Journal of Computer Science 6 (7): 794-799, 2010
ISSN 1549-3636
© 2010 Science Publications

# Experiment of Tamper Detection and Recovery Watermarking in Picture Archiving and Communication Systems

Siau-Chuin Liew and Jasni Mohamad Zain
Faculty of Computer Systems and Software Engineering,
University Malaysia Pahang Kuantan, Malaysia

**Abstract: Problem statement:** Medical images such as x-rays, ultrasounds and Magnetic Resonance Imaging (MRI) plays an important role in helping the physicians to diagnose a disease or body conditions. These images can be tampered with existing image processing tools that is easily available. The usage of security measures such as watermarking can protect the integrity of the images. Numerous watermarking schemes with basic security functions and even tampered image recovery are available. But there is no research on the experimentation of watermarking in the operational environment that involves Picture Archiving and Communication Systems (PACS). **Approach:** This study focused on the experiment of selected watermarking scheme running in a simulated Digital Imaging and Communications in Medicine (DICOM) compliant PACS environment. A tamper detection and recovery watermarking was applied to an ultrasound image. Image will then be transferred to another computer within the PACS. Transferred and non-transferred image were tampered in the exact manner. The effectiveness of the watermarking scheme is known by comparing its recovery rates between these two tampered images. **Results:** The result showed that both transferred and non-transferred image had the recovery rates of 100% and recovered areas were identical. **Conclusion:** The result of the experiment showed that the selected watermarking scheme remains effective in a PACS environment. Further development is needed for a program that embeds watermark into images before it is sent to the PACS archive server for storage. The watermarking scheme tested needs to be further improved to be reversible for better implementation in PACS.

**Key words:** Watermarking, medical image, PACS

## INTRODUCTION

Picture Archiving and Communication Systems (PACS) is a network of computers to store, retrieve, distribute and display medical images and data in a digital form. PACS handles various types of images from medical imaging equipments such as ultrasound, magnetic resonance, x-ray, mammogram, computed tomography, endoscopy and many more. The most common standard being used Digital Imaging and Communications in Medicine (DICOM). DICOM provides mechanism for the interchange of DICOM images in technological means in PACS.

A generic PACS infrastructure as described by (Huang, 2004) consist of patient data servers, imaging modalities, imaging modality, 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. It has three main tasks:

- Acquires image from the imaging modalities

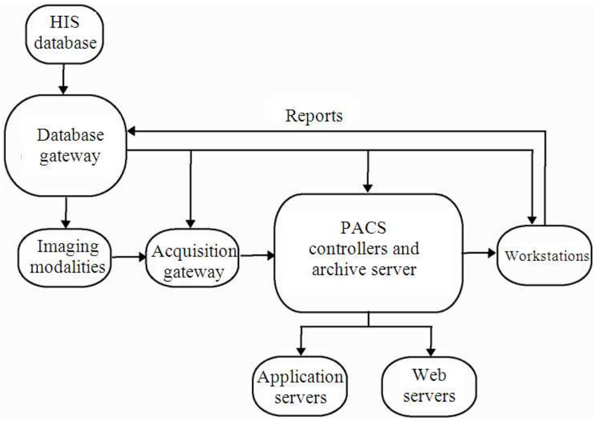


Fig. 1: Generic PACS components and data flow

**Corresponding Author:** Siau-Chuin Liew, Faculty of Computer Systems and Software Engineering, University Malaysia Pahang Kuantan, Malaysia

- Converts the data from manufacturer specifications to DICOM data formats
- Forwards the image to PACS controller or display workstations

Other tasks such as image preprocessing, compression and data security are also performed here. PACS controller and archive server have more complicated functions such as image receiving, image stacking, image routing, PACS database updating and RIS interfacing.

One of the major DICOM communication Service Object Pair (SOP) classes for image communications is the Storage Service Class. For example, it allows the acquisition gateway to play the role of a Storage Service Class User (SCU) that initiates storage request and transmits images to the PACS archive, which serves as a storage Service Class Provider (SCP) that stores the images to its local storage.

The integrity of the records such as medical images needs to be protected from unauthorized modification or destruction of information on the medical images. One of the security measures that can be used is watermarking. Watermark provides three objectives in medical images (Coatrieux *et al*., 2000):

- Data hiding, for embedding information to make the image useful or easier to use
- Integrity control, to verify that the image has not been modified without authorization
- Authenticity, that is to verify that the image is really what the user supposes it is

There is no current standard on the usage of watermarking in medical images. Numerous researches had been done in producing better watermarking schemes and techniques but there is no research on the experimentation of watermarking in medical images in an operational PACS environment.

In this study, we attempt to experiment a tamper detection and recovery watermarking on medical images in PACS. The effectiveness of the watermarking scheme will be tested.

**Watermarking in medical images:** Before proceeding to the implementations of watermarking in medical image in PACS, an example of watermarking system is shown in Fig. 2.

The encoder, E embeds the watermark, W inside original image I by using embedding function, E as shown in Eq. 1:

$$E(I, W) = I_W \quad (1)$$

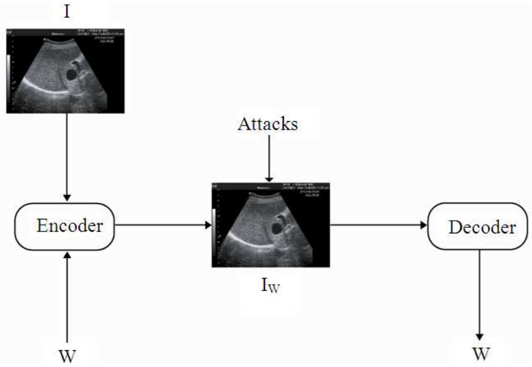


Fig. 2: Image watermarking

The output from this process is $I_W$, the watermarked image. The decoder, D will detect or extract the watermark, W from the original image as in Eq. 2.

$$D(I, I_W) = W \quad (2)$$

**Types of domain:** Watermarking techniques can be classified according to where the watermark is embedded namely spatial domain and transform domain:

- Spatial domain: One of the most straight forward and simple technique is to embed the watermarking into the least significant bits of the image. Since the last binary bits are the least significant bits, its modification will not perceived by human eyes. This technique is not as robust as transform domain techniques and rarely survives various attacks
- Transform domain: Most of the transform domain techniques embed the information into the transform coefficients of the cover image. Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT) are the three popular methods in this category. Methods used needs a certain amount of computation but it can overcome possible compression and more robust against geometric transformation such as rotation, scaling, translation and cropping

**Watermarking schemes:** There are various types of watermarking schemes that had been developed to be used for medical images. Watermarking schemes ranges from the usage of different domain that produces different image quality as shown in Table 1. Peak Signal to Noise Ratio (PSNR) is used to measure the similarity between images before or after watermarking. A higher value is a preference. Each watermarking schemes have its advantage and disadvantage.

Table 1: Summary of PSNR and types of domain

| Scheme by | Lim *et al.* (2008) | Fotopoulos *et al.* (2008) | Coatrieux *et al.* (2009) |
|---|---|---|---|
| Domain | DWT, spatial | Spatial | Spatial, DCT |
| PSNR (dB) | 19-51 | 36-37 | 37-42 |
| Advantage | Robust against median filter attack | Adaptable compression | Knowledge digest |
| Disadvantage | Time consuming | Less robust | Higher payload |

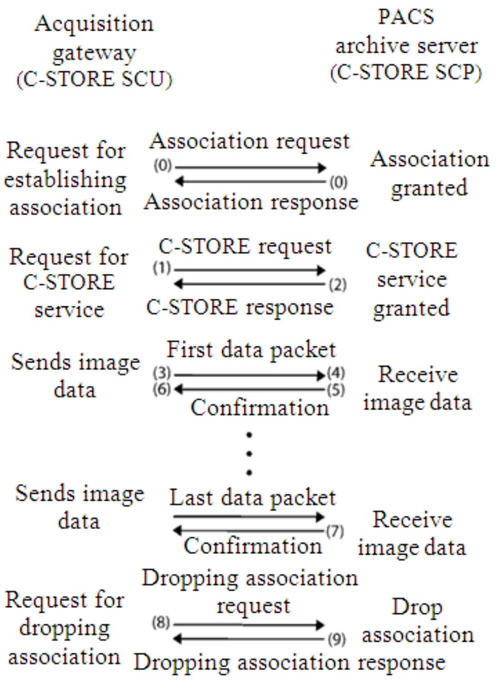


Fig. 3: C-STORE operation

There are also watermarking schemes that allow tamper detection and recovery of images. An example is a scheme proposed by (Zain and Fauzi, 2006). It uses block based method with multiple hierarchies where each blocks consists of 8×8 pixels. Each block will then be divided into sub-blocks of 4×4 pixels. A 3-tuple watermark embedded consists of 2 bits authentication watermark and 7 bits recovery watermark for other sub-block. Average intensity of a corresponding block and its sub-blocks is calculated to generate authentication watermark. Average intensity of a sub-block will be embedded as the 7 bits recovery watermark in another block which was predetermined in a mapping sequence. A parity bit is generated based on the 7 bits recovery watermark.

Detection of a tampered block is done by comparing the average intensity and parity bit. The detection of tampering is done in 3 levels from 4×4 pixel sub-blocks to 8×8 pixels blocks. Blocks that were mark invalid will be recovered.

**DICOM:** DICOM was developed in 1983 by American College of Radiology (ACR) and National Electrical Manufacturers Association (NEMA). It consists of 18 independent parts; file format definition and communication protocol. It uses Transmission Communication Protocol/Internet Protocol (TCP/IP) for communication and allows system that uses DICOM standard to be interconnected through compliant network. Current version of the standard is referred as DICOM 3.0 in terms of protecting the integrity of medical images; it outlines the usage of Rivest-Shamir-Adleman (RSA) encryption of Message Authentication Code (MAC) to generate a digital signature. Current DICOM standard does not have provisions for the implementation for watermarking.

In terms of transmission of an information object instance in PACS, C- STORE command can be used. It is one of the DICOM message service elements. Figure 3 below shows an example of a C-STORE operation for an image transmission between acquisition gateway and PACS archive server (Huang, 2004).

## MATERIALS AND METHODS

The purpose of this experiment is to implement watermarking in medical images in a simulated DICOM compliant PACS environment and to know the effectiveness of the watermarking scheme.

Watermarking scheme proposed by (Zain and Fauzi, 2006) will be implemented. This particular watermarking scheme is chosen because it uses the most straight forward method where the watermark is embedded in the least significant bits. It produces high PSNR value of the watermarked images. It also had been clinical evaluated to ensure that watermarked images does not affect clinical diagnoses (Zain *et al*., 2006) as PSNR value does not correlates well with perceived quality measurement (Navas *et al*., 2007).

The experiment uses open source dcm4chee and dcm4che2 DICOM toolkit as a PACS archive server and acquisition gateway. Both provide implementation of standard DICOM in creation, transmission and storage of digital medical image and report data. Two computers were used in the simulation. Acquisition gateway will execute dcmsnd application to perform a C-STORE operation as a SCU. The other computer, a PACS archive server will execute dcmrcv application to act as a SCP where it listens to incoming request for association.

The experiment focus on watermarked image transmitted from acquisition gateway to PACS archive Server as shown in Fig. 4. Below are the step by step descriptions of the image flow in the simulated PACS and point where the watermarking will be tested:

- Image is received from the imaging modalities and being processed by acquisition gateway to appropriate DICOM format. It is assumed that the images had been processed in this experiment
- Image is watermarked. It is proposed that medical images should be watermarked as soon as images are received from the imaging modalities before it is being stored in the archive server. Watermarked is tested
- Image is sent to archive server for storage. Watermarked image is also tested
- Both watermarked images at the acquisition gateway and archive server will be tampered to test the effectiveness of the watermark. It will then be recovered and recovery rate for both images will be compared

The following is the algorithm used for the image watermarking as proposed by (Zain and Fauzi, 2006).

**Preparation:** The image is divided into blocks of 8×8 pixels. One to one block mapping sequence is done A→B→C→D…→A for watermarking embedding, where each symbol denotes an individual block. The mapping sequence is based on Eq. 3 below:

$$\vec{B} = [(k \times B \bmod N_b] + 1 \quad (3)$$

Where:

$B, \vec{B}, k \in [1, N_b]$

k = A prime number

$N_b$ = The total number of blocks

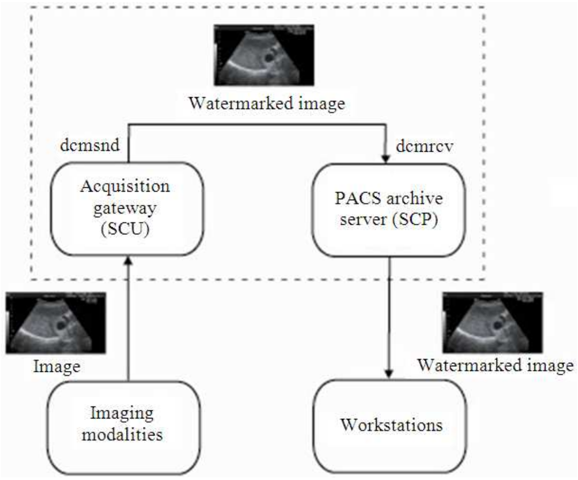


Fig. 4: Simulated PACS

A unique integer $B \in \{1, 2, 3, ..., N_b\}$ is assigned to each block. The maximum prime number $k \in [1, N_b]$ is picked. Equation 3 is applied to each block number B where $\vec{B}$ , the number of its mapping blocks in obtained. All pairs of B and $\vec{B}$ will form the block mapping sequence.

Embedding: Each block of 8×8 pixels in the image is divided into four sub-blocks of 4×4 pixels. The watermark in each sub-block is a block of 3×3 pixels where it contains 2 bit authentication watermark and a 7 bit recovery watermark for the corresponding sub-block within block A mapped to block B.

Least significant bits in the every block will be set to zero. Average intensity for each block and its sub-blocks will be computed. Authentication bit and parity bit is generated for each sub-block. From the mapping sequence generated in the image preparation step, block A recovery information will be stored in block B. The average intensity of sub-blocks As within block A, denoted as avg_As will be computed as the recovery intensity. The authentication bit, parity bit and the recovery intensity forms the watermark where it will be embedded in the corresponding sub-blocks of B.

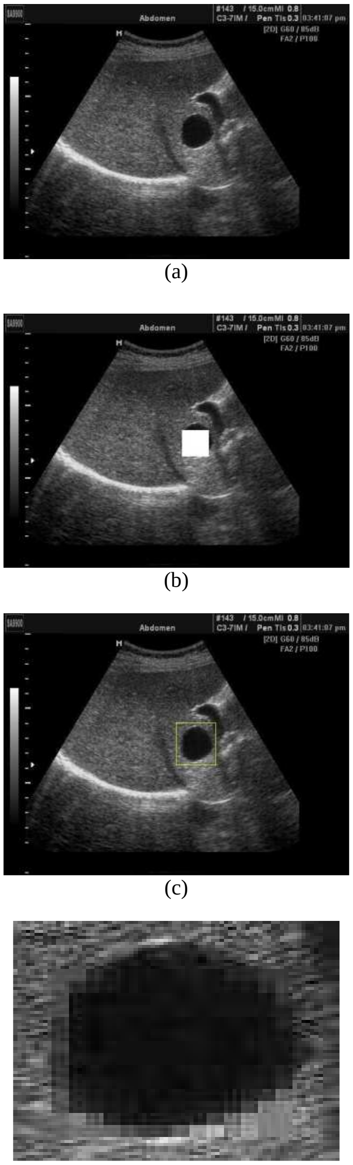
**Tamper detection and recovery:** The image is divided blocks of 8x8 pixels and the least significant bits in the sub-block of 4×4 pixels will be removed, as in the watermarking embedding process.

The average intensity of the block will be computed. For each sub-block of 4×4 pixels, authentication bit and parity bit will be extracted. The least significant bits in the sub-block will be set to zero and average intensity for each sub-block will be computed. Authentication bit and parity bit generated from the average intensity of block and sub-block will be compared to know whether the block had been tampered.

Tampered blocks will be recovered by locating its corresponding blocks by using the mapping sequence used in image preparation. For example, with the assumption that block A had been tampered and its recovery bits were stored in block B. Average intensity of each sub-block of block A stored in sub-blocks of block B will be obtained. Block A will be replaced with the recovered average intensity bits.

## RESULTS

An experiment was carried out to test a watermarked ultrasound image that has the size of 640×480 pixels as seen in Fig. 5a. In Fig. 5b, the watermarked image is manipulated by deleting an area of the image measuring 50×50 pixels. Both images at the acquisition server and archive server were manipulated in the exact manner. Figure 5c shows the recovered image and Fig. 5 shows the magnified area of image recovered. The recovery rates for both images are at 100% and the recovered areas are identical. The outcome of the experiment shows that chosen watermarking scheme functioned effectively in a DICOM compliant and simulated PACS environment.



(a)

(b)

(c)

(d)

Fig. 5: (a) Original watermarked image; (b) Tampered imaged; (c) Recovered image; (d) Magnified area of recovered image

## DISCUSSION

There are few issues that had been encountered during experiment. The process of watermarking should be fully automated to remain efficient if there are thousands of images to be watermarked in an operational environment. A disadvantage of the tamper detection and recovery watermarking scheme tested is that it is not reversible. Watermarked must be able to be removed if there is a request. The watermarking scheme also does not allow compression such as Joint Photographic Expert Group (JPEG) file format. A compression will be detected as a tampering on the whole watermarked image. A compressed medical image is an advantage in terms of file size as current PACS supports viewing of images in web browser.

## CONCLUSION

This study describes the basic functions of PACS components, watermarking in medical images and the DICOM standard. A chosen tamper detection and recovery watermarking scheme was tested in a simulated PACS environment to know its effectiveness. The result of the experiment shows that the watermarking scheme remains effective in a PACS environment.

Further development is needed for a program that embeds watermark into images before it is sent to the PACS archive server for storage. The watermarking scheme tested needs to be further improved to be reversible for better implementation in PACS.

## REFERENCES

Coatrieux, G., C. Le Guillou, J.M. Cauvin and C. Roux, 2009. Reversible watermarking for knowledge digest embedding and reliability control in medical images. IEEE Trans. Inform. Technol. Biomed., 13: 158-165. DOI: 10.1109/TITB.2008.2007199

Coatrieux, G., H. Main, B. Sankur, Y. Rolland and R. Collorec, 2000. Relevance of watermarking in medical imaging. Proceedings of IEEE-EMBS Information Technology Applications in Biomedicine, Nov. 9-10, IEEE Computer Society, Arlington, VA., pp: 250-255. DOI: 10.1109/ITAB.2000.892396

Fotopoulos, V., M.L. Stavrinou and A.N. Skodras, 2008. Medical image authentication and self-correction through an adaptive reversible watermarking technique. Proceedings of the 8th IEEE International Conference on BioInformatics and BioEngineering, Oct. 8-10, IEEE Computer Society, Athens, pp: 1-5. DOI: 10.1109/BIBE.2008.4696803

Huang, H.K., 2004. PACS and Imaging Informatics-Basic Principles and Applications. 1st Edn., John Wiley and Sons, New Jersey, pp: 11-184.

Lim, S.J., H.M. Moon, S.H. Chae, S.B. Pan, Y. Chung, M.H. Chang, 2008. Dual watermarking method for integrity of medical images. Proceedings of 2nd International Conference on Future Generation Communication and Networking, Dec. 13-15, IEEE Computer Society, Hainan Island, pp: 70-73. DOI: 10.1109/FGCN.2008.213

Navas, K.A., M. Sasikumar and S. Sreevidya, 2007. A benchmark for medical image watermarking. Proceedings of the 6th EURASIP Conference focused on Speech and Image Processing, Multimedia Communications and Services, June 27-30, IEEE Computer Society, Maribor, pp: 237-240. DOI: 10.1109/ IWSSIP.2007.438119.

Zain, J.M. and A.R.M. Fauzi, 2006. Medical image watermarking with tamper detection and recovery. Proceedings of the 28th Annual International Conference of the IEEE EMBS, Aug. 30-Sept. 3, IEEE Computer Society, New York, pp: 3270-3273. DOI: 10.1109/IEMBS.2006.260767.

Zain, J.M., A R.M. Fauzi and A.A. Aziz, 2006. Clinical evaluation of watermarked medical images. Proceedings of the 28th Annual International Conference of the IEEE EMBS, Aug. 30-Sept. 3, IEEE Computer Society, New York, pp: 5459-5462. DOI: 10.1109/IEMBS.2006.260245