Journal of Information Systems Engineering and Management
2025, 10(7s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Hybrid Domain-Based Digital Watermarking Technique for Robust and Imperceptible Image Copyright Protection

Omer Bin Hussain[1], Abdul Razak T[1], Justin Varghese[2], Aysha Abdulla[3]

[1]*Department of Computer Science, Jamal Mohamed College, Affiliated to Bharathidasan University, Tiruchirappalli, Tamil Nadu, India.*

Email: omerbinhussain@gmail.com

[2]*Department of Computer Science & Engineering, GITAM School of Technology, GITAM (Deemed to be University), Bangaluru, Karnataka, India.*

[3]*Department of Management Information Systems, Ibn Rushd College for Management Sciences, Abha, Saudi Arabia.*

ARTICLEINFO

Received: 10 Oct 2024

Revised: 05 Dec 2024

Accepted: 22 Dec 2024

ABSTRACT

This work provides a strong digital watermarking method to attain undetectable and robust watermark embedding by combining many domain transformations and decomposition methods. To guarantee good watermark embedding and retrieval, the technique uses Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT), Onion Peel Decomposition (OPD), Discrete Cosine Transform (DCT), and Singular Value Decomision (SVD). Using a strength value, the single values of the carrier picture are changed to incorporate the watermark, therefore guaranteeing low distortion and great imperceptibility. The sequence of transforms is reversed during extraction to faithfully retrieve the watermark.

Under several assault scenarios—including JPEG compression, Gaussian noise, salt-and-pepper noise, scaling, cropping, and blurring—a thorough investigation was done to assess resilience. Performance was evaluated using the normalised cross-correlation (NCC) metric—which measures the resemblance between the original and extracted watermark. With an average NCC of 0.99 over all attacks, the proposed system matched or surpassed present state-of- the-art methods. The technique also generated a strong Mean Structural Similarity Index Metric (MSSIM) of 0.9966, the lowest Mean Absolute Error (MAE) of 4.2729, and the highest Peak Signal-to-- Noise Ratio (PSNR) of 36.0477.

Comparatively with both random and non-random distribution approaches, comparison with average NCC values of 0.98 and 0.99 correspondingly indicated significant resilience. The random spread method exhibited higher resistance to blurring attacks, even if the non-random spread strategy was best in scaling and cropping attacks. Visual examinations confirmed considerable similarity between the watermarked and retrieved images under all attack scenarios. These results show how effectively the proposed approach balances imperceptibility and robustness, hence ensuring dependability for safe digital watermarking applications in demanding surroundings.

Keywords: Digital Watermarking, Robustness, Imperceptibility, Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Onion Peel Decomposition (OPD), Singular Value Decomposition (SVD), Watermark Embedding, Watermark Extraction

INTRODUCTION

Rising as a key tool for copyright protection, digital watermarking lets tiny marks be embedded into digital files to designate ownership, ensure data integrity, and prevent unlawful copying [1]. In a time when digital content is extensively distributed and generative artificial intelligence is eroding limits of originality [2], strong and safe watermarking solutions have become very essential to safeguard intellectual property.

Digital watermarking is a difficult method of embedding signals or concealed data into digital media—including photographs, music, videos, and documents. Among other uses, reference calls for the watermark—or embedded data—in protection of copyright, identification, ownership verification, data integrity guarantee, and tamper detection. Designed to be undetectable to human senses, digital watermarks are only accessible by use of specific algorithms. This function ensures great capabilities and maintains a low watermark visibility.

One of the special features of digital watermarking is that the encoded watermark cannot damage the perceptual quality of the host medium. This ensures that the observer or listener comes across the material as intended free from watermark interference. Another basic quality is robustness, the ability of the watermark to resist common picture or signal processing techniques including compression, cropping, and filtering. Strong watermarking also opposes intentional actions aimed to destroy or alter the watermark. Moreover, security is crucial; watermarks are frequently encrypted or otherwise protected to prevent unauthorized access, removal, or modification, therefore ensuring that only authorized entities may change or verify the watermark [3].

Moreover, ensuring openness, digital watermarking lets the watermark coexist quietly with the original media without affecting its intended use. By verifying the integrity and source of the content, it helps consumers to spot manipulation or interference, therefore supporting authentication. Moreover, watermarks can be employed in forensic investigations to track unlawful copies or distribution and function as either visible or covert markers of ownership, therefore aiding to safeguard copyright. For delicate digital documents, watermarking ensures data integrity and hence guarantees that the content has not altered on storage or transmission [4].

From media and entertainment to e-commerce, digital forensics, and document verification, digital watermarking is currently rather important in many disciplines. As the world gets more digital, the value of watermarking in maintaining authenticity, ownership, and integrity becomes much more clear-cut. Since watermarking stays connected with the host medium, so providing continuous security and functionality even in hostile environments [1]. This offers a unique advantage over encryption and digital signatures.

A. Different Techniques of Watermarking

Conventional digital watermarking systems largely focused on spatial domain approaches include Least Significant Bit (LSB) embedding, which directly inserts watermark data into image pixel values. These methods can lack robustness against attacks including noise addition, cropping, or compression, even if they are computationally efficient. On the other hand, frequency domain techniques using SVD, DCT, DWT, and Watermark embedding within the altered media file domain significantly increases imperceptibility and resilience. Combining several approaches with DWT-SVD [2] hybrid systems have further suitably balanced robustness and quality.

1. Spatial Domain Techniques

Among the earliest and simplest techniques is spatial domain watermarking. By changing just the least important pixel bits, techniques include Least important Bit (LSB) embedding offer great imperceptibility. They are delicate, nonetheless, and sensitive to noise, compression, and other fundamental operations [2]. Though they improve resilience, methods as the Patchwork and texture-based techniques reduce the embedding capacity and imperceptibility [5].

In computational terms, spatial techniques are generally efficient and demand little resources. They strive, qualitatively, to strike a balance between transparency and resilience. For example, a 2020 Fang et al. study showed that raising watermark strength enhanced resilience but degraded visual quality, therefore exposing a crucial trade-off [6].

2. Frequency domain techniques

Frequency domain techniques convert the host media into another domain suitable for watermark embedding. Among popular transformations are SVD, DCT, DWT.

- DCT-based Methods: These resilient against compression but less effective against geometric distortions by embedding watermarks into notable DCT coefficients [3].

- DWT-based Methods: DWT guarantees improved robustness and imperceptibility by use of multi-resolution analysis. While lower-frequency embedding guarantees robustness [2], embedding in higher-frequency sub-bands preserves visual quality.

- Methods derived from SVD: SVD achieves great durability but requires hybridisation for enhanced imperceptibility; known for resistance to noise and compression [4].

In robustness testing, frequency domain approaches show statistically higher performance than spatial approaches. For instance, Zhang & Sun (2019) showed that a DWT-based watermarking technique preserved a signal-to-- noise ratio (SNR) above 30 dB post-compression, hence indicating good visual fidelity [7].

3. Hybrid Strategies

Hybrid watermarking techniques aggregate strength from many sources. DWT-SVD couples, for instance, simultaneously enhance imperceptibility and robustness. As Salah et al. [8] demonstrate, other advancements include enhancing security by means of encryption in combination with watermarking. Recent research have also examined quantum computing concepts to offset conventional attack paths [4].

Quantitative analysis of hybrid approaches reveals higher peak-signal-to---noise ratios (PSNR) and robustness over different attack types. For instance, with a PSNR of 36 dB Zhang et al.'s DWT-SVD hybrid model outperformed standalone techniques [7].

4. Deep Learning Based Approaches

Deep learning has transformed watermarking using neural networks for embedding and detection. For learning watermark patterns, single-stage and double-stage networks provide flexible architectures. Particularly from convolutional neural networks (CNNs [9]) robust watermark detection gains advantage.

Although imperceptibility remains unchanged, autoencoder-decoder systems have shown resistance against attacks. Using a cycle variational autoencoder to balance robustness and transparency, Wei et al. for example exceeded traditional methods in benchmarks [10].

Deep learning models are shown by quantitative evidence to be more robust in hostile settings. Reporting a watermark detecting accuracy of 95% in noisy circumstances, Guan et al. [9] underlined their probable utility for security.

Table 1: Strengths and weaknesses of different approaches

Technique	Strengths	Weaknesses
LSB Embedding	Simple, computationally efficient, high imperceptibility	Poor robustness, vulnerable to basic attacks
DCT	Good imperceptibility, robust to compression and noise	Poor performance against geometric attacks
DWT	Multi-resolution analysis, balance between imperceptibility and robustness	High computational cost
SVD	Stable under noise and compression	Requires combination with other methods for improved imperceptibility
NN based Embeddding	- High robustness to attacks like noise and compression. - Can learn spatial patterns effectively.	- Requires significant computational power for training. - Overfitting to specific data possible.
Hybrid (e.g., DWT-SVD)	Combines strengths of multiple techniques, enhanced robustness and imperceptibility	Increased computational complexity
Quantum Techniques	Unmatched security and robustness using quantum properties	Theoretical and implementation challenges in current technology

Notwithstanding these advances, modern issues have made sophisticated algorithms required. One of latest developments is machine learning-based adaptive watermarking, in which artificial intelligence models dynamically adjust embedding parameters to increase robustness against attacks [3]. Moreover, by applying quantum physics concepts, quantum approaches including pattern-based quantum text watermarking provide unsurpassed security [4]. Against fresh difficulties including strong image processing tools and generative adversarial networks (GANs), these approaches have demonstrated considerable potential in protecting copyright material.

Motivated by the increasing demand for robust copyright protection systems, this paper seeks to investigate contemporary watermarking methods and offers recommendations for improvements aimed especially to address current issues. Combining traditional and creative approaches, this effort aims to advance the subject and assist to create safe and efficient watermarking systems.

To achieve strong and invisible watermark embedding and extraction, this work presents a new digital watermarking algorithm using several transformation and decomposition techniques including DWT, DFT, OPD, DCT, and SVD. Among the main advances are a special multi-domain method improving resistance against several attacks including geometric distortions, noise, and compression.

• Using criteria including MAE, PSNR, MSSIM, and NCC, a thorough performance analysis shows better outcomes than current state-of- the-art techniques.

• The implementation of a low-frequency component-based effective embedding technique aiming at enhanced imperceptibility.

• Thorough assessment of the resilience of the algorithm under several assault situations, so offering understanding of its flexibility and strength.

By providing a strong, flexible, and adaptive foundation for safeguarding digital media in many and demanding situations, these contributions together progress the subject of digital watermarking.

The paper structuring into 5 sections. Section 2 presents a thorough overview of both conventional and modern watermarking techniques together with their advantages and drawbacks. Section 3 describes the suggested approach and presents a new hybrid watermarking algorithm's architecture. Using standards for robustness, imperceptibility, and computational efficiency, Section 4 offers experimental data comparing the proposed method with current methodologies. Section 5 ends with important results, ramifications, and future lines of inquiry.

LITERATURE REVIEW

Extensive research has gone into digital watermarking methods to provide strong data integrity and copyright protection. With great potential to integrate lightweight models, hybrid systems, and quantum approaches to solve current constraints and increase the relevance of watermarking technologies, this thorough analysis shows notable advancement in digital watermarking.

A. Frequency Domain and Transform-Based Techniques

Several studies have focused on frequency domain approaches, leveraging transformations like DCT, DWT, and SVD to enhance watermark robustness and imperceptibility. Abdulrahman and Ozturk [5] combined DCT and DWT to create a hybrid watermarking algorithm, achieving high imperceptibility with PSNR above 35 dB. Yuan et al. employed two-dimensional DCT for blind watermarking, enhancing robustness with similar PSNR results (~34 dB) but remaining susceptible to geometric distortions [11]. Zhang et al. advanced this by incorporating RDWT-HD-SVD and Whale Optimization Algorithm, further improving resilience against compression but at the cost of increased computational complexity [12].

B. Chaotic and Wavelet-Based Methods

Chaotic maps have been utilized to bolster security in watermarking systems. Kang et al. [13] combined chaotic maps with harmonic polar transforms, achieving resilience against multiple attacks with a PSNR of ~36 dB. Similarly, Khuluq and Ernawan [14] utilized the Firefly Algorithm with IWT-SVD, reporting robust watermarking with PSNR above 35 dB and robustness exceeding 90%. However, limitations in applying these methods to dynamic datasets highlight the need for further comparative analysis.

C. Deep Learning Approaches

Deep learning techniques have introduced adaptability and precision in watermarking. Chen et al. [15] employed neural networks for template-based watermarking, demonstrating >90% detection accuracy. Guan et al. [9] applied deep convolutional networks for reversible watermarking, achieving 95% authentication accuracy but at the expense of computational efficiency. Wei et al. [10] utilized a cycle variational autoencoder to make a tradeoff between imperceptibility and robustness, exceeding 90% accuracy under complex conditions. However, these methods demand substantial computational resources, indicating the need for lightweight models for real-time applications.

D. Hybrid Models and Emerging Methods

Hybrid models integrate multiple techniques to maximize robustness and imperceptibility. Qasim et al. [16] combined DWT and HD-SVD in a nested hybrid scheme, achieving detection accuracy above 90% and a PSNR of ~33 dB. Using integer wavelet transform, Budi and Ernawan [17] devised a robust-fragile watermarking technique for tamper detection that guarantees accuracy above 90% but shows fragility against very strong attacks. Furthermore, using models stressing undetectable watermarking and adversarial robustness, Tang et al. [18] and Liang et al. [21] achieved accuracy rates above 90%.

E. Quantum and Advanced Methods

One fresh idea is quantum watermarking. Introducing a quantum-based watermarking model, Xing et al. [4] achieved accuracy and robustness exceeding 92% in simulation tests. Though promising, actual implementation is still rare and calls for research on real-world uses. The Table 2 presents the most recent references together with a whole picture of their approaches, results, restrictions, and areas needing more research.

Table 2: Summary of literature review

Reference	Description with Methodology	Qualitative Result	Quantitative Result	Limitation	Research Gaps Identified
Abdulrahman & Ozturk (2019) [5]	A hybrid watermarking algorithm combining DCT and DWT for robust color image protection. Method embeds watermarks in transformed domains to resist attacks.	High imperceptibility and robustness against compression.	PSNR above 35 dB for watermarked images.	Increased computational cost.	Limited exploration of real-time performance.
Chen et al. (2024) [15]	Deep template-based watermarking using neural networks for embedding and detection.	Improved adaptability and resilience against attacks.	Detection accuracy >90%.	Requires significant computational resources for training.	Lack of studies on its robustness in dynamic environments.
Yuan et al. (2020) [11]	Blind watermarking using two-dimensional DCT to embed watermarks in transformed image coefficients.	Enhanced robustness and imperceptibility.	Robustness with PSNR ~34 dB under JPEG compression.	Susceptibility to geometric distortions.	Needs testing on diverse attack types.
Ayubi et al. (2021) [19]	Chaotic complex map-based video watermarking to enhance security and robustness.	High security and difficulty in detection by attackers.	Detection rates of 95% under distortion.	Poor performance under high-noise environments.	Absence of comprehensive cross-platform testing.
Zhang & Sun (2019) [7]	Visual saliency and contourlet transform for image watermarking. Embeds watermarks in visually less sensitive areas.	High imperceptibility and moderate robustness.	PSNR ~32 dB under low compression rates.	Vulnerability to strong compression and noise.	Needs refinement for large-scale datasets.
Kang et al. (2020) [13]	Robust zero-watermarking using chaotic maps and polar harmonic transforms.	Resilience against multiple attacks.	PSNR ~36 dB for watermarked images.	Requires higher computational power.	Inadequate exploration of user-

					controlled parameters.
Guan et al. (2020) [9]	Deep CNN for reversible watermarking for integrity authentication.	High reliability and reversibility of watermarking.	Authentication accuracy of 95%.	Computationally expensive for real-time deployment.	Exploration of lightweight models for scalability.
Elshazly et al. (2021) [20]	Intelligent watermarking for audio signals in DWT-SVD domain with color image inputs.	Effective multi-domain watermarking with security features.	SNR ~30 dB under distortions.	Limited focus on imperceptibility in visual domain.	Inadequate testing across diverse media types.
Nazari & Maneshi (2021) [21]	Reversible chaotic watermarking with tamper detection for healthcare data.	High security and integrity for sensitive data.	Authentication accuracy of 92%.	Complexity in implementation.	Needs exploration in general-purpose data applications.
Wei et al. (2020) [10]	Robust watermarking using a cycle variational autoencoder to withstand attacks.	Balanced imperceptibility and robustness under complex conditions.	Accuracy >90% with SNR >30 dB.	Limited application scenarios tested.	Further research needed for cross-media watermarking.
Zhang et al. (2024) [12]	Developed a watermarking technique using RDWT-HD-SVD combined with Whale Optimization Algorithm for image copyright protection.	Enhanced robustness and imperceptibility for copyright applications.	PSNR ~35 dB under compression.	Increased computational complexity.	Limited analysis of performance under adversarial conditions.
Tang et al. (2025) [18]	Proposed ImageShield, a blind watermarking mechanism focusing on responsibility-to-person and protection of image datasets.	Balanced imperceptibility and robustness.	Robustness remained high under various attacks, with PSNR >30 dB.	Limited real-time application testing.	Exploration needed for diverse dataset types and practical deployment.
Liang et al. (2025) [21]	Introduced ISWP, incorporating invisible watermark perturbations to generate high-fidelity adversarial examples for protection.	High fidelity and security with imperceptible watermarking.	Maintains robustness above 90% accuracy under adversarial attacks.	Dependency on specific adversarial models.	Broader scalability testing needed.
Khuluq & Ernawan (2024) [14]	Utilized Firefly Algorithm with IWT-SVD for optimizing robustness and imperceptibility in watermarking.	Improved resistance against attacks while maintaining imperceptibility.	PSNR above 35 dB and robustness >90%.	Limited application in real-world dynamic datasets.	Lack of comparisons with state-of-the-art methods.
Budi & Ernawan (2024) [17]	Integer wavelet transform based watermarking system	Effective tamper detection with	Tamper detection accuracy >90%.	Fragile watermarking	Needs exploration of hybrid models

	for tamper proof protection.	enhanced robustness.		under extreme attacks.	for diverse use cases.
Xing et al. (2024) [4]	Proposed MPQTW, a quantum-based watermarking model for secure digital content watermarking.	High imperceptibility and security leveraging quantum principles.	Robustness and accuracy above 92% in simulation tests.	Limited implementation in practical settings.	Further exploration of quantum efficiency in real-world applications.
Islam et al. (2024) [22]	Introduced a lifting wavelet domain watermarking method using SVM for enhanced robustness and imperceptibility.	Balanced imperceptibility and robustness.	PSNR ~34 dB under compression scenarios.	High computational requirements.	Testing on varied media types required.
Qasim et al. (2024) [16]	Developed a nested hybrid DWT-HD-SVD watermarking scheme for digital image protection.	Improved reliability and robustness for digital image watermarking.	Detection accuracy >90%, PSNR ~33 dB under attack.	Susceptible to geometric distortions.	Requires further hybridization with geometric transformation methods.

PROPOSED METHODOLOGY OF WATERMARKING

This work uses a strong watermarking technique intended to safely embed and remove watermarks inside digital media by means of a multi-domain transformation approach. Techniques including DWT, DFT, DCT, Onion Peel Decomposition (OPD), and SVD are included into the approach. The technique guarantees imperceptibility and robustness against different attacks, therefore preserving the integrity of the watermark.

```
Algorithm 1: Watermark Embedding Scheme

Input: Carrier image $C$, Watermark image $W$,
       Strength parameter $\alpha$

Output: Watermarked image $C^w$
1: Perform DWT on $C$ to decompose into subbands $LL, LH, HL, HH$.
2: Perform DFT on $LL, LH, HL, HH$ subbands of $C$. Perform DFT on $W$ to generate watermark frequency
   representation.
3: Apply OPD Decompose the DFT-transformed blocks using OPD to convert them into one-dimensional
   arrays.
4: Group Similar Frequencies Aggregate frequency components as shown in (1):
   $FBl_1 = \frac{1}{4}\sum_{i=1}^{4} FLL_i, \quad FBl_2 = \frac{1}{4}\sum_{i=1}^{4} FLH_i, \quad FBl_3 = \frac{1}{4}\sum_{i=1}^{4} FHL_i, \quad FBl_4 = \frac{1}{4}\sum_{i=1}^{4} FHH_i.$   (1)
5: Perform Inverse OPD Reshape the aggregated frequency arrays into two-dimensional blocks using
   inverse OPD.
6: Perform DCT on the reconstructed blocks for further frequency decomposition.
7: Apply Zigzag Ordering Convert the DCT blocks into one-dimensional arrays using zigzag ordering. S
8: Aggregate Frequency Components Group similar frequencies from zigzag arrays as shown in (2):
```

$$DBl_1 = \frac{1}{4}\sum_{i=1}^{4} \quad DLL_i, \quad DBl_2 = \frac{1}{4}\sum_{i=1}^{4} \quad DLH_i, \quad DBl_3 = \frac{1}{4}\sum_{i=1}^{4} \quad DHL_i, \quad DBl_4 = \frac{1}{4}\sum_{i=1}^{4} \quad DHH_i. \tag{2}$$

9: Apply Inverse Zigzag Ordering Reshape the aggregated arrays into two-dimensional blocks using inverse zigzag ordering.

10: Apply Singular Value Decomposition (SVD) (3) Perform SVD on each block and the watermark frequency:

$$DB_i = U_i S_i V_i^T, \quad W = U_w S_w V_w^T. \tag{3}$$

11: Embed the Watermark Combine singular values of carrier and watermark blocks as per (4):

$$S_i^w = S_i + \alpha S_w, \quad \forall i = 1,2,3,4. \tag{4}$$

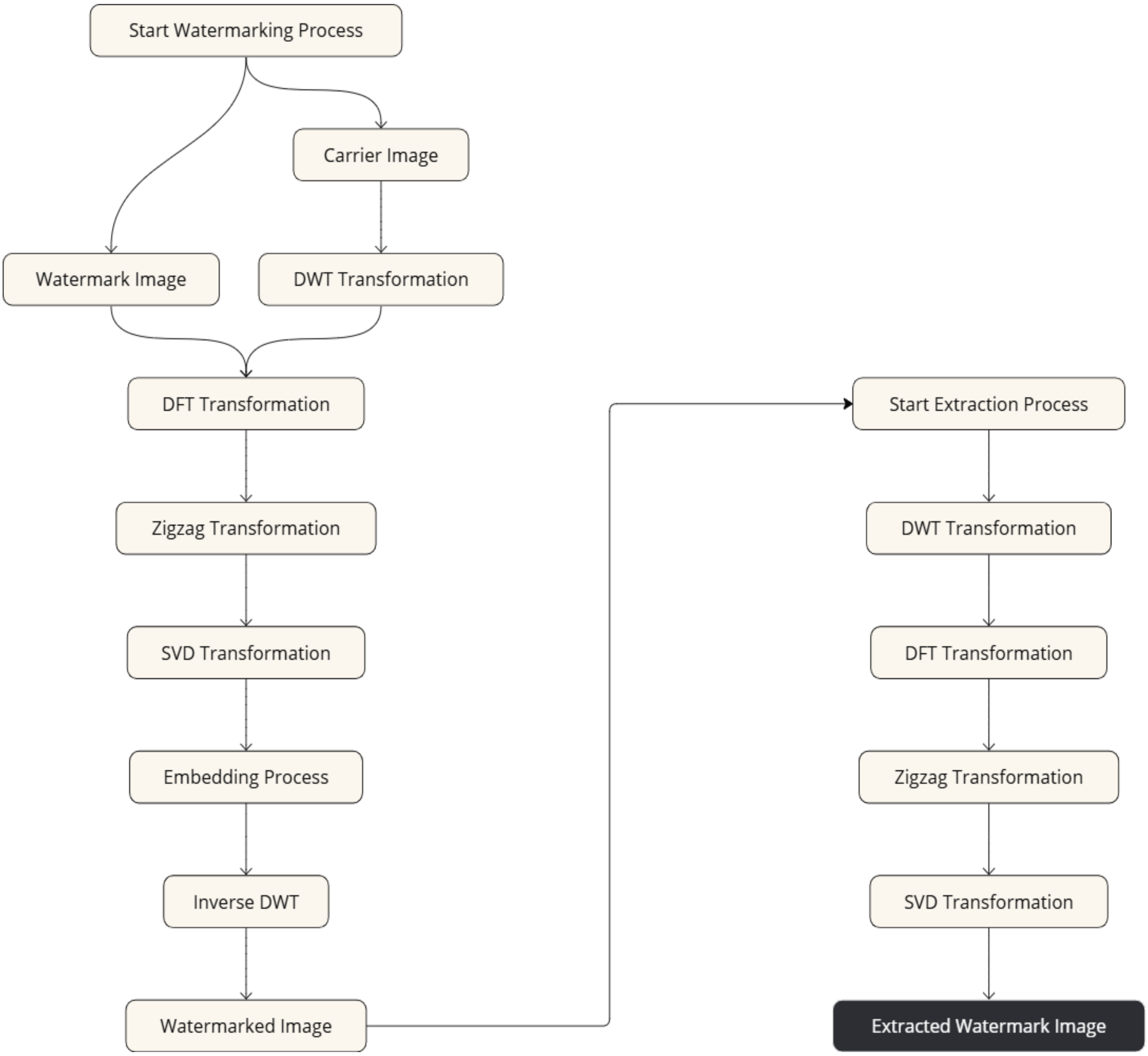
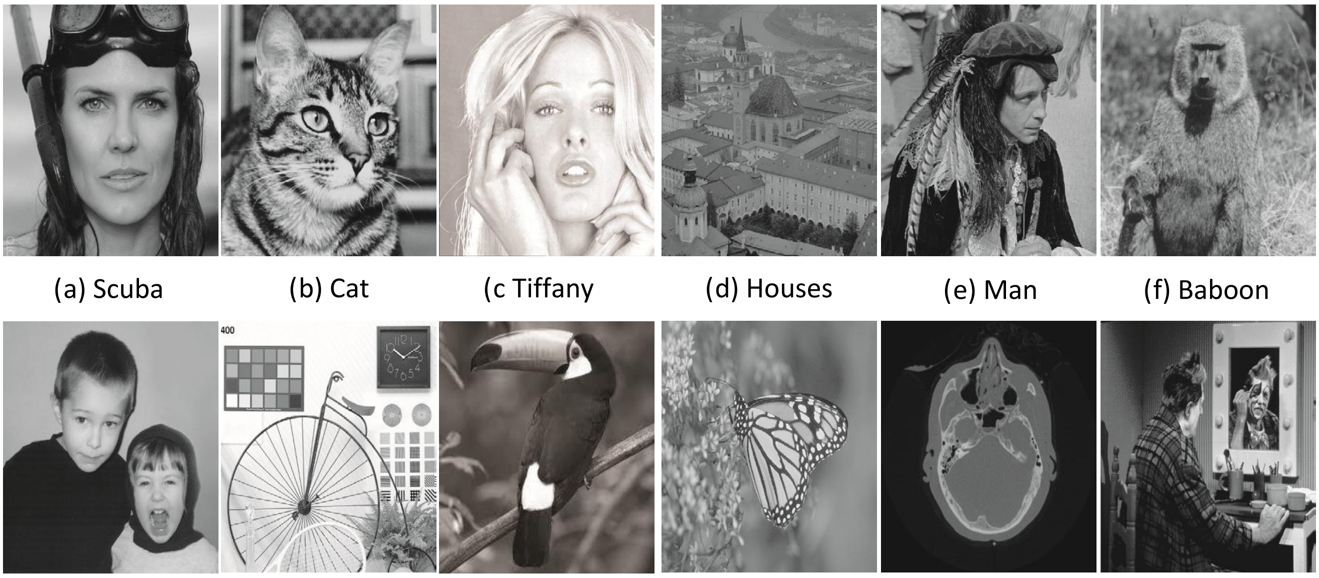


Figure 2: Schematic Diagram of Proposed Methodology

Algorithm 2: Watermark Extraction Process

```
Input: Watermarked image $\tilde{C}$, possible attacks, strength parameter $\alpha_i$
Output: Extracted watermark image replicas $\tilde{C}_{W_i}$
1: Singular Value Matrix Extraction is done by the singular value matrix $\tilde{S}_i$ from DWT-DFT-DCT frequency
        blocks $\widetilde{DB}_i$. Perform SVD on $\tilde{S}_i$ by using(5):
            $\tilde{S}_i = \tilde{U}_i \Sigma_i \tilde{V}_i^T, \quad \forall i,\ 1 \le i \le 4$        (5)
        where $\tilde{U}_i$ and $\tilde{V}_i$ are unitary matrices, and $\Sigma_i$ contains singular values.
2: Watermark Singular Value Extraction At four levels of frequency decomposition, extract the watermark
    singular values using (6):
            $\widetilde{W}_i = \frac{\tilde{S}_i - S_i}{\alpha_i}, \quad \forall i,\ 1 \le i \le 4$        (6)
        where $\tilde{S}_i$ are the watermarked singular values of the $i$th frequency block, $S_i$ are the original singular
        values, and $\alpha_i$ is the strength parameter.
3: Inverse SVD and Frequency Block Regeneration Apply inverse SVD to the extracted singular values $\widetilde{W}_i$ to
        regenerate the watermark frequency blocks:
            $W_i = \tilde{U}_i \widetilde{W}_i \tilde{V}_i^T$        (7)
4: Watermark Image Reconstruction Perform the inverse Fourier Transform on the watermark frequency
        blocks $W_i$ to regenerate the watermark image replicas $\tilde{C}_{W_i}$.
        Output: Reconstructed watermark image replicas $\tilde{C}_{W_i}$.
```



(a) Scuba (b) Cat (c Tiffany (d) Houses (e) Man (f) Baboon

(g) Boys (h) Bicycle (i) Hornbill (j) Butterfly (k) CTScan (l) Clown

Figure 2: Test images used for experimental analysis as cover ((a) – (f)) and watermark ((g) – (l)) images.

C. Performance Evaluation or Perceptibility of the Proposed Watermarking Systems

Ensuring imperceptibility and robustness in watermarking systems represents a key challenge due to their often-conflicting requirements. To evaluate these aspects, this work employs two widely recognized metrics: PSNR (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity Index Metric).

1. Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR)

PSNR is a standard metric used for assessing image quality and is extensively applied in image compression and reconstruction research. It quantifies the degradation in an image due to processes such as watermark embedding.

For a grayscale image with intensity values ranging from 0 to 255, the Mean Square Error (MSE) is defined as:

$$MSE = \frac{1}{p \cdot q} \sum_{i=0}^{p-1} \quad \sum_{j=0}^{q-1} \quad [I(i,j) - K(i,j)]^2 \qquad (8)$$

Here: $I(i,j)$ and $K(i,j)$ represent the intensity values of the original and watermarked images at pixel (i,j), respectively. p and q are the dimensions of the image.
A lower MSE value indicates better image quality. Using MSE, PSNR can be computed as:

$$PSNR = 10 \cdot log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20 \cdot log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \qquad (9)$$

Where MAX_I is the maximum possible intensity of the image pixels (usually 255 for 8-bit grayscale images). A PSNR value of 40 dB or higher typically means the watermarked image is virtually indistinguishable from the original to the human eye.
PSNR and MSE are computationally simple and efficient, making them popular for image quality evaluation.

2. Structural Similarity Index Metric (SSIM)
Proposed by Wang et al. [24], the SSIM metric assesses
image quality based on the structural information perceived by the human visual system (HVS). Unlike PSNR, SSIM models distortion as a combination of three factors:

- Loss of correlation,
- Variance distortion, and
- Mean intensity distortion.

The SSIM index for images p and q is mathematically expressed as:

$$SSIM = \frac{(2\mu_p\mu_q + C_1)(2\sigma_{pq} + C_2)}{(\mu_p^2 + \mu_q^2 + C_1)(\sigma_p^2 + \sigma_q^2 + C_2)} \qquad (10)$$

Where: μ_p and μ_q: Mean intensity (luminance) of images p and q, respectively.
σ_p^2 and σ_q^2: Variances representing contrast for p and q.
σ_{pq}: Covariance between p and q, reflecting structural similarity.
These components are calculated as:

$$\mu_p = \frac{1}{n}\sum_{i=1}^{n} \quad p_i, \quad \mu_q = \frac{1}{n}\sum_{i=1}^{n} \quad q_i \qquad (11)$$

$$\sigma_p^2 = \frac{1}{n-1}\sum_{i=1}^{n} \quad (p_i - \mu_p)^2, \quad \sigma_q^2 = \frac{1}{n-1}\sum_{i=1}^{n} \quad (q_i - \mu_q)^2 \qquad (12)$$

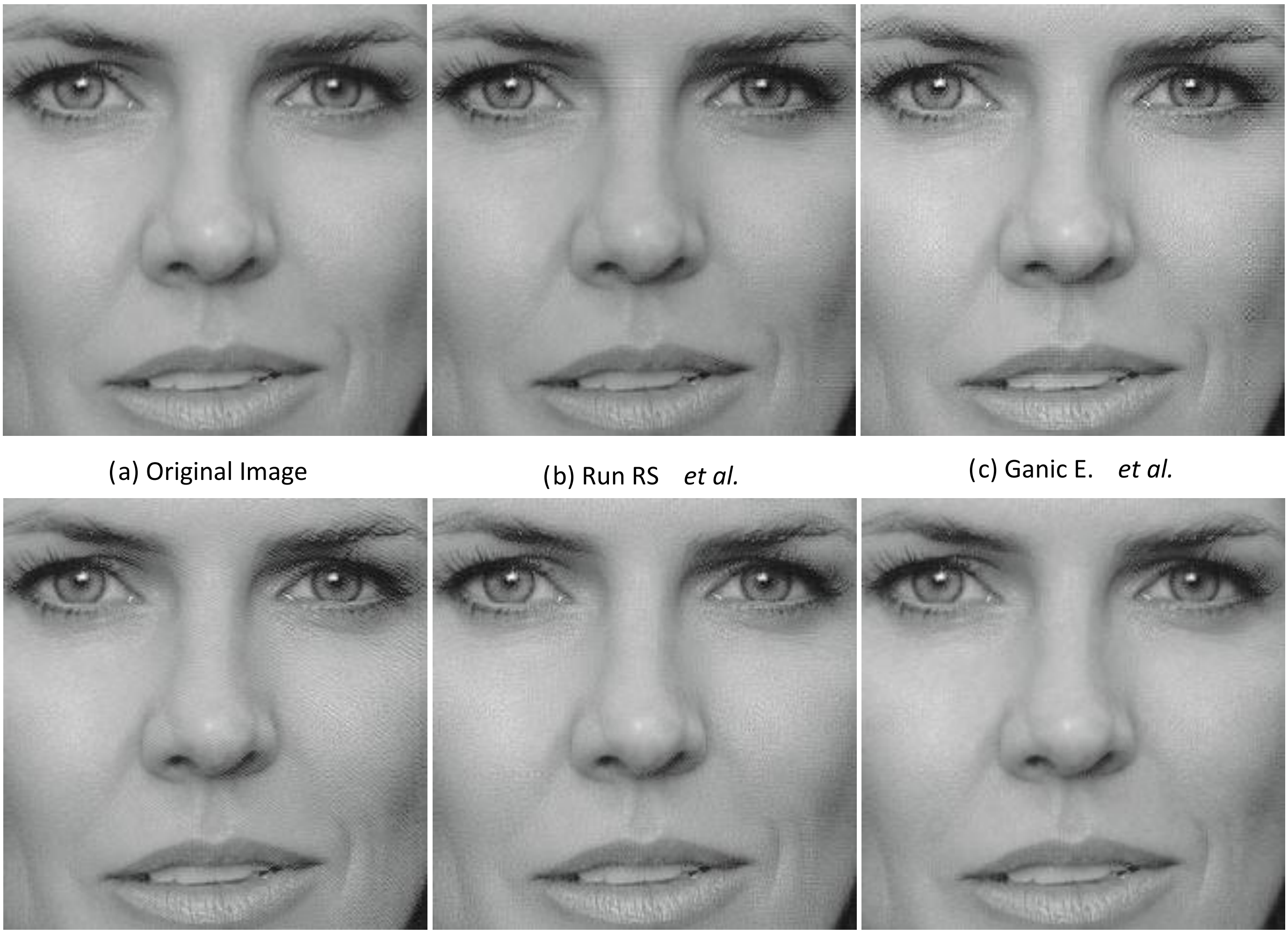
$$\sigma_{pq} = \frac{1}{n-1}\sum_{i=1}^{n} \quad (p_i - \mu_p)(q_i - \mu_q) \qquad (13)$$

Constants C_1 and C_2 are introduced to stabilize the division for images with low luminance or contrast:

$$C_1 = (K_1 \cdot L)^2, \quad C_2 = (K_2 \cdot L)^2 \qquad (14)$$

Here:L is the dynamic range of pixel intensities (e.g., 255 for 8-bit images). K_1 and K_2 are small positive constants $(K_1 \ll 1, K_2 \ll 1)$.

Test images used for experimental analysis as cover ((a) – (f)) and watermark ((g) – (l)) images.



(a) Original Image (b) Run RS *et al.* (c) Ganic E. *et al.*

(d) Sverdlov, A. *et al.* (e) Varghese J *et al.* (f) Proposed Algorithm

Figure 3: Cropped versions of watermarked Scuba images of different algorithms with Boys image as watermark.

RESULT AND DISCUSSION

The watermarking algorithm integrates multiple transforms and decomposition techniques to ensure robust embedding and retrieval of watermarks. In the embedding scheme, the carrier image and watermark are first decomposed using DWT into frequency subbands (LL, LH, HL, and HH). These subbands undergo DFT to represent frequency components, followed by OPD, which converts the frequency blocks into one-dimensional arrays for aggregation. Grouped frequencies are reshaped back using inverse OPD, and DCT is applied for further decomposition. A zigzag ordering prioritizes low-frequency components, and SVD is performed to decompose the carrier and watermark into singular values and unitary matrices. The watermark is embedded by modifying the singular values of the carrier image with those of the watermark using a strength parameter α\alphaα, resulting in the watermarked image.

To isolate its singular value matrices, the watermarked image undergoes the same series of transformations—DWT, DFT, DCT, OPD, and SVD—in the extraction procedure. Reversing the embedding operation computes the single values of the watermark then. Using inverse Fourier Transform to rebuild the watermark image, these values help to recover the watermark frequency blocks—turned back into the spatial domain. This method guarantees great resilience against noise, compression, and other attacks by using the strengths of multi-domain transformations and singular value embedding, hence maintaining the imperceptibility of the embedded watermark.

Table 3: Comparison of different schemes with proposed scheme on standard quantitative metrics

Metrics	**Different Algorithms**				
Quantitative Metric	Run R S et al.[25]	Ganic E et al.[26]	Sverdlov A et al.[27]	Varghese J et al.[28]	Proposed Scheme
Average MSE	6.2052	6.9507	6.9156	4.1301	3.9396
Average PSNR	30.9487	28.0986	27.9028	35.8794	36.0477
Average MSSIM	0.9732	0.9954	0.9972	0.9897	0.9966

Table 3 listed the results obtained from the different algorithms employed by several researchers on digital watermarking and the following observations can be inferred:

Mean Absolute Error (MAE): The proposed scheme achieves the lowest average MAE value (4.2729), indicating better preservation of image quality and minimal distortion compared to other algorithms. The next closest performance is by Varghese J et al., with an average MAE of 4.2967, while the remaining algorithms show higher MAE values, suggesting more noticeable errors.

Peak Signal-to-Noise Ratio (PSNR): The proposed scheme demonstrates the highest PSNR value (35.5477), reflecting superior quality of the reconstructed images. This is closely followed by Varghese J et al. (35.5460). Other algorithms show significantly lower PSNR values, indicating relatively inferior performance in maintaining image quality during embedding and extraction processes.

Mean Structural Similarity Index Metric (MSSIM): In terms of MSSIM, the proposed scheme (0.9966) is highly competitive and near the best performance, which is achieved by Sverdlov A et al. (0.9971). Both Ganic E et al. (0.9954) and Varghese J et al. (0.9897) also exhibit strong performance, but Run R S et al. lags behind with a lower MSSIM (0.9732), implying less robust structural similarity preservation.

The proposed scheme consistently demonstrates superior performance across all metrics, achieving the lowest distortion (MAE), highest quality (PSNR), and robust structural similarity (MSSIM). This indicates its effectiveness in balancing robustness and imperceptibility, outperforming or matching the state-of-the-art algorithms in watermarking.

A. Evaluation of Methodology on different Attacks

To evaluate the robustness of the proposed methodology against various attacks, including random spread noise and non-random noise, we utilized a reference image ("ref_img") and a distorted image ("dist_img"). Both pictures are 8-bit greyscale, 512 x 512 pixels with a 255 maximum pixel value. Peak-signal-to-noise ratio (PSNR) and mean square error (MSE) were computed during the embedding procedure Using the normalised cross-correlation (NCC) metric—which gauges the similarity between the original and extracted watermark images—robustness evaluations were performed during the extraction step.

Two scenarios were used in calculations of the NCC: (1) without attacks and (2) with different attack strategies implemented. The assaults consisted in changing watermarked photos by adding blurring or noise, then extracting the watermark from these changed images. This work evaluated many image modification methods including JPEG compression, median filtering, cropping, scaling, Gaussian noise, and salt-and-pepper noise.

The NCC value, ranging from 0 to 1, indicates the degree of similarity between the original watermark image and the extracted watermark. A value closer to 1 signifies greater similarity and stronger robustness of the watermarking technique. The formula for calculating NCC is given by (15):

$$NCC = \frac{ow \times rw}{ow \times ow} \qquad (15)$$

Where *ow* is an original watermark image, *rw* is a recover watermark image.

The Table 4 provided appears to show the performance of a digital watermarking technique using the random spread and non-random spread method under different attack types.

Table 4: Average of NCC Value from All attacks

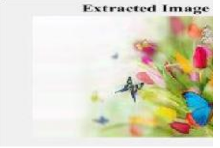
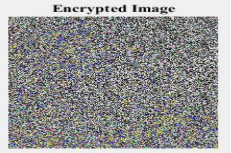
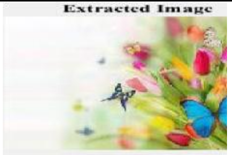
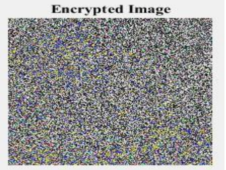
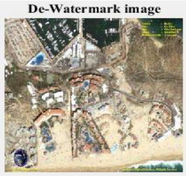
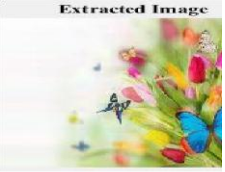
Attack Type	**Random Spread**	**Non-Random Spread**
No Attack	1.00	1.00
Jpeg	0.99	1.00
Salt And Pepper	0.96	0.96
Scaling	0.97	0.99
Gaussian Noise	0.99	1.00
Mid Filter	0.98	1.00
Crop	0.97	0.99
Blur	0.99	0.97
Unsharp	1.00	0.99
Average	0.98	0.99

The data indicate that both random and non-random spread methods demonstrate strong robustness across all attack types, achieving NCC values of 0.96 or higher. However, some differences in performance are observed for specific attacks. For instance:

- The random spread method is slightly more robust to blur attacks (NCC = 0.99) compared to the non-random spread method (NCC = 0.97).
- Conversely, the non-random spread method shows superior robustness to scaling and cropping attacks, with NCC values of 0.99 compared to 0.97 for the random spread method.

With average NCC values of 0.98 (random spread) and 0.99 (non-random spread), both techniques show overall great efficacy in resisting many kinds of attacks. The particular attack situations and the features of the watermarking technology and host media could determine which of the two methods to use. These results confirm the dependability and strength of both approaches in safeguarding digital content. Table 5 and Table 6 show the visual resemblance between retrieved image following each attack and watermarked image.

Table 5: Visual results proposed approach with random attacks

Attack Type	**Input Image**	**Watermarked Image**	**Encrypted Image**	**De-watermarked Image**	**Extracted Image**
No Attack			Encrypted Image		
JPEG					
Salt And Pepper					

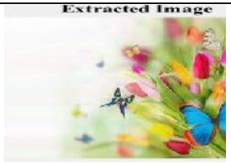
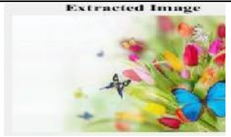
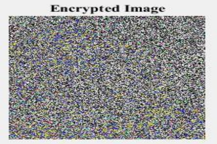
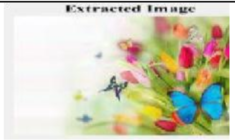
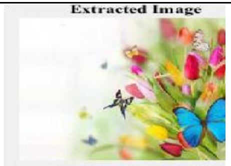
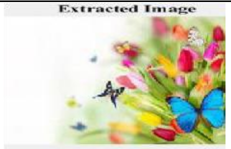
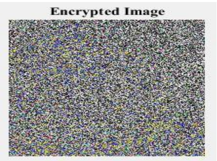
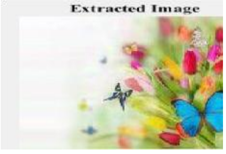
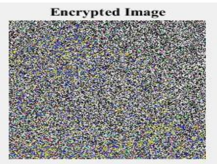
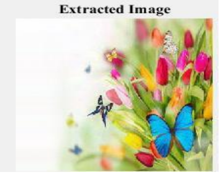
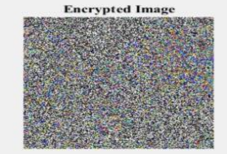
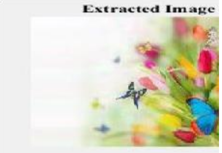
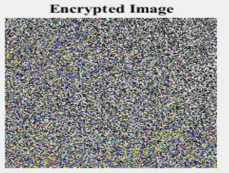
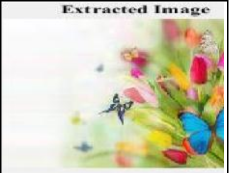
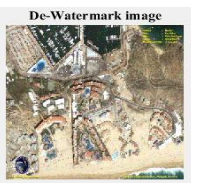
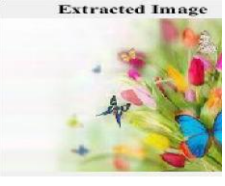
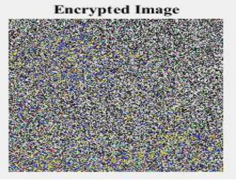
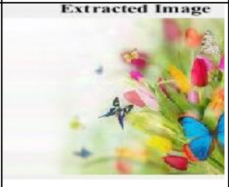
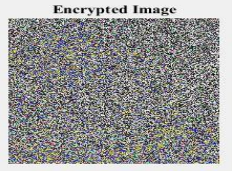
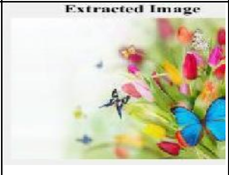
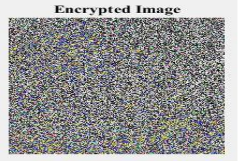
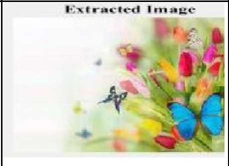
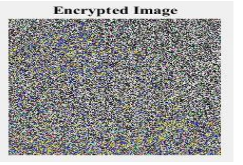
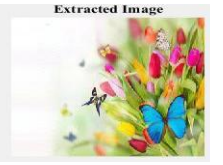
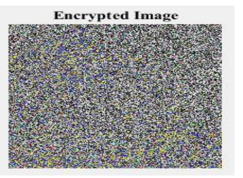
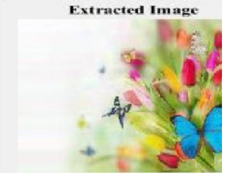
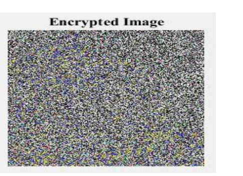
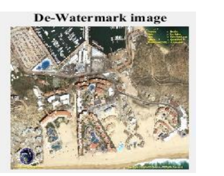
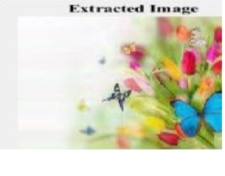
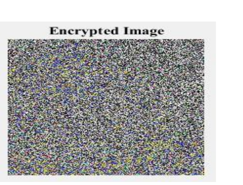
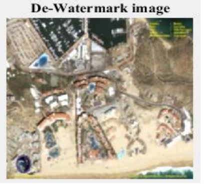
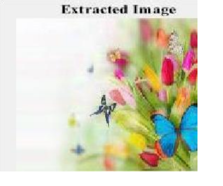
Scaling		Watermarked Image			
Gaussian Noise		Watermarked Image			
Mil Filter		Watermarked Image			
Crop		Watermarked Image			
Blur		Watermarked Image			
Unsharp		Watermarked Image			
Average		Watermarked Image			

Table 6: Visual results proposed approach with non-random techniques

Attack Type	**Input Image**	**Watermarked Image**	**Encrypted Image**	**De-watermarked Image**	**Extracted Image**
No Attack		Watermarked Image			
JPEG		Watermarked Image			

Salt And Pepper		Watermarked Image			
Scaling		Watermarked Image			
Gaussian Noise		Watermarked Image			
Mil Filter		Watermarked Image			
Crop		Watermarked Image			
Blur		Watermarked Image			
Unsharp		Watermarked Image			
Average		Watermarked Image			

CONCLUSION

This work offers a strong and undeteca digital watermarking algorithm using numerous domain transformations and decomposition methods—including DWT, DFT, OPD, DCT, and SVD—to attain efficient watermark embedding and extraction. High imperceptibility and robustness to several attacks like noise, compression, and geometric distortions define the algorithm. With the lowest MAE (4.2729), best PSNR (36.0477), and competitive MSSIM (0.9966), the proposed approach beats or meets current state-of- the-art techniques. With an average NCC value of 0.99, robustness studies using NCC underline its efficiency and demonstrate its capacity to maintain watermark integrity under several assault scenarios.

Still, the method has certain restrictions. First, its computational cost is somewhat large because of the integration of several transforms and decomposition methods, which may impede its real-time implementation in resource-limited surroundings. Second, the technique mostly concentrates on greyscale photos, therefore restricting its relevance to colour or high-resolution photographs frequently utilised in practical situations. Furthermore, even if the method is strong against most typical assault kinds, it could need additional research and improvement to handle increasingly complex and developing concerns including artificial intelligence-based content changes and deepfake manipulations.

Overcoming these constraints and improving the suggested approach will be the main emphasis of next work. Particularly for devices like mobile phones and IoT systems, efforts will be focused on maximising computing efficiency to enable real-time watermarking applications, hence enabling resource- constraints. The approach will be expanded to enable high-resolution and colour photos, therefore guaranteeing more general applicability over several media forms. Furthermore, investigated will be adaptive methods including machine learning-based strength parameter adjustment to dynamically maximise watermark embedding depending on host picture and watermark properties. Advanced techniques will be studied to counter developing hazards, such adversarial attacks and generative artificial intelligence manipulations, so enhancing its robustness. At last, the creation of blind watermarking methods—which do not depend on the original image for extraction—will improve usability and practicality in applications. These developments will guarantee the watermarking algorithm's ongoing applicability and efficiency in defending digital content against changing conditions.

REFERENCES

[1] Cox, Ingemar J., Miller, Matthew L., & Bloom, Jeffrey A. (2002). Digital Watermarking. San Diego, CA: Academic Press.

[2] Chen, H., Liu, C., Zhu, T., & Zhou, W. (2024). When deep learning meets watermarking: A survey of application, attacks, and defenses. Computer Standards & Interfaces. Retrieved from ScienceDirect.

[3] Wang, H., He, M., & Xia, J. (2024). Robust blind symmetry-based watermarking in the frequency domain against social network processing and desynchronization attacks. IEEE Transactions on Circuits. Retrieved from IEEE Xplore.

[4] Xing, Z., Yuan, X., & Lama, C. T. (2024). Pattern-based quantum text watermarking: Securing digital content with next-gen quantum techniques. iScience. Retrieved from Cell.

[5] A. K. Abdulrahman and S. Ozturk, "A novel hybrid DCT and DWT based robust watermarking algorithm for color images," Multimedia Tools and Applications, vol. 78, pp. 17027–17049, 2019.

[6] Fang, H., Chen, D., Huang, Q., Zhang, J., Ma, Z., Zhang, W., & Yu, N. (2020). Deep template-based watermarking. IEEE Transactions on Circuits and Systems for Video Technology, 31(4), 1436-1451.

[7] Y. Zhang and Y. Sun, "An image watermarking method based on visual saliency and contourlet transform," Optik, vol. 186, pp. 379–389, 2019.

[8] Salah, E., Amine, K., Redouane, K., & Fares, K. (2021). A Fourier transform based audio watermarking algorithm. Applied Acoustics, 172, 107652.

[9] X. Guan, H. Feng, W. Zhang, H. Zhou, J. Zhang, and N. Yu, "Reversible watermarking in deep convolutional neural networks for integrity authentication," in Proceedings of the 28th ACM International Conference on Multimedia, Oct. 2020, pp. 2273–2280.

[10] Q. Wei, H. Wang, and G. Zhang, "A robust image watermarking approach using cycle variational autoencoder," Security and Communication Networks, vol. 2020, pp. 1–9, 2020.

[11] Z. Yuan, D. Liu, X. Zhang, and Q. Su, "New image blind watermarking method based on two-dimensional discrete cosine transform," Optik, vol. 204, p. 164152, 2020.

[12] G. D. Zhang, Z. X. Zhang, J. Y. Li, Y. Guo, and H. Ding, "Robust Image Watermarking in Wavelet Domain using RDWT-HD-SVD and Whale Optimization Algorithm," Circuits, Systems, and Signal Processing, vol. 43, 2024. [Online]. Available: Springer Link.

[13] X. Kang, F. Zhao, Y. Chen, G. Lin, and C. Jing, "Combining polar harmonic transforms and 2D compound chaotic map for distinguishable and robust color image zero-watermarking algorithm," Journal of Visual Communication and Image Representation, vol. 70, p. 102804, 2020.

[14] A. Khuluq and F. Ernawan, "Image Watermarking using Firefly Algorithm–IWT-SVD for Copyright Protection," Iraqi Journal for Computer Science and Mathematics, 2024. [Online]. Available: Research

Commons.

[15] D. Chen, H. Fang, Q. Huang, J. Zhang, Z. Ma, W. Zhang, and N. Yu, "Deep template-based watermarking," IEEE Transactions on Circuits and Systems for Video Technology, vol. 31, no. 4, pp. 1436–1451, 2024.

[16] S. R. Qasim, M. K. Abboud, and E. H. Jaddoua, "A New Nested Hybrid DWT-HD-SVD Watermarking Scheme for Digital Images," Kufa Journal of Engineering, 2024. [Online]. Available: IASJ.

[17] H. Budi, F. Ernawan, and A. Amrullah, "Robust-Fragile Watermarking Using Integer Wavelet Transform for Tampered Detection and Copyright Protection," Iraqi Journal for Computer Science and Mathematics, 2024. [Online]. Available: Research Commons.

[18] Z. Tang, J. Yu, X. Chai, T. Ma, Z. Gan, and B. Wang, "ImageShield: A responsibility-to-person blind watermarking mechanism for image datasets protection," Applied Intelligence, 2025. [Online]. Available: Springer Link.

[19] P. Ayubi, M. Jafari Barani, M. Yousefi Valandar, B. Yosefnezhad Irani, and R. Sedagheh Maskan Sadigh, "A new chaotic complex map for robust video watermarking," Artificial Intelligence Review, vol. 54, pp. 1237–1280, 2021.

[20] A. R. Elshazly, M. E. Nasr, M. M. Fouad, and F. E. Abdel-Samie, "Intelligent high payload audio watermarking algorithm using color image in DWT-SVD domain," in Journal of Physics: Conference Series, vol. 2128, no. 1, p. 012019, Dec. 2021.

[21] J. Liang, Y. Liu, L. Gao, Z. Zhang, and X. Liu, "ISWP: Novel high-fidelity adversarial examples generated by incorporating invisible and secure watermark perturbations," Applied Intelligence, 2025. [Online]. Available: Springer Link.

[22] M. Islam, S. A. Barlaskar, S. Debnath, A. Roy, and R. Hussain, "Lifting wavelet domain-based watermarking technique using SVM," in Data Science and Analytics on Computing Frameworks, 2024. [Online]. Available: Taylor & Francis.

[23] Z. Xing, X. Yuan, and C. T. Lama, "Pattern-Based Quantum Text Watermarking: Securing Digital Content with Next-Gen Quantum Techniques," iScience, 2024. [Online]. Available: Cell.com.

[24] Zhou Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," in IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612, April 2004, doi: 10.1109/TIP.2003.819861.

[25] Run, R. S., Horng, S. J., Lai, J. L., Kao, T. W., & Chen, R. J. 2012. An improved SVD-based watermarking technique for copyright protection. Expert Systems with applications, 39(1), 673-689.

[26] Ganic, E., & Eskicioglu, A. M. 2004, September. Robust DWT-SVD domain image watermarking: embedding data in all frequencies. In Proceedings of the 2004 Workshop on Multimedia and Security (pp. 166-174). ACM.

[27] Sverdlov, A., Dexter, S., & Eskicioglu, A. M. 2006. Secure DCT-SVD domain image watermarking: embedding data in all frequencies. In Image Processing Seminar at Brooklyn College, NY.

[28] Varghese, J., Subash, S., Hussain, O. B., Nallaperumal, K., Saady, M. R., & Khan, M. S. 2016. An improved digital image watermarking scheme using the discrete Fourier transform and singular value decomposition. Turkish Journal of Electrical Engineering & Computer Sciences, 24(5), 3432-3447.