Proceedings of the 28th IEEE
EMBS Annual International Conference
New York City, USA, Aug 30-Sept 3, 2006

A Review of Image Watermarking Applications in Healthcare

G. Coatrieux, L. Lecornu, B. Sankur, *Members, IEEE,* Ch. Roux*, Fellow*, *IEEE*

Abstract—**In this article, we focus on the complementary role of watermarking with respect to medical information security (integrity, authenticity …) and management. We review sample cases where watermarking has been deployed. We conclude that watermarking has found a niche role in healthcare systems, as an instrument for protection of medical information, for secure sharing and handling of medical images. The concern of medical experts on the preservation of documents diagnostic integrity remains paramount.**

I. Introduction

ADVENTS of multimedia combined with information and communication technology boost the potential of medical information handling and sharing with applications ranging from telediagnosis to telesurgery and cooperative working session. At the same time, these benefits introduce concomitant risks for shared electronic patient records (EPR) and call for more secure information management.

Originally devoted to multimedia document Digital Rights Management[1], watermarking has also attractive properties that fit within the healthcare domain, although the interests at stake are different [2][3]. Watermarking is the insertion of a message, also called content or watermark message, in a host document in some multimedia format. It is required that the watermark information remains hidden to any unauthorized user (as for data encryption, a secret key is needed to access the watermark content), non-interfering with the use of the watermarked document and fragile (integrity) or robust (authentication) to any attempt to suppress it. Two main objectives of watermarking are foreseen in the medical domain [2]: data hiding for the purpose of inserting meta-data to render the image more usable and information protection with application like integrity control.

Despites its attractiveness, multimedia watermarking methods may encounter limitations in medical images. The added watermark signal frequently alters the host image in an irreversible manner and may mask subtle details. Consequently, proposed solutions try to preserve the image diagnosis quality value avoiding critical information loss.

In this paper, we aim to update watermarking objectives and its role through a critical review of recent watermarking proposals in healthcare. From this standpoint, we discuss in section 2, two main medical imaging watermarking schemes. In section 3, medical image watermarking techniques are presented and their requirements are discussed. Some concluding remarks are given in section 4.

II. Protecting and Enhancing Medical Images with Watermarking

A. *Medical Information Assurance & Watermarking*

Medical information protection derives from strict ethics and legislatives rules. Regulations like USA's HIPAA and Europe's EC 95/46 Directive are expressions of such a constraint. Focusing on medical information records, which for a patient are a complex set of clinical examinations, diagnosis annotations and other findings and images centered in its EPR, we recall the three mandatory security characteristics:

- Confidentiality, which means that only the entitled users have access to the information;
- Availability, that is the ability of an information system to be used in the normal scheduled conditions of access;
- Reliability, based on the outcomes of: i) Integrity - the information has not been modified by non-authorized people, and, ii) Authenticity - a proof that the information belongs to the correct patient and issued from the right source.

In Medical Information Systems (MIS), these characteristics are maintained through five security services [4]: integrity, availability, authentication, confidentiality, and non-repudiation. If availability, integrity and confidentiality services have similar definition in respect with the corresponding security component, the authentication service is "designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorizations to receive specific categories of information" [4]. Non-repudiation service manages proofs of delivery and of the message sender's identity.

As depicted in figure 1, reliability is extendable to traceability when it becomes possible to trace the information along its distribution. Traceability allows systematic information content validation, which is aimed at trustiness and quality control: actuality (precise interest of the information at a given instant) and reliability.

At the interface between the information and the MIS security services, watermarking can improve information protection from the information side. It allows a security layer the nearest as possible to the data because of its

G. Coatrieux, L. Lecornu and Ch. Roux are with the (1) ENST Bretagne, GET-ENST, Brest, F-29200 France; (2) Inserm , U650, Brest, F-29200 France. (phone:+33-2-29001508; fax: +33-2-29001098; e-mail: gouenou.coatrieux@enst-bretagne.fr).

B. Sankur is with the Electrical and Electronic Engineering Department, Bogazici University, Bebek, Istanbul, Turkey.

1-4244-0033-3/06/$20.00 ©2006 IEEE.

property to associate protection data with information to be protected in single object: a watermarked document. Nevertheless, confidentiality and reliability are the main objectives that watermarking has been proposed for, considering applications like e-diagnosis or medical image sharing through PACS (Picture Archiving and Communication System).

Medical image integrity control [5-14] is most of the time enabled by embedding a digital signature (DS) or a Message Authentication Code (MAC) [16] computed over the whole image or over some specific local or global image characteristics. A cryptographic DS aims for the exact, that is bit-by-bit, preservation and protection of the information. At the detection stage, any difference between the recomputed DS/MAC and the embedded ones will be proof of the image integrity. Alternatively, it can be designed to differentiate manipulated image blocks [5][11][13]. One advantage of DS, based on the cryptographic hashing functions, is that it is legally recognized in most countries. That is not the case of pure watermarking solutions, for example telltale evidence from a fragile watermark. Some research is presently being conducted for perceptual hashing or content-based integrity control methods, which tolerate "innocent" modifications that do not modify the image content (ex. lossy image compression) [16][17]. At the same time, once the image integrity violated, there is an interest to identify the modification [18]: is it a malicious one or not? This is one objective of image forensic research.

There are several solutions for the authentication of the image source, as required for distributed EPR [2]. All of them consider that medical images are issued from modalities in the DICOM format (an header accompanied of the raw image data). One approach naturally is based on inserting the UIDs (Unique IDentifiers) provided by the DICOM header [2][11][20][7]. The watermark allows verifying the header-raw data association and the image origin retrieval even if its format has been changed. A second approach consists in embedding the complete DICOM header [21] but because some of the header parts are updated each time the image is transmitted, a complex header information selection must be used, considering only patient information relevant to the image [19][8]. An alternative links the raw image data with the header by embedding a DS of the header. While this alternative minimizes the message length to be embedded,(an important constraint - see section 3), the header should be kept with the image when it is distributed. Hence, it becomes difficult to change the image format: a main advantage of watermarking is lost.

When dealing with e-health applications, some have proposed to improve data confidentiality by inserting EPR elements (annotation, signal, etc.) within images [23-26] [9-11]. Nevertheless, the interest of such an approach is limited to a small number of applications, where image embedding capacity is rather sizeable. This scheme cannot be generalized to a complete patient EPR, which sometimes does not contain any images.

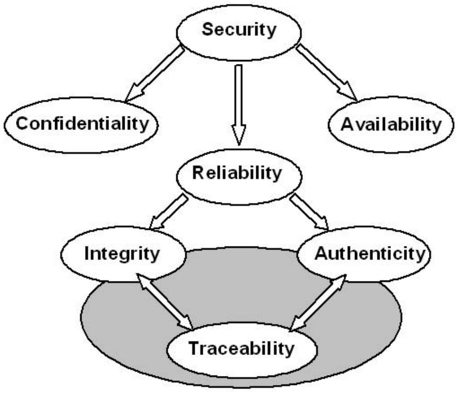

Fig. 1. Medical information security components.

In addition to the goals of authenticity, integrity and confidentiality, only a few works focus on image traceability. An experiment proposed in [22] aims at providing medical image tracing in a communication environment; i.e., a group of users. Based on a user key, a part of the watermark is removed from the protected image leaving a watermark signal in the image that identifies the user. As for the copyright purpose, this can be used to identify a final user (a "buyer") but not a complete distribution chain. In fact, medical image traceability has not been treated from the watermarking point of view.

Considering now the EPR content protection in a MIS, it may be suitable to authenticate the link between images and the medical report they are associated to. The system we propose in [20] takes into account the security services of the MIS and integrates an automatic process control, which verifies such a link giving information not only about the reliability of the image but also about the EPR reliability. The medical report contains image integrity and authenticity proofs, while the image contains similar information about the report. In that way, it becomes more difficult to tamper with information, as both have to be modified.

However, a lot remains to be done in interfacing data watermarking with MIS and more specifically with the security services. Watermarking introduces a new security layer that we expect to be preserved during data storage, transmission and also processing (only if the watermark doesn't interfere with the content) continuously protecting the information. This cannot be achieved by using only cryptographic mechanisms.

B. Enriched watermarked images

A second objective of watermarking, named data hiding, is just to make the image more usable or more informative with the insertion of meta-data. However, very few applications address this aspect in medical images.

The proposed data hiding applications focus on image management. In [12] the record indexing information is embedded into the media content to identify the media. An extension of this approach [27] suggests the embedding of the description of the identified pathology within the image.

This is helpful in knowledge management. The image contains its symbolic description that can be easily handled by database and data mining applications while preserving the image format. At the same time, database coherence and safety may be improved as it becomes possible to repair damaged index tables of an image database by retrieving from the watermarked images the needed information.

Beyond these few examples, data hiding has not been explored in healthcare. We conjecture that numerous applications are waiting to be discovered in medical knowledge and information use (teaching, research and health). As for information protection, data hiding can help in interfacing data management in and between MIS.

However, one important data hiding limitation is due to the size of the message that can be embedded in a medical image. This is a critical point, which depends on the watermarking method exploited.

III. WATERMARKING TECHNIQUES FOR MEDICAL IMAGING

A watermarking method is usually designed depending on an application framework striking a compromise between different requirements: capacity (amount of information that can be embedded), robustness (a fragile watermark will not survive any image processing), privacy (secret knowledge for watermark content access - usually a secret key) and imperceptibility. We can say that the higher the strength of the watermark signal, the more it is robust and/or of higher capacity albeit perceptibility is compromised. Consequently, if it is envisioned to process the image with an information loss, a robust watermark is desirable to authenticate the image origins, while at the same time the watermark should not interfere with the image content interpretation.

A. Watermarking methods

Three kinds of watermarking methods were identified for medical images [2]. A first class regroups methods that embed information within region of non-interest (RONI) in order not to compromise the diagnosis capability [5][28]. Various experiments suggest that RONI corresponds in general to the black background of the image, but sometimes RONI can include gray-level portions of little interest [6], hence leaves some room for the watermarker on the gray-level image itself. Since there is no interference with the image content, invisibility is less strict; consequently one can revert to methods with higher capacity and robustness [5]. Even though no interferences occurs with the data potentially useful for diagnostics, it has been pointed out that changing the black background in a salt and pepper like noisy pattern may annoy the physician. Consequently, the watermark signal amplitude has to be correctly selected.

The second approach corresponds to reversible watermarking. Once the embedded content is read, the watermark can be removed from the image allowing retrieval of the original image [21]. A great effort has been recently provided in developing this kind of method but the capacity is still way below the embedding capacity of non-reversible watermarking technique. Because of the fragility of reversible methods, such methods are used for the integrity purpose and data hiding. Actually, one method provides robustness [29] but sometimes it introduces in the image a highly visible salt-and-pepper noise.

The third approach consists in using classical watermarking methods while minimizing the distortion. In that case, the watermark replaces some image details such as the least significant bit of the image [26][8] or details lost after lossy image compression [22]. In [30], robust watermarking has been considered after a physician has selected the maximum power of the watermark just under the level of interference with the diagnosis. Nevertheless, it should be considered that the original captured image often undergoes certain processing, like enhancement and contrast stretching with parameters values varying from one user to another. Consequently, the watermark may become more or less "visible". This effect is emphasized by the diversity of medical images with pixels encoded on more than 8 bits.

B. Applications & methods requirements

Depending on the medical application area (health, administrative, teaching, research ...) the trade-offs among robustness, invisibility and capacity varies. For example, image application focused on patient’s healthcare are less tolerant of degradations, while teaching material can be enriched with metadata. Thus, the designer can interplay with watermarking requirements and watermarking tools. For example, RONI approaches will leave intact the diagnostic information, but they can be applied only if a RONI exists. Furthermore, the capacity is dependent upon the RONI area size. The embeddable size varies with image modality, and to a lesser degree among images within that category. An automatic RONI delineation is needed for security mechanisms to be transparent to the user or if it is the pristine sensor output image that is protected. For image tracing, RONI watermarking allows for watermark superimposition, with the concomitant risk that the ultimate watermark may alter the preceding ones.

While reversible watermarking facilitates watermark content updating, the image remains unprotected once the watermark has been removed. Since, due to capacity maximization the image is heavily watermarked, any watermark must be removed first before any interpretation. This is a situation similar to encryption. Nevertheless, the advantage of reversible watermark over encryption is that at least the image becomes authenticated. Nevertheless, some distortionless methods have been proposed [27] expecting the watermark to be kept in the image and invisible to image analysis.

An advantage of reversible watermarking over other competitors is that it leaves the field free for any desired image processing. In the RONI scheme, any image processing must maneuver clear of the RONI.

Whatever method is used, a caveat is the computational complexity should not cause uncomfortable time delays for the physician. This is especially important for the case of large image volumes or image sequences.

All this discussion points to the handicaps of the methods outside the RONI and reversible categories, which we could call as the classical methods. If exact preservation of information remains a paramount requirement, then we will see in the near future deployment of the techniques in the first two categories.

IV. Conclusion

Watermarking enables a security layer at the information level providing authentications and traceability abilities at the interface with security services in and between medical information systems, promising seamless information protection even if the information is processed. Cryptography and watermarking combination appears as a good compromise until equivalent and recognized pure watermarking solutions are provided.

However, watermarking of medical signals seems to be stalled at an early stage because of the lack of standard to quantitatively evaluate watermark interference with the diagnosis. Practically, there is a need for robust and distortionless methods adapted to various medical imaging modalities and services (radiology, surgery, etc.). Furthermore, flexible robustness and capacity tradeoffs would be essential in satisfying a multiplicity of applications in medical information protection, safety and management. The fusion of RONI and reversible watermarking methods may be one way in satisfying such objectives.

References

[1] M. Barni, F. Bartolini, "Data hiding for fighting piracy," IEEE Signal Processing Magazine, vol. 21, n°2, pp.28–39, 2004.

[2] G. Coatrieux, H. Maître, B. Sankur, Y. Rolland, R. Collorec, "Relevance of Watermarking in Medical Imaging," in Proc. IEEE Int. Conf. ITAB, USA,2000, pp. 250–255.

[3] E-.J. Delp, "Multimedia security: the 22nd century approach!," in Proc. workshop on Multimedia Systems, vol. 11, n°2, pp.95-97, 2005.

[4] C.D. Schou, J. Frost, W.V. Maconachy, "Information Assurance in Biomedical Informatics Systems," IEEE Engineering in Medicine and Biology Magazine, vol. 23, n°1, pp. 110–118, 2004.

[5] G. Coatrieux, B. Sankur, H. Maître, "Strict Integrity Control of Biomedical Images," in Proc. Electronic Imaging, Security and Watermarking of Multimedia Contents, SPIE, USA, 2001, pp.229-240.

[6] F. Y. Shih, Y-.Ta Wu, "Robust watermarking and compression for medical images based on genetic algorithms," Journal of Information Sciences, Elsevier, 2005, vol. 175, n°3, pp.200-216.

[7] C.-S. Woo, J. Du, B. Pham, "Multiple watermark method for privacy control and tamper detection in medical images," in Proc. APRS Workshop on Digital Image Computing, Australia, 2005, pp.59-64.

[8] X. Q. Zhou, H. K. Huang, S. L. Lou, "Authenticity and integrity of digital mammography images," IEEE Trans. on Medical Imaging, vol. 20, n°8, pp.784–791, 2001.

[9] H-.M. Chao, C-.M. Hsu, S-.G. Miaou, "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records," IEEE Trans. on Information Technology in Biomedicine, vol.6, n°1, pp.46-53, 2002.

[10] X. Luo, Q. Cheng, J. Tan, "A lossless data embedding scheme for medical images in application of e-diagnosis," in Proc. 25th Annual Int. Conf. of the IEEE EMBS, vol. 1, 2003, pp.852–855.

[11] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "A medical image watermarking scheme based on wavelet transform," in Proc. of the 25th Annual Int. Conf. of the IEEE EMBS, vol. 1, 2003, pp. 856–859.

[12] S. Cheng, Q. Wu, K.R. Castleman, "Non-ubiquitous digital watermarking for record indexing and integrity protection of medical images," in Proc. ICIP, vol. 2, 2005, pp.1062-1065.

[13] G.T. Oh, Y-.B. Lee, S.J. Yeom, "Security mechanism for medical image information on PACS using invisible watermark," in Proc. of Int. Conf. High Performance Computing for Computational Science, VECPAR, 2005, pp.315-324.

[14] F. Bao, R. H. Deng, B.C. Ooi, Y. Yang, "Tailored reversible watermarking schemes for authentication of electronic clinical atlas," IEEE Trans. on Information Technology in Biomedicine, vol. 9, n°4, pp.554–563, 2005.

[15] B. Schneier, "Applied Cryptography," 2nd second edition, Paris: International Thomson Publishing, 1997.

[16] C.G. Boncelet, "The NTMAC for authentication of noisy messages," IEEE Trans. on Information Forensics and Security, vol. 1, n°1, pp.320–323, 2006.

[17] O. Ekici, B. Sankur, B. Coskun, U. Naci, M. Akcay, "Comparative Assessment of Semifragile Watermarking Methods," Journal of Electronic Imaging, 13(1), pp. 209-216, 2004.

[18] S. Bayram, I. Avcibas, B. Sankur, N. Memon, "Image manipulation detection with binary similarity measures," in proc. EUSIPCO2005, pp.752-755.

[19] F. Cao, H.K. Huang, X.Q. Zhou, "Medical image security in a HIPAA mandated PACS environment," Computerized Medical Imaging and Graphics, vol. 27, n°2-3, pp.185-196, 2003.

[20] G. Coatrieux, J. Puentes, L. Lecornu, C. Cheze Le Rest, C. roux, "Compliant secured specialized electronic patient record platform," in Proc. of D2H2, USA, 2006, accepted.

[21] B. Macq, F. Dewey, "Trusted Headers for Medical Images," in DFG VIII-DII Watermarking Workshop, Erlangen, Germany, 1999.

[22] M. Li, R. Poovendran, S. Narayanan, "Protecting patient privacy against unauthorized release of medical images in a group communication environment," Computerized Medical Imaging and Graphics, vol. 29, n°5, pp. 367-383, 2005.

[23] R. Acharya, U.C. Niranjan, S.S. Iyengar, N. Kannathal, L.C. Min, "Simultaneous storage of patient information with medical images in the frequency domain," Computer Methods and Programs in Biomedicine, vol. 76, pp.13-19, 2004.

[24] J. Nayak, P.S. Bhat, M.S. Kumar, R. Acharya, "Reliable transmission and storage of medical images with patient information using error control codes," in Proc. IEEE INDICON, 2004, pp.147-150.

[25] Y. Srinivasan, B. Nutter, S. Mitra, B. Phillips, D. Ferris, "Secure transmission of medical records using high capacity steganography," in Proc. 17th IEEE Symposium on Computer Based Medical Systems, 2004, p.122-127.

[26] D. Anand, U.C. Niranjan, "Watermarking Medical Images with Patient Information," in Proc. Int. Conf. IEEE-EMBS, 1998, pp. 703–706.

[27] G. Coatrieux, M. Lamard, W. Daccache, J. Puentes, C. Roux, "A low distortion and reversible watermark: Application to angiographic images of the retina," in Proc. Int. Conf. of the IEEE-EMBS, 2005, pp.2224-2227.

[28] A. Wakatani, "Digital watermarking for ROI medical images by using compressed signature image," in Proc. 35th Hawaii International Conference on System Sciences, 2002, pp.2043-2048.

[29] C. De Vleeschouwer, J.-F. Delaigle, B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," IEEE trans. on Multimedia, vol.5, n°1, pp.97-105, 2003.

[30] A. Piva, M. Barni, F. Bartolini, A. De Rosa, "Data hiding technologies for digital radiography," in IEE Proc. Vision, Image and Signal Processing, vol. 152, n°5, pp.604-610, 2005.