International Journal of Electrical and Computer Engineering (IJECE)
Vol. 15, No. 6, December 2025, pp. 5770~5781
ISSN: 2088-8708, DOI: 10.11591/ijece.v15i6.pp5770-5781

Integrity verification of medical images in internet of medical things for smart cities using data hiding scheme

Kilari Jyothsna Devi[1], Ravuri Daniel[1], Bode Prasad[2], Mohamad Khairi Ishak[3], Dorababu Sudarsa[4], Pasam Prudhvi Kiran[5]
[1]Department of Computer Science and Engineering, Prasad V Potluri Siddhartha Institute of Technology, Vijayawada, India
[2]Department of Information Technology, Vignan's Institute of Information Technology, Visakhapatnam, India
[3]Department of Electrical and Computer Engineering at the College of Engineering and Information Technology, Ajman University, Ajman, United Arab Emirates
[4]Department of Computer Science and Engineering, Koneru Lakshmaiah University, Guntur, India
[5]Department of Computer Science and Engineering (IoT), R.V.R. and J. C. College of Engineering (A), Guntur, India

Article Info

Article history:

Received Mar 5, 2025
Revised Jul 29, 2025
Accepted Sep 16, 2025

Keywords:

Data hiding scheme
Internet of medical things
Medical image watermarking
Tamper detection
Tamper recovery

ABSTRACT

As technology has advanced, the internet of medical things (IoMT) has become incredibly useful. It is used to transmit a wide variety of medical images. Sensitive patient data may be altered during transmission or subject to illegal access. To overcome all of these challenges and preserve the integrity of medical images while transmission over IoMT, a blind region-based data concealing approach called medical image watermarking (MIW) is suggested. The region of interest (ROI) and region of non-interest (RONI) are the two sections that make up the medical image. The aim of the suggested MIW technique is to prevent transmission-related manipulation of medical image ROI. To provide high imperceptibility and resilience, confined integrity verification and recovery bits (CIVRB) bits are embedded in the RONI using hybrid integer wavelet transform–singular value decomposition (IWT-SVD). According to the experimental results, the suggested system is highly imperceptible (average peak signal-to-noise ratio (PSNR)=56 dB), robust (average NC=0.99), and exhibits integrity verification accuracy of over 98% against a variety of image processing attacks. In terms of several watermarking properties, the proposed technique performs over state-of-the-art schemes. This method offers a dependable framework for protecting medical images in real-time IoMT applications and is suitable for smart healthcare environments.

Corresponding Author:

Mohamad Khairi Ishak
Department of Electrical and Computer Engineering at the College of Engineering and Information Technology, Ajman University
University Street-Al Jerf 1-Ajman, United Arab Emirates
Email: m.ishak@ajman.ac.ae

1. INTRODUCTION

The internet of medical things (IoMT), in which every medical gadget is connected to the internet and under the supervision of medical professionals, is the future of healthcare systems. By using internet of things (IoT) devices to provide health data with healthcare teams, remote healthcare monitoring aids in the tracking of patients' health conditions [1]. IoMT offers a dependable channel for sending patient records and medical imaging in the healthcare industry. Although a variety of medical data and images can be sent, there are still concerns over the transmission process. When posted to a public network, medical images may be changed or altered. The medical professional could arrive at an incorrect diagnosis as a result [2]. Therefore,

it is vital to preserve the validity of medical images across communication. In the process of transmission of medical images, integrity decides whether the digital medical image is faultless or altered with [3]. To maintain integrity, data masking techniques such as watermarking have been widely utilized [4]. Medical image watermarking (MIW) is known to be an effective method of insuring integrity, authenticity, and copyright. A medical image is often divided into two diagnostic regions: the region of interest (ROI), which is required for diagnosis, and the region of non-interest (RONI), which is not necessary for diagnosis. To maintain ROI integrity and greater imperceptibility, add the watermark in the RONI [5]. To guarantee their integrity and identify any alterations, medical images are examined while they are being transmitted [6]. It is possible to retrieve and use watermarks that are part of RONI to identify instances of manipulation [7]. Most studies recommended watermarking with ROI. There are many disadvantages to using ROI for watermarking, including the low content change that could result in inaccurate diagnosis and even patient death [8]. Therefore, it is essential to accurately obtain the ROI, even for minimal tampering. Watermark embedding in this area is always forbidden due to the significance of ROI. Usually, the less important part of RONI contains the tamper and recovery bits.

Confined integrity verification and recovery bits (CIVRB) were created from the ROI section of the suggested system to preserve ROI integrity. Additionally, a hybrid integer wavelet transform-singular value decomposition transform is used to blend CIVRB data into RONI to guarantee its robustness, validity, and integrity. Lastly, as demonstrated in section 5.3, metrics like accuracy, true positive rate, and false positive rate are used to assess the integrity of the suggested scheme. Additionally, the proposed model is contrasted with the most advanced models in terms of robustness and imperceptibility features as outlined in section 5.5. The primary benefits and driving forces behind the suggested paradigm, as outlined in section 2. The subsequent portions of this work are organized as follows: section 2 shows contributions and motivation of the proposed model, section 3 analyses relevant work, section 4 details the suggested method in depth, section 5 gives a discussion of experimental outcomes, and section 6 concludes with potential enhancements.

2. CONTRIBUTIONS AND MOTIVATION OF THE SUGGESTED MODEL

The motivation behind the proposed system as:

- To guarantee the integrity of medical images sent across IoMT networks. And to enable safe embedding in non-critical locations (RONI) while preventing tampering with diagnostic content (ROI).
- To provide accurate tamper detection and localized recovery using embedded data without compromising diagnostic quality.
- To make MIW more resilient to different image processing attacks and imperceptible
- Improve detection accuracy, recovery performance, and visual quality compared to conventional watermarking systems.

The main contributions of the proposed model as described:

- Superior precision of ROI inspection and retrieval: to increase identify tampering and restoration accuracy, produce localized bits (CIVRB) for each 3×3 non-overlapping ROI block. High peak signal-to-noise ratio (PSNR) values for several medical image modalities demonstrate that the proposed technique detects tampering with higher than 98% accuracy and recovers ROIs with high visual quality. We can also expect better imperceptibility this way.
- Increased visibility of ROI: Any modifications to ROI could lead to an inaccurate diagnosis because it is essential for diagnosis. In order to avoid this, the suggested technique does not use ROI for the embedding process. Additionally, RONI is used for the recovery bits embedding procedure and ROI tamper detection in order to preserve integrity.
- Excellent resilience: The use of hybrid integer wavelet transform–singular value decomposition (IWT-SVD) makes the proposed method very resistant against geometric, non-geometric, and hybrid attacks.

3. LITERATURE REVIEW

Several researches offered a variety of data-hiding mechanisms, including cryptography, steganography, and watermarking, for secure exchange of medical images in IoMT. Because it streamlines image transfer without sacrificing critical aspects such as security, integrity, authenticity. MIW has garnered the most interest of these. Over the last fifteen years, research on this MIW has made significant progress, utilizing methodologies from the geographical, frequency, and mixed domains. The watermark can be added directly to the image using spatial domain techniques like least significant bit (LSB) and pixel value difference. although it is vulnerable to some image processing attacks [9]. Therefore, the strategies outlined in [10] proposed inserting the watermark at a frequency sub-band utilizing frequency-domain techniques as direct discrete wavelength transform (DWT) and discrete cosine transform (DCT), respectively. Although these methods strengthen the image, they also make it more challenging to conceal the watermark. However,

it is easier to conceal the image when the watermark is inserted at a higher frequency range, but this comes at the expense of imperceptibility [11], [12]. The hybrid transformations DCT-SVD, DWT-HMD-SVD, and IWT-SVD were employed in the techniques proposed in [13]–[15] to overcome this problem and provide good imperceptibility without sacrificing the image's resilience. But when it comes to safeguarding data integrity, they are inadequate. Localized tamper detection and recovery techniques were implemented by the schemes suggested in [16], [17]. However, it has been revealed that tamper detection and recovery could be more accurate. Schemes in [18] proposed watermarking systems with improved tamper detection and localization accuracy, however they used the entire image to contain tamper recovery bits. This has an impact on the ROI's visual quality and also modifies the ROI portion.

From the literature review, it was observed that many previous methods embedded watermark data directly into the entire medical image or even the ROI, which risked degrading diagnostic quality. While some used hybrid techniques like DWT-SVD or DCT-based approaches for robustness, they lacked efficient tamper detection, precise recovery, or introduced high computational overhead. The findings of this study contribute to the pool of expertise by presenting blind, region-based MIW systems with integrity verification. The watermark of the proposed MIW system is inserted in the medical image's non-diagnostic section, known as RONI. To ensure high robustness, the RONI component of the medical image's watermark is integrated with a hybrid IWT-SVD transform. Prior research has focused on tackling important imitations. Section 4 below also describes the methodology behind the proposed paradigm.

4. METHODOLOGY

A region-based image transmission technique for IoMT is provided, which ensures fidelity testing, high reliability, and concealment. The scheme includes a test medical image (M_{img}) with size X×Y. The suggested technique is divided into five steps, which include: i) ROI and RONI splitting, ii) create CIVRB bits, iii) CIVRB embedding and extraction, and iv) confined integrity verification.

4.1. ROI and RONI splitting

From the cover picture (M_{img}), the ROI and RONI components have been separated. Partitioning is done by hand in this technique. A healthcare professional or practitioner is required to record the ROI during the manual process. M_{img} is divided into ROI and RONI, as seen in Figure 1(a).

4.2. Generation of CIVRB bits

The CIVRB bits are created during transmission to guarantee the integrity of the ROI. Any image manipulation is detected using CIVRB. The ROI is also recovered using the CIVRB if any interference is found. The process of CIVRB bits generation as, divide ROI into Three-by-three independent blocks (B). If the last block size is not 3×3, fill the pixel position values with zero padding. Then apply algorithm 1 on B to generate RB.

Algorithm 1. RB generation

Require: B (3×3 ROI non-overlapping block).

Ensure**:** RB of size 57 bits.

1. Use the reference provided in (1) and divide each pixel value in B by 8 to round to the next whole number and store the resultant values into a block called B_1.

$$\sum_{i=1}^{3}\sum_{j=1}^{3} B_1\ (i,j) = \sum_{i=1}^{3}\sum_{j=1}^{3} round\left(\frac{B_1}{8}\right) \quad (1)$$

2. Determine the highest value among each pixel in B_1 using the relation (2).

$$L = max\left(\sum_{i=1}^{3}\sum_{j=1}^{3} B_1\,(i,j)\ \right) \quad (2)$$

where L is the maximal value of B_1

3. Compute the difference between the L and the pixel values in B_1, then use the relation (3) to store the resultant in the appropriate cells of B_2 and the first cell of B_2 as L.

$$\sum_{i=1}^{3}\sum_{j=1}^{3} B_2\ (i,j) = L - \sum_{i=1}^{3}\sum_{j=1}^{3} B_1\ (i,j) \quad (3)$$

4. Convert each value in B_2 into binary format (taken each cell value in 3 bits except first cell. Fill the first cell *i.e.* B_2(1,1) with 6 binary bits and store the min to the block B_3.
5. Using the relation provided in (4), perform the modulo 8 operations to the value of B's pixels. and store the resultant values into a block called B_4.

$$\sum_{i=1}^{3}\sum_{j=1}^{3} B_4\ (i,j) = \sum_{i=1}^{3}\sum_{j=1}^{3} mod(B(i,j),8) \quad (4)$$

6. Convert each value in B_4 into binary format (taken each cell value in 3 bits) and store the min to the blocks B_5.
7. Concatenate the B_3 and B_5 binary values presented in (5) cell by cell, and then add the minimum to the RB (recovery bits) vector. Thus, the generated RB will contain 57 bits for a chosen B.

$$RB = B_3||B_5 \quad (5)$$

where || is the concatenation symbol.

Repeat the steps from (1) to (7) in algorithm 1 for each of the 3×3 ROI block to generate 57 RB bits and then concatenate to get CIVRB vector using the relation (6).

$$CIVRB = RB1 \parallel RB2 \parallel \dots \parallel RBN \quad (6)$$

where || is the concatenation sign and N is the number of ROI blocks. Consequently, the CIVRB vector contains recovery and ROI tamper detection data. Block B's RB generation is shown numerically in Figure 1(b).

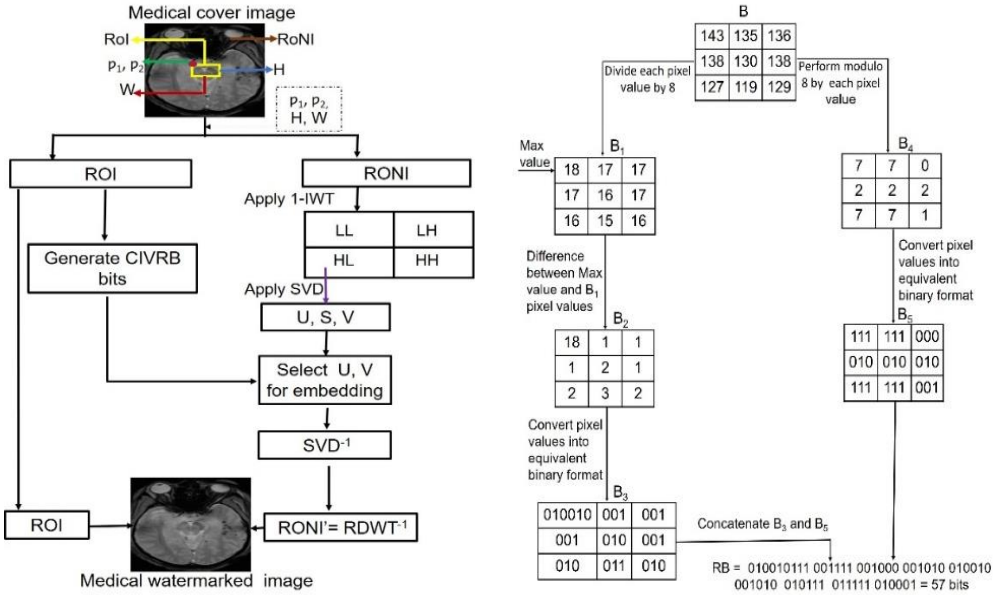


Figure 1. The block diagram of the recommended embedding process (a) flow diagram for the process of embedding and (b) generation of RB for the 3×3 ROI block

4.3. CIVRB embedding and extraction

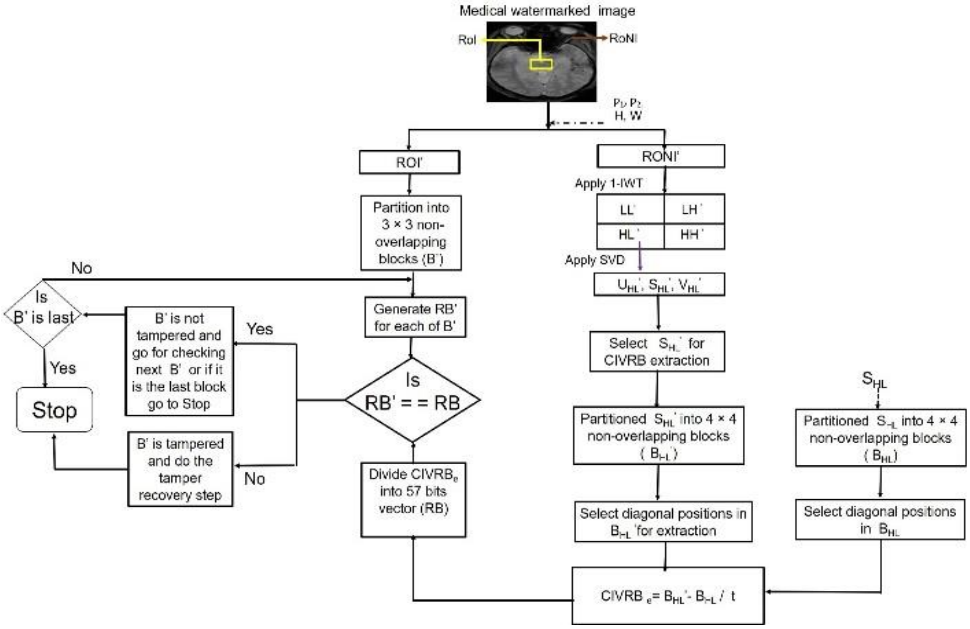
The proposed method uses the ROONI part of the M_{img} for CIVRB embedding. The block diagram of the recommended embedding process is shown in Figure 1. The integer wavelet transform (IWT) places a watermark in the targeted sub-bands (LL, LH, HL, and HH) to attain high imperceptibility [19]. The IWT sub-bands with the HL were chosen in order to strike a balance between concealment and resilience. IWT is perfect for the human visual system (HVS) when these characteristics are combined [20]. The primary benefit of SVD transformation is its exceptional unique value stability, even with minimal image changes. The system being discussed divides the application of one level IWT on RONI into four sub-bands. To the sub-bands HL, SVD is performed, taking advantage of resilience against specific image attacks. is further broken down into three submatrices: V_{HL}, S_{HL}, and U_{HL}. SVD and IWT hybridization provides great robustness and imperceptibility.

The singular matrices S_{HL} include the recovery bits CIVRB produced from ROI, as described in section 3.2. The singular values can only be slightly altered in the event of visual distortion. Additionally, the singular value is immune to mirror, zoom, and translation attacks. S_{HL} embeds the CIVRB bits because singular matrices typically provide less important picture information. The chosen S_{HL} matrix is split into 4×4 non-overlapping blocks (B_{HL}) to improve security. The watermarks are embedded in diagonally positions using an unpredictable scaling coefficient (t), which is also referred to as the watermark boosting variable. Applying the inverse SVD and inverse IWT adjustments results in the final watermarked RONI (RONI′).

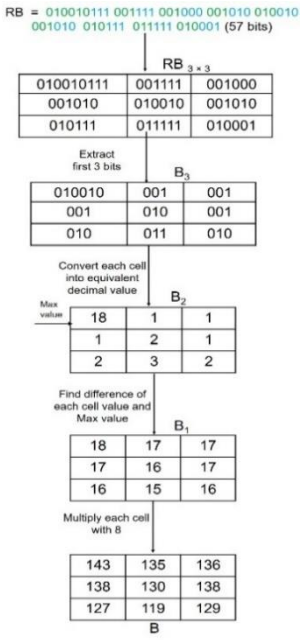
Figure 2(a) displays the schematic diagram for the CIVRB bits extraction procedure. Figure 2(b) illustrates the localized tamper recovery procedure for a 3×3 block. The equation (7) displays the relations used for extraction.

$$CIVRB_e = B_{HL}{}'(i,i) - B_{HL}(i.i)/t \quad (7)$$

where "*t*", B_{LH}, and B_{HL} are 4×4 non-overlapping chunks of the original S_{LH} and S_{HL}, and where i=1, 2, 3, and 4 accordingly. As shown in section 4.4, CIVRBe bits make it easier to identify image integrity verification and to guarantee the integrity of ROI. Because it enables the watermark to be extracted without utilizing the original cover image, the recommended technique is known as blind watermarking.



(a)



(b)

Figure 2. Overview of (a) the block diagram for the extraction and integrity of the watermark and (b) tamper recovery of 3×3 checking process

4.4. Confined integrity verification

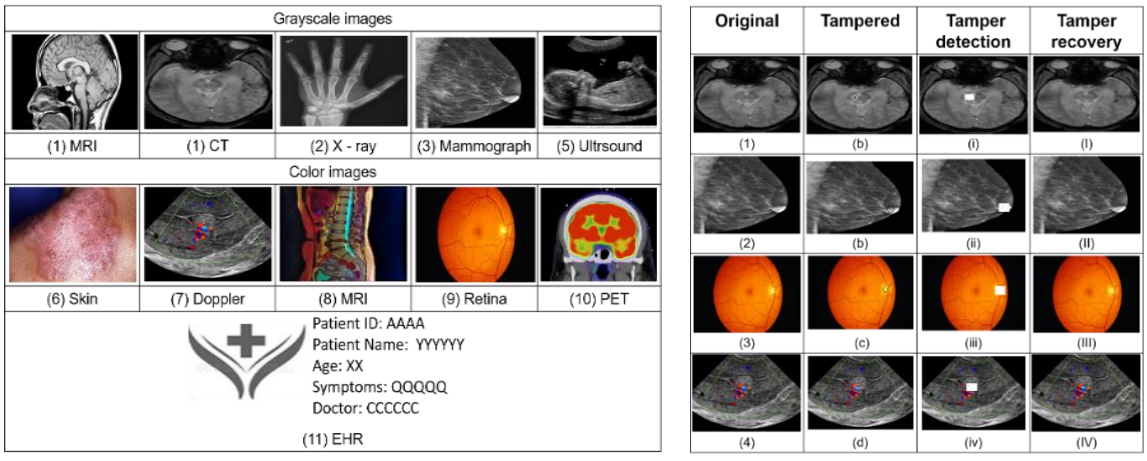
The recipient must confirm the ROI integrity after CIVRB has been extracted. Algorithm 2 describes the algorithmic procedures for tamper detection and recovery to verify ROI integrity. The procedure described in section 4.2 is used to create Recovery bits (RB′) for the ROI′. To identify tampering, the extracted RB (produced from CIVRB) and the generated RB′ are compared. The received ROI is unaltered if both are the same. A localized tamper restoration step is conducted if both are different, which suggests that the ROI has been tampered with. Figure 2(b) illustrates the localized tamper recovery procedure for a 3×3 block.

Algorithm 2. ROI integrity verification
Require: ROI′, CIV RBe.
Ensure: Recovered ROI (ROI_r)

1. Split the ROI′ into non-overlapping 3×3 blocks (B′).
2. Using the RB creation Algorithm 1 described in section 4.2, create RB′ (57 bits) for every B′.
3. Extract a 57-bit vector, say RB, from $CIVRB_e$.
4. Evaluate RB and RB′. The accompanying B′ is not tampered with if both are equal; if not, the block is tempered.
5. Move to step 8 if the B′ is unaltered; if not, move to step 6.
6. Transform all 57 bits of RB into 3×3 (RB 3×3) cell format by placing the first 9 bits in the first RB 3×3 cell and the remaining 6 bits in each of the remaining cells.
7. Use the following procedures to create B from RB3×3:
   a. Insert the first three bits of the first cell into the other cells of B_3, and the first six bits of the first cell into B_3 of the first cell position.
   b. Put each cell's binary value in B_2 after converting it to its corresponding decimal value. Given that the B_2's initial cell has the highest value
   c. Determine how the first cell value in B_2 differs from the other cells in B_2. Fill the first cell location with the maximum value and enter the resulting value in B_1.
   d. To obtain the retrieved B, multiply each cell in B_1 by 8. Figure 2(b) depicts the creation of B from RB (3×3).
8. For every B′, repeat steps 2 through 7 of the procedure. Step 9 is reached if every block in ROI has been processed.
9. Stop and return ROIr

5. EXPERIMENTAL RESULTS AND DISCUSSION

This part focuses on assessing the proposed scheme's effectiveness in terms of integrity, robustness, and imperceptibility. The simulations were performed on a MATLAB R2017b Windows 10 processor with an i5 core. As shown in Figure 3(a), test M_{img} are received from reputable organizations such as OPENi [21] and OASIS [22] for the proposed work's experiments. M_{img} was set to 256×256 pixels for both color and grayscale images. Figure 3(b) displays the original watermarked images (1-4), copy-paste tampered images (a-b), erase tampered image (c-d), tamper detected region marked with white pixels (i-iv) and the recovered images (I-IV).



(a) (b)

Figure 3. The simulations (a) test covers medical images in various modalities and (b) copy-paste and erase operations

5.1. Imperceptibility test

For medical image transmission via IoMT, concealment is an essential feature. Suggested system invisibility is evaluated using structural similarity index measure (SSIM) and PSNR measures. The PSNR

and SSIM relations are displayed in [23], [24]. The grayscale and color PSNR and SSIM of medical images of Figure 3(a) with t=0.01 are shown in Table 1. Both color and grayscale images had PSNRs greater than 55 dB. While color images get closer to the optimum value, grayscale images have an SSIM that is exactly equal to ideal value 1. The mean PSNR for color and grayscale images is 61.34 and 58.57 dB, respectively. The average SSIM for color and grayscale images is 0.9999 and 1, respectively. The imperceptibility of the specified scheme is further examined with an average PSNR and SSIM of 56.52 dB, 1 for 30 clinical pictures of different kinds; the findings are shown in Table 1. The recommended strategy is quite subtle in light of this discovery.

Table 1. For test medical images with t=0.01 for various image modalities obtained from OPENi [21], OASIS [22], PSNR, SSIM, NC, and BER (under zero assaults)

Grayscale images					Color images				
Image	PSNR	SSIM	NC	BER	Image	PSNR	SSIM	NC	BER
MRI	60.23	1	0.9999	0.0002	Skin	64.64	1	0.9998	0.0002
CT Scan	59.26	1	0.9999	0.0002	Doppler	60.27	1	0.9999	0
X- ray	58.52	1	0.9999	0.0004	MRI	61.72	0.9999	0.9997	0.0004
Mammograph	57.81	1	0.9998	0.0002	Retina	58.62	0.9999	0.9999	0.0002
Ultrasound	59.01	1	1	0	PET	61.46	0.9998	0.9999	0.0004
Average	58.97	1	0.9998	0.0002		61.34	0.9999	0.9998	0.0002
AVG. of 30 images	56.52	1	0.9997	0.0006					

5.2. Robustness test

Since medical images include sensitive information, their resilience is essential. It must be essential to protect its privacy. The robustness of the suggested method is examined using the NC and BER metrics. The NC, BER relation used in [23], [24] is displayed. The NC and BER of the images in Figure 1(a) with a "t "value of 0.01 are shown in Table 1. Color and grayscale visuals are almost identical in both situations. rather than BER reaching its optimal value. The average value of NC is 0.9997 for color photos and 0.9998 for grayscale images. BER is 0.0002 for both color and grayscale photos. This demonstrates that the NC and BER of color and grayscale images vary minimally.

The envisioned technique's resilience performance is further examined in the face of various image processing threats. For ease of presentation, Table 2 uses MRI, X-ray, skin, and retinal images to show NC and BER under attacking. Shear attacks, rotation, cropping, Poisson noise (PN), gaussian noise (GN), salt and pepper noise (SP), and speckle noise (SK). For watermarked MRI, X-ray, skin, and retinal images, the following filters are used: gaussian filter (GF), median filter (MF), Weiner filter (WF), Butterworth filter (BW), sharpening, histogram equivalent (HE), and JPEG compression. The suggested approach demonstrated NC greater than 0.96 and BER less than 0.19 for all four of the specified images while withstanding the highest filtering attacks (GF, WF, BF, and Sharp). The proposed method for MF, HE assaults displays NC and BER values above thresholds. JPEG is crucial for the Internet transmission of medical photos. For the JPEG compression attack, the proposed scheme's NC is above 0.99 and its BER is below 0.09. The provided technique demonstrates NC above the threshold due to noise and geometrical attacks like SP, SK, GN, and PN. The BER is less than the cutoff point. This fact leads to the conclusion that the proposed system is resistant to most attacks. The mean NC and BER for 30 clinical images from various modes are also displayed in Table 1. The average NC and BER of every picture are fairly near the threshold levels, as Table 1 demonstrates. The conclusion drawn from this discussion is that the suggested approach is resistant to most attacks.

5.3. Integrity test

The integrity of medical images is important for accurate diagnosis. This section looks over how good the suggested approach is at detecting and recovering tampering. True positive rate (TPR), False positive rate (FPR), Accuracy, and PSNR have all been used in the presented scheme to asses show well the proposed technique detects and recovers tampering. Their relationship pushed for TPR, FPR, and Accuracy for tamper detection and recovery is shown in [23], [24]. For the experiment, 10% of the watermarked image's altered region (with erase or copy-paste operations) is considered.

Table 3 displays TP (number of tampered pixels), TN (the number of unmodified pixels that were incorrectly identified as tampered), FP (number of tampered pixels that were in correctly assessed as unmodified), FN (the number of tampered pixels that were incorrectly assessed as unmodified), and the TPR, FPR, and Accuracy derived. The TPR is greater than 80%, and the FPR is less than 0.31, as shown in Table 3. This demonstrated increased tamper localization and good resistance against multiple attacks. The proposed approach is more than 98.30% reliable for all specified images, and PSNR values for all recovered

and watermarked images are nearly same, indicating that they are visually identical. Figure 3(b) displays the original watermarked images (1-4), copy – paste tampered images (a-b), erase tampered image (c-d), tamper detected region marked with white pixels (i-iv) and the recovered images (I-IV). The suggested approach is successful in identifying and recovering manipulated data during erase, copy-paste operations, as shown in Figure 3(b) and Table 3.

Table 2. For MRI, X-ray, skin, and retinal exam medical images with various modalities obtained from OPENi [21], OASIS [22], NC, BER (under various attacks)

Assaults	MRI		X- ray		Skin		Retina		AVG. of 30 images	
	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
GF(3×3)	0.9997	0.0004	0.9998	0.0004	0.9998	0.0006	0.9998	0.0002	0.9997	0.0004
MF(3×3)	0.8752	0.2529	0.8861	0.2495	0.8682	0.2496	0.8552	0.2595	0.8462	0.2851
WF(3×3)	0.9628	0.1862	0.9482	0.1215	0.9483	0.1962	0.9581	0.1961	0.9328	0.2013
BF(G=2, F=10)	0.9995	0.0018	0.9992	0.0025	0.9994	0.0021	0.9991	0.0038	0.9984	0.0058
Sharp	0.9642	0.1962	0.9702	0.1957	0.9742	0.1886	0.9632	0.1904	0.9637	0.2148
HE	0.8752	0.2628	0.8817	0.2603	0.8928	0.2492	0.8692	0.2006	0.8632	0.2041
JPEG	0.9903	0.0962	0.9967	0.0863	0.9986	0.0752	0.9985	0.0750	0.9915	0.0802
SP(0.0002)	0.8863	0.2385	0.8903	0.2041	0.8762	0.2742	0.8861	0.2184	0.8728	0.2072
SK(0.0002)	0.8052	0.2631	0.8162	0.2581	0.7951	0.2982	0.8041	0.2571	0.7984	0.2493
PN	0.7682	0.4013	0.7782	0.3961	0.8021	0.3415	0.7931	0.3712	0.7637	0.3863
GN(0.0002)	0.8261	0.3271	0.8421	0.3082	0.8228	0.3218	0.8327	0.3527	0.8026	0.3128
Rotate(10)	0.8522	0.1962	0.8452	0.1784	0.8428	0.1462	0.8293	0.1726	0.8351	0.1825
Crop	0.8053	0.2691	0.8261	0.2471	0.8168	0.2183	0.8292	0.2158	0.7924	0.2216
Shear	0.8162	0.2681	0.8371	0.2571	0.8271	0.2471	0.8042	0.2831	0.7936	0.2538

Table 3. TP, TN, FP, FN and TPR, FPR and Accuracy, PSNR of different images

Grayscale Image	TP	TN	FP	FN	TPR	FRP	Accuracy	PSNR
MRI	156	2514	05	29	84.32	0.19	98.74	56.73
CT Scan	157	2516	06	25	86.26	0.23	98.85	57.75
X-ray	146	2528	07	23	86.39	0.27	98.89	56.27
Mammograph	141	2525	06	32	81.50	0.23	98.59	56.24
Ultrasound	149	2510	08	37	80.10	0.31	98.33	57.82

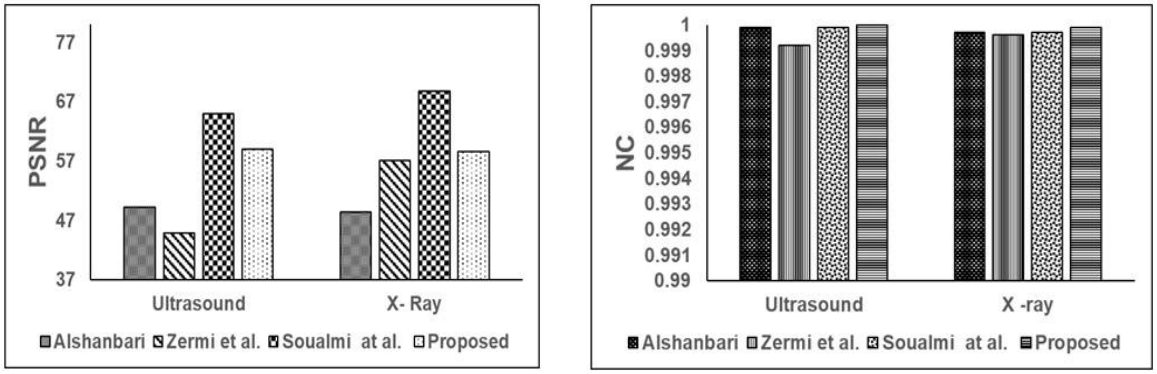
5.4. Discussion on experimental outcome

The proposed region-based MIW scheme demonstrates effective performance in ensuring the integrity, confidentiality, and robustness of medical images transmitted over IoMT systems. By separating the medical image into ROI and RONI, and embedding CIVRB into the RONI using a hybrid IWT SVD technique, the method ensures that diagnostic information remains unaffected while still enabling accurate tamper detection and recovery. The experimental results validate the effectiveness of the approach. The proposed method achieves high imperceptibility, with an average PSNR of over 56 dB, and maintains visual similarity with the original images, as evidenced by SSIM values close to 1. Additionally, the robustness tests under various image processing attacks—such as filtering, compression, noise addition, and geometric transformation show that the scheme can withstand distortions, maintaining NC values above 0.99 and BER below 0.0002 in most cases. The integrity verification accuracy exceeds 98%, and the system performs well in localized tamper detection and recovery, as demonstrated by high true positive rates and low false positive rates. These outcomes highlight that the proposed watermarking approach is not only secure but also practical for real-world deployment in smart healthcare systems. Unlike existing methods that embed data into diagnostic regions and risk compromising image quality, this work provides a non-invasive, blind watermarking solution that is both technically sound and medically safe. The findings also indicate that the framework is scalable and can be adapted to various image types and modalities, offering a reliable strategy for securing sensitive medical data in connected environments.

5.5. Comparative study

This section compares the proposed strategy with similar counter strategies. The proposed scheme is contrasted with those proposed by Alshanbari [23], Zermi *et al.* [24], and Soualmi *et al.* [25]. Alshanbari [23] proposes a region-based multiple watermarking strategy for the DWT + SVD domain. This approach recovers ROI integrity using Lempel-Ziv-Welch (LZW), and tamper detection is achieved by the generation of a 64-bit hash code using SHA-256. Zermi *et al.* [24] offer a hybrid DWT+SVD watermarking system for medical photos to ensure reliable transmission. On the other hand, LZW compression is used in the strategy proposed in [23] to guarantee ROI integrity. However, there are additional embedding overheads and a substantial computational cost associated with applying compression techniques. The concept suggests a

targeted way to improve counterfeit identification and restoration efficiency while preserving high ROI imperceptibility. As a result, PSNR (with embedding capacities of 0.0117, 0.01562, 0.25, and 0.02516, respectively) and NC metrics are used to compare the proposed scheme's imperceptibility and robustness to comparative schemes [23]–[25] on two different medical image modalities (X-ray and CT). Figure 4(a) and Figure 4(b) depict the PSNR and NC under zero assaults of the proposed scheme and schemes in relation to CT and X-ray images. Compared to the strategies presented in [23], [24], Figure 4(a) and Figure 4(b) show that the proposed technique is more robust and undetected. For CT images, the proposed technique has a higher PSNR and NC than the one described in [25]. In terms of NC, the technique in [25] is more similar to the proposed scheme and has a higher PSNR for X-ray images. Figure 5 depicts an assessment of resilience performance under various attacks. Compared to approaches in [23]–[25], the proposed approach has a higher NC for MF, GF, Sharp, JPEG, and HE attacks. Furthermore, it demonstrates significant NC for the GN and SP assaults when compared to the schemes in [23], [24], with the closest NC. As a result of this debate, the proposed method is substantially less obvious and reliable than the schemes provided in studies [23]–[25].



(a) (b)

Figure 4. Comparison of the proposed strategy with similar counter strategies (a) PSNR comparison and (b) NC (considering zero assaults)

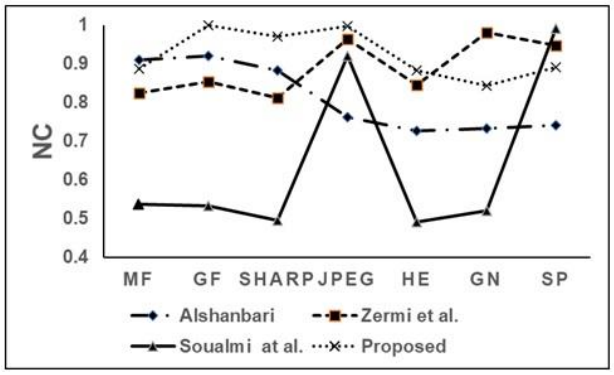


Figure 5. NC comparison of proposed scheme under different attacks and schemes presented in Alshanbari [23], Zermi *et al.* [24], Soualmi *at al.* [25]

6. CONCLUSION

This paper presents a secure region-based MIW technique that ensures high imperceptibility, integrity, and resilience while boosting long-term transmission of medical pictures over IoMT. RONI has embedded CIVRB bits, and the proposed method successfully ensures integrity while allowing for tamper identification and recovery. The suggested method's performance is evaluated using a variety of approaches for image processing, including as filtering, noise reduction, and geometrical attacks. Additionally, the experimental results show improved performance. The recommended method for tamper detection and recovery is more than 98% accurate.

Future enhancements of this work include automating ROI segmentation using AI-based techniques and supporting multiple ROIs for handling complex diagnostic images. Additional improvements involve adaptive watermark strength, hardware optimization for real-time processing, integration with encryption/blockchain for enhanced security, and extending the method to 3D images and medical video streams for advanced diagnostic applications.

FUNDING INFORMATION

Author state no funding.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Kilari Jyothsna Devi	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	
Ravuri Daniel	✓	✓		✓	✓	✓			✓		✓	✓		
Bode Prasad			✓	✓			✓				✓			
Mohamad Khairi Ishak	✓	✓	✓	✓	✓	✓		✓		✓		✓	✓	✓
Dorababu Sudarsa			✓				✓				✓			
Pasam Prudhvi Kiran			✓				✓		✓				✓	✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The authors confirm that the data supporting the findings of this study are available within the article.

REFERENCES

[1] S. Razdan and S. Sharma, "Internet of medical things (IoMT): overview, emerging technologies, and case studies," *IETE Technical Review*, vol. 39, no. 4, pp. 775–788, Jul. 2022, doi: 10.1080/02564602.2021.1927863.
[2] Z. Ashfaq *et al.*, "A review of enabling technologies for internet of medical things (IoMT) ecosystem," *Ain Shams Engineering Journal*, vol. 13, no. 4, p. 101660, Jun. 2022, doi: 10.1016/j.asej.2021.101660.
[3] Y. Sun, F. P.-W. Lo, and B. Lo, "Security and privacy for the internet of medical things enabled healthcare systems: a survey," *IEEE Access*, vol. 7, pp. 183339–183355, 2019, doi: 10.1109/ACCESS.2019.2960617.
[4] M. Magdy, K. M. Hosny, N. I. Ghali, and S. Ghoniemy, "Security of medical images for telemedicine: a systematic review," *Multimedia Tools and Applications*, vol. 81, no. 18, pp. 25101–25145, Jul. 2022, doi: 10.1007/s11042-022-11956-7.
[5] K. J. Giri, Z. Jeelani, J. I. Bhat, and R. Bashir, "Survey on reversible watermarking techniques for medical images," in *Multimedia security: algorithm development, analysis and applications*, 2021, pp. 177–198.
[6] S. M. Mousavi, A. Naghsh, and S. A. R. Abu-Bakar, "Watermarking techniques used in medical images: a survey," *Journal of Digital Imaging*, vol. 27, no. 6, pp. 714–729, Dec. 2014, doi: 10.1007/s10278-014-9700-5.
[7] S. Priya and B. Santhi, "A novel visual medical image encryption for secure transmission of authenticated watermarked medical images," *Mobile Networks and Applications*, vol. 26, no. 6, pp. 2501–2508, Dec. 2021, doi: 10.1007/s11036-019-01213-x.
[8] Swaraja K, "Medical image region based watermarking for secured telemedicine," *Multimedia Tools and Applications*, vol. 77, no. 21, pp. 28249–28280, Nov. 2018, doi: 10.1007/s11042-018-6020-7.
[9] Z. Bin Faheem *et al.*, "Image watermarking scheme using LSB and image gradient," *Applied Sciences*, vol. 12, no. 9, p. 4202, Apr. 2022, doi: 10.3390/app12094202.
[10] B. K and S. S, "A fuzzy based ROI selection for encryption and watermarking in medical image using DWT and SVD," *Multimedia Tools and Applications*, vol. 80, no. 5, pp. 7167–7186, Feb. 2021, doi: 10.1007/s11042-020-09981-5.
[11] Z. Yuan, Q. Su, D. Liu, and X. Zhang, "A blind image watermarking scheme combining spatial domain and frequency domain," *The Visual Computer*, vol. 37, no. 7, pp. 1867–1881, Jul. 2021, doi: 10.1007/s00371-020-01945-y.
[12] S. K, M. K, and P. Kora, "An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine," *Biomedical Signal Processing and Control*, vol. 55, p. 101665, Jan. 2020, doi: 10.1016/j.bspc.2019.101665.
[13] N. E. H. Goléa and K. E. Melkemi, "ROI-based fragile watermarking for medical image tamper detection," *International Journal*

of High Performance Computing and Networking, vol. 13, no. 2, pp. 199–210, 2019, doi: 10.1504/IJHPCN.2019.097508.
[14] H. Chaudhary, P. Garg, and V. P. Vishwakarma, "Enhanced medical image watermarking using hybrid DWT-HMD-SVD and Arnold scrambling," *Scientific Reports*, vol. 15, no. 1, p. 9710, Mar. 2025, doi: 10.1038/s41598-025-94080-4.
[15] R. Eswaraiah and E. Sreenivasa Reddy, "Medical image watermarking technique for accurate tamper detection in ROI and exact recovery of ROI," *International Journal of Telemedicine and Applications*, vol. 2014, pp. 1–10, 2014, doi: 10.1155/2014/984646.
[16] V. Rajput and I. A. Ansari, "Image tamper detection and self-recovery using multiple median watermarking," *Multimedia Tools and Applications*, vol. 79, no. 47–48, pp. 35519–35535, Dec. 2020, doi: 10.1007/s11042-019-07971-w.
[17] R. Bouarroudj, F. Souami, F. Z. Bellala, N. Zerrouki, F. Harrou, and Y. Sun, "Secure and reversible fragile watermarking for accurate authentication and tamper localization in medical images," *Computers and Electrical Engineering*, vol. 123, p. 110072, Apr. 2025, doi: 10.1016/j.compeleceng.2025.110072.
[18] S. Sun and R. Zhang, "Region of interest extraction of medical image based on improved region growing algorithm," in *Proceedings of the 2017 International Conference on Material Science, Energy and Environmental Engineering (MSEEE 2017)*, 2017, pp. 471–475, doi: 10.2991/mseee-17.2017.87.
[19] F. Kahlessenane, A. Khaldi, R. Kafi, and S. Euschi, "A DWT based watermarking approach for medical image protection," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 2, pp. 2931–2938, Feb. 2021, doi: 10.1007/s12652-020-02450-9.
[20] P. Khare and V. K. Srivastava, "A reliable and secure image watermarking algorithm using homomorphic transform in DWT domain," *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 131–160, Jan. 2021, doi: 10.1007/s11045-020-00732-1.
[21] J. Magro, "Tumor, lungs," *National Library of Medicine Open Acees Biomadical Search Engine*, 2013. https://openi.nlm.nih.gov (accessed Jun. 18, 2023).
[22] OASIS, "Open access series of imaging studies (OASIS)," *sites.wustl.edu*. Accessed: Jun. 18, 2023. [Online]. Available: https://www.oasis-brains.org/.
[23] H. S. Alshanbari, "Medical image watermarking for ownership & tamper detection," *Multimedia Tools and Applications*, vol. 80, no. 11, pp. 16549–16564, May 2021, doi: 10.1007/s11042-020-08814-9.
[24] N. Zermi, A. Khaldi, M. R. Kafi, F. Kahlessenane, and S. Euschi, "An SVD values ordering scheme for medical image watermarking," *Cybernetics and Systems*, vol. 53, no. 3, pp. 282–297, Feb. 2022, doi: 10.1080/01969722.2021.1983700.
[25] A. Soualmi, A. Alti, and L. Laouamer, "A novel blind medical image watermarking scheme based on Schur triangulation and chaotic sequence," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 1, Jan. 2022, doi: 10.1002/cpe.6480.

BIOGRAPHIES OF AUTHORS

Kilari Jyothsa Devi received Ph.D. degree from SRM University-A.P, Andhra Pradesh, India. M. Tech and B. Tech degree from JNTU–Hyderabad. She is currently working as an assistant professor in the Department of Computer Science and Engineering, at Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India. Her research interests include digital image watermarking, optimization techniques, image forensic and machine learning, image security, artificial intelligence. She can be contacted at email: kilari.jyothsna@pvpsiddhartha.ac.in.

Ravuri Daniel is an associate professor in the Department of Computer Science and Engineering at Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, India. With extensive experience in industry and both national and international academia, he holds a Ph.D. from Jawaharlal Nehru Technological University Kakinada (JNTU Kakinada), and M.Tech. from Andhra University, and a B.Tech. from Jawaharlal Nehru Technological University Hyderabad. His research interests are multiple domains, including computer networks, wireless sensor networks, internet of things (IoT), data analytics, artificial intelligence (AI), and embedded systems. His current work focuses on developing innovative IoT applications powered by AI edge computing. He has extensive hands-on experience with IoT hardware platforms such as Arduino and Raspberry Pi, along with software proficiency in C, Python, R, and MATLAB. He can be contacted at email: danielravuri@gmail.com.

Bode Prasad received his master's degree from Koneru Lakshmaiah Engineering College in Guntur, India, and obtained his Ph.D. degree from Andhra University College of Engineering, Visakhapatnam, India in the year 2015. He currently holds the position of professor in the Department of Information Technology at Vignan's Institute of Information Technology (A) in Visakhapatnam, India. His research interests span a wide range of topics, including computer networks, mobile ad-hoc networks, cloud computing, wireless networks, machine learning, data science, artificial intelligence, human action analysis, and sign language machine translation. He can be contacted at email: arjunprasad.bode@gmail.com.

Mohamad Khairi Ishak is an associate professor in the Department of Electrical and Computer Engineering at the College of Engineering and Information Technology, Ajman University, United Arab Emirates. He holds a B.Eng. in electrical and electronics engineering from the International Islamic University Malaysia (IIUM), an MSc in embedded systems from the University of Essex, United Kingdom, and a Ph.D. from the University of Bristol, United Kingdom. He is a member of IEEE and a registered graduate engineer with the Board of Engineers Malaysia (BEM). Dr. Khairi Ishak brings extensive teaching experience from Universities Sains Malaysia and Ajman University, where he engages students by leveraging emerging technologies and innovative teaching models. His research focuses on embedded systems, artificial intelligence (AI), real-time control communications, and the internet of things (IoT). He emphasizes the development of both theoretical and practical methods with real-world applications. His recent work has centered on tackling industrial challenges related to embedded networked control systems incorporating AI and IoT. He can be contacted at email: m.ishak@ajman.ac.ae.

Dorababu Sudarsa having M.Tech. in information technology from Sathyabama University, Chennai, 2009. JNT University, Hyderabad, awarded him a B.Tech. in computer science and information technology in 2002. He received the best teaching faculty award from Koneru Lakshmaiah University, Vadeswaram, Guntur, India, and Audi Sankara College of Engineering and Technology, Gudur, India. He taught 18 years total. cloud computing, data mining and warehousing, data science, and internet of things interest him. 15 international publications and conferences published him. He is an ISTE lifer. He can be contacted at email: dorababu.sudarsa@gmail.com.

Pasam Prudhvi Kiran having M.Tech. degree in information technology and pursuing his Ph.D. degree in CSSE Department from Andhra University College of Engineering, Visakhapatnam, In dia. His research area moves around IoT and artificial intelligence. He can be contacted at email: pasamprudhvi@gmail.com.