

Fragile Watermarking Technique of Multi Watermarks for Medical Image Authentication

Mohammed Ayad Kadhum, Suhad A. Ali and Majid Jabbar Jawad
Department of Computer Science, College of Science for Women, Babylon University, Hillah, Iraq

Abstract: Medical images are transmitted to another remote place in telemedicine. Medical images need to be protected against any modification which made by the attacker through the unsecured channel. Watermark can be used to check the integrity of a medical image before diagnosis. In this study, a new fragile watermarking technique has been suggested for medical image authentication, tampering localization. In the suggested scheme, two watermarks have been used. The first one is used for checking whether the medical image has tampered or not. The second one is used for localizing the tampered region within a medical image. These watermarks are embedded in the frequency domain of the medical image. Experimental results showed that the suggested scheme can decide whether the medical image is tampered or not, accurately. In addition, the tampered region is localized perfectly.

Key words: Digital watermark, medical image, e-Healthcare system, image authentication, accurately, medical

INTRODUCTION

The medical image is used as a useful medium to assist in the diagnosis of diseases that afflict the patient. Also, medical images are used for hiding the patient's data and the purpose of reducing the cost of storing data and time to transfer data. The above-listed benefits make this image plays important role in the e-Health systems. In addition, the availability and efficiency of communication channels (especially, the internet) make using the medical image easily. For example, through internet, doctor A can send the medical image to doctor B to seek high-quality diagnosis or second opinions. The sending and receiving of the medical images are done easily on the communication channel. In the other word, the image is shared on the unsecured channel. So, anyone can copy, edit and resend any image by using the smart software. The above ability represents challenging for the medical. For example, anyone can tamper any region within medical image imperceptibility and resend it to the doctor. Consequently, the doctor may make a wrong diagnosing. Several techniques are suggested for preserving the privacy and integrity of the medical image. One of the best is watermarking techniques. Most medical images contain one or more important areas that contain important diagnostic information called the Region of Interest (RoI) and the remaining area called the Region of Non-Interest (RoNI). RoI is of great importance in diagnostic decision making and for this not preferable

to embed any data inside it to provide better protection without prejudice to the diagnosis information (Al-Qershi and Khoo, 2011). In addition, any tampering, modifications or alteration within this area should be detected when the medical image is transferred. Many watermarking techniques for image authentication have been suggested for the medical image.

Golpira and Danyali (2009) presented a scheme of using blind watermarking approach for medical image authentication based on histogram shifting. In this scheme, after applying Integer Discrete Wavelet Transform (IDWT) on the medical image, select two thresholds (T_1 , T_2) and create two Zero-points: Z_1 (Shift the left side of T_1) and Z_2 (Shift the right side of T_2) which are used during watermarking, the watermark information is embedded into the high-frequency sub-band regions of the transformed image. The experimental results showed that this proposed method is better in terms of enabling lossless reconstruction of both original and watermark image, provide high quality for the watermarked image and it provides higher efficiency compared to some other methods that based on histogram shifting.

In 2012, multilevel authentication for the medical image is presented by Liew *et al.* (2013). In this technique, the medical image is segmented into two parts Region of Interest (RoI) and Region of Non-Interest (RoNI). RoI is also divided into non-overlapping blocks of 40×40 pixels as well RoNI is segmented into non-overlapping blocks

of 2×2 pixels (two areas), one to add reliability information and another to add recovery information (multilevel authentication). To determine the location of the tampering, the value of the hash (using SHA-256) for the RoNI is calculated and compared with the added value of the hash (SHA-256) of the RNI. Each segment of the RoI is stored in an individual JPEG file which is used for recovery purposes. This technology has been implemented in the frequency domain. Where the recovery and reliability information has been embedded in the LSB and second LSB of each pixel in the RoNI. The results showed that the process of detecting and locating tampering and retrieving the site of tampering has been successful by up to 100%.

Eswaraiah and Reddy (2015) presented robust medical image watermarking technique for medical image authentication and recovery purpose. In this schema the medical image is divided into two parts Region of Interest (RoI) and Region of Non-Interest (RoNI), the hash value of the RoI is then calculated, RoI is compressed to be used as recovery data and by using Integer Wavelet Transform (IWT) this hash value, recovery data and data of patient (after converting it to binary format) are embedded into RNI. The experiments result showed that this proposed method gives sufficient strength to the embedded data within the RoNI and has a high accuracy and ability to locate tampering inside RoI with a possibility to recover the original RoI.

Cetinel and Cerkezi (2016) presented scheme for patient information authenticity based medical image watermarking. In this scheme the patient information has been hidden inside the medical image as a binary watermark for authentication purpose by using Discrete Wavelet Transform (DWT) to divide the medical image into LL, LH, HL and HH sub-bands and then applied Singular Value Decomposition (SVD) for each sub-band of the cover medical image. In this method, Arnold Cat Map (ACM) is applied to the watermarked medical image which is called (chaotic watermark) to improve the security of the method. The experiment's result showed that this proposed method gives higher PSNR values than compared some other methods and it can be applied to any type and size of medical images.

Thanki *et al.* (2017) proposed a scheme for medical image authentication by using visible watermarking. In this scheme, the Region of Non-Interest (RNI) has been chosen from the cover of medical image by using Human Visual System (HVS) Model. Then, visible binary watermark logo is embedded into RNI and by using zeros padding method watermark mask is created which embedded to cover medical image to create watermarked medical image. This scheme has been implemented in the

spatial domain. The experimental results showed that this proposed method is better in terms of lack of computational complexity and better PSNR (better in term of imperceptibility) compared to other methods. But one of the disadvantages of this method is that it can't locate the tampering nor recover the tampering area.

MATERIALS AND METHODS

The proposed scheme: The overall diagram of the suggested system consists of two stages: the embedding and extracting procedures.

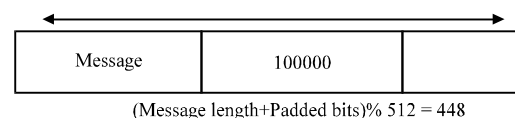
Embedding procedure: The embedding section can be listed as follows:

Medical image segmentation: In the proposed schema, Region of Interest (RoI) information is embedded into the Region of Non-Interest (RoNI) using block-based embedding in an IWT domain. To achieve this purpose, the medical image is divided into two areas (RoI and RoNI). Where RI is always determined by the specialist doctor.

Generation of watermarks: The suggested scheme uses two watermarks each one does the specific duty. These watermarks can be as follows:

Hash watermark (Hash 1): This watermark is used to check whether the medical image has tampered or not. During the extracting and verification procedure, the first step is using this watermark for checking the tampering decision, if the medical image has tampered the next steps will be done, otherwise, the next steps are not done. Approximately, most previous schemes don't use this watermark and do all next steps even if the image is tampered or not. So, the suggested scheme reduces the time needed for extracting and verification. Creation of hash watermark is done by MD5. MD5 is a cryptographic function that accepts a message of any length as input (the suggested scheme uses RI as input) and generates a digest of size 128 bits (32 hexadecimal digits) to be used for authenticating the original message. The work of the MD5 algorithm can be summarized in the following steps (Parashar *et al.*, 2017).

Append padded bits. A single "1" bit is appended to the message and then "0" bits are appended, so that, the length of the message in bits equals 448 modulo 512.



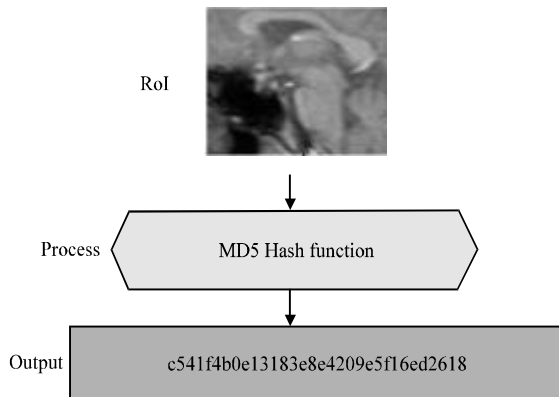
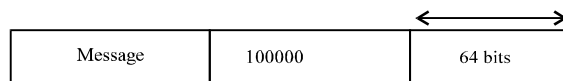


Fig. 1: The generation of MD5 Hash function (Hash 1)

Append length of the message: A 64 bit is appended to the end of the result of the previous step. The resulting message has a length that is an exact multiple of 512 bits.



Initialize MD buffer: Four-word buffer (A-D) is used to compute the message digest. Each of these buffers is a 32 bit register. These registers are initialized to the following values in hexadecimal:

Word A: 01234567
 Word B: 89abcdef
 Word C: fedcba98
 Word D: 76543210

Process message in 16-word blocks: Four auxiliary functions that take as input three 32 bit words and produce as output one 32-bit word:

$$F(X, Y, Z) = (X \wedge Y) \vee (\neg X \wedge Z)$$

$$G(X, Y, Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$$

$$H(X, Y, Z) = X \oplus Y \oplus Z$$

$$I(X, Y, Z) = Y \oplus (X \vee \neg Z)$$

Output: The message digest (Hash 1) produced as output is A-D. That is output begins with the low-order byte of A and end with the high-order byte of D. Figure 1 illustrates a case study of generation hash watermark (Hash 1) in our proposed system.

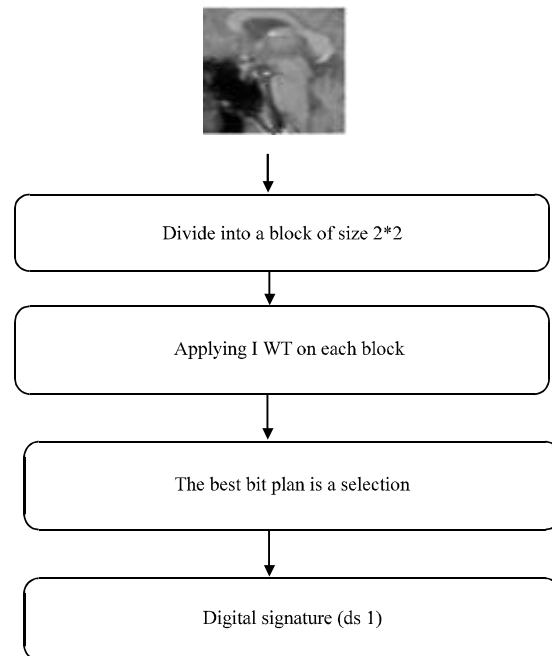


Fig. 2: The creation of digital signature (ds 1)

Digital signature (ds 1): This watermark is used to localize the tampered region within an image. This watermark is used just when hash watermark (Hash 1) decide that image has tampered. Figure 2 illustrates the creation of digital signature from the RoI. The generation phase of digital signature (ds1) takes several stages as shown in Fig. 2. These stages are:

Divide the ROI into 2*2 non-overlapped blocks. Applying Integer Wavelet Transforms (IWT). The purpose of using IWT in our proposal is to avoid fractional calculations and reduce the arithmetic time of the algorithm. Where it maps integers to integers. Since, the coefficients of IWT are integers, so, it is possible to achieve the ideal reconstruction of the transferred image (Piao *et al.*, 2008).

The best bit plan selection: in this step an effective bit plane will be selected. At this tests stage on different planes of ROI to select the best one. The selection of bit plane depends on the variation of zeros (0) and ones (1) values in each plane. At first, the IWT is applied on the 2*2 block, then the four values convert to it's bit planes as shown in Fig. 3.

This process will have applied to all blocks in RoI. Then count the number of ones and zeros in each bit planes from plane 0 to plane (2^{bi}) where (bi) represents number of bits. The bit plane that is selected must satisfy the condition absolute difference between count 0 and count 1 is the minimum. As shown in Fig. 3,

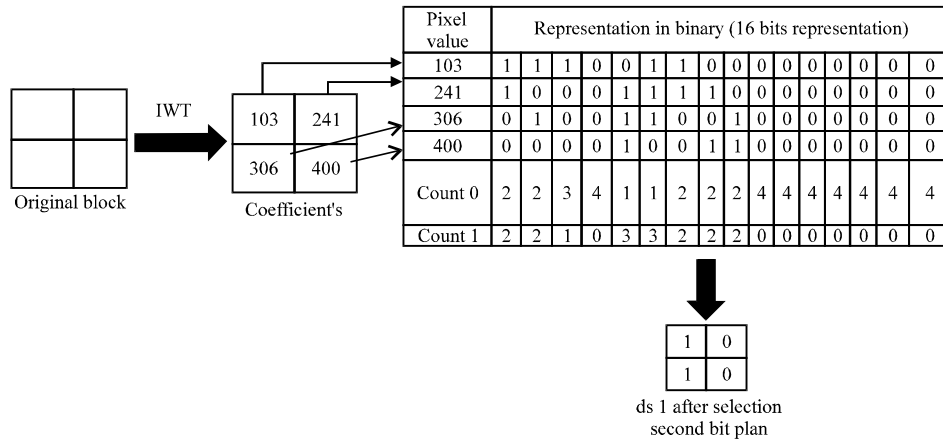


Fig. 3: The process of select the best bit plan

the second bitplane in most pixels is variable. This change helps determine the area of manipulation. Output: After choosing the second bit in the previous step we will get the digital signature (ds1).

Embedding the watermarks: The process of embedding watermarks to RONI begins after the watermarks have been converted into binary form. These watermarks are stored in the form of a single matrix. The first stages of this process begin with dividing the RONI into non-overlapping blocks of size 2×2 . The applying IWT on each of this block. RONI is transformed into the frequency domain which divided (decomposed) the RONI into four subbands ss, sd, ds and dd. Two bits of watermark data are embedded in the middle position (mid = 2 (second -bit plane)) of each sub-band (sd, ds and dd) of each block of RONI. Repeat this steps until all bits of the watermark data are embedded and formed watermark RONI.

Note: A problem that may arise after embedding watermarksis that a probability of overflow (the value of some pixels in the RONI blocks of watermarked image may exceed the upper bound ($2^{bi}-1$)) or underflow (the value of some pixels in the RONI blocks of watermarked image may exceed the lower bound (0)).

There are two methods for overcoming the above problem (Eswaraiah and Reddy, 2015). Identifying the blocks that cause this problem and ignore it during the embedding process. Using histogram shifting (in this method, the pixels whose values are close to zero or $2^{bi}-1$ are shifted towards the center).

In the proposed scheme, the second method (histogram shifting) is used. Algorithm 1 illustrates the embedding watermarks operations.

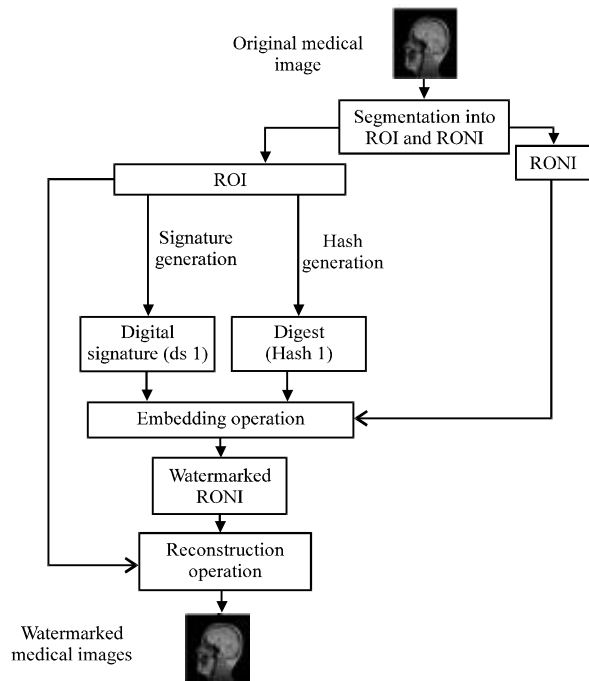


Fig. 4: Embedding procedure

Algorithm 1; The embedding watermarks algorithm:

Input: watermarks (secret)

Output: watermark medical image

Start:

- 1: Divided RoNI into non-overlapped 2×2 blocks
- 2: Apply Integer Wavelet Transform (IWT) on each block
- 3: Embed twowatermark bits in each sub-bands (sd, ds and dd) of each block
- 4: Repeat the above steps until all bits are embedded
- 5: Applying inverse IWT on each watermarked block
- 6: Reconstruct all watermarked blocks to get watermarked RONI
- 7: Merge ROI with watermarked RONI to get WMI

End

The block diagram of embedding procedure is shown in Fig. 4. The detail of the embedding procedure is

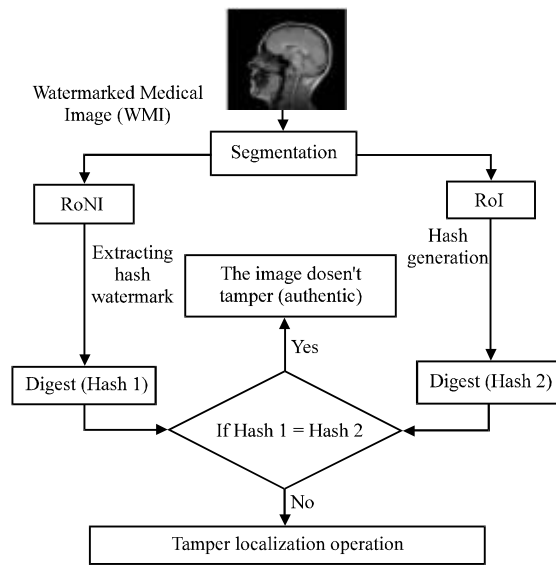


Fig. 5: The extracting and authentication operation

illustrated in algorithm 2. After the completion of embedding processes, the ROI is combined with RONI to configure Watermarked Medical Image (WMI).

Algorithm 2; The embedding algorithm:

Input: Medical Image (MI)

Output: Watermarked Medical Image (WMI)

Start:

- 1: Segment the MI into two regions, namely Region of Interest (RoI) and Region of Non-Interest (RoNI)
- 2: Generate two watermarks (Hash 1, ds1) from RoI as explained in section 2.1.2
- 3: Convert (Hash1, ds1) watermarks into binary format and combined into a vector (secret)
- 4: Embed the watermarks (secret) in the RoNI using algorithm 1

End

The extracting and verification procedure: Figure 5 illustrates the extracting and authentication operations. The details of extracting and authentication operations are illustrated in algorithm 3. Figure 6 illustrates the tamper localization operations. The localization and operations are illustrated in algorithm 4.

Extracting the watermarks data from RONI: At this procedure, the following steps are done to extract the watermarks data from RONI:

- Divided RONI into non-overlapped 2*2 blocks
- Apply Integer Wavelet Transform (IWT) on each block
- Extract twowatermark bits from each sub-band (sd, ds and dd) of each block
- Repeat the above steps until all bits are extracted

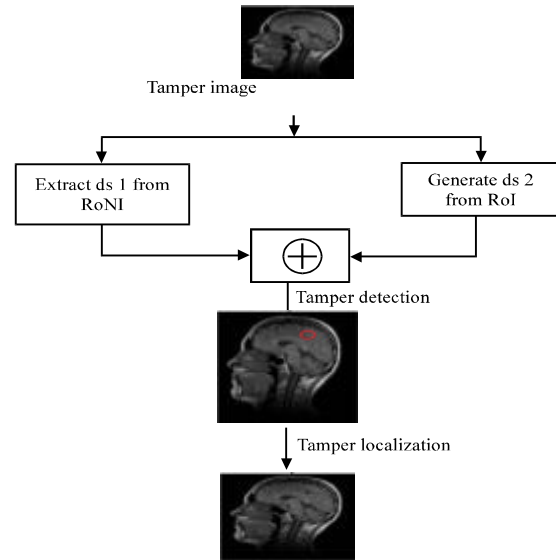


Fig. 6: The tamper localization operation

Algorithm 3; The tamper detection algorithm:

Input: Watermarked Medical Image

Output: Medical image (tampered or not)

Start:

- 1: Segment the watermarked medical image into two regions (RoI and RoNI) using the coordinates of RoI which sent to the receiver
- 2: Generate hash value of RoI (Hash 2) by using MD5 hash function method using the steps
- 3: Extract hash 1 from RoNI by using the same steps
- 4: Compare hash1 with hash2
- 5: If hash1== Hash2 then
The medical image does not tampered (the medical image is ready for diagnosing)
else

do localization algorithm (for localizing the tampered region).

End

Algorithm 4; The localization algorithm:

Input: Tampered Medical Image

Output: a localized tampered region in Medical Image

Start:

- 1: Generate digital signature (ds2) from RoI by using the same steps
Extract digital signature (ds1) from RONI by using the same steps
- 3: Applying XOR between (ds1 and ds2) resulting binary matrix (A (X, Y))
- 4: Divide ROI into non-overlapped 2*2 blocks
- 5: To identify tampered blocks in ROI, repeat steps 6 for each block B in RoI
- 6: If at least one a value in arrayA (X, Y) at allocation (X, Y) resulting from step 3 equal (1) then Mark block B around X, Y as tampered

End

RESULTS AND DISCUSSION

When designing any watermarking algorithm, knowing the efficiency and effectiveness of this algorithm and evaluating its performance is very important

(Saini and Shrivastava, 2014). The benchmarks that have been used to measure image deterioration or (an image watermarking method or algorithm) in our experiments are:

Mean Square Error (MSE): It is one way to compare two images (host image and watermark image) based on pixel pixels (Priya and Sadasivam, 2014) or it is a way to computes the average of the squares of the “errors” between the original image and its watermark version (Saini and Shrivastava, 2014). Mathematically MSE can be represented as follows:

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (p_1(i, j) - p_2(i, j))^2 \quad (1)$$

Where:

$p_1(i, j)$ = The original image and

$p_2(i, j)$ = The watermarked image

m, n = Represent the dimensions of two images

The distortion rate is high whenever the value of the MSE is high. In other words, the closer the MSE value of zero is the better (Priya and Sadasivam, 2014).

Peak Signal-to-Noise Ratio (PSNR): It is one of the methods of measuring the visual quality of the embedded image, it is used to measure the ratio of the distortion between the original image and its watermark version (Priya and Sadasivam, 2014). Or it is used to know the efficiency of the watermark in terms of noise (Saini and Shrivastava, 2014). Mathematically PSNR can be represented as follows:

$$PSNR(I, I_w) = 10 \log_{10} \left[\frac{(I_{MAX})^2}{MSE(I, I_w)} \right] \quad (2)$$

Where:

I = The original image

I_w = The watermarked image and

I_{MAX} = The maximum grey level of the image

In this case, I_{MAX} can have a maximum value of 255. The rate of distortion is very small whenever the value of the PSNR is high. There are some scholars such as Chen and Ramabagran (Priya and Sadasivam, 2014) who mentioned that the value of PSNR is acceptable if it is between 40 and 50 dB.

Experiments were conducted on 60 more medical images. In order to test the performance of the suggested scheme, we select several medical images. Figure 7 illustrates the selected test images.

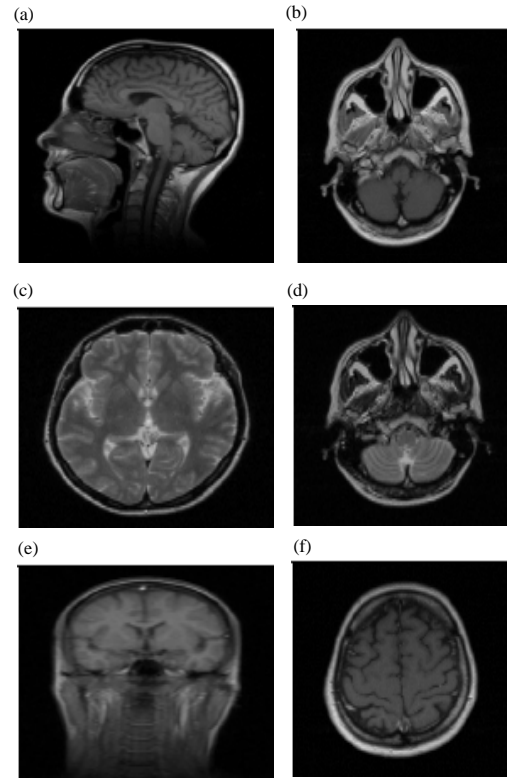


Fig. 7a-f: Selected test medical images

Table 1: Original medical image, watermarked medical image, size of ROI and values of PSNR

Original medical image	Watermarked medical image	Size of ROI (bits)	MSE	PSNR
		13872	1.5947	70.2205
		5616	0.6290	74.2605
		45696	4.7625	65.4688
		24288	2.4855	68.2930
		8064	1.1379	71.6863
		13872	1.5166	70.4385

Testing fidelity performance: Table 1 illustrates the medical images before and after implementing the suggested scheme. As shown in Table 1, the distortion

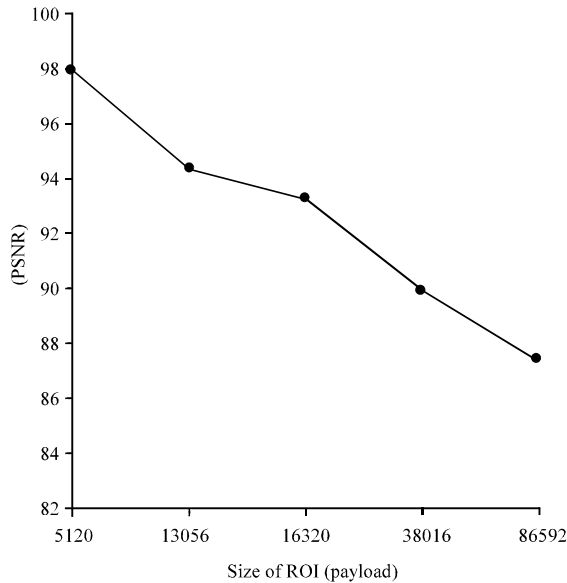
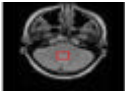
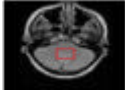


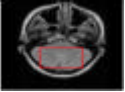


Fig. 8: Size of ROI (payload) vs. PSNR

Table 2: PSNR vs. size of ROI (payload)

Original medical image (with various selected ROIs)	Size of ROI (payload) (bits)	MSE	PSNR
	5120	0.6964	97.9010
	13056	1.5781	94.3482
	16320	2.0384	93.2366
	38016	4.4076	89.8876
	86592	7.8907	87.3584

visually is imperceptible. In medical image watermarking schemes, the preferred value of PSNR must be more than 40 dB (Eswaraiah and Reddy, 2015). The resultant of PSNR of the suggested scheme is more than 40 dB.

In order to show the relationship between PSNR and the size of ROI (payload), Table 2 and Fig. 8 illustrate this relationship.

Table 3: Tamper localization




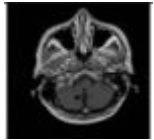

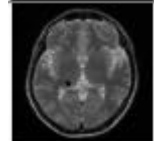

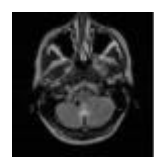
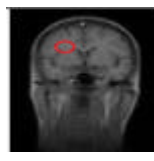
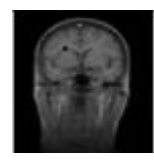

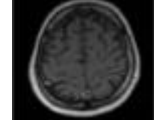
Tampered image (watermarked image)	Localized tampered region
	
	
	
	
	
	

Table 2 and Fig. 8 shows the relationship between PSNR and the size of ROI (payload) is an inverse relationship. As the size of the ROI increases, the value of the PSNR decreases. Therefore, the specialists (doctors) must choose the ROI perfectly.

Tamper localization testing: This section illustrates the performance of the suggested scheme, related to tampering localization region. Table 3 shows the localized tampered region within a medical image. Table 3 illustrates that the suggested scheme localizes the tampered image accurately.

Table 4 illustrates the comparison between the proposed method and some proposed schemes. Table 4 shows that the suggested scheme satisfied more requirements of medical image watermarking related to authentication applications.

Table 4: Comparison between the proposed scheme and the previously proposed schemes

Reference No.	Embedding distortion inside ROI	Identify blocks tampering accurately inside ROI	Recovery of original ROI	Identification of ROI is received medical image	Size of data embedded inside RONI	Robustness of the data stored within the RONI
10	Yes	No	No	Specified	Specified	Yes
11	No	Yes	No	Not specified	Not specified	Yes
12	-	-	No	Specified	Not specified	No
13	-	-	No	-	-	No
14	No	-	Yes	Not specified	Not specified	No
15	Yes	-	No	-	-	-
The proposed scheme	No	Yes	No	Specified	Specified	No

CONCLUSION

In this study, a fragile watermarking scheme is presented for medical image authentication. This scheme is used for checking whether the medical image has tampered or not. The presented scheme is used for helping the specialist in diagnosing the disease by medical image where any tampering on the medical image may leads to the false diagnosing. Consequently, may cause the death of the patient. So, the suggested scheme can be used as a recommendation system for choosing the true (authentic) image before diagnosing procedure. In addition, the suggested scheme has the ability for recovering the tampered region. With the suggested scheme the watermark is embedded in the frequency domain which is preferred domain. The suggested method is reduced the time consuming for image authentication operation by using hashing operation where most suggested scheme doesn't take the time consuming into account. The experimental results illustrate that the suggested scheme has the ability to localize even tiny tampered region.

REFERENCES

- Al-Qershi, O.M. and B.E. Khoo, 2011. Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images. *J. Digital Imag.*, 24: 114-125.
- Cetinel, G. and L. Cerkezi, 2016. Wavelet based medical image watermarking scheme for patient information authenticity. *Intl. J. Appl. Math. Electron. Comput.*, 1: 220-223.
- Eswaraiah, R. and E.S. Reddy, 2015. Robust medical image watermarking technique for accurate detection of tampered inside region of interest and recovering original region of interest. *IET. Image Process. Inst. Eng. Technol.*, 9: 615-625.
- Golpira, H. and H. Danyali, 2009. Reversible blind watermarking for medical images based on wavelet histogram shifting. *Proceedings of the IEEE International Symposium on Signal Processing and Information Technology*, December 14-17, 2009, Ajman, pp: 31-36.
- Liew, S.C., S.W. Liew and J.M. Zain, 2013. Tamper localization and lossless recovery watermarking scheme with ROI segmentation and multilevel authentication. *J. Digital Imaging*, 26: 316-325.
- Parashar, A.R., S. Lakhani and M. Gautam, 2017. Image encryption and authentication using repetitive application of linear transformations and MD5. *Proceedings of the 4th International Conference on Latest Trends in Engineering, Science, Humanities and Management (ICLTESHM-7)*, May 7, 2017, Indian Federation of United Nation Associations, New Delhi, Delhi, India, ISBN:978-93-86171-37-5, pp: 108-118.
- Piao, C.R., D.M. Woo, D.C. Park and S.S. Han, 2008. Medical image authentication using hash function and integer wavelet transform. *Proceedings of the 2008 Congress on Image and Signal Processing (CISP'08) Vol. 1*, May 27-30, 2008, IEEE, Sanya, Hainan, China, ISBN:978-0-7695-3119-9, pp: 7-10.
- Priya, R.L. and V. Sadasivam, 2014. A survey on watermarking techniques, requirements, applications for medical images. *J. Theor. Appl. Info. Technol.*, 65: 103-120.
- Saini, L.K. and V. Shrivastava, 2014. A survey of digital watermarking techniques and its applications. *Intl. J. Sci. Res.*, 2: 1-5.
- Thanki, R., S. Borra, V. Dwivedi and K. Borisagar, 2017. A RONI based visible watermarking approach for medical image authentication. *J. Med. Syst.*, 41: 1-11.