Invisible Watermarking for Image Data Protection in Sensor Network Environments

Seo-Yi Kim
Department of Convergence Security Engineering
Sungshin Women's University
Seoul, South Korea
email: sykim.cse@gmail.com

Na-Eun Park
Department of Future Convergence Technology Engineering
Sungshin Women's University
Seoul, South Korea
email: nepark.cse@gmail.com

Il-Gu Lee
Department of Convergence Security Engineering
Sungshin Women's University
Seoul, South Korea
email: iglee@sungshin.ac.kr

***Abstract*—Advancements in Artificial Intelligence (AI) have greatly increased the risk of digital-image tampering, underscoring the need to verify the integrity and authenticity of image data collected and transmitted within sensor networks and sensor-based systems. As visual threats, such as deepfakes and adversarial attacks proliferate, manipulated sensor images can trigger severe security incidents and false detections. This paper proposes a robust watermarking method that employs a three-level Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to repeatedly embed a watermark into the singular values of both low- and selected high-frequency components. Designed to account for transmission noise and environmental distortions in multi-sensor settings, the proposed approach leverages redundancy across multiple frequency bands to enhance resistance to diverse signal-distortion attacks while keeping the watermark imperceptible. Experimental results show that the proposed method significantly surpasses conventional techniques in watermark extraction accuracy while preserving high image quality, establishing it as a reliable security solution for protecting image integrity and detecting tampering in sensor-based environments.**

Keywords-Sensor camera; Digital watermarking; Image protection.

I. INTRODUCTION

The increasing prevalence of malicious video-based attacks, such as deepfakes and adversarial attacks, has increased the need for technologies that can verify the integrity and authenticity of image data obtained from sensor cameras [1].

For instance, a notable 2019 incident in China involved bypassing a facial recognition access control system with deepfake technology. An attacker manipulated facial images from existing surveillance camera footage into real-time deepfake videos, which were then used to deceive the system and compromise physical security [2]. This incident underscores the vulnerability of image sensor-based systems, particularly those integral to public safety.

Similarly, a 2020 experiment in the United States targeting autonomous vehicles demonstrated the threat of adversarial patches. By placing specially crafted patterns on road signs, researchers deceived a vehicle's camera into misinterpreting a "STOP" sign as a "SPEED LIMIT 45" sign [3]. This attack exploited vulnerabilities in AI-based recognition systems, posing serious safety risks during road operations [4].

These examples illustrate the significant security threats that arise when malicious actors manipulate sensor-captured images. Consequently, verifying the integrity and authenticity of sensor-based image data has emerged as a critical security challenge [5].

Digital watermarking is a promising solution to this challenge. This technique embeds identifiable information into image data to detect unauthorized modifications or trace copyright ownership. To be effective, digital watermarking must satisfy two key requirements: robustness against external attacks and imperceptibility, which preserves the original image's visual quality. To meet these criteria, frequency-domain-based methods—particularly those using the Discrete Wavelet Transform (DWT)—are commonly employed. However, DWT-based methods can be vulnerable to certain attacks such as Joint Photographic Experts Group (JPEG) compression, Gaussian or salt-and-pepper noise, filtering (e.g., low-pass/median), and geometric transformations like rotation, scaling, and cropping [6].

To overcome these limitations, recent studies have combined DWT with Singular Value Decomposition (SVD). SVD facilitates watermark insertion by modifying an image's singular values, which represent its essential features, thereby avoiding noticeable distortion [7]. Embedding a watermark into the singular values of DWT-decomposed frequency components has been shown to enhance robustness against both noise and compression attacks [8].

In this study, we propose a method that applies a three-level DWT to decompose an image into its low- and selected high-frequency components. Subsequently, SVD is used to embed the watermark repeatedly into these components. Embedding the watermark in the low-frequency region, which contains the image's core structural information, helps ensure imperceptibility, as even minor modifications in this area can significantly impact the visual appearance. Simultaneously, embedding in high-frequency components enhances resistance to filtering and other frequency-based attacks.

ISBN: 978-1-68558-304-0

During the extraction process, the correlation between the repeated watermark signals is leveraged to correct errors and accurately reconstruct the original watermark, even in the presence of distortion.

The main contributions of this study can be summarized as follows:

- We propose a novel invisible digital watermarking method that combines a three-level DWT with SVD for robust image integrity protection.
- The method demonstrates enhanced resilience against partial data loss and various signal distortion attacks, which is achieved by embedding the watermark with redundancy across multiple frequency components.
- We developed a comprehensive framework to systematically evaluate watermarking performance under diverse signal distortion conditions.
- Experimental validation confirms that the proposed method significantly outperforms conventional approaches in watermark extraction accuracy while maintaining high image quality.

The remainder of this paper is organized as follows: Section II discusses the conventional methods employed for image integrity protection, Section III details the proposed method, Section IV outlines the experimental setup and procedures, and Section V presents the performance evaluation results. Finally, Section VI concludes the paper.

II. Background

Prior studies have employed various techniques to verify the integrity and authenticity of image data, including digital signatures, hashing, and digital watermarking. This section analyzes the conventional methods used for protecting image data.

A. Digital Signature

Albahadily et al. [9] proposed a hash-based digital signature scheme to verify the integrity and authenticity of digital documents. This method generates a unique hash value from the document and user information using the MD5 algorithm and embeds it as a signature. To detect tampering, the receiver extracts the hash value and compares it with a newly generated hash from the received content. This approach employs a lightweight hashing algorithm, enabling fast computation suitable for real-time processing, and is applicable to various data formats, including text and images. However, a key limitation is that the signature data must be stored separately from the image; therefore, the overall content integrity is compromised if the signature is lost or the image is partially modified.

B. Hashing

Khan et al. [10] proposed an ElGamal-based digital signature and encryption scheme to ensure both privacy and authentication for biometric image data. The method first randomizes the image's pixel positions using a 3D Arnold transform and then encrypts both the transform parameters and the image data with the ElGamal public-key cryptosystem. Integrity verification is subsequently achieved using an ElGamal digital signature. The scheme offers strong security by leveraging a public-key cryptosystem based on the discrete logarithm problem. Additionally, the integration of randomization and encryption enables both tamper detection and authentication while significantly reducing the risk of data leakage. However, the method's general applicability is limited, and its high computational overhead makes it unsuitable for lightweight or real-time environments such as Internet of Things (IoT) systems.

C. Digital Watermark

Zhan et al. [11] proposed a reversible fragile watermarking scheme that can verify the integrity of digital images and restore their original content. The method divides an image into blocks and generates two types of data for each: Verification Information (VI) and Recovery Information (RI). VI is embedded directly into its corresponding block to detect tampering, whereas RI, used for content restoration, is concealed in different block locations using the Arnold transform. This dual-verification approach achieves high detection accuracy and supports both tamper detection and content recovery. However, recovery accuracy decreases if the areas containing the watermarks are tampered with, and the complex decoding logic limits its use in real-time applications.

In a related study, Kusumaningrum et al. [12] proposed an image-watermarking technique combining a two-level DWT with SVD, where the watermark is embedded in the low-frequency (LL2) subband, and a non-blind extraction method is employed. The authors compared their method against approaches using only DWT or SVD, evaluating robustness under various attacks, including salt-and-pepper noise, Gaussian filtering, and JPEG compression. However, their evaluation was limited, as it did not consider varying attack intensities or a sufficiently broad range of attacks to comprehensively validate robustness. Although their method outperformed individual DWT and SVD models in watermark extraction, it exhibited poor performance under certain attacks.

Conventional methods demonstrate strengths in areas such as processing speed, security, and recoverability, but they typically involve trade-offs that make it challenging to satisfy all requirements simultaneously. Therefore, this paper presents a watermarking method that minimizes image quality degradation while maintaining robustness against external attacks and tampering during transmission.

III. Image-Watermarking Method Based on DWT and SVD

This study proposes an invisible watermarking scheme that is robust against signal distortion attacks. The proposed method applies a three-level DWT to decompose an image into multiple frequency subbands, followed by SVD on both the low-frequency and selected high-frequency components. The watermark is embedded repeatedly into the singular values, which enhances resistance to attacks that exploit signal distortions. During extraction, the watermarks embedded in

Copyright (c) IARIA, 2025. ISBN: 978-1-68558-304-0

these multiple frequency regions are retrieved and integrated to successfully reconstruct the original watermark.

The design of the method leverages the different properties of an image's frequency components. High-frequency regions contain fine details such as edges and textures. Slight modifications to these regions are typically imperceptible to the human visual system, making them suitable for embedding invisible watermarks. However, these regions are vulnerable to noise attacks aimed at disrupting the watermark.

In contrast, an image's low-frequency components carry its global structure and essential information. Because modifications in this region can cause noticeable degradation in image quality and structure, embedding watermarks here requires minimal distortion to preserve visual fidelity. Watermarks in the low-frequency band are generally robust against JPEG compression, which primarily targets high-frequency content, and show lower sensitivity to attacks such as Gaussian noise and downsampling. As the low-frequency subband retains significant image information even after transformation, an embedded watermark can be reliably recovered unless the image undergoes severe degradation. However, this region has its vulnerabilities. High compression ratios can cause data loss in low-frequency components, and compression schemes like JPEG2000, which operate across the full frequency spectrum, can adversely affect the watermark. Moreover, global adjustments to image properties, such as brightness or contrast, can also impact the integrity of a watermark embedded in this region.

To address these respective challenges, the proposed method utilizes both low- and selected high-frequency components to implement a robust and invisible watermarking scheme.

A. Watermark Embedding Process

Although image-watermarking techniques that combine DWT and SVD typically follow a similar structure, specific procedures vary based on research objectives, such as enhancing robustness, imperceptibility, or efficiency. Typically, the process involves applying DWT to a host image to generate subbands (LL, LH, HL, HH), followed by performing SVD on a selected subband to embed a watermark by modifying its singular values.

The embedding process for the proposed method is illustrated in Figure 1. The size of the watermark image is fixed based on the host image's dimensions and the DWT level, as defined in (1):

$$W = \frac{N}{2^L} \tag{1}$$

where W denotes the side length of the watermark, N is the side length of the host image, and L represents the DWT level. In this study, a 512 × 512 host image and a three-level DWT were employed, necessitating a 64 × 64 watermark image.

When a three-level DWT is applied to the host image, the frequency domain is decomposed into four subbands: LL3, LH3, HL3, and HH3. SVD is then performed on the low-frequency (LL3) and selected high-frequency (LH3 and HL3) subbands to enable watermark embedding. The watermark is first embedded by modifying the singular values of these subbands, denoted as S_t. However, this modification can alter the host image's structural characteristics, which may degrade image quality or cause watermark extraction to fail if the new values do not align well with the original structure.

To address this potential issue, a second SVD is employed as a recalibration process to refine the modified singular values before reconstruction. This additional step helps integrate the modified singular values more naturally into the image's structural context, yielding new, updated singular values (S_w) that improve both the imperceptibility and robustness of the watermark. Using these updated values, the modified subbands (LL3t, LH3t, and HL3t) are reconstructed.

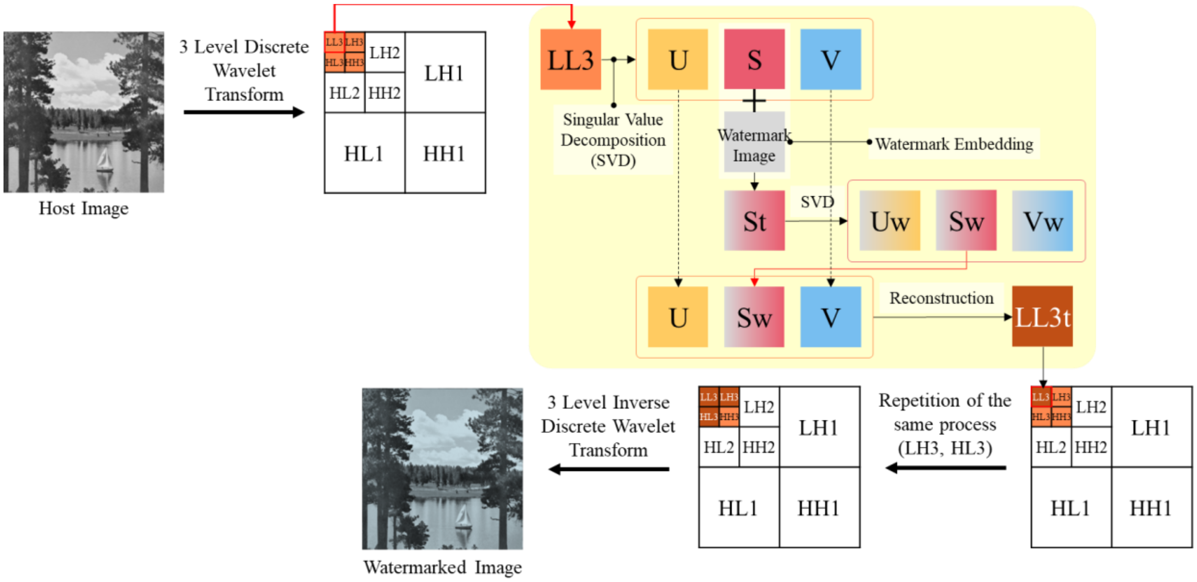

Host Image
3 Level Discrete Wavelet Transform
LL3
LH3
HL3
HH3
LH2
HL2
HH2
LH1
HL1
HH1
LL3
U
S
V
Singular Value Decomposition (SVD)
Watermark Image
Watermark Embedding
St
SVD
Uw
Sw
Vw
U
Sw
V
Reconstruction
LL3t
Repetition of the same process (LH3, HL3)
3 Level Inverse Discrete Wavelet Transform
Watermarked Image

Figure 1. Proposed watermark-embedding process.

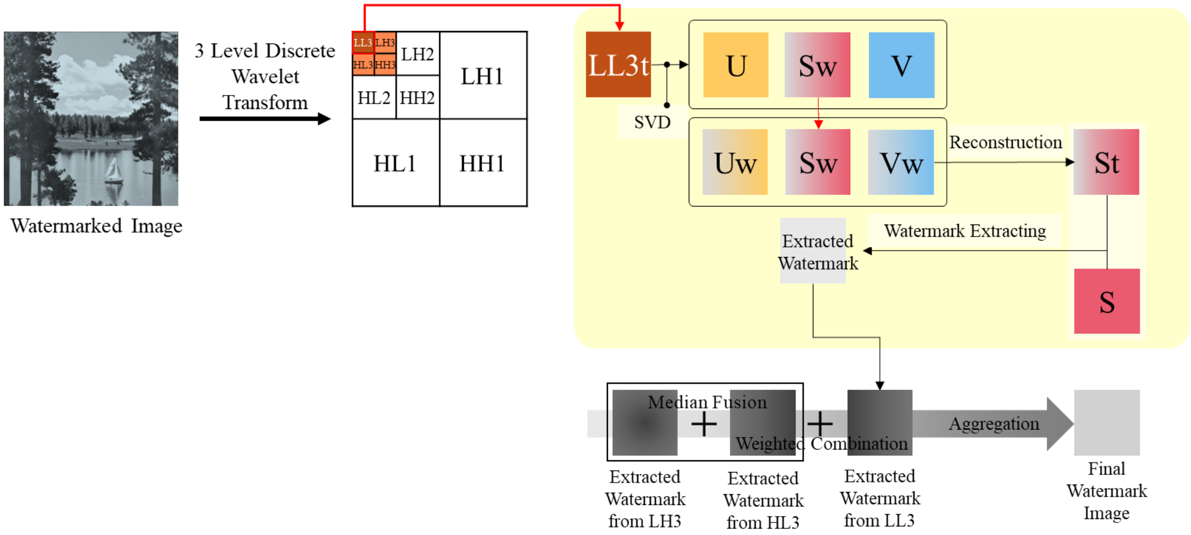


Figure 2. Proposed watermark-extraction process.

Finally, an Inverse DWT (IDWT) is performed to generate the watermarked image. This procedure results in the watermark being embedded thrice into different frequency subbands, creating a redundant watermark structure within the image.

B. *Watermark-Extraction Process*

The watermark extraction process, illustrated in Figure 2, follows a non-blind approach. First, a three-level DWT is applied to the watermarked image to decompose it into its constituent frequency subbands. SVD is then performed on the LL3, LH3, and HL3 subbands to extract the singular value matrices (S_w), where the watermark was embedded. Using these extracted matrices along with the corresponding original U_w and V_w matrices, the watermark images are reconstructed. Because the watermark is embedded separately into the LL3, LH3, and HL3 subbands, three distinct instances can be extracted for the final reconstruction.

The final watermark is reconstructed by fusing these three instances. Median fusion is first applied to the corresponding pixel values of the watermarks extracted from the high-frequency LH3 and HL3 subbands. This step integrates their information while reducing the influence of noise. The resulting intermediate watermark is then combined with the watermark from the LL3 subband using a weighted combination. Because the LL3 subband contains the most critical structural information and is least affected by distortions, its extracted watermark is assigned a higher weight. This ensures that the LL3 watermark plays a dominant role in the reconstruction, whereas the components from LH3 and HL3 serve as complementary sources of information.

IV. Evaluation Methodology

This section details the methodology used to evaluate the performance of the proposed DWT-SVD image-watermarking method. IT describes the experimental setup, attack scenarios, evaluation metrics, and the procedure for embedding and extraction.

A. *Experiment Environments*

As shown in Figure 3, the experiments employed 512 × 512 pixel grayscale host images and a 64 × 64 pixel grayscale watermark image.

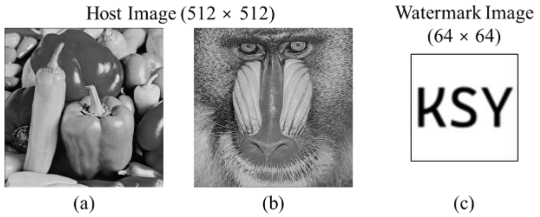


Figure 3. Host and watermark images used in the experiment: (a) Peppers, (b) Mandrill, and (c) watermark image.

To evaluate the robustness of the proposed watermarking scheme, seven distinct signal distortion attacks—encompassing noise, compression, and filtering—were applied to the watermarked images. Each attack was conducted at five intensity levels, from mild (Level 1) to severe (Level 5), to assess performance under varying conditions. The specific parameters controlling the intensity for each attack are summarized in TABLE I.

The intensity of each attack was controlled by specific parameters. For Gaussian noise, intensity was determined by the variance, where a higher value corresponds to stronger noise.

For salt-and-pepper noise, the density parameter represented the proportion of affected pixels; for instance, a density of 0.1 adds salt noise (white pixels, value = 255) to 5%

Copyright (c) IARIA, 2025. ISBN: 978-1-68558-304-0

TABLE I. ATTACK PARAMETERS AND INTENSITIES.

Attack	Parameter	Attack intensity (level)				
		1	2	3	4	5
Gaussian noise	Variance	0.001	0.005	0.01	0.05	0.1
Salt-and-pepper	Density	0.01	0.03	0.05	0.1	0.2
Speckle noise	Probability	0.01	0.03	0.05	0.1	0.2
JPEG	Quality factor	90	70	50	30	10
JPEG2000		90	70	50	30	10
Blurring attack	Kernel size	3	5	7	9	11
Low-pass filtering		3	5	7	9	11

of the pixels and pepper noise (black pixels, value = 0) to another 5%, resulting in a total of 10% corrupted pixels.

Speckle intensity was controlled by a probability parameter, which defines the likelihood that any given pixel will be corrupted by noise. Here, higher probability results in noisier pixels.

For JPEG and JPEG2000 compression, the attack intensity was set by the quality factor, with lower factors indicating stronger compression and greater image quality loss.

Finally, for blurring and low-pass filtering, the kernel size determined the intensity. A larger kernel produces a stronger blur effect (greater information loss) or, in the case of low-pass filtering, removes more high-frequency components. For instance, a kernel size of 3 corresponds to a 3 × 3 filter. Each attack was applied at five intensity levels, from weak (Level 1) to very strong (Level 5), to evaluate the method's robustness under all scenarios.

B. *Experimental Procedure*

The experimental workflow is illustrated in Figure 4. The embedding process begins by applying a three-level DWT to the 512 × 512 host image, using the Daubechies 4 (db4) wavelet with periodization to decompose it into LL3, LH3, HL3, and HH3 subbands. SVD is then applied to the LL3, LH3, and HL3 subbands. The watermark is embedded into the singular value matrices using a scaling factor, α, followed by the second SVD recalibration step. The modified subbands (LL3t, LH3t, and HL3t) are then reconstructed and used in an inverse DWT (IDWT) to generate the final watermarked image.

For the robustness evaluation, each signal distortion attack was applied to the watermarked image. The watermark was then extracted from the attacked image by first applying a three-level DWT, followed by SVD on the LL3t, LH3t, and HL3t subbands. The same scaling factor α used during embedding is applied during extraction. The three extracted watermarks are then combined to reconstruct the final image. This is done by first applying median fusion to the watermark data from the LH3 and HL3 subbands to reduce noise and produce an intermediate watermark. This watermark is then combined with the LL3 watermark using a weighted combination, assigning a weight of 0.9 to the low-frequency data and 0.3 to the high-frequency data.

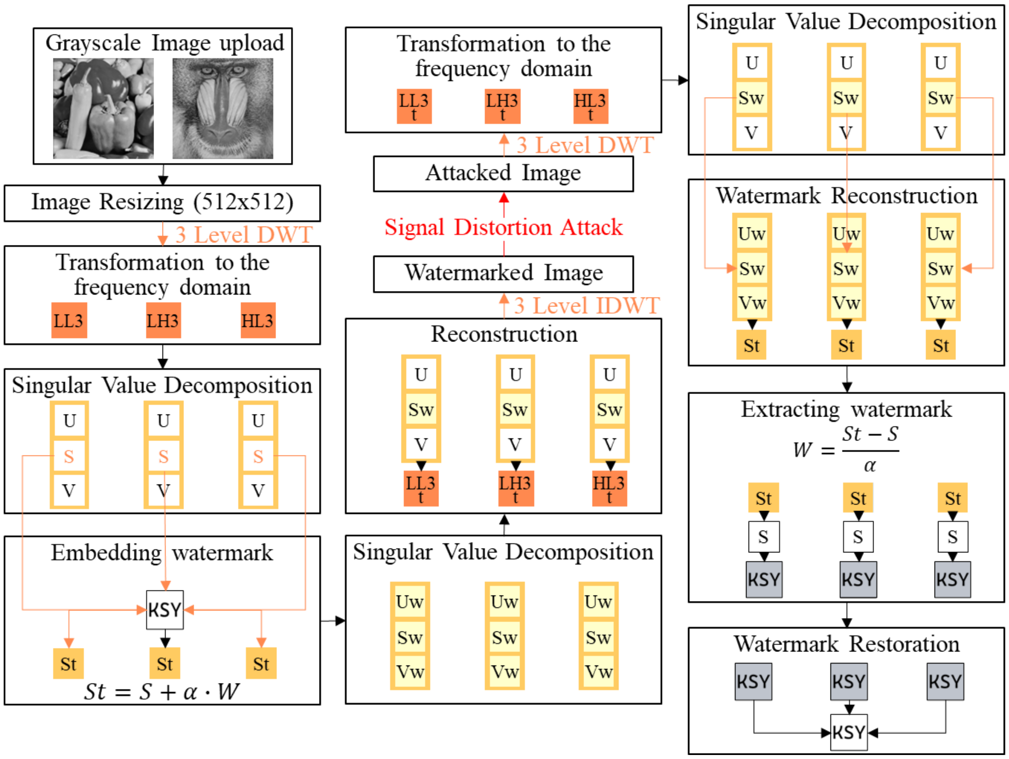


Figure 4. Flowchart of the experimental procedure.

C. *Performance Evaluation Metrics*

To assess watermark extraction accuracy and image quality, the following performance evaluation metrics were used:

Normalized Cross-Correlation (NCC) measures the similarity between two images, and in this study, it was used to compare the host image with the watermarked image and the original watermark with the extracted one [13].

Mean Squared Error (MSE) quantifies the pixel-wise numerical error between the original and altered images by averaging the squared differences between corresponding pixels, which evaluates the distortion caused by watermark embedding [14].

The Peak Signal-to-Noise Ratio (PSNR) is a widely used metric for assessing the quality of a distorted image compared to its original version; a higher PSNR value indicates better preservation of image quality after embedding [15].

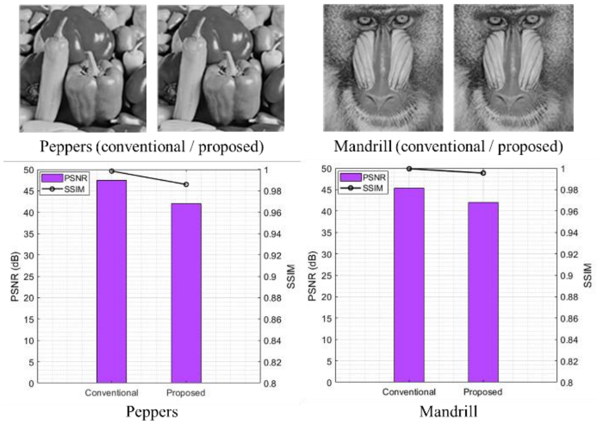
The Structural Similarity Index Measure (SSIM) evaluates the structural similarity between two images by incorporating characteristics of the human visual system, such as luminance, contrast, and structure, making it a more perceptually relevant indicator than PSNR [16].

V. EXPERIMENTS

To validate the performance of the proposed method, a comparative analysis was conducted against a conventional method, which employs a two-level DWT and SVD, embedding the watermark only in the low-frequency (LL2) subband [12]. Both methods used the same watermark embedding strength (α), and robustness was evaluated by applying seven signal distortion attacks at five different intensity levels to assess performance under varying degrees of attack severity.

A. *Image Quality Comparison*

Figure 5 compares the image quality of the conventional and proposed methods using the *Peppers* and *Mandrill* images. The conventional method yielded slightly better visual quality because it only embeds the watermark in the low-frequency subband (LL2), preserving more of the original image content.


Peppers (conventional / proposed)

Mandrill (conventional / proposed)

Peppers

Mandrill

Figure 5. Image-quality comparison between the conventional and proposed methods: (a, c) Peppers and (b, d) Mandrill.

With the proposed method, the PSNR for the *Peppers* and *Mandrill* images decreased by 11.5% and 7.28%, respectively, although both values remained high, exceeding 40 dB. Similarly, the SSIM values showed only a marginal decline of 1.25% and 0.4%, respectively, with scores remaining above 0.98, indicating excellent perceptual similarity.

B. *Watermark-Extraction Performance*

To compare the watermark extraction performance of the conventional and proposed methods, the seven signal distortion attacks were applied to the watermarked images at five intensity levels.

The performance was then evaluated using the NCC and PSNR metrics.

As shown in Figure 6, the conventional method exhibited significant performance degradation in NCC for the *Peppers* and *Mandrill* images as the intensity of Gaussian noise, sparkle noise, and low-pass filtering attacks increased, with noticeable drops also observed for salt-and-pepper and blurring attacks. Specifically, as attack intensity rose from Level 1 to 5, image deteriorated by 75% (Gaussian noise), 89.99% (sparkle noise), and 82.55% (low-pass filtering). The *Mandrill* image showed similar degradation rates of 65.95%, 90.44%, and 92.34% for the same attacks.

By contrast, while the proposed method's performance also declined with increasing attack intensity, the degradation was significantly lower. For instance, under the most impactful low-pass filtering attack, the proposed method's performance dropped by only 14.26% for *Peppers* and 16.10% for *Mandrill*, demonstrating its superior robustness.

While there was no substantial performance difference for most compression attacks, the proposed method was superior under severe JPEG2000 (Level 5) compression, outperforming the conventional method by 31.47% for *Peppers* and 94.66% for *Mandrill*.

As presented in Figure 7, the conventional method showed a sharp decline in PSNR for nearly all attacks, failing to maintain stable performance even at weak, Level 1 intensities (except for JPEG compression). The most severe degradation occurred with the speckle noise attack; for the *Peppers* image, PSNR dropped from 12.60 dB (Level 1) to -12.83 dB (Level 5), a 201.86% decline. By contrast, the proposed method demonstrated consistently stable PSNR performance. Only minor degradation was observed for noise and low-pass filtering attacks between Levels 1 and 2, with values remaining relatively stable thereafter. Although compression attacks caused some degradation, the decline was considerably less severe than that with the conventional method, and the proposed method maintained higher extraction performance across all attack intensities.

VI. CONCLUSION AND FUTURE WORK

This paper presented a digital-image watermarking scheme that achieves both high robustness against signal distortion attacks and strong imperceptibility. The method combines a three-level DWT with SVD, repeatedly embedding a watermark into the singular values of the low-

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

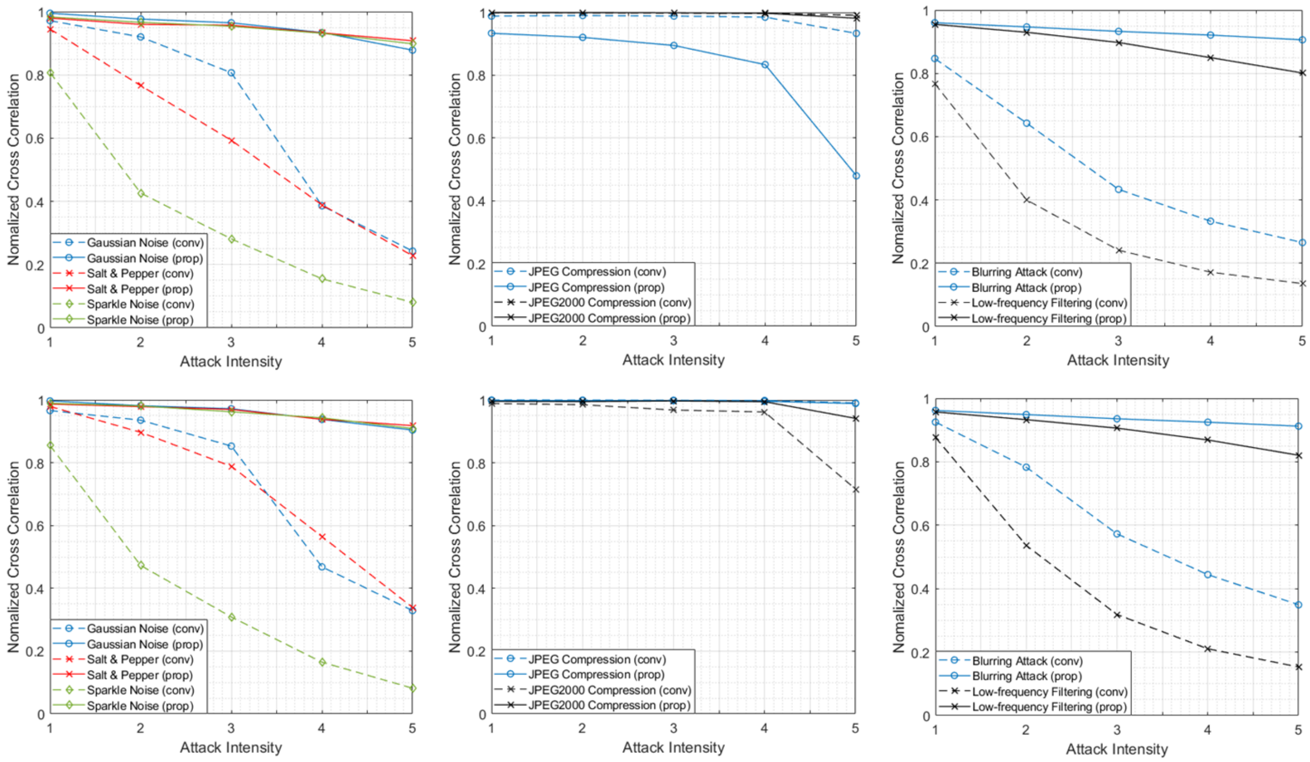


Figure 6. Extraction-performance comparison of conventional and proposed methods based on attack intensity—NCC (top: Peppers, bottom: Mandrill).

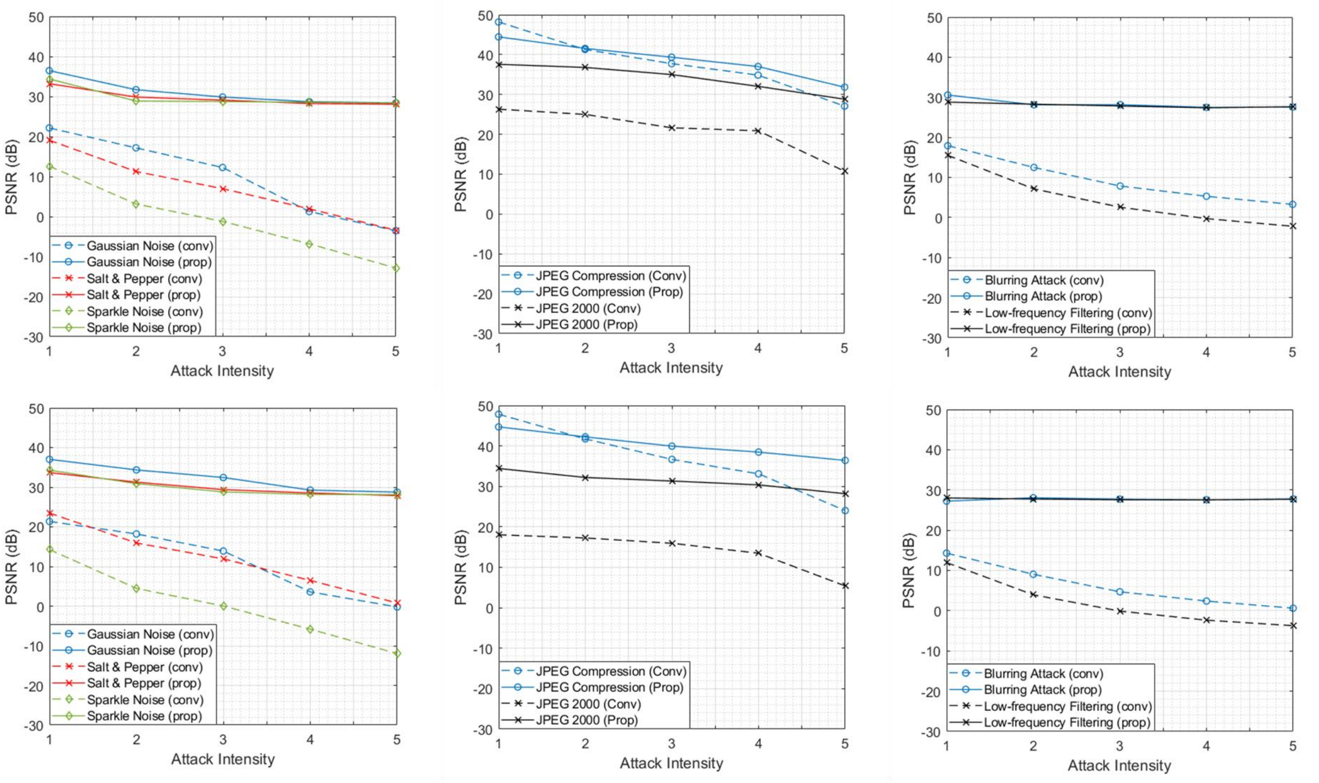


Figure 7. Extraction-performance comparison of conventional and proposed methods based on attack intensity—PSNR (top: Peppers, bottom: Mandrill).

frequency (LL3) and selected high-frequency (LH3, HL3) subbands. This redundant embedding enhances robustness against various attacks while allowing for the complementary recovery of damaged watermark data, effectively mitigating the typical trade-off between imperceptibility and robustness found in conventional methods.

Experimental results demonstrated that the scheme preserves excellent image quality, maintaining high PSNR and SSIM values after embedding. The redundancy led to significantly improved extraction performance; even when parts of the watermark were degraded, the copies enabled accurate reconstruction and reliable detection. Moreover, the method consistently showed strong performance under various levels of noise and compression attacks.

Therefore, the proposed method represents a practical solution for protecting image data in sensor network environments, offering an effective alternative for applications where high reliability and imperceptibility are essential.

Acknowledgment

This work was supported by the Ministry of Trade, Industry and Energy (MOTIE) under Training Industrial Security Specialist for High-Tech Industry (RS-2024-00415520), supervised by the Korea Institute for Advancement of Technology (KIAT), and the Ministry of Science and ICT (MSIT) under the ICAN (ICT Challenge and Advanced Network of HRD) program (No. IITP-2022-RS-2022-00156310), supervised by the Institute of Information & Communication Technology Planning & Evaluation (IITP).

References

[1] P. Zhou, X. Han, V. I. Morariu, and L. S. Davis, “Two-stream neural networks for tampered face detection,” in 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Jul. 2017, pp. 1831–1839. doi: 10.1109/CVPRW.2017.229.

[2] Y. Mirsky and W. Lee, “The creation and detection of deepfakes: a survey,” ACM Comput Surv, vol. 54, no. 1, p. 7:1-7:41, Jan. 2021, doi: 10.1145/3425780.

[3] A. Zolfi, M. Kravchik, Y. Elovici, and A. Shabtai, “The translucent patch: a physical and universal attack on object detectors,” in 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Jun. 2021, pp. 15227–15236. doi: 10.1109/CVPR46437.2021.01498.

[4] N. Wang, Y. Luo, T. Sato, K. Xu, and Q. A. Chen, “Does physical adversarial example really matter to autonomous driving? Towards system-level effect of adversarial object evasion attack,” in 2023 IEEE/CVF International Conference on Computer Vision (ICCV), IEEE, 2023, pp. 4389–4400, doi: 10.14722/vehiclesec.2024.25014.

[5] S. Pavlitska, J. Robb, N. Polley, M. Yazgan, and J. M. Zöllner, “Fool the stoplight: realistic adversarial patch attacks on traffic light detectors,” Jun. 05, 2025, arXiv: arXiv:2506.04823. doi: 10.48550/arXiv.2506.04823.

[6] D. Bhalke, C. Rupa, H. Dahiya, and V. Yadav, “Privacy protection of digital information using frequency domain watermarking technique,” in *Proc. 2021 4th Int. Conf. Recent Trends Comput. Sci. Technol. (ICRTCST)*, Feb. 2022, pp. 202–206, doi: 10.1109/ICRTCST54752.2022.9781929.

[7] N. Zermi, A. Khaldi, M. R. Kafi, F. Kahlessenane, and S. Euschi, “Robust SVD-based schemes for medical image watermarking,” Microprocess. Microsyst., vol. 84, p. 104134, Jul. 2021, doi: 10.1016/j.micpro.2021.104134.

[8] O. Evsutin and K. Dzhanashia, “Watermarking schemes for digital images: Robustness overview,” Signal Process. Image Commun., vol. 100, p. 116523, Jan. 2022, doi: 10.1016/j.image.2021.116523.

[9] H. K. Albahadily, I. A. Jabbar, A. A. Altaay, and X. Ren, “Issuing digital signatures for integrity and authentication of digital documents,” Al-Mustansiriyah J. Sci., vol. 34, no. 3, pp. 50–55, Sep. 2023, doi: 10.23851/mjs.v34i3.1278.

[10] Y. Qin and B. Zhang, “Privacy-preserving biometrics image encryption and digital signature technique using Arnold and ElGamal,” Appl. Sci., vol. 13, no. 14, pp. 8117–8132, 2023, doi: 10.3390/app13148117.

[11] C. Zhan, L. Leng, C.-C. Chang, and J.-H. Horng, “Reversible image fragile watermarking with dual tampering detection,” Electronics, vol. 13, no. 10, Art. no. 10, Jan. 2024, doi: 10.3390/electronics13101884.

[12] D. P. Kusumaningrum, E. H. Rachmawanto, C. A. Sari, and R. P. Pradana, “DWT–SVD combination method for copyrights protection,” Sci J Inf., vol. 7, no. 1, p. 311, 2020, doi: 10.15294/sji.v7i1.21050.

[13] W. Wang, N. Zhang, S. Sun, and W. Wang, “Electronic certificate images forgery detection with electronic certificate images database based on NCC and SSIM algorithms,” in International Conference on Image, Signal Processing, and Pattern Recognition (ISPP 2024), SPIE, Jun. 2024, pp. 924–931. doi: 10.1117/12.3033767.

[14] I. A. Sabilla, M. Meirisdiana, D. Sunaryono, and M. Husni, “Best ratio size of image in steganography using portable document format with evaluation RMSE, PSNR, and SSIM,” in 2021 4th International Conference of Computer and Informatics Engineering (IC2IE), Sep. 2021, pp. 289–294. doi: 10.1109/IC2IE53219.2021.9649198.

[15] Y. Al Najjar, “Comparative analysis of image quality assessment metrics: MSE, PSNR, SSIM and FSIM,” Int. J. Sci. Res. IJSR, vol. 13, no. 3, pp. 110–114, 2024, doi 10.21275/SR24302013533.

[16] Y.-J.-N. Gu, J. Zhang, Y. Piao, L.-J. Deng, and Q. Wang, “Integral imaging reconstruction system based on the human eye viewing mechanism,” Opt. Express, vol. 31, no. 6, pp. 9981–9995, Mar. 2023, doi: 10.1364/OE.484176