Neural Computing and Applications (2023) 35:23041–23062
https://doi.org/10.1007/s00521-023-08457-5

S.I. : NEURAL COMPUTING FOR IOT BASED INTELLIGENT HEALTHCARE SYSTEMS

Machine learning based multipurpose medical image watermarking

Rishi Sinhal[1] · Irshad Ahmad Ansari[1]

Received: 4 September 2021 / Accepted: 3 March 2023 / Published online: 24 March 2023

Abstract

Digital data security has become an exigent area of research due to a huge amount of data availability at present time. Some of the fields like medical imaging and medical data sharing over communication platforms require high security against counterfeit access, manipulation and other processing operations. It is essential because the changed/manipulated data may lead to erroneous judgment by medical experts and can negatively influence the human's heath. This work offers a blind and robust medical image watermarking framework using deep neural network to provide effective security solutions for medical images. During watermarking, the region of interest (ROI) data of the original image is preserved by employing the LZW (Lampel-Ziv-Welch) compression algorithm. Subsequently the robust watermark is inserted into the original image using IWT (integer wavelet transform) based embedding approach. Next, the SHA-256 algorithm-based hash keys are generated for ROI and RONI (region of non-interest) regions. The fragile watermark is then prepared by ROI recovery data and the hash keys. Further, the LSB replacement-based insertion mechanism is utilized to embed the fragile watermark into RONI embedding region of robust watermarked image. A deep neural network-based framework is used to perform robust watermark extraction for efficient results with less computational time. Simulation results verify that the scheme has significant imperceptibility, efficient robust watermark extraction, correct authentication and completely reversible nature for ROI recovery. The relative investigation with existing schemes confirms the dominance of the proposed work over already existing work.

Keywords Medical image watermarking · Ownership verification · Image authentication · ROI reversibility · Multipurpose watermarking

1 Introduction

In recent times, the advancements in digital technologies and communication fields have resulted the widespread use of digital data in various fields. Healthcare sector, industrial applications, forensics, e-governance, education and banking operations are some of important fields in which digital technology plays an important role in present time. Digital devices are frequently use to capture information in different forms. Digital data generation and sharing are increasing in a speedy manner [1]. People can complete many tasks using digital devices like smartphones; laptop etc. and they do not require going respective places in person. Thus, it saves time and reduces the traffic on roads, public gatherings indirectly [2]. However, there are different issues regarding data security also exist along with these advantages. Digital data security is an important and challenging area because a huge amount of digital data is easily accessible to users. The users can access and manipulate the data in an unauthentic manner [3]. Hence, it is important to ensure the safety of digital data for appropriate use.

Healthcare sector is one of the sensitive areas in which digital data security is essentially required because it directly relates to people's health [4]. Like many other fields, a large portion of digital data generation in the medical field includes digital images. Digital data in the form of X-ray, CT-scans and MRI images are used to diagnose the health issues and the experts decide further

✉ Irshad Ahmad Ansari
irshad@iiitdmj.ac.in

Rishi Sinhal
rishi.sinhal.jec@gmail.com

[1] Electronics and Communication Engineering, PDPM Indian Institute of Information Technology Design and Manufacturing, Jabalpur, Madhya Pradesh 482005, India

actions based on the investigation. People also find it easy to communicate with the healthcare professional on digital platforms. They can also share the medical information such as medical images. In this regard, it becomes essential to verify the medical data for each patient. Since, the exchange or mismatching of medical data may lead to insufficient or wrong diagnosis and can be devastating for the patient's health. The other challenges related to medical images include image data authentication, tamper/forgery localization and ROI (region of interest) reversibility. Although the complete medical image is important and expected in original form for the correct analysis, it can be classified into two parts namely ROI (region of interest) and RONI (region of non-interest). ROI is considered as the most important region in terms of diagnosis and need to be protected. Even if the ROI part of the medical images get tampered/attacked, the recovery of the ROI is necessary because the medical data (i.e., image) without the correct ROI cannot be used to examine the health issues. The remaining portion (i.e., excluding ROI) in medical images refers to RONI. In most cases, if the ROI portion is correct, the future actions can be decided regarding patient's wellness [5]. Digital watermarking [6] framework can efficiently handle these issues related to medical images.

Digital watermarking approaches are widely used in the field of data security in the last few decades. In digital image watermarking, the watermark information is embedded into the host signal using a set of rules (i.e., embedding algorithm). In addition, the host image should be similar before and after the embedding process for the human visual system, so that the watermark information remains hidden. This feature is known as imperceptibility and it can be measured using imperceptibility parameters such as peak signal to noise ratio (PSNR) [7] and structural similarity index matrix (SSIM) [8] etc. However, the watermark information can be extracted using a set of rules (i.e., extraction algorithm) from the watermarked or attacked image. The quality of the extracted information should be identical to the embedded information so that the watermark data can be achieved correctly. This feature is known as robustness [9, 10]. It can be analyzed by comparing embedded and extracted watermark information using robustness parameters like bit error rate (BER) and normalized cross-correlation (NC) [7]. The amount of watermark information that can be inserted into the host image without losing the visual quality of the host image is termed as watermarking payload or embedding capacity. The watermarking schemes should also have the ability to restrict illicit accessibility. Different encryption mechanisms can be used to get such protection for digital data. These encryption mechanisms are generally key-based, so the knowledge of a secret key is required to decrypt the data or process. Thus, even if users have access to the data; it cannot be used in an effective way without knowing the secret key. This feature represents the security characteristics of the watermarking scheme. All these features are significant and imperative for the digital image watermarking scheme [11]. In the existing scenario, the fast response (i.e., low processing time) also seems to be an important feature. It is highly demanding in this era of fast and advanced technology. Currently, machine learning mechanisms are widely used in different fields (including digital watermarking) to automate the process and get a fast response [12]. Initially, it seems to be a lengthy (time-consuming) process at the experimentation stage due to training dataset preparation and training time. But once train, it reduces the processing time effectively and can easily be used for the new data to get efficient results. Further, the availability of improved digital devices (i.e., digital computers) has improved the training procedure of the machine learning frameworks. Machine learning approaches can be used to improve the time complexity of the digital watermarking schemes. Therefore, the use of machine learning approaches in the field of digital watermarking is a challenging and continuously growing research area [13].

This work presents a new machine learning-based multipurpose image watermarking scheme for the medical imaging domain and other teleradiology applications. It has blind extraction nature, so there is no need for side information regarding host and watermark data. It can be used for different objectives such as ownership or EPR (Electronic Patient Record) verification, image authentication, and ROI recovery at the same time. The key contributions of this work are listed as follows:

1. Secret key based robust watermarking and the hash key based fragile watermarking procedures gives protection against false ownership verification, illegal access, and manipulation/tampering.
2. Deep neural network (DNN) based robust extraction process gives efficient results with low computational complexity as compared to other schemes.
3. It provides accurate authentication of ROI as well as RONI regions along with the complete reversibility for ROI region for better diagnosis.
4. It provides high performance in terms of imperceptibility, robustness and other watermarking features even after having blind and multipurpose nature.

The succeeding sections refer to the literature review, the proposed watermarking approach, results and discussion, and conclusion respectively.

2 Literature review

Coatrieux et al. [14] described the significance of digital watermarking in the area of medical imaging to offer effective solutions for different security issues like EPR protection, tamper detection and authentication etc. The manuscript addressed various medical imaging aspects and the existing issues along with their potential solutions by means of digital image watermarking. Chao et al. [15] offered a data hiding technique to protect EPR data in a non-blind manner. The technique used different varieties of information as EPR for the experimentation and found to be significant in terms of extraction ability. However, the non-blind nature of the scheme limits the practicability in many cases. Guo and Zhuang [16] proposed a medical image watermarking method using difference expansion and hash key-based approaches to offer image integrity authentication and recovery of images. The method has a non-blind nature and requires EPR data for the authentication purpose at the receiving end. Lai [17] presented an image watermarking framework based on the DCT (Discrete Cosine Transform) and SVD (Singular Value Decomposition) processes. The uniform block-based watermark insertion was performed by selecting the blocks with high complexity. Edge entropy and human visual system-based features were used to select the high complexity blocks. The DCT transform and the SVD approach were applied on each selected block in order to update the orthogonal matrix using bit value and embedding strength. The simulation results show adequate imperceptibility characteristics; however, the scheme has poor robustness while handling attacks like noising, scaling and image filtering etc. Das and Kundu [18] presented an image watermarking technique for the authentication of medical images. It can also recover the ROI region in a lossless manner in case of a non-tampered watermarked image. The scheme used AES (Advanced Encryption Standard) and SHA-256 techniques for enhanced security. Experimental results show high imperceptibility and embedding capacity. However, the technique is not able to provide restoration (in case of tampering) and ownership verification. Lei et al. [19] proposed a robust image watermarking technique for medical images based on wavelet transform, SVD, RDM (Recursive Dither Modulation), and DE (Differential Evolution) optimization approach. The scheme has high imperceptibility, significant payload, and acceptable robustness. However, the computation time is high due to the use of optimization and other processing operations such as transform/inverse transform, etc. The scheme was claimed to be reversible in nature, but this research work lacks the experimental outcomes/proofs for the reversibility. Moreover, the scheme is unable to authenticate and restore the tampered portions (such as ROI), which is one of the key requirements for medical imaging.

Badshah et al. [20] offered a medical image watermarking scheme using LSB modification and LZW (Lampel-Ziv-Welch) compression. The scheme used the LZW technique to compress the watermark information in order to improve the embedding capacity. RONI region was used as the embedding region and the LSB modification approach was used to insert the watermark data. Investigational results depict that the scheme has significant parametric performance with good imperceptibility, effective authentication of ROI, and recovery of the tampered ROI. The scheme is not able to authenticate the RONI (i.e., embedding region), so the authenticity of the extracted watermark information cannot be established. Moreover, the scheme lacks in providing ownership verification feature. Thakkar and Srivastava [21] presented a medical watermarking scheme using DWT (Discrete Wavelet Transform), SVD, and Hamming code. In this scheme, ROI is used as an embedding region, which modifies the ROI as compared to its original form. It is obvious that the ROI is a vital part of a medical image and medical experts need ROI in its original form for deciding future directions. However, ROI reversibility has not been provided in this work, which limits the practicability of the scheme in view of the diagnosis purpose. The scheme has acceptable imperceptibility and robustness, yet it is unable to detect tampering and restore the tampered portion. It can only be used for EPR verification and content authentication (i.e., ownership). Thanki et al. [22] proposed a robust image watermarking scheme for medical imaging applications to provide copyright protection. The scheme used the concepts of fast discrete curvelet transform, DCT transform, and noise sequences (i.e., White Gaussian Noise) for implementing the watermarking algorithm. Results show that the method has high imperceptibility, good payload, and acceptable robustness. However, image authentication, tamper localization, and restoration features have not been provided in the scheme. Moreover, the presence of noise in the extracted watermark (even in case of a no-attack) is a serious limitation of this scheme. Ernawan and Kabir [23] presented a watermarking technique for copyright protection/ownership verification using Arnold transform, and DCT transform. The embedding blocks identification were depended on the entropy and individual block co-ordinates were preserved as the side data for extraction process. After that each block was transformed using DCT transform and the specific coefficients were altered utilized watermark data. The method achieved significant outcomes in terms of visual quality, and security, nevertheless it performed poorly against attacks such as scaling and other noise attacks. Pourhadi and Nasab [24] introduced an image watermarking method utilizing bat optimization, SWT (Stationary Wavelet Transform), and SURF (speed-up robust feature). The optimization process was employed to adjust the strength of embedding and SURF detector made the scheme robust enough to handle geometric attacks. As per the investigational results, the scheme has poor robustness against filtering and compression attacks. Swaraja et al. [25] developed an image watermarking scheme for medical images using DWT transform, Schur decomposition, LZW compression, and PSBFO (Particle Swarm Bacterial Foraging Optimization) algorithm. This blind watermarking scheme provides EPR protection, tamper detection, and ROI recovery. Investigational results depict acceptable robustness and high capacity, but imperceptibility results are comparatively poor. In addition, the scheme is not able to authenticate the embedding region (i.e., RONI), which limits the reliability of the extracted watermark information. Alshanbari [26] offered a medical image watermarking technique having multipurpose nature for ownership verification, tamper detection, and ROI recovery. This non-blind watermarking scheme used DWT, SVD, LZW compression, and SHA-256 hash algorithm for implementing the watermarking process. The scheme has high imperceptibility, high capacity, and significant tamper detection (for ROI). However, the scheme has poor robustness (even in case of a no-attack) and lacks RONI authentication. Moreover, the possibility of tampering (or modification) in the embedding region (i.e., RONI) was not investigated, so the authenticity of the extracted watermark information remains doubtful. Recently, Sinhal et al. [27] developed a multipurpose image watermarking framework for medical images using Slantlet transform, LZW compression mechanism, SHA-256 hash algorithm, and LSB replacement approach. This scheme provided high robustness for EPR/ownership verification against various processing attacks. Further, the scheme can effectively deal with tampering/forgery and authenticate the ROI as well as RONI against changes. It can also retain the reversible nature of the ROI region even after facing tampering/alteration in ROI. The scheme has acceptable imperceptibility, high robustness, hash key-based security, and decent capacity. However, the processing time can be reduced by infusing the machine learning-based framework, which can enhance the practicality of the scheme for real-time or fast processing applications.

As per the available research in the field of medical image watermarking, there is wide scope of research to provide solutions for existing issues and limitations. In the proposed work, existing issues such as high processing time, inability to authenticate the embedding region (usually RONI) and lack of multipurpose nature etc. have been taken into consideration and effective solutions are provided along with superior parametric performance as compared to existing schemes.

3 Proposed scheme

This proposed work can be categorized into four parts namely watermark insertion, watermark extraction, image authentication and ROI recovery. At first, the ROI is selected from the medical image. It should be noted that the ROI selection might vary for different medical images. Therefore, the 100 × 100 size ROI has been selected (for fragile watermarking) for each image at random from different positions during experimentations. Now the complete medical host image is used for robust watermark insertion. The robust watermarked image is then divided into ROI and RONI regions. After that, the SHA-256 algorithm is used to obtain hash keys for ROI and RONI parts. These hash keys will be used to authenticate the ROI and RONI regions against illegal manipulation and tampering attacks after the fragile watermark extraction. Since the first LSB (least significant bit) of RONI pixels would be used for fragile watermarking, the hash key generation procedure is modified in such a way that it should not interrupt the self/other operations. Figure 1 shows the hash key generation procedure. In the next step, the selected ROI (original) information is compressed using LZW algorithm. This algorithm is lossless in nature and therefore it does not affect the quality of the data during decompression process. The compressed ROI information (recovery data) is then combined with the hash keys (authentication data) to generate the fragile watermark. This fragile watermark is inserted into the RONI portion by replacing the first LSB bits of the pixels. Thus, one watermark bit is inserted into each pixel (used for fragile embedding) of RONI. At last, the dual watermarked image is obtained.

At the extraction process, a trained deep neural network is employed to perform the robust watermark information extraction. This DNN framework is trained on a large dataset consisting of different types of medical images and their attacked forms. Different types of noise, filtering, geometrical, and compression attacks have been used for preparing the training datasets. DNN framework reduces the processing time of extraction process significantly. Further, it can be used for other test images directly to achieve better results. The detailed discussion about the selection of DNN architectures and their outcomes have given in the experimental section. On the other hand, the fragile watermark information was extracted from the RONI pixels. The extracted data is divided into the compressed ROI recovery information and authentication information (i.e., hash keys). Once again, hash key

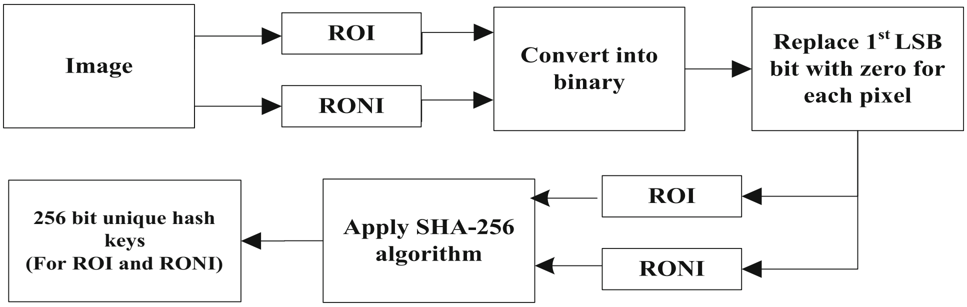


Image
ROI
RONI
Convert into binary
Replace 1st LSB bit with zero for each pixel
ROI
RONI
Apply SHA-256 algorithm
256 bit unique hash keys (For ROI and RONI)

Fig. 1 Hash key generation process

generation is done to generate hash keys for ROI and RONI regions using SHA-256 technique. The image authentication is done based on the comparison of generated and extracted hash key information. The extracted ROI recovery information is then decompressed, which further used for ROI reversibility. The detailed procedure of proposed scheme is presented as follows:

3.1 Watermark insertion

It can be categorized into two parts specifically robust watermark insertion and fragile watermark insertion. It should be noted that the ROI data have to be preserved from the host image before robust watermark insertion. Another important thing to note that the hash keys are obtained after the robust embedding process. The robust watermark embedding process is shown in Fig. 2.

3.1.1 Robust watermark insertion

The steps are given to perform robust watermark insertion process.

1. Select the test medical image and partitioned into uniform parts of 16 × 16-block size. Choose a 1024-bits binary watermark information for embedding.
2. Select blocks in a random fashion to embed one watermark bit into a block. This randomized block selection depends on a secret key (i.e., a value like 4536 etc.).
3. Perform the subsequent steps to embed a robust watermark bit (w_r_{bit}) into a block img_{block}.
4. Apply IWT transform on img_{block} to get four sub-bands LL1, LH1, HL1, and HH1. Again, apply IWT

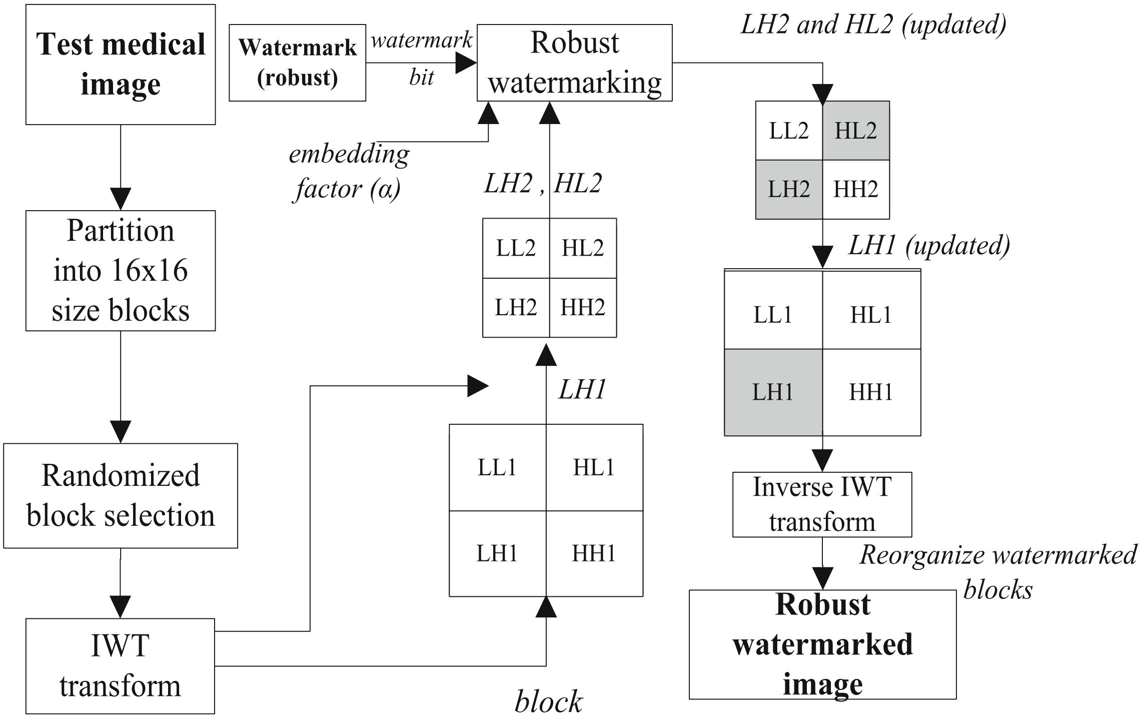


Fig. 2 Robust watermark embedding

transform on LH1 to obtain four sub-bands LL2, LH2, HL2, and HH2.

5. Calculate the average of LH2 and HL2. Further, embed the watermark bit w_r_{bit} by adjusting the coefficient (C) values of LH2 and HL2 sub-bands as described in Eqs. (1) and (2) respectively [28]. Here, α is the embedding factor value, which can be adjusted to set the tradeoff line in between robustness and imperceptibility features.

$$C_{new} = \begin{cases} C - \{\alpha - (Avg_{HL2} - Avg_{LH2})\}/2 & when\ w\_r_{bit} = 1\ and\ Avg_{HL2} - Avg_{LH2} < \alpha \\ C + \{\alpha - (Avg_{LH2} - Avg_{HL2})\}/2 & when\ w\_r_{bit} = 0\ and\ Avg_{LH2} - Avg_{HL2} < \alpha \\ C & otherwise \end{cases} \tag{1}$$

$$C_{new} = \begin{cases} C + \{\alpha - (Avg_{HL2} - Avg_{LH2})\}/2 & when\ w\_r_{bit} = 1\ and\ Avg_{HL2} - Avg_{LH2} < \alpha \\ C - \{\alpha - (Avg_{LH2} - Avg_{HL2})\}/2 & when\ w\_r_{bit} = 0\ and\ Avg_{LH2} - Avg_{HL2} < \alpha \\ C & otherwise \end{cases} \tag{2}$$

Perform inverse IWT transform and obtain the watermarked block w_img_{block}. In the same manner, embed the watermark bits into other blocks. After completing the robust insertion, the robust watermarked image (W_R_{img}) is obtained.

3.1.2 Fragile watermark insertion

The robust watermarked image W_R_{img} is used for embedding the fragile watermark. The fragile watermark embedding process is depicted in Fig. 3. The following steps are used to perform fragile watermark embedding.

1. At first, compress the preserved ROI information (i.e., before robust embedding) using the LZW compression technique.
2. Divide the image W_R_{img} into ROI and RONI segments. RONI region is further divided into two parts namely Embedding region ER_F(used for fragile embedding) and non-embedding region NER_F (not used for embedding).
3. Now generate the hash keys (authentication data) for both ROI and RONI $(ER_F\ and\ NER_F)$ based on SHA-256 algorithm. The hash key generation process is depicted in Fig. 1.
4. Obtain the fragile watermark by combining the recovery data (compressed ROI information in bits) and 768 bits authentication data (hash keys for ROI, ER_F and NER_F).
5. Select the ER_F (RONI pixels) and embed the fragile watermark information (one bit per pixel) by replacing the first LSB bit of the selected pixels.

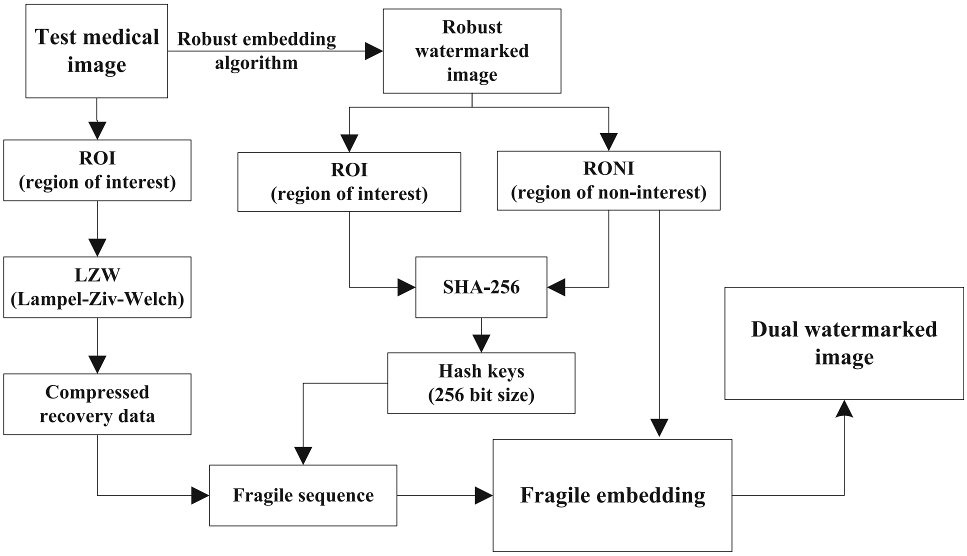


Fig. 3 Fragile watermark embedding

6. After performing the LSB replacement for all fragile watermark information, the dual watermarked image is obtained.

3.2 Watermark extraction

During extraction at the experimental stage, the watermarked images have been influenced by different attacks or signal processing operations. It helps to analyze the performance of the scheme against intentional/natural attacks or processes correctly.

3.2.1 Robust watermark extraction

A DNN framework is developed to extract the watermark data from the received (watermarked/attacked) image. It has been trained with the target data having three copies of the desired watermark information corresponding to each sample input. The proposed DNN framework has three hidden layers with 16, 32, and 16 neurons respectively. The proposed DNN architecture is shown in Fig. 4.

At first, the input and target datasets are prepared to train the proposed DNN framework. The size of input dataset is 256×1198080 and the target dataset size is 3×1198080. Here, each sample of target dataset contains 3 copies of target value for the corresponding input sample. This way, it is observed that the DNN framework performed more efficiently in order to achieve improved results. To prepare the training datasets, more than 100 different types of medical images were used. After the dataset preparation, the datasets are imported to the DNN framework for training. During DNN framework training, the prepared dataset is divided randomly into three subsets namely training data, validation data and testing data. 70% data is used for training, 15% data is used for validation and the remaining 15% data is used for testing. MSE (mean square error) is calculated as a performance measure to examine the performance of the proposed framework as shown in Fig. 5. The learning rate used for the proposed DNN framework is 0.01. The Hyperbolic tangent sigmoid transfer function (TANSIGMOID) is used as a transfer function to activate the neurons. This DNN architecture accepts 256 values as an input in the form of a 256x1 vector and provides 3x1 output. Once the DNN framework gets trained, it can be used for other images (excluding images used for training) to perform robust watermark extraction. The proposed DNN-based robust watermark extraction process is described in Fig. 6 and the extraction steps are as follows:

7. Partitioned the received (attacked/watermarked) image into predefined uniform blocks (i.e., 16 × 16-pixel size) by non-overlapping block-wise division.
8. Select the blocks based on the randomization using secret key. Convert each 16 × 16-pixel size block into a 256 × 1 row vector before using as an input for the proposed DNN framework.
9. After getting output results from the DNN framework, apply round off operation to convert the DNN results into binary (i.e., 1 or 0) watermark information.
10. Since three copies of the watermark information are obtained by the DNN architecture, use the voting mechanism to select the extracted bit value corresponding to each block.
11. Reorganize the resultant (1024-bit information) to generate the extracted robust watermark (i.e., 32 × 32) information.

3.2.2 Fragile watermark extraction

The fragile watermark extraction, authentication and ROI recovery processes are shown in Fig. 7. The subsequent steps are followed to get the fragile watermark information.

1. Divide the received image into ROI and RONI (ER_F and NER_F) regions.
2. Select ER_F for extracting the fragile watermark information. For this, extract the first LSB bit from the RONI pixels (used for embedding) to attain the fragile watermark sequence.

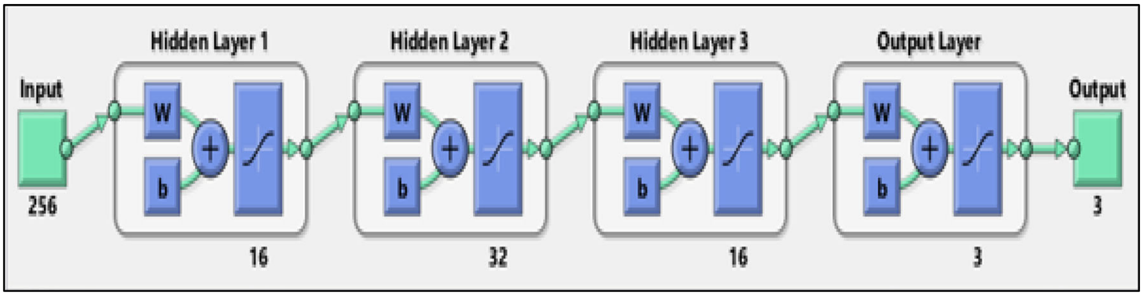
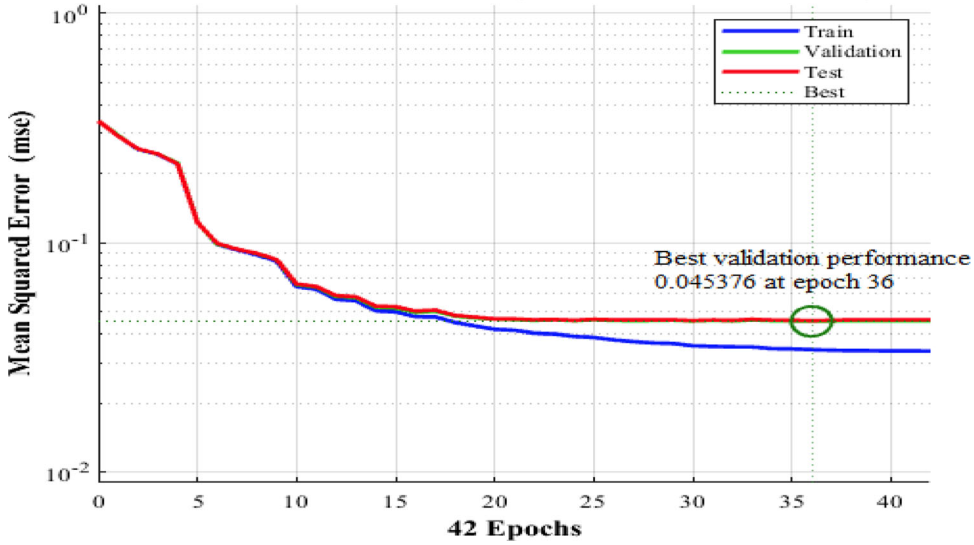


Fig. 4 Robust watermark extraction based on the proposed DNN framework

Fig. 5 Calculated performance measure (MSE) at each epoch during DNN training



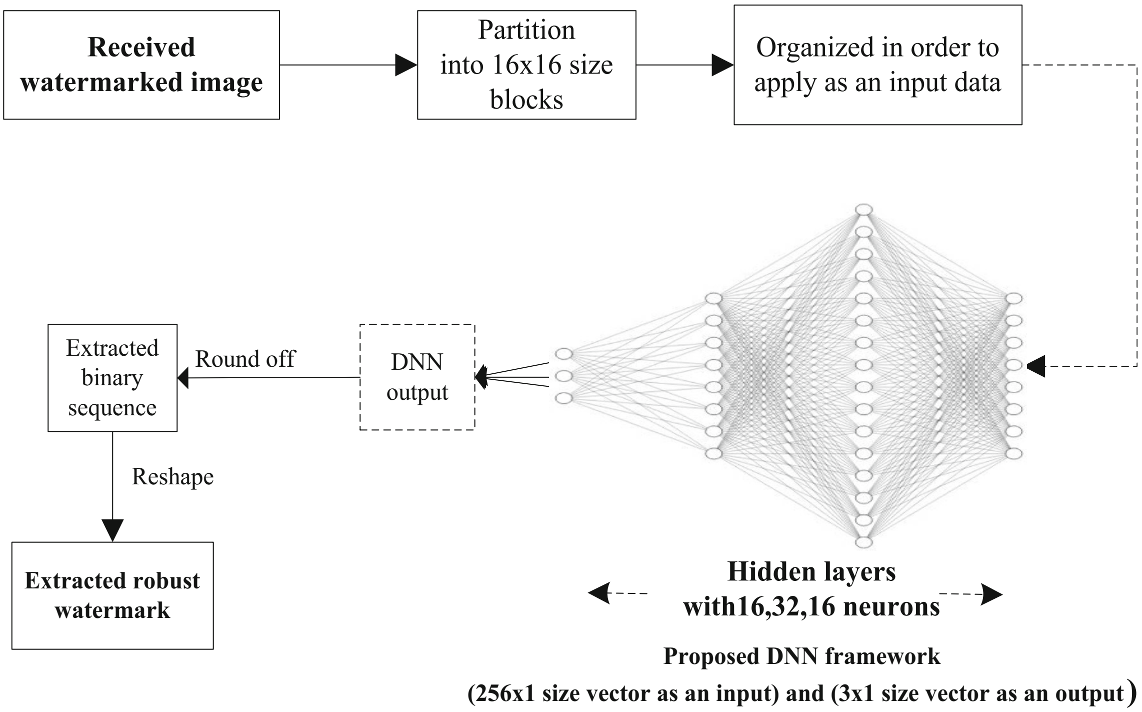

Received watermarked image
Partition into 16x16 size blocks
Organized in order to apply as an input data
DNN output
Round off
Extracted binary sequence
Reshape
Extracted robust watermark
Hidden layers with16,32,16 neurons
Proposed DNN framework
(256x1 size vector as an input) and (3x1 size vector as an output)

Fig. 6 Illustrative presentation of robust watermark extraction based on the proposed DNN framework

3. Separate the extracted data into the authentication data and the ROI recovery information.
4. Get the hash key values for ROI as well as RONI from the extracted authentication data.
5. Use the extracted recovery data to achieve perfect reversibility of the ROI.

3.3 Image authentication and ROI reversibility

Initially, generate the hash keys for ROI and RONI parts using the SHA-256 algorithm as similar to the insertion procedure. Further, compare the generated hash keys with the corresponding extracted key values for authenticating the received image. If the hash key values do not match, it means that the respective portion has been manipulated or

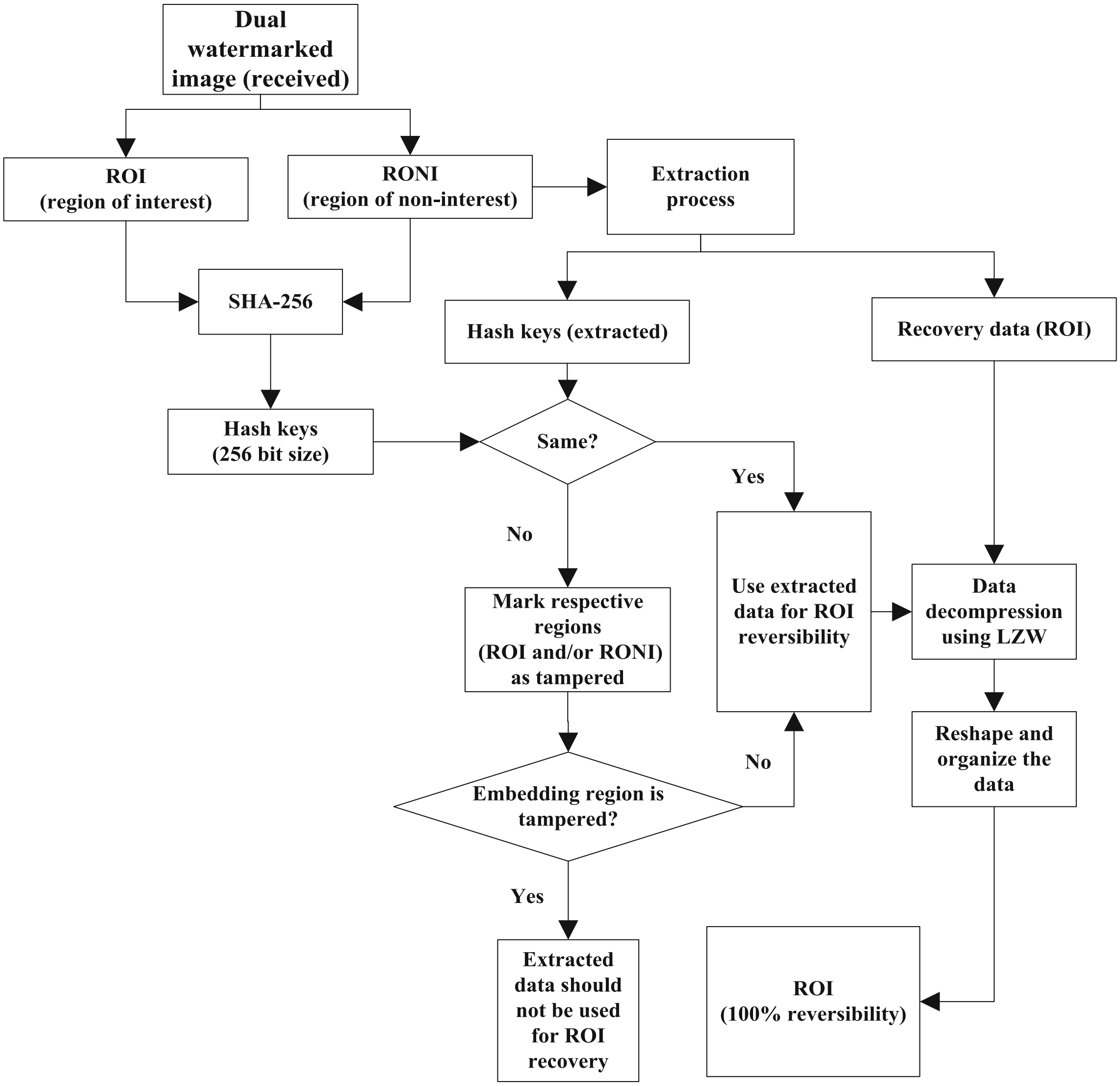

Dual watermarked image (received)
ROI (region of interest)
RONI (region of non-interest)
Extraction process
SHA-256
Hash keys (extracted)
Recovery data (ROI)
Hash keys (256 bit size)
Same?
Yes
No
Use extracted data for ROI reversibility
Data decompression using LZW
Mark respective regions (ROI and/or RONI) as tampered
Reshape and organize the data
No
Embedding region is tampered?
Yes
Extracted data should not be used for ROI recovery
ROI (100% reversibility)

Fig. 7 Fragile watermark extraction, image authentication and ROI reversibility

tampered. If the hash key values are the same, it shows that the respective portion has not been tampered. Nevertheless, the RONI portion has been divided into small segments to achieve better authentication. For instance, the part (i.e., set of pixels) used for fragile watermarking can be considered as one segment (i.e.,ER_F). On the other side, the remaining RONI portion can be considered as another part (i.e.,NER_F). Each part is authenticated with unique hash keys. This way even if the remaining RONI part gets manipulated, it will not affect the authentication and recovery processes. Additionally, the possibility of identifying the accuracy of the extracted information also increases.

4 Experimental results and discussion

The investigational study of the proposed watermarking framework is presented in this section. Different medical images have been selected for the experimentation purpose from the datasets available on Kaggle [29], USC-SIPI [30], and Image database [31]. The test images include normal chest x-ray images, chest x-ray images of patients suffering from COVID-19, brain MRI images, ultrasound images, and other medical images. In addition, other general images are also used for the parametric examination. Over 100 images have been used during DNN training and testing procedures. The test host images are having size 512 × 512 pixels and the robust watermark size is 32 × 32 bits. After the thorough experimentation, the value of embedding factor (α) is selected as 13 to obtain the results because it maintains a significant balance in between

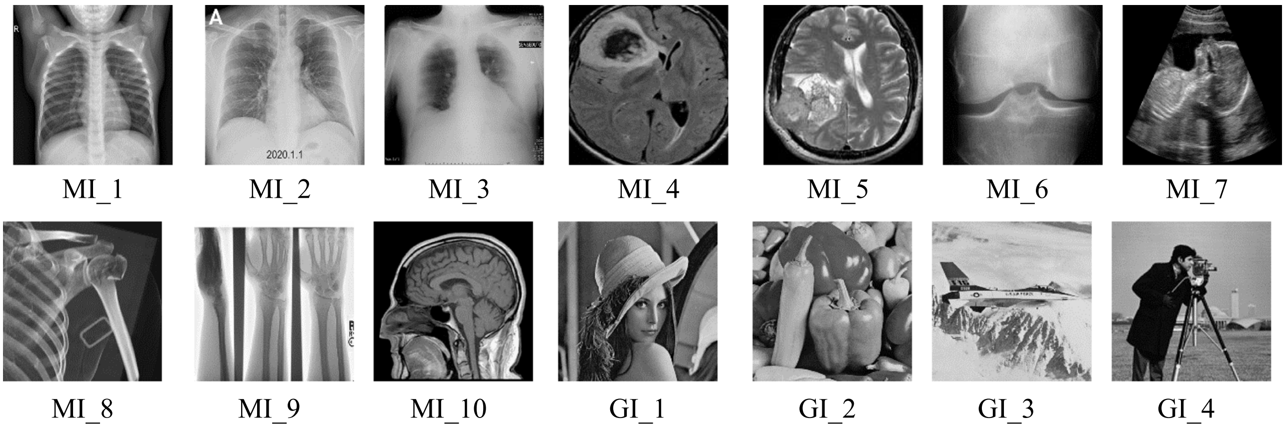


Fig. 8 Test images (512 × 512) including medical images (MI_1 to MI_10), and general images (GI_1 to GI_4)

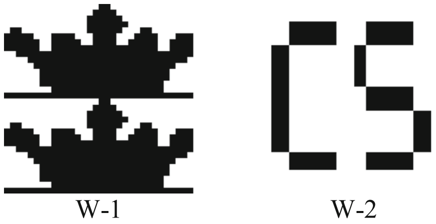


Fig. 9 Robust binary watermark (W-1 and W-2) with size 32 × 32 bits

robustness and imperceptibility. Different watermarking parameters have been utilized to examine the performance of the proposed work. Peak signal to noise ratio (PSNR) and structural similarity index (SSIM) are used for the imperceptibility analysis. PSNR stands for "Peak Signal to Noise Ratio". It is the ratio of signal power to the noise power. It is commonly presented in decibel (dB). In the field of digital image watermarking, it is expected to be high for better imperceptibility feature. SSIM compares the similarity between the images (i.e., host and watermarked images) based on perceptual features like structural information, luminance and contrast features. The mathematical expressions for PSNR and SSIM are depicted in Eqs. (3) and (4) respectively.

$$PSNR(I_h, I_w) = 10\log_{10}\frac{255^2}{MSE(I_h, I_w)}\ Where\ MSE = \frac{1}{N_1 \times N_2}\sum_{p=1}^{N_1}\sum_{q=1}^{N_2}\left(I_{\mathrm{h}_{p,q}} - I_{\mathrm{w}_{p,q}}\right)^2 \tag{3}$$

$$SSIM(I_h, I_{\mathrm{w}}) = l(I_h, I_{\mathrm{w}})c(I_h, I_{\mathrm{w}})s(I_h, I_{\mathrm{w}})$$
$$Where \begin{cases} l(I_h, I_{\mathrm{w}}) = \dfrac{2\mu_{\mathrm{h}},\mu_{\mathrm{w}} + C_{\mathrm{a1}}}{\mu_{\mathrm{h}}^2 + \mu_{\mathrm{w}}^2 + C_{\mathrm{a1}}} \\ c(I_h, I_{\mathrm{w}}) = \dfrac{2\sigma_{\mathrm{h}}\sigma_w + C_{\mathrm{a2}}}{\sigma_{\mathrm{h}}^2 + \sigma_{\mathrm{w}}^2 + C_{\mathrm{a2}}} \\ s(I_h, I_{\mathrm{w}}) = \dfrac{\sigma_{\mathrm{h,w}} + C_{\mathrm{a3}}}{\sigma_{\mathrm{h}}\sigma_w + C_{\mathrm{a3}}} \end{cases} \tag{4}$$

Here, size of the image is $N_1 \times N_2$, the original (host) and the processed (watermarked) images are signified as I_h and I_{w} respectively. μ_{h} and μ_w show the average intensity value of luminance for I_{h} and I_{w} respectively. Similarly, σ_h and σ_{w} indicate the average standard deviation of I_{h} and I_{w} respectively. $\sigma_{\mathrm{h,w}}$ denotes the covariance b/w I_{h} and I_{w}. C_{a1}, C_{a2} and C_{a3} are the constants (to avoid null denominator).

In order to investigate robustness feature, bit error rate (BER) and normalized cross-correlation (NC) are selected as the watermarking parameters for observing the similarity between original and extracted watermark. BER can be defined as the ratio of error bits to the total number of bits. NC is also utilized to verify the resemblance between original and extracted watermark images. The mathematical formulation for BER and NC are given in Eq. (5) and Eq. (6) respectively.

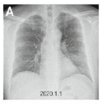
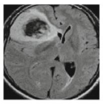
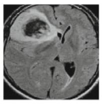
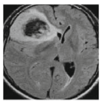
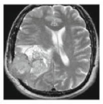
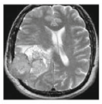
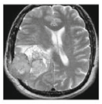
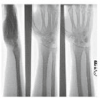
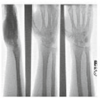
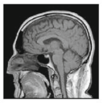
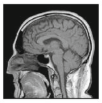
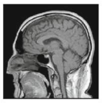
$$BER = \frac{\sum_{m=1}^{x_1}\sum_{\mathrm{n}=1}^{x_2} W_o(m, \mathrm{n}) \otimes W_e(m, n)}{x_1 \times x_2} \tag{5}$$

$$NC = \frac{\sum_{m=1}^{x_1}\sum_{\mathrm{n}=1}^{x_2} W_o(m, n) \times W_e(m, n)}{\sqrt{\sum_{m=1}^{x_1}\sum_{\mathrm{n}=1}^{x_2}[W_o(m, n)]^2} \times \sqrt{\sum_{m=1}^{x_1}\sum_{\mathrm{n}=1}^{x_2}[W_e(m, n)]^2}} \tag{6}$$

where W_o and W_e denote the original and extracted watermark information respectively. x_1 and x_2 present bit positions in binary watermark image. A thorough investigation of the proposed scheme's performance over different test images have done during the experimental study, yet some of the test images are used for the purpose of succinct presentation in this manuscript. The images used in the manuscript are given in Figs. 8, 9.

The imperceptibility analysis for different test images using robust watermark (W-1) is given in Fig. 10. The relative analysis in terms of imperceptibility parameters is shown in Figs. 11, 12 to verify the feasibility of the proposed scheme against different watermarks. For this, two

Fig. 10 Imperceptibility analysis of different test images in terms of visual quality, PSNR, and SSIM

Test images	Original image (host)	Robust watermarked image	Imperceptibility feature (PSNR, SSIM)	Dual watermarked image (robust + fragile)	Imperceptibility feature (PSNR, SSIM)
MI_1			40.39, 0.9460		40.27, 0.9445
MI_2			40.57, 0.9406		40.46, 0.9393
MI_3			40.36, 0.9287		40.26, 0.9272
MI_4			40.74, 0.9490		40.63, 0.9478
MI_5			40.87, 0.9590		40.73, 0.9577
MI_6			40.73, 0.9336		40.61, 0.9320
MI_7			40.57, 0.9348		40.49, 0.9198
MI_8			40.55, 0.9426		40.44, 0.9413
MI_9			41.13, 0.9493		41.03, 0.9482
MI_10			41.25, 0.9481		41.15, 0.9386
GI_1			40.39, 0.9606		40.26, 0.9573
GI_2			40.31, 0.9597		40.20, 0.9588
GI_3			40.27, 0.9494		40.15, 0.9477
GI_4			40.56, 0.9504		40.44, 0.9489

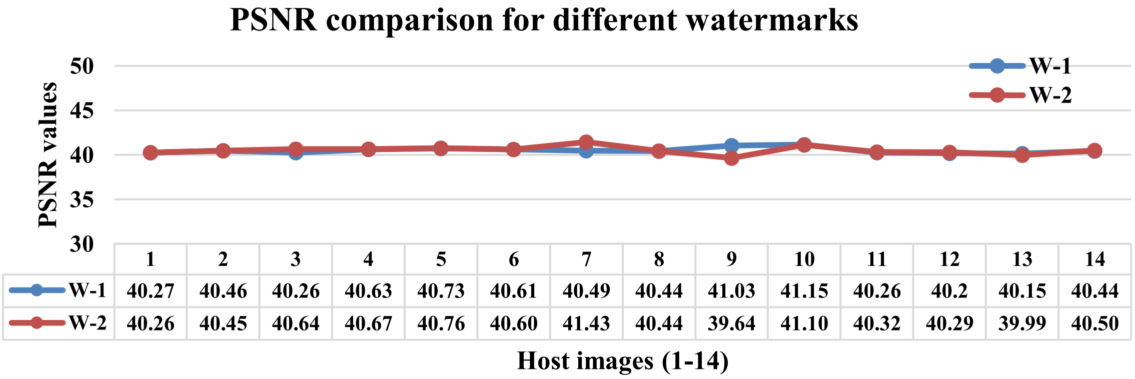


Fig. 11 PSNR (Dual watermarked, Host) comparison for test images while using different watermarks for embedding

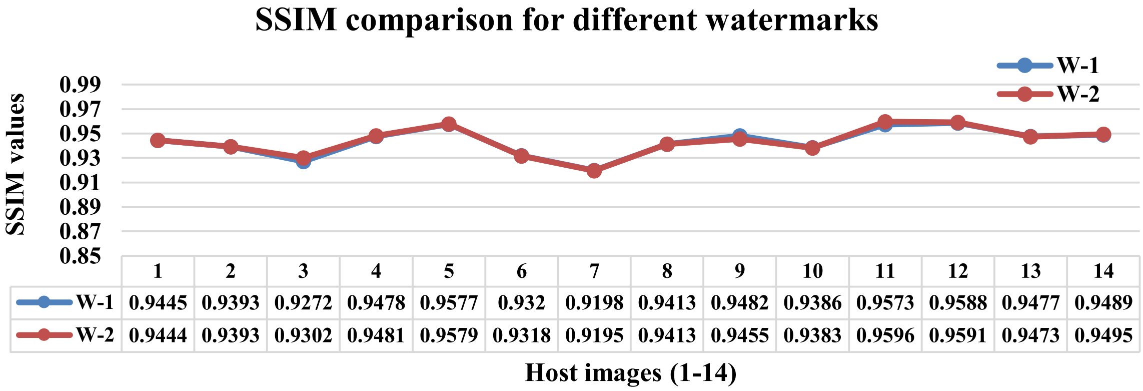


Fig. 12 SSIM (Dual watermarked, Host) comparison for test images while using different watermarks for embedding

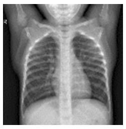
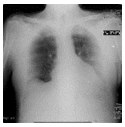
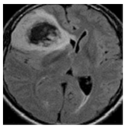
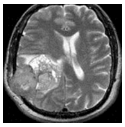
robust watermarks (W-1 and W-2) are used for watermark insertion process. These results show that the proposed scheme provides nearly similar results even for different watermark information. Therefore, the proposed watermarking framework can be utilized for different watermarks without losing the imperceptibility performance.

The proposed DNN framework based robust watermark extraction has been studied carefully for different signal processing attacks. During experimentation, different types of attacks were employed on the dual watermarked image. These attacks include JPEG compression, median filtering (MF), Gaussian filtering (GF), wiener filtering (WF), average filtering (AF), speckle noise, Gaussian noise, salt and pepper noise (S&P), gamma correlation, cropping, sharpening, copy-move, and copy-paste etc. After training, the DNN framework is tested for attacks with different intensity values to check the performance. The following tables (Tables 1 and 2) present the robustness results (BER, NC) for different test images using proposed DNN architecture against 30 processing/intentional attacks.

Figures 13, 14 depict the robustness feature in terms of average parametric values (i.e., average BER and average NC) for each attack. All the test images (presented in the manuscript) have been used to obtain the average robustness results with respect to each attack. Additionally, the application of different watermarks on the proposed scheme is also tested to examine the robust nature. It is found that the robustness results are similar even for dissimilar watermark data. So, the scheme can be utilized with the signals having diverse nature. Since the scheme is designed for medical images and their protection regarding sensitive diagnostic data and patient information, it becomes necessary to perform extensive experimentation on different type of medical images such as X-ray, CT scan, MRI, and ultrasound etc. Therefore, 200 medical images of four different categories (i.e., 50 images from each category) including X-ray [32], CT scan [33, 34], MRI [35–37], and ultrasound images [38, 39] are selected for the experimental investigation. Table 3 illustrates the average parametric results to clarify the performance of the proposed scheme in terms of watermarking features like imperceptibility and robustness.

The comparison with the existing watermarking schemes is given in the following tables (Tables 4, 5, and 6) for same payload (robust watermark size). However, it should be noted that the proposed scheme also embeds fragile sequence (authentication and recovery information). Thus, the actual embedding capacity of the proposed

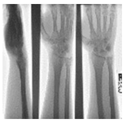
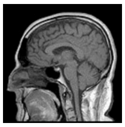
Table 1 Robustness analysis in terms of BER and NC for test images (MI_1 to MI_7) against attacks using robust watermark (W-1)

S. no	Attacks	Test images													
		MI_1		MI_2		MI_3		MI_4		MI_5		MI_6		MI_7	
															
		BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC
1	No attack	0	1	0	1	0	0.99	0	1	0	1	0	1	0	1
2	Speckle (0.001)	0	1	0	1	0	0.99	0	1	0	1	0	1	0	1
3	Speckle (0.005)	0	1	0.01	0.98	0.01	0.98	0	1	0	0.99	0	0.99	0	1
4	Gaussian (0.001)	0	1	0	0.99	0.01	0.99	0	1	0	0.99	0	1	0.03	0.94
5	Gaussian (0.005)	0.04	0.91	0.03	0.93	0.05	0.90	0.04	0.91	0.05	0.89	0.04	0.92	0.12	0.76
6	S & P (0.001)	0	1	0	1	0	0.99	0	1	0	1	0	1	0.01	0.99
7	S & P (0.005)	0	0.99	0.01	0.98	0.01	0.98	0	0.99	0.01	0.98	0.01	0.99	0.03	0.93
8	Median filter 2 × 2	0.01	0.99	0.01	0.98	0.03	0.94	0	0.99	0	1	0.01	0.98	0.01	0.99
9	Median filter 3 × 3	0.01	0.97	0.01	0.99	0.03	0.93	0	0.99	0.02	0.96	0.01	0.98	0.05	0.90
10	Wiener filter 2 × 2	0	0.99	0.01	0.98	0.01	0.97	0	1	0	1	0	1	0	0.99
11	Wiener filter 3 × 3	0	1	0	0.99	0	0.99	0	1	0	1	0	1	0	1
12	Gaussian filter 2 × 2	0	1	0	0.99	0.01	0.98	0	1	0	1	0	1	0	1
13	Gaussian filter 3 × 3	0	1	0	0.99	0.02	0.96	0	1	0	1	0	1	0	0.99
14	Average filter 3 × 3	0.03	0.94	0.02	0.95	0.03	0.94	0.01	0.98	0.01	0.97	0.03	0.95	0.03	0.95
15	Sharpening (0.2)	0	1	0	0.99	0	0.99	0	1	0	1	0	1	0	1
16	Sharpening (0.8)	0	1	0	1	0	0.99	0	1	0	1	0	1	0	1
17	Gamma correlation (0.6)	0	1	0	0.99	0	0.99	0	1	0	1	0	1	0	1
18	Gamma correlation (0.8)	0	1	0	0.99	0	0.99	0	1	0	1	0	1	0	1
19	Resize (0.5, 2)	0.04	0.93	0.04	0.91	0.04	0.91	0.04	0.91	0.05	0.89	0.02	0.95	0.09	0.82
20	Resize (2, 0.5)	0	1	0	0.99	0	0.99	0	1	0	1	0	1	0	1
21	Crop 5% @ centre	0.02	0.96	0.02	0.95	0.02	0.95	0.02	0.96	0.02	0.96	0.02	0.96	0.02	0.96
22	Crop 10% @ centre	0.05	0.91	0.05	0.90	0.05	0.90	0.05	0.91	0.05	0.91	0.04	0.91	0.05	0.91
23	Motion blur (θ = 7, len = 10)	0.01	0.99	0	0.99	0.01	0.97	0	1	0	1	0.01	0.98	0	0.99
24	Copy-move (60 × 60 pixel)	0.01	0.98	0.01	0.98	0.01	0.98	0.01	0.99	0.01	0.98	0.01	0.98	0.01	0.98
25	Copy-paste (60 × 60 pixel)	0	0.99	0.01	0.99	0.01	0.99	0	0.99	0	0.99	0	0.99	0	0.99
26	Histogram equalization	0	1	0	0.99	0	1	0	1	0	1	0	1	0	1
27	JPEG 50	0	1	0	0.99	0.01	0.97	0.01	0.99	0.03	0.94	0	1	0.15	0.71
28	JPEG 60	0	1	0	0.99	0.01	0.98	0	1	0	1	0	1	0.14	0.73
29	JPEG 70	0	1	0	0.99	0	0.99	0	1	0	1	0	1	0.06	0.89
30	JPEG 80	0	1	0	0.99	0	0.99	0	1	0	1	0	1	0	1

scheme is quite high than the other schemes. Even then, the average PSNR and average SSIM values are maintained at 40 dB, and 0.95 respectively. Moreover, the visual quality of the dual watermarked image is high and the viewers are not able to notice the embedded information. Table 4 confirms that the proposed scheme has decent imperceptibility even after having high payload. The robustness is also high as compared to the other schemes (as given in Tables 5 and 6).

After studying the robust nature of the proposed scheme, it is observed that the scheme can be used for robust applications for protecting electronic patient record (EPR) or ownership of medical images. Moreover, the scheme can also be used for other general images to verify the

Table 2 Robustness analysis in terms of BER and NC for test images (MI-8 to GI_4) against attacks using robust watermark (W-1)

S. no	Attacks	Test images													
		MI_8		MI_9		MI_10		GI_1		GI_2		GI_3		GI_4	
															
		BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC
1	No attack	0	1	0	0.99	0	1	0	1	0	1	0	0.99	0	1
2	Speckle (0.001)	0	1	0	0.99	0	1	0	1	0	1	0	0.99	0	1
3	Speckle (0.005)	0	1	0.03	0.94	0	1	0	1	0	1	0.01	0.98	0	1
4	Gaussian (0.001)	0	1	0.01	0.98	0.02	0.96	0	1	0	1	0	0.99	0	1
5	Gaussian (0.005)	0.03	0.94	0.05	0.91	0.09	0.81	0.04	0.93	0.04	0.93	0.04	0.91	0.04	0.92
6	S & P (0.001)	0	1	0.01	0.99	0	0.99	0	1	0	1	0	0.99	0	1
7	S & P (0.005)	0	1	0.01	0.98	0.02	0.95	0.01	0.98	0	0.99	0.01	0.98	0.01	0.99
8	Median filter 2 × 2	0.01	0.99	0.04	0.93	0.02	0.96	0.04	0.91	0.03	0.94	0.04	0.91	0.02	0.95
9	Median filter 3 × 3	0	0.99	0.07	0.85	0.03	0.95	0.03	0.93	0.06	0.88	0.06	0.88	0.01	0.99
10	Wiener filter 2 × 2	0	1	0.02	0.96	0.01	0.98	0.02	0.95	0.01	0.97	0.04	0.92	0.01	0.98
11	Wiener filter 3 × 3	0	1	0	0.99	0	1	0	1	0	1	0	0.99	0	1
12	Gaussian filter 2 × 2	0	1	0.02	0.96	0	1	0.01	0.99	0	1	0.02	0.96	0	1
13	Gaussian filter 3 × 3	0	1	0.03	0.94	0.01	0.99	0.02	0.97	0.02	0.96	0.05	0.91	0	0.99
14	Average filter 3 × 3	0.02	0.95	0.07	0.85	0.03	0.94	0.07	0.86	0.06	0.88	0.10	0.80	0.06	0.87
15	Sharpening (0.2)	0	1	0	0.99	0	1	0	1	0	1	0	1	0	1
16	Sharpening (0.8)	0	1	0	1	0	1	0	1	0	1	0	1	0	1
17	Gamma correlation (0.6)	0	1	0	1	0	1	0	1	0	1	0	0.99	0	1
18	Gamma correlation (0.8)	0	1	0	1	0	1	0	1	0	1	0	1	0	1
19	Resize (0.5, 2)	0.04	0.93	0.08	0.83	0.09	0.81	0.07	0.86	0.07	0.85	0.11	0.78	0.08	0.84
20	Resize (2, 0.5)	0	1	0	0.99	0	1	0	0.99	0	1	0.01	0.99	0	1
21	Crop 5% @ centre	0.02	0.96	0.02	0.95	0.02	0.96	0.02	0.95	0.02	0.96	0.03	0.95	0.02	0.96
22	Crop 10% @ centre	0.05	0.90	0.05	0.90	0.05	0.90	0.05	0.91	0.05	0.91	0.05	0.91	0.05	0.90
23	Motion blur (θ = 7, len = 10)	0	1	0.03	0.94	0	0.99	0	0.99	0.02	0.96	0.04	0.92	0.01	0.98
24	Copy-move (60 × 60 pixel)	0.01	0.99	0.01	0.98	0.01	0.99	0.01	0.99	0.01	0.99	0.01	0.98	0.01	0.98
25	Copy-paste (60 × 60 pixel)	0	0.99	0.01	0.99	0	0.99	0	0.99	0	0.99	0.01	0.99	0	0.99
26	Histogram equalization	0	1	0	1	0	0.99	0	0.99	0	1	0.01	0.98	0	0.99
27	JPEG 50	0	1	0.02	0.97	0.09	0.82	0.01	0.98	0	0.99	0.02	0.96	0	0.99
28	JPEG 60	0	1	0.01	0.97	0.08	0.85	0.01	0.98	0	0.99	0.02	0.96	0	0.99
29	JPEG 70	0	1	0.01	0.98	0.02	0.95	0.01	0.99	0	0.99	0.02	0.96	0.01	0.99
30	JPEG 80	0	1	0	0.99	0	1	0	0.99	0	1	0.01	0.98	0	0.99

ownership or copyright. The DNN based framework makes the scheme fast and effective, so it can be used for the applications that require rapid response without losing other parameter's quality. The average processing time for the embedding and extraction procedures are 0.7194 s and 0.0724 s respectively. It is obvious that the scheme can be useful for the real-time or fast response watermarking applications. A comparison of the computational time for watermark insertion and watermark extraction procedures has been presented in Table 7 in order to investigate the practicability of the proposed robust watermarking mechanism in terms of efficient and fast processing. From the analysis of computational time (as presented in Table 7), it is observed that the proposed scheme needs less

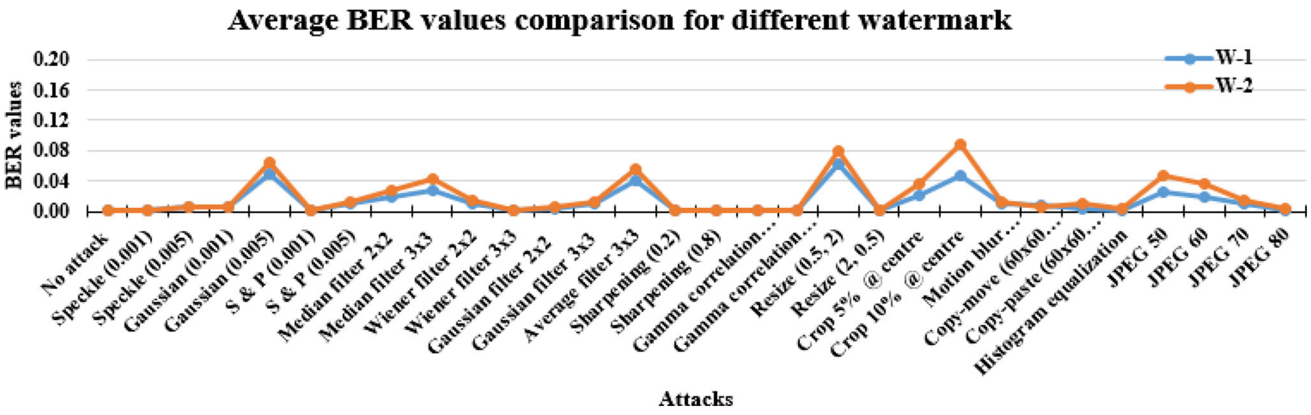


Fig. 13 Average BER comparison for different watermarks against attacks (while using different test images)

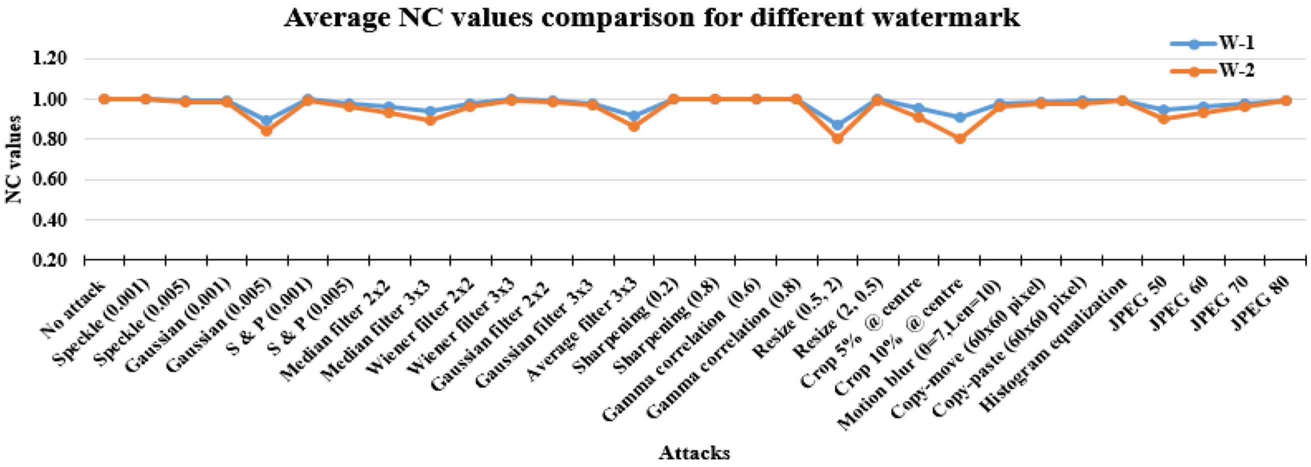


Fig. 14 Average NC comparison for different watermarks against attacks (while using different test images)

computational time as compared to the other schemes. Therefore, it can be used as an improved alternative for real-time applications regarding ownership/copyright verification.

The proposed scheme is also having the fragile nature and able to authenticate the medical images accurately. It is important because the medical image contain sensitive information, which is used to diagnose the health issues. Further, the scheme can recover the ROI part with the completely reversible nature. During the fragile watermarking, the LZW compression technique is used to improve the payload in a lossless manner. For the testing, a portion of 100 × 100 pixels is considered as the ROI portion. The remaining part of the image is considered as the RONI portion, which further classifies into the portions namely the embedding region (ER_F) and the non-embedding region (NER_F). The embedding region ER_F is used to embed the fragile watermark sequence, which contains the authentication data (hash keys) and the ROI recovery data. The non-embedding region (NER_F) has no change due to fragile embedding. This way, even if NER_F is tampered, it does not affect the extracted data and the ROI reversibility is possible. If ER_F is tampered then the extracted data is not suitable to use for further actions. In both the cases, the image authentication is helpful to verify the correctness of the extracted data. An illustrative sample image is represented in Fig. 15 to demonstrate the ROI and RONI regions of the image. Table 8 shows the investigational results for fragile watermarking to confirm its usability.

The obtained results confirms that the proposed scheme has an effective medical image authentication and ROI reversibility. It also alerts about the correctness of the extracted fragile data by separately authenticating the ER_F (RONI embedding region), NER_F (RONI non-embedding region), and ROI. Thus, it provides added precautions regarding patient's health. As shown in Table 9, the existing studies available in the literature lacks in RONI authentication, which may lead to the unauthentic extracted data and further wrong diagnosis. It can harm patient's health due to erroneous treatment. In the proposed scheme, this issue has been taken into consideration and RONI authentication is provided for the same. Hence, the

Table 3 Experimental investigation in terms of average parametric results (PSNR, SSIM, BER, NC) for different type of medical images

S. no	Attacks	X-ray PSNR_{avg} = 40.67 SSIM_{avg} = 0.93		CT scan PSNR_{avg} = 40.91 SSIM_{avg} = 0.92		MRI PSNR_{avg} = 41.27 SSIM_{avg} = 0.92		Ultrasound PSNR_{avg} = 40.60 SSIM_{avg} = 0.95	
		BER_{avg}	NC_{avg}	BER_{avg}	NC_{avg}	BER_{avg}	NC_{avg}	BER_{avg}	NC_{avg}
1	No attack	0.00	1.00	0.00	0.99	0.00	0.99	0.00	1.00
2	Speckle (0.001)	0.00	1.00	0.00	0.99	0.00	0.99	0.00	1.00
3	Speckle (0.005)	0.00	0.99	0.00	0.99	0.00	0.99	0.00	0.99
4	Gaussian (0.001)	0.01	0.99	0.02	0.95	0.02	0.94	0.01	0.98
5	Gaussian (0.005)	0.06	0.86	0.08	0.81	0.12	0.75	0.07	0.84
6	S & P (0.001)	0.00	0.99	0.01	0.99	0.01	0.98	0.00	0.99
7	S & P (0.005)	0.01	0.97	0.03	0.93	0.03	0.92	0.01	0.97
8	Median filter 2 × 2	0.01	0.98	0.02	0.95	0.02	0.95	0.02	0.96
9	Median filter 3 × 3	0.06	0.88	0.11	0.78	0.12	0.76	0.04	0.91
10	Wiener filter 2 × 2	0.00	0.99	0.01	0.97	0.02	0.96	0.01	0.97
11	Wiener filter 3 × 3	0.00	1.00	0.00	0.99	0.00	0.99	0.00	1.00
12	Gaussian filter 2 × 2	0.00	0.99	0.01	0.97	0.01	0.98	0.00	0.99
13	Gaussian filter 3 × 3	0.00	0.99	0.03	0.93	0.02	0.96	0.01	0.97
14	Average filter 3 × 3	0.02	0.94	0.04	0.92	0.04	0.92	0.05	0.88
15	Sharpening (0.2)	0.00	1.00	0.00	0.99	0.00	0.99	0.00	1.00
16	Sharpening (0.8)	0.00	1.00	0.00	0.99	0.00	0.99	0.00	1.00
17	Gamma correlation (0.6)	0.00	1.00	0.00	1.00	0.00	1.00	0.00	1.00
18	Gamma correlation (0.8)	0.00	1.00	0.00	1.00	0.00	1.00	0.00	1.00
19	Scaling (0.5)	0.06	0.87	0.08	0.82	0.09	0.80	0.10	0.78
20	Scaling (2)	0.00	1.00	0.00	0.99	0.01	0.99	0.00	0.99
21	Crop 5% @ centre	0.03	0.93	0.03	0.93	0.03	0.93	0.03	0.94
22	Crop 10% @ centre	0.07	0.85	0.07	0.85	0.07	0.85	0.07	0.85
23	Motion blur (θ = 7, len = 10)	0.01	0.99	0.01	0.98	0.01	0.97	0.02	0.96
24	Copy-move (60 × 60 pixel)	0.01	0.98	0.01	0.98	0.01	0.98	0.01	0.98
25	Copy-paste (60 × 60 pixel)	0.01	0.98	0.01	0.98	0.01	0.97	0.01	0.98
26	Histogram equalization	0.00	1.00	0.00	1.00	0.00	0.99	0.00	0.99
27	JPEG 50	0.04	0.92	0.12	0.77	0.18	0.69	0.06	0.88
28	JPEG 60	0.03	0.94	0.12	0.77	0.17	0.71	0.05	0.91
29	JPEG 70	0.01	0.99	0.03	0.93	0.04	0.91	0.01	0.98
30	JPEG 80	0.00	0.99	0.01	0.98	0.01	0.98	0.00	0.99

Table 4 Comparative investigation in terms of different watermarking features with existing schemes [17, 23] and [24]

Features	Watermarking schemes			
	Lai [17]	Ernawan and Kabir [23]	Pourhadi and Nasab [24]	Proposed scheme
Payload	32 × 32 bits	32 × 32 bits	32 × 32 bits	Robust watermark = 32 × 32 bits Fragile watermark = 768 bits ROI recovery data ≤ 80,000 bits
Avg. PSNR	48 dB	45 dB	40 dB	40 dB
Avg. SSIM	–	0.99	0.99	0.95
Avg. BER	0.13	0.07	0.09	**0.03**
Avg. NC	–	0.89	0.81	**0.96**

Table 5 Comparative robustness analysis with [17] and [23] in terms of BER for test images against different processing attacks

S. No	Attacks	Test images								
		Lai [17]	Ernawan and Kabir [23]	proposed	Lai [17]	Ernawan and Kabir [23]	proposed	Lai [17]	Ernawan and Kabir [23]	proposed
1	No Attack	0	0	0	0.01	0	0	0.10	0	0
2	Average filter 3 × 3	0.22	0	0.08	0.28	0.01	0.11	0.32	0.01	0.08
3	Wiener filter 3 × 3	0.21	0.01	0.02	0.28	0.01	0.04	0.32	0	0
4	Median filter 3 × 3	0.21	0.01	0.04	0.21	0.01	0.06	0.22	0.01	0.01
5	Gaussian filter 3 × 3	0.03	0	0	0.08	0	0.01	0.12	0	0
6	Gaussian (0.01)	0.37	0.06	0	0.35	0.07	0	0.41	0.07	0
7	Speckle (0.001)	0.27	0	0	0.34	0.03	0	0.27	0	0
8	S&P (0.01)	0.23	0.17	0.02	0.19	0.12	0.02	0.26	0.13	0.02
9	S&P (0.001)	0.03	0.02	0	0.03	0.03	0	0.12	0.02	0
10	Poisson Noise	0.43	0.23	0	0.44	0.27	0.02	0.44	0.02	0.01
11	JPEG 20	0.49	0.50	0.38	0.45	0.50	0.35	0.50	0.50	0.45
12	JPEG 30	0.20	0.24	0.07	0	0.28	0.12	0.29	0.29	0.08
13	JPEG 40	0.04	0.16	0.01	0	0.17	0.02	0.24	0.13	0
14	JPEG 50	0.01	0	0.01	0	0	0.02	0.26	0	0
15	JPEG 60	0	0	0.01	0	0	0.02	0.25	0	0
16	JPEG 70	0	0	0.01	0	0	0.02	0.25	0	0.01
17	JPEG 80	0	0	0.01	0	0	0.01	0.20	0	0
18	JPEG 90	0	0	0	0	0	0	0.13	0	0
19	JPEG 2K [2]	0	0	0	0	0	0	0.09	0	0
20	JPEG 2 K [4]	0	0	0	0	0	0	0.09	0	0
21	JPEG 2 K [6]	0	0	0	0	0	0	0.13	0	0
22	JPEG 2 K [8]	0.01	0.01	0.02	0	0.01	0.01	0.16	0	0
23	JPEG 2 K [10]	0.03	0.02	0.04	0	0.06	0.06	0.19	0	0
24	Scaling (0.8)	0.10	0	0.01	0.17	0	0.03	0.21	0	0.01
25	Scaling (0.5)	0.23	0.32	0.08	0.31	0.32	0.12	0.36	0.31	0.09
26	SPN (0.003) + MF [3,3]	0.21	0.01	0.04	0.21	0.01	0.07	0.22	0	0.01
Average results		0.13	0.07	0.03	0.13	0.07	0.04	0.24	0.06	0.03

proposed scheme has superior features than the existing work available in the literature of medical image watermarking schemes. This analysis with respect to other existing medical image watermarking methods favors the performance and superiority of the proposed work.

As shown in Table 9, many watermarking techniques were developed earlier for medical imaging. Some of them provide robust nature and can be used only for EPR/ownership protection such as [19, 21], and [22]. Many schemes like [18], and [20] can be utilized for tamper detection and ROI recovery. A very few schemes like [26] provide multipurpose nature and can be used for robust as well as fragile applications simultaneously. However, their practicability for many watermarking applications is limited due to their non-blind nature. Also, the use of optimization and other processing operations increases the processing time; which limits the use of the schemes for real-time or fast processing applications. Most of the existing fragile schemes available in the literature utilized the RONI region for the watermark insertion process, but none of them

Table 6 Comparative robustness analysis with [24] in terms of BER and NC for test images against different processing attacks

S. no	Attacks	Test images											
		NC		BER		NC		BER		NC		BER	
		Pourhadi and Nasab [24]	Proposed	Pourhadi and Nasab [24]	Proposed	Pourhadi and Nasab [24]	Proposed	Pourhadi and Nasab [24]	Proposed	Pourhadi and Nasab [24]	Proposed	Pourhadi and Nasab [24]	Proposed
1	JPEG [85]	0.82	0.99	0.08	0	0.89	1	0.05	0	0.86	0.99	0.06	0
2	JPEG [90]	0.97	0.99	0.01	0	0.98	1	0.01	0	0.98	1	0.01	0
3	JPEG [95]	1	1	0	0	1	1	0	0	1	1	0	0
4	Gaussian filter 3 × 3	1	1	0	0	1	1	0	0	1	1	0	0
5	Average filter 3 × 3	0.28	0.82	0.40	0.08	0.29	0.84	0.40	0.07	0.28	0.83	0.40	0.08
6	Wiener filter 3 × 3	0.39	0.96	0.24	0.02	0.33	0.95	0.26	0.02	0.22	0.99	0.31	0
7	Speckle (0.001)	1	1	0	0	1	1	0	0	1	1	0	0
8	Speckle (0.005)	1	1	0	0	0.99	1	0.01	0	0.98	1	0.01	0
9	Speckle (0.009)	0.96	0.98	0.02	0.01	0.96	0.97	0.02	0.01	0.96	0.97	0.02	0.01
10	Gaussian (0.001)	0.99	1	0	0	0.99	1	0	0	0.99	0.99	0	0
11	Gaussian (0.005)	0.85	0.90	0.06	0.04	0.83	0.91	0.07	0.04	0.84	0.90	0.07	0.04
12	Gaussian (0.009)	0.72	0.79	0.12	0.09	0.72	0.79	0.12	0.10	0.72	0.77	0.12	0.11
13	Scaling (2)	1	0.99	0	0	1	1	0	0	1	1	0	0
14	Scaling (0.9)	0.80	0.99	0.09	0.01	0.67	0.99	0.12	0	0.75	1	0.16	0
15	Scaling (0.7)	0.48	0.96	0.26	0.01	0.37	0.97	0.23	0.01	0.53	0.98	0.31	0.01
Average results		0.82	0.96	0.09	0.02	0.80	0.96	0.09	0.02	0.81	0.96	0.10	0.02

Table 7 Computational time comparison (in seconds) with the existing schemes [9, 17], and [10]

Methods	Images			
	Lena		Pepper	
	Embedding	Extraction	Embedding	Extraction
Lai [17]	2.58	0.63	2.33	0.63
Makbol et al. [9]	14.27	5.72	14.36	5.66
Ernawan and Kabir [10]	84.32	25.53	86.3	25.31
Proposed scheme	0.70	0.07	0.71	0.07

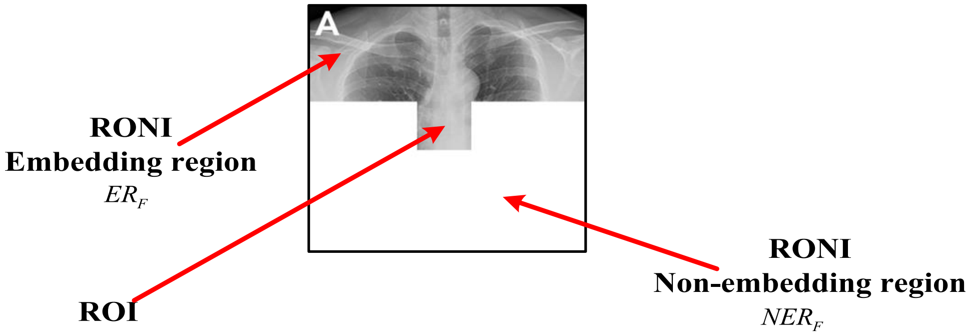


Fig. 15 An illustrative sample of division of an image into ROI and RONI regions

provided authentication for the region used for watermark insertion. Due to this, it could not be verified whether the extracted watermark information is accurate. Further, this extracted information (from the unauthenticated RONI region) has been directly used for ROI restoration in many schemes. It can harm or modify the ROI information significantly, which can further affect the diagnosis process and the patient's health. The proposed scheme provides effective and competent solutions to such existing issues. The proposed DNN-based robust watermark extraction process requires very low processing time and can be used for fast processing (real-time) applications. The proposed scheme has a multipurpose nature and can be used for robust and fragile applications at the same time. The fragile watermarking mechanism of the proposed scheme provides authentication of ROI as well as RONI (i.e., fragile watermark embedding region), which ensures the authenticity of the extracted watermark (authentication + recovery information) more effectively. The proposed scheme also has a significant imperceptibility, high robustness, high capacity, and enhanced security features. The comparative analysis in Table 9 establishes the fact that the proposed work provides an effective multipurpose nature for solving existing medical imaging issues.

5 Conclusion

This work offered a deep neural network-based image watermarking scheme for medical images. The scheme can be used to protect EPR/ownership in an efficient and quick manner. It also provides accurate image authentication and ROI reversibility. The IWT transform and randomize block selection based robust embedding was used to embed the robust watermark data. Further, LSB bit replacement based fragile embedding was performed in RONI embedding region (ER_F). The LZW compression technique was employed to preserve the ROI data to enhance the embedding capacity. On the other side, SHA-256 algorithm-based hash keys were used to authenticate the ROI and both RONI regions (ER_F and NER_F). At extraction, the proposed DNN architecture was used to extract the robust watermark information to verify the ownership. The fragile extraction would be used to extract the authentication information and recovery data. After the SHA-256 based authentication, if the RONI embedding region ER_F is found intact (not tampered) then the ROI region would be recovered with completely reversible nature using extracted recovery data. Experimental testing shows that the presented work has multipurpose nature and effective performance as compared to other schemes. Future work includes the improvement in the performance against other kinds of geometric attacks such as rotation etc. The pos-

Table 8 Fragile watermarking results with ROI reversibility

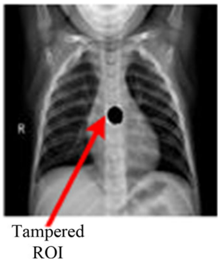
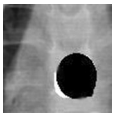
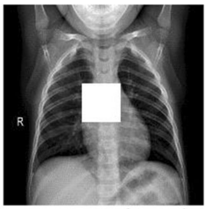
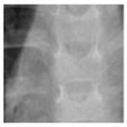
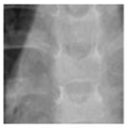
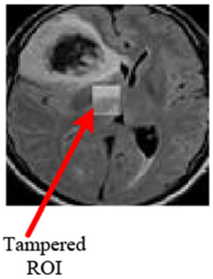
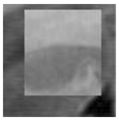
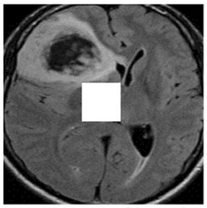
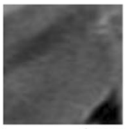
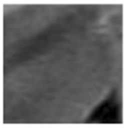
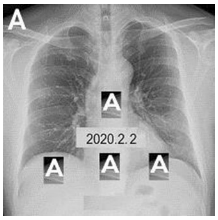
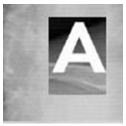
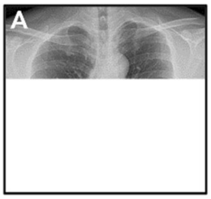
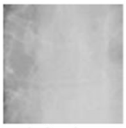
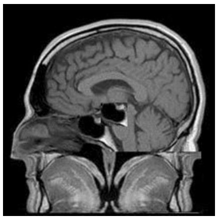
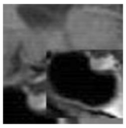
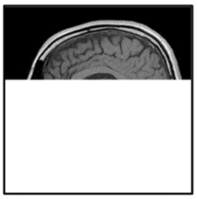
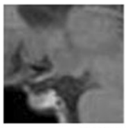
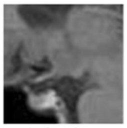
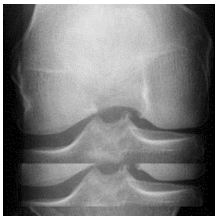
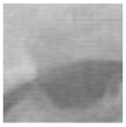
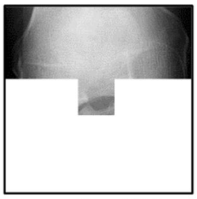
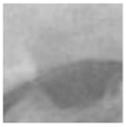
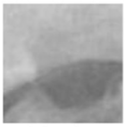
Attack type	Attacked image	ROI (Attacked image)	Tamper authentication	ROI (Recovered and original)	Observations
When a small part of ROI is tampered (content removal attack)			 Compete ROI is marked as tampered	 Recovered ROI  Original ROI	A tampered ROI is authenticated, and recovered with complete reversible nature. The PSNR between original ROI and the recovered ROI is $\propto$
When a large portion of ROI is tampered (copy paste attack)			 Compete ROI is marked as tampered	 Recovered ROI  Original ROI	A tampered ROI is authenticated, and recovered with complete reversible nature The PSNR between original ROI and the recovered ROI is $\propto$
When ROI as well as NER_F get tampered (illegal text editing + copy-move attack)			 ROI as well as NER_F are marked as tampered	 Recovered ROI  Original ROI	A tampered ROI and NER_F are authenticated, and the ROI is recovered with complete reversible nature The PSNR between original ROI and the recovered ROI is $\propto$
When ROI as well as NER_F get tampered (illegal editing + copy-move attack)			 ROI as well as NER_F are marked as tampered	 Recovered ROI  Original ROI	A tampered ROI and NER_F are authenticated, and the ROI is recovered with complete reversible nature The PSNR between original ROI and the recovered ROI is $\propto$
When only NER_F get tampered (Forgery)		 ROI is not tampered	 ROI as well as NER_F are marked as tampered	 Recovered ROI  Original ROI	A tampered RONI region (NER_F) is authenticated, and the ROI is recovered with complete reversible nature The ROI is not tampered but reversibility is required, as the ROI had been used for robust watermarking The PSNR between original ROI and the recovered ROI is $\propto$

Table 9 Subjective comparison with already proposed medical image watermarking methods

S. No	Characteristics		Das and Kundu [18]	Lei et al. [19]	Badshah et al. [20]	Thakkar and Srivastava [21]	Thanki et al. [22]	Alshanbari [26]	Proposed scheme
1	Implemented for medical imaging		Yes	Yes	Yes	Yes	Yes	Yes	Yes
2	Nature of the scheme		Fragile	Robust	Fragile	Robust	Robust	Robust + Fragile	Robust + Fragile
3	Watermarking domain		Spatial	Transform	Spatial	Transform	Transform	Transform + spatial	Transform + spatial
4	Nature of extraction		Blind	Blind	Blind	Blind	Blind	Non-blind	Blind
5	Imperceptibility (PSNR)		~ 44 dB	~ 48 dB	~ 51 dB	~ 45 dB	~ 50 dB	~ 48 dB	~ 40 dB
6	Payload capacity		High	High	High	Medium	High	High	High
7	Robustness		–	–	–	Medium	Poor	Poor	High
8	Copyright/EPR Protection		No	No	No	Yes	Yes	Yes	Yes
9	Tamper identification	ROI	Yes	No	Yes	No	No	Yes	Yes
		RONI	No	No	No	No	No	No	Yes
10	Region-wise Tamper Localization		No	No	No	No	No	No	Yes
11	Reversible nature (for ROI)		Yes (Only in case of no attack)	No	Yes	No	No	Yes	Yes

– signifies that the stated feature is not provided

sibility of RONI segmentation in a better way to localize tampering more specifically will also be investigated in the future work.

Declarations

Conflicts of interest There is no conflict of interest.

References

1. Casado-Vara R, Corchado J (2019) Distributed e-health wide-world accounting ledger via blockchain. J Intell Fuzzy Syst 36(3):2381–2386
2. Ray PP, Dash D, De D (2019) Edge computing for Internet of Things: a survey, e-healthcare case study and future direction. J Netw Comput Appl 140:1–22
3. Jabeen T, Ashraf H, Ullah A (2021) A survey on healthcare data security in wireless body area networks. J Ambient Intell Humaniz Comput, 1–14.
4. Zarour M, Alenezi M, Ansari MTJ, Pandey AK, Ahmad M, Agrawal A, Khan RA (2021) Ensuring data integrity of healthcare information in the era of digital health. Healthc Technol Lett 8(3):66
5. Singh AK, Anand A, Lv Z, Ko H, Mohan A (2021) A survey on healthcare data: a security perspective. ACM Trans Multimed Comput Commun Appl 17(2s):1–26
6. Ravichandran D, Praveenkumar P, Rajagopalan S, Rayappan JBB, Amirtharajan R (2021) ROI-based medical image watermarking for accurate tamper detection, localisation and recovery. Med Biol Eng Compu 59(6):1355–1372
7. Islam M, Roy A, Laskar RH (2020) SVM-based robust image watermarking technique in LWT domain using different sub-bands. Neural Comput Appl 32(5):1379–1403
8. Ma Z, Jiang M, Huang W (2020) Trusted forensics scheme based on digital watermark algorithm in intelligent VANET. Neural Comput Appl 32(6):1665–1678
9. Makbol NM, Khoo BE, Rassem TH (2015) Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. IET Image Proc 10(1):34–52
10. Ernawan F, Kabir MN (2020) A block-based RDWT-SVD image watermarking method using human visual system characteristics. Vis Comput 36(1):19–37
11. Shih FY (2017) Digital watermarking and steganography: fundamentals and techniques. CRC Press
12. Sun L, Xu J, Liu S, Zhang S, Li Y, Shen CA (2018) A robust image watermarking scheme using Arnold transform and BP neural network. Neural Comput Appl 30(8):2425–2440
13. Deeba F, She K, Dharejo F, Memon H (2020) Digital watermarking using deep neural network. Int J Mach Learn Comput 10(2):277–282
14. Coatrieux G, Maître H, Sankur B, Rolland Y, Collorec R (2000) Relevance of watermarking in medical imaging. In: Proceedings 2000 IEEE EMBS international conference on information technology applications in biomedicine. ITAB-ITIS 2000. Joint Meeting Third IEEE EMBS international conference on information technol (pp 250–255). IEEE
15. Chao HM, Hsu CM, Miaou SG (2002) A data-hiding technique with authentication, integration, and confidentiality for electronic patient records. IEEE Trans Inf Technol Biomed 6(1):46–53

16. Guo X, Zhuang TG (2009) A region-based lossless watermarking scheme for enhancing security of medical data. J Digit Imaging 22(1):53–64
17. Lai CC (2011) An improved SVD-based watermarking scheme using human visual characteristics. Opt Commun 284(4):938–944
18. Das S, Kundu MK (2013) Effective management of medical information through ROI-lossless fragile image watermarking technique. Comput Methods Programs Biomed 111(3):662–675
19. Lei B, Tan EL, Chen S, Ni D, Wang T, Lei H (2014) Reversible watermarking scheme for medical image based on differential evolution. Expert Syst Appl 41(7):3178–3188
20. Badshah G, Liew SC, Zain JM, Ali M (2016) Watermark compression in medical image watermarking using Lempel-Ziv-Welch (LZW) lossless compression technique. J Digit Imaging 29(2):216–225
21. Thakkar FN, Srivastava VK (2017) A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. Multimed Tools Appl 76(3):3669–3697
22. Thanki R, Borra S, Dwivedi V, Borisagar K (2017) An efficient medical image watermarking scheme based on FDCuT–DCT. Eng Sci Technol Int J 20(4):1366–1379
23. Ernawan F, Kabir MN (2018) A robust image watermarking technique with an optimal DCT-psychovisual threshold. IEEE Access 6:20464–20480
24. Pourhadi A, Mahdavi-Nasab H (2020) A robust digital image watermarking scheme based on bat algorithm optimization and SURF detector in SWT domain. Multimed Tools Appl 79:21653–21677
25. Swaraja K, Meenakshi K, Kora P (2020) An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine. Biomed Signal Process Control 55:101665
26. Alshanbari HS (2021) Medical image watermarking for ownership & tamper detection. Multimed Tools Appl 80(11):16549–16564
27. Sinhal R, Sharma S, Ansari IA, Bajaj V (2022) Multipurpose medical image watermarking for effective security solutions. Multimed Tools Appl 81(10):14045–14063
28. Sinhal R, Ansari IA (2022) Multipurpose image watermarking: ownership check, tamper detection and self-recovery. Circuits Syst Signal Process 41:3199–3221. https://doi.org/10.1007/s00034-021-01926-z
29. "Kaggle datasets", Last accessed: July. 2021. [Online]. Available: https://www.kaggle.com/datasets
30. "USC-SIPI database", Last accessed: July. 2021. [Online]. Available: http://sipi.usc.edu/database/database.php
31. "Image databases," Last accessed May. 2021. [Online]. Available: http://imageprocessingplace.com/root_files_V3/
32. Bustos A, Pertusa A, Salinas JM, de la Iglesia-Vayá M (2020) Padchest: a large chest x-ray image dataset with multi-label annotated reports. Med Image Anal 66:101797
33. Harmon SA, Sanford TH, Xu S et al (2020) Artificial intelligence for the detection of COVID-19 pneumonia on chest CT using multinational datasets. Nat Commun 11:4080. https://doi.org/10.1038/S41467-020-17971-2
34. Armato SG III, McLennan G, Bidaut L, McNitt-Gray MF, Meyer CR, Reeves AP, Clarke LP (2011) The lung image database consortium (LIDC) and image database resource initiative (IDRI): a completed reference database of lung nodules on CT scans. Med Phys 38(2):915–931
35. Clark K, Vendt B, Smith K et al (2013) The cancer imaging archive (TCIA): maintaining and operating a public information repository. J Digit Imaging 26:1045–1057. https://doi.org/10.1007/S10278-013-9622-7
36. Cheng J, Huang W, Cao S et al (2015) Enhanced performance of brain tumor classification via tumor region augmentation and partition. PLoS ONE 10:e0140381. https://doi.org/10.1371/JOURNAL.PONE.0140381
37. Imaging characterization of a metastatic patient derived model of bladder cancer: BL0293F (PDMR-BL0293-F563)—the cancer imaging archive (TCIA) public access—cancer imaging archive wiki. https://wiki.cancerimagingarchive.net/pages/viewpage.action?pageId=52757379#527573794dc5f53338634b35a3500cbed18472e0. Accessed 27 Apr 2022.
38. Saha A, Harowicz MR, Grimm LJ et al (2018) A machine learning approach to radiogenomics of breast cancer: a study of 922 subjects and 529 dce-mri features. Br J Cancer 119:508–516. https://doi.org/10.1038/S41416-018-0185-8
39. Al-Dhabyani W, Gomaa M, Khaled H, Fahmy A (2019) Dataset of breast ultrasound images. Data Br 28:104863. https://doi.org/10.1016/J.DIB.2019.104863

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.