A REVIEW OF REVERSIBLE WATERMARKING PROPERTIES, APPLICATIONS AND TECHNIQUES FOR MEDICAL IMAGES

Nuha Omran Abokhdair, Azizah Bt Abdul Manaf

Universiti Teknologi Malaysia.
54100 Kuala Lumpur, Malaysia
Abo_khdeir@yahoo.com, azizah07@citycampus.utm.my

Abstract

Medical image watermarking is a special branch of image watermarking. The main use of medical image watermarking is for authentication and tamper detection. In addition, it is used to insert the related electronic patient record (EPR) into the medical image. The objective of this paper is to conduct a research of medical image properties and applications. In addition, some of medical image watermarking schemes are reviewed. These schemes are reversible, i.e. the exact copy of the original image can be recovered.

Keywords - Data hiding, ROI-based watermarking, DICOM, EPR, Difference Expansion.

1 INTRODUCTION

Nowadays, the distribution and communication of medical information among health care providers and telemedicine systems are becoming increasingly crucial. One of the most significant types of medical information is medical images, where the transmission of medical images over wire and wireless networks is a daily routine in medical life [1]. On the other hand, the distribution of medical images over unsecured network channels, such as internet, produces potential risk of information disclosure to an unauthorized entity, where it is intentional or not intentional. A manipulation of the context of the medical image is a possible consequence of this, which may cause misdiagnosis [1][2].

In order to protect medical images from any unauthorized access, Medical image watermarking is used. The main use of medical image watermarking is for authentication and tamper detection in order to identify the source of the image and to detect and localize any manipulation of the image. In addition, it is used to insert the related electronic patient record (EPR) into the medical image in order to avoid detachment of EPR from its corresponding image [3].

In medical images, even a minor distortion of the image caused by watermarking is prohibited, because this may affect the diagnosis negatively. To overcome this problem, reversible watermarking is used. The main feature of reversible watermarking is that an exact copy of the original image can be recovered, if the watermarked image is considered authentic [4].

In this paper, the following sections are organized as follows; the properties and the applications of medical image watermarking are introduced in section II and section III, respectively. In section IV, an overview of the previous reversible watermarking techniques for medical images is given.

2 PROPERTIES OF MEDICAL IMAGE WATERMARKING

In general image watermarking, three main characteristics need to be kept reasonably very high, Transparency, Capacity and Robustness [5]. In medical image watermarking, additional characteristics are required including reversibility, authenticity and complexity.

2.1 Perceptual Transparency

The digital watermark should be embedded in the medical image so that it is not noticeable to human perception for confidentiality and secrecy. Although embedding a watermark in the image introduce some noise to the cover image, it is important to minimize its impact on the visual quality of the image [6].

2.2 Embedding Capacity

Embedding capacity or payload refers to the size of the watermark that can be inserted into the host image [1]. In Medical Image Watermarking, a high embedding capacity is required to provide enough space to insert the EPR, authentication and tamper detection information.

2.3 Robustness

Robustness of the watermark is its ability to remain intact if the watermarked image undergoes processing such as scaling and rotation, cropping, filtering, and lossy compression. The watermark should be difficult to destroy without degrading the visual quality of the cover image so as to render it unusable [2][6].

2.4 Reversibility

Reversibility refers to the ability to recover the original cover image perfectly after the marked image passes the authentication process. In Medical Image Watermarking, even a small manipulation of the medical image may lead to wrong diagnosis. Thus, it is essential to recover the original medical image after extracting the watermark from the image [2][6].

2.5 Authenticity

This means only authentic users are able to access the embedded data. Authentic users may include patients, Hospital Information System (HIS) personnel, clinicians and radiologists. To achieve this property, secret keys are used [5].

2.6 Complexity

Computational complexity is the number of operations required to embed and extract the watermark. To save the execution time the watermarking algorithm should be less complex. For telediagnosis, the speed becomes a vital issue if the situation is demands [5].

3 MEDICAL IMAGE WATERMARKING APPLICATIONS

According to the properties of medical image watermarking, one can discover that medical image watermarking techniques are developed based on the applications. Among others, the following applications of medical image watermarking are more common:

3.1 Patient's private information protection

Electronic Patient Record includes the private information of the patient that should be kept confidential and secure. Medical image watermarking is able to ensure the confidentiality of the private patient information by hiding it inside the medical image imperceptibility [3].

3.2 Authentication and tamper detection

In medical image area, it is essential to maintain the integrity and authenticity of the image because any kind of changes to the original image could lead doctors to make erroneous decisions and serve harmful consequences [4]. Authentication watermarking is able to assure that the medical image has not been tampered with by a hostile entity [5]. In order to maintain the integrity of the image, a watermark serves as a signature can be embedded into the image. Thus, if the image is manipulated, it can be easily detected as the pixel value of the embedded data will be changed [7].

3.3 Teleradiology and teleconference

Teleradiology is a technology used to transmit medical information and images into a remote location for diagnosis, consultation, treatment, or academic research by using a communication network such as LAN, WLAN or internet [8]. Therefore, in order secure the connection; watermarking is adopted to insert EPR and authentication code into the medical image, which ensures the confidentiality of the

EPR and the authenticity of the image. It is also save the memory and the bandwidth and can detect any tampering of data [5].

This technique can also be used for teleconference where a team of geographically dispersed radiologists and specialist can discuss and diagnose a medical image in hands.

4 REVERSIBLE MEDICAL IMAGE WATERMARKING TECHNIQUES

Medical image watermarking algorithms can be classified into two categories, reversible watermarking and irreversible watermarking. The watermarking techniques that are acceptable for diagnostic analysis are mainly based on reversible watermarking. Therefore, in this paper the focus will be on reversible watermarking. Based on the purpose of the watermarking, watermarking schemes of medical images can be categorized into:

4.1 Data hiding schemes

In [9], Lou et al. proposed a multiple-layer data hiding technique for medical image using a reduced difference expansion method to embed the bitstream in the least significant bits (LSBs) of the expanded differences. The proposed technique reduces the value of the expansion difference so that the value of the transformed expansion difference can be close to the original. The pixel pair will not be processed when overflow and underflow problem is encountered. The original image can be restored after extracting the hidden data from the marked image. The experimental results show that the proposed method effectively improves Tian's method [10] in embedding capacity and visual quality and large amount of data can be embedded in a medical image while quality can also be maintained.

Al-Qershi and Khoo proposed two reversible schemes based on DE for data hiding in medical images [11]. The first scheme combined Tian's technique with Chiang's scheme [10][12], and the second scheme combined Tian's technique with Alattar's scheme [13]. To embed the data in the image, the image is divided into blocks of 4×4 pixels each and classified into smooth and non-smooth blocks. The payload is embedded using Tian's scheme into the non-smooth blocks. The embedding map is compressed and embedded into smooth blocks using Chiang's scheme. For the second proposed scheme, Alattar's scheme is used to embed the compressed embedding map. The experimental results obtained show that the two proposed schemes are image dependent. The 2nd proposed scheme is better in terms of hiding capacity, while the 1st proposed scheme has better visual quality. However, the two proposed schemes are not suitable for X-ray images because of the lack of smooth areas.

4.2 Authentication and tamper detection schemes

Guo and Zhuang, in [14], presented a lossless watermarking scheme to verify the integrity and authenticity of medical images. In addition, the scheme has the capability of not introducing any embedding distortion in the region of interest (ROI) of a medical image. Difference expansion method is applied for embedding process. The image is divided into quads, where the quad is a vector u= (u0, u1, u2, u3) formed from non-overlap 2x2 adjacent pixel values. Then, a region of embedding, which is represented by a polygon, is chosen intentionally to prevent introducing embedding distortion in the ROI. For each quad u, 3 bit of information is embedded using difference expansion. Experimental results show that this scheme achieves high embedding capacity with low level of distortion. Moreover, Patient's fingerprint information is embedded into several image slices for enhancing authenticity. However, this scheme is not used to embed temper detection and recovery information, which needs higher embedding capacity.

Tan et al. introduced a dual layer reversible watermarking for hiding patient information and tamper detection information, and to ensure authenticity and integrity of the image in [15]. In this technique, the image is divided into 2x2 non-overlapping blocks. One of the pixels of each block is chosen randomly as an estimator. Each one of the other three pixels can carry one bit of the watermark, if the difference between them and the estimator is less than 2, by adding or subscribing the pixel by 2 based on the watermark value (0 or 1). To keep the estimator location secure, it is encrypted using RSA and watermarked into fixed location in the image. In the first layer, patient information, authentication information and the estimators' locations are embedded. Tamper localization information is embedded in layer 2. To detect tampering locations, the image is divided into 16×16

non-overlapping pixel blocks and CRC-16 is computed for each block and embedded into its own block. To avoid under and overflow, this scheme shifts pixel values of images by four gray levels values because many modalities produce images that do not utilize the full 16-bit range of pixel values. Theoretically, hiding capacity is 0.75 bpp, however the capacity depends on the pixels that have high correlation. Although this scheme is able to locate tampered area in the image, it cannot recover those locations.

In [3], Al-Qershi proposed a reversible ROI based fragile technique to hide patient data, authenticate ROI, and to detect and recover tampered region in DICOM image. ROI is used as a host to embed the patient information and authentication information in it using modified DE (Difference Expansion) proposed by Guo [14]. On the other hand, the watermarking map of the information embedded in the ROI and the compressed version of ROI for tamper recovery are inserted into the RONI of the image using the original DE produced by Tian [10]. However, this scheme can only authenticate ROI.

Another hybrid watermarking scheme was proposed by Al-Qershi, in [16], for authenticating DICOM images and hiding the patient data in it. In embedding process, the image is divided into ROI and RONI and then it is divided into blocks of 16x16 pixels. Patient's data and the hash of ROI are embedded into ROI using modified DE technique, developed by Guo [14], and to extract this watermark, the watermarking map is combined with recovery information and embedded into RONI using three-level DWT technique developed by Kundur [17]. The experimental results show that the scheme has some robustness against certain levels of salt and pepper and cropping noise. To recover the tampered area in the image, the size of the image must be at least 512×512 pixels. In addition, this scheme fulfils reversibility and authenticity requirement for ROI only.

Table 1 shows a comparison of the reviewed schemes of reversible medical image watermarking.

Table 1. A comparison of medical image watermarking techniques

Algorithm	Embedding technique	ROI-Based	EPR Hiding	Data Hiding/ Authentication	Tamper Localization	Tamper Recovery	Reversible	Performance
Lou *et al.* [9]	Reduced DE	X	x	Data Hiding	x	X	✓	The PSNR value becomes very low at high embedding capacity
Al-Qershi and Khoo [11]	DE DE	X	x	Data Hiding	x	x	✓	1st scheme better in visual quality. 2nd scheme is better in capacity. Capacity (0.5-0.7bpp). PSNR up to 37dB
Guo and Zhuang [14]	Quad of DE	✓	✓	Authentication	x	x	✓	The capacity is limited, because the data embedded only on ROE
Tan et al. [15]	Random location estimator signal	X	✓	Authentication	✓	x	✓	Capacity=74,190 to 581,524 bits PSNR = 34-35dB
Al-Qershi and Khoo [3]	modified DE + DE	✓	✓	Data Hiding & Authentication	✓	✓	✓	hiding capacity up to 0.52 only ROI is authentic
Al-Qershi and Khoo [16]	modified DE + DE	✓	✓	Data Hiding & Authentication	✓	✓	Only ROI	hiding capacity= 0.46– 0.50 bpp robust against certain levels of

	salt and pepper and cropping noise

5 CONCLUSION

Many medical image watermarking schemes were proposed in the last few years, but few of them were considering the reversibility requirement. In this paper, some of the recent reversible watermarking techniques for medical images are reviewed. The capacity of those techniques need to be increased in order to be able to conceal EPR, authentication information, and tamper detection and recovery information of bigger size of ROI. Additionally, a good trade-off between image quality and capacity would be critical in satisfying the variety of applications in healthcare community.

References

[1] W. Puech, "Image Encryption and Compression for Medical Image Security " presented at the Image Processing Theory, Tools and Applications, Sousse 2008.

[2] L. Eugene Y.S, "11 - Data Security and Protection for Medical Images," in *Biomedical Information Technology*, F. David Dagan, Ed., ed Burlington: Academic Press, 2008, pp. 249-257.

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

[4] M. K. Kundu and S. Das, "Lossless ROI Medical Image Watermarking Technique with Enhanced Security and High Payload Embedding," presented at the Proceedings of the 2010 20th International Conference on Pattern Recognition, 2010.

[5] K. A. Navas and M. Sasikumar, "Survey of Medical Image Watermarking Algorithms," presented at the 4th International conference: Sciences of Electronic, Technologies of Information and Telecommunications, Tunisia, 2007.

[6] F. I. Kallel, B. M. Salim and L. JC, "Improved Tian's Method for Medical Image Reversible Watermarking," *GVIP Journal,* vol. 7, pp. 1-5, 2007.

[7] A. M. Zeki, "Watermarking techniques using intermediate significant bit," Doctor of Philosophy (Computer Science), Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia, 2009.

[8] Suapang, P. Dejhan, K. Yimmun and Surapun, "Medical Image Archiving, Processing, Analysis and Communication System for Teleradiology," presented at the TENCON 2010 - 2010 IEEE Region 10 Conference Fukuoka 2010.

[9] D.-C. Lou, M.-C. Hu and J.-L. Liu, "Multiple layer data hiding scheme for medical images," *Comput. Stand. Interfaces,* vol. 31, pp. 329-335, 2009.

[10] J. Tian, "Reversible data embedding using a difference expansion," Circuits and Systems for Video *Technology, IEEE Transactions on,* vol. 13, pp. 890-896, 2003.

[11] O. M. Al-Qershi and B. E. Khoo, "High capacity data hiding schemes for medical images based on difference expansion," *J. Syst. Softw.,* vol. 84, pp. 105-112, 2011.

[12] 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.

[13] A. M. Alattar, "Reversible watermark using difference expansion of quads," in *Acoustics,. Proceedings. (ICASSP '04). IEEE International Conference on*, 2004, pp. iii-377-80 vol.3.

[14] X. Guo and T.-g. Zhuang, "A Region-Based Lossless Watermarking Scheme for Enhancing Security of Medical Data," *Journal of Digital Imaging,* vol. 22, pp. 53-64, 2009.

[15] C. Tan*, et al.*, "Security Protection of DICOM Medical Images Using Dual-Layer Reversible Watermarking with Tamper Detection Capability," *Journal of Digital Imaging,* vol. 24, pp. 528-540, 2011.

[16] O. Al-Qershi and B. Khoo, "Authentication and Data Hiding Using a Hybrid ROI-Based Watermarking Scheme for DICOM Images," *Journal of Digital Imaging,* vol. 24, pp. 114-125, 2011.

[17] D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," *Proceedings of the IEEE,* vol. 87, pp. 1167-1180, 1999.