World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:3, No:2, 2009

Authentication and Data Hiding Using a Reversible ROI-based Watermarking Scheme for DICOM Images

Osamah M. Al-Qershi, Khoo Bee Ee

Abstract**—** In recent years image watermarking has become an important research area in data security, confidentiality and image integrity. Many watermarking techniques were proposed for medical images. However, 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. Also the medical records, electronic or not, are linked to the medical secrecy, for that reason, the records must be confidential. To fulfill those requirements, this paper presents a lossless watermarking scheme for DICOM images. The proposed a fragile scheme combines two reversible techniques based on difference expansion for patient's data hiding and protecting the region of interest (ROI) with tamper detection and recovery capability. Patient's data are embedded into ROI, while recovery data are embedded into region of non-interest (RONI). 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 with a high quality version of the original area.

Keywords**—** DICOM, reversible, ROI-based, watermarking.

I. Introduction

During the last few years, medical data management systems have been changed in the consequence of the fast and significant advancements in information and communication technologies. One of the main activities that medical data management system involves is the exchange of databases between hospitals over efficient transmission channels. The process of data exchange involves transmission of different types of data format: medical images, texts, and graphs. 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 renders that data accessible to unauthorized personnel [1]. In order to overcome the capacity problem and to reduce storage and transmission overheads, data hiding techniques are used for interleaving patient information with medical images. Those data hiding techniques can be also used for authentication and tamper detection to judge images integrity and fidelity.

Watermarking techniques can by classified into two categories, reversible and irreversible. The main idea behind reversible watermarking is to avoid irreversible distortion in original image (the host image), by developing techniques that can extract the original image exactly. Medical image watermarking is one of the most important fields that need such techniques where distortion may cause misdiagnosis [2]. 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 [3].

Although reversible schemes seem to be adequate for medical images, it must meet all the requirements of medical image watermarking: imperceptibility, integrity control, and authentication [4]. From the literature, the purposes of medical image watermarking are classified into two categories:

1- Tamper detection and authentication
2- Electronic Patient Records (EPR) data hiding.

Tamper detection watermarks are able to locate the regions or pixels of the image where tampering was done. Authentication watermarks are used to identify the source of the image. EPR data hiding techniques give more importance in hiding high payload data in the images keeping the imperceptibility very high. Depending on the purpose of the watermarking (tamper detection, authentication, or data hiding), 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 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 II, we review watermarking techniques proposed for medical images. In section III, we present our watermarking scheme, including data embedding, extracting, verifying, tamper localization and recovery. In section IV, experimental results are provided to demonstrate the efficiency of the scheme. Finally, in section V we present our conclusion.

Osamah M. Al-Qershi is a master student at School of Electrical and Electronic Engineering, University Sains Malaysia, Seri Ampanan, 14300 Nibong Tebal, Seberang perai Selatan, Penang, Malaysia; (e-mail: osamahqershi.lm07@studnet.usm.my).

Khoo Bee Ee is a senior lecturer at School of Electrical and Electronic Engineering, University Sains Malaysia, Seri Ampanan, 14300 Nibong Tebal, Seberang perai Selatan, Penang, Malaysia; (e-mail:beekhoo@eng.usm.my).

II. II Overview of Watermarking Techniques

Many watermarking schemes were proposed for medical images. Those techniques can be spatial domain techniques [5]-[9], frequency domain techniques [10]-[16], or a combination of the two domains [17],[18]. An LSB-based reversible scheme was proposed by Zain *et al.* for ultrasound images, where the original image can be recovered completely [5],[6]. In embedding process, an SHA-256 hash code is calculated for the ROI selected. After that, the hash code is embedded into the LSB of RONI. The reversibility of the scheme based on the fact that the original values of RONI pixels were zeros before embedding, At the receiver end, the watermark is extracted from LSB's of RONI and those pixels which carried the watermark are reset back to zero. 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.

Another spatial domain technique was proposed by Zain *et al.* to improve the security of medical images by involving the ability to detect tamper and subsequently recover the image [7]. The scheme requires a secret key and a public chaotic mixing algorithm combined with simple operations such parity check and compression to embed and recover a tampered image. In embedding process, the image is divided into blocks of 8x8 pixels each. For each block B, we further divide it into four sub-blocks of 4x4 pixels. The watermark, which is embedded using LSB's, in each subblock is a 3-tuple (v, p, r), where both v and p are 1-bit authentication watermark, and r is a 7-bit recovery watermark 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 divide ROI and RONI into smaller blocks [8]. Besides, the authentication bits, v & p, are embedded into subblocks of ROI, while the 7-bits recovery information are embedded into the corresponding subblocks of RONI. This will improve the image quality in ROI as the maximum change is only 2 bits in every 4 pixels.

Raul *et al.* adopted image moment theory to normalize the image in order to obtain a robust watermarking scheme against active attacks such as filtering, compression, and geometrical attacks [9]. Embedding watermark is done in regions with low homogeneity, which can be obtained by scanning the image in a spiral way using the centroid as the origin of this scan. During extracting phase, the image is scanned in the same spiral way starting from the centroid of the image. A bit of the watermark is extracted from a region by comparing the grey scale level of the center pixel with the grey scale level mean of the region.

A frequency domain technique based on discrete wavelet transform (DWT) combined with a proper quantization method was proposed by Giakoimaki *et al.* [10]. They then improved that technique gradually to increase its robustness and security [11]-[14]. 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 the purpose of 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.

A fingerprint model suitable for many-to-many multicast was proposed by Li *et al*. [15]. The model is computationally efficient and scalable in user storage and communication. The main goal of their scheme is tracing the source of an unauthorized release of medical images to enhance patient's privacy. In order to increase the robustness of their scheme, they adopted an image adaptive scheme based on wavelet (IA-W). A four level IA Wavelet scheme is used as the underlying watermarking scheme. The watermark is inserted into LH and HL band of level two and four wavelet decompositions.

For tamper detection and recovery purposes, two schemes based on Modulo 256 and DCT was proposed by Wu *et al*. [16]. At first, the image is divided into several blocks, and for each block, an adaptive robust digital watermarking method combined with the 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 region of interest (ROI) is introduced into the second scheme. The JPEG 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.

Woo *et al*. proposed a multiple digital image watermarking method which is suitable for privacy control and tamper detection in medical images [17]. The multiple watermarks consist of an annotation watermark, and a fragile watermark, which can detect general image manipulations such as image compression, noise insertion, and copy attack. In 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, & 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 least significant bit (LSB) method.

A lossless scheme was proposed by Guo *et al*. based on difference expansion introduced by Tian [18],[19]. The scheme was proposed to overcome some of disadvantages of Tian's original scheme, which are the overhead of keeping a location map, which affect the hiding capacity, and the distortion induced by embedding watermark bits.

To overcome those drawbacks, they adopted difference expansion technique to restrict the embedded-induced distortion inside a given region and controlling the embedding capacity. The region of embedding (ROE) is chosen to prevent introducing any distortion inside the ROI. Instead of

expanding the difference between two adjacent pixels, the scheme is based on expanding the difference between 4 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.

Two reversible schemes based on DE technique were proposed by Chiang et al. for tamper detection and recovery [20]. In the two schemes proposed, the image is divided into blocks of 4x4 each, and each block is transformed using 2-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 2nd scheme is a ROI-based scheme, and the pixel values of ROI is used as the watermark in order to recovery the exact ROI in case of tampering. The drawback of this technique is the limited capacity because only smooth blocks are used for embedding, so that it cannot be used for all image modalities.

III. Our Scheme

To meet medical image watermarking requirements and overcome the drawbacks of the above mentioned schemes, we propose a reversible 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, the original image is recovered exactly after watermark extraction at the receiver end. A combination of two DE techniques developed by Tian and Gou *et al*. is adopted in our scheme to gain reversibility and high capacity. In this scheme, the 1st watermark, which consists of patient's data and the hash message of ROI using MD5 is embedded into ROI using modified DE technique developed by Gue *et al*., which has high embedding capacity. This step produces an embedding map which will be used later to extract the 1st watermark. Unfortunately, this map cannot be a part of the 1st watermark and embedded back into ROI as in the original DE technique. To overcome this problem, the map is combined with recovery information to become a part of the 2nd watermark. Now, this watermark can be embedded into RONI using the original DE technique of Tian. This step also produces another embedding map, but using the original DE technique this map can be a part of the 2nd watermark and embedded into RONI as well.

A. Embedding procedure

1. ROI is selected and defined as by a polygon, and then compressed using JPEG2000 forming ROI_{comp}. This compressed version of ROI will be used for recovery in case of tamper detection.
2. ROI is divided into blocks of 16 x 16 pixels. The average of each block is calculated as AV_i. These values will be used for tamper detection.
3. The hash message for ROI, $hash_1$, is calculated using MD5 algorithm.
4. Patient's data is compressed and concatenated with $hash_1$. The resultant bit stream is coded using RS code to form the first watermark w_1.
5. ROI is divided into quads, where a quad is 4 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, *EM1*, is formed.
6. Pixels in RONI are divided into pairs, which are scanned as in the previous step to find out the expandable pairs and form another map, *EM2*. For changeable pairs, the LSB's of the pixels difference values are collected as *B*.
7. A predefined secret area in RONI is used to embed side information necessary to initiate watermark extraction. The LSB's of pixels in this area is collected to form *Orgbits*.
8. *AV, EM1*, *EM2*, and *B* are compressed using Huffman coding technique to form AV_{comp}, $EM1_{comp}$, $EM2_{comp}$ and B_{comp}.
9. ROI_{comp}, AV_{comp}, $EM1_{comp}$, $EM2_{comp}$, B_{comp}, and *Orgbits* are encoded using RS code, and then concatenated to form the 2nd watermark w_2.
10. RONI is scanned again using *EM2*, if a pair is expandable; embed a bits of w_2 using DE technique. If a pair is changeable, embed a bit of w_2 in LSB of the difference value. The scan ends when all bits of w_2 are embedded.
11. The vertexes of the polygon mentioned in step 1 are embedded in LSB's of pixels in the secret area mentioned in step 7.

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. Side information is extracted from the secret area. The side information contains the vertexes of ROI.
2. Using the vertexes, ROI and RONI are defined.
3. RONI is divided into quads, and for each quad the LSB's of embedding pixels are collected. Those bits represents the 2nd watermark w_2.
4. The 2nd watermark is decomposed into its original parts; *compROI*, AV_{comp}, $EM1_{comp}$, $EM2_{comp}$, B_{comp}, and *Orgbits,* and all parts are then decoded using RS code. AV_{comp}, EM_{com}, B_{comp} are then decompressed to obtain the original data; *AV, EM1*, *EM2*, and *B*.
5. Using *EM1*, 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 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 $hash_{1=}\ hash_2$, the image is authenticated and the algorithm proceeds to step 10. If $hash_{1\neq}\ hash_2$, the image is not authenticated, and this means that some tampering is detected. In the next step the tampered area is localized and recovered.
8. ROI is divided into blocks of 16 x 16 pixels. The average value of each block is calculated and compared to the corresponding value in *AV*. If they are not equal, the block is marked as tampered and replaced by the corresponding

block of the compressed version of ROI, ROI_{comp} as a recovery process.

9. The pairs in RONI are scanned using *EM2* and reversed to obtain the original values using DE.
10. The LSB's of the pixels in the secret area are recovered using the bits of *Orgbits*.
11. RONI is combined with ROI to form the extracted image. If there is no tampering, the exact original image can be extracted.

IV. Experimental Results

Three DICOM images, 16-bit each, of different modalities and sizes were used to test our scheme, where a patient report of size 1.8KB is embedded inside ROI. Table. I and Fig.1 show the results of embedding the watermark.

The watermarked images show good visual quality in terms of PSNR, with high embedding capacity. The reversibility of our watermarking 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 authenticated. From the results, the original image can be extracted exactly in case of no tamper.

To demonstrate tamper localization and recovery, we replaced some pixel values inside ROI with pixel values from RONI in the watermarked image. During extraction, 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 it shown in Fig.2.

Table. II shows the comparison between our scheme and other reversible and near reversible schemes mentioned in section II, which clarifies the advantages of our scheme over those schemes.

V. Conclusion

In this paper, we proposed a fragile watermarking scheme that combines two techniques; DE and modified DE. 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 RONI using the original DE technique. This means that our scheme can be used for data hiding, with up to hiding capacity up to 0.52, 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 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.

From the results that we got, and compared to other schemes, our scheme has the advantage of high capacity which makes hiding patient's data and recovery information possible. Besides, our scheme is completely lossless, while Wu(1) & Wu (2) are near lossless. Moreover, our scheme can be used

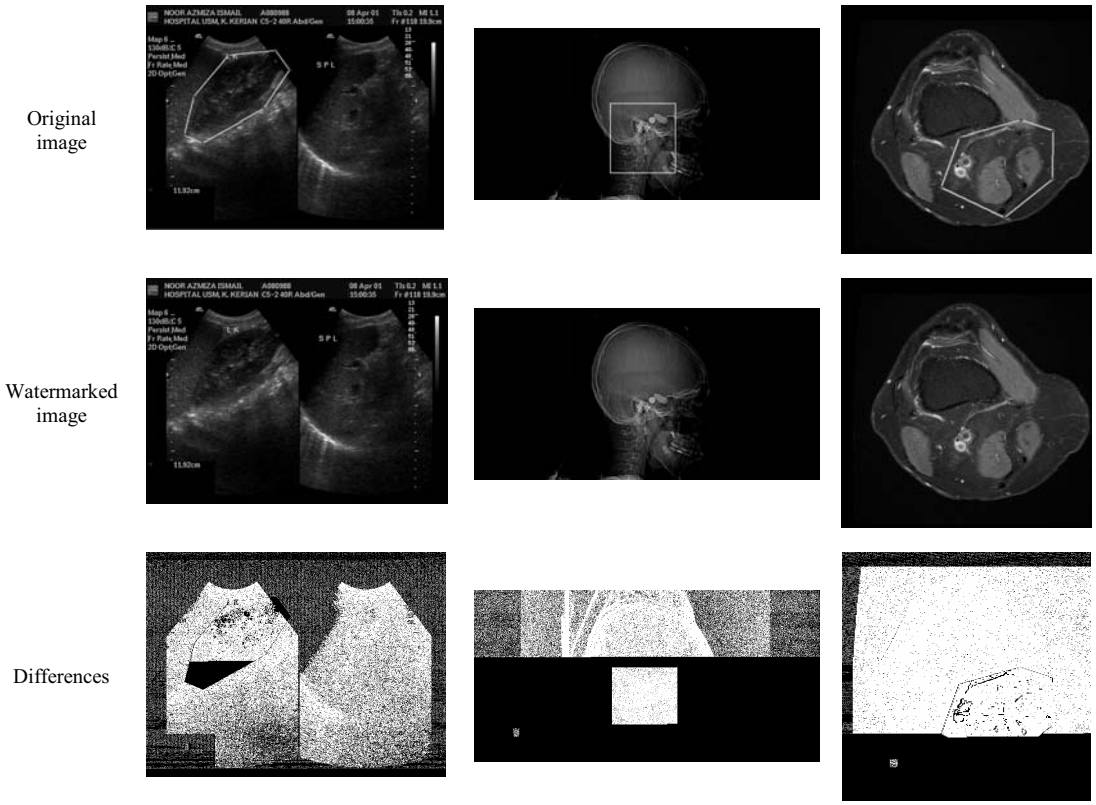

Fig. 1 Embedding patient's data in 3 images of different modalities

TABLE I
EMBEDDING RESULTS FOR 3 IMAGES OF DIFFERENT MODALITIES

Modality	Image size	Size of w1 (bits)	Size of w2 (bits)	Size of ROI (%)	Embedding Capacity (bpp)	PSNR (dB)	SSIM
US	576x768	18360	194,010	8.19	0.5101	40.9209	0.9795
CT	440x888	18360	77,586	7.00	0.5168	50.7038	0.9867
MR	512x512	18360	83,256	12.00	0.5238	41.2629	0.9558

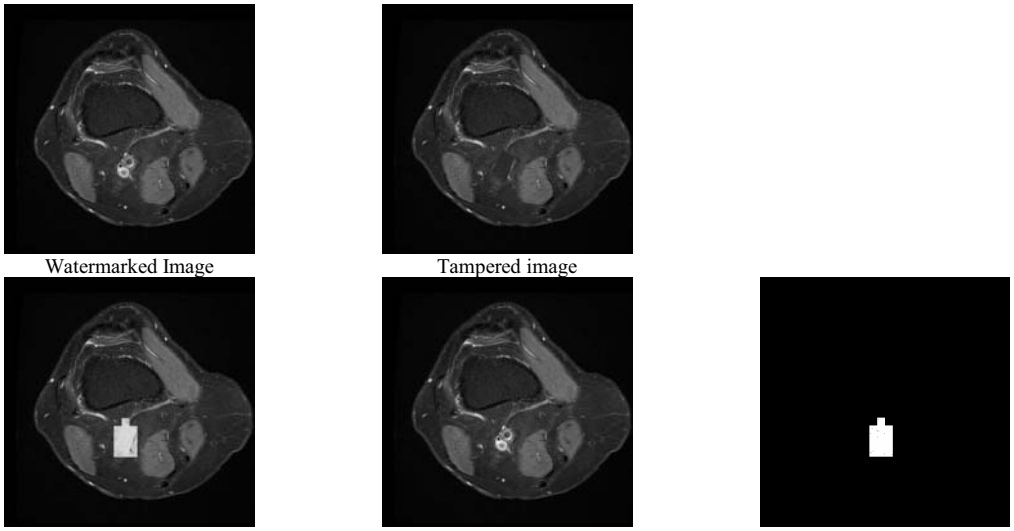

Fig. 2 Tamper localization and recovery

TABLE II
A COMPARISON BETWEEN OUR SCHEME AND OTHER REVERSIBLE SCHEMES MENTIONED IN SECTION II

Scheme	Objectives	Methodology			Capabilities		Hiding Capacity
		Embedding technique	ROI Based	Block Based	Tamper Localization	Tamper Recovery	
Zain (1,2) [5],[6]	Authentication	Spatial domain (LSB)	✓	×	×	×	No Patient's data are embedded. Only authentication data are embedded. However, It can be used for data hiding.
Gou [19]	Authentication	Modified DE	✓	4 x 4	×	×	Theoretically, 3 bits can be embedded into a block of 2x2, which means 0.75 bpp. But the actual embedding capacity depends on the threshold and ROI size. However, the authors didn't use the scheme for hiding patient's data.
Wu (1) [16]	Authentication	Frequency domain (DCT)	×	Size is not fixed	✓	Compressed form of each block	Low hiding capacity. No Patient's data can be embedded.
Wu (2) [16]			✓			✓	
Chiang (1) [20]	Authentication	Modified DE	×	4 x 4	✓	Average of blocks	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.
Chiang (2) [20]			✓			✓	
Our Scheme	Authentication and Patient's data Hiding	DE & modified DE	✓	2 x 2	✓	Compressed form of ROI	Hiding capacity in ROI is theoretically 0.75, but the overall hiding capacity is up to 0.52 bpp.

for different image modality, while Zain (1) & (2) can be used for US images, Chiang(1), Chiang(2) can be used for only images with big smooth areas.

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. Also, multiple-ROI concept can be added to make the scheme more practicable in medical informatics.

ACKNOWLEDGEMENTS

This work is supported by Ministry of Science, Technology and Innovation, Malaysia under eScienceFund grant 01-01-05-SF0114.

REFERENCES

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

[2] M. Awrangjeb, "An Overview of Reversible Data Hiding," in *The 6th International Conference on Computer and Information Technology (ICCIT-03)*, 2003, pp. 75-79

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

[4] G. Coatrieux and L. Lecornu, "A Review of Image Watermarking Applications in Healthcare," in *Proc. 28th Annual International Conference of the IEEE : Engineering in Medicine and Biology Society, EMBS '06.* , 2006, pp. 4691-4694.

[5] J. M. Zain, L. P. Baldwin, and M. Clarke, "Reversible watermarking for authentication of DICOM images," in *Proc. 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 2004, pp. 3237 - 3240.

[6] 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.

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

[8] 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.

[9] R.-C. Raúl, F.-U. Claudia, and T.-B. Gershom de J., "Data Hiding Scheme for Medical Images," in *Proc. 17th International Conference on Electronics, Communications and Computers CONIELECOMP '07* 2007, pp. 32-37.

[10] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "A medical image watermarking scheme based on wavelet transform," in *Proc. 25" Annual Intemational Conference of the IEEE Engineering in Medicine and Biology Society*, 2003, pp. 856 – 859

[11] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "A Multiple Watermarking Scheme Applied to Medical Image Management," in *Proc. 26th Annual International Conference of the IEEE EMBS*, 2004, pp. 3241- 3244.

[12] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "Multiple Digital Watermarking Applied to Medical Imaging," in *Proc. 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference*, 2005, pp. 3444 - 3447.

[13] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "Secure and efficient health data management through multiple watermarking on medical images" *Medical and Biological Engineering and Computing,* vol. 44, pp. 619-631, 2006.

[14] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "Multiple Image Watermarking Applied to Health Information Management," *IEEE Transactions on Information Technology in Biomedicine,* vol. 10, pp. 722- 732, 2006.

[15] M. Li, R. Poovendran, and S. Narayanan, "Protecting patient privacy against unauthorized release of medical images in a group communication environment," *Computerized Medical Imaging and Graphics,* vol. 29, pp. 367-383, 2005.

[16] 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,* vol. 21, pp. 59-76, 2008.

[17] C.-S. Woo, J. Du, and B. Pham, "Multiple Watermark Method for Privacy Control and Tamper Detection in Medical Images," in *Proc. APRS Workshop on Digital Image Computing Pattern Recognition and Imaging for Medical Applications*, 2005, pp. 43-48.

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

[19] 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.

[20] 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,* vol. 21, pp. 77-90, 2008.