2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal

An Innovative Blind Medical Image Watermarking Technique for IoMT Applications

M. Mounika[1], Busa Deepak kumar[2], Kummari Kavya[2], Sutharapu Chandra Shekar Sai[2], Bantu Jagadish[2]

[1]Assistant Professor, [2]UG Scholar, [1,2]Department of Information Technology

[1,2]Malla Reddy College of Engineering and Management Sciences, Kistapur, Medchal, Hyderabad-501401, 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: Digital watermarking, Internet of Things, medical IoT, wavelet transform, discrete cosine transform.

1. 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 ultrasounds. The primary objective of blind medical image watermarking is to ensure the integrity, 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.

Key aspects and features of blind medical image watermarking include:

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.

2. 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 [1]. 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. [11] developed a framework with blind dual medical image watermarking. This method was used to prevent the alteration of content. In the medical image, the region 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.

Zeng, C et al. [13] proposed a multi-watermarking algorithm on KAZE DCT for medical images. The features of the medical images were extracted with KAZE DCT and the sequent features of medical images were obtained with perceptual hashing. The multi-watermark images were encrypted by chaotic mapping. This method resulted in effective extraction of watermarks. This method could witheld both geometric and common attacks. Patel, N et al. [14] developed a DCT DWT hybrid ROI image compression for the application of telemedicine. This method recreated the medical image rapidly and eliminated the unwanted medical data with a compression algorithm. This method increased the data processing speed. The highest PSNR and lowest MSE were obtained using this technique. The best visual image was presented with this DCT compression method. It had bit rates higher than those obtained using wavelet compression algorithms.

3. Proposed methodology

Figure 1 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. 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.

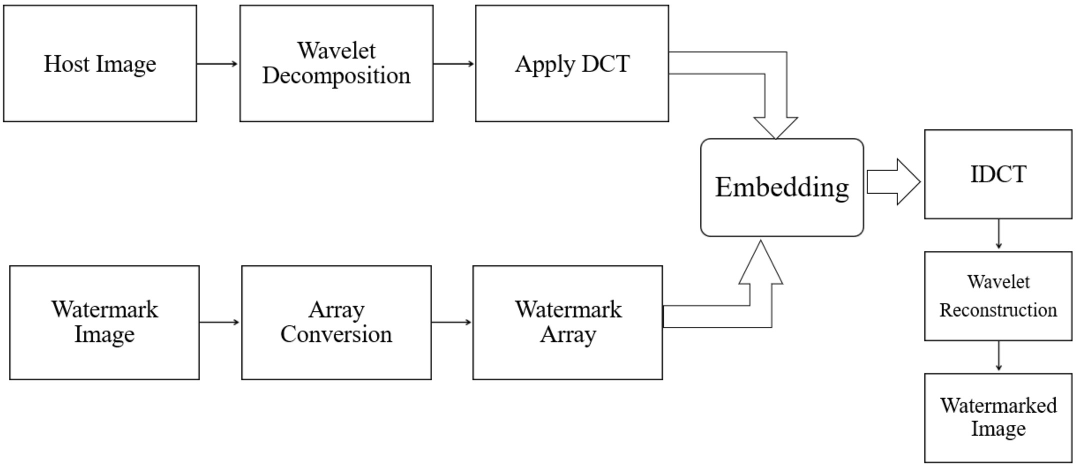
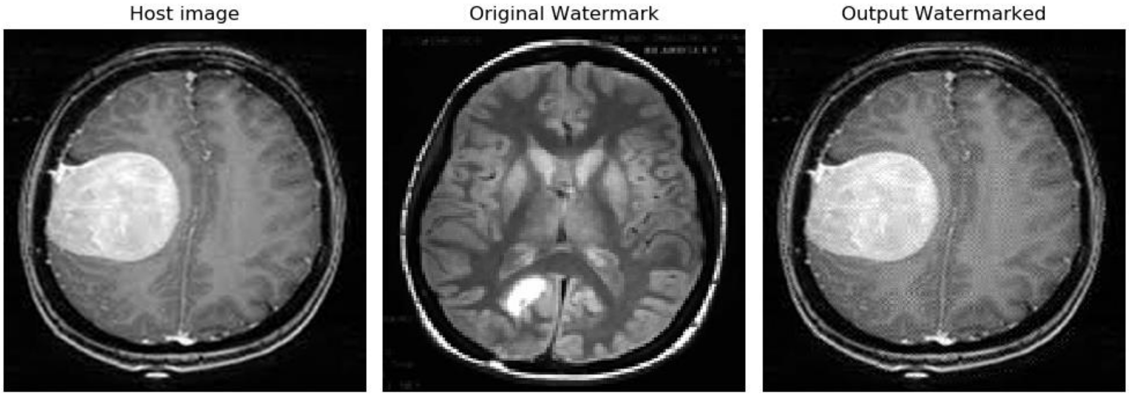


Figure 1. Proposed watermark embedding process.

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.

4. Results and Discussion

Figure 2 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.



(a) (b) (c)

Figure 2. Watermarking embedding performance. (a) brain medical image. (b) original watermark. (c) output watermarked image

5. Conclusion

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

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

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

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

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

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

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

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

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

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

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

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

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

[13]. Zeng, C.; Liu, J.; Li, J.; Cheng, J.; Zhou, J.; Nawaz, S.A.; Xiao, X.; Bhatti, U.A. Multi-watermarking algorithm for medical image based on KAZE-DCT. J. Ambient. Intell. Humaniz. Comput. 2022, 1–9.

[14]. Patel, N.; Dwivedi, V.V.; Kothari, A. Hybrid Dct-Dwt Based Roi Medical Image Compression for Telemedicine Application. Image 2020, 8, 8.