Computer Science Review 27 (2018) 45–60

Contents lists available at ScienceDirect

Computer Science Review

journal homepage: www.elsevier.com/locate/cosrev

Review article

Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review

Asaad F. Qasim[a,b,*], Farid Meziane[a], Rob Aspin[a]

[a] School of Computing, Science and Engineering, University of Salford, Greater Manchester, M5 4WT, UK
[b] Ministry of Higher Education and Scientific Research, Baghdad, Iraq

ARTICLE INFO

Article history:
Received 14 July 2017
Received in revised form 25 November 2017
Accepted 30 November 2017

Keywords:
Medical imaging
Digital watermarking
Reversible watermarking
Integrity
Authentication

ABSTRACT

Medical images can be intentionally or unintentionally manipulated both within the secure medical system environment and outside, as images are viewed, extracted and transmitted. Many organisations have invested heavily in Picture Archiving and Communication Systems (PACS), which are intended to facilitate data security. However, it is common for images, and records, to be extracted from these for a wide range of accepted practices, such as external second opinion, transmission to another care provider, patient data request, etc. Therefore, confirming trust within medical imaging workflows has become essential. Digital watermarking has been recognised as a promising approach for ensuring the authenticity and integrity of medical images. Authenticity refers to the ability to identify the information origin and prove that the data relates to the right patient. Integrity means the capacity to ensure that the information has not been altered without authorisation.

This paper presents a survey of medical images watermarking and offers an evident scene for concerned researchers by analysing the robustness and limitations of various existing approaches. This includes studying the security levels of medical images within PACS system, clarifying the requirements of medical images watermarking and defining the purposes of watermarking approaches when applied to medical images.

Contents

1. Introduction and motivation 46
 1.1. Introduction 46
 1.2. Motivation for medical image watermarking 46
 1.3. Digital watermarking requirements 47
2. Digital watermarking 48
 2.1. Principal components of a watermarking system 48
 2.2. Digital watermarking classifications 48
 2.3. Digital watermarking techniques 48
  2.3.1. Spatial domain techniques 49
  2.3.2. Transform domain techniques 50
3. State of the art 51
 3.1. Schools of thought in medical image watermarking 51
  3.1.1. Classical methods while minimising the distortion 51
  3.1.2. Region of interest and region of non-interest watermarking methods 52
  3.1.3. Reversible watermarking methods 52
 3.2. Purposes of medical image watermarking 54
  3.2.1. Authentication schemes 54
  3.2.2. EPR data hiding schemes 55
  3.2.3. Authentication and EPR data hiding schemes 56
4. Evaluation benchmarks of watermarking algorithms 56
 4.1. Imperceptibility assessment of watermarked image 56

[*] Corresponding author at: School of Computing, Science and Engineering, University of Salford, Greater Manchester, M5 4WT, UK.
E-mail addresses: A.Qasim@edu.salford.ac.uk (A.F. Qasim), F.Meziane@salford.ac.uk (F. Meziane), R.Aspin@salford.ac.uk (R. Aspin).

https://doi.org/10.1016/j.cosrev.2017.11.003
1574-0137/© 2017 Elsevier Inc. All rights reserved.

4.1.1. Mean square error 56
4.1.2. Peak signal to noise ratio..... 56
4.1.3. Structural similarity index 56
4.2. Robustness evaluation of extracted watermark..... 57
4.2.1. Correlation coefficient 57
4.2.2. Similarity measure..... 57
4.2.3. Bit error rate 57
4.2.4. Accuracy ratio (AR) 57
5. Discussion and conclusions..... 58
References 58

1. Introduction and motivation

Through the exponential development of modern technologies in the areas of communication and computer networks, the conventional diagnosis has mostly migrated to a technology enabled e-diagnosis. Most Hospital Information Systems (HIS) and medical imaging systems generate and store medical images in different modalities such as X-ray, Ultrasound, Magnetic Resonance Imaging (MRI) and Computerised Tomography (CT). These images are usually managed within a digital workflow based on the Digital Imaging and Communications in Medicine (DICOM) standard [1].

1.1. Introduction

In healthcare systems, a hierarchical scheme can be considered as a pyramid with hospitals at the base and the general Picture Archiving and Communication Systems (PACS) at its top. Images are taken in a hospital and are immediately saved in the PACS. Within few minutes, these images are transferred to an upper PACS, which collects data coming from hospitals belonging to the same division. These files stay in this system for some hours, typically staying for the night, during which time their integrity is not maintained accurately. Then, these files are transmitted to the hierarchically higher PACS until they reach the top-PACS. In the top-PACS, the data are eternally saved and collected in tapes, physical drives or optical supports with associated hash signature, to become ready for the diagnostic workflow operations. Furthermore, the data are encrypted utilising the secret key of the PACS manager. This operation is called consolidation [2].

For security purposes, the authorised archive is managed offline, while available data are kept on the top-PACS discs. In most situations, it is difficult to foretell the security issues for each intermediate system, and the data could be altered intentionally or unintentionally: this is the first serious case. Moreover; the data are not directly consolidated when reaching the top-PACS but after approximately 24/36 h. During this time, PACS professionals, which have access to both the metadata as well as the image's pixels due to the structure of DICOM images, are permitted to edit the files as needed for adjusting potential flaws in patients' data. This matter indicates to the second significant case which allows the malicious PACS manipulation to modify the images before the consolidation process. Hospital's system can retrieve the images from the top-PACS when requested by the physicians. In the case of expected claims, such as regular medical reports, files are pre-fetched in the hospital's PACS, e.g. through night-time or transmitted as soon as possible. The separation between the legal archive (secured data) and the available data (used by clinicians) points out the last crucial case of PACS scenario. If the medical images have been modified in the top-PACS discs, there will be no possibility to automatically discover the manipulation because the authorised archive is saved off-line and the data are not quickly accessible. Definitely, it will be possible to discover the alterations that have been applied to the data in PACS discs, but it might be too late for patients' safety [2].

Furthermore, transmitting medical images between hospitals, located at various locations and different administrative organisations has become a common practice for many reasons, such as diagnosis, treatment, distance learning, training purposes, teleconferences between clinicians and medical consultation between physicians and radiologists [3]. Malicious alterations on the medical images are feasible for getting counterfeit health insurance demands by some insurance company or for hiding medical situations for gaining personal advantages [4]. For instance, Fig. 1shows a liver disease of a patient which is altered by changing the position of the infected region of the liver by using available software (e.g. Adobe Photoshop) [5]. Many other cases of manipulation can be applied, but the issue is how they can be detected? Actually, by merely seeing the images, detecting such reasonable manipulations that include entirely forged abnormalities would be impossible.

1.2. Motivation for medical image watermarking

Security requirements of medical information are mostly derived from legislative rules and strong ethics of the security policy, that professionals and concerned patients must follow [6]. This requires three mandatory features: confidentiality, reliability and availability. Confidentiality indicates that only the authorised people, in the normally scheduled situations, have access to the data. Reliability may be decomposed into two aspects: *i Integrity* which verifies that the information has not been changed, and, *ii Authentication* which ensures that the data belongs to the right patient and is delivered from the verified source. Availability defines the capability of the authorised users to utilise the information system in the normally scheduled situations of access and practice [7].

Confidentiality of the image data can be accomplished by applying many techniques such as encryption, access control and firewall. Integrity can be fulfilled by encrypting the images when sharing them over the network. Authentication needs measures being implemented to discover whether confidentiality and/or the integrity of the data has been breached [8].

Two techniques are commonly employed to ensure integrity and authenticity within the data; metadata and digital watermarking [4,9]. In medical imaging, the metadata refers to the data stored along with the image [9]. The common approach of metadata inclusion is Part 15 of the DICOM standard, where the digital signature data is placed in its header [1]. The metadata has also been employed to offer confidentiality, using the data of DICOM header to encrypt the images [10]. Existing metadata techniques do not provide a robust link between the medical image and its metadata. It is, therefore, almost easy to decay the metadata rendering the image unreliable. This shortcoming can be fixed with digital watermarking [9]. Digital watermarking is a technique that hides data known as a watermark into the digital object such that the concealed watermark can then be detected/extracted to make a confirmation about the object [11]. Image watermarking is one of the earliest techniques to improve integrity and authenticity of the digital data. In recent times, authentication is one of the main watermarking requirements in medical applications [12].