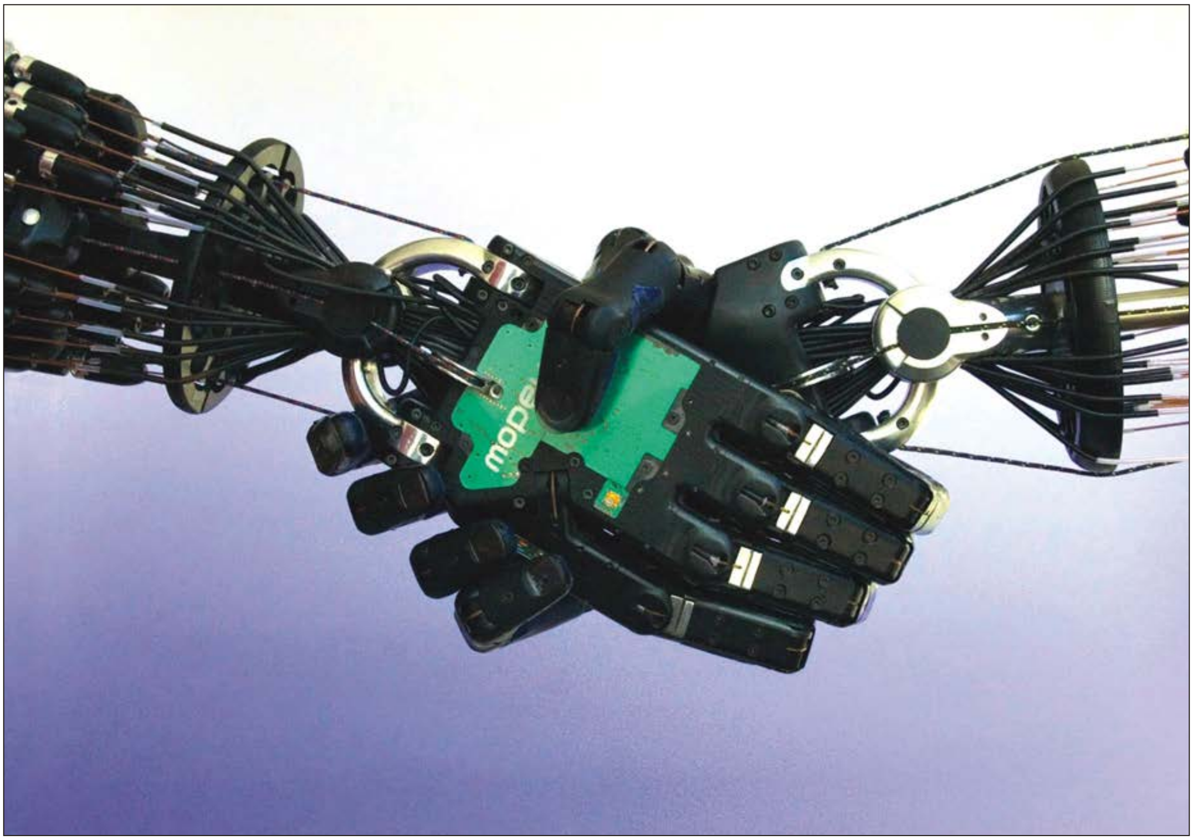

Journal of Artificial Intelligence

ISSN 1994-5450

OPEN ACCESS Journal of Artificial Intelligence

ISSN 1994-5450
DOI: 10.3923/jai.2017.32.41

Research Article
Watermarking for Content Integrity and Ownership Control of Medical Images

Fawaz Waselallah Alsaade

Department of Computer Science, College of Computer Science and Information Technology, King Faisal University, Hofuf, P.O. Box 380, 31982 Al-Ahsa, Saudi Arabia

Abstract

Background and Objective: Generally, there is problem of integrity and security of digital medical images contents for transferring from one hospital to another. There is no perfect procedure to protect and secure medical images from unauthorized users. The main objective of this study was to present a medical image watermarking system by hiding some secret codes in the medical images for verification of its integrity and ownership. **Materials and Methods:** The study integrated three different techniques namely the spatial domain watermarking, Least Significant Bit (LSB) and cryptographic hash functions for developing a medical image watermarking scheme. The study embedded three watermarks namely the Electronic Patient Record (EPR), index code (IDX) and doctor's ID (DID) for developing the watermark system. The Message Authentication Code (MAC) was calculated of the center part of original image and then compared with the MAC calculated from the received watermarked image for verifying the integrity of image content. The proposed medical image watermarking method utilized the Least Significant Bit (LSB) and was compared with dual watermarking (DUALWM) technique for accuracy. **Results:** The proposed LSB method utilized 8064 pixels for embedding the watermark information from a CT scan image as compared to 50400 pixels used by DUALWM technique. Consequently it required less time for segmentation process and delivered high rates of PNSR ratio for watermarked images. The proposed LSB method introduced less noise in the input image resulting in the production of watermarked images of high level imperceptibility. Additionally, the bandwidth required for the proposed LSB method was low as both the text and image files are transmitted as single entity instead of two separate files. **Conclusion:** The proposed LSB method is preferred over DUALWM technique because it does not require either additional memory storage or time overhead. The proposed system can facilitate the public and private sectors by providing security in the medical image data base archiving and retrieving systems.

Key words: Medical image watermarking, image content integrity, copyright protection, LSB substitution, hash algorithm, ROI, RONI

Received: September 16, 2016 Accepted: November 30, 2016 Published: December 15, 2016

Citation: Fawaz Waselallah Alsaade, 2017. Watermarking for content integrity and ownership control of medical images. J. Artif. Intel., 10: 32-41.

Corresponding Author: Fawaz Waselallah Alsaade, Department of Computer Science, College of Computer Science and Information Technology, King Faisal University, Hofuf, P.O. Box 380, 31982 Al-Ahsa, Saudi Arabia

Competing Interest: The author has declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

INTRODUCTION

Medical practitioners send medical information from one medical center to another through a reliable source such as the internet. This information contains medical images and diagnostic reports of the patient. Such information is exchanged for training and research and sometimes to obtain second opinion from the other doctor[1]. In order to ensure safety, legitimacy and administration of medical images and information, it is important to develop more reliable and secure techniques to handle such issues. The integrity deals with the confidentiality of patent's medical information which is private and personnel. Whereas security problem refers to the safety of medical information either from hacking or its modification by unauthorized persons from the hospitals, medical institutions and other private medical facilities. Recently digital watermarking approaches were developed to safeguard the medical evidences[2]. Basically, digital watermarking is a process of hiding or implanting an imperceptible signal (hidden data) called watermark using some secret key in the source media called as the cover work. The watermark should be embedded into the cover work in such a way that it should be robust enough to survive not only as the most common signal distortions, but also distortions caused by malicious attacks. The cover work can be an image, audio or video. A watermark algorithm usually consists of two phases namely an embedding phase and an extraction phase. The block diagrams of both the embedding and extraction phases are shown in Fig. 1a and b, respectively. Many investigators concluded that digital watermarking can be used for integrity and ownership control of the contents of medical images[3-5]. However, when the information is implanted inside the medical image, the watermarking does not show significant difference between the cover and the watermarking image. In this way watermarked image can easily be used for diagnosis by the medical practitioners.

Previously, many medical image watermarking techniques were reported. Al-Qershi and Khoo[6] reported a hybrid medical image watermarking scheme for DICOM medical images. According to their investigation, the scheme first segments the input medical image into Region of Interest (ROI) and Region of Non Interest (RONI). Then the Electronic Patient Record (EPR) and ROI hash message are implanted into ROI using reversible method as described by Tian[7]. The control of image integrity is achieved by implanting the watermark information consisting of ROI embedding map, the average value of block inside ROI, compressed form of ROI and recovery information in RONI using the Discrete Wavelet Transform (DWT). Finally using the DWT technique, a third watermark was implanted into border pixels of RONI containing the information about vertices to define ROI and the number of bits in the second watermark. Since the ROI is selected manually, therefore it is very time consuming process. Furthermore, the EPR is implanted in ROI by means of fragile watermark and it is not an appropriate method because the EPR is an important asset in medical image watermarking. Also due to its fragile nature, it can be lost due to some legitimate or illegitimate attacks performed on watermarked image. While, Vismanathan and Krishna[8] presented a medical image watermarking technique based on watermarking and cryptography. The EPR of the patient is encrypted first and then it is implanted in the input medical image using bit-wise operation for proving the authenticity of image content. However, in order to overcome the distortion introduced in the medical image, reversible watermarking technique was used to take the watermarked image back to its pristine state. The researchers claimed that their proposed technique might provide high embedding capacity, low computational complexity and best security. However, this technique is not efficient to tackle the problem of underflow and overflow and only supports 8 bits gray level medical images. In another study, Tjokorda *et al.*[9] reported a medical image watermarking technique where the size of ROI is more than the size of RONI. In this technique, all the LSBs of the input medical image were collected first and then set to zero. Later, the input image was divided into ROI and RONI regions followed by further sub-division into blocks of 6×6 and 6×1 size, respectively. A map was prepared into blocks of ROI to embed the recovery information to its mapped block. The stored original LSBs were compressed using RLE technique and then embedded into two LSBs of 6×1 blocks in RONI. The main drawback of this technique was that it does not involve any verification information to verify the authenticity of the entire ROI with

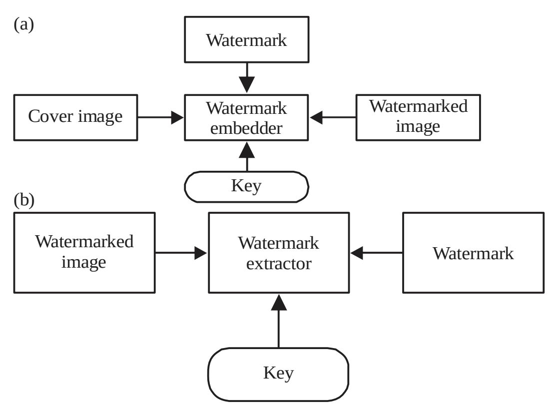

Fig. 1(a-b): Block diagram of (a) Embedding phase and (b) Extraction phase respect to its tempering. While, Deng *et al.*[10] presented a medical image watermarking technique based on reversible watermarking and quad tree decomposition with a major limitation of non-recovery of the input image to its pristine state after tempering.

The main objective of this study was to present a medical image authentication and verification system where the medical image database should be accessible safely only to authorized users.

MATERIALS AND METHODS

Proposed medical image watermarking system: In medical image archiving and communications systems, the EPR is usually stored and communicated by the image file and the text file. The image file is of any modality, such as, XRAY, MRI, CT scan or ultrasound etc., while the text file contains patient personal information and diagnostic report. However, there are a number of limitations in communicating the patient in two files. These limitations include; memory overhead: A separate storage space will be required for both the EPR and medical images, bandwidth overhead: Large amount of bandwidth will be required for the transmission of EPR and medical images if transmitted separately in the electronic environment such as telemedicine and the detachment threat: If the EPR and the image are separate, the chance of detachment of patient data from the image is too high. Thus, there can be a great chance of accessing wrong patient data due to detachment which may lead to wrong diagnosis by medical practitioner located at long distances[11]. Due to these facts, this study presented a watermarking method in which text information is embedded into its corresponding medical image to save memory, bandwidth and avoiding detachment on one side and providing the image content integrity and ownership control of medical image on other side. The scheme utilized the simple LSB substitution method.

Watermark embedding: The block diagram of proposed LSB method for implanting different watermarks in the input image is given in Fig. 2. The main steps for watermarking embedding process are:

Step 1: Divide the input image I into two parts, the border B and the center C

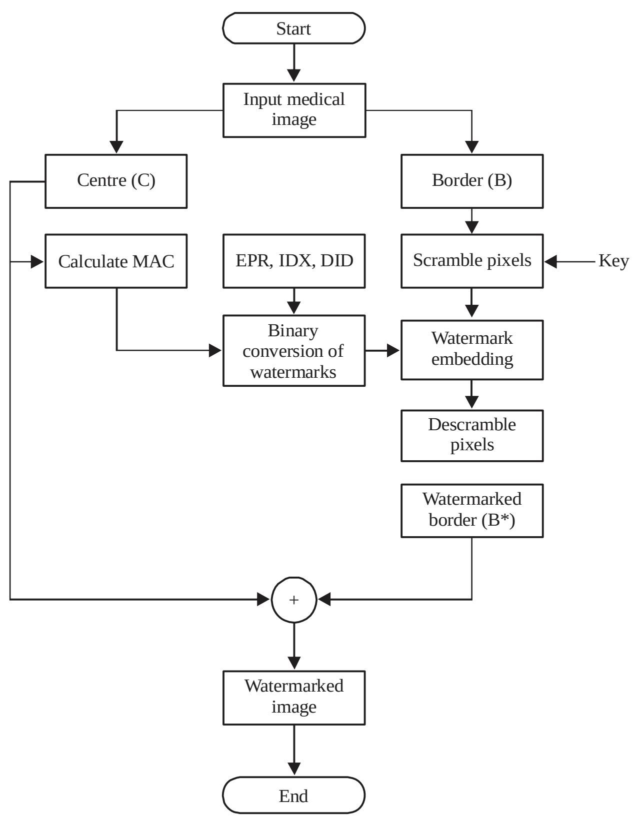

Fig. 2: Block diagram of proposed LSB method for implanting different watermarks in the input image, EPR: Electronic patient record, IDX: Index code, DID: Doctor's identified designation, MAC: Message authentication code, LSB: Least significant bit

Step 2: Generate the watermarks EPR, IDX, DID and MAC

Step 3: Embed EPR in top and bottom regions of border B by scrambling the pixels using some user defined key k and utilizing the first bit plane of B

Step 4: Embed IDX and DID in the left region and MAC in the right region of B, by scrambling the pixels using same user defined key, k as used in step 3 and utilizing the first bit plane of B

Step 5: Descramble the pixels of B to get the watermarked border B*

Step 6: Combine both B* and C to get the watermarked image I*

Generation of watermarks: The proposed method embeds different watermarks to achieve integrity and ownership control of medical images. A summary for the generation of these watermarks and step by step definition of algorithm are presented in the following.

Electronic Patient Record (EPR): The EPR contains patient's personal record (e.g., name, sex, age, etc.) and examination data (e.g., demographics, health history and diagnostic reports). In the proposed method, about 512 alphabetic characters of patient record were first read through text file, then each character was converted into its corresponding ASCII code and consequently each ASCII code was converted into its corresponding binary number of 8 bits in length. Finally all binary numbers were EPR = [epr(i), epr$\in$\{0 1\}, $1\leq i\leq 4096$].

Index code (IDX): A 16-character index code was used for facilitating image retrieval by database querying mechanisms. The insertion of indices into the images provided an alternative for efficient indexing and archiving of digital medical data in hospital information systems, which eliminates the storage and transmission bandwidth requirements. The 16-character index watermark was converted into binary vector with the same procedure as has been done for EPR such that IDX = [idx(i), idx$\in$\{0 1\}, $1\leq i\leq 128$].

Doctor's ID (DID): The doctor's ID contains physician's identification code or digital signature for image authentication or ownership. A pseudo random binary vector of 128 bits was generated based on the user's defined key, such that DID = [did(i), did$\in$\{0 1\}, $1\leq i\leq 128$].

Message Authentication Code (MAC): The MAC was calculated of the center part of original image and then compared with the MAC calculated from the received watermarked image for verifying the integrity of image content. For calculating MAC, the image was divided into two parts such as the border part (B) and the center part (C). Then MD5 algorithm was applied on the center part to calculate the MAC. This gave 32-character string. Each character of MAC was then converted into its corresponding binary number by following the same procedure as that for the creation of the binary vector EPR and IDX. The final binary vector for MAC is created in such a way that, MAC = [mac(i), mac$\in$\{0 1\}, $1\leq i\leq 256$].

The proposed system presents a medical image watermarking scheme that integrates three different techniques namely the spatial domain watermarking, Least Significant Bit (LSB) and cryptographic hash functions. These are described in the following.

Spatial domain watermarking: The spatial domain watermarking is considered as the best conventional method to conceal the watermark information into the cover content[12-14]. Historically watermarking started from the ancient times and is continued till today. For example: Watermarks in the paper bills were used in ancient times as in the present time all around. In an early research of watermarking algorithms, researchers usually used to add pseudo-random noise patterns as watermarks for both the embedding and extractions algorithms by changing the pixels values in spatial domain. Although the watermarks in spatial domain were embedded without any struggle but they are not robust i.e., that can easily be changed by simple manipulations.

Least Significant Bit (LSB) modification technique: The LSB alteration is usually used to insert watermark in the image content for watermarking[15-17]. The technique is based on the management the LSBs of images in such a way that it is untraceable and invisible to naked eye. The basic idea in LSB technique is that the LSBs of the actual 8 bits gray level image are disposed off first, then the LSBs are exchanged with the shuffled binary watermark of the same size as the original image to produce the watermarked image. In some applications, the LSBs of original image are compressed using some lossless compression algorithm. For example, the Run Length Encoding (RLE) or the Arithmetic Encoding (AE) needs to spare room for inserting the watermark. This way, the original image can be obtained to its pristine state by undoing the watermark process. Because, the LSB substitution technique is very easy to implant without any significant distortions in watermarking image.

Hash function for MAC calculations: A cryptographic hash function h takes a message of arbitrary length as an input and produces a message digest of fixed length as an output, for example 256 bits. Where certain properties should be satisfied:

- Given a message m, the message digest h(m) can be calculated very quickly
- Given a message digest y, it is computationally infeasible to find an m with h(m) = y (in other words, h is a one-way or pre-image resistant function)
- It is computationally infeasible to find messages m_1 and m_2 with $h(m_1) = h(m_2)$ (in this case, the function h is said to be strongly collision-free)

Different hash functions were found in the literature. However, secure hash algorithm (SHA-1) and message digest-5 (MD5) are frequently used for producing MACs. A hash function takes an input of arbitrary length and produces a message digest. Many investigators used hash functions in applications like authentication and copyright protection of digital content[18-20].

Evaluation metrics: The two evaluation metrics namely the Peak Signal to Noise Ratio (PSNR) was used for checking the imperceptibility of watermarked images and the Normalized Hamming Distance (NHD) to compare the embedded and extracted watermarks. The detail of each metric is given below.

Peak Signal to Noise Ratio (PSNR): In watermarking process, the imperceptibility of watermarked image is very important. It can be defined as how much noise was introduced in the cover image after embedding the watermark. Generally, PSNR metric is used for this purpose. If the value of PSNR is high, then the quality of the watermarked image is also considered as very high. It was reported that the image having the PSNR value equal to or higher than 38.00 dB is considered as good watermarked image. The PSNR is calculated by Eq. 1. Where, I_{max} is the maximum gray value in the input image which is usually considered as 255. The MSE is the mean square error and is calculated as given in Eq. 2. In Eq. 2, I_1 is the cover image and I_2 is the watermarked image[16]:

$$PSNR = 10\log_{10}\frac{I_{max}^2}{MSE} \tag{1}$$

$$MSE = \frac{\sum_{M,N}[(I_1(m,n) - I_2(m,n))]^2}{M \times N} \tag{2}$$

Normalized Hamming Distance (NHD): In order to verify the integrity and copyright protection of input medical image, the reference watermark is embedded in the cover image in the embedding phase and the extracted watermarked obtained at the extraction phase are compared. The NHD measure is usually used to compare the reference and the extracted watermarks bit by bit[21]. Value of 1 is recorded if both the reference and extracted watermarks bit are the same, otherwise value of 0 is recorded. The NHD is defined by the formula as given in Eq. 3:

$$NHD(w, w^*) = \frac{1}{N_w}\sum_{i=1}^{N_w} w(i) \oplus w^*(i) \tag{3}$$

where, w in the input watermark, w* is the extracted watermark and N is the length of the watermark. The range of NHD is always between 0 and 1. The lower the value of NHD, the better the quality of extracted watermark. The distance of 0 is considered best value for NHD.

Recently Memon *et al.*[5] presented a medical image watermarking technique, which inserts two marks into the input CT scan medical image. The technique is based on image segmentation, digital image morphology and LSB substitution method which is referred as the dual watermarking (DUALWM) technique in this study. In DUALWM technique, on embedding side two different watermarks namely the binary pattern and composite watermark are implanted into ROI and RONI regions, respectively in the input CT scan medical image. The binary pattern serves for the detection of tampers in ROI, whereas composite watermark serves for the copyright protection of the input image. Whereas, on the extraction side, the watermarks are extracted and compared with the reference watermarks for checking the content integrity and image ownership. The main limitations of this technique are: (i) The scheme require additional time overhead for segmenting the input CT scan image into ROI and RONI regions, (ii) Need more time of extraction for bringing back the image to its pristine state, (iii) The scheme introduces the noise in the whole RONI area after embedding the robust watermark covering about 76% area of the entire image and (iv) The scheme is confined only to CT scan medical images. A new LSB method was presented in this study that overcomes these limitations.

Watermark extraction: Few steps of watermark extraction process are the same as the embedding procedure. The block diagram of extraction process is given in Fig. 3 and step by step description of extraction procedure is given below:

Step 1: Divide the watermarked image I* into two parts, the border B* and the center C*

Step 2: Scramble all pixels of B* using the same user defined key k that was used at the time of embedding

Step 3: Calculate new MAC from the received image

Step 4: Extract the watermark EPR from the top and bottom parts of the border B by utilizing the first bit plane

Step 5: Extract IDX* and DID* from the left region and MAC* from the right region of B*

Step 6: The new calculated MAC was compared with extracted MAC*. If the authentication codes of both the messages are equal, then the content of the image is authentic and image integrity is maintained, otherwise image has been tampered during transmission

Step 7: If the extracted DID* and the reference DID (already received by doctor through some other source such as mobile phone) are equal, then the image belongs to the doctor who sent the image. Thus copyright control was maintained. Otherwise the image is not related to the source and is not authentic

RESULTS AND DISCUSSION

After generating the watermarks, these were embedded in the medical images and then extracted to verify the content integrity and copyright control of medical images. In order to show the validity of the proposed system, it was compared with the DUALWM technique. The watermarks were implanted in the border pixels B by utilizing the first bit plane. Figure 4a shows the input medical images of different modalities (e.g., CT scan image, x-ray image, MRI image, ultrasound image), Fig. 4b shows the corresponding watermarked images and Fig. 4c shows the residual images i.e., the difference between the original image and watermarked image. A total of four watermarks were embedded in upper, lower, right and left regions of B. The total binary information implanted was 4.5 kb. The size of input medical image was fixed as 256×256 pixels, whereas the size of border for implanting the watermark information was taken as 8×8 pixels. However, the proposed LSB method can be used for any size of medical images by selecting borders of different sizes. The residual images in Fig. 4c also showed that high amount of information is embedded in lower and upper border by scrambling the pixels and small amount of information is embedded in the left and right regions of the border pixels. Thus the upper and lower borders are highly thick populated with watermark information as compared to left and right borders which are highly thin populated with watermark information. In order to measure the noise introduced in the input image after watermarking, PSNR metric was used. The PSNR for each watermarked image is shown in Fig. 4c.

In order to check whether the information is being embedded effectively, the proposed LSB method read the first bit plane of top and bottom border pixels and converted these pixels into chunks of 8 bits. After converting each binary chunk in its corresponding ASCII code and successively converting each ASCII code into its corresponding alphabetic character,

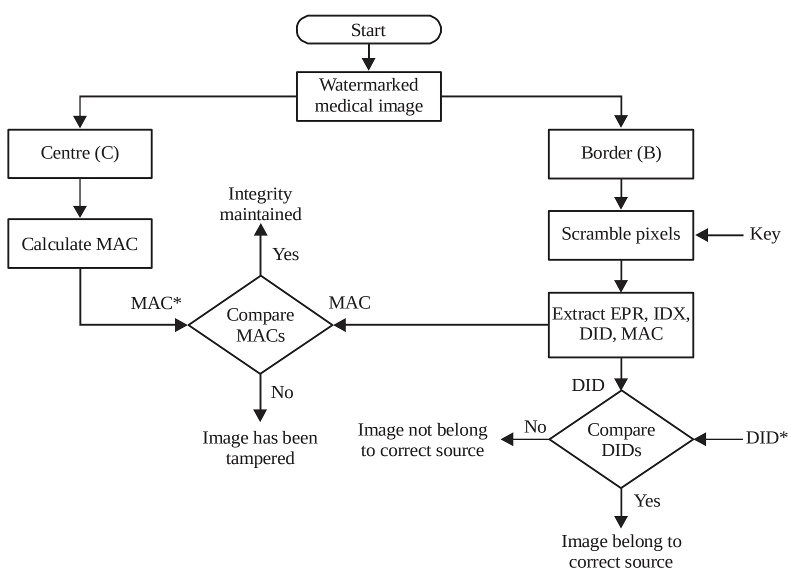

Fig. 3: Block diagram of watermark extraction process

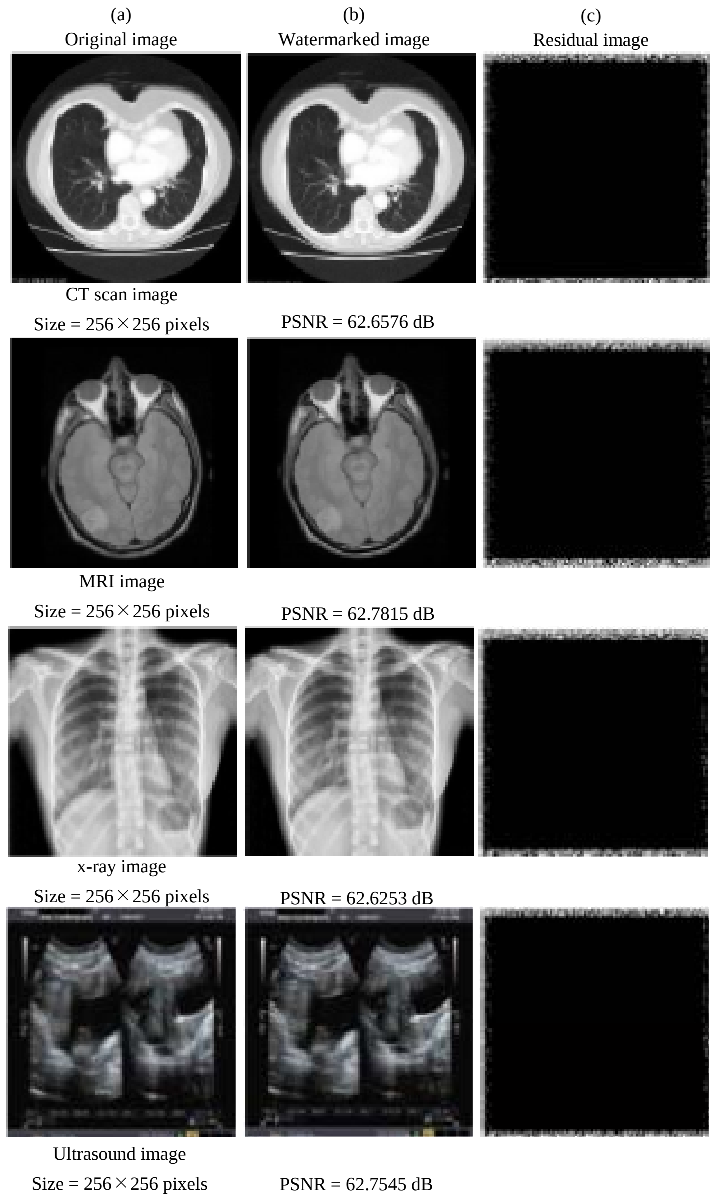

Fig. 4(a-c): (a) Original medical image, (b) Watermarked image with corresponding PSNR and (c) Difference of the original and watermarked image

Patient reference No.	xxxxxxxxxxxxxxxx
Name of examining doctor	xxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxx
Date of examination	xxxxxxxxxxxx
Name patient	xxxxxxxxxxxxxxxxxxxxxxxxxxxx
Gender	xxxxxxxxxxxx
Test performed	xxxxxxxxxxxxxxxxxxxxxxxxxxxx
Result	xxxxxxxxxxxxxxxxxxxxxxxxxxxx
Diagnosis	xxxxxxxxxxxxxxxxxxxxxxxxxxxx
Treatment	xxxxxxxxxxxxxxxxxxxxxxxxxxxx
Required tests	xxxxxxxxxxxxxxxxxxxxxxxxxxxx
Referred to	xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Fig. 5: A sample of patient record

a patient record was found as shown in Fig. 5. This record has the patient and doctor information as well as the diagnosis.

Some sample image sets were used to compare the proposed LSB method with the DUALWM technique. The experimental results are presented in Fig. 6, where Fig. 6a represents the images of initial, middle and lower part of lung CT, Fig. 6b shows the difference between original and watermarked images when information was implanted using DUALWM technique, whereas Fig. 6c shows the difference

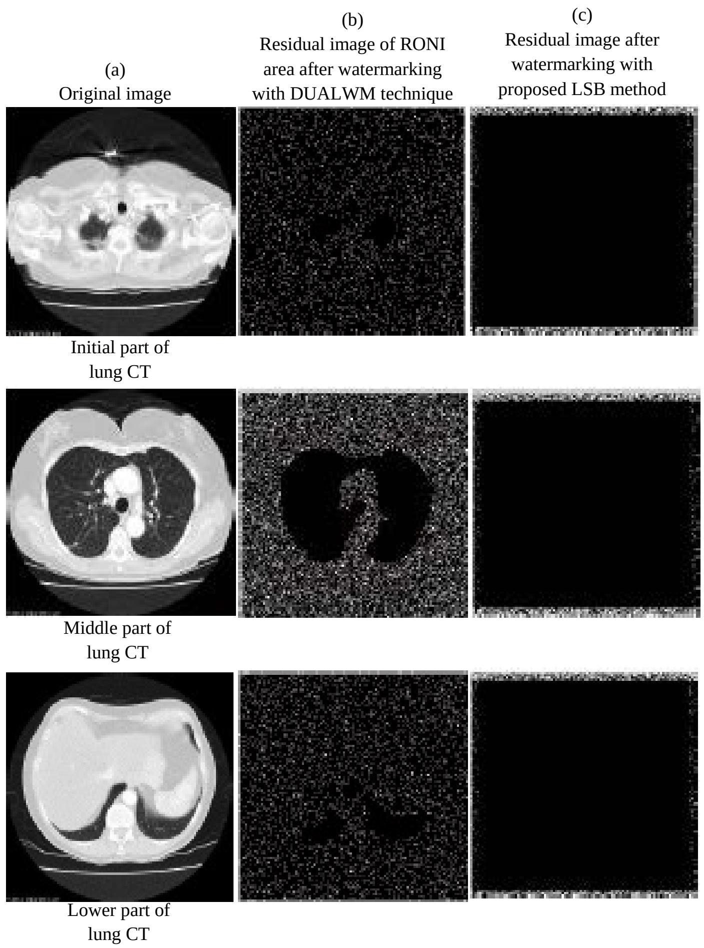

Fig. 6(a-c): (a) Original CT scan image, (b) Difference of original RONI and watermarked RONI when DUALWM technique was applied and (c) Difference of original border and watermarked border when proposed LSB method was applied

Table 1: Comparison of DUALWM technique and proposed LSB method for RONI area, segmentation time and PSNR

	RONI (pixels)		Segmentation time (sec)		PSNR (dB)	
Image type	DUALWM	Proposed LSB	DUALWM	Proposed LSB	DUALWM	Proposed LSB
CT	50,400	8064	12.04	0.3572	53.65	62.6576
x-ray	-	8064	-	0.3916	-	62.6253
MRI	-	8064	-	0.3634	-	62.7815
US	-	8064	-	0.3673	-	62.7545

between original and watermarked images when information was hidden using the proposed LSB method.

Table 1 shows the simulation results of both the DUALWM technique and proposed LSB method for different images modalities. Table 1 shows the images of different modalities. The ROI in pixels created by both the techniques shows in Table 1, respectively. Table 1 shows the segmentation time required for segmenting the input image in ROI and RONI by both techniques. The PSNR values after implanting the watermarks in each image by both the DUALWM and proposed LSB method represented in Table 1. By comparing the results (e.g., No. of pixels used for embedding the watermark information, segmentation time and PSNR) for the DUALWM technique with the corresponding results for the proposed system (Table 1), it is evident that considerably better performance can be obtained with the latter. Since, the performance of the images of different modalities (e.g., CT scan, x-ray, MRI and US) is comparable, the discussions presented below concentrate on the experimental results obtained with the CT scan image method only. The research findings of this study are in line with the findings of Tian[7] who stated that the Electronic Patient Record (EPR) and ROI hash

Table 2: Comparison of DUALWM technique and the proposed LSB method

DUALWM technique	Proposed LSB method
Additional time overhead is required for segmentation	Very less time is required for segmentation
Additional overhead of storage required for saving ROI-LSB information	Not required
Introduce noise in 76% area of entire image	Introduce noise in 12% area of entire image
The scheme is confined to only CT scan images	Can be used to any type of image modality

message are implanted into ROI for the security and integrity of the content of the medical images. Also, Vismanathan and Krishna[8] presented a medical image watermarking technique based on watermarking and cryptography which is identical to the proposed LSB method in the present study. In another study, Tjokorda *et al.*[9] also reported identical medical image watermarking technique to the proposed LSB technique where the size of ROI and RONI is significant to the security and integrity of the medical image.

It is evident from Table 1 that for CT scan image, the proposed LSB method utilized only 8064 pixels for embedding the watermark information as compared to 50400 pixels used by DUALWM technique. Consequently it requires less time for segmentation process and delivers high rates of PNSR ratio for watermarked images.

It can be seen from Table 1 that DUALWM technique segments the complete lung parenchyma from input CT scan image into ROI and RONI regions in an average time of 12.04 sec. On the other hand, the proposed LSB method segments the same CT scan image into the center (C) and border (B) regions in about 0.3572 sec. Thus proposed LSB method improves limitation of time overhead. The proposed LSB method did not embed any type of information in center (C), which avoids the need of storing ROI-LSB information in separate store as required by DUALWM technique. Thus, the proposed LSB method reduced the additional storage overhead. In proposed LSB method, watermark information composed of four different watermarks was embedded into four borders of input image of size 8×8 pixels. This introduces the noise in about 12% area of entire input image and delivers good result with PSNR values higher than 62 dB. In contrast, the DUALWM introduced the noise in 76% of the entire area of input medial image and produced the watermarked image with a PSNR ratio of 53.65 dB as shown in Table 1. Thus, the proposed LSB method improved the imperceptibility of watermarked image by reducing the noise and served the same purpose of content integrity and ownership control of medical images. The study results agree with the findings of Alsaade and Bhuiyan[2] who concluded that developed digital watermarking approaches proved useful to safeguard the medical evidences. Similarly, Deng *et al.*[10] presented a medical image watermarking technique based on reversible watermarking for the recovery of the tempered medical image to its pristine state.

A comparison between DUALWM technique and the proposed LSB method given in Table 2 shows that the proposed LSB method is more reliable, requires less time, less noise and can be applied to any types of image modality. Table 2, summarizes the comparison of DUALWM technique and the proposed LSB method.

CONCLUSION

This study proposed a medical image watermarking method utilizing Least Significant Bit (LSB) method which was compared with DUALWM to measure its accuracy. The proposed LSB method is preferred over DUALWM technique due to a number of reasons. For example, no additional memory storage or time overhead is required in the proposed LSB method as compared to DUALWM. Also, the proposed LSB method introduces less noise in the input image thus producing watermarked images with a high level of imperceptibility. In addition, the bandwidth required for the proposed LSB method is very low, because both the text and image files will be transmitted as single entity instead of two separate files. Consequently, the proposed LSB method seems more economical and an ideal solution for low budget hospitals where budget requirements for storage and communication of medical images is a limiting factor.

REFERENCES

1. Memon, N.A. and S.A.M. Gilani, 2008. NROI watermarking of medical images for content authentication. Proceedings of the 12th IEEE International Multi-topic Conference, December 23-24, 2008, Karachi, Pakistan, pp: 106-110.
2. Alsaade, F. and M.A.A. Bhuiyan, 2015. Digital watermarking for medical diagnosis. J. Applied Sci., 15: 1112-1119.
3. Coatrieux, G., L. Lecornu, B. Sankur and C. Roux, 2006. A review of image watermarking applications in healthcare. Proceedings of the 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, August 30-September 3, 2006, New York, USA., pp: 4691-4694.
4. Chang, Y.J., R.Z. Wang and J.C. Lin, 2008. A sharing-based fragile watermarking method for authentication and self-recovery of image tampering. EURASIP J. Adv. Signal Process. 10.1155/2008/846967.

5. Memon, N.A., Z.A. Keerio and F. Abbasi, 2014. Dual Watermarking of CT Scan Medical Images for Content Authentication and Copyright Protection. In: Communication Technologies, Information Security and Sustainable Development, Shaikh, F.K., B.S. Chowdhry, S. Zeadally, D.M.A. Hussain, A.A. Memon and M.A. Uqaili (Eds.). Springer, New York, USA., ISBN: 978-3-319-10987-9, pp: 173-183.
6. 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.
7. Tian, J., 2003. Reversible data embedding using a difference expansion. IEEE Trans. Circ. Syst. Video Technol., 13: 890-896.
8. Viswanathan, P. and P.V. Krishna 2011. Fusion of Cryptographic Watermarking Medical Image System with Reversible Property. In: Computer Networks and Intelligent Computing, Venugopal, K.R. and L.M. Patnaik (Eds.)., Springer-Verlag, Berlin, Heidelberg, ISBN: 978-3-642-22786-8, pp: 533-540.
9. Tjokorda, A.B.W., Adiwijaya and F.P. Permana, 2012. Medical image watermarking with tamper detection and recovery using reversible watermarking with LSB modification and Run Length Encoding (RLE) compression. Proceedings of the IEEE International Conference on Communication, Networks and Satellite, Bali, Indonesia, July 12-14, 2012, IEEE., New York, USA., pp: 167-171.
10. Deng, X., Z. Chen, F. Zeng, Y. Zhang and Y. Mao, 2013. Authentication and recovery of medical diagnostic image using dual reversible digital watermarking. J. Nanosci. Nanotechnol., 13: 2099-2107.
11. Navas, K.A. and M. Sasikumar, 2007. Survey of medical image watermarking algorithms. Proceedings of the 4th International Conference on Sciences of Electronic Technologies of Information and Telecommunications, March 25-29, 2007, Tunisia, pp: 1-6.
12. Nikolaidis, N. and I. Pitas, 1998. Robust image watermarking in the spatial domain. Signal Proc., 66: 385-403.
13. Shih, F.Y. and S.Y.T. Wu, 2003. Combinational image watermarking in the spatial and frequency domains. Pattern Recogn., 36: 969-975.
14. Kaur, M., S. Jindal and S. Behal, 2012. A study of digital image watermarking. Int. J. Res. Eng. Applied Sci., 2: 126-136.
15. Kaur, G. and K. Kuar, 2013. Image watermarking using LSB (Least Significant Bit). Int. J. Adv. Res. Comput. Sci. Software Eng., 3: 858-861.
16. Sharma, P.K. and Rajni, 2012. Analysis of image watermarking using least significant bit algorithm. Int. J. Inform. Sci. Techn., 2: 95-101.
17. Verma, R. and A. Tiwari, 2014. Copyright protection for watermark image using LSB algorithm in colored image. Adv. Electron. Electr. Eng., 4: 499-506.
18. Lin, C.Y. and S.F. Chang, 1998. Generating robust digital signature for image/video authentication. Proceedings of the Multimedia and Security Workshop at ACM Multimedia, September 1998, Bristol, UK., pp: 1-6.
19. Schneider, M. and S.F. Chang, 1996. A robust content based digital signature for image authentication. Proceedings of the International Conference on Image Processing, September 19, 1996, IEEE., Lausanne, Switzerland, pp: 227-230.
20. Guo, X. and T.G. Zhuang, 2009. A region-based lossless watermarking scheme for enhancing security of medical data. J. Digit. Imag., 22: 53-64.
21. Memon, N.A., A. Chaudhry, M. Ahmad and Z.A. Keerio, 2011. Hybrid watermarking of medical images for ROI authentication and recovery. Int. J. Comput. Math., 88: 2057-2071.