Journal of Cardiovascular Disease Research

ISSN:0975-3583,0976-2833 VOL15,ISSUE04,2024

ENHANCING SECURITY AND INTEGRITY IN MEDICAL IMAGING FOR INTERNET OF MEDICAL THINGS

Swayam Prabha[1*], G. Sandeep[1], Md. Ikrmuddin[1], N. Sai Charan[1], Y. Karthik[1]

[1]Department of Computer Science and Engineering (AI & ML), Sree Dattha Institute of Engineering and Science, Sheriguda, Hyderabad, Telangana, India

Corresponding E-mail: swayampraba@sreedattha.ac.in

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: Discrete Wavelet Transform¸ Discrete Cosine Transform, Medical Image Watermarking.

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 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.

Hu, K et al. [15] developed the zero watermarking algorithm used in medical field. The developed zero watermarking algorithm generated bi-dimensional empirical mode decomposition (BEMD) to detect the tampering regions. The images were divided into a number of residues and intrinsic mode functions (IMF). The singular value decomposition was used to extract feature matrices from the first IMF. Arnold transform was used in encrypting the watermark image to add security. The exclusive or operation was used to create feature images. These feature images were used to detect tampering and authenticate copyright. This algorithm created natural images and performed better than other algorithms in fighting various cyber-attacks.

3. Proposed methodology

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

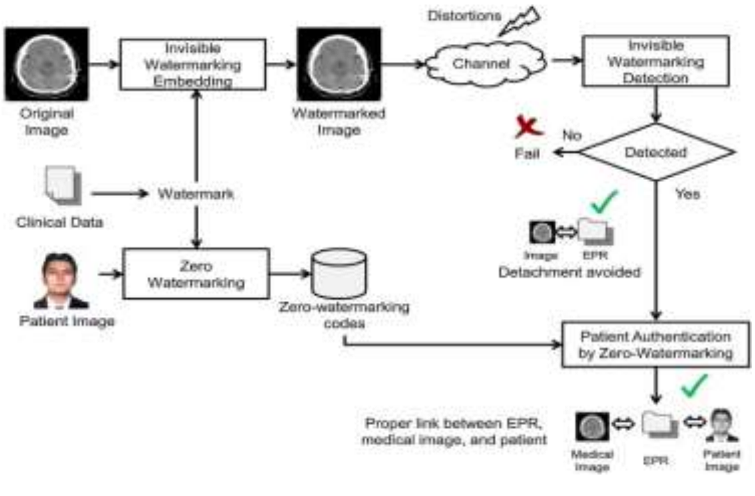


Figure 1: System architecture of proposed blind image watermarking system.

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 like the original host image but now contains the embedded watermark.

3.1 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 2. 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.

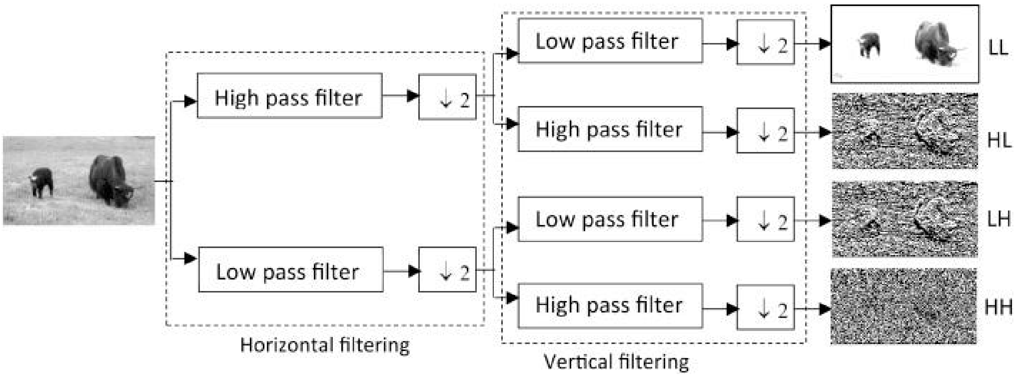


Figure 2. DWT decomposition.

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.

Reconstruction (Inverse DWT): The original signal or image can be reconstructed from the DWT coefficients as shown in Figure 3. This is done by applying the inverse DWT, which involves up-sampling (increasing the resolution) and applying the inverse of the filters used during decomposition.

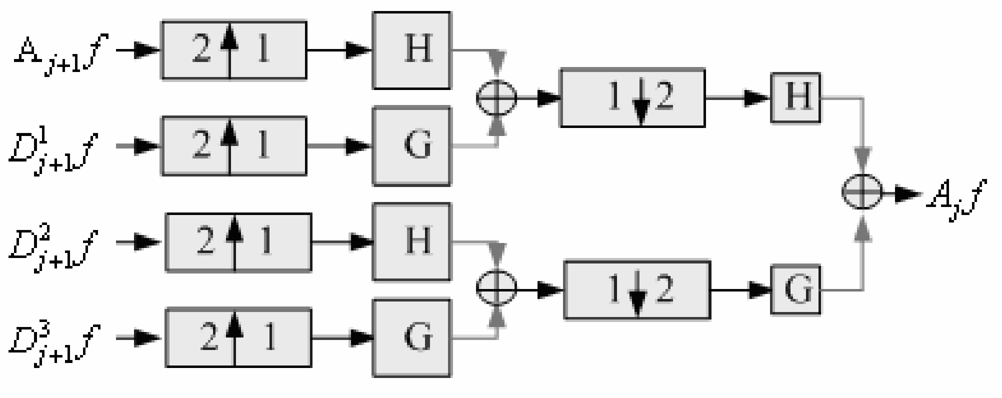


Figure 3. DWT reconstruction.

3.2 DCT

The Discrete Cosine Transform (DCT) is a mathematical technique used for signal processing and data compression. It's widely applied in various fields, including image and video compression, audio processing, and watermarking. The DCT essentially converts a signal from its spatial or time domain into the frequency domain, revealing the signal's frequency components. Here's a detailed explanation of the operation of the DCT:

Input Signal: The input to the DCT is typically a one-dimensional array or a two-dimensional matrix representing a signal or an image. For example, in image compression, each element of the matrix represents the intensity or color value of a pixel.

Block Division: In many applications, the input signal is divided into smaller blocks or segments. This is common in image and video compression, where blocks of pixels are transformed independently. The size of these blocks depends on the specific application but is often 8x8 or 16x16 pixels.

Normalization (Optional): Before applying the DCT, it's common to normalize the input signal by subtracting a constant value (e.g., 128) from each element. This helps center the signal around zero, which can improve the performance of the DCT.

DCT Coefficient Calculation: The DCT calculates a set of coefficients that represent the frequency components of the input signal. Each coefficient corresponds to a specific frequency component, with lower-order coefficients capturing lower-frequency variations and higher-order coefficients representing higher-frequency details.

$$D(u,v) = C(u)C(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left(\frac{(2x+1)u\pi}{2N}\right)\cos\left(\frac{(2y+1)v\pi}{2N}\right)$$

- The formula for calculating a single DCT coefficient for a given frequency component (u, v) in a block is as follows (for a 2D DCT):
- In this formula, D(u, v) is the DCT coefficient, C(u) and C(v) are scaling constants (typically set to 1/sqrt(2) for u or v equal to 0, and 1 for all other cases), N is the block size, and f(x, y) is the pixel value at position (x, y) in the input block.

Resulting DCT Coefficients: After applying the DCT formula to all possible (u, v) combinations within the block, you obtain a set of DCT coefficients. These coefficients represent the amplitude and phase of various frequency components within the signal or image.

Quantization: In lossy compression applications, such as JPEG image compression, quantization is applied to the DCT coefficients. Quantization reduces the precision of the coefficients, resulting in some information loss. Lower precision leads to higher compression but potentially lower image quality.

Inverse DCT: To reconstruct the original signal or image from the DCT coefficients, you apply the Inverse Discrete Cosine Transform (IDCT). The IDCT reverses the transformation, converting the coefficients back to the spatial or time domain.

Result: The output of the IDCT is the reconstructed signal or image, which should closely resemble the original input. In compression applications, the reconstructed signal may have some loss of detail due to quantization, but the goal is to minimize perceptible differences.

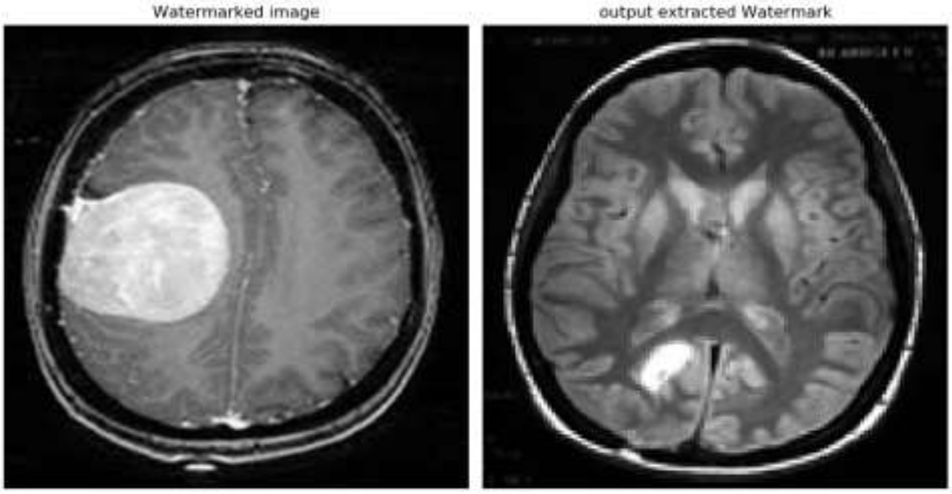
4. Results discussion

Figure 4 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 4. Watermarking embedding performance. (a) brain medical image. (b) original watermark. (c) output watermarked image

Figure 5 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.



(a) (b)

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

Table 1 provides a performance comparison between an existing watermarking method and a proposed watermarking method, using various metrics to evaluate their effectiveness. The purpose of this table is to showcase how the proposed method outperforms the existing method in terms of image quality and information preservation.

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.

Table 1. Performance comparison of watermarking system.

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

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. Looking to the future, there are several promising avenues for further research and development in this field. Firstly, enhancing the algorithm's computational efficiency to facilitate real-time watermarking for large-scale medical image datasets would be beneficial. Additionally, exploring ways to adapt the technique to emerging technologies like blockchain for enhanced data integrity and traceability could be explored. Moreover, the incorporation of machine learning and artificial intelligence for watermark detection and authentication could further bolster the system's robustness. Collaboration with medical professionals and institutions to establish standards and best practices for medical image watermarking is another important direction. Finally, continuous monitoring of advancements in image processing and encryption techniques will be essential to stay ahead of potential threats to medical image security. In summary, the future scope of blind medical image watermarking lies in optimizing efficiency, integrating with cutting-edge technologies, enhancing robustness through AI, establishing industry standards, and staying vigilant against evolving security challenges in healthcare data management.

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.

[15] Hu, K.; Wang, X.; Hu, J.; Wang, H.; Qin, H. A novel robust zero-watermarking algorithm for medical images. Vis. Comput. 2021, 37, 2841–2853.