Computer Assisted Methods in Engineering and Science
30(4): 557–581, 2023, doi: 10.24423/cames.547

This article belongs to the *Special Issue on Computer Aided Software Design for Multi-Concern Assurance* edited by Dr. J.I.-Z. Chen, Dr. K.-L. Du and Dr. H. Wang

Efficient and Robust Medical Image Watermarking Based on Optimal Subband Tree Structuring and Discrete Fractional Fourier Transform

Anusha CHACKO[1),2)*], Shanty CHACKO[3)]

[1)] *Department of Electronics and Communication Engineering, Karunya Institute of Technology and Science, Coimbatore, Tamil Nadu, India*

[2)] *Department of Electronics and Communication Engineering, Vimal Jyothi Engineering College, Chemperi, Kerala, India*

[3)] *Department of Electrical and Electronics Engineering, Karunya Institute of Technology and Science, Coimbatore, Tamil Nadu, India*

[*] *Corresponding Author e-mail: anushachacko@vjec.ac.in*

In order to solve the security problems associated with medical information and improve the robustness of watermarking algorithms for medical images, a unique approach to watermarking based on block operations is presented. This study considers the medical images as the cover image, with the watermark logo considered secret information that needs to be protected over the wireless transmission in telemedicine. In the embedding phase, input with the discrete fractional Fourier transform is first applied to the input, and then level 2 wavelet decomposition is carried out to determine the optimal sub-band tree. For each tree node on level 2, the approximated and detailed coefficient is determined through the feature analysis perspective. The novelty of the adopted methodology is its simplified transformation and embedding process. Upon receiving a complex matrix, it separates the real part from imaginary part where block transformation is carried out for embedding the watermark pixels. In the extraction phase, just a reverse operation is performed. The watermarking evaluation is performed by simulating various image processing attacks on watermarked medical images. The simulation outcome demonstrates the effectiveness of that proposed watermarking scheme against various attacks. The proposed watermarking technique is robust under various attacks based on image statistics such as PSNR, BER, and the correlation coefficient.

Keywords: medical image, watermarking, discrete FFT, decomposition, security.

1. Introduction

Medical experts and patients often seek additional opinions from other healthcare professionals for the purpose of better treatment, which requires the exchange of patient medical records such as radiological images, initial reports,

prescriptions, and more [1]. With the advent of advanced communication systems and electronic management of medical records, digital medical images can now be shared worldwide through services such as telemedicine or teleradiology [2]. Telemedicine eliminates geographical distance barrier enabling access to medical services available in remote areas. It enables the transfer of medical data over distances and direct exchange of medical information between medical professionals and patients [3]. Nevertheless, the transfer of medical images over an open wireless channel is prone to attacks, giving rise to significant security concerns [4]. For this reason, the exchange of medical images imposes a vital requirement that an unauthorized entity must not alter the medical images. Hence, a major concern for current medical systems is the development of robust and efficient solutions that ensure the confidentiality, reliability, and availability of medical images [5]. Watermarking is adopted to resist various threats, each employing different attack strategies aimed at intruding private information within an image, and thereby compromising it. These threats include removal, protocol, geometry, and cryptographic attacks [6]. Beyond the medical domain, watermarking can be used in various applications, e.g., monitoring broadcast, copyright management, identification of ownership, tracking of transactions, authentication of contents, etc. While the fundamental application remains consistent, new approaches continuously evolve towards more secure features using different algorithmic approaches. Applications designed for watermarking based on various algorithms are highlighted in Table 1.

Table 1. Application of watermarking.

Application based on algorithm	Advantage	Issues
Discrete Fourier transform (DFT) [7]	Better recovery	Higher cost of implementation
Discrete wavelet transform (DWT) [8]	Higher compression ratio	Consumes time for compression
Discrete cosine transform (DCT) [9]	Attacker cannot remove watermark	Disrupts invariant properties
Texture mapping [10]	Capable of better data hiding	Narrowed scope of implementation
Patchwork [11]	Higher robustness	Cannot hide large data
Correlation [12]	Increased gain	Low quality of image
Least significant bit (LSB) [13]	Simpler execution	Lacks robustness

The process of watermarking involves embedding information in digital images to verify their ownership and authenticity by retrieving the original information. Multiple watermarking techniques can be classified according to the processing domain, watermark signal type, and hiding state [14, 15]. The watermarking scheme in the spatial domain is easy to implement and computationally

inexpensive. However, the technique has an extremely low bit capacity and is not very robust against image processing attacks, such as compression [16]. Unlike the spatial domain, watermarking in the transform domain can embed more watermark bits and resist various attacks [17]. A reversible watermarking scheme is a lossless mechanism implemented to retrieve medical images completely without any distortion after removing the watermark [18].

The watermarking system gains strength by incorporating blindly extracted features because the original image is not necessary for watermark extraction. In addition to preventing unauthorized modification and access, the success of the watermarking process also relies on the ability to retrieve hidden data under various image processing attacks. In order to meet these requirements, the watermarking techniques must satisfy the requirements of imperceptibility, robustness, and payload attributes [19, 20]. To effectively balance all these properties, an appropriate coupling mechanism is needed to achieve an optimal security technique.

Therefore, this paper presents a computationally efficient and robust medical image watermarking scheme based on optimal sub-band tree structuring mechanisms and a discrete fractional Fourier transform (DFrFT). The proposed scheme considers a single-color intensity medical image as input, transformed next in the frequency domain, and decomposed into a level 2 sub-band tree for enhanced signal analysis. This process offers better localization of frequency so that the sub-bands where the watermark is embedded are determined. Furthermore, a distinctive block-based operation is carried out to embed watermark information into the input image. The simplified implementation strategy and effective block-based embedding operation, without the need for any external keys or resources, give the proposed system an advantage over similar existing schemes. The proposed system carries out the following operational steps to ensure the maximal quality of an image:

1) the proposed scheme constructs an attack model designed to illegitimately access secret information from the input image. This leads to enhanced flexibility in the analytical process allowing to assess the sustainability of the proposed watermarking model;
2) the proposed scheme translates the input image into grayscale, which is followed by applying DFrFT using a highly straightforward sampling strategy with uncomplicated operation of Fourier operators as linear combination;
3) the application of the DFrFT transformation technique leads to the decomposition of a reconstructed image without losing its essential properties when the inverse transformation is conducted;
4) the next step involves a unique embedding process where both real and imaginary values are derived from the outcome of an inverse transformation. This leads to retaining granular signal information while the watermark image is embedded in blocks of the original image.

The remaining section of this paper is organized as follows: Sec. 2 presents a review of existing literature, Sec. 3 highlights the problem statement, Sec. 4 discusses the techniques employed; Sec. 5 discusses the implementation procedure for watermark embedding and extraction phase, and Sec. 6 presents the results and performance analysis. Finally, Sec. 7 concludes the paper.

2. Review of literature

This section presents a review of existing watermarking techniques, with a focus on exploring their effectiveness and current research status to identify gaps in this crucial research area.

In eHealth field, arrangements usually suffer from major limitations when it comes to the authenticity of medical images and the integrity of patient health information. Hassan *et al.* [21] proposed a method for obtaining the authentication and integrity verification of medical documents by means of imperceptible watermarks. Using fast curvelet transforms and singular value decompositions (SVD), a watermark image of the electronic patient record is embedded into an optical image. Study results indicate that this watermark is more resilient and imperceptible than existing watermarks; however, the detachment problem between electronic records and their corresponding images is not addressed. Continuing in this line of research Nuñez-Ramirez *et al.* [22] presented an invisible watermarking scheme in the frequency domain. To validate the image's authenticity, the authors used their invisible watermarking scheme in the spatial domain.

Hosny *et al.* [23] addressed the issues of computational complexity in the execution of the watermarking algorithm. The authors proposed the use of parallel multi-core CPU-GPU technology to accelerate the watermarking process. In their work, the grayscale image is transformed with an embedded linear polar exponential using the simplified exact kernel, while quaternion moments are calculated using the simplified exact kernel applied to the main color image.

The self-recovery watermarking mechanism was implemented in Su *et al.* [24]. Turtle shells and embedding tables were used to incorporate information and verification codes into other blocks before embedding them into other blocks. Three-stage techniques utilized to obtain better accuracy in tamper detection and localization, whereas two-stage techniques were employed to recover the image at a higher level of quality during self-recovery. In an effort to maintain image authenticity while avoiding diagnostic bias, Liu *et al.* [25] employed recursive dither modulation in conjunction with the Slantlet transform and SVD. To develop an efficient watermark generation mechanism within the constraints of the embedding scale, the authors also separated regions of interest (RoI) from regions of non-interest (non-RoI).

Haddad *et al.* [26] introduced a combined watermarking-encryption-compression scheme for medical image protection. By encrypting and compressing image bitstreams, this scheme can provide watermark-based security without requiring users to decrypt or decompress any part of the image. In addition, the study makes it possible to trace images in encoded or compressed domains as well as to control their integrity and authenticity. Shehab *et al.* [27] designed a delicate watermark-based image authentication and self-retrieval scheme for medical applications. The trajectory of the block-wise SVD in the least significant bits of the image pixels is used to calculate the change in the original image. This method can detect forgeries and restore the original image, when necessary.

Liu *et al.* [28] introduced the zero-watermark concept, which is based on dual-tree complex wavelet transforms and multi-dimension hyperchaos. In this approach, binary sequences are used for features; first, the watermark is scrambled with three-dimensional hyperchaos, and then the medical volume data undergoes a three-dimensional DTCWT-DCT transformation. In order to represent the features, an algorithm is designed to select and binarize the low-frequency coefficients. Abd El-Latif *et al.* [29] developed a quantum steganography method for embedding a secret image into a quantum overlay image using a controlled--NOT gate. Controlled-NOT gates encrypt the embedded data to ensure data integrity. Two least significant qubits are used to embed and extract hidden information from CT images and restore the image to its original position at the receiving end in Memon and Alzahrani [30]. In this process, the host image is split into regions of interest ROI and non-ROI, and the scheme applies a fragile watermark to the ROI and a strong watermark to the non-ROI to protect copyright. Loan *et al.* [31] found that grayscale and color images could be visually adorned with watermarks using chaotic encryption. A discrete cosine transform (DCT) is applied before embedding a watermark into a host image, and the watermark bits are embedded by modifying the difference between neighboring DCT coefficients. The authors also utilized the Arnold-transform algorithm as part of their watermark algorithm, which added an additional layer of security to the chaotic encryption process.

As we can see, there are various watermarking techniques presented to date. But the existing techniques suffer from different issues such as simultaneously ensuring good image and watermark quality. Additionally, ensuring low computational complexity in the embedding and extraction process is a still challenging task. Furthermore, the existing techniques that achieve balance between visual quality and computational complexity lack robustness. Therefore, a simple and effective watermarking approach is required that can meet the requirement of telemedicine capable of transmitting medical data in secure and timely manner.

3. Research problem

After reviewing the existing watermarking approaches, following problems are identified:

- Existing SVD-based watermarking scheme [21, 28] does not address the problem of matrix decomposition, which does not ascertain the computational efficiency;
- While the adoption of multi-core technology [23] is a good option, it can be an expensive solution towards watermarking;
- Existing transform-based operation does not balance the computational efficiency and signal quality, making it more prone to various attacks [25];
- There are various encryption-based methodologies adopted; however, they are iterative and consume resources to accomplish its objectives [26, 31];
- There is still ambiguity in selection of specific area in ROI-based schemes, leading to outliers [26, 29].

Therefore, there is a significant level of degradation by the traditional digital watermarking processes when applied to diagnostic medical images. Consequently, the watermarking of medical images is the problem of balancing the tradeoff between the level of security and the visual quality of the medical image.

4. Proposed system

The core aim of the proposed study is to suggest an effective mechanism of digital medical image watermarking that can hide recognizable patterns in input medical images while remaining resilient against various image processing attacks. Over the past decade, numerous studies have used fast Fourier transform (FFT) for image watermarking. In addition, there are evolving researches exploring similar techniques in recent studies [32–36], demonstrating their potential for watermarking by adopting FFT with promising results. However, the use of conventional FFT in image watermarking is not without its challenges connected to the limited range of transformed waveforms along with a reliance on weighing function during the windowing process in order to mitigate spectral leakage. While discrete Fourier transform (DFT) is an alternative solution to FFT, it still poses challenges with computational time complexity. The proposed work aims to address these issues. The novelty of our study lies in developing a computationally simplified process to facilitate image watermarking process. Another novelty of the proposed scheme is its embedding process, which is based on real and imaginary components within a block operation followed by transforming process. The schematic architecture of the proposed scheme is depicted in Fig. 1.

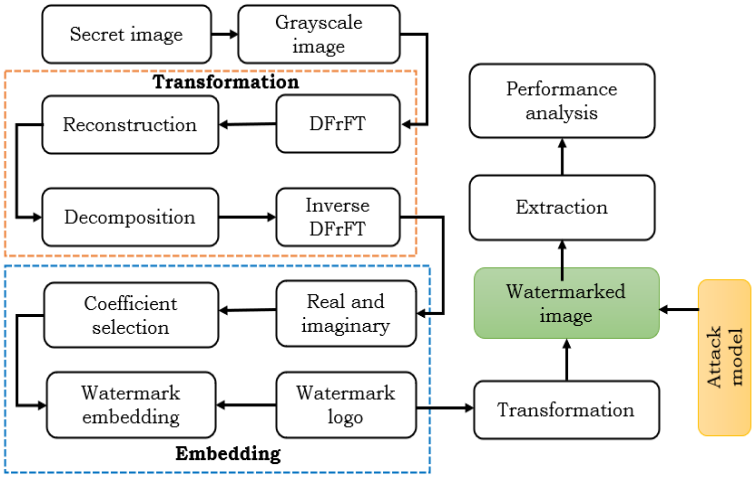


FIG. 1. The schematic outline of the proposed system.

As shown in Fig. 1, the proposed system consists of four key operational modules: i) transformation, ii) watermark embedding, iii) attack model, and iv) watermark extraction. In the transformation module, the study considers a single-channel intensity medical image subjected to a DFrFT operation and sub-band tree structuring for signal decomposition. DFrFT is used to transform the signal from the time domain to the frequency domain with the same signal sampled while preserving the non-stationary characteristics of real signals. Furthermore, the transformed image is subjected to the sub-band tree structuring mechanism for signal decomposition. As a result, the reconstructed image can be more precisely localized, allowing to determine the frequency component for the sub-band where the watermark is embedded. The study considers a binary image as the watermark logo to be embedded in the input image. In this process, the real and imaginary parts of the reconstructed image are initially extracted. Next, r, the real part of the image is divided into blocks of the same dimensions as the watermark logo. The watermark logo is then embedded in each block of the real part of the reconstructed image using a specified embedding intensity. An inverse operation is carried out in the watermark extraction process, which does not require the original input image. The proposed system also simulates various attacks scenarios in order to analyze the effectiveness of the proposed watermarking scheme.

4.1. Discrete fractional Fourier transform

To provide a concise overview, this section first throws light on the fractional Fourier transform (FrFT), which is a time-frequency analysis that uses frac-

tional powers of the conventional Fourier transform FT operator [38]. The FrFT of a signal $x(t)$ with an angle α is expressed as follows:

$$F_\alpha\left[x(t)\right] = \sqrt{\frac{1 - j\cot\alpha}{2\pi}} \int_{-\infty}^{\infty} K \cdot x(t)\,\mathrm{d}t, \tag{1}$$

$$K = \mathrm{e}^{\left(\frac{j}{2}\right)\left\{\left(t^2+u^2\right)\cot\alpha - 2\mathrm{tu}\csc\alpha\right\}}, \tag{2}$$

where j is the imaginary unit used to handle complex numbers and complex arithmetic in FrFt operation, t represents the independent variable of the signal $x(t)$, which is a function of time, while variable u refers to auxiliary variable for integration, and K denotes the kernel function of the FrFT given by

$$\alpha = \frac{p\pi}{2}, \tag{3}$$

where α denotes the angle parameter and variable $p \in \mathrm{Z}^+$ is the FrFT order. If the value of p is equal to 1, the FrFT is regarded as the FT. Likewise, if the value of p equals 2, it becomes an inverse operator, and for p equal to 3, it becomes the inverse FT. Figure 2 depicts the time-frequency analysis of the FrFT.

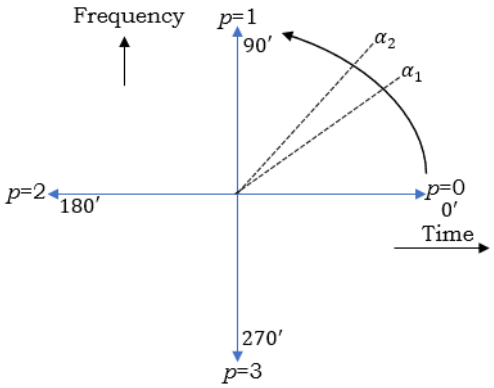


Fig. 2. Demonstration of signal in the time-frequency plane.

As can be seen from Fig. 2, the FrFT has an angle of rotation α concerning both the horizontal (x-axis) and vertical (y-axis) directions, indicating a greater number of logically independent values (with the freedom to vary) compared to the conventional FT. The following is the numerical expression for determining the inverse FrFT:

$$f(x) = F^{-p}\left[F^{p}\left(f(x)\right)\right], \tag{4}$$

where F^p represents the FrFT of order p, F^{-p} represents the inverse FrFT of order p.

Using Eq. (4), the discrete FrFT (DFrFT) of an image can be computed using the following expression:

$$F_{\alpha,\beta}(m,n) = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} f(p,q) K_{\alpha\beta}(p,q,m,n), \tag{5}$$

where both α and β denotes the order of transformation, and $K_{\alpha\beta}(p,q,m,n)$ represents the transformation kernel, such that $K_\alpha \otimes K_\beta$, while p, q are the pixel coordinates of the original input image, and m, n are the coordinates of output signal in the transformed domain.

4.2. Optimal sub-band tree structuring

In signal analysis, an optimal sub-band tree structure is formulated using a wavelet filter bank to decompose the signal into sub-bands while maintaining its temporal representation. This approach is often associated with wavelet packet analysis, which is similar to discrete wavelet transformation (DWT), except that both detail and approximate coefficients are decomposed [39]. Compared to other wavelet analyses, this mechanism provides a more comprehensive analysis of the input signal because of its ability to achieve better discrimination by analyzing the higher frequency domain of the signal. Based on the characteristics of the analyzed signal, the frequency domain can be easily selected and classified by wavelet packets. When WPD is of an n level, instead of producing $n+1$ sets of coefficients, $2n$ sets are produced. Mathematically, WPD can be described as follows:

$$\omega_{j,k}^{i}(t) = 2^{\frac{j}{2}} \omega^{i}\left(2^{j}t - k\right), \tag{6}$$

where $\omega_{j,k}^{i}$ signifies the wavelet packet function, which possesses properties of orthonormality and time-frequency localization. The parameter j is the frequency localization metric, k denotes the time localization metric and $i \in \{1,2,3,...,N\}$ represents the oscillation metric. Numerically, the wavelet function with oscillation metric ω^i can be expressed as follows:

$$\omega^{2i}(t) = \sqrt{2} \sum_{k=-\infty}^{\infty} g(k) \omega^{i}(2t-k), \tag{7}$$

$$\omega^{2i+1}(t) = \sqrt{2} \sum_{k=-\infty}^{\infty} h(k) \omega^{i}(2t-k), \tag{8}$$

where in Eq. (7), the component $g(k)$ represents a low-pass filter producing approximate coefficients, and in the Eq. (8), the component $h(k)$ represents a high-pass filter producing detail coefficients. The wavelet packet coefficients

($c^i_{j,k}$) of the signal $x(t)$ are embedded in the inner part of the signal for each wavelet packet expressed as follows:

$$c^i_{j,k} = \int_{-\infty}^{\infty} x(t)\omega^i_{j,k}(t)\,\mathrm{d}t, \tag{9}$$

where $c^i_{j,k}$ indicates the i-th set of wavelet packet decomposition coefficients at the j-th and k-th frequency localization and time localization parameters, respectively. All the frequency components and their occurrence are reflected in $c^i_{j,k}$ based on changes in the i-th, j-th and k-th parameters. Thus, each $c^i_{j,k}$ coefficient is measured by sub-band frequency content determined by the frequency positioning parameter j-th and the oscillation parameter i-th. In WPD, the filters $h(k)$ and $g(k)$ are used to perform filtering operations. Furthermore, wavelet packets can be reconstructed from signals by the inverse wavelet transform using Eq. (10):

$$x^i_j(t) = \sum_{k=-\infty}^{\infty} c^i_{j,k}\omega^i_{j,k}(t)\,\mathrm{d}t, \tag{10}$$

where computation is shown for the signal reconstruction $x^i_j(t)$ for each wavelet packet (i, j). However, by summating the reconstructed signals from packets decomposed at level j-th, the reconstructed signal retains its original form, as shown in Eq. (11):

$$x(t) = \sum_{i=0}^{2^j-1} f^i_j(t)\,\mathrm{d}t. \tag{11}$$

The numerical expression (12) can be used to determine the frequency bands in each packet decomposed at level j as follows:

$$F_j = \frac{F_s}{2^{j+1}}, \tag{12}$$

where the component F_s signifies the sampling frequency, and further downsampling can be employed to prevent unwanted or redundant data after the decomposition. By computing WPD on the signal $x(t)$ at the j-th level decomposition, there are $C_{j,m}$ sets of sub-band coefficients of length $N/2^j$. As a result, WPD divides frequency space into different parts and allows the signal to be more precisely located at different frequencies. This provides the richest analysis generating a quaternary tree, as shown in Fig. 3.

Figure 3 illustrates how a wavelet decomposition of an image leads to an optimal sub-band tree structure whose root is the input signal. The first layer

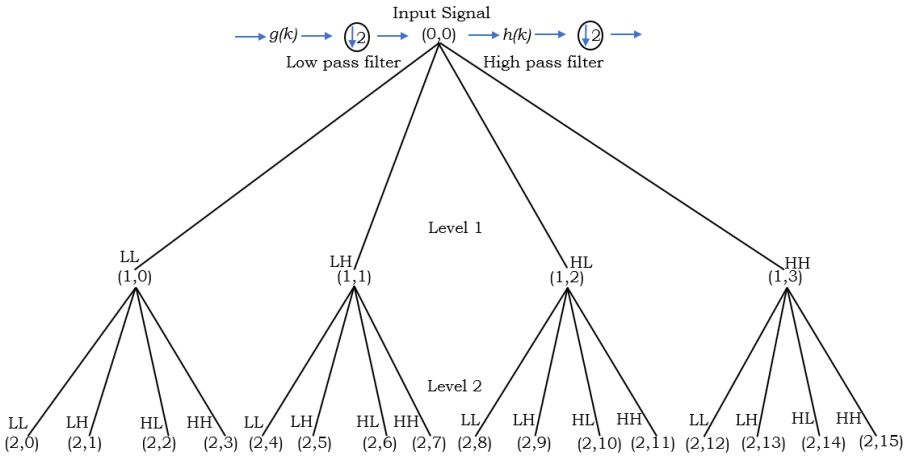


FIG. 3. Decomposition of wavelet packets in the quaternary tree of level 2.

of the tree is the result of a step in WPD that uses a low-pass filter $g(k)$ to create approximate coefficients, while detailed coefficients are constructed using a high-pass filter $h(k)$ at a specified level. The coefficients are then down-sampled by a factor of 2 and further subjected to the next level in the next layer. The process is repeated on both detailed and approximate coefficients at this level. The next step is to determine the last (target) level of approximated (LL) and detailed coefficients (LH, HL, HH), which are then combined into a matrix with $2n$ columns, where n represents the level of the decomposition. Also, this operation generates an object containing a number of coefficients subjected to input signals, which is required to perform an appropriate reconstruction of the signals after transformation. Choosing the appropriate wavelet packet for a given signal is vital, as there are many types of WPD, and each has distinct effects. This study uses the Shannon entropy principle to select the optimal wavelet packet. Using this principle, any wavelet packet with a high energy ratio concerning Shannon entropy is chosen as the optimal wavelet. The energy of the signal can be given as follows:

$$E_j^i = \sum_{k=1}^{n} \left(c_{j,k}^i\right)^2, \tag{13}$$

$$E_j = \sum_{i=0}^{m=2^{j-1}} E_j^i, \tag{14}$$

where E_j^i denotes the energy of the i-th wavelet packet node at the j-th level of the signal $x(t)$.

Whereas E_j indicates the sum of all energy packets at the j-th level equal to the energy of the original signal. Furthermore, the Shannon entropy $S(x)$ is expressed as follows:

$$S(x) = \sum_i \varphi \cdot \log_2 \varphi, \tag{15}$$

where $\varphi = \frac{E_j^i}{E_j}$ denotes the energy probability distribution.

Selecting the optimal packet typically involves a bottom-up search method that picks the optimal wavelet packet with the smallest $S(x)$. The low-frequency components are further decomposed during this process, and the wavelet transformation divides the frequency band into multiple levels. Moreover, by further decomposing the high-frequency parts, the time-frequency resolution is increased, and the image insensitivity to watermarks is improved. A wavelet packet basis with two-ordered wavelets was used in this study to decompose the input image for embedding the watermark.

5. Proposed watermarking scheme

This section discusses the implementation procedure for watermarking over the input medical image to provide a better form of security against various image processing attacks. The entire process of watermarking employing DFrFT with optimal sub-band tree structuring process includes two parts: embedding and extraction.

5.1. Watermark embedding

The proposed system considers the input medical image $\mathbf{I}_m$ as a cover image such that $\mathbf{I}_m \leftarrow (I_{m,n})_{M\times N}$ is a two-dimensional single-channel intensity image of M height and N width having gray value at coordinates $(m, n) \in \{1, 2, 3, ..., M, N\}$. Similarly, this study also considers a watermark logo $(\mathbf{W}_L)$ such that $\mathbf{W}_L \leftarrow (W_{r,c})_{R\times C}$ is a 1-bit bi-level image. A detailed description of the implementation procedure involves the following steps:

Step 1: Initialize transfer power $P \leftarrow [\alpha, \beta]$.

Step 2: Apply the DFrFT using Eq. (9) to the double-precision medical image $\mathbf{I}_m$ with P to compute both magnitude and phase. This step provides a complex-valued image $(\mathbf{I}'_m)$ with both real and imaginary parts. This process can be expressed as $\mathbf{I}'_m = \mathcal{F}^P(I_{m,n})$.

Step 3: Decompose $\mathbf{I}'_m$ to obtain the optimal sub-band tree structure of the filtered image such that

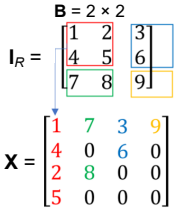
$$\mathbf{I}'_m(t) = \sum_k g_j(k)\varphi_{jk}(t) + \sum_{j=1}\sum_k h_j(k)\varphi_{jk}(t), \tag{16}$$

where $\varphi(t)$ denotes the frequency localization function or scaling function, with j-th decomposition level and k-th time wavelet decomposition. The discrete filter g_j is low-pass filter producing the approximation coefficient and h_j is a high-pass filter producing the detail coefficient. The complex-valued image $\mathbf{I}'_m$ is decomposed into level 2 wavelet decomposition using Haar wavelet. Applying WPD to the two-dimensional $\mathbf{I}'_m$ corresponds to a quaternary tree of order 4.

Step 4: Compute the coefficients associated with the tree nodes at level 2 using Eq. (9). As a result, a filtered image divided into four non-overlapping multi-resolution sub-bands images: LL2, LH2, HL2, and HH2 is obtained. These sub-band images correspond to approximation and detail coefficients, including vertical, horizontal, and diagonal in a respective manner. Next, an inverse operation of wavelet transformation is applied using Eqs. (10) and (11) to reconstruct an image which can be given as $\mathbf{I}_{\text{Rec}} = \{I_{i,j}\}_{L\times R}$, $[i,j] \in \{1,2,3,...,L,R\}$. Further, an inverse DFrFT is applied to $\mathbf{I}_{\text{Rec}}$ to obtain a referenced image denoted as $\mathbf{I}_R$ for watermarking embedding, which can be expressed as follows: $\mathbf{I}_{\text{Ref}} = \mathcal{F}^{-P}(I_{\text{Rec}})$. However, $\mathbf{I}_{\text{Ref}}$ is a complex-valued matrix that consists of real and imaginary parts such that $\mathbf{I}_{\text{Ref}} = \mathbf{I}_R + \mathbf{I}_I$.

Step 5: Initialize an embedding parameter $\vartheta > 1$ and separate the real ($\mathbf{I}_R$) and imaginary ($\mathbf{I}_I$) parts of the multi-dimensional vector $\mathbf{I}_{\text{Ref}}$. Next, divide $\mathbf{I}_R$ into distinct and non-overlapping blocks ($\mathbf{B}$) of size $(R \times C)$, and rearrange into a column of the resulting matrix $\mathbf{X}$. Here, R and C are the row and column of the watermark logo $\mathbf{W}_L$.

In order to understand this process, let us consider $\mathbf{I}_R$ is (3×3) matrix and block $\mathbf{B}_{R\times C}$ is (2×2):



The above illustration shows a procedure of the matrix to column transformation, i.e., arranging $R \times C$ block in the real part of image $\mathbf{I}_R$ into a column of resulting matrix $\mathbf{X} \leftarrow (X_{L,R})_{L\times R}$. Also, the insufficient block is padded with zero.

Step 6: Make the watermark logo image $\mathbf{W}_L$ bipolar and embed information in each block of matrix $\mathbf{X}$, given as:

for each column C of $\mathbf{X} \leftarrow \text{size}(\mathbf{X}_{[R]})$

// R denotes column of matrix $\mathbf{X}$

$\mathbf{X}_{[L\,R]} = \mathbf{X}(:, C) + (\vartheta \times \mathbf{W}_L)$

end

Afterward, rearrange the matrix $\mathbf{X}_{[L\,R]}$ into its original form by executing the operation of the column to matrix manipulation. In this process, the column of $\mathbf{X}_{[M\,N]}$ is rearranged into a matrix with blocks ($\mathbf{B}$) of size ($R \times C$) to construct a matrix $\mathbf{XI}_R$ of size ($M \times N$). Here, $M \times N$ indicates the size of the original input image $\mathbf{I}_m$.

Step 7: Add the newly obtained real part of image $\mathbf{XI}_R$ to the imaginary part $\mathbf{I}_I$ to obtain the watermark-embedded image $\mathbf{I}_w = \mathbf{XI}_R + (\mathbf{J} \times \mathbf{I}_I)$. Then, apply the DFrFT and wavelet decomposition followed by its inverse to the obtained image $\mathbf{I}_w$, to obtain the final watermarked image.

5.2. Watermark extraction

The watermark extraction process is just the inverse procedure of the embedding operations. Additionally, the proposed system also simulates an attack model to evaluate the performance of the proposed watermarking scheme. The attack model consists of the different image processing operations, such as compression, filtering, rotation, etc. The idea is to apply these image processing operations to the watermarked image and then extract the watermark. The process considers watermarked image $\mathbf{I}_w$ and, after applying a similar operation of embedding, the original input $\mathbf{I}_m$ and watermark image $\mathbf{W}_L$ are obtained. The extraction process is as follows:

Step 1: Apply the DFrFT to $\mathbf{I}_w$ and obtain the transformed image $\mathbf{I}'_w$ in the frequency domain using Eq. (9).

Step 2: Decompose $\mathbf{I}'_w$ to obtain an optimal sub-band tree structure and compute the approximation and detail coefficients. Further, reconstruct the decomposed image using Eqs. (10) and (11), and then apply the inverse DFrFT to obtain the decomposed frequency domain image in its original domain, $\mathbf{X}_w$.

Step 3: Divide $\mathbf{X}_w$ into blocks following a similar operation to the matrix to column transformation. This newly obtained image named $\mathbf{X}2$ is then evaluated with the coordinates of the image $\mathbf{X}$ such that

$$\mathbf{C} = \mathbf{X}2 > \mathbf{X}, \tag{17}$$

where $\mathbf{C}$ is a vector of the logical values $\rightarrow \mathbf{C}_{M\times 1}$.

Step 4: Compute the mean of the logical elements in vector $\mathbf{C}_{M\times 1}$ and convert it to a matrix of size ($R \times C$) i.e., transforming it from a 1D to a 2D block shape. Basically, this process provides extraction of the watermark block of size $R \times C$. This can be expressed as follows:

$$\mathbf{W}_L = f_r(\mathbf{C}, [r, c]), \tag{18}$$

where f_r denotes a function that reshapes the vector $\mathbf{C}_{M\times 1}$ whose elements are taken column-wise and returns an $R \times C$ matrix $\mathbf{W}_L$.

6. Result and performance analysis

The design and development of the proposed watermarking technique is carried out using the MATLAB numerical computing tool. The study uses a brain MRI dataset for the analysis [37]. The proposed study also simulated attack where various image preprocessing operations such as filtering, cropping, compression, etc., are applied to the watermarked image. The analysis is carried out to assess the technique's imperceptibility and robustness factors measured concerning the peak-signal to noise ratio (PSNR), bit error rate (BER), and correlation coefficient. Imperceptibility is crucial for watermarking, ensuring that the perceived quality of the host image is not significantly degraded. In this regard, PSNR is calculated to quantitatively measure imperceptibility expressed as follows:

$$\text{PSNR} = 10 \cdot \log_{10} \left(\frac{255^2}{\text{MSE}} \right) \text{ [dB]}, \tag{19}$$

where MSE denotes the mean square error between the input image $\mathbf{I}_m$ and the watermarked image $\mathbf{I}_w$ given as follows:

$$\text{MSE} = \frac{1}{M \times N} \sum_{m=1}^{M} \sum_{n=1}^{N} \left[\mathbf{I}_m(m,n) - \mathbf{I}_w(m,n) \right]^2. \tag{20}$$

The performance analysis concerning robustness involves assessing resistive strength of the watermarking technique against image processing operations to remove or degrade watermarks in the image. The study considers the assessment of similarity between the input watermark logo $\mathbf{W}_L$ and watermark extracted ($\mathbf{W}'_L$) from the attacked watermarked image. The measurement of the similarity factor between these two is carried out using correlation coefficient ρ given as follows:

$$\rho\left(\mathbf{W}_L, \mathbf{W}'_L\right) = \frac{\sum\limits_{i=1}^{N} \mathbf{W}_L, \mathbf{W}'_L}{\sum\limits_{i=1}^{N} \left(\mathbf{W}_L\right)^2 \sum\limits_{i=1}^{N} \left(\mathbf{W}'_L\right)^2}, \tag{21}$$

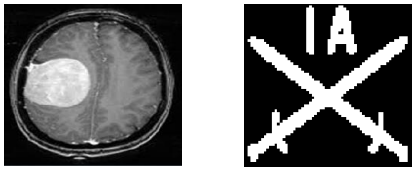
where N denotes the number of pixels in the $\mathbf{W}_L$ and $\mathbf{W}'_L$.

The performance of watermark extraction is also evaluated using BER given as follows:

$$\text{BER} = \left(\frac{N_e}{N} \times 100 \right) \text{ [\%]}, \tag{22}$$

where N_e denotes inaccurately extracted watermark bits and N represents the number of watermark bits.

Figure 4 presents a visualization of the input grayscale medical image $\mathbf{I}_m$ and the binary watermark logo $\mathbf{I}_w$ considered for the embedding process. The input image is a magnetic resonance image (MRI) of the brain, showing a tumor. The watermark logo is a sample image of the general logo and it is assumed that this image represents patient's information embedded in the input medical image. Although, in existing healthcare applications, patient's information can be accessed via electronic health record (EHR), but the proposed scheme does not consider EHR. Instead, it offers an additional flexibility to add more secret information to radiological images of a patient, which could be used for authenticating the ownership of that image by both the patient and healthcare unit.



Input $\mathbf{I}_m$ (256×256) Input $\mathbf{I}_w$ (64×64)

FIG. 4. Visualization of the input data.

Figure 5a exhibits watermark embed image in the frequency domain, Fig. 5b shows watermarked frequency, Fig. 5c demonstrates final watermarked image, and Fig. 5d represents extracted watermark when there is no attack performed on the watermarked image.

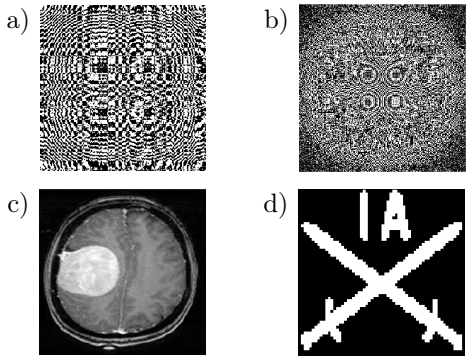


FIG. 5. Visualization of the watermarking process: a) embedded image, b) watermarked frequency, c) watermarked image, and d) recovered watermarked.

6.1. Visual outcome analysis

Figure 6 provides a visual outcome of the proposed watermarking technique under seven different attacks regarding the attacked watermarked image and the corresponding recovered watermark logo. The attack model-1 simulates JPEG

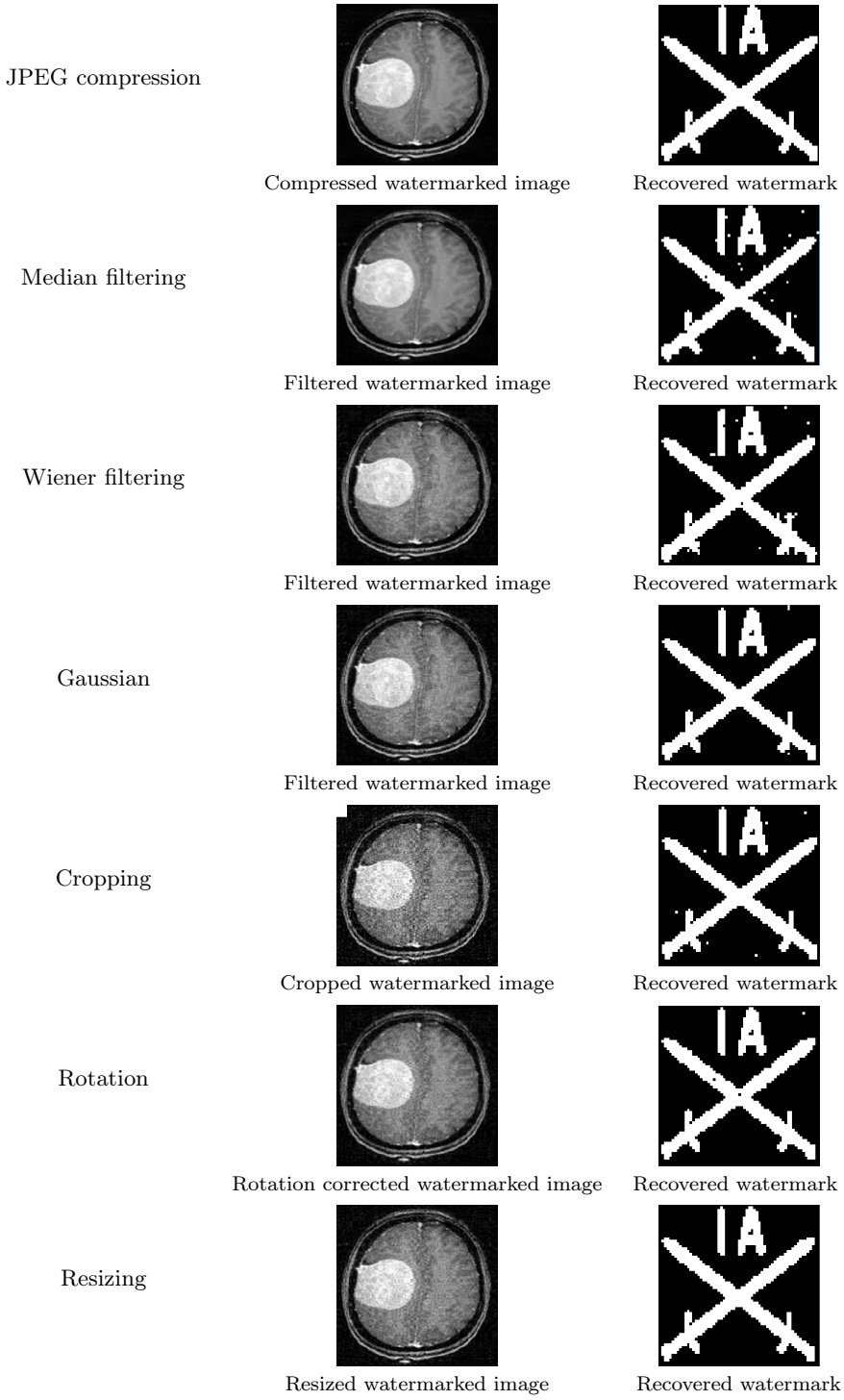


FIG. 6. Analysis of attacked watermarked image and recovered watermark.

compression of the watermarked image with a compression quality 30%. The attack model-2 and 3 are median and Wiener filtering with a filter size equal to 3. The attack model-4 simulates Gaussian filtering operation with a sigma value of 0.5. The attack model-5 simulates image cropping operation with a cropping area 20×20. The attack model-6 simulates image rotation with an angle of 20°, and the attack model-7 performs an image resizing with a resolution ratio factor of 2. It could be noted that the proposed scheme is completely independent of types and forms of a medical image. The proposed study executes a performance analysis regarding different embedding intensity values for the comprehensive analysis, and varying watermark resolutions are shown in a subsequent section.

6.2. Result discussion and implication

In Fig. 7, the performance analysis regarding the PSNR metric is carried out to assess the quality of the watermarked image across varying watermark embedding intensities. From the graph trend, it can be observed that PNSR value decreases with the increasing embedding intensity. But, in most cases, if the value of PSNR is greater than 37 dB (PSNR $>$ 37 dB), the watermarked image is considered suitable or considerable and is invisible to the human visual system (HVS). The graph trend shows that for embedding intensity ranging from 1 to 5, the proposed watermarking scheme achieves a SNR value of more than 37 dB. However, when the value of embedding intensity is 6, the proposed system shows smaller PSNR value, i.e., 35.9 dB. Overall, the proposed system reaches a higher PSNR value, which means that it has good invisibility. Thus, the proposed watermarking scheme meets the requirements for invisibility, both

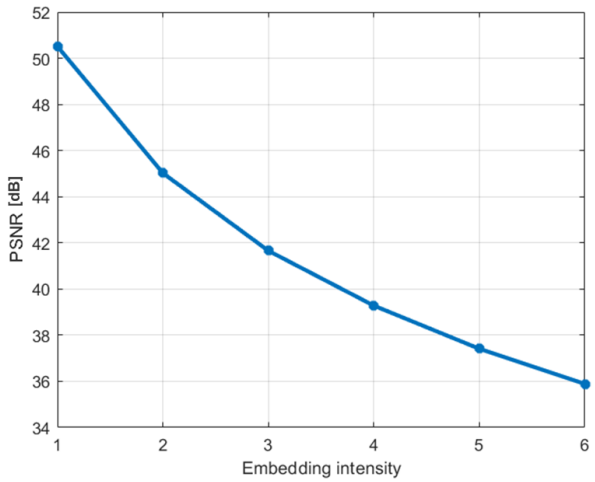


Fig. 7. Analysis of PSNR vs. embedding intensity.

from the perspective of subjective and objective analysis. It is important to note that the performance-based statistics score may vary from one image to another, depending on the visual characteristics of the input image.

Therefore, it does not mean that obtaining a low PSNR for this input image will be the same for different images. In this regard, further evaluation is carried out considering different watermark resolutions, as shown in Fig. 10. In this analysis, the graph trend in Fig. 10 exhibits varying PSNR values over different watermarked image resolutions. For a resolution size of 16×16, the PSNR value is observed at 39.258 dB; for a resolution size of 32×32, the PSNR is 39.263; for a watermark resolution size of 64×64, the PSNR value is 39.289, and for a resolution size of 128×128, the PSNR is 39.224. Based on the analysis, the highest PSNR is achieved for a watermark resolution size of 64×64, which is the original resolution. The remaining resolutions result from the interpolation method's upsampling and downsampling processes. Thus, the original resolution contains non-redundant and high-quality information, exhibiting a higher PSNR. The performance analysis for robustness is conducted regarding correlation coefficient assessment as shown in Figs. 8 and 11. Robustness specifies the effectiveness of the proposed watermarking scheme to resist any alteration or modification without compromising its original steady arrangement or configuration. Therefore, it is crucial to validate the robustness of the presented image watermarking scheme, which is done by assessing the quality of the recovered watermark logo when the watermarked image is attacked via different image processing operations.

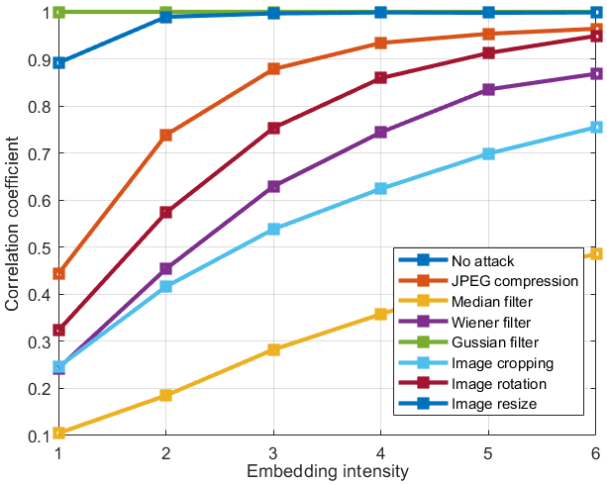


Fig. 8. Analysis of correlation coefficient vs. embedding intensities.

In Fig. 8, the correlation coefficient assessment is carried out for varying embedding intensities. Typically, a correlation coefficient equal to or above 0.75

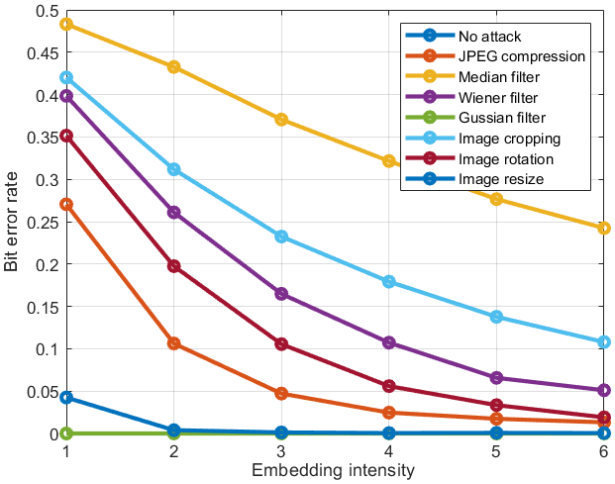


FIG. 9. Analysis of BER vs. embedding intensities.

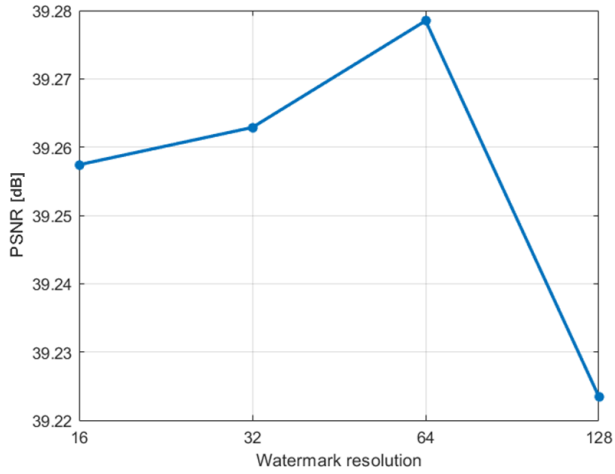


FIG. 10. Analysis of PSNR vs. different watermark resolution.

is considered acceptable. The graph trend indicates that the proposed watermarking technique is robust under most attacks, except for the median filtering attacks. Median filtering aims to substitute the gray level of an image pixel via the median of the gray levels in neighboring pixels, as opposed to utilizing the mean analysis. However, the proposed system exhibits better quality for other cases of embedding intensities. The performance analysis regarding BER is shown in Fig. 9 for varying embedding intensities and in Fig. 12 for various resolutions. The graph trends indicate lower BER at higher embedding intensities and for lower resolution. Notably, the proposed technique shows a higher BER for median filtering because the watermark logo is embedded in high-frequency

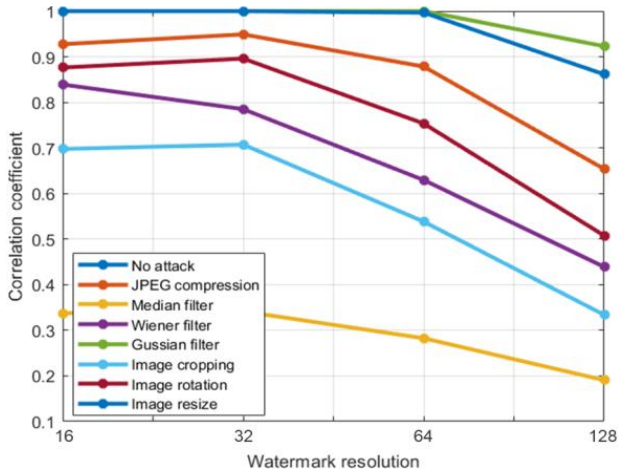


FIG. 11. Analysis of correlation coefficient vs. different watermark resolution.

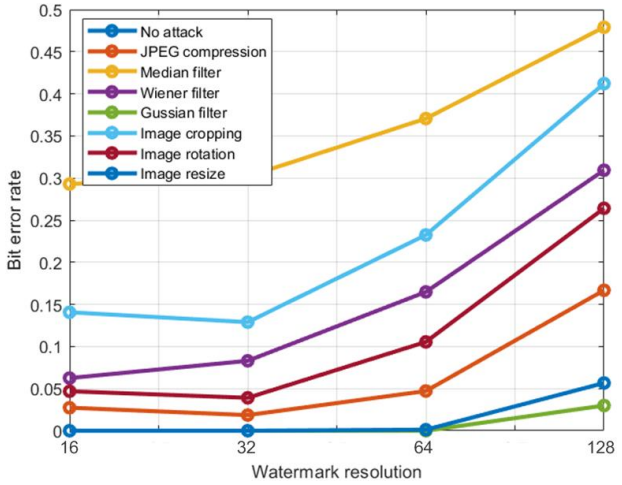


FIG. 12. Analysis of BER vs. different watermark resolution.

sub-bands, and when median filtering is applied, high-frequency components are distorted, leading to an increased BER. Adopting DICOM images is also permissible to carry out a similar experiment as MATLAB facilitates processing these images with exclusive processing methods. However, the trend of outcomes remains nearly same.

7. Conclusion

The proposed research introduced an effective watermarking scheme based on sub-band tree structuring and DFrFT transform. This alternative solution is

better than conventional transform-based techniques as it offers a balance between computational efficiency and signal quality simultaneously. Particularly, the sub-band tree structuring provides a smoother and deeper analysis of input sub-bands for watermark embedding. This approach offers a better progressive solution compared to iterative solution used in existing encryption-based watermarking strategies. The invisibility and robustness of the proposed watermarking scheme are assessed through the simulation analysis considering various image quality indicators. The results indicate that the watermarked image maintains good visual quality. Apart from this, the watermark logo can be efficiently extracted without compromising the quality of the watermarked image under various attacks. As the proposed system is a simplified computational framework, it overcomes the cost-based problems associated with existing usage of multi-core technologies. Also, it was noted that the proposed system achieved better invisibility and robustness with different resolutions. However, in the case of median filtering, the proposed system performance is not as strong compared to other attacks. Therefore, more improvement will be incorporated for the performance enhancement using optimal approaches in future work.

References

1. B. Al Hayani, H. Ilhan, Image transmission over decode and forward based cooperative wireless multimedia sensor networks for Rayleigh fading channels in medical internet of things (MIoT) for remote healthcare and health communication monitoring, *Journal of Medical Imaging And Health Informatics*, **10**(1): 160–168, 2020, doi: 10.1166/jmihi.2020.2691.

2. R.F. Mansour, E.M. Abdelrahim, An evolutionary computing enriched RS attack resilient medical image steganography model for telemedicine applications, *Multi-dimensional Systems and Signal Processing*, **30**(2): 791–814, 2019, doi: 10.1007/s11045-018-0575-3.

3. J. Zain, M. Clarke, Security in telemedicine: Issues in watermarking medical images, [in:] *3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications*, March 27–31, Tunisia, 2005.

4. R. Thanki, S. Borra, *Medical Imaging and Its Security in Telemedicine Applications*, Cham, Switzerland, Springer, 2019, doi: 10.1007/978-3-319-93311-5.

5. F. Cao, H.K. Huang, X.Q. Zhou, Medical image security in a HIPAA mandated PACS environment, *Computerized Medical Imaging and Graphics*, **27**(2–3): 185–196, 2003, doi: 10.1016/s0895-6111(02)00073-3.

6. S. Rai, R. Boghey, D. Shahane, P. Saxena, Digital image watermarking against geometrical attack, [in:] R.K. Shukla, J. Agrawal, S. Sharma, G. Singh Tomer [Eds.], *Data, Engineering and Applications*, pp. 129–145, Springer, Singapore, 2019, doi: 10.1007/978-981-13-6351-1_12.

7. M. Begum, M.S. Uddin, Implementation of secured and robust DFT-based image watermark through hybridization with decomposition algorithm, *SN Computer Science*, **2**(3): 221, 2021, doi: 10.1007/s42979-021-00608-6.

8. S. Kumar, B.K. Singh, DWT based color image watermarking using maximum entropy, *Multimedia Tools and Application*, **80**(10): 15487–15510, 2021, doi: 10.1007/s11042-020-10322-9.

9. D. Singh, S.K. Singh, DCT based efficient fragile watermarking scheme for image authentication and restoration, *Multimedia Tools and Application*, **76**(1): 953–977, 2017, doi: 10.1007/s11042-015-3010-x.

10. R. Sinhal, S. Sharma, I.A. Ansari, V. Bajaj, Multipurpose medical image watermarking for effective security solutions, *Multimedia Tools and Applications*, **81**(10): 14045–14063, 2022, doi: 10.1007/s11042-022-12082-0.

11. I.K. Yeo, H.J. Kim, Generalized patchwork algorithm for image watermarking, *Multimedia Systems*, **9**(3): 261–265, 2003, doi: 10.1007/s00530-003-0097-0.

12. F. Zhang, T. Luo, G. Jiang, M. Ju, H. Xu, W. Zhou, A novel robust color image watermarking method using RGB correlations, *Multimedia Tools and Applications*, **78**(14): 20133–20155, 2019, doi: 10.1007/s11042-019-7326-9.

13. M. Nazari, M. Mehrabian, A novel chaotic IWT-LSB blind watermarking approach with flexible capacity for secure transmission of authenticated medical images, *Multimedia Tools and Applications*, **80**(7): 10615–10655, 2021, doi: 10.1007/s11042-020-10032-2.

14. P. Priyadarshini, A. Dash, K. Naik, Secure sharing of medical images using watermarking technique, [in:] A.K. Das, J. Nayak, B. Naik, S. Vimal, D. Pelusi [Eds.], *Computational Intelligence in Pattern Recognition, CIPR 2022, Lecture Notes in Networks and Systems*, Vol. 480, pp. 592–604, Springer, Singapore, 2022, doi: 10.1007/978-981-19-3089-8_56.

15. A.K. Singh, B. Kumar, G. Singh, A. Mohan, Medical image watermarking techniques: a technical survey and potential challenges, [in:] *Medical Image Watermarking*, pp. 13–41, Springer, Cham, 2017, doi: 10.1007/978-3-319-57699-2_2.

16. P. Parashar, R.K. Singh, A survey: digital image watermarking techniques, *International Journal of Signal Processing, Image Processing and Pattern Recognition*, **7**(6): 111–124, 2014, doi: 10.14257/ijsip.2014.7.6.10.

17. A.K. Singh, N. Sharma, M. Dave, A. Mohan, A novel technique for digital image watermarking in spatial domain, [in:] *2021 2nd IEEE International Conference on Parallel, Distributed and Grid Computing*, pp. 497–501, Solan, India, 2012, doi: 10.1109/PDGC.2012.6449871.

18. H.J. Ko, C.T. Huang, G. Horng, S.J. Wang, Robust and blind image watermarking in DCT domain using inter-block coefficient correlation, *Information Sciences*, **517**(1): 128–147, 2020, doi: 10.1016/j.ins.2019.11.005.

19. A. Ray, S. Roy, Recent trends in image watermarking techniques for copyright protection: a survey, *International Journal of Multimedia Information Retrieval*, **9**(4): 249–270, 2020, doi: 10.1007/s13735-020-00197-9.

20. A. Anand, A.K. Singh, Watermarking techniques for medical data authentication: a survey, *Multimedia Tools and Applications*, **80**(20): 30165–30197, 2021, doi: 10.1007/s11042-020-08801-0.

21. B. Hassan, R. Ahmed, B. Li, O. Hassan, An imperceptible medical image watermarking framework for automated diagnosis of retinal pathologies in an eHealth arrangement, *IEEE Access*, **7**: 69758–69775, 2019, doi: 10.1109/ACCESS.2019.2919381.

22. D. Nuñez-Ramirez, M. Cedillo-Hernandez, M. Nakano-Miyatake, H. Perez-Meana, Efficient management of ultrasound images using digital watermarking, *IEEE Latin America Transactions*, **18**(8): 1398–1406, 2020, doi: 10.1109/TLA.2020.9111675.

23. K.M. Hosny, M.M. Darwish, K. Li, A. Salah, Parallel multi-core CPU and GPU for fast and robust medical image watermarking, *IEEE Access*, **6**: 77212–77225, 2018, doi: 10.1109/ACCESS.2018.2879919.

24. G.-D. Su, C.-C. Chang, C.-C. Lin, Effective self-recovery and tampering localization fragile watermarking for medical images, *IEEE Access*, **8**: 160840–160857, 2020, doi: 10.1109/ACCESS.2020.3019832.

25. X. Liu *et al.*, A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images, *IEEE Access*, **7**: 76580–76598, 2019, doi: 10.1109/ACCESS.2019.2921894.

26. S. Haddad, G. Coatrieux, A. Moreau-Gaudry, M. Cozic, Joint watermarking-encryption-JPEG-LS for medical image reliability control in encrypted and compressed domains, *IEEE Transactions on Information Forensics and Security*, **15**: 2556–2569, 2020, doi: 10.1109/TIFS.2020.2972159.

27. A. Shehab *et al.*, Secure and robust fragile watermarking scheme for medical images, *IEEE Access*, **6**: 10269–10278, 2018, doi: 10.1109/ACCESS.2018.2799240.

28. J. Liu, J. Ma, J. Li, M. Huang, N. Sadiq, Y. Ai, Robust watermarking algorithm for medical volume data in internet of medical things, *IEEE Access*, **8**: 93939–93961, 2020, doi: 10.1109/ACCESS.2020.2995015.

29. A.A. Abd El-Latif, B. Abd-El-Atty, M.S. Hossain, M.A. Rahman, A. Alamri, B.B. Gupta, Efficient quantum information hiding for remote medical image sharing, *IEEE Access*, **6**: 21075–21083, 2018, doi: 10.1109/ACCESS.2018.2820603.

30. N.A. Memon, A. Alzahrani, Prediction-based reversible watermarking of CT scan images for content authentication and copyright protection, *IEEE Access*, **8**: 75448–75462, 2020, doi: 10.1109/ACCESS.2020.2989175.

31. N.A. Loan, N.N. Hurrah, S.A. Parah, J.W. Lee, J.A. Sheikh, G.M. Bhat, Secure and robust digital image watermarking using coefficient differencing and chaotic encryption, *IEEE Access*, **6**: 19876–19897, 2018, doi: 10.1109/ACCESS.2018.2808172.

32. K. Gourrame, F. Ros, H. Douzi, R. Harba, R. Riad, Fourier image watermarking: Printcam application, *Electronics*, **11**(2): 266, 2022, doi: 10.3390/electronics11020266.

33. J. Arif, S.P. Gangwar, An efficient watermarking process based on three-level DWT and FFT technique, [in:] D. Harvey, H. Kar, S. Verma, V. Bhadauria [Eds.], *Advances in VLSI, Communication, and Signal Processing*, Vol. 683, Springer, pp. 303–311, 2020, doi: 10.1007/978-981-15-6840-4_24.

34. R. Kumari, A. Mustafi, An optimized framework for digital watermarking based on multi-parameterized 2D-FrFT using PSO, *Optik*, **248**: 168077, 2021, doi: 10.1016/j.ijleo.2021.168077.

35. N. Hasan, M.S. Islam, W. Chen, M.A. Kabir, S. Al-Ahmadi, Encryption based image watermarking algorithm in 2DWT-DCT domains, *Sensors*, **21**(16): 5540, 2021, doi: 10.3390/s21165540.

36. A. Dwivedi, M. Yadav, A. Kumar, FFT-based zero-bit watermarking for facial recognition and its security, [in:] M. Dave, R. Garg, M. Dua, J. Hussien [Eds.], *Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences: Algorithms for Intelligent Systems*, Vol. 195, pp. 403–417, Springer, Singapore, 2021, doi: 10.1007/978-981-15-7533-4_31.

37. N. Chakrabarty, *Brain MRI Images for Brain Tumor Detection*, Kaggle, 2019, https://www.kaggle.com/datasets/navoneel/brain-mri-images-for-brain-tumor-detection.

38. A. Das, Discrete Fourier transform, [in:] *Signal Conditioning*, *Signals and Communication Technology*, Springer, Berlin, Heidelberg, pp. 159–192, 2012, doi: 10.1007/978-3-642-28818-0_7.

39. J. Evers, F. Evers, F. Goppelt, R. Schmidt-Vollus, Singular spectrum analysis-based image sub-band decomposition filter banks, *EURASIP Journal on Advances in Signal Processing*, **2020**: 29, 2020, doi: 10.1186/s13634-020-00685-4.

Received March 18, 2022; revised version May 18, 2022; accepted June 6, 2022.