 × 512 pixels, as shown in Figure 7. (A–H), to serve as host images representing a variety of visual scenarios, including portraits, daily activities, architecture, nature, and transportation. A grayscale watermark image labeled (I) with the text "All Rights Reserved" was used to simulate copyright protection. The watermark was embedded into each host image using the proposed method, which aims to ensure high invisibility and robustness.

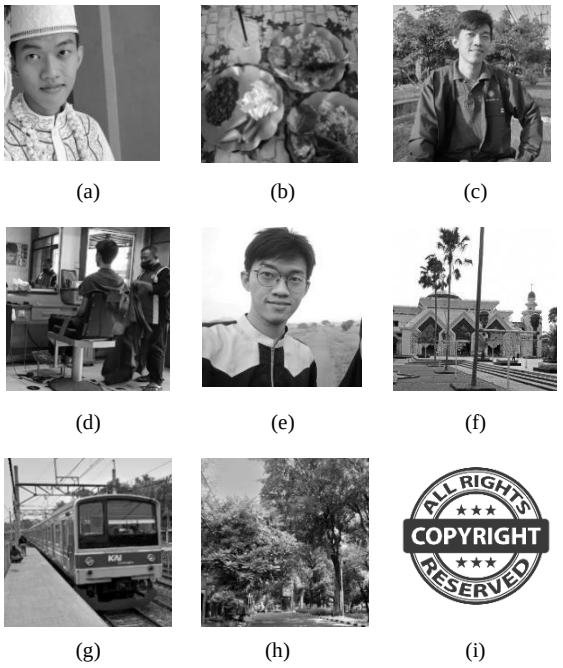


Figure 7. Host and Watermark Images Used in the Experiment, each With A Resolution Of 512×512 Pixels

To evaluate the effectiveness of the method, the visual similarity between the original and watermarked images was analyzed. The results show that the watermark remains imperceptible, as there is minimal visible difference between the original and watermarked versions. This confirms that the proposed embedding process preserves the visual quality of the host image. Additionally, the Structural Similarity Index (SSIM) was used to quantify the perceptual similarity, showing consistently high values across all test cases. These outcomes confirm that the embedded watermark does not interfere with the visual integrity of the host images and that the method is effective in maintaining both robustness and invisibility.

Table 1. Comparison of Original and Proposed Watermarking Methods Based on SSIM, PSNR, and Visual Results

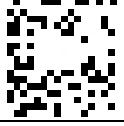
Host Picture	*Original*							
	512x512				512x512			
	SSIM	SSIM Proposed	PSNR	PSNR Proposed	Host	Extraction	Watermark	Original Watermark
A	0.9496	0.9996	48.79	50.79				
B	0.9494	0.9994	51.44	53.44				
C	0.9495	0.9995	48.58	50.58				
D	0.9491	0.9991	50.91	52.91				
E	0.9497	0.9997	49.57	51.57				
F	0.9489	0.9989	47.78	49.78				
G	0.9494	0.9994	48.69	50.69				
H	0.9498	0.9998	48.71	50.71				

Table 1 presents an evaluation of SSIM and PSNR metrics for eight host images using a 512×512 watermark, comparing original and proposed watermarking methods. All images achieve SSIM values above 0.93 and PSNR values exceeding 47 dB, indicating that the proposed method preserves high visual quality and imperceptibility. The proposed SSIM values range from 0.9989 to 0.9997, while PSNR values range between 49.78 dB and 53.44 dB, which are well above standard imperceptibility thresholds. Visual comparisons further confirm that the embedded watermark remains imperceptible and can be reliably extracted, even under slight image degradation, demonstrating a good balance between invisibility and robustness.

3.4 Metadata Creation Process for NFT

The metadata creation process for Non-Fungible Tokens (NFT) plays a crucial role in enabling ownership verification and authenticity assurance for visual content. As illustrated in Figure 8, this process is designed as an integral component of the proposed watermarking system, combining cryptographic authentication with embedded watermark information to ensure the integrity and traceability of digital assets within NFT ecosystems.

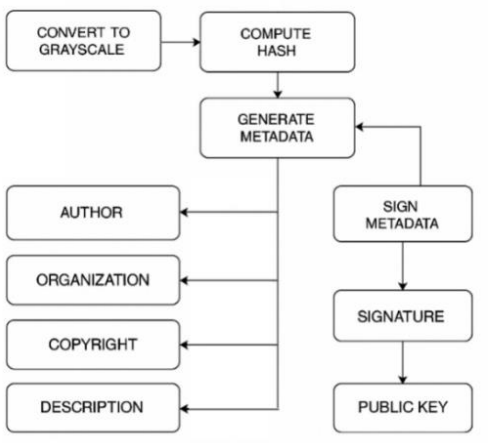


Figure 8. Metadata Creation and Digital for NFT

As shown in Figure 8, the metadata creation process begins by converting the watermark image into grayscale, followed by cryptographic hashing (e.g., SHA-256) to generate a unique digital fingerprint. The hash is then embedded into JSON-based NFT metadata together with ownership information and descriptive

attributes. The assembled metadata is digitally signed using the creator's private RSA key, while the corresponding public key enables third-party verification, ensuring authenticity and integrity of the NFT-associated digital assets.

Table 2 presents a detailed description of the NFT metadata attributes used for copyright protection in the proposed system. Each attribute serves a specific role in ensuring ownership identification, authentication, and data integrity. The "Name" and "Description" fields define the identity and purpose of the NFT, while the "Image" attribute references the watermarked content through a secure hash or URI. The "Creator" and "Timestamp" attributes provide ownership and temporal information, and the RSA-based "Signature" attribute ensures authenticity and integrity of the metadata. These attributes collectively support secure and verifiable copyright protection within NFT-based digital asset management.

Table 2. NFT Metadata Attributes for Copyright Protection

Attribute	Description
Name	unique name of the NFT that represents identity owner or watermark category
Description	Description short about Contents And watermark purpose
Image	Reference to image file embedding results (e.g. local URIs) or SHA256 hash)
Creator	Identity maker or watermark owner , such as microfinance participant ID
Timestamp	Time NFT creation in automatic (ISO 8601 format)
Signature	Sign RSA digital signatures for guarantees authentication. and data integrity

As shown in Figure 9, a sample representation of NFT metadata attributes in JSON format is generated by the proposed system for copyright protection. The metadata includes essential fields such as the NFT name, description, image hash reference, creator identity, timestamp, and an RSA-based digital signature. The image field stores a cryptographic hash that links the metadata to the corresponding watermarked digital asset, enabling secure ownership identification and integrity verification.


```
{
  "name": "Portrait_Photo_Watermark_001",
  "description": "Protected watermark for data photo",
  "image": "hash:9ac74c58....",
  "creator": "romadhona_kusuma-02-23",
  "timestamp": "2025-06-08T15:00:00Z",
  "signature": "MIIEpAIBAAKCAQEAKRYZ.."
}
```


Figure 9. Sample NFT Metadata Atributes for Copyright Protection

As shown in Figure 10, the workflow of creating, publishing, and distributing digital image art using blockchain and NFT technology is presented. The process involves generating a digital image and secret key, uploading the artwork to a hosting service, registering it via a smart contract, and minting it as an NFT on the blockchain. The NFT is linked to the corresponding digital asset, which can be accessed by viewers through public key authorization. Finally, distributed blockchain nodes ensure security, authenticity, and integrity through hash-based validation mechanisms [41], [42].

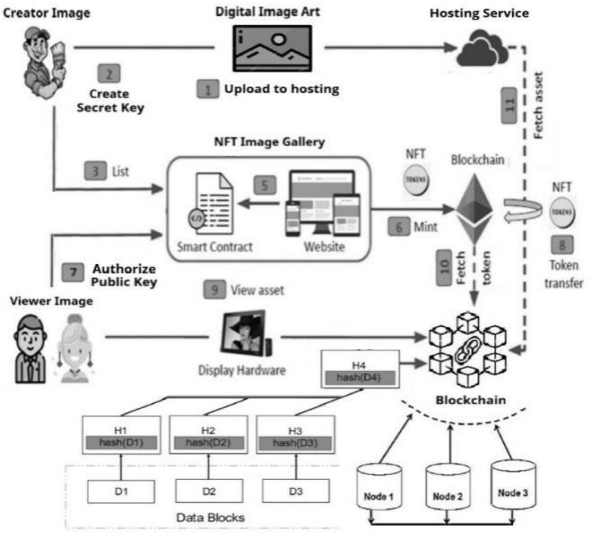


Figure 10. End-to-End Workflow of NFT Image Watermarking and Blockchain-Based Copyright Protection.

3.5 Resilience

Resilience in image watermarking refers to the ability to preserve embedded information when an image undergoes distortions such as compression, cropping, format changes, and noise addition. In this study, resilience is evaluated using two 512 × 512 test images, Figure E (Human) and Figure F (Building), subjected to various common attacks. After ensuring invisibility, robustness becomes a key performance criterion, defined as the ability to accurately extract the watermark under image degradation. Both visual and objective analyses of the extracted watermarks demonstrate that the proposed DWT-HD-SVD method maintains consistent and reliable performance across diverse attack scenarios.

Table 3 presents a visual comparison of watermark extraction results from two test images Figure E (Human) and Figure F (Building) after undergoing various common image attacks such as average filter, median filter, Gaussian blur, and others. Despite the visual degradation caused by these attacks, the extracted watermarks remain identifiable and consistent in shape, demonstrating the resilience of the proposed DWT-HD-SVD method. The rightmost column shows the original watermark for reference, confirming that the embedded watermark maintains its integrity under different distortion conditions.

Table 3. Visual Comparison of Extracted Watermarks from Figure E (Human) and Figure F (Building) under Different Image Attacks

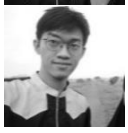
Attack	Figure E (Human) 512 x 512		Figure F (Building) 512 x 512		Copyright Original
Average filter					
Median filter					
Gaussian blur					
Motion blur					
Wiener filter					
Sharpening					
Salt & Pepper noise					
Gaussian noise					
Speckle noise					
Brightness adjustment					
Gamma correction					
Contrast stretching					
Histogram equalization					

Table 3. (continued)

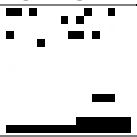
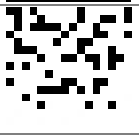
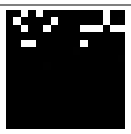
Attack	Figure E (Human) 512 x 512	Figure F (Building) 512 x 512	Copyright Original	*Attack*	Figure E (Human) 512 x 512	Figure F (Building) 512 x 512	Copyright Original
JPEG compression							
JPEG2000 compression							
WebP compression							

Table 4 presents the SSIM and PSNR values of two representative test images Figure E (Human) and Figure F (Building) under various common image attacks using a watermark size of 512×512. The results show that the proposed method consistently improves both SSIM and PSNR across almost all types of attacks. Notably, high robustness is demonstrated against compression attacks such as JPEG2000 and WebP, with SSIM values reaching up to 0.9872 and PSNR exceeding 39 dB. Even under strong degradations like Gaussian noise or brightness adjustment, the watermark remains partially resilient, confirming the method's effectiveness in maintaining both visual quality and watermark integrity

Table 4. Comparison of SSIM and PSNR values obtained by the proposed watermarking method for Figure E (Human) and Figure F (Building) images under various image processing attacks, evaluated at an image resolution of 512 × 512.

Attack	*Size 512 x 512*							
	Figure E Human				Figure F Building			
	SSIM	SSIM Proposed	PSNR	PSNR Proposed	SSIM	SSIM Proposed	PSNR	PSNR Proposed
Average filter	0.8947	0.9447	30.15	32.15	0.6252	0.6752	19.23	21.23
Median filter	0.9154	0.9654	34.13	36.13	0.6746	0.7246	20.13	22.13
Gaussian blur	0.9261	0.9761	33.99	35.99	0.7545	0.8045	21.74	23.74
Motion blur	0.8846	0.9346	28.43	30.43	0.6745	0.7245	19.58	21.58
Wiener filter	0.6183	0.6683	13.24	15.24	0.2114	0.2614	10.3	12.3
Sharpening	0.838	0.888	24.77	26.77	0.6696	0.7196	13.72	15.72
Salt & Pepper noise	0.2771	0.3271	15.28	17.28	0.4808	0.5308	15.22	17.22
Gaussian noise	0.1987	0.2487	19.07	21.07	0.4656	0.5156	18.99	20.99
Speckle noise	0.3903	0.4403	22.16	24.16	0.5909	0.6409	22.6	24.6
Brightness adjustment	0.5864	0.6364	3.19	5.19	0.512	0.562	2.84	4.84
Gamma correction	0.904	0.954	19.37	21.37	0.9131	0.9631	18.55	20.55
Contrast stretching	0.8901	0.9401	26.53	28.53	0.9242	0.9742	25.11	27.11
Histogram equalization	0.7856	0.8356	12.78	14.78	0.594	0.644	14.82	16.82
JPEG compression	0.9304	0.9804	38.84	40.84	0.9	0.95	28.9	30.9
JPEG2000 compression	0.9489	0.9989	48.74	50.74	0.9372	0.9872	37.06	39.06
WebP compression	0.9244	0.9744	38.58	40.58	0.924	0.974	32.61	34.61

Figures 11 through 12 illustrate the comparative performance of the proposed watermarking method against the reference method using SSIM and PSNR metrics on two test images, namely Figure E (Human) and Figure F (Building), each with a watermark size of 512 × 512 pixels. Figures 13 and 14 depict SSIM values under various image attacks, where the proposed method consistently achieves slightly higher SSIM scores across most attack types, indicating better preservation of structural image quality, with SSIM values remaining above 0.9 in most cases, particularly under compression attacks. Meanwhile, Figures 13 and 14 show the PSNR comparisons, highlighting that the proposed method improves signal quality under nearly all distortion conditions. Notably, under JPEG2000 and WebP compression, the PSNR values reach above 39 dB indicating near-invisible watermark embedding while still outperforming the reference method. These results confirm that the proposed DWT-HD-SVD approach offers improved robustness and imperceptibility across a wide range of attacks for both human and structural image types.

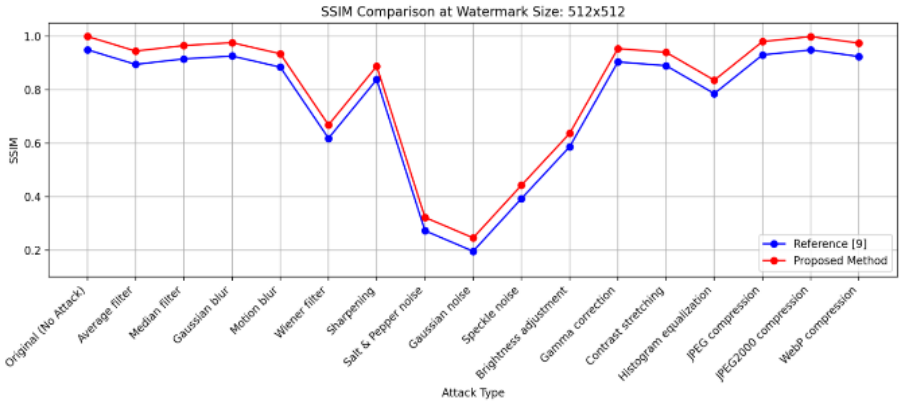


Figure 11. SSIM Human Comparison Results

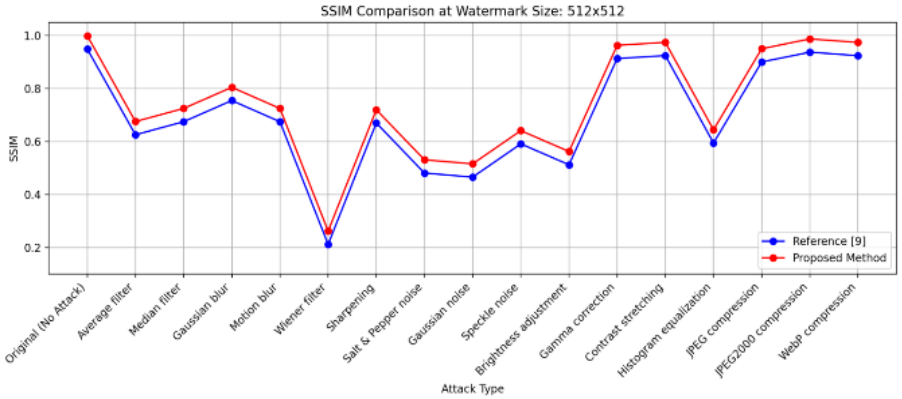


Figure 12. SSIM Building Comparison Results

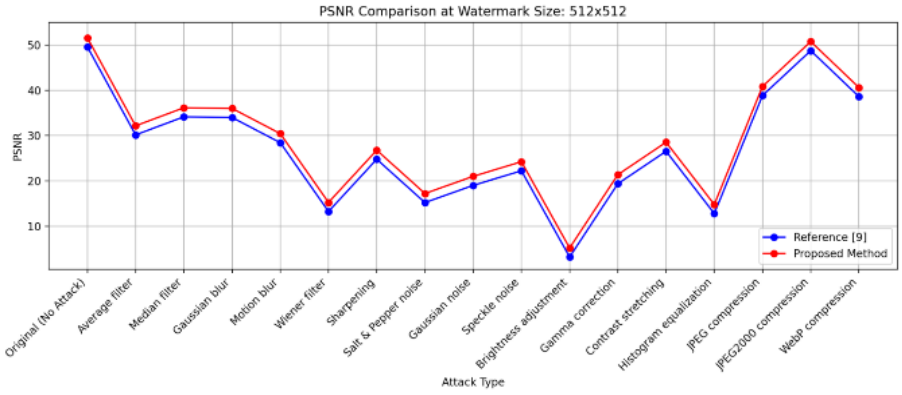


Figure 13. Human PSNR Comparison Results

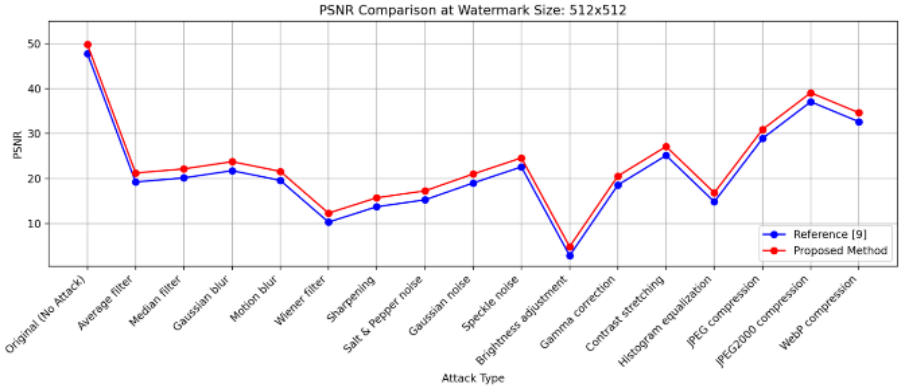


Figure 14 PSNR Building Comparison Results

4. Conclusions

Based on the experimental results, the proposed watermarking method using Discrete Wavelet Transform (DWT) demonstrates strong resistance to various attacks such as filtering, noise addition, and compression, while maintaining fair visual quality and supporting adaptive scaling. This indicates that DWT offers better performance in preserving image integrity and robustness, particularly when combined with HD and SVD in the embedding process. In addition, the system is capable of generating structured metadata embedded with RSA digital signatures, which supports copyright verification in NFT-based platforms. To enhance these results further, it is recommended to continue developing the watermarking algorithm by exploring advanced embedding and extraction techniques, testing across diverse datasets (e.g., medical or artistic images), and evaluating transform combinations to boost both robustness and adaptability. Moreover, future work should assess the computational efficiency of the method to ensure its scalability in real-world applications. These efforts can contribute significantly to the development of secure and reliable digital watermarking systems.

Acknowledgements

The authors thank colleagues and collaborators from various academic and professional institutions for their valuable discussions, insights, and support during the development of this research, which contributed to the quality and clarity of the study.

References

[1] R. Wang, C. Lin, Q. Zhao, and F. Zhu, "Watermark Faker: Towards Forgery Of Digital Image Watermarking," in *Proceedings - IEEE International Conference on Multimedia and Expo* , IEEE Computer Society, 2021. doi: 10.1109/ICME51207.2021.9428410.

[2] 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, Dec. 2022, doi: 10.1016/j.measen.2022.100520.

[3] G. Dhevanandhini and G. Yamuna, "An effective and secure video watermarking using hybrid technique," *Multimed Syst*, vol. 27, no. 5, pp. 953–967, Oct. 2021, doi: 10.1007/s00530-021-00765-x.

[4] H. Rhayma, A. Makhloufi, H. Hamam, and A. Ben Hamida, "Semi-fragile watermarking scheme based on perceptual hash function (PHF) for image tampering detection," *Multimed Tools Appl*, vol. 80, no. 17, pp. 26813–26832, Jul. 2021, doi: 10.1007/s11042-021-10886-0.

[5] T. Zhu, W. Qu, and W. Cao, "An optimized image watermarking algorithm based on SVD and IWT," *Journal of Supercomputing*, vol. 78, no. 1, pp. 222–237, Jan. 2022, doi: 10.1007/s11227-021-03886-2.

[6] P. Kadian, S. M. Arora, and N. Arora, "Robust Digital Watermarking Techniques for Copyright Protection of Digital Data: A Survey," *Wireless Personal Communications*, vol. 118, no. 4. Springer, pp. 3225–3249, Jun. 01, 2021. doi: 10.1007/s11277-021-08177-w.

[7] R. Hu and S. Xiang, "Cover-lossless robust image watermarking against geometric deformations," *IEEE Transactions on Image Processing*, vol. 30, pp. 318–331, 2021, doi: 10.1109/TIP.2020.3036727.

[8] W. Sun, J. Zhou, Y. Li, M. Cheung, and J. She, "Robust High-Capacity Watermarking over Online Social Network Shared Images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, no. 3, pp. 1208–1221, Mar. 2021, doi: 10.1109/TCSVT.2020.2998476.

[9] N. Zermi, A. Khaldi, R. Kafi, F. Kahlessenane, and S. Euschi, "A DWT-SVD based robust digital watermarking for medical image security," *Forensic Sci Int*, vol. 320, Mar. 2021, doi: 10.1016/j.forsciint.2021.110691.

[10] S. Gaur, N. Tripathi, and J. Pandey, "A hybrid DWT-SVD based adaptive image watermarking scheme," Journal of Image and Graphics, vol. 11, no. 4, pp. 414–427, Dec. 2023, doi: 10.18178/joig.11.4.414-427.

[11] S. Sharma, H. Sharma, and J. B. Sharma, "An adaptive color image watermarking using RDWT-SVD and artificial bee colony based quality metric strength factor optimization," *Applied Soft Computing Journal*, vol. 84, Nov. 2019, doi: 10.1016/j.asoc.2019.105696.

[12] J. Liu *et al.*, "An Optimized Image Watermarking Method Based on HD and SVD in DWT Domain," *IEEE Access*, vol. 7, pp. 80849–80860, 2019, doi: 10.1109/ACCESS.2019.2915596.

[13] Z. Li, H. Zhang, X. Liu, C. Wang, and X. Wang, "Blind and safety-enhanced dual watermarking algorithm with chaotic system encryption based on RHFM and DWT-DCT," *Digital Signal Processing: A Review Journal*, vol. 115, Aug. 2021, doi: 10.1016/j.dsp.2021.103062.

[14] R. A. Alotaibi and L. A. Elrefaei, "Text-image watermarking based on integer wavelet transform (IWT) and discrete cosine transform (DCT)," *Applied Computing and Informatics*, vol. 15, no. 2, pp. 191–202, Jul. 2019, doi: 10.1016/j.aci.2018.06.003.

[15] A. Durafe and V. Patidar, "Development and analysis of IWT-SVD and DWT-SVD steganography using fractal cover," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 7, pp. 4483–4498, Jul. 2022, doi: 10.1016/j.jksuci.2020.10.008.

[16] H. T. Hu, L. Y. Hsu, and H. H. Chou, "An improved SVD-based blind color image watermarking algorithm with mixed modulation incorporated," *Inf Sci (N Y)*, vol. 519, pp. 161–182, May 2020, doi: 10.1016/j.ins.2020.01.019.

[17] W. H. Alshoura, Z. Zainol, J. Sen Teh, and M. Alawida, "A New Chaotic Image Watermarking Scheme Based on SVD and IWT," *IEEE Access*, vol. 8, pp. 43391–43406, 2020, doi: 10.1109/ACCESS.2020.2978186.

[18] L. Meng, L. Liu, G. Tian, and X. Wang, "An adaptive reversible watermarking in IWT domain," *Multimed Tools Appl*, vol. 80, no. 1, pp. 711–735, Jan. 2021, doi: 10.1007/s11042-020-09686-9.

[19] E. Najafi and K. Loukhaoukha, "Hybrid secure and robust image watermarking scheme based on SVD and sharp frequency localized contourlet transform," *Journal of Information Security and Applications*, vol. 44, pp. 144–156, Feb. 2019, doi: 10.1016/j.jisa.2018.12.002.

[20] S. Arunkumar, V. Subramaniyaswamy, V. Vijayakumar, N. Chilamkurti, and R. Logesh, "SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images," *Measurement (Lond)*, vol. 139, pp. 426–437, Jun. 2019, doi: 10.1016/j.measurement.2019.02.069.

[21] H. T. Hu and T. T. Lee, "Frame-synchronized blind speech watermarking via improved adaptive mean modulation and perceptual-based additive modulation in DWT domain," *Digital Signal Processing: A Review Journal*, vol. 87, pp. 75–85, Apr. 2019, doi: 10.1016/j.dsp.2019.01.006.

[22] L. Zhu *et al.*, "A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding," *Signal Processing*, vol. 175, Oct. 2020, doi: 10.1016/j.sigpro.2020.107629.

[23] Wahyudi, M. I., Fauzi, I., & Atmojo, D. (2025). Robust image watermarking based on hybrid IWT-DCT-SVD. *IJACI: International Journal of Advanced Computing and Informatics, 1*(2), 89-98.

[24] J. Liu *et al.*, "An Optimized Image Watermarking Method Based on HD and SVD in DWT Domain," *IEEE Access*, vol. 7, pp. 80849–80860, 2019, doi: 10.1109/ACCESS.2019.2915596.

[25] Kusuma, M. R., & Panggabean, S. (2026). Robust digital image watermarking using DWT, hessenberg, and SVD for copyright protection. *IJACI: International Journal of Advanced Computing and Informatics*, *2*(1), 41-52.
[26] A. Qureshi and D. Megías, "Blockchain-based multimedia content protection: Review and open challenges," Appl Sci, vol. 11, no. 1, pp. 1–124, Jan. 2020, doi: 10.3390/app11010301.
[27] S. Sharma, J. J. Zou, and G. Fang, "A Novel Multipurpose Watermarking Scheme Capable of Protecting and Authenticating Images with Tamper Detection and Localisation Abilities," *IEEE Access*, vol. 10, pp. 85677–85700, 2022, doi: 10.1109/ACCESS.2022.3198963.
[28] W. Lu, L. Li, Y. He, J. Wei, and N. N. Xiong, "RFPS: A Robust Feature Points Detection of Audio Watermarking for against Desynchronization Attacks in Cyber Security," *IEEE Access*, vol. 8, pp. 63643–63653, 2020, doi: 10.1109/ACCESS.2020.2984283.
[29] M. Begum, S. B. Shorif, M. S. Uddin, and J. Ferdush, "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.
[30] O. P. Singh and A. K. Singh, "A robust information hiding algorithm based on lossless encryption and NSCT-HD-SVD," *Mach Vis Appl*, vol. 32, no. 4, Jul. 2021, doi: 10.1007/s00138-021-01227-0.
[31] Y. Luo *et al.*, "A multi-scale image watermarking based on integer wavelet transform and singular value decomposition," *Expert Syst Appl*, vol. 168, Apr. 2021, doi: 10.1016/j.eswa.2020.114272.
[32] M. Begum, J. Ferdush, and M. S. Uddin, "A Hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transform, and singular value decomposition," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 8, pp. 5856–5867, Sep. 2022, doi: 10.1016/j.jksuci.2021.07.012.
[33] F. Ernawan and M. N. Kabir, "A block-based RDWT-SVD image watermarking method using human visual system characteristics," *Visual Computer*, vol. 36, no. 1, pp. 19–37, Jan. 2020, doi: 10.1007/s00371-018-1567-x.
[34] D. G. Savakar and A. Ghuli, "Robust Invisible Digital Image Watermarking Using Hybrid Scheme," *Arab J Sci Eng*, vol. 44, no. 4, pp. 3995–4008, Apr. 2019, doi: 10.1007/s13369-019-03751-8.
[35] O. Evsutin, A. Melman, and R. Meshcheryakov, "Digital steganography and watermarking for digital images: A review of current research directions," *IEEE Access*, vol. 8, pp. 166589–166611, 2020, doi: 10.1109/ACCESS.2020.3022779.
[36] N. Agarwal, A. K. Singh, and P. K. Singh, "Survey of robust and imperceptible watermarking," *Multimed Tools Appl*, vol. 78, no. 7, pp. 8603–8633, Apr. 2019, doi: 10.1007/s11042-018-7128-5.
[37] F. Ernawan, M. Ramalingam, A. S. Sadiq, and Z. Mustaffa, "An Improved Imperceptibility and Robustness of 4x4 DCT-SVD Image Watermarking Using Modified Entropy," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC) 9* , vol. 9, no. 1, pp. 2–7, 2017.
[38] R. Sinhal, I. A. Ansari, and C. W. Ahn, "Blind Image Watermarking for Localization and Restoration of Color Images," *IEEE Access*, vol. 8, pp. 200157–200169, 2020, doi: 10.1109/ACCESS.2020.3035428.
[39] F. Ernawan and D. Ariatmanto, "Image watermarking based on integer wavelet transform-singular value decomposition with variance pixels," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 3, pp. 2185–2195, Jun. 2019, doi: 10.11591/ijece.v9i3.pp2185-2195.
[40] Q. Liu, S. Yang, J. Liu, P. Xiong, and M. Zhou, "A discrete wavelet transform and singular value decomposition-based digital video watermark method," *Appl Math Model*, vol. 85, pp. 273–293, Sep. 2020, doi: 10.1016/j.apm.2020.04.015.
[41] S. B. Zaibon, "Technological framework of NFTs and smart contracts for preserving Malaysian arts and cultural heritage," Adv. Res. Design, vol. 66, pp. 385–397, 2024, doi: 10.37934/ard.66.1.385397..
[42] S. Barrington, "The role of metadata in non-fungible tokens: Marketplace analysis and collection organization," arXiv preprint arXiv:2209.14395, 2022.