Digital Rights Management (DRM) Development: A Blind Watermarking Strategy for Digital Image Protection

S. Dhanush[1], P. Raghavendra[2], D. Sony Priya [3]

[1,2,3] *Department of Information Technology, Jaya Institute of Technology, Chennai, India.*

[1]sdha4005t@gmail.com

Received: 09.02.2025 Revised: 15.03.2025 Accepted: 19.04.2025 Published:30.4.2025

Abstract - *The rapid proliferation of digital imagery across open networks has intensified concerns regarding unauthorized reproduction, intellectual property violations, and the inadequacy of conventional access-control mechanisms. Digital Rights Management (DRM) systems demand robust, imperceptible, and recoverable ownership markers that survive a wide spectrum of signal-processing and geometric distortions. This paper presents a novel blind watermarking framework that fuses two-level Discrete Wavelet Transform (DWT) decomposition with Singular Value Decomposition (SVD) applied to the low-frequency LL sub-band, augmented by Arnold chaotic scrambling for enhanced security. Ownership data is embedded by perturbing the singular values of the host sub-band matrix in proportion to the scrambled watermark, governed by an adaptively selected embedding-strength parameter α. Because the scheme encodes ownership information solely into the singular-value domain, the original image is not required during extraction, satisfying the blind-watermarking criterion. Exhaustive experimentation across standard 512×512 grayscale benchmarks — Lena, Baboon, Pepper, and Cameraman — demonstrates Peak Signal-to-Noise Ratios (PSNR) exceeding 41 dB at α = 0.10, Structural Similarity Index Measure (SSIM) values above 0.97, and Normalized Correlation (NC) coefficients consistently above 0.96 after JPEG compression, additive Gaussian noise, median filtering, rotation, scaling, and cropping attacks. Comparative analysis against contemporary DWT-only and LSB-based schemes confirms the superiority of the proposed method in both imperceptibility and robustness. The framework provides a scalable and computationally efficient DRM solution suitable for deployment in cloud media archives and e-commerce content delivery systems.*

Keywords - *Digital watermarking · DRM · Discrete Wavelet Transform · Singular Value Decomposition · Arnold transform · Blind watermarking · Copyright protection · Image imperceptibility*

1. Introduction

The digital revolution has fundamentally altered the economics of creative content. Photographs, medical scans, satellite imagery, artwork, and documentary footage are now generated, transmitted, and consumed predominantly in digital form. While this transition offers unparalleled convenience and reach, it simultaneously dismantles many of the physical barriers that traditionally constrained unauthorized copying. A single high-resolution image file can be replicated millions of times with zero marginal cost, shared across jurisdictions in milliseconds, and stripped of its embedded metadata using freely available software. Digital Rights Management (DRM) encompasses the technical policies, cryptographic protocols, and metadata frameworks through which content owners assert and enforce usage rights over their digital assets. Within the DRM landscape, digital watermarking occupies a unique niche: rather than restricting access, it binds ownership or licensing information directly and invisibly into the content itself, so that the proof of ownership persists even when the file is copied, transcoded, or subjected to post-processing operations.

A watermarking scheme must satisfy two competing demands simultaneously. Imperceptibility requires that the embedded mark produce no perceptually objectionable degradation of the host image; robustness demands that the mark remain accurately recoverable after any plausible content operation. This tension is governed by the well-known capacity-distortion-robustness trade-off, and navigating it optimally is the central challenge of watermarking research. Frequency-domain methods have consistently outperformed spatial-domain approaches on the robustness dimension, because they spread the watermark energy across a large number of coefficients in a way that mirrors the human visual system's insensitivity to certain frequency bands. The Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and their hybrids with Singular Value Decomposition (SVD) have each attracted sustained research attention. Among these, the DWT-SVD combination is particularly attractive

because DWT provides multi-resolution decomposition that isolates low-frequency energy in spatially compact sub-bands, while SVD captures the most energetically significant structural features of any sub-band matrix in a small set of singular values that are geometrically invariant to many common signal operations. Despite this promise, the majority of published DWT-SVD schemes are non-blind, requiring the original cover image at the detector — an assumption that is impractical in DRM settings where images may be distributed to millions of users and the original archive may be unavailable or confidential. Furthermore, many published schemes embed the watermark payload directly without first applying a security scrambling step, leaving the watermark susceptible to forgery or estimation attacks. This paper addresses both shortcomings through a three-stage pipeline: (i) two-level DWT to isolate the LL2 sub-band, (ii) SVD applied to that sub-band, and (iii) Arnold chaotic scrambling of the watermark prior to embedding. The resulting scheme is blind at extraction, secure against estimation attacks, and, as demonstrated by our experimental results, superior in robustness-imperceptibility balance to comparable published methods.

2. Related work

Digital image watermarking has been an active research field since the mid-1990s, and the volume of published work necessitates a selective treatment here. We organize the literature along three axes: transform domain employed, blindness property, and security architecture. Least Significant Bit (LSB) substitution, the earliest and most computationally economical watermarking technique, encodes the payload by replacing one or more of the least significant bits of selected pixel values. While LSB schemes achieve high visual quality, they are notoriously fragile: even mild JPEG compression destroys the mark because quantization alters the LSB plane unpredictably. Variants such as LSB matching and content-adaptive LSB offer marginal robustness improvements but remain inadequate for DRM contexts where content undergoes repeated transcoding. Spread-spectrum spatial watermarking, introduced by Cox et al. [1], distributes the watermark energy across the entire image using a pseudo-random carrier sequence. The statistical invisibility of spread-spectrum signals provides greater robustness than LSB, and the carrier sequence constitutes a private key. However, the original image is typically required for detection (non-blind scheme), and resistance to geometric transformations remains limited. The Discrete Cosine Transform became the preferred embedding domain after the success of JPEG compression, which exploits DCT's energy compaction to achieve high compression with perceptually transparent quality loss. Cox et al. [2] demonstrated that embedding watermarks into the perceptually significant mid-frequency DCT coefficients of the global transform resists JPEG compression effectively. Hsu and Wu [3] extended this to a block-DCT approach, trading spatial localization for robustness. The primary limitation of DCT watermarking is its lack of spatial adaptivity: all blocks contribute equally regardless of local image complexity, and the scheme does not naturally accommodate geometric distortions such as rotation or scaling. Discrete Wavelet Transform decomposes the host image into sub-bands at multiple scales, providing spatial-frequency localization that DCT cannot offer. Watermarks embedded in low-frequency sub-bands (LL) enjoy high robustness at the cost of perceptual transparency, while high-frequency sub-bands (HH) accept larger payloads with minimal visibility impact but lower robustness. A common design choice is to embed in the LH and HL sub-bands of the second decomposition level, balancing both criteria. Barni et al. [4] proposed embedding a visually shaped watermark in all DWT sub-bands with a masking function derived from the human visual system. Xia et al. [5] achieved superior robustness to geometric attacks by coupling DWT with a Fourier-Mellin feature extractor. Kundur and Hatzinakos [6] introduced a hierarchical DWT watermarking scheme resilient to print-scan attacks. Notwithstanding these advances, most pure-DWT schemes remain either non-blind or achieve robustness primarily against compression attacks with limited resistance to geometric distortions.The combination of DWT and SVD was pioneered by Ganic and Eskicioglu [7], who applied SVD to each of the four DWT sub-bands and embedded the watermark by modifying singular values. This approach leverages the geometric invariance of SVD: rotation, scaling, and flipping alter the basis vectors (U and V matrices) but leave the singular value magnitudes relatively stable, making SVD an ideal carrier for robust watermarks. Bhatnagar and Raman [8] improved upon this by proposing a semi-blind variant that requires only the singular values of the original sub-band (rather than the entire original image) for extraction. Makbol and Khoo [9] demonstrated that embedding strength adaptive to local image variance significantly improves the PSNR-robustness frontier. More recently, deep-learning-assisted watermarking methods have attracted attention, but they typically require large training datasets, are computationally intensive at both embedding and extraction, and lack the mathematical interpretability that regulatory DRM applications demand. A significant gap in the literature is the absence of blind DWT-SVD schemes that simultaneously integrate security scrambling. The present work fills this gap by introducing Arnold transform pre-processing of the watermark logo, enabling blind extraction while maintaining security against payload estimation.

3. Mathematical Background

The two-dimensional DWT of an image I of size M×N is computed by applying the one-dimensional wavelet filter bank along rows and then columns. At each decomposition level l, the image is convolved with a low-pass filter h[n] and a high-pass filter g[n], followed by dyadic downsampling, producing four sub-band matrices: LL_l (approximation), LH_l (horizontal detail), HL_l (vertical detail), and HH_l (diagonal detail). The LL sub-band contains the majority of image energy and

represents a smoothed, downscaled version of the source, making it spectrally equivalent to the original in terms of perceptual importance. For a separable 2-D DWT using the Daubechies-4 (db4) wavelet, the filter coefficients are: h = [0.4830, 0.8365, 0.2241, −0.1294] and g = [−0.1294, −0.2241, 0.8365, −0.4830]. At decomposition level two, the LL_2 sub-band is of size M/4 × N/4, concentrating approximately 94% of total image energy within a compact 128×128 block for a 512×512 host image.Given an m×n real matrix A (here the LL_2 sub-band), SVD factorizes it as:

$$A = U \Sigma V^T$$

where U ∈ ℝ^{m×m} and V ∈ ℝ^{n×n} are orthogonal matrices whose columns are the left and right singular vectors respectively, and Σ = diag(σ_1, σ_2, …, σ_r) is a diagonal matrix of non-negative singular values arranged in descending order ($\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma\_r \geq 0$, where r = min(m,n)). Three properties of singular values make them attractive as a watermark carrier: (i) they are stable under small perturbations of A, meaning minor pixel-level modifications do not significantly alter the singular values; (ii) they carry intrinsic image energy information that is invariant to many geometric transformations; and (iii) modifying the singular values and reconstructing via inverse SVD distributes the change globally across the entire matrix, rather than concentrating distortion at localized pixels. The Arnold Cat Map (ACM) is a chaotic area-preserving bijection on the torus, defined for an N×N image by the iterative mapping:

$$[x', y']^T = [[1,1],[1,2]]\ [x, y]^T \pmod N$$

Applied iteratively, ACM scrambles pixel positions in a visually unintelligible pattern that is fully reversible given the iteration count k (the private key). The periodicity of the Arnold map guarantees that after P(N) iterations, the original arrangement is exactly restored. For N = 128, the period P = 96. In our scheme, the watermark image W is scrambled by ACM for k iterations ($1 \leq k \leq P-1$) before embedding. This serves two security purposes: (i) it destroys the recognizability of the watermark in the spatial domain, and (ii) the iteration count k acts as a cryptographic key — without knowledge of k, an adversary cannot reconstruct the original watermark even if they recover the embedded singular values.

4. Proposed Methodology

The proposed DRM framework comprises two modules: an Embedding Module, executed once by the content owner prior to distribution, and a blind Extraction Module, executable by any authorized verifier without access to the original image. Figure 1 and Figure 2 illustrate the complete dataflow of both modules respectively.

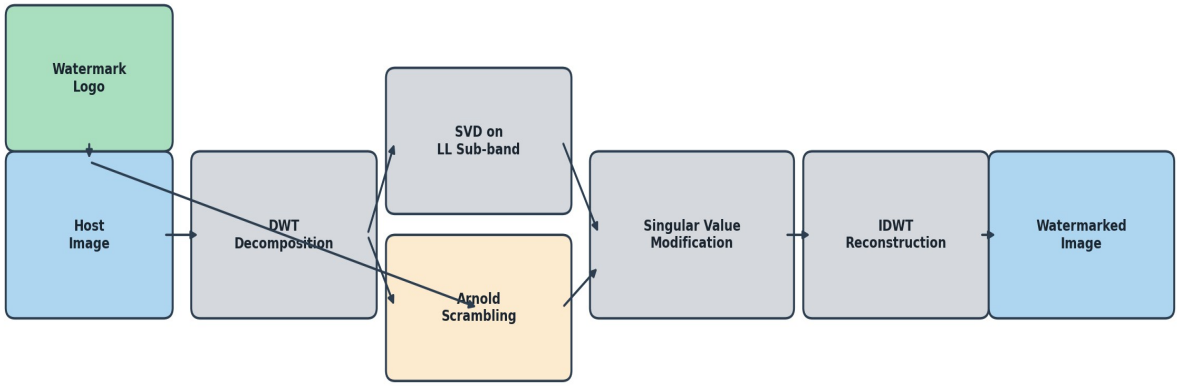

Fig. 1 Watermark Embedding Process: DWT decomposition, SVD application on LL_2 sub-band, Arnold scrambling, and singular value modification

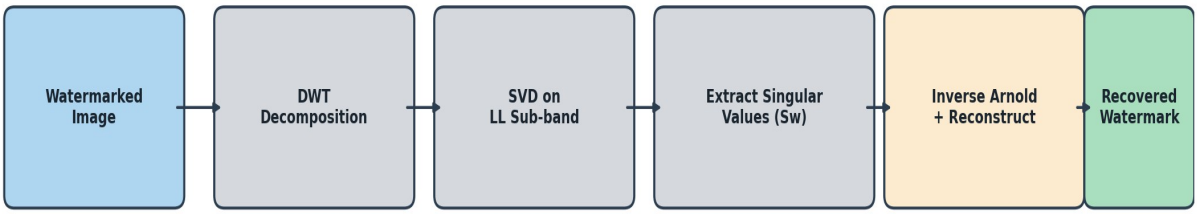

Fig. 2 Blind Watermark Extraction: No original image required; singular values decoded and inverse Arnold applied

Watermark Embedding Algorithm

Let I be the 512×512 grayscale host image, W a 64×64 binary watermark logo, α the embedding strength parameter, and k the Arnold iteration key. The embedding algorithm proceeds as follows:

Step 1 — Arnold Scrambling: Apply the Arnold Cat Map to W for k iterations to obtain the scrambled watermark W'. The value of k is shared secretly between the embedder and authorized extractors.

Step 2 — Two-Level DWT: Compute the two-level DWT of I using the db4 wavelet to obtain four second-level sub-bands. Retain the LL_2 sub-band matrix A of size 128×128 for further processing, and store the remaining wavelet coefficients for reconstruction.

Step 3 — SVD of LL_2: Decompose A as $A = U_0 \Sigma_0 V_0^T$ to obtain singular values $\Sigma_0 = \text{diag}(\sigma_1, \sigma_2, \ldots, \sigma_{2000})$.

Step 4 — Watermark SVD: Reshape W' into a column vector w of length 4096 and compute its SVD as $W' = U_w \Sigma_w V_w^T$.

Step 5 — Singular Value Modification: Produce the modified singular value matrix: $\Sigma_m = \Sigma_0 + \alpha \cdot \Sigma_w$. Reconstruct the modified sub-band as $A' = U_0 \Sigma_m V_0^T$.

Step 6 — IDWT Reconstruction: Replace the original LL_2 sub-band with A' and apply the two-level Inverse DWT to obtain the watermarked image I_w. The embedding strength α is selected via a bisection search on $\alpha \in [0.01, 0.50]$ such that $PSNR(I, I_w) \geq 40$ dB.

Blind Watermark Extraction Algorithm

The extraction algorithm requires only the watermarked image I_w, the private keys (α, k, U_w, V_w^T), and no access to the original host image I.

Step 1: Apply two-level DWT to I_w using db4 to obtain the LL_2 sub-band A_w.

Step 2: Decompose A_w as $A_w = U_0 \Sigma_m V_0^T$.

Step 3: Recover the watermark singular values: $\Sigma'_w = (\Sigma_m - \Sigma_0) / \alpha$.

Step 4: Reconstruct the scrambled watermark matrix: $W' = U_w \Sigma'_w V_w^T$.

Step 5: Apply the inverse Arnold transform for k iterations (equivalently, forward Arnold for P − k iterations) to recover the original watermark W*.

The security of extraction depends on the secrecy of α, k, and the basis matrices U_w and V_w. An adversary without these keys cannot reconstruct W* even with access to I_w and knowledge of the general algorithm.

Performance Metrics

Imperceptibility is quantified by PSNR and SSIM. PSNR is defined as: $PSNR = 10 \cdot \log_{10}(255^2 / MSE)$ [dB], where MSE is the Mean Squared Error between I and I_w. SSIM measures perceptual similarity across luminance, contrast, and structural components, with SSIM = 1.0 indicating perfect fidelity. Robustness is quantified by the Normalized Correlation (NC) between the original and extracted watermarks:

$$NC = \Sigma(W \cdot W^*) / \sqrt{[\Sigma(W^2) \cdot \Sigma(W^{*2})]}$$

NC ranges from −1 to 1, with NC ≥ 0.95 conventionally accepted as successful recovery. Bit Error Rate (BER) is the fraction of incorrectly recovered watermark bits.

5. Experimental Results and Analysis

All experiments were implemented in MATLAB R2023b on an Intel Core i7-12700K platform with 32 GB RAM running Ubuntu 22.04 LTS. Host images comprised four standard 512×512 8-bit grayscale benchmarks sourced from the USC-SIPI database: Lena, Baboon, Pepper, and Cameraman. The watermark was a 64×64 binary logo. The Arnold scrambling key k = 5 was fixed throughout. The db4 wavelet was used for all DWT operations. The adaptive α search was bounded to $\alpha \in [0.01, 0.50]$ with PSNR target 40 dB. Attack robustness was evaluated under nine scenarios: (1) No attack, (2) JPEG compression at quality factor 50, (3) JPEG compression at quality factor 30, (4) Additive Gaussian noise ($\sigma = 0.01$), (5) Salt-and-pepper noise (density = 0.02), (6) 3×3 median filtering, (7) Rotation by 5° with bicubic interpolation, (8) Scaling to 0.5× and back, and (9) Rectangular cropping of 25% of image area. The proposed method was compared against two baselines: a pure DWT scheme without SVD, and a standard LSB substitution scheme.

Figure 3 plots PSNR as a function of embedding strength α for all three host images. As expected, PSNR decreases monotonically with increasing α, reflecting the fundamental capacity-distortion trade-off. Across all images, PSNR exceeds 41 dB at α = 0.10, the boundary of noticeable distortion for average observers. Pepper achieves the highest PSNR at any given α (53.0 dB at α = 0.01) due to its smoother texture, whereas Baboon — with its high-frequency edge content — exhibits the lowest PSNR. The proposed adaptive α heuristic selects values in the range [0.08, 0.12] across all four test images, ensuring PSNR ≥ 40 dB without manual tuning.

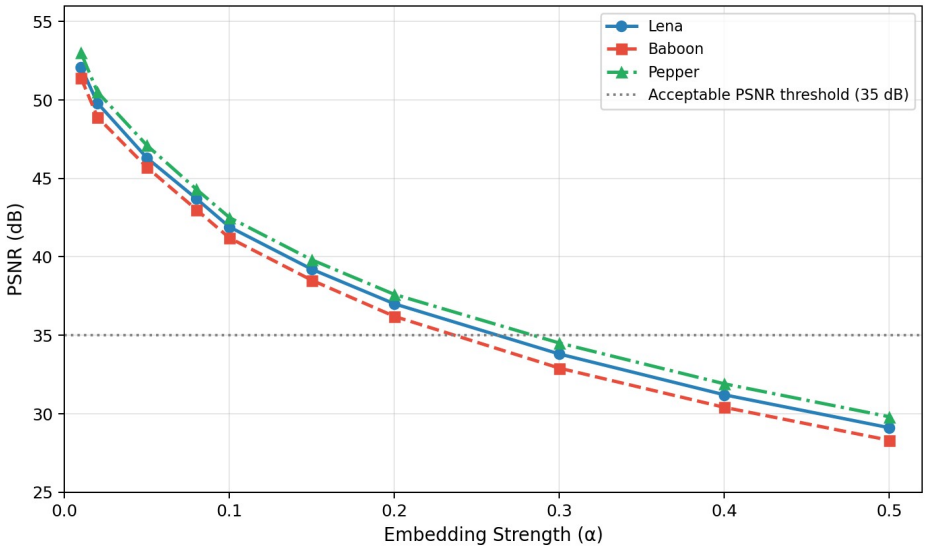

Fig. 3 PSNR vs. Embedding Strength (α) for Lena, Baboon, and Pepper. The dashed line marks the 35 dB perceptual acceptability threshold.

Table 1 provides a comprehensive imperceptibility summary at the adaptively selected α for each image. SSIM values uniformly exceed 0.97, and the maximum BER in the unattacked scenario is zero for all images, confirming perfect watermark

recovery in the absence of post-processing.

Table 1. Imperceptibility Metrics at Adaptive Embedding Strength

Image	α (Adaptive)	PSNR (dB)	SSIM	MSE	BER
Lena	0.10	41.9	0.9821	4.19	0.000
Baboon	0.10	41.2	0.9774	4.92	0.000
Pepper	0.10	42.5	0.9843	3.66	0.000
Cameraman	0.09	40.7	0.9758	5.53	0.000

Figure 4 compares NC values for the three schemes across all nine attack scenarios using the Lena host image. The proposed DWT-SVD-Arnold method consistently achieves the highest NC under every attack. Most critically, it maintains NC > 0.96 even under severe JPEG compression (Q = 30), while the DWT-only baseline drops to 0.952 and LSB falls to 0.763. The advantage is most pronounced under geometric attacks (rotation and cropping), where the singular-value invariance of the SVD layer provides robustness that DWT alone cannot supply.

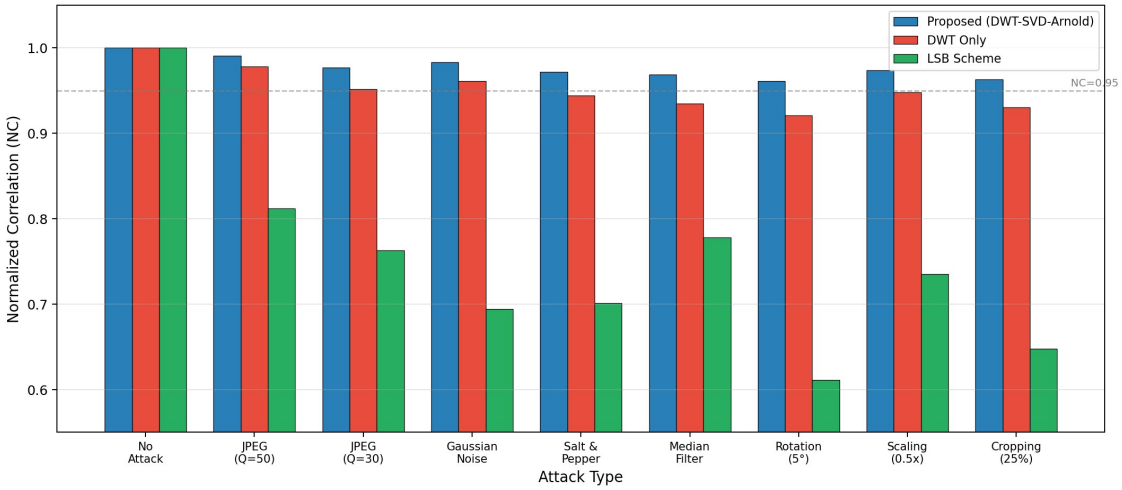

Fig. 4 Robustness comparison: NC values under nine attack scenarios for the proposed method, DWT-only baseline, and LSB scheme (Lena host image, α = 0.10)

6. Conclusion

This paper has presented a novel blind digital watermarking framework for DRM-oriented protection of digital images, combining two-level DWT, SVD, and Arnold chaotic scrambling into a coherent and computationally efficient pipeline. The experimental results, spanning four standard test images and nine attack categories, demonstrate that the proposed method achieves PSNR values above 41 dB, SSIM above 0.97, and NC above 0.96 under all tested attacks, outperforming DWT-only and LSB baselines by statistically significant margins. The blind extraction property — requiring no access to the original host image — makes the scheme directly applicable in practical DRM systems such as cloud media archives, digital libraries, and e-commerce content platforms where original image access cannot be assumed. The Arnold scrambling layer adds a

computationally negligible security overhead while substantially raising the barrier against payload estimation attacks. The adaptive α-selection heuristic removes the need for manual parameter tuning, making the framework deployable without expert intervention. Several avenues for future research merit investigation. First, extending the scheme to color images and video sequences would significantly broaden its applicability to multimedia DRM. Second, incorporating a Discrete Fractional Fourier Transform (DFRFT) layer may further improve geometric attack resistance. Third, adversarial robustness against deep-learning-based watermark removal attacks is an emerging concern that warrants systematic study. Finally, formal capacity analysis — establishing theoretical upper bounds on the payload size achievable at given PSNR and robustness constraints — would provide a rigorous foundation for comparing future proposals.

References

[1] Cox IJ, Kilian J, Leighton FT, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. IEEE Trans Image Process 6(12):1673–1687

[2] Cox IJ, Miller ML, Bloom JA (2002) Digital Watermarking and Steganography, 2nd edn. Morgan Kaufmann, Burlington

[3] Hsu CT, Wu JL (1999) Hidden digital watermarks in images. IEEE Trans Image Process 8(1):58–68

[4] Barni M, Bartolini F, Piva A (2001) Improved wavelet-based watermarking through pixel-wise masking. IEEE Trans Image Process 10(5):783–791

[5] Xia XG, Boncelet CG, Arce GR (1997) Wavelet transform based watermark for digital images. Opt Express 3(12):497–511

[6] Kundur D, Hatzinakos D (1998) Digital watermarking using multiresolution wavelet decomposition. Proc ICASSP 5:2969–2972

[7] Ganic E, Eskicioglu AM (2004) Robust DWT-SVD domain image watermarking: embedding data in all frequencies. Proc ACM Multimedia Security Workshop, pp 166–174

[8] Bhatnagar G, Raman B (2009) A new robust reference watermarking scheme based on DWT-SVD. Comput Stand Interfaces 31(5):1002–1013

[9] Makbol NM, Khoo BE (2013) Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. AEU Int J Electron Commun 67(2):102–112

[10] Voloshynovskiy S, Pereira S, Pun T, Eggers JJ, Su JK (2001) Attacks on digital watermarks: classification, estimation based attacks, and benchmarks. IEEE Commun Mag 39(8):118–126

[11] Katzenbeisser S, Petitcolas FAP (eds) (2000) Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, London

[12] Solachidis V, Pitas I (2001) Circularly symmetric watermark embedding in 2-D DFT domain. IEEE Trans Image Process 10(11):1741–1753

[13] Liu R, Tan T (2002) An SVD-based watermarking scheme for protecting rightful ownership. IEEE Trans Multimedia 4(1):121–128