International Conference on Computational Science and Information Management (ICoCSIM)
Vol. 1 (2012) 1-6

A Quick Glance at Digital Watermarking in PACS

Syifak Izhar Hisham, Siau-Chuin Liew, Jasni Mohd Zain

Faculty of Computer Systems and Software Engineering,
Universiti Malaysia Pahang, Lebuhraya Tun Razak, 26300 Kuantan, Pahang, Malaysia

Abstract

Nowadays PACS is used widely at hospitals and clinical departments globally. It able to help the clinical professionals doing diagnosis and smoothen the transmission process and storage of medical images. Since PACS handles thousands of crucial data in medical, security and authentication method is seen as very important in PACS. Digital watermarking is a field that receives many attentions and actively developed in researches lately. However, only a little of them had been tested in PACS. This paper surveys and reviews some researches about digital watermarking in PACS. This paper also provides some future perspective towards the improvement of application in PACS.

Keywords: Watermarking; PACS; Medical Image; DICOM; Security

1. Introduction

Picture archiving and communication system (PACS) is a work flow-integrated system for managing medical image and related data. It is designed to streamline operations throughout the whole patient care delivery process [1]. It is seen as a big help the clinical professionals doing diagnosis and smoothen the transmission process and storage of medical images [2]. PACS was originally developed for radiology services over 20 years ago to capture digital medical images rather than in film-based media. PACS transmits medical images using the standard named DICOM (digital imaging and communications in medicine).

Moving with the technology of PACS, with the rapid development of biomedical engineering, digital images watermarking has been becoming increasingly important and in the concern of professionals in hospitals and clinical environment. A digital watermarking system considered as a solution for preserve the integrity, confidentiality and the authenticity of digital media. The demand for the authentication methods of digital media becomes significant issue in order to ensure that work have not been tampered with, especially for crucial data as medical images.

2. PACS

A picture archiving and communication system (PACS) consists of image and data acquisition, storage, and display subsystems integrated by digital networks and application software [3]. It is a system for the transmission and storage of medical images. In a PACS, the digital imaging modalities such as CT, MRI, US, CR as well as their archives and display workstations are connected by various digital networks [4, 5]. PACS had been developed in the late 1980s, and after developing for 20 years, it becomes widely adopted in clinical departments and hospitals.

A generic PACS infrastructure as described by [3] consist of patient data servers, imaging modalities, PACS controllers with database and archive and also display workstations connected by communication networks as shown in Fig. 1. Application servers are where images and data are extracted from the PACS archive for various usages. Acquisition gateway acts as a buffer between imaging modalities and the PACS controllers. Its tasks are such as acquiring image from the imaging modalities, converting the data from manufacturer specifications to DICOM data formats and forwarding the image to PACS controller or display workstations. Other tasks such as image pre-processing, compression and data security are also performed here. PACS controllers and archive servers have more complicated functions such as image receiving, image stacking, image routing, image archiving, PACS database updating and RIS interfacing.

Starting about 10 years ago, PACS was much discussed in scientific meetings [5]. Refresher courses on PACS were offered in the annual meetings of the Radiological Society of North America (RSNA). Various manufacturers organized special private workshops by application specialists. However, the emphasis of such training was on how to retrieve images and reports and display them on the review workstations and how to use the tools in the workstations to enhance image interpretation [7]. Many clinical professionals concern about the data security in the system.

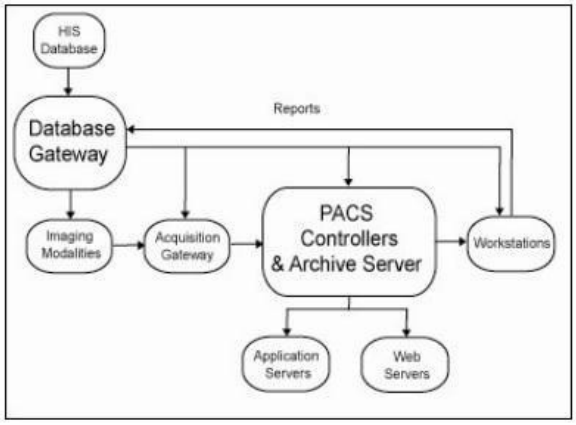

Figure 1. PACS basic components and data flow by Huang (2004) (Image courtesy: Liew & Jasni, 2010)

3. Issues in using PACS

Law and Zhou (2003) had made a survey among clinical professionals about the problem they encountered when using PACS system. A few examples of issues frequently raised by them are about the security of images in the system. The professionals were concern about the access of the image and data, the route that should be taken by images when transferring to another workstation, external or private radiologist, and modified images which could not be read. Since the images will be viewed in various workstations, such as PACS Lab, Image Lab, Health Clinic and Radiologist, thus, the possibility to be modified and attacked by anybody is quite high. In short words, the stability of the system as well as security and privacy of the patient's data were added concerns [5].

The PACS involves integration of 10s to 100s of components, including all imaging modalities and other information systems such as RIS or HIS [5]. Even though the system is proven as safe to be used to handle important data in medical images, watermarking is being said as one of the method to control the security, give authenticity and detect any tamper.

4. Image watermarking in PACS

Fontani et al. (2010) described PACS in a hierarchical manner. The hierarchical structure can be viewed as a pyramid with hospitals at its bottom and the PACS at its top. Images are acquired in a hospital and are immediately stored in its PACS. The images are forwarded to a superior PACS and remain in this system for several hours and during this time the integrity of the images is not always strictly protected. The images are then forwarded to the hierarchically superior PACS, until they reach the top-PACS. The top-PACS will permanently store the images along with their hash signatures, encrypted using the private key of the PACS administrator. In order to implement watermarking in PACS, it was proposed by Fontani et al. (2010) that the images are watermarked after they were acquired by the imaging modalities.

Authentication of the images can be performed at every level of the hierarchy from bottom to top and vice versa. Cao et al. (2002) had proposed the digital envelope (DE) concept which is similar to watermarking. This concept is for ensuring data integrity, authenticity and privacy during image transmissions. DE consists of digital signature (DS) of the image and selected information from the DICOM image header, can be embedded in the background area of the image as an invisible permanent watermark.

Cao et al. (2002) developed a method to generate DE and embed it in mammogram and MR sectional images. DS is a major application of public-key cryptography. DE includes the DS of the image as well as decoded patient information from the DICOM image header. The concept of DE is that someone can 'seal' a message (DS plus patient information) in such a way that no one other than the intended recipient can 'open' the sealed message. The DE method can be revamped as a general method to assure data security for communication of medical images over public networks [9].

The disadvantage of this method is time consuming and CPU-intensive process. Algorithm optimization and revamp of the DE method are needed in order to speed up the whole process for real-time image transmission. The method by Cao et al. (2002) can only detect if any pixel or any bit in the data stream had been altered, but not the exact location, which pixel(s) or bit(s), which has been compromised. In summary, Cao et al. (2002) approach is that once the RS determines the image/data had been altered, it will discard the image, notify and alert the SS, and request the information to be retransmitted.

Improving this method, Huang (2004) had also proposed an image security system based on the digital envelope (DE) concept. The method applies to both the sender and receiver sides. The sender side consists of the following four steps:

- Image pre-processing: The image is segmented from its background and relevant patient information is extracted from the DICOM image header.
- Image hashing: The segmented image is hashed using MD5 hashing algorithm.
- Data encryption: RSA public key encryption is used to produce DS by encrypting the image hash value. Data encryption standard is used to encrypt the DS and patient data to produce DE.
- Data embedding: The DE is embedded into the image or the background of the image. LSBs of a random pixel are replaced with DE bits.

The receiver side has the reversed process of the four steps that consist of data extraction and decryption. A mammogram was processed using the described method. A total of 6720 bits were embedded and the whole process took approximately 75 seconds. The disadvantage of this method is that tampering of an image can be detected but without tamper localization. It only provides protection for images during the transmission process. The DE method needs a different public key for a different user and thus requires intensive processing.

Huang (2004) had also proposed the implementation of this method in a PACS environment as shown in Fig. 2. This implementation consists of a dedicated image authority server that was designed to solve the limitations of the DE method. All images from the modalities are digitally signed at the DICOM gateway using the authority server's public key instead of the individual user's key. Whenever a remote user needs to verify the origin authenticity or integrity of an image, a request can be made to the system authority and in this case, the PACS security server. The PACS security server is the only one that has the private key which is used to extract and decrypt the DE embedded in the image.

The watermarking scheme proposed by Tan et al. (2011) had also applied public keys in its watermarking embedding. The scheme is a fully reversible, dual-layer watermarking scheme with tamper detection capability for medical images. The scheme was tested using medical modalities such as MRI, CT, US and X-ray images in DICOM format. The results show that the scheme is able to ensure image authenticity and integrity, and to locate tampered regions in the images. The reversible watermarking algorithm used in this scheme is adapted from the method proposed by Coatrieux et al. (2000) but with modifications which include public-key cryptography and a tamper detection and localization feature. It has a multi-layer watermarking approach to increase the data-hiding capacity. The proposed watermarking scheme enables only authorized personnel to access the patient's medical images.

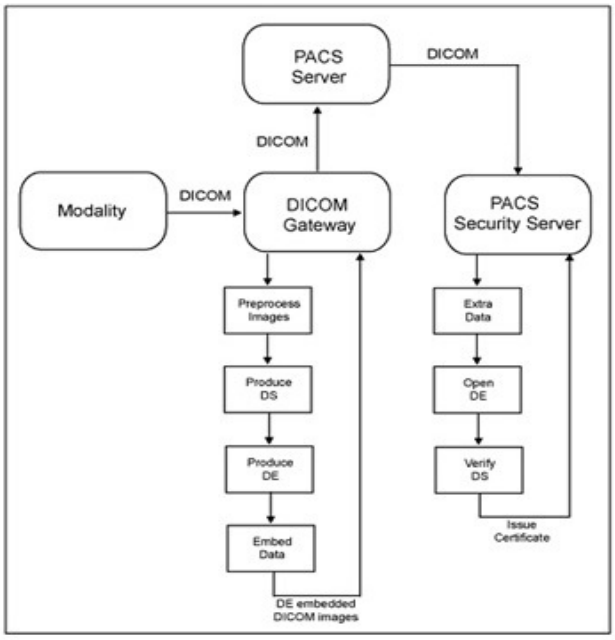

Figure 2. Generic PACS components and its data flow (Huang, 2004).

Tan et al. (2011) had also proposed the implementation of the scheme in a PACS based on the image security system proposed by Huang (2004). In this implementation, the encryption and decryption of the watermark is done by the sender and the receiver as shown in Fig. 3.

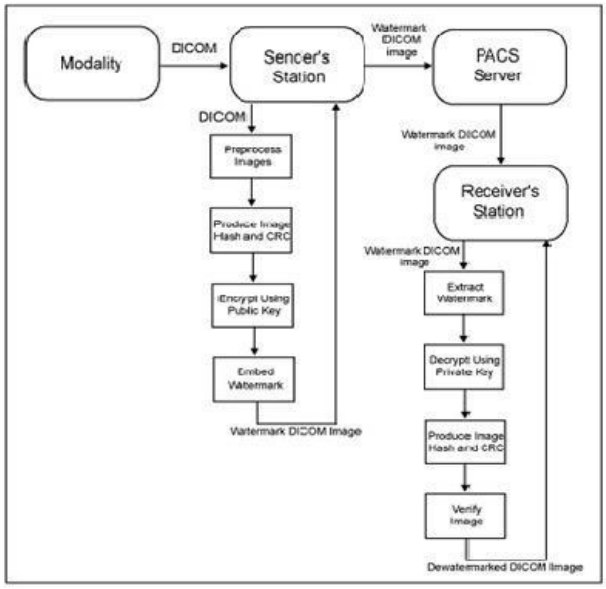

Figure 3. The implementation of scheme by Tan et al. (2011) in a PACS (Source: Tan et al. (2011))

Both proposed implementations by Huang (2004) and Tan et al. (2011) has the disadvantage where the keys used for encryption and decryption needs to be properly managed. The issue of how medical images can be watermarked and authenticated efficiently without affecting the operation of the PACS was not addressed.

Liew (2011) proposed three schemes named R-TLR and TALLOR/TALLOR-RS, which were subjected to effectiveness test in a PACS. Reversible tamper localization and recovery (R-TLR) watermarking scheme is a scheme that uses the characteristic of the ultrasound images to allow the watermarking process to be reversed. The method used to allow reversibility is simple and requires very minimum processing. The original bits were embedded in the region of non-interest (RONI). The watermarked images have a high average PSNR of 53.9 dB. The success rate of the tamper localization and recovery is close to 100%. The watermarked image has a low distortion level and can be reversed to its original state.

Another two schemes by Liew (2011) are tamper localization and lossless recovery (TALLOR) scheme and tamper localization and lossless recovery with region of interest (ROI) segmentation (TALLOR-RS). The ROI segmentation and multilevel authentication method used in TALLOR-RS managed to reduce the tamper localization and recovery average processing time by approximately 53%. Both schemes do not need to be reversed as the watermark is being embedded in the RONI. The average PSNR of the watermarked images for both schemes is at 48.3 dB and 48.2 dB for TALLOR and TALLOR-RS respectively.

A high PSNR indicates low distortion in the watermarked image, which is an important factor to be considered in medical image watermarking. The proposed schemes have 100% success rate for tamper localization and recovery which is better than the R-TLR scheme. The tampered area can be exactly recovered using information stored with lossless compression. The recovered image may be used for clinical diagnoses due to its high quality. Both schemes also have the most accurate tamper localization of one pixel when being compared to other schemes reviewed in the literature. Lossy compression may also be applied to achieve higher compression ratio. The RONI can be authenticated using hash function.

It was concluded that the proposed schemes remains effective in a simulated PACS. The design of a watermark embedder and image authenticator (WEIA) is also proposed. WEIA acts as the interface between the user and the proposed watermarking schemes, namely R-TLR and TALLOR/TALLOR-RS. The advantages of WEIA are ease of use, scalable and platform independent. On the other hand, R-TLR and TALLOR/TALLOR-RS watermark may not survive geometry attack and some removal attack such as compression. Any compression of the watermarked image will be considered as tampering.

Liew (2011) also proposed a new infrastructure and its workflows. It allows WEIA to operate in a PACS. The proposed workflows are flexible and customizable due to the portability of WEIA. However, WEIA and its workflow is only a design and have not been tested yet.

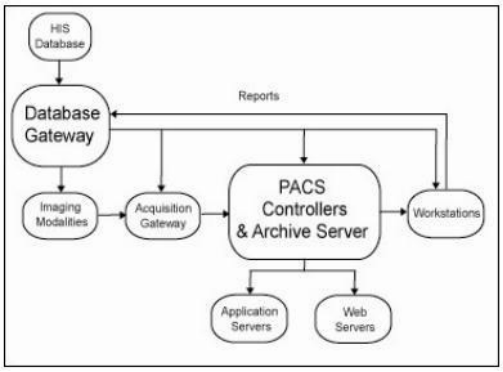

Figure 4. The process of watermark embedding will be done using WEIA in the authentication server (Source: Liew, 2011)

5. Future perspective

Although there are many researches for medical images in recent years [13 - 19] especially for DICOM images in PACS [13, 14], but there are very little that had been tested in PACS. Liew (2011) has proposed the schemeswhich are superior in terms of capacity, PSNR, localization accuracy, recovery quality and simplicity when being compared to existed methods which were tested in PACS. However, the limitation is R-TLR and TALLOR/TALLOR-RS were developed specifically for ultrasound images. R-TLR and TALLOR/TALLOR-RS must be applied and tested to images from other modalities such as magnetic resonance imaging (MRI), computed tomography (CT) and nuclear imaging.

An interface of watermarking scheme can also be further developed into a working application and be tested. The processing time needed by R-TLR and TALLOR/TALLOR-RS can be tested on real operation hardware with better computing capability. A PACS simulation is needed to be developed in order to have a real operation system.

Up till now, only little survey had been done among the clinical professionals to distinguish the original and watermarked images using those new proposed schemes. Further study is needed to determine whether watermarked images in PACS can be used for diagnoses purposes or not.

6. Summary

This review paper starts from some basic knowledge of PACS, problems in using PACS, digital watermarking in PACS and some future perspective related to the issue. There are various kinds of digital watermarking on different medium for medical images. A lot of researches have invented new schemes, which produce significant result day by day. The current interest is whether it can be operated in real PACS or not. This paper is hoped to be a help to students and researchers in doing researches in PACS.

References

1. H.K. Huang, Enterprise PACS and image distribution. Computerized Medical Imaging and Graphics, 27(2-3), pp. 241-53 (2003).
2. K. Fridell, P. Aspelin, L. Edgren, L. Lindskold, and N. Lundberg, PACS influence the radiographer's work. Radiography (2009)15, 121e133.
3. H.K. Huang, PACS and Imaging Informatics-Basic Principles and Applications. New Jersey: John Wiley & Sons, pp.409-430 (2004).
4. M. Osteaux, R. Van den Broeck, F. Verhelle and J. De Mey, Picture archiving and communication system (PACS): a progressive approach with small systems. European Journal of Radiology, 22 (1996), pp. 166-174.
5. M.Y.Y. Law and Z. Zhou, New direction in PACS education and training. Computerized Medical Imaging and Graphics, 27 (2003), pp. 147–156.
6. S.C. Liew and Jasni M.Z., Experiment of Tamper Detection and Recovery Watermarking in PACS. Proceedings of the IACSIT 2nd International Conference on Computer Research and Development (ICCRD2010), 7-10 May 2010, Kuala Lumpur, Malaysia.
7. Z. Protopapas, E.L. Siegel, B.I. Reiner, S.M. Pomerantz, E.R. Pickar, M. Wilson and F.J. Hooper, Picture archiving and communication system training for physicians: Lessons learned at the Baltimore VA Medical Center. Journal of Digital Imaging, Volume 9, Number 3 (1996), 131-136, DOI: 10.1007/BF03168608.
8. M. Fontani, A.D. Rosa, R. Caldelli, F. Filippini, A. Piva, M. Consalvo and V. Cappellini, Reversible watermarking for image integrity verification in hierarchical PACS. Proceedings of the 12th ACM workshop on Multimedia and security, pp. 161-168 (2010).
9. F. Cao, H.K. Huang and X.Q. Zhou, Medical image security in a HIPAA mandated PACS environment. Comput. Med. Imag. Graphics, 27 (2003), pp. 185–196.
10. C.K. Tan, C. Ng, X. Xu, C.L. Poh, L.G. Yong and K. Sheah, Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability. Journal of Digital Imaging, 24(3):528-540 (2011).

11. G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec, Relevance of watermarking in medical imaging. Proc IEEE EMBS Information Technology Applications in Biomedicine. Arlington, VA 2000, pp. 250–255 (2000).
12. S.C. Liew, Tamper Localization and Recovery Watermarking Schemes for Medical Images in PACS. Doctor of Philosophy (Computer Science) Thesis, Universiti Malaysia Pahang, Malaysia, pp. 32-36 (2011).
13. F. Rahimi and H. Rabbani, A dual adaptive watermarking scheme in contourlet domain for DICOM images. BioMedical Engineering OnLine, 201110:53 (2011).
14. L.O.M. Kobayashi and S.S. Furuie, Proposal for DICOM Multiframe Medical Image Integrity and Authenticity Journal of Digital Imaging. Vol 22, No 1 (February), pp. 71Y83 (2009).
15. P. Fakhari, E. Vahedi and C. Lucas, Protecting patient privacy from unauthorized release of medical images using a bio-inspired wavelet-based watermarking approach. Digital Signal Processing 21 (2011) 433–446.
16. K. S. Kim, M. J. Lee, J. W. Lee, T. W. Oh and H.Y. Lee, Region-based tampering detection and recovery using homogeneity analysis in quality-sensitive imaging. Computer Vision and Image Understanding, 115 (2011) 1308–1323.
17. F.Y. Shih and Y.T. Wu, Robust watermarking and compression for medical images based on genetic algorithms. Information Sciences 175 (2005) 200–216.
18. Z. Zhou, Data security assurance in CAD-PACS integration. Computerized Medical Imaging and Graphics 31 (2007) 353–360.
19. J. Hu, A pixel-based scrambling scheme for digital medical images protection. Fengling Han Journal of Network and Computer Applications, 32 (2009) 788–794.