


Robust medical image watermarking in frequency domain

Roop Singh¹ , Pavan Kumar Shukla², Tarun Kumar³, and Vinod M Kapse⁴

^{1,2,4}Department of Electronics and Communication Engineering, Noida Institute of Engineering & Technology, Gr. Noida, UP, India, ¹roopsolanki@gmail.com, ²pavanfec@gmail.com, ⁴vinodmkapse@gmail.com

³School of Computing Science & Engineering, Galgotias University, Gr. Noida, UP, India, tarunsharma2910@gmail.com

*Correspondence: roopsolanki@gmail.com

ABSTRACT- Protecting patient information in medical image watermarking poses a significant challenge, especially when traditional methods like the Arnold transform prove inadequate in ensuring security. This paper introduces a novel approach within the Discrete Wavelet Transform (DWT) domain to address this issue effectively. By employing the Advanced Encryption Standard (AES), the security and robustness of the system are greatly enhanced through the encryption of both the medical image and patient data. The encrypted medical image undergoes a 2-level DWT process, allowing the concealment of encrypted patient information while maintaining its invisibility. This proposed scheme surpasses others in experimental evaluations, as evidenced by metrics such as PSNR and NC, solidifying its position as a more secure choice for medical image watermarking. The results validate the scheme's robustness and imperceptibility.

General Terms: Patient information, Security.

Keywords: Medical watermarking, Discrete Wavelet Transform, Advanced Encryption Standard, Arnold Transform, Security.

ARTICLE INFORMATION

Author(s): Roop Singh, Pavan Kumar Shukla, Tarun Kumar, and Vinod M Kapse;

Received: 14/07/2023; **Accepted:** 25/09/2023; **Published:** 28/09/2023;

e-ISSN: 2347-470X;

Paper Id: IJEER 1407R6;

Citation: 10.37391/IJEER.110333

Webpage-link:

<https://ijeer.forexjournal.co.in/archive/volume-11/ijeer-110333.html>

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.



1. INTRODUCTION

The evolution of information technology has made it easier to duplicate, manipulate, and distribute digital data, resulting in an increased need for secure control over digital multimedia content such as images, videos, and audio [1]. This has increased the importance of continuous authentication and copyright protection for multimedia content [2]. In parallel, as telemedicine applications gain prominence in healthcare, there is a growing emphasis on ensuring the security of electronic patient records (EPR) during their transmission, storage and sharing between healthcare institutions and open channels. Adhering to the digital imaging and communications in medicine (DICOM) standards is essential for effective EPR data exchange. However, when combined with other header files, DICOM medical image files often come with headers containing critical patient information, making them vulnerable to loss, tampering, or corruption. Steganography, cryptography, and watermarking are three primary methods for securing multimedia content. Steganography and cryptography are valuable for certain security aspects but may not address data integrity and authenticity concerns.

Conversely, watermarking is better suited for ensuring

multimedia content's integrity and authenticity is a priority [3].

Medical image watermarking strikes a balance between security and accessibility, making it a preferred choice over steganography and cryptography in healthcare settings where data integrity, authenticity, and privacy are paramount, while maintaining the clinical utility of medical images [4]. Medical image watermarking offers several advantages over steganography and cryptography in the healthcare sector: 1. *Data Integrity and Authenticity:* Unlike steganography and cryptography, which may not inherently ensure data integrity and authenticity, watermarking provides a way to embed information directly into the image, allowing for easy verification of data integrity and authenticity. This is crucial for maintaining the trustworthiness of medical records and images. 2. *Accessibility:* Watermarked medical images retain their diagnostic value, making them readily accessible for healthcare professionals. In contrast, cryptography can render images unreadable without decryption, potentially delaying critical diagnoses or treatments, and steganography may alter the image in ways that impact its clinical utility. 3. *Patient Privacy:* Watermarking allows for the secure embedding of patient data within images, ensuring confidentiality while enabling authorized access. Cryptography may require separate decryption steps that can introduce potential privacy risks, and steganography may not provide the same level of data protection. 4. *Data Traceability:* Watermarking can include information about the source, ownership, or timestamps, facilitating traceability and accountability in healthcare data. This traceability is often more challenging to achieve with steganography, which focuses on hiding information, or with cryptography, which prioritizes confidentiality over traceability. 5. *Visual Verification:* Watermarks can be visible or invisible, allowing for easy visual verification of the presence of embedded information.

This transparency is valuable in healthcare, where medical professionals can quickly identify watermarked data, while steganography and cryptography may require additional steps for verification. 6. *Data Recovery*: In data loss or corruption cases, watermarking may offer advantages by allowing for partial data recovery or reconstruction from the watermarked images. Cryptography may not provide the same level of data recovery capabilities, and steganography may render data irretrievable if the hidden information is compromised.

Watermarking techniques for digital media can be applied in either the spatial or frequency domain or a combination of both [5]. Popular spatial domain watermarking techniques include Least Significant Bit (LSB). Spatial domain watermarking is more superficial and offers high imperceptibility but is less robust against attacks. In the frequency domain, commonly used schemes encompass Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), and numerous additional methods. In contrast, frequency-domain watermarking provides excellent resistance to various threats and allows flexible watermark placement within different frequency components [6]. The choice of technique depends on factors such as the desired level of security, robustness against attacks, and the specific characteristics of the watermarked multimedia content.

Watermarking techniques for digital media can be applied in either the spatial or frequency domain or a combination of both [5]. Popular spatial domain watermarking techniques include Least Significant Bit (LSB). Spatial domain watermarking is more superficial and offers high imperceptibility but is less robust against attacks. In the frequency domain, commonly used schemes encompass Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), and numerous additional methods. In contrast, frequency-domain watermarking provides excellent resistance to various threats and allows flexible watermark placement within different frequency components [6]. The choice of technique depends on factors such as the desired level of security, robustness against attacks, and the specific characteristics of the watermarked multimedia content.

Researchers have explored numerous techniques for embedding patient information, both directly and indirectly, in both spatial and frequency domains [7]. Some authors have incorporated encryption methods before watermarking, while others have chosen to embed patient data directly, bypassing encryption. However, the existing schemes have exhibited vulnerabilities, failing to safeguard patient data against attacks adequately. Consequently, this paper introduces an innovative watermarking scheme based on Advanced Encryption Standard (AES) encryption to enhance the security of patient data in a multi-resolution framework. The presented work offers several vital contributions:

1. It introduces an innovative watermarking scheme based on AES encryption, implemented within a multi-resolution framework.

2. The scheme strategically embeds the watermark at the 2-level LL sub-band, ensuring high imperceptibility.
3. while simultaneously leveraging AES encryption methods' security and robustness advantages.

1.1 Literature review

This section reviews the schemes related to the presented method. The existing schemes are summarized in Table 1. Bw et al. [8] introduced a watermarking method utilizing LSB Modification for tamper detection and recovery within the ROI. We employ RLE to embed the original LSBs in the RONI to enhance reversibility, enabling a higher embedding capacity. Experimental results showcase the system's ability to achieve up to 100% accuracy in tamper detection and localization, along with a 100% image recovery rate. Elbasi et al. [9] used watermarking to embed patient data in medical MR images, employing two methods: one in the frequency domain (DWT, DCT, and DFT) and the other in the spatial domain (LSB). Experiments showed that frequency domain embedding resisted one set of attacks, while spatial domain embedding with LSB provided resilience against different attacks. Genetic algorithm (GA) and LSB (Least Significant Bit)-based grayscale medical watermarking presented in [10].

Table 1: Comparison of related Watermarking Schemes for Medical Images

Reference	Embedding Method	Encryption Method	Domain	Objective
Bw et al. [8]	LSB Modification with RLE (Reversible)	None	Spatial	Tamper detection and recovery in ROI
Elbasi et al. [9]	Frequency (DWT, DCT, DFT) and Spatial (LSB)	None	Mixed	Robustness against various attacks
Soni et al. [10]	LSB-based grayscale watermarking (Reversible)	None	Spatial	Patient data embedding and security
Shehab et al. [11]	Singular Value Decomposition (SVD)	None	Spatial	Image tamper detection and self-recovery
Singh et al. [12]	LWT and DCT with MD5 and BCH (Encryption)	MD5 (Signature Watermar)	Frequency	Identity verification and secure patient data

Khare et al. [13]	Homomorphic Transform, RDWT, and SVD (Reversible)	None	Mixed	Integrity and security of patient information
Soni et al. [14]	Wavelet-based with three-level DWT and BCH (Reversible)	None	Mixed	Enhanced decision support with embedded data
Soualmi et al. [15]	Combination of DCT, Weber Descriptors, and Arnold Chaotic Map (Reversible)	Arnold Chaotic Map (Encryption)	Spatial	Robustness against various attacks and data integrity
Nazari et al. [16]	Chaotic IWTLBSB with adjustable capacity (Reversible)	None	Mixed	Secure transmission of authenticated medical images
Singh et al. [17]	NSCT, DCT, and SVD (Reversible)	None	Mixed	Security and robustness for medical images and EPR

This scheme encodes the patient information in a 2D barcode, which is then embedded into the original image using LSB. This combination enhances the security of patient information. A fragile medical watermarking scheme tailored for authentication and self-recovery, presented in [11]. This scheme detects image tampering while also restoring the original image. The process involves dividing the host image into 4×4 blocks and utilizing Singular Value Decomposition (SVD). We then embed the SVD block traces into LSB bits of the image pixels to identify transformations in the host medical image.

Patient information in the previously mentioned schemes is concealed within the spatial domain, rendering them vulnerable to attacks. To counter this vulnerability, researchers have explored embedding patient information in either the frequency domain or both domains. Singh et al. [12] introduced a robust watermarking technique for telehealth using LWT and DCT. It adds a 'signature watermark' for identity and a 'patient report' to medical images. The signature is encrypted with message-digest (MD5), and the patient report is encoded with BCH. It's effective, secure, and minimally distorts the image. A secure watermarking scheme is presented in [13], which maintains the integrity of patient

information. This approach combines homomorphic transform, redundant discrete wavelet transforms, and singular value decomposition to create a robust watermarking technique for medical images. The method enhances security through 2-D chaotic Arnold transform encryption and has shown improved robustness and imperceptibility in experiments under various attacks. In Ref. [14], a digital watermarking scheme for medical images relies on wavelet-based techniques presented, which explicitly employ a three-level Discrete Wavelet Transform (DWT) and BCH coding. This scheme aims to assist medical practitioners in making precise and informed decisions based on the watermark-embedded medical images. Soualmi et al. [15] developed a watermarking technique for medical images, which combines DCT, Weber descriptors, and the Arnold chaotic map, significantly boosting robustness against various attacks while preserving data integrity. This approach offers practical and adequate security for medical image applications. Ref. [16] introduces an innovative blind watermarking method that combines chaotic IWT-LSB techniques, offering adaptable capacity for securely transmitting authenticated medical images. Singh et al. [17] utilizing NSCT, DCT, and SVD, provides a balanced solution for securing medical images with electronic patient records (EPRs). This non-blind approach, dependent on the cover image at the receiver, ensures watermark accuracy through preprocessing. By embedding EPR data within specific sub-bands with optimal gain factors, we strike a practical balance between imperceptibility, robustness, and capacity. The method's resilience against various attacks as indicated by high PSNR and CC values.

Frequency or mixed domain schemes can conceal patient information with or without encryption, and although many of these schemes have utilized Arnold transform for encryption, it is acknowledged that Arnold transform may not provide sufficient security. Consequently, in this paper, the AES algorithm is adopted for encrypting both the host image and patient information, enhancing data security.

The remainder of the paper is structured as follows: Section 2 delves into the related methods relevant to the proposed scheme. Section 3 outlines the procedure of the proposed scheme, while Section 4 presents and discusses the experimental results. Lastly, in Section 5, the paper concludes by summarizing its contributions.

2. RELATED TECHNIQUE

2.1 Discrete Wavelet Transform

The Discrete Wavelet Transform (DWT) is a vital mathematical and signal processing technique used to dissect and process digital data, especially in digital signal and image processing. It decomposes data into wavelet coefficients by applying high-pass and low-pass filters and down sampling, resulting in a multiresolution representation with various scales or frequency components [18]. DWT is extensively employed in diverse applications, including image compression, noise reduction, feature extraction, and data analysis, making it indispensable for tasks requiring multi-

scale analysis and efficient representation of data with varying levels of detail.

2.2 Advanced Encryption Standard

Advanced Encryption Standard (AES), is a widely used symmetric-key encryption algorithm designed to secure and protect data from unauthorized access. AES is highly regarded for its security and efficiency. It provides strong encryption, making it computationally infeasible for attackers to recover the original data without the correct key [19]. In AES, data is encrypted and decrypted using the same secret key, making it suitable for confidentiality and integrity protection. AES operates on fixed-size data blocks (128 bits) and supports key lengths of 128, 192, or 256 bits. The encryption process involves several rounds (10, 12, or 14 rounds depending on the key length), each consisting of well-defined mathematical operations. These operations include substitution (SubBytes), permutation (shiftrows), mixing (mixcolumns), and adding a round key (XOR with a subkey derived from the primary encryption key). These operations are performed in a precise sequence for each round.

3. PROPOSED SCHEME

In this section, we comprehensively explain the proposed scheme, which is termed as DWT-AES. The DWT-AES scheme combines DWT and AES algorithm to enhance security and robustness in medical image watermarking. Initially, the AES algorithm is applied to encrypt the medical image and the patient information, ensuring heightened security. Subsequently, a 2-level DWT process is carried out on the encrypted medical image, focusing on the LL sub-band, where the encrypted patient information is concealed to enhance imperceptibility. To better understand the embedding and extraction process illustrated in *figure. 1 and 2*.

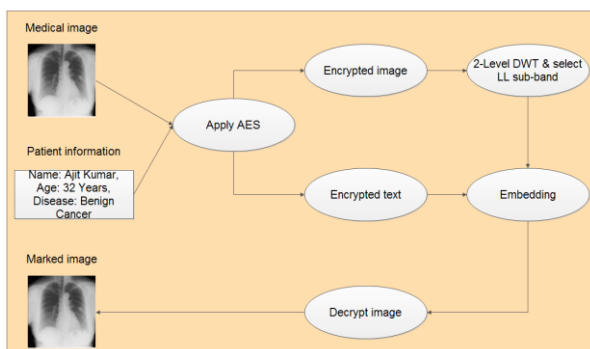


Figure 1: Embedding procedure of proposed scheme.

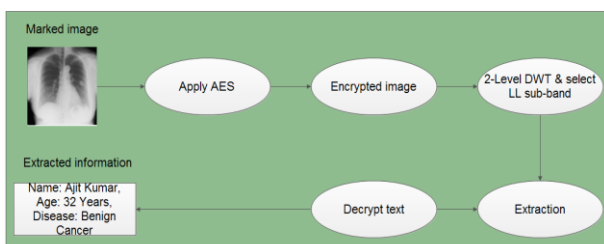


Figure 2: Extraction procedure of proposed scheme.

3.1 Embedding scheme

The pseudocode of embedding procedure is given in *Algorithm 1*.

3.2 Extraction scheme

The To retrieve patient information, the reverse process of *Algorithm 1* is executed. The pseudocode for this extraction procedure can be found in *Algorithm 2*.

Algorithm 1: Watermark Embedding Algorithm

```

Data: cover_img: The medical cover image;
patient_info_path: Path to patient information text file;
key: AES encryption key;
reps: Number of encryption repetitions
Result: wmarked_img: The watermarked image;
PSNR: Peak Signal-to-Noise Ratio;
SSIM: Structural Similarity Index
while true do
    // Read the selected cover image
    cover_path = strcat(pathname, filename);
    cover_img = imread(cover_path);
    // Access and read patient information
    fileID = fopen(patient_info_path, 'r');
    patient_info = textscan(fileID, '%s %s', 'Delimiter', '|');
    patient_info1 = fileread(patient_info_path);
    fclose(fileID);
    // Encrypt patient information
    text_msg = patient_info1;
    s2 = uint8(text_msg);
    x2 = de2bi(s2);
    abc = size(x2);
    a1 = 1;
    foreach i in abc do
        | a1 = a1 * i;
    end
    x2 = reshape(x2, 1, a1);
    s = encrypt(x2, reps, key);
    ax = size(s);
    in = 1;
    foreach i in ax do
        | in = in * i;
    end
    new_size = in;
    n = reshape(s, 1, new_size);
    m = int2str(n);
    // Map binary digits to alphabets
    foreach digit in m do
        | // Map binary digits to alphabets here
    end
    // Save the encrypted message
    fid = fopen('AES_encrypted.txt', 'wt');
    fprintf(fid, m);
    fclose(fid);
    // Embed the encrypted message into the cover image
    img = cover_path;
    text = 'AES_encrypted.txt';
    out = 'stego_image.png';
    wmarked_img = embed(img, text);
    imwrite(wmarked_img, 'wmarked_img.png');
    wmarked_path = 'wmarked_img.png';
    // Evaluate performance metrics
    PSNR = psnr(cover_img, wmarked_img);
    SSIM = ssim(cover_img, wmarked_img);
end

```

Algorithm 2: Patient information extraction algorithm

```

Data: wmarked_img: The watermarked image;
Result: ext_img: The extracted patient information;
BER: Bit error rate;
NC: Normalised correlation;
while true do
    // Extract the watermark
    k = extract(wmarked_path);
    m = k;
    // Map characters to digits
    m = str2num(m);
    // Calculate dimensions
    n = size(m);
    // Decrypt patient information
    final_data = decrypt(input_data, reps, user_key);
    si = size(final_data);
    a2 = 1;
    foreach i2 in si do
        | a2 = a2 · i2;
    end
    ans1 = reshape(final_data, 1, a2);
    ans1 = num2str(ans1);
    // Calculate dimensions
    ac = size(ans1);
    // Map digits back to characters
    m = k;
    m = str2num(m);
    // Calculate dimensions
    n = size(m);
    a1 = 1;
    foreach i1 in n do
        | a1 = a1 · i1;
    end
    abc = √a1;
    input_data = reshape(m, abc, abc);
    // Decrypt patient information
    xx = reshape(ans1, 1, b);
end
    
```

4. Experimental Results

In this section, we conduct a comprehensive performance evaluation of the DWT-AES scheme. The effectiveness of the proposed scheme (DWT-AES) is assessed with a focus on imperceptibility and robustness using a set of five medical images, specifically CT scans, MRIs, and X-rays retrieved from [20] (as depicted in *figure 3*). The patient information is showcased in *figure 1*. Imperceptibility is quantified by comparing the cover medical image with the marked image, employing metrics such as PSNR and SSIM. Meanwhile, robustness is evaluated by comparing the embedded patient information with the extracted patient information using the NC metric.

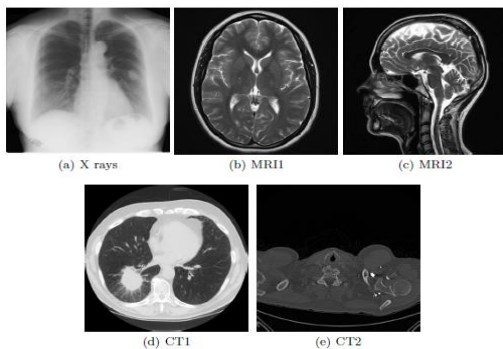


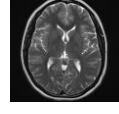
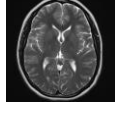
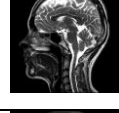
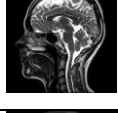


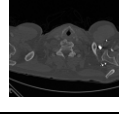
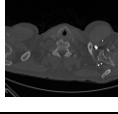


Figure 3: Medical (a-e): (a) X-ray, (b) MRI1, (c) MRI2, (d) CT1, and (e) CT2.

4.1 Imperceptibility and Robustness Analysis without Attack

The proposed scheme (DWT-AES) evaluates imperceptibility and robustness in terms of PSNR, SSIM, and NC. The analysis presented in *table 2* provides a comprehensive overview of the quality of marked images alongside their corresponding PSNR, SSIM, and NC values. Notably, the table reveals a remarkable similarity between the quality of the marked images and the original medical images. Furthermore, the proposed DWT-AES scheme consistently achieves impressively high PSNR values exceeding **44**, SSIM values exceeding **0.9972**, and NC values surpassing **0.9978** across all images considered in the evaluation. These compelling results underscore the exceptional imperceptibility of the proposed scheme.

Table 2: Qualitative and quantitative analysis of DWT-AES.




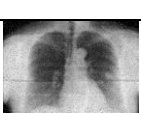


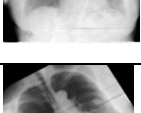
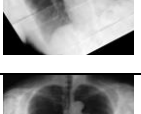
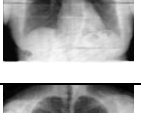
Cover image	Marked image	PSNR	SSIM	NC
		47.51	0.9987	0.9996
		45.63	0.9972	0.9978
		46.47	0.9981	0.9990
		44.86	0.9973	0.9984
		46.51	0.9982	0.9991

4.2 Imperceptibility and robustness analysis with attack

The performance of DWT-AES scheme is also evaluated under various attacks. These attacks are encountered on marked image to measure robustness. The list of attacks are as follows: (i) Gaussian low pass filtering, (ii) Average filtering, (iii) Median filtering, (iv) Salt pepper noise, (v) Gaussian noise, (vi) Cropping, (vii) Rotation, (viii) Histogram, and (ix) JPEG compression.

Table 3 presents a comprehensive view of the quality of attacked images alongside their NC values for each specific attack. From table, it becomes evident that the proposed scheme consistently achieves commendable NC values, demonstrating its resilience and effectiveness.

Table 3: Qualitative and quantitative analysis of DWT-AES.

S. No.	Attack Type	Attacked Image	NC
1	Gaussian low pass filtering ($\sigma = 0.5$)		0.9992
2	Average filtering (3×3)		0.9996
3	Median filtering (3×3)		0.9995
4	Salt pepper noise (density = 0.07)		0.9989
5	Gaussian noise (Var = 0.05)		0.9983
6	Cropping (50%)		0.9973
7	Rotation (30°)		0.9985
8	Histogram		0.9994
9	JPEG compression (quality = 60%)		0.9993

4.3 Comparison with Related Schemes

The proposed scheme (DWT-AES) is compared with three recent schemes, namely, Singh et al. [12], Soualmi et al. [15], and Nazari et al. [16] in terms of PSNR and NC.

4.3.1 Imperceptibility comparison in terms of PSNR

Table 4 provides a quantitative comparison of PSNR values achieved by different methods with the proposed method. It can be observed from the table that the Proposed method stands out with the highest PSNR value of 47.51, signifying superior image quality compared to the other methods.

Table 4: Comparative analysis of PSNR values.

S. No.	Work	PSNR
1	Proposed	47.50
2	Singh et al. [12]	40.71
3	Soualmi et al. [15]	39.05
4	Nazari et al. [16]	38.83

Table 5: Comparative analysis of NC values against each attack.

S. No.	Attack	Singh et al. [12]	Soualmi et al. [15]	Nazari et al. [16]	Proposed
1	Gaussian filtering ($\sigma = 0.6$)	0.9810	0.9843	0.9871	0.9990
2	Average filtering (5,5)	0.9917	0.9863	0.9917	0.9977
3	Median filtering (5,5)	0.9891	0.9901	0.9897	0.9916
4	Salt pepper noise (3%)	0.9814	0.9846	0.9873	0.9891
5	Gaussian noise (12%)	0.9813	0.9821	0.9827	0.9882
6	Cropping (60%)	0.9784	0.9790	.9774	0.9915
7	Rotation (50°)	0.9773	0.9803	0.9847	0.9961
8	Histogram	0.9856	0.9782	0.9794	0.9967
9	compression (75%)	0.9902	0.9918	0.9886	0.9990

4.3.2 Robustness comparison in terms of NC

Various attacks are encountered on marked images to measure the robustness of the proposed scheme. Table 5 tabulates the NC values against each attack. This table confirms the proposed scheme consistently achieves the highest NC values over each considered attack. These results strongly suggest that the proposed scheme is robust and highly effective in maintaining the fidelity of images subjected to diverse image processing challenges. The proposed scheme consistently performs better than existing schemes while recovering patient data.

5. CONCLUSION

Protecting patient information in medical image watermarking has emerged as a formidable challenge. This paper has introduced an innovative approach within DWT domain,

offering a highly effective solution to this problem. Leveraging AES, the proposed scheme significantly enhances the system's security and robustness by encrypting medical image and patient data. Incorporating a 2-level DWT process allows for the seamless embedding of encrypted patient information while preserving its visual imperceptibility. The presented approach is the preferred choice for secure medical image watermarking, with results affirming its exceptional robustness and imperceptibility.

In future research, Authors will focus on optimizing efficiency and adaptability to various data types, as well as staying ahead of emerging security challenges in order to establish this approach as a trusted solution for data protection in various domains.

REFERENCES

- [1] Moad MS, Kafi MR, Khaldi A (2022) Medical image watermarking for secure e-healthcare applications. *Multimedia Tools and Applications* 81(30):44,087–44,107.
- [2] Moad MS, Kafi MR, Khaldi A (2022) A wavelet based medical image watermarking scheme for secure transmission in telemedicine applications. *Microprocessors and Microsystems* 90:104,490.
- [3] Zermi N, Khaldi A, Kafi R, Kahlessenane F, Euschi S (2021) A dwt-svd based robust digital watermarking for medical image security. *Forensic science international* 320:110,691.
- [4] Singh R, Saraswat M, Ashok A, Mittal H, Tripathi A, Pandey AC, Pal R (2022) From classical to soft computing based watermarking techniques: A comprehensive review. *Future Generation Computer Systems*.
- [5] Singh R, Ashok A, Saraswat M (2023) High embedding capacity-based color image watermarking scheme using sbbo in rdwt domain. *Multimedia Tools and Applications* 82(3):3397–3432.
- [6] Singh R, Mittal H, Pal R (2022) Optimal keyframe selection-based lossless video-watermarking technique using igs in lwt domain for copyright protection. *Complex & Intelligent Systems* 8(2):1047–1070.
- [7] Saraswat M, Pal R, Singh R (2022) Ds-at: An efficient watermarking technique based on arnold transform in dct and svd domain. In: *Proceedings of the 2022 Fourteenth International Conference on Contemporary Computing*, pp 11–14.
- [8] BW TA, Permana FP, et al (2012) Medical image watermarking with tamper detection and recovery using reversible watermarking with lsb modification and run length encoding (rle) compression. In: *2012 IEEE International Conference on Communication, Networks and Satellite (ComNetSat)*, IEEE, pp 167–171.
- [9] Elbasi E, Kaya V (2018) Robust medical image watermarking using frequency domain and least significant bits algorithms. In: *2018 International Conference on Computing Sciences and Engineering (ICCSE)*, IEEE, pp 1–5.
- [10] Soni GK, Rawat A, Jain S, Sharma SK (2020) A pixel-based digital medical images protection using genetic algorithm with lsb watermark technique. In: *Smart Systems and IoT: Innovations in Computing: Proceeding of SSIC 2019*, Springer, pp 483–492.
- [11] Shehab A, Elhoseny M, Muhammad K, Sangaiah AK, Yang P, Huang H, Hou G (2018) Secure and robust fragile watermarking scheme for medical images. *IEEE access* 6:10,269–10,278.
- [12] Singh AK (2019) Robust and distortion control dual watermarking in lwt domain using dct and error correction code for color medical image. *Multimedia Tools and Applications* 78:30,523–30,533.
- [13] Khare P, Srivastava VK (2021) A secured and robust medical image watermarking approach for protecting integrity of medical images. *Transactions on Emerging Telecommunications Technologies* 32(2), 3918.
- [14] Soni M, Kumar D (2020) Wavelet based digital watermarking scheme for medical images. In: *2020 12th international conference on computational intelligence and communication networks (CICN)*, IEEE, pp 403–407.
- [15] 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* 43:7893–7905.
- [16] Nazari M, Mehrabian M (2021) A novel chaotic iwt-lsb blind watermarking approach with flexible capacity for secure transmission of authenticated medical images. *Multimedia Tools and Applications* 80(7):10,615–10,655.
- [17] Singh S, Singh R, Singh AK, Siddiqui TJ (2018) Svd-dct based medical image watermarking in nscd domain. *Quantum computing: an environment for intelligent large scale real application* pp 467–488.
- [18] Singh R, Izhar LI, Elamvazuthi I, Ashok A, Aole S, Sharma N (2022) Efficient watermarking method based on maximum entropy blocks selection in frequency domain for color images. *IEEE Access* 10:52,712–52,723.
- [19] Awasthi D, Srivastava VK (2023) Hessenberg decomposition-based medical image watermarking with its performance comparison by particle swarm and jaya optimization algorithms for different wavelets and its authentication using aes. *Circuits, Systems, and Signal Processing* pp 1–32.
- [20] dataset (2023) Ct and mri brain scans — kaggle. <https://www.kaggle.com/datasets/darren2020/ct-to-mri-cgan>, (Accessed on 09/04/2023).



© 2023 by the Roop Singh, Pavan Kumar Shukla, Tarun Kumar, and Vinod M Kapse. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).