

# Secure Image Watermarking Using DWT-DFT-DCT and Arnold Transform

T Aruna Jacintha <sup>1</sup>, \*Sanjath Raja<sup>2</sup>, Khajavali Melgade<sup>3</sup>, Ramesh C Naik<sup>4</sup>, G Govardhan Sai<sup>5</sup>

<sup>1</sup>Department of Electronics and Communication, RR Institute of Technology, (VTU), Bengaluru, India

<sup>2</sup>Department of Electronics and Communication, RR Institute of Technology, (VTU), Bengaluru, India

<sup>3</sup>Department of Electronics and Communication, RR Institute of Technology, (VTU) Bengaluru, India

<sup>4</sup>Department of Electronics and Communication, RR Institute of Technology, (VTU) Bengaluru, India

\*Corresponding Author : sanjath2006@gmail.com

## Abstract

Digital image watermarking serves as a key mechanism for asserting copyright ownership and safeguarding multimedia content during online transmission. Existing methods tend to prioritize either attack resilience or perceptual quality, making it difficult to achieve both at once. This work introduces a watermarking framework that incorporates DWT, DFT, DCT, Arnold Transform and PSO, targeting simultaneous gains in robustness, imperceptibility and security. Prior to embedding, the watermark undergoes Arnold Transform encryption. The host image is then subjected to DWT decomposition, after which DCT and DFT are applied to selected frequency coefficients for watermark insertion. The resulting scheme withstands various attacks including JPEG compression, Gaussian noise, filtering, cropping, rotation and scaling. Embedding parameters are optimized through PSO to balance attack resistance with visual fidelity. Evaluation employs PSNR, MSE, SSIM and NC as performance indicators. Findings confirm that the proposed scheme outperforms standard DFT-based methods in terms of robustness, imperceptibility and security.

**Keywords-** Digital Image Watermarking, DFT, DWT, DCT, Arnold Transform, PSO, Robustness, Imperceptibility, Copyright Protection.

## 1. Introduction

The rapid expansion of digital networks and content-sharing platforms has made protecting the authenticity and ownership of images an increasingly urgent matter. Unauthorized copying, content manipulation and intellectual property violations have emerged as major challenges for image creators and distributors. Digital image watermarking provides an effective countermeasure by invisibly encoding ownership details within the image itself.

Any practical watermarking solution must fulfil three core properties. First, robustness: the hidden data must survive various forms of intentional or accidental image modification. Second, imperceptibility: the watermarked image must be visually indistinguishable from the unwatermarked

version. Third, security: unauthorized access to or removal of the embedded data must be prevented.

Frequency-domain techniques have gained prominence in watermarking over the past decade. DFT handles geometric distortions well. DWT supports hierarchical image decomposition while retaining visual fidelity. DCT groups image energy compactly, making it resistant to lossy compression. Arnold Transform scrambles the watermark for added protection, while PSO automates the selection of embedding parameters.

The proposed work unifies DWT, DFT, DCT, Arnold Transform and PSO into a single watermarking pipeline. The watermark is scrambled using Arnold Transform before being inserted into frequency-domain coefficients selected through PSO

optimization. Performance is quantified via PSNR, MSE and NC, with the aim of surpassing conventional DFT-only watermarking methods.

The standard embedding relationship is given by:

where  $I_2$  denotes the watermarked output,  $I$  is the original host image,  $W$  is the watermark signal and  $\alpha$  controls the embedding intensity.

The 2-D DFT expression used during embedding is:

$$F(u, v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) e^{-j2\pi(\frac{xu}{M} + \frac{yv}{N})}$$

The Discrete Cosine Transform equation is given by:

$$C(u, v) = \alpha(u)\alpha(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cos\left[\frac{(2x+1)u\pi}{2N}\right] \cos\left[\frac{(2y+1)v\pi}{2N}\right]$$

## 2. Related Work

Research into digital image watermarking has grown considerably, with numerous transform-domain methods proposed to improve copyright enforcement and image fidelity. DFT, DWT and DCT-based techniques dominate this space due to their inherently stronger defence against both content-based and geometric attacks relative to pixel-domain methods.

Frequency-domain processing has become a standard foundation in modern watermarking systems. DFT resists affine distortions effectively. DWT offers a flexible multi-scale representation that preserves perceptual quality. DCT achieves compact energy representation that proves beneficial under compression.

Ansari et al. proposed a DWT-DFT scheme aimed at affine transformation and JPEG compression robustness. DFT-guided synchronization strengthened attack resistance, though the method carried a relatively high computational cost.

Jain and Rajpal introduced a DFT-DCT approach with Arnold Transform pre-processing of the watermark, yielding stronger security and visual transparency. Identifying suitable embedding coefficients remained a key challenge.

Cedillo-Hernandez et al. investigated DFT-based geometric attack mitigation covering rotation, scaling and noise. Watermark detection improved, yet increasing the embedding strength degraded image quality noticeably.

Loukhaoukha et al. utilized an evolutionary search strategy to automate the choice of embedding parameters, improving robustness and image quality through strength and coefficient optimization. Higher computational load and implementation effort were identified as limitations.

Multi-transform hybrid schemes incorporating DWT, DFT, DCT and SVD have also been studied. Spreading the watermark across several frequency domains boosted extraction reliability under attack conditions, at the cost of greater algorithmic complexity.

In summary, achieving robustness and imperceptibility in tandem continues to be an open problem. This gap motivates the present hybrid approach that integrates all five components within a PSO-driven optimization loop.

## 3. Materials and Methods

The proposed system assembles DWT, DFT, DCT, Arnold Transform and PSO into a cohesive four-stage architecture covering watermark encryption, frequency-domain embedding, parameter optimization and watermark recovery.

**Watermark Encryption:** Arnold Transform is used to scramble the watermark image into a visually meaningless pattern. Reconstruction requires knowledge of the exact transform parameters, preventing unauthorized decoding.

**Host Image Decomposition:** The host image is analysed using DWT, which separates it into sub-bands covering different frequency ranges. The lowest-frequency sub-band is chosen for embedding owing to its concentration of image energy and natural resilience to attack.

**DCT Processing:** DCT transforms the chosen sub-band to achieve compact energy representation and improve tolerance to compression-related distortion.

**DFT Processing:** DFT is then applied to the DCT output, adding resilience against spatial transformations including rotation and scaling.

The watermark embedding equation is:

$$F(u, v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) e^{-j2\pi(\frac{ux}{M} + \frac{vy}{N})}$$

where  $C$  are the chosen frequency coefficients and  $\alpha$  is the PSO-determined strength factor.

The DCT equation is:

$$C(u, v) = \alpha(u)\alpha(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cos\left[\frac{(2x+1)u\pi}{2N}\right] \cos\left[\frac{(2y+1)v\pi}{2N}\right]$$

PSO searches for the  $\alpha$  value and coefficient positions that maximize robustness while keeping perceptual degradation minimal. PSNR and NCC are used as the optimization objective.

Once embedding is complete, inverse DFT, DCT and DWT are applied in order to produce the final watermarked image. The extraction path reverses these operations and concludes with inverse Arnold Transform to retrieve the original watermark. Performance is evaluated using:

PSNR:

$$PSNR = 10 \log_{10} \left( \frac{MAX^2}{MSE} \right)$$

MSE:

$$MSE = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [I(x, y) - I_w(x, y)]^2$$

Normalized Correlation (NC):

$$NC = \frac{\sum W(x, y) \times W'(x, y)}{\sqrt{\sum W(x, y)^2 \sum W'(x, y)^2}}$$

### 3.1 MATLAB Implementation

All components were coded in MATLAB. Both input images were converted to grayscale at the outset. The DWT-DCT-DFT chain handled watermark insertion and recovery. Arnold Transform encryption and PSO-based tuning were incorporated as described. To test robustness, the watermarked images were subjected to compression, noise,

filtering, cropping and rotation. Quality was then quantified using PSNR, MSE, SSIM and NC.

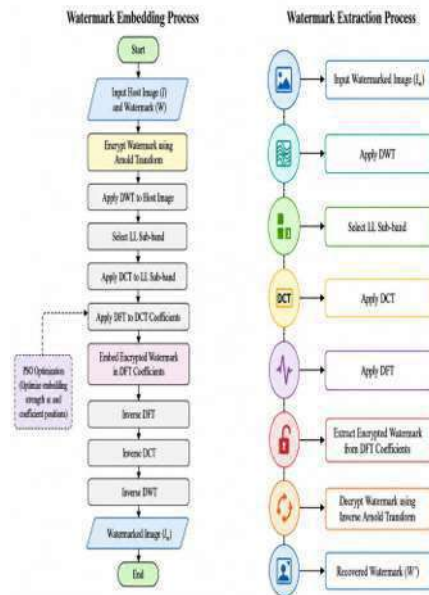


Fig. 1: Proposed System Block Diagram

### 3.2 Proposed Methodology

The framework draws on five techniques—DWT, DFT, DCT, Arnold Transform and PSO—to construct a watermarking system that achieves robustness, imperceptibility and security concurrently.

The pipeline covers four stages:

- Watermark encryption via Arnold Transform
- Frequency-domain embedding using DWT-DCT-DFT
- PSO-based parameter optimization
- Watermark extraction and decryption

The process is divided into two phases: (i) embedding and (ii) extraction.

Through this coordinated multi-transform design, the system targets improvements across all three key watermarking criteria simultaneously.

### 3.3 Watermark Embedding Process

Inputs to the embedding stage are the host image and the watermark image. The watermark is scrambled using Arnold Transform to block unauthorized extraction. DWT is applied to the host image,

producing four sub-bands: LL, LH, HL and HH. The LL sub-band is retained for its strong energy content and resilience to signal-based attacks. DCT compacts the energy within this sub-band and improves tolerance to compression. DFT is applied next to add robustness against spatial distortions. The scrambled watermark is finally inserted into the DFT coefficients using the PSO-chosen factor  $\alpha$ .

PSO tunes  $\alpha$  so the watermark is both strong and visually imperceptible, using PSNR and NCC as fitness measures. Inverse DFT, DCT and DWT then reconstruct the watermarked image.

DWT Decomposition:  $I(x, y) \rightarrow \{LL, LH, HL, HH\}$

Watermark Embedding Equation:  $We = C + \alpha W$

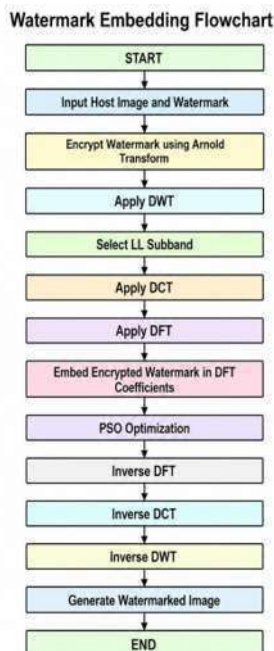


Fig. 2: Watermark Embedding Flowchart

### 3.4 Watermark Extraction Process

Extraction mirrors the embedding path in reverse order. The watermarked image passes through DWT decomposition, LL sub-band selection, DCT and DFT. Stored embedding parameters are used to isolate the watermark coefficients. Inverse Arnold Transform is then applied to decode the scrambled watermark and reconstruct the original watermark image.

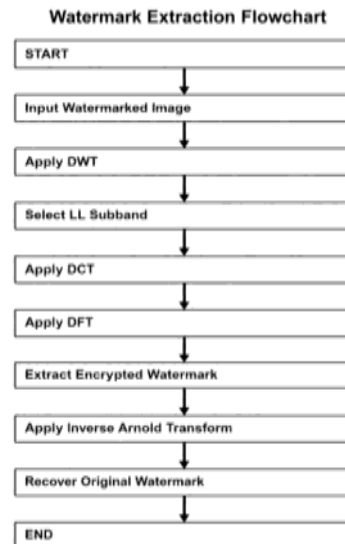


Fig. 3: Watermark Extraction Flowchart

### 4.3 Algorithm Steps

Step 1: Read the host image and watermark image.

Step 2: Scramble the watermark using Arnold Transform.

Step 3: Decompose the host image using DWT.

Step 4: Choose the LL sub-band from the DWT result.

Step 5: Process the LL sub-band with DCT.

Step 6: Process the DCT output with DFT.

Step 7: Insert the scrambled watermark into the DFT coefficients.

Step 8: Optimize the embedding factor  $\alpha$  using PSO.

Step 9: Reconstruct the image via inverse DFT  $\rightarrow$  inverse DCT  $\rightarrow$  inverse DWT.

Step 10: Save the watermarked image.

Step 11: For extraction, apply forward transforms and retrieve the watermark coefficients.

Step 12: Decode the watermark using inverse Arnold Transform.

## 4. Results and Discussion

### 4.1 Experimental Setup

The hybrid watermarking system was developed in MATLAB. Host and watermark images were converted to grayscale at the start. DWT, DCT, DFT, Arnold Transform and PSO were integrated as outlined in Section 4. The watermark was embedded within specific frequency coefficients to maintain imperceptibility and robustness. PSNR and NCC were used to evaluate output quality. Gaussian noise was introduced to test system resilience under degraded conditions.

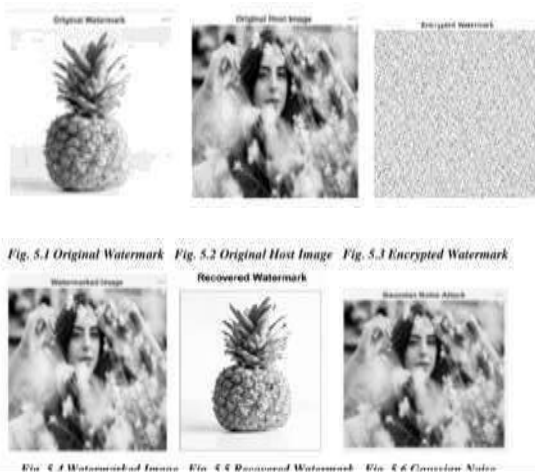


Fig. 5.1–5.6: Original Watermark, Host Image, Encrypted Watermark, Watermarked Image, Recovered Watermark, Gaussian Noise Attack

#### 4.1.1 Host Image

Fig. 5.2 depicts the host image acting as the carrier for the embedded watermark. Grayscale conversion was performed beforehand to ensure compatibility with the frequency-domain processing pipeline.

#### 4.1.2 Watermark Image

Fig. 5.1 shows the watermark carrying the ownership data. Its dimensions were chosen to support efficient embedding and reliable recovery during extraction.

#### 4.1.3 Encrypted Watermark

Fig. 5.3 displays the watermark following Arnold Transform scrambling. The output is visually noise-like and conveys no recognizable information without the correct inverse transform parameters.

#### 4.1.4 Watermarked Image

Fig. 5.4 presents the host image with the watermark embedded. No perceptible difference exists between it and the original, validating the imperceptibility of the approach. The PSNR attained was 57.6103 dB, indicating very high image fidelity after embedding.

#### 4.1.5 Recovered Watermark

Fig. 5.5 shows the watermark retrieved during extraction. The recovered image has slight degradation yet the embedded content is clearly readable. An NCC of 0.74996 confirms strong similarity with the original watermark.

#### 4.1.6 Gaussian Noise Attack

Fig. 5.6 depicts the watermarked image after Gaussian noise was added. The watermark remained detectable following the attack. Post-attack PSNR was 30.0333 dB, verifying adequate image quality retention under noisy conditions.

### 4.2 Watermark Embedding Results

The embedding stage processed the host and watermark images after Arnold Transform encryption of the watermark. The DWT-DCT-DFT chain inserted the scrambled watermark into the host. The output image closely resembles the input, with no visible distortion introduced by the embedding process.

[PSNR = 57.6103 dB]

The achieved PSNR demonstrates that embedding the watermark does not meaningfully degrade the visual appearance of the host image.

### 4.3 Watermark Extraction Results

The extraction process reversed the transform sequence and applied inverse Arnold Transform to decode the watermark. The recovered watermark shows minor degradation but the core content is intact and recognizable, confirming successful retrieval.

[NCC = 0.74996]

The NCC result reflects an adequate level of similarity between the recovered and original watermarks, confirming the method restores embedded data reliably.

### 4.4 Attack Analysis

A Gaussian noise attack was used to stress-test the watermarking system. The watermark survived the attack and remained detectable, with only marginal changes in both the distorted image and the extracted watermark.

[PSNR {Attack} = 30.0333 dB]

These results demonstrate that the system maintains both image quality and watermark integrity when subjected to noise-based attacks.

#### 4.5 Performance Discussion

The experimental findings confirm that the multi-transform design successfully balances robustness and imperceptibility. DWT contributes multi-resolution decomposition; DCT improves compression tolerance; DFT adds geometric attack resistance; Arnold Transform secures the watermark through encryption; PSO identifies the embedding parameters that yield the best trade-off.

Watermarked images retain strong visual similarity to their originals, and the embedded watermark survives noise attacks, highlighting the practical value of the approach for image copyright enforcement.

#### 5. Conclusion

A hybrid digital watermarking scheme combining DWT, DFT, DCT, Arnold Transform and PSO has been presented. The method inserts an encrypted watermark into the frequency domain of the host image without noticeable degradation.

Arnold Transform encryption is applied before embedding to strengthen security. The combined DWT-DCT-DFT processing delivers robustness across diverse attack types. PSO automates parameter selection to optimize the robustness-imperceptibility balance.

The system recorded a PSNR of 57.6103 dB and an NCC of 0.74996, confirming strong imperceptibility and reliable watermark recovery. A post-attack PSNR of 30.0333 dB validated noise robustness.

The proposed design offers improvements over single-transform DFT methods. Future research may investigate neural network-based optimization and more sophisticated encryption to further boost recovery accuracy and geometric attack resistance.

#### References

- [1] M. Cedillo-Hernandez, M. Nakano-Miyatake and H. Perez-Meana "Improving DFT-Based Image Watermarking Using Particle Swarm Optimization Algorithm" *Expert Systems with Applications* vol. 40 No. 15 Pp. 6075–6089, 2013.
- [2] I. A. Ansari, M. Pant and C. W. Ahn "Blind Watermarking in DWT Domain Using Weighted PSO" *Multimedia Tools and Applications* vol. 75 No. 18 Pp. 1–23, 2016.
- [3] R. Jain and N. Rajpal "A Image Watermarking Scheme Using DWT, DCT and SVD" *International Journal of Computer Applications* vol. 43 No. 15 Pp. 7–12 2012.
- [4] K. Loukhaoukha, J. Y. Chouinard and A. Berdai "A Secure Image Watermarking Technique Using Arnold Transform and Genetic Algorithm" *Applied Soft Computing* vol. 11 No. 2 Pp. 1742–1753, 2011.
- [5] S. Singh, V. Kumar and H. K. Verma "A Hybrid Digital Image Watermarking Approach for Copyright Protection" *Procedia Computer Science* vol. 70 Pp. 177–184, 2015.
- [6] X. Kang, J. Huang, Y. Q. Shi and Y. Lin "A DWT-DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression" *IEEE Transactions on Circuits and Systems for Video Technology* vol. 13 No. 8 Pp. 776–786, Aug. 2003.
- [7] A. Al-Haj and A. Mohammad "Hybrid Blind Robust Image Watermarking Technique Based on DFT-DCT and Arnold Transform" *Multimedia Tools and Applications* vol. 79 No. 5 Pp. 1–20, 2020.
- [8] S. Pereira and T. Pun "Perceptual DFT Watermarking with Improved Detection and Robustness to Geometrical Distortions" *Proceedings of SPIE* vol. 3657 Pp. 329–343, 1999.
- [9] S. Thanki and K. Borisagar "A Hybrid Digital Image Watermarking Scheme Incorporating DWT, DFT, DCT and SVD Transformations" *Journal of Information Security and Applications* vol. 47 Pp. 1–15, 2019.