Multiple Watermark Method for Privacy Control and Tamper Detection in Medical Images

Chaw-Seng Woo[1], Jiang Du[1], and Binh Pham[2]
[1]Information Security Institute
[2]Faculty of Information Technology
Queensland University of Technology
GPO Box 2434, Brisbane, QLD4001, AUSTRALIA
cs.woo@student.qut.edu.au, {j2.du, b.pham}@qut.edu.au

Abstract

Medical images in digital form must be stored in a secure way to preserve stringent image quality standards and prevent unauthorised disclosure of patient data. This paper proposes a multiple watermarking method to serve these purposes. A multiple watermark consists of an annotation part and a fragile part. Encrypted patient data can be embedded in an annotation watermark, and tampering can be detected using a fragile watermark. The embedded patient data not only save storage space, it also offers privacy and security. We also evaluate the images' visual quality after watermark embedding and the effectiveness of locating tampered regions.

1. Introduction

As we move into the digital era, patient records in hospital environments can be stored in electronic media. This is made possible with more mature and reliable technologies in information and communication technology (ICT). Confidentiality, integrity, and authenticity are the mandatory security requirements of medical information. Medical images in digital form must be stored in a secured environment to preserve patient privacy. It is also important to prevent unintentional distortion and malicious modifications on the image's perceptual quality. To achieve these objectives, digital watermarking techniques can be employed.

Although medical imaging is a matured field, the application of watermarking technologies in medical images is rather new. Furthermore, hybrid systems that combine fragile and robust watermarks had been explored by a relatively small group of researchers for medical images. To date, little research works have been published on such hybrid systems for medical images, and there is room for improvement. The main reason behind such scenario could be due to the stringent quality requirements of medical images. For example, the Health Insurance Portability and Accountability Act 1996 (HIPAA) in the United States sets out healthcare data security guidelines [1]. Typically, watermarks embedded in medical images must not cause any visual artefacts that may affect the interpretation by medical doctors. Also, patient information embedded must be detected and recovered in an accurate manner.

Multiple watermarks that consist of an annotation part and a fragile part can be used to serve multiple purposes. For example, the annotation part can store patient information in a secure and private way, and the fragile part can detect tampering. Furthermore, the embedding information helps to reduce storage space of digital contents [2]. For instance, the annotation watermark eliminates the need to store plain text of patient information on addition files.

This paper proposes a multiple digital image watermarking method which is suitable for privacy control and tamper detection in medical images. The annotation watermark can be detected in a blind manner, i.e. the original un-watermark image is not required to detect the annotated watermark. In addition, the fragile watermark can detect general image manipulations such as image compression, noise insertion, and copy attack [3].

Storage space reduction provided by the robust watermark is measured in bits. The effectiveness of locating tampered regions using the fragile watermark is investigated. Images quality after watermark embedding is measured in weighted peak-signal-to-noise-ratio (WPSNR). The proposed watermarking scheme would be suitable for use in a hospital environment.

2. Multiple watermarking approach

Robust digital image watermarks are suitable for copyright protection because they remain intact with the protected content under various manipulative attacks. The annotation watermark can take the robust form in order to preserve data integrity. Annotation information can be patient name, hospital name, date and time of imaging process, and image dimension. On the other hand, the fragile watermarks are good for tamper detection.

Wakatani [4] proposed a watermarking method that avoids embedding watermark in the region of interest (ROI). Although it preserves the image quality in that region, the major drawback is the ease of introducing copy attack on the non-watermarked regions. In contrast to that method, we propose to embed a fragile watermark that covers the entire central region of an image. This way, tampering in small regions can be located easily.

Giakuomaki et al. [5] proposed a wavelet-based watermarking scheme to embed multiple watermarks in medical images. Although the scheme offers medical confidentiality and record integrity, the visual quality of watermarked images can be improved to achieve higher PSNR values.

Another approach is to create a virtual border by inserting extra line of pixels around image borders in order to embed watermarks within it [6]. This approach increases file size and storage space. Such approach is in contrast to space saving objective of watermarking. In addition, the absent of a fragile watermark makes it vulnerable to tampering.

We propose a multiple watermark system as shown in Figure 1 below. The annotation watermark and the fragile watermark are embedded separately into different regions of the image.

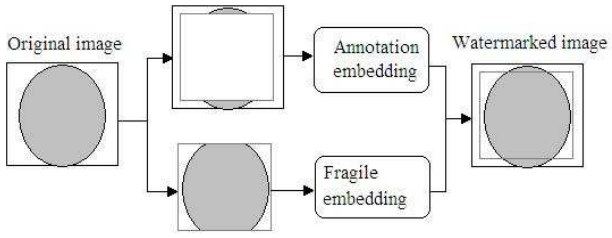

Figure 1. Multiple watermark embedding.

2.1 Annotation watermark for privacy control

To provide data security and patient privacy, patient information can be encrypted and embedded into an annotation watermark. In addition, the identity of the medical practitioner involved in the imaging process can be digitally signed using a digital signature which is then embedded into the annotation watermark for authentication.

The annotation watermark is embedded into the border pixels of the image using a robust embedding method proposed in [7]. A watermark message is arranged in a frame pattern as illustrated in Figure 2. Then, it is embedded using a linear additive method into the three high pass bands of discrete wavelet transform (DWT) of the original image borders. This is carried out at the first level of the DWT sub-bands. An inverse DWT is performed on the marked coefficients to obtain the marked image border. This is depicted in Figure 3. Although the illustrations use fixed size borders for a square image, the proposed method can be easily adapted to rectangular images of any sizes.

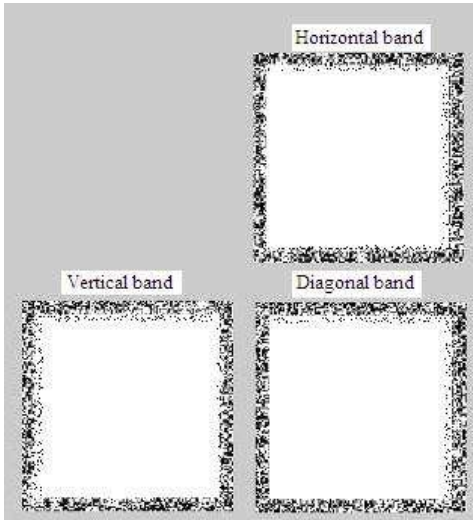

Figure 2. Annotation watermark arranged in frame pattern.

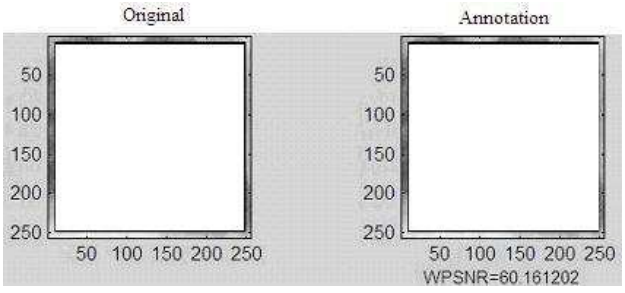

Figure 3. Image borders used in annotation watermark embedding.

2.2 Fragile watermark for tamper detection

The integrity of the medical image can be authenticated using a fragile watermark. Tampering on the image can be detected by examining the tiled fragile watermark patterns.

The fragile watermark is embedded into the central region of the original image using the least significant bit (LSB) method. Note that we took the image borders for annotation watermark embedding. A binary watermark pattern is tiled to cover the whole image, and its binary pixel values are used to overwrite the corresponding LSBs of the cover image pixels. Figure 4 gives an example of the process using X ray image of the chest.

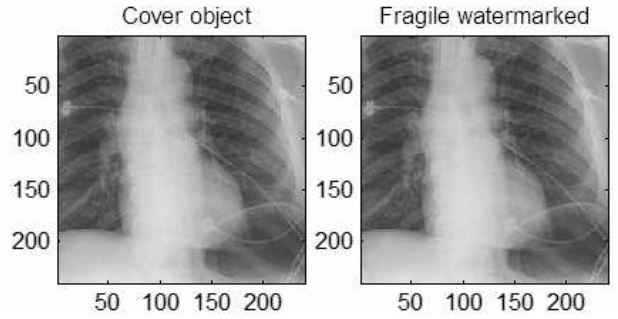

Figure 4. Fragile watermark embedded into central region of an X ray chest image.

After the annotation watermark and fragile watermark are embedded, the two parts are combined to form a complete multiple-watermarked image. See Figure 5.

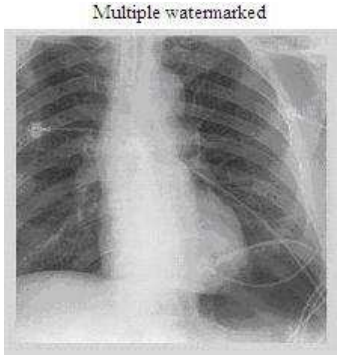

Figure 5. Multiple-watermarked image.

2.3 Watermark detection

For watermark detection, the annotation watermark and the fragile watermark are detected separately, similar to their embedding steps. The detection of annotation watermark takes a few steps similar to its embedding process. Firstly, the border of the watermarked image is decomposed into its DWT sub-bands. Then, the correlation value is calculated using the three high pass band coefficients. Finally, the calculated value is compared with a dynamically computed threshold value to determine successful watermark detection [7]. The fragile watermark is detected using a simple LSB detection method. The LSBs of each pixel in the watermarked image is read to form the tiled binary watermark pattern. Figure 6 shows the correctly tiled fragile watermark detected in the central region of the image, and the annotation watermark patterns around the image borders.

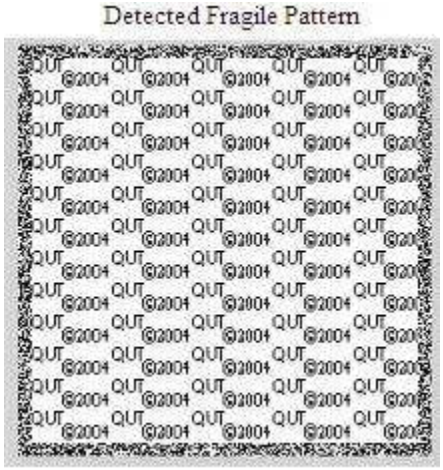

Figure 6. Fragile and annotation watermark patterns detected without attacks.

3. Analysis of experimental results

Three types of medical images that represent soft tissues and hard tissues characteristics were used in the experiment, i.e. X ray image of the chest, MR image of the skull, and CT image of the brain. See Figure 7.

3.1 Visual quality of watermarked images

The visual quality of watermarked image is measured in weighted PSNR (WPSNR) because it is generally more accurate than PSNR [8]. A test on X ray chest image provided very good imperceptibility of 60.78dB, well above the 50dB benchmark. The annotation part and fragile part were detected correctly.

CT brain image gives WPSNR of 60.80dB, and the MR of the skull gives WPSNR 60.70dB. Figure 7 provides a visual quality comparison between the original and the watermarked images.

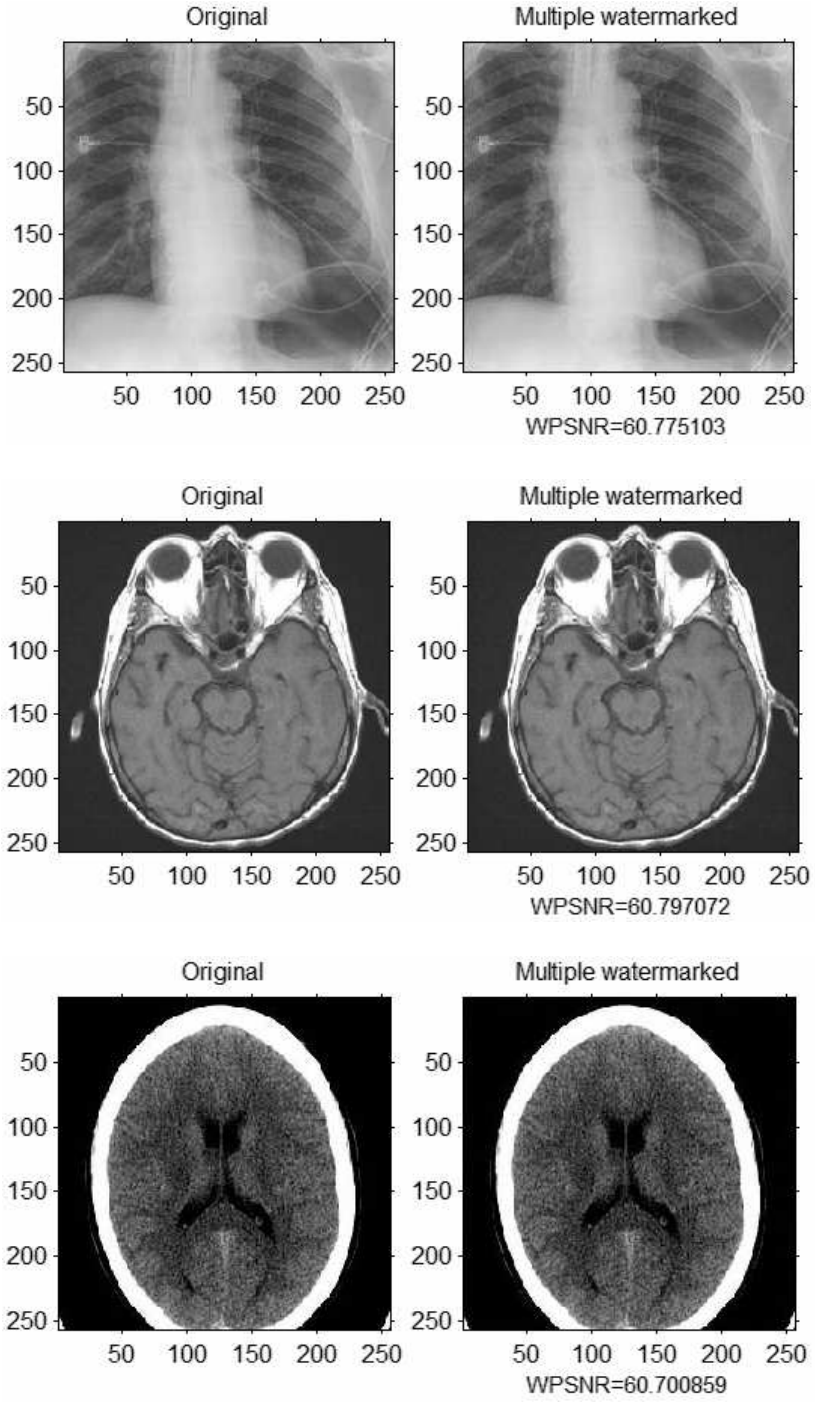

Figure 7. The test image and its multiple watermarked image with its respective WPSNR: from top to bottom are X ray image of the chest, MR image of the skull, and CT image of the brain.

3.2 Tamper detection using the fragile watermark

Some of the general image manipulations were performed as attacks to evaluate the effectiveness of the fragile watermark. These attacks are easy to perform using off-the-shelf image processing software, and they pose a significant threat to the integrity of medical images. The effects of these attacks are hard to be identified by human eyes. Fortunately, it can be detected using the fragile watermark. The attacks are tabulated in Table 1.

Table 1. General attacks on fragile watermark

No.	Attack	Descriptions
1	Noise insertion	Gaussian noise with zero mean and variance 0.0002.
2	JPEG compression	Quality factor 90%.
3	Copy attack	Copy a region and paste it on another region with similar texture.

Gaussian noise with zero mean and variance 0.0002 was inserted into the watermarked image to evaluate the effectiveness of the fragile watermark in tamper detection. Figure 8 illustrates the test results.

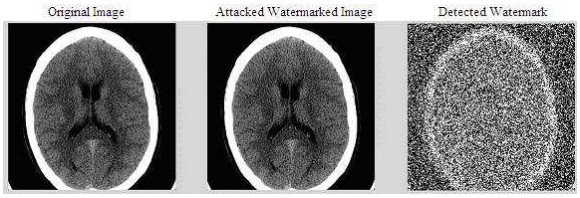

Figure 8. Left: Original CT brain image; Middle: Gaussian noise with zero mean and variance 0.0002 inserted into the watermarked image; Right: Fragile watermark tile pattern destroyed by the Gaussian noise.

A test on JPEG compression with quality factor 90% on the CT brain image is shown in Figure 9. The JPEG compressed watermarked image looks very similar to the original image. However, the fragile watermark tile pattern is destroyed by the JPEG compression. This alerts us that the image is not authentic.

Figure 9. Left: Original CT brain image; Middle: JPEG compression on the watermarked image with quality factor 90%; Right: Fragile watermark tile pattern destroyed by the JPEG compression attack.

Figure 10 shows an example of copy attack detected by the fragile watermark. Although it is hard for human eyes to identify the tampered regions, the proposed method makes it possible to do so by highlighting the distorted tiled patterns.

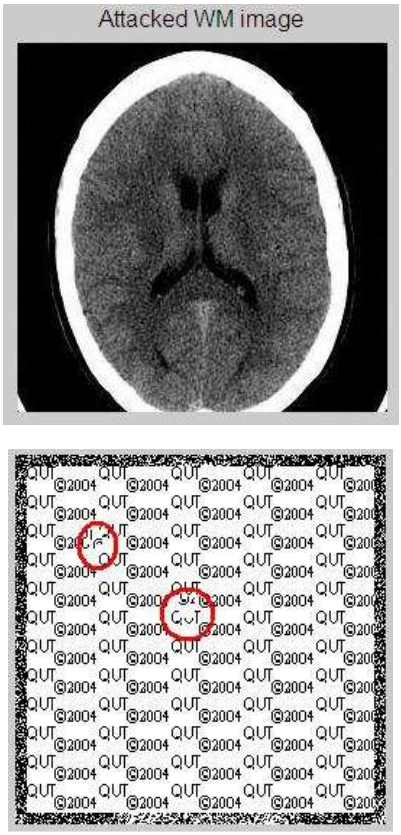

Figure 10. Top: Copy attack on a watermarked image. Bottom: Two tampered regions are detected by the fragile watermark (the circled regions).

4. Conclusions and future work

The multiple-watermarking method presented has shown to be suitable for use in medical images. The annotation watermark can be used to embed patient information in a private and secure manner, while the fragile watermark offers tamper detection. The visual quality of watermarked image is very good. The effectiveness of the fragile part in tamper detection has been proven under some general image manipulation attacks. The annotation watermark is meant to store context information in a private manner without increasing storage space requirement. Nevertheless it is possible to destroy it on purpose using malicious attack techniques. To overcome such weakness, the annotation watermark should be embedded in textured regions of the image instead of in the image borders. In addition, a hash-block-chaining watermarking approach [9] can be adopted in the fragile watermarking part to improve its security. These issues will be investigated in our ongoing work.

Acknowledgements

This work is supported by the Strategic Collaborative Grant on Digital Rights Management (DRM) awarded by Queensland University of Technology (QUT), Australia. The authors would like to thank the e-Health Research Centre for assistance with acquiring test images.

References

[1] Health Insurance Portability and Accountability Act 1996 (HIPAA). Online at http://aspe.os.dhhs.gov/admnsimp/pl104191.htm Last accessed: 27 January 2005.

[2] Rajendra Acharya, U., Acharya, D., Subbanna Bhat, P., Niranjan, U.C., "Compact storage of medical images with patient information", *IEEE Transactions on Information Technology in Biomedicine*, Vol. 5, Issue 4, pp. 320–323, December 2001.

[3] Cox, I.J., M.L. Miller, and J.A. Bloom, *Digital Watermarking*. 2002: Morgan Kaufmann.

[4] Wakatani, A., "Digital watermarking for ROI medical images by using compressed signature image", *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS) 2002*, 7-10 Jan. 2002, pp. 2043–2048, 2002.

[5] Giakoumaki, A., Pavlopoulos, S., Koutouris, D., "A medical image watermarking scheme based on wavelet transform", *Proceedings of the 25th Annual International Conference of the Engineering in Medicine and Biology Society IEEE*, 17-21 Sept. 2003, Vol.1, pp.856–859, 2003.

[6] Trichili, H., Boublel, M., Derbel, N., Kamoun, L., " A new medical image watermarking scheme for a better telediagnosis", *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics 2002*, 6-9 Oct. 2002, Vol.1, pp. 556–559, 2002.

[7] Chaw-Seng Woo, Jiang Du, Binh Pham, "Performance Factors Analysis of a Wavelet-based Watermarking Method", *Proceedings of the Australasian Information Security Workshop (AISW 2005)*, Vol. 44, pp.89– 97, 31 January - 4 February 2005, Newcastle, Australia.

[8] Voloshynovskiy, S., Pereira, S., Iquise, V. and Pun, T., "Attack modelling: Towards a second generation watermarking benchmark", *Signal Processing - Special Issue on Information Theoretic Issues in Digital Watermarking*, 2001, pp. 1177– 1214.

[9] F. Deguillaume, S. Voloshynovskiy, T. Pun, "Secure hybrid robust watermarking resistant against tampering and copy attack", *Signal Processing*, Elsevier, Vol. 83, 2003, pp. 2133–2170.

[10] Coatrieux, G., Maitre, H., Sankur, B., Rolland, Y., Collorec, R., "Relevance of watermarking in medical imaging", Proceedings of IEEE EMBS International Conference on Information Technology Applications in Biomedicine 2000, pp. 250–255, 9-10 Nov. 2000.

[11] Xuan Kong, Rui Feng, "Watermarking medical signals for telemedicine", *IEEE Transactions on Information Technology in Biomedicine*, Vol. 5, Issue 3, pp. 195–201, September 2001.

[12] F. Cao et. al., "Medical image security in a HIPAA mandated PACS environment", Computerized Medical Imaging and Graphics, Elsevier Science, Vol. 27, pp. 185–196, 2003.