Towards Improving Medical Images Security using a Hybrid Watermarking Technique Based on DWT and DCT

Rania HAMAMI[1], Narima ZERMI[1], Larbi BOUBCHIR[2], Amine KHALDI[3]

[1]LASA Laboratory, Badji Mokhtar University, Annaba, Algeria.

[2]LIASD research Lab, University of Paris 8, Paris, France.

[3]LINAT laboratory, University of Kasdi Merbah, Ouargla, Algeria.

E-mail: rania.hamami@univ-annaba.dz, naili.narima@gmail.com, larbi.boubchir@univ-paris8.fr, khaldi.amine@univ-ourgla.dz

Abstract - In medical imaging, protecting the confidentiality and security of sensitive medical images is of the highest importance. This article presents a new approach to improve the security of these images by directly embedding logos, patient, and hospital information. The technique uses a combination of discrete wavelet transform (DWT) and discrete cosine transform (DCT) to guarantee robustness and enhanced security. In addition, the watermark data is hashed using the MD5 algorithm before embedding, further enhancing protection against unauthorized use and distribution. Experimental results demonstrate the outstanding performance of the method, with a maximum signal-to-noise ratio PSNR in excess of 53 dB, and its robustness against a variety of attacks. The proposed technique offers an effective solution for protecting medical images while preserving patient confidentiality and integrity in diagnostic and treatment processes.

Keywords - Medical image, Watermarking, Discrete cosine transform, Discrete wavelet transform.

I. INTRODUCTION

Medical imaging has become a crucial data source in the healthcare sector. However, when these images are in use by hospitals, clinics, and doctors on public networks, there is a risk of unauthorized modification of patient information. To remove this problem, digital watermarking technology can offer an intelligent solution, by embedding the patient’s personal information directly into the medical images as a digital watermark [1]. In the world of digital watermarking for medical images, today’s studies focus on both the spatial domain, where the values of certain pixels are modified, and the transform domain, which encompasses techniques such as discrete cosine transform, discrete Fourier transform, and discrete wavelet transform. In the transform domain, the watermark is incorporated by changing the values of the coefficients, offering another approach to maintaining the privacy and security of medical images [2]. The digital watermarking process consists of three essential phases: integration, attacks, and detection/extraction. In the integration phase, the watermark is inserted into the image. Then, in the attack phase, the watermarked image is exposed to various potential attacks. Finally, the detection/extraction phase consists of restoring the original image from its watermarked version [3]. The most important requirements for an effective watermarking algorithm are imperceptibility and robustness [4]. The imperceptibility factor means that the watermarking process causes minimal deformation of the original image. On the other hand, robustness refers to the ability of the watermarking method to successfully recover the embedded watermark even when the watermarked image undergoes various manipulations and attacks [5]. In [6], the authors proposed an approach where they first perform sub-band decomposition of the medical image using discete wavelet transform (DWT). Then, they apply Singular Value Decomposition (SVD) to the LL subbands. To identify the most suitable regions for embedding, they utilize the particle swarm optimization algorithm on the LL sub-bands. In [7], Alshanbari et al. Combined two different watermarking methods. They integrated multiple watermarks into the medical image. Initially, they generated a secret key using the SHA-256 algorithm based on the image's Region of Interest (ROI). The ROI undergoes compression using the Lempel-Ziv-Welch (LZW) algorithm, followed by integration with signature data. Subsequently, the resulting watermark is inserted into the Region of Non-Interest (RONI) segment of the host image. The study's authors [2], introduce two blind watermarking approaches aimed at safeguarding medical images. In the initial approach, the authors merge discrete cosine transform (DCT) with Schur decomposition, embedding watermarks within the medium frequencies of the image. In the subsequent scheme, they employ a blend of discrete wavelet transform (DWT) and Schur decomposition. Both strategies are designed to safeguard patient information and uplold the confidentiality of personal data. In our study, a novel watermarking system is introduced, ensuring both robustness and imperceptibility. The primary aim of this research is to devise a watermarking method adapted for both RGB and grayscale medical images, leveraging the hybrid DWT-DCT domain [6], [8]. The system incorporates three watermarks, patient data, hospital information, and a hospital logo, which are transformed into secure binary sequences through a hash function and then embedded into DCT coefficients. This innovative approach significantly enhances the security and traceability of medical images, ensuring their integrity and authenticity. The rest of the paper is structured as follows: In Section 2, we explain our proposed method. In Section 3, we share the results of our experiments and discuss our findings in detail. Finally, in Section 4, we provide a summary of our approach.

II. PROPOSED METHOD

This section provides a concise overview of our poposed method, which consists of three main processes: generation of the watermark, embedding of the watermark and extraction of the watermark. Extensive tests were conducted on various medical images [9]–[11], including RGB and grayscale formats with a resolution of 1024 by 1024 pixels. Figure . 1 illustrates the original medical images (a), (b), and (c), and their corresponding watermarked images (d), (e), and (f).

A) Watermark Generation Process

The provided program performs watermark generation using a combination of hospital logo image (see Figure 2), hospital information, and patient data. The logo image is loaded and resized to a 32x32 resolution, while the hospital information and patient data are read from respective text files. For each data source, the program calculates the MD5 hash using the data hash function, resulting in a unique representation for the logo image, hospital information, and patient data. These MD5 hashes are then converted into binary vectors of 128 bits, creating watermarks for the respective data sources. The binary watermarks can be utilized in watermarking schemes to protect and authenticate the associated data, ensuring data integrity and origin verification.

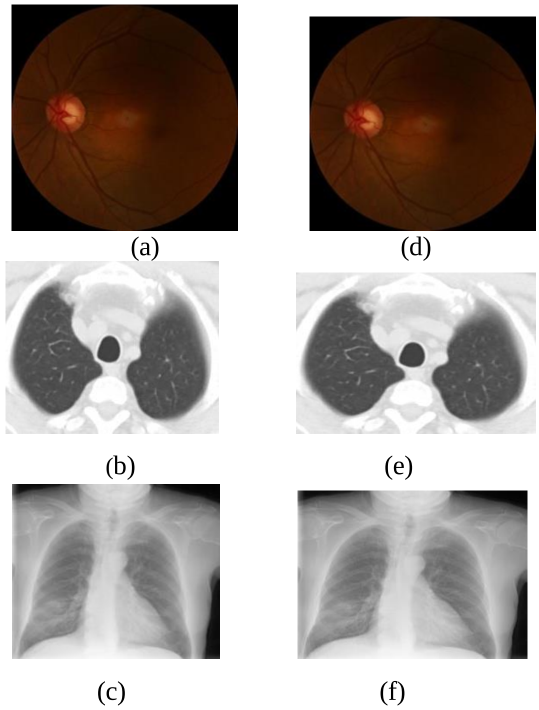

Fig.1. Medical images were used for the analysis of the proposed scheme. (a) and (b) represent RGB medical images, while (c) shows a grayscale medicalimage. (d), (e), and (f) are the corresponding watermarked images.

(a) (b)

Fig. 2. ”(a) Original hospital logo. (b) Processed hospital logo used for watermarking.”

B) Watermark Embedding Process

The proposed watermarking algorithm is divided into two subroutines: one for grayscale images and another for RGB images. For grayscale images, the DWT is applied directly to the image to obtain subbands, which are then processed using the DCT to embed watermark bits. On the other hand, for RGB images, the process is more intricate. After selecting and resizing the image, each color channel is denoised individually using a median filter. Then, a three-level Haar wavelet transform is applied to each channel. Similar to grayscale images, DCT is utilized to insert watermark binary data, such as logos into HH3, patient information into LH3, and hospital information into HL3 subbands. The watermarked subbands are reconstructed using Inverse DCT (IDCT), followed by the reconstitution of the 3-level Haar wavelet decomposition. Ultimately, the watermarked image is reconstructed using Inverse DWT (IDWT) after combining the watermarked color channels. In Figure 3, we illustrate the watermark embedding process into the medical image.

C) Watermark Extraction Process

The process of extracting watermark binary data from a watermarked image follows a sequential procedure. Different steps are taken depending on whether the image is grayscale or RGB. In the case of grayscale images, the DWT is directly applied to the image, and the DCT is used to extract the watermark bits from the subbands. On the other hand, the process becomes more complex for RGB images. After selecting and resizing the image, each individual color channel is denoised using a median filter. Then, a three-level Haar wavelet transform is applied to each channel. Similar to grayscale images, the DCT is employed to extract watermark binary data, including logos in HH3, patient information in LH3, and hospital information in HL3 subbands. It is important to note that the extracted hidden information, such as logos and sensitive data, cannot be directly viewed due to the protection of hash functions that ensure their confidentiality. However, the binary watermark can still be extracted.

III. EXPERIMENTAL RESULTS AND DISCUSSIONS

In this section, we present experimental results for assessing the imperceptibility and robustness of our proposed watermarking technique. The experimental setup utilized MATLAB version 2018a for the implementation of our watermarking technique.

A) Imperceptibility Test

For the imperceptibility evaluation, we measured three important metrics: Peak signal-to-noise ratio (PSNR), Normalized Correlation (NC), and Structural Similarity Index (SSIM). These metrics provide quantitative assessments of the visual quality and similarity between the original and watermarked images. The imperceptibility results for three sample images (a), (b), and (c) are presented as follows in Table 1.

Table 1. Imperceptibility Results.

Original image	PSNR	NC	SSIM
(a)	53.83dB	0.9996	0.9974
(b)	53.16dB	1	0.9975
(c)	55.36dB	1	0.9979

Table 2 provides a comprehensive comparison of the Peak Signal-to-Noise Ratio (PSNR) values obtained from our proposed method and the techniques developed by [2], [6], and [7].

Table 2. PSNR comparison of different methods.

Method	PSNR
K.Faresetal.[2]	49.20dB
Gangadharetal.[6]	43.52dB
Alshanbari[7]	48.37dB
Proposed method	≥53.16dB

B) Robustness Test

To assess the resilience of our watermarking technique, we exposed the watermarked images (d), (e), and (f) to various attacks wich are JPEG compression, gamma correction, Gaussian noise, salt and pepper noise, and sharpening. The robustness results for these attacks, measured in terms of Bit Correct Rate (BCR), are summarized in Table 3.

The table provides a comparison of the BCR values between our proposed method and other techniques proposed by [5], [12], and [13] under different attacks.

The experimental results validate the effectiveness of our proposed watermarking technique, which achieves an impressive balance between imperceptibility and robustness. The high PSNR values indicate the preservation of image details and minimal noise interference. Moreover, the NC values exceeding 0.9 demonstrates a strong correlation between the original and watermarked images, while consistently high SSIM scores signify the preservation of image structure and texture.

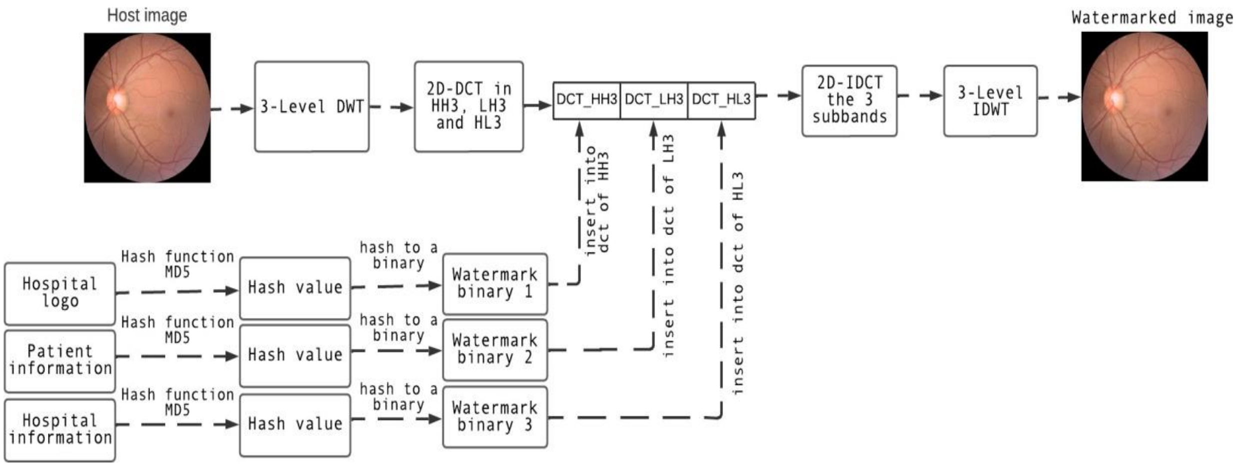

Fig. 3. Watermark Embedding Algorithm.

Table 3. Comparison of BCR (%) values under Attacks.

Attacks	Proposed method			Method by [5]	Method by [12]	Method by [13]
	(a)	(b)	(c)			
JPEG compression 40	99.5015%	99.9375%	99.5502%	92%	83.50%	69.85%
Gamma correction	99.89%	99.9734%	99.7942%	97%	-	-
Gaussian noise(0.01)	98.4881%	99.8321%	98.281%	-	99.06%	68.26%
Saltand pepper(0.01)	97.5098%	99.4686%	97.8352%	99%	99.17%	81.74%
Sharpening	99.4616%	99.969%	99.7691%	-	-	-

Furthermore, the proposed method exhibits resilience against various attacks, including JPEG compression, gamma correction, Gaussian noise, salt and pepper noise, and sharpening. This robustness reflects its ability to withstand image manipulations while maintaining watermark integrity.

By combining wavelet transform and discrete cosine transform, our technique enables secure embedding of patient information, hospital details, and the hospital logo into medical images. The utilization of an MD5-based watermark generation process enhances the uniqueness and integrity of the embedded watermarks. Overall, our watermarking technique shows great potential in enhancing healthcare services by safeguarding sensitive medical data and ensuring the authenticity of diagnostic imaging.

The imperceptibility of the watermarked images ensures that their integrity and diagnostic value remain unaffected, making them highly suitable for practical applications in medical image protection and authentication.

IV. CONCLUSION

In conclusion, the article introduced a robust watermarking technique that was specifically designed to safeguard both RGB and grayscale medical images from unauthorized use and distribution. The proposed approach integrated wavelet transform and discrete cosine transform, and
implemented the MD5 algorithm for watermark data hashing. The method excelled in achieving a balance between imperceptibility and robustness, securely embedding watermarks while preserving the high-quality of the original images. Compared to existing
approaches, our method exhibited superior performance and remarkable resilience against diverse attacks. As a result, it represented a promising and practical solution for securely and imperceptibly watermarking color medical images. This advancement carried significant implications in safeguarding sensitive medical data and ensuring the integrity of diagnostic imaging, contributing significantly to enhancing healthcare services and patient privacy. In our future research, we plan to investigate the integration of advanced neural networks for enhancing and streamlining the watermarking process.

V. REFERENCES

[1] Alzahrani, A., Memon, N. A. (2021). Blind and robust watermarking scheme in hybrid domain for copyright protection of medical images. IEEE Access, 9, 113714-113734.

[2] Fares, K., Khaldi, A., Redouane, K., Salah, E. (2021). DCT DWT based watermarking scheme for medical information security. Biomedical Signal Processing and Control, 66, 102403.

[3] Ali, M. (2023). Robust Image Watermarking in Spatial Domain Utilizing Features Equivalent to SVD Transform. Applied Sciences, 13(10), 6105.

[4] Allaf, A. H., Kbir, M. A. (2019). A review of digital watermarking applications for medical image exchange security. In Innovations in Smart Cities Applications Edition 2: The Proceedings of the Third International Conference on Smart City Applications (pp. 472-480). Springer International Publishing.

[5] 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, 110691.

[6] Anand, A., Singh, A. K. (2020). An improved DWT-SVD domain watermarking for medical information security. Computer Communications, 152, 72-80.

[7] Alshanbari, H. S. (2021). Medical image watermarking for ownership tamper detection. Multimedia tools and applications, 80, 16549-16564.

[8] Novamizanti, L., Suksmono, A. B., Danudirdjo, D., Budiman, G. (2023). Robust and Imperceptible Watermarking on Medical Images using Coefficient Pair Modification. IIUM Engineering Journal, 24(1), 88-105.

[9] Bodin Y. Ocular Disease Intelligent Recognition (ODIR-2019). DataScientest 2023. https://medium.com/datascientest/ocular diseaseintelligent- recognition-odir-2019-77bb62d42f1b (accessed July 29, 2023).

[10] Chest CT-Scan images Dataset n.d. https://www.kaggle.com/datasets/mohamedhanyyy/chest-ctscan-images (accessed July 29, 2023).

[11] COVID-19 Radiography Database n.d. https://www.kaggle.com/datasets/tawsifurrahman/covid19 radiographydatabase (accessed August 8, 2023).

[12] Ernawan, F., Kabir, M. N. (2018). A robust image watermarking technique with an optimal DCT-psychovisual threshold. IEEE Access, 6, 20464-20480.

[13] Sukanti, B. M. (2016). A Blind digital Watermarking Algorithm based on DWT-DCT Transformation/Sukanti B. Mardolkar, NayanaShenvi. International Journal of Innovative Research inElectrical, Electronics, Instrumentation and Control Engineering, 3.