DIGITAL IMAGE WATERMARKING FOR COPYRIGHT PROTECTION AND AUTHENTICATION

P. Bavith babu

Abhishek

ABSTRACT :

This report presents a blind, frequency-domain image watermarking system designed to balance imperceptibility, robustness, and practicality. A pseudo-random binary watermark is embedded in DWT-DCT coefficients using spread-spectrum modulation and a secret key for secure coefficient selection. We evaluate performance under common attacks (compression, noise, filtering, mild geometric transforms) using PSNR, SSIM, BER, and NCC. Results show high visual quality and reliable detection for typical real-world processing, with expected limitations under strong geometric desynchronization. We conclude with practical operating points and directions for synchronization and content-adaptive embedding.

INTRODUCTION :

Digital images are widely shared, modified, and republished, making intellectual property protection and integrity verification essential. Invisible watermarking embeds information directly into content so that the signal remains present after typical processing and is not disruptive to viewers. The challenge is balancing three goals: high visual quality, robust recovery after processing/attacks, and blind detection without needing the original image. This work implements and evaluates such a system, focusing on frequency-domain embedding for resilience and imperceptibility.

OBJECTIVES :

- Design a blind watermarking algorithm with strong imperceptibility (high PSNR/SSIM).
- Achieve robust detection under compression, noise, filtering, and mild geometry (low BER, high NCC).
- Implement a modular pipeline for embedding, attacking, detection, and reporting.

- Analyze trade-offs (embedding strength vs. quality/robustness) and identify practical defaults.

LITERATURE REVIEW :

Watermarking Paradigms

- Spatial domain (e.g., LSB): simple but fragile to compression, filtering, and resizing.
- Frequency domain (DCT, DWT, DFT): improved robustness via energy compaction and perceptual control.

Blind vs. Non-Blind

- Blind detection avoids storing/transmitting the original image, improving practicality.
- Non-blind can be more accurate but is less convenient in deployment.

Perceptual Considerations

- Human Visual System (HVS) suggests embedding more in textured regions and mid-frequencies to stay imperceptible while remaining resilient.

Synchronization and Attacks

- JPEG compression and noise are commonly handled by frequency-domain methods.
- Geometric attacks (rotation, scaling, cropping) cause desynchronization; templates or feature-based invariants improve robustness.

Evaluation Metrics

- Quality: PSNR, SSIM between original and watermarked images.
- Robustness: BER for decoded bits and NCC/correlation for detection strength.

METHODOLOGY :

Data and Payload

- Diverse image set (natural scenes, objects, portraits, text-like, low-light) to test across textures and brightness.
- Watermark: a short binary sequence or logo-like pattern, mapped to a pseudo-random sequence keyed by a secret.

Embedding

- Transform: 1–2 level DWT followed by 8×8 block DCT on selected sub-bands (usually LH/HL; LL for maximum robustness if quality permits).
- Coefficient selection: key-driven indexing ensures security and consistent detection.
- Modulation: spread-spectrum addition scaled by embedding strength α.
- Reconstruction: inverse DCT and inverse DWT to obtain the watermarked image.

Typical targets:

- PSNR ≈ 38–42 dB, SSIM ≥ 0.96 with moderate α on varied content.

Detection (Blind)

- Apply identical DWT + block DCT pathway to the suspect image.
- Use the secret key to extract the same coefficient indices.
- Compute correlation/NCC against the known pseudo-random sequence; decide with threshold τ.
- For bit payloads, estimate BER via sign/distance rules on correlation outputs.

Attack Suite and Protocol

- Signal processing: JPEG (QF 10–90), Gaussian noise, blur (Gaussian), median filtering, sharpening.
- Geometry: small rotations (±1–3°), scaling (0.75–1.25×), cropping (≤30%).
- Metrics: PSNR/SSIM for imperceptibility; NCC/BER post-attack for robustness.
- Reproducibility: fixed seeds, logged parameters, per-image and averaged reports.

SYSTEM ARCHITECTURE

- Input/Config: loads images and watermark; centralizes α, sub-bands, block size, key, τ, attack parameters.
- Embedding Engine: DWT-DCT transforms, keyed coefficient selection, spread-spectrum embedding.
- Attack Simulator: configurable transformations for robustness evaluation.
- Detection Engine: correlation-based detection and BER/NCC computation.
- Metrics & Reporting: aggregates quality/robustness metrics and exports summaries.

- Storage: organized directories for originals, watermarked images, attacked images, and outputs.

Data flow: Ingestion → Embedding → Watermarked Output → Attacks → Detection → Metrics/Reports.

RESULTS AND DISCUSSION :

Imperceptibility

- Watermarked images retain high fidelity on most content. Typical PSNR > 40 dB and SSIM ≥ 0.97 with moderate α.
- Texture-rich regions mask embedding well, permitting higher α; flat or edge-heavy images may require lower α to avoid ringing or banding.

Robustness to Common Processing

- JPEG compression: reliable detection down to QF ~30 with low BER when embedding in mid-frequency DCT coefficients. At QF ≤ 20, BER increases but NCC often remains usable with tuned thresholds.
- Noise and blur: Gaussian noise moderately degrades correlation; spread-spectrum maintains detectability at modest noise levels. Gaussian blur reduces mid-band energy; small σ is tolerable. Median filtering is harsher but still recoverable with conservative α and tuned τ.

Geometric Transformations

- Mild scaling and small rotations remain partially detectable; larger changes cause desynchronization and degrade NCC/BER significantly.
- Cropping up to ~20–30% is mitigated by redundancy across blocks, though payload capacity and confidence decrease.

Trade-offs and Practical Settings

- Embedding strength α: higher α improves robustness but lowers PSNR/SSIM. A balanced operating point: PSNR ~ 40 dB, SSIM ~ 0.98, robust to QF ≈ 30 and mild blur/noise.
- Sub-band choice: LH/HL balances imperceptibility and robustness; LL improves compression robustness but risks visibility.
- Block size: 8×8 offers a good compromise between robustness and artifact control.

Limitations

- Desynchronization under strong rotation/scale remains the main weakness without templates or feature-based invariants.
- Uniform α is not content-adaptive; HVS-guided or learned saliency maps could improve quality/robustness.
- Very low-resolution or heavily compressed sources reduce headroom for imperceptible embedding.

CONCLUSION :

We implemented a blind, frequency-domain watermarking pipeline that achieves high visual quality and robust detection against common signal processing, with partial resilience to mild geometric transformations. Key ingredients include DWT-DCT embedding, spread-spectrum modulation, and key-based coefficient selection. Experiments support practical operating points with PSNR around 40 dB and strong NCC under JPEG and noise/blur conditions.Future enhancements should focus on:

- Synchronization: templates or feature-invariant embedding to counter rotation/scale/cropping.
- Content-adaptive embedding: HVS-aware or learned models to optimize α locally.
- Extended media: scaling to video and integrating cryptographic primitives for end-to-end authenticity.