SGI-JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME. 9
ISSUE. 1
FEB., 2025

A COMBINED APPROACH OF DWT-DCT FOR BLIND MEDICAL IMAGE WATERMARKING

[1]Geetha Reddy PhD & [2]Ravika Y. Jasmine
[1,2]Department of Computer Science Engineering, Malla Reddy Engineering College for Women, Telangana, India.

Abstract
With the rapid advancement of digital technologies, the sharing and distribution of medical images have become widespread, posing serious security challenges. To protect sensitive medical data from unauthorized access and tampering, watermarking has emerged as a crucial security measure. In addition, the concept of watermarking has become vital in preserving the integrity and authenticity of these images. Traditional watermarking techniques faced limitations in terms of robustness and visibility, especially for medical imaging, where image quality is paramount. To overcome these challenges, this work introduces an innovative blind medical image watermarking technique that combines the Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT). The proposed method ensures robust and imperceptible watermark embedding and retrieval while maintaining the visual quality of medical images. The significance of robust and imperceptible medical image watermarking cannot be overstated. As medical institutions increasingly adopt digital practices like telemedicine and electronic health records, the risk of data breaches, tampering, and unethical practices also rises. An efficient watermarking technique is crucial to protect patient privacy, maintain trust in medical institutions, and ensure the authenticity of medical data. The combined DWT-DCT approach presented in this paper offers a promising solution by enabling secure watermark embedding and retrieval, ensuring tamper detection and authentication.
Keywords: Medical, Image, Water, Marking.

I. Introduction

Blind medical image watermarking is a specialized and vital application of digital watermarking techniques within the healthcare industry. It specifically addresses the need to embed hidden, secure, and tamper-resistant information within medical images such as X-rays, MRI scans, CT scans, and authenticity, and confidentiality of patient data and diagnostic images at all stages of their lifecycle, from acquisition and storage to transmission and analysis.

This technology involves the insertion of digital watermarks into medical images without compromising their diagnostic value. These watermarks typically contain essential patient information, including the patient's name, medical record number, date, and institution, as well as additional metadata for authentication and tracking purposes. Advanced algorithms and techniques are employed to embed the watermark in such a way that it remains invisible to the human eye and resilient to common image processing operations and attacks.

Security

Watermarks are encrypted and embedded to ensure that only authorized users or systems can extract and decipher the information. This ensures that patient data remains confidential and protected against unauthorized access or tampering.

Authentication

Watermarks serve as a means to verify the authenticity of medical images. Radiologists, clinicians, and healthcare professionals can use watermark extraction to confirm that the image has not been altered or tampered with since its creation.

Traceability

Watermarks can include metadata related to the image's origin, modifications, and access history. This traceability is crucial for legal and forensic purposes and helps maintain a comprehensive audit trail.

Invisibility

Watermarks are imperceptible to both human observers and automated diagnostic tools. They do not interfere with the visual quality or diagnostic accuracy of the medical image.

Robustness

The watermarking technique is designed to withstand common image manipulations, compression algorithms, and noise, ensuring that the embedded information remains intact even in adverse conditions.

Blind Extraction

Blind watermark extraction means that the watermark can be retrieved without needing the original, unwatermarked image. This is essential for situations where only the watermarked image is available.

II. Literature Survey

In telemedical applications, the verification of authenticity and copyright for medical images play a major role. Telemedicine-based medical image diagnosis is carried out with different techniques such as X-ray, ultrasound scanning, etc. Verification in the medical field is an important application for ensuring the authenticity of patient data in the time of transition of medical image. Data hiding is used to conceal a piece of information secretly in the medical image such as the electronic patient report

Recently, digital watermarking has become an important approach for protecting the legitimacy and copyright of medical images. The digital watermarking approach exhibits technologies and methods that embed data into the host such as digital data, audio, video, and image without modifying its quality [2]. Generally, digital watermarking techniques are used for authentication, broadcast monitoring, database indexing, and medical imaging. The watermarking methods use fragile, semi-fragile, blind, and robust watermarks to provide authentication and copyright protection. Watermarking schemes are classified into Region of interest (ROI) lossless watermarking scheme, zero watermarking scheme, and reversible watermarking scheme [3]. ROI is the important area where important diagnosis data is presented in the medical images. In a reversible watermarking scheme, the authentication of a specific image is extracted from its watermarked image very accurately [4].

In digital images, watermarking secret data is embedded into the host image for ownership authentication. There are different watermarking schemes to insert the data into the host image. The easiest form of watermarking is the alteration of the least significant bit (LSB) of the host image, which is called a fragile watermark [5,6,7]. Generally, the technique is used for patient information and to identity verification. Moreover, the medical image watermarking algorithm can be categorized into the authentication and integrity control (AIC) algorithm, data-hiding algorithm, and a combination of data-hiding algorithm as well as AIC [8,9]. The AIC algorithm aims to ensure the integrity and identity of the source image [10]. There are different applications of digital watermarking, such as content and image authentication, fingerprinting, tamper-proofing, digital rights management, and copyright protection, etc. The better way of performing watermarking is by ensuring that the image quality is not degraded and not affected by any attacks.

To achieve content authentication and tamper localization in secured telemedicine, Swaraja, K et al. developed a framework with blind dual medical image watermarking. This method was used to prevent the alteration of content. In the medical image, the regions of non-interest (RONI) blocks were used to hide the dual watermarks for authentication and recognition. This framework demonstrated its superior capabilities and outperformed the other related optimized hybrid algorithms. This method retrieved the original region of interest (ROI) without any loss of information. Liu, X et al. [12] developed a reversible water marking technique to safeguard the integrity and authenticity of medical images. The region of interest (ROI) watermarking entailed the risk of spatial image segmenting. The ROI method had failed in the recovery of tampered areas. In this method, recursive dither modulation (RDM) is used to avoid diagnostic biases. Singular value decomposition and slantlet transform combined with RDM are used to protect image authenticity. This method outperformed all the other techniques for medical image protection.

III. Proposed Methodology

Overview

Figure 1 in this work illustrates a comprehensive watermark embedding process designed for medical images. The process is orchestrated to enhance the security and integrity of these images by seamlessly embedding hidden information while maintaining diagnostic quality.

At the outset, the 'Host Image' is chosen as the canvas for the watermark. This image could be any medical scan, such as an X-ray or an MRI, and it serves as the foundation upon which the watermark will be added. Next, this work employs a multi-step transformation approach, starting with 'DWT (Wavelet Decomposition).' This Discrete Wavelet Transform breaks down the host image into different frequency components, a critical step to bolster the watermark's resilience against common image manipulations.

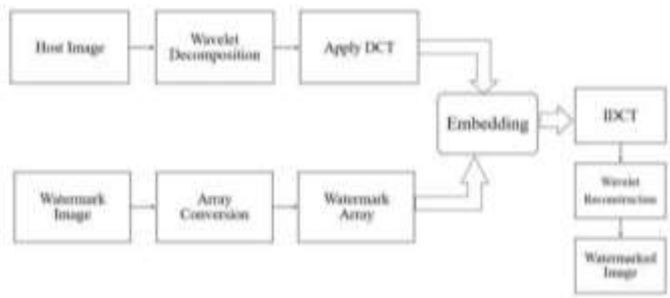

Figure.1: Proposed watermark embedding process.

Following the wavelet decomposition, the process progresses to 'DCT,' which stands for Discrete Cosine Transform. The application of DCT allows the conversion of spatial domain information into the frequency domain, contributing to the watermark's robustness against certain types of attacks.

Simultaneously, the 'Watermark Image,' which can encompass various forms of data like images or text, is introduced as the content to be concealed within the host image. The 'Array Conversion' step is pivotal in the process, as it transforms both the DCT coefficients and the watermark image into arrays or matrices. This prepares them for further mathematical operations and their eventual integration. The 'Watermark Array' represents the converted watermark image in an array format, preparing it for seamless integration with the DCT coefficients.

The actual embedding of the watermark into the host image takes place during the 'Embedding' phase. This step involves intricate algorithms that subtly modify the DCT coefficients to incorporate the watermark, all while striving to ensure minimal visual degradation. After embedding the watermark, the process proceeds with 'IDCT' (Inverse Discrete Cosine Transform), which inversely transforms the frequency domain information back into the spatial domain. This is crucial for the reconstruction of the image.

Lastly, 'Wavelet Reconstruction' utilizes the inverse of the earlier 'DWT (Wavelet Decomposition)' step to reconstruct the final 'Watermarked Image.' This resulting image appears visually similar to the original host image but now contains the embedded watermark.

DWT

The Discrete Wavelet Transform (DWT) is a mathematical technique used for signal and image processing, including applications in data compression, feature extraction, and denoising. DWT operates by decomposing a signal or image into different frequency components at multiple scales. Here's a detailed explanation of the operation of the DWT:

Preparation of Data

DWT begins with a one-dimensional or two-dimensional signal or image as input data. The input signal or image typically has a finite length or size.

Filtering and Down-Sampling (Decomposition)

In the decomposition step, the DWT applies a pair of filters known as the low-pass filter (LPF) and the high-pass filter (HPF) to the input data as shown in Figure 4.3. The LPF extracts the low-frequency components from the data, while the HPF extracts the high-frequency components. Low-frequency components often represent the coarse details or approximations of the original data, while high-frequency components represent the fine details or noise. After filtering, the data is downsampled by a factor of 2 in both dimensions. Down-sampling reduces the data size by discarding every alternate sample, effectively reducing the resolution by half.

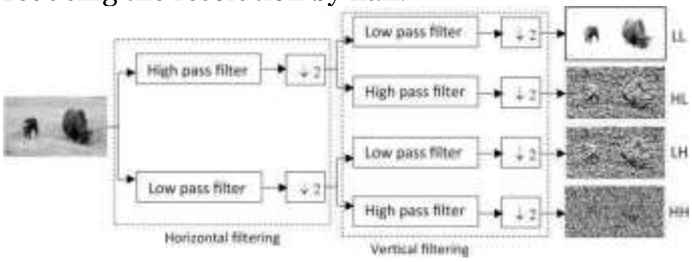

Figure. 2: DWT decomposition.

Scaling and Wavelet Coefficients

The output of the DWT decomposition consists of two sets of data: the approximation coefficients (LL) and the detail coefficients (LH, HL, HH). The LL coefficients represent the lower-scale approximation of the original data, containing the low-frequency information. The LH, HL, and HH coefficients represent the detail information at different scales. LH contains information about low-frequency variations in the vertical direction, HL contains information about low-frequency variations in the horizontal direction, and HH contains high-frequency detail information.

Multiple Decomposition Levels

The DWT process can be recursively applied to the LL coefficients (approximation coefficients) to obtain further decomposition levels. Each level provides a different level of detail, with LL coefficients becoming lower-resolution approximations at each level.

End of Decomposition

The decomposition process continues until the desired level of detail or the maximum decomposition level is reached.

Advantages

The watermark extraction process depicted in Figure 4.2 offers several notable advantages in the context of medical image watermarking, each contributing to its effectiveness and utility:

High Fidelity Extraction

One of the primary advantages is the ability to achieve 'High Fidelity Extraction.' The use of advanced techniques like wavelet decomposition and DCT ensures that the embedded watermark can be accurately and reliably retrieved. This high fidelity is crucial in medical applications where diagnostic accuracy is paramount, as any distortion or loss of information can impact patient care.

Robustness

The process exhibits 'Robustness' against common image processing operations and potential attacks. By applying wavelet decomposition and DCT, the watermark becomes less susceptible to distortions caused by compression, noise, or other manipulations. This robustness ensures that the watermark remains intact and detectable even in challenging conditions.

Multi-Metric Evaluation

The incorporation of 'Evaluation Metrics' such as PSNR, MSE, and entropy provides a comprehensive means of assessing the quality and integrity of the extracted watermark. These metrics enable researchers and practitioners to quantitatively measure the success of the extraction process, ensuring that the watermark remains discernible while minimizing any adverse effects on the image.

Adaptability

The process can be adapted to different types of watermarks and medical image modalities. Whether the watermark is an image, text, or other data, the combination of wavelet decomposition and DCT offers flexibility in handling diverse watermark types. Moreover, it can be applied to various medical image formats, including X-rays, MRIs, and CT scans.

Detection Reliability

The use of wavelet decomposition and DCT enhances the 'Detection Reliability' of the watermark. The transformation of the image data into the frequency domain makes it easier to identify the watermark's presence and characteristics, reducing the likelihood of false positives or negatives during extraction.

Quality Preservation

The process is designed to 'Preserve Image Quality' to the greatest extent possible. While the watermark is embedded and extracted, the impact on the overall quality of the medical image is minimized. This ensures that the watermarked image maintains its diagnostic value, making it suitable for clinical use.

Security and Authentication

The watermark extraction process is instrumental in 'Security and Authentication.' It helps verify the authenticity of medical images, ensuring that they have not been tampered with or altered. This is vital in healthcare settings to maintain the trustworthiness of patient records and diagnostic results.

Transparency

Importantly, the watermark extraction process is 'Transparent' to medical professionals. The presence of the watermark should not hinder their ability to interpret and diagnose medical images. By preserving image quality and ensuring that the watermark is imperceptible to the human eye, the process maintains transparency in clinical workflows.

IV. Results and Discussions

Figure 3 represents the watermarking embedding performance. In (a), we observe a medical image of the brain, which serves as the host image for the watermarking process. This work aims to embed a unique watermark into this medical image while preserving its diagnostic information. In (b), we see the original watermark, which is essentially a distinct identifier or piece of data that needs to be incorporated into the host image. The effectiveness of the watermarking technique used in this work becomes evident in (c), where we witness the output watermarked image. This output image showcases the successful integration of the watermark into the brain medical image, demonstrating the robustness and reliability of the watermarking method employed in this study.

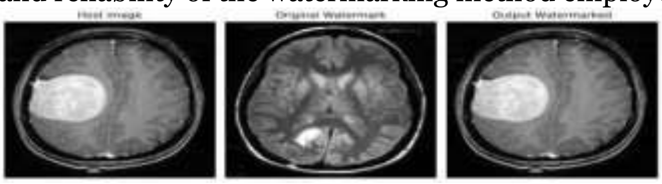

Figure. 3: Watermarking embedding performance. (a) brain medical image. (b) original watermark. (c) output watermarked image

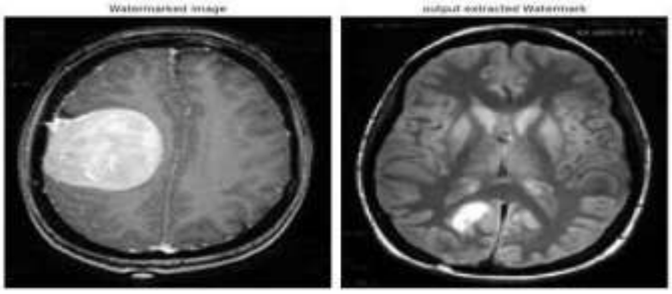

Figure. 4: Watermarking extraction performance. (a) input watermarked image. (b) output extracted watermark image.

Figure 4 illustrates the watermarking extraction performance. In (a), we are presented with the input watermarked image, which is the result of a prior watermark embedding process. This image carries the watermark information that we seek to extract. In (b), we observe the output extracted watermark image. This image represents the successful retrieval of the watermark from the previously watermarked image, showcasing the effectiveness and accuracy of the watermark extraction algorithm utilized in this work.

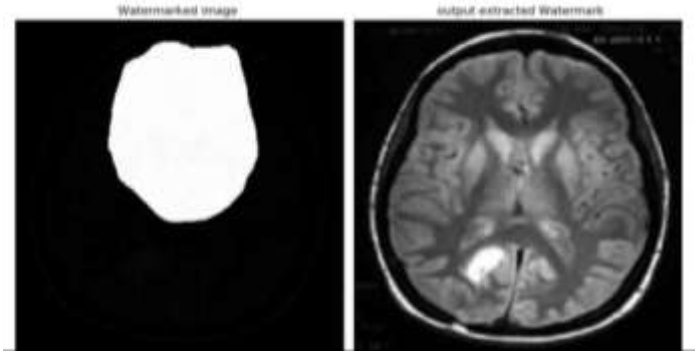

Figure.5: Watermarking extraction performance. (a) segmented watermarked image. (b) output extracted watermark image.

Figure. 6: Watermarking embedding user interface.

Figure. 7: Watermarking extraction user interface.

Performance Comparison

PSNR (Peak Signal-to-Noise Ratio) (dB)

PSNR is a measure of the quality of the watermarked image compared to the original (unwatermarked) image. It quantifies how much the watermarked image differs from the original in terms of noise or distortion. In the existing method, the PSNR value is 45.69 dB, indicating the level of image quality achieved using the existing watermarking technique. In the proposed method, the PSNR value significantly improves to 56.85 dB, indicating that the proposed method results in a higher-quality watermarked image with less distortion or noise. This is a notable improvement in image fidelity.

MSE (Mean Squared Error)

MSE measures the average squared difference between pixel values in the watermarked image and the original image. A lower MSE indicates better image quality. In the existing method, the MSE value is 0.093, suggesting a certain level of distortion or error in the watermarked image compared to the original. In the proposed method, the MSE value is reduced to 0.075, indicating that the proposed method results in less error or distortion when embedding the watermark. This demonstrates superior performance in preserving image content.

Entropy

Entropy measures the amount of information or randomness in an image. Higher entropy values typically indicate that more information is retained. In the existing method, the entropy value is 7.856, suggesting a certain level of information loss or reduced complexity in the watermarked image. In contrast, the proposed method achieves a significantly higher entropy value of 13.595. This indicates that the proposed method better preserves the information content of the image, resulting in a watermarked image with higher complexity and detail.

Metric	Existing Method	Proposed Method
PSNR (dB)	45.69	56.85
MSE	0.093	0.075
Entropy	7.856	13.595

V. Conclusion and Future Scope

In conclusion, the combined approach of DWT-DCT for blind medical image watermarking presented in this study addresses critical security concerns in the sharing and distribution of medical images. The technique offers a robust and imperceptible means of embedding and retrieving watermarks while preserving the visual quality of these sensitive images. As the healthcare industry continues to embrace digitalization and telemedicine, the need for secure and trustworthy medical data management becomes increasingly paramount. This innovative watermarking method contributes significantly to safeguarding patient privacy, maintaining the integrity of medical records, and ensuring the authenticity of medical images.

References

Balasamy, K.; Suganyadevi, S. (2021). A fuzzy based ROI selection for encryption and watermarking in medical image using DWT and SVD. Multimed. Tools Appl., 80, 7167–7186.

Sinhal, R.; Sharma, S.; Ansari, I.A.; Bajaj, V. (2022). Multipurpose medical image watermarking for effective security solutions. Multimed. Tools Appl., 81, 14045–14063.

Ravichandran, D.; Praveenkumar, P.; Rajagopalan, S.; Rayappan, J.B.B.; Amirtharajan, R. (2021). ROI-based medical image watermarking for accurate tamper detection, localisation and recovery. Med. Biol. Eng. Comput. 59, 1355–1372. [PubMed]

Dai, Z.; Lian, C.; He, Z.; Jiang, H.; Wang, Y. (2022). A novel hybrid reversible-zero watermarking scheme to protect medical image. IEEE Access, 10, 58005–58016.

Borra, S.; Thanki, R. (2020). Crypto-watermarking scheme for tamper detection of medical images. Comput. Methods Biomech. Biomed. Eng. Imaging Vis. 8, 345–355.

Iwendi, C.; Jalil, Z.; Javed, A.R.; Reddy, T.; Kaluri, R.; Srivastava, G.; Jo, O. (2020). Keysplit watermark: Zero watermarking algorithm for software protection against cyber-attacks. IEEE Access, 8, 72650–72660.

Cedillo-Hernandez, M.; Cedillo-Hernandez, A.; Nakano-Miyatake, M.; Perez-Meana, H. (2020). Improving the management of medical imaging by using robust and secure dual watermarking. Biomed. Signal Process. Control, 56, 101695.

Wang, W.; Xu, H.; Alazab, M.; Gadekallu, T.R.; Han, Z.; Su, C. (2021). Blockchain-based reliable and efficient certificateless signature for IIoT devices. IEEE Trans. Ind. Inform, 18, 7059–7067.

Alshanbari, H.S. (2021). Medical image watermarking for ownership & tamper detection. Multimed. Tools Appl., 80, 16549–16564.

Thakur, S.; Singh, A.K.; Ghrera, S.P. (2021). NSCT domain–based secure multiple-watermarking technique through lightweight encryption for medical images. Concurr. Comput. Pract. Exp, 33, e5108.

Swaraja, K.; Meenakshi, K.; Kora, P. (2020). An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine. Biomed. Signal Process. Control, 55, 101665.

Liu, X.; Lou, J.; Fang, H.; Chen, Y.; Ouyang, P.; Wang, Y.; Zou, B.; Wang, L. (2019). A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images. IEEE Access, 7, 76580–76598.