IGI PUBLISHING ITJ 5310
701 E. Chocolate Avenue, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, International Journal of Digital Crime and Forensics, Volume 1, Issue 4
edited by **Chang-Tsun Li © 2009, IGI Global**

Medical Images Authentication through Repetitive Index Modulation Based Watermarking

Chang-Tsun Li, University of Warwick, UK

Yue Li, University of Warwick, UK

ABSTRACT

In this work we propose a Repetitive Index Modulation (RIM) based digital watermarking scheme for authentication and integrity verification of medical images. Exploiting the fact that many types of medical images have significant background areas and medically meaningful Regions Of Interest (ROI), which represent the actual contents of the images, the scheme uses the contents of the ROI to create a content-dependent watermark and embeds the watermark in the background areas. Therefore when any pixel of the ROI is attacked, the watermark embedded in the background areas will be different from the watermark calculated according to the attacked contents, thus raising alarm that the image in question is inauthentic. Because the creation of the watermark is content-dependent and the watermark is only embedded in the background areas, the proposed scheme can actually protect the content/ROI without distorting it.

Keywords: *Medical Image Authentication, Digital Watermarking, Data Hiding, Digital Forensics, Integrity Verification*

INTRODUCTION

Due to privacy concerns and authentication needs, many digital watermarking schemes (Bao et al, 2005; Coatrieux et al, 2001; Guo & Zhuang, 2007; Kong & Feng, 2001; Osborne et al, 2004; Planitz & Maeder; 2005; Zhou et al, 2001) have been proposed to embed authentication data into the contents of medical images. Methods proposed in the literature can be broadly classified into two categories: *spatial domain watermarking* (Bao et al, 2005; Coatrieux et al, 2001; Kong & Feng, 2001) and *transform domain watermarking* (Wakatani, 2002; Lie et al, 2003; Osborne et al, 2004). Most transform domain *watermarking* methods are designed to work with lossy compression standards, such as JPEG and JPEG 2000. The main concern surrounding this type of watermarking schemes is that in most cases lossy compression is not allowed to be applied to medical images, thus restricting their applicability. On the other hand, most spatial domain embedding methods are developed for the applications in which no lossy compression is expected. Many spatial domain embedding methods (Bao et al, 2005; Coatrieux

DOI: 10.4018/jdcf.2009062403

et al, 2001; Kong & Feng, 2001) require that the least significant bits (LSBs) of the image pixels be replaced with the authentication codes or watermarks. Although the distortion due to this kind of "destructive" watermark embedding is usually visually insignificant, medical images with watermarks embedded with this type of irreversible watermarking schemes may not be acceptable as feasible evidence in the court of law, should medical disputes occur. Many reversible data hiding schemes (Li, 2005; Thodi & Rodriguez, 2007), although not specifically proposed for the purpose of medical image authentication, have been developed to facilitate reversible data hiding, in which the original images can be recovered after the hidden data is extracted from the watermarked images. A reversible watermarking scheme specifically developed for authenticating medical data has been proposed in (Kong & Feng, 2001). The common problem with these reversible data hiding schemes is that, apart from the actual payload (i.e., the watermark, secret data, authentication codes, etc), side information for reconstructing the exact original image has to be embedded as well. The side information wastes limited embedding capacity and is usually the compressed form of the location map of the original data that is expected to be affected by the embedding process. The waste of embedding capacity reduces the authentication power of the scheme and the resolution of tamper localization, as explained in (Li & Yuan, 2006). Moreover, authentication schemes are also expected to be resistant against attacks, such as the Holliman-Memon counterfeiting attack (Holliman & Memon, 2000), the birthday attack (Stallings, 1998) and the transplantation attack (Barreto et al, 2002), by involving the contents in the watermarking process in a non-deterministic manner (Kim et al, 2008; Li & Yuan, 2006). Therefore schemes with high payload, high resolution of tamper localization, high security and zero distortion to the ROI are desirable.

Proposed Method

It is observed that, apart from the ROI, which represents the actual contents of images, many types of medical images have significant background areas. Exploiting this characteristic, a few transform domain watermarking schemes have been proposed to extract features/signature from the ROI for embedding in the background areas to serve the purposes of copyright protection (Wakatani, 2002; Lie et al, 2003) or integrity verification (Osborne et al, 2004). However, as mentioned in the previous section, the applicability of transform domain watermarking methods is restricted to the cases where lossy compression is allowed. In the light of this limitation, in this work we propose a new spatial domain scheme, which uses the contents of the ROIs to create a content-dependent watermark and embeds the watermark in the background areas without adding any embedding distortion to the ROI. Without loss of generality, we will use mammograms with gray level range [0, 255] in the presentation of this work. Because the background areas contain no information of interest and the gray levels of their pixels fall in the low end of the intensity range, wherein human eyes are not sensitive to variation, a greater degree of embedding can be carry out to strengthen security and/or increase resolution of tamper localization (Li & Yuan, 2006). The main components of our scheme are described in the following subsections.

Segmentation

The mission of the image segmentation operation is that when given either the original image, I_o, during the *watermarking* process or the watermarked image, I_w, during the *authentication* process as input, the segmentation function should partition the input image into the same bi-level output image, with one level corresponding to the background areas and the other to the ROIs. Figure 1(a) shows a typical mammogram with intensity represented with 8 bits. We can see that it has a dark background with intensity below 30 and a significantly brighter area of a breast