



A fuzzy based ROI selection for encryption and watermarking in medical image using DWT and SVD

Balasamy K¹  · Suganyadevi S²

Received: 20 November 2019 / Revised: 18 September 2020 / Accepted: 24 September 2020 /

Published online: 26 October 2020

© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract

Nowadays secure medical image watermarking had become a stringent task in telemedicine. This paper presents a novel medical image watermarking method by fuzzy based Region of Interest (ROI) selection and wavelet transformation approach to embed encrypted watermark. First, the source image will undergo fuzzification to determine the critical points through central and final intensity along the radial line for selecting region of interest (ROI). Second, watermark image is altered to time-frequency domain through wavelet decomposition where the sub-bands are swapped based on the magnitude value obtained through logistic mapping. In the each sub-band all the pixels get swapped, results in fully encrypted image which guarantees the watermark to a secure, reliable and an unbreakable form. In order to provide more robustness to watermark image, singular values are obtained for encrypted watermark image and key component is calculated for avoiding false positive error. Singular values of the source and watermark image are modified through key component. Experimental results reveal that the proposed algorithm attains high robustness and improved security to the watermarked image against various kinds of attacks.

Keywords Fuzzy ROI · Wavelet transform · Encryption · Key component · Watermarking

1 Introduction

Telemedicine based medical image diagnosis is done through various techniques like computed tomography, ultrasound scanning, X-ray, magnetic resonance imaging, positron

✉ Balasamy K
balasamyk@gmail.com

¹ Department of Information Technology, Dr.Mahalingam College of Engineering and Technology, Pollachi, India

² Department of ECE, School of Engineering, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India

emission tomography. The investigative images are widely kept and it will undergo transmission for texture collection [8], image de-noising [2], segmentation [38], information hiding [34], and compression [12]. Consequently, medical images are scattered via hospital intranet and in the internet, where patient's privacy information are available. However, hospital intranet will lack in the security issues related to patient information results in data leak [11, 28, 30].

With reference to visibility, medical image watermarking is categorized into visible and invisible domain [3, 19]. Further invisible watermarking is categorized into transform and time domain approaches [19, 20]. In transform domain approach, the host image will undergo transformation before embedding the watermark. Alternatively, time domain mechanism uses changes in the pixel values with respect to watermark information. Transform domain are classified into ridgelet transform [45], IWT [3], DCT [7], DWT [20, 21, 26], SVD [14], moments transform [36], curvelet transform [49].

The rest of the article is organized as follows: In Section 2 state of art of medical image watermarking is briefly presented. In Section 3 we discuss the fundamental concepts of wavelet transform, logistic mapping and SVD. Section 4 describes about the proposed algorithm in detail. In Section 5, results obtained from the proposed algorithm and performance evaluation is described in detail. In Section 6, the conclusion is provided.

2 Related work

In medical imaging, various watermarking methods are proposed previously [1, 4–6, 9, 10, 13, 15–18, 22–25, 27, 29, 31–33, 35, 37, 39–48, 50, 51]. In [37] Chao et al. have proposed bipolar multiple base conversion for information hiding, where multiple data can be encrypted in a single image. Acharya et al. [15, 42] proposes embedding patient's information in two different ways. In [42], authors use error correction (EC) scheme, which improves the Least Significant Bit (LSB) algorithm efficiency in medical image transmission and storage, where the medical image is embedded with patient data. Same author in [15] uses coefficients of discrete cosine transform (DCT) for embedding graphical signals and text data in the last bit of DCT. Zainet al [48] proposes medical image authentication through obtaining region of interest (ROI) in the spatial domain. In [44] author proposed a multiple watermark method results in good imperceptibility and detecting the tamper in medical images for privacy control. Block based schemes proposed by Wu et al. in [5, 32, 45], uses modulo operation with adaptive watermarking technique results in tamper detection and recovery. In [9, 24, 43] author uses region based medical image watermarking (MIW) along with adjacent pixel value differential expansion method for authentication and security enhancement.

Chaotic systems and Region of Interest (ROI) become more sensitive in the past few years for maintaining the robustness of the watermark. Medical images can be segmented into ROI (Region of Interest) and RONI (Region of Non-Interest). This is to increase the diagnostic purpose and authenticating medical images. ROI section includes the useful region for diagnostic, whereas RONI represents the black background of the image. ROI based method proposed in [41], divides the medical image into blocks and uses LSB based substitution method in RONI region for watermark embedding. In [29] Wu et al. presents a watermarking method in medical images for contrast enhancement. Similarly, in [1], an author uses hybrid technique for medical images, which combines encryption and watermarking. Additionally in [4, 35] authors proposed dual watermarking methods, both in ROI an RONI region, tamper

detection and recovery information of medical images. In [17] parameter α determines the objective function along with neighbourhood effect, which maintains a balancing solution between robustness and preserving the homogenous region. Subsequently an expert knowledge is introduced into the FCM model to form Supervised FCM algorithm (S_FCM).

Das and Kundu [9] developed a blind, fragile and ROI reversible watermarking scheme. This system joins lossless compression and encryption to hide DICOM metadata, image hash and tamper localization information into digital medical image. Secure Hash Algorithm (SHA-256) is adopted to calculate the ROI hash. Medical image integrity is confirmed by comparing the embedded and recalculated hash data. Eswaraiah and Reddy [10] presented a fragile watermarking method for validating the integrity of ROI, identifying the manipulated blocks inside ROI and recovering the original ROI region. In this technique, the medical image is divided into three parts; ROI, RONI and border region. The hash code of the ROI is computed using SHA-256 and hidden in the border region. Authentication and ROI recovery information are encoded into the RONI. Several limitations can be observed in these schemes [9, 10]; the ROI part needs to be defined manually, the ROI can only be retrieved after extracting the concealed data, and a substantive location map is required for extraction.

Gao, et al. [14] present a reversible watermarking approach to achieve contrast enhancement of ROI and tamper detection against attacks on the ROI. The watermark is embedded along with distortion-less contrast enhancement of the ROI by expanding of the peak-pairs of the ROI histogram. The feature-bit matrix created from the ROI is encoded into the LSBs of the background pixels to ensure the reversibility of the ROI. The major limitations of this approach are the need for embedding the feature-bit matrix and only the ROI part of the image can be retrieved at extraction. A novel medical image authentication approach was proposed by Balasamy et al. [3] using Discrete Wavelet Transform (DWT) and Particle Swarm Optimization (PSO). This approach finds optimal wavelet coefficients for concealing the watermark data using PSO to produce a watermarked image with low distortion. The extraction process does not require auxiliary information, but this approach has high image deformation in comparison to the low hiding capacity of the technique. Yang, et al. [39] propose a reversible and high capacity data hiding scheme for secure archiving of medical images. The contrast of the ROI part is enhanced by extending the gray-scale values and encoding the data into peak bins of the extended histogram without stretching the histogram bins. The remaining large data is embedded into the RONI part without considering visual image quality. Evaluation of the scheme shows low invisibility between the original image and watermarked versions in terms of Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index (SSIM) due to applying contrast enhancement to the watermarked images. Pan, et al. [45] presents a fragile reversible watermarking approach for digital radiographic images. This technique differentiates the background from anatomical details within the image. Histogram Shifting (HS) modulation is used to encode the watermark into the background section while HS is applied to wavelet detail coefficients of the anatomical object, encoding watermark data with the image quantum noise. This scheme delivers a reasonable visual image quality, but hiding capacity is very low. Another approach [47] uses input image to S_FCM clustering to create LAWS_S_FCM variant. To reduce the noisy pixels on segmentation, weighted-sum image (WI) is calculated through the original $N \times M$ image (I) and convolving LAW 5×5 . However, this results in the high image deformation. The computational requirements other than ROI detection are not calculated in our work.

Our research proposes a blind, fragile and reversible watermarking technique for encoding the watermark into the cover image by extracting smooth ROI and to confirm authenticity and

integrity of both image pixel data and image header. The scheme embeds the data into smooth blocks inside the ROI to achieve a watermarked image with low distortion. The proposed scheme uses closed watermark for embedding, which is more secure. Encryption is done for analysing the correlation coefficient between two data sequences in order to avoid the loss of information, due to low correlation among the pixels that are adjacent. At extraction, the whole original image is fully recovered without the need for location map. The proposed method has been evaluated based on defined medical image watermarking requirements and compared to recent reversible watermarking approaches to verify its efficiency.

Our proposed system deals with the three main contributions,

- i) Identifying the region of interest (ROI) through fuzzy based model by determining the critical points along the radial line and incorporating the spatial function with membership function, results in increase in the compactness of partitions.
- ii) The encryption algorithm which we proposed operates on the frequencies in the wavelet transformed images, and the sub-bands of the images are swapped based on the magnitude value obtained through logistic mapping in the each sub-band by which all the pixels get swapped, results in fully encrypted image.
- iii) To make proposed system from providing more security and avoiding false positive error, Key Component is calculated from the encrypted watermark image and embedded into the DWT transformed source image.

3 Fundamental concepts

3.1 Wavelet transform

The implementation of the DWT is achieved through decomposing the source signal into high and low passes filters. This technique is generally called as multi-resolution analysis (MRA), where the signal is discretized based on the varying frequency bands and resolution.

Standard DWT decomposition results in four sub-bands. At first level of decomposition LL, LH, HL, and HH sub-bands are obtained. L and H denote high and low frequency components respectively. The fine scale wavelet coefficients of detail images are represented by LH, HL, & HH and coarser level low frequency coefficients of approximation image are represented by LL. Coefficients thus obtained from DWT of approximate and detail sub-bands in the source image are fundamental features.

3.2 Logistic mapping

The logistic map is a chaotic behaviour [15, 44, 47, 48] of non-linear mathematical equation to represents the complex equations in polynomial form, which is represented in Eq. 1

$$X_{n+1} = \mu \cdot x_n (1 - x_n) \quad (1)$$

Where $x_n \in [0, 1]$ that represent the ratio of standing population to the maximum potential population. The values for the parameter μ are in the interval $[0, 4]$ and a property value of the logistic map lies between 3.57 to 4.

3.3 SVD

Today almost every watermarking method is proposed as hybrid schemes (combining two or more transforms). A hybrid scheme utilizes the features of the combined transforms to attain the proposed system goal. This attainment is possible only if exact selections of the transforms are done. Three matrices namely U , S and V^T are obtained by decomposing a matrix through SVD, where all the matrices U , S and V^T represents the exact size of the source matrix as given below in Eq. 2,

$$M = USV^T \quad (2)$$

Where S represents the singular values, and U and V^T are singular vectors, respectively.

3.4 Avoiding false positive error

In spite of the strength and robustness of SVD-based medical image watermarking that conceal the watermark by singular vector modification, but these systems fails in determining the rightful ownership issue because they are not resistant to false positive error. The representation of SVD based watermarking is shown in Eq. 3,

$$I_w = I_h + \alpha * I_{wm} \quad (3)$$

In his watermarking scheme, the watermark will undergo SVD and the embedding procedure is achieved by modifying the I_h (singular values) by incorporating I_{wm} (watermark) and finally scaling factor α is multiplied with it. However, when false matrices are supplied it will result in the false watermark. If this issue continuous, final generated matrix will totally associated with false watermark, results in the false positive error. To overcome this issue, key component (KC) of the watermark is calculated through singular value and embedded into the watermark. The key component can be calculated as represented below in Eq. 4,

$$KC = U \times S \quad (4)$$

4 Proposed fuzzy based ROI segmentation and watermarking method

Our proposed method starts by finding region of interest (ROI) of source medical image through fuzzy method, and second level wavelet decomposition is carried out along with SVD to the source medical image. Watermark image will undergo 2-level DWT and permutation is applied on 2nd level sub-bands and substitution is applied on 1st level sub-bands. Singular value decomposition is applied on permuted watermark image and key component is calculated and then singular values of source medical image and watermark image are modified. Watermarked image is obtained by performing inverse wavelet transformation. The watermarking process is represented in Fig. 1.

4.1 Fuzzy based ROI selection

Using ROI regions for embedding the watermark, the pixels in those regions will deform, which results in wrong diagnosis. On the other hand, RONI watermarking approaches embed watermarks in areas that unimportant in medical diagnosis, but they have several drawbacks such as they can be only implemented if RONI exists, the amount of information to be

embedded depend on the RONI area size and ROI may not be protected against malicious attacks. The representation of ROI extraction is shown in Fig. 2.

One of the unsupervised systems for clustering is Fuzzy C-Means (FCM) clustering [20], which has extensive reputation. These promising methods are widely used in the applications like medical imaging, image segmentation and remote sensing and uses spatial locality [51] for clustering. Our method integrate this method with SS_FCM method, to form a new hybrid system, which membership value function of the neighbourhood pixels. The general representation of the spatial function is shown in Eq. 5,

$$S_{i_k}^u = \sum_{j \in NB(p_k)} U_{ij} \tag{5}$$

U_{ij} represents initial membership function and $NB(p_k)$ represents a square 5×5 window centred at pixel(p_k).

The spatial function is incorporated in the membership function and resultant function is represented as shown in Eq. 6

$$U_{i_k}^u = \frac{U_{i_k}^u S_{i_k}^u}{\sum_{j=1}^c U_{j_k}^u S_{j_k}^u} \tag{6}$$

The membership function $U_{i_k}^u$ is calculated and incorporated into the spatial function $S_{i_k}^u$ by partitioning the host image pixel into c clusters. Defuzzification is done to cluster the data points that provide hard labels to the pixels. Resulting segmented image is obtained by maximum membership method.

ROI of the proposed system is obtained by identifying central point in the host medical image and forming the radial lines from that point. In general, radial line is used for pattern development of any objects that have a tapering form with lines converging to a common point. In proposed

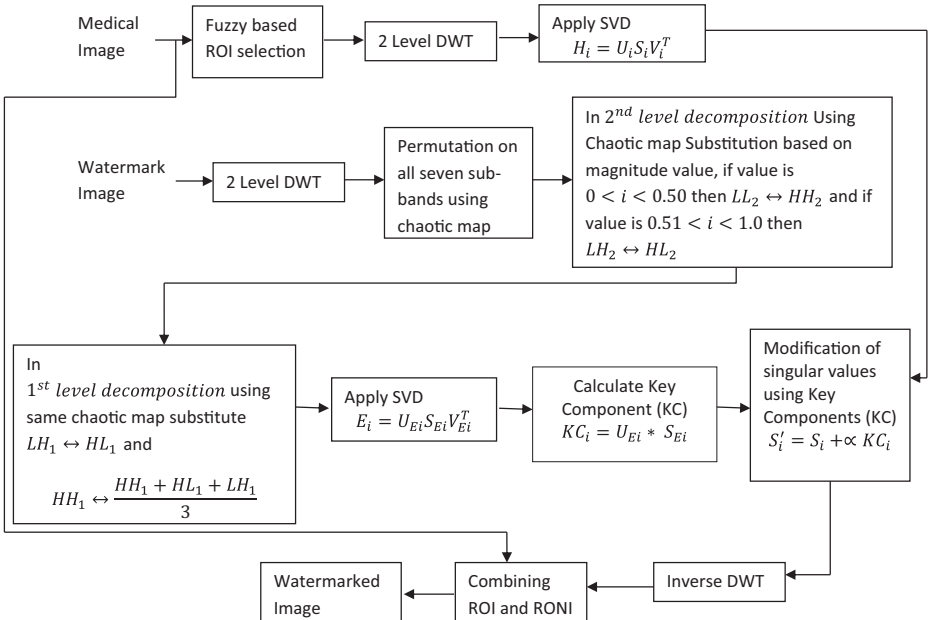


Fig. 1 Watermark embedding procedure

system, radial lines are used for determining the critical points from the converging common point. ROI of the medical image is obtained with high non-linearity, results in imposing two boundary conditions. First one is the determination of critical points, having three inputs i) intensity at the centre of ROI, ii) radial line in the final intensity and iii) intensity at the current point.

In our fuzzy system, only one output point is determined, which is either value 1 (inside ROI) or value 0 (outside ROI). While executing all the three input rules at same time, it is observed that all radial line (input 1 and input 2) are not varying as much, but the critical points are calculated either outside or inside ROI as represented in Fig. 3.

The introduced intensity difference rules have been reduced to only 12 rules (as represented in Table 1). Two cases PS (positive small) or NS (negative small) only exists in the rules, which reduces the total proposed system reduction in rules to 62%. The major reason for rules reduction is the variation that exists between inside and outside ROI.

4.2 Proposed encryption method using logistic map

The proposed encryption algorithm starts with a sequence of bytes in the 1D transformed image. Logistic mapping is applied on the 1st and 2nd level sub-bands of the wavelet transformed watermark image to provide fully encrypted image. So we use independent logistic map to exchange pixel positions are represented in Eq. 7,

$$x_{j+1} = \mu_1 x_j (1 - x_j) \tag{7}$$

Where $j \geq 0$, x initial seeds $\in [0, 1]$ then we follow the steps to encryption:

1. Process 2 level wavelet transformation on watermark image
2. Convert each sub-band of size $M \times N$ to one array Z^0 of size $8 \times M \times N$
3. Specify iteration of logistic map $r = 1, 2, \dots, R$ where R no. of round on all sub-bands
4. Specify initial condition,
 - keys of encryption x_0
 - $\alpha = 10^d$ is constant to scale x_{j+1}^r and compute $d = \text{floor}[\log_{10} z] + 3$
 - σ^r value of secret key according round
 - $r = 1$ and $Z^r = Z^0$ where Z^r image array at round r ,
 - $X = x_0^r, Y = y_0^r$
5. Handle the array of Z consecutive using loop $i = 0$ to $i = Z - 2$ then a new position j is computed by using the chaotic function as in eq.(11),

$$j = i + 1 + [\text{floor}[\alpha X_{i+1}] \text{mod } H] \text{ --- (11)}$$

Where H is initialize $Z - i$, i.e it decrease every iteration by 1 because modular operation select value of $\alpha X_{i+1} > H$.

6. The elements of 2nd level sub-bands are transformed based on Z^r magnitude value ,
 - if value is $0 < Z^r < 0.50$ then $LL_2 \leftrightarrow HH_2$ and
 - if value is $0.51 < Z^r < 1.0$ then $LH_2 \leftrightarrow HL_2$
7. The elements of 1st level sub-bands are transformed based on Z^r magnitude value
 - if value is $0 < Z^r < 0.50$ then
 - $LH_1 \leftrightarrow HL_1$ and

$$HH_1 \leftrightarrow \frac{HH_1 + HL_1 + LH_1}{3}$$

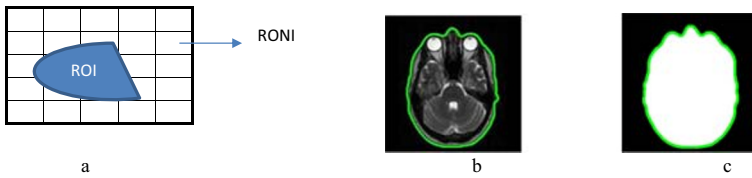


Fig. 2 a Image representation with ROI and RONI. b ROI contour. c ROI extraction

4.3 Watermarking algorithm

Embedding process is given below,

1. Read the source medical image S
2. Segment ROI through fuzzy based segmentation method as explained in section 2
3. Apply 2-level DWT on Segmented ROI of S , $S = [LL_2, HL_2, LH_2, HH_2]$
4. Apply SVD to HH_2 sub-band

$$HH_i = U_i S_i V_i^T$$

5. Read the watermark image W
6. Apply 2-level DWT on W , $W = [LL_2, HL_2, LH_2, HH_2]$
7. Use logistic map for encryption as explained in section 4.1
8. Apply SVD to HH_2 sub-band Encrypted image E_i ,

$$E_i = U_{Ei} S_{Ei} V_{Ei}^T$$

9. Calculate Key Component

$$KC_i = U_{Ei} * S_{Ei}$$

10. Modify the singular values of source and watermark image using Key Components (KC)

$$S'_i = S_i + \alpha KC_i$$

11. Apply Inverse DWT
12. Combine ROI and RONI region and finally watermarked image is obtained.

Extraction process follows,

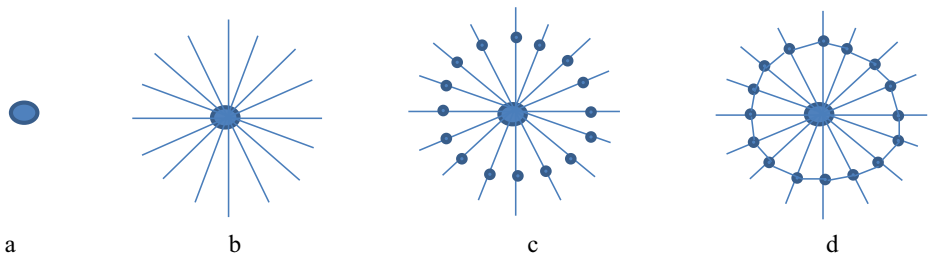


Fig. 3 a Centre point. b Radial line. c Critical points. d ROI contour

Table 1 Rules for intensity difference for selecting ROI in medical images

Rule: 1–3	IF	I_{centre} is Zero I_{centre} is Low I_{centre} is Medium	AND	I_{final} is Low I_{final} is Medium I_{final} is High	THEN	$I_{difference}$ is NS
Rule: 4–6	IF	I_{centre} is Zero I_{centre} is Zero I_{centre} is Low	AND	I_{final} is Medium I_{final} is High I_{final} is High	THEN	$I_{difference}$ is NB
Rule: 7–9	IF	I_{centre} is Low I_{centre} is Medium I_{centre} is High	AND	I_{final} is Zero I_{final} is Low I_{centre} is Medium	THEN	$I_{difference}$ is PS
Rule: 10–12	IF	I_{centre} is Medium I_{centre} is High I_{centre} is High	AND	I_{final} is Zero I_{final} is Zero I_{final} is Low	THEN	$I_{difference}$ is PB

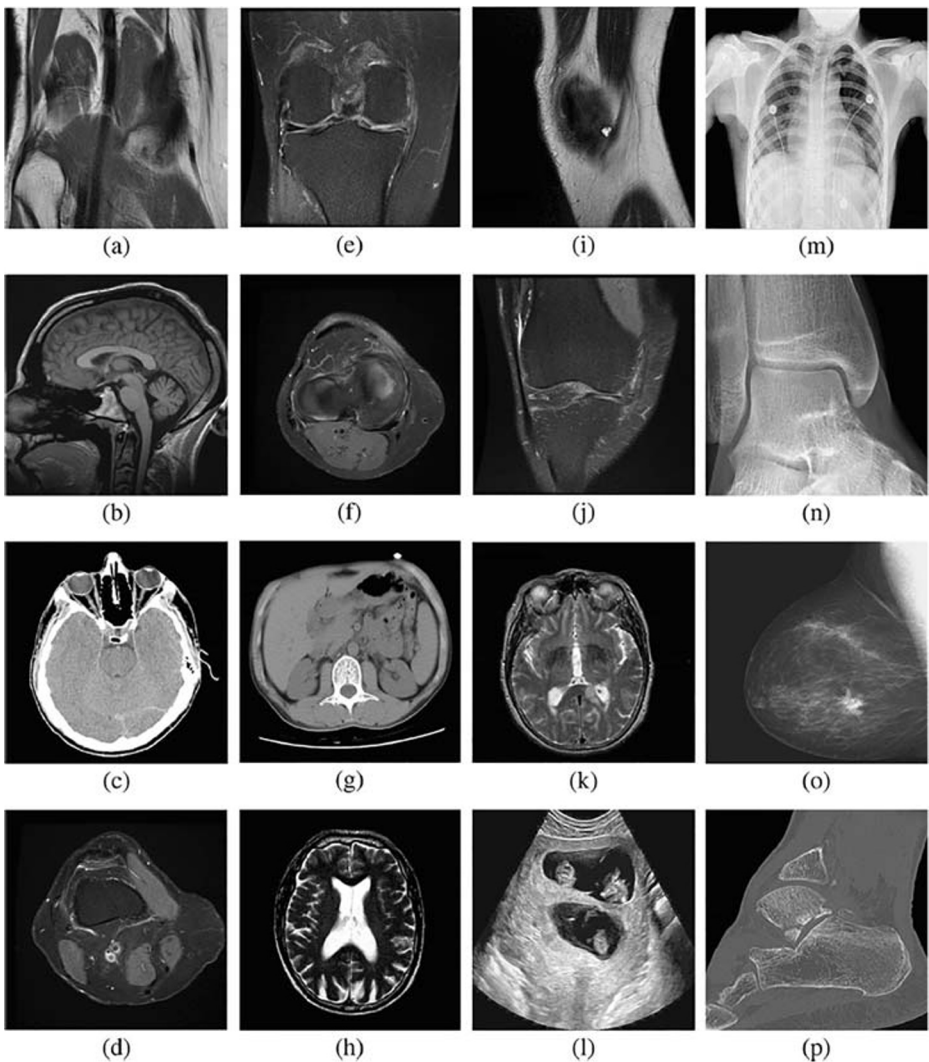


Fig. 4 Different kinds of medical images (CT images, MRI images, US images)

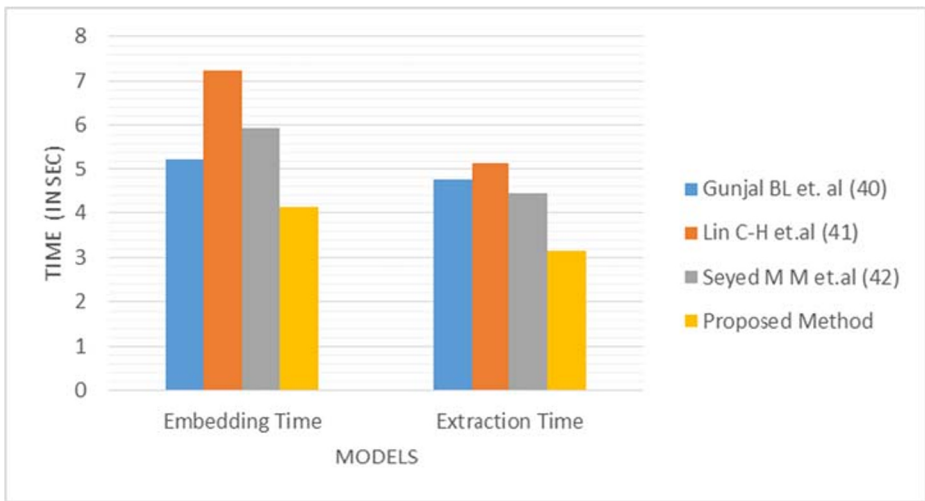


Fig. 5 Comparative analysis of computational efficiency for detecting ROI

1. Read the watermarked image W_i
2. Segment ROI through fuzzy based segmentation method as explained in section 2
3. Apply DWT on the segmented ROI
4. Apply SVD to HH_2 sub-band Encrypted image E_i
5. Calculate Key Component

$$KC_{wi} = U_{Ei} * S_{Ei}$$

6. Modification of singular values using Key Components (KC)

$$S'_i = S_i - \alpha KC_{wi}$$

7. Use same logistic map for decryption as used in encryption and shuffle the sub-bands to obtain original watermark image.

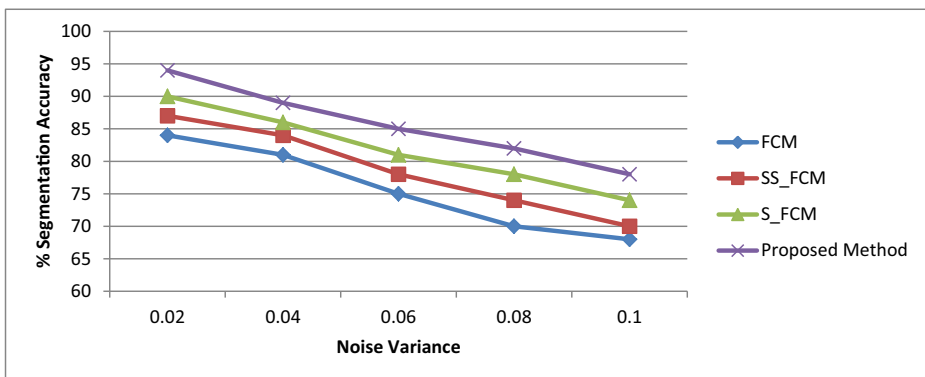


Fig. 6 Average segmentation accuracy vs noise variance(gaussian noise with variance 0.1)

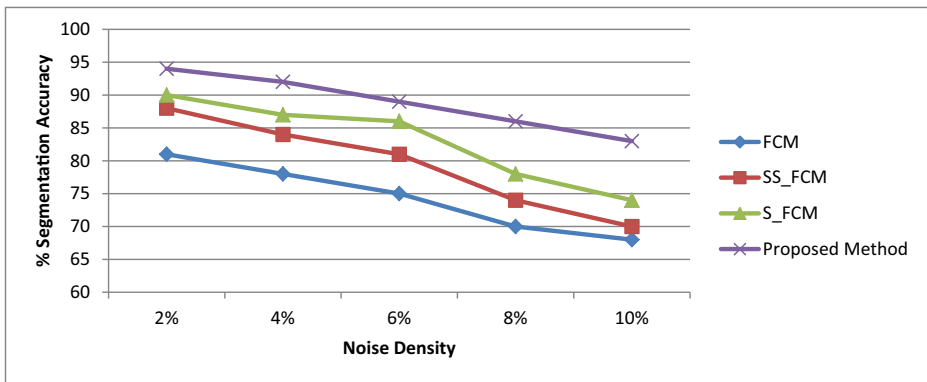


Fig. 7 Average segmentation accuracy vs noise density(10% salt and pepper noise)

5 Experimental results

The proposed system performance is assessed over simulation experiments using MATLAB 2017b with a system configuration of 8 GB RAM and core i7 processor of 2.2 GHz. The proposed system is evaluated with sixteen medical images of size 512 ×512 including CT,MRI, ultrasound (US) and one watermark of size 64 ×64 is used, which are shown in Fig. 4 and Table.5. The metrics used for performance evaluation are capacity, complexity, robustness, reversibility and imperceptibility. The three ROI based watermarking schemes are simulated in MATLAB with unoptimized program code. In order to have a fair comparison, only the ROI extraction phase computational times are calculated without considering the time required for embedding and extraction computation.

The simulation time is averaged for 10 images considering the cameraman image and copyright image as watermark images. It is observed from the bar plot of Fig. 14 that our proposed scheme has lower computation time in ROI extraction of both watermark embedding and extraction stages (Fig. 5).

5.1 Performance analysis for proposed fuzzy ROI selection algorithm

The Gaussian noise at various levels against segmentation accuracy is represented in Fig. 6. It shows that proposed method is stable with various noise levels at increasing rate while FCM and SS_FCM are decreased rapidly. However, while adding salt and pepper noise, the efficiency of S_FCM is decreased which is shown in Fig. 7.

Computational complexity for ROI detection with CPU time for manual detection and automatic detection are analysed. It shows that the computation-intensive multiplications are

Table 2 Comparative analysis of ROI detection methods

Parameters	Gunjal BL et. al [42]	Lin C-H et.al [43]	Seyed M M et.al [44]	Proposed Method
Image type	All	Medical	Medical	Medical
Reversibility	Reversible	Non-Reversible	Non-Reversible	Reversible
Capacity	Low	High	Low	High
Detection type	Manual	Manual	Automatic	Automatic
Computational time	Low	High	High	Low

Table 3 Average results of proposed method tested on the brain image and lung CT scans dataset

Fuzzy Methods	Brain MRI Images		Lung CT Scan	
	<i>pcIndex</i>	<i>peIndex</i>	<i>pcIndex</i>	<i>peIndex</i>
FCM [19]	0.8992	0.0934	0.9003	0.0750
SS_FCM [36]	0.9216	0.0816	0.8807	0.0739
S_FCM [7]	0.9424	0.0458	0.9504	0.0476
SS_FCM_W [13]	0.9097	0.0804	0.8959	0.0729
SS_FCM_LAWS [47]	0.8997	0.0863	0.8940	0.0767
Proposed Method	0.9534	0.0437	0.9608	0.0424

completely eliminated automatic detection cases. The proposed ROI detection method is compared with previous detection methods are shown in Table.2. The soft computing based ROI detection shows better region selection, when compared with previous methods as shown in Fig. 5.

5.1.1 Fuzzy ROI evaluation

Coefficient and entropy index are used for evaluating the fuzzy algorithm performance, which are represented as *pcIndex* and *peIndex*. The measurement of the fuzziness degree is shown in Eqs. 8 and 9,

$$pcIndex = \frac{\sum_{k=1}^n \sum_{i=1}^c U_{ij}^2}{n} \tag{8}$$

$$peIndex = \frac{-\sum_{k=1}^n \sum_{i=1}^c [U_{ij} \log U_{ij}]}{n} \tag{9}$$

One of the direct measurements for evaluating segmentation algorithm is Segmentation accuracy (*SA*) is calculated as shown in Eq. 10,

$$SA = \frac{\#correctly\ classified\ pixels}{total\ \# \ of\ pixels} \tag{10}$$

Datasets were described to test and evaluate the proposed method on various experiments shows that better performance is obtained when it has the maximum *pcIndex* value and segmentation accuracy, but *peIndex* value is minimum. Table 3 represents the results of different algorithms test on brain MRI images and Lung CT scans.

Table 4 Correlation coefficients of the original and cipher-images using various encryption schemes

Encryption methods	Vertical	Horizontal	Diagonal
Our Method	0.5554	0.5496	0.5126
Radwan’s [35]	-0.0038	-0.0124	-0.0090
Rhouma [39]	-0.0256	0.2725	-0.0661
Decom-Crypt[Y.Zhou] [51]	-0.0350	0.0285	-0.0102

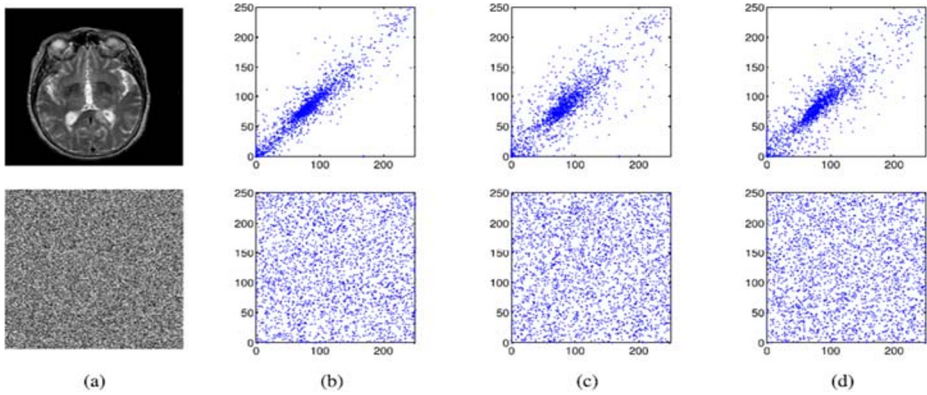


Fig. 8 Correlation between original and cipher image

5.2 Performance analysis for proposed encryption method

Various image sizes as represented in Fig. 4 (g) are considered for evaluating the proposed encryption method performance. Table 4 lists the results of various encryption algorithms with respect to NPCR and UACI. The resultant values shows that UACI is closer to 33% and NPCR value is closer to 99%, which means that proposed algorithm is secured to various kinds of attacks.

5.2.1 Analysing correlation between images

The methods that are used to measure the randomness of an image are correlation analysis, which avoids the loss of information, due to low correlation among the pixels that are adjacent.

Table 5 Comparing proposed scheme NPCR and UACI results with various encryption methods

Image	NPCR				UACI			
	[35]	[39]	[51]	Proposed Encryption Method	[35]	[39]	[51]	Proposed Encryption Method
a	0.9012	0.9127	0.9692	0.9941	0.3012	0.3145	0.2147	0.3354
b	0.9124	0.9241	0.9757	0.9924	0.3004	0.3201	0.2416	0.3368
c	0.9245	0.9258	0.9780	0.9958	0.3102	0.3185	0.2319	0.3314
d	0.9041	0.9127	0.9509	0.9953	0.3018	0.3210	0.2514	0.3391
e	0.9143	0.9327	0.9454	0.9967	0.3057	0.3197	0.2134	0.3318
f	0.9257	0.9512	0.9415	0.9947	0.3081	0.3178	0.2612	0.3354
g	0.9343	0.9432	0.9397	0.9952	0.3051	0.3185	0.2513	0.3316
h	0.9147	0.9511	0.9581	0.9962	0.3068	0.3211	0.2214	0.3352
i	0.9150	0.9323	0.9452	0.9943	0.3082	0.3179	0.2261	0.3324
j	0.9314	0.9531	0.9348	0.9942	0.3058	0.3245	0.2315	0.3318
k	0.9417	0.9514	0.9512	0.9913	0.3067	0.3199	0.2241	0.3327
l	0.9143	0.9127	0.9153	0.9954	0.3059	0.3177	0.2354	0.3338
m	0.9257	0.9327	0.9257	0.9968	0.3073	0.3183	0.2613	0.3375
n	0.9345	0.9512	0.9314	0.9925	0.3063	0.3213	0.2413	0.3358
o	0.9146	0.9432	0.9328	0.9923	0.3025	0.3175	0.2146	0.3364
p	0.9154	0.9511	0.9412	0.9912	0.3077	0.3255	0.2365	0.3359

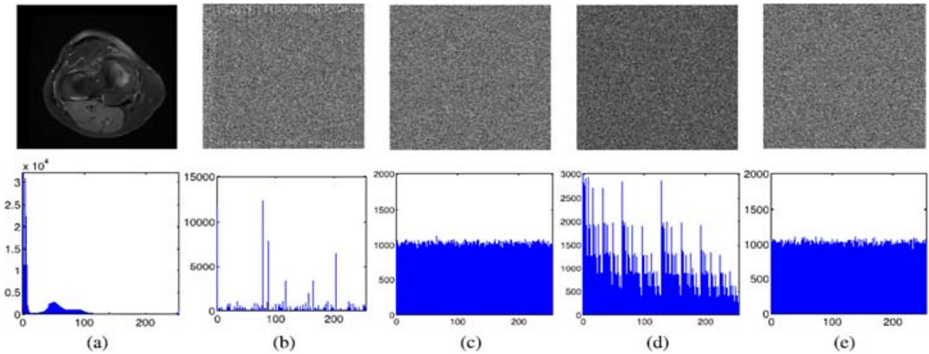


Fig. 9 Histogram analysis of different methods

Calculation of the two data sequences for analysing the correlation coefficient is represented in Eq. 11,

$$CORR(P, Q) = \frac{E \left[\left(p - \mu_p \right) \left(q - \mu_q \right) \right]}{\sigma_p \sigma_q} \tag{11}$$

where p is a sequence of adjacent pixels and q is the neighbouring pixels that corresponds to any one of the diagonal, horizontal and vertical directions. μ_p and μ_q represents the p and q mean values respectively. The standard deviations of p and q are represented as σ_p and σ_q . Fig. 8 shows the correlation among original and cipher images where the coefficients are in the range of $[0, 1]$ as shown in Table 4.

The methods that are used to measure the change in the pixel values are Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). They are represented as shown in Eqs. 12 and 13,

$$NPCR = \frac{\sum_{m=1}^M \sum_{n=1}^N D(m, n)}{MN} \times 100 \tag{12}$$

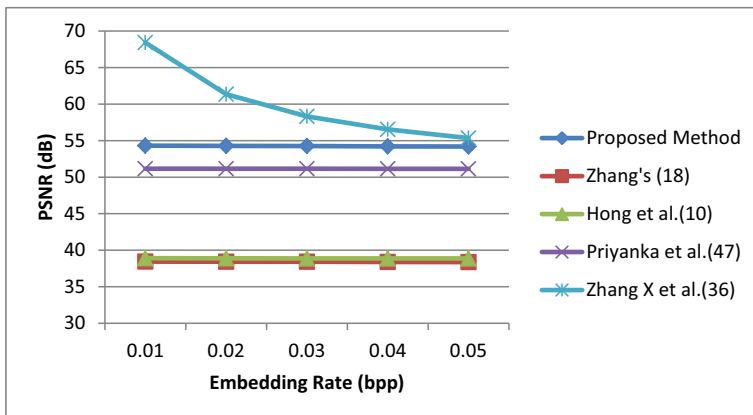


Fig. 10 Performance comparisons of various methods under varying embedding rates of various medical images

Table 6 Performance comparison of proposed scheme based on embedding rate

Fuzzy ROI	Embedding Rate		PSNR	
	Proposed	[26]	Proposed	[26]
1%	0.010	0.0019	54.32	68.43
5%	0.060	0.0097	54.27	61.35
10%	0.10	0.020	54.26	58.31
15%	1.08	0.029	54.21	56.54
20%	1.25	0.039	54.19	55.34

$$UACI = \frac{1}{MN} \left[\sum_{m,n}^{M,N} \frac{|C_1(m,n) - C_2(m,n)|}{G-1} \right] \times 100 \tag{13}$$

where C_1 and C_2 are two encrypted images having minor changes with respect to original images. The image width and height are represented as m, n and function $D(m, n)$ is the number of variations that exists between C_1 and C_2 . The experimental result of proposed method is compared with various schemes are shown in Table 5.

5.2.2 Histogram analysis

To evaluate the proposed system for histogram analysis, we compared it with the methods of Rhouma, Radwan, and Decom-Crypt and the results are shown in Fig. 9.

Table 7 PSNR comparison of various methods



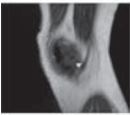

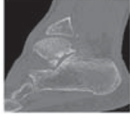



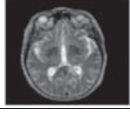

Host Image	Watermark	Proposed Method					
		[5]	[6]	[8]	[9]	Encryption + watermarking	Fuzzy ROI + Encryption + Watermarking
		45.271	44.843	48.327	49.029	49.243	49.419
		46.521	41.381	44.367	48.543	49.021	49.357
		45.287	43.623	46.529	49.627	49.351	49.513
		43.270	41.823	45.419	48.721	49.217	49.309
		44.827	40.287	46.524	47.571	49.097	49.201

Table 8 Comparing robustness in terms of average NC

Attack Type	Attack Degree		M.K. Kundu et al.	O.M.A. Wershi et al.	Y.L. Liu et al.	R. Keshavarzian et al.	Proposed Method	
							Without Fuzzy ROI	With Fuzzy ROI
Gaussian LPF	Window size	3 × 3	0.981	0.985	0.987	0.992	0.991	0.997
	Window size	4 × 4	0.847	0.812	0.894	0.912	0.901	0.954
Sharpening	Window size	3 × 3	0.975	0.947	0.981	0.987	0.972	0.989
	Variance	0.001	0.832	0.744	0.796	0.815	0.794	0.851
Salt & pepper	Density	0.1	0.941	0.843	0.914	0.901	0.891	0.924
	Histogram Equalization		0.981	0.968	0.971	0.946	0.937	0.956

Fig. 9 (b) represents the Rhouma's method, which is having non-uniform distribution of histogram, which is similar to Decom-Crypt in Fig. 9 (d). However, our proposed method shown in Fig. 9 (e) shows equal distribution of histogram as similar to Radwan's scheme in Fig. 9 (c). This result shows that proposed scheme is having better or equal performance than other methods.

5.3 Performance analysis for proposed watermarking

Peak Signal to Noise ratio (PSNR) and Normalized Cross Correlation (NCC) are the two basic parameters that are used to measure the watermarking strength in the watermarked image. The proposed method achieves better results than other existing watermarking algorithms, which is shown in Fig. 10. The algorithms proposed in [26] are having low watermarking strength when compared to the proposed scheme, which is represented in Table.6. PSNR comparison for different schemes is detailed in Table 7. Features taken into consideration for comparing various schemes are represented in Table 8.

To estimate the quality of the image, PSNR is calculated as shown in Eq. 14,

$$PSNR = 10 \log_{10} \left(\frac{255^2}{\left(\frac{1}{m} \right) \sum_{i=1}^m H_i - H'_i} \right) \quad (14)$$

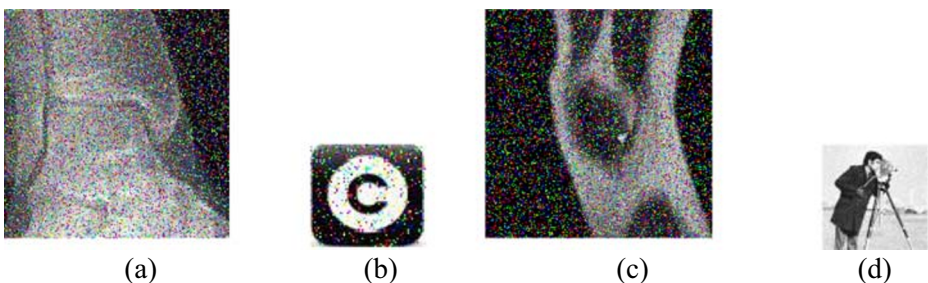


Fig. 11 a and c 0.2 density salt & pepper noise watermarked medical images b and d extracted watermarks from various medical images of salt & pepper attack

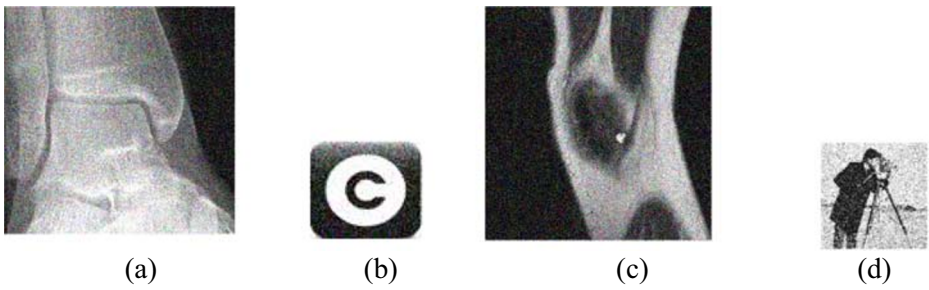


Fig. 12 a and c 0.1 density gaussian noise watermarked image b and d extracted watermarks from various medical images undergone gaussian attack

NCC is used to calculate the correlation coefficient between the original and extracted watermark. It is represented in Eq. 15

$$NCC = \frac{\sum_{k=1}^{w_p \times w_q} w_k w'_k}{\sqrt{\sum_{k=1}^{w_p \times w_q} w_k^2 \sum_{k=1}^{w_p \times w_q} w_k'^2}} \tag{15}$$

Where w_k and w'_k are the original and the extracted watermarks respectively. NC comparison for various methods is represented in Table 8.

5.3.1 Analyzing robustness of watermark

To analyze the proposed method on basis of robustness on geometric and non-geometric attacks, experiments are conducted on watermarked image, where noise affects a portion of the image or the whole image. Experiments are conducted by introducing these noises at different amounts and area. Experiments are also conducted by replacing part of watermarked image by one or more icons. Different amount of noise is introduced on each image. The effect on the embedded watermark is studied by extracting the watermark from the noise affected image. Here the Copyright logo and cameraman image are shown as watermark image with Gaussian, Speckle, Salt & Pepper and Sharpening attacks. Fig. 11 shows the salt & pepper attack on watermark with density 0.2 and their NC = 0.924 for copyright logo and NC = 0.931 for cameraman image which shows the better robustness.

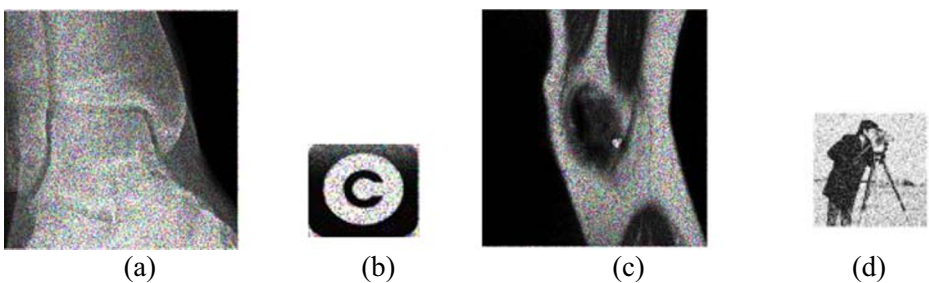


Fig. 13 a and c 0.1 density speckle noise watermarked image b and d extracted watermarks from various medical images undergone speckle attack

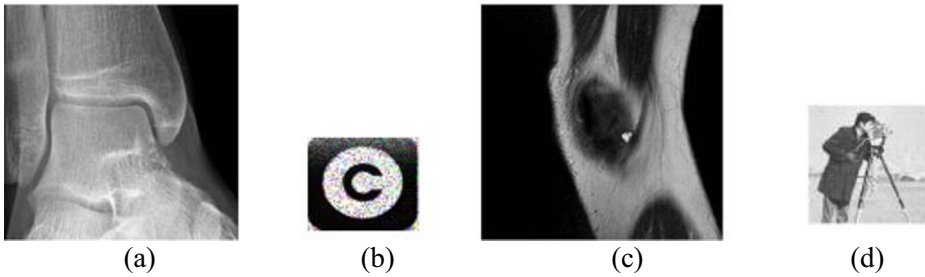


Fig. 14 a and c watermarked medical images undergone sharpening attack, b and d extracted watermarks

As shown in Fig. 12, Gaussian noise attack with variance 0.1 results in better NC. Similarly in Fig. 13 with speckle noise with variance 0.1 and Fig. 14 with sharpening attack also shows the better performance of the proposed algorithm.

6 Conclusion

Our proposed algorithm combines the watermark and encryption for better medical image security, which are processed for diagnosis. The experimental results demonstrate that the proposed method better authentication to the system with high integrity to the medical images and good confidentiality to the watermarked information which possess high efficiency when proposed scheme is compared with other algorithms on varying digital images such as: nuclear medicine, ultrasound, MRI, computed radiography (CR), computed tomography (CT). PSNR value for proposed method is about 49.5 mean that proposed method does not affect the image quality and in the same time securing watermark information. Proposed algorithm shows that high embedding rate is achieved with low distortion. This indicates that the quality of the watermarked image is high and provides good payload. Experimental images for proposed algorithm are grey scale images that can be extended to color images in future.

References

1. Ahmed MN, Yamany SM, Mohamed N, Farag AA, Moriarty T (2012) A modified fuzzy C-means algorithm for Bias field estimation and segmentation of MRI data. *IEEE Trans Med Imaging* 21:193–199
2. A Al-Haj and A. Amer (2014) Secured telemedicine using region-based watermarking with tamper localization, *J Digit Imaging*, 27(6):pp.737–750
3. Balasamy K, et al (2019). An intelligent reversible watermarking system for authenticating medical images using wavelet and PSO, *Cluster Computing*, Springer, pp. 4431–4442
4. Bensaid AM, Hall LO, Bezdek JC, Clarke LP (2006) Partially supervised clustering for image segmentation. *Pattern Recogn* 29:859–871
5. Bouslimi D, Coatrieux G, Roux C (2012) A joint encryption/watermarking algorithm for verifying the reliability of medical images: application to echographic images. *Comput Methods Prog Biomed* 106(1): 47–54
6. Campisi P, Kundur D, Neri A (2004) Robust digital watermarking in the ridgelet domain, *IEEE signal process. Lett.* 11(10):826–830
7. Cao F, Huang HK, Zhou XQ (2003) Medical image security in a HIPAA mandated PACS environment. *Comput Med Imaging Graph* 27:185–196
8. Cedillo-Hernandez M, Cedillo-Hernandez A, Nakano-Miyatake M, Perez-Meana H (2019) An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD. *Futur Gener Comput Syst* 101:1223–1246

9. S Das, MK Kundu (2011). Hybrid contourlet-DCT based robust image watermarking technique applied to medical data management, in: Proceedings of 4th International Conference on Pattern Recognition and Machine Intelligence, pp. 286–292
10. Eswaraiyah R, Reddy ES (2014). Medical image watermarking technique for accurate tamper detection in ROI and exact recovery of ROI. *Int J Telemed Appl* ,1–10
11. Favorskaya M, Savchina E, Gusev K (2019) Feature-based synchronization correction for multilevel watermarking of medical images. *Procedia Computer Science* 159:1267–1276
12. Gangadhar Y, Giridhar Akula VS, Chenna Reddy P (2018) An evolutionary programming approach for securing medical images using watermarking scheme in invariant discrete wavelet transformation. *Biomedical Signal Processing and Control* 43:31–40
13. Ganic E, Eskicioglu AM (2005) Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition. *J Electron Imaging* 14(4):043004–043004
14. Gao G, Wan X, Yao S, Cui Z, Zhou C, Sun X (2017) Reversible data hiding with contrast enhancement and tamper localization for medical images. *Inf Sci* 385:250–265
15. Giakoumaki A, Pavlopoulos S, Koutsouris D (2006) Multiple image watermarking applied to health information management. *IEEE Trans Inf Technol Biomed* 10(4):722–732
16. Gunjal BL, Mali SN (2012). ROI based embedded watermarking of medical images for secured communication in telemedicine. *Int J Comput Commun Eng*: 293–298
17. Guo X, Zhuang T (2009) A region-based lossless watermarking scheme for enhancing security of medical data. *J Digit Imaging* 22(1):53–64
18. Guo X, Zhuang T (2009) Lossless watermarking for verifying the integrity of medical images with tamper localization. *J Digit Imaging* 22(6):620–628
19. Hong W, Chen TS, Wu HY (2012) An improved reversible data hiding in encrypted images using side match. *IEEE Signal Process Lett* 19(4):199–202. <https://doi.org/10.1109/LSP.2012.2187334>
20. Ji Z, Xia Y, Sun Q, Cao G, Chen Q (2015) Active contours driven by local likelihood image fitting energy for image segmentation. *Inf Sci* 301:285–304
21. Jung H, Sung K, Nayak KS, Kim EY, Ye JC (2009) K-t focuss: a general compressed sensing framework for high resolution dynamic MRI. *Magn Reson Med* 61:103–116
22. Keshavarzian R, Aghagolzadeh A (2016) ROI based robust and secure image watermarking using DWT and Arnold map. *Int.J.Electron.Communic.(AEU)* 70:278–288
23. Balasamy Krishnasamy, Balakrishnan M, Christopher A (2021). A Genetic Algorithm Based Medical Image Watermarking for Improving Robustness and Fidelity in Wavelet Domain. *Intelligent Data Engineering and Analytics. Advances in Intelligent Systems and Computing*, vol 1177. Springer, Singapore. https://doi.org/10.1007/978-981-15-5679-1_27
24. MK Kundu, S Das (2010). Lossless ROI medical image watermarking technique with enhanced security and high payload embedding, in: Proc. of 2010 Int. Conf. on Pattern Recognition, IEEE Computer Society, pp. 1457–1460
25. Lavanya A, Natarajan V (2012) Watermarking patient data in encrypted medical images. *Sadhana-Acad Proc Eng Sci* 37(6):723–729
26. Li C, Lo K-T (2011) Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. *Signal Process* 91:949–954
27. Lin C-H, Yang C-Y, Chang C-W (2010) Authentication and protection for medical image. Berlin: Springer-Verlag 6422:278–287
28. X. Liu, J. Lou, H. Fang, H. Fang, L. Wang (2019) A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images, *IEEE Access*, vol. 7, pp. 76580–76598
29. Liu YL, Qu XX, Xin GJ (2015) ROI-based reversible data hiding scheme for medical images with tamper detection. *IEICE Trans Inf Syst E98-D(4)*:769–774
30. Mothi R, Karthikeyan M (2019) Protection of bio medical iris image using watermarking and cryptography with WPT. *Measurement* 136:67–73
31. Seyed Mojtaba Mousavi & Alireza Naghsh & SAR Abu-Bakar (2015). A Heuristic Automatic and Robust ROI Detection Method for Medical Image Watermarking, *J Digit Imaging*, <https://doi.org/10.1007/s10278-015-9770-z>
32. Nambakhsh MS, Ahmadian A, Zaidi H (2011) A contextual based double watermarking of PET images by patient ID and ECG signal. *Comput Methods Prog Biomed* 104(3):418–425
33. Pan W, Bouslimi D, Karasad M, Cozic M, Coatrieux G (2018) Imperceptible reversible watermarking of radiographic images based on quantum noise masking. *Comput Methods Prog Biomed* 160:119–128
34. Qasim AF, Meziane F, Aspin R (2018) Digital watermarking: applicability for developing trust in medical imaging workflows state of the art review. *Computer Science Review* 27:45–60
35. Radwan AG, AbdElHaleem SH, Abd-El-Hafiz SK (2016) Symmetric encryption algorithms using chaotic and non-chaotic generators: a review. *J Adv res (JAR)* 7(2):193–208

36. Ramakrishnan S, Gopalakrishnan T, Balasamy K (2011) SVD based robust digital watermarking for still images using wavelet transform, CCSEA 2011. CS IT 02:155–167
37. Rastegar S, Namazi F, Yaghmaie K, Aliabadian A (2011) Hybrid watermarking algorithm based on singular value decomposition and radon transform, AEU-Int. J Electron Commun 65(7):658–663
38. E Rayachoti, S Tirumalasetty, SC Prathipat (2020). SLT based watermarking system for secure telemedicine, Clust Comput. <https://doi.org/10.1007/s10586-020-03078-2>
39. Rhouma R, Solak E, Belghith S (2010) Cryptanalysis of a new substitution-diffusion based image cipher. Commun Nonlinear Sci Numer Simul 15(7):1887–1892
40. Singh P, Raman B (2017) Reversible data hiding for rightful ownership assertion of images in encrypted domain over cloud. Int J Electron Commun (AEU) 76:18–35
41. Tan CK, Ng JC, Xu XT et al (2011) Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability. J Digit Imaging 24(3):528–540
42. Tsougenis ED, Papakostas GA, Koulouriotis DE, Tourassis VD (2012) Performance evaluation of moment-based watermarking methods: a review. J Syst Softw 85(8):1864–1884
43. Wershi OMA, Khoo BE (2011) Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images. J Digit Imaging 24(1):114–125
44. Wu JHK, Chang RF, Chen CJ, Wang CL, Kuo TH, Moon WK, Chen DR (2008) Tamper detection and recovery for medical images using near-lossless information hiding technique. J Digit Imaging 21(1):59–76
45. Wu H, Huang J, Shi Y (2015) A reversible data hiding method with contrast enhancement for medical images. J Vis Commun Image Represent 31:146–153
46. Yang Y, Zhang W, Liang D, Yu N (2018) A ROI-based high capacity reversible data hiding scheme with contrast enhancement for medical images. Multimed Tools Appl 77:18043–18065
47. JM Zain, LP Baldwin, M Clarke (2004). Reversible watermarking for authentication of DICOM images, in: Proceedings of the 26th Annual International Conference on IEEE EMBS, September, pp. 3237–3240
48. JM Zain, AM Fauzi (2006). Medical image watermarking with tamper detection and recovery, in: Proceedings of the 28th IEEE EMBS Annual Intern. Conference, pp. 3270–3273
49. Zhang X (2011) Reversible data hiding in encrypted image. IEEE Signal Process Lett 18(4):255–258
50. Zhang X, Wang Z, Yu J, Qian Z. (2015). Reversible visible watermark embedded in encrypted domain. p. 826–30. <https://doi.org/10.1109/ChinaSIP.2015.7230520>
51. Zhou Y, Panetta K, Aгаian S, Chen CLP (2013) (n, k, p)-gray code for image systems, IEEE trans. Cybern. 43:515–529

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