

Article

Not peer-reviewed version

Optimizing Image Watermarking with Dual-Tree Complex Wavelet Transform and Particle Swarm Intelligence for Secure and High-Quality Protection

[Abed Al Raouf Bsoul](#)^{*} and Alaa Bani Ismail

Posted Date: 24 December 2024

doi: 10.20944/preprints202412.2009.v1

Keywords: Dual Tree Complex Wavelet Transform; Particle Swarm Optimization Algorithm; Imperceptibility



Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Article

Optimizing Image Watermarking with Dual-Tree Complex Wavelet Transform and Particle Swarm Intelligence for Secure and High-Quality Protection

Abed Al Raouf Bsoul ^{1,*} and Alaa Bani Ismail ²

¹ Information Systems Department, Yarmouk University, Jordan

² Computer Science Department, Yarmouk University, Jordan

* Correspondence: raofbsoul@yu.edu.jo

Abstract: Watermarking is a technique used to address issues related to the widespread use of the internet, such as copyright protection, tamper localization, and authentication. However, most watermarking approaches negatively affect the quality of the original image. In this research, we propose an optimized image watermarking approach that utilizes the Dual Tree Complex Wavelet Transform and Particle Swarm Optimization Algorithm. Our approach focuses on maintaining the highest possible quality of the watermarked image by minimizing any noticeable changes. During the embedding phase, we break down the original image using a technique called Dual-Tree Complex Wavelet Transform (DTCWT) and then use Particle Swarm Optimization (PSO) to choose specific coefficients. We embed the bits of a binary logo into the least significant bits of these selected coefficients, creating the watermarked image. To extract the watermark, we reverse the embedding process by first decomposing both versions of the input image using DTCWT and extracting the same coefficients to retrieve back those corresponding bits (watermark). In our experiments, we use a common dataset from watermarking research to demonstrate the functionality against various watermarked copies and (PSNR) Peak Signal to Noise Ratio and Normalized Cross Correlation (NCC) metrics. The PSNR is a measure of how well the watermarked image maintains its original quality, and the NCC reflects how accurately the watermark can be extracted. Our method gives a mean PSNR and NCC of 80.50% and 92.51%, respectively.

Keywords: watermarking; dual tree complex wavelet transform; particle swarm optimization algorithm; imperceptibility

1. Introduction

Online piracy has caused significant financial losses and job displacement in some countries, amounting to over \$12 billion annually and 70,000 lost jobs according to the Recording Industry Association of America (RIAA) [1]. The increased use of the internet positively rising privacy concerns for digital media usage. To alleviate the effect of piracy of such media, digital watermarking is one solution. Digital Watermarking is a form of data hiding technology [2] that involves masking a pre-designed information into a digital medium such as images, videos, or audio. There are various types of digital watermarking schemes, including those based on spatial and frequency domains, and classified as robust, semi-fragile, and fragile methods [3]. A given technique has of course its advantages and disadvantages. However, the use of a specific method, depends on the application itself.

The internet's widespread use has made it effortless and quick to distribute digital media such as audio, video, and images. However, this convenience has also resulted in critical issues such as copyright infringement and authentication. Watermarking is one of the most effective and widely used techniques to address these concerns. Typically, image watermarking techniques follow a

general set of steps that include a watermark embedder and a watermark detector, as depicted in Figure 1.

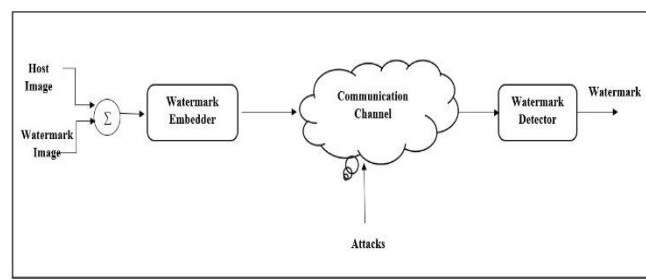


Figure 1. The architecture of a digital image watermark system.

Watermarking systems must have specific properties tailored to their intended applications, and as such, there is no standard set of properties that all watermarking systems must meet. However, one of the most critical requirements is imperceptibility [4]. Image watermarking involves embedding secret data into a host image without degrading the quality of the watermarked image (imperceptibility). Imperceptibility requires that the quality of the original image is preserved even after inserting the watermark such that it remains invisible to human eyes [5]. A watermarking approach is considered imperceptible if the host and watermarked images are visually indistinguishable. A robust watermarking scheme should not introduce artifacts into the images, and to assess imperceptibility, objective methods such as Peak Signal to Noise Ratio (PSNR) are commonly used [6,7].

In addition to immanence, the watermark method must also meet robustness. A robust watermark is one that can largely survive variations to the host image (maintaining content with a level of compute-independence), whilst other non-domain attack vectors are in play, i.e. crop, resize (scaling), contrast adjustment and JPEG compression [4]. Balancing these numbers to find the watermark's secret formula, one that is strong enough, but which does not cause severe degradation of the image, can be difficult. Thus, we should evaluate with caution a watermarking algorithm that is good enough to resist attacks and also prevent significant change on quality of embedded image.

The way of watermarking that is most well suited for proof of copyright and ownership in digital images are robust watermarking techniques. They are intended to withstand several image processing attacks that would either tamper with or erase the watermark. So robust watermarking techniques are employed to support intellectual property rights which includes but not limited to digital image copyright, content authentication and ownership proof [3]. The sensitive watermark enabled methods are useful when one requires copyright protection, whilst fragile watermarking topics provide for image authentication to confirm the integrity of an image without manipulation or modification. Semi-fragile watermarking is good and strong, but also sensitive to higher image processing operations can be employed for several tamper detecting schemes [3].

The frequency domain watermarking schemes are generally preferred over the spatial domain watermarking approaches due to their inherent resistance against image processing attacks [8]. Also, as an embedding capacity extension is achieved the frequency domain can provide more space while full imperceptibility [4]. Although, use of frequency domain techniques would incorporate some noise in the watermarked image which may be perceivable [9]. This was countered by some researchers who came up with an idea to use optimization methods for selecting the best coefficients to embed watermark, like Particle Swarm Optimization (PSO) [10,11] and Genetic Algorithm (GA) [12,13]. An alternative solution to increase the invisibility of watermarks is based on multiresolution decomposition techniques, such as Dual Tree Complex Wavelet Transform (DTCWT) [14,15].

In recent years. GA has been successfully applied to, in particular for optimization problems in watermarking. GA based wavelet-based image watermarking scheme was given in [9]. The embedding energy of a DWT-based watermarking scheme was optimized by means of an artificial neural network in. A fuzzy clustering technique was used in [16] to determine the optimal embedding

locations for a DCT-based watermarking scheme. These AI techniques enhance the performance of watermarking schemes, and their parameters (capacity, strength or location).

In 2017, Liu et al. [17] proposed an image watermarking scheme in contourlet transform domain, in connection with a probabilistic neural network. They distilled watermark extraction to a great degree of robustness. The Hamamoto and Kawamura [18] proposed an approach using autoencoder to train two distinct neural networks (embedder and extractor) with digital image using DCT coefficients. Ding et al in [19] proposed a generalized approach of using deep neural networks in digital watermarking. They presented a method that obtained great robustness under common image processing attacks, such as filtering, compression and geometric transformations.

Since selection of transformation coefficients for embedding affects any watermarking method, researchers exploit evolutionary algorithm to optimize the selection criteria. Researchers have used genetic algorithms widely in watermarking of images in the last few years, and it has become an important research branch for many researchers [12,20–22]. Moreover, PSO is proved to give promising accuracies in terms of robustness and impeccability. As such, several research exploited this fact in literature and give the light for outstanding approaches such as the work done in [11,23,24]. Other interesting approaches can be found in literature that incorporates one of the nature-inspired optimization algorithms such as Artificial Bee Colony Optimization [25,26], Bat algorithm [27] and Gray wolf Optimization [28].

Despite the advancements in digital watermarking techniques, significant challenges remain in balancing imperceptibility and robustness. Conventional methods like DWT, DCT or DFT may usually leave visible artifacts on images or fail in preserving integrity of the watermark under common malicious attacks (e.g., cropping, compression and scaling). Although optimization algorithms have been applied in watermarking, their integration with newer wavelet-based transforms, like DTCWT, has not been fully explored. This study will address these gaps by exploring the following research questions:

- How to incorporate the use of DTCWT and PSO to improve the imperceptibility of watermarked images while retaining high robustness?
- How well does the proposed method compare with traditional techniques like DWT and DCT in terms of PSNR (Peak Signal-to-Noise Ratio) and NCC (Normalized Cross-Correlation) under standard image processing manipulations: compression, cropping, scaling?
- What are the practical challenges in this watermarking scheme when applying it to real-world digital media applications, and how can these limitation be addressed?

The motivation underlying this work is to contribute in the domain of image watermarking and proposing an invisible and fragile method using DTCWT along with PSO algorithms. The main theoretical contribution of this work is the exploitation of shift invariance, redundancy and directionality selection properties of DTCWT that when applied in image applications give better results than traditional transform techniques as DWT, DCT or DFT. These features make the watermark to be more robust against a number of image processing attacks, while preserving exceptional quality for images. In order to improve the method and reduce any distortion of watermarked images, PSO is used as an optimization algorithm. The proposed application of PSO has been integrated very well in research, which in this work is to determine better coefficients embedding with optimal performance that will lead towards good robustness and lesser visual distortion in watermarked image. Additionally, DTCWT has a parallel dual-tree structure that enables efficient computation and is perfectly reconstruction, and thus it suits well for real-world applications requiring both quality and security [29]. However, the proposed method faces limitations in computational complexity, applicability to colour images, and resistance to advanced attacks.

2. Methodology

2.1. Overall Research Design

The proposed watermarking system is composed of two main phases: watermark embedding and watermark extraction. The system works as follows: The watermark image and the host image are first pre-processed and then inputted into the watermarking system. In the embedding phase, the host image is transformed into the frequency domain by applying DTCWT. The embedding process is optimized to choose the most suitable coefficients for watermark insertion. The watermark is then inserted into the least significant bit (LSB) of the selected coefficients. In the extraction phase, the watermark image is extracted by reversing the embedding process. To evaluate the proposed approach, the similarity between the watermark image and the extracted watermark is measured by computing the normalized cross-correlation (NCC). Additionally, the imperceptibility of the proposed approach is evaluated by calculating the Peak Signal-to-Noise Ratio (PSNR) of the watermarked images. Figure 2 illustrates the framework of the proposed approach.

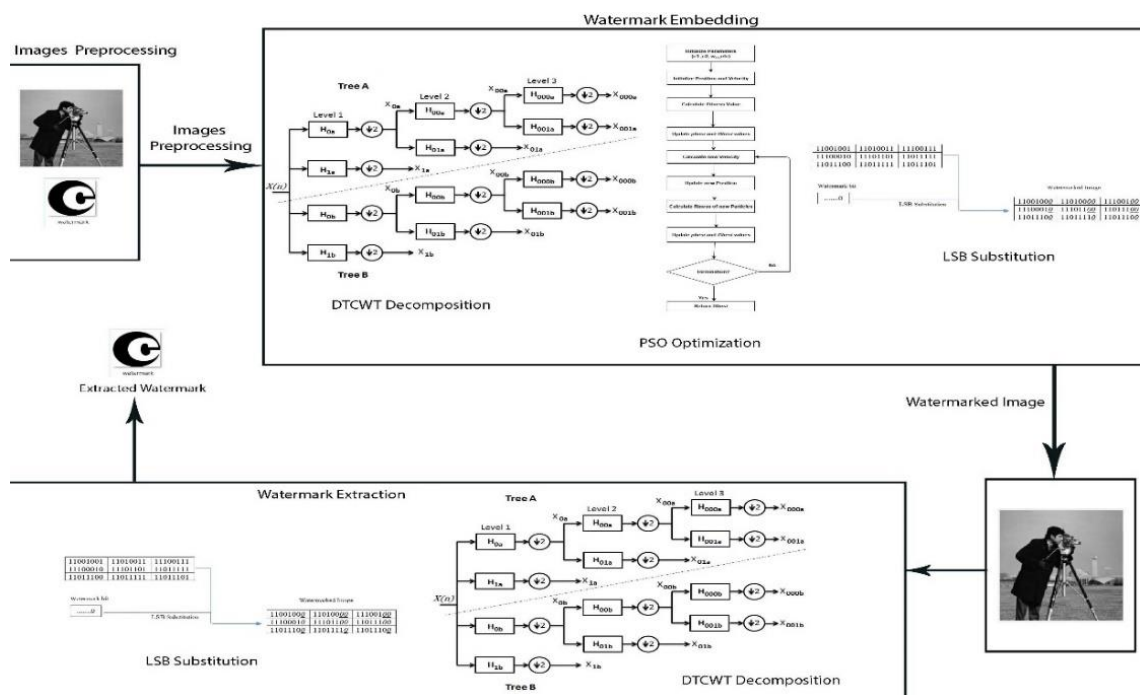


Figure 2. The Overall design of the proposed method.

2.2. Dataset

In this study, we used a standard dataset commonly employed in watermarking research. The experiments were performed on seventeen standard testing images: Lena, Cameraman, Baboon, Airplane, Boat, House1, House2, House3, Barbara, Elaine, Pirate, Zelda, Living room, Kiel, Lighthouse, Lake, and Pepper. All images are 512×512 in size, grayscale, and have an 8-bit depth.

The watermark image used in the experiments is the black and white logo for Yarmouk University, with a size of 100×109 bits. The logo of Yarmouk University is illustrated in Figure 3.

To ensure the reproducibility of the experiments, all images are publicly available and widely accepted in digital watermarking research. Further details about the dataset source can be provided upon request.



Figure 3. The logo used for embedding in this research. Actual logo size is 100x112 black and white color.

2.3. Watermark Embedding

Watermark embedding is the process of inserting the watermark image into the host image. In this research, this step mainly involves three sub-steps:

2.3.1. Frequency Domain Transformation

The insertion of the watermark image is performed in the frequency domain, which involves converting the host image into the frequency domain using DTCWT. This transformation technique has gained attention due to its advantageous properties over DWT. The most notable properties are approximate shift invariance, directionally selective filters, and perfect reconstruction [29]. DTCWT utilizes two real DWT trees to produce the real and imaginary parts of the transformed image. After applying DTCWT, the image is decomposed into eight sub-bands, including Low-Low (LL), Low-High (LH), High-Low (HL), and High-High (HH) for both the real and imaginary parts of a one-level decomposition. Figure 4 illustrates a multi-level decomposition for the LL sub-band. The coefficients from the LL sub-band are selected for embedding the watermark image.

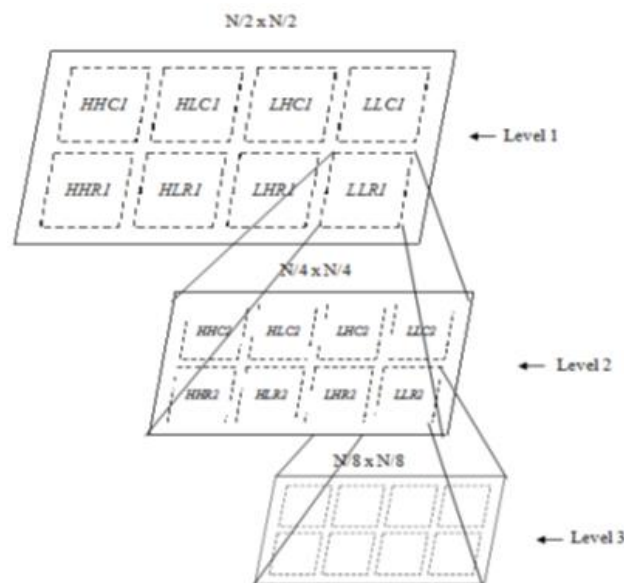


Figure 4. DTCWT sub bands using multi-level decomposition.

The dual tree complex wavelet transform differs from DWT in that it uses two orthogonal parallel transforms of the real wavelet, with the first DWT tree producing the real part and the second tree producing the imaginary part. Each tree contains a unique set of orthogonal filters. This results in DTCWT being able to obtain coefficients of six directions, namely $\pm 15^\circ$, $\pm 45^\circ$, and $\pm 75^\circ$, which solves the problem of poor directionality. At each level of decomposition, DTCWT produces two complex low-frequency sub-bands and six high-frequency complex detailed sub-bands, which are oriented by these angles. This property provides superior perceptual characteristics compared to DWT and enables the development of a watermarking approach with high imperceptibility. In mathematical terms, the low-frequency coefficients can be expressed as shown in Equation (1) [29].

$$x(\lambda, L, u, v) = \text{Re}(x(\lambda, L, u, v)) + j\text{Im}(x(\lambda, L, u, v)) \quad (1)$$

where λ is scaling factor (wavelength), L is the decomposition level, Re is the real part of the tree, Im is the imaginary part of the tree, u and v indicate the location of the coefficient in each sub-band, and j represents the square root of -1.

In this equation, the image is factorized using both real and imaginary parts to preserve information during processing.

The high-frequency coefficients can be written as in Equation (2).

$$\begin{aligned} x(\theta, u, v) &= \text{Re}(x(\theta, u, v)) + j\text{Im}(x(\theta, u, v)) \\ \theta &\in \{-75, -45, -15, +15, +45, +75\} \end{aligned} \quad (2)$$

In the embedding process, the frequency component at location u and v in the decomposition is represented by the complex coefficient after applying the DTCWT. So, modifying the least significant bits of these coefficients, the watermark data can be embedded without significantly altering the image's appearance.

2.3.2. Optimizing the Embedding Process

To embed a watermark in an image, we first should select frequency domain coefficients from the decomposed host image. Usually, this process is applied sequentially on the coefficients. However, in this research, we will use the Particle Swarm Intelligence algorithm to optimize the selection of the coefficients. The optimization algorithm fitness function is used for minimizing the degradation in the watermarked image.

PSO is a type of stochastic optimization algorithm and its process is inspired by the social interaction behaviour of flocking birds or schooling fish, which differs significantly from traditional individual cognitive elements. This algorithm consists of a population of candidate solutions (particles), which exist in the search space and is given a fitness value for the maximization function. PSO algorithm focus on the purpose to Minimize or Maximize the objective function. All particles update their position based on their own experience (cognitive behaviour) and development as well as the best location reached so far by all other particles (social behaviour).

For a brief overview of the PSO algorithm, the methodology was introduced in [30]. Each particle in the swarm consists of three 3-dimensional vectors: the current position (x_i), the best position reached by that particle (p_{best_i}), and the velocity (v_i) as shown in Equation (3). The velocity vector (v_i) controls the optimization process and enables information exchange between particles as well as utilizing the historical knowledge of each particle, as given in Equation (4). By adding the velocity coordinates (v_i) to the current position (x_i), the updated position of each particle (x'_i) is calculated.

$$v_i = \omega v_i + C_1\varphi_1 (p_{best_i} - x_i) + C_2\varphi_2 (g_{best} - x_i) \quad (3)$$

$$x'_i = x_i + v_i \quad (4)$$

where inertia weight (ω) is a constant that determines the balance between global and local search, while φ_1 and φ_2 represent uniformly distributed random values between [0,1]. Additionally, positive acceleration constants C_1 and C_2 are used to scale the contribution of cognitive and social components, respectively, in the particle's movement.

As an example, suppose a particle's current velocity is $v_i=2$, its personal best is at position 5, and the global best is at position 8. If the inertia weight is $\omega=0.7$, and C_1 and C_2 are both set to 1.5, with random values $\varphi_1=0.9$ and $\varphi_2=0.7$, the updated velocity would be

$$v_i = 0.7(2) + 1.5(0.9)(5 - x_i) + 1.5(0.7)(8 - x_i)$$

This gives the new velocity based on how far the particle is from its personal best and the global best, allowing it to move closer to an optimal solution.

PSO is applied to the coefficients obtained from the decomposition step. The pseudocode for finding the optimal set of coefficients using PSO is shown in Algorithm 1.

As the algorithm shows, the coefficients are divided into m swarms where each swarm have several particles. Each coefficient in a swarm is considered as a particle. The objective function is calculated over each particle in each swarm and the best value in swarm i is denoted as p_{best_i} while the best objective function over all swarms is considered as g_{best} . The inertia is calculated for each iteration and used as a weight contribution of the previous velocity. The updated velocity is

computed from the weighted velocity in the previous iteration along with the distance of particle i from the $pbest_i$ and the distance of particle i from $gbest$.

After finding out the velocity of particle i , we generate a random number from [0,1] and compare the obtained number by the sigmoid value of the new velocity. If the random number is less than the sigmoid value, we will choose that particle (coefficient) as an embeddable particle by setting it to 1. Then, the $pbest$ and $gbest$ are updated and the iteration continues.

After optimizing the selected coefficients in the transformed image using PSO, we calculated their mean, variance, skewness and kurtosis as well as the entropy and the energy of the selected coefficients. We found that the selected coefficients exhibit a non-Gaussian distribution. As a result, this fact will help in identifying the embeddable coefficients during the reconstruction of the stego-image.

2.3.3. Insertion in the Least Significant Bit (LSB)

A digital image is composed of small dots called pixels, where each pixel is a series of zeros and ones that represent a given color. When masking the least significant bits of the color value with a message bits, an embedding is happened. This process is called least significant bit (LSB) technique, and it is a widely used method in image manipulation. The more bits used in masking, the more noticeable distortion in the image exists. On the other hand, using more bits in the masking process provide more embeddable data. As a result, a compromise should be taken to balance the quality of the resulted watermarked image and the amount of data embedded. The process of LSB is repeated in a given manner until the whole message is embedded. Although it has been used in various applications such as information hiding, copyright protection, and authentication. The LSB has some limitations specially when implemented in time domain. For example, using advanced steganalysis techniques may result in corrupting the whole method. Therefore, to overcome these limitations, researchers have developed more complex steganography techniques that provide better security and greater capacity for hiding data while maintaining imperceptibility.

One such technique is the transform of the image to frequency domain and apply LSB on selected coefficients of the transformation. By utilizing other image domains, larger amounts of data can be hidden while still maintaining excellent transparency. As more steganalysis techniques are introduced, more advanced and secure steganography techniques is of paramount importance.

2.3.4. Watermarking Evaluation

According to the applied method for watermarking, the performance can change dramatically. To find out the performance of a given watermark method, one can measure the method's transparency. Since there are artifacts introduce during the watermarking process, the host image's quality is affected. Transparency is defined as the amount of information disclosed after the watermark operation. In practice, transparency is usually measured by evaluating the imperceptibility of the algorithm, which in turn is measured by an objective image quality metric called Peak Signal-to-Noise Ratio (PSNR). Measuring the PSNR of a method is straightforward and simple, as a result, PSNR became widely used metric for watermarking methods. The PSNR is evaluated by comparing the host image I , of size $N \times M$, with the watermarked image I_w as follow [6]:

$$PSNR = 10 \log \frac{255^2}{\frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M (I(i,j) - I_w(i,j))^2} \quad (5)$$

Alongside transparency, the degree of similarity between the watermarked image and the original image is also crucial in assessing the performance of a watermarking technique. Evaluating and measuring the similarity between the extracted watermark and the original one is essential in determining the level of distortion introduced by the method. The normalized correlation (NCC) is used to measure image similarity between the original and extracted images in watermarking.

The NCC is computed as follow; where W, W' is the original watermark image and the extracted watermark, respectively, while $\mu_w, \mu_{w'}$ represent the mean of the original and extracted watermark.

$$NCC(W, W') = \frac{\sum_{i=1}^M \sum_{j=1}^N [W(i, j) - \mu_w][W'(i, j) - \mu_{w'}]}{\sqrt{\sum_{i=1}^M \sum_{j=1}^N [W'(i, j) - \mu_{w'}]^2} \sqrt{\sum_{i=1}^M \sum_{j=1}^N [W(i, j) - \mu_w]^2}} \quad (6)$$

NCC is particularly useful in evaluating the accuracy of the watermark extraction process.

3. Results

In this study, the performance of the proposed algorithm was evaluated using the images in dataset described previously in section 2.2. The validation of the proposed scheme was performed as described in section 2.3.4 by calculating PSNR between the host and watermarked images and the NCC between the embedded logo image and the extracted image logo. The implementation of the method was carried out in MATLAB on a laptop computer equipped with Core i7 Intel processor, 16 GB RAM, and Windows 10. The cognitive component (C1) and social component (C2) were both set to a value of 1.5, empirically. The inertia weight (ω), which controls the search direction, was set to the maximum weight ($W_{max} = 0.9$) and a minimum weight ($W_{min} = 0.4$). Additionally, φ_1 and φ_2 were assigned uniformly distributed random values between [0,1]. The number of swarms was set to be 20. The convergence of the objective function was observed, and after 100 iterations, the solution reached a stable value.

To embed the watermark logo into the host image, the host image was decomposed using DTCWT. The filters "near_sym_b" and "qshift_b" were empirically found to produce the best coefficients, and a decomposition level of four was chosen. The PSO algorithm described in section 2.3.2 was utilized to select the best embeddable coefficients from the LL subband. It should be noted that this insertion process may introduce artifacts and distortion into the watermarked image. To evaluate the impact of these distortions, the PSNR was measured for the watermarked image. A visual comparison between some standard cover images before and after the watermark was applied, along with the PSNR between the two images, is provided in Table 1.

As shown in Table 1, the proposed method achieved a high PSNR between the host and watermarked images, indicating that the watermark was embedded effectively. The shift-invariant properties of DTCWT were found to be crucial in achieving this high PSNR. These properties allow for robust watermark embedding while preserving the quality of the host image.

To verify the embedding algorithm, we performed an extracting of the logo embedded in the images and measure the NCC between the original image logo and the extracted logo image. The results are provided in Table 2.

The proposed scheme was evaluated using the dataset described in section 2.2 and the validation of the proposed scheme was performed as described in section 2.3.4 by calculating PSNR between the host and watermarked images and NCC between the embedded logo image and the extracted image logo. The implementation of the approach was carried out in Python on a laptop computer equipped with an Intel Core i7 processor, 32 GB RAM, and running the Windows 10 operating system. Empirical settings were used for the parameters of the PSO algorithm. Specifically, the cognitive component (C1) and social component (C2) were both set to a value of 1.5. The inertia weight (ω), which controls the search direction, was set to have a maximum weight ($W_{max} = 0.9$) and a minimum weight ($W_{min} = 0.4$). Additionally, φ_1 and φ_2 were assigned uniformly distributed random values between [0,1]. The number of swarms was set to be 20. The convergence of the objective function was observed, and after 100 iterations, the solution reached a stable value.

To embed the watermark logo into the host image, the host image was decomposed using DTCWT. The filters "near_sym_b" and "qshift_b" were empirically found to produce the best coefficients, and a decomposition level of four was chosen. The PSO algorithm described in section 2.3.2 was utilized to select the best embeddable coefficients from the LL subband. It should be noted that this insertion process may introduce artifacts and distortion into the watermarked image. To evaluate the impact of these distortions, the PSNR was measured for the watermarked image. A visual comparison between some standard cover images before and after the watermark was applied along with the PSNR between the two images is provided in Table 1.

As shown in Table 1, the proposed method achieved a high PSNR between the host and watermarked images, indicating that the watermark was embedded effectively. The shift-invariant properties of DTCWT were found to be crucial in achieving this high PSNR. These properties allow for robust watermark embedding while preserving the quality of the host image.

To verify the embedding algorithm, we performed an extraction of the logo embedded in the images and measured the NCC between the original image logo and the extracted logo image. The results are provided in Table 2.

Table 2 examines the robustness of our watermarking method through various images. The high NCC values indicate that, even after possible distortions or manipulations to the image, the watermarking technique is effective at embedding and extracting the watermark even after possible distortions or manipulations to the image. The consistency in NCC values across different images means that the method is functionally robust to image content or complexity.

Table 1. The original host images along with the watermarked image for visual comparison; filters used are near_sym_b and qshift_b while the decomposition level is 4.

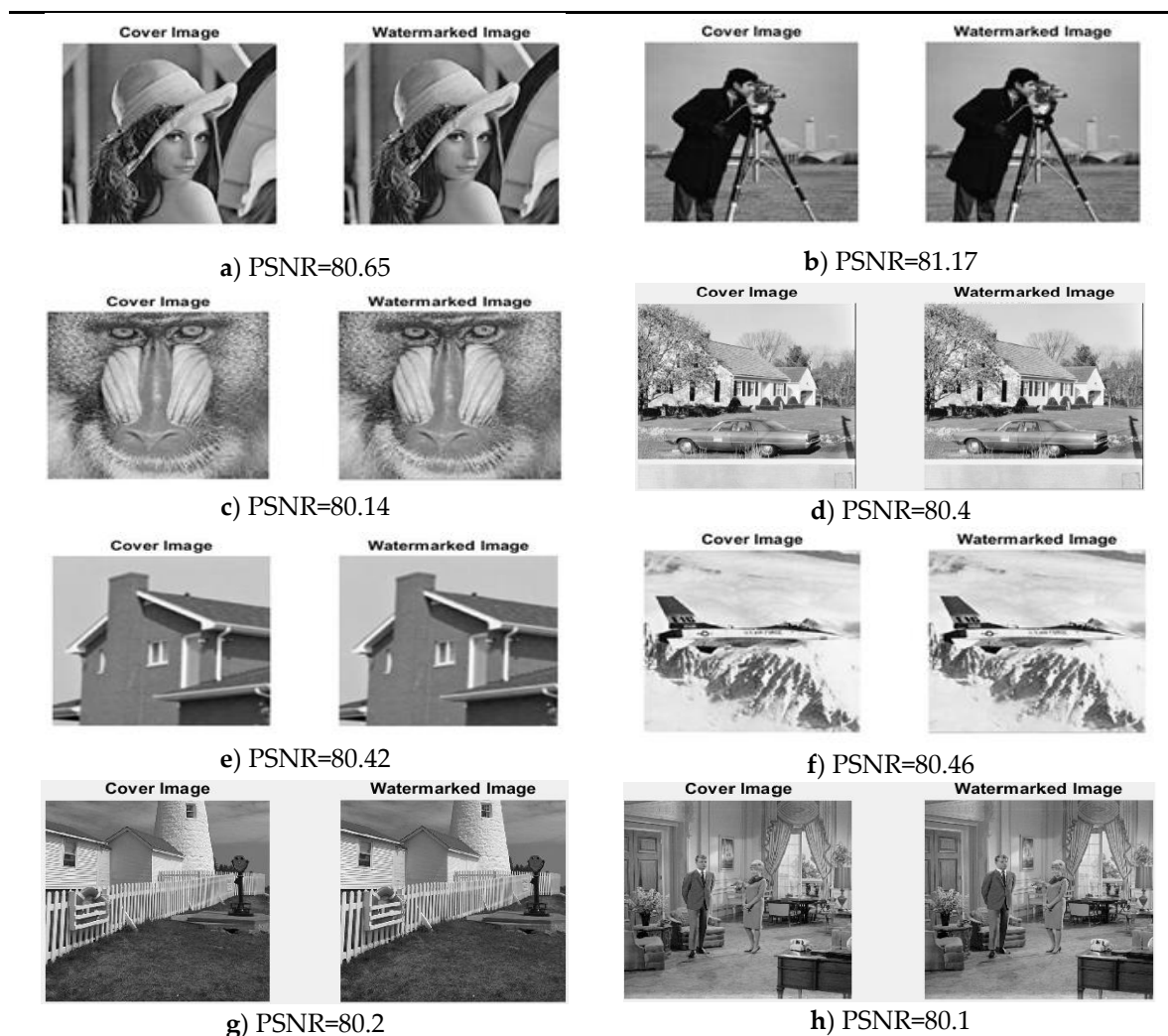









Table 2. NCC Values for Extracted Watermarks.

Image	Extracted Logo	NCC
Leena		93.3%
Cameraman		94.9%
Mandrill		89.2%
Homecar		91.1%
House		96.1%
Airplane		90.7%
Lighthouse		91.3%

Bedroom



93.5%

4. Discussion and Conclusion

Using Dual-Tree Complex Wavelet Transform (DTCWT) and Particle Swarm Optimization (PSO), the watermarking method proposed revealed drastic improvements in terms of imperceptibility, resilience against attack with a high capacity to embed large bits of messages into target images. Higher PSNR values indicate less degradation in the quality of host images due to watermarking operation. The technique shows a good performance in preserving the image's quality up to a mean PSNR value of 80.50% across the dataset.

Moreover, the average NCC value of 92.51% indicates a high accuracy in extracting watermarks from an original image to its corresponding retrieved version (Figure This highlights the robustness of the proposed method in authenticating and verifying forgeries performed on watermarked images.

Utilizing DTCWT for frequency domain transformation conferred benefits such as shift invariance and directional selectivity, pivotal in obtaining high imperceptibility. The PSO algorithm's optimization of coefficient selection augmented the watermark's robustness against frequent image manipulation attacks. Overall, combining DTCWT and PSO in the proposed watermarking method delivers a highly effective solution for secure and superior image watermarking. Further investigations might explore applying this method to different environments such as IoT [31] and enhance the algorithm parameters to better its performance.

The integration of PSO for optimization and DTCWT for data decomposition provides a powerful framework that is not limited to digital watermarking but can also be applied in complex optimization problems such as optimization in uncertain task environments as in [32–35]. By leveraging PSO's ability to find optimal solutions in uncertain environments and DTCWT's capacity for multi-dimensional data analysis, the proposed approach can effectively address uncertainties, improve efficiency, and provide robust solutions across various industrial applications.

The proposed watermarking method has limitations in terms of computational complexity, applicability to color images, and advanced attack resistance. Future work must be considered to minimize the effect of these limitations and widen the use of the algorithm in other domains. Future research can be applied to improve such limitations in 3D gray scale and color images, optimizing PSO parameters, and applying the method in real-time and IoT environments.

References

1. S. E. Siwek, "The true cost of sound recording piracy to the US economy," 2007, Institute for Policy Innovation Lewisville, TX.
2. M. Rizzi, M. D'Aloia, and A. Longo, "Digital watermarking for healthcare: a survey of ECG watermarking methods in telemedicine," *International Journal of Computational Science and Engineering*, vol. 23, no. 3, pp. 235–249, 2020.
3. R. Kumar, P. K. Singh, and J. Yadav, "Digital image watermarking technique based on adaptive median filter and HL sub-band of two-stage DWT," *International Journal of Computer Aided Engineering and Technology*, vol. 18, no. 4, pp. 290–310, 2023.
4. M. Begum and M. S. Uddin, "Digital image watermarking techniques: a review," *Information*, vol. 11, no. 2, p. 110, 2020.
5. P. Garg and R. R. Kishore, "Performance comparison of various watermarking techniques," *Multimed Tools Appl*, vol. 79, no. 35, pp. 25921–25967, 2020.

6. D. R. I. M. Setiadi, "PSNR vs SSIM: imperceptibility quality assessment for image steganography," *Multimed Tools Appl*, vol. 80, no. 6, pp. 8423–8444, 2021.
7. S. Rustad, P. N. Andono, G. F. Shidik, and others, "Digital image steganography survey and investigation (goal, assessment, method, development, and dataset)," *Signal Processing*, vol. 206, p. 108908, 2023.
8. O. Evsutin and K. Dzhnashia, "Watermarking schemes for digital images: Robustness overview," *Signal Process Image Commun*, vol. 100, p. 116523, 2022.
9. Z. Yuan, Q. Su, D. Liu, and X. Zhang, "A blind image watermarking scheme combining spatial domain and frequency domain," *Vis Comput*, vol. 37, pp. 1867–1881, 2021.
10. P. Garg and R. R. Kishore, "Optimized color image watermarking through watermark strength optimization using particle swarm optimization technique," *Journal of Information and Optimization Sciences*, vol. 41, no. 6, pp. 1499–1512, 2020.
11. A. Husain, A. D. Mishra, and S. K. Jena, "A robust approach for digital watermarking of satellite imagery dataset," *International Journal of Swarm Intelligence*, vol. 7, no. 1, pp. 82–93, 2022.
12. S. A. Barlaskar, S. V. Singh, K. Anish Monsley, and R. H. Laskar, "Genetic algorithm based optimized watermarking technique using hybrid DCNN-SVR and statistical approach for watermark extraction," *Multimed Tools Appl*, vol. 81, no. 5, pp. 7461–7500, 2022.
13. T. Zhu, W. Qu, and W. Cao, "An optimized image watermarking algorithm based on SVD and IWT," *J Supercomput*, vol. 78, no. 1, pp. 222–237, 2022.
14. T. Huang, J. Xu, Y. Yang, and B. Han, "Robust zero-watermarking algorithm for medical images using double-tree complex wavelet transform and Hessenberg decomposition," *Mathematics*, vol. 10, no. 7, p. 1154, 2022.
15. N. Nouioua, A. Seddiki, and A. Ghaz, "Blind Digital Watermarking Framework Based on DTCWT and NSCT for Telemedicine Application," *Traitement du Signal*, vol. 37, no. 6, pp. 955–964, 2020.
16. K. Balasamy and S. Suganyadevi, "A fuzzy based ROI selection for encryption and watermarking in medical image using DWT and SVD," *Multimed Tools Appl*, vol. 80, no. 5, pp. 7167–7186, 2021.
17. J.-X. Liu, X. Wen, L.-M. Yuan, and H.-X. Xu, "A robust approach of watermarking in contourlet domain based on probabilistic neural network," *Multimed Tools Appl*, vol. 76, pp. 24009–24026, 2017.
18. I. Hamamoto and M. Kawamura, "Digital watermarking method by encoder using neural network," *IEICE Technical Report; IEICE Tech. Rep.*, vol. 117, no. 282, pp. 17–22, 2017.
19. W. Ding, Y. Ming, Z. Cao, and C.-T. Lin, "A generalized deep neural network approach for digital watermarking analysis," *IEEE Trans Emerg Top Comput Intell*, vol. 6, no. 3, pp. 613–627, 2021.
20. P. Kumsawat, K. Attakitmongcol, and A. Srikaew, "A new approach for optimization in image watermarking by using genetic algorithms," *IEEE Transactions on Signal Processing*, vol. 53, no. 12, pp. 4707–4719, 2005.
21. Q. Wu, A. Qu, D. Huang, and L. Ma, "Robust and blind audio watermarking scheme based on genetic algorithm in dual transform domain," *Math Probl Eng*, vol. 2021, no. 1, p. 3378683, 2021.
22. R. Thanki, "Genetic algorithm-based intelligent watermarking for security of medical images in telemedicine applications," in *Intelligent Data Security Solutions for e-Health Applications*, Elsevier, 2020, pp. 185–204.
23. Laxmanika and P. K. Singh, "Robust and imperceptible image watermarking technique based on SVD, DCT, BEMD and PSO in wavelet domain," *Multimed Tools Appl*, vol. 81, no. 16, pp. 22001–22026, 2022.
24. D. Awasthi and V. K. Srivastava, "Performance enhancement of SVD based dual image watermarking in wavelet domain using PSO and JAYA optimization and their comparison under hybrid attacks," *Multimed Tools Appl*, vol. 82, no. 23, pp. 35685–35717, 2023.
25. S. Sharma, H. Sharma, and J. B. Sharma, "Artificial intelligence based watermarking in hybrid DDS domain for security of colour images," *International Journal of Intelligent Engineering Informatics*, vol. 8, no. 4, pp. 331–345, 2020.
26. P. Garg and R. R. Kishore, "An efficient and secured blind image watermarking using ABC optimization in DWT and DCT domain," *Multimed Tools Appl*, vol. 81, no. 26, pp. 36947–36964, 2022.

27. A. Pourhadi and H. Mahdavi-Nasab, "A robust digital image watermarking scheme based on bat algorithm optimization and SURF detector in SWT domain," *Multimed Tools Appl*, vol. 79, no. 29, pp. 21653–21677, 2020.
28. M. Gupta and M. Saraswat, "Grey wolf optimisation-based colour image watermarking," *World Review of Entrepreneurship, Management and Sustainable Development*, vol. 16, no. 6, pp. 648–664, 2020.
29. I. W. Selesnick, R. G. Baraniuk, and N. C. Kingsbury, "The dual-tree complex wavelet transform," *IEEE Signal Process Mag*, vol. 22, no. 6, pp. 123–151, 2005.
30. D. Wang, D. Tan, and L. Liu, "Particle swarm optimization algorithm: an overview," *Soft comput*, vol. 22, no. 2, pp. 387–408, 2018.
31. M. Anitha and M. Senbagavalli, "Dynamic Mobile Cloud Eco System Security - A Review," *International Journal of Data Informatics and Intelligent Computing*, vol. 2, no. 1, pp. 62–69, Mar. 2023, doi: 10.59461/IJDIIC.V2I1.44.
32. Ö. Y.-C. O. R. Review and undefined 2020, "Robust optimization for U-shaped assembly line worker assignment and balancing problem with uncertain task times," *hrcak.srce.hr Ö F Yılmaz Croatian Operational Research Review, 2020 • hrcak.srce.hr*, vol. 11, pp. 229–239, 2020, doi: 10.17535/crorr.2020.0018.
33. T. C. Phan, H. C. Tran, T. Chi, P. Quang, T. Teacher, and T. College, "Consideration of Data Security and Privacy Using Machine Learning Techniques," *International Journal of Data Informatics and Intelligent Computing*, vol. 2, no. 4, pp. 20–32, Dec. 2023, doi: 10.59461/IJDIIC.V2I4.90.
34. U. D. Maiwada, K. U. Danyaro, A. B. Sarlan, and A. A. Aliyu, "Dynamic Handover Optimization Protocol to enhance energy efficiency within the A-LTE 5G network's two-tier architecture," *International Journal of Data Informatics and Intelligent Computing*, vol. 3, no. 3, pp. 8–15, Aug. 2024, doi: 10.59461/IJDIIC.V3I3.124.
35. S. Chaturvedi, "IoT-Based Secure Healthcare Framework Using Blockchain Technology with A Novel Simplified Swarm-Optimized Bayesian Normalized Neural Networks," *International Journal of Data Informatics and Intelligent Computing*, vol. 2, no. 2, pp. 63–71, Jun. 2023, doi: 10.59461/IJDIIC.V2I2.59.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.