

# Slantlet based hybrid watermarking technique for medical images

Roopam Bamal<sup>1</sup>  · Singara Singh Kasana<sup>1</sup>

Received: 9 December 2016 / Revised: 10 April 2017 / Accepted: 1 June 2017 /  
Published online: 13 July 2017  
© Springer Science+Business Media, LLC 2017

**Abstract** Watermarking techniques are widely used for copyright protection, confidentiality and integrity issues in medical field. Reversibility, robustness, embedding capacity and invisibility are the essential requirements of a watermarking technique. Cogitating the need of security for medical images, this paper proposes a reversible high embedding capacity, high image fidelity, a hybrid robust lossless data hiding technique by using both transform and spatial domains. Proposed technique alters the mean of the selected non-overlapping slantlet transformed blocks of the host image whereas RS vector considers flipping factor for data embedding. The optimum thresholds to select the blocks are calculated through *PSO* technique and watermark is generated by using patient details, biometric id and region of interest (ROI) blocks of host image. This watermark is further compressed by applying *LZW* technique and encrypted by *AES* as well as *MD5*. The watermark bits are embedded in all three *RGB* channels of a cover image, to increase the embedding capacity up to 3.3675 *bpp*. The credibility of the proposed technique in comparison with other medical watermarking techniques is evidenced through experimental results.

**Keywords** Watermarking · Slantlet · RS vector · SIM · PSNR · BPP · IER

## 1 Introduction

Today's corporate world requires digital data transmission through the Internet, in multiple wide manifestations, using blogs, mails and social media. This digital data can be in the form of audio, image, file, document, video etc. As digital data travel through the Internet,

---

✉ Roopam Bamal  
roopambamal@gmail.com

Singara Singh Kasana  
singara@thapar.edu

<sup>1</sup> Computer Science and Engineering Department, Thapar University, Patiala, Punjab 147004, India

it can encounter many hurdles like corruption of data, integrity hampering of data, losing confidentiality of data, intruder's encounter etc. So, protecting as well as controlling sensitive data and its confidentiality has become extremely important. Corporate professionals are facing tampering problems with digital data. The case is similar with medical images, which are the visual representation of the inner body for clinical purposes. Corruption of information stored in medical image can affect the life of a person. Thus, there is a need of a highly secure, robust and reliable technique that can appropriately prevent falsification of clinically useful data from corruption. Electronic Medical Information System (MIS) and Hospital Information System (HIS) are used to manage the healthcare organizations, whereas medical images are exchanged through a computer network or the Internet. The medical images are considered as the most important entities in the healthcare diagnostic procedures. These medical images have variety of usage ranging from viewing features of patients such as anatomical cross sections of internal organs and tissues. Physicians use medical images to evaluate patient diagnosis, these medical images are used to monitor the effects of the treatment and for disease researches. Therefore, protecting medical images from unauthorized access is an essential requirement of this field.

There are many significant techniques for the security of digital data like steganography and watermarking. Steganography means covered writing i.e. concealment of secret data within another data whereas watermarking is the technique for hiding information in the carrier data for the confidentiality, security, copyright and ownership issues. This unique digital information is always imperceptible to humans but can sometimes be detected by computers, web networks and other various digital devices like printers, scanners etc. So, highly trustful watermarking technique should be in existence which is resistible against such attacks. In case of medical image, a watermark is a part of patient's information such as patient *ID* or would be better to include his/her unique biometric identity with the image hash value that can be embedded inside the medical image without corrupting the image. Original image along with the watermark should be retrieved at the receiver's side.

This paper proposes a reversible robust hybrid watermarking technique for medical image to support *MIS* and *HIS*. This technique provides source and patient's authentication services, medical image integrity services and patient information confidentiality services with high efficiency. It is reversible because the original medical image as well as watermark can be retrieved at receiver's side without any distortion. Proposed technique focuses on watermark security, robustness, invisibility and embedding capacity at the same time.

The paper is organized as: Section 2 reviews existing watermarking techniques applicable to medical image watermarking and in Section 3, the proposed medical image authentication technique is described and in Section 4, the experimental results are illustrated. Finally in Section 5, the proposed work is concluded.

## 2 Literature review

Anand et al. [5] proposed an efficient watermarking technique in spatial domain of medical image for hiding the watermark by swapping its bits with the grey level pixels of watermark. The privacy of patient's information was protected because of the encryption of the watermarked information and the diagnostic value of the medical images after watermarking is not lessened in any way, with no change in the system configuration or software, the methodology could be employed to other types of patient data such as Electroencephalogram (EEG), Phonocardiogram (PCG) etc. Maximum Normalized Root Mean Square Error (MNR MSE) is used as evaluating parameter which valued as 0.0042% for Computed

Tomography (CT) scan and 0.0052% for ultrasound image. Coatrieux et al. [7] described the relevance of watermarking in medical images by presenting different scenarios, one devoted to the authentication and other to the integrity while doing trace of the images with control of the patient's records. Milanova et al. [16] proposed three watermarking techniques. The first technique embeds *ROI* with the digital signature of the image and the image can be reverted back to its original value. This technique is known as Strict Authentication Watermarking (SAW). The second technique which is known as Strict Authentication Watermarking with Joint Photographic Experts Group Compression (JPEG) also uses the same principal as the first technique however, it is able to survive some degree of *JPEG* compression. The third technique is known as Authentication Watermarking with Tamper Detection and Recovery (AW-TDR) which can localise tampering. At the same time it can reconstruct the original image. Zain and Clarke [42] proposed method that increases security of telemedicine by looking at the attacks against security. In doing so, it looks through the function of the computer system, as a portal of information. The issues that are raised in these watermarked medical images are reversible watermarking Vs. permanent/irreversible watermarking, content authentication Vs. complete authentication and the practical issue of compression. Coatrieux et al. [8] designed a watermarking technique in which different identifiers like Digital Imaging and Communications in Medicine (DICOM) standard, unique patient identifier or Anonymous European Patient Identifier are combined in order to improve medical image protection in terms of maintainability and authenticity. Manasrah and Haj [15] proposed a wavelet-based image multi-watermarking technique to implement issues like image source authentication, image annotation and image retrieval. A unique watermarking method for tamper detection for *ROI* with the complete recovery of *ROI* was given by Eswaraiyah and Sreenivasa [10]. This is a fragile block based medical image watermarking technique. This technique is used to avoid embedding distortion inside *ROI*, the tampered blocks inside *ROI* are accurately detected with integrity verification and lossless original *ROI* pixels. *ROI* pixels, border pixels and region of noninterest (RONI) pixels are the three sets of pixels in which medical image are segmented. Border pixels are then, embedded with authentication data, information of *ROI* and *RONI*. Mohananthini and Yamuna [18] introduced an algorithm by using Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) for watermarking process. Red Green Blue (RGB) components of original images are decomposed by using *SVD* on two level *LL* subband. Watermark used contains Patient's identification number, Patient name, Patient age, Patient sex, Patients diagnosis information, Patient treatment information and Doctor's signature. This algorithm produces better results with salt and pepper noise, robustness, Gaussian noise, Gaussian blur, median filtering, *JPEG* compression with quality of 50, rotation, smoothening, sharpening, intensity transformation and row column blanking. Priya and Sadasivam [23] proposed a lossless reversible watermarking scheme in which watermark is embedded using a reversible Least Significant Bit (LSB) embedding scheme. This scheme combines hashing, compression, and digital signature techniques to create a content dependent watermark making use of compressed *ROI* for recovery of *ROI*. Kishore et al. [13] proposed an efficient watermarking technique in medical images. The medical images for this algorithm are used in the similar manner as an envelope image in the watermarking procedure, which remains visible to everyone on the network with patient images in wavelet domain. *BAT* algorithm is used optimally to perform the embedding process which results high Peak Signal to Noise Ratio (PSNR) and normalized cross correlation coefficient (NCC) values. Umamageswari and Suresh [34] introduced a mechanism for medical images based on open network security. The contents of altered medical image can be recovered with this technique based on lossless watermarking with help of Digital Signature (DS).

Additive hash functions are used so that if  $DS$  is lost through the network than the watermarked image is used for extracting  $DS$  in another format. Hence the  $ROI$  region for all types of medical images like US (Ultrasonic), Angiographic images, Magnetic Resonance Imaging (MRI), Endoscopic, and  $CT$  are covered. Shaji and Prakash [27] gave a unique way of securing medical images using Chaos Game Representation (CGR). This technique provides image integrity service as the  $CGR$  involves treating an image as an abstract string of numbers.  $CGR$  algorithm has been used as a substitution of hashing algorithm. The generated  $CGR$  watermarked into the medical image using  $DWT$  algorithm. Since  $DWT$  is a reversible method, the original medical image can be retrieved at the receiver side without any distortion. Balasamy et al. [6] generated a multiple watermarking technique which created watermarks by fusing more than one images by arithmetic blend extension method. This method is not vulnerable against different types of geometric attacks. Khor et al. [12] proposed a watermarking technique in multiframe for medical images and for saving processing time, multicores technology is used. The experimental results show that elapsed time is much less on parallel than in sequential watermarking processing along with imperceptibility and robustness. Dong et al. [9] developed a feasible and novel watermarking algorithm in the encrypted domain by using Discrete Cosine Transform (DCT) and logistic chaotic map. Zero watermarking technique is used for ensuring the authenticity and integrity of medical image. Experimental results show the improved results in comparison with non-encrypted image watermarking in terms of robustness and various attacks. Sharma et al. [28] proposed a watermark embedding technique using wavelet transform. First level  $DWT$  is used for the transforming the cover and watermark images to frequency domain.  $LL$  subband is selected from watermark image and format it using modulus functions. The watermarked image is encrypted by using the stream cipher cryptographic techniques in order to achieved two level of security which may provide a potential solution to existing telemedicine security problem of patient's identity theft.

Watermarking in medical images is much curtailed because of its data tampering problem as the data shown in medical image is highly important for the patient. Watermarking techniques for medical have flaws like some techniques lack in watermark embedding capacity, resistance towards network attacks, watermark recovery, low Bit Error Rate (BER), application on color images, protection of  $ROI$ , recovery of corrupted watermark and high degree of invisibility. So, there is a requirement of a technique which can provide high embedding capacity, high security, high robustness against attacks, fully reversible, without lowering the PSNR value.

As discussed above, all watermarking techniques are efficient while considering one or other parameters like limited robustness, low visual quality, limited capacity and incomplete reversibility but lacks in improving all the parameters parallelly. The proposed technique improves simultaneously the following required parameter for watermarking.

- i. Slantlet Transform (SLT) is used for data embedding, as it increases the percentage of the energy of image/signal after compression which enhances the embedding capacity.
- ii.  $SLT$  proves to be better than other transformations like  $DWT$ ,  $DCT$  etc. in removing noise form signals and provides better performance in signal compression, which further improves  $BER$ .
- iii.  $SLT$  can be used to extract the features of the image in order to be used in region classification.
- iv. RS vector is also used for embedding which increases the capacity and security because of hybrid embedding approach.

- v. Robustness is high, due to usage of *SLT* as it uses three filters in its implementation.
- vi. Execution time of the proposed technique is much lower.
- vii. Visual quality of watermarked images is improved significantly along with smoothness.
- viii. Security issues are extensively resolved by the usage of techniques like *MD5*, Advanced Encryption Standards (AES) and biometric thumb print of the patient.
- ix. Tamper detection and localization are also provided by the proposed technique.
- x. Experimental results prove that the factors like correlation, Similarity Index (SIM), Signal-to-Noise Ratio (SNR), *PSNR*, Bit Per Pixel (BPP) and time complexity are better in comparison with the results of existing techniques.

### 3 Proposed watermarking technique

In this section, review of *SLT*, watermark creation algorithm, embedding algorithm, extraction algorithm, overflow and underflow handling process are discussed.

#### 3.1 Review of Slantlet transform

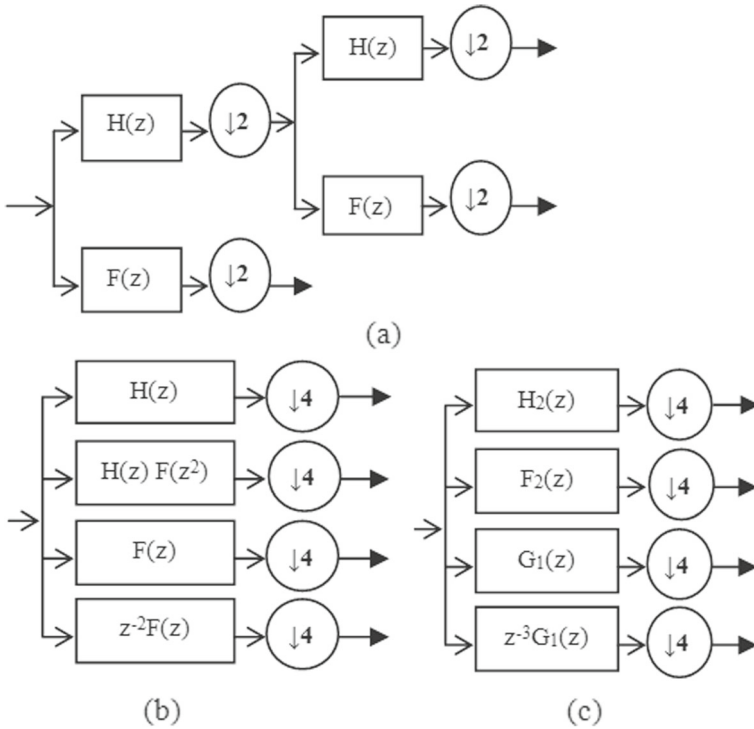
*DWT* has been applied in different applications because of its effective description to the piecewise smooth signals. The performance of the *DWT* can be improved by developing two criterias, which are the time-localization and the smoothness characteristics [25]. To obtain a good trade-off between these two criterias, Selesnick [25, 26], introduced an equivalent form of the *DWT* called *SLT*. This transform provides good time-localization and better smoothness properties by controlling the lengths of the discrete-time basis functions and their moments. *SLT* depends on the equivalent form of the filter bank representation of the *DWT* to give a solution for the filter coefficients, Fig. 1 shows the 2-scale filter banks. *SLT* filter bank is implemented using a parallel structure and different filters have been used instead of filters product. Since the filters that have been used in the *SLT* filter bank are not products, the length of these filters is shorter than the filters of the length *DWT*. The aim of implementing the *SLT* matrix [26] was to prove the orthogonality of this transform. In this paper, depending on the method of image transformation that was explained by Mulcahy [20], the matrix is used to calculate the *SLT* of the image blocks instead of using the conventional *SLT*.

$$S = SLT_N s SLT_N^T \quad (1)$$

Where  $S$  is the *SLT* of the original signal, and  $SLT_N$  is an  $N \times N$  Slantlet matrix. Note that  $s$ ,  $S$ , and  $SLT_N$  have the same size. The *SLT* coefficients in matrix ( $S$ ) are divided into 4-subbands (*LL*, *HL*, *LH*, and *HH*) as shown in Fig. 2. This approach is used to obtain the *SLT* coefficients for each image block. The inverse *SLT* transform (ISLT) can be obtained by:

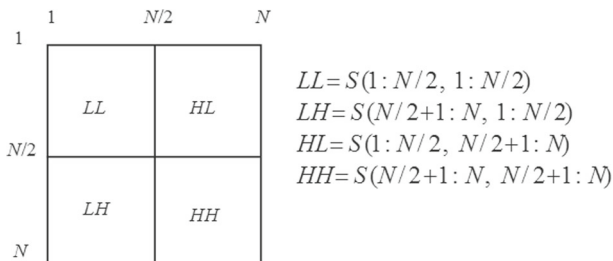
$$s = SLT_N^T S SLT_N \quad (2)$$

The *SLT* has been used in different applications and the performance of the *SLT* schemes is found better than the previous methods in each specific application. For instance, in [25, 26] the *SLT* has been used instead of the *DWT* to remove the noise from the signal and it has been proven that the *SLT* performs better than the *DWT*. In [22] the *SLT* obtained better performance in signal compression as compared to the *DCT* and *DWT* methods. It has been observed that the *SLT* based algorithm can keep higher percentage of the image/signal energy after compression compared to the *DWT* approach. In [21] the *SLT* has been applied in steganography scheme and it was better than the *DWT* in terms of the stego-image visual



**Fig. 1** Decomposition structures for: (a) DWT, (b) equivalent structure of DWT, and (c) SLT

quality and the execution time of the algorithm. In [1, 2] the *SLT* has been used to extract the features of the signals in order to be used in signal classification systems and the results proved that the *SLT* based schemes are better than the *DWT* based schemes. *SLT* has been applied in image watermarking schemes and its performance was better than the *DWT* based schemes in terms of [17] visual quality and robustness [14, 17]. Previous work [17] illustrates a preliminary study of the *SLT* in which a robust irreversible image watermarking has been presented. The reversible watermarking methods in the transform domain are based on the integer wavelet transform [4, 19, 38–41, 45]. The use of *SLT* to implement a robust reversible watermarking scheme in [31], proves the possibility of implementing a reversible data hiding method based on non-integer transform. The algorithm in [31] divides the image



**Fig. 2** Decomposition of the *SLT* coefficients into 4-subbands

into non-overlapping blocks and transform the blocks using *SLT* matrix, then one high frequency subband (either *HL* or *LH*) is chosen to carry the watermark bits. The algorithm scans all the blocks to find the maximum mean value of the carrier subband in order to set the threshold value. Using this threshold value, a pre-processing step has been applied to prepare the original image blocks before applying the watermark embedding process. Thereafter, the prepared blocks are transformed using *SLT* matrix and if the watermark bit is '1', the mean value of the carrier subband is shifted by the same shift value that has been used in the pre-processing step. At the receiver side, the mean value of the carrier subband is compared with the threshold value to extract the watermark bits. The scheme in [31] performs better in comparison with the previous methods, however, the capacity and the visual quality still needs more improvement. The use of the pre-processing method to prepare the image blocks degrades the visual quality of the water-marked image especially for medical images and the watermark embedding method that depends on the maximum mean value limits the capacity of scheme.

### 3.2 Watermark creation algorithm

In this subsection, the algorithm used to generate the watermark is illustrated:

- Step 1. **Division of Original image:** The original image is divided into non-overlapping blocks (NB) of  $8 \times 8$ .
- Step 2. **Apply MD5:** Apply Message-Digest algorithm 5 on each block of original image for 128-bit resulting hash value [24]. An example of MD5 encryption of biometric thumbprint is shown in Fig. 3.
- Step 3. **Apply AES:** Apply 14 rounds of *AES* with key size of 256 bits on the output of Step 2 along with the concatenation of patient's biometric *ID*, key1 and patient *ID* (Fig. 4). A round has several processing steps which includes transposition, substitution, mixing of the input plaintext and transform it into the final output of cipher text.
- Step 4. **LZW:** Apply *LZW* on the output of Step 3 to compress the watermark bits. Lempel et al. [37] described *LZW* as a table-based lookup algorithm used to compress file into smaller files.
- Step 5. **Watermark:** The output from step 4 is the final watermark.

### 3.3 Watermark embedding algorithm

The watermark embedding algorithm, shown in Fig. 5, is summarized in the following steps:

- Step 1. **Division of Original image:** The original image is divided into non-overlapping blocks,  $NB_i$ , where  $i$  is the index of the block. Each of these blocks are



**Fig. 3** Biometric watermark with MD5

PATIENT ID: DANILKRVII6114  
 ADDRESS: 37 DEFENCE COLONY ROOP NAGAR INDIA  
 HOSPITAL ID: 1312SUJATA2412SUM  
 HOSPITAL NAME: CH. SUBE SINGH HOSPITAL  
 DOCTOR ID: 3219SAHIL0401  
 DISEASE: MRI SCAN FOR TUMOUR SIGNS

Fig. 4 “Text Watermark”

transformed by using *SLT* (1) to get four subbands- *HH*, *HL*, *LH* and *LL*. High frequency subbands *HL* and *LH* are used for the watermark embedding in proposed technique.

Step 2. **Calculating the threshold value:** Particle Swarm Optimization (PSO) (Eberhart and Kennedy [11]) is used for calculating threshold *Th*, for each and every block and *T* for the whole image, by using the following (3) and (4).

$$V_i^{k+1} = (w \times V_i^k) + (c_1 \times rand_1(\dots) \times x \times (pbest_i - s_i^k)) + (c_2 \times rand_2(\dots) \times x \times (gbest - s_i^k)) \tag{3}$$

$$s_i^{k+1} = s_i^k + V_i^{k+1} \tag{4}$$

where,  $V_i^k$  : velocity of agent *i* at iteration *k*,

- w*: weighting function,
- $c_j$ : weighting factor,
- rand*: uniformly distributed random number between 0 and 1,

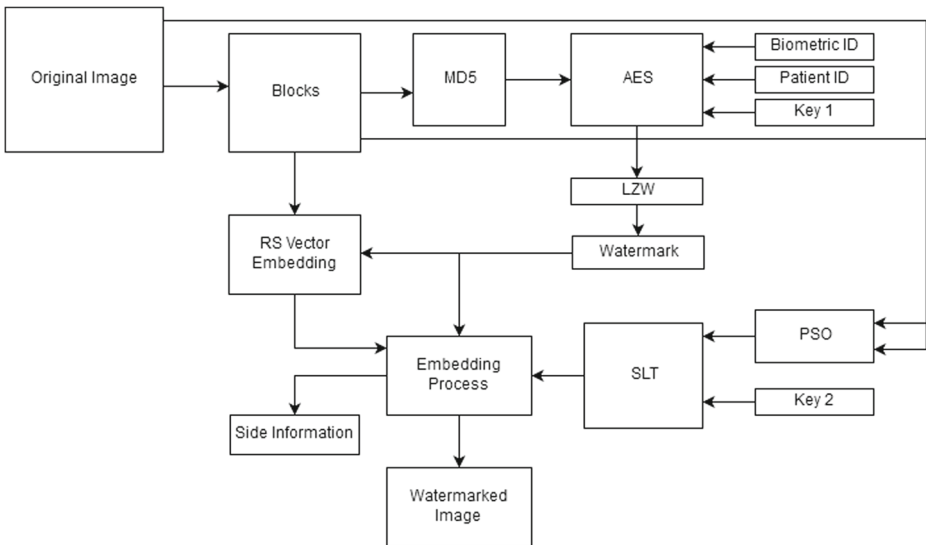


Fig. 5 Proposed Watermark embedding technique



- $s_i^k$ : current position of agent  $i$  at iteration  $k$ ,
- $pbest_i$ : pbest of agent  $i$ ,
- $gbest$ : gbest of the group.

Step 3. **Embedding watermark:** To embed a watermark bit in each selected block, the difference between the mean values of the *SLT* coefficients in the high frequency subbands (i.e., *HL* and *LH*) of that block are altered. Mean value of the *SLT* coefficients in the *HL* subband is made more than the mean value of the *SLT* coefficients in the *LH* subband when the watermark bit is ‘1’. When the watermark bit is ‘0’, the alteration is applied to make the mean value of the *LH* subband more than the mean value of the *HL* subband. To explain the embedding process, consider a watermark sequence ( $w$ ) as a vector of bits  $w=[w_1, \dots, w_j, \dots, w_{len}]$ , where  $j=1, 2, \dots, len$  and  $len = \text{length}(w)$ , to embed a watermark bit  $w_j$ , in a block, threshold ( $T$ ) from step 2 has been used and alteration factors, given in (5), (6), with each watermark bit  $w_j$ , can be embedded according to the following rules:

- If  $w_j = 1$  and  $(\mu^{HL} - \mu^{LH}) \geq T$ , then the block remains unchanged.
- If  $w_j = 1$  and  $(\mu^{HL} - \mu^{LH}) < T$ , then  $\mu_{new}^{HL} = \mu^{HL} + A_1$  and  $\mu_{new}^{LH} = \mu^{LH} - A_1$ .
- If  $w_j = 0$  and  $(\mu^{LH} - \mu^{HL}) \geq T$ , then the block remains without change.
- If  $w_j = 0$  and  $(\mu^{LH} - \mu^{HL}) < T$ , then  $\mu_{new}^{HL} = \mu^{HL} - A_2$  and  $\mu_{new}^{LH} = \mu^{LH} + A_2$

Alteration factors,  $A_1$  and  $A_2$ , have been calculated as

$$A_1 = [T - (\mu^{HL} - \mu^{LH})] / (2 \times Th) \tag{5}$$

$$A_2 = [T - (\mu^{LH} - \mu^{HL})] / (2 \times Th) \tag{6}$$

Because of the reversibility requirements, the difference between the mean values of selected subbands will be saved as side information when the mean values are changed to embed the watermark bit.

Step 4. **Applying the ISLT:** The process of watermark embedding is executed until all the watermarked bits are embedded. The original subbands are substituted by the modified subbands and *ISLT* is applied through matrix multiplication process by using (2). Now, to ensure the reversibility, the resultant output must be rounded up to integer numbers. Thus, the original image and the watermarked image can be resynthesized exactly the same at the receiver end.

Step 5. **Embedding through RS vector:** Image is divided into groups of four pixels and each group will be considered as a single value. Discrimination and Flipping functions must be defined before making groups.

Discrimination Function ( $f$ ) is used to describe the state of the group and it is calculated as

$$f(\text{group}) = \sum_{i=1}^{i=3} |x_{i+1} - x_i| \tag{7}$$

Where: Group =  $\{x_1, x_2, x_3, x_4\}$ ,  $x_i$  is the value of the pixel  $i$  in the current group.

Flipping function is used to modify the pixel value by flipping the *LSB* of the two middle pixels of each block. The discrimination function by using (7) is calculated for each group before ( $fr$ ) and after ( $fs$ ) using the flipping function, the state of each group is determined as follows:

- RG* Group: if  $fs > fr$
- SG* Group: if  $fs < fr$
- UG* Group: if  $fs = fr$

Creating RS Vector: Each group of pixels has a single value, watermark bit ‘1’ is embedded in Regular group (RG), ‘0’ in Singular group (SG) and no bit is embedded in Unused group(UG). The unused groups are ignored because they are not affected by the flipping function, therefore, the RS Vector consists of a stream of bits (zeros and ones), and each bit represents the state of a group of pixels in the image. Finally, the watermarked image is obtained by combining the groups along with the side information.

### 3.4 Handling the overflow and underflow

During the watermark embedding process there may arise a situation of underflow and overflow in some pixel values. Earlier different methods were suggested to avoid this particular problem. But most of them relied on the process called as histogram modification process [31, 32], in which the histogram of the image is narrowed from both sides before embedding the watermark data. This process has been applied in many watermarking techniques. Instead of using histogram modification as a pre-processing step, a new and improved histogram modification process was proposed in which histogram will be modified only when required [33]. Modified pixel values are saved as side information and sent to the receiver side along with the watermarked image.

In [7] an investigation is done about the effect of changing the wavelet coefficients on the pixel values, to select the highest scale pixel change. Then the pixel adjustment method came into play i.e. the pixel values that undergo from overflow or underflow are modified before the watermark embedding process. In this method, the locations of the pixel values with such behaviour and the adjustment scale are saved as part of side or extra information which needs to be sent at the receiver channel. Although the method solved the problems of overflow and underflow but it degraded the visual quality of the watermarked image by a greater extend because of shifting process. In the proposed technique, the use of pixel adjustment as a side-processing along with the watermark embedding is done instead of using it as a preprocessing step or post processing step.



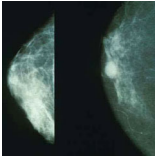
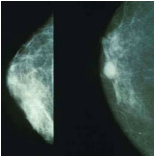
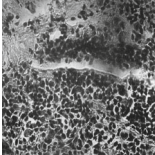
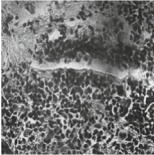
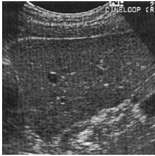
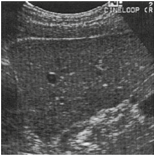


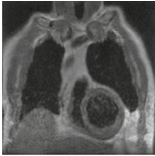
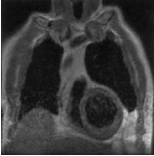
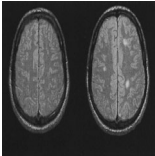
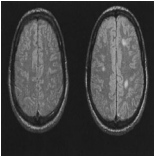
In the proposed technique, each individual target pixel is changed by shifting its value that is required for the watermark embedding process and hence the visual quality of the watermarked image will be enhanced. The pixel values which are suffering from the condition of overflow or underflow are used to change the desired formulae of watermarking along with their information is saved along with side information and then these pixel values will be adjusted as follows:

$$I_w(i, j) = \begin{cases} 255 & \text{if } I_w(i, j) > 255 \\ 0 & \text{if } I_w(i, j) < 0 \end{cases}$$

where  $I_w$  is the watermarked image before pixel adjustment,  $(i, j)$  are the coordinates of the pixel in the image, and  $I_w(i, j)$  is the modified pixel value.

Hence, the total overhead of the algorithm includes five things i.e. Key1, Key2, size of the block, the difference of mean values of the blocks and the total number of bits in overflow/underflow. The size of side information is directly proportional to the size of the image and size of the watermark. Also, its inversely proportional to the  $i$  of  $NB_i$  For an image of size  $512 \times 512$  with block size of  $4 \times 4$ , the size of side information will be 2096 bytes approx. The side information together with the block size must be sent with the watermarked image to the receiver side. The variation of total overhead is shown in Table 6 for original image(4.) from Table 1.

**Table 1** Watermarked images along with PSNR (dB)

Original image	Watermarked Image	PSNR(RS)	PSNR(SLT)	PSNR(RS then SLT)
a. 		55.8439	50.7585	51.0727
1. 		55.8782	58.8271	49.3297
2. 		55.9123	51.9748	50.9343
3. 		55.9184	53.4858	51.1411
4. 		54.3898	60.9701	50.7663
5. 		55.3495	56.3128	47.3072
6. 		55.2765	52.6306	49.4132

### 3.5 Watermark extraction algorithm

Step 1. **Dividing the image:** At receiver’s side, firstly read the watermarked image along with the side information and then the pixels that were adjusted are relocated

back to their original locations. Now, non-overlapping blocks are formed from the watermarked image.

- Step 2. **Applying SLT:** Transform each and every block using *SLT* to obtain its subbands.
- Step 3. **Extraction of SLT based Watermark:** For each and every block, the coefficient mean values in the high frequency subbands i.e. *HL* and *LH* are calculated and the desired watermark bits are extracted according to the following equation:

$$w_j^* = 1, \text{ if } \mu_{new}^{HL} \geq \mu_{new}^{LH}$$

$$w_j^* = 0, \text{ if } \mu_{new}^{HL} < \mu_{new}^{LH}$$

where  $w_j^*$  is the extracted bit. Here,  $\mu_{new}^{HL}$  is the mean values of the slantlet transformation coefficients in high frequency *HL* subband and  $\mu_{new}^{LH}$  is the mean values of the slantlet transformation coefficients in high frequency *LH* subband.

- Step 4. **Extraction of RS Vector based Watermark:** Create groups of 4 pixels. Determine  $f$  and  $F$  for each RS vector. Extract the embedded watermark by determining  $RG$ ,  $SG$  and  $UG$ .
- Step 5. **Recovery of the Original Image:** The values that are extracted as watermark bits and the difference values which are already saved in the side information, the original mean value of each block will be recovered by enforcing the inverse process that was applied in the watermark embedding side. Every block that contains the difference value, extracted watermark value and the original mean value can be recovered through shifting back, the mean values and hence the original image will be obtained by re-arranging the image blocks.

## 4 Experimental results

The experiments have been conducted to evaluate the basic requirements of the watermarking schemes, which are maintaining the image quality parameters, security, integrity, confidentiality, tamper detection and localization, invisibility, robustness, capacity, reversibility and the effect of block size with threshold values. To test the performance of the proposed technique, we used 100 medical images. To make the comparison easier, all the images are converted to grayscale and resized to (512 × 512 pixels). The parameters that have been calculated for performance evaluation are explained as follows:

### 4.1 Invisibility evaluation

To evaluate the visual quality (i.e., the invisibility) of the watermarked images, the *PSNR* between the original and the watermarked image is calculated as:

$$PSNR = 10 \times \log_{10} \frac{(2^b - 1)^2}{MSE} \tag{8}$$

where  $b$  is the bit depth of the image and *MSE* is defined as,

$$MSE = \sum_{i=1}^M \sum_{j=1}^N \frac{\delta(i, j)^2}{H \times W} \tag{9}$$

where  $\delta(i, j)$  is defined as

$$\delta(i, j) = S(i, j) - C(i, j) \tag{10}$$

where  $S(i, j)$  is the pixel of stego image and  $C(i, j)$  is the pixel of cover image,  $H$  and  $W$  is the height and width of image respectively.

Table 1 shows the  $PSNR$  value for Lena image as 51.0727 dB and  $PSNR$  values for different medical images after all three cases i.e..

- i.  $PSNR$  of the image through the embedding with RS vector having 30,720 hidden bits.
- ii.  $PSNR$  of the image only embedding though  $SLT$  with 30,720 hidden bits.
- iii.  $PSNR$  of the image after the proposed technique after embedding 61,440 bits.

Comparison of the above cases is shown in Fig. 6 with corresponding watermarked images from Table 1.

### 4.2 Capacity evaluation

Capacity is measured by the size of the image and size of hidden bits i.e.

$$Capacity(C) = (H \times W)/Y \tag{11}$$

For an image  $I_m$  with size  $H \times W$  with total number of hidden bits  $Y$ . whereas, the pure capacity depends on the size of the original image and the size of the block. For an image  $I_m$  with size  $H \times W$  and a spatial domain block with size  $b_{size} = h \times w$ , the pure capacity can be calculated by:

$$Capacity(C) = (H/h) \times (W/w) \tag{12}$$

If the block size in the transform domain ( $B_{size}$ ) is  $r \times s$ , where  $r = h/2$ , and  $s = w/2$ , then the relationship between the capacity and the block size can be calculated as follows:

$$Capacity(C) = (H/2 \times r) \times (W/2 \times s) \tag{13}$$

The parameter  $C$  calculates the total number of bits that can be embedded in the image at a specific block size. To calculate the capacity in terms of bits-per-pixel (bpp),  $C$  is divided by the total number of pixels in the image. Proposed technique in transform domain has the capacity of 0.0625 bpp using (13) and the capacity from RS vector embedding is calculated by (11) is 1.06 bpp. Table 2 is constructed by taking Fig. 7 as original image, showing embedding capacity for each channel. The capacity is calculated after compression by  $LZW$ .

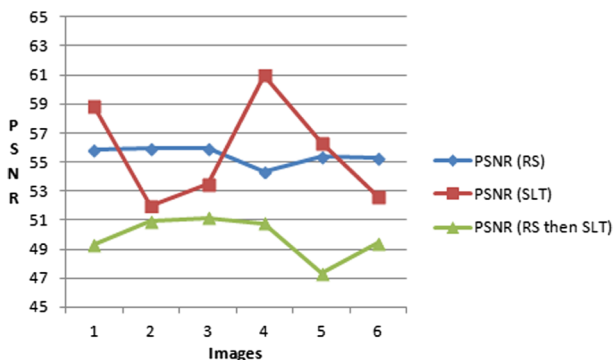


Fig. 6 PSNR comparison for medical images

**Table 2** PSNR, Capacity (bits), BPP for different channels

No of Channels	Average PSNR(dB)	Capacity	BPP
R	50.1308	61,440	1.1225
RG	50.1347	1,22,880	2.2450
RGB	50.1392	1,84,320	3.3675

### 4.3 Reversibility evaluation

To evaluate the reversibility, Image Error Rate (IER), (i.e., the ratio of the number of the images recovered with errors to the total number of each kind of the test images) has been calculated. For the proposed technique, IER is “ZERO”, it shows that all cover images and watermark are recovered without any loss of data.

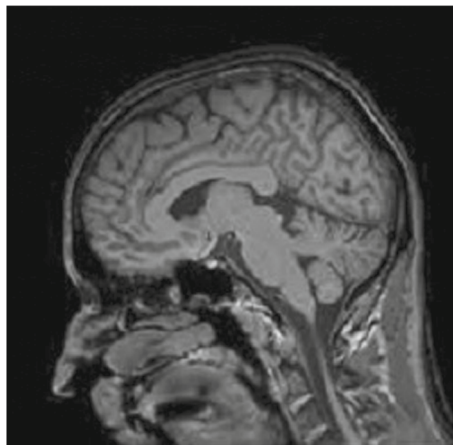
### 4.4 Robustness evaluation

For robustness evaluation, watermarked images are tested against many attacks and watermarks are extracted after attacks along with *PSNR* values as shown in Table 3, against various unintentional attacks. Attacks like *JPEG* compression is done with the quality factor equals to (20, 30, ..., 100), Additive Gaussian Noise (AGN) with zero-mean and a variance equals to (0.001, 0.002, ..., 0.01). Resistance against these attacks show the strength of proposed technique.

Figure 8 shows variation on the *PSNR* values after attacks as the *PSNR* value of the watermarked image before attacks was 50.76dB and the least destruction was done with average filter attack. Similarly Figs. 9, 10, 11 and 12 show the variations in the values of *SIM*, *BER*, *SNR* and *NC* with the images from Table 3. *BER* is ‘ZERO’ for Gamma correction(0.5) and sharpening alpha(0.2) attacks. Results show that the proposed technique have high strength and good recovery of watermark after attacks.

### 4.5 Authenticity and integrity

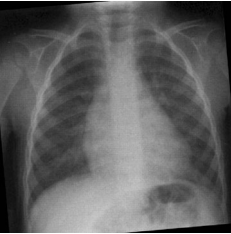



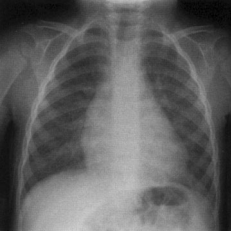

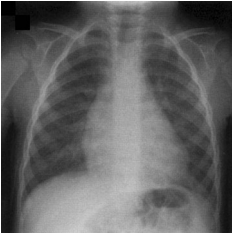

In the case of medical images, security and authenticity are most important criteria because if there is any tampering with the contents of the image than it can damage the *ROI* whereas

**Fig. 7** MRI brain image (256 × 256)

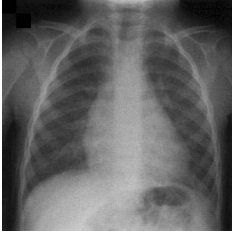



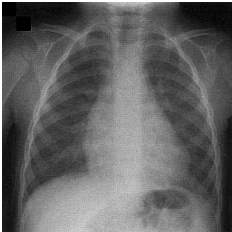

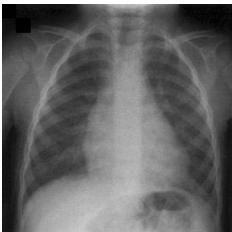

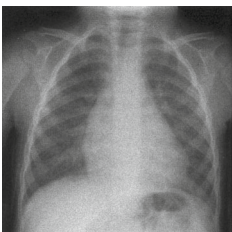

maintaining the integrity of the image is equally viable. So, the proposed technique can be used for checking the authenticity and integrity of the medical image.

**Tamper detection and localization** If the watermarked image is tampered within the network or by intruders, it is detectable and can be localized through the proposed technique. As, it creates an encrypted watermark by using three components i.e. the biometric *ID*, patient *ID* for the purpose of checking integrity and original image blocks from *ROI*. Patient *ID* is in the form of text watermark which secures the personnel details of the patient for confidentiality. Biometric *ID* i.e. thumbprint is the unique identification mark of the patient which secures the authenticity and integrity of the patient. *ROI* blocks from the original image help in tamper detection and localization of the corrupted region of medical image.

**Table 3** Types of attacks with extracted watermark and PSNR

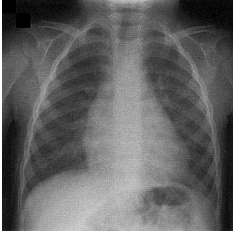

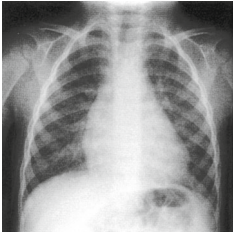

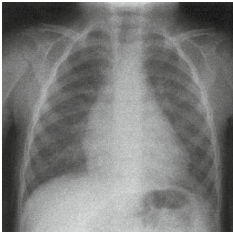



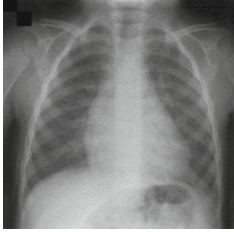

Type of Attack	Image after Attack	Extracted Watermark	PSNR
A. Rotation(5 degree)			30.2142
B. Salt and Pepper			32.03
C. Filtering(average)			49.5695
D. Cropping(128×128)			42.2059

**Table 3** (continued)

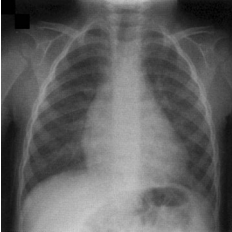

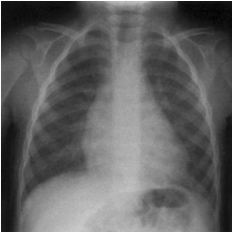

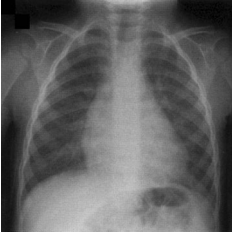

Type of Attack	Image after Attack	Extracted Watermark	PSNR
E. JPEG Comprssion			38.0628
F. Median Filter			32.6737
G. Smoothing			34.2089
H. Gaussian			41.7804
I. Speckle noise			29.98



**Table 3** (continued)

Type of Attack	Image after Attack	Extracted Watermark	PSNR
J. Sharpening			30.8433
K. Histogram Equalization			15.7809
L. Poission attack			31.02
M. Blurring			34.6018
N. Motion Blur			39.6919

**Table 3** (continued)

Type of Attack	Image after Attack	Extracted Watermark	PSNR
O. Resize(1.2)			25.1450
P. Wiener Attack			39.9482
Q. Scaling			30.1988

Experimental results shown in Table 4, for image(4.) from Table 1, prove the efficiency of the proposed technique.

#### 4.6 Security of the watermark

*MD5* and *AES* are very efficient cryptographic algorithms used for security of digital data. As, watermark used in proposed technique consists of four parts i.e. blocks of original image, biometric *ID* of the patient, patient *ID* as text watermark and key1. The original image blocks are encrypted with *MD5*, giving abundant security while generation hash functions. The hash values are then fused with other three components of watermark, which are encrypted using *AES-256*. It does provide a defence against the possibility of Quantum Computers, specifically Grover's Algorithm which can reduce the search space by effectively half. There is the protection for encrypted watermarks for more than 50+ years against any kind of cryptographic attacks like collision attacks, bruteforce attack, algebraic attacks, exhaustive key searching, boomerang attacks meet-in-the-middle attack and bicliques attack.

#### 4.7 Effects of parameters

In this section, analysis is done to check the effect of two parameters. The first parameter is the block size (*Bsize*) (i.e., the size of the *SLT* coefficients subband), the changes in the

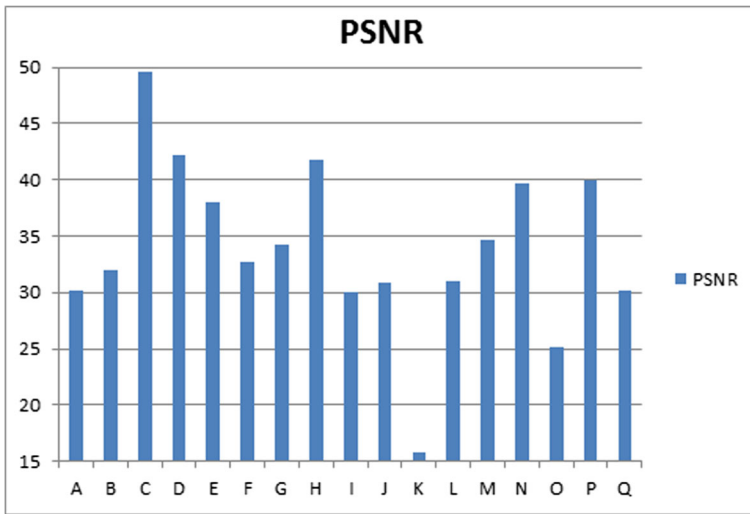


Fig. 8 PSNR variation after attacks on watermarked image

Bsize influence the capacity, the invisibility, the robustness, and the run-time of the software. The second parameter is the threshold values ( $T$  and  $Th$ ) (i.e., the watermark strength), the change in the threshold value has an effect on the invisibility and robustness. The proposed scheme has been tested for different threshold values ( $T = 1, 2, \dots$ ) and different block sizes.

#### 4.7.1 Threshold

The change in the threshold value will affect the invisibility and robustness whereas it has no effect on the capacity. *PSNR* decreases with the increase of the threshold value and *BER*

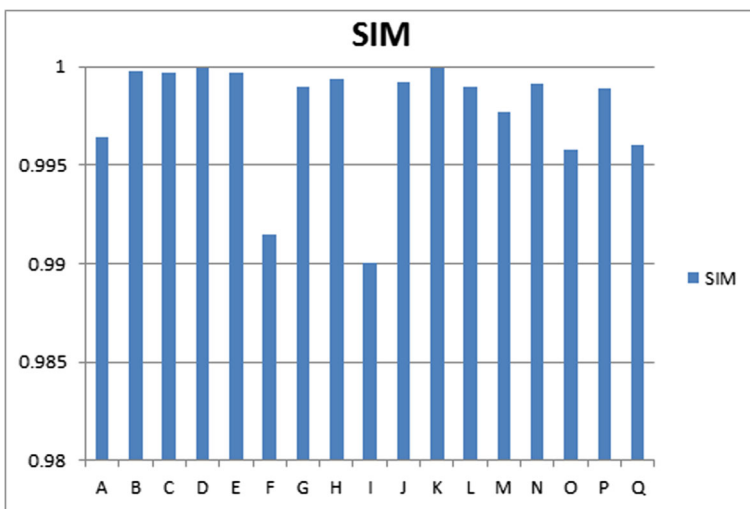
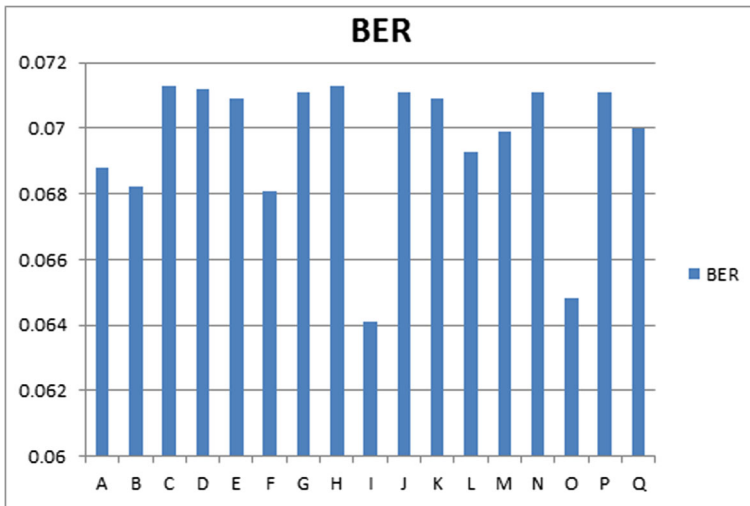


Fig. 9 SIM after attacks on watermarked image

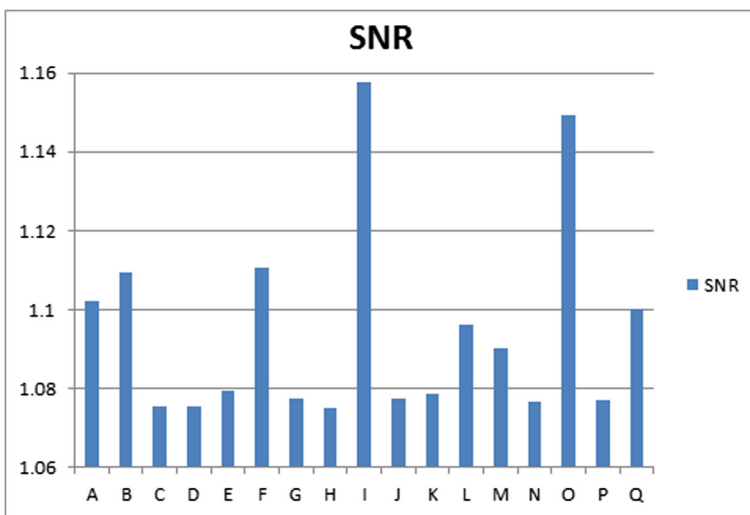


**Fig. 10** BER after attacks on watermarked image

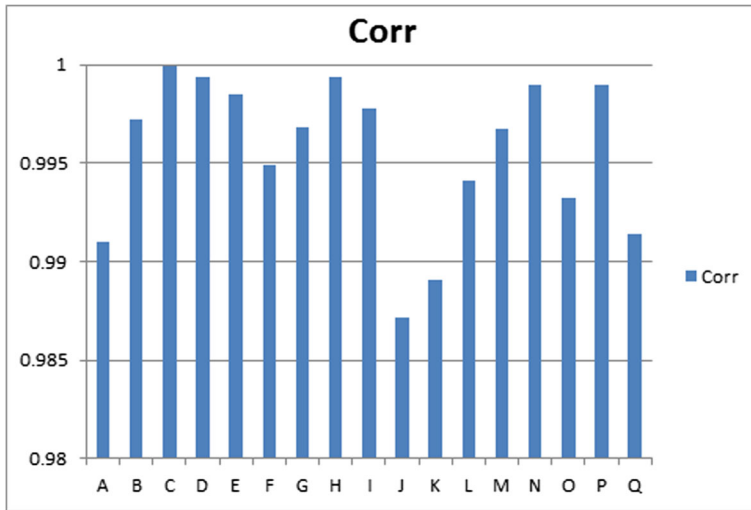
will decrease with the increase in threshold values. Threshold value ( $Th$ ) is however fully dependent on the block sizes.

#### 4.7.2 Block size

The capacity has been calculated using (13) for different block sizes when the original image size is  $(256 \times 256)$  as shown in Table 5, the capacity decreases with the increase of the Bsize. Also, the value of  $PSNR$  increases with Bsize. Higher the Bsize, the running time will decrease because of the decrement in the total number of blocks.  $BER$  is also affected with Bsize, it decreases with increase in Bsize.



**Fig. 11** Signal to noise ratio after attacks on watermarked image



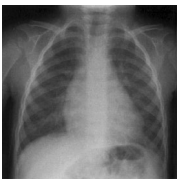





**Fig. 12** Correlation values after attacks on watermarked image

Furthermore, proposed technique allows flexible adjustment on the Bsize and threshold that controls the tradeoff between image fidelity and embedding capacity.

### 4.8 Overall execution time

Execution time is computed for the program at different block sizes. Overall execution time includes the time taken for watermark creation, embedding with Rs vector as well as *SLT* and watermark extraction. The results have been calculated on the personnel computer with processor: Intel(R) Core(TM)i7-4510U CPU @ 2.00 GHz 2.60GHz and 8GB memory. Matlab(R2015a) have been used to record the programs run time in seconds with the tic and toc commands. The average execution time for 100 medical test images have been calculated

**Table 4** Extracted watermarks with original and tampered image

Image Type	Watermarked Image	Original image watermark	Biometric ID watermark	Text watermark
Untampered				PATIENT ID: DANILKRVII6114
Tampered				PA=09ET01D:D12IL5HV6I314

**Table 5** Block Size in transform domain with Capacity(bits)

Block Size	Capacity
$2 \times 2$	16384
$4 \times 4$	4096
$8 \times 8$	1024

and the results are shown in Table 6 for original image(4.) from Table 1. The recorded results illustrate that the execution time in transform domain is inversely proportional to the Bsize due to the higher number of bits that are embedded in the image and higher number of blocks increase the repetition of embedding process. Total overhead created by the proposed technique is reduced with the increase in block size.

#### 4.9 Comparison with existing techniques

In this section, the performance of the proposed scheme is compared with existing robust reversible medical watermarking techniques.

These comparisons indicate that the proposed technique has significantly achieved high quality and high capacity. In addition, the comparison is conducted by embedding a watermark into  $256 \times 256$  MRI brain image with block size of  $4 \times 4$ . As compared to [3], the proposed technique can improve *PSNR* to 71.536%, *BPP* to 51.689% and has low time complexity as quad based algorithm is applied once on the image data. As compared to [30], the proposed technique can improve *PSNR* to 3.317% and *BPP* to 2.045%. As compared to [29], the proposed technique can improve *PSNR* from to 31.947%, *BPP* to 12.25% and high time complexity as it takes 4 minutes for embedding. As compared to [32], the proposed technique can improve *PSNR* to 70.602% and *BPP* to 13.383%. As compared to [33], the proposed technique can improve *PSNR* to 59.275%, *BPP* to 129.081 and low time complexity as it uses difference expansion with a low computational complexity.%. As compared to [35], the proposed technique can improve *PSNR* to 124.239%. Although *BPP* is 43.875% lower, it could be increased if the block size is reduced to  $2 \times 2$ . As compared to [36], *PSNR* is lowered by 2.146% for the proposed technique but *BPP* is improved by 107.870% and possess low time complexity. As compared to [43], the proposed technique can improve *PSNR* up to 58.170% and *BPP* to 5.896%. As compared to [44], the proposed technique can improve *PSNR* to 12.320% and *BPP* to 410.227%. The above comparison is performed by considering only one channel of the image for the proposed technique. If all three channels

**Table 6** Block size wise Overall Execution Time (in seconds) and Total Overhead (in Bytes)

Block Size	Embedding Time	Extraction Time	Overall Time	Total Overhead
$2 \times 2$	1.4998	0.9562	5.4966	8240
$4 \times 4$	0.4008	0.2132	3.6546	2096
$8 \times 8$	0.1592	0.0631	3.2629	560
$16 \times 16$	0.0723	0.0287	3.1416	176
$32 \times 32$	0.0598	0.0125	3.11308	80

**Table 7** Comparison with existing techniques

Techniques	PSNR( <i>dB</i> )	BPP	Time Complexity
[3]	29.23	0.74	Low
[30]	48.53	1.10	–
[29]	38.0	1.00	High (240 sec.)
[32]	29.39	0.99	–
[33]	31.48	0.49	Low
[35]	22.36	2.00	–
[36]	51.24	0.54	Low
[43]	31.70	1.06	–
[44]	44.64	0.22	–
Proposed Algorithm	50.14	1.1225	Low (3.65 sec.)

are considered then capacity of the proposed technique is increased by 211.67% approximately than all existing techniques shown in Table 7, with *BPP* 3.3675 i.e. 206.13% higher than [30]. Time complexity for the embedding process is low i.e. 3.6546 seconds and it improves with the increase in block size as shown in Table 6. Also, ‘–’ is used for the existing algorithms, which have not discussed the time complexity.

In summary, the proposed technique maintains visual quality of watermarked images while simultaneously increasing the capacity for medical image watermarking because proposed techniques uses the advantages of embedding in both transform and spatial domains.

## 5 Conclusion

Medical images are very high resolution images so it is difficult to secure such images through watermark. This work is proposed for the security of watermark and the cover image. Slantlet transformation along with RS vector is used for watermark embedding in selected blocks of the cover image. Cryptographic techniques *MD5* and *AES*. are used for watermark security along with the compression techniques for increasing the capacity. *PSNR* between cover and watermarked image is improved through the proposed technique as compared with existing techniques. Also many attacks done on the watermark and watermarked image which gave very promising results as compared to the existing medical watermarking techniques. Biometric security is applied for the integrity of the designed watermark.

## References

1. Abou-Loukh SJ, Gatea SM (2011) Spoken word recognition using slantlet transform and dynamic time warping. Nahrain University. Coll Eng J (NUCEJ) 14(1):34–45
2. Abou-Loukh SJ, Zeyad T, Thabit R (2010) Ecg classification using slantlet transform and artificial neural network. J Eng 16(1):4510–4528
3. Alattar AM (2004) Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans Image Process 13(8):1147–1156
4. An L, Gao X, Li X, Tao D, Deng C, Li J (2012) Robust reversible watermarking via clustering and enhanced pixel-wise masking. IEEE Trans Image Process 21(8):3598–3611

5. Anand D, Niranjan UC (1998) Watermarking medical images with patient information. In: Proceedings of the 20th annual international conference of the IEEE on engineering in medicine and biology society, vol 2. IEEE, pp 703–706
6. Balasamy K, Dharshini MD, Gayathri S, Geetha MM (2016) Image authentication system using fused watermarking technique. *Int J Innov Res Comput Commun Eng* 4(1):189–193
7. Coatrieux Gouenou, Maitre H, Sankur B, Rolland Y, Collorec R (2000) Relevance of watermarking in medical imaging. In: Proceedings IEEE EMBS international conference on information technology applications in biomedicine. IEEE, pp 250–255
8. Coatrieux G, Quantin C, Montagner J, Fassa M, Allaert F-A, Roux C (2008) Watermarking medical images with anonymous patient identification to verify authenticity. In: *MIE*, vol 136, pp 667–672
9. Dong J, Li J, Duan Y (2015) A robust watermarking algorithm for encrypted medical images based on dct encrypted domain. In: International conference on electronic science and automation control. Citeseer, pp 140–143
10. Eswaraiah R, Sreenivasa Reddy E (2014) Medical image watermarking technique for accurate tamper detection in roi and exact recovery of roi. *Int J Telemed Appl* 2014:13
11. Kennedy J, Eberhart R (1995) Particle swarm optimization. In: Proceedings of the IEEE international conference on neural networks, 1995, vol 4, pp 1942–1948
12. Khor HL, Liew S-C, Zain JM (2016) Parallel digital watermarking process on ultrasound medical images in multicore environment. *J Biomed Imag* 2016:4
13. Kishore PVV, Kishore SRC, Kiran Kumar E, Kumar KVV, Aparna P (2015) Medical image watermarking with dwt-bat algorithm. In: 2015 international conference on signal processing and communication engineering systems (SPACES). IEEE, pp 270–275
14. Lafta MM, Alwan IM (2011) Watermarking in image using slantlet transform. *Iraqi J Sci* 52(2):225–230
15. Manasrah T, Al-Haj A (2008) Management of medical images using wavelets-based multi-watermarking algorithm. In: IIT 2008 international conference on innovations in information technology 2008. IEEE, pp 697–701
16. Milanova MG, Ford C, Kountchev R, Kountcheva R (2003) Digital watermarking for medical images. In: *METMBS*, pp 509–520
17. Mohammed RT, Khoo BE (2012) Image watermarking using slantlet transform. In: 2012 IEEE symposium on industrial electronics and applications (ISIEA). IEEE, pp 281–286
18. Mohananthini N, Yamuna G (2015) A study of dwt-svd based multiple watermarking scheme for medical images. *IJ Netw Secur* 17(5):558–568
19. Mohanty SP (1999) Digital watermarking: a tutorial review. <http://www.csee.usf.edu/~smohanty/research/Reports/WMSurvey1999Mohanty.pdf>
20. Mulcahy C (1997) Image compression using the haar wavelet transform. *Spelman Sci Math J* 1(1):22–31
21. Mutt SK, Kumar S (2009) Secure image steganography based on slantlet transform. In: Proceeding of international conference on methods and models in computer science, 2009. ICM2CS 2009. IEEE, pp 1–7
22. Panda G, Dash PK, Pradhan AK, Meher SK (2002) Data compression of power quality events using the slantlet transform. *IEEE Trans Power Deliv* 17(2):662–667
23. Lakshmi Priya R, Sadasivam V (2015) Protection of health imagery by region based lossless reversible watermarking scheme. *Sci World J* 2015
24. Rivest R (1992) The md5 message-digest algorithm. <https://www.ietf.org/rfc/rfc1321.txt>
25. Selesnick IW (1998) The slantlet transform. In: Proceedings of the IEEE-SP international symposium on time-frequency and time-scale analysis. IEEE, pp 53–56
26. Selesnick IW (1999) The slantlet transform. *IEEE Trans Signal Process* 47(5):1304–1313
27. Shaji V, Prakash VV (2015) Medical image watermarking using cgr. *Int J Eng Res General Sci* 3(5):580–586
28. Sharma A, Dave M, Singh AK, Ghrera SP (2015) Encryption based medical image watermarking against signal processing attacks. In: Proceedings of international conference on future computational technologies (ICFCT 2015), pp 82–88
29. Shih FY, Wu Y-T (2005) Robust watermarking and compression for medical images based on genetic algorithms. *Inform Sci* 175(3):200–216
30. Shih FY, Zhong X (2016) High-capacity multiple regions of interest watermarking for medical images. *Inform Sci* 367:648–659
31. Thabit R, Khoo BE (2014) Robust reversible watermarking scheme using slantlet transform matrix. *J Syst Softw* 88:74–86



32. Thodi DM, Rodríguez JJ (2007) Expansion embedding techniques for reversible watermarking. *IEEE Trans Image Process* 16(3):721–730
33. Tian J (2003) Reversible data embedding using a difference expansion. *IEEE Trans Circ Syst Vid Technol* 13(8):890–896
34. Umamageswari A, Suresh GR (2015) Analysis of secure medical image communication with digital signature and reversible watermarking. *Ind J Electr Eng Comput Sci* 15(3):544–553
35. Wakatani A (2002) Digital watermarking for roi medical images by using compressed signature image. In: *Proceedings of the 35th annual Hawaii international conference on system sciences, 2002. HICSS. IEEE*, pp 2043–2048
36. Wang Z-H, Lee C-F, Chang C-Y (2013) Histogram-shifting-imitated reversible data hiding. *J Syst Softw* 86(2):315–323
37. Welch TA. (1984) A technique for high-performance data compression. *Computer* 6(17):8–19
38. Xuan G, Shi YQ, Yang C, Zheng Y, Zou D, Chai P (2005) Lossless data hiding using integer wavelet transform and threshold embedding technique. In: *IEEE international conference on multimedia and expo, 2005. ICME 2005. IEEE*, pp 1520–1523
39. Xuan G, Shi YQ, Chai P, Teng J, Ni Z, Tong X (2009) Optimum histogram pair based image lossless data embedding. In: *Transactions on data hiding and multimedia security IV. Springer*, pp 84–102
40. Xuan G, Yao Q, Yang C, Gao J, Chai P, Shi YQ, Ni Z (2006) Lossless data hiding using histogram shifting method based on integer wavelets. In: *International workshop on digital watermarking. Springer*, pp 323–332
41. Xuan G, Zhu J, Chen J, Shi YQ, Ni Z, Wei S (2002) Distortionless data hiding based on integer wavelet transform. *Electron Lett* 38(25):1646–1648
42. Zain J, Clarke M (2005) Security in telemedicine: issues in watermarking medical images. In: *International conference: science of electronic, technologies of information and telecommunications*
43. Zain JM, Clarke M (2011) Reversible region of non-interest (roni) watermarking for authentication of dicom images. [arXiv:1101.1603](https://arxiv.org/abs/1101.1603)
44. Zhao Z, Luo H, Zhe-Ming L, Pan J-S (2011) Reversible data hiding based on multilevel histogram modification and sequential recovery. *AEU-Int J Electron Commun* 65(10):814–826
45. Zou D, Shi YQ, Ni Z (2004) A semi-fragile lossless digital watermarking scheme based on integer wavelet transform. In: *IEEE 6th workshop on multimedia signal processing*, pp 195–198



**Roopam Bamal** was born in 1990 in Hisar, Haryana, India. She graduated and received her M.E degree in 2013 in the field of Software Engineering from Thapar University, Patiala, Punjab, India. From 2013 to 2014, she served as an assistant professor in computer science and engineering department in Bharat Institute of Technology, Meerut, UP, India. In 2014, she enrolled herself as doctoral student, PhD, at the Thapar University, Patiala, Punjab, India. Her research interest is focused on Image Processing and Network Security particularly on watermarking in medical images, 3D watermarking, Cryptography and information security.



**Singara Singh Kasana** is working as Assistant Professor in Computer Science and Engineering Department, Thapar University, Patiala, India. He has fifteen years of teaching and research experience. He received his PhD degree in image compression from Thapar University. His research interests include image processing, wireless networks, and information security. He has published many research papers in reputed International Journals and Conferences. He is currently guiding Ph.D. on Information Security, Image and Video Watermarking, Cryptography and Remote Sensing.