INTEGRITY AND AUTHENTICITY OF QUALITY ASSURANCE AND CONTROL IN AN IMAGING EXAMINATION WORKFLOW

Chung-Yueh Lien
Institute of Biomedical Engineering, National YangMing University
No. 155, Sec. 2, Linong st., Beitou District, Taipei 112, Taiwan

Chia-Hung Hsiao
Department of Medical Informatics, TzuChi University, Hualien City, Taiwan

Tsung-Lung Yang
Department of Radiology, Kaohsiung Veterans General Hospital, Kaohsiung City, Taiwan

Tsair Kao
Department of Biomedical Engineering, Hungkuang University, Taichung, Taiwan

Keywords: Security, DICOM, Digital Signature, Key Object Selection, Modality Performed Procedure Steps, PACS.

Abstract: In this paper, we evaluated the implementation of a digital signature for medical imaging quality assurance and control (QA/C) by a technician in accordance with the Digital Image and Communication in Medicine (DICOM). After QA/C, a set of DICOM images were collected into a DICOM Key Object Selection (KOS) document with digital signatures. The digital signature was implemented by RSA public-key cryptography combined with a public-key health certificate and health professional card (HPC) to digitally sign a series of DICOM images. Our method includes the DICOM Modality Performed Procedure Steps (MPPS) mechanism that assures the image transmission completeness and accuracy in an image examination workflow. The results show that the method is more efficient and requires less loading time to create the technician's signature in an imaging examination workflow.

1 INTRODUCTION

In the past decade, many institutions have accommodated the increased variety of imaging modalities and their communication protocols in accordance with Digital Image and Communication in Medicine (DICOM) to create a filmless environment. Medical imaging quality assurance and control (QA/C) is a key factor for a high-quality filmless medical environment. Ensuring quality of services for medical image transmission among modality, QA/C station, and image archive has become an important issue. The DICOM storage commitment service allows the modality to verify that images have been sent to an image archive before deleting the images locally. Image loss can happen when a technician does not check to see whether the image has been sent to the QA/C site. With the DICOM Modality Performed Procedure Step (MPPS) service, the image transmission completeness and accuracy in an imaging examination workflow are assured (Moore 2003; Noumeir 2005). Physicians will have more confidence in using a picture-archiving and communication system (PACS) with MPPS.

Security protection is a necessary requirement in a filmless environment. DICOM has also adopted public-key cryptography for protecting medical images transmitted in PACS (ACM-NEMA 2009; Schüze et al. 2004). Based on public-key infrastructure (PKI), mechanisms needed to comply with medical information security regulations could

Lien C., Hsiao C., Yang T. and Kao T. (2010).
INTEGRITY AND AUTHENTICITY OF QUALITY ASSURANCE AND CONTROL IN AN IMAGING EXAMINATION WORKFLOW.
In *Proceedings of the Third International Conference on Health Informatics*, pages 155-158
DOI: 10.5220/0002689501550158
Copyright © SciTePress

be implemented (Brandner *et al.* 2002; Cao *et al.* 2003). In PACS, digital-signature technology can be implemented to assure the integrity of medical images and to authenticate the operators in the workflow of medical image examination (Brandner *et al.* 2002). The report showed that the use of a digital signature can reduce time needed for reporting, thereby increasing efficiency (Lepanto *et al.* 2003).

DICOM defined a specific instruction regarding digital signatures in DICOM Part 15: Security and System Management Profiles (ACM-NEMA 2009). However, most digital signatures deal only with single images and do not provide a satisfactory solution for multiple images (Kobayashi *et al.* 2009). The DICOM Supplement 86 offered a solution by creating the digital signature in structured reports (SR) with selected images. In this paper, we propose a novel approach to assuring the integrity and authenticity of QA/C in an imaging examination workflow. Using the MPPS mechanism, the QA/C site receives a complete set of DICOM images created from a certain modality and creates a signed key object selection (KOS) document with secure references to all of the DICOM images that comprise the examination.

2 METHODS

A general description of a modality acquisition system consists of modality, QA/C site, MPPS manager, and image archive (Figure 1). The modality receives an imaging request from the modality worklist server. After imaging, the modality generates an MPPS list and then forwards the list to the MPPS manager. The MPPS manager uses the list to record the status of each modality. The QA/C site receives the images transmitted from modality and checks the MPPS status to assure that the transformation of images has been completed. A technician can manually read and adjust the examination data such as the number of images, and the window level at the QA/C site.

Figure 2 shows the flowchart of the digital signature of the DICOM KOS document by technician at the QA/C site. A DICOM KOS document consists of the signed information of all images, and the QA/C technician will digitally sign the DICOM KOS document with the QA/C signature. If images are transferred completely, the image archive will update the MPPS status to the MPPS manager as “COMPLETE,” and the MPPS status of modality also will be updated; images are deleted from the cache of modality consequently. The mechanism of MPPS ensures the completeness of image transmission. After transmission is complete, the technician creates the QA/C digital signature for the QA/C result. The images and signatures are forwarded to the image archive.

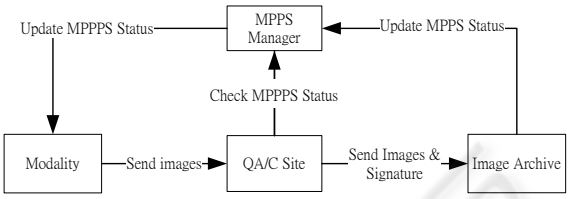

Figure 1: System overview.

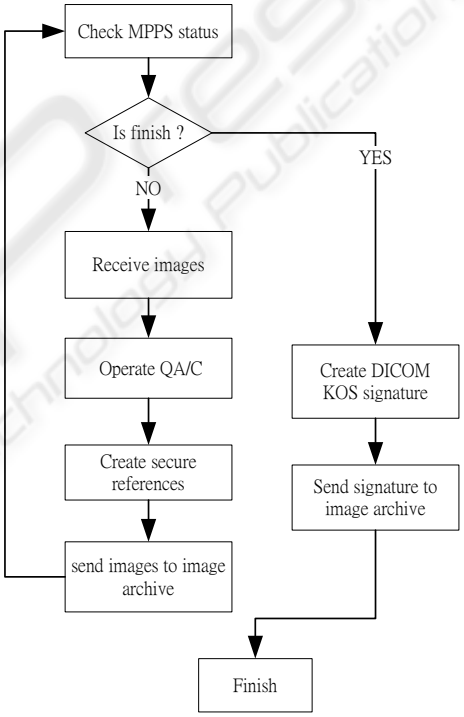

Figure 2: The block diagram of a DICOM KOS document generation that is digitally signed by technician at the QA/C site.

2.1 Digital Signature of DICOM KOS Document

After the QA/C site receives all of the images from the modality, the MAC (message authentication code) references of all of the images are also collected into a set of DICOM data objects in a DICOM KOS document. In order to increase the signing performance at the QA/C site, we did not directly sign all images, but we indirectly signed a DICOM KOS document, which also protects the

data integrity. The DICOM KOS document contains multiple MAC references (Figure 3). The MAC reference contains four attributes that represent signed information for each image: 1) MAC Calculation Transfer Syntax UID presents the encode type of MAC; 2) MAC algorithm presents the algorithm used in generating the MAC; 3) Data Elements Signed presents a list of data element tags in the order they appear at the top level of the referenced image to identify the signed range; and 4) the MAC presents the digest value of the referenced image. The digest value is calculated by a hash function that creates a "digital fingerprint" of an image. The DICOM supports three hash algorithms: RIPEMD-160, MD5, and SHA-1.

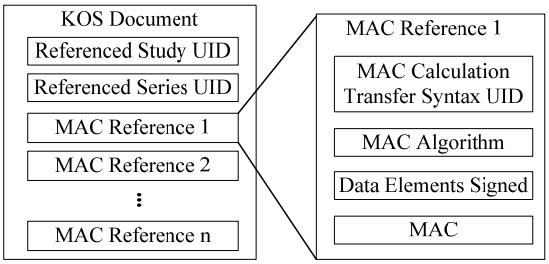

Figure 3: The architecture of a DICOM KOS document containing *n* MAC references.

2.2 Data Elements Signed

The attribute "Data Elements Signed" is used to select the range data elements to be included with the image before signing. In accordance with different departmental policies and roles, the data elements signed attributes can be adjusted and well-defined, creating a customized information base designed by each institution using the DICOM digital signature system. Only the selected data elements are created or modified by the signer according to his/her responsibility.

3 RESULTS

For this evaluation, all attributes of a DICOM-formatted image were selected to be included in the digital signature. The hash algorithm is SHA1 with a 160-bit output. The digital signature was implemented by RSA public-key cryptography combined with a public-key health certificate and health professional card (HPC). The result of MAC calculation was stored as a MAC Parameters Sequence (4FFE, 0001), and the digital signature was stored in as a Digital Signature Sequence (FFFA, FFFA), as defined in DICOM part 15.

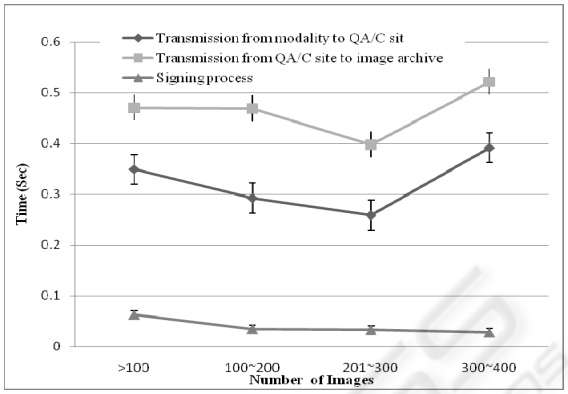

Figure 4: Time required per image for image transmission among modality, QA/C site, image archive, and signing process at the QA/C site.

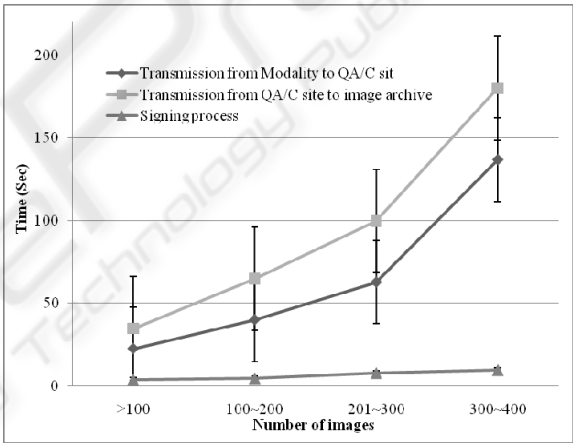

Figure 5: Time required per exam for image transmission among modality, QA/C site, image archive, and signing process at the QA/C site.

Fifty-three CT examinations were recorded at the QA/C site. The number of images for each examination ranged from 30 to 394. Two CT scanners (Toshiba Aquilion 64 and Siemens Sensation 16) support MPPS and automatic DICOM transfer. The image archive was installed on a PC in the department of radiology. All stations were connected via 100 MB-based Ethernet to the PACS.

Figure 4 illustrates the time required per image for image examination. Figure 5 illustrates the time dependence on the number of images in an examination. We calculated the percentage of time spent on each transition in an imaging examination workflow. The average percentage of signing time was 5.12±1.73%; transmission from modality to QA/C site was 38.55±10.22%; and transmission

from QA/C site to image archive was 56.33±10.57%, respectively.

4 DISCUSSION

The delivery time of images is an important issue in the department of radiology. Several steps are involved: The images are created by a modality and the image is transferred to the QA/C site. The technician performs QA/C of the images, combines the images with the study, then sends the images to be stored to the image archive. The introduction of digital signatures should avoid much extra loading time in a normal workflow. Although the signing time increases depending on the number of images, the percentage of time spent loading is still less. The impact of digital signatures in an imaging examination workflow was significant in our evaluation.

The implementation of digital signatures in DICOM is not yet widespread. The main reason is that the public-key infrastructures are not well accepted in the domain of healthcare. Several hospitals have followed the DICOM security profile to sign medical images in their systems. However, it is difficult to use the recommended DICOM signature specification in the workflow of image examination. It is not necessary to sign each image in a study, which reduces the signing time. Specifically, the technician can sign only one image using DICOM KOS document while inserting secure references into all of the DICOM images that comprise one examination. The results of the present study show that this method is more efficient and requires less loading time to create the technician's signature.

5 CONCLUSIONS

In PACS, the security protection of medical images is very important. Although the DICOM regulates the digital signature for a single image, it can be improved for implementation in an imaging examination workflow. The implementation of digital signatures for QA/C by a technician following the DICOM Supplement 86 with MPPS mechanism offers a satisfactory solution for multiple images. These results show that this method is more efficient and requires less extra load to create the technician's signature.

ACKNOWLEDGEMENTS

This work was supported by the National Science Council of Taiwan under Grant NSC 97-2114-E-010-002. The authors would like to acknowledge the technical support provided by Mr. Wei-Chung Chen of Department of Radiology, Kaohsiung Veterans General Hospital.

REFERENCES

ACM-NEMA, 2009. Digital Imaging and Communications in Medicine [online]. Available from: http://medical.nema.org/dicom/ [Accessed 11 July 2009].

Brandner, R., M. Van der Haak, et al., 2002. Electronic signature for medical documents - Integration and evaluation of a public key infrastructure in hospitals. *Methods of Information in Medicine* 41(4), 321-330.

Cao, F., H. K. Huang, et al., 2003. Medical image security in a HIPAA mandated PACS environment. *Computerized Medical Imaging and Graphics* 27(2-3): 185-196.

Kobayashi, L., Furuie S., et al., 2009. Providing Integrity and Authenticity in DICOM Images: a Novel Approach. *IEEE Transactions on Information Technology in Biomedicine* 13(4), 582-589.

Lepanto, L., 2003. Impact of Electronic Signature on Radiology Report Turnaround Time. *Journal of Digital Imaging* 16(3), 306-309.

Moore, S. M., 2003. Using the IHE Scheduled Work Flow Integration Profile to Drive Modality Efficiency. *Radiographics* 23(2), 523-529.

Noumeir, R., 2005. Benefits of the DICOM Modality Performed Procedure Step. *Journal of Digital Imaging* 18(4), 260-269.

Schüze, B., Kroll, M., et al., 2004. Patient data security in the DICOM standard. *European Journal of Radiology* 51(3), 286-289.