

Authentication and Data Hiding Using a Hybrid ROI-Based Watermarking Scheme for DICOM Images

Osamah M. Al-Qershi¹ and Bee Ee Khoo¹

Authenticating medical images using watermarking techniques has become a very popular area of research, and some works in this area have been reported worldwide recently. Besides authentication, many data-hiding techniques have been proposed to conceal patient's data into medical images aiming to reduce the cost needed to store data and the time needed to transmit data when required. In this paper, we present a new hybrid watermarking scheme for DICOM images. In our scheme, two well-known techniques are combined to gain the advantages of both and fulfill the requirements of authentication and data hiding. The scheme divides the images into two parts, the region of interest (ROI) and the region of non-interest (RONI). Patient's data are embedded into ROI using a reversible technique based on difference expansion, while tamper detection and recovery data are embedded into RONI using a robust technique based on discrete wavelet transform. The experimental results show the ability of hiding patient's data with a very good visual quality, while ROI, the most important area for diagnosis, is retrieved exactly at the receiver side. The scheme also shows some robustness against certain levels of salt and pepper and cropping noise.

KEY WORDS: Watermarking, Data hiding, Medical Image Authentication, Electronic patient record

INTRODUCTION

Medical Images are stored for different purposes such as diagnostic, long-term storage, and research.¹ When a medical image is diagnosed by a doctor at distant site, it cannot be exposed to the public by using unsecured channel to transmit it.² Moreover, any unauthorized person can access images within a medical database and can modify those images maliciously. So, medical information database must be protected and secured.

A common data security concern in medical information systems is the assurance of image identity and integrity. Image identity means that the

image is of the correct patient and is from the correct source. These facts may be detailed elsewhere in the medical records associated with the image (but stored separately), but a possibility exists that wrong details may have been recorded. Image integrity here means information confirming that no changes have been made to the original image as acquired by the medical imaging device, by a variety of manipulations which can occur during transferring or processing.³ To overcome those security issues, digital image watermarking techniques are used.

Many watermarking techniques were proposed for medical images during the last few years. Those techniques are based on general purpose watermarking methods. However, the techniques proposed must consider medical image watermarking requirements: capacity, robustness, security, and imperceptibility. Coatrieux et al. identified three classes of watermarking algorithms used for medical images.⁴ The first class groups methods that embed information within region of non-interest (RONI) in order not to compromise with the diagnoses capabilities.⁵⁻¹³ The second group of algorithms corresponds to reversible watermarking. Once the embedded content is read, the watermark can be removed from the image

¹From the School of Electrical and Electronic Engineering, Engineering Campus, Universiti Sains Malaysia, 14300 Nibong Tebal, Seberang Perai Selatan, Pulau Pinang, Malaysia.

Correspondence to: Osamah M. Al-Qershi, School of Electrical and Electronic Engineering, Engineering Campus, Universiti Sains Malaysia, 14300 Nibong Tebal, Seberang Perai Selatan, Pulau Pinang, Malaysia; tel: +604-5996032; fax: +604-5941023; e-mail: osamahqershi.lm07@student.usm.my

Copyright © 2009 by Society for Imaging Informatics in Medicine

Online publication 25 November 2009

doi: 10.1007/s10278-009-9253-1

allowing retrieval of the original image.^{14–17} The third class includes algorithms based on using classical watermarking methods while minimizing the distortion. In that category, the watermark replaces some image details such as the least significant bit (LSB) of the image or details lost after lossy image compression.^{18–24}

We adopt another classification based on the purposes of medical image watermarking. Medical image watermarking schemes may be classified into three categories: authentication schemes (including tamper detection and recovery); data-hiding schemes (for hiding electronic patient records); and schemes that combine authentication and data hiding. Authentication schemes are used to identify the source of the image, and tamper detection watermarks are able to locate the regions or pixels of the image where tampering was done. In some cases, tampered areas may be recovered. Data-hiding schemes give more importance in hiding high amount of data in the images and keep the imperceptibility very high. Depending on the purpose of the watermarking (authentication, data hiding, or both), a proper watermarking technique is chosen accordingly.

In this paper, we give an overview of the previous watermarking techniques for medical images. We then propose a hybrid region of interest (ROI)-based watermarking scheme being capable of hiding patient's data, verifying authenticity of ROI, localize tampered areas, and recover those tampered areas inside ROI. In the “[Overview of Watermarking Techniques](#),” we review watermarking techniques proposed for medical images. In “[Our Scheme](#),” we present our watermarking scheme, including data embedding, extracting, verifying, tamper localization, and recovery. In “[Experimental Results](#),” experimental results are provided to demonstrate the efficiency of the scheme. Finally, in “[Discussion and Conclusion](#),” we present our conclusion.

OVERVIEW OF WATERMARKING TECHNIQUES

Depending on the purpose of the watermarking, watermarking schemes can be classified into three categories:

A. Authentication schemes

A good example of this category of watermarking schemes is the work done by Zain et al.^{12,13} They

proposed an LSB-based scheme for ultrasound images, where the original image can be recovered completely. In embedding process, an SHA-256 hash code is calculated for the ROI selected. After that, the hash code is embedded into the LSBs of RONI. At the receiver end, the watermark is extracted from LSBs of RONI, and those pixels which carried the watermark are reset back to 0. This will produce the original image before embedding watermark. The authentication is achieved by comparing the extracted hash values with the hash values of the extracted image. If they are the same, then the image is authentic. The reversibility of the scheme is based on the fact that the original values of RONI pixels were zeros before embedding, but for nonzero values, the scheme is not reversible.

Another spatial domain technique was proposed by Zain et al. to integrate the ability of detecting tampering and subsequently recovering the image.²³ The scheme requires a secret key and a public chaotic mixing algorithm combined with simple operations such as parity check and compression to embed and recover a tampered image. In embedding process, the image is divided into blocks of 8×8 pixels each. Each block B is further divided into four sub-blocks of 4×4 pixels. The watermark, which is embedded using LSBs, in each sub-block is a 3-tuple (v, p, r) . A 3-tuple consists of two bits, v and p , for authentication, and a 7-bit recovery watermark, r , for the corresponding sub-block within block A mapped to B using a mapping function. During extraction, v and p are used for tamper detection and localization. This scheme was modified by Zain et al. by dividing ROI and RONI into smaller blocks.²⁴ Besides, the authentication bits, v and p , are embedded into sub-blocks of ROI, while the 7-bits recovery information is embedded into the corresponding sub-blocks of RONI. This will improve the image quality in ROI as the maximum change is only 2 bits in every 4 pixels.

Wu et al. proposed two schemes based on modulo 256 and discrete cosine transform (DCT).¹⁶ At first, the image is divided into several blocks, and for each block, an adaptive robust digital watermarking method combined with modulo operation is used to hide the watermark. In the first scheme, each block is embedded with the watermark, which is a combination of an authentication message (hash value of the block) and the recovery information of other blocks. Because the recovered block is too small and excessively compressed, the concept of ROI is introduced into the second scheme. The bits of ROI

are combined with hash value to form the watermark, and the watermark is embedded into RONI only. If there are no tampered blocks, the original image can be obtained with only the stego image. When the ROI is tampered with, an approximate image will be obtained from other blocks. The drawback of this scheme is limited hiding capacity, where only authentication and recovery data are embedded. Besides, the scheme is not reversible exactly due to preprocessing used to avoid pixel flipping.

Two reversible schemes based on difference expansion technique (DE) were proposed by Chiang et al. for tamper detection and recovery.¹⁷ In the two schemes proposed, the image is divided into blocks of 4×4 each, and each block is transformed using two-level DE technique. Only smooth blocks, with equal pixel values, are used for embedding watermark. In the first scheme, the average of each block is calculated and concatenated together to form the watermark, which is used as recovery information. The second scheme is a ROI-based scheme, and the pixel values of ROI are used as the watermark in order to recover the exact ROI in case of tampering. The drawback of this technique is the limited capacity because only smooth blocks are used for embedding; thus, it cannot be used for all image modalities.

B. Data-Hiding Schemes

Anand et al. proposed one of the classic schemes that belong to this category.¹⁸ In their scheme, a simple algorithm based on spatial domain technique is adopted, and two data files, a text document and an electrocardiogram (ECG) graph, are used as watermarks to be interleaved into a medical image. The text image, which contains patient data, and the ECG, which is a stream of binary numbers, are encrypted first producing the watermark. Then, the embedding process is done by swapping the LSB of the gray values of chosen pixels of the medical image with that of the watermark.

Nayak et al. improved the algorithm proposed by Anand et al. by using error correcting codes (Reed Solomon Code) in order to enhance the reliability and robustness of the watermarking.²¹

C. Authentication and Data-Hiding Schemes

This category of schemes is multipurpose schemes as they can achieve several tasks, i.e., hiding patient's report, authenticating the image,

localizing the tampered area if any, and recovering those tampered areas when needed. Of course not all schemes that belong to this category can perform all those tasks, but the more tasks the scheme can perform, the more practical the scheme is.

A good example of this category of watermarking schemes is the work done by Giakoumaki et al. First, they proposed a frequency domain technique based on discrete wavelet transform (DWT) combined with a quantization method.⁶ They then improved that technique gradually to increase its robustness and security.⁷⁻¹⁰ The technique takes the advantages of dyadic rational form of Haar wavelet coefficients and the decreased eye sensitivity to noise in high-resolution bands. The scheme embeds a robust watermark containing the physician's digital signature for source authentication and a caption watermark including patient's personal data, health history, diagnosis reports, etc. Additionally, a fragile watermark provides information on whether and where the image might have been tampered with. The fragile watermark is a reference watermark used for tamper detection. The drawback of this scheme is the lack of recovery capability in case of tamper detected.

A lossless scheme was proposed by Guo et al. based on difference expansion introduced by Tian.^{15,25} The scheme was proposed to overcome some of disadvantages of Tian's original scheme. Those disadvantages are the wasted space for embedding the location map, which in turn reduces the actual hiding capacity, and the distortion induced by embedding watermark bits. To overcome those drawbacks, they modified difference expansion technique to restrict the embedded-induced distortion inside a given region and controlling the embedding capacity. The region of embedding is chosen to prevent introducing any distortion inside the ROI. Instead of expanding the difference between two adjacent pixels, the scheme expands the differences between four adjacent pixels as a quad. Three bits of the watermark are embedded into each expandable quad. The watermark consists of a hash value and patient's data. The drawback of this scheme is the lack of tamper localizing and recovery capability. Woo et al. proposed a multiple digital image watermarking method which is suitable for privacy control and tamper detection in medical images.²² The multiple watermarks consist of an annotation

watermark, which contains patient's data, and a fragile watermark, which is used for tamper detection. During embedding process, the annotation watermark is embedded into the border pixels of the image using a robust embedding method. The watermark message is embedded using a linear additive method into the three high pass bands (HL1, LH1, and HH1) of DWT of the original image borders. The fragile watermark, which is a binary watermark pattern is tiled to cover the whole image, is embedded into the central region of the original image using the LSB method. The drawback of this scheme is the lack of reversibility and recovery capability.

OUR SCHEME

To meet medical image watermarking requirements, i.e., including all the abovementioned purposes in one scheme, we propose a hybrid ROI-based watermarking scheme, which can be used for hiding patient's data, authenticating ROI, localizing tampered areas inside ROI, and recovering those tampered areas when needed. Moreover, ROI of the original image is retrieved exactly after watermark extraction at the receiver end in order to avoid any misdiagnosis that may happen.

A combination of modified DE technique, developed by Gou et al., and DWT-based technique, developed by Kundur et al., is adopted in our scheme.^{15,26} Besides reversibility, the modified DE technique has the advantages of high capacity, theoretically 0.75 bpp, as 3 bits are embedded in each quad. On the other hand, DWT has a good performance in terms of visual quality and security, since it increases robustness without compromising imperceptibility.²⁷

In our scheme, the image is divided into blocks of 16×16 pixels each. The first watermark, which consists of patient's data and the hash message of ROI, is embedded into blocks belonging to ROI using modified DE technique, which has high embedding capacity. For simulation purposes, we chose MD5 because it is easy to implement for simulation purpose. However, stronger encryption algorithms, like RSA and SHA-256, may be used. The first step produces an embedding map which will be used later to extract the first watermark.

The map is combined with recovery information to form the second watermark. Then, the second watermark is embedded into blocks belong to RONI using a three-level DWT combined with a proper quantization method. Each block in RONI will be embedded separately by a part of the second watermark as shown in Fig. 1. The reason of this is to avoid errors during extraction.

The original quantization method, developed by Kundur et al., does not consider the characteristics of medical images, i.e., the dark areas in medical images. From the experiments, their method results in errors in those dark areas, which have gray values near zero. Those errors can be avoided by preprocessing the image before embedding by forcing the medical image's gray levels to be in the range from 4 to 255 (in case of 8-bits images). Unfortunately, the preprocessing step will affect the visual quality of the image permanently. To solve this problem, we choose to watermark blocks in RONI separately; thus, not all blocks will be preprocessed. Only blocks that may cause errors will be preprocessed. From the experimental results, those blocks can be identified by average and standard deviation. Blocks with low average and high standard deviation must be preprocessed to avoid any possible error. Embedding the second watermark also produces some side information needed to initiate the extraction phase. The side information is embedded into the border of the image using DWT as well (Fig. 2).

LL3	LH3	LH2	LH1
HL3	HH3		
HL2		HH2	
HL1			HH1

Fig 1. Bands that are used for embedding second watermark in each block; 124 bits are embedded in each block.

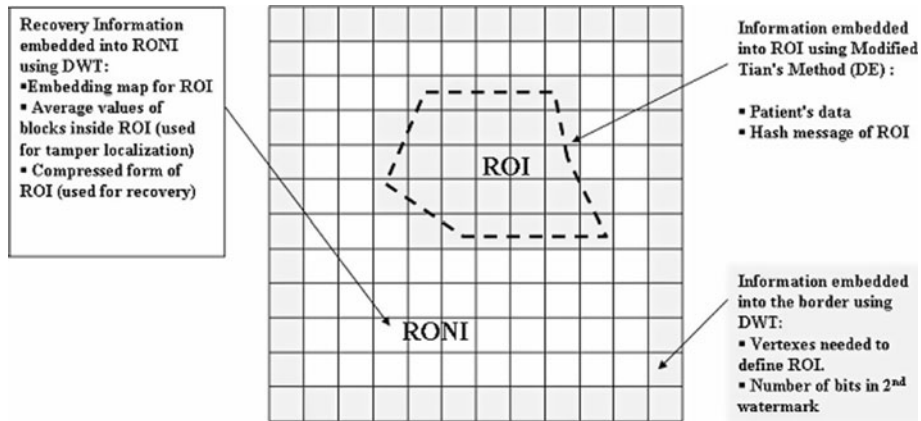


Fig 2. The three areas used for embedding the watermark.

The characteristics of our scheme can be summarized as:

1. Robust against certain types of attacks (salt and pepper and cropping). The robustness comes from using DWT combined with RS code to embed recovery information in RONI
2. Enough embedding capacity to conceal patient's data and recovery information as well (theoretically 0.75 bpp in ROI, as 3 bits are embedded into a quad, and 0.48 bpp in RONI, as 124 bits are embedded of each block)
3. Reversibility of ROI

The following section describes the embedding and extracting procedures.

A. Embedding procedure

1. ROI is selected, by a radiologist, and defined by a polygon, and then the image is divided into blocks of 16×16 pixel each, where the blocks belong to each part, ROI and RONI, are marked. Now ROI is represented by a group of adjacent blocks.
2. ROI is compressed using JPEG2000 forming ROI_{comp} . This compressed version of ROI will be used for recovery in case of tamper detection. Figure 3 shows an example of compression quality. Lossy compression is used in order to save the capacity in RONI.
3. The average of each block in ROI is calculated as AV_i . These values will be used for tamper detection.
4. The hash message for ROI, $hash_1$, is calculated using MD5 algorithm.

5. Patient's data is compressed and concatenated with $hash_1$. The resultant bit stream is coded using Reed Solomon code (RS code) to form

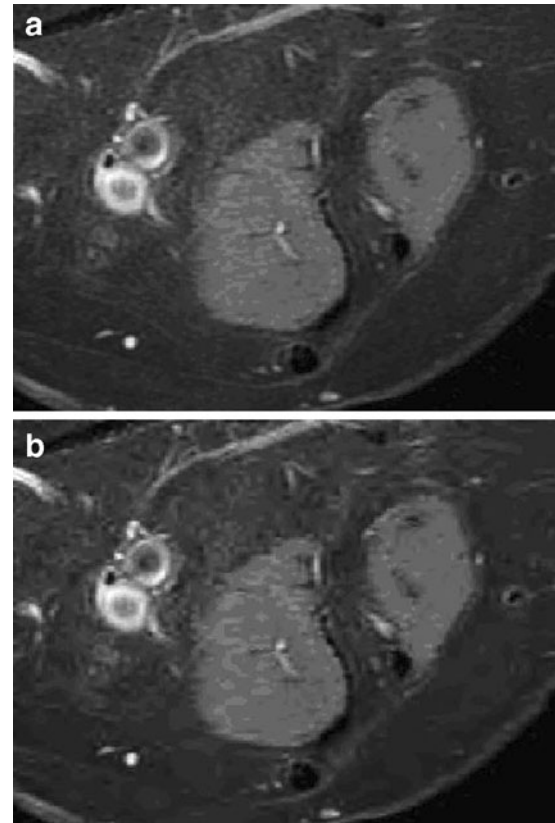


Fig 3. a The original ROI and b the compressed version using JPEG2000.

- the first watermark w_1 . Using RS code will increase the robustness and reliability.
6. ROI is divided into quads, where a quad is four adjacent pixels. The quads are scanned sequentially, and for each expandable quad, 3 bits of w_1 are embedded using modified DE technique. The process ends when all w_1 bits are embedded, and the embedding map, EM, is formed.
 7. AV and EM are compressed using Huffman coding technique to form AV_{comp} and EM_{comp} , respectively.
 8. ROI_{comp} , AV_{comp} , and EM_{comp} are encoded using RS code and then concatenated to form the second watermark w_2 .
 9. Blocks in RONI are scanned sequentially, and for each block, three-level Haar DWT is performed; 124 bits of w_2 are embedded in each block. The process ends when no bits are left to be embedded.
 10. The side information needed to initiate the extraction phase is embedded into blocks belonging to the border using the same DWT technique. Side information contains location of ROI, size of w_2 , etc.

The watermarked image is now ready to be stored in the hospital's database system or can be sent to another medical institution.

B. Extracting procedure

1. The image is divided into blocks as in embedding phase.
2. Side information extracted from the blocks of the border. Side information is used to mark blocks belong to each part, ROI and RONI.
3. Blocks in RONI are scanned, and w_2 is extracted.
4. The w_2 is decomposed into its original parts which are then decoded using RS code to obtain ROI_{comp} , AV_{comp} , and EM_{comp} . To start extracting w_1 , EM_{comp} is decompressed to obtain the original embedding map EM.
5. Using EM, quads in ROI are scanned, and w_1 bits are extracted. Those quads which hold the watermark bit are reversed during extraction resulting in the original ROI.
6. Then, w_1 is decoded using RS code, and patient's data and $hash_1$ are obtained.
7. A hash message for the recovered ROI, $hash_2$, is calculated. If $hash_1 = hash_2$, then the image is authentic and the procedure ends. If $hash_1 \neq$

Table 1. Embedding and Extracting Results for Four Images of Different Modalities

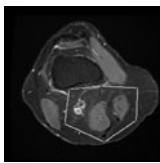
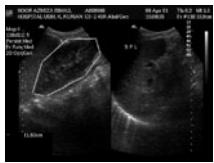
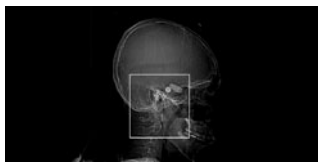

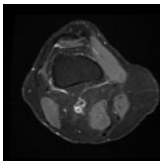
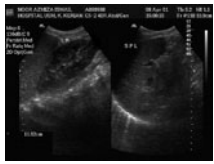


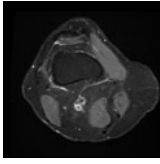
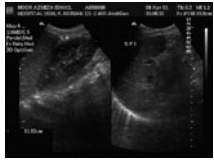


Original Image				
Watermarked Image				
The reconstructed image				

Table 2. Embedding and Extracting Results for Four Images with ROI Size is 12% of Image Size

Modality	Image size	Size of w_1 (bits)	Size of w_2 (bits)	Embedding capacity (bpp)	Available capacity (bpp)	PSNR (dB)		SSIM	
						After watermarking	After extracting	After watermarking	After extracting
MR	512 × 512, 16 bit	18,360	85,808	0.2009	0.46	69.71	85.88	0.9287	0.9390
US	576 × 768, 8 bit	18,360	118,420	0.3091	0.47	36.71	37.30	0.7708	0.7911
CT	440 × 888, 16 bit	18,360	73,780	0.1888	0.47	85.50	90.95	0.9765	0.9826
CR	2500 × 2,048, 12 bit	18,360	395,436	0.0808	0.50	65.22	69.26	0.9977	0.9984

Embedding capacity calculated as: (size of w_1 + size of w_2)/image size

hash₂, then the image is not authentic, and this means that some tampering is detected. Proceed to the next step where the tampered area is localized and recovered.

8. ROI is divided into blocks of 16×16 pixels. The average value of each block is calculated and compared with the corresponding value in AV. If they are not equal, the block is marked as

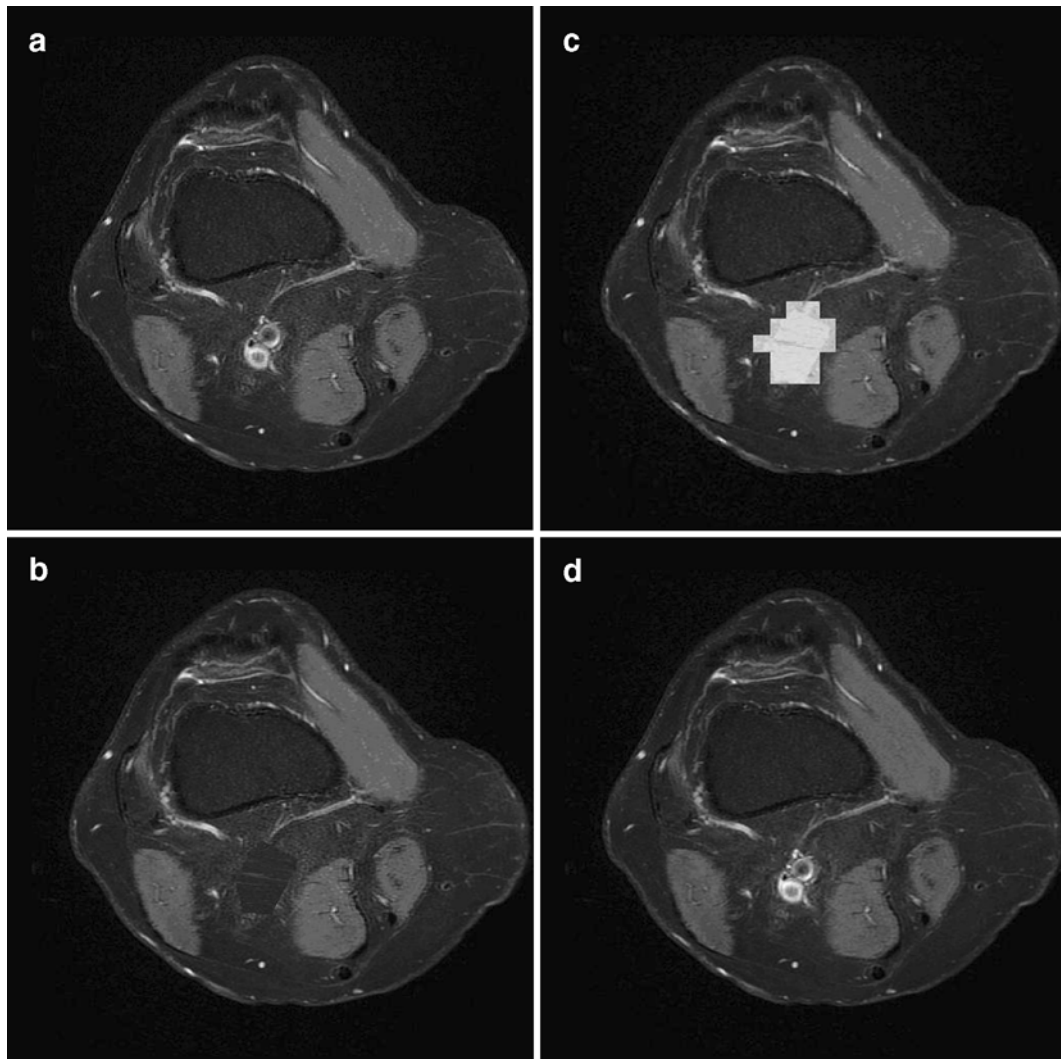


Fig 4. Tamper localization and recovery after replacing a part of ROI: a watermarked image, b tampered image, c localizing tampered area, and d recovering tampered area.

tampered and replaced by the corresponding block of the compressed version of ROI, ROI_{comp} as a recovery process.

EXPERIMENTAL RESULTS

Four DICOM images, two 16-bit, one 12-bit, and one 8-bit, of different modalities and sizes were used to test our scheme, where a patient report of size 1.8 KB is embedded inside ROI. The values of the average standard deviation used to identify blocks to be preprocessed are 16 and 40, respectively. Tables 1 and 2 show the results of embedding the watermark.

The watermarked images show very good visual quality in terms of PSNR, especially in case of 16-bit images. The reversibility ROI can be verified by comparing the extracted image with the original image pixel by pixel, while the authenticity of ROI can also be verified by comparing the embedded hash value with the calculated one during extraction phase. If they are identical, ROI is authentic. From the results, the original ROI can be extracted exactly in case of no tamper.

To demonstrate tamper localization and recovery, we replaced some pixel values inside ROI in the watermarked image. During extraction, our scheme can success-

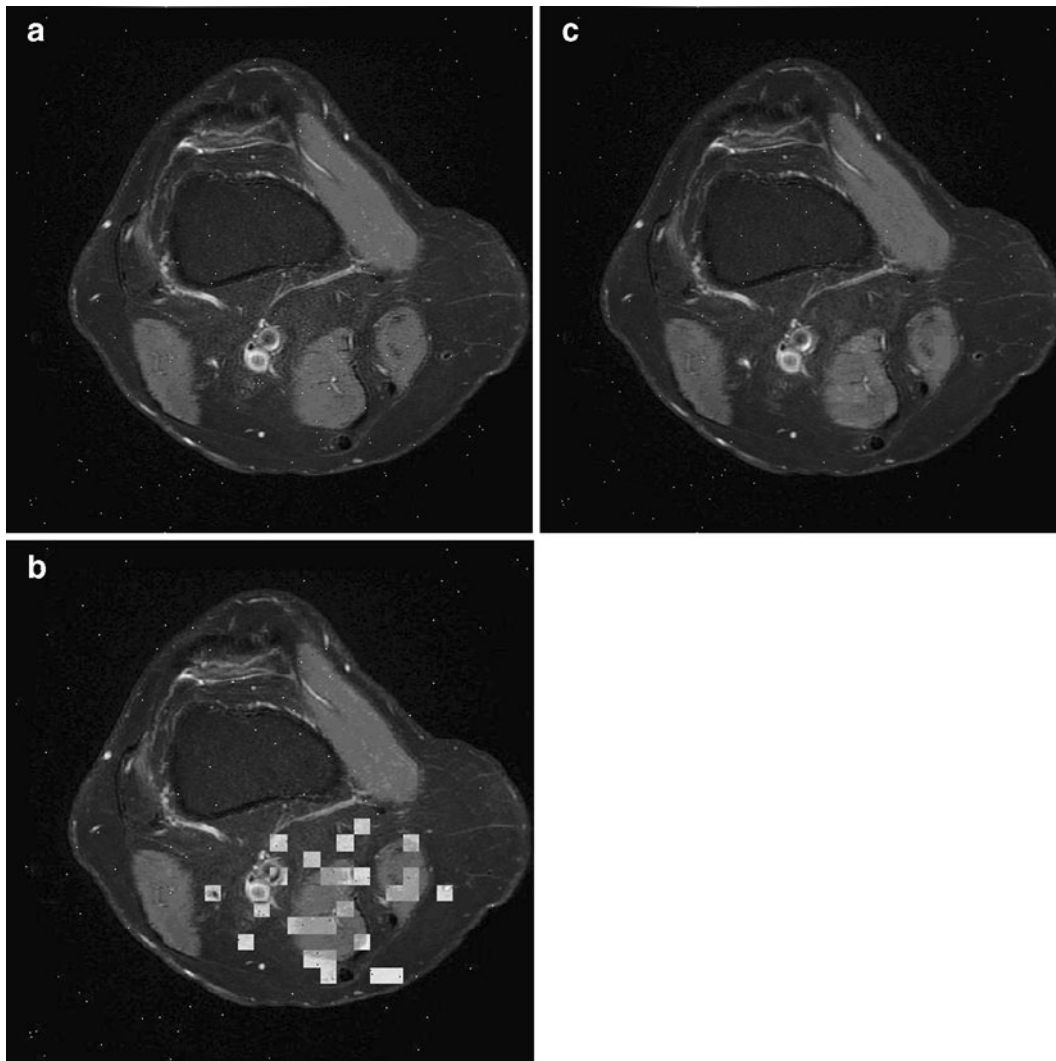


Fig 5. Tamper localization and recovery adding salt and pepper noise: a the watermarked image after adding salt and pepper noise, b localizing tampered areas, and c recovered image.

Table 3. A Comparison Between Our Scheme and the Reviewed Schemes

Scheme	Objectives	Methodology				Capabilities			Characteristics		Visual quality
		ROI-based	Embedding technique	Block-based	Reversible	Taper localization	Temper recovery	Robustness	Hiding capacity		
Zain ^{12,13}	Authentication	✓	Spatial LSB	×	✓	×	×	Fragile	No Patient's data are embedded. Only authentication data are embedded. No Patient's data are embedded. Only authentication and recovery data are embedded. Hiding capacity = 0.44 bpp	Good	
Zain ²³	Authentication	×	Spatial LSB	16 × 16	×	✓	Average of blocks	Fragile	No Patient's data are embedded. Only authentication and recovery data are embedded. Hiding capacity = 0.44 bpp	Good	
Zain ²⁴	Authentication	✓	Spatial LSB	4 × 4, 2 × 4	×	✓	Average of blocks	Fragile	No Patient's data are embedded. Only authentication and recovery data are embedded. Only authentication data are embedded.	Good	
Wu ¹⁶ (1)	Authentication	×	Frequency DCT	Size is not fixed	✓	✓	Compressed form of each block	Robust (based on modulo 256 addition), but no test results provided by the authors.	No Patient's data are embedded. Only authentication data are embedded	Good	
Wu ¹⁶ (1)	Authentication	✓	Frequency DCT	Size is not fixed	✓	✓	✓		embedded	Good	
Chiang ¹⁹ (1)	Authentication	✓	Modified DE	4 × 4	✓	✓	Average of blocks	Fragile	Low hiding capacity. No Patient's data can be embedded. Moreover, it cannot be used for all image modalities since embedding is done in smooth blocks only.	Good	
Chiang ¹⁹ (2)		✓			✓	✓	✓	Fragile		Good	
Anand ¹⁸	Data Hiding	✓	Spatial LSB	✓	✓	✓	✓	Fragile	High embedding capacity up to 1 bpp	Good	
Nayak ²¹	Data Hiding	✓	Spatial LSB	✓	✓	✓	✓	Fragile	High embedding capacity up to 1 bpp	Good	
Giakoimaki ⁶⁻¹⁰	Authentication and Data Hiding	✓	Frequency DWT	×	×	×	×		For images of size m × n: Total size of patient data that can be embedded (with no ECC) = 21 mn/256 bits. With ECC it will be decreased to forth of that. Hiding capacity is 0.08 bpp without ECC and 0.02 bpp with ECC	Good	

Table 3. (continued)

Scheme	Objectives	Methodology		Capabilities			Characteristics		Visual quality
		ROI-based	Embedding technique	Block-based	Reversible	Taper localization	Tamper recovery	Robustness	
Woo ²²	Authentication and Data Hiding	×	DWT + LSB	×	×	×	×	<p>Although the robustness wasn't tested, it easy to figure out that the scheme is fragile as it is based on LSB. Only the data hid in the border may survive certain attacks.</p> <p>Only the border of the image is used for embedding patient's data. The size of the border is not determined but it quite small. This means low hiding capacity</p> <p>Theoretically, 3 bits can be embedded into a block of 2×2, which means 0.75 bpp. However, the authors did not use the scheme for hiding patient's data. It can be used for data hiding.</p>	Very good
Gou ¹⁵	Authentication and Data Hiding	✓	Spatial + DE	4×4	✓	×	×	<p>Fragile</p> <p>Shows some robustness against cropping and certain level of salt and pepper noise</p>	Very good
Our scheme	Authentication and Data Hiding	✓	Modified DE + Frequency DWT	16×16	Only ROI	✓	Compressed form of ROI	<p>The overall capacity is in the range 0.46–0.50 bpp</p>	Very good

fully extract the embedded patient's data, localize tampered area, and recover that area with the corresponding compressed version of the same area as shown in Fig. 4.

Also, we tested our scheme by adding salt and pepper noise of 0.0005 to simulate transmission errors. In this case, our scheme can successfully extract the embedded patient's data, localize tampered area, and recover that area with the corresponding compressed version of the same area as shown in Fig. 5. A comparison between our scheme and the previous schemes is illustrated in Table 3.

DISCUSSION AND CONCLUSION

In this paper, we proposed a watermarking scheme that combines two techniques; DE and DWT. The modified DE technique is used to embed patient's data into ROI. The information needed to extract data from ROI is concatenated with recovery information and embedded into ROI using DWT combined with a quantization method. This means that our scheme can be used for data hiding, with up to hiding capacity of 0.46–0.50 bpp, and authentication as well. It not only can detect the locations of tampered areas inside ROI of the watermarked image but also can recover the content of those areas with high visual quality. Besides, if the watermarked image is announced authentic, this means it is not tampered and the original ROI can be extracted exactly from the watermarked image. If the image is not authentic, the tamper localization and recovery capabilities depend on the amount tampering and the areas that have been tampered. Using RS code increases localization and recovery capabilities significantly but generates bigger watermark and, thus, more data to be embedded. As the result of this, the size of the image is very critical. To allow tamper localization and recovery capabilities, the size of the image must be at least 512×512 pixels. For smaller images, the algorithm can be applied but without recovery facility as there will not be enough space to embed the compressed form of ROI.

Usually, time is not measured in evaluating watermarking algorithm. This makes it difficult to compare our scheme to other schemes found in the literature in terms of time. Among the four tested modalities, CR images may consider time con-

suming because of its size, i.e., one CR image equals about 20 images of MR modality.

However, in comparison to other schemes previously mentioned, our scheme shows better performance in terms of:

1. **Functionality:** It can be used of data hiding and authentication.
2. **Generality:** It can be applied for different image modality.
3. **Accuracy:** A good quality version of ROI is used for recovery.
4. **Embedding capacity:** 0.46–0.50 bpp.
5. **Robustness:** It can stand cropping and certain level of salt and pepper noise.
6. **Imperceptibility:** ROI can be retrieved exactly at the receiver end.

For future work, we expect to expand the proposed scheme to be used for sequential watermarking where the image can be embedded several times with patient's data by different physicians when needed. This means the scheme must have higher capacity. Also, we will work on enhancing the robustness of the scheme against a wider spectrum of attacks.

ACKNOWLEDGMENT

This work is supported by Ministry of Science, Technology, and Innovation through eScienceFund grant 01-01-05-SF0114 and Ministry of Higher Education through Fundamental Research Grant Scheme.

REFERENCES

1. Raúl R-C, Claudia F-U, Trinidad-Bias de GJ. Data Hiding Scheme for Medical Images. In proceedings of the 17th International Conference on Electronics, Communications and Computers CONIELECOMP '07 2007
2. Frommer MH: Telemedicine: the next generation is here. In Proceedings of Academia/Industry Working Conference on Research Challenges, 2000: pp. 197–203
3. Maeder AJ, Planitz BM: Medical Image Watermarking for Multiple Modalities. in proceedings of the 34th Applied Imagery and Pattern Recognition Workshop (AIPR'05). 2005
4. Coatrieux G, Lecornu L: A Review of Image Watermarking Applications in Healthcare. in proceedings of the 28th Annual International Conference of the IEEE: Engineering in Medicine and Biology Society, EMBS '06. 2006
5. Wakatani A: Digital Watermarking for ROI Medical Images by Using Compressed Signature Image. In proceedings of the 35th Hawaii International Conference on System Sciences. 2002
6. Giakoumaki A, Pavlopoulos S, Koutsouris D: A medical image watermarking scheme based on wavelet transform. in

Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society. 2003

7. Giakoumaki A, Pavlopoulos S, Koutsouris D: A Multiple Watermarking Scheme Applied to Medical Image Management. in proceedings of the 26th Annual International Conference of the IEEE EMBS. 2004
8. Giakoumaki A, Pavlopoulos S, Koutsouris D: Multiple Digital Watermarking Applied to Medical Imaging. In Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference. 2005
9. Giakoumaki A, Pavlopoulos S, Koutsouris D: Secure and efficient health data management through multiple watermarking on medical images. *Med Biol Eng Comput* 44:619–631, 2006
10. Giakoumaki A, Pavlopoulos S, Koutsouris D: Multiple Image Watermarking Applied to Health Information Management. *IEEE Trans Inf Technol Biomed* 10(4):722–732, 2006
11. Lee H-K et al.: ROI Medical Image Watermarking Using DWT and Bit-plane, in Asia-Pacific Conference on Communications. 2005: Perth, Western Australia
12. Zain JM, Baldwin LP, Clarke M: Reversible watermarking for authentication of DICOM images. In Proceedings of the 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society. 2004
13. Zain JM, Clarke M: Reversible region of non-interest (RONI) watermarking for authentication of DICOM images. *Int J Comput Sci Network Secur* 7:19–28, 2007
14. Macq B, Deweyand F: Trusted headers for medical images. in DFG VIII-D II Watermarking Workshop. 1999. Erlangen, Germany
15. Guo X, Zhuang T-g: A region-based lossless watermarking scheme for enhancing security of medical data. *J Digit Imaging* 0:1–12, 2007
16. Wu JHK, et al: Tamper detection and recovery for medical images using near-lossless information hiding technique. *J Digit Imaging* 21:59–76, 2008

17. Chiang K-H, et al: Tamper detection and restoring system for medical images using wavelet-based reversible data embedding. *J Digit Imaging* 21(1):77–90, 2008

18. Anand D, Niranjana UC: Watermarking medical images with patient information. In proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 1998
19. Zhou XQ, Huang HK, Lou SL: Authenticity and integrity of digital mammography images. *IEEE Trans Med Imag* 20(8):784–791, 2001
20. Boucherkha S, Benmohamed M: A lossless watermarking based authentication system for medical images. *IEEE Trans Engg Comput Technol* 1:240–243, 2004
21. Nayak J, et al.: Reliable transmission and storage of medical images with patient information using error control codes. in proceedings of the First India Annual Conference, IEEE INDICON 2004. 2004
22. Woo C-S, Du J, Pham B: Multiple Watermark Method for Privacy Control and Tamper Detection in Medical Images. In Proceedings of the APRS Workshop on Digital Image Computing Pattern Recognition and Imaging for Medical Applications. 2005
23. Zain JM, Fauzi ARM: Medical Image Watermarking with Tamper Detection and Recovery in Proceedings of the 28th IEEE EMBS Annual International Conference. 2006
24. Zain JM, Fauzi ARM: Evaluation of Medical Image Watermarking with Tamper Detection and Recovery (AW-TDR). In The 29th Annual International Conference of the IEEE EMBS. 2007
25. Tian J: Reversible data embedding using a difference expansion. *IEEE Trans Circuits Syst Video Technol* 13(8):890–896, 2003
26. Kundur D, Hatzinakos D: Digital watermarking for telltale tamper proofing and authentication. in Proceedings of the IEEE. 1999
27. Hartung F, Kutter M: Multimedia watermarking techniques. *Proc IEEE* 87(7):1079–1107, 1999