Relevance of Watermarking in Medical Imaging

G. Coatrieux(1,2), H. Maître(1), B. Sankur (3), Y. Rolland(2), R. Collorec(2)
(1) ENST, Département TSI - Paris, France ;
(2) LTSI, INSERM, Université de Rennes I, Rennes, France ;
(3) Boğaziçi University, Bebek, Istanbul, Turkey;
coatrieu@.tsi.enst.fr

Abstract— *Because of the importance of the security issues in the management of medical information, we suggest to use watermarking techniques to complete the existing measures for protecting medical images. We discuss the necessary requirements for such a system to be accepted by medical staff and its complementary role with respect with existing security systems. We present different scenarios, one devoted to the authentication and tracing of the images, the second to the integrity control of the patient's record.*

Keywords—**Medical Imaging, Medical information, Watermarking, PACS, Security, Confidentiality, Authentication, Integrity.**

I. Introduction

Digital information management in hospitals, HIS (Hospital Information System), and its special cases of RIS (Radiology Information System), PACS (Picture Archiving and Communication System) forms the information infrastructure of modern health care [1]. Recently the advent of multimedia has boosted the potential of telemedecine applications ranging from teleconsulting, telediagnosis etc. to cooperative working session [2] and telesurgery. These advances in information and communication technology provide in fact new ways to store, access and distribute medical data, and introduces new practices for the profession, as well as the patient themsleves by accessing to their own medical files [3]. With these benefits there are concomitant risks for electronic patient records (EPR) and strictly personal documents circulating in open networks, and being accessible, e.g., via Internet. Thus it is a widely shared point of view that there is an urgent need for network level security measures and protocols in medical information systems.

This paper aims to provide a critical review of security practices currently used and to introduce watermarking as a complementary element in the context of medical information security.

Section 2 defines security needs in medical information systems and the methods currently used; it points out possible security breaches. Section 3 introduces watermarking techniques, describes the niche role that watermarking can play in medical imaging along with its requirements and it discusses some case studies. Some concluding remarks are given in Section 4.

II. Security Issues in Medical Information Systems

A. Security and Medical Information

Medical information record of a patient is a complex of clinical examinations, diagnosis annotations, prescriptions, histological and other findings, and images in various modalities [4]. In the digital format they are centered in the EPR (Electronic Patient Record). This information is gathered over years by a number of health professionals and used as well for different purposes (patient care but also clinical research, epidemiological studies or insurance companies). All patient records, electronic or not, linked to the medical secrecy, must be confidential. The digital handling of EPR on network requires a systematic content validation which is aimed at quality control: actuality (precise interest of the information at a given instant) and reliability (authentication of the origin and integrity).

Security of medical information, derived from strict ethics and legislatives rules, gives rights to the patient and duties to the health professionals. This imposes three mandatory characteristics: confidentiality, reliability and availability [5] [6]:

- confidentiality means that only the entitled users, in the normally scheduled conditions, have access to the information;

Fig. 1. Components of security and their threats.

• reliability which has two aspects; i) Integrity: the information has not been modified by non-authorized people, and, ii) Authentication: a proof that the information belongs indeed to the correct patient and is issued from the correct source;
• availability is the ability of an information system to be used by the entitled users in the normal scheduled conditions of access and exercise.

B. Current Security Tools

The tools commonly used for ensuring confidentiality and integrity of information in a computer system, connected or not to a network, are depicted in Fig.1 to 3.

The threats to confidentiality are disclosures and re-routing of the information. This can occur during transmission (when for example an ill-intentionned person intercepts and illicitly copies files and records), or in the database, resulting in intrusion, identity usurpation, or Trojan horse virus (which keeps an open access through the network). Fighting against confidentiality violation (Fig.2), consists in access control, and secure transmission protocols. With a stand-alone workstation, the access can be performed in the same way as the credit-card control, and a daily notebook of data access can be generated. When dealing with an open environment, the access can be controlled using firewalls, and during the transmission of data, confidentiality can be achieved by encryption.

For integrity, which threats are destruction and modification of the contents of files and records, the same solutions may also be used or extended (Fig.3), since the violations are indeed in most cases identical, the only finality being different. Server security, can be carried out by authenticating and identifying the user against identity usurpation, the use of access rights for writing and reading and also daily notebook of access. To fight

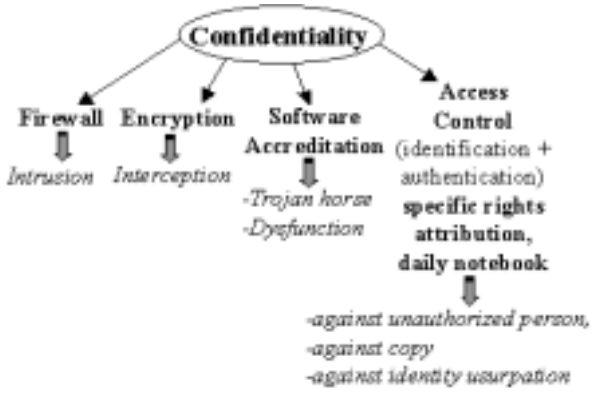

Fig. 2. Actual security tools for the protection of medical information confidentiality.

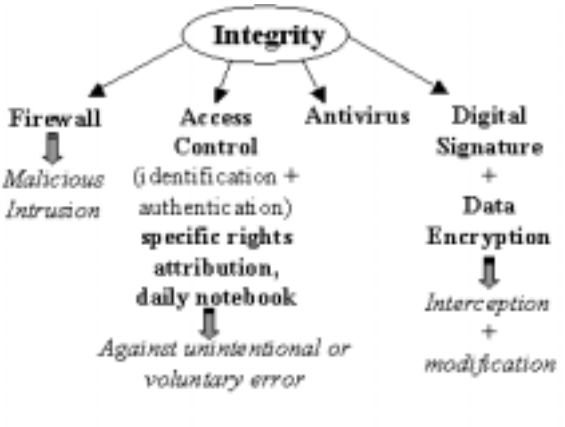

Fig. 3. Actual security tools for the protection of medical information integrity.

against viruses, antivirus and accreditation of software are the rules. Again firewalls can protect for intrusion. During transmission, data integrity can be guaranteed by digital signatures, which generate secure hash or digest resume sent with the data.

As long as availability is concerned, the main threats take the form of file management system disablement, destruction of a hard disk, or as a consequence of a malicious pirate who disrupts or alters surreptitiously the organization or content of the data. As a complement of the previous tools, as in any security system, the human intelligence and strict utilization of data handling rules (access, auditing, etc.) forms the most important part of security, but at the same time it is the most difficult to manage.

C. Limitations of current security measures

Security tools have also their limits. Regarding the information system access, firewalls provide a certain level of isolation between the intra-net and Internet, but are easily bypassed by hackers. For storage and transmission, cryptography is probably a very efficient tool, but once the sensitive data is decrypted, the information is not protected anymore. Furthermore the file headers are in the plain-text format and can be usurped by a pirate. Cipher text, on the other hand, unless protected by error correction facility, is very sensitive to bit errors occurring during storage and transmission. Once the images are in the open (plain-text form), the major threat is the violation of the access rights and of the daily logs by the intruder. Breaking of the confidentiality implies that integrity and authenticity of the data cannot anymore be guaranteed.

Finally let's note that a surprisingly large proportion of authenticity problems are not due to any intrusion, but due to errors in the manual entry of patient data. Kolodner [1] quotes that errors of this type occurs in 15 to 20% of cases.

Watermarking is made to introduce identifiers which, by construction, are inseparable from the document they are attached to. They may be seen as ultimate ramparts against usurpation and fabrication. It can be claimed that, in the medical domain, watermarking is an additional tool in the repertoire of security measures, specifically adapted to images, which can be used to thwart certain attacks, as discussed in the next section.

III. Watermarking in Medical Imaging

Recently there has been much interest in watermarking of all intellectual property in digital format such as multi-media products, images, video, graphics, software etc. [7] [8] [9]. As a consequence of this surge in interest a great number of watermarking techniques have been advanced.

The number of studies in the literature dedicated to watermarking of medical images is, however, not very expensive. Anand *et al.* [10] , proposed, to insert an encrypted version of the EPR in the LSB (Least Significant Bit) of the gray levels of medical-image pixels. Although the damage to the diagnostic image quality is minimal, the limitations and fragility of LSB watermarking is well-known. Miaou *et al.* [11], have similarly proposed an LSB technique. The image carrier authenticates the origin of the transmission (hospital), and the message to be embedded is composed of an ECG record, the diagnosis report and the doctor's seals. As Macq and Dewey [12], he gives attention to trusted header by watermarking the root part in the image data.

A. Watermarking techniques

The purpose of watermarking is the insertion of a message, also called content or watermark, in a document, also called carrier, which could be text, sound, image or video. Unlike steganography, which also has the same objective, watermarking explicitly requires that the text remains hidden to any unauthorized user and be resistant to any attempt to suppress it. There exists a plethora of methods for the watermarking of images. Watermarking can be executed in the pixel domain or in some transform domain. The two paradigms of embedding watermark data are based on i) addition of a spread-spectrum signal to the pixels or transform coefficients, ii) substitution of the pixel or transform coefficients by other values (e.g., fixed quantization values). In either case properties of the human visual system are exploited to control the quality of the image.

To address the specific application needs of watermarking in the context of biomedical images we refer to the classification made in [13]. Three main objectives are foreseen in the medical domain:

- data hiding for the purpose of inserting metadata, annotations and other information that just makes the image more useful or easier to use;
- integrity control, that is the verification that the image is intact, in that it has not been modified in an unauthorized manner, (this meets the "secure camera" paradigm);
- authenticity, that is the verification that the image is really what the user supposes it is.

B. Different application domains in the medical field

Within the medical imaging domain, two extreme situations may be experimented and a large

variety of intermediary cases which may be more or less interpolated from these cases.

At one extremity, one family of applications covers the transmission of medical documents over public networks, like in telemedecine, remote or collaborative telediagnosis or telesurgery, distance learning and several applications dealing with data base consulting. In this case, the demand is very close from the desiderata of image watermarking as expressed for e-commerce or multi-media applications over open networks. The images will face transmission errors and lossy compressions; the protocols will probably be heterogeneous; secure modalities (firewalls, accredited softwares) will be rare and the end-terminals will not be secured. Under these circumstances, we find watermarking solutions very similar to the many developed in other domains of image communication, the basic constraints of medical images being taken as additional guide-lines for selecting the watermarking method (see for instance [9] for a review).

On the other extremity, within the hospital network and under the complete security system developed in the framework of HIS, very different problems will be faced. Transmissions are done most of the time without loss and specific workstations with adequate protocols and softwares may be available for handling local security problems. Under these conditions, security problems may only arise from either malicious attempts to break the security protocol, or human negligence or mistakes.

Because this last situation is more specific, it deserves original solutions that will be discussed more in the following lines.

C. Requirements for medical image watermarking

The usual constraints of watermarking are invisibility of the mark, capacity (expressed in bit per host pixel), secrecy to unauthorized persons, robustness to attempts to suppress the mark. These demands also exist in the medical domain but additional constraints are added.

C.1 Imperceptible / Reversible Watermarking

Medical tradition is very strict with the quality of biomedical images, in that it is often not allowed to alter in any way the bit field representing the image (non-destructive). Thus the watermarking method must be reversible, in that the original pixel values must be exactly recovered [12]. This limits significantly the capacity and the number of possible methods. It also constrains to have dedicated routines to automatically suppress and introduce the mark in order to prevent the transmission of unprotected documents.

A second interesting alternative for inserting the watermark, however, would be to define regions of interest, to be left intact, and regions of insertion [14]. In other words the watermark protects the regions of interest while being inserted in the rest of the image plane. One could be, in fact, much more tolerant with the alterations caused in the regions of non-interest, as they do not contribute to the diagnosis. For example to increase capacity and/or robustness, one can allow the watermarking signal to be somewhat perceptible, provided its level does not interfere with or disturb the radiologist. Finally it has been shown that judicious alterations, such as occurring in image compression, does not in any way interfere with the diagnosis ability [15]. Therefore in time the attitude demanding strict preservation of the images as a number field will be relaxed. Thus as a third alternative, watermark insertion methods that use the whole image, and bring about imperceptible alterations in the pixels, as commonly used in all multi-media signals, will creep into medical field as well.

C.2 Integrity Control:

The "secure camera" concept applies also to biomedical images, especially in the context of legal aspects and insurance claims. There is thus a need to prove that, the images on which the diagnoses and any insurance claims are based, have preserved their integrity. One must define the "start point" of integrity, as the original captured image often must undergo certain processing, like enhancement and contrast stretching, to be more useful to the radiologist. Thus it must be decided which version of the image, whether the pristine sensor output or the processed and standardized image at a certain stage by the radiologist, is taken as the reference for integrity control. The integrity control based on the exact preservation of all the bit planes of the image may be unnecessarily strict. Thus alterna-

tives, specifically content-based integrity control, as in [16], are still open to discussion.

C.3 Authentication:

A critical requirement in patient records is to authenticate the different parts of the electronic patient record, in particular the images. More often an image is identified by an attached file or a header which carries all the needed information (the Dicom solution to the radiology images is well known). However, keeping the meta-data of the image in a separate header file, is prone to forgeries or clumsy practices. An alternative would be to embed all such information into the image data itself. Another possible scheme, is to have both the DICOM header in a separate file and embed the digest of the same information in the image. An important issue arrives here: how much information can be put in a watermark for a medical application? In the multi-media domain, current applications usually embed marks with a payload of 1 to 100 bits approximately for images with TV format. Medical applications are more demanding in quality but on the other hand are less prone to degradations. We may therefore expect that capacities of some tens of bits per Megabits of data will be achievable within the medical constraints.

An interesting variant application of authentication is the marking of volume images, such as MRI. In this case the voxels are marked with the patient identity. Such watermarking must satisfy the critical requirement that any arbitrary 2-D slice extracted from this volume, even with unknown slicing angle, must provide sufficient authentication evidence on the patient [17].

D. Case Studies of Watermarking of Medical Images

In order to illustrate the possible ways of using watermarking technologies in the medical field, let us examine two different scenarios where the use of watermarks may be an added security element.

D.1 Authentication and tracing

Medical images may go through several services and receive different processing and annotations. These transformations are recorded in a historical resume which is attached to the image as meta-data along with the patient references and the acquisition data. If a watermark is introduced in the image carrying an identifier also present in the resume, it guarantees that no error or falsification has been committed in the simultaneous processing of the image and the resume. The automatic handling of the watermark and the resume by authorized workstations is an additional security for the documents and may allow for instance the practice of reversible watermarking. If non-reversible watermarks are used, incremental marks may hold track of the different services which handled the document.

D.2 EPR diffusion

If the EPR is kept by the patient him/her-self, or distributed on several sites, and transmitted to the different services in charge of further considerations or treatments, some mechanisms should be introduced to guarantee the integrity of the document. These mechanisms not only will tell the medical persons whether the document is the same as the original one, but also if some differences exist, their location and importance. The decision could then be taken to consider the document as valuable or not. Watermarking as a tool for integrity control is well adapted for this purpose [18] [19].

As the checking of complex watermark may be heavy, it is probably not likely that it is done every time the image is displayed. The resume file attached to the image or the image header will be the prime identifier, and the control of the adequacy between the image and the resume or header be made when necessary for instance before entering the documents in a data base or before a diagnosis or when a conflict happens. In this scenario, the watermark is the ultimate security proof, most of the time ignored by the system, which is only used when important security issues arrive.

IV. Conclusion

The relevance of watermarking schemes for medical imaging has been analyzed in the very specific case of the HIS context. Note that the previous comments which were addressing image security, can be extended to other types of data such as

text, signal, speech and video, all of them also important in the diagnosis and sharing most of the security requirements previously examined.

We advocated that, as a complement to the actual security tools, watermarking can raise up the security level of information system by detecting system failure, manipulation errors, virus and malicious actions. It provides an ultimate guarantee of authentication that no other protection may ensure.

Careful selection or adaptation of the many watermarking schemes as developed for multimedia protection and e-commerce applications, should be made to guarantee the acceptability of this new technique in the medical field. A narrow collaboration between software developers and medical end-users is mandatory and specific developments for the different modalities (X-rays, CT, NMR, US, etc.) and the different services (pneumology, radiology, surgery, etc.) is necessary to insure that even in the worst case the watermarking is transparent to the diagnosis.

The capability to put a maximum amount of information without discarding the image quality, could not only ensure security of medical imaging data, but also generate a multiplicity of useful applications with the incoming distributed EPR.

References

[1] S. Kolodner, *Filmless Radiology*, Collection Health Informatics. Springer Verlag, NewYork, USA, 1999.

[2] X. Riot, M. Véron, F. Wendling, G. Coatrieux, J.L. Coatrieux, J. Bezy-Wendling, and D.Bouchard, "MONNET : Une Application du Travail Coopératif en Imagerie Médicale," *Innovation et Technologie en Biologie et Médecine*, vol. 20, no. 5, pp. 263–270, 1999.

[3] R. Beuscart, "Rapport au Premier Ministre : Rapport sur les enjeux de la Société de l'Information dans le domaine de la Santé," Tech. Rep., Mission interministérielle de soutien technique pour le développement des Technologies de l'Information et de la Communication, MTIC, Paris, France, 2000.

[4] L. Dusserre, H. Ducrot, and F.-A. Allaert, *L'information Médicale-L'ordinateur et la Loi*, Techniques et Documentation. Editions Médicales Internationales, Cachan, France, 1999.

[5] F.-A. Allaert and L. Dusserre, "Security of Health System in France. What we do will no longer be different from what we tell," *International Journal of Biomedical Computing*, vol. 35, no. Suppl. 1, pp. 201–204, 1994.

[6] J.L. Lamère, *Sécurité des Systèmes d'information*, Dunod, Paris, 1991.

[7] E.T. Lin and E.J. Delp, "A Review of Data Hiding in Digital Images," in *Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference*, PICS '99, Ed., Apr. 1999, pp. 274–278.

[8] M.D. Swanson, M. Kobayashi, and A.H. Tewfik, "Multimedia Data Embedding and Watermarking Technologies," *Proceedings of the IEEE*, vol. 86, no. 6, pp. 1064–1087, June 1998.

[9] S. Katzenbeisser and F. A. P. Petitcolas, *Information hiding techniques for steganography and digital watermarking*, Artech House Books, Norwood, MA, USA, 1999.

[10] D. Anand and U.C. Niranjan, "Watermarking Medical Images with Patient Information," in *proc. IEEE/EMBS Conference*, Hong Kong, China, Oct. 1998, pp. 703–706.

[11] S.G. Miaou, C.H. Hsu, Y.S. Tsai, and H.M. Chao, "A Secure Data Hiding Technique with Heterogeneous Data-Combining Capability for Electronic Patient Records," in *Proceedings of the World Congress on Medical Physics and Biomedical Engineering, Session Electronic Healthcare Records*, IEEE-EMB, Ed., Chicago, USA, July 2000.

[12] B. Macq and F. Deweyand, "Trusted Headers for Medical Images," in *DFG VIII-DII Watermarking Workshop*, Erlangen, Germany, Oct. 1999.

[13] F. Mintzer, G.W. Braudaway, and M.M. Yeung, "Effective and Ineffective Digital Watermarks," in *IEEE ICIP'97*, Santa-Barbara, California, USA, Oct. 1997, vol. III, pp. 9–12.

[14] G. Coatrieux, B. Sankur, and H. Maître, "Strict Integrity Control of Biomedical Images," in *Electronic Imaging 2001, Security and Watermarking of Multimedia Contents III*, SPIE, Ed., San Jose, CA, USA, submitted, Jan. 2001.

[15] S.M. Perlmutter, P.C. Cosman, R.M. Gray, R.A. Olshen, D. Ikeda, C.N. Adams, B.J. Betts, M.B. Williams, K.O. Perlmutter, J. Li, A. Aiyer, L. Fajardo, R. Birdwell, and B.L. Daniel, "Image Quality in Lossy Compressed Digital Mammograms," *Signal Processing*, vol. 59, pp. 189–210, 1997.

[16] P. Lamy, J. Martinho, T. Rosa, and M.P. Queluz, "Content-Based Watermarking for Image Authentication," in *Proceedings of the Third Workshop on Information Hiding*, IHW'99, Ed., Dresden, Germany, Sept. 1999, pp. 195–206.

[17] H. Maître, B. Sankur, and G. Coatrieux, "Watermarking of 3D Data Inherited by its 2D Slides," *IEEE Processing Letters, submitted*, 2000.

[18] E.T. Lin and E.J. Delp, "A Review of Fragile Image Watermarks," in *Proceedings of the Multimedia and Security Workshop at ACM Multimedia'99*, ACM, Ed., Orlando, Florida, USA, Oct. 1999, pp. 35–39.

[19] J. Fridrich, "Methods for Tamper Detection in Digital Images," in *Proceedings of the Multimedia and Security Workshop at ACM Multimedia'99*, ACM, Ed., Orlando, Florida, USA, Oct. 1999, pp. 29–33.