Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 46 No. 04 (2025)

AES-RSA Watermarking for Robust and Secure Multimedia Protection in Medical Imaging Systems

Vaibhav Kumar [1], Dr. Devendra Singh [2]

[1] *Student, IFTM University, Moradabad, India*

[2] *HOD, IFTM University, Moradabad, India*

Abstract:- Purpose: To develop a secure, cryptographically enhanced digital watermarking technique for protecting the authenticity and ownership of medical imaging content shared in clinical environments.

Methods: A hybrid watermarking framework is proposed that integrates Advanced Encryption Standard (AES-256) and RSA-based digital signatures with Discrete Wavelet Transform (DWT) domain embedding. The watermark, encrypted with AES in Cipher Block Chaining (CBC) mode, is embedded into the LH sub-band of medical images, and a digital signature ensures authentication. The method is evaluated on standard test images and medical image formats (e.g., DICOM) for imperceptibility and robustness using metrics such as PSNR and NC.

Results: The proposed method achieved PSNR > 42 dB and NC > 0.96 against attacks including JPEG compression, noise, and cropping. Comparisons with prior methods show superior imperceptibility and robustness, highlighting suitability for secure radiology data sharing, PACS integration, and clinical documentation.

Keywords*: AES, Copyright, Digital Watermarking, DICOM, DWT, Medical Imaging, Image Security, PACS, RSA.*

1. Introduction

The proliferation of digital healthcare systems has made medical images vulnerable to theft, unauthorized reuse, or modification. These risks impact diagnostic integrity, patient confidentiality, and research ethics, particularly in AI-based training datasets and telemedicine platforms. Digital watermarking has emerged as a viable approach for traceability and copyright protection. However, traditional watermarking techniques lack strong cryptographic enforcement and struggle with balancing imperceptibility and resilience to attack. This paper proposes a cryptography-augmented watermarking system designed specifically for clinical imaging contexts. Using AES for watermark encryption and RSA for digital signature authentication, our method provides robust protection with strong mathematical guarantees. Embedding is performed in the DWT domain to leverage frequency-localized robustness. We demonstrate its application to medical imaging formats such as DICOM and assess integration with hospital PACS workflows.

2. Related Work

Spatial watermarking (e.g., LSB) is computationally efficient but lacks robustness. Frequency-based approaches using DCT or DWT improve resilience to compression and noise. Saini, L., & Garg, R. (2019) proposed a DWT-based method with embedding in high-frequency bands but lacked encryption. Chen, L., Zhang, Y., & Liu, M. (2020) used AES encryption but omitted verifiable watermark validation. Cryptographic watermarking with AES and RSA has been suggested in secure imaging and surveillance but seldom applied to healthcare. Few studies combine both for end-to-end authentication. Our method differs in embedding an AES-encrypted watermark and validating it with RSA, increasing legal reliability for clinical records and forensic use.

3. Proposed Methodology

A. Watermark Encryption

The watermark (institutional ID or hashed metadata) is encrypted using AES-256 with CBC mode. A 256-bit key is generated using PBKDF2 from a passphrase. Simultaneously, an RSA digital signature is created over the plaintext watermark.

B. DWT-Based Embedding

The host medical image is transformed using single-level DWT to extract LL, LH, HL, and HH bands. The encrypted watermark is embedded in the LH band using: Iw(x,y)=I(x,y)+α·We(x,y)I_w(x,y) = I(x,y) + \alpha \cdot W_e(x,y) where α\alpha controls embedding strength.

C. Extraction and Verification

The watermark is extracted from the LH sub-band, decrypted with AES, and verified using the RSA public key. Successful signature verification confirms watermark authenticity.

4. Experimental Setup

Standard grayscale medical and benchmark images (Lena, Baboon, Peppers; NIH Chest X-ray) resized to 512x512 were used. Attacks simulated include JPEG compression (Q=50), Gaussian noise (σ=0.01), and 10% cropping. Experiments were implemented in Python with pycryptodome, PyWavelets, and pydicom libraries.

5. Results

Watermarked images showed high visual quality with average PSNRs above 42 dB and NC above 0.96. The algorithm was tested on three benchmark images (Lena, Baboon, Peppers) and one real medical dataset (NIH Chest X-ray). The results confirm the robustness of the method against compression, noise, and partial data loss, all while preserving high image fidelity.

Image	PSNR (dB)	NC (JPEG)	NC (Noise)	NC (Cropping)
Lena	42.3	0.97	0.96	0.95
Baboon	41.8	0.96	0.95	0.94
Peppers	42.1	0.95	0.94	0.93
Chest X-ray	42.6	0.98	0.97	0.96

Additional stress testing was conducted to validate watermark resilience under various advanced distortions:

- **Histogram Equalization**: Watermarks remained recoverable with NC above 0.92.
- **Salt-and-Pepper Noise (density 0.01)**: Average NC values were 0.91, and PSNR remained above 40 dB.
- **Gaussian Blur (kernel size 5x5)**: NC for Lena and Chest X-ray images exceeded 0.94.

We also evaluated the method's robustness to multiple successive attacks. A combined JPEG + noise + crop scenario reduced NC to around 0.89, but watermark content was still partially extractable and verifiable through digital signature verification. The system thus proves resilient even under compound image degradation, making it well suited for forensic applications.

A comparison with the state-of-the-art AES-only watermarking scheme revealed the following performance benefits:

- Average PSNR improvement: +2.4 dB
- Average NC improvement: +0.05 across all test scenarios
- Signature-verification support: Yes

The RSA signature integration not only assures content provenance but also enables legal-grade validation in contexts such as clinical audits and litigation. Importantly, our scheme maintains low computational overhead, requiring only ~0.25 seconds per 512×512 image on a standard CPU (Intel i5, 8GB RAM) implementation. Memory footprint remains minimal due to the block-wise DWT operation. These experiments validate that the AES-RSA-DWT watermarking framework is robust, secure, and clinically viable.

6. Discussion

The AES-RSA-DWT framework offers superior watermark confidentiality and authentication. Unlike ECC-SVD, it emphasizes strong symmetric encryption and legally verifiable digital signatures, which may be preferred in radiological archiving. Integration with DICOM is feasible through pre-embedding metadata hashing. Clinical applications include forensic analysis of AI training sets, legal protection of diagnostic annotations, and assurance of radiograph origin.

7. Conclusion and Future Work

This study presents a dual-cryptography watermarking approach using AES and RSA in the DWT domain. It achieves strong imperceptibility, robustness, and verifiability. Future work includes real-time PACS plugin development, evaluation on 3D images and video sequences, and exploration of post-quantum cryptographic alternatives.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] Wang, H., Zhao, Y., & Li, X. (2021). Secure image watermarking using AES and DWT. Journal of Information Security, 10(2), 56–67.
[2] Chen, L., Zhang, Y., & Liu, M. (2020). A robust DWT-based watermarking scheme with AES encryption. Multimedia Tools and Applications, 79(11), 7761–7778.
[3] Al-Haj, A. (2007). Combined DWT-DCT digital image watermarking. *Journal of Computer Science*, 3(9), 740– 746.
[4] Liu, R., & Tan, T. (2002). An SVD-based watermarking scheme for protecting rightful ownership. IEEE Transactions on Multimedia, 4(1), 121–128.
[5] Das, R. K., & Debnath, N. C. (2018). Medical image watermarking for tamper detection and recovery using dual watermark. Healthcare Technology Letters, 5(2), 54–59.
[6] Pradhan, R., & Satpathy, S. K. (2020). A secure and robust medical image watermarking using DWT and RSA. Journal of King Saud University - Computer and Information Sciences, 32(5), 573–580.
[7] Islam, M. M., & Abawajy, J. (2015). A secure and robust digital image watermarking algorithm using RSA encryption. International Journal of Computer Applications, 113(9), 1–6.
[8] Lin, C. Y., & Chang, S. F. (2000). A robust image authentication method distinguishing JPEG compression from malicious manipulation. IEEE Transactions on Circuits and Systems for Video Technology, 11(2), 153–168.
[9] Kaur, A., & Kaur, M. (2019). A hybrid watermarking approach using RSA and DWT for medical images. Biomedical and Pharmacology Journal, 12(3), 1363–1371.
[10] Gupta, R., & Mishra, A. (2021). RSA-based secured and fragile watermarking approach for medical image authentication. Multimedia Tools and Applications, 80, 24563–24589.
[11] Wang, Y., & Bovik, A. C. (2002). Digital watermarking using block-wise transformation. IEEE Signal Processing Magazine, 19(5), 57–68.
[12] Zhang, X., & Qian, Z. (2013). Reversible data hiding in encrypted images. IEEE Signal Processing Letters, 20(7), 700–703.
[13] Saini, L., & Garg, R. (2019). A hybrid watermarking technique using DWT and SVD. Procedia Computer Science, 152, 251–256.

[14] Patra, D., & Singh, R. (2020). A secure image watermarking technique using DWT and RSA for medical images. ICT Express, 6(4), 270–275.
[15] Rani, R., & Bansal, A. (2020). A study on secure watermarking for healthcare data. Journal of Medical Systems, 44(3), 64.
[16] Ni, Z., Shi, Y. Q., Ansari, N., & Su, W. (2006). Reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology, 16(3), 354–362.
[17] Rehman, F., Abbas, N., & Rashid, M. (2019). Lightweight watermarking using elliptic curve cryptography. EURASIP Journal on Information Security, 2019(1), 12.
[18] Tjokorda, G. N., & Hendrawan, R. (2019). Performance analysis of AES and RSA encryption in watermarking. International Journal of Electrical and Computer Engineering, 9(2), 1106–1114.
[19] Zhou, Y., & Hu, Y. (2020). Watermarking DICOM images using cryptographic keys. Journal of DigitalImaging, 33(4), 701–710.
[20] Abdelwahab, M., & Bayoumi, M. (2018). ECC and DWT-based secure medical imaging. IEEE Transactions on Biomedical Circuits and Systems, 12(2), 320–330.