Medical Image Authentication over Public Communication Networks using Secret Watermark

Keun-Tak Oh, Young-Ho Kim and **Yun-Bae Lee,** *Member, KIMICS*

Abstract—The evolution of modern imaging modalities, followed by the rapid development of computer technology has introduced many new features in the communication networks used in medical facilities. Since it is very important to keep patient's record accurately, the ability to exchange medical data securely over the communication network is essential for any medical information.

In this paper, therefore, we introduce some problems which occur from digitizing medical images such as MRI (Magnetic Resonance Imaging), CT (Computed Tomography), CR(Computed Radiography), etc., and then we propose a authentication mechanism for medical image verification using secret watermark images.

I. INTRODUCTION

Traditionally, the film has been used to capture, store, and display radiographic images in hospital. Today, many radiological modalities generate digital images that can be viewed directly on monitor displays. Picture Archiving and Communication System (PACS) consists of image acquisition archiving and retrieval, communication, image processing, distribution, and display of patient information from various imaging modalities [1]. Digital archival will eliminate the need for bulky film room and storage site and the possibility of lost films. Digital image acquisition requires interfacing the PACS to the digital imaging modalities such as CT, MRI, CR, DSA (Digital Subtraction Angiography), ultrasonic, endoscope, and film digitizer. The modality interfaces require that the devices to be used comply with the digital imaging and communication in medicine (DICOM) standard. DICOM represents an international standard of definitions and methods for transferring information and images between devices thus to advertise reliable interoperability among different modules [2].

The PACS system offers an efficient means of viewing, analyzing, and documenting study results, and furnishes a method for effectively communicating study results to the referring physicians [1]. Therefore, because of possibility of making wrong diagnosis, all the images from medical equipments must ensure at least same quality when they are transmitted through the public media as internet.

Manuscript received July 22, 2004.

Keun-Tak Oh, is with field of Information Engineering chosun university, Gwangju, Korea.(email:osc9744@chol.com)

Young-Ho Kim, is with field of Information Engineering chosun university, Gwangju, Korea.

Yun-Bae Lee is with field of Information Engineering chosun university, Gwangju, Korea.(email:yblee@mina.chosun.ac.kr)

In this paper, we introduce and prove some possibilities of medical image fabrication or modulation, and we provide a solution to varify medical images from malicious fabrication. The remainder of this paper is organized as follows. In section II, the brief introduction about DICOM and DICOM standards are presented. We also illustrate the experimental evidence for possibilities of medical image fabrication in section II. In section III, we provide a semi-public authentication mechanism to verify medical image from malicious modulation, and finally, the conclusion in section IV.

II. DIGITAL IMAGE COMMUNICATION IN MEDICINE

A. Background

DICOM (Digital Image Communication in Medicine) is the industry standard for the transmission of digital images and other associated information between digital imaging equipment. The American College of Radiology (ACR) and the National Electrical Manufacturers Association (NEMA) formed a joint committee to develop a standard for DICOM. This DICOM Standard was developed according to the NEMA procedures. This standard is developed in liaison with other standardization organizations including CEN TC251 in Europe, and JIRA and MEDIS-DC in Japan, with review also by other organizations including IEEE, HL7 and ANSI in the USA [2].

DICOM enables digital communication between image acquisition devices, image archive, hardcopy devices and other diagnostic and therapeutic equipment that is connected into a common information infrastructure. In order to provide the support for connecting different devices from various manufacturers on standard networks, it is closely connected with network protocols like OSI and TCP/IP. It also defines data structures/formats for medical images and related data, network-oriented service such as image transmission and query of an image archive, etc.

The DICOM standard does not address issues of security policies, though clearly adherence to appropriate security policies is necessary for any level of security [2]. The standard only provides mechanisms that can be used to implement security policies with regard to the interchange of DICOM objects between Application Entities (AE) using TCP/IP protocol that could not ensure security issues between AEs [2].

Application entities may not trust the communications channel by which they communicate with other Application entities. Thus, this standard provides mechanisms for AEs to authenticate each other securely, AEs to detect any tampering with or alteration of messages exchanged

and AEs to protect the confidentiality of those messages while they are traversing the communication channel. However, as mentioned in ISO7498-2, the DICOM standard does not provide the protection mechanism for the medical image itself [2]. This weak point will cause the serious problems when transmitting the medical information on the public communication channels.

DICOM image file contains both a header, which include text information such as patient's name, image size, medical record number, imaging modality, and other demographic information in the same file. For purpose of image processing, extraction of pixel data value is needed. Thus, the only part of pixel data from DICOM image is needed, in the other word, the pixel data element tagged as (7FE0, 0010) can be extracted.

The Pixel Data Element (7FE0, 0010) and Overlay Data Element (60XX, 3000) shall be used for the exchange of encoded graphical image data. These elements along with additional Data Elements, specified as attributes of the image information entities defined in PS3.3-2001, shall be used to describe the way in which the Pixel Data and Overlay Data are encoded and shall be interpreted [2].

The Pixel Data Element and Overlay Data Element have a VR[1](Value Representation) of OW (Other Word String:uncompressed) or OB (Other Byte String: compressed), depending on the negotiated Transfer Syntax[2]. The only difference between OW and OB being that OB, a string of bytes, shall be unaffected by Byte Ordering [2]. Notice that because of the most of medical image has more than 8 bit length in each pixel it cannot be extracted as BMP or JPEG. Therefore, it must be modulated as 8 bit pixel for easy processing. It is not difficult to modulate a DICOM image into BMP or JPEG using PACS. However, because the DICOM image has its header that contains Patient Name, ID and Study Date etc., modulating BMP or JPEG image into DICOM image is not easy. It is also difficult to decide the Transfer Syntax of DICOM image.

B. Medical Image Modulation and Diagnostic Results

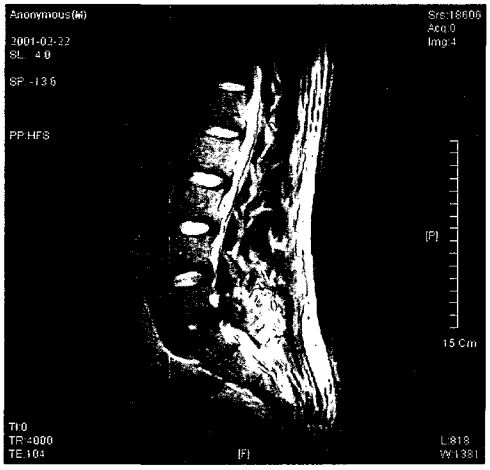

Fig. 1 MRI of normal patient's L-Spine Lateral

1 Specifies the data type and format of the Values contained in the value field of a data element.

2 Transfer Syntax : A set of encoding rules able to unambiguously represent one or more abstract syntaxes [6].

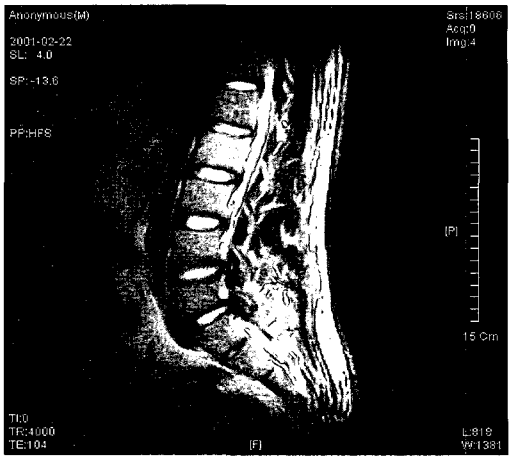

Fig. 2 Fabricated MRI

The digitalized image and the modulated images have been tested intentionally by some experts for the reason how this reading affects the diagnostic results. A MRI (Magnetic Resonance Imaging) of normal vertebra(shown in fig 1) is modulated as HNP (Herniated Nucleus Pulpous, shown in fig 2).

Then the modulated image is examined by two radiotherapists and three residents who work for the C university MRI laboratory in Gwangju. The study result was either Herniation of Intervertebral Disk or Bulging Disc. Since the wrong diagnostic result could cause the serious problems, the fabricated medical image must be verified. Therefore, we provide the secret image watermarking mechanism to verify fabricated medical image in this paper.

III. AUTHENTICATION MECHANISM

A. Digital Watermark

Compared to ordinary paper or film form medical image, digitized medical information including both image and text provides many advantages, such as easy and inexpensive duplication and re-use, less expensive and more flexible transmission either electronically (e.g. through the Internet) or physically (e.g. as CD-ROM). Furthermore, transferring such information electronically through network is faster and needs less effort than physical paper copying, distribution and update. However, these advantages also significantly increase the problems associated with enforcing copyright on the electronic information [3]. The use of digital imaging technique and digital contents based on internet has grown rapidly for last several years, and the needs of digital image protection become more important. For the purpose of medical image protection from modulation/fabrication, the secret image watermarking technique is adapted to the medical image. The fabrication or alteration of medical image is shown and verified by an experimental works.

One of the important issues in watermarking is the need to accese the original image to reliably extract the embed watermarks [4, 5]. Watermarking techniques aim at producing watermarked image that suffer no little quality degradation and perceptually identical to the original versions [6]. Without the original image, the

extracted watermarks may be degraded [7]. A.Z. Tirkel et al.[8] have pointed out that the original image may help to overcome geometric transformation attacts. However, for security reasons, a watermarking technique which does not use the original source is always preferable.

B. Secret Image Authentication

In this section, we introduce the secret image authentication method, then the experimental results are shown in the next section. The basic principle of the JPEG-based embedding method is that quantized elements have a moderate variance level in the middle frequency coefficient ranges, where scattered changes in the image data should not be noticeably visible [3]. In general, the value of each pixel in a binary image can be represented as either '1' or '0'. This can possibly assumes that there is no 'noise' space which can be used for embedding additional information. In this paper, we use the Yeung's [6] algorithm to embed a watermark. The Yeung's algorithm for binary images is based on the ratio of '1' and '0' in a selected block. In Yeung's algorithm, they suppose '1' represent black bit and '0' represent white bit in the source binary image. According to Yeung's algorithm, the rate of blacks and number of 1s in the block b can be expressed as:

$$P_1(b) = \frac{N_1(b)}{64} \tag{1}$$

Since $P_1(b)$ and $N_1(b)$ represent the probability of rate of blacks in the block b and the number of 1s in the block b respectively, the probability of rate of whites can be expressed as equation (2).

$$P_0(b) = 1 - P_1(b) \tag{2}$$

A bit indicating black is embedded into the block of b if $P_1(b) > t$ (where t is a certain threshold), otherwise the white bit is embed into the block b until given threshold is reached. In order to obtain better security for a binary watermark, each foreground pixel is doubly embedded by modifying the corresponding positive and negative wavelet coefficients of the original image according to the mapping functions: $b(x_{pos}, y_{pos}) = (x_i, y_i)$ and $b(x_{neg}, y_{neg}) = (x_i, y_i)$, where $b(x_{pos}, y_{pos})$ is the wavelet coefficient of positive position on the original image, $b(x_{neg}, y_{neg})$ is the wavelet coefficient of negative positions on the original image, and (x_i, y_i) is the position of a foreground pixel in a binary watermark. After the negative modulation, the absolute magnitudes of the modified wavelet coefficients become smaller, and if this value increases after an attack, its corresponding pixel does not belong to a binary watermark.

Original image varitication is considered extremely important in medical information system. In some watermarking schemes, the original image is required for extract watermarks from a watermarked image [9]. However, it is always preferable to retrieve watermarks without accessing the original image through the public communication networks[10]. We use a extra set of secret image instead of a secret key to retrieve watermarks without using the original images. It is reasonable to use secret images rather than the original images, because even if the secret image is intercepted, there will be no way to find out its contents. To generate the secret images, the result of image-dependent permutation mapping and the wavelet coefficients of the original image are combined. The image-independent permutation used in our approach is in the form of a mapping function shown in section 3.2. The mapping function is designed based on the significance of the wavelet coefficients, and it makes the security level raised because the watermarks are embeded into those components which have larger coefficients. Especially, these significant coefficients are more secure than the insignificant coefficients from the compression attacts. As the result, the proposed mechanism overcomes the quality and authentication problems of medical image verification simultaneously.

C. Experimental Results

For the proof of identifying fabricated medical images, following four steps are tested:

Step 1: A watermark is inserted into the original image (shown in fig 1).

Step 2: The watermarked image (shown in fig 4, which looks same as original image) is fabricated (shown in fig 5) on purpose.

Step 3: The fabricated image is studied from two radiotherapists and three residents of MRI laboratory in the university hospital.

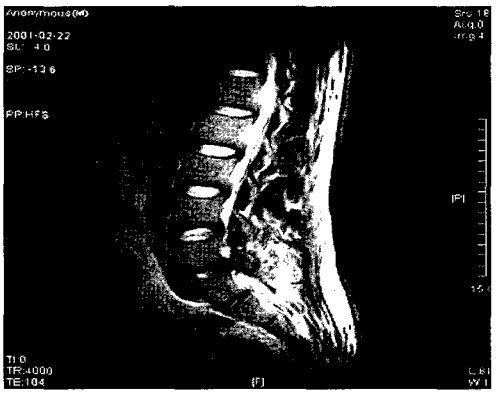

Fig 4. Original image with watermark

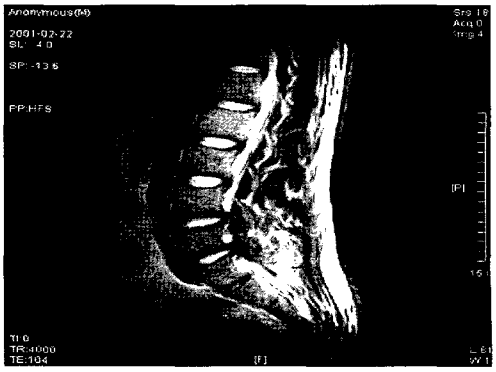

Fig 5. Fabricated image

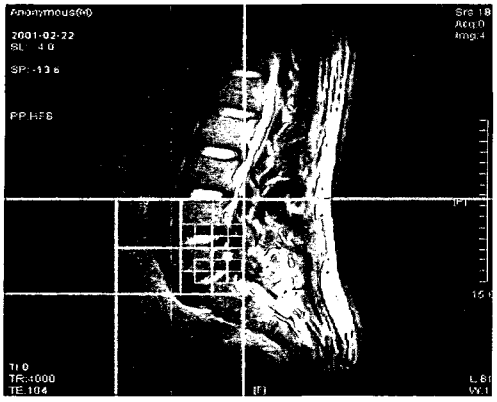

Fig 6. Fabricated image

Fig 7. Extracted watermark from fabricated image

Step 4: The watermark image is extracted (shown in fig 7) from fabricated image to identifying whether the image was fabricated or not.

The study result from step 3 mentioned above was either HID (Herniation of Intervertebral Disk) or Bulging Disc. However, as shown in fig 7, surgeons or radiotherapists can verify that the image was fabricated somewhere in the middle of the image as marked by blocks.

IV. CONCLUSION

Recently, the trade of PACS considers a scheme to apply protection mechanism like watermarking for transferring medical information on the public network to prevent medical information from fabrication or modification of medical data. There are mainly two points of views for applying the digital watermarking into medical image. One is to strengthening the security issues of PACS, and the other one is to waiting until the global standardization of medical information protection scheme on the communication channel is accomplished. In particular, the group who has opposite opinion insists the security issues of PACS is insignificance since the medical image could not be shared on the Internet or external communication channels at all.

However, for the assumption of convenience adapting IT and mobile communication technology into medical information system, it is obvious that real time online retrieving of medical information will become reality soon. Thus, it is very important to presuppose and preventing the counter measurement of the problems of security issues, which can possibly occurred from transferring the medical information on the public communication channels. We provide a mechanism for varifying medical images from the malricious attacks by using the secret image authentication. Hereafter, the secured transmission scheme of the medical image on the mobile communication network should be studied seriously.

ACKNOWLEDGMENT

We are grateful to surgeon Dr. C. H. Jeung from the neuro-logical department of Wooil Hospital in Gwangju, who examine and compare the medical images that were fabricated intentionally. We also want to thank two radiotherapists and three residents of C university MRI laboratory in Gwangju.

REFERENCES

[1] Wayne T. Dejarnette, "Web Technology and its Relevance to PACS and Teleradiology," Applied Radiology, August 2000.

[2] DICOM (Digital Imaging and Communications in Medicine), Part 1~15(PS3.1-2001~PS3.15-2001), Published by National Electrical Manufacturers Association, 1300 N. 17th Street Rosslyn, Virginia 22209 USA, 2001 at http://medical.mena.org/dicom/2003.html

[3] J. J. Eggers, J. K. Su, and B. Girod, "Performance of a practical blind watermarking scheme," *in Proc. of SPIE* Vol. 4314: Security and Watermarking of Multimedia Contents III, (San Jose, Ca, USA), January 2001.

[4] I. J Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Trans. Image Processing*, Vol. 6, pp. 1673-1687, 1997.

[5] C. I. Podilchuk and W. Zeng, "Image-Adaptive Watermarking Using Visual models", *IEEE Journal on Selected Areas in Communications,* Vol. 16, pp. 525-539, 1998.

[6] Minerva M. Yeung & Sharath Pankanti, "Verification Watermarks on Fingerprint Recognition and Retrieval", Proc. of SPIE Conference on Security and Watermarking of Multimedia Contents, P.W Wong and E.J. Delp (eds), Vol. 3657, San Jose, January 1999.

[7] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "Copyright Protection of Digital Images by Embeded Unperceivable Marks", *Image and Vision Computing*, Vol. 16, pp. 897-906, 1998.

[8] A. Z. Tirkel, C. F. Osborne and T. E. Hall, "Image and Watermark Registration", Signal Processing, Vol. 66, pp. 373-384, 1998.

[9] J.Eggers and B. Girod, "Blind Watermarking Applied to Image Authentication", *in Proc. IEEE ICASSP*, Salt Lake City, UT. May 2001.

[10] C.-S Lu and H. Liao, "Multipurpose watermarking for image authentication and protection", *in IEEE Trans. Image Processing, 2001*, vol. 10, pp. 1579-1592.

Kuan-Tak Oh
Recevied B.S. degree in Donshin university, Gwangju, korea in 1998. Since 2004 to now, he has been M.S student in multimedia Lab, Electronics & Information Engineering, chosun university, Gwangju, korea. The mobile & Information security.
Mr Oh is member of the KIMICS.

Yung-Ho Kim
Recevied B.S. degree in kwangju university, Gwangju, korea in 1989. Since 2004 to now, he has been M.S student in multimedia Lab, Electronics & Information Engineering, chosun university, Gwangju, korea. The mobile & EC.
Mr Kim is member of the KIMICS.

Yun-Bae Lee
Recevied B.S. and M.S degree in Computer Science from kwangwoon University in 1983 and in 1985 and Recevied Ph.D degree in Computer Science from Soongsil University in 1993.
He has published more than 100 paper in journals and conferences and has filed more than 26 industrial property .
He is a Member of KIMICS, KIPS, KISS, IEEK .
Since 1992, has been a professor in the department of compuer science, Chosun University, Korea.