IGI PUBLISHING
ITJ 4566
701 E. Chocolate Avenue, Suite 200, 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 1
edited by **Chang-Tsun Li © 2009, IGI Global**

Protection of Digital Mammograms on PACSs Using Data Hiding Techniques

Chang-Tsun Li, University of Warwick, UK

Yue Li, University of Warwick, UK

Chia-Hung Wei, Ching Yun University, Taiwan

ABSTRACT

Picture archiving and communication systems (PACS) are typical information systems, which may be undermined by unauthorized users who have illegal access to the systems. This article proposes a role-based access control framework comprising two main components – a content-based steganographic module and a reversible watermarking module, to protect mammograms on PACSs. Within this framework, the content-based steganographic module is to hide patients' textual information into mammograms without changing the important details of the pictorial contents and to verify the authenticity and integrity of the mammograms. The reversible watermarking module, capable of masking the contents of mammograms, is for preventing unauthorized users from viewing the contents of the mammograms. The scheme is compatible with mammogram transmission and storage on PACSs. Our experiments have demonstrated that the content-based steganographic method and reversible watermarking technique can effectively protect mammograms at PACS.

Keywords: *biomedical informatics; data hiding; digital watermarking; information security; PACS; steganography*

INTRODUCTION

A picture archiving and communication system (PACS) integrates imaging modalities and acts as the interface between hospitals and departmental information systems in order to manage the storage and distribution of images to radiologists, physicians, specialists, clinics, and imaging centers. As medical image databases are interconnected through PACSs, those medical images are subject to security breaches, such as loss or manipulation of sensitive information, if their contents are not protected in some ways. For example, if a medical image is illegally obtained or if its content is malevolently changed, the patient's privacy, health care and legal rights could be undermined. Given the fact that medical image databases are

accessed by users of various roles, e.g., doctor, administrator, interns, etc., a role-based access control mechanism is an obvious approach to the prevention of the afore-mentioned security breaches. For instance, a doctor could be given full access to the images and patients' textual information, while an intern's or administrator's access should be restricted according to the roles they are allowed to play. A common practice of managing textual information associated with images is to store the information in the header segment of the image file. Although the textual information can be protected through encryption, however the file formats are known publicly and the header field is separated from the content; that means the very location of the encrypted information is known. This opens a security gap for the attackers to manipulate the information. For example, even without knowing the secret key, an attacker can replace patient *A*'s encrypted information in the header with patient *B*'s encrypted information. This suggests that the location of the patients' information should not be made known to the unauthorized users and the information itself should be made inseparable from the pictorial contents of the images. Moreover, an overhead of the header is that it takes up physical disk spaces. We proposed in this work a role-based access control framework consisting of two key modules – a *content-based steganographic module* for hiding patients' textual information in the contents of medical images in a non-deterministic manner so as to prevent leaks of sensitive information and to save disk space. We also propose a *reversible watermarking module* for 'masking' the contents of the images with hidden patients' textual information (called *stego-images*) in order to prevent unauthorized users from viewing the images. The main objectives set out in this work are:

1. To design a conceptual framework for protecting mammograms on PACSs. The framework should not only provide reliable protection for mammograms, but also support management functions for users with different access rights.
2. To develop a novel content-based steganographic method for hiding patients' textual information in mammograms and verifying the authenticity and integrity of mammograms. The data hiding process should not change the important pictorial details of mammograms and the data extraction process should not require the availability of original mammograms.
3. To develop a watermarking technique capable of masking the contents of mammograms for protecting mammograms against illegal access. The watermark can be removed to reveal the masked mammogram when authorization for viewing is given.

LITERATURE REVIEW

Main methods used in media industries for protecting digital information against malicious usage can be broadly classified into *cryptography-based* and *authorization-based* approaches. The approach of cryptography-based methods is to devise various protocols for the Internet and local area networks (LAN) to protect the digital information through encryption during the transmission in networks (Long, 2006; Xu, 2005). The idea of the authorization-based methods is to use digital signature certifications to achieve authorization for digital information storage and transmission. Since cryptography-based methods mainly focus on image transmission while laying less emphasis on the storage and management phases, the latter is therefore considered as more desirable in achieving higher reliability and security.

An early example of authorization-based method is the framework proposed by Thomas and Sandhu (1994), which depicted a conceptual model for task-based authorization methods. The concept of task-based authorization is that whether the users can pass the authorization or not depends on the tasks the users are charged with. They discussed several authorization functions and the business activities and mapped the semantic interpretations for the practical activities to computer functions. In