e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

WATERMARKING SCHEME FOR MEDICAL IMAGES UTILIZING WAVELET TRANSFORM

Mrs. Uzma Khan[*1], Dr. Ankit Temurnikar[*2], Dr. Sunil Patidaar[*3]

[*1]Madhyanchal Professional University, India.

[*2,3]Assistant Professor, Madhyanchal Professional University, India.

DOI : https://www.doi.org/10.56726/IRJMETS45316

ABSTRACT

The exchange of medical images between hospitals has become a routine practice to enhance decision-making in healthcare. Digital watermarking has played a crucial role in the field of medical sciences, ensuring the reliability, availability, and confidentiality of images used for diagnosis and treatment. While various methods have been proposed for watermarking medical images using spatial and transform domains, existing mechanisms still suffer from a high rate of data falsification during image exchange. Therefore, we propose a wavelet-based digital watermarking scheme for medical images, employing three-level Discrete Wavelet Transform (DWT) and BCH coding. This scheme aims to assist medical practitioners in making accurate decisions. We have conducted a security analysis of our proposed approach to assess its robustness, and the performance results are discussed to confirm its feasibility for implementation in the medical sector.

Keywords: Data; Medical; Security; Watermarking.

I. INTRODUCTION

Digital watermarking involves the concealment of important information within digital data, allowing for the identification or verification of the embedded watermark. This technique offers various benefits such as theft protection, limited marketing, component tracking, and credibility. However, it also presents disadvantages such as interference with the image, increased processing overhead, and time consumption. In the field of medical sciences, watermarking plays a significant role in safeguarding the reliability, availability, and confidentiality of medical images used for diagnosis and treatment. There are four main categories of watermarking techniques used for medical images: robust, fragile, semi-fragile, and hybrid watermarking. Robust watermarking methods are difficult to remove from digital information and can be utilized for copyright protection. Fragile watermarks can be easily eliminated through tampering, while semi-fragile watermarks protect information from unauthorized alterations. Hybrid watermarking combines different techniques to achieve accuracy, authenticity, and ownership security simultaneously [1].

A. Security Requirements in Medical Images

In medical image watermarking, certain essential features are required, including confidentiality, reliability, and availability. Confidentiality ensures that only authorized individuals can access health data, which can be achieved through encryption, firewalls, and access management. Reliability encompasses two aspects: integrity, which ensures that information remains unaltered, and authentication, which guarantees that data is obtained from a verified source. Integrity is maintained through encryption during image communication over networks, while authentication requires measurements to verify the integrity and confidentiality of the data. Availability refers to the authorized users' ability to utilize the information system under normal conditions [2].

B. Current Watermarking Approaches for Medical Images

Medical images are typically divided into two regions: the region of interest (ROI) and the region of non-interest (RONI). The ROI contains the informative area used for diagnostic purposes, which should be preserved without distortion. Conversely, the RONI usually represents the background of an image, although it may occasionally include minor areas of interest. In ROI, spatial or transform-based techniques are applied to preserve information securely. While spatial domain methods are simple, fast, and offer high embedding capacity, they are susceptible to operations such as noise addition and poor compression. Additionally, spatial domain methods can be easily distorted by unauthorized users when attempting to reveal the embedded

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

watermark. In the medical field, previous algorithms either did not consider ROI and RONI segmentation or employed spatial domain techniques for digital watermarking [3].

II. LITERATURE SURVEY

Various mechanisms have been proposed to protect medical images from tampering and misuse during network transfers. Wu et al. [5] suggested a block-based approach using Discrete Cosine Transform (DCT) to watermark medical images with a focus on the ROI. However, this approach requires significant computational effort to recover ROI data and embed it in each part of the image. Mostafa et al. [6] proposed a methodology for storing Electronic Patient Records (EPR) within an image, reducing storage memory and communication costs while ensuring data protection. Watermark embedding was performed using Discrete Wavelet Packet Transform (DWPT) combined with Bose-Chaudhuri-Hocquenghem (BCH) error correcting codes to enhance robustness.

The security of many proposed algorithms suffers from the watermark being either unencrypted before embedding or weak encryption algorithms being used. Solanki et al. [7] proposed an embedding scheme utilizing the RSA technique, embedding the watermark in the ROI using Discrete Wavelet Transform (DWT). Fontani et al. [8] embedded information following DICOM regulations, positioning a digital signature in the header. This approach robustly links metadata to the medical image, ensuring it is not easily distorted. Eswaraiah et al. [9] developed a mechanism to detect image defects by separating images into ROI, RONI, and border pixels and comparing their statistical properties. Baiying et al. [10] proposed a reversible watermarking technique using wavelet transforms and singular value decomposition (SVD), employing recursive dither modulation (RDM) for embedding signature and logo. Shabir et al. [11] introduced a pixel-to-block conversion technique (PTB) to improve capacity and localization, but the stability of the embedded watermark remains a challenge. Parah et al. [12] presented two watermarking algorithms for medical images, embedding the watermark either in the entire image or the RONI part using DCT in an 8x8 block-wise manner. However, the risk of distortion is high when embedding in the whole image, and the lack of protection against image manipulation is a limitation when embedding in only the RONI part.

Other approaches incorporate encryption and cryptographic techniques to enhance security. Ali et al. [13] proposed a crypt-based mechanism to achieve confidentiality, integrity, and authenticity for pixel and header data, involving encryption, signature construction, decryption, and signature verification. Soualmi et al. [14] combined DCT transform, Weber descriptors (WDs), and Arnold chaotic map for watermarking. Al-Haj et al. [15] employed DWT-based watermarking, demonstrating improved results compared to existing approaches in terms of peak signal-to-noise ratio (PSNR). Al-Nabhani et al. [16] proposed an undetectable blind watermarking mechanism using a probabilistic neural network to ensure the hiddenness and quality of the watermarked image. Liu et al. [17] developed a multi-watermarking system based on dual-tree complex wavelet transform and discrete cosine transform (DTCWT-DCT), enhancing watermark data through Henon map chaotic encryption.

III. BACKGROUND

A. System Model

In the system model, a sender transmits a watermarked image with an encoded watermark using a secret key. The watermark consists of patient information, doctor information, diagnostic data, least significant bits (LSB) of the ROI part of a health-related image, and a logo for integrity verification. The receiver receives the watermarked medical image, extracts the watermark using an extraction algorithm, and decodes the embedded watermark using the same key. Figure 1 provides an overview of the process of transmitting and extracting medical images.

B. Problem Statement

Spatial domain watermarking techniques embed data directly into the image pixels, lacking robustness and being susceptible to geometric attacks. Using DCT for watermarking medical images is time-consuming due to the need for extensive computations to extract and insert vital data into image blocks. Embedding medical data into the entire image instead of separating ROI and RONI leads to significant distortion of the ROI, making it difficult for medical practitioners to diagnose based on the image [1], [2]. Therefore, a watermarking technique

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

is required that provides a robust watermark without compromising the quality of medical images, while also being efficient in terms of time and computational resources.

IV. PROPOSED SOLUTION

Our proposed solution introduces a wavelet-based digital watermarking system that fulfills security requirements. To achieve this, we employ a three-level discrete wavelet transform (DWT) combined with BCH coding, enhancing the system's undetectability and ability to counter various threats. The DWT is applied to the Region of Non-Interest (RONI) of a health-information image, generating distinct frequency sub-bands (LL, LH, HL, HH) at each separation stage. The encoding process involves non-overlapping blocks in the LL sub-band, where the watermark is embedded. Subsequently, a three-level inverse DWT is performed to obtain a watermarked health-data image that ensures confidentiality, availability, and reliability during image transfer. We first describe the recommended embedding procedure, followed by the extraction process.

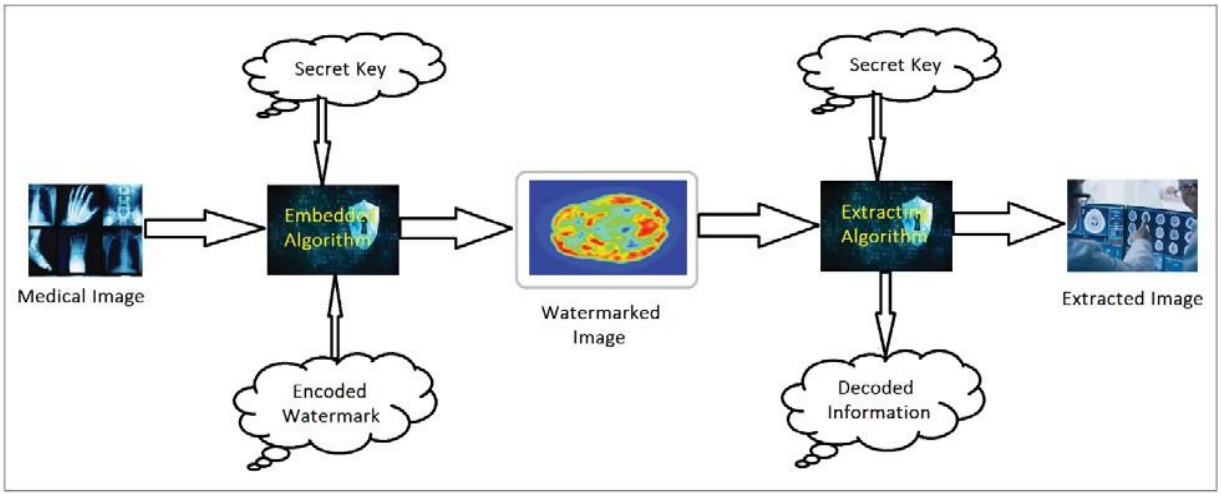

Figure 1

The information to be transmitted as the watermark is encoded using a BCH encoder, which generates a BCH cipher. BCH codes are cyclic error-correcting codes constructed using polynomials in a finite field. One crucial feature of BCH codes is their ability to accurately control the number of representational errors that can be corrected by the code during construction. Binary BCH codes capable of correcting multiple bit faults can be created. Additionally, BCH codes are easily deciphered using an algebraic technique called syndrome decoding. The proposed system combines three-level DWT and BCH coding to fulfill essential security requirements. Figure 2 illustrates the suggested watermark embedding algorithm, while the process of original image recovery is depicted in Figure 3.

A. Watermark Embedding Scheme

In the ROI part of the image, a fragile watermark is introduced using the Least Significant Bit (LSB) algorithm. This algorithm alters the LSBs of a grayscale picture to embed the imprint for a health image.

The original LSBs of the ROI, along with patient information, doctor's information, diagnostic information, and a logo, are first encoded using a secret key and then inserted into the RONI region of a medical image as a robust watermark.

The RONI region is divided into N x N blocks and subjected to a three-level DWT. The robust watermark generated as described above is inserted into the image. The image is then subjected to a three-level Inverse Discrete Wavelet Transform (IDWT) to bring it back to the spatial domain. Finally, the ROI and RONI regions are merged to obtain an imprinted picture, which is then sent to the receiver.

B. Watermark Extraction Scheme

The watermarked image received from the sender is split into ROI and RONI parts.

The RONI part is divided into N x N blocks and subjected to a three-level DWT. Subsequently, it is extracted and decrypted to retrieve patient information, doctor's information, diagnostic information, and the logo, along

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

with the LSBs of the ROI region. The doctor's information helps verify the authenticity, while the logo serves to test the truthfulness of the picture.

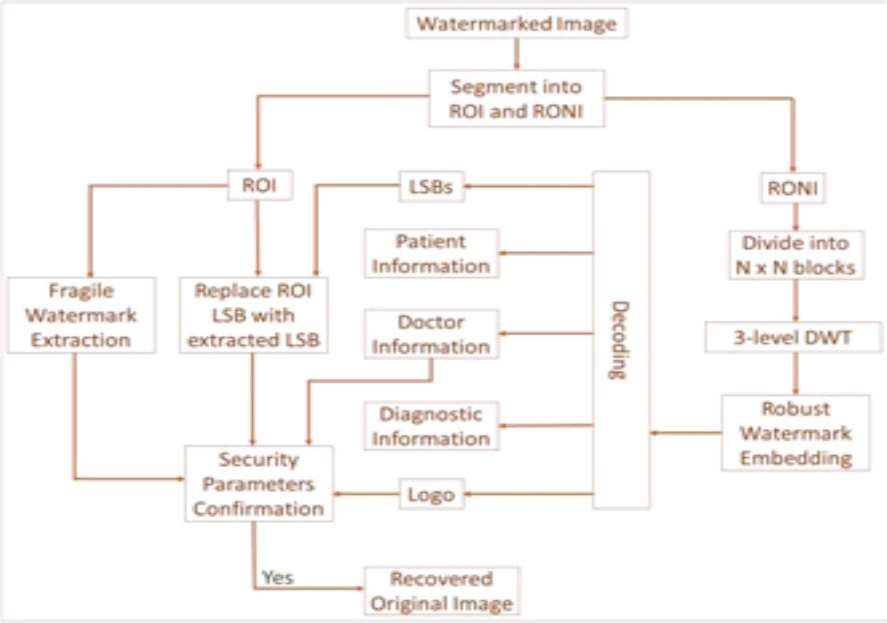

Figure 2. The process of watermark image embedding

In the ROI portion, the fragile imprint is extracted to test the accuracy of the picture, and the LSBs are obtained from the robust watermark. These LSBs are used to recover the original unaltered picture by switching the corresponding bits in the ROI portion.

The RONI portion undergoes a three-level Inverse DWT and is then combined with the ROI part to reconstruct the initial health-information image.

V. SECURITY ASSESSMENT

We have conducted a comprehensive evaluation of the security features in our proposed solution to assess its resilience across different security parameters. Furthermore, we delve into the effectiveness of the suggested approach in countering various incidents.

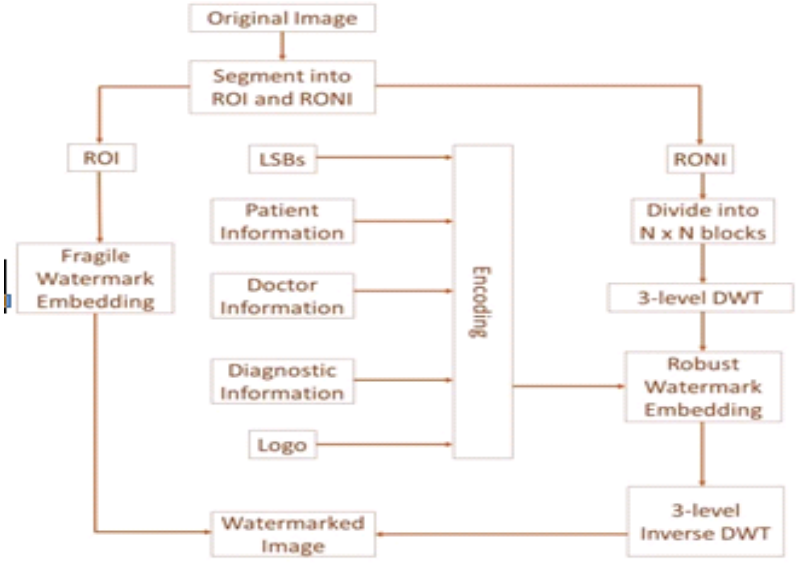

Figure 3. The process of original image extraction

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

A. Security Parameters

To ensure confidentiality, two keys have been generated. The first key is a 256 x 256 matrix used to embed information during the initial level of DWT decomposition. This key is created by combining the RONI part of the image (converted into matrix form) and a separately generated random matrix of the same size (256 x 256). The second key is a 128 x 128 matrix derived from the previously computed key.

Reliability is divided into two aspects: Integrity and Authentication. Integrity is achieved by embedding a logo along with the relevant information in the watermark of each health picture. If the manipulated image is tampered with, the extracted logo will reveal forgery, allowing the receiver to detect and ensure the integrity of the image. Authentication is provided by encoding vital data of both the client and doctor within the image.

B. Security Attacks

In order to assess the security of the proposed solution, we conducted several security attacks on the system:

Gaussian Noise: This involves intentionally adding noise signals to a health-information image, resulting in graphical distortions and inaccuracies.

Salt and Pepper Attack: This attack introduces random occurrences of white and black pixels in a health-information image, following a unique probability distribution function different from Gaussian noise.

Median Filtering Attack: By applying this image processing technique, noise presence in a vital-information image is reduced, improving image quality. However, the embedded watermark signals may also be affected or even eliminated.

Gaussian Smoothing Attack: Similar to median filtering, Gaussian smoothing aims to reduce noise in a health-information image to enhance its quality. The difference lies in the approach taken for smoothing the image.

Modification: This attack involves modifying specific bits of the watermarked image, resulting in changes to the stored data. Any attempt to alter information in the image will be immediately identified.

VI. PERFORMANCE ANALYSIS

Preserving the quality of health-information images is crucial. To evaluate the performance of the proposed approach, we need to verify the accuracy of the recovered images. The results are measured against the following benchmarks:

A. Peak Signal to Noise Ratio (PSNR): PSNR assesses the relationship between the highest achievable signal value and the influence of altering noise. It indicates image accuracy and similarity between two images. A higher PSNR value implies greater similarity.

B. Signal to Noise Ratio (SNR): SNR represents the ratio of signal power to noise power, measured in decibels (dB). A higher ratio (greater than 0 dB) indicates a stronger signal compared to noise.

C. Mean Squared Error (MSE): MSE calculates the average squared difference between the predicted and actual numbers as the median of the squared errors.

These performance measures are essential in determining the efficiency of the proposed scheme for implementation in the network. We implemented the suggested system in MATLAB software to analyze the results, enabling the receiver party to identify any alterations in transferred images. Any changes in the images will directly reflect in the aforementioned measures, allowing for easy detection. To ensure accurate results, we calculated PSNR, MSE, and SNR using C programming language codes for various relevant mechanisms and the proposed system. Additionally, we compared the PSNR and SNR values for the existing relevant mechanisms with the proposed scheme, as shown in Figure 4. Higher PSNR and SNR values indicate fewer chances of image variations. The MSE values were found to be 0.0075 in [15], 0.0109 in [16], and 0.0012 in the proposed mechanism. A lower MSE is preferable, as it indicates a lower potential error rate in the images.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

Figure 4. PSNR and SNR Comparison for Schemes

VII. CONCLUSION

The protection of health-information images and related client records is crucial not only for confidentiality but also to prevent falsifications that can occur from both authorized and unauthorized entities. Numerous methods have been proposed to address these challenges. Experiments have shown that DWT-based methods are favorable due to their accurate correspondence with the human visual system. The medical field has stringent requirements for the quality of health-information images, disallowing non-scientific alterations. Our proposed solution aims to fulfill all security requirements outlined in the problem statement. The implementation results demonstrate that the suggested mechanism performs well while considering security needs. Therefore, the potential of this work lies in making it more resistant to attacks when transmitting critical images in a public environment.

VIII. REFERENCES

[1] Qasim, A. F., Meziane, F., & Aspin, R. (2018). Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. Computer Science Review, 27, 45-60.

[2] Mohanarathinam, A., Kamalraj, S., Venkatesan, G. P., Ravi, R. V., & Manikandababu, C. S. (2019). Digital watermarking techniques for image security: a review. Journal of Ambient Intelligence and Humanized Computing, 1-9.

[3] Qasim, A. F., Aspin, R., Meziane, F., & Hogg, P. (2019). ROI-based reversible watermarking scheme for ensuring the integrity and authenticity of DICOM MR images. Multimedia Tools and Applications, 78(12), 16433-16463.

[4] Abraham, J., & Paul, V. (2019). An imperceptible spatial domain color image watermarking scheme. Journal of King Saud University- Computer and Information Sciences, 31(1), 125-133.

[5] Wu, J. H., Chang, R. F., Chen, C. J., Wang, C. L., Kuo, T. H., Moon, W. K., & Chen, D. R. (2008). Tamper detection and recovery for medical images using near-lossless information hiding technique. Journal of Digital Imaging, 21(1), 59-76.

[6] Mostafa, S. A., El-Sheimy, N., Tolba, A. S., Abdelkader, F. M., & Elhindy, H. M. (2010). Wavelet packets-based blind watermarking for medical image management. The open biomedical engineering journal, 4, 93.

[7] Solanki, N., & Malik, S. K. (2014). ROI based medical image watermarking with zero distortion and enhanced security. International Journal of Education and Computer Science, 10, 40-48.

[8] Fontani, M., De Rosa, A., Caldelli, R., Filippini, F., Piva, A., Consalvo, M., & Cappellini, V. (2010, September). Reversible watermarking for image integrity verification in hierarchical pacs. In Proceedings of the 12th ACM workshop on Multimedia and security (pp. 161-168).

[9] Eswaraiah, R., & Sreenivasa Reddy, E. (2014). Medical image watermarking technique for accurate tamper detection in ROI and exact recovery of ROI. International journal of telemedicine and applications, 2014.

[10] Lei, B., Tan, E. L., Chen, S., Ni, D., Wang, T., & Lei, H. (2014). Reversible watermarking scheme for medical image based on differential evolution. Expert Systems with Applications, 41(7), 3178- 3188.

[11] Parah, S. A., Ahad, F., Sheikh, J. A., & Bhat, G. M. (2017). Hiding clinical information in medical images: a new high capacity and reversible data hiding technique. Journal of biomedical informatics, 66, 214-230.

[12] S.S. Bedi, G.S. Tomar & Shekhar Verma, "Robust Watermarking of Image in the Transform Domain using Edge Detection", IEEE International Conference on simulation UKSIM 2009, pp.233-238, Mar 25-29, 2009.

[13] Parah, S. A., Sheikh, J. A., Ahad, F., Loan, N. A., & Bhat, G. M. (2017). Information hiding in medical images: a robust medical image watermarking system for E-healthcare. Multimedia Tools and Applications, 76(8), 10599-10633.

[14] Ali, M., Ahn, C. W., & Pant, M. (2014). A robust image watermarking technique using SVD and differential evolution in DCT domain. Optik, 125(1), 428-434.

[15] Al-Haj, A. (2015). Providing integrity, authenticity, and confidentiality for header and pixel data of DICOM images. Journal of digital imaging, 28(2), 179-187.

[16] Yahya, A. N., Jalab, H. A., Wahid, A., & Noor, R. M. (2015). Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network. Journal of King saud university-Computer and Information sciences, 27(4), 393-401.

[17] Soualmi, A., Alti, A., & Laouamer, L. (2018). A new blind medical image watermarking based on weber descriptors and Arnold chaotic map. Arabian Journal for Science and Engineering, 43(12), 7893-7905.

[18] Liu, J., Li, J., Ma, J., Sadiq, N., Bhatti, U. A., & Ai, Y. (2019). A robust multi-watermarking algorithm for medical images based on DTCWT- DCT and Henon map. Applied Sciences, 9(4), 700.