

Robust Digital Watermarking for Multimedia Content Authentication in DWT-DCT Domain

Roop Singh^{1*} , Sumit Kumar², Pavan Kumar Shukla³, Priyanka Chandani⁴, Urvashi Gupta⁵, and Lalit Garg⁶

¹Amity Institute of Defence Technology, Amity University, Uttar Pradesh, Noida, India

²Amity School of Engineering and Technology, Amity University, Uttar Pradesh, Noida, India

³School of Engineering and Technology, CGC university, Mohali, India

⁴Bennett University, Greater Noida, Uttar Pradesh, India

⁵Department of Electronics Communication Engineering, Krishna Institute of Engineering Technology, Ghaziabad, Delhi-NCR, Uttar Pradesh, India

⁶Faculty of Information & Communication Technology, University of Malta, Malta, Europe

*Correspondence: Roop Singh, roopsolanki@gmail.com

ABSTRACT- Most of the existing single domain Watermarking schemes suffer with security of multimedia content. To address this limitation, a hybrid watermarking framework integrating DWT and DCT transforms is introduced in this study. The proposed approach initially applies the Arnold transform to the color cover image to strengthen data security through image scrambling. Subsequently, the encrypted image is decomposed using a single-level discrete wavelet transform (DWT), where the selected sub-bands (*LL1* and *HH1*) are utilized for further watermark embedding operations. To achieve a balanced trade-off between visual quality and robustness, the chosen sub-bands are partitioned into 8×8 blocks and transformed using the discrete cosine transform (DCT). Finally, the watermark logo is embedded into the mid-frequency DCT coefficients, resulting in the generation of a secure and imperceptible watermarked image. The performance is measured on SIPI dataset in terms of PSNR, SSIM, NC. The experimental finds demonstrate that the presented method outperforms with the existing relevant schemes.

Keywords: Medical images, Color Images, Watermarking, Security, DWT, DCT.

ARTICLE INFORMATION

Author(s): Roop Singh, Sumit Kumar, Pavan Kumar Shukla, Priyanka Chandani, Urvashi Gupta, and Lalit Garg;

Received: 14/03/26; **Accepted:** 09/07/26; **Published:** 30/09/26;

E- ISSN: 2347-470X;

Paper Id: IJEER 0404B12;

Citation: 10.37391/ijeer.140301

Webpage-link:

<https://ijeer.forexjournal.co.in/archive/volume-14/ijeer-140301.html>



Publisher's Note: FOREX Publication stays neutral with regard to jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

Rapid advancements in digital technologies have significantly enhanced the creation, storage, and distribution of multimedia content [1, 2]. While this widespread availability has improved accessibility, it has also exposed digital data to various security threats, including unauthorized copying, manipulation, forgery, and tampering [3]. Such vulnerability raises serious concerns regarding ownership protection and data integrity. Therefore, it has become essential to develop robust and secure mechanisms that can effectively safeguard multimedia content against illegal access, modification, and redistribution [4, 5].

To address these challenges, several techniques such as steganography, cryptography, and digital watermarking have been proposed for digital content protection [5]. Among these,

digital watermarking has emerged as a highly effective approach due to its ability to embed imperceptible information directly into the host media. This embedded information, which may include text, logos, or authentication codes, enables copyright protection, ownership verification, and tamper detection without significantly degrading the perceptual quality of the original content [6].

The performance of a digital watermarking system is typically evaluated based on three critical factors: imperceptibility, robustness, and security [7]. Imperceptibility refers to the capability of a watermarking system to preserve the original visual appearance of the cover image after the embedding process. An effective watermark should remain visually unnoticeable so that the embedded information does not introduce perceptible distortions or degrade image quality. Robustness refers to the ability of the watermark to resist various intentional and unintentional attacks, such as noise addition, compression, filtering, and geometric distortions. Security in watermarking protects the embedded information from unauthorized detection, modification, or removal, ensuring reliable authentication and tamper resistance. Digital watermarking techniques are broadly classified as robust and fragile based on application requirements. Robust watermarking methods are designed to resist various attacks, ensuring that the embedded watermark remains detectable after modifications, and are commonly used for copyright protection. Fragile watermarking is extremely sensitive to image modifications and is mainly employed for

authentication and tamper identification purposes. [3]. Furthermore, watermarking techniques are classified into blind and non-blind approaches based on the watermark retrieval mechanism. Blind watermarking methods extract the embedded watermark without requiring access to the original host image or the original watermark data, making them more practical for real-world applications. Non-blind methods, however, depend on the availability of original data, which limits their usability. Hence, blind watermarking approaches are generally preferred due to their simplicity and convenience.

Based on the embedding domain, digital watermarking techniques are broadly classified into spatial domain and frequency (transform) domain methods [8]. Spatial domain watermarking methods embed hidden information by directly altering the pixel intensities of the cover image. Popular approaches in this category include least significant bit (LSB) substitution, histogram shifting, prediction error expansion, and difference expansion. These methods are computationally efficient and provide high imperceptibility; however, they generally lack robustness when subjected to common image processing and geometric attacks [9].

In contrast, frequency domain techniques operate by first transforming the host image into a frequency representation, followed by embedding the watermark into selected transform coefficients. The watermarked image is then reconstructed using the inverse transform. Commonly used transforms include DCT, DFT, DWT, and SVD. These methods offer superior robustness and maintain good perceptual quality compared to spatial domain techniques. Due to these advantages, recent research in digital watermarking has increasingly focused on transform domain approaches for developing more reliable and secure watermarking systems [9].

Researchers have proposed numerous watermarking techniques based on individual transform domains as well as hybrid combinations. However, single-domain methods often exhibit limited performance in terms of robustness and imperceptibility. To address these issues, hybrid approaches that integrate multiple transforms have been developed to enhance overall performance. In this context, this paper presents a DWT–DCT-based hybrid watermarking scheme for effective copyright protection. The major contributions of the proposed work are summarized in three aspects.

1. *Hybrid DWT–DCT Framework*: Combines multi-resolution and energy compaction properties to improve performance.
2. *Robust Embedding Scheme*: Ensures high imperceptibility and resistance to common attacks.
3. *Blind Extraction Method*: Enables watermark recovery without requiring the original image.

2. LITERATURE REVIEW

This section reviewed the most relevant and related digital watermarking schemes in both spatial and frequency domain done by researchers. Yasin et al. [10] presented an FPGA-

based parallel processing method using the LSB technique in the spatial domain for video watermarking to ensure copyright protection and content authentication. High speed (139.47 fps), excellent imperceptibility (PSNR 45 dB, SSIM 0.99), hardware-efficient for real-time use. Limited robustness to attacks due to classic LSB fragility. Faheem et al. [11] developed a spatial domain method combining LSB substitution and Canny edge detection for digital image watermarking aimed at authentication. Improves capacity and security by targeting edges, simple implementation. Still vulnerable to noise and compression as LSB-based. Anam et al. [12] presented a pure LSB method in the spatial domain for image watermarking, focusing on copyright protection through high imperceptibility. Superior visual quality (high PSNR), computationally lightweight. Extremely fragile to common attacks like noise or compression.

Spatial domain watermarking schemes offer simplicity, low computational complexity, and high imperceptibility but suffer from inherent fragility against common image processing attacks and manipulations, often requiring hybrid enhancements for practical robustness. To address these issues, researchers developed watermarking schemes in frequency domain.

Roy et al. [13] introduced a robust reversible watermarking technique using DCT and histogram shifting for embedding binary bits into AC coefficients, enabling perfect image recovery and high capacity (4096 bits with PSNR 46.62 dB). Jana et al. [14] devised a robust image watermarking scheme based solely on DCT in JPEG-YCbCr space using Cellular Automata for secure embedding. Further, Alshour et al. [15] developed a secure image watermarking method using IWT and SVD enhanced by chaos models for flexibility and robustness. The existing work is summarized in *table 1*.

3. PRELIMINARIES

This section briefly discusses the most relevant methods to the proposed scheme. The proposed scheme combines DWT–DCT. So here DCT and DWT are discussed how there are used in watermarking.

3.1. Discrete Wavelet Transform

DWT is a multi-scale transform method that separates an image into multiple frequency components for efficient analysis and processing, while preserving both spatial and frequency information [16]. Due to its strong localization capability and energy compaction property, DWT has been extensively adopted in image processing and watermarking systems due to its efficient frequency decomposition capability. In watermarking, DWT improves imperceptibility and robustness by embedding watermark information into suitable frequency sub-bands.

A 1-level 2D- DWT separates an image into four distinct frequency sub-bands, identified as LL, LH, HL, and HH. The LL sub-band contains most of the image energy, whereas the HH sub-band is more sensitive to noise and compression. Therefore, the middle-frequency sub-bands (LH and HL) are

generally preferred for watermark embedding as they provide a better balance between robustness and visual quality. Among various wavelet families, the Haar wavelet is commonly used because of its simplicity and computational efficiency. Fig. 1 demonstrates the 1-level DWT decomposition of the Lena image into four sub-bands.

Table 1. Comparison of spatial and frequency domain watermarking schemes

Author	Used Method	Domain	Application	Limitations
Yasin et al. [10]	LSB Substitution	Spatial Domain	Video copyright protection and authentication	Fragile against attacks, low robustness, highly sensitive to modifications
Anam et al. [12]	LSB Embedding	Spatial Domain	Image copyright protection	Fragile, vulnerable to noise, weak against compression attacks
Roy et al. [13]	DCT + Histogram Shifting	Frequency Domain (DCT)	Reversible image authentication	Limited embedding capacity, fragile against minor image manipulations
Jana et al. [14]	DCT + Cellular Automata	Frequency Domain (DCT)	Robust image watermarking	Singular value issues, computationally intensive
Alshoura et al. [15]	IWT + SVD	Frequency Domain (IWT-SVD)	Secure image protection	False-positive problem, ambiguity due to SVD decomposition

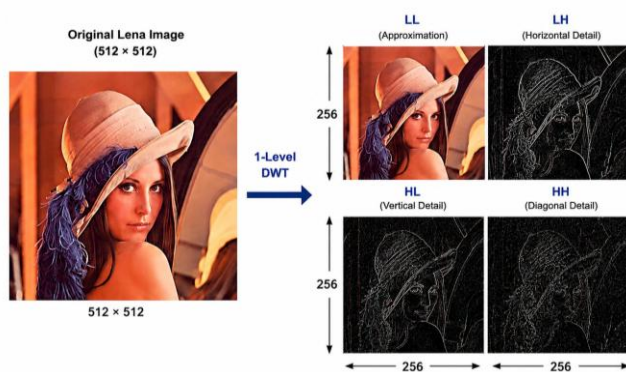


Figure 1. Pictorial representation of 1-level 2D-DWT decomposition of a 512 × 512 Lena image into four sub-bands

3.2. Discrete Cosine Transform

DCT is widely employed in digital image watermarking due to its strong energy compaction capability and robustness against common image processing operations [17]. In DCT-based watermarking, the cover image is converted into the frequency domain, where the transform coefficients are categorized into low-, mid-, and high-frequency regions. The low-frequency coefficients contain the primary visual content and significant structural information of the image whereas the high-frequency components are highly sensitive to noise and compression attacks. Therefore, watermark data are generally embedded into the middle-frequency coefficients to achieve an

effective balance between imperceptibility and robustness. Furthermore, DCT provides improved resistance against JPEG compression, making it a suitable and efficient approach for secure copyright protection and image authentication applications. For a given image represented by X , the forward and IDCT can be expressed as follows. The forward DCT converts the spatial representation into frequency coefficients, while the inverse DCT reconstructs the image from the transformed coefficients. Depending on the application, DCT can be implemented either on the entire image or on non-overlapping image blocks.

$$C(u, v) = \beta(u)\beta(v) \sum_{r=0}^{P-1} \sum_{s=0}^{Q-1} X(r, s) \cos \left[\frac{\pi(2r+1)u}{2P} \right] \cos \left[\frac{\pi(2s+1)v}{2Q} \right]$$

$$X(r, s) = \sum_{u=0}^{P-1} \sum_{v=0}^{Q-1} \beta(u)\beta(v) C(u, v) \cos \left[\frac{\pi(2r+1)u}{2P} \right] \cos \left[\frac{\pi(2s+1)v}{2Q} \right] \quad (1)$$

where $X(r, s)$ denotes the spatial-domain pixel intensity at location (r, s) , and $C(u, v)$ represents the corresponding DCT coefficient in the frequency domain. The parameters P and Q indicate the dimensions of the image. The normalization factors are defined as

$$\beta(u) = \begin{cases} \frac{1}{\sqrt{P}}, & u = 0 \\ \sqrt{\frac{2}{P}}, & u \neq 0 \end{cases} \quad (2)$$

$$\beta(v) = \begin{cases} \frac{1}{\sqrt{Q}}, & v = 0 \\ \sqrt{\frac{2}{Q}}, & v \neq 0 \end{cases} \quad (3)$$

4. A HYBRID DWT-DCT BASED WATERMARKING

The proposed watermarking model is composed of two primary stages, namely watermark embedding and watermark retrieval. A detailed explanation of each stage is presented in the subsequent subsections.

4.1. Watermark Embedding Phase

The watermark insertion procedure of the developed framework is presented in fig. 2. At the beginning, a 512×512 color host image undergoes Arnold scrambling to provide an additional level of security. Subsequently, a single-level DWT is employed to decompose the encrypted image into four frequency sub-bands. The LL and HH components are then segmented into separate 8×8 non-overlapping blocks, followed

by the application of DCT on each block. The watermark information is incorporated into the selected transform coefficients according to the defined embedding strategy. After watermark insertion, inverse DCT and inverse DWT operations are executed to generate the final water-marked image. The embedding pseudocode is shown in *Algorithm 1*.

Algorithm 1. DWT-DCT Based Watermark Embedding

Require:

Original color image I
Watermark logo W

Ensure:

Watermarked image IW

- 1: Input:** Read original image I of size 512×512
- 2: Encrypt the image using Arnold transform:
 $IE = \text{ArnoldEncrypt}(I, t)$
- 3: Apply 1-level DWT on encrypted image:
 $[LL, LH, HL, HH] = \text{DWT}(IE)$
- 4: Divide LL and HH subbands into non-overlapping 8×8 blocks
- 5: **for** each block B_i in LL and HH **do**
 $D_i = \text{DCT}(B_i)$
end for
- 6: Embed watermark bit W_i into selected DCT coefficient:
 $D'_i = D_i + \alpha \times W_i$
- 7: Apply inverse DCT:
 $B_i = \text{IDCT}(D'_i)$
- 8: Reconstruct modified LL and HH sub-bands.
- 9: Apply inverse DWT:
 $IW = \text{IDWT}(LL, LH, HL, HH)$
- 10: Output:** Watermarked image IW

4.2. Watermark Extraction Phase

The watermark extraction phase of the proposed scheme is depicted in *fig. 3*. First, the received watermarked image is encrypted using the same Arnold transform key employed during the embedding process. Next, a 1-level DWT is applied to obtain four sub-bands. The LL and HH sub-bands are then divided into non-overlapping 8×8 blocks, followed by DCT to each block. The embedded watermark information is extracted from the selected DCT coefficients using the predefined extraction rule. Finally, IDCT, IDWT, and decryption operations are performed to recover the embedded watermark logo. The extraction pseudocode is also given in *Algorithm 2*.

Algorithm 2. DWT-DCT Based Watermark Extraction

Require:

Watermarked image IW, secret key K'

Ensure:

Extracted watermark logo W'

- 1: Input:** Read received watermarked image IW
- 2: Encrypt the image using Arnold transform:

- IWE = Arnold Encrypt (IW, K')
- 3: Apply 1-level DWT:
 $[LL, LH, HL, HH] = \text{DWT}(IWE)$
- 4: Divide LL and HH sub bands into non-overlapping 8×8 blocks
- 5: for each block B_i in LL and HH do
 $D_i = \text{DCT}(B_i)$
end for
- 6: Extract watermark bit from selected coefficient:
 $W'_i = (D'_i - D_i) / \alpha$
- 7: Reconstruct extracted watermark logo:
 $W' = \{W'_1, W'_2, \dots, W'_n\}$
- 8: Output:** Extracted watermark logo W'

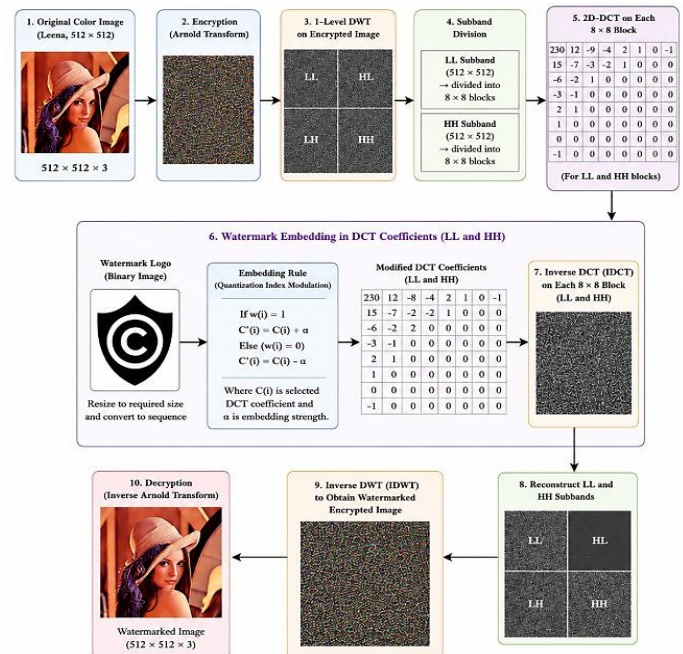


Figure 2. Flowchart of the proposed DWT-DCT based watermark embedding phase

5. RESULT ANALYSIS

The proposed watermarking scheme was evaluated using five standard color images from the SIPI image database, namely Lena, Peppers, Baboon, Airplane, and Sailboat, each having a resolution of 512×512 . In addition, grayscale watermark logo images, including Cameraman, Logo, Fingerprint, Text, and Binary Seal, of size 64×64 were utilized for watermark embedding experiments.

The performance of the proposed watermarking approach was examined in terms of visual quality preservation and resistance against different attacks. PSNR and SSIM metrics were utilized to quantify the perceptual similarity between the original and watermarked images, whereas NC was adopted to evaluate the accuracy of watermark recovery under attack conditions. The corresponding mathematical formulations of these performance measures are provided below. *Fig. 4* presents the host images along with the watermark logos.

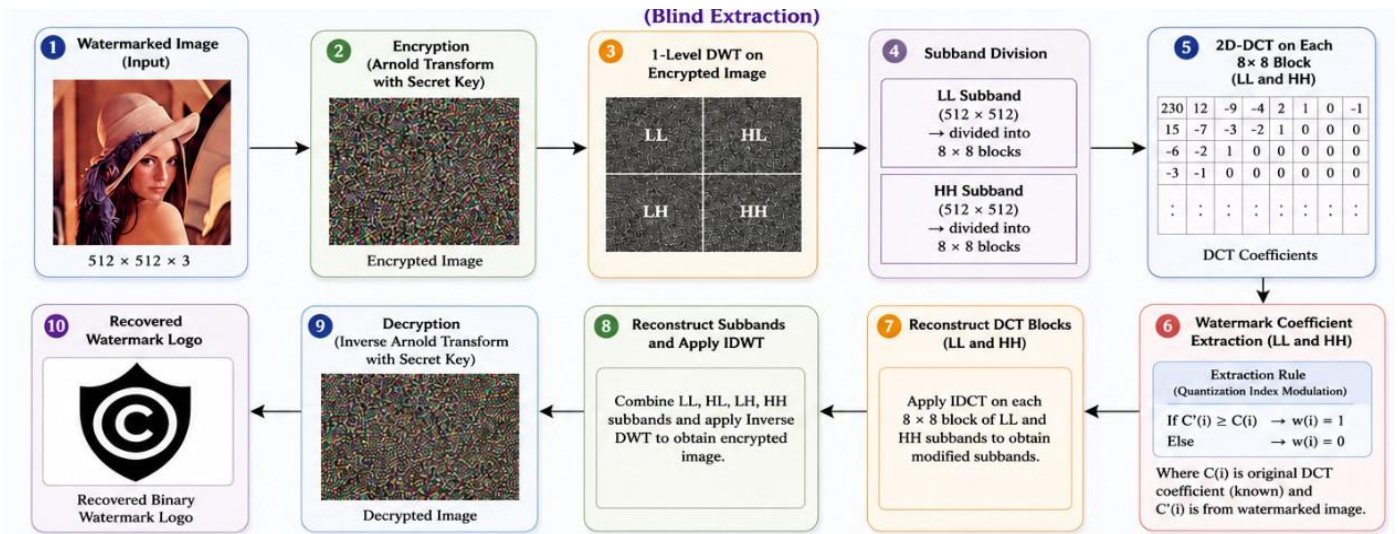


Figure 3. Flowchart of the proposed DWT–DCT based watermark extraction phase



Figure 4. Experimental images used in the proposed watermarking framework: (a) Lena, (b) Airplane, (c) Sailboat, (d) House, (e) Pepper, and (f) Logo watermark

6. PERFORMANCE EVALUATION METRIC

The proposed watermarking framework is assessed using four performance measures, namely PSNR, SSIM, NC, and BER. Among these metrics, PSNR and SSIM are adopted to PSNR quantifies the difference between the original and watermarked images in terms of reconstruction quality. Larger PSNR values correspond to reduced embedding distortion and improved visual similarity. examine the visual fidelity of the watermarked image, while NC and BER are considered for analyzing the robustness and extraction accuracy of the embedded watermark. The formulas for evaluation parameters are given below.

Peak Signal-to-Noise Ratio: PSNR quantifies the difference between the original and watermarked images in terms of

reconstruction quality. Larger PSNR values correspond to reduced embedding distortion and improved visual similarity.

$$PSNR(dB) = 10 \log_{10} \left(\frac{L^2}{MSE} \right) \quad (4)$$

where L denotes the maximum possible pixel intensity value of the image, and MSE indicates the mean.

To squared error between the reference and watermarked images. MSE is calculated by eq. (5)

$$MSE = \frac{1}{PQ} \sum_{x=1}^P \sum_{y=1}^Q [C(x,y) - W(x,y)]^2 \quad (5)$$

where P and Q indicate the height and width of the image, respectively. The terms $C(x,y)$ and $W(x,y)$ correspond to the pixel intensities of the cover image and the watermarked image at location (x,y) .

Structural Similarity Index Measure: SSIM measures the resemblance between the host and water-marked images by analyzing variations in brightness, contrast, and structural information.

$$SSIM(I, I_w) = \frac{(2\mu_I\mu_{I_w} + C_1)(2\sigma_{II_w} + C_2)}{(\mu_I^2 + \mu_{I_w}^2 + C_1)(\sigma_I^2 + \sigma_{I_w}^2 + C_2)} \quad (6)$$

where μX and μY represent the average intensity values of the reference and watermarked images, respectively. The terms σ^2 and σ^2 indicate the corresponding variance values, while σ_{XY} denotes the covariance.

Table 2. Performance analysis of the proposed watermarking scheme

Host Image	Imperceptibility		Robustness	
	PSNR (dB)	SSIM	NC	BER
Lena	48.92	0.9987	0.9991	0.0012
Airplane	47.85	0.9979	0.9985	0.0021
House	48.34	0.9982	0.9989	0.0015
Baboon	46.71	0.9968	0.9974	0.0034
Sailboat	47.96	0.9981	0.9987	0.0018
Average	47.96	0.9979	0.9985	0.0020

between the two images. The parameters C_1 and C_2 are introduced to maintain numerical stability during computation.

Normalized Correlation: NC is employed to quantify the correlation between the embedded watermark and the retrieved watermark. A value approaching unity signifies accurate and reliable watermark extraction.

$$NC = \frac{\sum_{m=1}^R \sum_{n=1}^S A(m, n) B(m, n)}{\sqrt{\sum_{m=1}^R \sum_{n=1}^S A(m, n)^2} \sqrt{\sum_{m=1}^R \sum_{n=1}^S B(m, n)^2}} \quad (7)$$

where R and S denote the dimensions of the water-mark image. The symbols $A(m, n)$ and $B(m, n)$ correspond to the embedded watermark and the recovered watermark values at position (m, n) , respectively.

Bit Error Rate (BER): The Bit Error Rate (BER) is calculated between the embedded watermark $A(m, n)$ and the extracted watermark $B(m, n)$ as follows:

$$BER = (1 / MN) \sum_{m=1}^M \sum_{n=1}^N [A(m, n) \oplus B(m, n)] \quad (8)$$

where $A(m, n)$ and $B(m, n)$ denote the embedded and extracted watermark bits, respectively, and $M \times N$ is the total number of watermark bits. The XOR ($\oplus$) operation gives 1 when the corresponding bits differ and 0 when they are identical. A lower BER indicates better watermark recovery, with $BER = 0$ representing a perfect match.

6.1. Imperceptibility Analysis

Imperceptibility is a key criterion for evaluating the quality of a watermarking scheme, as it measures how effectively the embedded watermark remains visually unnoticeable in the host

image. In this study, imperceptibility is assessed using the Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM). The performance comparison presented in *table 2* demonstrates that the proposed DWT–DCT-based watermarking framework achieves superior visual quality after watermark embedding.

The proposed approach records a maximum PSNR of 48.92 dB and an SSIM value of 0.9987, indicating that the watermark introduces negligible distortion while preserving the structural information of the original image. Furthermore, the method exhibits a maximum Normalized Correlation (NC) of 0.9991 and a minimum Bit Error Rate (BER) of 0.0012, confirming the accurate extraction of the embedded watermark even under various conditions. On average, the proposed technique achieves 47.96 dB PSNR, 0.9979 SSIM, 0.9985 NC, and 0.0020 BER, demonstrating its ability to maintain high image fidelity along with reliable watermark recovery. These results validate the effectiveness and stability of the proposed watermarking framework.

6.2. Robustness Analysis

The proposed framework evaluates robustness using NC and BER metrics. Robustness indicates the similarity between the original watermark logo and the extracted logo. A higher NC value near 1 and a lower BER approaching zero demonstrate the effectiveness of the proposed method. Robustness is evaluated qualitatively and quantitatively. Qualitative results and quantitative performance are shown in *fig. 5* and *table 3*.

Attack Name	Attacked Watermarked Lena Image	Extracted Watermark
1. Gaussian Noise (0, 15%)		
2. Salt & Pepper Noise (10%)		
3. Poisson Noise		
4. Median Filtering (5 × 5)		
5. Average Filtering (5 × 5)		
6. Wiener Filtering (5 × 5)		
7. Gaussian Filtering (5 × 5)		

Attack Name	Attacked Watermarked Lena Image	Extracted Watermark
8. Rotation (45°)		
9. Translation (30, 30)		
10. Cropping (Center 75%)		
11. Gamma Correction ($\gamma = 0.5$)		
12. Sharpening		
13. Histogram Equalization		

Figure 5. Qualitative analysis of robustness over various attacks on Lena image

Table 3 presents the quantitative robustness analysis of the proposed DWT–DCT based watermarking scheme in terms of NC and BER under different attacks. The obtained results demonstrate that the proposed framework maintains high NC values and low BER values for most image processing and enhancement attacks. The best robustness performance is achieved against Gamma Correction attack with an NC value of 0.9972 and BER value of 0.0028, followed by Wiener Filtering with NC and BER values of 0.9968 and 0.0031, respectively. In contrast, geometric attacks such as Cropping and Rotation produce relatively lower NC values of 0.9798 and 0.9824 along with higher BER values of 0.0194 and 0.0173, respectively, indicating comparatively degraded extraction performance. Furthermore, the proposed scheme achieves an average NC value of 0.9927 and average BER value of 0.0071, which confirms the strong robustness and reliability of the developed watermarking framework against various attacks. Furthermore, Fig. 5 illustrates the robustness performance of the proposed DWT–DCT based watermarking framework under various image processing, filtering, geometric, and enhancement attacks. It can be observed that the extracted watermark logos remain visually recognizable for most attacks, demonstrating the strong robustness and reliable watermark recovery capability of the proposed method.

Table 3. Robustness analysis of the proposed watermarking method under various attacks

Attack Category	Configuration	NC	BER
Rotation	(45°)	0.9824	0.0173
Gaussian Filtering	(5 × 5)	0.9957	0.0041
Histogram Equalization	–	0.9934	0.0062
Salt & Pepper Noise	(10%)	0.9885	0.0112
Translation	(30, 30)	0.9869	0.0126
Wiener Filtering	(5 × 5)	0.9968	0.0031
Cropping	(25%)	0.9798	0.0194
Sharpening	–	0.9961	0.0037
Gaussian Noise	(0, 15%)	0.9921	0.0078
Average Filtering	(5 × 5)	0.9951	0.0047
Gamma Correction	($\gamma = 0.5$)	0.9972	0.0028
Poisson Noise	–	0.9942	0.0059
Median Filtering	(5 × 5)	0.9964	0.0035
Overall Average	–	0.9927	0.0071

6.3. Comparative Analysis with Recent Methods

Table 4 compares the visual quality performance of the developed watermarking approach with previously reported techniques using the Lena image. The proposed hybrid DWT–DCT framework attains a PSNR of 48.92 dB and an SSIM of 0.9987, outperforming the methods presented by Yasin et al. [10], Roy et al. [13], and Alshoura et al. [15]. These findings confirm that the embedding process introduces minimal visual distortion while effectively preserving structural image characteristics. The robustness comparison under different attacks is summarized in table 5 using NC and BER performance measures. The proposed scheme exhibits superior extraction accuracy by producing consistently larger NC values along with reduced BER values across all attack scenarios. Moreover, the framework achieves an average NC of 0.9927 and an average BER of 0.0071, indicating strong resistance against noise, filtering, and geometrical distortions.

Table 4. Comparative analysis of imperceptibility performance over Lena image

Method	PSNR (dB)	SSIM
Yasin et al. [10]	42.18	0.9854
Roy et al. [13]	44.76	0.9912
Alshoura et al. [15]	46.03	0.9941
Proposed DWT–DCT Method	48.92	0.9987

7. CONCLUSION

The study presented a hybrid DWT–DCT based watermarking framework for secure and robust image copyright protection. Arnold transform was employed to enhance security, while watermark embedding in selected transform coefficients preserved image quality and extraction reliability. Experimental results demonstrated strong imperceptibility and robustness against different image processing and geometrical attacks. Comparative evaluation also indicated improved NC

and BER performance compared with existing methods. Future research may focus on integrating optimization and deep learning techniques to improve resilience against advanced attacks and extend the framework toward real-time image and video watermarking applications.

Conflicts of Interest: "The authors declare no conflict of interest."

REFERENCES

- [1] Dubolia, Rakhi, et al. "Digital image watermarking by using discrete wavelet transform and discrete cosine transform and comparison based on PSNR." *2011 International conference on communication systems and network technologies*. IEEE, 2011.
- [2] Singh, Roop, Alaknanda Ashok, and Mukesh Saraswat. "Robust video watermarking in frequency domain for copyright protection." *Proceedings of the 2021 Thirteenth International Conference on Contemporary Computing*. 2021.
- [3] Abdulhakeem O Mohammed, Haval I Hussein, Ramadhan J Mstafa, and Adnan M Abdulazez. A blind and robust color image water-marking scheme based on dct and dwt domains. *Multimedia Tools and Applications*, 82(21):32855–32881, 2023.
- [4] Rakhi Dubolia, Roop Singh, Sarita Singh Bhadoria, and Rekha Gupta. Digital image watermarking by using discrete wavelet transform and discrete cosine transform and comparison based on psnr. In *2011 International conference on communication systems and network technologies*, pages 593–596. IEEE, 2011.
- [5] Roop Singh, Raju Pal, Himanshu Mittal, and Deepak Joshi. Multi-objective optimization-based medical image watermarking scheme for securing patient records. *Computers and Electrical Engineering*, 118:109303, 2024.
- [6] Thien Huynh-The, Cam-Hao Hua, Nguyen Anh Tu, Taeho Hur, Jaehun Bang, Dohyeong Kim, Muhammad Bilal Amin, Byeong Ho Kang, Hyonwoo Seung, and Sungyoung Lee. Selective bit embedding scheme for robust blind color image watermarking. *Information Sciences*, 426:1–18, 2018.
- [7] Roop Singh, Raju Pal, and Deepak Joshi. Optimal frame selection-based watermarking using a meta-heuristic algorithm for securing video content. *Computers and Electrical Engineering*, 121:109857, 2025.
- [8] B Bolourian Haghighi, Amir Hossein Taherinia, and Reza Mon-sefi. Trlf: An effective semi-fragile watermarking method for tam-per detection and recovery based on lwt and fnn. *arXiv preprint arXiv:1802.07119*, 2018.
- [9] Seyyed Hossein Soleymani, Amir Hossein Taherinia, and Amir Hossein Mohajerzadeh. Waca: a new blind robust watermarking method based on arnold cat map and amplified pseudo-noise strings with weak correlation. *Multimedia Tools and Applications*, 78(14):19163–19179, 2019.
- [10] HM Yasin, AB Sallow, and RZ Mahmood. High-speed fpga-based video watermarking using lsb technique in the spatial domain. *Int. J. Intell. Syst. Appl. Eng.*, 12:644–653, 2024.
- [11] Zaid Bin Faheem, Abid Ishaq, Furqan Rustam, Isabel de la Torre Diez, Daniel Gavilanes, Manuel Masias Vergara, and Imran Ashraf. Image watermarking using least significant bit and canny edge detection. *Sensors*, 23(3):1210, 2023.
- [12] Rizal Khoirul Anam. Robustness and imperceptibility analysis of hybrid spatial-frequency domain image watermarking. *arXiv preprint arXiv:2511.10245*, 2025.
- [13] Soumitra Roy, Varish Naushad, Syed Irfan Yaqoob, Md Sham-sul Haque Ansari, and Abu Taha Zamani. Dct-based robust re-versible watermarking technique based on histogram modification. *International journal of electrical and computer engineering systems*, 16(6):473–484, 2025.
- [14] Manasi Jana and Biswapati Jana. A new dct based robust image watermarking scheme using cellular automata. *Information Security Journal: A Global Perspective*, 31(5):527–543, 2022.
- [15] Wafa Hamdan Alshoura and Moatsum Alawida. Secure and flexible image watermarking using iwt, svd, and chaos models for robustness and imperceptibility. *Scientific Reports*, 15(1):7231, 2025.
- [16] Fauzia Yasmeen and Mohammad Shorif Uddin. An efficient water-marking approach based on ll and hh edges of dwt–svd. *SN Computer Science*, 2(2):82, 2021.
- [17] Zihan Yuan, Decheng Liu, Xueting Zhang, and Qingtang Su. New image blind watermarking method based on two-dimensional discrete cosine transform. *Optik*, 204:164152, 2020.



© 2026 by Roop Singh, Sumit Kumar, Pavan Kumar Shukla, Priyanka Chandani, Urvashi Gupta, and Lalit Garg. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).