International Journal of Computers and Informatics

Journal Homepage: https://www.ijci.zu.edu.eg

Int. j. Comp. Info. Vol. 6 (2025) 1–15

Paper Type: Original Article

Robust Blind Watermarking of Medical Images using ResNet-50 and Redundant Wavelet Transform

Mostafa M. Abdel-Aziz [1,*], Nabil A. Lashin [2], Hanaa M. Hamza [2] and Khalid M. Hosny [2]

[1] Department of Information Technology, Faculty of Information Technology and Computer Science, Sinai University, Arish Branch, Al-Arish 45518, Egypt; eng_mostfa_it@yahoo.com.

[2] Department of Information Technology, Faculty of Computer and Informatics, Zagazig University, Zagazig 44519, Egypt. Emails: nlashin@yahoo.com; hanaa_hamza2000@yahoo.com; k_hosny@zu.edu.eg.

Received: 14 Nov 2024 **Revised:** 21 Dec 2024 **Accepted:** 30 Dec 2024 **Published:** 01 Jan 2025

Abstract

Medical images are crucial in identifying and detecting certain disorders within healthcare necessities. Numerous secure and insecure networks communicate medical imaging, impacting critical clinical information. Despite the effectiveness of numerous medical image protection solutions, their robustness against complex intrusions has not received enough attention. This indicates the necessity to enhance medical image protection techniques against sophisticated attackers. To address this issue, we created a new strong blind watermarking method for medical images that uses ResNet-50 and the Redundant Wavelet Transform (RDWT) in a hybrid domain. We first divide the input image into 8x8 non-overlapping blocks for rapid computation and then feed it into the pre-trained ResNet-50 model to extract the stable feature vector accurately. RDWT transforms the obtained feature vector to generate the detailed coefficients LL, LH, HL, and HH. To improve security, we first encrypt the binary watermark (BW) using Arnold encryption to embed it in the selected LL sub-band. The pre-trained ResNet50 model, when combined with RDWT in a hybrid domain, effectively captures more intrinsic and localized features. The study's findings are highly promising, demonstrating the proposed method's effectiveness in robustness and invisibility. The embedded watermark can be extracted free of distortion. The extracted watermark appears genuine, demonstrating optimal BER and NC values. The BER values neared zero in nearly all attack scenarios, while the NC values approached one.

Keywords: ResNet-50; RDWT; Hybrid Domain; Robust Blind Watermarking.

1 | Introduction

The swift progression of contemporary healthcare and the increasing demand for enhanced living standards have generated an immediate necessity for tailored medical care. This speedy advancement enabled physicians to identify diseases and select appropriate treatments more efficiently. The transfer of medical images across many potentially insecure networks directly affects critical clinical information. Despite numerous effective solutions, we have neglected the robustness of medical imaging security against advanced attacks. Therefore, improving methods for safeguarding medical images against sophisticated adversaries is crucial. The fundamental principle of medical watermarking is embedding confidential patient information into a carrier medical image, thus creating a watermarked image [1]. The watermarking algorithm should produce

Corresponding Author: eng_mostfa_it@yahoo.com

inescapable results, preserving the invisibility of images while avoiding distortion and ensuring robustness [2]. Attempts to obscure or remove the watermark should be complex, if not impossible. Modern approaches have focused on integrating deep learning with conventional watermarking methods, showing improved effectiveness over traditional approaches [3, 4]. Nonetheless, the deep learning system must address concerns regarding durability and privacy. When selecting a deep learning model for watermarking, it is essential to identify the most effective embedding process within the host image, establish the optimal embedding strength, and conduct an attack simulation to ensure precise watermark recovery.

Recent advancements in deep learning-based watermarking techniques have become essential for preserving copyright. Current research discusses multiple deep learning-based watermarking methods. Convolutional Neural Networks (CNNs) represent a fundamental model that produces notable outcomes in digital watermarking. Multiple network architectures have developed within the CNN layers, with ResNet and VGGNet predominantly employed for feature extraction [5, 6]. CNN is essential for identifying the most comprehensive and distinctive characteristics. Over the years, numerous articles have been published on medical image watermarking. The essential requirements of a medical watermarking system are robustness, imperceptibility, and substantial capacity.

Achieving a balance between these requirements leads to developing more effective domain strategies [7, 8]. Nyeem et al. [9] reviewed medical image watermarking techniques related to confidentiality and safety. Gull and Parah [10] reviewed and compared different watermarking techniques for their practicality in medical imaging. Before applying, they examine all the challenges associated with conventional watermarking in medical images. DL algorithms autonomously discern data hierarchically, eliminating the need for feature representations. CNN is a DL architecture that employs convolution features. Kandi et al. [11] pioneered the initial method of DL-based watermarking. They introduced a CNN-based system that uses distinct codebooks to produce images of varying sizes for embedding and extraction processes. The technique analyzes the host and inverted images to attain a diminished image resolution. The method fundamentally enlarges the resultant image to reconstruct the relevant codebooks. The method inserts the BW by adjusting the pixel values to align with the derived codebook.

Guo et al. [12] Guo et al. employed a CNN model to develop a series of batch normalizations that would minimize resource consumption throughout the watermarking routine. Mahapatra et al. [13] presented a watermarking technique that utilizes a CNN auto-encoder. The embedding network extracts and concatenates feature maps concerning the host and watermark pictures. The extraction network integrates the RLU function at a specific block level to extract watermark information from the extracted features. Fan et al. [14] proposed a watermarking approach that employs CNN Inception V3 and DCT to enhance the diagnostic precision in medical images by handling, modifying, and encrypting watermarks. They used Google Neural Network transfer learning to make the system more private, protect against geometrical attacks, and allow watermark embedding. This method incorporates pre-trained networks and Henon chaos encryption.

Zhang et al. [15] introduced a strong multi-watermarking method for medical images that uses Google Neural Network transfer learning to improve privacy, resistance to geometrical attacks, and the ability to embed watermarks. The technique employs pre-trained networks and Henon chaos encryption. The approach described in [16] employed DarkNet53 for transfer learning, effectively extracting 128-bit features from encrypted medical images. The procedure subsequently employs DCT to extract 32-bit features, referred to as feature 1, thereby enhancing the algorithm's robustness. In [17], the authors developed a watermarking algorithm that uses contourlet and SVD transforms to deal with problems like false positives, scaling factor identification, attack resistance, and poor image quality.

Sharma and Mir [18] showed a rapid and effective way to use machine learning to improve image watermarking. They use the DCT, ant colony optimization, and the light gradient boosting algorithm to make the method strong and difficult to spot. Darwish et al. [19] presented an innovative zero-watermarking technique for color images, employing CNN and 2D-LACM to extract deep feature maps, encrypt copyright watermarks, and jumble the binary feature matrix to enhance invisibility and robustness. The hybrid

watermarking mechanism integrates classical transform domain techniques with CNN-based methods to improve robustness and invisibility. This mechanism uses watermarks in frequency coefficients to make them more resistant to attacks. At the same time, CNNs improve feature learning and watermark extraction, which makes the system safer and more efficient.

Traditional watermarking systems frequently exhibit insufficient security protocols and limited resilience to diverse attacks. Their imperceptibility is inadequate, making the watermark visible or readily discernible. Furthermore, they exhibit deficiencies in advanced encryption and scrambling techniques, rendering them susceptible to tampering and unauthorized access. Considering these limitations, we are driven to innovate an efficient blind watermarking scheme that reduces processing time, enhances security, and provides high resilience in medical image watermarking. The subsequent points delineate the key contributions of our research:

- Recent studies show that, despite using various watermarking algorithms, they are not sufficiently resilient to multiple attacks. Therefore, we present a new blind and robust watermarking method, ResNet-50 and RDWT, in an amalgamation domain to maintain robustness capabilities.
- We employ ResNet-50 to generate a feature vector, and its advantageous inherent characteristics guarantee that the proposed method exhibits markedly enhanced resilience to geometric and signal processing assaults.
- RDWT is providing synchronous identification in both the time and frequency domains. It is extremely computationally effective and has the advantage of distinguishing intricate details in images.
- Implementing the novel hybrid ResNet50-RDWT methodology streamlines feature extraction and deformation management, facilitating distinct native and local attributes. It significantly enhances conceptual effectiveness and promotes resilience.
- The proposed algorithm adeptly balances sturdiness and imperceptibility, surpassing previous algorithms in security and robustness, as evidenced by experimental results.

This paper is structured as follows: Section 2 outlines the proposed approach's fundamental components. Section 3 presents the empirical findings. Section 4 provides a summary of the study's conclusions.

2 | Preliminaries

2.1 | ResNet-50 Model Architecture

ResNet-50 employs residual learning and comprises 50 layers organized into five blocks. Residual blocks protect data from earlier layers, which lets the network get better representations of input data and makes it easier to train deep neural networks. The gradient can traverse directly across the network via bypass connections or conveniences. The ResNet-50 architecture includes batch normalization, residual blocks, global average pooling, fully linked classification layers, and convolutional layers. These layers are used to ensure successful identification mapping [20]. Figure 1 depicts the simulation framework of the ResNet-50 model.

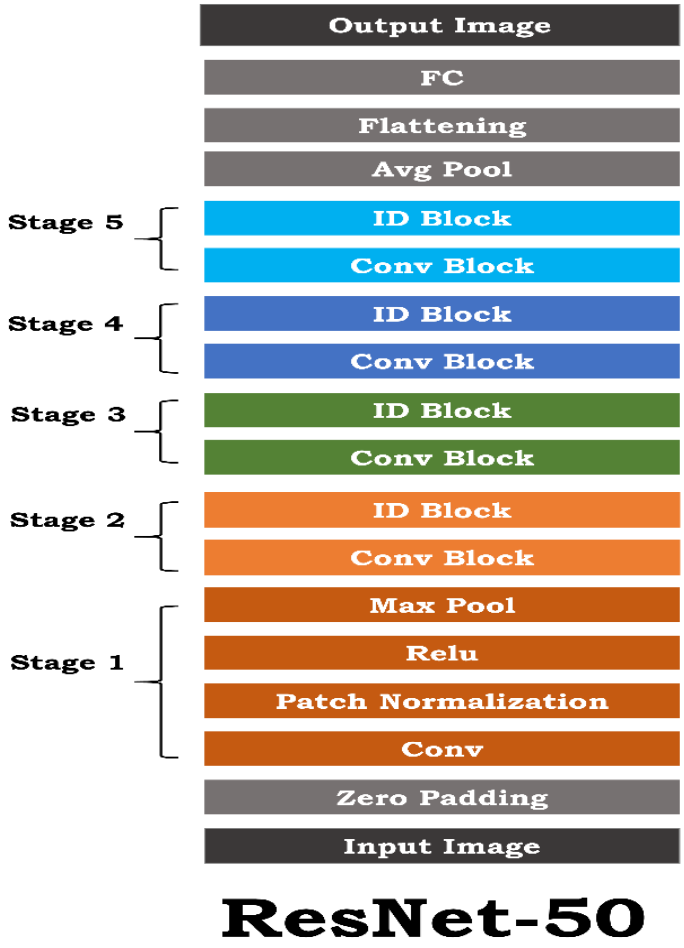


Figure 1. A simplified depiction of the ResNet-50 architecture.

2.2 | Redundant Wavelet Transform (RDWT)

RDWT is a technique that removes the up-sampling and down-sampling of coefficients encountered in the ordinary DWT during filter-bank rounds. RDWT has been developed to address this issue due to its shift invariance property [21]. The subsequent equations can express the analysis and synthesis of RDWT. Eqs. (1) and (2) pertain to RDWT analysis, while Eq. (3) addresses RDWT synthesis.

Where

$$k_x[y] = (k_{x+1}[y] * h_x[-y] \tag{1}$$

Where $h_x[-y]$ is the low-pass analysis filter.

$$L_x[y] = (k_{x+1}[y] * g_x[-y] \tag{2}$$

Where $g_x[-y]$ is the high-pass analysis filter.

$$k_{x+1}[y] = {}^{1}/_{2}\,(k_x[y] * h_x[y] + l_x[y] * g_x[y] \tag{3}$$

$h[y]$ and $g[y]$ denote low and high pass synthesis filters. k_x and l_x refer to the low and high band coefficients.

3 | Proposed Method

This section explores the proposed watermarking scheme. We produce the watermarked image using host medical and secret images as inputs. The proposed scheme aims to improve the host watermarked image's invisibility and robustness against multiple attacks. We used the pre-trained ResNet-50 model to construct a robust feature vector from the selected medical image. We subject the constructed feature vector to the RDWT to extract the detailed coefficients. We embed the scrambled watermark bit stream in the LL sub-band to enhance security and confidentiality. Figure 2 illustrates a schematic diagram of the proposed method.

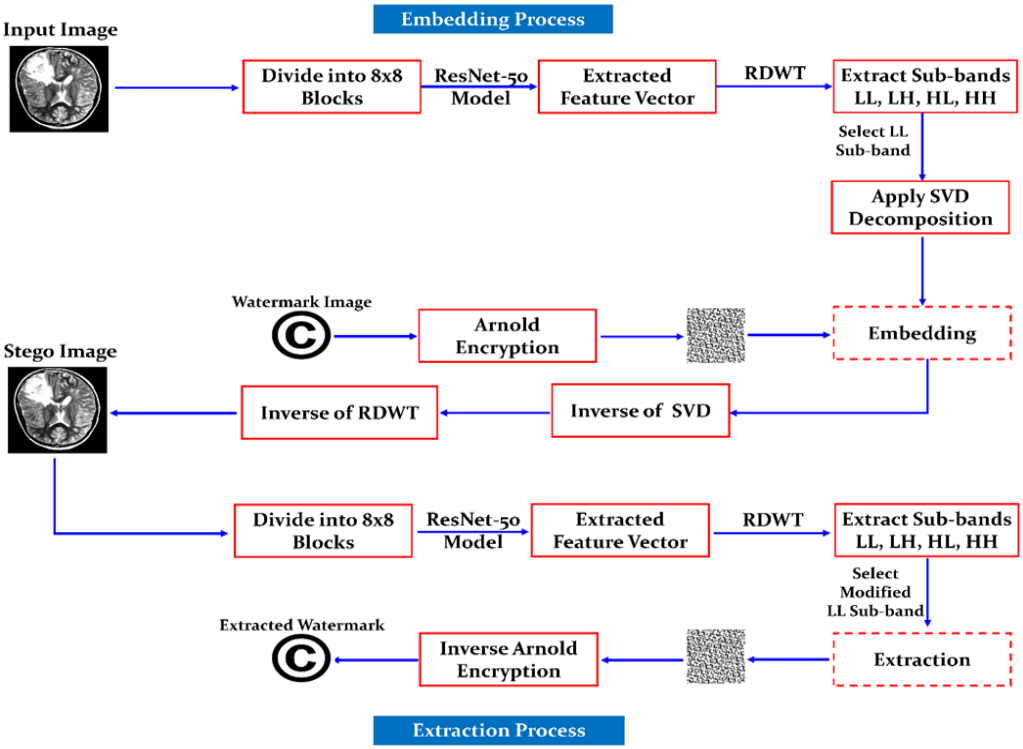


Figure 2. The proposed method overview.

3.1 | Embedding Process

Consider a watermark image $W(p,q)$, and host image $H(i,j)$. To simplify computations, let $p = q = 64$ and $i = j = 512$.

Embedding Algorithm

Input: Host and watermark images
Step 1: Split the host image into $\mathbf{8 \times 8}$ nonoverlapping blocks. Step 2: Apply the pre-trained ResNet-50 model to the obtained blocks to construct a robust feature vector. Step 3: Apply the obtained feature vector to the RDWT to construct the detailed coefficients LL, LH, HL, and HH. Step 4: Apply the SVD to the selected LL sub-band. Step 5: Encrypt the watermark bits sequence using Arnold encryption. Step 6: Embed the scrambled bits stream using the following norm: Norm: $\begin{cases} \boldsymbol{If\ U_{3,1} = x.m + \propto/2,\ U_{4,1} = x.m - \propto/2,\ For\ (1)\ Embedding} \\ \boldsymbol{If\ U_{3,1} = x.m - \propto/2,\ U_{4,1} = x.m + \propto/2,\ For\ (0)\ Embedding} \end{cases}$ Step 7: Apply the inverse of SVD and RDWT.
Output: Watermarked image

3.2 | Extraction Process

The extraction algorithm below provides the steps for blind watermark extraction.

Extraction Algorithm

Input: Watermarked image
Step 1: Split the watermarked image into $\mathbf{8 \times 8}$ nonoverlapping blocks. Step 2: Apply the pre-trained ResNet-50 model to the obtained blocks. Step 3: Apply the obtained feature vector to the RDWT to construct the detailed coefficients LL, LH, HL, and HH. Step 4: Apply the SVD to the selected LL sub-band. Step 5: Extract the scrambled bits stream using the following norm: Norm: $\begin{cases} \lvert U_{3,1}\rvert - \lvert U_{4,1}\rvert > 0, & \textbf{\textit{For (1) Extraction}} \\ \textbf{\textit{Otherwise,}} & \textbf{\textit{For (0) Extraction}} \end{cases}$ Step 7: Apply the inverse of Arnold encryption to recover the watermark image.
Output: Extracted watermark image

4 | Experiments and Results

The proposed method conducts experiments on medical images with pixel dimensions of 512×512 were selected from COVID-19 Dataset [22] and Brain Tumor Dataset [23], and three watermark images of size 64×64, as shown in Figures 3 and 4, respectively.

In this section, we adhered to the established experimental procedures prescribed by previous watermarking algorithms for critical performance assessment. First, we assessed the quality of the watermarked and extracted watermark images. Second, we outlined the statistical metrics utilized to evaluate the suggested method's resilience to malicious attacks.

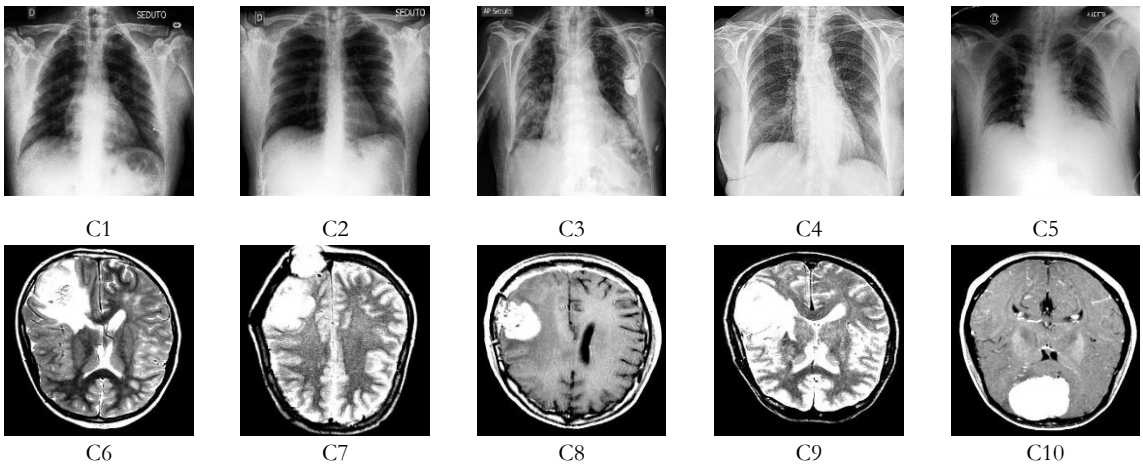


Figure 3. Selected medical images from datasets.

Figure 4. Binary watermark images.

4.1 | Invisibility Assessment

The first experiment assesses the invisibility of the proposed watermarking method utilizing two prevalent metrics: PSNR and SSIM. Eqs. (4) and, (5) calculate PSNR and SSIM as follows:

$$\mathrm{PSNR} = 10\log\left[\frac{\mathrm{XYMax_{ij}(H(m,n)^2}}{\sum_m \sum_n (\mathrm{I(m,n)} - \mathrm{(H'(m,n)^2}}\right] \tag{4}$$

$$\mathrm{SSIM(F,F')} = \frac{(2\mu F\mu F' + C1)(2\sigma FF' + C2)}{(\mu_S^2 + \mu_{S'}^2 + C1)(\sigma_S^2 + \sigma_{S'}^2 + C2)} \tag{5}$$

We implanted a watermark (W1) into host medical images (C1-C5) to detect differences in intensity maps between the original and watermarked images. This was conducted to evaluate the proposed algorithm's invisibility efficacy. Table 1 displays the obtained PSNR results for the selected medical image under the assumption of no attacks.

Experiments have yielded high PSNR values for all tested images, varying from 51.99 dB to 54.45 dB. The average PSNR value for the tested medical images was 53.52 dB, with low variations between host and watermarked images. The average SSIM value was 0.9998 for the selected images.

We tested the visual impact on some selected medical images to estimate the degree of influence between them. The absolute difference between images is not noticeable, as shown in Table 2.

Table 1. Image concealment and recovery visualization.

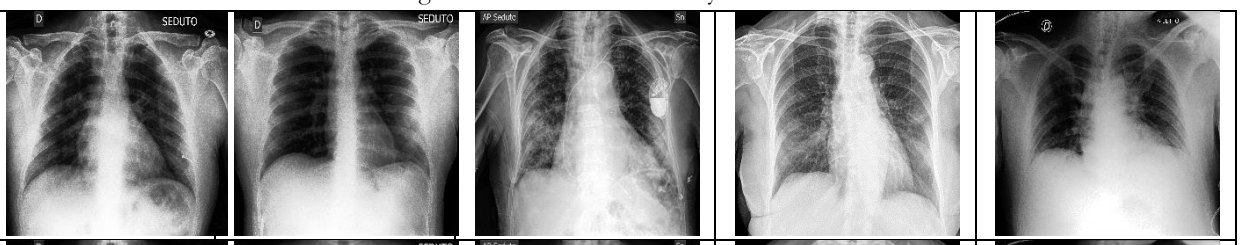
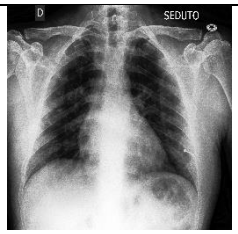
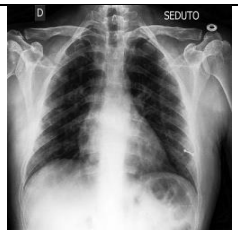
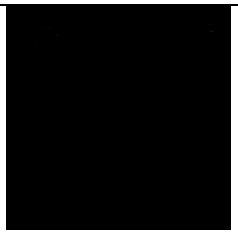
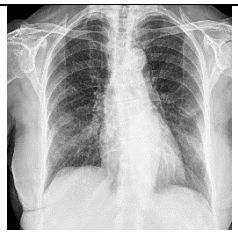
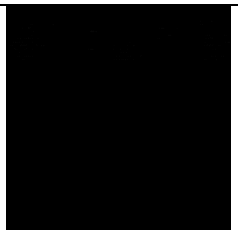
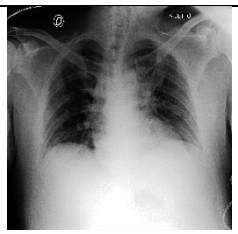
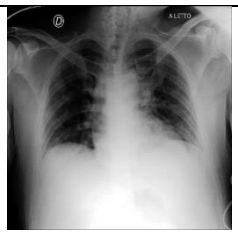
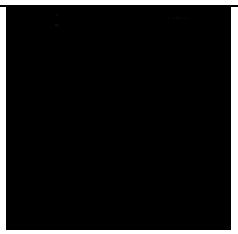
Host Image					
Watermarked Image					
Extracted Watermark	©	©	©	©	©
PSNR	53.33	54.42	54.45	51.99	53.41
SSIM	0.9998	0.9999	0.9999	0.9997	0.9998
BER	0	0	0	0	0
NC	1	1	1	1	1

Table 2. Images difference analysis.

Host Image	Watermarked Image	Difference Image
		
		
		
		
		

4.2 Robustness Analysis for Different Attacks

In this experiment, we employed BER and NC to evaluate the similarity between the recovered watermark image and its genuine counterparts. We demonstrate a superior correspondence between the original and restored watermark images. We calculate the NC and BER using equations 6 and 7.

$$\mathrm{BER} = \frac{1}{a \times b} \sum_{i=1}^{a} \sum_{j=1}^{b} [W(i,j) \oplus W'(i,j)] \tag{6}$$

$$\mathrm{NC} = \frac{\sum_i \sum_j W(i,j) W'(i,j)}{\sum_u \sum_v W(i,j)^2} \tag{7}$$

We conduct several trials using standard classical attacks to assess the proposed method. This test employs various geometric and processing distortions, including median filtering, JPEG compression, Poisson noise, Gaussian noise, and speckle noise, as well as transformations such as scaling, rotation, translation, shearing,

and cropping, each characterized by distinct parameters. The increase in NC and the decrease in BER values indicate that our method successfully reconstructed the retrieved secret image with minimal distortion, closely resembling the original. Below is a summary of the results that were conducted.

In the first investigation, we analyzed a suited medical image, "C1," measuring 512×512, and a binary secret image, "W1," measuring 64×64. Table 3 calculates NC and BER values for each evaluated geometrical attack associated with the retrieved image. The retrieved image has withstood multiple tested attacks, achieving high NC and low BER values within optimal bounds. The results indicate that the retrieved images remain detectable despite various attacks.

In the second investigation, we analyzed an image named "C2" with a pixel resolution of 512×512 and a binary watermark image known as "W2" with a pixel resolution of 64×64. Tables 4 and 5 display the PSNR, NC, and BER values for all assessed noise-adding and filtering attacks.

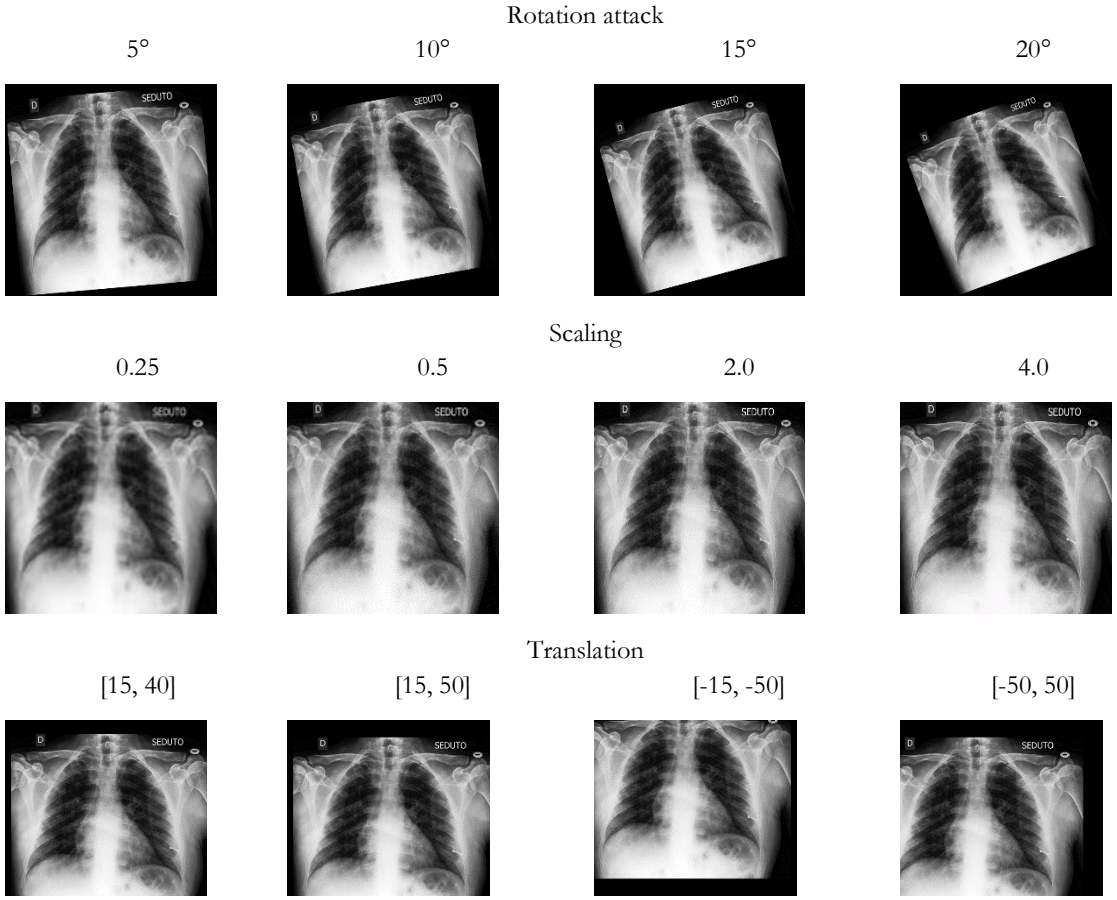


Figure 5. Geometrical attacks simulation for the attacked watermarked image.

The proposed watermarking method exhibited considerable robustness to multiple attacks. The selected medical image experiences various disturbances, including rotation, scaling, translation, and shearing attacks. Table 3 demonstrates the recovery of the concealed image with minimal distortion. The obtained NC and BER results were 1 and 0 for most evaluated assaults, respectively. The results obtained for all assessed assaults approached optimal values, demonstrating the methodology's significant robustness. We systematically applied various noise-adding and filtering attacks under different conditions to assess the robustness of the selected medical image against multiple threats. We conducted filter assaults using average, median, Gaussian, and sharpening filters. Tables 4 and 5 present the outputs from both the simulation and numerical analyses. The results indicate optimal BER and NC values, demonstrating effective secret image reconstruction with minimal distortion.

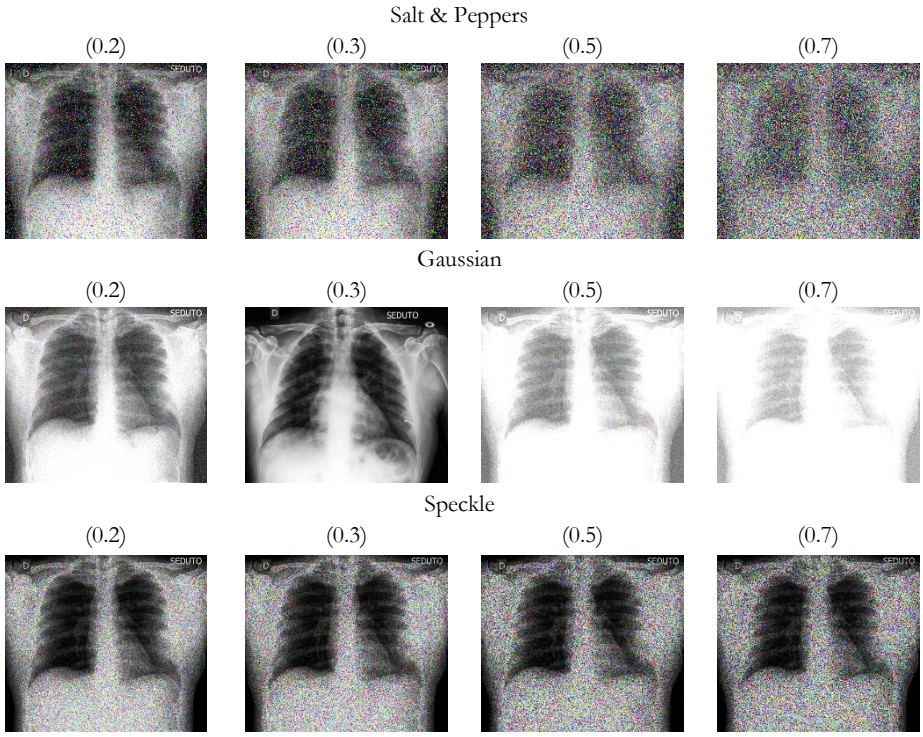


Figure 6. Processing attacks simulation for the attacked watermarked image.

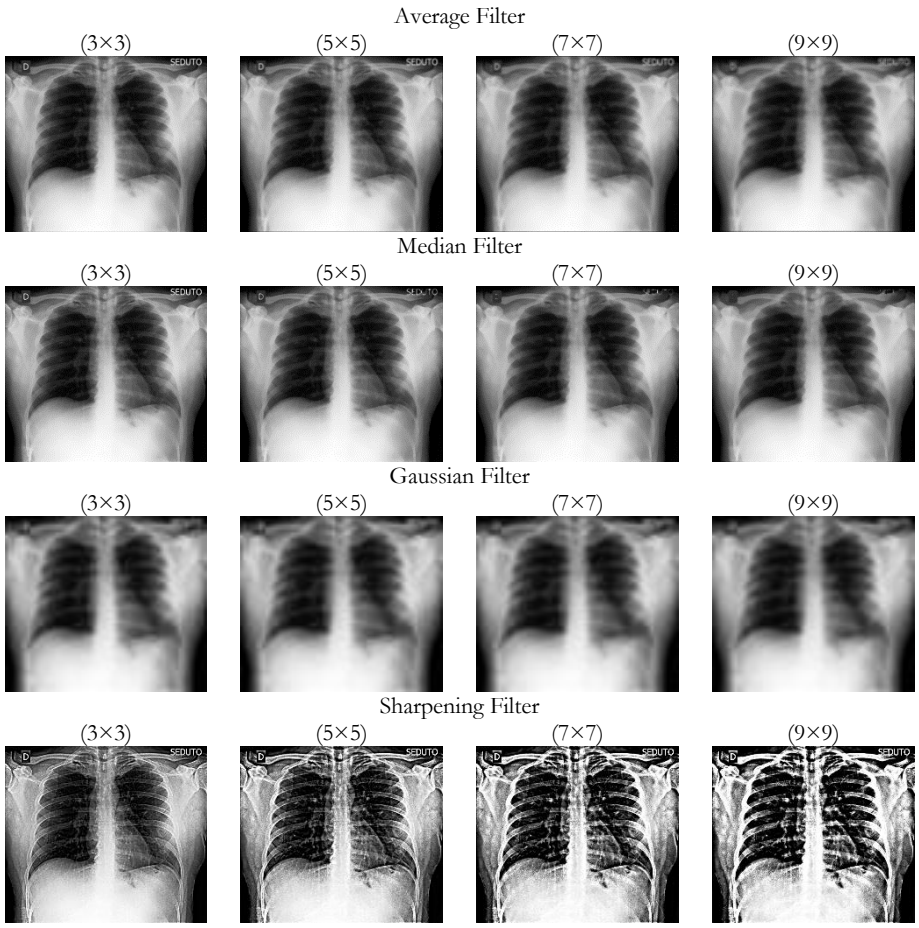


Figure 7. Filtering attacks simulation for the attacked watermarked image.

Table 3. Analysis of geometrical attacks.

Attack	Rotation			
	5°	10°	15°	20°
Extracted Watermark				
BER	0	0	0	0
NC	1	1	1	1
Attack	Scaling			
	0.25	0.5	2.0	4.0
Extracted Watermark				
BER	0	0	0.0002	0
NC	1	1	0.9999	1
Attack	Translation			
	[15, 40]	[15, 50]	[-15, -50]	[-50, 50]
Extracted Watermark				
BER	0	0	0.0003	0.0002
NC	1	1	0.9998	0.9994
Attack	Shearing			
	Fill (0.45)	Fill (0.60)	Fill (0.70)	Fill (0.80)
Extracted Watermark				
BER	0	0	0	0.0003
NC	1	1	1	0.9996

Table 4. Analysis of processing attacks.

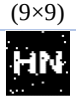
Attack	Average Filter			
	(3×3)	(5×5)	(7×7)	(9×9)
Extracted Watermark				
BER	0	0	0	0
NC	1	1	1	1
Attack	Median Filter			
	(3×3)	(5×5)	(7×7)	(9×9)
Extracted Watermark				
BER	0	0	0. 0003	0. 0005
NC	1	1	0.9998	0.9997
Attack	Gaussian Filter			
	(3×3)	(5×5)	(7×7)	(9×9)
Extracted Watermark				
BER	0	0	0	0.0005
NC	1	1	1	0.9992
Attack	Sharpening Filter			
	(3×3)	(5×5)	(7×7)	(9×9)
Extracted Watermark				
BER	0	0.0004	0.0005	0.0009
NC	1	0.9994	0.9996	0.9993

Table 5 Analysis of filtering attacks.

Attack	**Salt & Peppers**			
	(0.2)	(0.3)	(0.5)	(0.7)
Extracted Watermark				
BER	0	0	0	0.0001
NC	1	1	1	0.9999
Attack	Gaussian			
	(0.2)	(0.3)	(0.5)	(0.7)
Extracted Watermark				
BER	0	0	0	0.0005
NC	1	1	1	0.9997
Attack	Speckle			
	(0.2)	(0.3)	(0.5)	(0.7)
Extracted Watermark				
BER	0	0	0	0. 0002
NC	1	1	1	0.9998

4.3 | Comparative Analysis

We assessed our method's invisibility relative to prior SOTA methods [13, 18, 24, 25, 26], utilizing PSNR and SSIM as standard metrics. Table 6 shows that the proposed scheme had a high SSIM of 0.9999 and a maximum PSNR of 54.45 dB when there were no attacks. This demonstrated its superior invisibility compared to all other tested methods.

Table 6. Invisibility analysis for SOTA methods.

Scheme	**Adaptive CNN [13]**	**Optimized LGBA [18]**	**DWT-CNN [24]**	**Hybrid CNN [25]**	**Powerful CAE [26]**	**Proposed**
PSNR	40.58	46.70	50.9	43.29	36.36	54.45
SSIM	0.9940	----	----	0.9876	0.9760	0.9999

Table 7 judges the durability of the proposed scheme by subjecting the watermarked image to common attacks and comparing the quality of the extracted watermark with prior SOTA methods [14, 15, 16, 17, 18, 19]. We calculated the extracted watermark's opposite NC value for each attack with an average value. Table 7 demonstrates that our method provides superior robustness results. Figure 5 shows the average PSNR value for all compared schemes.

Our method demonstrates remarkable resilience against multiple attack scenarios. Despite multiple attempted assaults, the watermark preserves its exact identity. For nearly assessed assaults with precise criteria, the NC value was 1.0; nevertheless, for other attacks with varying features, it attained acceptable values.

The results underscore the algorithm's significant benefits in complex attack situations, especially in advanced rotation, rescaling, translation, and specific high-intensity filtering attacks. They validate the superiority of our method in watermark retrieval accuracy and exhibit considerable resistance against various attack scenarios compared to other existing techniques.

Table 7. Robustness comparison with SOTA methods.

Attacks	Inception V3-DCT [14]	Henon Map-GoogLeNet [15]	DCT-DarkNet53 [16]	PSO-DnCNN [17]	Optimized LGBA [18]	2D-LACM-CNN [19]	Proposed
Gaussian	0.35	0.86	0.94	0.9380	----	0.9996	0.9999
Salt & Pepper	----	----	---	0.9859	0.672	0.9998	0.9999
JEPEG	0.63	0.69	0.94	0.9734	0.994	0.9996	0.9998
Average Filter	---	----	---	0.9772	0.986	0.9996	1
Median Filter	0.29	0.89	1	0.9761	0.905	0.9996	0.9998
Rotation	0.05	0.91	0.80	0.8672	0.691	0.9992	1
Scaling	0.32	1	1	0.9741	0.989	0.9992	0.9999
Translation	0.39	0.97	0.68	----	----	----	0.9998
Cropping	0.76	0.97	0.84	0.9722	0.988	----	0.9997
Sharping	----	----	----	0.9615	0.988	1	0.9995
Average	0.4066	0.8984	0.8784	0.9584	0.9016	0.9995	0.9998

5 | Conclusions

In this study, we proposed a new robust blind watermarking method for medical images that combines the adaptability and efficiency of CNN in a fusion domain. We first divide the input image into 8x8 non-overlapping blocks for rapid computation and then feed it into the pre-trained ResNet-50 model to extract the stable feature vector. We transmute the extracted feature vector using RDWT to generate the detailed coefficients LL, LH, HL, and HH. We embed the scrambled BW in the selected LL sub-band to enhance robustness and reliability. The embedded watermark is detected in a blind extraction routine without addressing the host image, which leverages the detection capability. Extensive investigations show that our method prevails over prior schemes regarding PSNR, BER, and NC. Finally, our innovative hybrid watermarking method efficiently meets various watermarking security concerns. In the future, we intend to enhance the proposed method by integrating contemporary deep learning techniques with conventional techniques in a swift fusion domain, and we will utilize this integration to broaden its application in medical video authentication.

Acknowledgments

The authorsaregrateful to the editorial and reviewers, aswell as the correspondent author, who offered assistance in the form of advice, assessment, and checking during the study period.

Author Contribution

All authors contributed equally to this work.

Funding

This research has no funding source.

Data Availability

The datasets generated during and/or analyzed during the current study are not publicly available due to the privacy-preserving nature of the data but are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there is no conflict of interest in the research.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

References

[1] Gull, S., Parah, S.A. Advances in medical image watermarking: a state of the art review. Multimed Tools Appl 83, 1407–1447 (2024). https://doi.org/10.1007/s11042-023-15396-9.

[2] S.S. Roy, A. Basu, A. Chattopadhyay, On the implementation of a copyright protection scheme using digital image watermarking, Multimedia. Tools Appl. 79 (2020) 13125–13138, https://doi.org/10.1007/s11042-020-08652-9

[3] Himanshu Kumar Singh, Amit Kumar Singh, "Comprehensive review of watermarking techniques in deep-learning environments," J. Electron. Imag. 32(3) 031804 (29 November 2022) https://doi.org/10.1117/1.JEI.32.3.031804.

[4] Huajie Chen, Chi Liu, Tianqing Zhu, Wanlei Zhou, When deep learning meets watermarking: A survey of application, attacks, and defenses, Computer Standards & Interfaces, Volume 89, 2024, 103830, ISSN 0920-5489, https://doi.org/10.1016/j.csi.2023.103830.

[5] Ruotong Xiang, Gang Liu, Ke Li, Jing Liu, Ziyi Zhang, Min Dang, Zero-watermark scheme for medical image protection based on style feature and ResNet, Biomedical Signal Processing and Control, Volume 86, Part A, 2023, 105127, ISSN 1746-8094, https://doi.org/10.1016/j.bspc.2023.105127.

[6] Tongyuan Huang, Jia Xu, Shixin Tu, Baoru Han, Robust zero-watermarking scheme based on a depthwise overparameterized VGG network in healthcare information security, Biomedical Signal Processing and Control, Volume 81, 2023, 104478, ISSN 1746-8094, https://doi.org/10.1016/j.bspc.2022.104478.

[7] X. Zhang, Q. Su, Y. Sun, et al., A robust and high-efficiency blind watermarking method for color images in the spatial domain, Multimed. Tools Appl. (2023), https://doi.org/10.1007/s11042-023-14479-x.

[8] Hah, T., Batool, A. Triple byte nonlinear component of block cipher and its application in frequency domain watermarking. Multimed Tools Appl 82, 40937–40952 (2023). https://doi.org/10.1007/s11042-023-15125-2.

[9] Gull, S., Parah, S.A. Advances in medical image watermarking: a state of the art review. Multimed Tools Appl 83, 1407–1447 (2024). https://doi.org/10.1007/s11042-023-15396-9.

[10] Tripathi M, Tripathi SP (2013) Rev Med image Watermark Schemes 2(3):1–10.

[11] Haribabu Kandi, Deepak Mishra, Subrahmanyam R.K. Sai Gorthi, Exploring the learning capabilities of convolutional neural networks for robust image watermarking, Computers & Security, Volume 65, 2017, Pages 247-268, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2016.11.016.

[12] Guo, X., Yang, W., Zhang, L. et al. Deep image watermarking with loss-driven modification. Multimed Tools Appl (2023). https://doi.org/10.1007/s11042-023-16809-5.

[13] Mahapatra, Debolina & Amrit, Preetam & Singh, Om & Singh, Amit & Agrawal, Amrit. (2022). Autoencoder-convolutional neural network-based embedding and extraction model for image watermarking. Journal of Electronic Imaging. 32. 10.1117/1.JEI.32.2.021604.

[14] Fan, Y., Li, J., Bhatti, U.A., Shao, C., Gong, C. et al. (2023). A multi-watermarking algorithm for medical images using inception v3 and dct. Computers, Materials & Continua, 74(1), 1279-1302. https://doi.org/10.32604/cmc.2023.031445.

[15] Zhang, W., Li, J., Bhatti, U.A., Liu, J., Zheng, J. et al. (2023). Robust multi-watermarking algorithm for medical images based on Googlenet and Henon map. Computers, Materials & Continua, 75(1), 565-586. https://doi.org/10.32604/cmc.2023.036317.

[16] Li, Dekai, Jingbing Li, Uzair Aslam Bhatti, Saqib Ali Nawaz, Jing Liu, Yen-Wei Chen, and Lei Cao. 2023. "Hybrid Encrypted Watermarking Algorithm for Medical Images Based on DCT and Improved DarkNet53" Electronics 12, no. 7: 1554. https://doi.org/10.3390/electronics12071554.

[17] Amiri, A., Kimiaghalam, B. Robust watermarking with PSO and DnCNN. SIViP 18 (Suppl 1), 663–676 (2024). https://doi.org/10.1007/s11760-024-03182-5.

[18] Vipul Kumar Sharma, Roohie Naaz Mir, An enhanced time-efficient technique for image watermarking using ant colony optimization and light gradient boosting algorithm, Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 3, 2022, Pages 615-626, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2019.03.009.

[19] Darwish, M.M., Farhat, A.A. & El-Gindy, T.M. Convolutional neural network and 2D logistic-adjusted-Chebyshev-based zero-watermarking of color images. Multimed Tools Appl 83, 29969–29995 (2024). https://doi.org/10.1007/s11042-023-16649-3.

[20] Ali, L.; Alnajjar, F.; Jassmi, H.A.; Gocho, M.; Khan, W.; Serhani, M.A. Performance Evaluation of Deep CNN-Based Crack Detection and Localization Techniques for Concrete Structures. Sensors 2021, 21, 1688. https://doi.org/10.3390/s21051688.

[21] F. Ernawan and M. N. Kabir, "A blind watermarking technique using redundant wavelet transform for copyright protection," 2018 IEEE 14th International Colloquium on Signal Processing & Its Applications (CSPA), Penang, Malaysia, 2018, pp. 221-226, doi: 10.1109/CSPA.2018.8368716.

[22] COVID-19 Dataset available at: https://www.kaggle.com/datasets/pranavraikokte/covid19-image-dataset. (Accessed on November 10, 2024).

[23] Brain Tumor Dataset is available at: https://www.kaggle.com/datasets/abhranta/brain-tumor detection-MRI. (Accessed on November 10, 2024).

[24] Avakoli, A., Honjani, Z. & Sajedi, H. Convolutional neural network-based image watermarking using discrete wavelet transform. Int. j. inf. tecnol. 15, 2021–2029 (2023). https://doi.org/10.1007/s41870- 023-01232-8.

[25] Nguyen, Sy & Ha, Kha & Hoàng, Nguyễn. (2020). An Efficient Robust Blind Watermarking Method Based on Convolution Neural Networks in Wavelet Transform Domain. International Journal of Machine Learning and Computing. 10. 675-684. 10.18178/ijmlc.2020.10.5.990.

[26] Sharma, S.S., Chandrasekaran, V. A robust hybrid digital watermarking technique against a powerful CNN-based adversarial attack. Multimed Tools Appl 79, 32769–32790 (2020). https://doi.org/10.1007/s11042.