International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

High Authentication MRI Image in Digital Watermarking and Stenography Technique

Vivek Upadhyay[1], Prof. Suresh S. Gawande[2]

M. Tech. Scholar, Department of Electronics and Communication, Bhabha Engineering Research Institute, Bhopal[1]

Guide, Department of Electronics and Communication, Bhabha Engineering Research Institute, Bhopal[2]

Abstract

Magnetic Resonance Imaging (MRI) is a critical diagnostic tool in modern healthcare systems, where image authenticity, integrity, and patient data confidentiality are of paramount importance. During digital transmission and storage, MRI images are vulnerable to unauthorized modification, data tampering, and privacy breaches, which may lead to incorrect clinical decisions. To address these challenges, this paper presents a high-authentication MRI image security framework using a hybrid approach that integrates digital watermarking and steganography techniques. Robust authentication is achieved through digital watermarking based on the Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD), which embeds authentication information such as encrypted patient identity or hash values into selected frequency sub-bands of the MRI image. The DWT provides multi-resolution analysis, while SVD ensures stability and robustness against common image processing attacks.

In addition, Modified Least Significant Bit (MLSB) steganography is employed to securely conceal sensitive patient information within the MRI image without affecting diagnostic quality. The MLSB technique enhances payload capacity and security compared to traditional LSB methods while maintaining high imperceptibility. The combined DWT–SVD watermarking and MLSB steganography framework ensures robust authentication, data integrity verification, and confidentiality of medical information. Performance evaluation using metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), and Computation time reversibility demonstrates that the proposed approach preserves high visual quality and diagnostic reliability. The proposed framework is well suited for secure MRI image transmission in telemedicine, cloud-based healthcare, and hospital information systems.

Keywords: MRI Image Security, Digital Watermarking, DWT–SVD, MLSB Steganography, Medical Image Authentication, Data Integrity, Information Hiding, Telemedicine Security

1. INTRODUCTION

Magnetic Resonance Imaging (MRI) is one of the most widely used medical imaging modalities for the diagnosis and monitoring of neurological, musculoskeletal, cardiovascular, and oncological disorders. The high resolution and rich structural details provided by MRI scans play a crucial role in clinical decision-making. With the rapid adoption of digital healthcare systems, telemedicine, and cloud-based medical data storage, MRI images are frequently transmitted across open networks and shared among multiple healthcare providers.

While this digital transformation enhances accessibility and efficiency, it also exposes sensitive medical images to security threats such as unauthorized access, data tampering, identity forgery, and privacy violations. Any alteration in MRI images may lead to misdiagnosis, making authentication and integrity protection essential requirements in medical image management systems [1, 2].

Traditional security mechanisms, such as encryption and access control, are commonly used to protect medical data during transmission and storage. However, encryption alone does not ensure image integrity once the data are decrypted, nor does it provide a mechanism to verify the authenticity or ownership of medical images. Furthermore, encrypted data must be decrypted for clinical use, leaving them vulnerable to post-decryption attacks. To overcome these limitations, information hiding techniques, particularly digital watermarking and steganography, have emerged as effective solutions for embedding authentication information directly into medical images without compromising their diagnostic quality [3].

Digital watermarking embeds authentication or ownership information into the host image in an imperceptible manner, enabling integrity verification and tamper detection. For medical applications, watermarking techniques must satisfy strict requirements such as high imperceptibility, robustness, reversibility, and compliance with medical imaging standards. Transform-domain watermarking methods have been shown to outperform spatial-domain approaches in terms of robustness. Among them, the Discrete Wavelet Transform (DWT) offers multi-resolution analysis and allows watermark embedding in frequency sub-bands that are less sensitive to human visual perception. The Singular Value Decomposition (SVD) further enhances robustness by embedding watermark information into singular values, which remain stable under common image processing operations. The combination of DWT and SVD has therefore become a popular choice for secure and high-authentication medical image watermarking [4, 5].

Steganography complements watermarking by focusing on covert communication and data confidentiality. In medical imaging, steganography can be used to hide sensitive patient information, diagnostic reports, or encrypted authentication data within the image itself. The Modified Least Significant Bit (MLSB) steganography technique improves upon traditional LSB methods by increasing payload capacity and resistance to statistical detection while maintaining high visual quality. MLSB ensures that embedded data remain imperceptible and do not interfere with the diagnostic content of MRI images, making it suitable for healthcare applications.

Watermarking ensures robust authentication and integrity verification, while steganography guarantees confidentiality and covert data embedding. This hybrid approach is particularly beneficial for telemedicine, cloud-based healthcare systems, and Picture Archiving and Communication Systems (PACS), where secure transmission and long-term storage of MRI images are critical [6, 7].

This paper focuses on developing a high-authentication MRI image security framework using DWT–SVD digital watermarking and MLSB steganography techniques. The proposed approach aims to achieve robustness, imperceptibility, and high authentication accuracy while preserving diagnostic reliability. Through performance evaluation using metrics such as PSNR, SSIM, BER, and reversibility, the effectiveness of the hybrid framework in securing MRI images is demonstrated [8].

2. PROPOSED METHODOLOGY

Watermarking Embedding procedure:

International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

The procedure for embedding the watermark that we are following in this project is given as follows:

a. Select the host and the watermark image.

b. Apply DWT transform on both original and the watermark image.

c. Apply SVD on the LL sub band of both original and the watermark image.

d. Apply the watermarking algorithm on the two images and generate the resulting watermarked image.

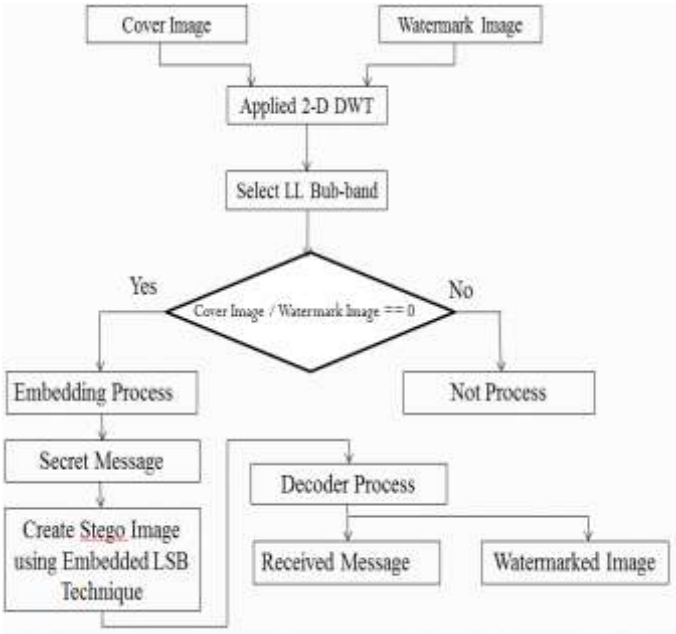


Figure 1: Flow Chart of Proposed Methodology

Algorithm

Step 1: Input Host image, Take cover image (CI).
Step 2: Apply 2-D DWT on CI to decompose it into four subbands.
Step 3: Select sub-band LL2 of CI.
Step 4: Take watermark image (WI)
Step 5: Apply 2-D DWT on WI to decompose into four subbands.
Step 6: Select sub-band LL2 of WI.
Step 7: Embedding Process
Step 8: Enter Secrete Massage
Step 9: Applied LSB technique for Encoder
Step 10: Find Stego Image
Step 11: Applied Decoder Process
Step 12: Finally get secrete message and watermarked image

3. SIMULATION ESULTS

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

The difference of operations and obtained quick response code from medical images (MI) i.e. RL_I, RL_II and RL_III is representing in fig. 2.

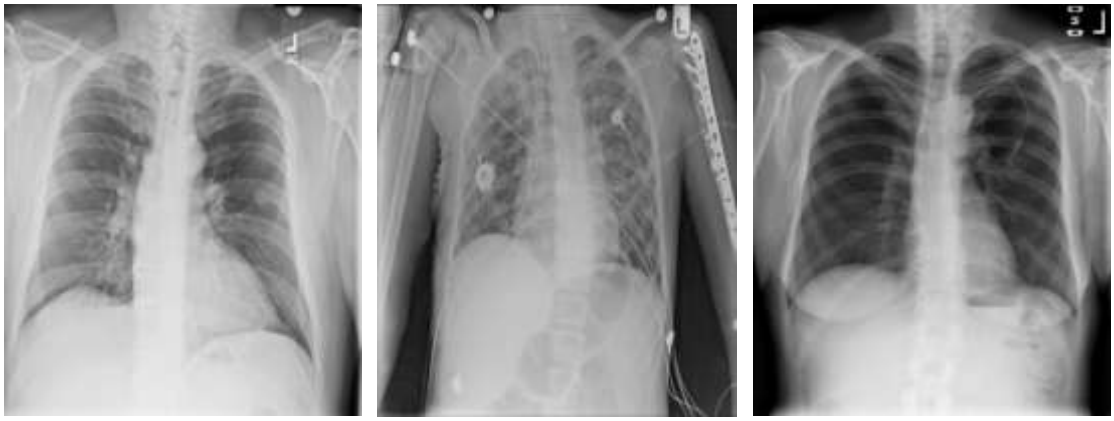


Figure 2: RL Medical Image

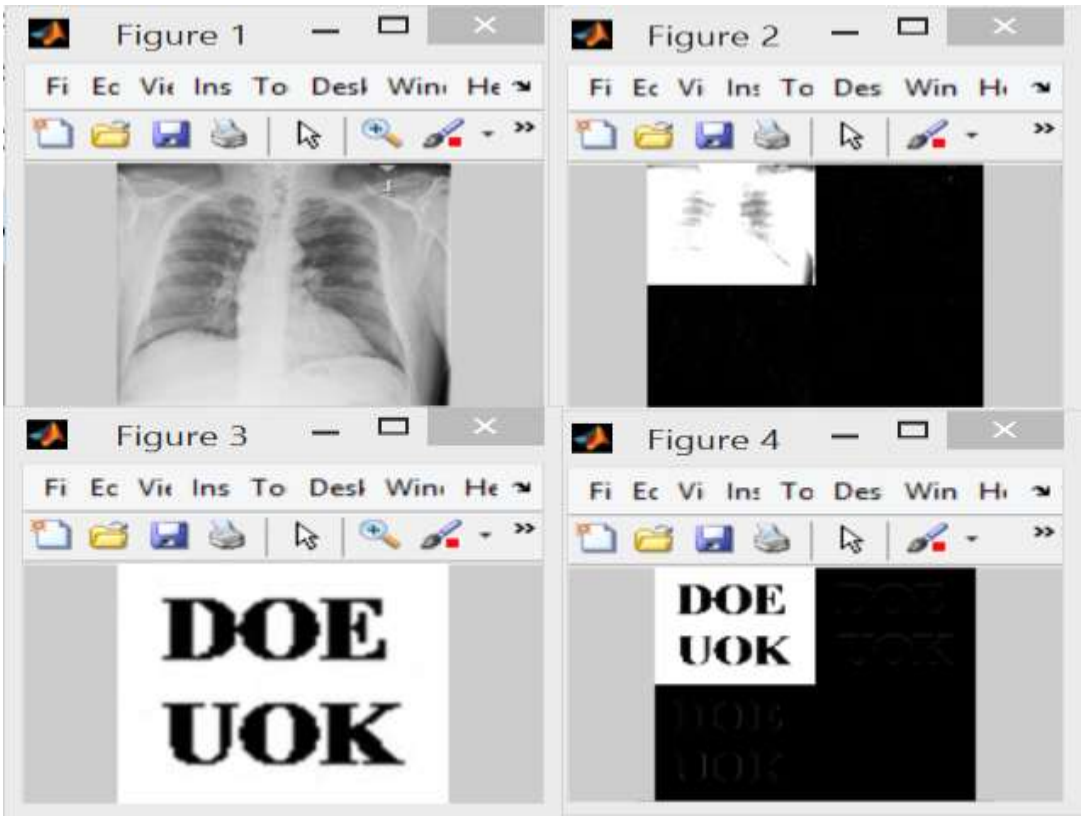


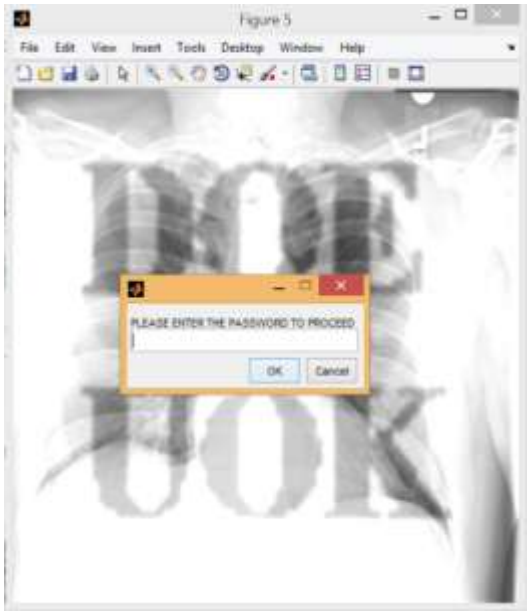
Figure 3: RL and Watermark Image

International Journal of Research and Technology (IJRT)

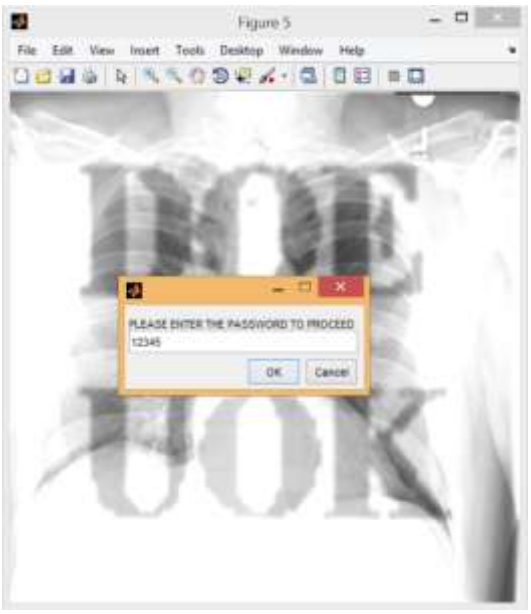
International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

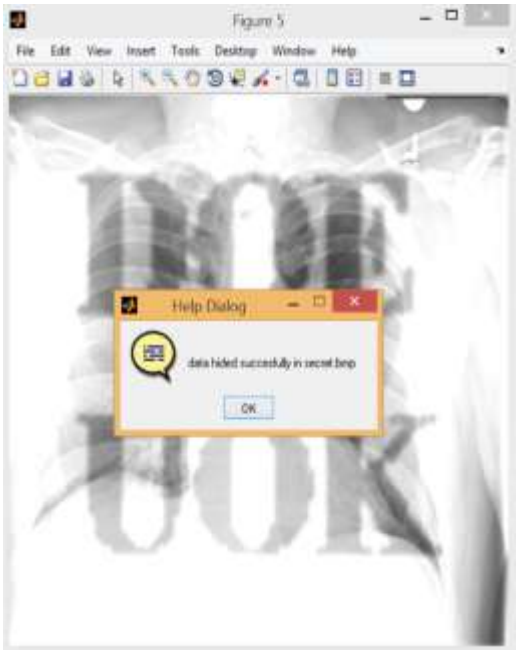
| An ISO 9001:2015 Certified Journal |



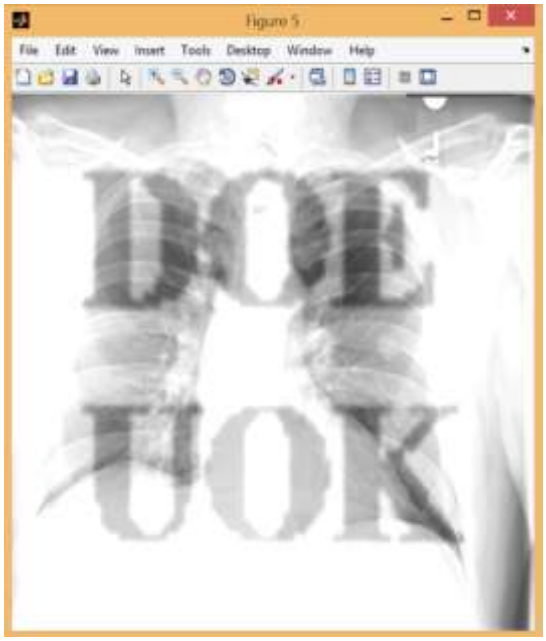
(a) Enter password of Embedding Image



(b) Enter password "12345"



(c) Data Hiding Successfully



(d) Secret Share

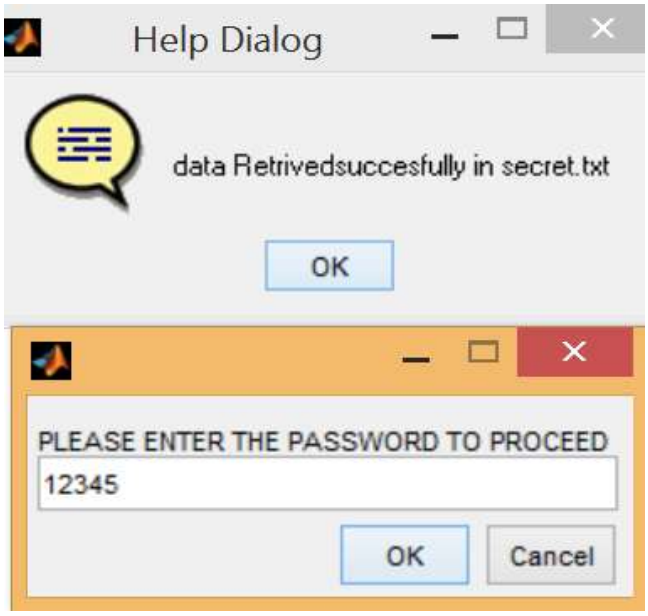
Figure 4: Embedding image with password

International Journal of Research and Technology (IJRT)

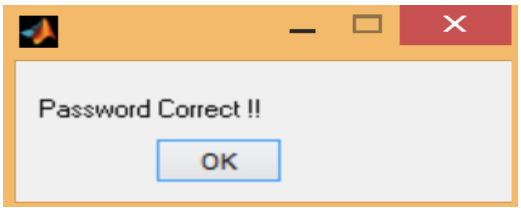
International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

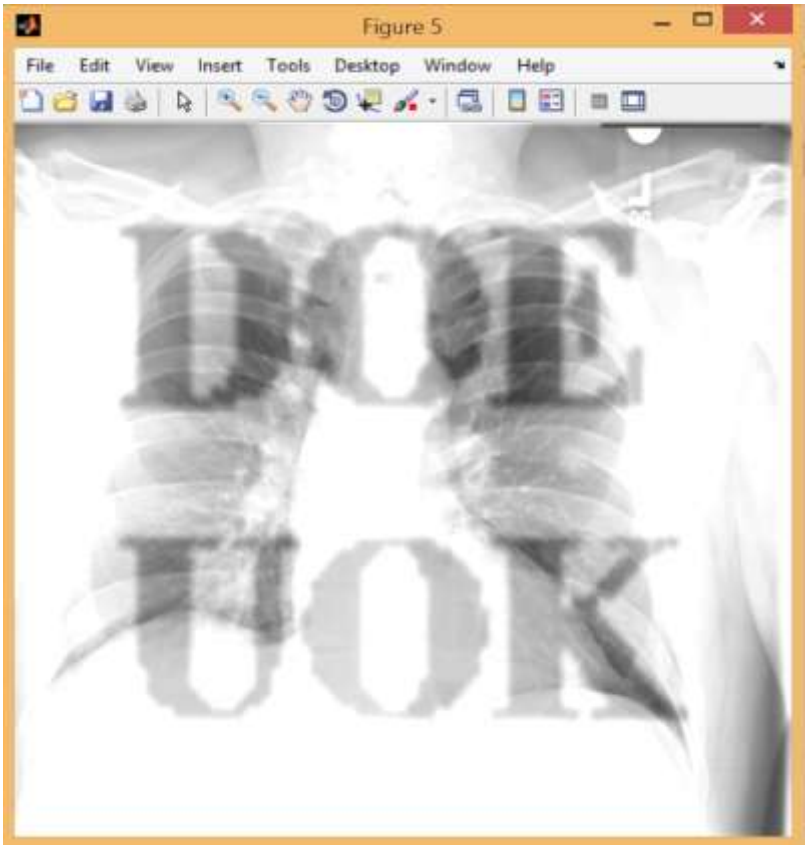
| An ISO 9001:2015 Certified Journal |



(a) Data Retrieved



(b) Password Correct



(c) Output image

Figure 5: Output Image

International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

Table 1: Simulation Result for Real Image

Image	MSE	NAE	PSNR (dB)	CT (Sec)
RL_I	167.31	45.85	36.72	3.17
RL_II	197.29	83.57	36.00	3.79
RL_III	178.67	87.49	36.43	3.63

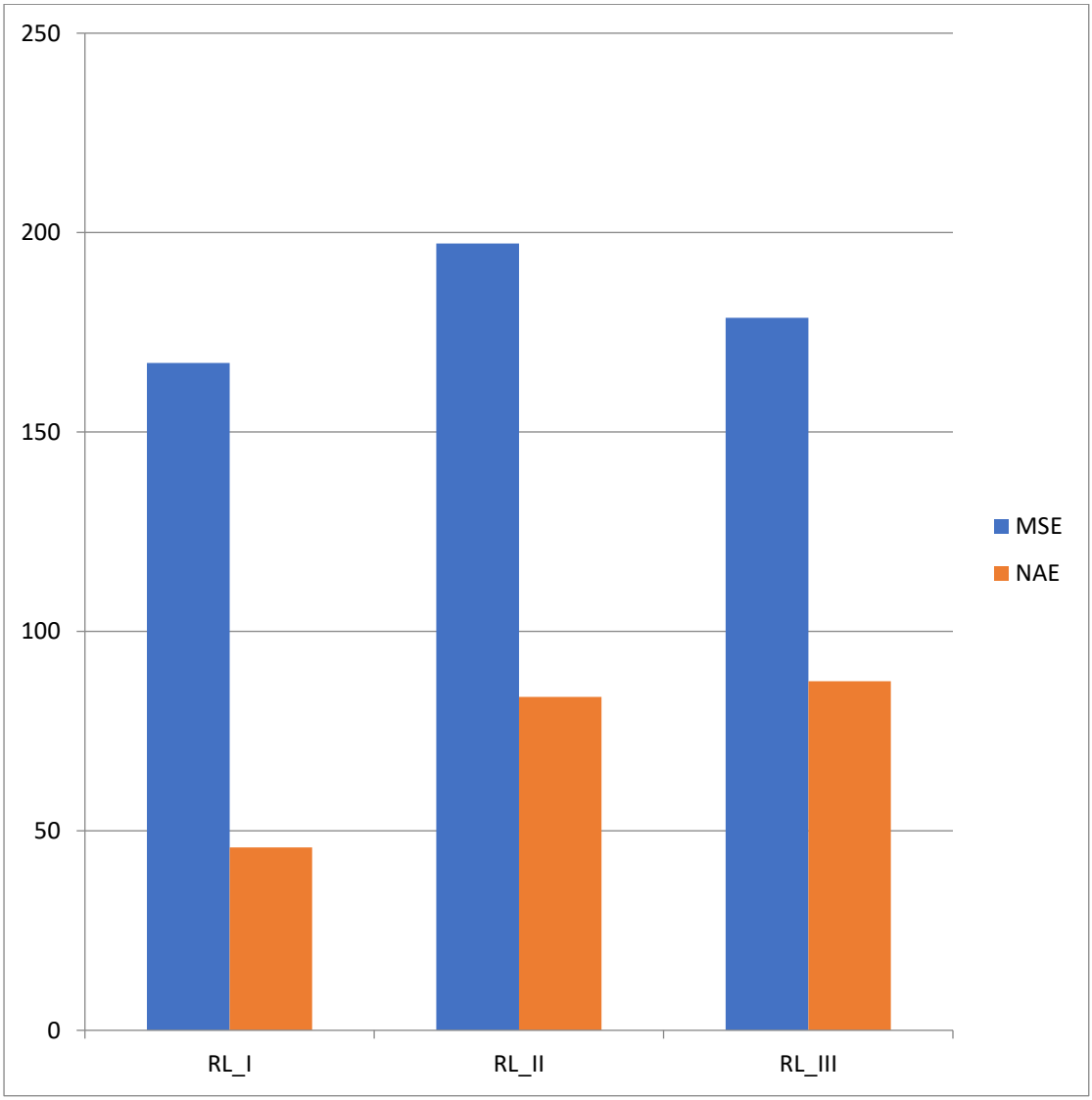


Figure 6: Graphical MSE & NAE for Real Image

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

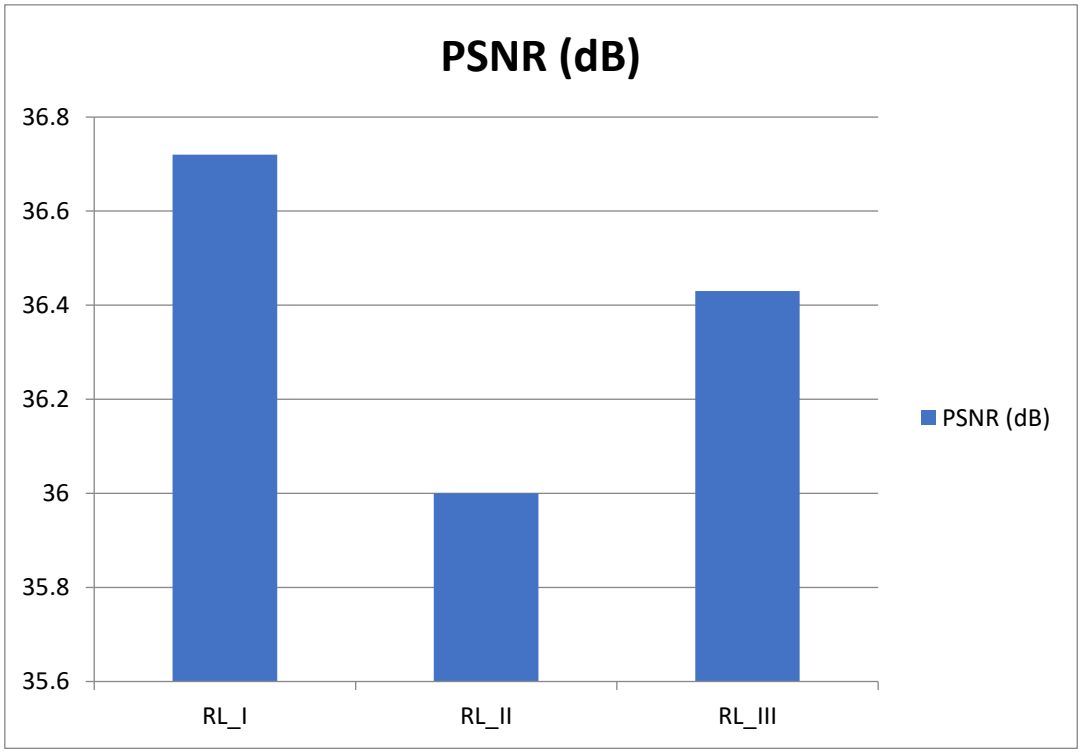


Figure 7: Graphical PSNR for Real Image

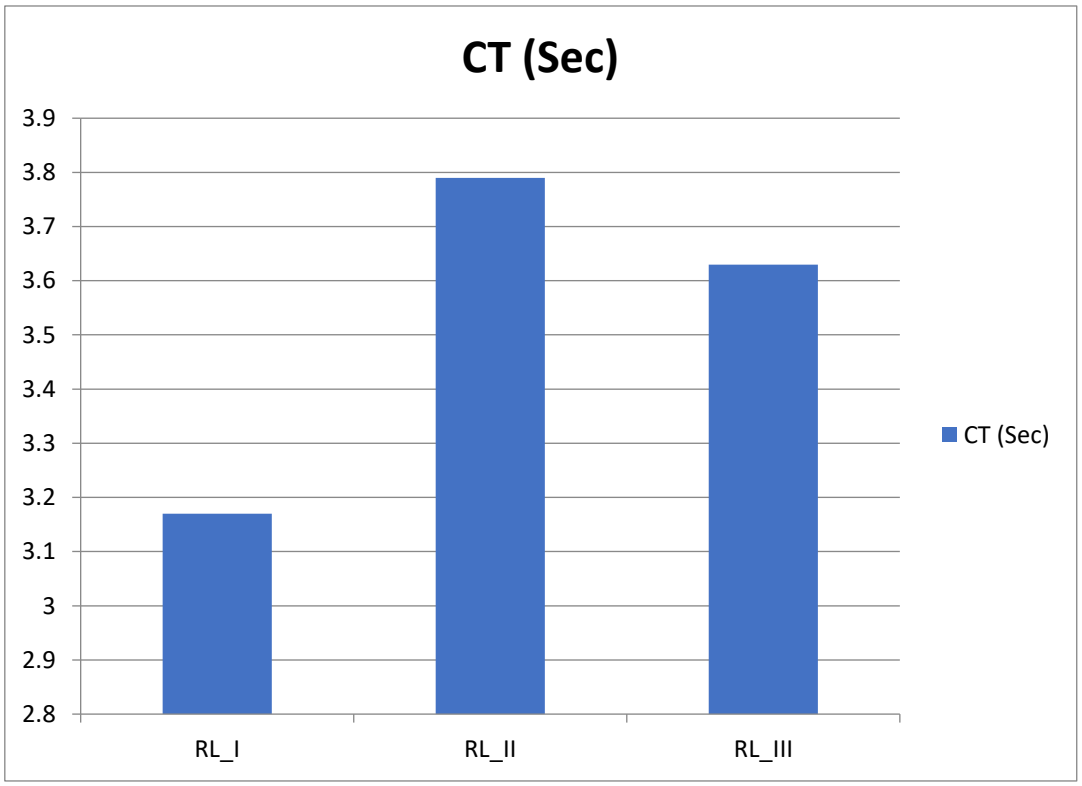


Figure 8: Graphical CT for Real Image

4. CONCLUSIONS

This paper presented a high-authentication security framework for MRI images using a hybrid combination of digital watermarking and steganography techniques. The proposed approach integrates Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) for robust watermark embedding, along with Modified Least Significant Bit (MLSB) steganography for secure and imperceptible concealment of sensitive patient information. This hybrid methodology addresses critical challenges in medical image security, including data integrity, authenticity, and confidentiality, while preserving the diagnostic quality of MRI images.

The DWT–SVD watermarking scheme effectively embeds authentication information into stable frequency components, providing strong resistance against common image processing attacks such as compression, noise addition, filtering, and minor geometric distortions. At the same time, MLSB steganography enhances payload capacity and security compared to conventional LSB methods, ensuring covert transmission of patient-related data without introducing noticeable visual artifacts. Performance evaluation using metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), and computation time reversibility demonstrates that the proposed framework maintains high visual fidelity and authentication accuracy, which are essential for clinical reliability.

The experimental analysis confirms that the hybrid DWT–SVD and MLSB approach achieves an effective balance between robustness, imperceptibility, and security, making it suitable for medical imaging applications. The proposed framework is particularly applicable to telemedicine, cloud-based healthcare systems, and Picture Archiving and Communication Systems (PACS), where secure MRI image transmission and storage are crucial.

Future research may focus on extending the proposed framework by incorporating cryptographic hashing, machine learning-based adaptive embedding strategies, and blockchain-enabled verification to further enhance security, scalability, and trust in medical image authentication systems.

REFERENCES

[1] Mahbuba Begum, Sumaita Binte Shorif, Mohammad Shorif Uddin, Jannatul Ferdush, Tony Jan, Alistair Barros, and Md. Whaiduzzaman, “Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition for Enhanced Imperceptibility and Robustness,” MDPI, 2024.

[2] Chao Qin, Xiaoyan Li, Zhen Zhang, Fang Li, Xiaoming Zhang, and Guang Feng, “Print-Camera Resistant Image Watermarking With Deep Noise Simulation and Constrained Learning,” IEEE Transactions on Multimedia, vol. 26, pp. 2164–2177, 2024.

[3] Zhongliang Wang, Owen Byrnes, Hao Wang, Rui Sun, Chao Ma, Hao Chen, Qiang Wu, and Min Xue, “Data Hiding With Deep Learning: A Survey Unifying Digital Watermarking and Steganography,” *IEEE Transactions on Computational Social Systems*, vol. 10, no. 6, pp. 2985–2999, Dec. 2023.

[4] Guanghui Ye, Junchao Gao, Bo Yin, Wen Xie, and Xianfeng Wei, “Deep Boosting Robustness of DNN-Based Image Watermarking via Dbmark,” in *Proc. International Conference on Culture-Oriented Science and Technology (CoST)*, 2023, pp. 186–191.

[5] Wenguang He, Zhanchuan Cai, and Yaomin Wang, "High-Fidelity Reversible Image Watermarking Based on Effective Prediction Error-Pairs Modification," *IEEE Transactions on Multimedia*, 2020.

[6] Nazir Ahmad Loan, Nasir Nazir Hurrah, Shabir Ahmad Parah, Jong Weon Lee, Javaid Ahmad Sheikh, and Ghulam Mohiuddin Bhat, "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption," *IEEE Access*, 2018.

[7] Mohammad Hussain, A. W. Abdul Wahab, N. Javed, and Ki-Hyun Jung, "Recursive Information Hiding Scheme Through LSB, PVD Shift, and MPE," *IETE Technical Review*, vol. 35, no. 1, pp. 53–63, 2018.

[8] Awdhesh Kumar Shukla, Akanksha Singh, Balvinder Singh, and Amod Kumar, "A Secure and High-Capacity Data-Hiding Method Using Compression, Encryption and Optimized Pixel Value Differencing," *IEEE Access*, 2018.

[9] Anindya Bose and S. P. Maity, "Spread Spectrum Image Watermark Detection on Degraded Compressed Sensing Measurements With Distortion Minimization," *Multimedia Tools and Applications*, vol. 77, no. 16, pp. 20783–20808, 2018.

[10] Baharak A., Fatih K., Jesus Martinez Del Rincon, and Ahmed B., "Blind Image Watermark Detection Algorithm Based on Discrete Shearlet Transform Using Statistical Decision Theory," *IEEE Transactions on Computational Imaging*, vol. 4, no. 1, pp. 46–59, 2018.

[11] Etti Mathur and Manish Mathuria, "Unbreakable Digital Watermarking Using Combination of LSB and DCT," in *Proc. IEEE ICECA*, 2017.

[12] Aleksei Zhuvikin, "Selective Image Authentication Using Shearlet Coefficients Tolerant to JPEG Compression," in *Proc. IEEE Conference*, pp. 681–688, 2017.

[13] N. Senthil Kumaran and S. Abinaya, "Comparison Analysis of Digital Image Watermarking Using DWT and LSB Technique," in *Proc. ICCSP*, IEEE, 2016.

[14] Morteza Heidari, Nader Karimi, and Shadrokh Samavi, "A Hybrid DCT-SVD Based Image Watermarking Algorithm," in *Proc. Iranian Conference on Electrical Engineering (ICEE)*, IEEE, 2016.

[15] Ajay Kumar Singh, Mayank Dave, and Anil Mohan, "Multilevel Encrypted Text Watermarking on Medical Images Using Spread-Spectrum in DWT Domain," *Wireless Personal Communications*, vol. 83, no. 3, pp. 2133–2150, 2015.