IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 11, November 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.625

© 2024 IJIRCCE | Volume 12, Issue 11, November 2024| DOI: 10.15680/IJIRCCE.2024.1211094

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Advancement of IoMT Security with the Utilization of Multipurpose Watermarking Techniques

Diksha Kori, Siddharth Bhalerao

PG Student, Department of I.T., GGITS, Jabalpur, MP, India

Assistant Professor, Department of CSE, GGITS, Jabalpur, MP, India

ABSTRACT: The continuous collection and transmission of physiological data from patient-worn sensors to remote servers has revolutionized the healthcare industry. This advancement enables medical professionals to analyse sensitive data continuously and provide real-time monitoring and interventions. However, the wireless communication of this data introduces significant security and privacy challenges, as it is susceptible to interception. Traditional security methods, such as cryptography, are often unsuitable for the resource-constrained medical devices that constitute the Internet of Medical Things (IoMT). To address these issues, this research proposes a novel security framework based on robust and fragile digital watermarking technology. The robust watermark is designed to protect the integrity of physiological data by embedding a watermark resistant to various signal processing procedures and attacks, ensuring that any unauthorized alterations can be detected. Conversely, the fragile watermark acts as a tamper detection mechanism, incorporating a watermark that is sensitive to even minor changes in the data, thus providing an additional layer of security. The proposed framework aims to enhance the overall security and privacy of the IoMT ecosystem, safeguarding sensitive patient information and supporting the continuous monitoring and analysis critical for improved healthcare outcomes.

KEYWORDS: IoMT, Image Attack, Temper Detection, Robust watermarking, Fragile watermarking, Embedding, Extraction, BER.

I. INTRODUCTION

Watermarking is the process of hiding some data in the cover data in order to protect the cover data. It can be applied to different types of data like images, videos, audios, physiological signals. When watermarking is applied to digital images it is called as digital image watermarking. The Internet of Medical Things (IoMT) is made up of resource-constrained medical devices, making traditional security techniques like cryptography inappropriate. Because of their often constrained processing speed, memory capacity, and battery life, these devices make it difficult to effectively implement standard safety measures. This study presents a novel security Approach that makes use of both robust and fragile digital watermarking technology in order to overcome these issues[4].By implementing a watermark that is strong to different signal processing techniques and attacks, the robust watermark is designed to preserve the authenticity of medical data. This guarantees that any illegal changes to the data may be found and identified, offering a reliable method to ensure the accuracy of the data [4,5]. The fragile watermark, on the other hand, acts as a tamper detection system. It has a watermark built in that can detect even the smallest changes in the data, making it possible to detect any attempts at data tampering [4,6]. This dual technique permits the detection of unauthorized modifications while simultaneously ensuring the integrity of the data. The entire security and privacy of the IoMT ecosystem are intended to be greatly improved by the proposed architecture. Protecting private patient data helps to ensure ongoing observation and evaluation, which is essential to enhancing patient outcomes. Better patient care and treatment are made possible by this security architecture, which guards against data breaches and tampering while simultaneously ensuring the accuracy and dependability of the data gathered and sent by medical equipment [1,2].Image attacks refer to a range of techniques designed to manipulate or distort images, aiming to deceive detection systems such as image recognition algorithms. Image attacks are malicious activities that exploit digital images to compromise systems, steal sensitive information, or disrupt operations. These attacks leverage vulnerabilities in image processing, transmission, and storage, posing significant threats in cybersecurity and artificial intelligence [2,3].

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. RELATED WORK

The research by Parah et al. [1] emphasizes the critical need for enhanced security and authentication mechanisms in the Internet of Medical Things (IoMT), particularly for safeguarding Electronic Health Records (EHR). Their proposed solution integrates advanced techniques such as Left Data Mapping (LDM) and RC4 encryption, significantly improving tamper detection and reducing computational costs. This innovative approach not only secures EHR data but also ensures efficient information embedding and extraction. In [3], a unique method for secure image watermarking that detects and localizes tampering successfully has been proposed. This method uses a key-based authentication scheme to fragment images into 4 × 4 segments with unique block keys for watermark embedding, hence improving tamper detection. The SHA-1 hashing algorithm and LSB substitution are used to generate and insert hash-key codes into each block, ensuring robust tamper detection and localization. The study emphasizes the importance of multimedia signal security and the need for effective tamper detection systems, demonstrating greater performance over current techniques. The suggested technique is resistant to common tampering attacks and produces high-quality results, as indicated by high PSNR and SSIM values, indicating that it's suitable for real-world applications. Future developments will strive to improve the algorithm's robustness and self-recovery characteristics, hence enhancing its overall performance and efficiency in practical circumstances. Gull et al. [2] introduced a novel reversible data hiding method that enhances data security in IoMT-based healthcare networks, focusing on the integrity of Electronic Health Records (EHR) during cloud transfers. This method employs Huffman encoding and dual images, achieving a 33.2% increase in embedding capacity and a PSNR improvement of 1.32, addressing the critical need for robust data protection in healthcare systems, While the proposed method shows significant advancements in data hiding techniques, challenges remain in balancing security with computational efficiency, particularly in real-time applications where speed is crucial. In [6], the multipurpose medical image watermarking scheme proposed by Rishi Sinhal et al. effectively enhances the security of medical images through a combination of advanced techniques. This approach not only ensures high imperceptibility and robustness but also facilitates tamper detection and localization, particularly in the regions of interest (ROI) and non-interest (RONI).

III. PROPOSED ALGORITHM

SHA256 Algorithm:

Watermarking techniques use the SHA256 hash function for ensuring the authenticity and integrity of digital images and videos. The watermark is embedded into particular parts of the images or video, such as the least significant bits (LSBs) of image blocks, by creating a 256-bit binary watermark using SHA256. By comparing the retrieved watermark with the original hash value, this procedure makes it possible to identify any tampered regions and identify any unauthorized modifications. This emphasizes the necessity of constantly enhancing and perfecting these methods in order to boost security and ward off potential threats [6].

Discrete Wavelet Transform (DWT):

A common technique for embedding and recovering watermarks from digital media is the Discrete Wavelet Transform (DWT). Enhancing the flexibility and imperceptibility of watermarking systems is a major aspect of DWT. Watermarks can be highly accurately embedded into images with DWT, providing protection from a range of manipulative attacks, such as noise addition, filtering, and rotation. It has been demonstrated that DWT, with its capacity to process images in both the spatial and frequency domains, DWT is a flexible and robust watermarking technology that may be used to secure digital files from copyright and unauthorized access [10,12]. DWT is an effective technique for digital watermarking because it can extract temporal and frequency information from an image. Because of its ability to perform multi-resolution analysis—that is, to break down an image into several frequency bands—the DWT is frequently used for watermarking. This allows the watermark to be placed in different areas of the image with varying degrees of resilience and imperceptibility [9,13,15].

Watermark Embedding Process:

The watermarking embedding process is a critical aspect of robust watermarking systems, designed to embed a watermark into an image while preserving its perceptual quality and ensuring resilience against potential attacks or modifications.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

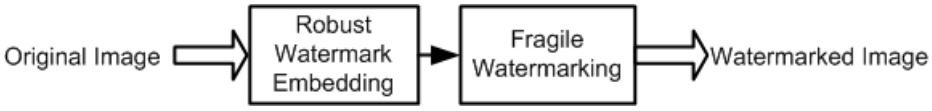


Fig.1. Block Diagram of Watermark Embedding Process

The dual watermarking process effectively enhances the security and integrity of digital images by embedding both robust and fragile watermarks. This approach ensures that the watermarked image remains visually indistinguishable from the original while providing mechanisms for copyright protection and tamper detection. The robust watermark, embedded in the frequency domain, withstands various attacks such as compression and noise, while the fragile watermark, embedded in the spatial domain, degrades upon any unauthorized modifications, thus serving as a reliable integrity verification tool. This combination not only protects the ownership of digital content but also facilitates the detection of alterations, making it suitable for secure transmission and storage in various applications, including medical imaging and copyright protection.

Watermark Extraction and Tamper Detection Process:

The critically important phase in a watermarking system is the watermark extraction process, which is responsible for removing the embedded watermark and assuring the integrity of the watermarked image. The watermarked image, which has both robust and fragile watermarks integrated during the watermarking process, is the first input in this method. First, the image's integrity will be assessed through fragile watermark extraction, tamper detection and temper localization. If the image is verified to be unmodified or only minimally modified, the robust watermark will then be extracted.

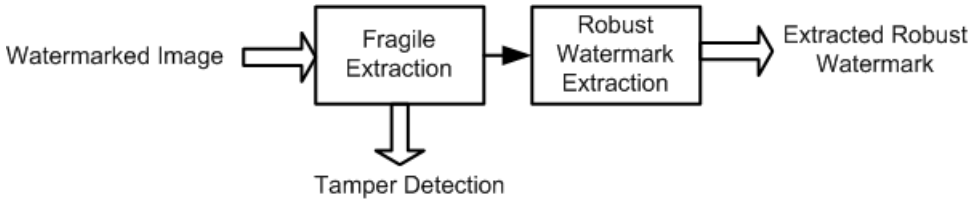
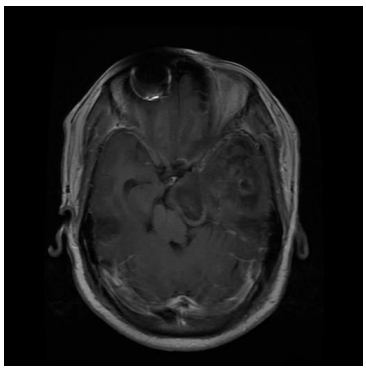
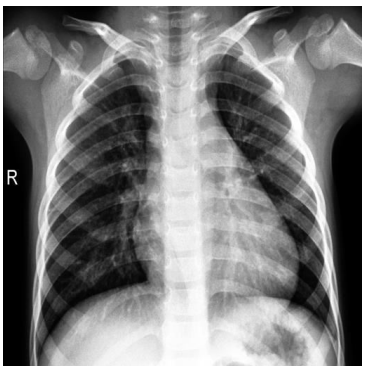


Fig 2. Block Diagram representing process to extract watermark image and temper detection

The extracted watermark image is the final result, and its integrity and authenticity is verified by comparing it to the original watermark. The embedded watermark is still possible to recover even if the image has undergone certain changes because it is made to resist common attacks like compression, noise, and geometric distortions. This two-step procedure, which combines effective watermark extraction with sensitive watermark-based tamper detection, ensures a complete solution for image integrity verification and image intellectual property protection.

Images used for performance evaluation of proposed work:





www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

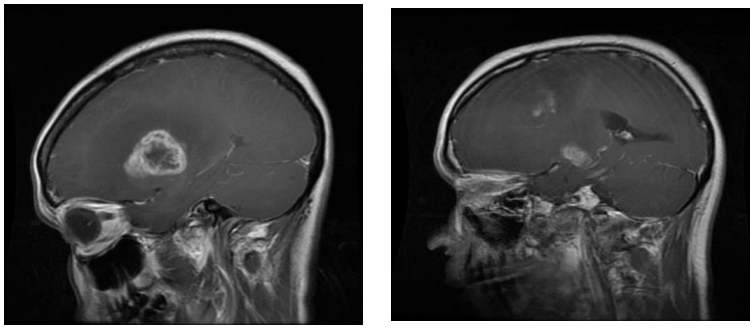


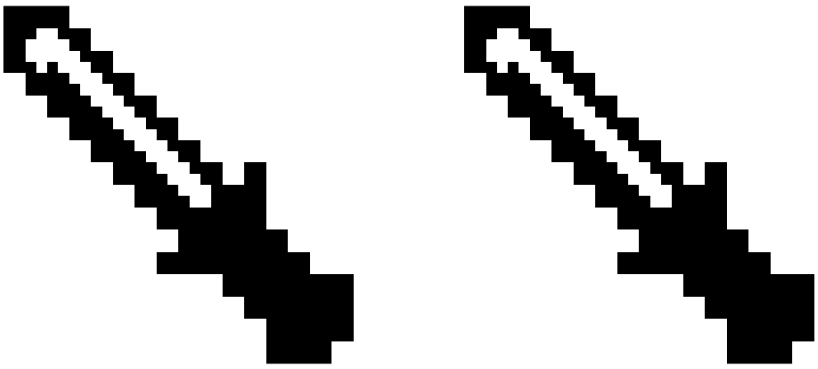
Fig.3. Images used for performance evaluation of proposed work

The performance of the proposed work is evaluated in terms of PSNR and SSIM. The overall performance of the work is found to be good in terms of both PSNR and SSIM. The results for images present in Fig.3. are present in table.

Table.1: Performance of Proposed Work in terms of PSNR and SSIM

Image	PSNR	SSIM
1	42.65	0.94
2	41.39	0.96
3	41.60	0.96
4	41.75	0.96

Fig.4. illustrates the process of robust watermarking in digital images, showcasing two key stages: (a) the embedded watermark that was embedded into the original image, serving as a reference for extraction and (b) the extracted watermark retrieved from the tampered image, with a Bit Error Rate (BER), indicating high fidelity in watermark recovery despite tampering.



(a) **(b)**

Fig.4. Logo watermark image for robust watermarking, (a) embedded watermark, (b) Extracted Watermark

Performance Matrices:

Structural Similarity (SSIM) index is a useful evaluation indicator to use for evaluating performance. To calculate how similar two photos are, utilize SSIM. Compared to PSNR and RMSE, which depend on the Euclidean distance, SSIM is an effective method that evaluates the image based on human perception. A better-looking image has a lower PSNR

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

than a high PSNR image, which may make the better image look unpleasant to us [1,7]. SSIM is used to remove this discrepancy. The formula used to calculate SSIM is as follows:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\mu_x^2 + \mu_y^2 + C_2)} \qquad eq.1$$

The estimated mean intensities, μx and μy, are computed as follows:

$$\mu_x = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad eq.2$$

Likewise, the mean of the y image can be calculated. The standard deviation is employed as a contrast estimate. As follows:

$$\sigma_x = (\frac{1}{N-1}\sum_{i=1}^{N} (x_i - \mu_x)^2)^{0.5} \qquad eq.3$$

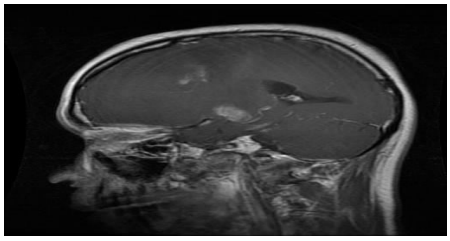
To prevent instability when the denominator is zero, C1 and C2 are used. A value between the range of 0 and 1 is the result. The higher the SSIM, the more similar the image is to the original; 0 indicates no similarity [11,14].

IV. SIMULATION RESULTS

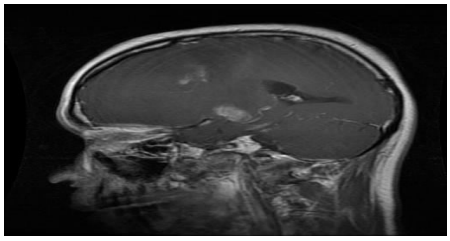
The results of the medical image watermarking process reveal the effectiveness of both fragile and robust watermarking techniques in ensuring image integrity and ownership. The study utilized a 512x512 pixel resolution images, applying fragile watermarking for tamper detection and robust watermarking for image copyright protection. The findings indicate that fragile watermarking excels in identifying tampering, while robust watermarking effectively preserves the authenticity of the medical image, affirming the combined approach's suitability for secure medical image handling. This dual technique not only enhances security but also addresses the critical need for integrity in medical imaging, as highlighted in the literature on watermarking applications in telemedicine.

Crop Attack:

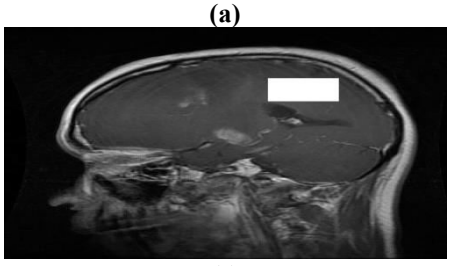
The results of the thesis demonstrate the effectiveness of a multipurpose watermarking algorithm in ensuring image integrity and copyright protection. The performance metrics indicate a low Bit Error Rate (BER) of 0.0098 for the extracted watermark, showcasing the robustness of the proposed method against various attacks.



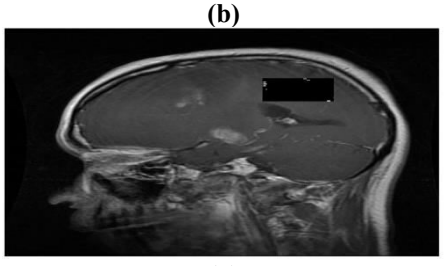
(a)



(b)



(c)



(d)

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

(e) **(f)**

Fig.5. Performance of proposed work (a) Original Image (b) Watermarked image using multipurpose algorithm (c) Crop Attack Image (d) Temper-detection Image (e) Original Watermark (f) Extracted Watermark with BER=0.0098

V. CONCLUSION

The proposed work presents a comprehensive multipurpose watermarking algorithm designed to enhance the security and integrity of medical images in the digital healthcare environment. By employing both robust and fragile watermarking techniques, the framework effectively addresses the challenges posed by the Internet of Medical Things (IoMT). The robust watermark ensures image authenticity against various attacks, while the fragile watermark detects even minor alterations, thereby reinforcing security. The dual watermarking strategy significantly contributes to safeguarding sensitive patient data during transmission While the proposed algorithm shows promise, it is essential to consider the evolving landscape of digital security threats, which may necessitate ongoing advancements in watermarking techniques to stay ahead of potential vulnerabilities.

REFERENCES

1. Parah, S. A., Kaw, J. A., Bellavista, P., Loan, N. A., Bhat, G. M., Muhammad, K., & de Albuquerque, V. H. C. (2020). Efficient security and authentication for edge-based internet of medical things. *IEEE Internet of Things Journal*, *8*(21), 15652-15662.
2. Gull, S., Parah, S. A., & Muhammad, K. (2020). Reversible data hiding exploiting Huffman encoding with dual images for IoMT based healthcare. *Computer Communications*, *163*, 134-149.
3. Bhalerao, S., Ansari, I. A., & Kumar, A. (2021). A secure image watermarking for tamper detection and localization. *Journal of Ambient Intelligence and Humanized Computing*, *12*(1), 1057-1068.
4. Shehab, A., Elhoseny, M., Muhammad, K., Sangaiah, A. K., Yang, P., Huang, H., &Hou, G. (2018). Secure and robust fragile watermarking scheme for medical images. *IEEE access*, *6*, 10269-10278.
5. Liu, Jing, et al. "Robust watermarking algorithm for medical volume data in internet of medical things." *IEEE Access* 8 (2020): 93939-93961.
6. Sinhal, R., Sharma, S., Ansari, I. A., & Bajaj, V. (2022). Multipurpose medical image watermarking for effective security solutions. *Multimedia Tools and Applications*, *81*(10), 14045-14063.
7. Bhalerao, S., Ansari, I. A., & Kumar, A. (2021, December). Analysis of DNN based image watermarking data generation for self-recovery. In *2021 international conference on control, Automation, Power and Signal Processing (CAPS)* (pp. 1-6).IEEE.
8. Bhalerao, S., Ansari, I. A., & Kumar, A. (2023). A reversible medical image watermarking for ROI tamper detection and recovery. *Circuits, Systems, and Signal Processing*, *42*(11), 6701-6725.
9.Sai, B. J. An Innovative Blind Medical Image Watermarking Technique for IoMT Applications.
10. Bhalerao, S., & Dutta, P. Image Denoising Using Riesz Wavelet Transform and SVR. *International Journal of Engineering Research & Technology (IJERT), ISSN*, 2278-0181.
11. Singh, P., Devi, K. J., Thakkar, H. K., &Kotecha, K. (2022). Region-based hybrid medical image watermarking scheme for robust and secured transmission in IoMT. *IEEE Access*, *10*, 8974-8993.
12. Rahman, S. M., Ahmad, M. O., &Swamy, M. N. S. (2009). A new statistical detector for DWT-based additive image watermarking using the Gauss–Hermite expansion. *IEEE transactions on image processing*, *18*(8), 1782-1796.
13. Preda, R. O. (2013). Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain. *Measurement*, *46*(1), 367-373.
14. Rupa, C., Sultana, S. A., Malleswari, R. P., Dedeepya, C., Gadekallu, T. R., Song, H. K., &Piran, M. J. (2024). IoMT Privacy Preservation: A Hash-Based DCIWT Approach for Detecting Tampering in Medical Data. *IEEE Access*.
15. Elbasi, E. (2020, December). B-DCT based watermarking algorithm for patient data protection in IoMT. In *2020 International Conference on Information Security and Cryptology (ISCTURKEY)* (pp. 1-4).IEEE.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details