ROI–based Tamper Detection and Recovery for Medical Images Using Reversible Watermarking Technique

Osamah M. Al-Qershi, Bee Ee Khoo
School of Electrical and Electronic Engineering
Universiti Sains Malaysia
Penang, Malaysia
E-mail: osamahqershi.lm07@student.usm.my, beekhoo@eng.usm.my

Abstract—**Digital image watermarking is proposed to overcome the problems of security, capacity and cost in health care management systems. Medical images, unlike most of images, require extreme care when embedding additional data within them because the additional information must not affect the image quality and readability. In order to overcome any misdiagnose caused by embedding data into medical images, lossless data hiding techniques have been developed. This paper presents a lossless watermarking technique for Ultrasound (US) images. The proposed technique adopts a high-capacity reversible data hiding scheme based on difference expansion (DE). It can be used to hide patient's data hiding and protecting the region of interest (ROI) with tamper detection and recovery capability. The experimental results show that the original image can be exactly extracted from the watermarked one in case of no tampering. In case of tampered ROI, tampered area can be localized and recovered losslessly.**

Keywords—reversibale watermarking; ROI-basd, Tamper detection; medical image

I. INTRODUCTION

Most hospitals and health care systems involve a large amount of data storage and transmission such as administrative documents, patient information, medical images, and graphs. Among these data, the patient information and medical images need to be organized in an appropriate manner in order to facilitate using and retrieving such data and to avoid mishandling and loss of data [1]. On the other hand, the transmission of such a large amount of data when done separately using ordinary commercial information transmitting channels like Internet, it results in excessive memory utilization, an increase in transmission time and cost and also make that data accessible to unauthorized personnel [2]. In order to overcome the capacity problem and to reduce storage and transmission cost, data hiding techniques are used for concealing patient information with medical images. Those data hiding techniques can be also used for authentication and tamper detection to judge the images integrity and fidelity [3].

Watermarking techniques can be classified into two categories, reversible and irreversible. The reversible watermarking techniques are used to avoid irreversible distortion in image by extracting the original image exactly at the receiver end. Medical image watermarking is one of the most important fields that need such techniques where distortion may cause misdiagnosis [4]. Of course, the reversibly watermarked image is not distortion-free, but that distorted image is used as a carrier for data to be embedded and not for diagnosis. The losslessly recovered image is the final one for diagnosis [5].

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 [6]. 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 propose a reversible 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 section 2, we review watermarking techniques proposed for medical images. In section 3, we present our proposed watermarking technique, including data embedding, extracting, verifying, tamper localization and recovery. In section 4, experimental results are provided to demonstrate the efficiency of the scheme. Finally, in section 5 we present our conclusion.

978-1-4244-6941-3/10/$26.00 ©2010 IEEE

II. Relative work

The earlier watermarking techniques were proposed for data hiding applications only [2, 7]. Then, the authentication capability became an important aspect in medical image watermarking techniques. However, a practical watermarking technique for medical images should be able to hide Electronic Patient Records (EPR), and also able to authenticate the images with tamper detection and recovery [6].

A good example of such techniques is the work done by Zain *et al.* [8, 9]. 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. The drawback of these two schemes is that 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.

Two techniques were proposed by Zain *et al.* to integrate the ability of detecting tampering and subsequently recovering the image [10,11]. 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. The drawbacks of these two schemes are the lack of reversibility and using of averages as recovery information.

Wu *et al.* proposed two schemes based on modulo 256 and discrete cosine transform (DCT) [12]. 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. 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.

A lossless scheme was proposed by Guo *et al.* based on difference expansion introduced by Tian [13, 14]. To overcome the drawbacks of Tian's method, they modified difference expansion technique to restrict the embedded induced distortion inside a given region and controlling the embedding capacity. The drawback of this scheme is the lack of tamper localizing and recovery capability.

Two reversible schemes based on difference expansion technique (DE) were proposed by Chiang *et al*. for tamper detection and recovery [15]. In the two proposed schemes, 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. 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.

Also, we proposed two watermarking techniques for data hiding and authentication [3]. The first one is a fragile watermarking scheme that combines two techniques: DE and modified DE. The modified DE technique developed by Gou et al 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 RONI using the original DE technique. This means that the scheme can be used for data hiding and authentication. 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, when available, with high visual quality. Besides, if the watermarked image is announced authentic, this means it is not tampered and the original image can be extracted exactly from the watermarked image. The second one was proposed to enhance the robustness of the 1st scheme to make it able to survive certain types of attacks [6]. This was achieved by using a combination of modified DE technique, developed by Gou et al., and DWT-based technique, which turned it into a hybrid scheme. Moreover, Reed-Solomon (RS) code was used to increase the robustness of the scheme. Using RS code generates bigger watermark, and thus more data to be embedded. As the results of this, the size of the image is very critical. This scheme has the same drawbacks of the previous one.

III. The proposed technique

In order to overcome the drawbacks of our previous techniques, a DE-based data hiding scheme with very high capacity is adopted in the proposed technique. Such a scheme will ease embedding the recovery information of ROI without lossy compression which was used previously.

The original DE technique involves pairing the pixels of the host image and transforming them into a low-pass image containing the integer averages and a high-pass image containing the pixel differences [13, 16]. During embedding, differences are classified into three groups: expandable, changeable, and non-changeable. Data bits are embedded only into expandable and changeable. A location map is formed to distinguish between the three different groups.

The map is then compressed, concatenated with the payload, and then embedded into the image.

In this paper we adopt a two-dimensional DE (2D-DE) which is a modified form of DE with a very high embedding capacity [17]. In this scheme, the image is divided into non-overlapping blocks of 4 × 4 pixels. Each block is transformed into frequency domain using Haar wavelet transform in the horizontal direction and then in the vertical direction, which represents the two dimensions of the block. Using difference expansion, 16 bits are embedded into those blocks which do not cause overflow or underflow.

Our proposed technique can be used for hiding patient's data, authenticating ROI, localizing tampered areas inside ROI, and recovering those tampered areas when needed. Moreover, the original image is recovered exactly after watermark extraction at the receiver end. The technique divides the image into three regions, ROI, RONI, and the border. The payload is embedded into RONI using 2D-DE scheme, and this produces an embedding map which will be used later during extraction phase. The embedding map is embedded into LSB's of border pixels. The payload consists of:

1. Patient's data.
2. Hash message of ROI; which will be used to authenticate ROI.
3. ROI pixels; which will be used for tamper detection and recovery when needed.
4. LSB's of border pixels, which will be used to restore the original border pixels.

A. The embedding phase:

1- ROI is selected and the RONI and the border regions are defined.

2- ROI is divided into blocks of 16 x 16 pixels.

3- The hash message for ROI, *H*, is calculated using MD5 algorithm.

4- The bits of ROI pixels are collected as *P*.

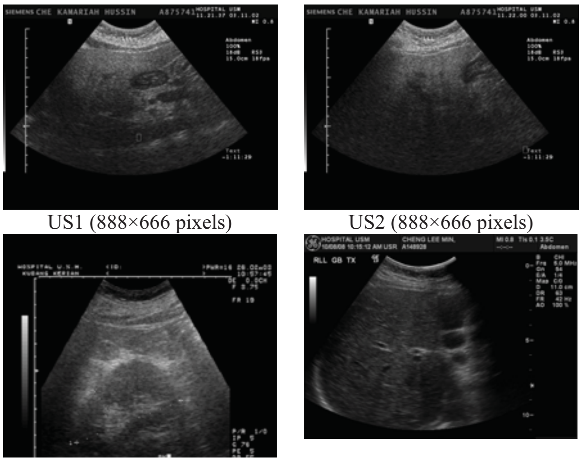
5- The LSB's of border's pixels are collected as *L*.

6- The patient' data, *D*, is concatenated with *H*, *P*, and *L* and then compressed using Huffman coding to the form the payload.

7- The payload is embedded into RONI using 2D-DE scheme mentioned above, and the embedding map is generated.

8- The embedding map is concatenated with ROI coordinates, compressed, and then embedded into LSB's of border's pixels.

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



US1 (888×666 pixels) US2 (888×666 pixels)

US3 (704×576 pixels) US4 (640×480 pixels)

Figure 1. US images which were used for testing

B. The extracting phase

1- The LSB's of the border's pixels are collected. The collected bit stream is depressed and the embedding map is generated and ROI coordinates are extracted.

2- Using ROI coordinates; ROI and RONI regions are defined.

3- The payload is extracted from RONI, decompressed, and then decomposed to the five parts; *H*, *P*, *L*, *D*.

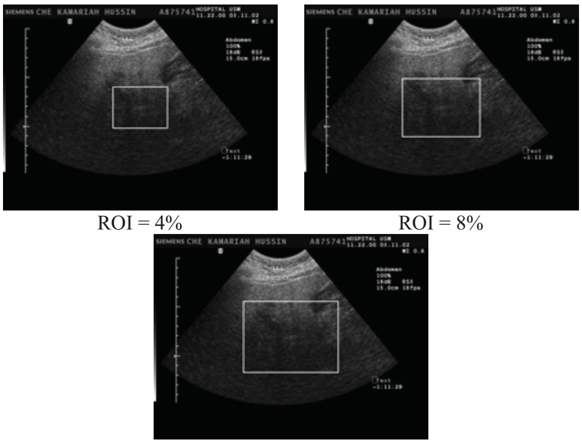
4- The hash message of ROI is calculated and compared to the extracted one. If they are equal, the image is said to be authentic and proceed to step 6. If not, the image is not authentic, and this means that some tampering is detected. In the next step the tampered area is localized and recovered.

5- ROI is divided into blocks of 16 x 16 pixels. The average value of each block is calculated and compared to value of the average of the corresponding pixel in the extracted ROI; *P*. If they are not equal, the block is marked as tampered and replaced by the corresponding pixels *P*.

6- The LSB's of the border's pixels are recovered using the bits of *L*.

IV. The Experimental Results

Four DICOM images of US modality with different sizes were used to test the proposed technique as shown in Figure 1. The proposed technique was tested on the four images with different ROI sizes and different patient's data sizes as shown in Figure 2. The watermarked images show good visual quality in terms of PSNR, with high embedding capacity as shown in Table I. From the results, the original image can be extracted exactly in case of no tamper. The reversibility of the proposed scheme can be verified by comparing the extracted image with the original image pixel by pixel, while the authenticity of ROI can also verified by comparing the embedded hash value with the calculated on during extraction phase. If they are identical, ROI is authentic.



ROI = 4%

ROI = 8%

ROI = 12%

Figure 2. Different ROI size were tested

To demonstrate tamper localization and recovery, some pixel values inside ROI were replaced with pixel values from RONI in the watermarked image. During extraction, the proposed scheme can successfully extract the embedded patient's data, localize tampered area, and recover that area with the corresponding pixel values of the same area as it is shown in Figure 3.

VII. Discussion

From the results, it obvious that the technique shows very high capacity as 10 KB of data, in addition to the recovery data, can be embedded with very good quality in terms of peak signal to noise ratio (PSNR). The improved efficiency of the proposed scheme compared to our previous hybrid techniques mentioned in section 2 is illustrated in Table II. However, applicability of the proposed techniques depends on three factors, image size, ROI size, and patient's data size as it is illustrated in Table I.

TABLE I. THE EMBEDDING RESULTS WITH DIFFERENT ROI SIZES AND PATIENTS'S DATA SIZES
'N/A' MEANS NO SPACE TO EMBED THE PAYLOAD

	2K			6K			10K		
ROI size	Payload (bit)	Hiding Capacity (bpp)	PSNR	Payload (bit)	Hiding Capacity (bpp)	PSNR	Payload (bit)	Hiding Capacity (bpp)	PSNR
4%	169,424	0.287	37.01	209,520	0.354	36.42	246,768	0.417	36.07
8%	260,704	0.441	35.99	299,760	0.507	35.54	335,312	0.567	35.28
12%	395,680	0.669	35.63	436,528	0.738	35.60	n/a	n/a	n/a

US1

	2K			6K			10K		
ROI size	Payload (bit)	Hiding Capacity (bpp)	PSNR	Payload (bit)	Hiding Capacity (bpp)	PSNR	Payload (bit)	Hiding Capacity (bpp)	PSNR
4%	155,808	0.264	37.46	194,816	0.329	36.81	230,112	0.389	36.46
8%	245,376	0.415	36.45	283,872	0.480	36.09	319,024	0.539	35.86
12%	376,368	0.636	36.13	417,056	0.705	36.09	n/a	n/a	n/a

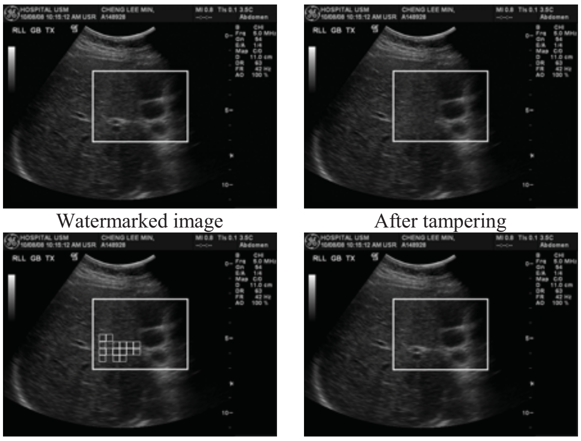
US2

	2K			6K			10K		
ROI size	Payload (bit)	Hiding Capacity (bpp)	PSNR	Payload (bit)	Hiding Capacity (bpp)	PSNR	Payload (bit)	Hiding Capacity (bpp)	PSNR
4%	122,848	0.303	41.88	163,136	0.402	40.13	200,176	0.494	39.15
8%	207,776	0.512	39.36	245,824	0.606	38.34	281,200	0.694	37.75
12%	263,984	0.651	38.24	n/a	n/a	n/a	n/a	n/a	n/a

US3

	2K			6K			10K		
ROI size	Payload (bit)	Hiding Capacity (bpp)	PSNR	Payload (bit)	Hiding Capacity (bpp)	PSNR	Payload (bit)	Hiding Capacity (bpp)	PSNR
4%	82,832	0.270	41.25	119,088	0.388	39.81	153,968	0.501	38.57
8%	151,552	0.493	38.84	191,024	0.622	37.94	n/a	n/a	n/a
12%	190,912	0.622	38.10	n/a	n/a	n/a	n/a	n/a	n/a

US4



Watermarked image

After tampering

Localizing the tampered areas

The recovered image

Figure 3. Tamper localizing and recovering

TABLE II. A COMPARIOSN BETWEEN THE PROPOSED TECHNIQUE AND THE HYBRID ONE

	Hiding Capacity	Visual quality (@ 2KB)	Recovery of ROI
The proposed technique	up to 10KB of data	up to 41.25 dB	The exact ROI is used
The hybrid technique	up to 2KB of data	up to 36.43 dB	Losslessly compressed ROI

For images US1 and US2, the proposed technique can hide less than 10 KB of data with ROI size up to

12% of the image, but cannot hide such amount of data in US3 and US4 which are smaller in size.

VIII. Conclusion

In this paper, we proposed a watermarking technique which is based on a reversible data hiding scheme with very high capacity. The proposed technique can be used for hiding patient's data for 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 exactly. It shows very good performance in terms of hiding capacity and visual quality as well.

For future work, we expect to adopt different hiding schemes with higher embedding capacity to overcome the problems of ROI size and image size. We will also try to extend the technique to be used for sequential watermarking where the image can be embedded several times with comments by different physicians when needed. Also, multiple-ROI concept can be added to make the scheme more practicable in medical informatics.

Acknowledgment

This work is supported by Ministry of Science, Technology and Innovation through eScienceFund grant (305/PELECT/6013101) and Ministry of Higher Education through Fundamental Research Grant Scheme (203/PELECT/6071135).

References

[1] J. Nayak , P. S. Bhat, R. Acharya U, and M. S. Kumar, "Efficient Storage and Transmission of Digital Fundus Images with Patient Information Using Reversible Watermarking Technique and Error Control Codes," *Journal of Medical Systems,* 2008.

[2] D. Anand and U. C. Niranjan, "Watermarking medical images with patient information," in proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 1998, pp. 703-706

[3] O. M. Al-Qershi and B. E. Khoo, "Authentication and Data Hiding Using a Reversible ROI-based Watermarking Scheme for DICOM Images," in Proceedings of International Conference on Medical Systems Engineering (ICMSE), 2009, pp. 829-834.

[4] X. Guo and T.-g. Zhuang, "Lossless Watermarking for Verifying the Integrity of Medical Images with Tamper Localization," Journal of Digital Imaging, 2009, vol. 22, pp. 620-628.

[5] X. Luo, Q. Cheng, and J. Tan, "A Lossless Data Embedding Scheme for Medical Images in Application of e-Diagnosis," in Proceedings of the 25" Annual International Conference of the IEEE EMBS, 2003, pp. 852-855.

[6] O. M. Al-Qershi and B. E. Khoo, "Authentication and Data Hiding Using a Hybrid ROI-Based Watermarking Scheme for DICOM Images " Journal of Digital Imaging, (Online first) 2009.

[7] J. Nayak, P. S. Bhat, M. S. Kumar, and U. R. Acharya, "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, pp. 147-150.

[8] J. M. Zain, L. P. Baldwin, and M. Clarke, "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, pp. 3237 - 3240.

[9] J. M. Zain and C. M., "Reversible Region of Non-Interest (RONI) Watermarking for Authentication of DICOM Images," International Journal of Computer Science and Network Security, vol. 7, pp. 19-28, 2007.

[10] J. M. Zain and A. R. M. Fauzi, "Medical Image Watermarking with Tamper Detection and Recovery " in Proceedings of the 28th IEEE EMBS Annual International Conference, 2006, pp. 3270-3273.

[11] J. M. Zain and A. R. M. Fauzi, "Evaluation of Medical Image Watermarking with Tamper Detection and Recovery (AW-TDR)," in The 29th Annual International Conference of the IEEE EMBS, 2007, pp. 5661-5664.

[12] J. H. K. Wu, R.-F. Chang, C.-J. Chen, C.-L. Wang, T.-H. Kuo, W. K. Moon, and D.-R. Chen, "Tamper Detection and Recovery for Medical Images Using Near-lossless Information Hiding Technique " Journal of Digital Imaging, 2008, vol. 21, pp. 59-76.

[13] J. Tian, "Reversible Data Embedding Using a Difference Expansion," IEEE Transactions on Circuits and Systems for Video Technology, 2003, vol. 13, pp. 890-896.

[14] X. Guo and T.-g. Zhuang, "A Region-Based Lossless Watermarking Scheme for Enhancing Security of Medical Data," Journal of Digital Imaging, vol. 0, pp. 1-12, 2007.

[15] K.-H. Chiang, K.-C. Chang-Chien, R.-F. Chang, and H.-Y. Yen, "Tamper Detection and Restoring System for Medical Images Using Wavelet-based Reversible Data Embedding," Journal of Digital Imaging, 2008, vol. 21, pp. 77-90.

[16] J. Tian, "Wavelet-based reversible watermarking for authentication," Proc. SPIE , Security and Watermarking of Multimedia Contents IV, 2008, vol. 4675, pp. 679-690.

[17] O. M. Al-Qershi and B. E. Khoo, "Reversible Watermarking Scheme Based on Two-Dimensional Difference Expansion (2D-DE)," in The 2010 International Conference on Computer Research and Development, ICCRD, 2010, pp. 228-232.