International Journal of Engineering & Technology, 7 (4) (2018) 2137-2148

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.128554
Research paper

A novel approach to medical image watermarking for tamper detection and recovery of region of interest using block compression and checksum

K. Chaitanya [1] *, K. Gangadhara Rao [2]

[1] Assistant Professor, Dept. of CSE, ANU College of Engineering and Technology, Acharya Nagarjuna University, Andhra Pradesh, India
[2] Professor, Dept. of CSE, ANU College of Sciences, Acharya Nagarjuna University, Andhra Pradesh, India
**Corresponding author E-mail: anu.konda.chaitanya@gmail.com*

Abstract

Effective use of telecommunication and information technology in telemedicine increases the medical services to the patients who are from far away locations. The doctors provide these services by evaluating the patient details & scans like CT Scan, MRI and Ultra Sound. The patient information is exchanged between doctors and patients on a public network which is not safe. In medical image, specific regions are very important to diagnosis known as Region of Interest (ROI) and the rest of the regions are not of much importance known as Region of Non-Interest (RONI). Providing security to the ROI is an important issue hence medical image watermarking is used to transmit the medical images by embedding the ROI into RONI. At the destination, if tampering is found in ROI then recovery of ROI is possible by extracting the ROI from RONI. In the proposed method, the medical image is divided into three parts: BORDER, ROI and RONI. Further the ROI and RONI are divided into blocks and each ROI block is mapped to RONI block by applying division hash function. Lossless block compression technique is applied to each ROI block and embedded the compressed ROI block into mapped RONI block. To provide authenticity to ROI, checksum is calculated for ROI and embed this checksum in BORDER. Again checksum is calculated for each ROI block and placed in mapped RONI blocks. Whether ROI is tampered or not, is to be identified by extracting the checksum from BORDER and if it is tampered then recover the ROI by mapped RONI. The efficiency of the proposed algorithm is estimated by the performance measures mainly Peak Signal to Noise Ratio (PSNR). The proposed method gives good results on average 55 dB of PSNR compared to the previous methods [21] by efficiently compressing the ROI and by checking the authenticity.

Keywords: *Region of Interest; Region of Non-Interest; Division Hash Function; Lossless Block Compression; Checksum.*

1. Introduction

In recent days, diagnosing the patients from the far away locations is an important task performed by the doctors through transmission of patient information like patient details and patient scanned reports like CT Scan, MRI and Ultra Sound through internet. This is the main objective of telemedicine applications like teleconsulting and telediagnosis etc. During the transmission of patient details through public network there is a chance of tampering the data in the medical images by the unauthorized persons. Hence, the three security services must be implemented in telemedicine: authenticity, confidentiality and integrity. Therefore, transmission of medical images safely to the destination is an important task needed to perform for diagnosing the patient correctly [1], [2]. For the safe transmission of medical images, medical image watermarking is used [3].

Digital image watermarking is the process of embedding of the relevant information as watermark into the digital image for providing copyright protection, checking authenticity, detection of tampers in the image and recovery of tampered images [4]. Based on the perception of human, watermarking can be divided into visible and invisible watermarking. The watermark that is embedded into the image is visible, that is called as visible watermarking [5], [6]. Visible watermarking is useful for providing copyright protection to the owner. The watermark which is not visible even after embedding into the image is called invisible watermarking [7].Invisible watermarking is useful for copyright protection and authentication. Further invisible watermarking can be divided into fragile, semi-fragile, robust watermarking methods. In fragile watermarking, the watermark that is embedded into the image is sensitive on applying general operations like compression, adding noise, etc. This is suitable for checking the authenticity of ROI. In semi-fragile watermark, the watermark is survived for general operations and it is sensitive to the geometrical attacks. This method is suitable for content authentication [8]. In robust watermarking, the watermark is not removed from cover images after applying the general operations as well as geometrical attacks like scaling, re-sizing etc. It is used for ownership protection [9].

Digital watermarking is implemented by frequency domain techniques and spatial domain techniques. In frequency domain techniques, the watermark is embedded into the image after applying transformation techniques. Some of the transformation techniques are Discrete Fourier Transform, Discrete Wavelet Transform and Discrete Cosine Transform [10]. The main advantage of frequency domain techniques is the robustness of the watermark during the occurrence of attacks. The disadvantage is difficult to implement as it also needed transformation techniques [11], [12]. In spatial domain watermarking, the watermark is embedded directly into the image without conversion. The main

advantages of spatial domain technique are easy to implement, high embedding capacity. Also it has a major disadvantage of weak security during attacks [13], [14]. The payload of the watermark can be decreased by using compression techniques. So that, more data can be embedded by using spatial domain techniques.

The compression of the watermark is done by two techniques irrespective of its type: text, image or video. They are lossy and lossless compression techniques. In lossy compression, some of the data is lost in the watermark and the lost information cannot be recovered at decoding side. So, lossy compression is also called irreversible compression technique. The main advantage of lossy compression is more amounts of data are compressed and the disadvantage is some of the data is permanently deleted [15].In lossless compression, compression is carried without loss and at the decoding side the original watermark can be retrieved. The advantage of lossless compression is no loss of information in watermark after compression and the disadvantage is it cannot achieve higher levels of compression [16].

In spatial domain, by compressing watermark more data to be stored in cover image. In medical image watermarking lossless data compression of watermark is used, as the medical image contains very important information for diagnosis. Number of lossless compression techniques is available like Huffman coding, Shannon-Fano algorithm, dictionary coding, run length coding etc., [17].

In Al-Haj, Ahmad Mohammad [18], the medical image is divided into ROI and RONI and applied Discrete Wavelet Transform (DWT) to the medical image, where hash value of watermark is embedded in sub-bands. The disadvantage of this method is that, it is only used for authentication of ROI but it fails in recovering the ROI in case of tampering of ROI. In Al-Haj [19], the medical image is divided into ROI and RONI regions. The ROI pixels are randomly selected and those least significant bits are embedded in RONI. The main disadvantage in this method involves in detecting the tampered regions in ROI. As the method uses randomly selecting LSB's of ROI pixels to detect ROI tampering, if remaining pixels of ROI are tampered then it is difficult to identify the tamper. In Khor [20], the medical image is divided into ROI and RONI. ROI is compressed by JPEG and embedded in RONI. One of the disadvantage of this method is, hash256 generate 256 bits of data which is more to embed. Another disadvantage is JPEG is a lossy compression which is applied on ROI. So, some of the information of ROI is permanently lost. In case of both ROI and RONI parts are tampered then ROI recovery is not possible.

In Eswaraiah R [21], the medical image is divided into BORDER, ROI and RONI regions. Hash function is applied for ROI and embedded into the two LSB's of BORDER area. The ROI is divided into 4×4 blocks and RONI into 8×8 blocks and each ROI block is mapped with RONI block. For each ROI, embedded the ROI into two LSB's of the mapped RONI. ROI blocks are combined into ROI matrix and RONI blocks into RONI matrix. BORDER, ROI and modified RONI are combined to get the watermarked medical image. At the destination, the watermarked medical image is divided into BORDER, ROI and RONI parts. Hash value for ROI is calculated and hash value from BORDER is extracted and these two hash values are compared. If these two hash values are same then there is no tampering in ROI, if not then divided ROI into 4×4 blocks and RONI into 8×8 blocks and map them. For each ROI, average and median are calculated and from mapped RONI average and median are extracted. If these two are same then no tamper in ROI block. If these two are not same then tampering in ROI is occurred and recovered from RONI. The disadvantage in the above method is calculation of hashing which is more complex, generated more number of bits and also ROI is not compressed while embedding into the RONI. So, the embedding payload capacity becomes high which needs more RONI blocks. Another disadvantage is that, if average and mean of both ROI and extracted ROI are not same then tamper may be done at ROI or at RONI. But this paper focuses only on tampering in ROI.

To overcome the disadvantages of the above mentioned methods, there is a need to develop the new method with the following objectives:

1) Use less number of bits for authentication process.
2) ROI must be recovered even though both ROI and RONI are tampered.
3) As random RONI blocks are selected for embedding then the chances of recovery of ROI increases.

To achieve the above objectives, the proposed method uses the checksum, division hash function, and lossless block compression techniques. In the proposed method, the fragile block based medical image watermarking is introduced. The medical image is divided into three regions: BORDER area, ROI part and RONI part. Modulo sum (M), checksum (CS) are calculated for ROI part and the ROI coordinates, M, CS and patient details are embedded into the BORDER area. The ROI and RONI are divided into blocks, map each ROI block with RONI block using division hash function. The ROI block is compressed using lossless block compression technique and embedded the compressed ROI block information into mapped RONI block. At the decoding side, M and CS of ROI are calculated and compared with extracted modulo sum (EM) and checksum (ECS) of ROI from BORDER area and based on that the ROI is tampered or not is identified. If tampered recovered the ROI block from the mapped RONI block. The detailed explanation of the proposed method is given in the following sections organized as Section 2 for preliminaries, Section 3 for proposed method, Section 4 for performance measures, Section 5 for results and Section 6 for conclusion and future scope.

2. Preliminaries

The concepts used in the proposed method are discussed below:

2.1. Watermark procedure

The proposed method of medical image watermarking contains two phases: Watermark embedding also called encoding phase and Watermark authentication and recovery of ROI also called decoding phase. In encoding phase, the watermark (ROI) is embedded in RONI region. In watermark authentication and recovery phase, first the ROI is authenticated and if it is tampered then recovery of ROI is done from RONI. The Fig. 1 shows the encoding and decoding phase of medical image watermarking.

2.2. Medical image selection

Different medical image modalities like CT scan, MRI are used for medical image watermarking for diagnosis purpose. Some of the images are taken from DICOM (Digital Imaging and Communications in Medicine) Library and some of the images are taken from MedPix® library which is a searchable database in medicine and converting them to PNG format which is lossless. The Fig. 2 shows some of the medical images from left to right MRI1, MRI2, MRI3, CTSCAN1, CTSCAN2, CTSCAN3 used in the proposed method and their sampled ROI regions.

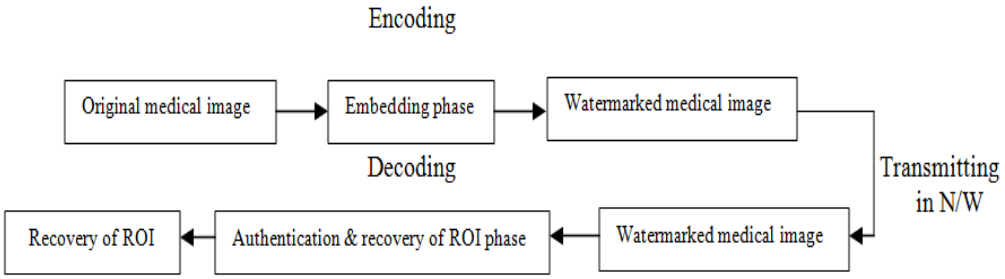


Fig. 1: Encoding and Decoding Phase of Medical Image Watermarking.

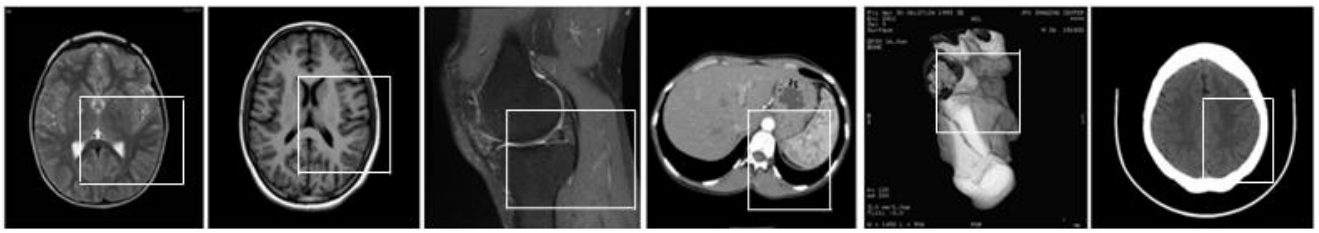


Fig. 2: MRI and CT scan Medical Images.

2.3. ROI selection

In the proposed method, the original medical image is divided into three parts: BORDER area, ROI part and RONI part. The 8 rows and 8 columns of four sides of the image are considered as BORDER area. As the ROI is changing from image to image, the ROI part is selected by the physician. Selected the number of rows and columns of the ROI part are multiples of 4, as the ROI is further divided into 4 × 4 blocks and RONI is divided into 8 × 8 blocks. After choosing the ROI part, the ROI coordinates, the modulo sum (M), checksum (CS) of ROI and patient details are embedding into the two least significant bit positions of the BORDER area. Modulo sum (M) and checksum (CS) calculation for ROI is discussed in Section 2.4. Fig. 3 shows the medical image and the three parts of the medical image. Table 1 shows the medical images, their ROI sizes and number of ROI and RONI blocks.

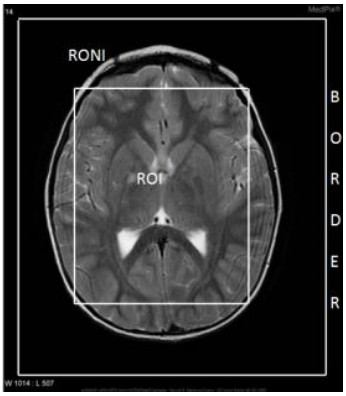


Fig. 3: Division of Medical Image into Parts.

Table 1: Different Medical Images and Their Selected ROI Sizes and Number of ROI and RONI Blocks

S. No	Image name	Image size	ROI size	Total RONI blocks	Total ROI blocks
1	MRI1	584×512	184 × 184	4079	2116
2	MRI2	737×743	200 × 200	7705	2500
3	MRI3	512×512	184 × 192	3480	2208
4	CTSCAN1	512×512	176 × 184	3526	2024
5	CTSCAN2	512×512	232 × 104	3655	1508
6	CTSCAN3	512×512	168 × 176	3634	1648

2.4. Checksum calculation

In medical image watermarking, the authenticity of the ROI is very important. The checksum is an error detection method to find the authenticity of ROI. Checksum is a value calculated from a block of data. In the proposed method, checksum is used to find whether the ROI is transmitted securely from source to destination without any tampering or not. The following are the steps used for calculating the checksum of ROI:

1) Find the sum (S) of all pixels of ROI.
2) Perform modulus operation on sum (S) with 256 and store the result in M as shown in Eq.1.

$$M = S \% 256 \quad (1)$$

3) Convert M into binary form and perform one's complement and converted into decimal to get checksum (CS).

The coordinates of ROI, M, CS and patient details are embedded into the least two significant bit positions of the BORDER area. Fig.4 shows the sample ROI region.

71	68	66	69
70	67	65	66
71	68	65	64
72	70	67	65

Fig. 4: Sample ROI Region.

The checksum (CS) calculation for Fig. 4 is explained below:
The calculated sum (S) =71+68+66+69+70+67+65+66+71+68+65+64+72+70+67+65 = 1084
The modulo sum (M) = S % 255 = 1084 % 255 = 64
Binary form of M = 01000000
One's complement of M = 10111111
The checksum (CS) = 191

The calculated M (8 bits) and CS (8 bits) values are embedded into the least significant bit positions of the BORDER area. At the decoding side, modulo sum (M) and checksum (CS) are calculated for ROI. Modulo sum (EM) and checksum (ECS) of ROI are extracted from BORDER area. If M and EM are same then no tampering is occurred in ROI. If not same then extracted modulo sum (EM) and checksum (ECS) are added. If the sum result (RESULT1) is ZERO then tampering occurred in ROI part. Hence, further actions are performed to recover ROI.

2.5. Division hash function

Hashing is a technique used to map the elements into the hash table. Division method is one of the popular hash functions to find the hash table index to map the element. In the proposed method, ROI is divided into 4 × 4 non-overlapping blocks and placed in ROI_VECTOR in sequential order and RONI is divided into 8 × 8 non-overlapping blocks and placed in RONI_VECTOR in sequential order as shown in Fig.5. Division hash function is used to map the ROI block of ROI_VECTOR into the RONI block of RONI_VECTOR. After mapping, the ROI block information is compressed and embedded into the mapped RONI block. Such that, if any tampering occurred in the ROI block at destination, the ROI block is recovered from the mapped RONI block. Here, the number of RONI blocks must be greater than the number of ROI blocks, otherwise collisions will occur. The Eq.2 is used for mapping ROI block to RONI block.

$$BN_{RONI} = ((PK \times BN_{ROI}) \bmod TB) + 1 \qquad (2)$$

Where BN_{RONI} is the block number of RONI_VECTOR, PK is any primary key between 1 and TB, BN_{ROI} is the block number of ROI_VECTOR and TB is total number of RONI blocks.

2.6. ROI block compression

In the proposed method, the ROI part is divided into number of 4 × 4 non-overlapping blocks. The reason for selecting the 4 × 4 size for ROI is, as the block size increases the pixel differences in the ROI block will be high and as the block size decreases the embedding data size increases. Hence, the reasonable size of ROI block such as 4 × 4 then the pixel differences decreases and embedding capacity is also decreases. Calculate modulo sum (MR), checksum (CSR) for each 4 × 4 ROI block (B) as specified in Section 2.4. Each ROI block (B) of the ROI_VECTOR is compressed and embedded the MR, CSR, compressed ROI block (CB) of ROI_VECTOR into the mapped RONI block of RONI_VECTOR. Following are the steps used for compression of each ROI block (B) at encoding side:

1) Find the highest value (H) of the ROI block (B).
2) Subtract each pixel of B from H then get the compressed ROI block (CB).
3) Find the highest value (H1) of the compressed ROI block (CB).
4) Find the maximum number of bits (N) needed for binary form of H1.
5) The maximum number of bits needed for each pixel of compressed ROI block is N.
6) The 4 × 4 ROI block contains 16 pixels. The total number of bits (T) needed for each ROI block to embed into the mapped RONI block is product of 16 and N.

If N is less than 8 then embed MR (8 bits), CSR (8 bits), H(8 bits), N(3 bits) and T bits of compressed ROI block (CB) into the least one or two or three significant bit positions of the mapped RONI block. If N is 8 then no need to apply the compression because after compression also each pixel of ROI block need 8 bits. In this case embed the ROI block as it is without any compression i.e., embeds MR (8 bits), CSR (8 bits) and ROI block (B). Fig.6 shows the ROI block compression at the encoding side.

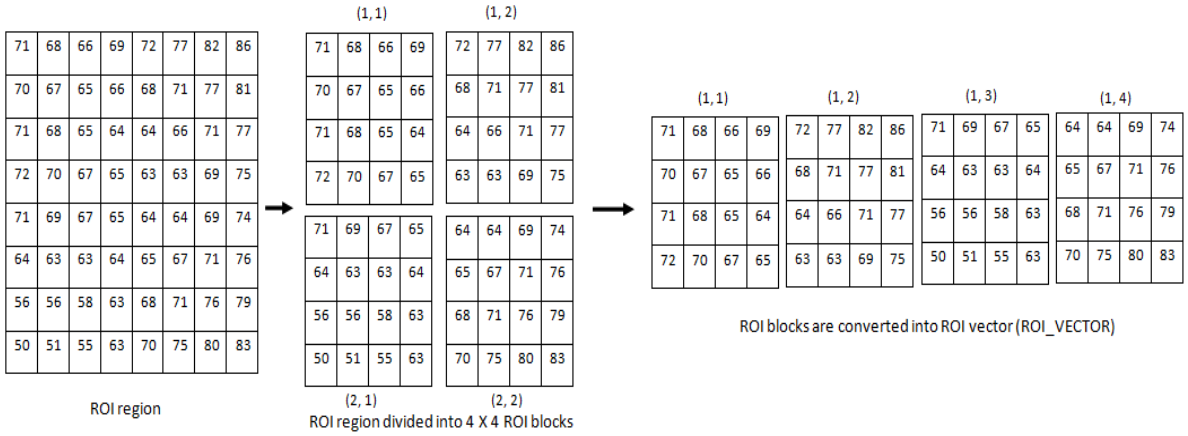


Fig. 5: Process of Converting ROI Region into ROI_VECTOR.

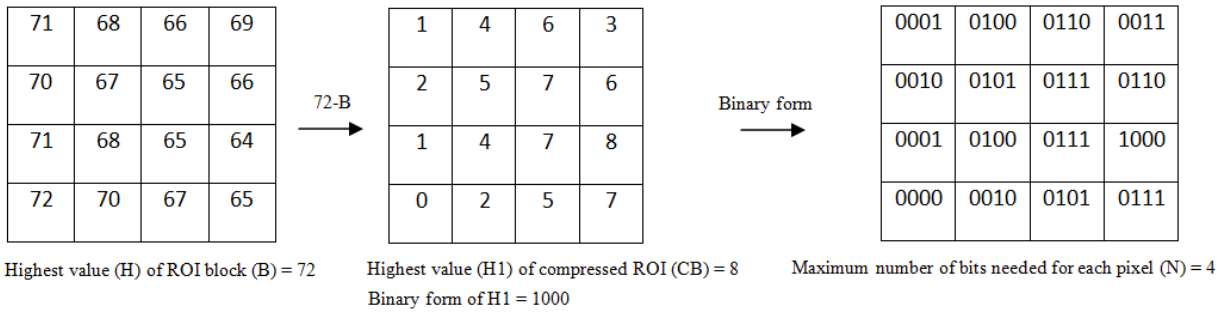


Fig. 6: ROI Block Compression.

At the decoding side, the authenticity of each ROI block of ROI_VECTOR is checked by calculating modulo sum (MR) and checksum (CSR) of ROI block (B) and extracting the modulo sum (EMR) and checksum (ECSR) of the ROI block (B) from the mapped RONI block of RONI_VECTOR. If MR and EMR are same then no tampering in ROI block (B) and no need to extract the remaining data from RONI. If MR and EMR are not equal then add EMR and ECSR and perform one's complement

(RESULT2).If RESULT2 is ZERO then no tampering in mapped RONI block and recover the compressed ROI block by extracting the H, N and T bits from the mapped RONI block. Decompress the compressed ROI and replace the tampered ROI with the decompressed ROI. Following are the steps used for decompression of each tampered ROI block (B) at decoding side:

1) Extract the H (8 bits) and N (3 bits) from mapped RONI block.
2) Convert H and N into decimal form.
3) Extract 16 × N number of bits (T) from mapped RONI block.
4) Divide T bits into 16 parts and convert into decimal values.
5) Subtract each decimal value from H and arrange them into matrix form to get recovered ROI.

ROI decompression for the example in Figure 6 is given below:

1) If ROI is tampered then extract next 8 bits (H) and 3 bits (N) from RONI.
2) Extracted bits = 01001000100
3) H = 01001000(8 bits) = 72, N = 100(3 bits) = 4
4) ROI block= 16 pixels × N = 16 × 4 = 64 bits
5) Extract next 64 bits from mapped RONI and divided into 16 parts: 0001, 0100, 0110, 0011, 0010, 0101, 0111, 0110, 0001, 0100, 0111, 1000, 0000, 0010, 0101, 0111
6) Convert bits into decimal form: 1, 4, 6, 3, 2, 5, 7, 6, 1, 4, 7, 8, 0, 2, 5, and 7
7) Subtract each value from H (72): 71, 68, 66, 69, 70, 67, 65, 66, 71, 68, 65, 64, 72, 70, 67, and 65
8) Convert the above values from vector to matrix to get the recovered ROI as shown in Fig.7.

71	68	66	69
70	67	65	66
71	68	65	64
72	70	67	65

Fig. 7: Recovered ROI.

3. Proposed method

The proposed method uses checksum to authenticate whether the ROI is tampered or not. The division hash function is used to map the ROI block with the RONI block. The lossless block compression technique is used to compress the ROI block and embedded into the mapped RONI block. If the ROI block is tampered then the recovery of ROI is done from the mapped RONI block. The Section 3.1 shows the watermark embedding procedure and Section 3.2 shows the ROI recovery in case of tampering of ROI.

3.1. Watermark embedding procedure

Following are the steps used to embed the ROI region into the RONI area and Fig. 8 shows the embedding process based on the proposed method:

1) Read the medical image and divide it into three parts: BORDER part, ROI part and RONI part as specified in Section 2.3.
2) Calculate modulo sum (M) and checksum (CS) for ROI part as specified in Section 2.4.
3) Embed the ROI coordinates, modulo sum (M), checksum (CS) and binary form of patient details into the least two significant bit positions of the BORDER from starting position.
4) Divide RONI into 8 × 8 non-overlapping blocks and ROI into 4 × 4 non-overlapping blocks.
5) Place RONI 8 × 8 blocks into RONI_VECTOR in sequential order and place ROI 4 × 4 blocks into ROI_VECTOR in sequential order as specified in Fig.5.
6) Map each ROI block (B) of ROI_VECTOR into RONI block of RONI_VECTOR by using the division hash function as specified in Section 2.5.
7) Compress each ROI block (B) of ROI_VECTOR and embedded into the mapped RONI block of RONI_VECTOR as specified in Section 2.6.
8) Place modified RONI blocks of RONI_VECTOR into their original positions of the medical image and ROI blocks of ROI_VECTOR into their original positions.
9) Combine BORDER part, ROI part and modified RONI part to get the watermarked medical image.

3.2. ROI authentication and recovery process

Authentication of ROI is necessary after transmitting the watermarked medical image from source to destination. If there is any tampering in ROI then recovery of ROI must be done from RONI. ROI authentication and recovery process is performed in different cases.

CASE 1: BORDER area is not tampered and ROI is not tampered.
CASE 2: BORDER area is not tampered and ROI is tampered.
CASE 3: BORDER area is tampered and ROI is not tampered.
CASE 4: BORDER area is tampered and ROI is also tampered.

The following are the procedures needed for the authentication and recovery of ROI for the above 4 cases.

Procedure for CASE 1:

1) Divide the image into 3 parts namely BORDER area, ROI and RONI parts.
2) Calculate sum(S) of all pixels of ROI and perform modulus operation with 256 and place the result in (M).
3) Extract modulo sum (EM) and checksum (ECS) of ROI and patient details from BORDER.
4) Compare modulo sum (M) and extracted modulo sum (EM). If these two are same then no tampering in BORDER area and in ROI else check CASE 2.

Procedure for CASE 2:

1) Add extracted modulo sum (EM) and checksum (ECS) to perform one's complement and call it as RESULT1. If RESULT1 is ZERO then tampering is not done in BORDER area and tampering is done in ROI area and recovers the ROI area from RONI region by executing the procedure from step 2 to step 8.
2) Divide the ROI part into 4 X 4 non-overlapping blocks and RONI into 8 X 8 non-overlapping blocks.
3) Place the 4 X 4 ROI blocks into the ROI_VECTOR in sequential order and place the 8 X 8 RONI blocks into the RONI_ VECTOR in sequential order as shown in Fig.5.
4) Map each ROI block (B) in the ROI_VECTOR into the RONI block in the RONI_VECTOR by using the division hash function as specified in Section 2.5.
5) For each ROI block (B) in the ROI_VECTOR repeat the following steps:

i) Calculate modulo sum (MR) of all pixels of 4 X 4 ROI block.
ii) Extract modulo sum (EMR) and checksum (ECSR) of ROI block from the mapped RONI block.
iii) If MR and EMR are same then ROI block is not tampered.
iv) If not same then add EMR and ECSR to perform one's complement and store the result in RESULT2. If the RESULT2 is ZERO then no tampering in RONI block and tampering in ROI block. Hence, recover ROI block from the mapped RONI block as specified in Section 2.6.

6) Convert the ROI_VECTOR into ROI matrix by combining the blocks. Calculate modulo sum (RM) of recovered ROI part.

7) If extracted modulo sum (EM) of ROI from BORDER and recovered modulo sum of ROI (RM) are same then recovery of ROI is done from mapped RONI block.
8) If these two are not same then recovery of ROI is not done from RONI, because some of the mapped RONI blocks of the tampered ROI blocks are also tampered. Hence, recovery of ROI is not possible.
9) If RESULT1 is not ZERO then tampering is done at BORDER area. So, ROI may or may not tampered then check CASE 3 and CASE 4.

Procedure for CASE 3:

1) Perform steps from 2 to 6 of CASE 2.
2) If modulo sum (M) of ROI and recovered modulo sum (RM) of ROI are same then ROI is not tampered and BORDER area is tampered. Hence, ROI is safe.
3) If M and RM are not same then BORDER area and ROI both are tampered then check CASE 4.

Procedure for CASE 4:

1) If modulo sum (M) of ROI and recovered modulo sum (RM) of ROI are not same then tampering is done both at BORDER area and ROI part.
2) Recover the tampered ROI part from the RONI part by performing steps from 2 to 6 of CASE 2.
3) If the mapped RONI blocks of tampered ROI blocks are also tampered then ROI recovery is not possible, otherwise ROI recovery is possible even though some of the RONI blocks are tampered.

Fig. 9 shows the ROI authentication and recovery process.

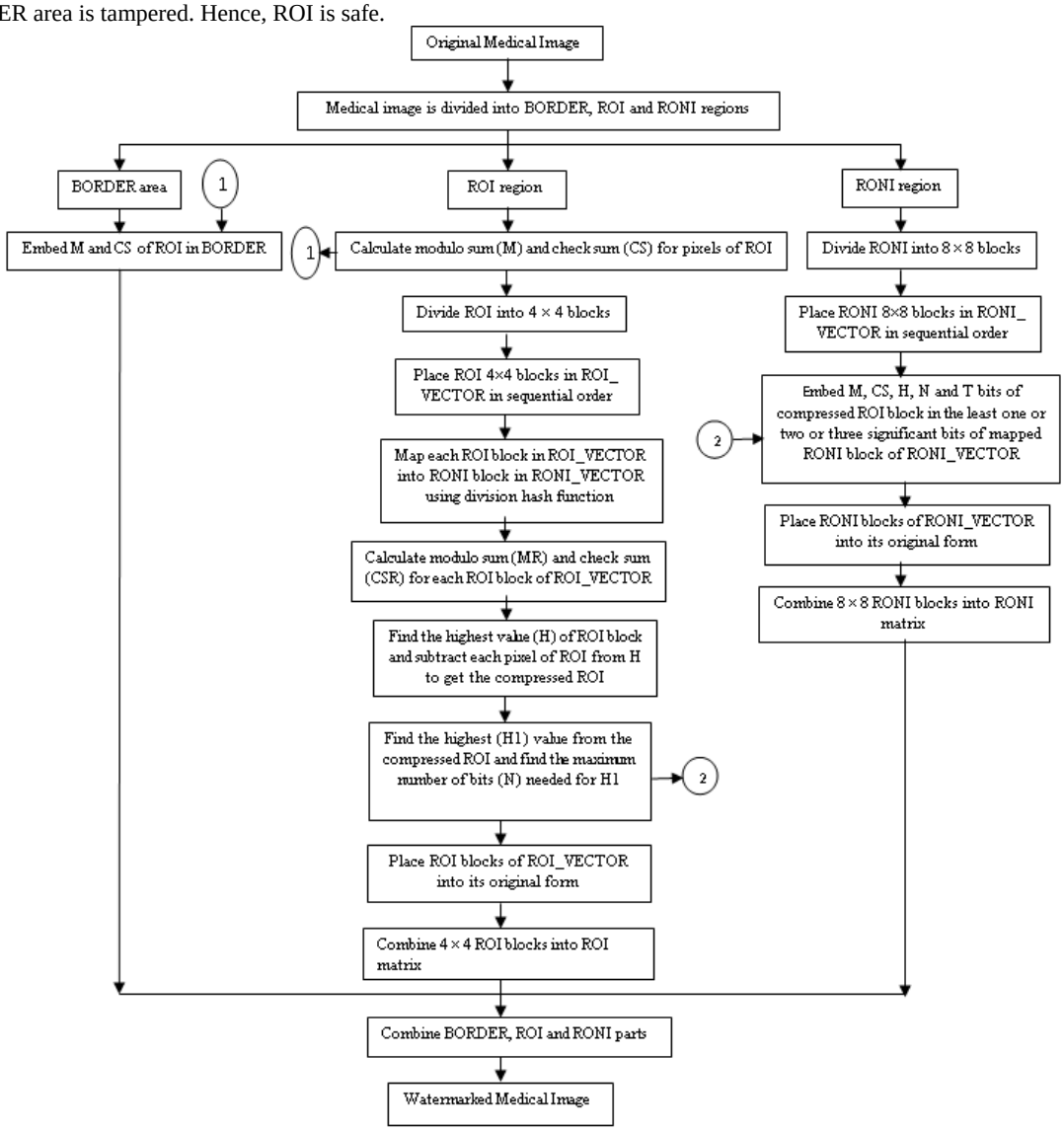


Fig. 8: Watermark Embedding Process.

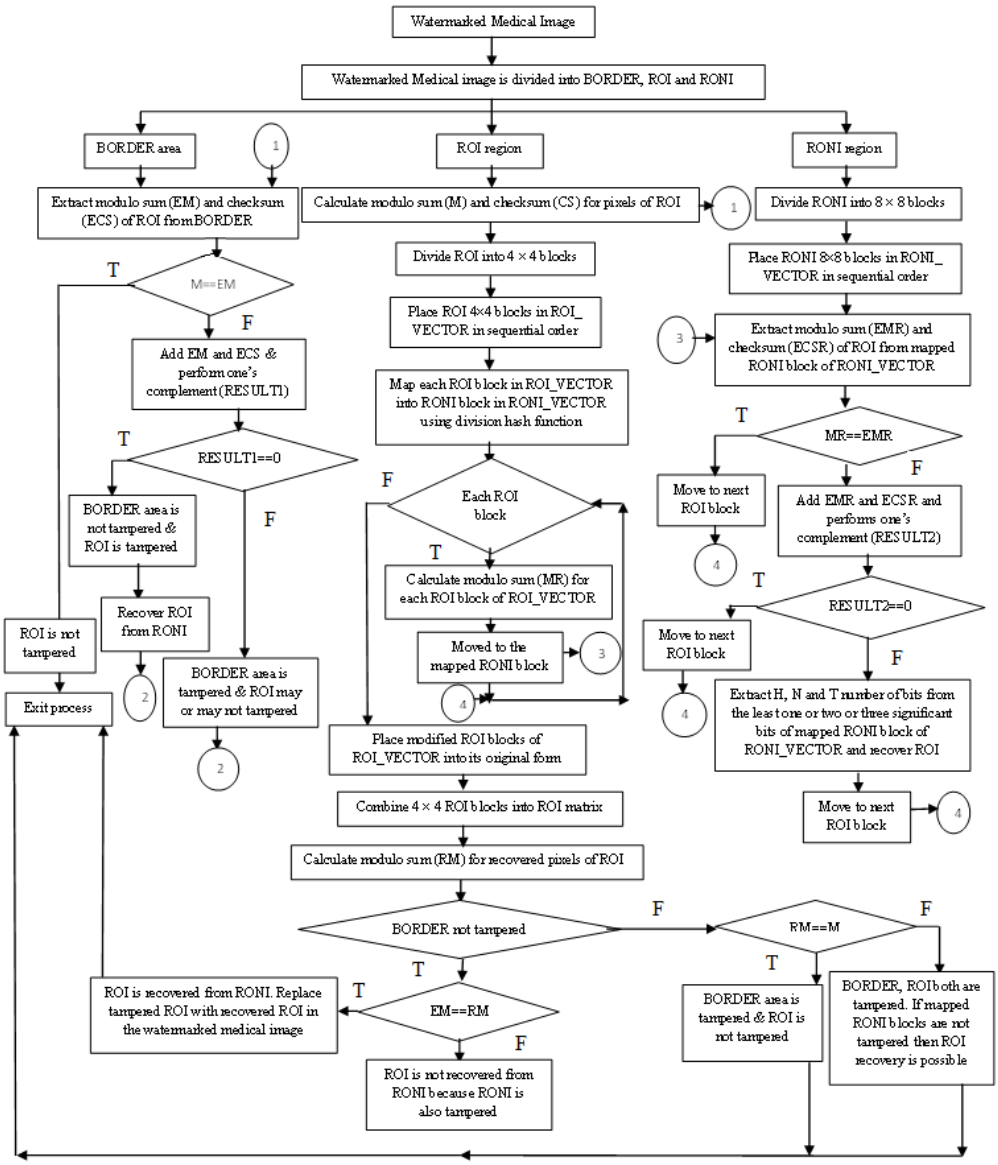


Fig. 9: ROI Authentication and Recovery Process.

4. Performance measures

The performance measures like MSE, PSNR, BER, AD, MD, SC and IF are used to measure the quality of the watermarked medical image and recovered ROI. The quality measures are divided into subjective and objective measures. Some of the objective measures are given below:

4.1. Mean square error (MSE)

It measures the difference between the original medical image and watermarked medical image. In order to measure the quality of the watermarked image MSE is used. If the value of MSE is closer to ZERO then the quality of the watermarked image is high. The equation for MSE is given in Eq.3.

$$\text{MSE} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(O(i,j)-W(i,j))^2}{MXN} \quad (3)$$

O is the original medical image, W is the watermarked medical image and M, N are the rows and columns of the medical images and $1 \le i \le M$ and $1 \le j \le N$.

4.2. Peak signal to noise ratio (PSNR)

The PSNR measures the peak error between the original medical image and watermarked medical image and is represented in decibels. If PSNR is high then watermarked medical image quality is also high. The equation for PSNR is given in Eq.5.

$$\text{PSNR} = 10 \log_{10}\left(\frac{R^2}{\text{MSE}}\right) \quad (4)$$

R is the maximum fluctuation in the original medical image.

4.3. Bit error rate (BER)

It is the ratio of number of bits changed from original medical image to watermarked medical image and total number of bits received. It is used to measure the quality of a digital transmission system. The equation for BER is given in Eq.5.

$$\text{BER} = \frac{N_C}{N_T} \quad (5)$$

Where N_C is number of bits changed after watermark embedding process and N_T is total number of bits in the medical image.

4.4. Average absolute difference (AD)

AD is used to find the average of difference between the original medical image (O) and watermarked medical image (W) of size M rows and N columns. The equation for AD is given in Eq.6.

$$AD=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}O(i,j)-W(i,j) \quad (6)$$

4.5. Maximum difference (MD)

It is used to find the maximum difference between the original medical image (O) and watermarked medical image (W). The equation for MD is given in Eq.7.

$$MD=MAX\ |O(i,j)-W(i,j)| \quad (7)$$

4.6. Structural content (SC)

It is used to find the similarity between the original medical image (O) and watermarked medical image (W) of size M rows and N columns. The equation for SC is given in Eq.8.

$$SC=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}W(i,j)^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}O(i,j)^2} \quad (8)$$

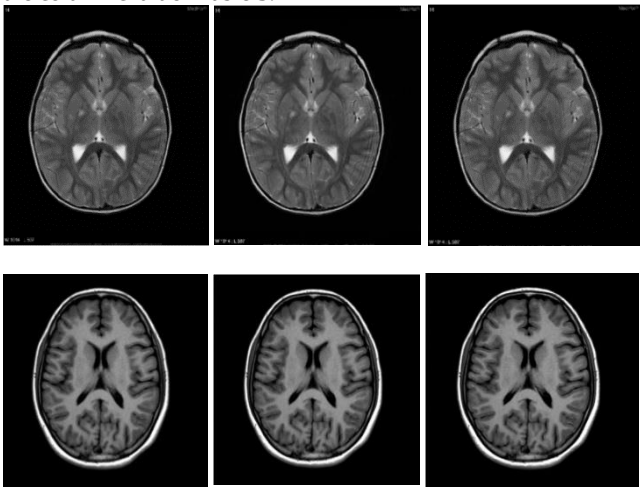
4.7. Image fidelity (IF)

It is used to find the closeness of the original medical image (O) and watermarked medical image (W) of size M rows and N columns. The equation for IF is given in Eq.9.

$$IF=1-\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(O(i,j)-W(i,j)^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}(O(i,j))} \quad (9)$$

5. Experimental results

The experiments are conducted on 80 medical images, 40 of type CT scan and 40 of type MRI. All these medical images are DICOM formatted and MedPix® library medical images and are converted into PNG format which is lossless. The matlab17a version is used to run the program on a standalone computer with Intel core i5 processor and a RAM of 4GB.Fig. 10 shows the different types of medical images and their watermarked medical images after encoding with block compression and checksum calculation and their recovered medical images after decoding if no tampering in watermarked medical image as specified in CASE 1. Table 2 shows the PSNR, BER, AD, MD, SC and IF of the given six medical images and Table 3 shows the comparison of PSNR of the proposed method with the existing method [21] and Fig. 11 shows the column chart of Table 3.



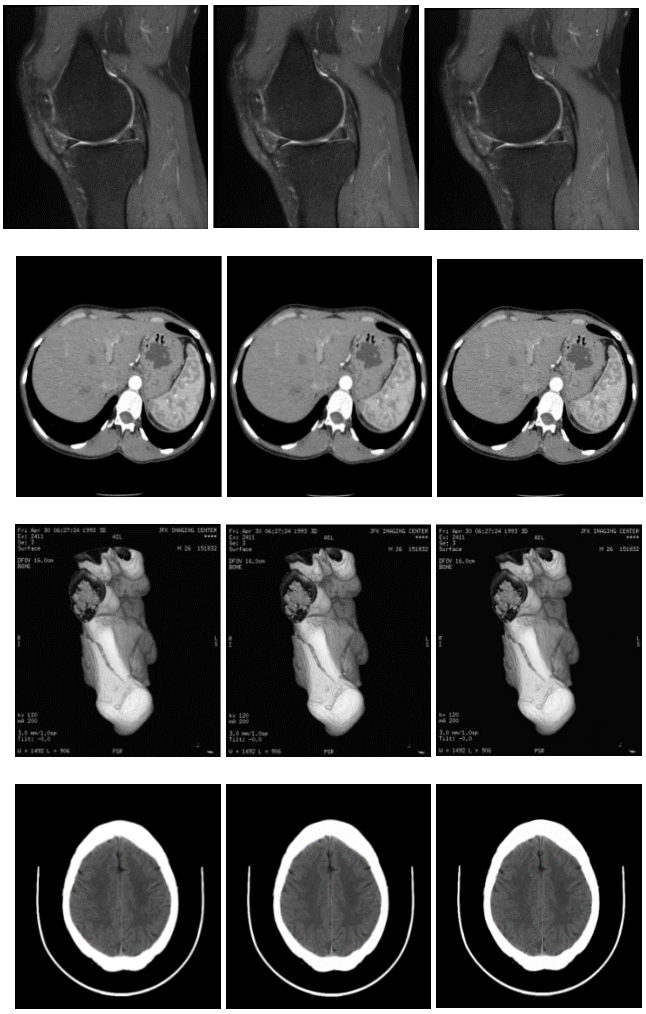


Fig. 10: Original Medical Images are at Column 1, Watermarked Medical Images are at Column 2 and Recovered Medical Images are at Column 3.

Table 2: The PSNR, BER, AD, MD, SC and IF for Six Medical Images

S. No	Image Name	PSNR	BER	AD	MD	SC	IF
1	MRI1	55.0755	0.0918	0.0051	7	1.0004	0.1228
2	MRI2	56.0476	0.0427	-0.0715	7	1.0005	0.1572
3	MRI3	54.1123	0.0859	0.0201	7	1.0006	0.1314
4	CTSCAN1	53.7450	0.0638	-0.0525	7	1.0004	0.1139
5	CTSCAN2	53.3277	0.0889	0.0709	7	1.0006	0.1435
6	CTSCAN3	53.5156	0.0843	-0.0782	5	1.0011	0.1405

Table 3: PSNR Comparison of Proposed Method with the Existing Method [21]

S. No	Image Name	PSNR (proposed)	PSNR [21]
1	MRI1	55.0755	53.0326
2	MRI2	56.0476	53.6034
3	MRI3	54.1123	52.8430
4	CTSCAN1	53.7450	51.3742
5	CTSCAN2	53.3277	51.0536
6	CTSCAN3	53.5156	51.0860

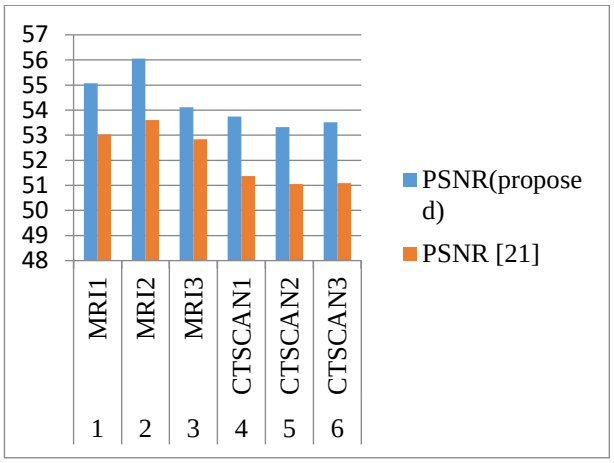


Fig. 11: Column Chart for Values in Table 3.

While transmitting the watermarked medical images through public networks there may be a chance of occurring tampers on different parts of the medical images then recovery of ROI is necessary to diagnose the patients correctly. The tampering may occurs at different areas like BORDER, ROI, RONI and combination of BORDER, ROI and RONI. Section 3.2 discussed about different cases of occurrence of tampers and the procedures used for recover the ROI. If the tampering occurred in ROI and not in BORDER area then CASE 2 procedure is used to recover the ROI. Fig. 12 shows the tampered ROI and recovered ROI from RONI region if RONI region is not tampered as specified in CASE 2.

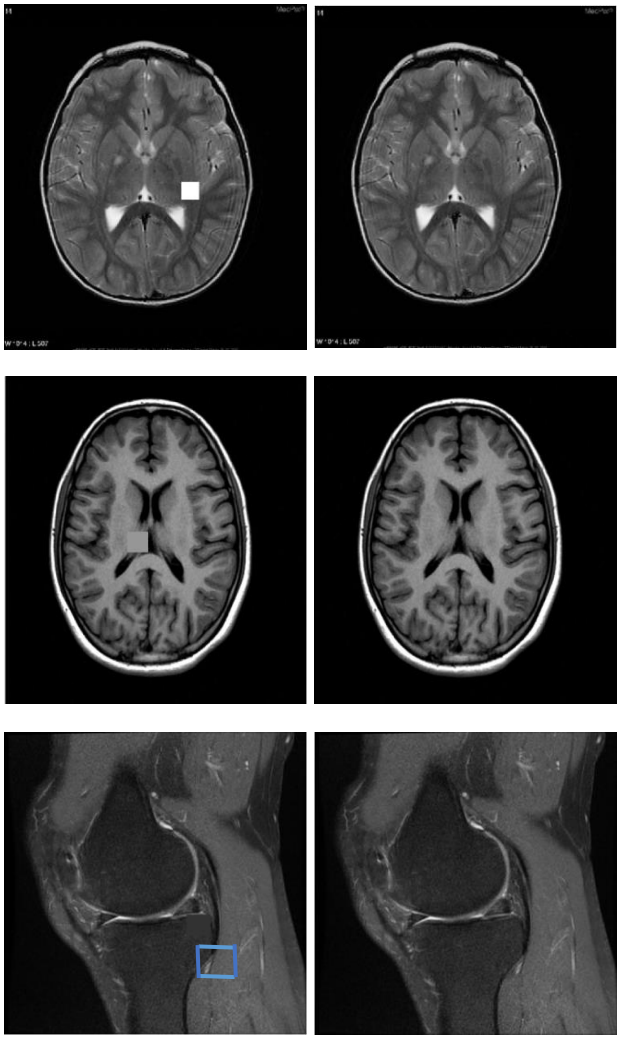
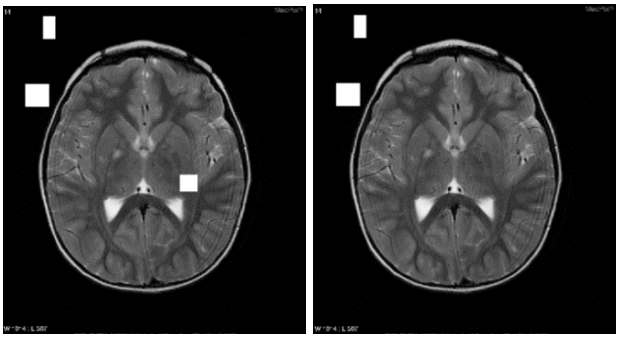


Fig. 12: Tampered ROI in Column 1, Recovered ROI in Column 2.

The tampers occurs in ROI and also in RONI and not in BORDER then the recovery of ROI may or may not done based on the RONI. If the ROI block and mapped RONI block of ROI both are tampered at the same time then ROI block recovery is not possible else ROI recovery is possible. Fig. 13 shows the recovered ROI if the mapped RONI blocks are not tampered. Fig. 14 shows the cases of tampering in ROI block and mapped RONI blocks then those ROI blocks are not recovered and the remaining ROI blocks whose mapped RONI blocks are not tampered are recovered.



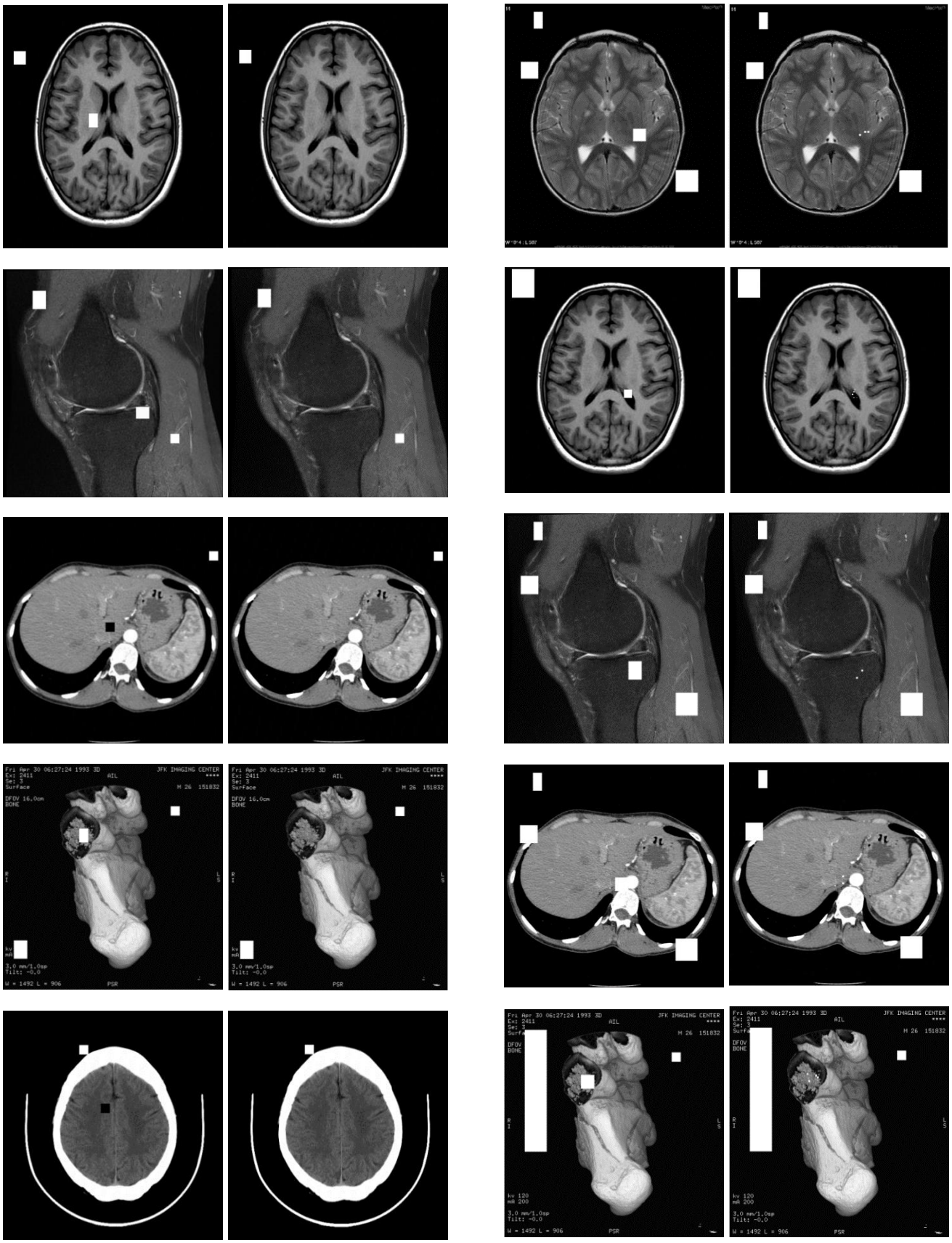


Fig. 13: Column 1 Shows both ROI and RONI are Tampered and Column 2 Shows the Recovered ROI.

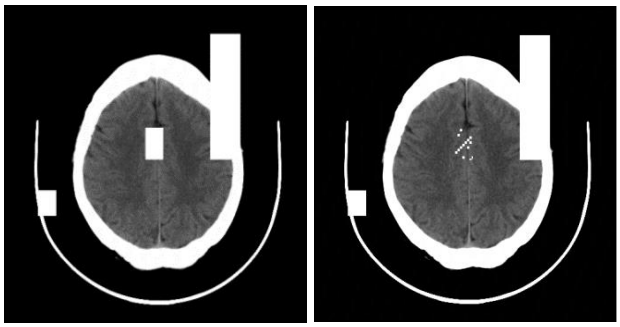


Fig. 14: Column 1 Shows the Tampered ROI and RONI Blocks and Column 2 Shows Some of the Recovered ROI Blocks.

The tampering may also occur in BORDER area and not occurred in ROI region as specified in CASE 3. The CASE 3 procedure is used to identify the authenticity of ROI whether it is safe or not. Fig. 15 shows the tampers at BORDER and also at RONI and not at ROI.

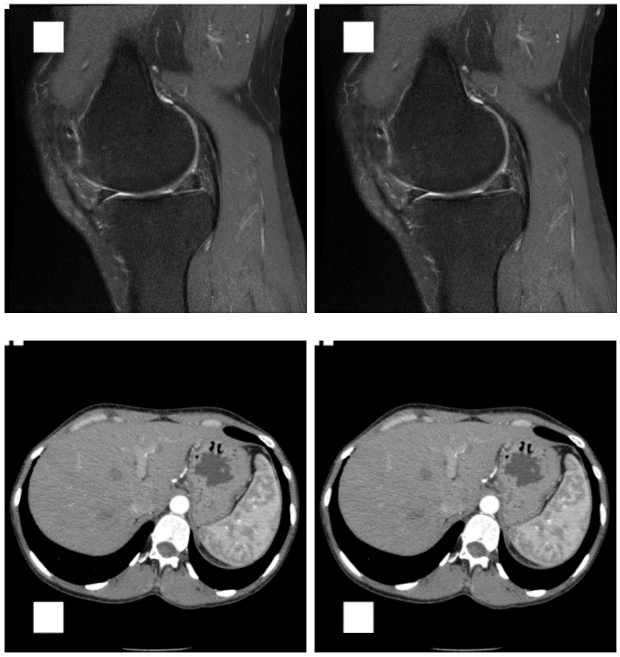


Fig. 15: Column 1 Shows the Occurrence of Tampers at BORDER and RONI and Column 2 shows the Recovered ROI.

As discussed in CASE 4 the tampering may occur at both BORDER and ROI. In this case the ROI is recovered or not is checked manually by calculating the difference between original and recovered images. Fig.16 shows the original and recovered ROI images if tampering occurs at BORDER and at ROI and mapped RONI blocks are not tampered. If the mapped RONI blocks are also tampered then some of the ROI blocks are not recovered as shown in Fig.17.

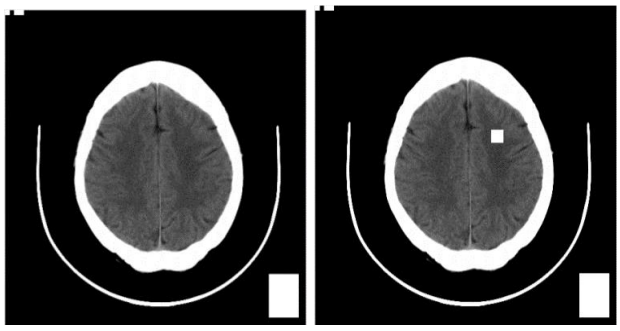


Fig. 16: Column 1 Shows the Occurrences of Tampers at BORDER and ROI and Not at Mapped RONI Blocks and Column 2 Shows the Recovered ROI.

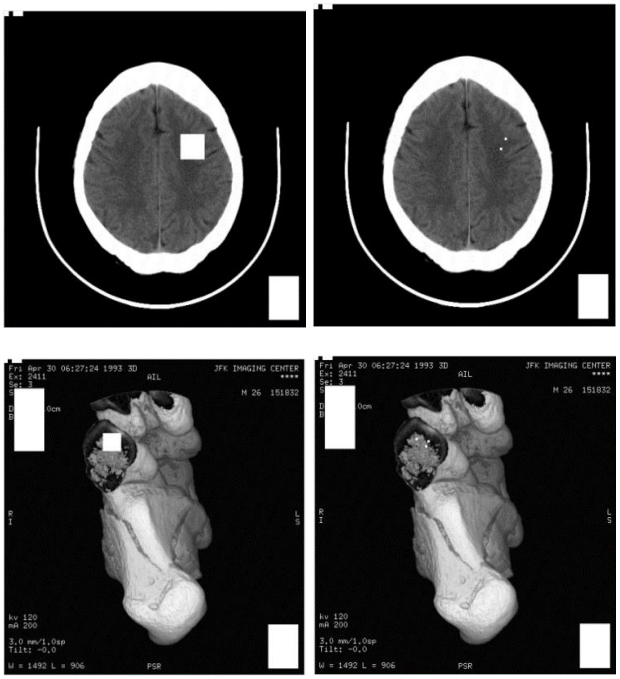


Fig. 17: Column 1 Shows the Occurrences of Tampers at BORDER, ROI and Some of Mapped RONI Blocks and Column 2 Shows Recovered ROI at Some Part.

6. Conclusion

In the proposed fragile block based medical image watermarking method, to authenticate the ROI, checksum calculation is used and the payload of the checksum is also less compared to the other hashing techniques like SHA-256, SHA512 etc. To decrease the payload capacity of ROI, lossless block based compression technique is used. In the lossless block based compression technique, compress the ROI before embedding into the RONI. The division hash function is used to map each ROI block into RONI block randomly. So that the ROI is distributed in RONI randomly and the chances of tampering at a time in both ROI and the mapped RONI blocks are reduced. The performance measures PSNR, BER etc. are used to find the difference between the original and the watermarked medical images. The proposed method recovered the ROI in case of tampering occurred in both ROI and RONI. But it is possible only if mapped RONI blocks of the tampered ROI blocks are not tampered.

References

[1] Lee WB, Lee CD. A cryptographic key management solution for HIPAA privacy/security regulations. IEEE Trans Inf Technol Biomed. 2008; 12 (1):34-41. https://doi.org/10.1109/TITB.2007.906101.

[2] Kocabas O, Soyata T, Aktas MK. Emerging Security Mechanisms for Medical Cyber Physical Systems. IEEE/ACM Trans Comput Biol Bioinform. 2016; 13(3):401-16. https://doi.org/10.1109/TCBB.2016.2520933.

[3] Nyeem H, Boles W, Boyd C. A review of medical image watermarking requirements for teleradiology. J Digit Imaging. 2013; 26(2):326-43. https://doi.org/10.1007/s10278-012-9527-x.

[4] Pujar JH, Kadlaskar LM. A new lossless method of image compression and decompression using Huffman coding techniques. Journal of Theoretical & Applied Information Technology. 2010; 15.

[5] BW TA, Permana FP, editors. Medical image watermarking with tamper detection and recovery using reversible watermarking with LSB modification and run length encoding (RLE) compression. Communication, Networks and Satellite (ComNetSat), 2012 IEEE International Conference on; 2012: IEEE.

[6] Liew S-C, Liew S-W, Zain JM. Reversible medical image watermarking for tamper detection and recovery with Run Length Encoding compression. World Academy of Science, Engineering and Technology. 2010; 72:799-803.

[7] Al-Qershi OM, Khoo BE. Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images. Journal of Digital Imaging. 2011; 24(1):114-25. https://doi.org/10.1007/s10278-009-9253-1.

[8] Kundu MK, Das S, editors. Lossless ROI medical image watermarking technique with enhanced security and high payload embedding. Pattern Recognition (ICPR), 2010 20th International Conference on; 2010: IEEE.

[9] 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. Journal of Digital Imaging. 2008; 21(1):77-90. https://doi.org/10.1007/s10278-007-9012-0.

[10] Pandey R, Singh AK, Kumar B, Mohan A. Iris based secure NROI multiple eye image watermarking for teleophthalmology. Multimedia Tools and Applications. 2016; 75 (22):14381-97. https://doi.org/10.1007/s11042-016-3536-6.

[11] Kumar B, Anand A, Singh S, Mohan A. High capacity spread-spectrum watermarking for telemedicine applications. World Academy of Science, Engineering and Technology. 2011; 79:2011.

[12] Nambakhsh M-S, Ahmadian A, Zaidi H. A contextual based double watermarking of PET images by patient ID and ECG signal. Computer methods and programs in biomedicine. 2011; 104 (3):418-25. https://doi.org/10.1016/j.cmpb.2010.08.016.

[13] Ansari IA, Pant M, Ahn CW. SVD based fragile watermarking scheme for tamper localization and self-recovery. International Journal of Machine Learning and Cybernetics. 2016; 7(6):1225-39. https://doi.org/10.1007/s13042-015-0455-1.

[14] Viswanathan P, Krishna PV. A joint FED watermarking system using spatial fusion for verifying the security issues of teleradiology. IEEE journal of biomedical and health informatics. 2014; 18(3):753-64. https://doi.org/10.1109/JBHI.2013.2281322.

[15] Gaidhane VH, Hote YV, Singh V. A new approach for estimation of eigenvalues of images. International Journal of Computer Applications. 2011; 26 (9):1-6. https://doi.org/10.5120/3136-4324.

[16] Hashemi-Berenjabad S, Mahloojifar A, Akhavan A, editors. Threshold based lossy compression of medical ultrasound images using contourlet transform. Biomedical Engineering (ICBME), 2011 18th Iranian Conference of; 2011: IEEE. https://doi.org/10.1109/ICBME.2011.6168553.

[17] Badshah G, Liew S-C, Zain JM, Hisham SI, Zehra A. Importance of watermark lossless compression in digital medical image watermarking. Research Journal of Recent Sciences ISSN. 2015; 2277:2502.

[18] Al-Haj A, Mohammad A. Crypto-watermarking of transmitted medical images. Journal of digital imaging. 2017; 30(1):26-38. https://doi.org/10.1007/s10278-016-9901-1.

[19] Al-Haj A. Secured telemedicine using region-based watermarking with tamper localization. Journal of digital imaging. 2014; 27(6):737-50. https://doi.org/10.1007/s10278-014-9709-9.

[20] Khor HL, Liew S-C, Zain JM. Region of Interest-Based Tamper Detection and Lossless Recovery Watermarking Scheme (ROI-DR) on Ultrasound Medical Images. Journal of digital imaging. 2017; 30(3):328-49. https://doi.org/10.1007/s10278-016-9930-9.

[21] Eswaraiah R, Reddy ES. Medical image watermarking technique for accurate tamper detection in ROI and exact recovery of ROI. International journal of telemedicine and applications. 2014; 2014:13. https://doi.org/10.1155/2014/984646.