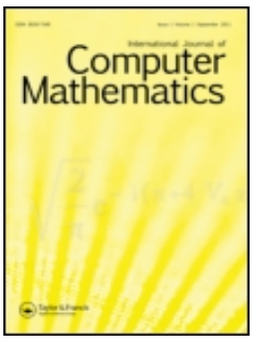


International Journal of Computer Mathematics

ISSN: 0020-7160 (Print) 1029-0265 (Online) Journal homepage: https://www.tandfonline.com/loi/gcom20

Watermarking of chest CT scan medical images for content authentication

Nisar Ahmed Memon & S. A.M. Gilani

To cite this article: Nisar Ahmed Memon & S. A.M. Gilani (2011) Watermarking of chest CT scan medical images for content authentication, International Journal of Computer Mathematics, 88:2, 265-280, DOI: 10.1080/00207161003596690

To link to this article: https://doi.org/10.1080/00207161003596690

International Journal of Computer Mathematics
Vol. 88, No. 2, January 2011, 265–280

Taylor & Francis
Taylor & Francis Group

Watermarking of chest CT scan medical images for content authentication

Nisar Ahmed Memon[a]* and S.A.M. Gilani[b]

[a]*Faculty of Computer Science and Engineering, Ghulam Ishaq Khan (GIK) Institute of Engineering Sciences and Technology, Topi-23460, Swabi, Pakistan;* [b]*Department of Computer Science, National University of Computer and Emerging Sciences, Lahore, Pakistan*

(*Received 1 April 2009; revised version received 25 September 2009; second version received 16 November 2009; accepted 23 December 2009*)

Image processing techniques have played a very significant role in the past decades in the field of medical sciences for diagnosis and treatment purposes. In some applications, medical images are divided into region of interest (ROI) and region of non-interest (RONI). Important information regarding diagnosis is contained in the ROI, so its integrity must be assured. We propose a fragile watermarking technique to ensure the integrity of the medical image that avoids the distortion of the image in ROI by embedding the watermark information in RONI. The watermark is composed of patient information, hospital logo and message authentication code computed using a hash function. Earlier encryption of watermark is performed to ensure inaccessibility of embedded data to the adversaries.

Keywords: medical images, spatial domain watermarking; region of interest; data authentication; electronic patient record

2010 AMS Subject Classifications: 94A62; 55S36; 91G20; 94A08; 94A05

1. Introduction

Recently, due to the development of latest technologies in the areas of communications and computer networks, exchange of medical images between hospitals has become a common practice. These medical images are exchanged for number of reasons among which are [13]:

- teleconferences among clinicians;
- interdisciplinary exchange between clinicians and radiologists for consultative purposes or to discuss diagnostic and therapeutic measures;
- for distant learning of medical personnel.

However, these applications require more attention towards image protection (availability, confidentiality and reliability) [6]. To facilitate sharing and remote handling of medical images in a secure manner, watermarking guarantees attractive properties. It allows permanent association of

*Corresponding author. Email: memon_nisar@yahoo.com

ISSN 0020-7160 print/ISSN 1029-0265 online

DOI: 10.1080/00207161003596690
http://www.informaworld.com

image content with proofs of its reliability by modifying the image pixel values, independently of the image file format [5,26].

For protecting the digital images, three categories of watermarking have been reported in the literature, i.e. *robust* watermarking [7], *fragile* watermarking [21,22] and *semi-fragile* watermarking [7,8] . *Robust watermarks* are most difficult to remove from the digital content; are robust against legitimate or illegitimate operations/distortions such as compression, scaling, cropping, filtering, A/D or D/A conversion, etc. and one of their use may be for the copyright protection. *Fragile watermarks* are those that are easily destroyed by tampering or modifying the watermarked content, hence the absence of watermark to the previously watermarked content points to the conclusion that data have been tampered with, and thus are used for data authentication applications. *Semi-fragile watermarks* protect images from illegal modifications/operations, e.g. active/passive attacks, collusion attacks and forgery attacks, while allows unintentional modifications, e.g. compression, scaling, cropping, etc.

One can use the fragile watermarking for authentication of medical images. In this case, the robustness of watermark in the image is of less concern, while detection and localization of the slight changes of the images are more important [4].

In this paper, the authors have extended their work [13] and have proposed a blind fragile watermarking scheme that does not require the original host image during the extraction of watermark. First the image has been segmented that separates the lung parenchyma from the rest of the CT scan image, then three different types of watermarks are embedded in the host image by replacing the least significant bits (LSBs) of the cover segmented image. LSB is a simple fragile embedding technique with a high embedding capacity and small embedding distortions. The LSBs of the image are generally considered as noise inherent due to the image acquisition devices. So, these bits can be used for secret message embedding without greatly disturbing the image appearance [3]. The scheme serves for both the purposes of medical image authentication and hiding electronic patient record (EPR).

A medical image in the case of clinical outcome can be divided into two parts: the region of interest (ROI) where the diagnosis focuses and the region of non-interest (RONI), which is the remaining area [10]. Usually, it is desirable to embed data outside of ROI to give better protection without compromising the diagnosis information [15].

2. Related work

Different groups of authors have contributed a number of medical image watermarking techniques. A technique of embedding EPR data in medical images is suggested by Achariya *et al.* [1]. EPR data consist of text file and graphs, where text file is the preliminary report about the patient from the radiology department of the hospital and graphs are ECG or EEG. It is an LSB technique implemented in the spatial domain. The ASCII characters in EPR data are encrypted before interleaving in medical images to improve the security of the data. In another technique proposed by Nayak *et al.* [16], the ASCII characters in the EPR text are encrypted using Rijndael algorithm before hiding it in the image. Signal graphs (ECG, EEG, EMG, etc.) are compressed using differential pulse code modulation technique before hiding. To enhance the robustness of the embedded information, the patient information is coded by error-correcting codes such as (7,4) Hamming, Bose–Chaudhuri–Hocquengham and Reed Solomon code. The noisy scenario is simulated by adding salt and pepper noise to the embedded image. For different signal-to-noise ratio of the image, bit error rate (BER), number of characters altered for text data and percentage distortion for the signal graph are evaluated. Xuanwen *et al.* [25] utilizes compressed binary bit planes to embed EPR data. Grey-scale images with pixel values ranging from 0 to 255 are

composed of 8 bit planes. In order to obtain the sufficient embedding capacity, each binary bit plane is compressed losslessly and data is embedded into the saved space. In the detection phase, the embedded data are extracted and the compressed image is decompressed. The original image is recovered because the compression was lossless. Rodriguez *et al*. [18] searches for the suitable pixels to embed information using the spiral scan starting from the centroid of the image. Then, obtain a block with its centre at the position of the selected pixel. If the bit to be embedded is '1', change the luminance value of the central pixel by adding the grey-level mean of the block with the luminance of the block. If the bit to be embedded is '0', change the luminance value of the central pixel by subtracting the luminance of the block from the grey-level mean of the block. In the extraction procedure, marked pixels are located using the spiral scan starting in the centroid of the image. If the luminance value of the central pixel is greater than the grey-scale level mean of the block, then the embedded bit is identified as 1, otherwise as 0.

All these algorithms have the limitations that the ROI, which is diagnostically an important area in medical images, has not been protected in data embedding methods. Some of the important requirements in the medical field are to recover the EPR with zero BER, to have the cover image without any distortion. Another requirement is that the ROI should be protected [20].

3. Proposed scheme

In the proposed scheme, during the embedding phase the watermark is constructed from three different entities. Later on, the watermark is embedded in the LSBs of RONI of the original image using the proposed scheme. In the detection stage, the embedded watermark is extracted. The process is the reverse of the embedding process. The extracted logo is compared with the logo already known to the detector for subjective authentication. For objective authentication, the message authentication code (MAC) is calculated as was done at the time of embedding and is compared with the extracted authentication code for verifying image integrity.

3.1 *Hash functions for calculating MAC*

In information security, message authentication is an essential technique to verify that the received message come from the alleged source and have not been altered. A key element of the authentication schemes is the use of MAC. One technique to produce an MAC is based on using hashing functions [9]. A hash function is any well-defined procedure or mathematical function that converts a large, possibly variable-sized amount of data into a small datum. The values returned by a hash function are called hash values, hash codes, hash sums or simply hashes. The authors in [2] define the hash function as follows:

Definition. A function $H(\cdot)$ that maps an arbitrary length message M to a fixed message digest MD is a one-way hash function, if it satisfies the following properties:

(1) The description of $H(\cdot)$ is publicly known and should not require any secret information for its operation.
(2) Given M, it is easy to compute $H(M)$.
(3) Given MD in a range of $H(\cdot)$, it is hard to find a message M such that $H(M) = \text{MD}$ and given M and $H(M)$, it is hard to find a message M' ($\neq$M) such that $H(M') = H(M)$.

A number of hash functions are given; however, secure hash algorithm (SHA-1) and message digest-5 (MD5) are well-known algorithms for calculating MAC. One application of hash functions lies in the area of image authentication and watermarking [12,19,23].

3.1.1 *MD5 algorithm*

MD5 [17] is a message digest algorithm developed by Ron Rivest at MIT. It is basically a secure version of his previous algorithm MD4, which is little faster than MD5. This is one of the most widely used SHAs-1. The function takes an input of arbitrary length and produces a message digest. This message digest is typically expressed as a 32-digit hexadecimal number. MD5 is used in many situations; potentially long message needs to be processed and/or compared quickly.

3.2 *Watermark generation*

In order to generate the watermarks, following steps are implemented:

(1) Read the hospital logo as shown in Figure 1, convert this grey intensity image into a binary vector and call this vector as W_1 such that $W_1 = [w_1(i), w_1 \in \{0, 1\}, 1 \leqslant i \leqslant 4096]$.
(2) Read the text file containing the patient information, convert each character of text file into its corresponding ASCII code [15].
(3) Convert each ASCII code into its corresponding binary code and form the vector W_2 that may have a length of M bits such that $W_2 = [w_2(i), w_2 \in \{0, 1\}, 1 \leqslant i \leqslant M]$. Note that the length of W_2 depends upon the number of characters used to represent EPR multiplied by 8, as 8-bit binary representation is used to represent ASCII codes into the binary form. In our simulations, 1024 characters of patient data are used, therefore value of M is $1024 \times 8 = 8192$ bits.
(4) Set LSBs of all the pixels in the input image to zero and compute the hash function of this image using the MD5 algorithm. This gives 32 characters string.
(5) Convert the string obtained from Step 4 into binary vector W_3 in the same way as described for patient information in Step 3, such that $W_3 = [w_3(i), w_3 \in \{0, 1\}, 1 \leqslant i \leqslant 256]$.
(6) Now concatenate all the watermarks W_1, W_2 and W_3 and call it W having length say N, such that $W = [w(i), w \in \{0, 1\}, 1 \leqslant i \leqslant N]$.

3.3 *Watermark preprocessing*

The generated watermark W is preprocessed before the embedding because if the attacker has knowledge of the watermark he/she may have easily forged it. The method proposed in [24] is used for preprocessing the watermark.

A pseudo-random binary vector P of the size same as W is generated by a secret key k. The binary pseudo-random vector P is represented as

$$P = [p(i), p \in \{0, 1\}, 1 \leqslant i \leqslant N].$$

The following formula is used to get the ultimate watermark W^*

$$W^* = W \oplus P, \tag{1}$$

where $\oplus$ denotes the exclusive-OR operation.

The W^* is the resultant watermark that is to be embedded in the host image.

Figure 1. Hospital logo (64×64).

3.4 *Selection of RONI for embedding the watermark*

The proposed method selects the RONI for embedding the watermark in order to assure the integrity of ROI and not to compromise with the diagnosis value of the medical image. To achieve this, it is necessary first to separate the original image into ROI and RONI areas. Usually, in radiological images the ROI is taken as a square [15,20]. For example in the images of size 512×512 pixels, square of size 256×256 was taken which almost cover the entire ROI [11]. But in some cases especially for radiological CT scan images of the chest area, taking logical square for isolating the ROI eradicate some part of ROI as shown in Figure 2. This is because of the lung parenchyma on lung CT, which is elliptical in shape by nature and taking the square as boundary for isolating ROI eradicates some part of ROI. In the technique proposed by the authors in [13], the logical ellipse has been drawn to cover the ROI. This technique though covers the entire lung parenchyma it also takes the area (like some part of the thorax area and some other part lying between the two lung parts) as shown in Figure 3. Thus, this technique of isolating ROI includes the image parts that are not of the interest for the doctor for diagnosis point of view thus can be used for embedding watermark information. To cope with this problem, an algorithm has been proposed that completely separates the lung parenchyma from the CT scan image, thus increasing the capacity for embedding the data that is some times crucial in medical image watermarking. To

Figure 2. Isolating ROI using white square [11].

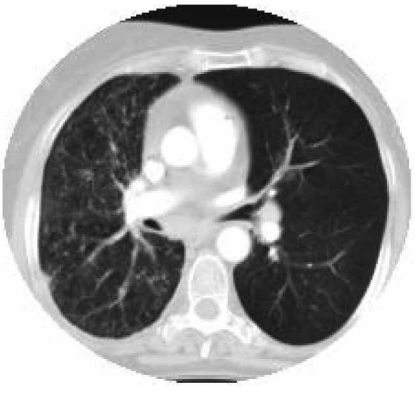


Figure 3. Isolating ROI using ellipse [13]

segment the lung parenchyma instead of drawing the logical square or ellipse not only separates the ROI efficiently but also increases the embedding capacity.

3.4.1 *Separation of lung parenchyma*

For isolating the lung parenchyma, an optimal thresholding scheme has been proposed that selects the threshold based on the object and background pixel means. Once the threshold has been selected and applied, region growing and connectivity analysis are used to extract the exact cavity region with accuracy [14]. The segmentation algorithm for the segmentation of the lung parenchyma from the input CT scan image is described as follows:

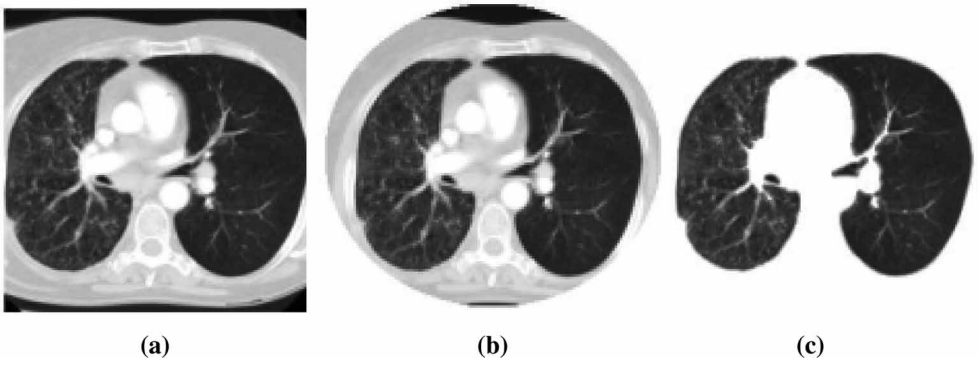
(1) Read the input image.
(2) Draw the black boundary on the input image.
(3) Find the grey threshold of the input image using the Otsu method and call it T_{final}.
(4) Based on the threshold T_{final} found from Step 3, turn all pixels white that have the grey values greater than the threshold.
(5) Find the location of seed pixel and its value for starting the region-growing process by searching through all the boundaries leaving black boundary already drawn in Step 2;
(6) Find the tagged image by assigning 1 and 0 to the pixels as follows:

$$I_{\text{tag}}(x, y) = \begin{cases} 1 & \text{if } I(x, y) = 255 \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

(7) Turn those pixels and neighbours white that are not tagged. The resultant image will now contain the isolated lung parenchyma.

3.4.2 *Increasing the embedding capacity*

By isolating the lung parenchyma with the technique described in Section 3.4.1, one may have an increased embedding capacity for the watermark insertion. By taking the square for isolating the lung parenchyma from the input CT scan image with size 256×256 pixels, it was necessary to take at least square of size 192×192 pixels in order to cover the whole lung parenchyma as shown in Figure 4(a). This gives $[(256 \times 256) - (192 \times 192)] = 28672$ pixels for embedding the watermark information. Similarly taking the ellipse as shown in Figure 4(b) gives $[(256 \times 256) - 33749] = 31787$ pixels as the embedding capacity. With the proposed scheme shown in



(a) **(b)** **(c)**

Figure 4. (a) ROI as in [11]; (b) ROI as in [13] and (c) proposed algorithm.

Figure 5. (a) Start of lung; (b) middle of lung and (c) end of lung.

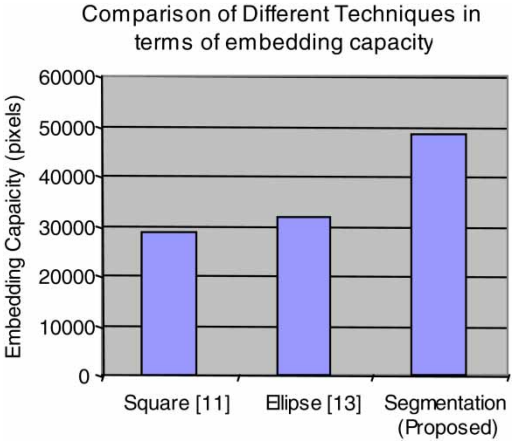


Figure 6. The graph showing the embedding capacities of different techniques.

Figure 4(c), $[(256 \times 256) - 17114] = 48422$ pixels can be obtained for embedding watermark information. All these experiments are performed on the image shown in Figure 5(b). From the above calculations, it is clear that the proposed scheme have achieved the more embedding capacity as compared with that in [11,13]. It is about 40.78% more than [11] and 34.35% more than [13]. The graph depicted in Figure 6 shows the comparative results. It is also worth to mention over here that the segmentation technique [14] is adaptive, so the more and more embedding capacity can be achieved when images shown in Figure 5(a) and (c) are used.

3.5 *Embedding process*

The embedding process starts with the generation of watermarks as described in Section 3.2, then the host image is divided into ROI and RONI. Later on the watermark is embedded in RONI. The process is described step by step as follows:

(1) Generate the watermark.
(2) Encrypt the watermark W with pseudo-random binary vector P to produce W^*.
(3) Separate the image into ROI and RONI.
(4) Scramble the pixels in RONI using the key.
(5) Embed the watermark in the scrambled pixels in LSBs of RONI.

(6) Re-scramble the pixels in RONI to take them back to the original position.
(7) Combine ROI and RONI to get the watermarked image.

The block diagram of the embedding process is shown in Figure 7.

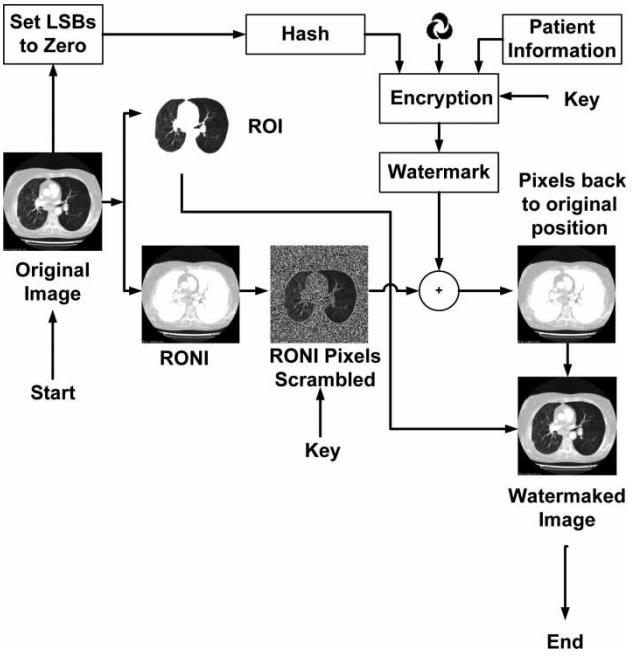


Figure 7. Block diagram of the embedding process.

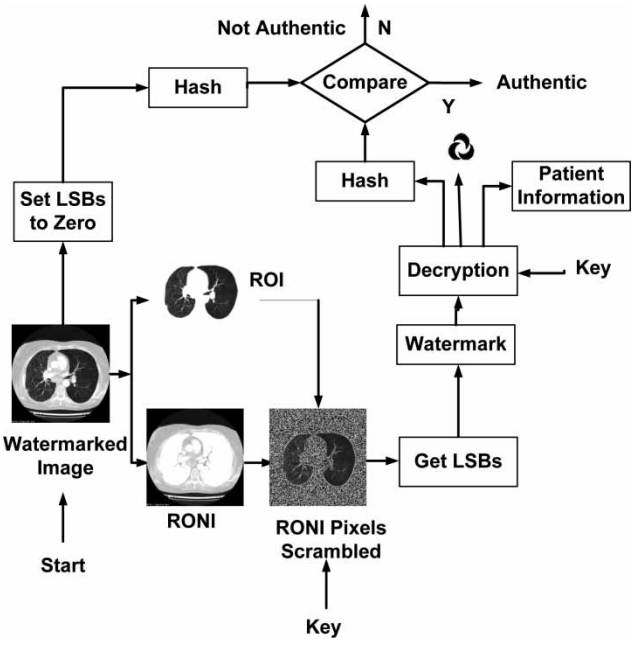


Figure 8. Block diagram of the extraction process.

3.6 *Extraction process*

The extraction process is the inverse of the embedding process. Since the proposed scheme is blind so there is no need of the original image to extract the embedded watermark. The extraction process has the following steps:

(1) Separate the watermarked image into ROI and RONI by using the segmentation algorithm.
(2) Scramble the pixels in RONI using the same key used for embedding.
(3) Extract the LSBs from all the selected pixels.
(4) Decrypt the extracted watermark W^* using the P to get W.
(5) Split the extracted watermark W into W_1, W_2 and W_3.

The block diagram of the extraction process is shown in Figure 8.

4. Experimental results

This section describes the experimental results of the proposed scheme. The experiments were carried out using the data set of 11 patients received from AGA Khan University Karachi, Pakistan. Each patient's data set contained about 60–100 slices of CT scan images with varying slice thicknesses. All the images are of 256 × 256 pixels and 8-bit grey-level images. The start, middle and end of the lung CT slices of one patient are shown in Figure 5.

4.1 *Imperceptibility*

As a first step, watermarks are generated and concatenated to form a single watermark as described in Section 3.2. Later on this watermark is encrypted with pseudo-random binary vector generated by using the secret key in order to increase the robustness of embedded data [24]. Table 1 shows the size of different watermarks generated and used in simulations of this work.

Figure 9(a) shows the ROI and Figure 9(b) shows the RONI after dividing the CT scan image of the middle part of lung into two regions. Figure 9(c) shows the scrambled coefficients of RONI. Figure 10(a) shows the watermarked image and Figure 10(b) shows the difference between the cover image and the watermarked image. The degradation introduced in the watermarked image with respect to the original one is determined by using peak signal-to-noise ratio (PSNR) and mean square error (MSE) metrics as described in [18] and is given in the Equations (3) and (4):

$$\mathrm{PSNR} = 10 \log_{10} \frac{R^2}{\mathrm{MSE}}, \tag{3}$$

where R is the maximum intensity value of the input image data type. For example, if the image has double precision floating point data type then R is 1 and if the input image has an 8-bit unsigned integer data type then R is 255:

$$\mathrm{MSE} = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{MxN}, \tag{4}$$

Table 1. The size and type of each watermark.

Watermark	Size	Binary conversion	Total (bits)
Logo	64 × 64 (grey)	4096 (bitmap)	4096
EPR	1024 (char)	1024 × 8	8192
MAC	32 (char)	32 × 8	256

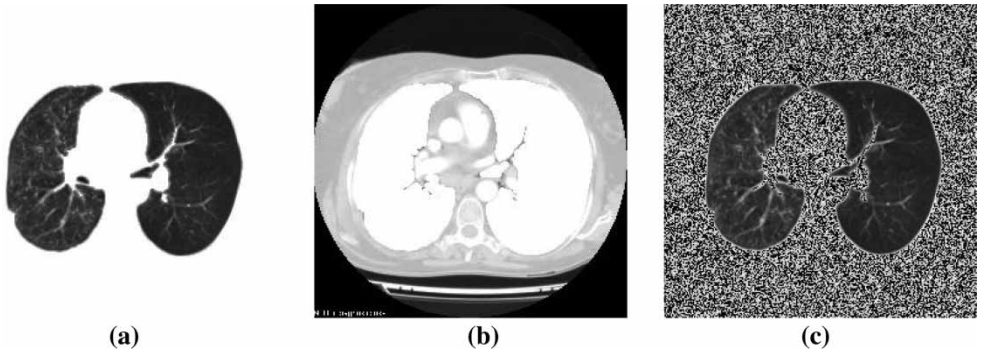


Figure 9. (a) ROI; (b) RONI and (c) pixels scrambled in RONI.

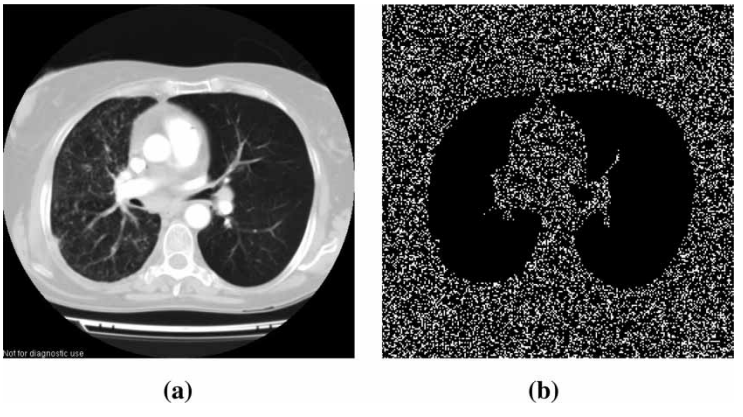


Figure 10. (a) Watermarked image (PSNR = 58.34 dB) and (b) difference between the original and the watermarked image.

Table 2. Imperceptibility shown between original and watermarked images in terms of PSNR and MSE.

Image	Size	PSNR (dB)	MSE
Start of lung	256 × 256	58.35	0.0950
Middle of lung	256 × 256	58.29	0.0964
End of lung	256 × 256	58.30	0.0961

where M and N are number of rows and number of columns in both the cover (I_1) and watermarked image (I_2).

The degradation in terms of PSNR and MSE in the cover image and watermarked image for different images are shown in Table 2. For the images of size 256 × 256, 73.88% of total image pixels were found as RONI. The watermarks of different strengths were embedded in these RONI pixels. Table 3 shows the degradation in visual quality of the watermarked image with respect to the original image by embedding watermarks of varying strengths in terms of PSNR and MSE. It can easily be observed that PSNR decreases with increase in the strength of watermark, which is a usual trade-off in the watermarking techniques. This scenario is also shown in Figure 11.

4.2 *Authenticity*

The integrity of images at the receiving end can be authenticated using the proposed technique. Both the subjective and objective measures are used.

Table 3. Imperceptibility shown in the original and watermarked image with different payloads.

Image	Payload (bits)	PSNR (dB)	MSE
Middle of lung, size 256 × 256	8000	60.35	0.0599
	16,000	57.30	0.1209
	24,000	55.51	0.1825
	32,000	54.24	0.2449
	40,000	53.27	0.3036
	48,000	52.49	0.3663
	56,000	51.81	0.4284
	64,000	51.23	0.4898

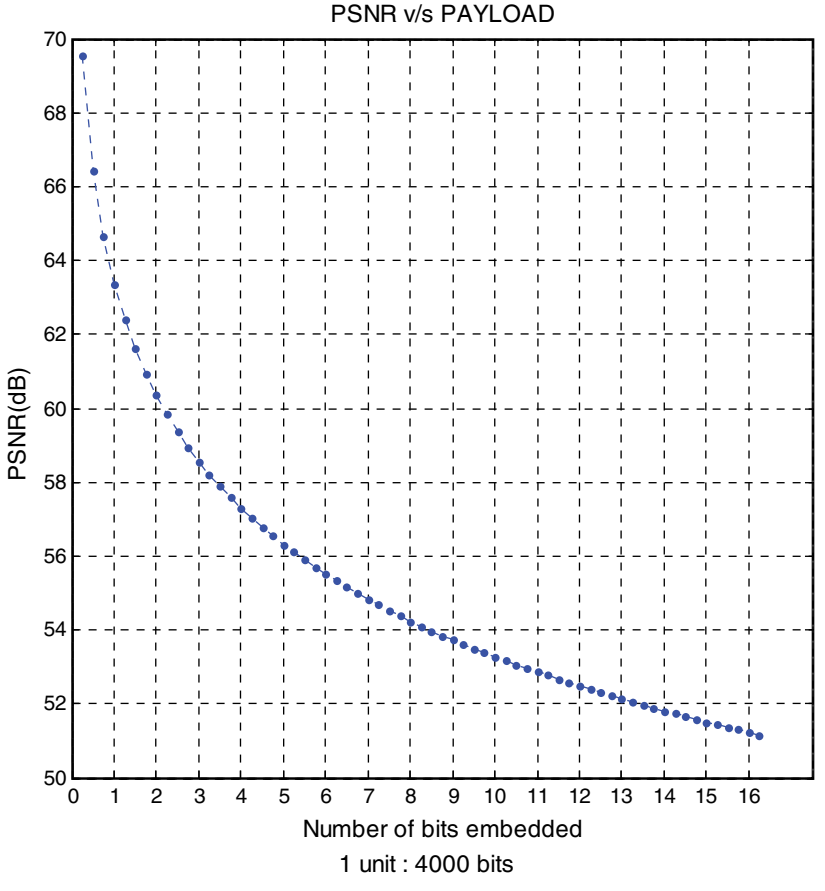


Figure 11. Degradation in visual quality with the embedded information.

4.2.1 *Subjective analysis*

The visual inspection is used for subjective authentication. A number of image manipulations were performed on the watermarked images. All the attacks were performed using the off-the-shelf image processing software. The analysis of attacks is given as follows.

4.2.1.1 *Gaussian noise.* The Gaussian noise attack was performed with zero mean and variance of 0.0001 on the watermarked image to evaluate the technique for tamper detection. Figure 12 shows the results. It can be easily observed that the watermarked image did not sustain the attack.

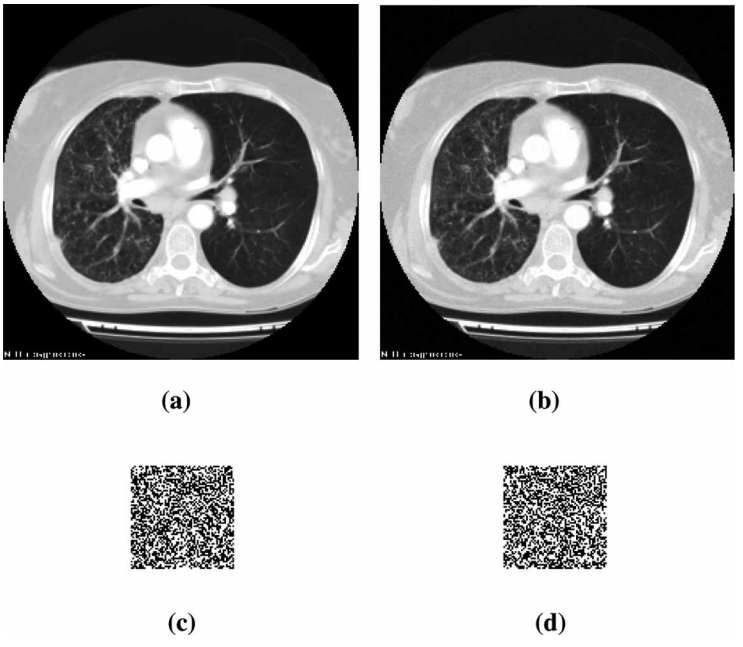


Figure 12. (a) Watermarked image; (b) image with Gaussian noise added; (c) extracted watermark and (d) difference between embedded and extracted watermark.

Thus, the algorithm verified that the image is not authentic and has been tampered by the hacker during the transmission.

4.2.1.2 *Median filtering.* The median filtering attack was performed on the watermarking image. The effect of filter cannot be easily observed by the naked eye of the human being. However, the algorithm easily identified the distortion introduced by the attack. Figure 13 shows the results.

4.2.1.3 *JPEG compression.* The watermarked image was compressed with the quality factor of 90%. The resultant image shown in Figure 14 almost looks same as the original. However, the embedded hospital logo was completely destroyed.

4.2.1.4 *Copy attack.* A square block of 16×16 pixels was copied from upper left corner of the image and pasted on lower right corner of the image. This manipulation again cannot be easily observed by the practitioner of the medical hospital. The algorithm detects this distortion and can easily be observed in the results shown in Figure 15.

4.2.1.5 *Histogram equalization.* The histogram equalization attack was applied on the watermarked image. The histogram usually expands the dynamic range of the input image. One cannot easily recognize this change because there are no visible artefacts on the image. The proposed technique also recognizes this distortion and proves the authenticity of the image by reporting that the image has been tampered with. Figure 16 illustrates the results.

4.2.2 *Objective analysis*

For the objective analysis, normalized hamming distance measure is used for authentication

$$\mathrm{NHD}(w, w^*) = \frac{1}{N} \sum_{k=1}^{N} w(k) \oplus w^*(k), \tag{5}$$

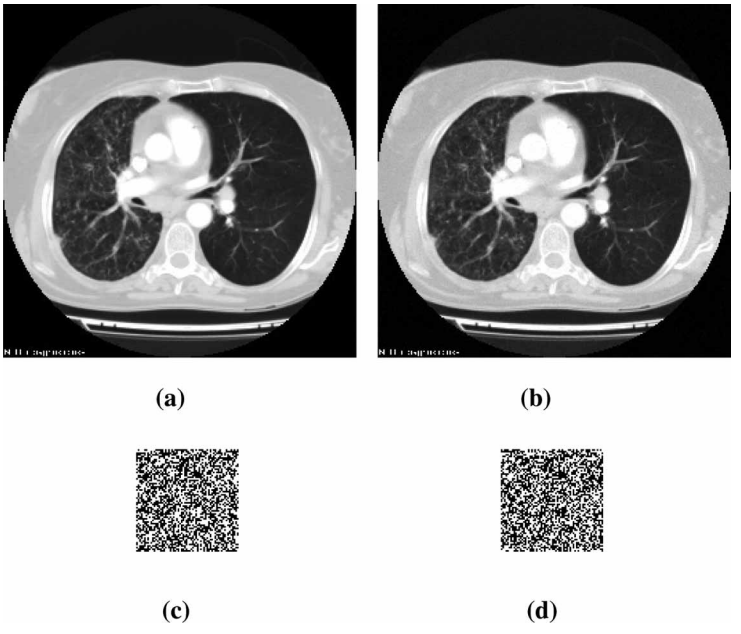


Figure 13. (a) Watermarked image; (b) image after median filter attack; (c) extracted watermark and (d) difference between embedded and extracted watermark.

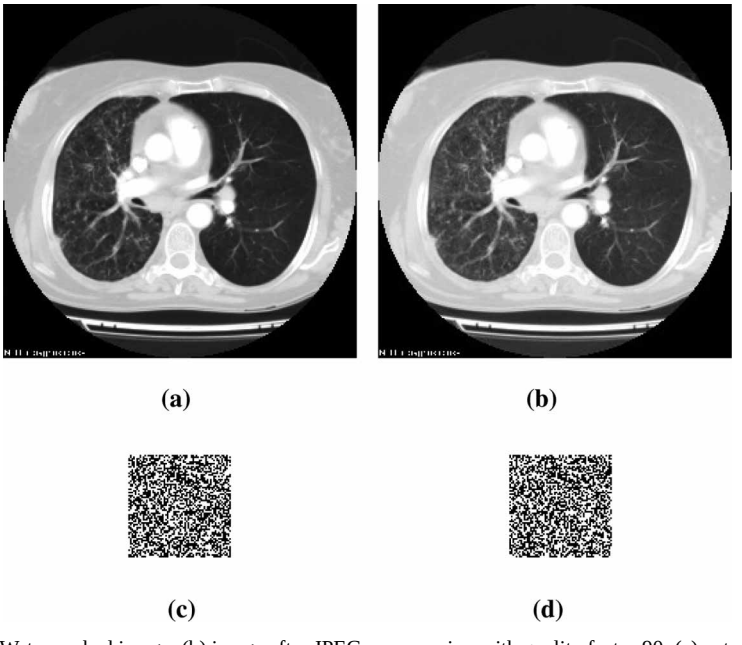


Figure 14. (a) Watermarked image; (b) image after JPEG compression with quality factor 90; (c) extracted watermark and (d) difference in embedded and extracted watermark.

where w and w^* are the original and extracted watermarks, respectively, N is the length of watermark and $\oplus$ is the exclusive-OR operator. The distance ranges between (0,1) and application-dependent decision can be made concerning the integrity of the content of the medical image. The values closer to zero give better results. Table 4 illustrates the results after applying the

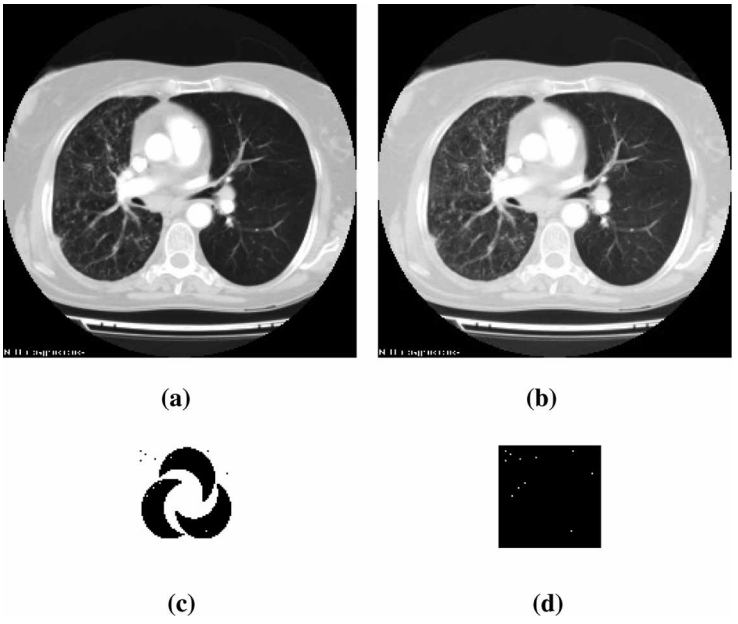


Figure 15. (a) Watermarked image; (b) image after copy paste attack; (c) extracted watermark and (d) difference in embedded and extracted watermark.

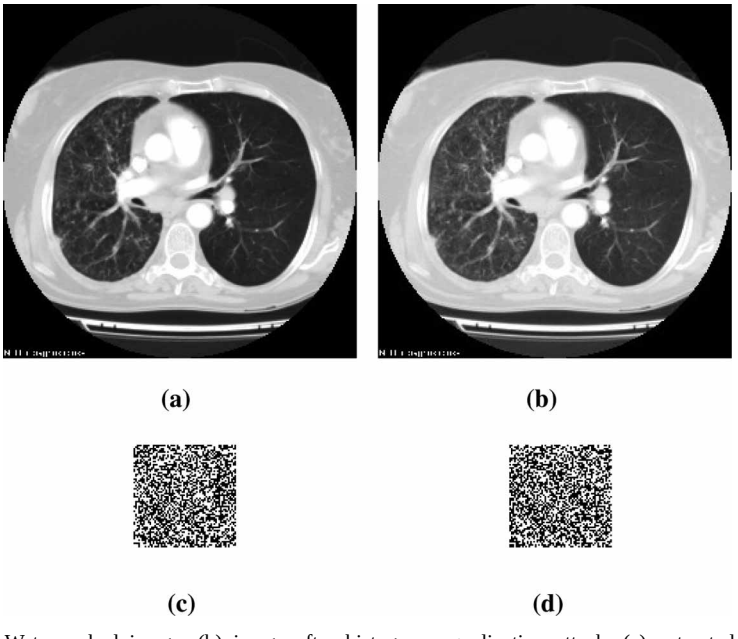


Figure 16. (a) Watermarked image; (b) image after histogram equalization attack; (c) extracted watermark and (d) difference in embedded and extracted watermark.

different attacks on the images given in Figure 5. It can be observed that almost all the attacks were recognized by the proposed scheme.

The proposed scheme is very sensitive. It can detect even one bit of distortion in the image. The hospital logo used as watermark can easily detect the authenticity of the image when the image is tampered with in the RONI area. However, if the hacker manipulates the

Table 4. Distortion measurement against the various attacks performed on the images.

	Normalized hamming distance				
Attacks performed	Gaussian noise	Median filtering	JPEG QF = 90	Copy attack	Histogram equalization
Start of lung					
Logo	0.5095	0.4512	0.5039	0.0012	0.4768
EPR	0.4878	0.4895	0.4980	0.0023	0.5117
MAC	0.5117	0.5117	0.4922	0.0000	0.4883
Middle of lung					
Logo	0.5039	0.4968	0.4941	0.0027	0.4624
EPR	0.4984	0.4983	0.50082	0.0023	0.5014
MAC	0.5273	0.4805	0.5273	0.0000	0.5352
End of lung					
Logo	0.5015	0.3967	0.4988	0.0012	0.4800
EPR	0.4923	0.3954	0.5024	0.0022	0.5192
MAC	0.4961	0.4219	0.5000	0.0000	0.5234

image in ROI, where the watermarked has not been inserted, the embedded MAC works. It is calculated again at the receiving end and can be compared with the extracted MAC to verify the integrity of the content. One shortcoming of the proposed technique is that it can not distinguish between the intentional and unintentional attacks. During transmission from one hospital to the other, medical images are generally compressed via Joint Photographic Experts Group (JPEG) compression in order to save the bandwidth and memory. In this case, JPEG compression can be considered as an unintentional attack and the authentication system should deem the image as authentic. However, the proposed scheme declares the image unauthentic in this scenario as shown in Figure 14, because every time a new hash is calculated even for a change of a single bit of information. The future work will be to propose the semi-fragile watermarking technique for medical images that can survive against the legitimate attacks like common signal processing operation and cannot survive against illegitimate attacks.

5. Conclusions

A blind fragile watermarking technique is proposed in the spatial domain to preserve the history of the medical image by embedding the medical diagnosis report. While embedding the data, ROI of the medical image is avoided to ensure the integrity of ROI. The scheme allows the simultaneous storage and transmission of EPR that can be extracted at the receiving end without the original image. Encryption of the embedded data is done to provide additional security. It also provides sufficient capacity for storing about more than half of kilo bytes of patient data for the images of size 256×256. The scheme can easily be used in e-diagnosis applications.

Acknowledgements

Authors are very grateful to the Ghulam Ishaq Khan Institute of Engineering Sciences and Technology for providing resources and environment for carrying out this research and AGA Khan Hospital Karachi, Pakistan, for providing the database for the experimental work. Also, this work was supported by Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, Sindh, Pakistan, under Inland Scholarship Programme.

References

[1] U.R. Achariya, P. Subhanna Bhat, S. Kumar, and L. Choo Min, *Transmission and storage of medical images with patient information*, J. Comput. Biol. Med. 33 (2003), pp. 303–310.

[2] S. Bakhtiari, R. Safavi-Naini, and J. Pieprzyk, *Cryptographic Hash Functions: A Survey*. Available at http://eprints.kfupm.edu.sa/33106.
[3] S. Boucherkha and M. Benmohamed, *A lossless watermarking based authentication system for medical images*, Proc. World Acad. Sci. Eng. Technol. 1 (2005), pp. 100–103.
[4] P. Chang-Ri, W. Dong Min, P. Dong-Chul, and H. Seung Soo, *Medical image authentication using hash function and integer wavelet transform*, IEEE 2008 Congress on Image and Signal Processing, Snaya, Hainan, China, May 27–30, 2008, pp. 7–10.
[5] G. Coatrieux, L. Lecornu, B. Sankur, and Ch. Roux, *A review of image watermarking applications in healthcare*, Proceedings of IEEE-EMBC Conference, New York, 2006, pp. 4691–4694.
[6] G. Coatrieux, J. Montagner, H. Huang, and Ch. Roux, *Mixed reversible and RONI watermarking for medical image reliability protection*, 29th IEEE International Conference of EMBS, Cite Internationale, Lyon, France, August 23–26, 2007.
[7] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon, *Secure spread spectrum watermarking for multimedia*, Trans. Image Processing 6(12) (1997), pp. 1673–1687.
[8] I.J. Cox, M.L. Millter, and J.A. Blom, *Digital Image Watermarking*, Morgan Kaufman Publishers, San Francisco, CA, 2004.
[9] J. Deepakumara, H.M. Heys, and R. Venkateson, *FPGA implementation of MD5 hash algorithms*, Canadian Conference on Electrical and Computer Engineering, Vol. 2, 2001, pp. 919–924.
[10] V. Fotopoulos, M.L. Stavrinou, and A.N. Skodras, *Medical image authentication and self-correcting through an adaptive reversible watermarking technique*, Proceedings of 8th IEEE International Conference on Bio Informatics and Bio Engineering (BIBE2008), October 8–10, 2008, pp. 1–5.
[11] H.K. Lee, H.J. Kim, K.R. Kwon, and J.K. Lee, *ROI medical image watermarking using DWT and bit-plane*, IEEE 2005 Asia-Pacific Conference on Communications, Perth, Western Australia, October 3–5, 2005.
[12] C.-Y. Lin and S.-F. Chang, *Generating robust digital signature for image/video authentication*, Proceedings of Multimedia and Security Workshop at ACM Multimedia '98, Bristol, UK, September 1998.
[13] N.A. Memon and S.A.M. Gilani, *NROI watermarking of medical images for content authentication*, IEEE Conference, Karachi, Pakistan, December 23–24, 2008.
[14] N.A. Memon, A.M. Mirza, and S.A.M. Gilani, *Segmentation of lungs from CT scan images for early diagnosis of lung cancer*, Proceedings of 2006 Enformatika, XIV International Conference Prague, Czech Republic, August 25–27, 2006.
[15] K.A. Navas, S.A. Thampy, and M. Sasikumar, *EPR hiding in medical images for telemedicine*, Proc. of the World Academy of Science, Engineering and Technology, Rome, 2008, pp. 292–295.
[16] J. Nayak, P. Subbanna Bhat, M. Sathish Kuamr, and U.R. Achariya, *Reliable and robust transmission and storage of medical images with patient information*, International Conference on Signal Processing and Communication (SPCOM), Lisbon, Portugal, 2004.
[17] R. Rivest, *The MD5 Message Digest Algorithm*, RFC 1321, MIT LCS & RSA, Data Security, Inc., 1992.
[18] C.R. Rodriguez, F. Uribe Claudia, and J. Trinidad Blas Gershom De, *Data hiding scheme for medical images*, IEEE 17th International Conference on Electronics, Communications and Computers (CONIELECOMP), Cholula, Puebla, Mexico, 2007.
[19] M. Schneider and S.-F. Chang, *A robust content based digital signature for image authentication*, Proceedings of ICIP-96, Vol. 3, September 1996, pp. 227–230.
[20] B. Smitha, K.A. Navas, "*Spatial domain-high capacity data hiding in ROI images*," Proc. Int. Conf on Signal Processing, Communication andNetworking IEEE-ICSCN-2007, Chennai, India, pp. 528–533. 22–24 Feb 2007.
[21] S. Walton, *Information authentication for a slippery new age*, Dr Dobbs J. 20(4) (1995), pp. 18–26.
[22] P. Wong, *A public key watermark for image verification and authentication*, Proceedings of ICIP'98, 1998, pp. 425–429.
[23] G. Xiaota and Z. Tian-ge, *A Region-based lossless watermarking scheme for enhancing security of medical data*, J. Digit. Imaging, 22(1) (2009), pp. 53–64.
[24] W. Xiaoyun, H. Junquan, C. Zhixiong, and H. Jiwu, *A secure semi-fragile watermarking for image authentication based on integer wavelet transform with parameters*, Proceedings of 2005 Australian Workshop on grid computing and e-research, vol. 44, Newcastle, New South Wales, Australia, 2005, pp. 75–80.
[25] L. Xuanwen, Q. Cheng, and J. Tan, *A lossless data embedding scheme for medical in application of e-diagnosis*, Proceedings of the 25th Annual International Conference of the IEEE EMBS Cancun, Mexico, September 17–21, 2003.
[26] X.Q. Zhou, H.K. Huang, and S.L. Lou, *Authenticity and integrity of digital mammography images*, IEEE Trans. Med. Imag. 20(8) (2001), pp. 784–791.