iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 Issue: IV Month of publication: April 2026

DOI: https://doi.org/10.22214/ijraset.2026.79470

Digital Watermarking for Medical Images: Current Methods and Issues

Kruti B. Patel[1], Rahul N. Gonawala[2],
[1, 2]*Department of Electronics and Communication Engineering, Bhagwan Mahavir College of Engineering and Technology, Bhagwan Mahavir University, Surat, Gujarat, India*

Abstract: The use of digital medical imaging has increased significantly in healthcare. Hospitals produce large amount of medical images. These medical images include imaging modalities like computed tomography (CT), magnetic resonance imaging (MRI), ultrasound, and X-ray. Also. these medical images are stored in hospital databases, transmitted across healthcare net works, and shared through telemedicine platforms. Although, they provide accessibility and efficiency, they still raise the con cern of security and privacy. Because medical images frequently contain sensitive patient data, they are susceptible to malicious manipulation, unauthorized distribution, and privacy violations. Medical images are frequently protected during transmission and storage using traditional security techniques like encryption. Encryption can prevent unauthorized access because the data remains encrypted. However, once the image is decrypted for clinical analysis, images may be modified and used illegally. This limitation makes use of encryption alone insufficient for long term protection of medical images. Digital watermarking offers an additional layer of protection by embedding hidden infor mation directly into the image itself. The embedded watermark remains within the image even after decryption. Which provides authentication, ownership verification, and integrity checking. Over the last two decades, many watermarking techniques have been proposed for medical images. Although these techniques have shown promising results, several challenges remain. They are limited in robustness, lack of adaptability, and sensitivity to image processing operations. This paper reviews existing medical image watermarking techniques and discusses their strengths and limitations. The survey focuses on spatial-domain and transform domain approaches, more recent developments in watermarking methods. Also, it describes evaluation metrics, and open research challenges. The goal is to provide a clear overview of the current state of research and highlight possible future directions for secure medical image management.
Keywords: Medical image watermarking, digital water marking, data integrity, patient privacy, healthcare security.

I. INTRODUCTION

The use of digital technologies has significantly changed healthcare systems over the last few decades. These days, clinical diagnosis, treatment planning, and patient monitoring all heavily rely on medical images. Imaging modalities like CT, MRI, ultrasound, and X-ray are frequently used to view internal body structures and detect the disease. Moreover, the picture Archiving and Communication Systems (PACS) enables medical professionals to store, retrieve, and share medical images. It is typically used in hospitals to manage medical images. Additionally, it can achieve remote consultation and diagnosis across various locations. Hence, telemedicine plat- forms have further increased this capability.

With all these advantages, they also introduce new chal lenges related to data security and patient privacy. Medical images are extremely sensitive because they contain both clin ical information and patient identifiers. Even a small change in a medical image can lead to incorrect interpretation by doctors. Such modifications may occur intentionally through malicious tampering or unintentionally during transmission and storage. Hence, the reliability of the diagnostic process may be compromised. Additionally, digital images can be easily copied, redistributed, or reused without authorization, increasing the risk of privacy violations and misuse of patient data [1]. To overcome these limitations medical images are protected during transmission and storage using encryption. While the image content is encrypted, it guarantees that unauthorized users cannot access it. However, this protection is limited to the encrypted phase. The security that encryption offers is lost when the image is decrypted for clinical analysis. The medical image is still be susceptible to alteration, duplication, or unauthorized distribution. This raises questions on patient safety and clinical judgments. Digital watermarking has emerged a solution to overcome this limitation. In watermarking, hidden information is em bedded directly into the image in a way that is visually imperceptible but can still be detected or extracted when required. Because the watermark becomes part of the image data itself, the protection continues even after the image is decrypted. Watermarking can therefore support several impor tant functions, including integrity verification, authentication of the image source, and identification of ownership or origin [3].

In medical imaging applications, watermarking techniques often embed information such as patient identifiers, hospital codes, or authentication signatures. However, embedding addi tional data into medical images must be performed very care fully. Unlike general multimedia images, medical images con tain subtle visual details that are important for diagnosis. Any noticeable distortion introduced by watermarking may reduce diagnostic reliability. For this reason, watermarking methods designed for general multimedia content cannot always be directly applied to medical images without modification.

Most existing watermarking techniques are divided two cat egories: spatial-domain methods and transform-domain meth ods [14]. Spatial-domain approaches embed watermark by directly modifying pixel values. These techniques are simple and computationally efficient. But they are sensitive to image processing operations such as compression, filtering, or noise addition. Hence, they are not suitable for many medical imaging applications [4]. Transform-domain techniques tries to improve the robustness by embedding watermark data in frequency coefficients obtained using transforms such as the discrete cosine transform (DCT), discrete wavelet transform (DWT), or discrete Fourier transform (DFT). However, they increase computational complexity and affected by geometric distortions such as rotation or scaling [6].

Another limitation of many traditional watermarking meth ods is their limited adaptability. These methods rely on fixed embedding rules or manually designed features. Hence, they do not generalize well across different medical image modal ities or attack scenarios. In reality, medical images are depen dent on the imaging equipment, scanning protocols, and clin ical conditions. Therefore, designing a watermarking method that performs consistently across different scenarios remains a difficult problem. Additionally, watermarking method must balance several requirements. These requirements include ro bustness, imperceptibility, payload capacity, and security [12].

In recent years, researchers have explored learning-based watermarking methods. They utilize machine learning or deep learning. These methods automatically learn embedding and extraction strategies from medical images. Moreover, these methods have shown promising improvements in adaptability and robustness. However, they also introduce some challenges, such as high computational requirements, complex training procedures, and limited interpretability of the learned models [15]. To address these challenges is essential before such methods are adopted in real life scenarios.

II. FUNDAMENTALS OF MEDICAL IMAGE WATERMARKING

Medical image watermarking involves embedding additional information into medical images in such a way that diagnostic content are not affected. Medical image watermarking operates under much stricter constraints compared to general multime dia watermarking. Even small distortions introduced during the embedding process may affect medical images intensity. Also, these medical images such as MRI, CT, ultrasound, and X-ray scans often contain fine intensity variations that help clinicians identify abnormalities. Therefore, watermarking techniques designed for entertainment or commercial images cannot be directly applied to medical images without careful adaptation and validation [13]. In healthcare systems, watermarking is used to embed patient details, hospital identifiers, authentication codes, or integrity verification data directly into the image. This embed ded information provides secure medical image transmission, tamper detection, and ownership verification. Also, they ensure compliance with medical data protection regulations. As a result, medical image watermarking techniques must balance security requirements with strict clinical reliability.

A. Objectives of Medical Image Watermarking

The primary objectives of medical image watermarking are data integrity verification and patient privacy protection. One of the most critical objectives is data integrity verification, which ensures that medical images have not been altered during storage or transmission. Any unauthorized modification of a medical image can lead to misdiagnosis or incorrect treatment decisions.

Another key objective is patient privacy protection. Sensitive patient information embedded as a watermark can be securely embedded in the medical image. This reduces the risk of unauthorized access to medical image. Authentication is also essential to verify the source of medical images. In some applications, ownership verification and traceability are required to identify the responsible medical facility or imaging device. Region of Interest (ROI)-based watermarking plays a vital role in achieving these objectives. ROI-based approaches preserve clinical reliability. Also, it embeds watermark in less critical regions [7], [17].

B. Types of Watermarks

Based on perceptibility, medical image watermarks are broadly classified into visible and invisible watermarks. Visible watermarks are useful for ownership declaration. But they are not suitable for medical imaging because they interfere with diagnostic interpretation. As a result, invisible watermarks are predominantly used in healthcare applications.

From a robustness perspective, watermarks are commonly categorized as robust, fragile, and semi-fragile. Robust watermarks are designed in way that they can stand against common image processing operations such as compression, filtering, and noise addition. This ability makes them suitable for ownership verification and copyright protection. Fragile watermarks are highly sensitive to modifications and they are used for tamper detection and image authentication. Semi fragile watermarks offer a compromise by tolerating benign operations while detecting malicious alterations. This is particularly useful in medical environments where routine processing should not trigger false alarms [8].

C. Watermark Detection and Extraction Techniques

Watermark detection techniques are classified as blind, semi-blind, or non-blind depending on the information re quired during extraction. Blind watermarking techniques do not require access to the original image during watermark extraction. Moreover, they are scalable and they reduce stor age requirements. Hence, they are preferred in large-scale healthcare systems. These methods are particularly suitable for telemedicine and distributed clinical environments.

Non-blind watermarking techniques require the original image for watermark extraction, which typically improves detection accuracy and robustness. However, the need to store and manage original images limits their practicality in real-world medical systems. Semi-blind techniques represent a compromise by requiring partial information, such as a watermark key or feature set, during detection. The choice of detection technique directly impacts system complexity, storage overhead, and security performance [13].

D. ROI and RONI-Based Watermarking

A fundamental concept in medical image watermarking is the distinction between the Region of Interest (ROI) and the Region of Non-Interest (RONI). The ROI contains di agnostically significant information, such as tumors, lesions, or anatomical structures, and must be preserved without distortion. Any modification within the ROI may compromise diagnostic accuracy and is therefore unacceptable in most clinical applications. In contrast, the RONI consists of background or non critical areas that do not contribute directly to diagnosis. Many watermarking schemes exploit the RONI for embedding water mark information to ensure imperceptibility and clinical safety. Accurate ROI identification is thus a crucial prerequisite for effective watermarking. However, ROI segmentation is often modality-dependent and may require manual intervention or automated segmentation algorithms, which introduces additional complexity [7], [10].

E. Evaluation Metrics

The performance of medical image watermarking techniques is evaluated using several quantitative metrics. Im perceptibility is typically measured using Peak Signal-to Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM), which assess the visual similarity between the original and watermarked images. High PSNR and SSIM values indi cate minimal distortion and better preservation of diagnostic quality [18]. Robustness is evaluated using metrics such as Normalized Correlation (NC) and Bit Error Rate (BER), which measure the accuracy of watermark extraction under various attacks. Payload capacity refers to the amount of information that can be embedded without degrading image quality. In medical applications, payload requirements are typically modest but must be sufficient to store patient or authentication data. Balancing imperceptibility, robustness, capacity, and security remains a fundamental challenge in medical image watermarking. Improving one metric often leads to degradation in another, making multi-objective optimization a central research problem in this domain.

III.TAXONOMY AND METHODOLOGY OF MEDICAL IMAGE WATERMARKING

All Medical image watermarking techniques can be systematically categorized based on embedding domain, reversibility, robustness requirements, and region-based constraints. Establishing a clear taxonomy is essential for understanding the methodological differences among existing approaches and for identifying suitable techniques for specific clinical applications.

A. Spatial-Domain Watermarking Methods

Spatial-domain watermarking techniques embed watermark information by directly modifying pixel intensity values of medical images. Common approaches include least significant bit (LSB) modification and pixel value differencing. These methods are computationally efficient and easy to imple ment; however, they are highly sensitive to common image processing operations such as noise addition, filtering, and compression. Due to their poor robustness and vulnerability to attacks, spatial-domain techniques are rarely suitable for medical imaging applications where diagnostic integrity must be preserved [4], [5].

B. Transform-Domain Watermarking Methods

Transform-domain techniques embed watermark informa tion into frequency coefficients obtained through transforms such as discrete cosine transform (DCT), discrete wavelet transform (DWT), and discrete Fourier transform (DFT). These methods exploit human visual system characteristics to achieve better imperceptibility and robustness compared to spatial-domain approaches. Among them, DWT-based wa termarking is widely adopted in medical imaging due to its multi-resolution representation. However, transform-domain methods involve higher computational complexity and remain vulnerable to geometric attacks such as rotation and scaling [4], [6].

C. Reversible Watermarking Techniques

Reversible or lossless watermarking techniques enable ex act recovery of the original medical image after watermark extraction. Also, they ensures zero distortion of diagnostic content. These properties are highly desirable in medical imaging. Common reversible techniques include difference expansion and prediction-error expansion. Despite their ad vantages, reversible watermarking methods typically suffer from limited payload capacity and reduced robustness under aggressive attacks. That restricts their applicability in hostile environments [9], [11].

D. ROI-Based Watermarking Techniques

Region of Interest (ROI)–based watermarking techniques preserve diagnostically significant regions by embedding wa termark information in the Region of Non-Interest (RONI). These methods significantly enhance imperceptibility and clin ical reliability. However, their effectiveness depends heavily on accurate ROI segmentation, which varies across imag ing modalities and clinical contexts. Hence, automatic and modality-independent ROI detection is a challenging problem [7], [8].

E. Learning-Based Watermarking Frameworks

Recent research has explored machine learning and deep learning–based watermarking frameworks that learn optimal embedding and extraction strategies directly from data. These methods demonstrate superior adaptability and robustness across diverse attack scenarios. However, they have certain challenges such as, their black-box nature, high computational cost, and lack of explainability [15], [19]

IV. COMPARATIVE ANALYSIS OF MEDICAL IMAGE WATERMARKING TECHNIQUES

Early watermarking research established fundamental prin ciples of robustness and imperceptibility [2]. Spatial-domain techniques were initially used for simplicity but they were later shown to be fragile under common attacks [4]. Transform domain approaches improved robustness but increased com plexity and vulnerability to geometric distortions [6].

ROI-based medical watermarking techniques preserve di agnostic regions and enhance imperceptibility [8]. Reversible watermarking enables perfect recovery of original images but suffers from limited payload and robustness [9], [11]. Recent surveys emphasize that traditional methods lack adaptability [14]. Deep learning–based methods show promise but raise concerns regarding interpretability and computational cost [15], [16].

This section provides a detailed comparative analysis of representative medical image watermarking techniques re ported in the literature. The comparison focuses on embedding domain, robustness, imperceptibility, reversibility, Region of Interest (ROI) preservation, and key limitations. This also shows the current research directions and helps show why tra ditional watermarking techniques often fail to satisfy stringent clinical requirements.

From the comparison presented in Table I, it is evident that no single watermarking technique fully meets all the demanding requirements of medical imaging applications. Spatial-domain methods are simple and efficient but they are fragile under noise, compression, and filtering. That makes them unsuitable for most clinical contexts. Transform-domain techniques such as DCT- and DWT-based watermarking im prove robustness compared to purely spatial methods. DWT are better with multi-resolution decomposition. However, these methods still struggle with geometric attacks such as rotation and scaling. And they often need careful parameter customiza tion to maintain diagnostic quality. ROI-based watermarking protects important diagnostic regions by embedding watermark information outside the ROI. This approach improves clinical safety but they are heavily depend on accurate ROI seg mentation. Moreover, they are labor-intensive or error-prone depending on the imaging modality.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

TABLE 1:
COMPARATIVE ANALYSIS OF MEDICAL IMAGE WATERMARKING TECHNIQUES

Method	Embedding Domin	ROI Support	Robustness	Reversible	Major Limitations
LSB-based watermarking [2]	Spatial	No	Low	No	Highly sensitive to noise, compression, and filtering; unsuitable for medical diagnosis
DCT-based watermarking [4]	Transform (DCT)	Partial	Medium	No	Vulnerable to geometric attacks; increased computational complexity
DWT-based watermarking [4]	Transform (DWT)	Partial	High	No	Trade-off between robustness and imperceptibility; parameter tuning required
ROI-based watermarking [8]	Spatial/ Transform	Yes	Medium	No	Accurate ROI segmentation required modality dependent
Reversible watermarking [9], [10]	Spatial/ Transform	Yes	Low-Medium	Yes	Limited payload capacity; fragile under attacks
Prediction based reversible watermarking [11]	Spatial	Yes	Medium	Yes	Increased complexity; limited robustness
Learning-based watermarking [15], [19]	Data-driven	Yes	High	Partial	High computational cost; lack of explainability
Hybrid DCT-SVD watermarking 2026 [20]	Transform (DCT SVD)	Partial	High	No	Complex embedding, requires careful parameter tuning
Light weight dual watermarking 2025[21]	Hybrid (DWT DCT + CNN decoder)	Yes	High	Partial	Adds training overhead; may need GPU for real-time use
Zero-watermarking GAN-based 2026 [22]	Zero /Deep learning	Yes	High	Yes	Relies on GAN training; may require large datasets
DTCWT+PSO Optimized watermarking 2026 [23]	Transform + Optimization	Partial	High	No	Optimization increases computation; security tied to PSO parameters

Reversible watermarking techniques are highly valued in medical imaging because they allow the original image to be fully recovered after watermark extraction. Also, it ensures zero distortion to diagnostic content. However, many reversible schemes have limited payload capacity and robustness under aggressive attacks. Recent hybrid and learning-based methods have shown stronger performance in balancing impercepti bility, robustness, and ROI support. For example, a DCT SVD hybrid watermarking approach combines discrete cosine and singular value decomposition transforms to improve ro bustness through block- and region-based embedding [20]. A lightweight dual watermarking framework uses DWT–DCT and a small convolutional neural network for efficient ex traction. Also, it maintains high extraction fidelity and good resistance to noise and geometric distortions [21]. Another recent study [22] explores zero-watermarking using a residual based GAN. It achieves high robustness without modifying the original image, which is desirable. Additionally, a DTCWT + PSO optimization scheme has been proposed to adaptively tune watermark embedding parameters. It achieves the strong performance across multiple attack types.[23].

Overall, hybrid and learning-driven techniques are becom ing more common in recent years. Because they offer more adaptability across imaging modalities and better resistance to attacks. But they often come with increased computa tional cost and implementation complexity. Recently proposed learning-based watermarking techniques demonstrate superior adaptability and robustness by learning embedding strategies directly from data. These techniques show promise in handling diverse attack scenarios and imaging modalities. However, their practical deployment in clinical environments remains challenging due to high computational requirements and the lack of interpretability.

V. DISCUSSION

The comparative analysis shows that major problem wa termarking medical images face is to maintain a balance between clinical dependability and security requirements. The methods which focuses on robustness sacrifice the impercep tibility. Furthermore, methods that maintain diagnostic quality are vulnerable to attacks. Because diagnostic information is crucial, this trade-off is more important in medical imaging. Many traditional watermarking methods use fixed embedding rules. ROI-based and reversible watermarking techniques are limited by payload limitations. Also, they are dependent on the medical image modality. The learning-based watermarking methods provide data-driven and adaptive watermark embed ding. However, they lack in explainability, trust, and regulatory compliance. Additionally, future watermarking systems must not only be robust and imperceptible but they have to be interpretable and clinically validated.

VI. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

Several challenges are still there in the development of watermarking for medical images. Hence, it is essential to address these challenges to ensure secure and trustworthy management of medical images. One of the major challenges is to maintain balance between robustness and imperceptibility. By increasing the strength of watermark embedding may improve robustness against attacks. But it can also introduce visible distortions in the image. In medical imaging applications, the small amount of distortions can affect clinical interpretation. Therefore, watermark should be carefully embedded to pre serve medical image quality.

Another challenge involves resistance to geometric attacks such as rotation, scaling, cropping, and translation. Many existing watermarking techniques perform well against simple signal processing attack but fail when images are transformed using geometric operations. Also, medical images may be resized or reformatted during storage and transmission. So, the resistance against attacks remains an important research problem. Computational complexity is another issue. Advanced watermarking algorithms that combine multiple transforms or optimization techniques often require significant processing time. In large healthcare systems where thousands of medical images are generated daily, high computational cost may may limit the practical deployment of such techniques. Recently, machine learning and deep learning methods have been explored to design watermarking methods. These methods allow models to automatically learn embedding patterns. Also, they improve robustness against various attacks. However, they have challenges such as the need for large training datasets, high computational requirements, and limited interpretability of model decisions [15].

Future research should focus on developing adaptive and lightweight watermarking methods that can operate efficiently in real clinical environments. We can combine traditional signal processing techniques with modern learning-based techniques. That may offer promising solutions. Additionally, integrating watermarking with other security mechanisms such as encryption and blockchain technology could further strengthen the protection of medical image data.

VII. CONCLUSION

This survey reviewedmedical imagewatermarking tech niques. It highlights the limitations of traditional spatial and transform-domainmethods. ROI-based, reversible, and learning-based approaches improve security and reliability.

However,nosinglemethodsatisfiesallclinical requirements. Future researchmust focusonrobust, adaptive, andexplain able watermarking frameworks to support secure medical imagesharing

REFERENCES

[1] A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Attacks on copyright marking systems,” in Proc. Int. Workshop on Information Hiding, 1998, pp. 218–238.

[2] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[3] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography. San Francisco, CA, USA: Morgan Kaufmann, 2007.

[4] C. I. Podilchuk and W. Zeng, “Digital image watermarking techniques and applications,” IEEE Signal Process. Mag., vol. 18, no. 4, pp. 33–46, Jul. 2001.

[5] D. Kundur and D. Hatzinakos, “Digital watermarking for telltale tamper proofing and authentication,” Proc. IEEE, vol. 87, no. 7, pp. 1167–1180, Jul. 1999.

[6] M. Barni, F. Bartolini, and A. Piva, “Improved wavelet-based watermark- ing through pixel-wise masking,” IEEE Trans. Image Process., vol. 10, no. 5, pp. 783–791, May 2001.

[7] J. L. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, and R. Collorec, “Relevance of watermarking in medical imaging,” in Proc. IEEE EMBS, 2000, pp. 2504–2507.

[8] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, “Medical image watermarking for health information management,” IEEE Trans. Inf. Technol. Biomed., vol. 10, no. 4, pp. 722–732, Oct. 2006.

[9] J. M. Zain and A. R. M. Fauzi, “Reversible watermarking for medical images,” in Proc. IEEE EMBS, 2006, pp. 380–383.

[10] X. Guo and Y. Zhuang, “A reversible watermarking scheme using integer transform for medical images,” IEEE Trans. Inf. Technol. Biomed., vol. 13, no. 2, pp. 241–248, Mar. 2009.

[11] D. M. Thodi and J. J. Rodriguez, “Prediction-error based reversible watermarking,” in Proc. IEEE ICIP, 2010, pp. 1549–1552.

[12] P. Moulin and J. A. Koetter, “Data-hiding codes,” Proc. IEEE, vol. 93, no. 12, pp. 2083–2126, Dec. 2005.

[13] H. Nyeem, W. Boles, and C. Boyd, “Medical image watermarking: A survey,” EURASIP J. Image Video Process., vol. 2014, no. 1, pp. 1–21,2014

[14] S. Rawat and B. Raman, “A review on secure medical image water marking,” Multimedia Tools Appl., vol. 78, no. 21, pp. 30189–30233, 2019.

[15] Y. Liu, M. Zhang, and J. Wang, “A deep learning based watermarking method for medical images,” IEEE Trans. Inf. Forensics Security, vol. 14, no. 12, pp. 3202–3215, Dec. 2019

[16] X. Zhang, Z. Qian, and G. Feng, “Medical image watermarking using deep neural networks,” IEEE Access, vol. 8, pp. 103675–103687, 2020.

[17] A. Nia and M. A. T. Fard, “ROI-based reversible watermarking for medical images,” J. Digit. Imaging, vol. 28, no. 4, pp. 460–471, Aug. 2015.

[18] Z. Wang, A. Bovik, H. Sheikh, and E. Simoncelli, “Image quality assessment: From error visibility to structural similarity,” IEEE Trans. Image Process., vol. 13, no. 4, pp. 600–612, Apr. 2004.

[19] A. Ahmed and R. Mohanty, “Deep learning based robust watermarking for medical images,” Multimedia Tools Appl., vol. 80, no. 3, pp. 3951 3970, 2021.

[20] E. Aksu and M. Karakoyun, “DCT-SVD based hybrid approach for digital watermarking of medical images,” ICCK Transactions on Swarm and Evolutionary Learning, vol. 2, no. 1, pp. 1–18, Jan. 2026. :con tentReference[oaicite:0]index=0

[21] R. Taj et al., “Lightweight dual-watermarking framework for medical image authentication and integrity preservation,” Sci. Rep., vol. 16, Art. no. 1018, 2026. :contentReference[oaicite:1]index=1

[22] W. Zhang et al., “Robust zero-watermarking for medical image security using residual-based GAN,” J. King Saud Univ. Comput. Inf. Sci., 2026. :contentReference[oaicite:2]index=2

[23] R. Wang et al., “A medical image watermarking method based on the combination of DTCWT and PSO optimization,” 2026. :contentRefer ence[oaicite:3]index=3