# Experiment of Tamper Detection and Recovery Watermarking in PACS

**CONFERENCE PAPER** · MAY 2010

DOI: 10.1109/ICCRD.2010.37



**2 AUTHORS:**

Siau-Chuin Liew
Universiti Malaysia Pahang
**24** PUBLICATIONS **30** CITATIONS
SEE PROFILE

Jasni Mohamad Zain
Universiti Malaysia Pahang
**69** PUBLICATIONS **293** CITATIONS
SEE PROFILE

# Experiment of Tamper Detection and Recovery Watermarking in PACS

Siau-Chuin Liew
Faculty of Computer Systems and Software Engineering
Universiti Malaysia Pahang
Kuantan,Malaysia
eliewsc@gmail.com

Jasni Mohamad Zain
Faculty of Computer Systems and Software Engineering
Universiti Malaysia Pahang
Kuantan,Malaysia
jasni@ump.edu.my

***Abstract*— Medical images such as x-rays, ultrasounds and MRI (Magnetic Resonance Imaging) 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 PACS (Picture Archiving and Communication Systems). This paper will focus on the experiment of selected watermarking scheme running in a simulated operation environment. The watermarked images will be tested to know its effectiveness by comparing its recovery rates.**

***Keywords-component; Watermarking; Medical Image; PACS***

## I. INTRODUCTION

PACS (Picture Archiving and Communication Systems) 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 DICOM (Digital Imaging and Communications in Medicine). DICOM provides mechanism for the interchange of DICOM images in technological means in PACS.

A generic PACS infrastructure as described by [1] 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
- converts the data from manufacturer specifications to DICOM data formats
- forwards the image to PACS controller or display workstations.

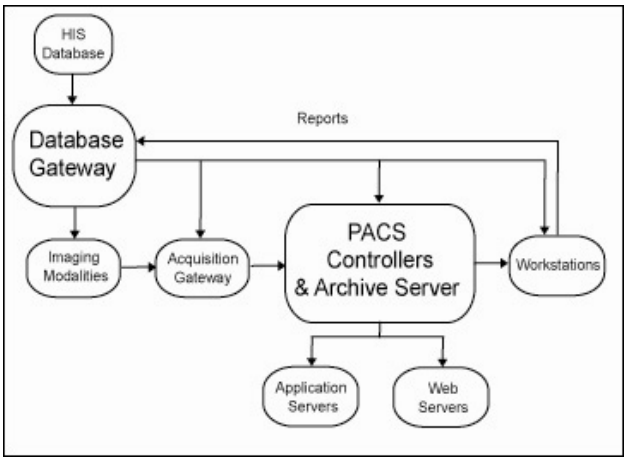



Figure 1. Generic PACS components and data flow.

Other tasks such as image preprocessing, compression and data security are also performed here. PACS controller & 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 SOP (Service Object Pair) classes for image communications is the Storage Service Class. For example, it allows the acquisition gateway to play the role of a SCU (Storage Service Class User) that initiates storage request and transmits images to the PACS archive, which serves as a SCP (Storage Service Class Provider) 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 [2]:

- 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

978-0-7695-4043-6/10 $26.00 © 2010 IEEE
DOI 10.1109/ICCRD.2010.37

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

## II. WATERMARKING IN MEDICAL IMAGES

Before proceeding to the implementations of watermarking in medical image in PACS, an example of watermarking system is shown as below Fig. 2.

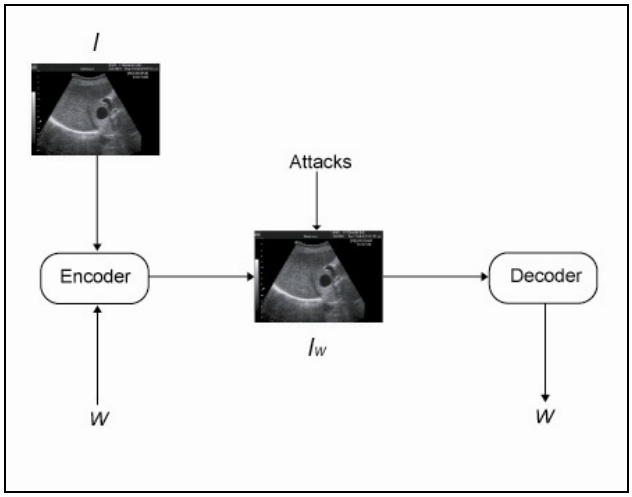



Figure 2. Image watermarking

The encoder, *E* embeds the watermark, *W* inside original image *I* by using embedding function, *E* as shown in equation (1).

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

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 equation (2).

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

### A. Types of domain

Watermarking techniques can be classified according to where the watermark is embedded namely spatial domain and transform domain.

*1) 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.

*2) Transform domain:* Most of the transform domain techniques embed the information into the transform coefficients of the cover image. DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform) and DFT (Discrete Fourier Transform) 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.

### B. 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 I. PSNR (Peak Signal to Noise Ratio) 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 I. SUMMARY OF PSNR AND TYPE OF DOMAIN

| Scheme by | [3] | [4] | [5] |
|---|---|---|---|
| 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 |

There are also watermarking schemes that allow tamper detection and recovery of images. An example is a scheme proposed by [6].It uses block based method with multiple hierarchies where each blocks consists of 8 x 8 pixels. Each block will then be divided into sub-blocks of 4X4 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 4x4 pixel sub-blocks to 8x8 pixels blocks. Blocks that were mark invalid will be recovered.

## III. DICOM

DICOM was developed in 1983 by ACR (American College of Radiology) and NEMA (National Electrical Manufacturers Association). It consists of 18 independent

parts; file format definition and communication protocol. It uses TCP/IP (Transmission Communication Protocol/Internet Protocol) 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 RSA (Rivest-Shamir-Adleman) encryption of MAC (Message Authentication Code) 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. Fig 3. below shows an example of a C-STORE operation for an image transmission between acquisition gateway and PACS archive server[1].

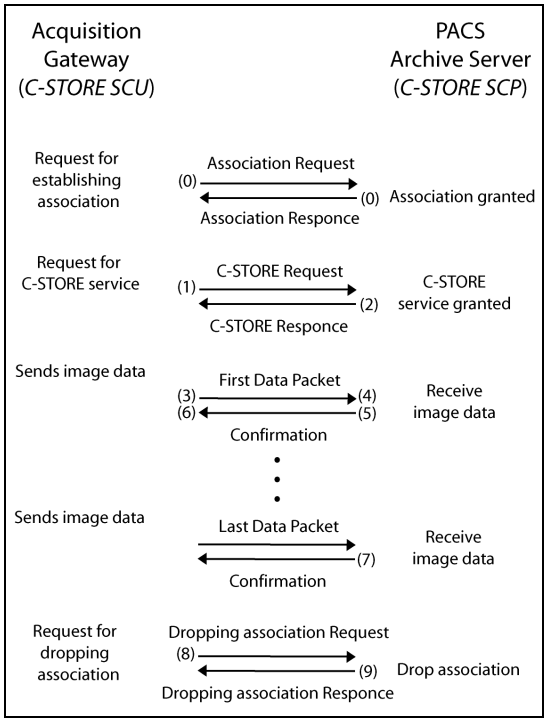



Figure 3. C-STORE operation

## IV. METHODOLOGY

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 [6] 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 [7] as PSNR value does not correlates well with perceived quality measurement [8].

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.

1. 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.
2. 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
3. Image is sent to archive server for storage. Watermarked image is also tested.

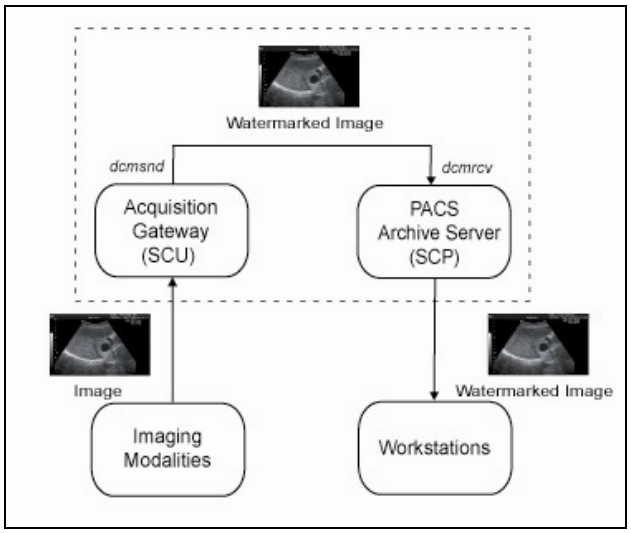


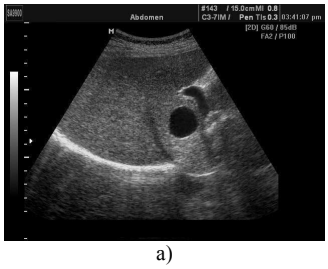

Figure 4. Simulated PACS

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.

## V. RESULTS AND DISCUSSIONS

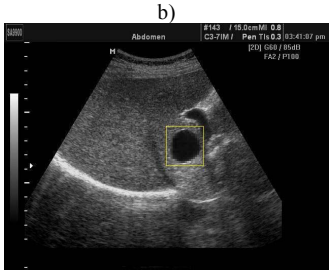
An experiment was carried out to test a watermarked ultrasound image that has the size of 640 x 480 pixels as seen in Fig 5. a). In Fig. 5 b), the watermarked image is manipulated by deleting an area of the image measuring 50 x 50 pixels. Both images at the acquisition server and archive server were manipulated in the exact manner. Fig 5. c) shows the recovered image and Fig 5. d) 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.

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 JPEG (Joint Photographic Expert Group) 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.

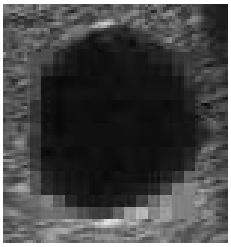


a)

b)



c)



d)

Figure 5. a) Original watermarked image b) Tampered imaged

c) Recovered image d) Magnified area of recovered image

## VI. CONCLUSIONS

This paper 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


[1] Huang, H. K, PACS and imaging informatics-Basic principles and applications, New Jersey: John Wiley & Sons, 2004, pp.11,184.

[2] Coatrieux, G., Main, H., Sankur, B., Rolland, Y., Collorec, R., "Relevance of watermarking in medical imaging", in Proceedings of IEEE-EMBS Information Technology Applications in Biomedicine, 2000 pp. 250-255, doi:10.1109/ITAB.2000.892396.

[3] Sung Jin Lim, Hae Min Moon, Seung-Hoon Chae, Sung Bum Pan, Yongwha Chung, Min Hyuk Chang, "Dual watermarking method for integrity of medical images", in Proceedings of Second International Conference on Future Generation Communication and Networking, 2008, vol.2, pp.70-73, doi: 10.1109/FGCN.2008. 213.

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

[5] Coatrieux, G, Le Guillou, C., Cauvin, J.-M., Roux, C., "Reversible watermarking for knowledge digest embedding and reliability control in medical images", IEEE Transactions on Information Technology in Biomedicine, vol 13, issue 2, Mac 2009,pp.158 – 165,doi: 10.1109/TITB.2008.2007199

[6] Jasni M. Zain, Abdul R.M. Fauzi, "Medical Image Watermarking with Tamper Detection and Recovery", in Proceedings of the 28th Annual International Conference of the IEEE EMBS, New York, 2006,pp. 3270-3273, doi: 10.1109/IEMBS.2006.260767.

[7] Jasni M. Zain, Abdul R.M Fauzi, Azian A. Aziz , "Clinical evaluation of watermarked medical images", in Proceedings of the 28th Annual International Conference of the IEEE EMBS, New York City,2006,pp.5459-5462, doi:10.1109/IEMBS.2006.260245.

[8] Navas,K.A, Sasikumar,M., Sreevidya,S.,"A benchmark for medical image watermarking", in Proceedings of the 6th EURASIP Conference focused on Speech and Image Processing, Multimedia Communications and Services,2007,pp.237-240, doi: 10.1109/ IWSSIP.2007.4381197.