Watermarking in Regional Medical Imaging

MICHAL JAVORNIK, OTTO DOSTAL
Institute of Computer Science
Masaryk University
Botanicka 68a, 602 00, Brno
CZECH REPUBLIC
javor@ics.muni.cz, otto@ics.muni.cz

ALES ROCEK
Faculty of Electrical Engineering and Communication
Brno University of Technology
Technicka 3058/10, 616 00, Brno,
CZECH REPUBLIC
xrocek00@stud.feec.vutbr.cz

Abstract: Today's rapidly evolving distributed business environments in medical imaging are enhancing the quality of healthcare, but are also introducing significant patient safety and security challenges. In this paper we focus on securing of regional medical image processing through the combination of reversible-RONI (Region of Non-Interest) watermarking and utilizing of asymmetric encryption scheme. Watermarking is introduced as a complementary mechanism for enhancing the medical image security. We propose a concept of complex image security implemented as a set of features of Radiological Communication System ReDiMed, implemented at Masaryk University, Brno, Czech Republic.

Key-Words: Watermarking, Picture Archiving and Communication in Medicine, Telemedicine, Medical Imaging, Information Security.

1 Introduction

Sharing of medical knowledge, sharing of accurate sources of information, close cooperation using tools supporting or assisting in decision making, all play a very important role in healthcare, enhance the synergy among the medical community and consequently brings benefits to all people.

Traditional medical image data processing is mostly organised within the scope of one healthcare institution. Secure medical image workflows are currently limited to the private computer networks of individual healthcare institutions. But current requirements in this area are mobility, flexibility of provided medical services and especially global cooperation.

The goal of this article is to present an integration concept how to support regional and national cooperation in the area of processing of medical image data, how to integrate independently provided medical services, how to share an expensive medical facilities or medical specialists, how to make diagnostic process more efficient, etc.

This article describes an advanced system developed at the Institute of Computer Science, Masaryk University, Czech Republic [1], [2], [3]. The system enables full communication among relevant applications and individuals from remote institutions.

Conventional hospital clinical information systems do not support functionalities enabling medical specialists to deliver particular services via the computer network. This concept is known as telemedicine and is based on distant expert centres or specialised medical departments providing services like for instance consultations of urgent cases. Practises of telemedicine bring higher quality as well as higher economic efficiency. For example in the area of medical imaging the image studies can be referred to distant healthcare institution for a diagnostic, second opinion or consultation.

2 Medical Imaging

Processing of medical image data is almost exclusively based on international communication standard DICOM (Digital Image Communication in Medicine). The standard enables interoperability between medical devices and applications of the different manufacturers. DICOM communication protocol works over TCP/IP layer.

The term PACS (Picture Archiving and Communication System) means a system for streamlining of distribution of image studies (patient examination) throughout the healthcare enterprise. It enables delivering of medical images, delivering of structured reports describing the medical findings as well as other relevant information. As an important component of hospital information system, all PACS communication interfaces are supposed to be fully compatible with DICOM standard.

Effective usage of PACS technology means distribution of processed information at the scope of at least the whole healthcare enterprise. The best way how to utilize all of the advantages of PACS

ISBN: 978-1-61804-355-9

technology is its implementation at the regional or national level.

The regional implementation of PACS technology is in accordance with the concept of electronic patient record. The electronic patient record is defined as a systematic collection of electronic health information about patient. It gradually brings quite new quality into healthcare. It means that healthcare professionals are able to retrieve or update (according to individual access rights) all the necessary information about their patients originating from a variety of hospital information systems. There are many legal and organizational barriers to overcome when implementing this concept. One of the basic steps towards the concept of electronic patient record is secure regional medical imaging.

3 Security Considerations

Today's rapidly evolving distributed business environments in medical imaging are enhancing the quality of healthcare, bud are also introducing significant patient safety and security challenges. The distributed business in the area of medical imaging covers especially image interpretation or second opinion, services like long-term storage of image data, research and education activities utilizing huge databases of medical images, etc.

The solution must provide remote access to data and information for those who need it, from where it is necessary, 24 hours a day, 7 days a week. Simultaneously, all the patient data need to be secured. Distributed system must maintain legitimate access (according to applicable law regulations), enable monitoring, reporting and auditing as well.

It means the expansion of security perimeter outside the environment of an individual healthcare institution. So, traditional security measures (conventional network security protections) like firewalls, intrusion detection, etc., are there no longer applicable. We are going towards an environment providing progressive communication methods between remote healthcare providers (hospitals, clinics, physicians working off-premises), universities and other research/education centers as well.

Applied security measures cannot complicate the continuity of critical healthcare functions, cannot complicate access to critical data. The access for authorised physicians and people who have a professional need, to protect patient health, must be as easy as possible.

4 Watermarking & Medical Imaging

The general idea of digital watermarking is to hide a known watermark (information) into source data and consequently be able to extract this hidden information. In this application domain any permanent distortion of the medical image, or at least of any of its critical parts, is not acceptable. We must be able to insert and then extract the watermark without loss of any information.

The extracted watermarks (embedded information) must be easily identified by human eyes. The protection mechanism must be accomplished without modifying any of the critical parts of the original image. The protection scheme must effectively resist common image processing operations.

In this paper we focus on securing medical image information through the combination of reversible-RONI (Region of Non-Interest) watermarking and asymmetric encryption. Watermarking is thus introduced as a complementary mechanism for enhancing the medical image security.

The principle of reversible watermarking is based on insertion of the watermark data into source image the way that the source image can be, if necessary, reconstructed into original quality. Generally, the differential information generated during this process and enabling the reconstruction of the original image (removing the watermark) afterwards, is supposed to be transmitted/stored via another secure channel. Alternatively, we can use the RONI area of source image to hide this information and then employ secret algorithm to completely restore the original medical image at recipient‘s side [4]. One of the most significant reversible watermarking techniques is described in [7], [8].

The main advantage of so called zero watermarking, as a complementary mechanism, is that no source data is modified. It means zero distortion of ROI (Region if Interest) area of the medical image (no effect to the patient's diagnosis). As the ROI area is unchanged, the correct diagnostic process is also possible without extraction of the watermark.

So, applying the zero watermarking to the most valuable ROI area, while incorporating patient demographic information and other important image related data, links all the most critical data together. The final watermark is then inserted into RONI area.

ISBN: 978-1-61804-355-9

5 Radiological Communication System

Radiological Communication System ReDiMed, implemented at Masaryk University, creates the opportunity to transfer highly sensitive patient image data between secured PACS environments of distant medical institutions or directly between two DICOM compatible medical devices via open Internet. System ReDiMed consists of central servers located at the Masaryk University and components on the client side (security gateways) deployed inside private networks of involved medical institutions. The security gateways are equipped with DICOM communication interface and represent standard DICOM nodes within DICOM application domain of the institution.

Security gateway represents the interface to the services provided by the remote hospital or by other institution dealing with some kind of processing of medical image data. Security gateway has two communication interfaces. One interface is used for communication with the local applications, the second interface communicates with the central communication node of the system ReDiMed. The communication between security gateways, through the central communication node, is generally supposed to go over an insecure computer network like the open Internet. These transfers are always protected by asymmetric encryption scheme.

Asymmetric cryptography is commonly used to assure confidentiality (preserving authorised restrictions on information access), integrity (guarding against improper information modification) and authenticity (verifying the identity of the patient, acquisition modality or institution).

The above described communication system supports simple workflows as well as quite complex solutions like distribution of medical images through the whole region. These days it enables secure communication of more than 400 healthcare institutions and medical specialists mostly from the Czech and Slovak Republic.

6 Image Centric Security

We propose a concept of complex image security supposed to be implemented as a set of features of the above described regional system for secure exchange of medical images. The image centric approach enables permanent assurance of the images being processed outside of the protected PACS environments of particular healthcare institutions. It enables secure transfer of medical images and image related data among secured environments and supports additional image manipulation as well.

In the proposed protection scheme there are two basic procedures necessary to implement: the ownership share generation and the ownership verification. Revelation of the hidden watermark and performance of the ownership verification procedure is supposed to be done when a dispute over the host image arises [8], [9], [10], [11], [12].

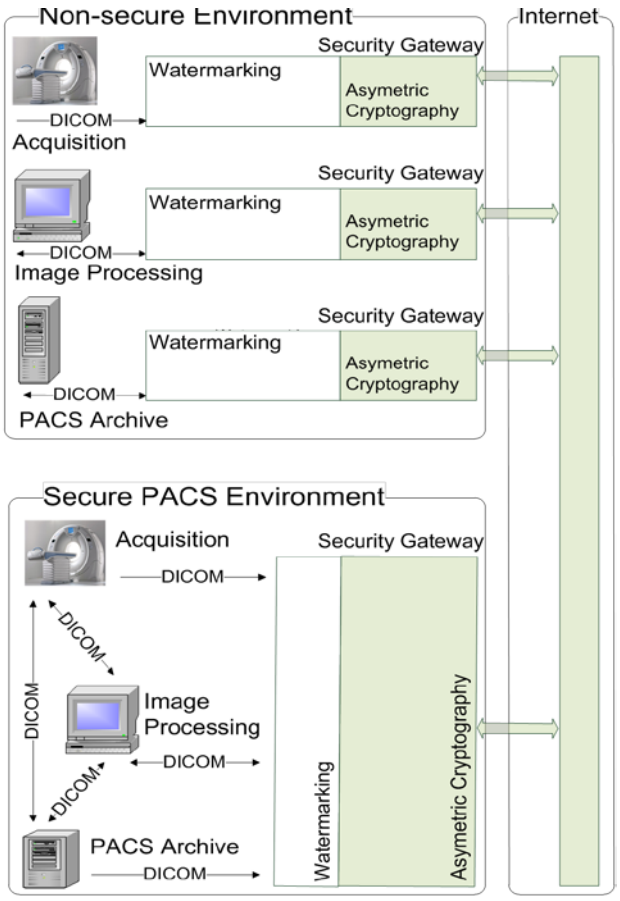

Fig. 1. Medical imaging in regional environment

Watermark services available at the sender side:

- Detection (automatic or semiautomatic) of critical parts of the image (parts carrying information necessary for diagnosis). It means identification of ROI and RONI areas. In practice, there are many methods for automatic RONI selection [5], [6].
- Applying the zero watermarking method to the ROI area and incorporating the important image related data (patient information, the institution where the image was processed, referring physician or the author of the image interpretation, etc.).
- Embedding the watermark into RONI area of the image, employing reversible watermarking scheme.

ISBN: 978-1-61804-355-9

Services available at the receiver side:
- Integrity verification after transmission via internet (asymmetric encryption scheme) or anytime during the image processing (watermarking scheme).
- Authenticity verification (whether incorporated data belongs to the right patient, whether the data comes from the right healthcare institution, the authorship of diagnose description, etc.).
- Full restoration of the original image (for some procedures it could be required).

The scheme, depicted in Fig. 1, describes two possible scenarios of the watermarking usage. The first one assures data protection in within the healthcare institution environment. Medical image generated at acquisition modality, before archived, goes through the security gateway, where the watermark is inserted. This way the watermark links together the critical part of the image with the relevant patient and imagesource identification at the initial stage of the image lifecycle.

The second scenario assumes that the whole image processing over the internal institution network is secure and the protection mechanism comes only when the communication extends over the internet. The asymmetric cryptography (to assure the confidentiality and integrity during transmission of images between institutions) is mandatory in both cases.

The security gateways (providing a user interface) of communication system ReDiMed, can upon request check the integrity and origin of the image. These components are incorporated into secure PACS environments of the particular institution interconnecting the individual image security domains.

7 Knowledge Management

Watermarking plays an important role also as a verification mechanism in research and education: the ownership of a medical image study, verification of informed consent for research purposes, etc.

For radiological training (to become an excellent radiologist), as well as for research purposes, it is necessary to have an access to a large knowledge database of case studies. A case study forms a basic didactic unit consisting of structured information about real patient: image data (radiological images, pathology images, video recordings, demonstrations from surgeries, data from nuclear medicine, etc.) and other relevant clinical information. Personal data involved in image studies as well as in other related files are modified, patients are made anonymous. As the patient can be treated in many healthcare institutions, the coordinated modification of his/her identity (replacement with fictitious one) is necessary. We need to prevent disclosure of his/her identity as well as not to lose complex view of a particular case, even if the patient is being treated in different hospitals. The principle of fictitious identity removes the legal barriers preventing usage of confidential and highly sensitive patient data in the area of research and for education in medical faculties as well.

8 Conclusion

This paper describes the scheme of secure regional medical image processing through the combination of reversible-RONI watermarking and asymmetric encryption. Watermarking is introduced as a complementary mechanism for enhancing the medical image security.

Much more important, than employed technology, is growing network of radiologists and other medical specialists. As they use our secure network and secure applications, they change their traditional thinking, cooperate in the regional level, share data and information about their patients, etc.

Radiological communication system, implemented at Masaryk University, enables secure communication of more than 400 healthcare institutions. The capacity of fast accessible long term medical archive located at the Masaryk University is more than 200TB of image studies. Shared knowledge database of interesting case studies serves not only for education of medical students and young radiologists but also enables much more effective decision making during medical routine.

References:

[1] A. Rocek, M. Javornik, Securing a Publicly Accessible Database of Medical Images Using Watermarking with Direct Diagnosis Capability. *In: Proceedings of the 13th International Conference on Applications of Computer Engineering (ACE 2014)*. WSEAS Press 2014, pp. 97-86, ISSN 1790-5109, ISBN 978-960-474-393-3.

[2] O. Dostal, M. Javornik, K. Slavicek, Integration of Telemedicine Activities in the Czech Republic. *In: Proceedings of the 4th International Conference on Innovations in Information Technology*. UAE University, 2007, ISBN 978-1-4244-1841-1.

[3] M. Javornik, K. Slavicek, O. Dostal, Integration Concept in Regional Medical Imaging. *International Conference on Computer Engineering and Bioinformatics (ICCEB 2013), IACSIT Press*, 2013, pp. 26-31, ISSN 2010-4618.

[4] Ch.K. Tan, J.Ch. Ng,X. Xu, Ch.L. Poh, Y. L.

Guan, K. Sheah, Security Protection of DICOM Medical Images Using Dual-Layer Reversible Watermarking with Tamper Detection Capability, *Journal of Digital Imaging*, vol. 24, No 3, 2011, pp. 528-540.

[5] F. Rahimi, H. Rabbani, A dual adaptive watermarking scheme in contourlet domain for DICOM images, BioMedical Engineering OnLine 2011, http://www.biomedical-engineering-online.com/content/10/1/53.

[6] O.M. Al-Qershi, B.E. Khoo, Authentication and Data Hiding Using a Hybrid ROI-Based Watermarking Scheme for DICOM Images, *Journal of Digital Imaging*, vol. 24, No 1, 2011, pp. 114-125.

[7] J. Tian, Reversible data embedding using a difference expansion, *Circuits and Systems for Video Technology*, 2003, vol. 13, no. 8, pp. 890-896.

[8] A. Alattar, Reversible watermark using difference expansion of triplets, In: *Image Processing*, 2003. ICIP 2003, vol. 1, pp. 14-17.

[9] A.H.Abusitta, A visual cryptography based digital image copyright protection, I*n Journal of Information Security*, 2012, vol. 3, pp. 96–104.

[10] S.C. Tai C.C. Wang and C.S. Yu, Repeating image watermarking technique by the visual cryptography, *in IE-ICE Trans. Fundamentals*, August 2000, vol. E83-A(8), pp. 1589–1598.

[11] B. Surekha and G.N. Swamy, Sensitive digital image watermarking for copyright protection, *In International Journal of Network Security*, January 2013, vol. 15(1), pp. 95–103.

[12] A. Sleit and A. Abusitta, A Visual Cryptography Based Watermark Technology for Individual and Group Images Systemics, Cybernetics and Informatics, 2006, vol. 5(2), pp. 24-32.

[13] S. Radharani and M.L. Valarmathi, Multiple Watermarking Scheme for Image Authentication and Copyright Protection using Wavelet based Texture Properties and Visual Cryptograph, In *International Journal of Computer Applications*, 2001, vol. 23(3), pp. 29-36.

ISBN: 978-1-61804-355-9