J Digit Imaging (2017) 30:695–709
DOI 10.1007/s10278-017-9961-x

# Medical Image Tamper Detection Based on Passive Image Authentication

**Guzin Ulutas**[1] · **Arda Ustubioglu**[1] · **Beste Ustubioglu**[1] · **Vasif V. Nabiyev**[1] · **Mustafa Ulutas**[1]

Published online: 8 May 2017

**Abstract** Telemedicine has gained popularity in recent years. Medical images can be transferred over the Internet to enable the telediagnosis between medical staffs and to make the patient's history accessible to medical staff from anywhere. Therefore, integrity protection of the medical image is a serious concern due to the broadcast nature of the Internet. Some watermarking techniques are proposed to control the integrity of medical images. However, they require embedding of extra information (watermark) into image before transmission. It decreases visual quality of the medical image and can cause false diagnosis. The proposed method uses passive image authentication mechanism to detect the tampered regions on medical images. Structural texture information is obtained from the medical image by using local binary pattern rotation invariant (LBPROT) to make the keypoint extraction techniques more successful. Keypoints on the texture image are obtained with scale invariant feature transform (SIFT). Tampered regions are detected by the method by matching the keypoints. The method improves the keypoint-based passive image authentication mechanism (they do not detect tampering when the smooth region is used for covering an object) by using LBPROT before keypoint extraction because smooth regions also have texture information. Experimental results show that the method detects tampered regions on the medical images even if the forged image has undergone some attacks (Gaussian blurring/additive white Gaussian noise) or the forged regions are scaled/rotated before pasting.

**Keywords** Copy move forgery · Medical image security · LBPROT · SIFT · Passive image authentication

## Introduction

Data communication over the Internet has become a necessity for many applications to share information (file and resource sharing, online transaction processing, telemedicine, etc). Especially telemedicine applications have gained popularity recently. Telemedicine enables transmission of medical data over the Internet and provides helpful interaction between patients and specialists. It helps early diagnosis of deadly diseases and let doctors to share information about diseases and treatments.

Protecting integrity, ensuring confidentiality, and source authentication are some of the requirements during medical image transmission. Integrity protection guarantees that a user has not modified that medical image. Confidentiality ensures that medical image is accessible by only authorized person. Authentication provides the verification of the source of the medical image and guarantees correctness of the corresponding patient info.

Many medical image watermarking techniques have been proposed recently to meet the requirements defined above [1–3]. Especially, integrity control of the medical images is important because any modification on the medical image can cause false diagnosis. Medical images can be attacked during transmission over the Internet and can cause false diagnosis. Figure 1b, c shows the results of the covering and duplication attacks, respectively, of the test image given in Fig. 1a. Tampered images show that modification on the image cannot be perceived by visual inspection. This type of forgeries can be called as meaningful forgery because it modifies medical image to reason false diagnosis.

✉ Guzin Ulutas
gulutas@ktu.edu.tr

[1] Computer Engineering Department, Karadeniz Technical University, Trabzon, Turkey

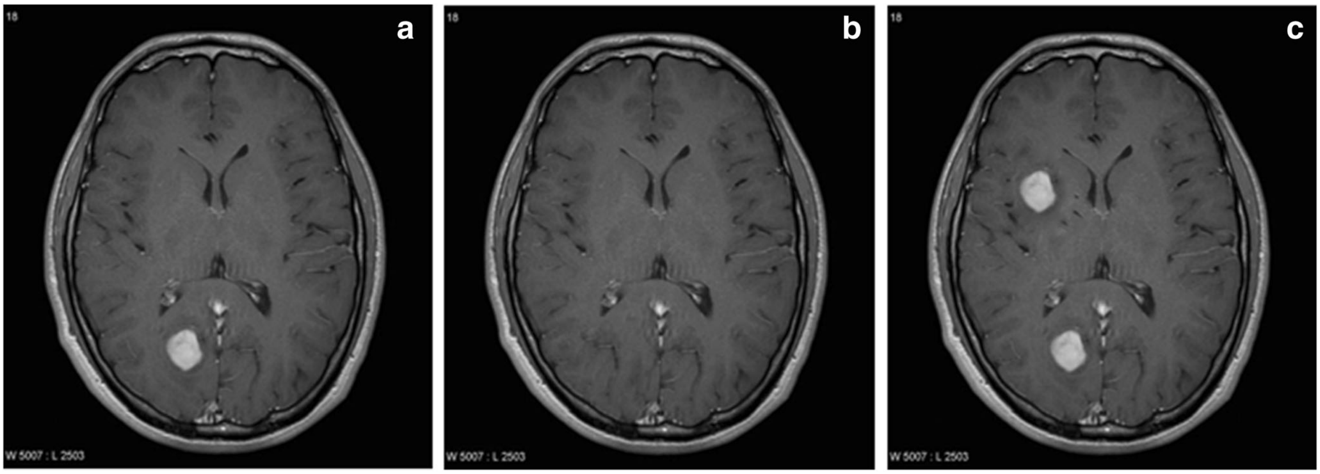


**Fig. 1** **a** Medical image. **b**, **c** Tampered medical image after covering attack and duplicating attack, respectively

Some watermarking techniques have been used in order to check the integrity of medical images in recent years. These techniques given in "Related Work" section have been designed not only to check integrity but also to detect tampered regions in the image. Although watermarking-based methods can detect even one pixel modification on the medical image, the most important disadvantage of them is to necessitate embedding extra information into medical images as explained above. Specially created information (watermark) must be embedded into the host image (medical image) to detect tampered regions by these methods. Separate information embedding step performed by a software after medical image acquisition and deteriorated visual quality due to watermark are two disadvantages of these techniques. Any alteration on the medical image can cause serious misdiagnosis and using a program to create and embed watermark can be unpractical. Therefore, detection of the tampered regions without embedding extra information into medical image becomes an important goal if these disadvantages are considered.

In 2003, Fridrich et al. suggested a method called passive image authentication to detect copied and pasted regions on the tampered image [4]. The method does not require any information (watermark or digital signature) for authentication. Passive image authentication techniques attract more attention due to the following reasons:

1. They do not necessitate any information to authenticate images.
2. They eliminate visual degradation due to embedding a watermark.

A new passive image authentication technique is proposed in this work for medical image tamper detection. The method does not necessitate embedding of extra information on the medical image for tamper detection. It takes the advantages of local binary pattern rotational invariant (LBPROT) operator and scale invariant feature transform (SIFT) to detect any tampering operation on the medical images. The method extracts the structural texture information from the test image by using LBPROT operator, and then, SIFT is used on it to extract the keypoints. Tampered regions are detected by matching the keypoints.

Keypoint-based passive authentication methods do not detect forgery operations that hide a region with smooth region like in Fig. 1b because keypoints are not obtained from smooth regions. Extraction of the statistical texture information from the medical image by LBPROT reveals the texture on the seemingly smooth regions. Then, keypoint extraction algorithms can detect keypoints on the textured image. Thus, the proposed method solves the problem of the keypoint-based passive image authentication techniques. Experimental results show that the method can detect tampered regions even if they are rescaled or rotated. Results also show that the method is robust against additive white Gaussian noise (AWGN) or blurring attacks.

The paper is organized as follows. "Related Work" section summarizes some of the related works reported in the literature. The details of the proposed method and experimental results are given in "Proposed Method" and "Experimental Results" sections, respectively. Conclusions are drawn in the last section.

## Related Work

Many watermarking-based methods are proposed to detect tampered regions on the medical images recently. Some of them are listed below to summarize literature about tamper detection on the medical images.

Zain and Fauzi developed a technique in 2006 to detect the tampered regions on medical images [5]. Their method uses a block-based approach and divides the image into non-overlapping 8 × 8 pixel blocks. Each block is then divided into 4 × 4 pixel subblocks, and a 9-bit watermark is generated. Watermark information is then embedded into least significant bits (LSBs) of the first nine pixels of the 4 × 4 pixel subblocks. Three-level hierarchical approach is used during tamper detection to detect the modified regions. Their results indicate that watermarked image has approximately 54 dB peak signal to noise ratio (PSNR).

Wu et al. developed a method based on robust watermarking and combined with modulo addition [6]. The method generates the joint photographic experts group(JPEG) bit string of the selected region of interest (ROI) and then divides them into fixed length segments. Medical image is divided into blocks by the method, and hash bits are calculated for each of them excluding the block with ROI. Robust watermarking technique is used to embed the hash bits of the block and the corresponding segment of JPEG bit string into the block. At last, all watermarked blocks and ROI portion are combined to get the watermarked image. Hash bits are used to check whether the block is tampered or not. Their results show that PSNR for the watermarked image is approximately 49 dB.

Chiang et al. used symmetric key cryptography and modified difference expansion technique to propose block-based tamper detection methods [7]. Their work presents two different methods according to recovery capability. The first method divides the image into 4 × 4 pixel blocks. Average intensity values of all blocks are calculated and concatenated and then are encrypted with two symmetric keys. Smooth blocks are determined by the method by using Haar wavelet transform. Average values are embedded into smooth blocks for the purpose of tamper detection. Their results show that watermarked image has approximately 49 dB PSNR.

Al-Qershi and Khoo embedded the patient info, average intensity values of the blocks in ROI, and hash value of ROI into ROI using the method described in [8]. Hash value of ROI is used for coarse tamper detection. If the extracted hash value mismatches the calculated hash value, finer tamper detection is realized. ROI is divided into blocks, and average intensity pixel values are calculated. If the extracted average value mismatches calculated value, corresponding block is signed as tampered.

The same authors proposed a method based on two-dimensional difference expansion [9]. Border pixels are also determined in this work as the third region. Patient record, hash value of ROI, LSBs of border pixels, and bits of intensity values in ROI are concatenated and compressed with Huffman coding. Compressed data is embedded into region of non-interest (RONI) using 2D-DE approach. Location map of the embedding procedure is embedded into border pixels. Tamper detection approach defined in their previous work is also used in this work. Experimental results show that PSNR of the watermarked image is approximately 37 dB.

Liew et al. proposed two block-based approaches in their work [10]. The medical image is separated into two regions in their first method: ROI and RONI. The method divides the ROI into 8 × 8 pixel blocks and RONI into 6 × 6 pixel blocks. A mapping between the ROI and RONI blocks is constituted, and LSBs of the ROI blocks are embedded into corresponding RONI blocks to realize the recovery. The method uses approach in [5] to detect the tampered regions. The second method in their work compresses LSBs of the ROI blocks with run length encoding scheme before embedding. PSNR for watermarked images is not reported in their work.

In 2011, Memon et al. embeds the watermark information into LSBs of the ROI portion by using fragile watermarking [11]. RONI portion of the image is divided into $N \times N$ pixel blocks, and then, embeddable blocks are determined. Location map of these blocks and a robust watermark are embedded into blocks on the RONI using integer wavelet transform (IWT). LSB replacement is applied on the LL3 subband of the blocks to hide the location map for recovery purposes. After the embedding procedure, ROI and RONI portions are combined to form the watermarked image. Robust watermark in RONI is used for tamper detection. Their results indicate that WPSNR value of the watermarked image is approximately 59 dB.

Tan et al. construct the first layer watermark from source information and location information in encrypted form [12]. The second layer watermark accommodates the cyclic redundancy check (CRC) values of all blocks in the medical image. CRC values are used for tamper detection.

In 2012, Tjokorda et al. collected the LSBs of all pixels in medical image and altered them with zero value [13]. ROI and RONI regions after the modification are divided into 6 × 6 and 6 × 1 pixel blocks, respectively. Original LSBs are compressed with RLE scheme, and result string is embedded into blocks on RONI. The algorithm proposed by [5] is used for tamper detection at the receiver side. Experimental results show that watermarked images have approximately 47 dB PSNR.

Deng et al. used reversible watermarking technique in their work [14]. Their method also takes the advantage of quadtree decomposition. The image is divided into blocks by using quadtree decomposition. Linear interpolation of pixels is embedded into the image via invertible integer transformation. The second watermark is constructed using quadtree information and embedded with LSB technique. At the receiver's side, the embedded watermark is extracted and the original image is reconstructed because the technique has used reversible embedding approach during watermarking. Linear interpolation of the pixels is again calculated and compared with extracted ones. Thus, tampering detection and localization will be achieved.

Eswaraiah et al. segments the medical image into three parts: ROI, RONI, and border pixels in 2014 [15]. Secure hash algorithm is used to extract the hash of ROI. ROI and RONI parts of the medical image are divided into 4 × 4 and 8 × 8 pixel blocks, respectively. A mapping scheme is constructed between ROI and RONI, and it collects ROI block pixels and embeds them into corresponding RONI block with LSB replacement technique. A key encrypts hash value and information of ROI. Border pixels are used for hiding the encrypted bits. Information of ROI and hash value are used for tamper detection. Watermarked medical image is divided into ROI and RONI portions using the extracted ROI information. Hash value of ROI is calculated and compared with extracted one. If there exists a mismatch, block-based search is realized. Each ROI block is consulted using the corresponding RONI block to detect the absence of any modification. PSNR of the watermarked medical images with different modalities is in [50–55] decibel range.

The method explained in [22] exploits two watermarking approaches based on slantlet transform (SLT) to embed data. Their method used IWT coefficients to generate recovery information. ROI is divided into non-overlapping 16 × 16 pixel blocks. IWT is used to calculate average pixel intensities and recovery information from ROI blocks. These values are embedded into RONI using a robust irreversible technique. Reversible technique is used to embed EPR information into ROI. Two drawbacks of this method are as follows: It uses average information from 16 × 16 blocks to detect the tampered regions, and it must send some side information with watermarked medical image.

Eswaraih et al. uses IWT to watermark a medical image [23]. The medical image is segmented into ROI and RONI regions. IWT is used to embed hash of ROI, recovery information, and EPR into RONI. The disadvantages of the method are as follows: The coordinates of ROI and the size of watermark are sent to the other side as side information; authentication of ROI depends on hash function, and it can be applied to only medical images whose ROI size does not exceed 20% of the whole image.

Existing methods necessitate embedding extra information into medical images to ensure tamper detection [5–15]. Hiding extra information into medical image causes degradation in image quality. However, clarity of the medical image is important for medical personnel to prevent misdiagnosis. The novelty of the proposed method is that it does not necessitate embedding any information into medical image and hence does not deteriorate image quality. The proposed method uses a new passive image authentication method to determine tampered areas without hiding extra information into the medical image. The method extracts texture information of the medical image by LBPROT and then extracts SIFT keypoints from textured medical image. However, SIFT does not work well on smooth regions that are encountered in most of the medical images. That is why LBPROT operator is used before keypoint extraction. Matched SIFT keypoints designate the tampered regions.

## Proposed Method

The details of the proposed method are presented in this section. Tampered regions in the medical image are detected in three steps: extraction of the statistical and structural texture information from the image using LBPROT, detection of the SIFT keypoints from the LBPROT image, and matching the keypoints to detect tampered regions. General framework of the method is also given in Fig. 2. The details of the method are given in the subsections below.

### Extraction of the Statistical and Structural Texture Information

The proposed method is a passive image authentication mechanism. Passive image authentication methods in the literature can be divided into two groups: block-based and keypoint-based methods. Keypoint-based methods have gained popularity recently compared to block-based methods because they are invariant to rotation, translation, and scaling. However, both methods have a major vulnerability. Both techniques do not work properly if one copies a smooth region of the image and pastes it on another region to hide a clue as a forgery. Since block-based methods divide input image into overlapping blocks and use threshold to judge similarity among group of blocks, large number of similar group of blocks (e.g., two groups of blocks corresponding to sky in the image) must be ignored to deal with false negatives. Therefore, these methods cannot detect forgery if forged region is smooth or have no texture. Likewise, keypoint-based authentication methods cannot detect smooth forged regions because keypoint extraction algorithms extract keypoints from complex regions.

In this work, structural texture information from the medical image is extracted as the first step to use keypoint extraction methods on them. Seemingly smooth regions of images also have a texture (due to sensor and/or quantization noise), and the proposed method reveals the structure of these regions by using the LBPROT operator. Thus, keypoint extraction algorithms can obtain keypoints from the textural information of the image.

LBPROT, the rotation invariant version of the basic LBP operator [16], is used to extract the texture information from input image in this work. LBP operator computes binary difference of center pixel and its neighbors in each block as shown in Fig. 3.

Generic LBP has no restriction on the number of sampling points and size of the neighborhood. Ojala et al. proposed a generalized version of LBP after years [16]. Assume that gray-level image denoted by $I$ and a pixel at $x$th row and $y$th column denoted by $i_c = I(x, y)$. Circular neighborhood of point $(x, y)$ with evenly spaced $P$

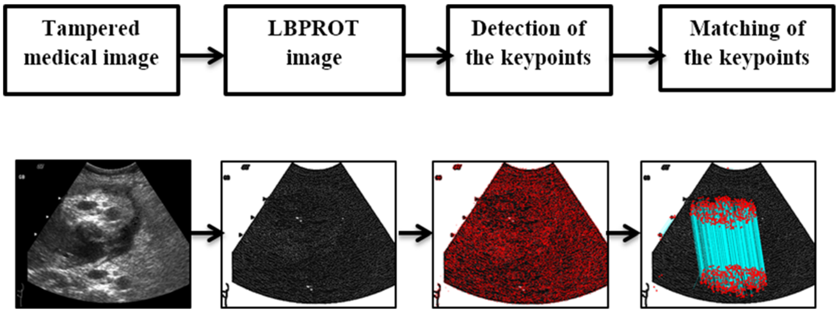


**Fig. 2** General framework of the proposed method

sampling points and radius $R$ will be used. Circular neighborhood examples for eight sampling points with various $R$ values are given in Fig. 4. Let any point $i_p$ denote the gray value of sampling point from the $P$ points. Sampling point at $(x, y)$ will be calculated as in (1). The proposed method uses circular neighborhoods and radial filter to allow the choice of any radius $R$. Circular neighborhood of point $(x, y)$ with evenly spaced eight sampling points and radius $R$ will be used in this work.

$$\begin{aligned} i_p &= I\left(x_p, y_p\right), p = 0, \cdots, P-1 \\ x_p &= x + R\cos(2\pi p/P) \\ y_p &= y - R\sin(2\pi p/P) \end{aligned} \tag{1}$$

Assume that $s(t)$ is the unit step function. If $t \geq 0$, the function returns one; otherwise, it returns zero. Using the unit step function, LBP value of a point with radius $R$ and eight sample points can be calculated as in (2).

$$\mathrm{LBP}\left(x_p, y_p\right) = \sum_{p=0}^{7} s\left(i_p - i_c\right) 2^p \tag{2}$$

LBP patterns of regions rotate about their center if a region from an image is rotated before pasting it on another region. The proposed method uses LBPROT operator to improve performance under rotation attack. LBPROT operator is defined as in (3). ROR$(x, i)$ denotes circular bitwise right rotation of bit sequence $x$ by $i$ steps.

$$\mathrm{LBP}^{ri}_{x_p, y_p} = \min_i \mathrm{ROR}\left(\mathrm{LBP}\left(x_p, y_p\right), i\right) \tag{3}$$

LBPROT operator chooses the minimum LBP code among the results of circular bitwise operations. Minimum LBP code, $\mathrm{LBP}^{ri}_{x_p, y_p}$, is used to label center pixel of the current 3 × 3 block. Figure 5a shows the medical image, and Fig. 5b, c denotes the tampered medical image and its LBPROT image, respectively.

In this step of the algorithm, the method extracts rotation invariant texture information from the medical image. Thus, smooth regions are textured, and the proposed method can apply keypoint extraction algorithms on the textured image to detect smooth region forgery operations. However, the method must normalize medical image into 0–255 range before it applies texture extraction algorithm. Table 1 shows that a medical image can have various modalities. Therefore, the method must normalize it before LBPROT operation. Medical images have textural information because of their nature. Thus, texture extraction from them before the keypoint extraction algorithm enhances accuracy of the method. The next section will extract keypoints on the LBPROT image to detect tampered regions.

## Keypoint Extraction from LBPROT Image

The proposed method extracts keypoints from the LBPROT image using scale invariant feature transform proposed by Lowe et al. in 2004 [17]. Scale-space extrema detection, keypoint localization, orientation assignment, and determination of the keypoint descriptors are the steps of the SIFT.

First, scale space is constructed to detect the local interest points called keypoints. Potential keypoints are searched over all scales. Variable scale Gaussian function $G(x, y, \sigma)$ convolved with an input image $I(x, y)$ to construct the scale space function. Scale space of an image $L(x, y, \sigma)$ is calculated as in (4).

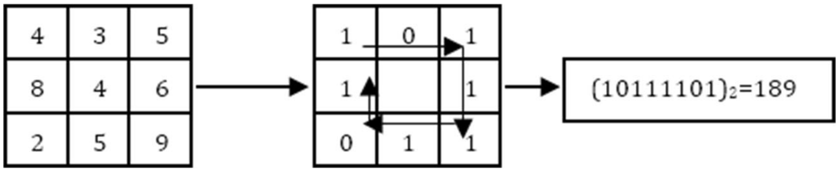


**Fig. 3** An example of basic LBP operator

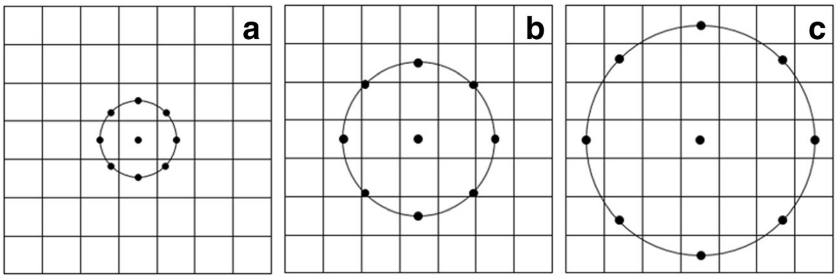


**Fig. 4** Circular neighborhood examples for eight sampling points with various *R* values. **a** LBP(8, 1). **b** LBP(8, 2). **c** LBP(8, 3)

$$L(x,y,\sigma) = G(x,y,\sigma)^{*}I(x,y) \qquad G(x,y,\sigma) = \frac{1}{2\pi\sigma^2}e^{-\left(x^2+y^2\right)/2\sigma^2} \tag{4}$$

The difference between two nearby scaled images separated by a multiplicative factor *k* is convolved with the image *I*(*x*, *y*) as in (5) to extract stable keypoint location.

$$D(x,y,\sigma) = (G(x,y,\mathrm{k}\sigma) - G(x,y,\sigma))*I(x,y) = L(x,y,k\sigma) - L(x,y,\sigma) \tag{5}$$

Simple image extraction is used to compute *D*. Figure 6 shows an example of images at different scales. The initial image is convolved with Gaussian function to create the scale space images in each octave. Difference of Gaussian (DoG) images are calculated by subtracting corresponding adjacent Gaussian images. Scale space images and DoG images are shown in Fig. 6 at left and right, respectively. The Gaussian image is down sampled by a factor of 2 after each octave.

Keypoint localization is the next step during the algorithm. Extrema points in the DoG pyramid is detected in this step. Each point in *D* is compared with its eight neighboring pixels and nine pixels in neighboring scales. If the center value is the minimum or maximum, this point is an extrema and it is a potential keypoint. Keypoints obtained by the algorithm are denoted by $X = \{x_1, \cdots, x_n\}$.

Then, localization of keypoints is improved to subpixel accuracy using second-order Taylor series expansion. Keypoints are rejected if the intensity at any extrema is less than a threshold. Edge points are also eliminated in this stage. As a result, key point localization algorithm eliminates low-contrast keypoints and edge keypoints.

Each keypoint is assigned to an orientation to achieve rotation invariance. A neighborhood of each keypoint is taken according to scale to judge the orientation. Gradient magnitude and direction is calculated in that neighborhood. Assume that blurred image in that scale be *L*. Gradient magnitude *m* and orientation *θ* are calculated by the following Eq. (6), respectively. One or more orientation assignment to each keypoint is realized using the neighborhood pixels.

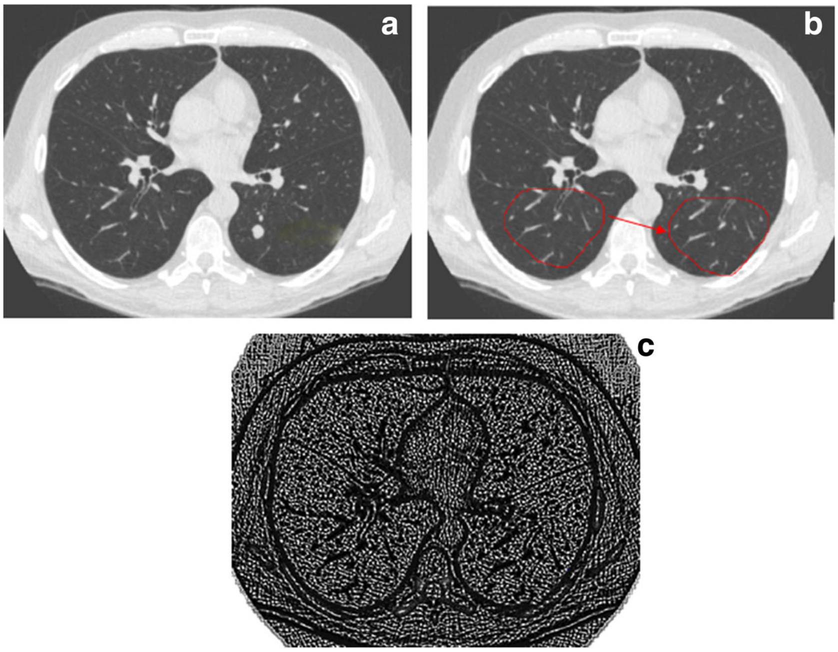


**Fig. 5** **a** Medical image. **b** Tampered medical image. **c** LBPROT image of **b**

**Table 1** Medical image dimensions and bit depth for various image modalities [21]

| Modality | Image dimension (pixels) | Gray level (bits) | Avg. size/exam (Mbytes) |
|---|---|---|---|
| Nuclear medicine (PET, SPECT) | 128 × 128 | 12 | 1–2 |
| Magnetic resonance imaging | 256 × 256 | 12 | 8–20 |
| Ultrasound | 512 × 512 | 8 | 5–10 |
| Computed tomography | 512 × 512 | 12 | 20–40 |
| Spiral or helical CT | 512 × 512 | 12 | 80–160 |
| Digitized electronic microscopy | 512 × 512 | 8 | Varies |
| Digitized color microscopy | 512 × 512 | 24 | Varies |
| Digital subtraction angiography (per run) | 512 × 512 or 1024 × 1024 | 8 | 100–500 |
| Digitized X-rays | 2048 × 2048 | 12 | 8 |
| Computed radiography | 2048 × 2048 | 12 | 8 |
| Digitized mammography | 4096 × 4096 | 12 | 128 (4 images) |

$$
\begin{aligned}
m(x,y) &= \sqrt{(L(x+1,y)-L(x-1,y))^2 + (L(x,y+1)-L(x,y-1))^2} \\
\theta(x,y) &= tan^{-1}\Big((L(x,y+1)-L(x,y-1))\Big/(L(x+1,y)-L(x-1,y))\Big)
\end{aligned}
\tag{6}
$$

Keypoint descriptors are created as the last step. A 16 × 16 pixel neighborhood around the keypoint is taken, and this region is divided into 4 × 4 pixel sub-blocks. Eight-bin orientation histogram is constructed

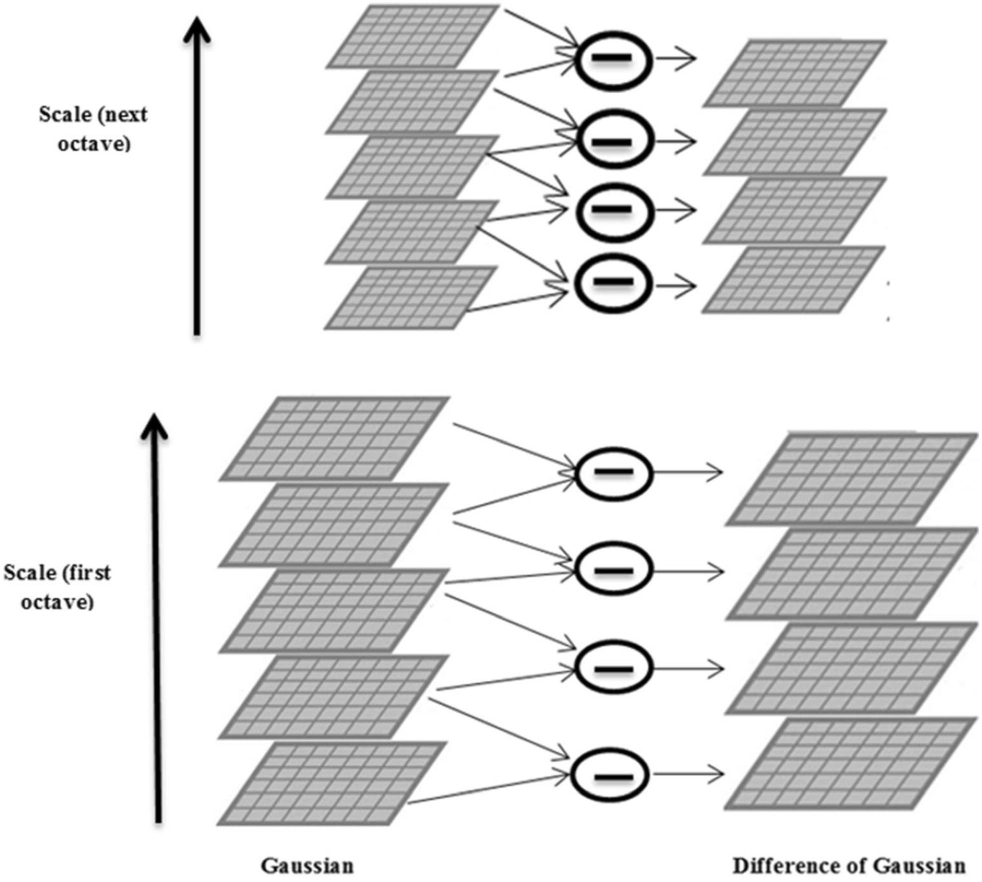


**Fig. 6** Images at different scales and DoG images

for each subblock. One hundred twenty-eight bin values are obtained from all subblocks, and they are represented as a vector to form keypoint descriptor $\{f_1, \cdots, f_n\}$.

### Matching Keypoints to Determine Tampered Regions

In this step of the algorithm, keypoint descriptor vectors are processed to find matches corresponding to similar regions. Best candidate keypoints are determined for each key point $x_i$ by inspecting other keypoint descriptor vectors. The method does not use comparison test on the Euclidian distance with a global threshold to decide the similarity of any two keypoints as suggested by [18] because some descriptors are much more discriminative from the others. The proposed method uses the approach defined in [18] to judge similar keypoints. Keypoint matching algorithm defined by Amerini et al. is applied for a keypoint descriptor as explained below.

1. Dot products are calculated between current keypoint descriptor and the others, $\{d_1 \cdots d_n\}$.
2. Dot product angles are computed by inverse cosine and then sorted, and dot product values and their corresponding indexes are stored.
3. The ratio of two neighbors,$(d_i, d_{i+1})$ is compared with a predefined threshold $t$ until the ratio is greater than $t$. Assume that the procedure stops at $k$th index; keypoints corresponding to $\{d_i \cdots d_{i+k}\}$ are considered as match for the current keypoint. We set $t$ value to 0.5 as suggested by [18].

The procedure defined above is applied to all keypoints in $X$. Matched keypoints designate forged regions and provide information about the authenticity of the image.

## Experimental Results

This section introduces the contents of medical image dataset to test and metrics used to evaluate the performance of the proposed method. Effectiveness and robustness tests are given, in turn, to demonstrate improved forgery detection of the method.

### Dataset and Evaluation Metrics

Experiments are realized on the dataset that was created by our research group. The dataset contains 420 Gy level tampered medical images with varying modalities (rotating, scaling, blurring, AWGN). The following scenarios are applied on the original medical images gathered from the Internet and [20] to create the tampered images.

- A region/multiple region from the medical image is copied and pasted into another region/regions on the same image. Fifty-eight tampered medical images are created in this way.
- A portion of the medical image is copied and then rotated with degrees of [20, 90, 180, 220]. Rotated portion is then used for concealing or duplicating purposes. Forty-eight tampered medical images are created with rotation attack.
- Resizing operation with scaling factors between 80, 90, 110, and 120 on the copied regions before pasting. Fifty-nine tampered medical images are created by this way.
- Gaussian blurring operation is applied on the 58 tampered medical image with the following parameters ($w = 5$ and $\sigma$ is in the range of 1.5–3)
- AWGN is applied on the 58 tampered medical images with SNR values of 30 and 60 dB.

Tamper detection capability of the proposed method for a $N \times M$ test image is evaluated using a metric called by detection ratio (DR) given in (7). The first part of the metric is the ratio of matched keypoints inside tampered regions, $K_F$, to the total number of pixels, $F$, that reside on those regions. The second part is the ratio of the number of matched keypoints that are not on the forged regions, $K_B$, to the total number of pixels excluding the forged regions, $B$. Independence from image size is ensured by multiplying these metric by $NM/100$. Higher DRs correspond to better accuracy in detecting tampered regions.

$$\mathrm{DR} = \left(\frac{K_F}{|F|} - \frac{K_B}{|B|}\right)\frac{NM}{100} \tag{7}$$

Since the method employs LBPROT operator before extracting keypoints by SIFT to detect tampered regions in medical images, radius of the LBPROT operator $R$ should be carefully selected to maximize DR. In order to find the optimum radius of the LBPROT operator, average DR of the proposed method for $R$ values from 1 to 4 on the test dataset is calculated. A bar graph of average DR as a function of radius $R$ is given in Fig. 7. This experiment proved that the method yields higher average detection ratios for radius value of 3.

Three different scenarios given below are applied to show the superiority of the method. The first two scenarios are implemented to make a comparison between two popular keypoint extraction algorithms (SIFT and SURF) and to show the reason of preferring SIFT in the proposed method. We implement the third scenario to test the success of the SURF method on the texture information.

Scenario 1: SIFT is applied on the tampered medical image to extract keypoints, and keypoint matching algorithm is used to detect tampered regions.

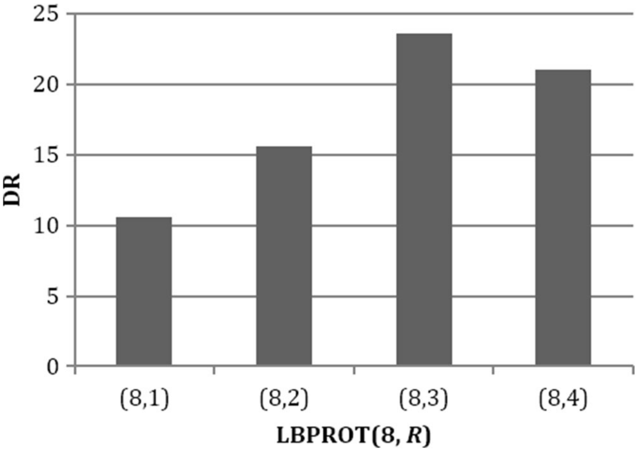


**Fig. 7** Comparison of the DR for various *R* values 1 to 4

Scenario 2: SURF is applied on the tampered medical image for keypoint extraction different from the previous scenario [19].

Scenario 3: LBPROT operator is used to extract structural information from the tampered image, and then, SURF algorithm is used to extract keypoints.

The proposed method is compared with scenarios described above to show both effectiveness and robustness of the proposed method.

## Effectiveness Test

In this set of experiments, two different types of attacks are applied on the medical image to create the tampered versions: simple and multiple attacks. Figure 8b is an example of a simple attack. A region with a tumor on the mammogram image given in Fig. 8a is covered by another region from the same image to create the tampered image given in Fig. 8b. Border smoothing is also applied during forgery to hide the clues on the peripheral of the covered area. The numbers of matched keypoints on the tampered regions for three scenarios are 19, 26, and 43, and the total numbers of keypoints detected by these scenarios are 886, 816, and 2059, respectively, as can be seen in Fig. 8c–h. Figure 8h shows that the third scenario detects more matched keypoints on the forged regions. However, the proposed method finds 3791 keypoints on the tampered image and matches 121 of them as can be seen in Fig. 8i, j. Other scenarios find less matched keypoints on the forged regions. Figure 8j also shows that the method detects tampered regions with more matched keypoints compared to other scenarios.

Multiple attack is used to create more than one forged regions on the medical image. Tumor region on the mammogram image is copied and pasted on the other two regions on the same image as indicated by the red arrows to create the tampered one given in Fig. 9a. The total matched keypoints and keypoints for three scenarios are (14, 16, 3) and (470, 769, 2667), respectively, as given in Fig. 9b–g. The proposed method extracts 4868 keypoints from the tampered medical image as shown in Fig. 9h and matches 57 of them. Figure 9i indicates that the proposed method detects more keypoints on the forged regions.

In this section, the results show that effectiveness test results for the proposed method are better than the three scenarios defined above. Structural texture information causes the increase on the number of keypoints and matched keypoints as shown in the results. The method detects more keypoints on the forged regions.

## Robustness Test

The capability of the proposed method is also tested against some attacks: rotation, scaling, blurring, and noise addition. Results of the proposed method and the three other scenarios are given in this section, respectively.

Brain MR image given in Fig. 10a is used as a test image for rotation test. Tumor region on the image is covered by another region on the same image as can be seen in Fig. 10b. However, copied region is rotated 30° clockwise before it is pasted. Border smoothing is also applied on the forged regions to hide clues of forgery. Results of the three scenarios are also given below of each corresponding image. The number of matched keypoints and the number of total keypoints for these scenarios are (0, 4, 0) and (531, 691, 2197), respectively. The proposed method detects 111 keypoints on the tampered region, while other methods cannot detect more than 4 keypoints. Visual results (Fig. 10c–j) show the intensity of the keypoints on the forged regions. The proposed method reveals the forged region with more matched keypoints. The most important advantage of the method becomes visible in this experiment. When the forgery operation hides a portion of the image with a smooth region, other methods do not find any keypoints in tampered regions or they detect a few keypoints outside tampered regions.

The second experiment scaled the copied region before it is pasted. A portion from the ultrasound image given in Fig. 11a is scaled 120% and then used to cover the cystic component on the same image. Red arrows given in Fig. 11b indicate the forged region. Figure 11c, e, g shows that the three scenarios detect 1559, 2325, and 5967 keypoints, respectively. These scenarios as shown in Fig. 11d, f, h match 32, 59, and 2 of them. However, the proposed method finds 10,668 keypoints on the tampered medical image and matches 260 of them as given in Fig. 11i, j. Even though LBPROT with SURF algorithm finds 5967 keypoints, it is unsuccessful in this experiment, because it cannot match even one of them. The second scenario using only SURF is more successful than the other two; however, the proposed method finds approximately four times as many as keypoints compared with it.

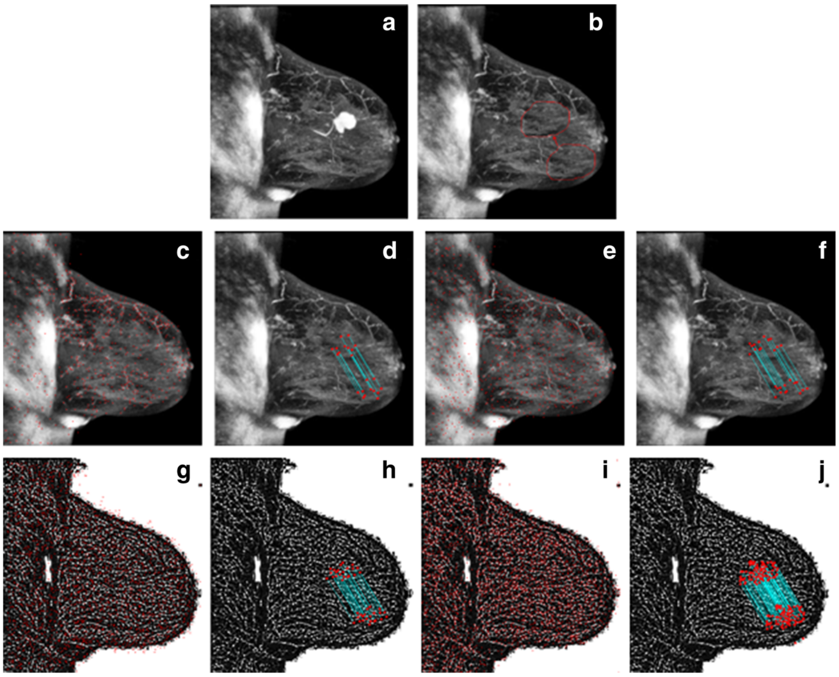


**Fig. 8** **a** Medical image. **b** Tampered medical image. **c**, **d** The result of scenario 1: SIFT-based method (total keypoints 886, matched keypoints 19). **e**, **f** The result of scenario 2: SURF based (total keypoints 816, matched keypoints 26). **g**, **h** The result of scenario 3: LBPROT + SURF based (total keypoints 2059, matched keypoints 43). **i**, **j** The result of the proposed method (total keypoints 3791, matched keypoints 121)

Blurring operation is used in the third experiment to blur the tampered medical image. Figure 12a shows the tampered image after Gaussian blurring with $w$ = 5 and $\sigma = 3$ parameters. The total numbers of keypoints detected by the three scenarios are 267, 583, and 1864, respectively, as given in Fig. 12b, d, f. The numbers of matched keypoints are given in Fig. 12c, e, g as 27, 50, and 26, respectively. The proposed method detects 2485 keypoints on the tampered image, and 84 of them are matched by the method as shown in Fig. 12i. The second scenario (that uses only SURF) finds the best result

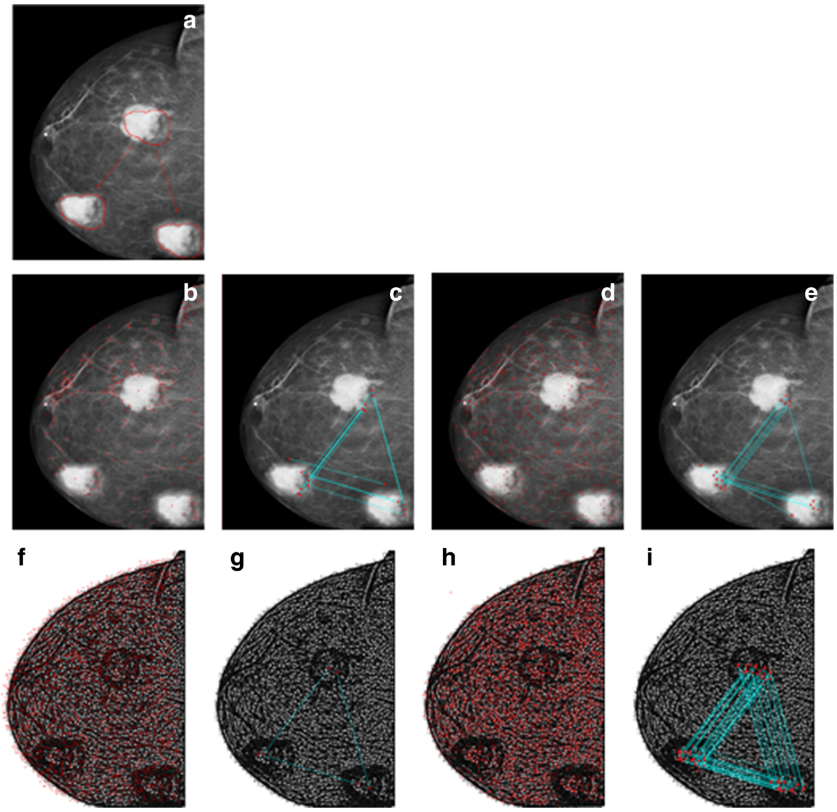


**Fig. 9** **a** Tampered medical image. **b**, **c** The result of scenario 1: SIFT-based method (total keypoints 470, matched keypoints 14). **d**, **e** The result of scenario 2: SURF based (total keypoints 769, matched keypoints 16). **f**, **g** The result of scenario 3: LBPROT + SURF based (total keypoints 2667, matched keypoints 3). **h**, **i** Proposed method (total keypoints 4868, matched keypoints 57)

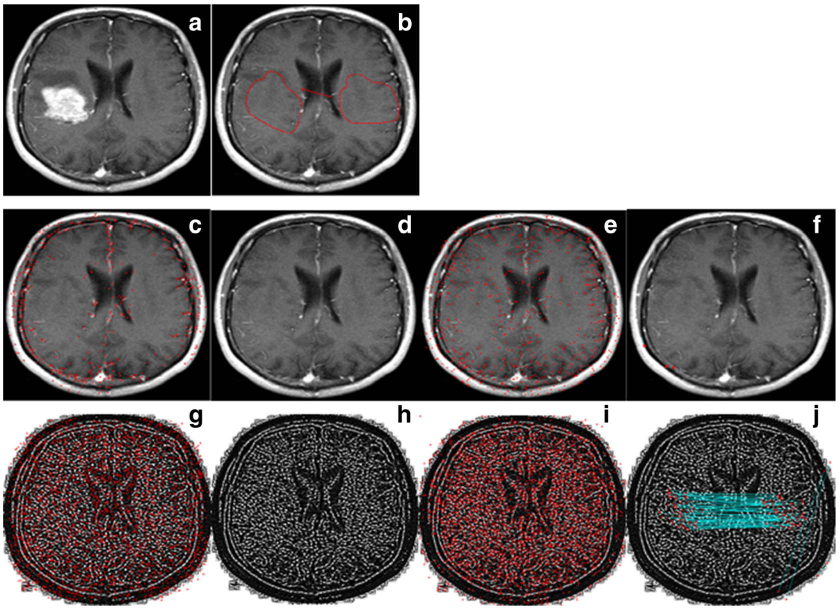


**Fig. 10** **a** Medical image. **b** Tampered medical image. **c**, **d** The result of scenario 1: SIFT-based method (total keypoints 531, matched keypoints 0). **e**, **f** The result of scenario 2: SURF based (total keypoints 691, matched keypoints 4). **g**, **h** The result of scenario 3: LBPROT + SURF based (total keypoints 2197, matched keypoints 0). **i**, **j** Proposed method (total keypoints 3958, matched keypoints 111)

according to the number of keypoints compared to the other two scenarios. However, the proposed method finds more keypoints on the forged regions compared with it.

Additive white Gaussian noise is applied on the tampered medical image to test the robustness of the method against noise addition. Medical image given in Fig. 13a is modified, and 30 dB noise is added on tampered image to hide tampering clues as shown in Fig. 13b. The proposed method detects 4730 keypoints and matched 194 of them as shown in Fig. 13i, j. The other scenarios detected less keypoints on the forged region as shown in the visual results (Fig. 13d, f, h). The third scenario that uses LBPROT with SURF yields the worst result according to the number of keypoints. The second scenario shows priority compared to other ones. But the proposed method finds 28 more keypoints on the forged regions of the image.

When we evaluate the three scenarios, the third scenario exhibits the worst robustness results and the second scenario that uses only SURF gives the best robustness. On the other hand, the proposed method detects more keypoints on the forged regions compared to the other three scenarios for all tests especially rotation and scaling attacks. From these

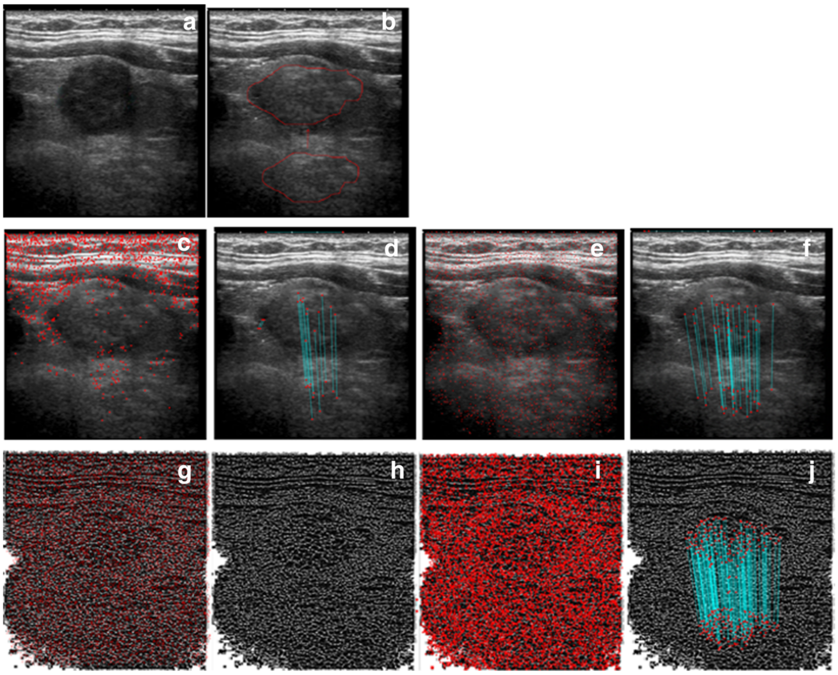
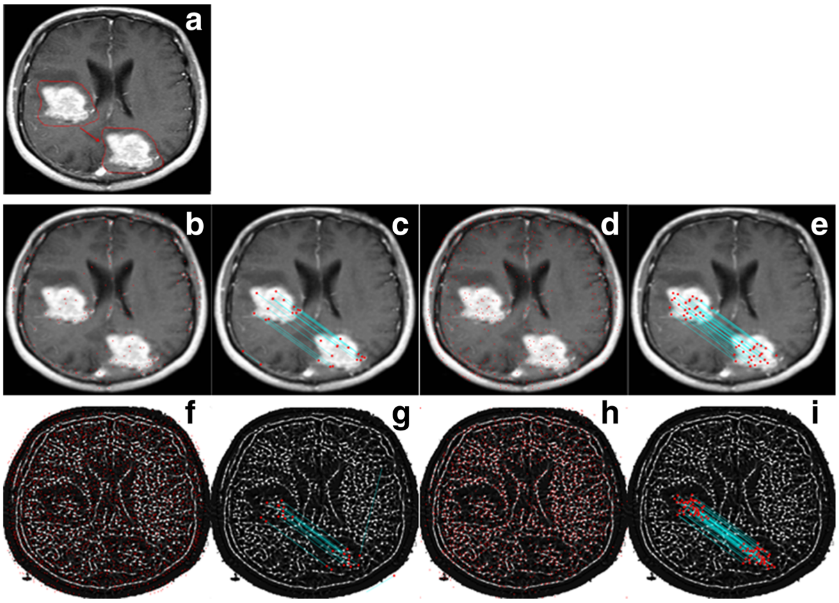


**Fig. 11** **a** Medical image. **b** Tampered medical image. **c**, **d** The result of scenario 1: SIFT-based method (total keypoints 1559, matched keypoints 32). **e**, **f** The result of scenario 2: SURF based (total keypoints 2325, matched keypoints 59). **g**, **h** The result of scenario 3: LBPROT + SURF based (total keypoints 5967, matched keypoints 2). **i**, **j** Proposed method (total keypoints 10,668, matched keypoints 260)

Fig. 12 **a** Tampered medical image. **b**, **c** The result of scenario 1: SIFT-based method (total keypoints 267, matched keypoints 27). **d**, **e** The result of scenario 2: SURF based (total keypoints 583, matched keypoints 50). **f**, **g** The result of scenario 3: LBPROT + SURF based (total keypoints 1864, matched keypoints 26). **h**, **i** Proposed method (total keypoints 2485, matched keypoints 84)



experiments, extracting structural texture information with LBPROT and keypoint extraction/matching with SIFT yield improved detection of tampered region(s) in medical images.

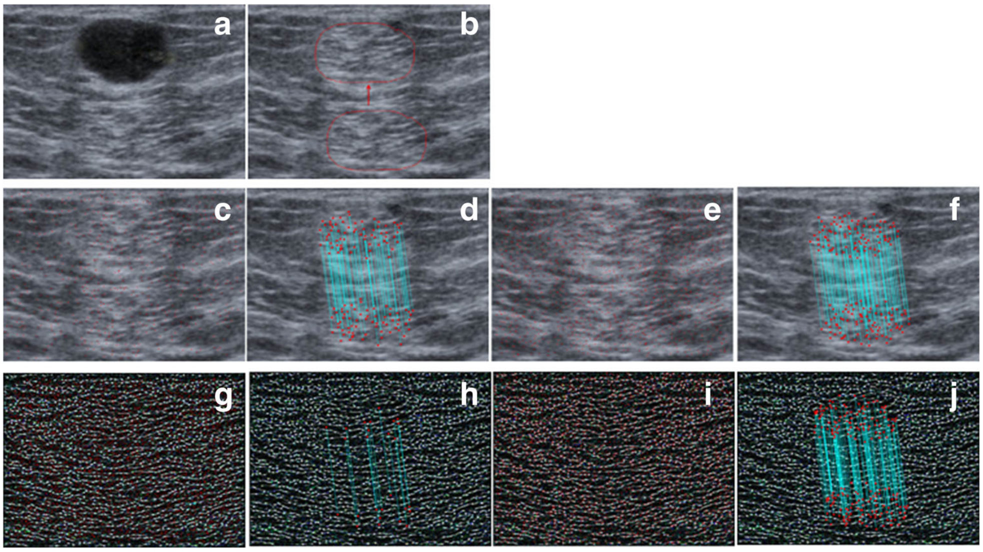
In the last experiment in this section, we give the result of the proposed method for medical image with symmetric properties. In this experiment, we investigate the effectiveness of the keypoint-based method on the medical image with symmetric properties. Figure 14a, b gives the original medical images. Detection results of the proposed method for the medical images with symmetric properties show that keypoint-based method cannot reason the false positives. Figure 14c, d indicates that the proposed method does not match the symmetric region because it uses pattern information of the medical image. Pattern is different even if the regions contain symmetric nature.

## Comparison Tests

In the last experiment, the method is compared with the three other scenarios described before in this section. Many tampered medical images (the details of the test set are given in "Dataset and Evaluation Metrics" section) are used during the tests to determine average detection ratio of the proposed method and the three other scenarios. Higher detection ratio indicates more matched keypoints in forged regions and hence the reliability of detection. A higher DR value in a test corresponds to a higher detection capability of a method.

In the first test, the proposed method and others are evaluated on the tampered medical images without any post-processing operations given in "Dataset and Evaluation Metrics" section. Average detection ratios of the methods for

Fig. 13 **a** Medical image. **b** Tampered medical image. **c**, **d** The result of scenario 1: SIFT-based method (total keypoints 784, matched keypoints 130). **e**, **f** The result of scenario 2: SURF based (total keypoints 1469, matched keypoints 166). **g**, **h** The result of scenario 3: LBPROT + SURF based (total keypoints 3043, matched keypoints 20). **i**, **j** Proposed method (total keypoints 4730, matched keypoints 194)



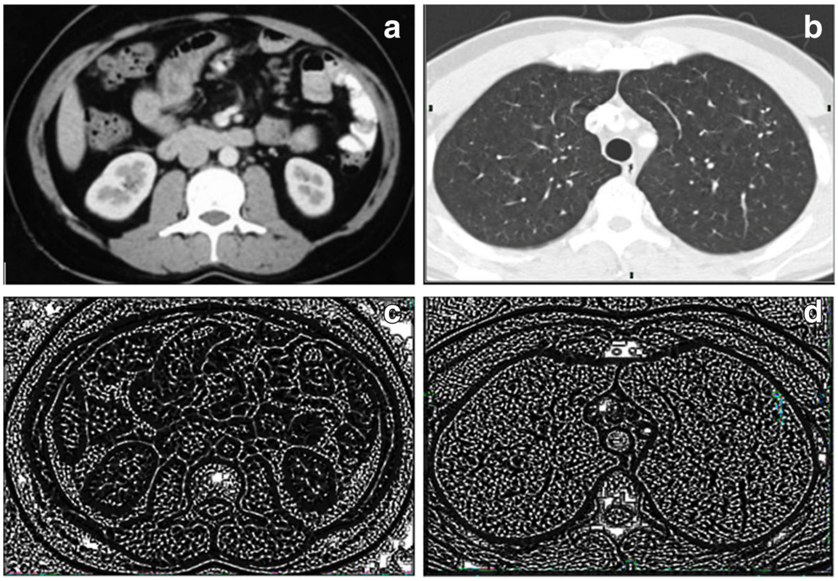


**Fig. 14** **a**, **b** Original medical images with symmetric properties. **c**, **d** Detection results of the proposed method for these images

58 test images are calculated and plotted in Fig. 15a. The proposed method has a DR of approximately 46.8. SURF-based, LBPROT + SURF, and SIFT-based scenarios yield approximately 22.06, 16.03, and 10.11 of DR, respectively. The experiment shows that the method detects more keypoints in forged regions compared to other scenarios. Among the three scenarios, SURF based yields the best result. However, the proposed method finds nearly hundred times more keypoints in forged regions compared to SURF-based scenario. The first test clearly indicates that the method has higher detection ratio compared to other keypoint-based methods.

We also test the robustness of the proposed method compared to other scenarios for post-processed tampered medical images and rotated/scaled forged regions. Results of the robustness experiments are summarized below.

AWGN is used on tampered medical images in the dataset as the first experiment for the robustness test. Thirty decibel and 60 dB signals are used to hide the clues of the forgery operations on the tampered medical images. Figure 15b shows average DR of the method and other scenarios. The method yields higher average DR compared to others as shown in the bar chart. Average DR for the proposed method is

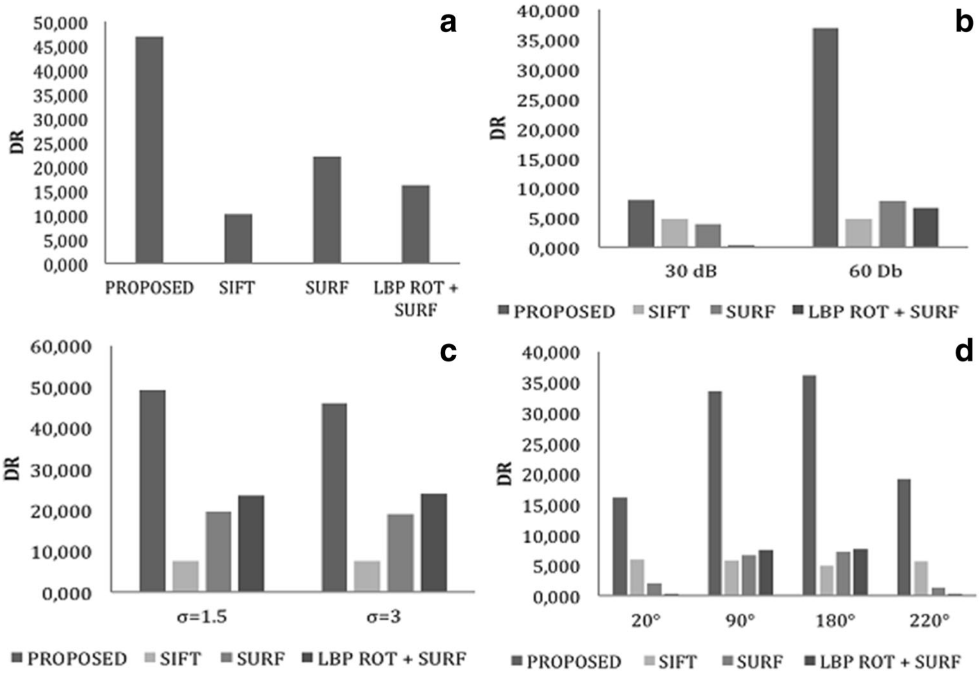


**Fig. 15** Comparison test results. **a** Simple attack. **b** Noise addition attack. **c** Gaussian blurring attack. **d** Rotation attack. **e** Scaling attack

approximately 7.8, if tampered images are distorted with 30 dB AWGN. SIFT-based method has the best result of the three scenario after the proposed method with approximately 4.8 DR. However, for 60 dB AWGN, SURF-based method becomes second best with approximately 7.7 DR after the proposed method with 36.86 DR. The third scenario is unsuccessful for even with 30 dB AWNG where the proposed method yields higher DR compared to the others. The method also has higher DR for 60 dB AWGN as shown in Fig. 15b.

One of the most common post-processing operations is blurring with a kernel which removes artifacts on the tampered region boundaries. Another robustness test is realized for blurring tampered images with a Gaussian kernel of window size 5 and $\sigma = 1.5$ and 3. The proposed method has higher DR compared to the three other scenarios. The third scenario (LBPROT + SURF) has approximately a DR of 23 for two conditions, and DRs of 49.29 and 46.05 are obtained by the proposed method for the same blurred images as shown in Fig. 15c. The figure indicates that the proposed method detects 100 times more keypoints in forged regions compared to the third scenario. The other two scenarios (SIFT based and SURF based) have approximately DRs of 7 and 19, respectively, and have worse results compared to the proposed method.

Another test is performed for 48 tampered images where the forged region is rotated before pasting as given in "Dataset and Evaluation Metrics" section. This experiment provides a closer look to the capabilities of the scenarios under rotation operation. Figure 15d shows DRs for rotation 20°, 90°, 180°, and 220°. SURF-based two scenarios yield better results for 90° and 180°. However, the first scenario (SIFT based) is more successful than the other two for 20° and 220°. The proposed method gives higher DRs compared to others regardless of the rotation angle. It yields 16.06, 33.48, 36.15, and 19.07 DRs for 20°, 90°, 180°, and 220°, respectively. DRs for 90° and 180° are higher than that of 20° and 220°. On the other hand, the method has the best results compared to others for all rotation angles.

In the last experiment, 59 test images are created by scaling copied regions by 80, 90, 110, and 120% before pasting to test the robustness of the method against scaling. Figure 15e shows average DRs for all methods with 59 test images. The figure indicates that the proposed method yields higher average DR compared to others for scaling. While the proposed method has approximately 6.2 DR for scaling 80%, the others have approximately 0.9, 0.2, and 0 DRs, respectively. The difference between DRs becomes more noticeable for scaling 90 and 110%. DR of the proposed method decreases for 120% scaling compared to 80%. However, the other methods have still approximately a DR of 1 for all scaling operations.

In this section, average DRs of the proposed method and the three other scenarios are reported for various post-processing operations performed to hide forgery clues. Results show that the method has higher DR compared to the others.

## Conclusion

Region duplication or region covering attacks is possible on medical images, and passive authentication mechanisms can detect tampered regions created by these attacks. A novel passive image authentication scheme is proposed for tampered medical image detection in this work. It eliminates the need to embed a watermark during or after image capture as in active authentication methods. Watermarking techniques use either ROI or keypoint-based approaches. Since keypoint-based techniques make use of structural information such as image texture, they cannot detect forgery on the smooth regions mostly encountered in medical images. The proposed method is based on keypoint selection and uses LBPROT before SIFT to emphasize texture information. LBPROT extracts texture information from medical images with seemingly smooth regions. Thus, keypoint extraction algorithms are applicable on the structural information and extract keypoints from the structural information of the smooth regions. Thus, one of the most important disadvantages of the keypoint-based passive authentication mechanisms reported in the literature is eliminated by the proposed method.

### Compliance with Ethical Standards

**Competing Interests** The authors declare that they have no conflict of interest.

## References

1. Das S, Kundu MK: Effective management of medical information through ROI-lossless fragile image watermarking technique. Computer Methods and Programs in Biomedicine 111(3):662–75, 2013
2. Nyeem H, Boles W, Boyd C: A review of medical image watermarking requirements for teleradiology. J Digit Imaging 26(2):326–43, 2013
3. Arsalan M, Malik SA, Khan A: Intelligent reversible watermarking in integer wavelet domain for medical images. J Syst Softw. 85(4): 883–94, 2012
4. Fridrich AJ, Soukal BD, and Lukáš AJ: Detection of copy-move forgery in digital images. Proceedings of Digital Forensic Research Workshop 3(2):652–63, 2003
5. Zain JM, Fauzi AM: Medical image watermarking with tamper detection and recovery. Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE 1:3270–3, 2006
6. Wu JHK, Chang RF, Chen CJ, Wang CL, Kuo TH, Moon WK, et al: Tamper detection and recovery for medical images using near-lossless information hiding technique. J Digit Imaging 21(1):59–76, 2008

7. Chiang K-H, Chang-Chien K-C, Chang R-F, Yen H-Y: Tamper detection and restoring system for medical images using wavelet-based reversible data embedding. J. Digit. Imaging. p. 77–90, 2008
8. Al-Qershi OM, Khoo BE: Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images. Journal of Digital Imaging 24(1):114–25, 2011
9. Al-Qershi OM, Khoo BE: ROI-based tamper detection and recovery for medical images using reversible watermarking technique. 2010 I.E. Int Conf Inf Theory Inf Secur 151–5, 2010
10. Liew SC, Zain JM: Reversible medical image watermarking for tamper detection and recovery. Proc - 2010 3rd IEEE Int Conf Comput Sci Inf Technol ICCSIT 2010. p. 417–20, 2010
11. Memon NA, Chaudhry A, Ahmad M, Keerio ZA. Hybrid watermarking of medical images for ROI authentication and recovery. International Journal of Computer Mathematics. 2011; 88(10): 2057–71.
12. Tan CK, Ng JC, Xu X, Poh CL, Guan YL, Sheah K: Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability. J Digit Imaging. 24(3):528–40, 2011
13. Tjokorda Agung BW, Adiwijaya Permana FP: Medical image watermarking with tamper detection and recovery using reversible watermarking with LSB modification and run length encoding (RLE) compression. Proceeding - COMNETSAT 2012 2012 I.E. Int Conf Commun Networks Satell. p. 167–71, 2012
14. Deng X, Chen Z, Zeng F, Zhang Y, Mao Y. Authentication and recovery of medical diagnostic image using dual reversible digital watermarking. Journal of nanoscience and nanotechnology. 13(3), 2099–107, 2013.
15. Eswaraiah R, Sreenivasa Reddy E: Medical image watermarking technique for accurate tamper detection in ROI and exact recovery of ROI. Int J Telemed Appl. Hindawi Publishing Corporation; 2014; 2014:1–10. Available from: http://www.hindawi.com/journals/ijta/2014/984646/
16. Ojala T, Pietikäinen M, Mäenpää T: Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. IEEE Trans Pattern Anal Mach Intell. 24(7):971–87, 2002
17. Lowe G: SIFT, the scale invariant feature transform. Int J. Of Computer Vision, 60(2), 91–110, 2004
18. Amerini I, Ballan L, Caldelli R, Del Bimbo A, Serra G: A SIFT-based forensic method for copy-move attack detection and transformation recovery. IEEE Trans Inf Forensics Secur. 6(3 PART 2): 1099–110, 2011
19. Bay H, Tuytelaars T, Van Gool L SURF: speeded up robust features. Lect Notes Comput Sci (including Subser Lect Notes Artif Intell Lect Notes Bioinformatics). p. 404–17, 2006
20. Barre S 1999 Available at: http://www.barre.nom.fr/medical/samples/.
21. Ulutas M, Ulutas G, Nabiyev VV: Medical image security and EPR hiding using Shamir's secret sharing scheme, Journal of Systems and Software, 84, 3, 341–353, doi: 10.1016/j.jss.2010.11.928 , ISSN 0164-1212, 2011
22. Thabit R, Khoo BE: Medical image authentication using SLT and IWT schemes. Multimed Tools App 1–24,2015. Available from: doi: 10.1007/s11042–015-3055-x
23. Eswaraiah R and Sreenivasa Reddy E: Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest, IET Image Processing, 9, 8, pp. 615–625, 2015