Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Artificial Protozoa Optimizer for Enhanced Robust and Secure Image Watermarking

Hadouda Ali[1], Trache Najia[2], Khelfi Mohamed Fayçal[3]
[1] *RIIR Laboratory, Department of Computer Science, Université Oran1, Oran 31000, Algeria*
E-mail : hadouda.ali@edu.univ-oran1.dz | alihadouda111@gmail.com
[2] *RIIR Laboratory, Department of Computer Science, Université Oran1, Oran 31000, Algeria*
E-mail : trache.najia@univ-oran1.dz | n_khelfi@yahoo.fr
[3] *RIIR Laboratory, Department of Computer Science, Université Oran1, Oran 31000, Algeria*
E-mail : Khelfi.faycal@univ-oran1.dz | mf_khelfi@yahoo.fr

ARTICLE INFO

Received: 31 Dec 2024

Revised: 20 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

Digital image watermarking faces significant challenges in balancing imperceptibility and robustness under diverse distortions. With the growing prevalence of deepfake and image manipulation technologies, preserving the authenticity and integrity of digital images has become increasingly critical. This paper presents a novel hybrid optimization-based framework for digital image watermarking, integrating the Arnold Transform (AT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), and the Artificial Protozoa Optimizer (APO). The watermark, such as a QR code, is first encrypted using the Arnold Transform and embedded into the low-frequency sub-band via SVD, while the APO determines the optimal scaling factor α through an objective function combining the Structural Similarity Index Measure (SSIM) and Normalized Cross-Correlation (NCC) ensuring an optimal balance between imperceptibility and robustness. Experiments on a diverse set of images, including medical (e.g., MRI and chest X-ray) and standard benchmark images (e.g., Baboon, Peppers), demonstrate that the proposed framework achieves high SSIM and NCC, along with low Learned Perceptual Image Patch Similarity (LPIPS) and Bit Error Rate (BER). These metrics ensure accurate watermark extraction under attacks such as JPEG compression, noise, and rotation, while supporting ownership protection and multimedia authentication.

Keywords: Artificial Protozoa Optimizer, Image Watermarking, Scaling Factor, Objective function, QR code, Medical Image, Robustness, Imperceptibility

INTRODUCTION

With the rapid advancement of digital technologies, protecting multimedia content against unauthorized use and tampering has become a critical challenge, Digital image watermarking is a widely studied technique that Embeds imperceptible information, called a watermark, into a host image for purposes such as copyright protection, authentication, and data integrity verification [1,2]. Watermarking methods are generally categorized into spatial and frequency domain techniques. Spatial domain methods, such as Least Significant Bit (LSB) modification, directly manipulate pixel values, to embed watermarks into the image's spatial structure [3]. Frequency domain [4] techniques address these limitations by embedding watermarks into transformed coefficients of the image using methods such as Transform (DCT) [5], the Discrete Fourier Transform (DFT) [6], Discrete Wavelet Transform (DWT) [7,8], Singular Value Decomposition (SVD) [9,10], and Hessenberg Decomposition (HD) [11]. These methods leverage energy compaction to embed watermarks in high-energy regions, which are less susceptible to manipulations, thereby enhancing their effectiveness. However, existing watermarking techniques still face significant challenges in achieving an optimal trade-off between imperceptibility and robustness [12]. Traditional methods often lack adaptability to varying image characteristics, resulting in inconsistent performance under complex attack scenarios. Furthermore, many existing approaches fail to dynamically optimize the embedding parameters, which limits their ability to maintain a good balance between robustness and imperceptibility. To address this trade-off, recent studies have investigated the use of metaheuristic optimization algorithms have been

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

widely applied in digital image watermarking to enhance performance and adapt embedding parameters Among the most commonly used methods are Particle Swarm Optimization (PSO) [13], Artificial Bee Colony (ABC) [14], Ant Colony Optimization (ACO) [15], Cuckoo Search Algorithm (CSA) [16], Fruit Fly Optimization Algorithm (FOA) [17], and recently Forensic-Based Investigation (FBI) [18]. These optimizers aim to automatically adjust critical embedding parameters to improve both robustness and imperceptibility. In particular, a key parameter is the scaling factor, which controls the strength of the watermark. By fine-tuning this parameter, the optimizers can maximize performance metrics such as SSIM, NCC, LPIPS, and BER, even under various attacks. Addressing these optimization challenges is essential to advance watermarking technologies, notably in security-critical domains [19] and multi-media authentication [2021]. This study presents a novel optimization-based watermarking framework that combines Arnold Transform (AT) [22], DWT, and SVD. The DWT enables imperceptible embedding in the low-frequency sub band, while SVD enhances robustness against noise and compression. The Artificial Protozoa Optimizer (APO) [23] determines the optimal scaling factor using a custom objective function that balances imperceptibility (SSIM) and robustness (NCC), achieving adaptive and efficient watermark embedding. The key contributions of this study are as follows:

- A hybrid watermarking framework integrating AT, DWT, and SVD.
- An optimization strategy based on APO for adaptive embedding.
- A custom objective function combining SSIM and NCC.
- Experimental results demonstrate significant improvements in SSIM, NCC, LPIPS, and BER under various attacks.

The remainder of this paper is organized as follows. Section 2 presents a comprehensive review of related work. Section 3 introduces the preliminaries and the methodological foundations of the proposed framework, and Section 4 reports the experimental results and provides comparative analyses against state-of-the-art approaches.

RELATED WORKS

This section reviews digital image watermarking techniques, with a focus on optimization-based methods, hybrid transform-domain approaches, and metaheuristic algorithms. These methods aim to address two major challenges: robustness against various attacks and imperceptibility to pre-serve the host image's visual quality. Despite considerable progress, key limitations persist, particularly in selecting the optimal scaling factor. Numerous hybrid techniques, such as DWT-DCT [24], DWT-SVD-HD [25], and DWT-SVD [26], have been proposed to improve performance. However, the effectiveness of these methods largely depends on how well the scaling factor balances robustness and invisibility. To overcome this, several studies have integrated metaheuristic optimization methods. For instance, [27] applied PSO to optimize the scaling factor in a robust medical image watermarking scheme that combines redundant discrete wavelets transform (RDWT), HD, and randomized singular value decomposition (RSVD). The method embeds dual watermarks text and image based Electronic Patient Records (EPRs) to achieve a balance between imperceptibility and robustness. Similarly, in [28] PSO is integrated with the Contourlet transform and SVD to enhance resistance to common attacks while improving watermark imperceptibility. In [29] ABC algorithm is employed to optimize the scaling factor in a semi-blind color image watermarking scheme based on DWT, SVD, and HD. The color watermark is first scrambled using the Arnold transform to enhance security, then embedded into the Y (luminance) channel of the host image in the YCbCr color space. The proposed method achieves high imperceptibility and robustness, as demonstrated by strong PSNR and NCC values, and shows resilience against various image processing and geometric attacks. In [30], the CSA was applied in the wavelet domain to optimize scaling factors, improving robustness against compression and noise, in [31] a blind image watermarking scheme based on Lifting Wavelet Transform (LWT) is proposed, embedding binary watermarks and using Hu's invariant moments for extraction. A stochastic Firefly algorithm is applied to optimize PSNR and SSIM, showing improved performance over benchmark techniques. and [32] FBI algorithm for watermark security, achieving high imperceptibility and robustness against various attacks incorporated Arnold Transform for watermark encryption to enhance security, combined with DWT and SVD for robust and efficient image watermarking. Despite their strengths, optimization-based methods face challenges such as computational inefficiency and difficulty in adapting to diverse attack conditions, [25] A hybrid method based on the Fruit Fly Optimization Algorithm (FOA), Integer Wavelet Transform (IWT), HD, and SVD was proposed to improve resilience to false positives and noise-based attacks.

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

However, frequency-domain methods often prioritize robustness at the expense of imperceptibility and may struggle to effectively handle geometric distortions. In [33], a blind watermarking method combining IWT, SVD, and chaos models is proposed. The scheme introduces multiple scaling factor (MSF) matrices generated from chaotic keys to control the embedding strength. This improves robustness and imperceptibility while enhancing security and overcoming false positives and capacity limitations. In [34] a hybrid image watermarking technique combining 4-level DWT and 2-level SVD with Arnold encryption. The scheme optimizes the trade-off between imperceptibility and robustness by using a dynamically sized watermark to resist various attacks. To overcome these challenges, this paper proposes a robust hybrid-watermarking framework in which the Artificial Protozoa Optimizer (APO) plays a central role, adaptively determining the optimal scaling factors through a custom objective function that balances imperceptibility and robustness. The framework integrates DWT, SVD, and the Arnold Transform to embed and secure the watermark, significantly enhancing its resilience against various attacks.

PRELIMINARIES AND METHODLOGY

This section presents the main mathematical formulations and methodological steps involved in the proposed approach.

3.1 Arnold Transform, DWT, and SVD

The proposed watermarking framework integrates encryption, embedding, and extraction stages to ensure both robustness and imperceptibility, as illustrated in **Figure 1**. First, the watermark is encrypted using the Arnold transformation [22], which permutes its pixels to enhance security against attacks is given by:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \times \begin{bmatrix} x \\ y \end{bmatrix} \ mod\, N \tag{1}$$

where (x, y) and (x', y') represent the pixel coordinates before and after the Arnold Transform, respectively, and N represents the size of the square image used as the modulo parameter.

The host image I is then decomposed using the DWT [8] into four sub-bands:

$$I \longrightarrow \{DWT\}\{LL, LH, HL, HH\} \tag{2}$$

where the LL subband is selected for watermark embedding due to its stability and high energy concentration. SVD [9] is applied to both the LL subband and the encrypted watermark:

$$LL = U_I S_I V_I^T \quad W = U_W S_I V_W^T \tag{3}$$

and embedding is achieved by modifying the singular values:

$$U_{new} = S_I + \alpha\, S_W \tag{4}$$

where α is a scaling factor that controls the trade-off between imperceptibility and robustness. The modified subband is reconstructed as:

$$LL_{new} = U_I S_{new} V_I^T \tag{5}$$

and the final watermarked image is obtained by applying IDWT with LL_{new}, LH, HL, and HH. During extraction, SVD is applied to the LL subband of the watermarked image, and the embedded singular values are recovered as:

$$S_W = (S_{new} - S_I) / \alpha \tag{6}$$

Finally, the inverse Arnold transformation is applied to reconstruct the original watermark, ensuring accurate retrieval even under attacks.

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

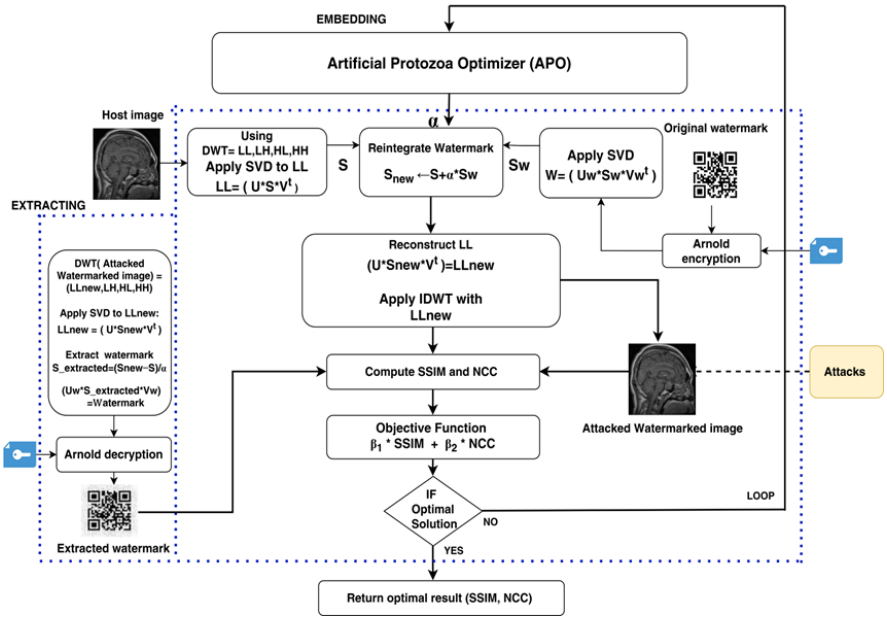

Figure 1: Proposed image watermarking framework.

3.2 Artificial Protozoa Optimizer (APO)

The APO is a nature-inspired metaheuristic optimization algorithm that mimics the foraging, reproduction, and survival mechanisms of protozoa. this algorithm is characterized by a dynamic balance between exploration and exploitation, which allows it to efficiently search complex and nonlinear solution spaces. apo relies on the collective behavior of protozoa to explore promising regions while avoiding local optima. thanks to its adaptive search strategy and low computational complexity, APO has demonstrated strong performance in solving various optimization problems across different engineering and scientific applications [23].

3.3 Objective Function and Evaluation Metrics

The paper introduces a novel objective function designed to optimize wa-termarking performance by balancing imperceptibility and robustness. Since enhancing imperceptibility often decreases robustness and vice versa, the proposed function addresses this trade-off by integrating two key metrics, SSIM and NCC. It is defined as:

$$F = \beta_1 \cdot NCC + \beta_2 \cdot SSIM \tag{7}$$

where β_1 and β_2 are weighting coefficients such that $\beta_1 + \beta_2 = 1$. Higher values of F indicate better robustness and visual quality.

The overall objective function is defined as the average of the objective values obtained for each attack scenario, including the result from the non-attacked watermarked image:

$$F_{global} = \frac{1}{N}\sum_{\{i=1\}}^{N} F_i \tag{8}$$

where F_i denotes the objective value corresponding to the i-th attack. To evaluate performance, the SSIM and NCC metrics are calculated as follows:

SSIM measures the perceptual similarity between the original image I and the watermarked image I^*:

$$SSIM(I, I^*) = \frac{\left((2\,\mu_I\mu_{\{I*\}} + C1)(2\,\sigma_{\{I\,I*\}} + C2)\right)}{\left(\left(\mu_I^2 + \mu_{\{I*\}}^2 + C1\right)\left(\sigma_I^2 + \sigma_{\{I*\}}^2 + C2\right)\right)} \tag{9}$$

Where μ_I and $\mu_{\{I*\}}$ are the mean intensities of the original and watermarked images, σ_I^2 and $\sigma_{\{I^*\}}^2$ are the variances, $\sigma_{\{I\,I^*\}}$is the covariance, and C1, C2 are constants to stabilize the formula.

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

NCC evaluates the robustness by measuring the similarity between the original and extracted watermarks:

$$NCC = \frac{(\sum\_(i=1)\^m \sum\_(j=1)\^n W(i,j)\, W\_e(i,j))}{sqrt\left(\sum_{i=1}^{m}\sum_{j=1}^{n} W(i,j)^2\right) * sqrt\left(\sum_{i=1}^{m}\sum_{j=1}^{n} W_{e(i,j)}^2\right)} \quad (10)$$

Where W(i, j) and W_e(i, j) represent pixel values of the original and extracted watermarks.

3.4 Scaling factor optimization process using APO

In this work, APO is applied to determine the optimal scaling factor α that achieves the best trade-off between imperceptibility and robustness in the watermarking process **Figure 2**. The process begins with the initialization of a population of candidate solutions α within the search space. The initial fitness of each individual is then computed using the objective function F**.** An iterative optimization loop is carried out until the maximum number of iterations is reached, at each iteration, the population is ranked according to fitness, and a subset of protozoa is selected for evolution. Each selected individual undergoes one of several adaptive behaviors inspired by protozoan life cycles : dormancy ($a_i \times U(1-\sigma, 1+\sigma)$) to maintain stability, where σ controls the uniform perturbation range; reproduction (mean of a_i and a_j, where a_j is another randomly selected individual) to promote diversity; or foraging, modeled as either autotrophic ($a_i + N(O, \sigma)$) for local search, where σ defines the Gaussian noise intensity, or heterotrophic ($a_i + B(a_j - a_k)$)**,** where a_i and a_k are two other randomly selected individuals, and B regulates their influence for global exploration. After these adaptive operations, all solutions are clipped within feasible bounds, re-evaluated using the objective function, and updated through elitist selection until convergence is reached, at which point the optimal scaling factor a_i and the minimized fitness value $(1 - F)$ are obtained.

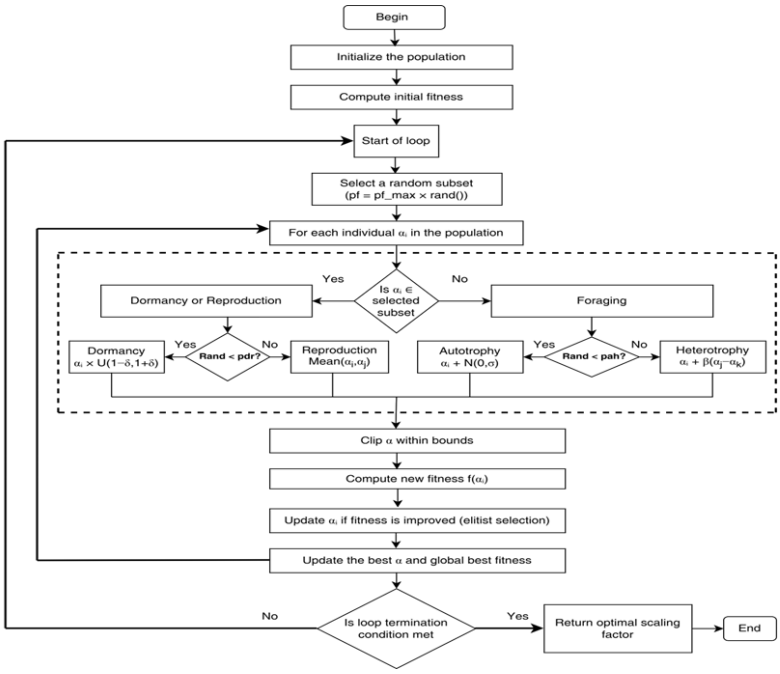

Figure 2: Scaling factor optimization using APO.

EXPERIMENTAL RESULTS

The simulation experiments were conducted in Python 3.12 on a PC equipped with an Intel® Core™ Ultra 7 155H processor (1.40 GHz) and 16 GB of RAM. The host images had a size of 512×512 pixels, while the watermark images measured 256×256 pixels. Two types of watermarks were considered in the experiments: a simple copyright mark and a QR code. The QR code watermark offers the additional advantage of embedding not only visual information but also machine-readable data, which increases robustness and facilitates reliable extraction, as illustrated in **Figure 3**. The host image was obtained from **Kaggle**, and **ImageProcessingPlace**. To evaluate the APO

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

optimizer's performance, multiple configurations were tested by varying key parameters such as population sizes (10, 50, 100) and maximum iterations (50 and 100), allowing us to assess the stability and robustness of the optimization process, as summarized in **Table 1**.

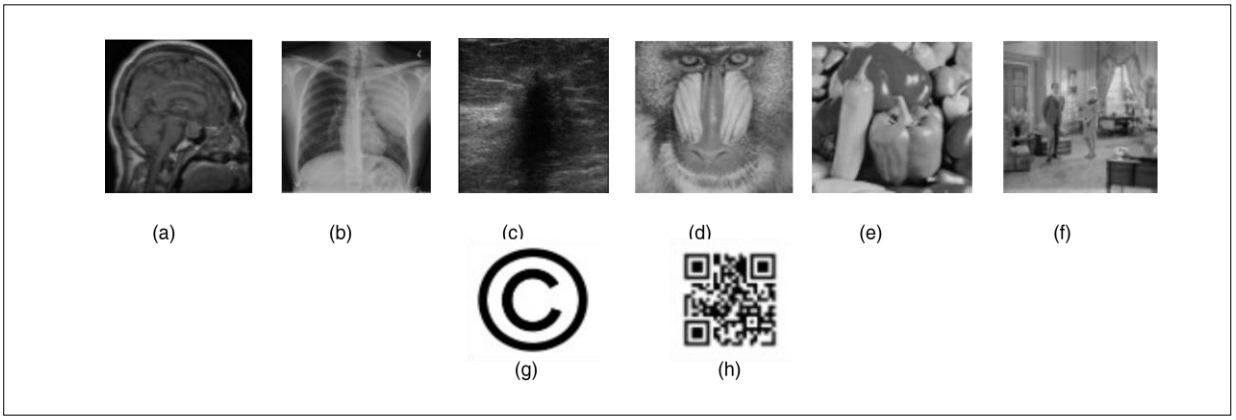

Figure 3: Test images: (a) sT1MRI, (b) Chest X-ray, (c) Ultrasound, (d) Baboon, (e) Peppers, (f) Livingroom, (g) Watermark WM 1, (h) Watermark WM 2.

Table 1: Parameter settings of the APO and Objectif function.

Parameter	Value
Population size (N)	10, 50, 100
Maximum iterations (T_{max})	50, 100
Dormancy probability (p_{dr})	0.5
Autotrophic search probability (p_{ah})	0.7
Maximum dormant proportion (p_{f_max})	0.4
Alpha initialization range	[0.01, 1]
Objective function Coefficients β_1, β_2	0.5, 0.5

Table 2: SSIM and LPIPS of the watermarked images, and NCC and BER of the extracted watermark (WM1) without attack

	sT1MRI	Baboon	Peppers	Ultras.	Ch X-ray	Living.
SSIM	0.9479	0.9833	0.9716	0.9472	0.9298	0.9762
LPIPS	0.0632	0.0158	0.0278	0.0847	0.0940	0.0226
NCC	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999
BER	0.0014	0.0020	0.0016	0.0010	0.0018	0.0014

Table 3: SSIM and LPIPS of the watermarked images,and NCC and BER of the extracted watermark (WM2) without attack

	sT1MRI	Baboon	Peppers	Ultras.	Ch X-ray	Living.
SSIM	0.9574	0.9847	0.9749	0.9524	0.9360	0.9784
LPIPS	0.0855	0.0142	0.0246	0.0757	0.0855	0.0204

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

	sT1MRI	Baboon	Peppers	Ultras.	Ch X-ray	Living.
NCC	0.9999	0.9998	0.9999	0.9999	0.9999	0.9999
BER	0.0005	0.0012	0.0008	0.0003	0.0010	0.0007

To evaluate the robustness and imperceptibility of the proposed watermarking method without attacks, **Table 2** and **Table 3** report SSIM, LPIPS, NCC, and BER metrics for different test images. The results show consistently high structural similarity (SSIM between 0.9298 and 0.9847), low perceptual distortion (LPIPS from 0.0142 to 0.0940), near-perfect watermark correlation (NCC), and minimal bit errors (BER), demonstrating high imperceptibility and accurate recoverability across diverse image types.

4.1 Results using the NCC and BER metrics

From **Figure 4**, it can be observed that the extracted watermarks correspond to cases with relatively low NCC values and correspondingly high BER values. Despite the numerical degradation, the visual content of the watermark remains recognizable. To further validate the robustness of the proposed method, these extracted watermarks were tested using standard decoding tools, such as QR code or barcode readers. The results indicate that the watermark is still decodable and correctly displays the text "**watermaking**" demonstrating that the embedded information remains intact and functionally recoverable even under severe attacks.

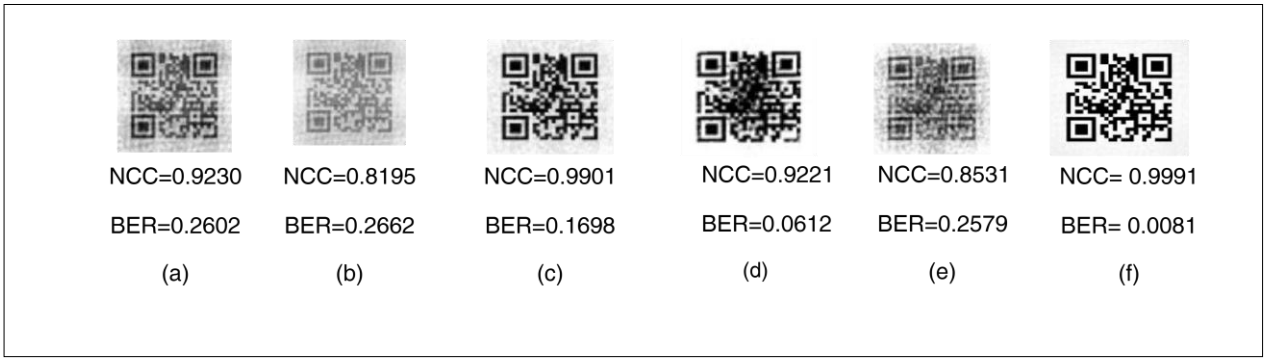

Figure 4: Extracted watermark (WM2) under the following attacks: a) Rotation 10, b) Cropping 0.25, c) JPEG 30, d) Histogram Eq, e) Average 3, f) Scaling 0.5

Table 4: NCC values of proposed method under different attacks using watermark WM1.

Attaque	ST1MRI	Baboon	Peppers	Ultras.	Chest	Living.
JPEG 50	0.9948	0.9969	0.9946	0.9965	0.9953	0.9971
JPEG 30	0.9991	0.9961	0.9896	0.9949	0.9919	0.9944
GaussNoise 0.05	0.9975	0.9991	0.9984	0.9980	0.9977	0.9984
GaussNoise 0.1	0.9938	0.9980	0.9958	0.9950	0.9950	0.9996
MedianFilter 3	0.9727	0.9452	0.9525	0.9669	0.9643	0.9247
SaltPepper 0.01	0.9890	0.9941	0.9870	0.9856	0.9912	0.9884
SaltPepper 0.05	0.9753	0.9761	0.9853	0.9615	0.9734	0.9616
Cropping 0.1	0.9598	0.9510	0.9457	0.8728	0.9199	0.9356
Cropping 0.2	0.9806	0.9078	0.8668	0.9402	0.9554	0.9305
Cropping 0.25	0.9744	0.8648	0.7982	0.9203	0.9463	0.9460
Rotation 10°	0.8999	0.9477	0.9163	0.9141	0.8591	0.8877

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Attaque	ST1MRI	Baboon	Peppers	Ultras.	Chest	Living.
Rotation 5°	0.9069	0.9555	0.9206	0.9052	0.9456	0.9321
Speckle 0.01	0.9998	0.9997	0.9997	0.9998	0.9997	0.9997
Speckle 0.05	0.9990	0.9984	0.9976	0.9987	0.9972	0.9973
Histogram Eq	0.9873	0.8933	0.8768	0.9843	0.9337	0.8687
AverageFilter 3	0.9286	0.8827	0.8409	0.9350	0.9095	0.9150
Scaling 0.5	0.9989	0.9987	0.9993	0.9990	0.9993	0.9993
Scaling 2	0.9999	0.9995	0.9999	0.9999	0.9999	0.9998

Table 5: NCC values of proposed method under different attacks using watermark WM2.

Attack	sT1MRI	Baboon	Peppers	Ultras.	Chest	Living.
JPEG 50	0.9954	0.9968	0.9945	0.9964	0.9955	0.9971
JPEG 30	0.9992	0.9964	0.9901	0.9953	0.9921	0.9944
GaussNoise 0.05	0.9969	0.9987	0.9980	0.9976	0.9970	0.9980
GaussNoise 0.1	0.9929	0.9974	0.9952	0.9944	0.9941	0.9955
MedianFilter 3	0.9725	0.9459	0.9548	0.9647	0.9651	0.9241
SaltPepper 0.01	0.9858	0.9932	0.9848	0.9818	0.9877	0.9869
SaltPepper 0.05	0.9625	0.9950	0.9849	0.9466	0.9940	0.9885
Cropping 0.1	0.9542	0.9544	0.9462	0.8754	0.9099	0.9411
Cropping 0.2	0.9811	0.9177	0.8761	0.9373	0.9573	0.9360
Cropping 0.25	0.9712	0.8791	0.8195	0.9171	0.9506	0.9076
Rotation 10°	0.9199	0.9558	0.9230	0.9332	0.8834	0.9027
Rotation 5°	0.9247	0.9606	0.9289	0.9272	0.9522	0.9413
Speckle 0.01	0.9987	0.9979	0.9995	0.9997	0.9995	0.9995
Speckle 0.05	0.9987	0.9979	0.9970	0.9983	0.9965	0.9969
Histogram Eq	0.9807	0.9016	0.9221	0.9878	0.9590	0.9376
AverageFilter 3	0.9284	0.8867	0.8531	0.9322	0.9138	0.9135
Scaling 0.5	0.9987	0.9985	0.9991	0.9988	0.9991	0.9991
Scaling 2	0.9998	0.9992	0.9997	0.9998	0.9998	0.9996

Table 4 and **Table 5** present the NCC results of the proposed method under various attack scenarios using two watermark types: WM1 (copyright logo) and WM2 (QR code). Both watermark types exhibit high robustness and reliable extraction performance across all test images. For most attacks, NCC values remain consistently above 0.99, particularly under JPEG compression, Gaussian noise, scaling, and speckle noise, where the method reaches peak correlations up to 0.9999. Slight degradations appear under cropping and rotation, where NCC values range between 0.87 and 0.96, yet the watermark remains clearly detectable. Overall, the results confirm that the proposed method achieves excellent robustness and stability for both watermark types, demonstrating effective resistance to diverse image distortions.

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 6: BER values of proposed method under different attacks using watermark WM2

Attack	sT1MRI	Baboon	Peppers	Ultras.	Ch X-ray	Living.
JPEG 50	0.1434	0.1329	0.1516	0.1960	0.1275	0.1276
JPEG 30	0.0679	0.1364	0.1698	0.1828	0.1446	0.1588
GaussNoise 0.05	0.0091	0.0091	0.0091	0.0078	0.0100	0.0090
GaussNoise 0.1	0.0152	0.0095	0.0109	0.0173	0.0130	0.0104
MedianFilter 3	0.2501	0.2604	0.2403	0.2607	0.2392	0.2632
SaltPepper 0.01	0.0431	0.0173	0.0342	0.0304	0.0194	0.0317
SaltPepper 0.05	0.0669	0.0444	0.1491	0.0345	0.0299	0.1046
Cropping 0.1	0.2662	0.2488	0.2587	0.2087	0.2640	0.1720
Cropping 0.2	0.2662	0.2518	0.2660	0.2574	0.2654	0.2268
Cropping 0.25	0.2662	0.2535	0.2662	0.2574	0.2650	0.2328
Rotation 10°	0.1851	0.2585	0.2602	0.1315	0.2005	0.2066
Rotation 5°	0.2087	0.2616	0.2641	0.1559	0.2315	0.2617
Speckle 0.01	0.0089	0.0093	0.0090	0.0036	0.0090	0.0090
Speckle 0.05	0.0089	0.0093	0.0099	0.0084	0.0108	0.0096
Histogram Eq	0.2662	0.0641	0.0612	0.2662	0.0820	0.0510
AverageFilter 3	0.2623	0.2645	0.2579	0.2651	0.2534	0.2659
Scaling 0.5	0.0083	0.0081	0.0081	0.0061	0.0086	0.0082
Scaling 2	0.0015	0.0089	0.0044	0.0004	0.0021	0.0063

In **Table 6**, the proposed method achieves very low BER values under most attacks, particularly against Gaussian noise, speckle, and scaling, where the values remain close to zero. Although slightly higher BER values are observed under stronger distortions such as median filtering, rotation or cropping, The QR-code watermark remains decodable and fully retrievable under all tested attacks. These findings demonstrate the robustness and reliability of the proposed scheme under a broad range of image processing attacks.

4.2 Comparison with Previous Works

To evaluate the proposed APO-based watermarking framework, we compared it with four recent studies from 2024–2025 that employed the same experimental settings, including a host image of size 512×512 and a watermark of size 256×256. Among these, two studies utilized Particle Swarm Optimization (PSO), a widely adopted and proven metaheuristic in recent watermarking research. Selecting PSO as a benchmark ensures a fair and objective comparison, as it allows the proposed APO framework's improvements in imperceptibility and robustness to be clearly demonstrated relative to an established reference method.

Table 7: Comparison of results with [27, 28, 33 and 34] for various attacks in terms of NCC.

Year	2024	2024	2024	2025		
Ref	[34]	[27]	[28]	[33]	Prop. (WM2)	Prop. (WM1)
Method	DWT+SVD	RDWT+HD+ RSVD	SVD+ DnCNN	IWT+SVD	DWT+SVD	DWT+SVD
Optimizer (α)	manually	PSO	PSO	chaotic MSF	APO	APO
Without attack	-	0.9992	0.9868	0.9949	**0.9999**	**0.9999**
JPEG 50	0.9946	0.9938	0.9734	0.9942	**0.9948**	**0.9954**

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

JPEG 30	-	-	-	0.9940	**0.9991**	**0.9992**
GaussNoise 0.001	-	0.9970	0.9386	-	**0.9998**	**0.9996**
GaussNoise 0.1	0.9923	-	-	0.9913	**0.9975**	**0.9929**
MedianFilter 3	-	0.9676	-	**0.9935**	0.9727	0.9725
SaltPepper 0.01	**0.9951**	-	-	0.9931	0.9890	0.9858
SaltPepper 0.001	-	0.9985	-	0.9934	**0.9992**	**0.9991**
SaltPepper 0.005	-	-	**0.9974**	-	0.9952	0.9942
Cropping 0.02	-	**0.9829**	-	-	0.9822	0.9827
Cropping 0.2	-	-	0.8704	**0.9941**	0.9806	0.9811
Rotation 1°	-	0.9287	-	-	**0.9609**	**0.9484**
Rotation 2°	-	0.9246	-	-	0.9199	**0.9283**
Rotation 30°	-	-	0.9359	-	0.9313	**0.9492**
Rotation 110°	-	-	-	**0.9934**	0.8974	0.9297
Speckle 0.01	-	-	-	0.9901	**0.9998**	**0.9996**
Speckle 0.001	-	0.9984	-	0.9931	**0.9998**	**0.9996**
Histogram Eq.	-	0.9938	-	0.9941	0.9873	**0.9987**
AverageFilter 3	-	0.9458	**0.9754**	-	0.9286	0.9284
Scaling 0.5	-	-	0.9720	-	**0.9993**	**0.9987**
Scaling 2	-	0.9535	-	-	**0.9998**	**0.9998**

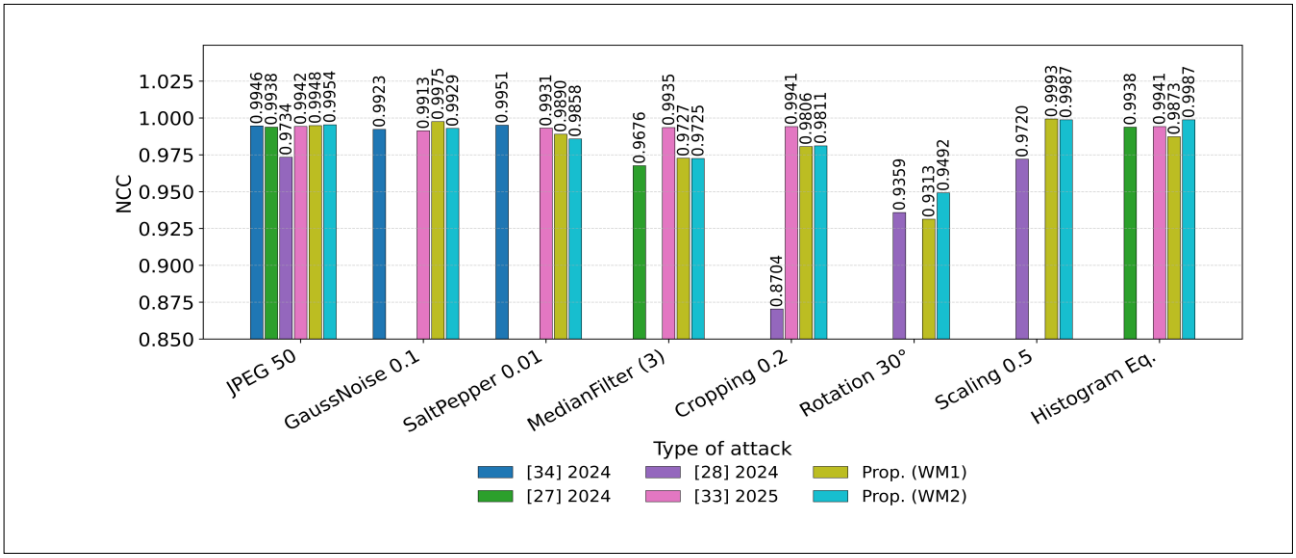

Figure 5: NCC performance comparison on the sT1MRI image with Singh et al. [27], Amiri et al. [28], Alshoura et al. [33], and Begum et al. [34].

Figure 5 and the values presented in **Table 7** provide a comprehensive comparison of the NCC values obtained under various signal and geometric attacks, demonstrating the superior performance of the proposed framework. The evaluation was performed using two watermark types, WM1 (copyright logo) and WM2 (QR code), and compared against recent methods [27,28], and [33,34]. The proposed framework consistently maintains NCC values close to 1, even under severe distortions such as JPEG compression, Gaussian noise, and filtering..., These results clearly demonstrate the remarkable robustness and high watermark extraction accuracy of the proposed methods. WM1 achieves NCC values ≥ 0.99 for most common attacks, whereas WM2 demonstrates slightly higher NCC values, particularly under rotation and histogram equalization attacks. Compared with the reference methods, the proposed framework exhibits enhanced robustness against additive noise and geometric distortions, highlighting that the use of the Artificial Protozoa Optimizer (APO) for adaptive scaling factor optimization significantly enhances the hybrid DWT–SVD framework's ability to preserve watermark fidelity, even under challenging and diverse attack scenarios.

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 8: Comparison of results with [27] for various attacks in terms of BER.

Year	2024	
Ref	[27]	Prop. (WM2)
Method	RDWT+HD+RSVD	DWT+SVD
Optimizer (α)	PSO	APO
JPEG 50	0	0.1434
GaussNoise 0.001	0	0
SaltPepper 0.001	0	0
Cropping 0.02	0.4238	**0.2509**
Rotation 1°	0.4056	**0.2292**
Rotation 2°	0.4056	**0.2206**
Histogram Eq.	0	0.2662
Average filter 3	0	0.2623

Figure 6 and **Table 8** illustrate the BER comparison between the proposed watermarking framework with WM2 and the method of [27] under various attacks applied to the sT1MRI image. The proposed approach demonstrates strong robustness against most common distortions, achieving a BER of 0 under Gaussian noise, Salt Pepper, histogram equalization, and average filtering attacks. However, slightly higher BER values are observed under geometric attacks such as cropping and rotation, which is consistent with typical watermarking behavior. Compared to [27], the proposed framework exhibits significantly lower BER values in most cases, confirming its enhanced resilience to both signal and geometric degradations.

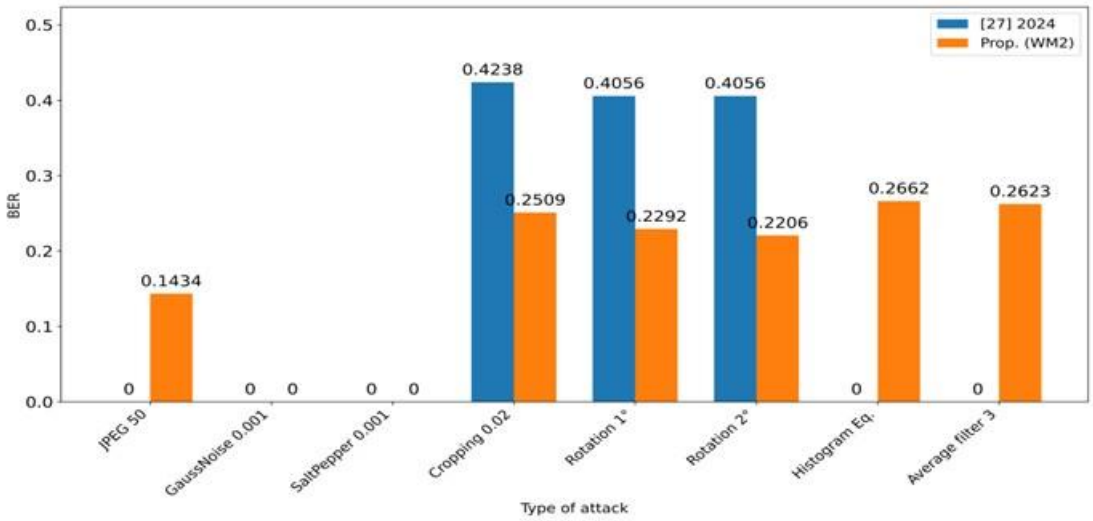

Figure 6: BER comparison with Singh et al. [27] under different attacks on the sT1MRI image.

4.3 Results of Objective Functions

The objective function evaluates the trade-off between imperceptibility and robustness, where lower values indicate better performance. As shown in **Table 9**, both WM1 and WM2 achieve low objective values, with the best results obtained for Chest image (WM1: 0.1804) and sT1MRI image (WM2: 0.1754), confirming the framework's efficiency. These results confirm that the proposed framework effectively minimizes the trade-off between imperceptibility and robustness for different types of host images under diverse attacks.

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 9: Objective Function Values for Different images.

Images	sT1MRI	Baboon	Peppers	Ultras.	Chest	Living.
WM1	0.1813	0.2268	0.2068	0.2080	**0.1804**	0.2040
WM2	**0.1754**	0.1975	0.2008	0.1947	0.1767	0.2038

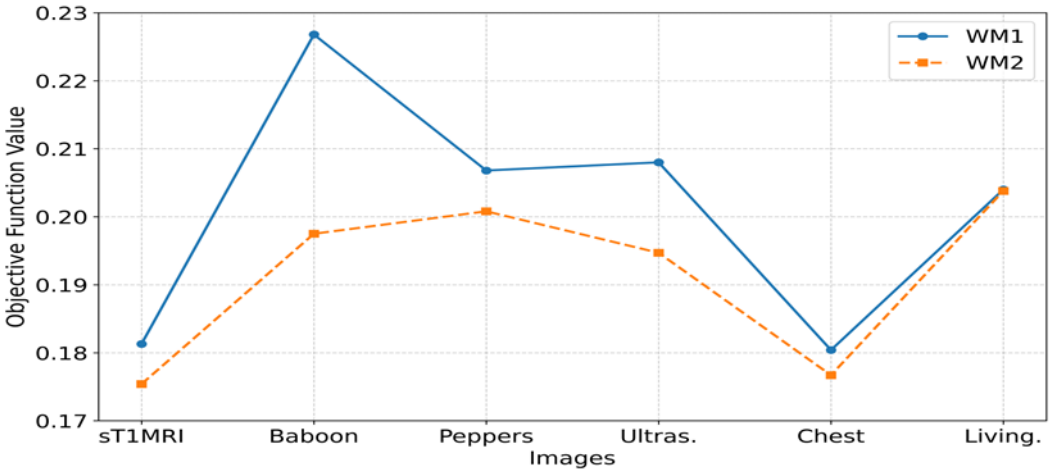

Figure 7: Variation of the objective function for different images.

CONCLUSION

The Artificial Protozoa Optimizer (APO) is an innovative, biologically inspired optimization algorithm that provides a powerful alternative to conventional approaches, such as Particle Swarm Optimization (PSO). By emulating the adaptive and intelligent behavior of protozoa, APO achieves an exceptional exploration–exploitation balance and converges rapidly toward optimal solutions. Its dynamic adjustment of watermarking parameters enables an optimal compromise between transparency and resilience, making it a highly promising tool for image authentication and bioinspired optimization research. This paper introduces a novel hybrid watermarking framework that combines AT, DWT, and SVD with the APO to determine the optimal scaling factor. A custom objective function jointly maximizes visual quality and robustness by balancing SSIM and NCC, while a weighting factor β provides additional adaptability. Experimental evaluations using SSIM, LPIPS, NCC, and BER metrics validate the stability and superior robustness of the proposed APO-driven watermarking framework against diverse attacks. In future work, the APO-based watermarking framework could be extended to color images and videos, and the objective function could be refined to further improve the balance between imperceptibility and robustness. Moreover, the framework could be adapted to enhance resilience against emerging threats, such as deepfake and other advanced image manipulation techniques.

REFRENCES

[1] Mahmood, S. D., Drira, F., Mahdi, H. F., & Alimi, A. M. (2025). Secure medical image sharing: Technologies, watermarking insights, and open issues. IEEE Access, 103995–104026.
[2] Naem, S. A. S., & Hameed, S. M. (2025). Digital watermarking techniques, challenges, and applications: A review. Mesopotamian Journal of Cybersecurity, 5(2), 453–476.
[3] Mehraj, S., Mushtaq, S., Parah, S. A., Giri, K. J., Sheikh, J. A., Gandomi, A. H., Hijji, M., & Muhammad, K. (2022). Spatial domain-based robust watermarking framework for cultural images. IEEE Access, 10, 117248–117260.
[4] Fan, Y., Li, J., Bhatti, U. A., Nawaz, S. A., & Chen, Y. (2025). Medical image hybrid watermark algorithm based on frequency domain processing and Inception V3. Advanced Intelligent Systems, 7(6), 2400654.
[5] Byun, S.-W., Son, H.-S., & Lee, S.-P. (2019). Fast and robust watermarking method based on DCT specific location. IEEE Access, 7, 100706–100718.
[6] Varghese, J., Hussain, O. B., Subash, S., & Razak, A. (2023). An effective digital image watermarking scheme incorporating DCT, DFT and SVD transformations. PeerJ Computer Science, 9, e1427.

[7] Tay, R., & Havlicek, J. (2002). Image watermarking using wavelets. In 45th Midwest Symposium on Circuits and Systems (MWSCAS), 3, III–III. IEEE.
[8] Kanwal, S., Tao, F., Taj, R., Abbas, Q., & Amin, F. (2025). Discrete cosine transform and discrete wavelet transform based hybrid method for robust and blind medical image watermarking. Peer-to-Peer Networking and Applications, 18(5), 251.
[9] Teoh, Y. J., Ling, H.-C., Wong, W. K., Chew, I. M., Basuki, T. A., & Karim, H. A. (2025). A robust SVD-based watermarking scheme using orthogonal vectors and PSO-enhanced scaling factor. Cluster Computing, 28(13), 850.
[10] Zainol, Z., Teh, J. S., Alawida, M., Alabdulatif, A., et al. (2021). Hybrid SVD-based image watermarking schemes: A review. IEEE Access, 9, 32931–32968.
[11] Su, Q., Wang, G., Lv, G., Zhang, X., Deng, G., & Chen, B. (2017). A novel blind color image watermarking based on contourlet transform and Hessenberg decomposition. Multimedia Tools and Applications, 76(6), 8781–8801.
[12] Aberna, P., & Agilandeeswari, L. (2024). Digital image and video watermarking: Methodologies, attacks, applications, and future directions. Multimedia Tools and Applications, 83(2), 5531–5591.
[13] Marini, F., & Walczak, B. (2015). Particle swarm optimization (PSO): A tutorial. Chemometrics and Intelligent Laboratory Systems, 149, 153–165.
[14] Karaboga, D., & Ozturk, C. (2011). A novel clustering approach: Artificial bee colony (ABC) algorithm. Applied Soft Computing, 11(1), 652–657.
[15] Blum, C. (2024). Ant colony optimization: A bibliometric review. Physics of Life Reviews, 51, 87–95.
[16] Mareli, M., & Twala, B. (2018). An adaptive cuckoo search algorithm for optimisation. Applied Computing and Informatics, 14(2), 107–115.
[17] Pan, W.-T. (2012). A new fruit fly optimization algorithm: Taking the financial distress model as an example. Knowledge-Based Systems, 26, 69–74.
[18] Chou, J.-S., & Nguyen, N.-M. (2020). FBI inspired meta-optimization. Applied Soft Computing, 93, 106339.
[19] Benyoucef, A., Goudjil, A., Hamadouche, M., Boutalbi, M. C., Ammar, M., & Daho, M. E. H. (2025). High-capacity DWT-SVD watermarking for MRI images embedding MITR medical information. Results in Engineering, 105795.
[20] Sharma, S., Zou, J. J., Fang, G., Shukla, P., & Cai, W. (2024). A review of image watermarking for identity protection and verification. Multimedia Tools and Applications, 83(11), 31829–31891.
[21] Malanowska, A., Mazurczyk, W., Araghi, T. K., Megías, D., & Kuribayashi, M. (2024). Digital watermarking—A meta-survey and techniques for fake news detection. IEEE Access, 12, 36311–36345.
[22] Jaiswal, S., & Pandey, M. K. (2023). Performance analysis of image watermarking for different sub-bands using LWT and Arnold map. ECTI Transactions on Computer and Information Technology (ECTI-CIT), 17(2), 278–291.
[23] Wang, X., Snášel, V., Mirjalili, S., Pan, J.-S., Kong, L., & Shehadeh, H. A. (2024). Artificial protozoa optimizer (APO): A novel bio-inspired metaheuristic algorithm for engineering optimization. Knowledge-Based Systems, 295, 111737.
[24] Kang, X.-B., Zhao, F., Lin, G.-F., & Chen, Y.-J. (2018). A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength. Multimedia Tools and Applications, 77(11), 13197–13224.
[25] Liu, J., Huang, J., Luo, Y., Cao, L., Yang, S., Wei, D., & Zhou, R. (2019). An optimized image watermarking method based on HD and SVD in DWT domain. IEEE Access, 7, 80849–80860.
[26] Araghi, T. K., & Megías, D. (2024). Analysis and effectiveness of deeper levels of SVD on performance of hybrid DWT and SVD watermarking. Multimedia Tools and Applications, 83(2), 3895–3916.
[27] Singh, K. S., & Singh, H. V. (2024). Enhancing medical image security through machine learning and dual watermarking-based technique. Automatika: ˇCasopis za automatiku, Mjerenje, Elektroniku, Raˇcunarstvo i Komunikacije, 65(4), 1579–1592.
[28] Amiri, A., & Kimiaghalam, B. (2024). Robust watermarking with PSO and DnCNN. Signal, Image and Video Processing, 18(Suppl. 1), 663–676.

[29] Sahir, M., Bekkouche, T., Belilita, F., & Amardjia, N. (2025). An optimized color image watermarking scheme based on HD and SVD in DWT domain. Engineering, Technology & Applied Science Research, 15(2), 21639–21646.
[30] Ali, M., & Ahn, C. W. (2018). An optimal image watermarking approach through cuckoo search algorithm in wavelet domain. International Journal of System Assurance Engineering and Management, 9, 602–611.
[31] Sharma, S., Malik, M., Prabha, C., Al-Rasheed, A., Alduailij, M., & Almakdi, S. (2023). Robust image watermarking using LWT and stochastic gradient firefly algorithm. Computers, Materials & Continua, 75(1), 393–407.
[32] Trache, N., Salem, M., & Khelfi, M. F. (2024). Forensic-based investigation approach for an enhanced robust and secure image watermarking scheme. Computer Science Journal of Moldova, 32(2).
[33] Alshoura, W. H., & Alawida, M. (2025). Secure and flexible image watermarking using IWT, SVD, and chaos models for robustness and imperceptibility. Scientific Reports, 15(1), 7231.
[34] Begum, M., Shorif, S. B., Uddin, M. S., Ferdush, J., Jan, T., Barros, A., & Whaiduzzaman, M. (2024). Image watermarking using discrete wavelet transform and singular value decomposition for enhanced imperceptibility and robustness. Algorithms, 17(1), 32.