Multimed Tools Appl (2017) 76:10599–10633
DOI 10.1007/s11042-015-3127-y

Information hiding in medical images: a robust medical image watermarking system for E-healthcare

Shabir A. Parah[1] · **Javaid A. Sheikh**[1] · **Farhana Ahad**[1] ·
Nazir A. Loan[1] · **G. M. Bhat**[1]

Received: 1 August 2015 / Revised: 21 October 2015 / Accepted: 30 November 2015 /
Published online: 9 December 2015

Abstract Electronic transmission of the medical images is one of the primary requirements in a typical Electronic-Healthcare (E-Healthcare) system. However this transmission could be liable to hackers who may modify the whole medical image or only a part of it during transit. To guarantee the integrity of a medical image, digital watermarking is being used. This paper presents two different watermarking algorithms for medical images in transform domain. In first technique, a digital watermark and Electronic Patients Record (EPR) have been embedded in both regions; Region of Interest (ROI) and Region of Non-Interest (RONI). In second technique, Region of Interest (ROI) is kept untouched for tele-diagnosis purpose and Region of Non-Interest (RONI) is used to hide the digital watermark and EPR. In either algorithm 8×8 block based Discrete Cosine Transform (DCT) has been used. In each 8×8 block two DCT coefficients are selected and their magnitudes are compared for embedding the watermark/EPR. The selected coefficients are modified by using a threshold for embedding bit a '0' or bit '1' of the watermark/EPR. The proposed techniques have been found robust not only to singular attacks but also to hybrid attacks. Comparison results viz-a - viz payload and robustness show that the proposed techniques perform better than some existing state of art techniques. As such the proposed algorithms could be useful for e-healthcare systems.

Keywords Region of interest · Region of non interest · Discrete cosine transform · Robustness

1 Introduction

Nowadays the usage of internet has crept in almost every sphere of day-to-day life. The areas like Electronic Commerce (e-commerce), Electronic Banking (e-banking), Electronic Shopping and Electronic Healthcare (e-healthcare) are achieving new heights with each passing day.

✉ Shabir A. Parah
shabireltr@gmail.com

[1] Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar, J&K, India 190006

Electronic healthcare refers to an internet based system wherein a patient can avail the services of an expert doctor available at other corner of globe. Though electronic healthcare is coming to rescue of millions of people globally, but there are a lot of challenges that need to be addressed, so as to make this technology more effective. With an aim to improve the e-healthcare services a lot of research is being carried out by research community round the globe. Some of the vital areas which are receiving more attention include Automatic Disease Inference (ADI), medical terminology assignment, biomedical image processing and authentication/security of biomedical data during transition [8, 10–12, 21]. The chief aim of the undertaken research is to effectively bridge the gap between health care knowledge seekers and knowledge providers [13].

The current online health services are broadly classified into two categories: (a) Portals run by renowned organizations and professional health providers, (b) community based health services. In either case, for proper tele-diagnosis by a remote expert, critical patient information such as patient images/videos and other Electronic Health Record (EHR) need to be shared over networked infrastructure. This critical and sensitive patient information being shared on a network requires excessive care, as one cannot afford loss of this information for a proper diagnosis. Thus, integrity, security and confidentiality of this patient data is of major concern, when transferred electronically [1, 9]. Digital watermarking plays a significant role in such a scenario. Digital watermarking techniques are used to provide confidentiality and integrity in the medical images. Further copy control and tamper detection of digital data which are the main objectives of the Digital Rights Management (DRM) can be achieved by digital watermarking [22, 25]. When embedding the additional Electronic Patients Record (EPR) or the digital watermark within the medical image; the image quality must not be affected [19]. Luckily, information contained in the images is not uniformly distributed across images. Some parts of the images contain more information compared to other ones. Various schemes are used for separating different objects/regions in images [24, 32]. From diagnosis point of view a medical image is divided into two regions; Region of Interest (ROI) and Region of Non Interest (RONI) [4, 30]. The more informative part of the medical image is Region of Interest which is used for the diagnosis and has to be taken care of [7]. Therefore, it is appropriate to embed the watermark in the Region of Non-Interest [14].

The digital watermark can be embedded in the cover medium using spatial domain techniques or the Transform domain techniques [29]. In a spatial domain technique, the data is directly embedded in the pixels by replacing the bits of the pixel by the data bits [15]. The spatial domain embedding is not robust but can be used whenever high payload is required. However, these techniques are easy and simple to implement and are sufficient in an attack - free environment and lossless compression [18]. In a transform domain technique, the coefficients of the cover medium are modified. Transform domain embedding techniques offers high robustness and more security to attacks [16]. Rest of the paper is organized as follows: Section 2 presents related work. Section 3 presents proposed work. Experimental results & discussions are presented in section 4. The paper concludes in section 5.

2 Related work

The advancement in the network infrastructure coupled with exponential rise in the internet users has resulted in tremendous increase in usage of online healthcare services. One of the fundamental challenges in such services is integrity and security of data being shared via unsecure networks. Digital watermarking of medical data like images/videos and EHR, of late, is being used as a potent tool to address these issues. Some of the related work wherein watermarking has been used to solve above mentioned concerns is as follows:

N. Solanki and S. K. Malik [27], have proposed a watermarking technique for medical images. The watermark has been encrypted using RSA algorithm and has been embedded in ROI using DWT algorithm. However, the proposed method needs pre-processing before actual embedding takes place. D. Bouslimi et al., in [2] reported an encryption based watermarking technique for medical images. RC4 stream cipher has been used for encryption purpose. The Least Significant Bit (LSB) embedding technique has been used for embedding the watermark. The high payload is achieved by LSB embedding technique but at the cost of higher vulnerability towards the different image processing operations. S. Das and M. K. Kundu in [5], have proposed a contourlet transform-based digital watermarking technique. After three level contourlet transform the low pass sub-bands are chosen for embedding the data. Even though the payload is less, the perceptual quality reported by authors in terms of PSNR value does not exceed 35 dB for less than 1400 bits of data. A. K. Singh et al., in [26] have proposed a robust non-blind and imperceptible dual watermarking technique for telemedicine application. Using the spatio- frequency localization properties of DWT and visual perception quality of the SVD, the proposed work assures the improvement in the robustness and imperceptibility of the medical images. The payload, however, is very low. One of current research problems of computer vision and image processing community is remote analysis of human behavior from the data collected by wearable cameras [31]. In such a scenario Activity of Daily Living (ADL) is recorded by wearable cameras. The huge data generated in such a way (in terms of Images/ Videos) needs to be authenticated and protected for proper behavior analysis and hence diagnosis of any behavioral disorders. One such technique for medical image data has been proposed in [17]. The authors have come up with a blind digital watermarking scheme for DICOM images. The watermarking has been done in wavelet and contourlet domains having payload 2010 bits for the whole image and 1840 bits for Region of Interest (ROI) part of the medical image. The proposed algorithm however, has not been tested for various hybrid image processing attacks.

As on date to best of our knowledge no medical image watermarking technique has been reported in transform domain which is robust to both the singular attacks as well as to hybrid attacks. This paper presents a robust medical image watermarking system which besides being robust to various singular image processing attacks, has been found robust to different hybrid (two or more simultaneous) attacks. In this context, the proposed work presents two medical image watermarking algorithms. In the first algorithm, the Electronic Patient Record (EPR) and the watermark is embedded in the whole image. In the second algorithm, the watermark is embedded in the RONI part of the medical image. The proposed techniques have been implemented in DCT domain. 8×8 block wise DCT is computed and DCT coefficients are modified for the embedding purpose.

3 Proposed work

The data embedding process in medical images is generally different from that of the embedding in other standard images. This is due to the fact that medical images contain critical information which is used for an e-diagnostic purpose. As already discussed medical images from diagnosis point of view are divided into two regions; Region of Interest and Region of Non-Interest. Based on the region in which data is embedded, two different watermarking approaches for medical image watermarking have been put forward. Discrete Cosine Transform (DCT) domain has been used for transforming the image into the frequency domain. The embedding has been carried out in the frequency domain. The transformation equations used to convert spatial domain information into frequency domain are using DCT as follows:

$$F(p,q) = \alpha_p \alpha_q \sum\nolimits_{x=0}^{N-1} \sum\nolimits_{y=0}^{N-1} A_{x,y} \cos\frac{(2x+1)p\pi}{2N} \cos\frac{(2y+1)q\pi}{2N} \tag{1}$$

Where F (p, q) denotes the image coefficient in transform domain and ($A_{x,\ y}$) denotes the image pixel in spatial domain. If p=q=0, $\alpha_p = \alpha_q = \sqrt{\frac{1}{N}}$:

$$\text{Else}\, \alpha_p = \alpha_q = \sqrt{\frac{2}{N}}$$

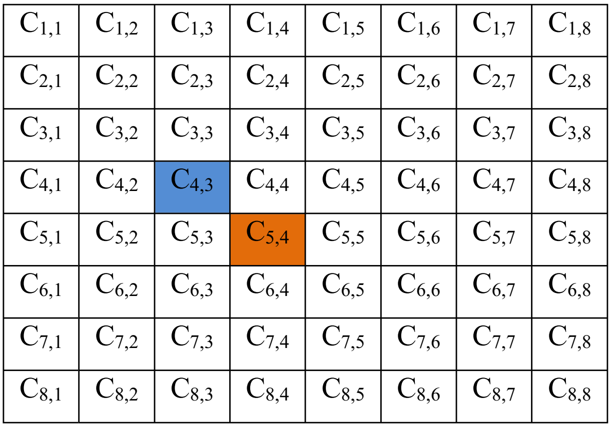
The inverse DCT can be represented as follows:

$$A_{x,y} = \sum\nolimits_{p=0}^{N-1} \sum\nolimits_{q=0}^{N-1} \alpha_p \alpha_q F(p,q) \cos\frac{(2x+1)p\pi}{2N} \cos\frac{(2y+1)q\pi}{2N} \tag{2}$$

DCT on an image is generally carried out in two ways; global DCT and block based DCT. Block based DCT has been used in the proposed algorithms. 8×8 DCT blocks have been chosen due to various advantages associated with this block size [3, 6]. A typical 8×8 DCT block is shown in Fig. 1. In both the proposed algorithms any two mid frequency coefficients (in a given 8×8 block) are selected and compared. The relative adjustment in the selected coefficient magnitudes is done using a watermarking embedding factor 'K'.

For the said work the highlighted coefficients $C_{4,\ 3}$ and $C_{5,\ 4}$ have been used. The relative difference of the selected coefficients $C_{i,\ j}$ [1≤(i, j)≤8] are adjusted depending upon the nature of watermark bit to be embedded. The adjustment is carried out as follows:

For embedding a watermark bit 0;



$C_{1,1}$	$C_{1,2}$	$C_{1,3}$	$C_{1,4}$	$C_{1,5}$	$C_{1,6}$	$C_{1,7}$	$C_{1,8}$
$C_{2,1}$	$C_{2,2}$	$C_{2,3}$	$C_{2,4}$	$C_{2,5}$	$C_{2,6}$	$C_{2,7}$	$C_{2,8}$
$C_{3,1}$	$C_{3,2}$	$C_{3,3}$	$C_{3,4}$	$C_{3,5}$	$C_{3,6}$	$C_{3,7}$	$C_{3,8}$
$C_{4,1}$	$C_{4,2}$	$C_{4,3}$	$C_{4,4}$	$C_{4,5}$	$C_{4,6}$	$C_{4,7}$	$C_{4,8}$
$C_{5,1}$	$C_{5,2}$	$C_{5,3}$	$C_{5,4}$	$C_{5,5}$	$C_{5,6}$	$C_{5,7}$	$C_{5,8}$
$C_{6,1}$	$C_{6,2}$	$C_{6,3}$	$C_{6,4}$	$C_{6,5}$	$C_{6,6}$	$C_{6,7}$	$C_{6,8}$
$C_{7,1}$	$C_{7,2}$	$C_{7,3}$	$C_{7,4}$	$C_{7,5}$	$C_{7,6}$	$C_{7,7}$	$C_{7,8}$
$C_{8,1}$	$C_{8,2}$	$C_{8,3}$	$C_{8,4}$	$C_{8,5}$	$C_{8,6}$	$C_{8,7}$	$C_{8,8}$

Fig. 1 8×8 DCT block showing 64 Co-efficient

Coefficients are adjusted in such a way that the process culminates at | $C_{4,\,3}$ |>| $C_{5,\,4}$ |. This is ensured by following steps:

```
    $If\left(C_{4,3}\right)\leq\left(C_{5,4}\right)$
        $Swap\left(C_{4,3},C_{5,4}\right)$
        $If\ \left|C_{4,3}-C_{5,4}\right|>K$
        $No\ Change$
            $Else\ if\left|C_{4,3}-C_{5,4}\right|<K$
                $Then\left[\left(C_{4,3}\right)=\left(C_{4,3}\right)+K/2\right]and\left[\left(C_{5,4}\right)=\left(C_{5,4}\right)-K/2\right]$
```

For embedding a watermark bit 1;

Coefficients are adjusted in such a way that the process culminates at | $C_{4,\,3}$ |<| $C_{5,\,4}$ |. This is ensured by following steps.

```
$If\left(C_{4,3}\right)>\left(C_{5,4}\right)$
    $Swap\left(C_{4,3},C_{5,4}\right)$
    $If\ \left|C_{4,3}-C_{5,4}\right|\geq K$
    $No\ Change$
        $Else\ if\left|C_{4,3}-C_{5,4}\right|<K$
            $Then\left[\left(C_{4,3}\right)=\left(C_{4,3}\right)-K/2\right]and\left[\left(C_{5,4}\right)=\left(C_{5,4}\right)+K/2\right]$
```

The flowchart of the basic embedding algorithm used for data embedding in the proposed algorithms is shown in Fig. 2.

The complete embedding procedure for two proposed algorithms is in tune with above embedding procedure and is described as under:

3.1 First algorithm

1) Read the cover (medical) image, Electronic Patients Record (EPR) and digital watermark.
2) Convert the EPR and digital watermark in a binary sequence.
3) Compute block wise DCT of 8×8 non-overlapping blocks of the cover image
4) Embed the watermark information using an embedding factor (K) by choosing two coefficients C1, C2 from an 8×8 DCT block.
5) For embedding bit 0, Coefficient (C1) is adjusted and made relatively greater than Coefficient (C2), i.e., $(C1>C2)$.
6) For embedding bit 1, Coefficient (C1) is adjusted and made relatively smaller than Coefficient (C2), i.e., $(C1<C2)$.
7) Compute inverse DCT of modified block.
8) Steps 3 to 7 are repeated to embed the whole information

It is pertinent to mention that, in this technique both Electronic Patients Record (EPR) and watermark is embedded in ROI and RONI of medical image. Ten different CT scans of the patient have been chosen as cover medium. 32×32 logo and 1024 bits of EPR is embedded using this technique. The embedding factor ‘K’ has been chosen as 10 and 20.

3.2 Second algorithm

1) Read the cover (medical) image.

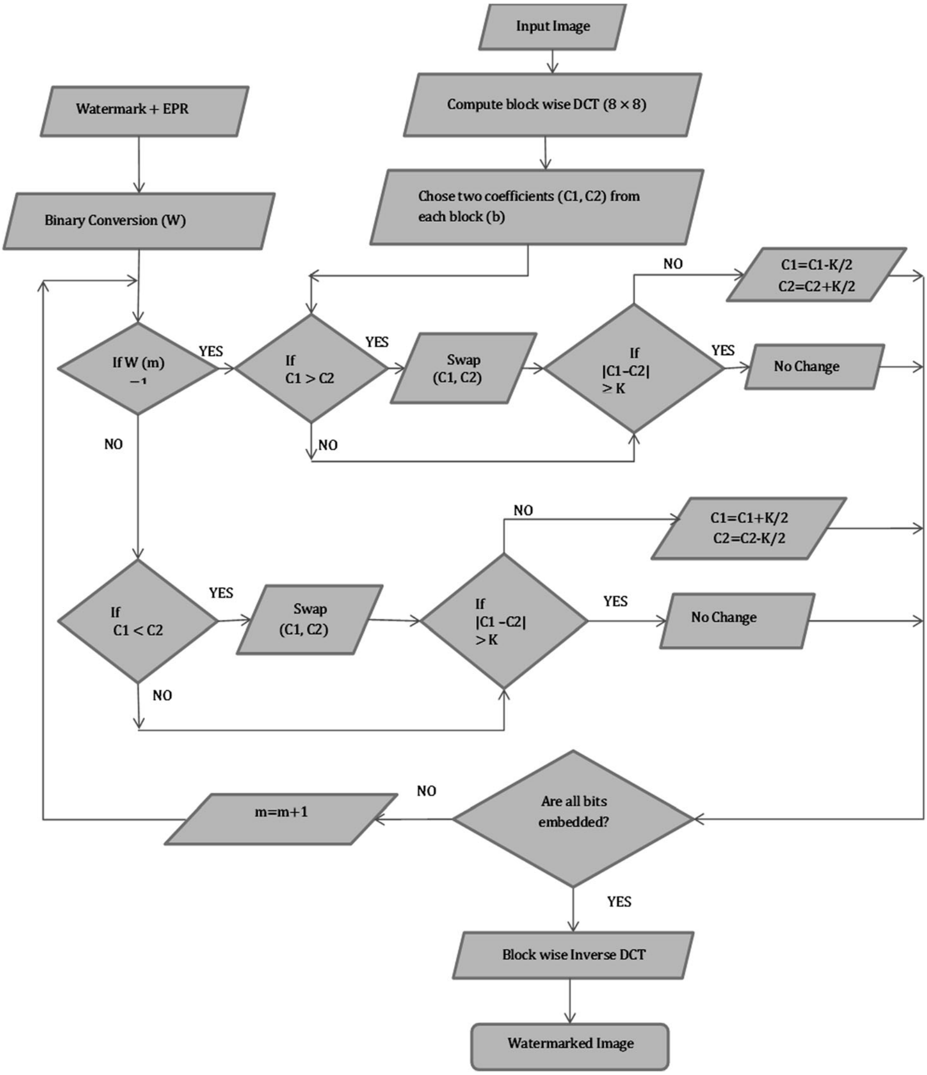


Fig. 2 Flow chart of the embedding algorithm

2) Separate ROI and RONI of cover image.
3) Read the digital watermark.
4) Convert the digital watermark in a binary sequence.
5) Compute block wise DCT of 8×8 non-overlapping blocks of the cover image.
6) Embed the watermark information using an embedding factor (K) by choosing two coefficients C1, C2 from an 8×8 DCT block.
7) For embedding bit 0, Coefficient (C1) is adjusted and made relatively greater than Coefficient (C2), i.e., $(C1 > C2)$.
8) For embedding bit 1, Coefficient (C1) is adjusted and made relatively smaller than Coefficient (C2), i.e., $(C1 < C2)$.

Table 1 Objective quality indices

Image	Proposed Scheme [Payload (2048 bits)]					
	Embedding factor (K=10)			Embedding factor (K=20)		
	PSNR (dB)	SSIM	NAE	PSNR (dB)	SSIM	NAE
Image 1	36.9428	0.9861	0.0126	36.7111	0.9631	0.0157
Image 2	38.1753	0.9859	0.0117	37.8887	0.9631	0.0148
Image 3	38.5361	0.9862	0.0111	38.2066	0.9638	0.0136
Image 4	41.5438	0.9867	0.0084	40.8584	0.9624	0.0124
Image 5	38.1864	0.9866	0.0136	37.8967	0.9617	0.0184
Image 6	45.6741	0.9899	0.0053	43.9117	0.9655	0.0090
Image 7	43.4975	0.9864	0.0068	42.5320	0.9593	0.0106
Image 8	48.2852	0.9884	0.0051	45.6102	0.9586	0.0098
Image 9	43.2698	0.9886	0.0065	41.9542	0.9644	0.0107
Image 10	37.4104	0.9857	0.0113	37.1221	0.9647	0.0150
Average	41.1521	0.9857	0.0092	40.2692	0.9627	0.0130

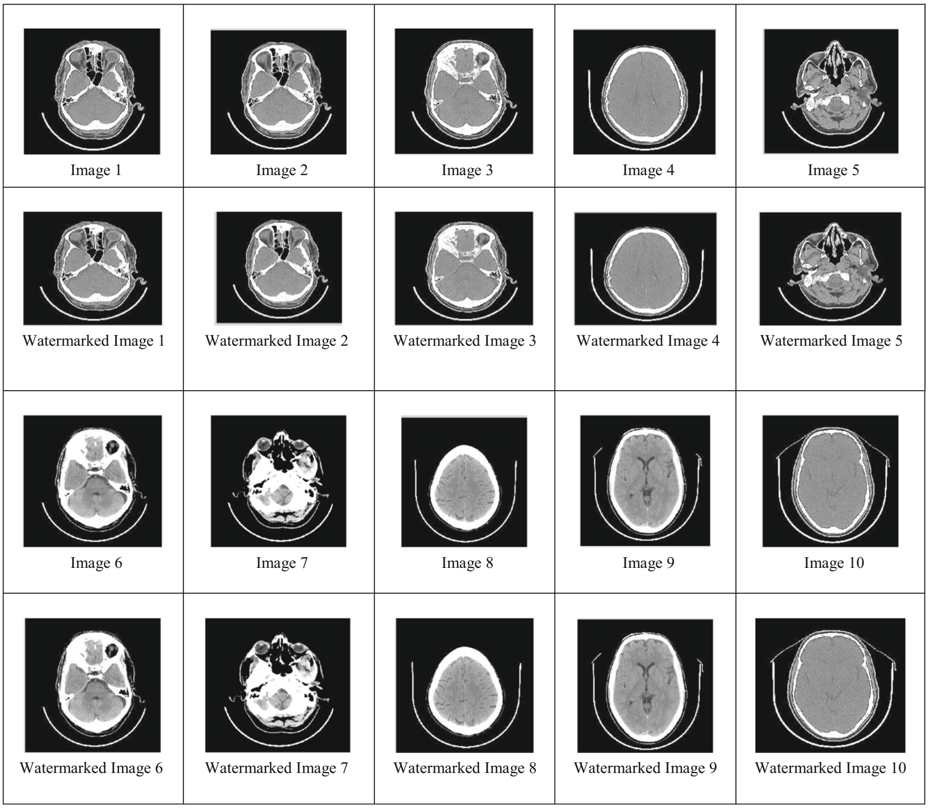


Image 1 Image 2 Image 3 Image 4 Image 5

Watermarked Image 1 Watermarked Image 2 Watermarked Image 3 Watermarked Image 4 Watermarked Image 5

Image 6 Image 7 Image 8 Image 9 Image 10

Watermarked Image 6 Watermarked Image 7 Watermarked Image 8 Watermarked Image 9 Watermarked Image 10

Fig. 3 Original CT scan images and respective watermarked images

Table 2 Perceptual transparency comparison

Image	Rahimi and Rabbani [17] Payload (2010 bits)	Proposed Scheme Payload (2048 bits)	
	SSIM	SSIM (K=10)	SSIM (K=20)
Image 1	0.9435	0.9861	0.9631
Image 2	0.9408	0.9859	0.9631
Image 3	0.9395	0.9862	0.9638
Image 4	0.9411	0.9867	0.9624
Image 5	0.9383	0.9866	0.9617
Average	**0.94064**	**0.9863**	**0.96282**

9) Compute inverse DCT of modified block.
10) Repeat steps 5 to 9 to embed the whole information.

In this technique the medical image is divided into Region of Interest (ROI) and Region of Non Interest (RONI). The Region of Non Interest is separated from Region of Interest using Color Thresholder application of MATLAB2014a. The digital watermark of size 47×47 (i.e., 2209 bits) is embedded in RONI part of the medical image. The watermarked RONI part of host image is combined with ROI part after the watermark embedding. The robustness analysis is carried out using different values of embedding factor.

3.3 Watermark and EPR extraction

Extraction process is the reverse of the embedding process. The watermarked medical image is subjected to block based DCT at the receiver. The DCT Coefficients modified during

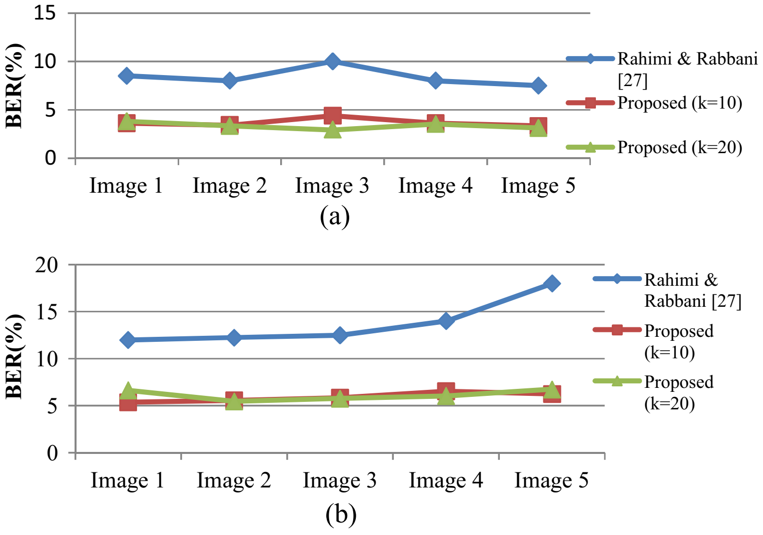


Fig. 4 **a** BER comparison at noise density (σ=0.003). **b** BER comparison at noise density (σ=0.005)

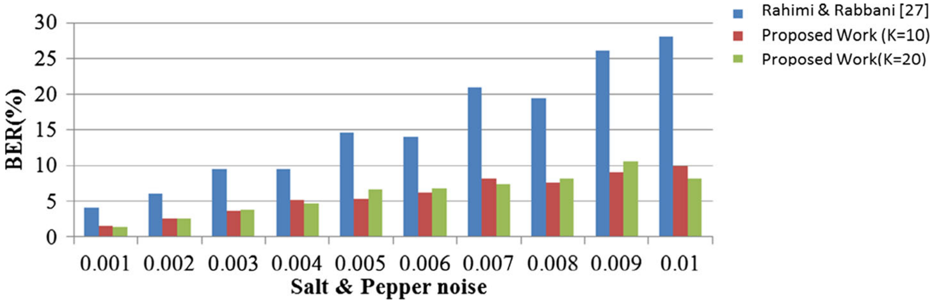
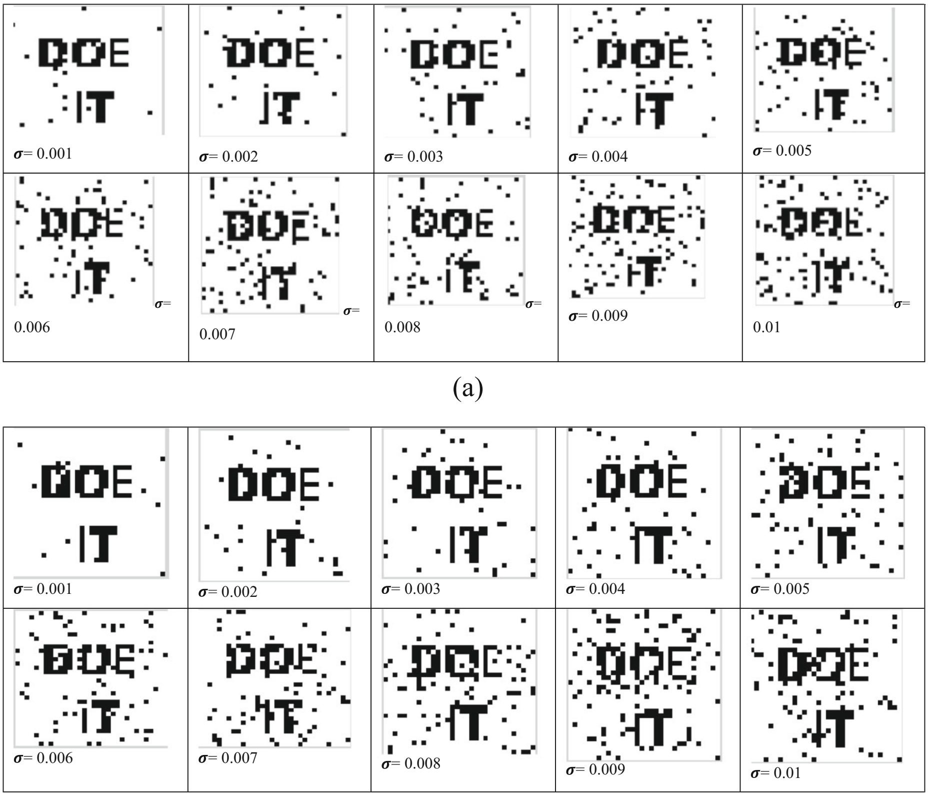


Fig. 5 BER comparison of Image 1 with [17]

embedding processes are compared for the extraction of watermark/EPR. If Coefficient C1 is greater than Coefficient C2 ($C1 > C2$), bit ‘0’ is extracted else bit ‘1’ is extracted. The only difference between the two extraction processes is that for second technique the ROI and RONI are separated before the actual extraction process takes place.



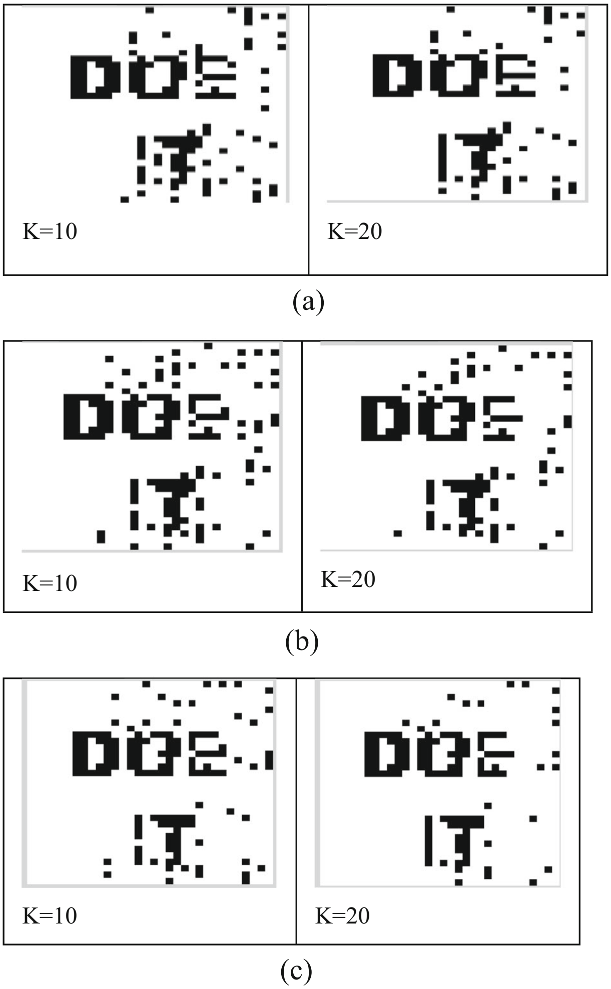
(a)

(b)

Fig. 6 **a** Extracted watermarks at K=10 for varying noise densities. **b** Extracted watermarks at K=20 for varying noise densities

4 Experimental results

The experimentation has been carried out using MATLAB R2014a platform for different 512×512 CT scan images of the patient. The digital watermarks used for copyright protection are of the size 32×32 and 47×47 for the two techniques. Further, EPR of 1024 bits is also embedded in the test medical images. The mask for ROI separation in medical images has been created by Color Thresholder application of MATLAB R2014a. The image quality is analyzed from objective analysis by calculating Peak Signal to Noise Ratio (PSNR), Normalized Absolute Error (NAE) and Structural Similarity Measure Index (SSIM) between original image and 'watermarked & attacked' image. The PSNR and NAE have been computed as in [20, 23]. The robustness of the proposed scheme is evaluated by calculating Bit Error Rate (BER %) and Normalized Cross-Correlation (NCC) between embedded 'watermark and EPR' and extracted 'watermark and EPR' for various attacks.



(a)

(b)

(c)

Fig. 7 **a** Extracted watermark after Median filtering for Image 1. **b** Extracted watermark after Average filtering for Image 1. **c** Extracted watermark after Wiener filtering for Image 1

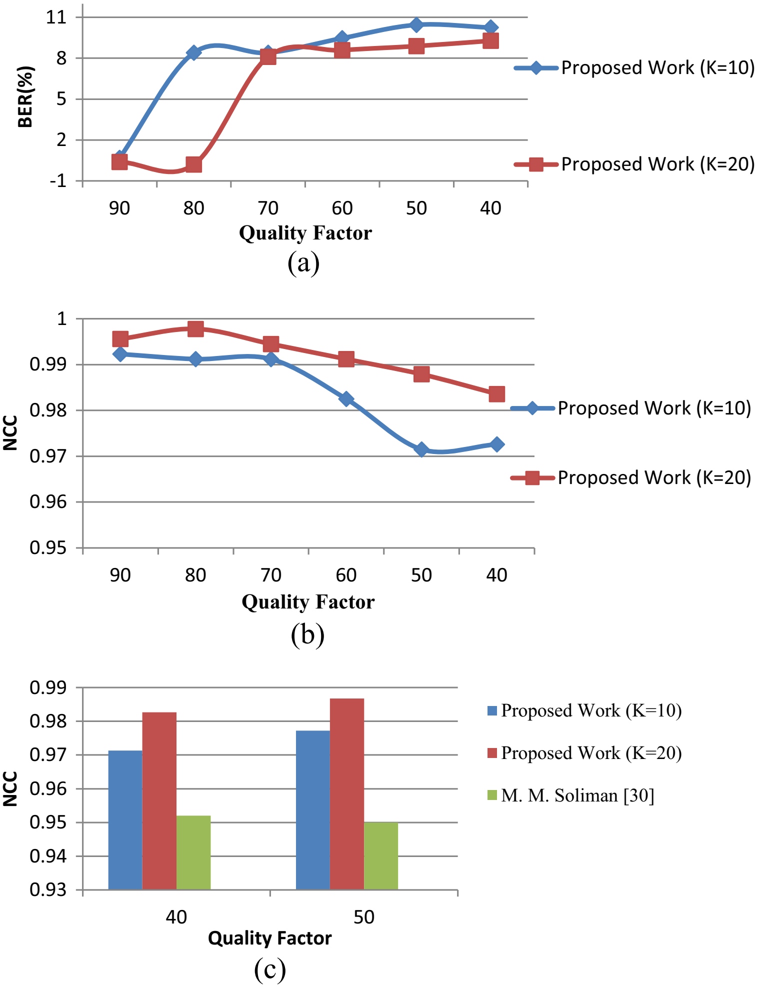
Equation (8) is used for calculating BER (%) and Eq. (9) for NCC. The Structural Similarity Index (SSIM) is based on the calculations of three terms, namely the luminance, contrast and structure. The overall index is a given by:

$$SSIM(x,y) = [l(x,y)]^{\alpha}\cdot[c(x,y)]^{\beta}\cdot[s(x,y)]^{\gamma} \tag{3}$$

Where;

$$l(x,y) = \frac{2\mu_{\mathrm{x}}\mu_{\mathrm{y}} + C1}{\mu_{\mathrm{x}}^2 + \mu_{\mathrm{y}}^2 + C1} \tag{4}$$

$$c(x,y) = \frac{2\sigma_x\sigma_y + C2}{\sigma_x^2 + \sigma_y^2 + C2} \tag{5}$$



(a)

(b)

(c)

Fig. 8 **a** The plot between the BER and Quality Factor. **b** The plot between the NCC and Quality Factor. **c** Average NCC verses Quality Factor

$$s(x,y) = \frac{\sigma_{xy} + C3}{\sigma_x \sigma_y + C3} \tag{6}$$

where μ_x, μ_y, σ_x, σ_y, and σ_{xy} are the local means, standard deviations, and cross-covariance for images x, y. For default exponents and default selections of C3 the expression is given by:

$$SSIM(x,y) = \frac{\left(2\mu_x\mu_y + C1\right)\left(2\sigma_{xy} + C2\right)}{\left(\mu_x^2 + \mu_y^2 + C1\right)\left(\sigma_x^2 + \sigma_y^2 + C2\right)} \tag{7}$$

Table 3 Robustness parameters against JPEG compression at K=10 and K=20

IMAGES	QF	K=10				K=20			
		WATERMARK		EPR		WATERMARK		EPR	
		BER (%)	NCC	BER (%)	NCC	BER (%)	NCC	BER (%)	NCC
IMAGE 1	90	0.68	0.9923	1.66	0.9849	0.39	0.9956	0.88	0.9931
	80	8.40	0.9912	18.20	0.9794	0.20	0.9978	1.37	0.9849
	70	8.40	0.9912	19.18	0.9698	8.11	0.9945	17.81	0.9849
	60	9.47	0.9825	20.25	0.9602	8.59	0.9912	18.40	0.9794
	50	10.45	0.9715	22.21	0.9438	8.89	0.9879	18.98	0.9753
	40	10.25	0.9726	24.46	0.9177	9.28	0.9836	20.35	0.9588
IMAGE 2	90	0.88	0.9923	1.37	0.9835	0.78	0.9934	0.78	0.9904
	80	9.28	0.9846	18.20	0.9781	1.17	0.9890	1.17	0.9863
	70	9.67	0.9792	19.18	0.9671	9.08	0.9846	18.10	0.9808
	60	9.77	0.9781	21.14	0.9410	8.79	0.9890	17.91	0.9822
	50	10.35	0.9737	22.02	0.9396	9.28	0.9846	18.59	0.9739
	40	11.13	0.9649	24.07	0.9218	10.25	0.9748	20.25	0.9602
IMAGE 3	90	0.59	0.9934	0.59	0.9959	0.20	0.9978	0.39	0.9973
	80	8.98	0.9879	16.73	0.9945	0.49	0.9956	0.39	0.9973
	70	9.57	0.9814	18.30	0.9767	8.69	0.9912	17.03	0.9918
	60	10.16	0.9748	29.47	0.9671	9.08	0.9868	17.12	0.9918
	50	10.25	0.9737	22.02	0.9355	9.38	0.9836	17.42	0.9890
	40	11.23	0.9660	23.09	0.9246	9.86	0.9792	19.37	0.9616
IMAGE 4	90	0.20	0.9978	0.78	0.9918	0.20	0.9978	0.39	0.9945
	80	10.45	0.9978	19.18	0.9712	0.20	0.9978	1.17	0.9877
	70	10.84	0.9934	19.77	0.9712	10.45	0.9978	17.71	0.9890
	60	11.43	0.9868	20.94	0.9534	10.74	0.9945	18.30	0.9863
	50	11.62	0.9868	23.39	0.9300	11.04	0.9912	18.88	0.9822
	40	12.70	0.9737	25.54	0.9067	11.23	0.9901	20.45	0.9630
IMAGE 5	90	0.20	0.9978	1.47	0.9863	0.09	0.9989	0.98	0.9918
	80	11.04	0.9978	19.37	0.9835	0.20	0.9978	1.17	0.9918
	70	11.43	0.9934	19.86	0.9739	11.23	0.9956	18.79	0.9849
	60	11.91	0.9879	21.62	0.9547	11.72	0.9901	19.08	0.9835
	50	12.60	0.9803	23.09	0.9342	12.02	0.9868	19.57	0.9781
	40	12.70	0.9792	25.64	0.9150	12.11	0.9857	21.23	0.9588

$$BER = \frac{1}{MN}\left[\sum\nolimits_{i=1}^{M}\sum\nolimits_{j=1}^{N} w_m(i,j)\oplus w_{me}(i,j)\right] \times 100 \tag{8}$$

$$NCC = \frac{\sum\nolimits_{\mathrm{i=1}}^{\mathrm{M}}\sum\nolimits_{\mathrm{j=1}}^{\mathrm{N}} w_m(i,j) \times \mathrm{w}_{me}(i,j)}{\sum\nolimits_{\mathrm{i=1}}^{\mathrm{M}}\sum\nolimits_{\mathrm{j=1}}^{\mathrm{N}} w_m(i,j)^2} \tag{9}$$

In above equations; M, N are the dimensions of the original logo and extracted logo; $\mathrm{w_m}$ (i, j) is the (i, j)$^{\mathrm{th}}$ pixel of original watermark and $\mathrm{w_{me}}$ (i, j) is the (i, j)$^{\mathrm{th}}$ pixel of the extracted logo. The perceptual quality and robustness analysis for the two proposed algorithms are presented below.

I) Analysis of first algorithm

4.1 Imperceptibility analysis

The objective quality indices viz. PSNR and SSIM obtained for various images are shown in Table 1. The perceptual transparency of the watermarked images obtained in our scheme has been shown in Fig. 3. The average PSNR values (greater than 40 dB) indicate that the proposed system is capable of producing good quality watermarked images. This is substantiated by very small NAE values of 0.0092 and 0.0130 for different values of embedding factor K, as well as the subjective quality of the watermarked images as shown in Fig. 3.

A comparison of the image quality of our technique with that of Rahimi and Rabbani [17] on the basis of the SSIM has been shown in Table 2. It is evident from the Table that the average SSIM value of the watermarked images as obtained in our scheme is more than that of [17]. The average SSIM in our scheme is 0.9857 at K=10 and 0.9627 at K=20 while as it is 0.94064 in [17].

Table 4 Robustness parameters against cropping K=10

Cropping (top left corner)		IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Watermark	BER	5.66	5.66	5.66	5.66	5.66	**5.66**
	NCC	1.0000	1.0000	1.0000	1.0000	1.0000	**1.0000**
EPR	BER	14.58	14.58	14.58	14.58	14.58	**14.58**
	NCC	1.0000	1.0000	1.0000	1.0000	1.0000	**1.0000**
Cropping (at center)							
Watermark	BER	0.29	0.29	0.09	0.49	0.98	**0.42**
	NCC	0.9967	0.9967	0.9989	0.9945	0.9890	**0.9952**
EPR	BER	26.07	24.80	26.07	24.71	25.88	**25.50**
	NCC	1	1	0.9980	0.9980	0.9980	**0.9988**

Table 5 Robustness parameters against cropping K=20

Cropping (top left corner)		IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Watermark	BER	5.66	5.66	5.66	5.66	5.66	**5.66**
	NCC	1.0000	1.0000	1.0000	1.0000	1.0000	**1.0000**
EPR	BER	14.58	14.58	14.58	14.58	14.58	**14.58**
	NCC	1.0000	1.0000	1.0000	1.0000	1.0000	**1.0000**
Cropping (at center)							
Watermark	BER	0.29	0.29	0.09	0.20	0.78	**0.33**
	NCC	0.9967	0.9967	0.9989	0.9978	0.9912	**0.9962**
EPR	BER	26.07	23.93	25.20	25.10	23.44	**24.75**
	NCC	0.9980	1	1	0.9981	1	**0.9992**

4.2 Robustness analysis

The robustness of the proposed scheme has been evaluated by subjecting watermarked images obtained from the system to various singular and hybrid attacks like, salt and pepper noise, Gaussian noise, JPEG compression, rotation, different filtering processes (Median filtering, Average filtering etc.). The results obtained are presented and discussed below:

4.2.1 Robustness analysis against salt & pepper attack

The watermarked medical images have been attacked by salt & pepper noise of varying noise densities (0.001 to 0.01). The result obtained for various images have been shown in Fig. 4a and b. A comparison of the results with [17] proves that the proposed technique is more robust.

Figure 5 shows the robustness of Image 1 to 'salt & pepper' noise at noise densities ranging from 0.001 to 0.01. It is clear from the figure that for all the noise densities our scheme performs better. A visual demonstration of this fact is presented in Fig. 6a and b. The mentioned figures show extracted watermarks for embedding factor values of K=10 and K=20 for various noise density values.

It is clear from the above figures that the system is more robust to salt and pepper noise for embedding factor value of K=20.

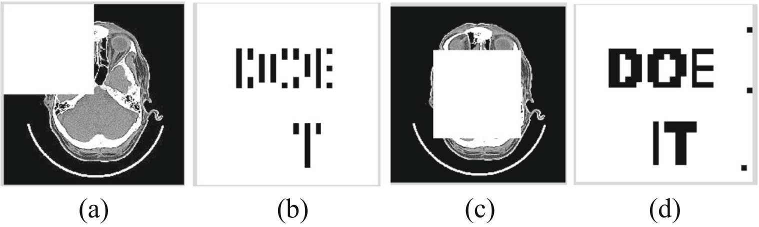


Fig. 9 **a** *Top left* corner cropped (**b**) Extracted watermark (**c**) 25 % cropping at center of Image 1 (**d**) Extracted watermark

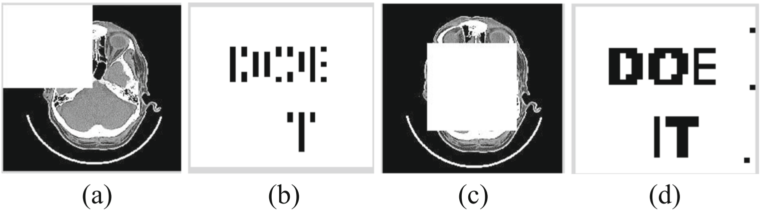


Fig. 10 **a** *Top left* corner cropped Image 1 (**b**) Extracted watermark (**c**) 25 % cropping at center of Image 1 (**d**) Extracted watermark

4.2.2 Robustness analysis against different filtering attacks

Various filtering attacks have been carried out on the watermarked images. The filter kernel used for Median filtering, Average filtering and Wiener filtering is 3×3. The description of filtering attacks is as under:

Median filtering The watermarked images as obtained in the first technique have been subjected to Median filtering [3×3]. The NCC and BER of the extracted watermark is 0.9430 and 5.96 % for K=10 and 0.9857 and 4.98 % for K=20 respectively. The BER values of the EPR obtained in our algorithm for K=10 and 20 are 14.68 and 12.52 % respectively. It is pertinent to mention here that for same number of bits, [17] reports BER 20.18 %. Figure 7a shows the extracted watermark.

Average filtering Figure 7b shows the extracted watermark after average filtering attack. The NCC and BER of extracted watermark equals to 0.9354 and 6.54 % for K=10 and 0.9485 and 5.47 % for K=20 respectively which is 0.7960 and 27.35 % in case of [17]. The BER of the EPR obtained is 12.43 % when K=10 and 10.47 % when K=20 while as that reported in [17] is 34.72 %.

Table 6 Robustness parameters against cropping K=10

Rotation 1°		IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Watermark	BER	3.61	3.91	3.52	1.86	3.22	**3.22**
	NCC	0.9638	0.9583	0.9638	0.9792	0.9638	**0.9658**
EPR	BER	8.59	6.45	5.76	6.74	8.69	**7.25**
	NCC	0.9113	0.9548	0.9456	0.9338	0.9071	**0.9305**
Rotation 5°							
Watermark	BER	4.39	3.52	4.98	2.15	2.83	**3.57**
	NCC	0.9550	0.9616	0.9452	0.9770	0.9682	**0.9614**
EPR	BER	8.51	8.90	9.39	10.18	10.76	**9.55**
	NCC	0.9040	0.8930	0.8944	0.8930	0.8875	**0.8944**
Rotation 10°							
Watermark	BER	4.30	5.57	4.88	1.86	3.52	**4.03**
	NCC	0.9561	0.9441	0.9485	0.9803	0.9605	**0.9579**
EPR	BER	13.41	12.92	9.39	10.96	11.45	**11.63**
	NCC	0.8669	0.8779	0.9053	0.8820	0.8848	**0.8834**

Table 7 Robustness parameters against cropping K=20

Rotation 1°		IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Watermark	BER	2.93	3.03	2.83	1.17	2.93	**2.59**
	NCC	0.9704	0.9682	0.9715	0.9868	0.9671	**0.9728**
EPR	BER	6.64	6.45	4.69	4.00	5.57	**5.47**
	NCC	0.9361	0.9548	0.9548	0.9587	0.9844	**0.9577**
Rotation 5°							
Watermark	BER	3.91	2.83	3.71	1.37	2.34	**2.83**
	NCC	0.9605	0.9682	0.9594	0.9857	0.9737	**0.9695**
EPR	BER	6.16	6.95	6.75	5.97	8.41	**6.85**
	NCC	0.9287	0.9163	0.9232	0.9438	0.9122	**0.9248**
Rotation 10°							
Watermark	BER	3.71	4.20	3.91	1.56	3.13	**3.30**
	NCC	0.9627	0.9572	0.9583	0.9836	0.9649	**0.9653**
EPR	BER	11.45	11.35	7.34	8.22	10.08	**9.69**
	NCC	0.8875	0.8903	0.9287	0.9122	0.9026	**0.9045**

Wiener filtering Figure 7c shows the extracted watermark after Wiener filtering attack. The NCC and BER of extracted watermark equals to 0.9539 and 4.88 % for K=10 and 0.9704 and 3.32 % for K=20 respectively. The BER of the EPR obtained is 10.67 % when K=10 and 7.44 % when K=20. For same amount of data [17] reports BER of 32.85 %.

The above discussions reveal that irrespective of the type of filtering attacks (Median Filtering, Average Filtering, and Wiener filtering) carried out on the watermarked images yielded by our method; our scheme outperforms the one reported in [17].

4.2.3 Robustness analysis against JPEG attack

JPEG is usually used for the compression purpose which reduces the storage requirements and lowers the bandwidth required for transmission. Figure 8a and b shows various results of BER and NCC for different values of Quality Factor and embedding factor 'K'. Table 3 shows various image quality matrices when watermarked image is subjected to JPEG compression of different quality factors. The authors of [17] have not tested their algorithm for JPEG compression; however a comparison of the proposed technique for this attack with [28] has

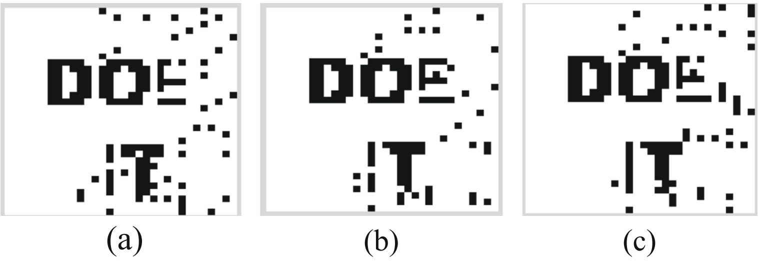
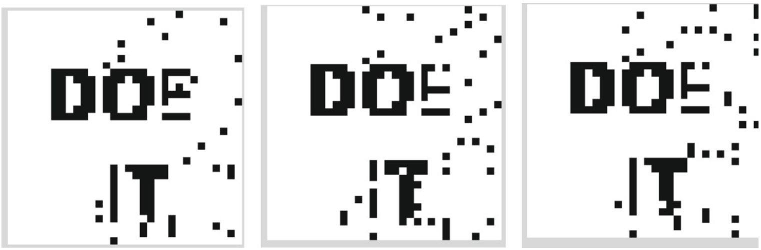

(a) (b) (c)

Fig. 11 Extracted watermarks from Image 1 at: (**a**) 1° (**b**) 5° (**c**) 10°



(a) (b) (c)

Fig. 12 Extracted watermarks from Image 1 at: (**a**) 1° (**b**) 5° (**c**) 10°

been carried out. A comparison of proposed technique with [28] for average NCC values is shown in Fig. 8c.

It is clear from Fig. 8a that BER reduces with the increase in Quality Factor. Further the system robustness improves with increasing value of embedding factor K. Figure 8b shows that the value of the NCC decreases with the decrease in Quality Factor.

It is worth to mention that for a given Quality Factor BER decreases as the 'K' is increased. Further, the value of NCC improves for higher value of 'K', for a given Quality Factor. The comparison of NCC for different quality factors show that our technique performs better for JPEG compression attack.

From the above Table, it is clear that the percentage BER values vary from 0.2 to 12.7 as quality factor is reduced from 90 to 40 for various medical images for extracted watermarks. Generally speaking, BER improves with increase in quality factor and embedding factor 'K'. Further, NCC values are very close to unity for quality factor of 70 and above, showing that our scheme is capable of withstanding JPEG compression.

4.2.4 Robustness analysis against cropping attack

The watermarked images have been tested for cropping attack. The results obtained after cropping 25 % of the watermarked image from top left corner and center in terms of BER (%) and NCC are shown in Tables 4 and 5 for embedding factor 'K'=10 and 'K'=20 respectively. The cropped watermarked images with extracted watermarks are also shown in Figs. 9 and 10.

Table 8 BER (%) and NCC of extracted watermarks for sharpening attack

Sharpening (K=10)		IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Watermark	BER	1.66	0.88	1.27	0.98	1.27	**1.21**
	NCC	0.9814	0.9912	0.9890	0.9901	0.9857	**0.9875**
EPR	BER	3.52	3.62	2.64	2.25	3.72	**3.15**
	NCC	0.9588	0.9630	0.9726	0.9136	0.9547	**0.9525**
Sharpening (K=20)							
Watermark	BER	1.27	0.68	0.68	0.49	0.98	**0.82**
	NCC	0.9857	0.9923	0.9945	0.9945	0.9890	**0.9912**
EPR	BER	2.15	2.45	1.17	0.88	1.96	**1.72**
	NCC	0.9726	0.9781	0.9904	0.9890	0.9767	**0.9814**

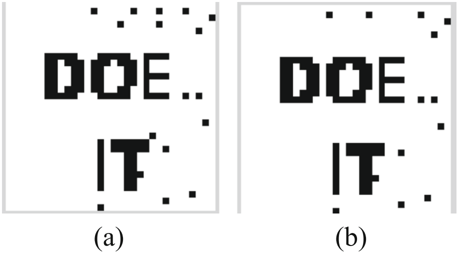


Fig. 13 **a** Extracted watermark at 'K'=10 (**b**) Extracted watermark at 'K'=20

It is evident from the mentioned tables that average BER decreases as K is increased. Further we are able to extract the watermark from the cropped images successfully indicating that proposed algorithm is robust to cropping.

4.2.5 Robustness analysis against rotation attack

The watermarked images obtained, using proposed algorithm have been subjected to rotation attack of various degrees. The results obtained after rotating the watermarked image by various angles for 'K'=10 and 'K'=20 are shown in Tables 6 and 7 respectively. The small BER values obtained show that the system is robust to cropping. This is substantiated by visual quality of extracted watermarks as shown in Figs. 11 and 12. It is pertinent to mention that average BER (K=10) for 1° rotation is 3.22; for 5° rotation is 3.57 and for 10° rotation is 4.03. The same indices for K=20 come down to 2.59, 2.83 and 3.30 for 1°, 5° and 10° rotation respectively. This shows that robustness to cropping improves with increasing value of K.

4.2.6 Robustness analysis against sharpening attack

The results obtained from various watermarked images for sharpening attack have been presented in Table 8.

The results show that for K=10, BER of extracted watermark is 1.21 and for K=20, it reduces to 0.82. This shows that the proposed method is highly resilient

Table 9 BER (%) and NCC for Histogram Equalization

Histogram Equalization (K=10)		IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Watermark	BER	0.36	0.98	0.98	0.78	0.88	**0.80**
	NCC	0.9956	0.9901	0.9934	0.9912	0.9901	**0.9921**
EPR	BER	1.47	2.15	2.05	0.78	1.37	**1.56**
	NCC	0.9849	0.9767	0.9767	0.9890	0.9835	**0.9822**
Histogram Equalization (K=20)							
Watermark	BER	0	0.59	0.59	0.29	0.36	**0.36**
	NCC	1	0.9934	0.9967	0.9978	0.9956	**0.9967**
EPR	BER	0.59	0.68	0.78	0.39	0.39	**0.56**
	NCC	0.9931	0.9918	0.9904	0.9945	0.9959	**0.9931**

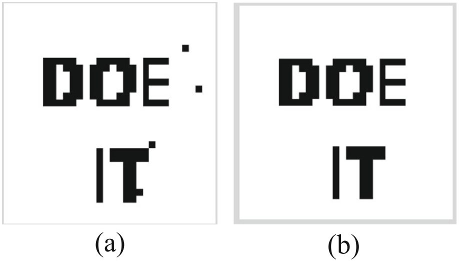


Fig. 14 **a** Extracted watermark at 'K'=10 (**b**) Extracted watermark at 'K'=20

to sharpening attack. Extracted watermarks, as shown in Fig. 13 substantiate this fact.

4.2.7 Robustness analysis against histogram equalization

The results obtained in terms of BER and NCC at K=10 and K=20 after Histogram Equalization are shown in Table 9. Further the extracted watermarks are shown in Fig. 14.

The results show that the proposed algorithm performs outstandingly well for the histogram equalization as BER is less than 1 %. Further, the robustness improves with increasing K.

4.2.8 Robustness analysis against gaussian noise

The watermarked images have been subjected to Gaussian noise of variance 0.0001. BER (%) and NCC at K=10 and K=20 of the watermarked image after Gaussian Noise attack is shown in Table 10. The extracted watermarks are shown in Fig. 15.

The above results show that the proposed scheme is robust to Gaussian noise and improving K enhances the robustness. Besides this, the extracted watermark visibility improves for higher values of K as expected. The average BER at K=10 is 8.00 % and at K=20 is 0.46 %.

Table 10 BER (%) and NCC for Gaussian Noise (v=0.0001)

Gaussian Noise (K=10)		IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Watermark	BER	7.91	7.42	8.50	8.59	7.62	**8.00**
	NCC	0.9156	0.9265	0.9200	0.9167	0.9287	**0.9215**
EPR	BER	5.58	5.09	4.99	4.89	5.68	**5.24**
	NCC	0.9451	0.9506	0.9534	0.9616	0.9561	**0.9534**
Gaussian Noise (K=20)							
Watermark	BER	0.39	0.59	0.39	0.68	0.29	**0.46**
	NCC	0.9956	0.9945	0.9956	0.9923	0.9967	**0.9949**
EPR	BER	0.68	0.59	0.39	0.59	1.17	**0.68**
	NCC	0.9945	0.9931	0.9959	0.9931	0.9877	**0.9926**

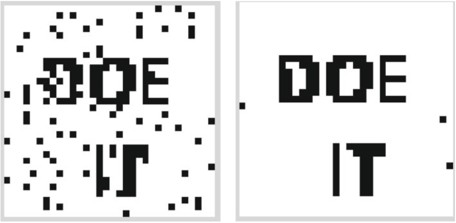

(a) (b)

Fig. 15 **a** Extracted watermark at 'K'=10 (**b**) Extracted watermark at 'K'=20

4.2.9 Robustness analysis for hybrid attacks

The watermarked images are subjected to various hybrid attacks, recognizable watermarks are obtained from each case. The detailed analysis for hybrid attacks is presented below:

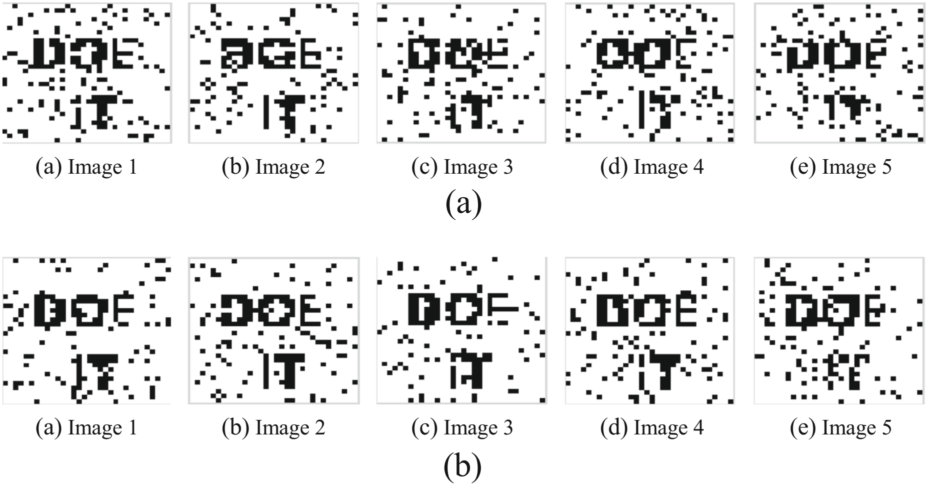
Salt and pepper noise plus sharpening attack The watermarked images are distorted with salt and pepper noise with noise density 0.01 and then the attacked images are sharpened. The results of extracted watermarks, in terms of BER and NCC are shown in Table 11. Figure 16a and b depicts the extracted watermarks after testing the watermarked image to the above said hybrid attack for K=10 and K=20 respectively. It is evident from the results that robustness of our scheme to the hybrid attack under discussion increases with K.

Histogram equalization plus sharpening attack The watermarked images are tested for histogram equalization and then the attacked images are sharpened. Table 12 shows the detailed robustness parameters. Figure 17a and b shows the extracted watermarks after histogram equalization plus sharpening attack for K=10 and K=20 respectively. Clearly, our scheme performs well for this hybrid attack. As observed BER values lie between 1.05 and 0.58 % for watermark extraction.

Salt & Pepper noise plus Median filtering plus Histogram equalization attack The watermarked images are simultaneously attacked by salt & pepper noise with noise density 0.01, histogram equalization and Median filtering. Various observed parameters for robustness

Table 11 Robustness parameters for K=10 and K=20

Salt & Pepper+Sharpening (K=10)		IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Watermark	BER	11.72	11.04	10.35	10.45	11.62	**11.04**
	NCC	0.8816	0.8816	0.8958	0.8947	0.8827	**0.8873**
EPR	BER	11.04	8.89	8.40	7.62	10.74	**9.39**
	NCC	0.8793	0.9114	0.9204	0.9284	0.8939	**0.9067**
Salt & Pepper+Sharpening (K=20)							
Watermark	BER	7.91	7.62	8.40	7.62	8.30	**7.97**
	NCC	0.9243	0.9243	0.9200	0.9265	0.9134	**0.9217**
EPR	BER	8.50	6.64	5.27	4.79	8.20	**6.68**
	NCC	0.9098	0.9391	0.9593	0.9437	0.9278	**0.9359**


(a) Image 1 (b) Image 2 (c) Image 3 (d) Image 4 (e) Image 5

(a)

(a) Image 1 (b) Image 2 (c) Image 3 (d) Image 4 (e) Image 5

(b)

Fig. 16 **a** Extracted watermarks from five attacked images (K=10). **b** Extracted watermarks from five attacked images (K=20)

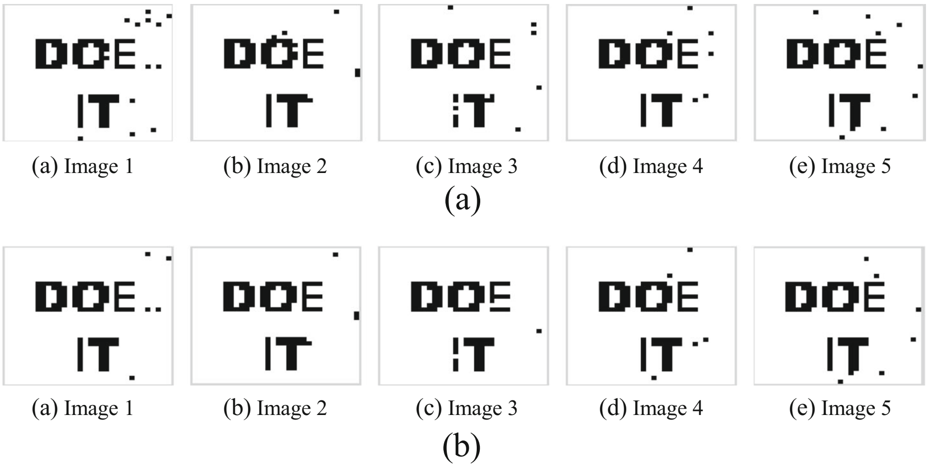
check are shown in Table 13. The extracted watermarks have been shown in Fig. 18a for K=10 and Fig. 18b for K=20 respectively. Low values of BER (2 to 4.5 %) have been observed for this three tier attack. Further, the visual quality of the extracted watermarks shows that the scheme robustness improves with increasing K.

Rotation plus Median filtering plus Sharpening attack The watermarked images are rotated by 10° and then it is attacked by Median filtering and finally the same attacked image is sharpened. Table 14 shows the different observed parameters for K=10 and K=20. The results observed in terms of BER and NCC show that our scheme is capable of withstanding this hybrid attack. The robustness of proposed scheme increases with increasing embedding factor.

The overall results obtained in our proposed scheme are better than that of [17]. The technique shows better robustness when the value of embedding factor is increased. However, the perceptual quality in some cases gets degraded. Throughout the analysis the watermarked images were subjected to different imperceptibility and robustness tests for different values of

Table 12 Robustness parameters for K=10 and K=20

Histogram Equalization +Sharpening (K=10)		IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Watermark	BER	1.56	1.46	0.78	0.59	0.88	**1.05**
	NCC	0.9846	0.9857	0.9945	0.9934	0.9901	**0.9897**
EPR	BER	3.81	3.61	1.27	0.78	2.44	**2.38**
	NCC	0.9641	0.9541	0.9882	0.9857	0.9814	**0.9747**
Histogram Equalization+Sharpening (K=20)							
Watermark	BER	0.78	0.68	0.29	0.49	0.68	**0.58**
	NCC	0.9923	0.9934	0.9989	0.9945	0.9923	**0.9943**
EPR	BER	1.86	1.76	0.49	0.20	1.56	**1.17**
	NCC	0.9774	0.9795	0.9944	0.9980	0.9819	**0.9862**



(a) Image 1 (b) Image 2 (c) Image 3 (d) Image 4 (e) Image 5

(a)

(a) Image 1 (b) Image 2 (c) Image 3 (d) Image 4 (e) Image 5

(b)

Fig. 17 **a** Extracted watermarks from five attacked images (K=10). **b** Extracted watermarks from five attacked images (K=20)

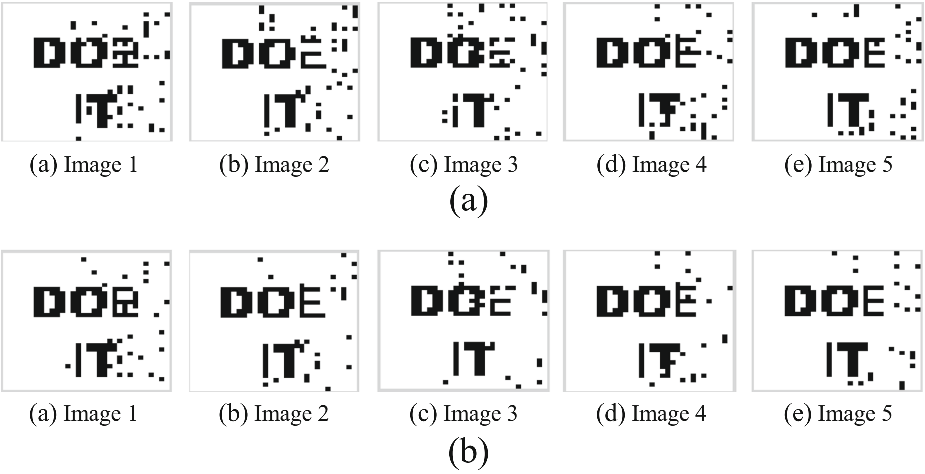
embedding factor 'K'. It can be clearly seen from the above detailed results and discussions that as the value of 'K' increase the robustness of the system increases. This is due to the fact that with an increase in the 'K' values, DCT coefficients are modified by relatively larger values, which in turn increases the difference between the coefficients. The increased difference between the two coefficients provides a wide guard band between them. With a relatively large difference between coefficients it is less likely for a singular or hybrid attack to change the difference to an erroneous zone. This results in the fulfillment of the condition for extraction of the correct bits even when the watermarked image is subjected to different image processing attacks.

II) Analysis for Second Algorithm

The second technique involves the embedding in the RONI region only, thus ensuring better quality of ROI for diagnostic purpose.

Table 13 Robustness parameters for K=10 and K=20

Salt & Pepper+Median filtering +Histogram equalization (K=10)		IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Watermark	BER	6.35	4.39	4.49	3.81	3.42	**4.49**
	NCC	0.9518	0.9529	0.9550	0.9594	0.9616	**0.9561**
EPR	BER	11.62	12.11	11.23	9.96	10.45	**11.07**
	NCC	0.8878	0.8953	0.8782	0.8834	0.8880	**0.8865**
Salt & Pepper+Median filtering+Histogram equalization (K=20)							
Watermark	BER	3.32	2.34	2.05	1.76	2.64	**2.42**
	NCC	0.9638	0.9770	0.9803	0.9814	0.9704	**0.9746**
EPR	BER	8.98	9.28	7.91	5.96	7.71	**7.97**
	NCC	0.9045	0.9157	0.9291	0.9403	0.9291	**0.9237**


(a) Image 1 (b) Image 2 (c) Image 3 (d) Image 4 (e) Image 5

(a)

(a) Image 1 (b) Image 2 (c) Image 3 (d) Image 4 (e) Image 5

(b)

Fig. 18 **a** Extracted watermarks from five attacked images (K=10). **b** Extracted watermarks from five attacked images (K=20)

4.3 Imperceptibility analysis

For testing the imperceptibility of the RONI/ ROI based embedding scheme. A watermark of size 47×47 has been used. Image indices, PSNR, SSIM and NAE have been used to evaluate perceptual transparency. The results obtained have been presented in Table 15, where in five CT scan images have been used.

It is evident from the Table that proposed scheme is capable of providing high quality watermarked images as average PSNR obtained is above 54 dB and average SSIM is 0.9875 without having the ROI tampered. The relatively better results of PSNR, observed in this algorithms is due to the fact that critical information region, is not used for embedding.

4.4 Robustness analysis

The robustness analysis of the proposed scheme has been carried out by subjecting watermarked images obtained from the system to various attacks like, salt and pepper noise,

Table 14 Robustness parameters for K=10 and K=20

Rotate+Median filtering +Sharpening (K=10)		IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Watermark	BER	7.32	7.32	8.79	3.52	4.98	**6.39**
	NCC	0.9276	0.9276	0.9123	0.9627	0.9441	**0.9349**
EPR	BER	20.31	16.89	18.36	15.04	17.87	**17.69**
	NCC	0.8344	0.8446	0.8111	0.8410	0.8318	**0.8326**
Rotate+Median filtering+Sharpening (K=20)							
Watermark	BER	6.15	7.03	8.01	3.03	4.88	**5.82**
	NCC	0.9397	0.9309	0.9189	0.9682	0.9452	**0.9406**
EPR	BER	15.23	15.92	13.87	12.01	15.72	**14.55**
	NCC	0.8639	0.8541	0.8712	0.8752	0.8669	**0.8663**

Table 15 Imperceptibility parameters

Image	Proposed Scheme [Payload (2209 bits)]		
	PSNR (dB)	SSIM	NAE
Image 1	54.3147	0.9875	0.0035
Image 2	54.3754	0.9876	0.0034
Image 3	54.3684	0.9875	0.0031
Image 4	54.3715	0.9876	0.0033
Image 5	54.3764	0.9875	0.0043
Average	54.3613	0.9875	0.0035

Gaussian noise, JPEG compression, rotation, different filtering processes (Median filtering, Wiener filtering and Average filtering) and other image processing techniques.

4.4.1 Robustness analysis against salt & pepper attack

The watermarked medical images are tested for salt & pepper noise with varying noise densities from 0.001 to 0.01. The results of the proposed technique are shown in Fig. 19 and the extracted watermarks for various noise densities are shown in Fig. 20. It has been observed that average BER values increase from 1.5 to 12 % as noise density is increased from).001 to 0.01. The visual quality of the extracted watermark shows that robustness reduces with increased noise density.

4.4.2 Robustness analysis against different filtering attacks

Various filtering attacks have been applied to watermarked images. The filter kernel used for Average filtering, Median filtering and Wiener filtering is 3×3. Figure 21 shows the extracted watermark of Image 1 after the application of the different filtering attacks. The observations made in this regard are discussed below:

Median filtering The test images are subjected to Median filtering of filter size 3×3. The average NCC and BER of the extracted watermarks is 0.9990 and 0.16 % for K=10. These figures indicate that proposed algorithm is highly robust to Median filtering. The numerical results observed are substantiated by Fig. 21a.

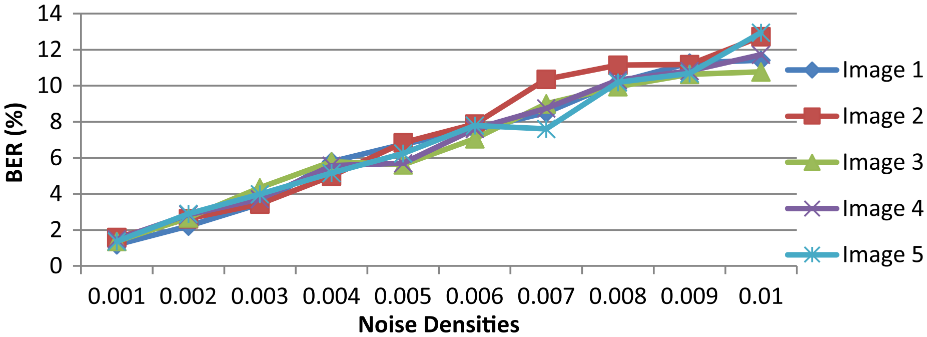


Fig. 19 BER (%) for salt and pepper noise at different noise densities

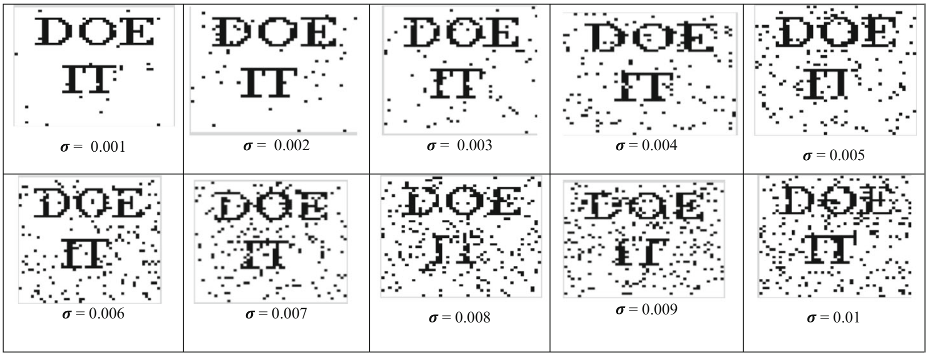


Fig. 20 Extracted watermarks after salt and pepper noise attacks (0.001 to 0.01) for Image 1

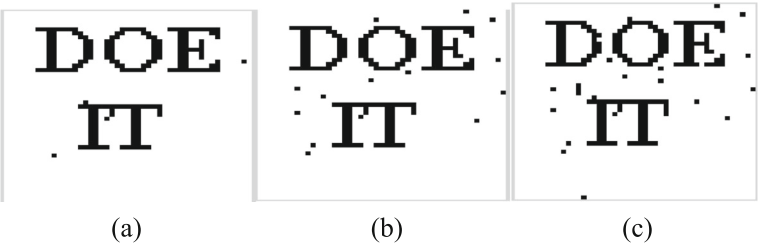


Fig. 21 Extracted watermarks (**a**) Median filtering (**b**) Wiener filtering (**c**) Average filtering

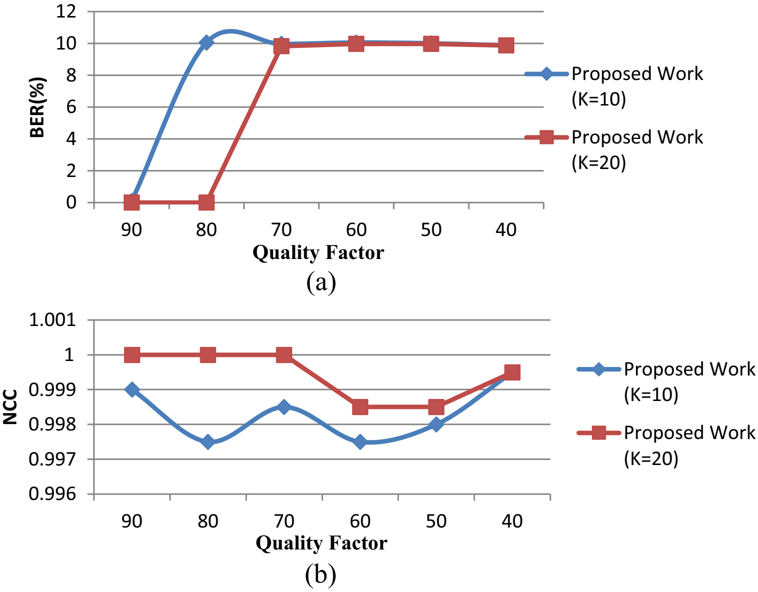
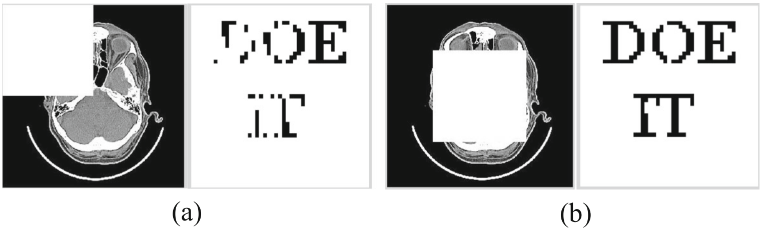


Fig. 22 **a** Plot between the BER (%) and Quality Factor for Image 1. **b** Plot between the NCC and Quality Factor for Image 1

Table 16 BER (%) and NCC against different Quality Factors for the test images

IMAGES	QF	K=10		K=20	
		BER (%)	NCC	BER (%)	NCC
IMAGE 1	90	0.09	0.9990	0	1
	80	10.05	0.9975	0	1
	70	9.96	0.9985	9.82	1
	60	10.05	0.9975	9.96	0.9985
	50	10.00	0.9980	9.96	0.9985
IMAGE 2	90	0	1	0	1
	80	9.82	1	0	1
	70	9.82	1	9.82	1
	60	9.82	1	9.82	1
	50	9.87	0.9995	9.82	1
IMAGE 3	90	0.04	0.9995	0	1
	80	9.87	0.9995	0	1
	70	9.87	0.9995	9.82	1
	60	9.87	0.9995	9.87	0.9995
	50	9.87	0.9995	9.87	0.9995
IMAGE 4	90	0	1	0	1
	80	9.91	0.9990	0	1
	70	9.87	0.9995	9.82	1
	60	9.87	0.9995	9.82	1
	50	9.91	0.9990	9.87	0.9995
IMAGE 5	90	0	1	0	1
	80	9.87	0.9995	0	1
	70	9.87	0.9995	9.82	1
	60	9.87	0.9995	9.87	0.9995
	50	9.87	0.9995	9.87	0.9995

Wiener filtering The extracted watermark after Wiener filtering attack is shown in Fig. 21b. The average NCC and BER of extracted watermarks is 0.9960 and 0.44 % for K=10. The observed BER values (less than 0.55 %) show that the scheme is highly robust to Wiener filtering.



(a) (b)

Fig. 23 **a** 25%Left corner cropped image, Extracted watermark (**b**) 25%centre cropped image, Extracted watermark

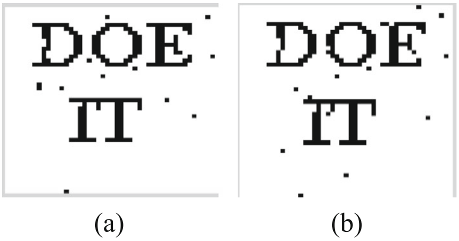


Fig. 24 **a** Extracted watermark after 5° rotation (**b**) extracted watermark after 10° rotation

Table 17 BER (%) and NCC of different images for sharpening attack

Sharpening		IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Watermark	BER	0.04	0.00	1.27	0.00	0.00	**0.26**
	NCC	0.9995	1.0000	0.9890	1.0000	1.0000	**0.9977**

Average filtering Figure 21c shows the extracted watermark after Average filtering attack. The average NCC and BER equals to 0.9909 and 0.89 % for K=10. The results show that our technique is robust to average filtering.

4.4.3 Robustness analysis against JPEG attack

The watermarked images, as obtained, using the second algorithm have been tested for JPEG comparison for various quality factors. Figure 22a shows the plot between the BER and the Quality factor. The figure indicates that as Quality Factor increases the BER decreases. Figure 22b shows the plot between the NCC and the Quality factor. It is further obvious from the results that for a given Quality factor, BER and NCC improve as the value of K is increased.

The proposed algorithm has been tested for five different test images and the results are shown in Table 16. It could be seen that the scheme performs well for JPEG compression. The results are found to improve with increase in K.

Fig. 25 Extracted watermark after sharpening attack

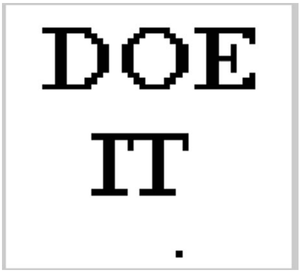


Table 18 BER (%) and NCC for Histogram Equalization of watermarked images

Histogram Equalization		IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Watermark	BER	0.0000	0.0000	0.0000	0.0000	0.0000	**0.0000**
	NCC	1.0000	1.0000	1.0000	1.0000	1.0000	**1.0000**

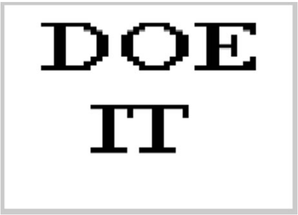


Fig. 26 Extracted watermark after histogram equalization

4.4.4 Robustness analysis against cropping

The proposed work has been tested for cropping attack. After cropping 25 % (at top left corner) of the watermarked image at K=10 the average BER (%) obtained for watermark is 3.63 and average NCC is 1.0000. After cropping 25 % (at center) of the watermarked image at K=10 the average BER (%) obtained for watermark is 0.252 and average NCC is 1.0000. Figure 23 shows the watermarked images and extracted watermarks and it is clear that the proposed technique is robust to cropping attack.

4.4.5 Robustness analysis against rotation attack

The watermarked images have been tested for rotation attack. The average BER and NCC results obtained for 5° are 0.68 % and 0.9950 (K=10), while as for same value of 'K' and a rotation of 10° the average BER and NCC values are respectively 0.88 % and 0.9955. Results reveal that the proposed technique is robust to rotation attack. This is confirmed by Fig. 24 also.

4.4.6 Robustness analysis against sharpening attack

The watermarked images have been tested for sharpening attack. Table 17 shows the results of different images at K=10. The NCC values close to unity and BER as less

Table 19 BER (%) and NCC for Gaussian Noise (v=0.0001) of watermarked images

Gaussian Noise		IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Watermark	BER	10.14	10.10	9.10	10.64	9.19	**9.83**
	NCC	0.9006	0.8996	0.9106	0.8941	0.9101	**0.9030**

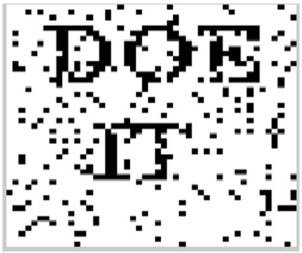


Fig. 27 Extracted watermark after Gaussian Noise

Table 20 BER and NCC values for hybrid attack (Salt and pepper+Median Filtering)

Salt & Pepper+Median Filtering		IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Watermark	BER	0.18	0.09	0.04	0.09	0	**0.08**
	NCC	0.9980	0.9990	0.9995	0.9990	1	**0.9985**

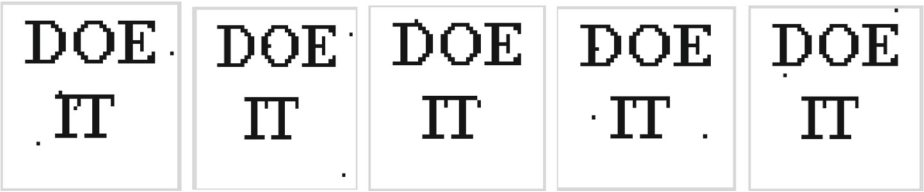
as 0.26 % indicate that the proposed algorithm is robust to this attack. Figure 25 authenticates our argument.

4.4.7 Robustness analysis against histogram equalization

Watermarked images obtained using the proposed technique were subjected to Histogram Equalization. The BER and NCC values for K=10, after Histogram Equalization is shown in Table 18. The average BER(%) obtained is 0 and average NCC is 1.0000. From Fig. 26 and Table 18 it is clear that the proposed algorithm is completely robust to histogram equalization.

4.4.8 Robustness analysis against gaussian noise

The watermarked images are subjected to Gaussian Noise attack (variance=0.0001). The BER and NCC at K=10 of the watermarked images is shown in Table 19. Figure 27 shows the extracted watermark. Though the results obtained are not as convincing as in case of histogram equalization, however the watermark is still recognizable.

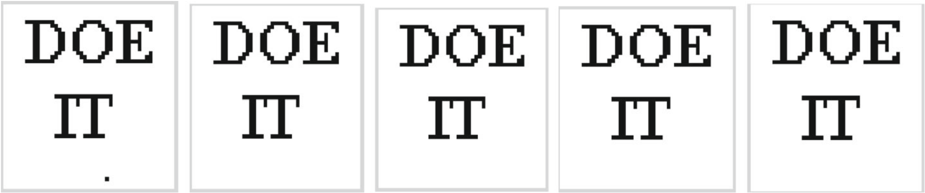


(a) Image 1 (b) Image 2 (c) Image 3 (d) Image 4 (e) Image 5

Fig. 28 Extracted watermarks from five different images

Table 21 Robustness parameters for hybrid attack (Histogram Equalization+Sharpening)

Histogram Equalization+Sharpening		IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Watermark	BER	0.04	0	0	0	0	**0.008**
	NCC	0.9995	1	1	1	1	**0.9999**



(b) Image 1 (b) Image 2 (c) Image 3 (d) Image 4 (e) Image 5

Fig. 29 Extracted watermarks if five different images

4.4.9 Robustness analysis for hybrid attacks

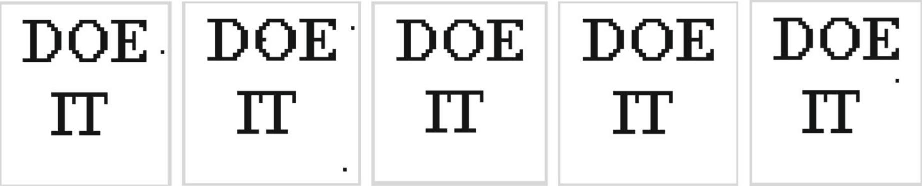
The watermarked images are subjected to various hybrid attacks. It has been observed that recognizable watermarks are obtained from each case. The detailed analysis for hybrid attacks is presented below:

Salt and pepper noise plus Median Filtering The watermarked images are distorted with salt and pepper noise with noise density 0.01 and then the attacked images are filtered using Median filtering. Watermarks extracted from the attacked images with BER and NCC is shown in Table 20. It is pertinent to mention here that embedding factor of K=10 has been used here. Figure 28 shows the extracted watermarks from five used images. The low values of BER obtained coupled with the extracted perceptual quality of watermarked images show that the proposed technique is robust to this hybrid attack.

Histogram equalization plus sharpening attack The watermarked images are tested for histogram equalization and then the attacked images are sharpened. Table 21 shows the detailed robustness parameters while as Fig. 29 shows the extracted watermarks from various attacked images. It is observed from quality indices that our scheme is highly robust to this hybrid attack

Table 22 BER and NCC values for hybrid attack (Salt and Pepper noise+Median Filtering+Histogram Equalization)

Salt & Pepper+Median filtering +Histogram equalization		IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Watermark	BER	0.04	0.14	0	0	0.04	**0.044**
	NCC	0.9995	0.9985	1	1	0.9995	**0.9995**



(a) Image 1 (b) Image 2 (c) Image 3 (d) Image 4 (e) Image 5

Fig. 30 Extracted watermarks for five different images

Table 23 Robustness parameters for hybrid attack (Rotation+Median Filtering+Sharpening)

Rotate+Median filtering+ Sharpening		IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Watermark	BER	0.77	0.72	0.36	0.86	0.81	**0.70**
	NCC	0.9985	0.9980	0.9975	0.9975	0.9980	**0.9979**

Salt & Pepper noise plus Median filtering plus Histogram equalization attack The watermarked images are simultaneously attacked by salt & pepper noise with noise density 0.01, histogram equalization and Median filtering with K=10. The different observed parameters are shown in Table 22. The robustness of the proposed scheme to this three tier attack is substantiated by very low BER(less than 0.05 %). The results are substantiated by Fig. 30.

Rotation plus Median filtering plus Sharpening attack The watermarked images are rotated 10° and then it is attacked by Median filtering and finally sharpened. Table 23 shows the different observed parameters for K=10 and the extracted watermarks are shown in Fig. 31. It can be observed from the Table that average BER value for such an attack is (0.70 %). Further near unity NCC values and quality of extracted watermarks show that the proposed algorithm is robust to this attack.

The results obtained in the second algorithm show better perceptual quality and robustness as compared to the first algorithm because of the fact that only RONI region is used for embedding purpose. Since, in RONI the pixels have high correlation as compared to that of the ROI region. Therefore, the relative difference between the selected DCT coefficients is small which in turn brings a small change in original image when watermark is embedded.

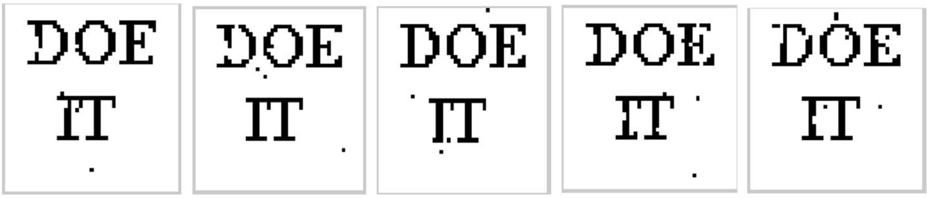


Fig. 31 Extracted watermarks of five different images

5 Conclusion

E-Healthcare is a buzz word nowadays. The concept of E-health care has made the distance in healthcare irrelevant. However, the practical implementation of an E-Healthcare system poses its own set of challenges. One of the major challenges is to maintain integrity of the vital medical data during transit. Watermarking is being currently used as a potent solution for ensuring integrity, authentication and copyright protection of medical data. This paper presents two different blind approaches for watermarking of medical images. In both the approaches relative magnitude of preselected DCT coefficients is used for embedding the watermark/EPR. In the first approach the watermark is embedded in Region of Interest and Region of Non Interest of the medical image. However, in second approach the embedding takes place in the Region of Non Interest only. The embedding is carried out in the transform domain, where in block based (8×8) DCT has been used. The watermarked images have been tested for various singular and hybrid image processing operations. The results reveal that the proposed techniques are highly imperceptible besides being robust to various image processing attacks like sharpening, Salt and Pepper noise, JPEG, Gaussian noise and rotation, Cropping, Filtering etc. Given the performance of both the techniques to various attacks the proposed algorithms can prove to be handy in an E-health system.

References

1. Baiying L, Ee-Leng T, Siping C, Dong N, Tianfu W, Haijun L (2014) Reversible watermarking scheme for medical image based on differential evolution. Expert Syst Appl 41:3178–3188
2. Bousilimi D, Coatrieux G, Roux C (2012) A joint encryption/watermarking algorithm for verifying the reliability of medical images: application to echographic image. Comput Methods Programs Biomed 106:47–54
3. Chen YH, Chang TY, Li CY (2011) High throughput DA- based DCT with high accuracy error compensated adder tree. IEEE Trans VLSI Syst 19:709–714
4. Coatrieux G, Montagner J, Huang H, Roux C (2007) Mixed reversible and RONI watermarking for medical image reliability protection. 29th International conference of the IEEE. Eng Med Biol Soc Lyon 5653–6
5. Das S, Kundu MK (2012) Effective management of medical information through a novel blind watermarking technique. J Med Syst 36:3339–3351
6. Das C, Panigrahi S, Sharma VK, Mahapatra KK (2014) A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. Int J Electron Commun 68:244–253
7. Fotopoulos V, Stavrinou ML, Skodras AN (2008) Medical image authentication and self-correcting through an adaptive reversible watermarking technique. Proceedings of 8th IEEE International Conference on Bio Informatics and Bio Engineering (BIBE2008) 1–5
8. Ghulam MB, Muhammad M, Shabir AP, Javaid A (2010) Field programmable gate array (FPGA) implementation of novel complex PN-code-generator-based data scrambler and descrambler. Maejo Int J Sci Technol 4(1):125–135
9. Giakoumaki, Pavlopoulos AS, Koutsouris D (2010) Multiple image watermarking applied to health information management. IEEE Trans Inf Technol Biomed 4:722–732
10. Liqiang N, Meng W, Luming Z, Shuicheng Y, Zhang B, Tat-Seng C (2015) Disease inference from health-related questions via sparse deep learning. IEEE Trans Knowl Data Eng 27(8):2107–2119
11. Liqiang N, Mohammad A, Tao L, Jialie S, Tat-Seng C (2014) A joint local–global approach for medical terminology assignment. In Proc. Int. ACM SIGIR Conf., 2014
12. Liqiang N, Tao L, Mohammad A, Jialie S, Tat-Seng C (2014) WenZher: comprehensive vertical search for healthcare domain. (2014). The 37th International ACM SIGIR Conference on Research and Development in Information Retrieval(SIGIR'14). doi:10.1145/2600428.2611176
13. Liqiang N, Yi-Liang Z, Mohammad A, Jialie S, Tat-Seng C (2015) Bridging the vocabulary Gap between health seekers and healthcare knowledge. IEEE Trans Knowl Data Eng 27(2):396–409
14. Navas KA, Thampy SA, Sasikumar M (2008) EPR hiding in medical images for telemedicine. Proc World Acad Sci Eng Technol Rome 292–295

15. Osamah M, Al-Qershi O, Khoo BE (2009) Authentication and data hiding using a reversible ROI-based watermarking scheme for DICOM images. Int J Inf Commun Eng 5:801–806
16. Priya RL, Sadasivam V (2014) A survey on watermarking techniques, requirements, application for medical images. J Theor Appl Inf Technol 65
17. Rahimi F, Rabbani H (2011) A dual adaptive watermarking scheme in contourlet domain for DICOM images. Biomed Eng Online
18. Rao NA, Meena Kumari V (2011) Watermarking in medical imaging for security and authentication. Taylor & Francis Inf Secur J A Global Perspect 20:148–155
19. Raul RC, Claudia FU, Gershom de JTB (2007) Data hiding scheme for medical image. IEEE 17th International Conference on Electronics Communications and Computers (CONIELECOMP'07)
20. Shabir AP, Javaid AS, Muheed H, Ghulam MB (2014) A Secure and robust information hiding technique for covert communication. Int J Electron 102:1253–1266
21. Shabir AP, Javaid AS, Umer IA, Ghulam MB (2015) Hiding in encrypted images: a three tier data hiding scheme. Multidim Syst Sign Process 1–24
22. Shabir AP, Javaid AS, Ghulam MB (2014) Fragility evaluation of intermediate significant bit embedding (ISBE) based digital image watermarking scheme for content authentication. International Conference on Advances in Electronics, Computers and Communications (ICAECC), 1–6
23. Shabir AP, Javaid AS, Ghulam MB (2014) A secure and efficient spatial domain data hiding technique based on pixel adjustment. Am J Eng Technol Res 14(2):33–39
24. Shaoqing R, Kaiming H, Ross G, Jian S (2015) Faster R-CNN: towards real-time object detection with region proposal networks. Computer Vision and pattern recognition. In arXiv:1506.01497
25. Singh R (2001) Emerging technologies that will change the world: digital rights management. MIT Technol Rev. http://www.technologyreview.com/infotech/12264
26. Singh AK, Kumar B, Dave M, Mohan A (2015) Robust and imperceptible dual watermarking for telemedicine application. Wirel Pres Commun 80:1415–1433
27. Solanki N, Malik SK (2014) ROI based medical image watermarking with zero distortion and enhanced security. Int J Educ Comput Sci 10:40–48
28. Soliman MM, Hassanien AE, Ghali NI, Onsi HM (2012) An adaptive watermarking approach for medical imaging using swarm intelligent. Int J Smart Home 6:37–50
29. Subhashini D, Nalini P, Chandrasekhar G (2012) Comparison analysis of spatial Domain and compressed Domain steganographic techniques. Int J Eng Res & Technol (IJERT) 1
30. Wakatani A (2002) Digital watermarking for ROI medical images by using compressed signature image. Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS) 7–10 Jan 2002
31. Yan Y, Elisa R, Gaowen L, Nicu S (2015) Egocentric daily activity recognition via multitask clustering. IEEE Trans Image Process 24(10):2984–2995
32. Zitnick CL, Doll'ar P (2014) Edge boxes: locating object proposals from edges. In ECCV

Shabir A. Parah has completed his M. Sc and M. Phil and Ph.D in Electronics from University of Kashmir, Srinagar in the year 2004, 2010 and 2013 respectively in the field of Signal processing and Data hiding. He is working as Assistant Professor in the department of Electronics and I. T, University of Kashmir, Srinagar. His fields of interest are Signal Processing, Secure Communication, Digital Watermarking and Steganography. Dr. Shabir A. Parah has guided about tewnty five PG projects. He has published more than sixty research papers in International/National journals and conference proceedings.

Javaid A. Sheikh has completed his M.Sc., M. Phil and Ph. D in Electronics from University of Kashmir, Srinagar in the year 2004, 2008 and 2012 respectively in the field of communications and Signal Processing. He is working as Assistant Professor in the department of Electronics and I. T University of Kashmir, Srinagar. His fields of interest are Wireless Communications, design and development of efficient MIMO OFDM based wireless communication techniques, Spread Spectrum modulation, Digital Signal Processing, Electromagnetics. He has published about sixty research papers in International and National journals and conference proceedings.

Farhana Ahad is a doctoral scholar in the Department of Electronics and IT, University of Kashmir. She is currently working on development of watermarking algorithms for e-healthcare systems.

Nazir A. Loan is a doctoral scholar in the Department of Electronics and IT, University of Kashmir and is currently working on the Development of Robust watermarking algorithms for multimedia applications. He is INSPIRE fellow of Department of Science and Technology Government of India.

G. Mohiuddin Bhat obtained his M.Sc. (Electronics) from the University of Kashmir, Srinagar (India) in 1987, M.Tech. (Electronics) from Aligarh Muslim University (AMU), Aligarh (India) in 1993 and Ph.D. Electronics Engg. from AMU, Aligarh, (India) in 1997. The major field of research of Dr. Bhat is Signal Processing Techniques and Secure Message Communication. He has served as Assistant Professor, Associate professor and now as Professor & Head, Department of Electronics and Instrumentation Technology, University of Kashmir. He has published many research papers on his area of interest. He has worked in the area of Mobile Radio Communication, Spread Spectrum Communication and Neural Networks and has guided many research degrees leading to the award of M.Phil and Ph.D. His present research interests include Secure Message communication, Neural networks and Signal Processing techniques for communication.