Security in Teleradiology: watermarking and electronic signature

ICT and Medical Image Computing Group:

A.Beux(2), P.Bianco(7), P.Boggiatto(6), R.Borri(3), R.Caldelli(8), T.Cammarota(2), D.Cavagnino(5), M.Collura(7), R.De Paoli(7),A. Del Bimbo(8), M.Grosso(2), M.Lucenteforte(5), L.Mantovani(7), D.Minniti(2), A.Oliaro(6), G.Pagana(2), A.Panzica(2), G.Pescarmona(4), S.Pero(3), R.Picco(7), F.Pollastri(7), F.Ricchiuti(3), S.Sagliocco(3), F.P.Sellitti(2), R.Servetto(1), A.Vernone(4), A.Veronesi(2);
(1)ASL2 Alba-BraTorino
(2)Azienda Ospedaliero Universitaria San Giovanni Battista Torino
(3)CSP Piemonte
(4)Dipartimento di Genetica Biologia e Biochimica dell'Università di Torino
(5)Dipartimento di Informatica dell'Università di Torino
(6)Dipartimento di Matematica dell'Università di Torino
(7)INRIM-CNR Istituto Nazionale di Ricerca Metrologica Torino
(8)MICC - Media Integration And Communication Center-Firenze

1. ABSTRACT

The article proposes a scheme to ensure the authenticity, integrity and privacy of a radiographic image in Dicom format which is transmitted through a generic transmission channel.

The scheme involves the combined use of techniques of digital signature and fragile and reversible watermarking in order to include in the original image the patient data and the signature data.
The use of reversible watermarking allows to extract the original X-ray image for the medical diagnosis.

2. INTRODUCTION

The diffusion of telemedicine and home care is giving rise to a progressive change in the supply of services related to patient management [1].

Services which allow to check patient data in real time are requested more and more. It means that it is necessary to work in a secure, fast, reliable and anonymous way, particularly for the sensitive data. All these aspects open security issues, in particular using Web or E-mail.

However, E-mail and Web allow the sharing of the digital radiographic images and the related patient data quicker and more effectively and, at the same time, speed up the procedures to submit material for medical report.

The safety aspects include: authentication, compliance testing, guarantee of privacy for sensitive data.
Through the hashing techniques and digital signature it is possible to ensure authenticity and verify the integrity of digital image transmitted while identifying both any random errors and malicious attack.

The signature, the data control and any patient data can be inserted in the image header, but the disadvantage is that this is easily readable and editable by using appropriate software tools. Furthermore, the image header depends strictly on the format.

Watermarking techniques [2], on the contrary, allow to embed such data in the image in an invisible, not separable from the image itself, and reversible way.

3. MEDICAL IMAGE WATERMARKING

Watermarking techniques generally realize a compromise between the capacity of the watermark (number of bits of information that it is possible to insert in the image), robustness / fragility, imperceptibility of the watermark and privacy (that is the information contained in the watermark).

The greater increases the watermark strength the greater increases the image noise. The artifacts produced by the algorithm become more visible. So, what we try to achieve, is a good compromise between strength and invisibility.

In particular, for medical applications, we have to preserve integrity of digital image and so, the watermark must be fragile [4].

The robust watermark [5] is used for applications where it is necessary to preserve the integrity of the watermark against several attacks, for example geometric attacks.

For medical applications, on the opposite, we want to preserve the integrity of the digital image, and so the watermark has to be corrupted or not recoverable also with minimum changes of the digital object.

If the watermark is corrupted, we can say that the digital object was somehow altered and therefore it is no longer reliable for a possible diagnosis.

The reversibility [6] requirement comes together with fragility requirement.

The reversibility indicates that it must be possible to reconstruct the original object from the watermarked one. The reconstructed image may be used for diagnosis.

The watermark creates an imperceptible noise on the digital image that has to be completely removed from digital image.

4. THE METHOD

The radiographic images follow the standard Dicom which provides the unique association between the patient information and the related image.

Watermark is the message which may contain the patient data joined with radiographic investigation (for example the department and the examination date). These information are embedded into the pixels of the image and are invisible to human eye.

The message embedded is not readable or recoverable even if it is present in the pixels. This process has to be reversible [5] as it must be possible to recover the original X-ray image for medical diagnosis.

The message, for privacy reasons, contains the patient unique identifier and possibly, the exam unique identifier. It is possible to retrieve, at any time, the patient data from these unique identifiers. It is possible to send the single watermarked image and to retrieve the patient data or the examination data, using the recover procedure to retrieve the watermark. In the next section we will see the embedding procedure and the recover procedure in detail.

In the case we are analyzing the watermark is fragile [7] because the minimum alteration of the digital watermarked image make impossible the extraction of the watermark and so the patient data included in the watermark are not recoverable. This guarantees in case of malicious attacks or unintended changes.

The proposed scheme covers the combined use of the digital signature techniques and the fragile and reversible watermarking to embed the patient data and the digital signature in the original image.

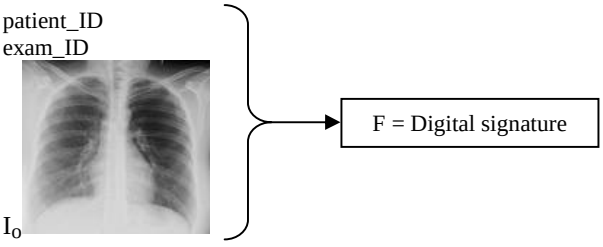
4.1 Generation of the watermarked and signed image

The embedding procedure can be summarized as follows:

1.Generation of uncompressed digital X-ray image in Dicom format.

2.Generation of the digital signature using private key. The digital signature is computed on the digest of the Dicom image join with patient_ID and exam_ID (Fig. A)

[Fig A] Electronic signature generation



As far as the RSA digital signature is concerned, the signature length is the same as the keys length used. Typically, key length is 1024 or 2048 bits.

3.Watermark generation composed by: signature data + patient_ID + exam_ID.

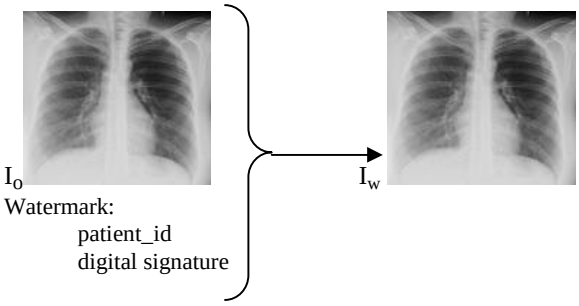
4.Watermark embeddig in the original Dicom image (Fig. B).

5.Storage of the Dicom Watermarked image.

At the end of the embedding phase, we obtain the digital watermarked and signed image. At any time we can reconstruct the original X-ray image starting from watermarked image.

A further possible compression step makes the watermark unreadable and the reconstructed original image not reliable.

[Fig. B]



4.2 Detection phase of the watermarked and signed image.

The steps for recovering the original image, the watermark and the signature are the following:

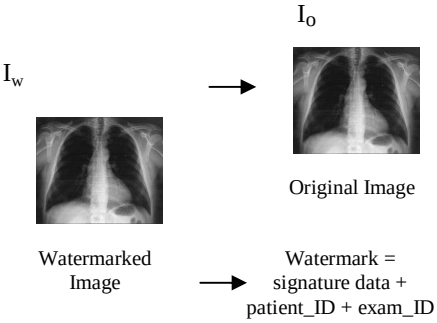
1. Watermark extraction starting from the uncompressed watermarked Dicom image.

2. Digital signature extraction and check by using the public key starting from the watermark. The digital signature extracted is related to the digital image, the patient_ID and the exam_ID.

3.Recover of the original image, the patient_ID and the exam_ID only if the step 2 tested positive.

Otherwise, the image may have been attacked and it cannot be considered reliable.

[Fig. C] Recover



By step 3 of the embedding phase, we can guarantee privacy as the only patient image is transmitted while the patient data are hidden within the image itself.
The digital signature is generated through the private key computed on the digital image as well as on the patient data.

Afterwards, along with the patient data, it is inserted by the watermark.

During recovery phase, the watermark is extracted and the signature here contained is verified by the public key. Such procedure enables to check authenticity and the integrity of both the image and the patient data.

By using the reversibility technique to reconstruct original image for a diagnosis.

5. CONCLUSION

Nowadays, is under development, an algorithm wich executes a redundant watermarking on Dicom radiographic images.

The algorithm is fragile and reversible.

It divides the image into blocks and embed the watermark and the signature information using a appropriate grid and some correlation functions.

The payload generated is large enough to save in the image not only watermark, signature data and ID, but any other data, such as diagnosis.

The recover phase, using statistics functions, finds the watermark and starting from this, the signature data and the data connected with the image. In this phase we can reconstruct also the original image.

In case of geometric attacks, or simple pixels deletion, it is no more possible to recover the watermark or the digest message anyway.

So it is not possible to generate false positives because the check is executed on whole image.

In this first phase, the algorithm will be tested on Dicom radiographic uncompressed images in order to verify the behavior under various attacks such as: different compression levels, geometric attacks, new watermark embedding and filtering.

References

[1] S. Barbera, A. Beux, G. Borasi, F. Bui, D. Caramella , A. Cazzulani, P. Cortivo, F. Dalla Palma, F. De Ferrari, G. Giordano, R. Lagalla, F. Lucà, E. Moser, P. C. Muzzio, G. Norelli, G. Pagani, G. Pellicanò, M. Pignataro, R. S. Pozzi Mucelli, A. Rotondo, O. Tamburrini, N. Villari, F. Vimercati, "Teleradiologia. Indicazioni e raccomandazioni all'uso", La Radiologia Medica, Edizioni Minerva Medica – Torino, 2001, 102: 2-13.

[2] M. Sadicoff, María M. Larrondo Petrie, "Digital Watermark Survey and Classification" Second LACCEI International Latin American and Caribbean Conference for Engineering and Technology (LACCEI'2004), Miami, Florida, USA 2-4 June 2004.

[3] Coatrieux G, Lecornu L, Sankur B, Roux Ch., "A Review of Image Watermarking Applications in Healthcare" Conf Proc IEEE Eng Med Biol Soc. 2006;1:4691-4.

[4] E Lin, E Delp , "A Review of Fragile Image Watermarks", ACM Multimedia '99, Multimedia Contents, Orlando, October 1999, pp. 25-29.

[5] Swanson, Mitchell D. and Zhu, Bin and Tewfik, Ahmed H. "Transparent robust image watermarking", IEEE Proc. Int. Conf. Image Processing, 1996.

[6] Jen-Bang Feng, Ioun-Chang Lin, Chwei-Shyong Tsai, and Yen-Ping Chu, "Reversible Watermarking: Current Status and Key Issues", International Journal of Network Security, May 2006 Vol.2, No.3, pp.161–171.

[7] Wang Gang, Rao Ni-ni, "A fragile watermarking scheme for medical image".Conf Proc IEEE Eng Med Biol Soc. 2005;4:3406-9.