VFAST Transactions on Software Engineering
https://vfast.org/journals/index.php/VTSE@ 2025, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 13, Number 4, October-December 2025 pp:97-107

Protection and Authentication of DICOM Images with Iris Recognition

Muhammad Zubair[1], **Shaukat Ali**[1*], **Yasir Saleem Afridi**[2]

[1]Department of Computer Science, Islamia College Peshawar, Pakistan; [2]University of Engineering and Technology Peshawar, Pakistan

Keywords: *DICOM Images, Steganography, Watermarking, Security, PSNR, healthcare*

Journal Info:
Submitted:
November 04, 2025
Accepted:
December 05, 2025
Published:
December 30, 2025

Abstract

Protection of medical images over the internet is a challenging task regarding its communication and usefulness. This work proposes a novel mechanism for the protection of DICOM images. The technique provides the facility to embed the iris (image) as a watermark to protect its integrity. After retrieval of the watermark, the mechanism is so robust that it recognizes the iris efficiently and correctly. Similarly, the system protects the Region of Interest (ROI) before the extraction of watermark as it is quite difficult to find volume, visualize or analyze the ROI. The technique not only protects the watermark but also gives the protection to ROI, which may be different in various medical images. Experimental results provide a deep view about the robustness of the technique in real time against both the intentional and unintentional attacks. The empirical results also show that after extraction of the watermark, the system has the capability to accurately find the volume, visualize and analyze the ROI.

***Correspondence author email address:** shaukat@icp.edu.pk
DOI: 10.21015/vtse.v13i4.2277

1 Introduction

A huge communication over internet explores its benefits transforming the world in electronic world. The transmission of the images is used over the internet for better interpretation and healthcare improvement. Although such transmission raises complex issues which include retention, tempering, copyright violation and protection which leads to unbearable consequences [1, 2].To subdue these issues, digital watermarking is a workable solution to dealt these security measures which is suitable choice for copyright protection and tempering [3].

Watermarking is a technique to embed a code or image as a watermark in digital data. This watermark is used to verify the ownership of the digital data owner [4]. Watermark is basically a logo or pattern of bits which reflects a signature or image of authentication [5]. The watermark is embedded in host image, which is the original image, document or content to be transmitted. It is important to embed a watermark in host image while do not affect the quality of the image [6].

Imperceptibility is important for good technique mean that watermark in invisible and the host image do not loss its visual information [7]. Various attacks are applied on watermark image to check robustness level of the technique. Robustness means the survival of the watermark in the host image after attack. Different types of attack are Compression attacks (image compressed), removal attack (removal of watermark without cracking the key) , noise attacks (adding noise), Geometric attacks (rotation, cropping), cryptographic attack, protocol attack and coping attack [8]. These are the parameters on which the robustness and imperceptibility of watermarking techniques are tested and ensured that the watermarking mechanism is resilient to attacks.

Watermarking techniques are categorized into transform and spatial domain watermarks. Spatial domain watermarking requires less computational time and requires minimum hardware for watermarking [9]. In contest of spatial domain, the transform domain watermarking mechanism enriched the properties of robustness, payload, and imperceptibility while the transform domain is more robust by opting the desire properties for advancement, refinement, and overshadow for evaluation. Intentional and unintentional attacks are the set points for those transform domains. There are many transform domain such as Discrete Fourier transform (DFT), Discrete Cosine transformation (DCT), Discrete Wavelet transform (DWT) [10]. These methods ensure the robustness and high imperceptibility than the spatial domain, the computational cost is higher than the spatial domain.

Each transformation technique has some uniqueness in account of the said properties [11], however, every domain have some limitations. To overcome the drawbacks domain transform watermarking, more than one transformation watermarking domains are combined to improve the efficiency [12]. The embedding of watermark is visible or invisible it has certain application now-a-days the invisibility gives stratification to owner for protection and authentication, SVD provide a chance to embedded in V or D for invisibility and robustness [13, 14].

Different domain has different properties which are important against different attacks, like frequency Fourier transform (FFT, FRFT) is rotation invariant [14], but not resist against noise attack effectively. Discreet wavelet domain introduced for robustness and imperceptibly but discreet wavelet transform (DWT) techniques is not resists against geometrically attacks.

The medical watermarking techniques not only authenticate the image but it also secures the image from manipulation and tempering. Medical images manipulation and authentication are more threatening, because it directly links with life. To protect life, we need secure communication for our medical data [15, 25]. Medical data has many types, however, the data we deal with is DICOM (Digital Imaging and Communication in Medicine). A single DICOM consists of a header and image data. Header consist of patient information, scan types and image dimension, while image data may be in compressed or in uncompressed form [16].

Zain et al [17] proposed a technique of reversible watermarking technique for DICOM series. The technique has high imperceptibility but do not resists against mentioned attacks and they neglecting the quality of the watermark.

Tan et al [18] proposed a fully reversible watermarking technique in transform domain. The technique uses dual tree complex wavelet transform for embedding the watermark. The technique has high imperceptibility but the technique failed to recovered full watermark.

Qeraishi et al. [19] proposed watermarking hybrid technique to authenticate and hide data in transform domain. The method protected medical images, however, this method failed against various attacks. It important during that era was DICOM series watermarking in transform domain.

Das et al. [20] proposed technique of fragile watermarking for DICOM images. ROI crops from NROI, the watermark embeds in ROI and then added to NROI to make full watermarked image. Since, the technique is fully fragile, therefore, it is unable to recover full watermark.

Thanki et al. [21] proposed a technique for the protection of medical images in different compressed format. The technique qualifies many tests against the various attacks but the technique does not recover full watermark.

The problem with existing technique is that it has lacking the robustness in the real time embedding and regeneration at the receiving side. Similarly, the performance during the watermark embedding and extraction is also slow. This article proposes a robust digital DICOM Image watermarking technique developed in the spatial domain-based with tested threshold according to Human Visual System. The Host image DICOM Image and watermark image (Iris) combine in the real time. The embedded intensities from DICOM series images selected by a manual technique from a single slice and then applied to a series, which pledge the robustness, watermark recognition and imperceptibility after being recovered or extracted. The embedding process with threshold value is tested as per the Human Visual System(HVS). Normalized correlation and peak signal to noise ratio are the performance metrics commissioned for comparing the different watermarking techniques. The host image (DICOM image) is tested by employing both the intentional and unintentional attacks. Experimental results manifested that the technique not only robust against different attacks but also successfully recognized the watermark.

The novelty of the proposed technique is summarized as follows:

- The proposed technique is for DICOM series of images. It provides opportunity in real time to embed watermark in series of images and after extraction the watermark is recognized.
- After the extraction of the watermark (iris) it is recognizable through iris recognition system.
- The RPSNR is calculated for watermark(iris).
- The proposed technique not only focused on recovered image but it also satisfies the extracted watermark at recognition level.

2 Proposed Methodology

The following steps are used to embed, extract and recognize the watermark.

2.1 Embedding

The proposed technique takes series of DICOM image $\mathbf{D}_H^Z$ Which contain suitable slice and are selected for the first manual cropping and pointing the Region of Interest (ROI).

$S_H = (S^{i+3} + S^{n-3})/2$

The ROI is selected manual by defining the coordinates of the tumor estimated location by human eye R_H. Segmentation is applied for the sake of isolating the selected Region of Interest (ROI) and non-region of interest (NROI).

The manual segmentation of ROI from the DICOM image is conducted by using four clicks as shown in figure 1. The area inside the click remains in its original state while the outside intensities become zero.

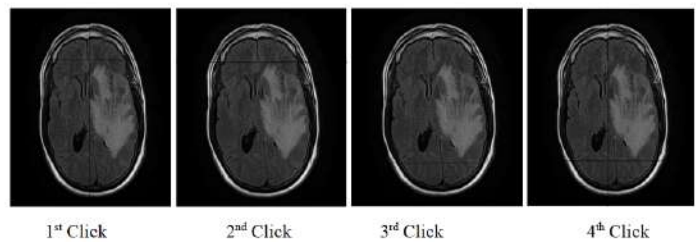


Figure 1. Segmentation of ROI from the DICOM Image

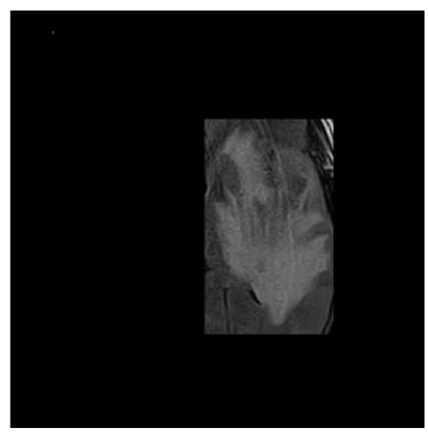


Figure 2. Region of Interest(ROI)

For region of non-interest we subtract the region of Interest R_H from the original selected slice S_H

$$N_H = S_H - R_H$$

The coordinates of the segmented (ROI) and area of the ROI R_H of selected slice S_H applied on all DICOM series of images D_H^S to segment the (ROI) R_H^D from all the slices of the DICOM series. The biometric iris is taken

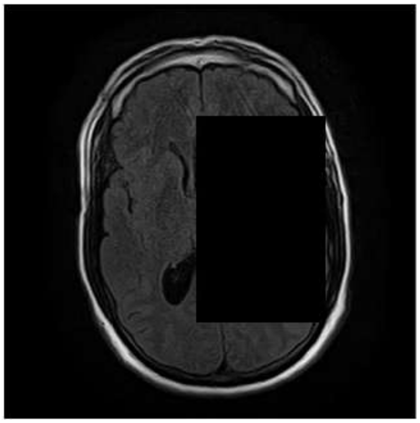
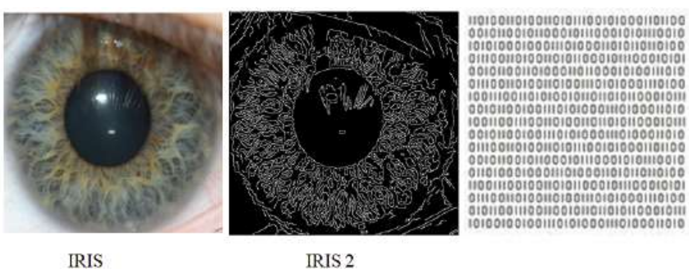


Figure 3. Region of non-interest (NROI)

as a watermark I_W, the watermark resize according to the area of the ROI R_H of selected slice S_H The watermark is further encrypted through a secret key K_W and the encrypted watermark is obtained K_W^I.



The ROIs R_H^D of the series of DICOM images D_H^S is combined with the encrypted watermark with a tested scaling factor to get watermarked region of interest of DICOM series of images R_W^D.

Non-region of interest (NROI) series of images combined with watermarked Region of Interest of DICOM series of images R_W^D as per defined coordinates and areas to get watermarked DICOM images series W_H^D.

The entire embedding process is shown diagrammatically in figure 6 , similarly, the algorithmic steps are given in algorithm 1.

2.2 Extraction and Recognition of the Watermark

The process of extraction is also in real-time, the series of watermarked DICOM images is taken and then an automatic segmentation technique is used

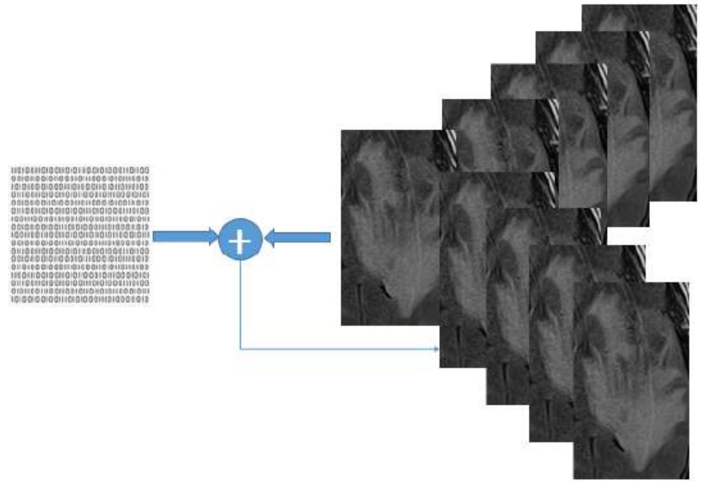


Figure 4. Embedding of Iris in ROI

for the segmentation of ROIs from the DICOM images. The size and coordinates are specified; therefore, the watermarked ROIs are easily segmented from the whole DICOM series. The segmented watermark ROIs are then processed for the extraction of watermark from the watermarked ROIs. The watermark then multiplies with the multiplicative inverse of the scaling factor to achieve the targeted watermark for recognition. Due to spatial domain watermarking and 16 bit intensities of the DICOM image the watermark are easily extracted.

The watermarked DICOM Series are received W_H^D, the images automatic segmentation is applied to extract the ROIs R_H^D from the NROIs N_H. The encrypted watermark K_W^I is separated from the Watermark ROIs R_H^W to get R_H. The encrypted watermark is decrypted by using decryption key K_W to obtain the original watermark D_H^W.

Now the proposed methodology has three possibilities to be going on.

1. The recognition of the watermark and retrieving of information from database through existing techniques.
2. The user can take the DICOM images and ended up the entire system. It also has the flexibility.
3. The proposed technique has the capability to visualize the tumor, brain in three dimensions, volume calculation of the tumor and brain, and clas-

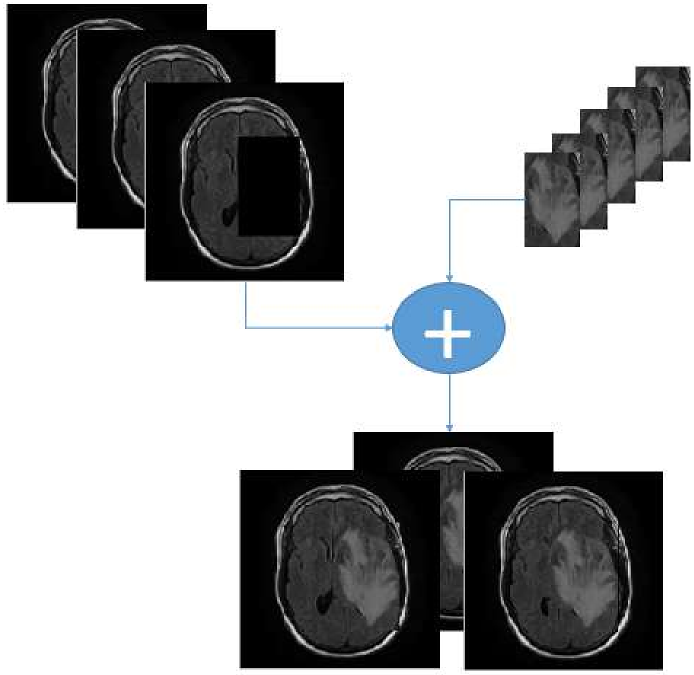


Figure 5. Combining the NROIs and Watermarked ROIs

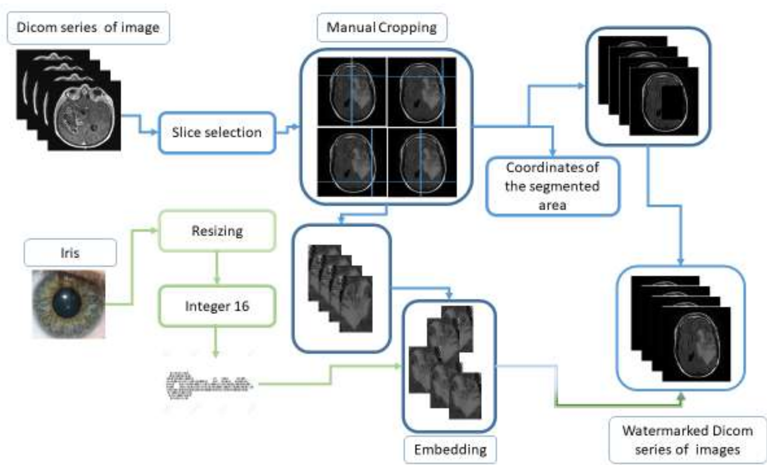


Figure 6. Illustration of the watermark embedding procedure

sification of the tumor to give report either it benign or malignant.

In first possibility, the entire proposed system is responsible to recognize the watermark (Iris) by taking the original watermark D_H^W as input for recognition software. It produces the DICOM images D_H as output to by combining extracted ROIs R_H^D and segmented N_H.

$$D_H = R_H^D + N_H$$

The DICOM images is used for the future processing or as an output can it be utilizing according to the needs of radiologist or patient. Therefore, the proposed system is used for image protection and authentication simultaneously. Second possibility, the proposed system has the capability to recover DICOM series of images and use it for protection only. DICOM series of image is obtained through above mentioned procedure.

Algorithm 1. Watermark Embedding Algorithm

Input: Series of DICOM Images D^{SH}, Watermark I_W, Secret Key K_W, Filter for Host Image F_{I_H}
1. Select a series of DICOM as a Host Images D^S_H
2. Select a series of DICOM as a Host Images S_H Where $S_H = (S_{i+3} + S_{i-3})$
3. Crop Region of Interest (ROI) R_H
4. Apply segmentation automatically on series of images D^S_H according to the area and coordinates of ROI R_H of selected slice S_H to get region of interest of all DICOM images R^D_H
5. Resize the Iris as watermark I_W according the area of ROI R_H of selected slice S_H
6. Encrypt (I_W) using key K_W, to generate K^I_W, where K^I_W is the encrypted watermark
7. Embed the watermark to the series of region of interest R^W_H
8. Region of interest of series of DICOM images combine with non-region of interest NROI to form watermarked DICOM images series W^D_H

Return: Watermarked DICOM Images W^D_H

The third possibility finalize the proposed system as a unique and full version for protection, authenticity, 3D visualization, and volume calculation of brain and tumor and class prediction for the tumor. This facility optimized the proposed system according to the demand. The authenticity is validated in account of recognition of watermark through existing techniques. The protection demands the DICOM images in the form of usability. The proposed system segmented the tumor from DICOM series of images through K-Mean Algorithm.

The DICOM series of images D^S_H is converted into one-dimensional array A^S_H for k-Mean 3D implementation. It is required to define the number of cluster for the segmentation of the DICOM series of images. Four cluster are defined in this case, because the number of interested region also same in numbers. The cluster one is the Brian area of the DICOM series of images C^1_B, the cluster two is tumor in series of images C^2_T, the cluster three is the skull bone in the series of images C^3_S, and the cluster four is the background of the DICOM images C^4_N.

$$J = \sum_{j=1}^{k} \sum_{i=1}^{n} \left\| x_i^{(j)} - c_j \right\|^2 \quad (1)$$

Now we reshape the one-dimensional array A^S_H into DICOM series of image which has the four defined clusters.

Now we segment the DICOM series of images according to the four clusters. The entire extraction process of the watermark at receiving side is diagrammatically shown in figure 7 and the algorithmic steps are given in algorithm 2.

3 Experimental Results

The proposed technique is assimilated through various analyzation's parameters. The DICOM images of the human bodies are tested simultaneously in various groups, which have been taken from eight classes of various body organs. These images have been examined through the proposed technique for its optimality. Series of DICOM images have been taken in real-time and Iris watermark is embedded in it. The performance the proposed technique evaluated with the comparison to its related state of the art techniques which are proposed by Mei [22], li [23], li [24] Ledya [26] and [27]. For the sack of simplicity, we will use Mei 2012, Li 2013, Li 2014 Ledya 2023 and Eko 2024 in rest of discussion in this paper. The DICOM images are used for comparison in account of evaluation of the proposed technique. In order to verify the robustness, we manipulate the images before embedding the watermark and calculated the volume of both brain, tumor and suggest class of tumor. The technique is tested in MATLAB2016a and run on laptop with Core

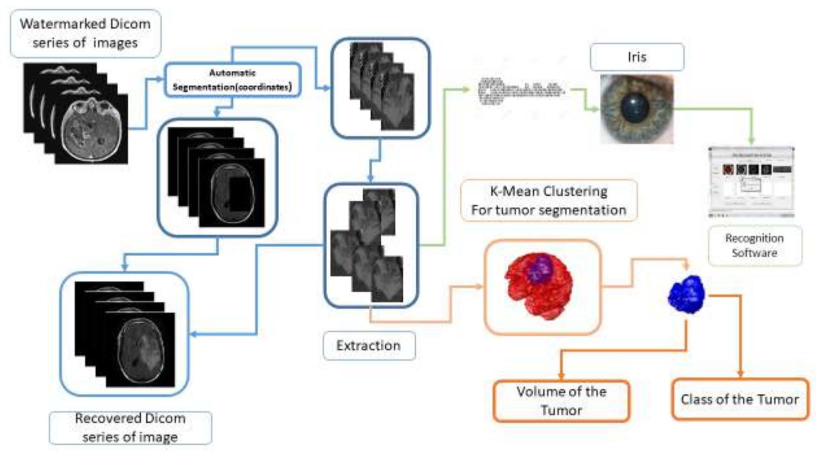


Figure 7. Illustration of the watermark extraction and recognition procedure.

i5 processor, 4GB RAM and Windows 10 as operating system. In order to justify the result, the best result is highlighted in bold and italic among the results.

3.1 Imperceptibility

In invisible watermarking technique, the inserted watermark is undetectable. The transparency depends upon the property of the Human Visual System. If the original DICOM series of images are mutually same with watermarked DICOM series of images, the technique is considered as imperceptible. To evaluate the imperceptibility of the technique both subject and objective processes are tested. The common objective analysis of the imperceptibility is through Peak Signal Noise Ratio (PSNR). The PSNR is calculated and compared with the state-of-the-art techniques, and the results are shown in Table 1. It is clear from the table 1 that the proposed technique has the dominancy over the existing techniques. While the performance of Mei 2012 is low as in comparison table. In addition, the PSNR of the watermark of the proposed technique is computed for the series of DICOM images. The PSNR is obtained from the mutual similarity between the original iris watermark and recovered watermark after extraction. The PSNR is enlisted in Table 2 which shows that the watermark is suitable for the input of recognition. If the PSNR is less than the 55.00 db, it is difficult to recognize it through the existing techniques. However, it is clear from the table 2 that the PSNR value is higher than 60, therefor, the watermark can easily be recognized through the proposed technique.

Table 1. PSNR of State-of-the-Art and Proposed Techniques

S.No	DICOM Sets	Mei 2012	Li 2013	Li 2014	Ledya 2023	Eko 2024	Proposed
1	001	51.83	53.47	55.65	55.6	58.7	60.45
2	002	52.49	54.19	56.35	56.1	58.5	59.99
3	003	50.00	54.50	56.45	55.9	68.6	60.89
4	004	52.14	53.68	55.34	55.8	57.8	60.87
5	005	51.87	53.75	56.68	56.2	58.3	59.95
6	006	52.45	54.95	55.78	55.8	58.5	60.12
7	007	52.78	54.86	56.78	56.4	57.9	60.13
8	008	52.87	54.65	55.75	56.3	58.3	60.45
Average		**52.05**	**54.25**	**56.09**	**56.1**	**58.7**	**60.36**

Table 2. PSNR of Recovered Watermark

S.No	Iris Watermark	Proposed
1	01	62.95
2	02	63.99
3	03	61.89
4	04	62.56
5	05	61.45
6	06	62.12
7	07	63.24
8	08	62.54
Average		**62.59**

Algorithm 2. Watermarked Extraction Algorithm

Input: Received Image W_H^D and key K_W
1. Select the DIOCM Images W_H^D and parameters extraction.
2. Apply automatic segmentation on DICOM Image W_H^D
3. Extract the region of Interest ROI R_H^D from watermarked DICOM images W_H^D
4. Extract the watermark K_W^I from region of Interest ROI R_H^D
5. Apply decryption on watermark K_W^I the resultant is I_W
6. The Iris watermark I_W is recognized through recognition software.
7. Combined the R_H^D with the non-region of interest NROI for recovering the DICOM series of Images DR_H^D
8. Apply k-mean on region of interest ROI R_H^D for tumor segmentation T_H^D
9. Apply 3D visualization on T_H^D
10. Calculate the volume of tumor V_T^D
11. Classify the tumor by taking it roundness of the tumor R_T^D
12. Shows result P_T^R

Output: Host Image D_H, Watermark I_W, Tumor class P_T^R, Volume of the tumor V_T^D 3D image of the T_H^D

3.2 Robustness

The proposed technique is robust against different manipulation and distortion in the original images. It is categorized with respect to recognition of the watermark iris after extraction, the volume calculation and classification of the tumor. In order to justify the volume calculation and tumor classification, the volume of the tumor and brain is computed before and after embedding the watermark as shown in Table 4.

It is clear from the results that it is difficult to calculate the area of tumor accurately, similarly, embedding the watermark is indirectly proved that the proposed technique is strongly committed in the protection of the DICOM images. The volume of brain and tumor are calculated accurately after extraction watermark. The volume of the brain and tumor is absolutely equal, before embedding and after extraction of the watermark. The volume calculated after the embedding and before extraction have a visible difference which is shown in table 4. The visualization is also possible after extraction as in mentioned in Table 3.

Recognition of watermark is also a valid property for the robustness. The Recognition rate of the watermark The visual result of the recovered DICOM series of images and recovered watermark are shown in Table 3. 3D-visualization is also possible after the extraction of the watermark, the proposed technique secures and protects the voxel intensities of ROI of the DICOM series for its robustness and optimality. To obtain clear structural view, brain and tumor is visualized. The results are shown in Table 5 and Table 3 before embedding and after extraction of watermark, which guarantees the robustness of the proposed technique.

Table 3. Visual Recovered Watermark and DICOM Image

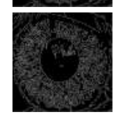
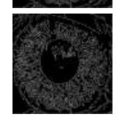
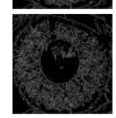
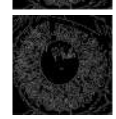
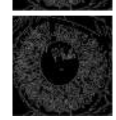
S.No	DICOM Set	Recovered DICOM Image	Recovered Watermark
1	001		
2	002		
3	003		
4	004		
5	005		
6	006		
7	007		
8	008		

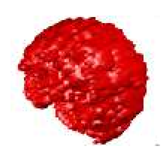
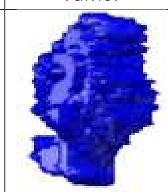
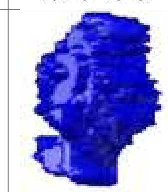
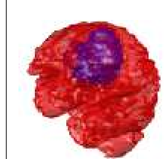
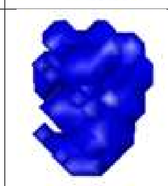
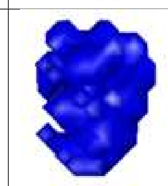
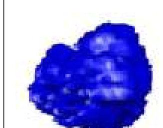
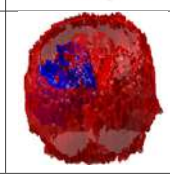
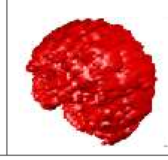
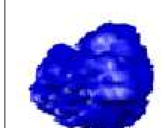
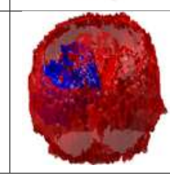
Table 4. Brain and Tumor Volumes Before Embedding, After Embedding, and After Extraction

S.No	Total Voxel	Before Embedding		After Embedding		After Extraction	
		Brain Volume (mm³)	Tumor Volume (mm³)	Brain Volume (mm³)	Tumor Volume (mm³)	Brain Volume (mm³)	Tumor Volume (mm³)
1	7,782,400	1,407,700	28,373	1,407,700	78,345	1,407,700	28,373
2	2,419,200	823,650	52,544	823,650	85,936	823,650	52,544
3	7,782,400	953,800	58,426	953,800	73,456	953,800	58,426
4	2,544,640	837,270	76,482	837,270	95,876	837,270	76,482

Table 5. Voxel Statistics Before Embedding and After Extraction

Data Set	Slices	Voxel Size	Brain Voxel (Before)	Tumor Voxel (Before)	Total Voxel (After)	Brain / Tumor (After)
1	28	0.7088	1,345,697	20,342	1,366,039	1,345,697 / 20,342
2	19	1.5509	828,958	82,432	911,390	828,958 / 82,432
3	17	2.5830	318,871	104,943	423,814	318,871 / 104,943
4	28	2.0008	283,626	32,075	315,701	283,626 / 32,075

Table 6. A 3D-visualization of the Brain and Tumor

Data set	No. of slices	Voxel Size	Before Embedding			After Extraction		
			Brain	Tumor	Brain and Tumor	Brain voxel	Tumor voxel	Brain and Tumor
1	28	0.7088						
2	19	1.5509						
3	17	2.5830						

4 Conclusion

This work is for real-time domain; it leads the watermarking field into a new era. The proposed watermarking technique guides the watermarking embedding process through human known security system, which are unique than existing techniques. It enhances the level of security and gives a full input for authentication and recognition. The proposed work not only focuses the medical image noiselessness but also the watermark, which is a key factor. It is the output of the extraction and input to recognition. The experimental results show the robustness against various attacks. Thus, the proposed technique seems better in resolving the problem of authentication and recognition.

Author Contributions

Muhammad Zubair: Conceptualization, Methodology, Software **Shaukat Ali**: Data curation, Writing-Original draft preparation,Visualization, Investigation, Supervision. **Yasir Saleem Afridi**: Software, Validation, Writing- Reviewing and Editing

Compliance with Ethical Standards

It is declared that all authors don't have any conflict of interest. It is also declare that this article does not contain any studies with human participants or animals performed by any of the authors. Furthermore, informed consent was obtained from all individual participants included in the study.

References

[1] A. Benyoucef *et al.*, "High-capacity DWT-SVD watermarking for MRI images embedding MITR medical information," *Results in Engineering*, p. 105795, 2025.

[2] A. F. Qasim *et al.*, "Assessment of perceptual distortion boundary through applying reversible watermarking to brain MR images," *Signal Processing: Image Communication*, vol. 70, pp. 246–258, 2019.

[3] A. M. A. Awwad, "A novel zero-watermarking scheme based on two-dimensional cellular automata," *Multimedia Tools and Applications*, vol. 83, no. 23, pp. 62829–62851, 2024.

[4] A. F. Qasim, F. Meziane, and R. Aspin, "Digital watermarking: Applicability for developing trust in medical imaging workflows—A state-of-the-art review," *Computer Science Review*, vol. 27, pp. 45–60, 2018.

[5] M. S. Moad, M. R. Kafi, and A. Khaldi, "A wavelet-based medical image watermarking scheme for secure transmission in telemedicine applications," *Microprocessors and Microsystems*, vol. 90, p. 104490, 2022.

[6] A. Singh and M. K. Dutta, "A robust zero-watermarking scheme for tele-ophthalmological applications," *Journal of King Saud University–Computer and Information Sciences*, vol. 32, no. 8, pp. 895–908, 2020.

[7] W. Etoom and A. Al-Haj, "A robust and imperceptible watermarking method for 3D DIBR images," *Multimedia Tools and Applications*, vol. 81, no. 20, pp. 28165–28182, 2022.

[8] C.-P. Wang, X.-Y. Wang, and Z.-Q. Xu, "Geometrically invariant image watermarking based on fast radial harmonic Fourier moments," *Signal Processing: Image Communication*, vol. 45, pp. 10–23, 2016.

[9] B. P. Devi, K. M. Singh, and S. Roy, "New copyright protection scheme for digital images based on visual cryptography," *IETE Journal of Research*, vol. 63, no. 6, pp. 870–880, 2017.

[10] A. Y. Altay and G. Ulutaş, "Self-adaptive step firefly algorithm-based robust watermarking method in DWT-SVD domain," *Multimedia Tools and Applications*, vol. 80, no. 15, pp. 23457–23484, 2021.

[11] G. Bhatnagar and Q. M. J. Wu, "A new logo watermarking based on redundant fractional wavelet transform," *Mathematical and Computer Modelling*, vol. 58, no. 1–2, pp. 204–218, 2013.

[12] A. Taheri and S. M. Boroujeni, "A new high robust digital image watermarking algorithm using discrete wavelet transform and recurrent neural network," in *Proc. 9th Iranian Conf. on Intelligent Systems (ICIS)*, IEEE, 2024.

[13] Z. Zainol *et al.*, "Hybrid SVD-based image watermarking schemes: A review," *IEEE Access*, vol. 9, pp. 32931–32968, 2022.

[14] Y. Zhang, H. Wang, and J. Zhao, "Eliminating orthonormal constraints of SVD to guarantee full retrievability of blind watermarking," *Multimedia Tools and Applications*, vol. 83, no. 9, pp. 25365–25391, 2024.

[15] T.-Y. Fan, H.-C. Chao, and B.-C. Chieu, "Lossless medical image watermarking method based on significant difference of cellular automata transform coefficient," *Signal Processing: Image Communication*, vol. 70, pp. 174–183, 2019.

[16] P. K. Mannepalli *et al.*, "A robust blockchain-based watermarking using edge detection and wavelet transform," *Multimedia Tools and Applications*, vol. 84, no. 14, pp. 12739–12763, 2025.

[17] J. M. Zain, L. P. Baldwin, and M. Clarke, "Reversible watermarking for authentication of DICOM images," in *Proc. 26th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, IEEE, 2004.

[18] C. K. Tan *et al.*, "Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability," *Journal of Digital Imaging*, vol. 24, no. 3, pp. 528–540, 2011.

[19] O. M. Al-Qershi and B. E. Khoo, "Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images," *Journal of Digital Imaging*, vol. 24, no. 1, pp. 114–125, 2011.

[20] S. Das and M. K. Kundu, "Effective management of medical information through ROI-lossless fragile image watermarking technique," *Computer Methods and Programs in Biomedicine*, vol. 111, no. 3, pp. 662–675, 2013.

[21] R. Thanki *et al.*, “An efficient medical image watermarking scheme based on FDCuT–DCT,” *Engineering Science and Technology, an International Journal*, vol. 20, no. 4, pp. 1366–1379, 2017.

[22] M. Yu *et al.*, “A new stereo image watermarking method for 3D media,” *Procedia Engineering*, vol. 29, pp. 2399–2404, 2012.

[23] X. W. Li and S. T. Kim, “Optical 3D watermark-based digital image watermarking for telemedicine,” *Optics and Lasers in Engineering*, vol. 51, no. 12, pp. 1310–1320, 2013.

[24] X. W. Li and S. T. Kim, “An improved cellular automata-based digital image watermarking scheme combining pixel-wise masking and 3D integral imaging,” *Optics Communications*, vol. 319, pp. 45–55, 2014.

[25] M. Papaioannou *et al.*, “A survey on security threats and countermeasures in internet of medical things (IoMT),” *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 6, 2022.

[26] Novamizanti, Ledya, Andriyan Bayu Suksmono, Donny Danudirdjo, and Gelar Budiman. "Robust and imperceptible watermarking on medical images using coefficient pair modification." IIUM Engineering Journal 24, no. 1 (2023): 88-105.

[27] Harshavardhan Sai, B., D. Sheela, R. Mahaveerakannan, and K. Sudhakar. "Improvement of PSNR for Digital Image Watermarking Using Discrete Wavelet Transform in Comparison with Discrete Cosine Transform Algorithm." In International Conference on Computing and Communication Networks, pp. 423-435. Singapore: Springer Nature Singapore, 2024.