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

Digital Watermarking in Telemedicine Applications – Towards Enhanced Data Security and Accessibility

Aggeliki Giakoumaki, *Member, IEEE,* Konstantinos Perakis, *Student Member, IEEE,*
Anastassios Tagaris, *Member, IEEE,* and Dimitris Koutsouris, *Senior Member, IEEE*

***Abstract*—Implementing telemedical solutions has become a trend amongst the various research teams at an international level. Yet, contemporary information access and distribution technologies raise critical issues that urgently need to be addressed, especially those related to security. The paper suggests the use of watermarking in telemedical applications in order to enhance security of the transmitted sensitive medical data, familiarizes the users with a telemedical system and a watermarking module that have already been developed, and proposes an architecture that will enable the integration of the two systems, taking into account a variety of use cases and application scenarios.**

I. Introduction

THE term e-Health came into use in the year 2000 and refers to the use of modern information and communication technologies to meet the needs of citizens, patients, healthcare professionals, healthcare providers as well as policy makers [1]. E-Health applications are very promising and have great potentials. They can play a very important role in service provision by improving access, equity and quality through connecting healthcare facilities and healthcare professionals and diminishing geographical and physical barriers [2]. Nevertheless, in order for e-Health to be viable and broadly accepted by the public, certain challenges need to be met and certain barriers need to be overcome.

Contemporary information access and distribution technologies raise critical issues that urgently need to be addressed, especially those related to security. Digital watermarking is a technology that addresses a wide range of applications, but the research community has just recently started to realize its potentials in the healthcare sector. Health data management issues that could be addressed by digital watermarking include among others enhanced security of sensitive data, source and data authentication, efficient image archiving and retrieval, and highlighting of diagnostically significant regions [3].

This paper suggests the use of watermarking in telemedical applications, in order to enhance security of the transmitted sensitive medical data and to provide value-added services for efficient health information management. The authors propose an architecture that enables the integration of digital watermarking in an already developed telemedical system, which can cover a wide range of applications; such applications include homecare, monitoring of patients with chronic diseases, emergency telemedicine, telediagnosis and teleconsultation. Furthermore, the perspectives of the integrated system in a variety of application scenarios are presented.

II. System Architecture

A. Description of the Telemedical System

The research team of the Biomedical Engineering Laboratory at the National Technical University of Athens has developed a telemedical system, suitable for the purposes of patient monitoring and teleconsultation [4]. The system supports the monitoring of various physiological parameters of the patients, whether they have developed chronic symptoms and are treated at home, or they are tangled in road accidents and are considered emergency incidents; it also supports the transmission of still images from the patient to the consulting doctor. The biosignals and the images are transmitted to a Central Station, where they are being monitored and stored locally for both security and educative reasons.

The system is based upon a client-server architecture, where both sides communicate over TCP/IP, in a transparent to the user way. The client side corresponds to the patient who is being monitored, while the server side corresponds to the health centre or the consultation site where the medical experts are located. The monitoring devices collect the biosignals and establish a connection with the client so as to transmit the data. After the connection has been established,

A. Giakoumaki is with the Biomedical Engineering Laboratory, School of Electrical and Computer Engineering, National Technical University of Athens, 9 Iroon Polytechniou str., 15773, Athens, Greece (phone: +30 210 7723516; fax: +30 210 7722431; e-mail: agiakoum@biomed.ntua.gr).

K. Perakis is with the Biomedical Engineering Laboratory, School of Electrical and Computer Engineering, National Technical University of Athens, 9 Iroon Polytechniou str., 15773, Athens, Greece (e-mail: kperakis@biomed.ntua.gr).

A. Tagaris is with the Biomedical Engineering Laboratory, School of Electrical and Computer Engineering, National Technical University of Athens, 9 Iroon Polytechniou str., 15773, Athens, Greece (e-mail: tassos@biomed.ntua.gr).

D. Koutsouris is with the Biomedical Engineering Laboratory, School of Electrical and Computer Engineering, National Technical University of Athens, 9 Iroon Polytechniou str., 15773, Athens, Greece (e-mail: dkoutsou@biomed.ntua.gr).

the client attempts to establish a connection with the server over TCP/IP, and as soon as the server accepts the call, real-time teleconsultation takes place via the transmission of the collected data, namely the biosignals and the images of the patient. The transmitted biosignals can be compressed using a variation of the Lempel-Ziv algorithm or the Huffman algorithm, while the images are compressed before transmission using the JPEG algorithm.

The device enables physicians to provide pre-hospital care more effectively, as up to seven-lead ElectroCardioGram, Invasive and Non-Invasive Blood Pressure, Heart Rate, Respiration Rate, Blood Oxymetry, Temperature and still images of the patients can be sent from the portable device to the base station. The system supports telediagnosis and teleconsultation both over fixed lines (PSTN, ISDN and LAN) as well as over wireless networks, namely GSM, GPRS, 3G and satellite networks. The deployed GSM and GPRS networks limited the functionality of the device, providing a bandwidth of up to 56 Kbps. Yet, the recently deployed 3G networks maximize the capabilities of this system and provide the means for more accurate and reliable telediagnosis [5].

Nevertheless, since sensitive data are involved, both parties need to employ security strategies, so that the integrity of the images sent is not tampered with, and the authentication of the sender is verified at the base station.

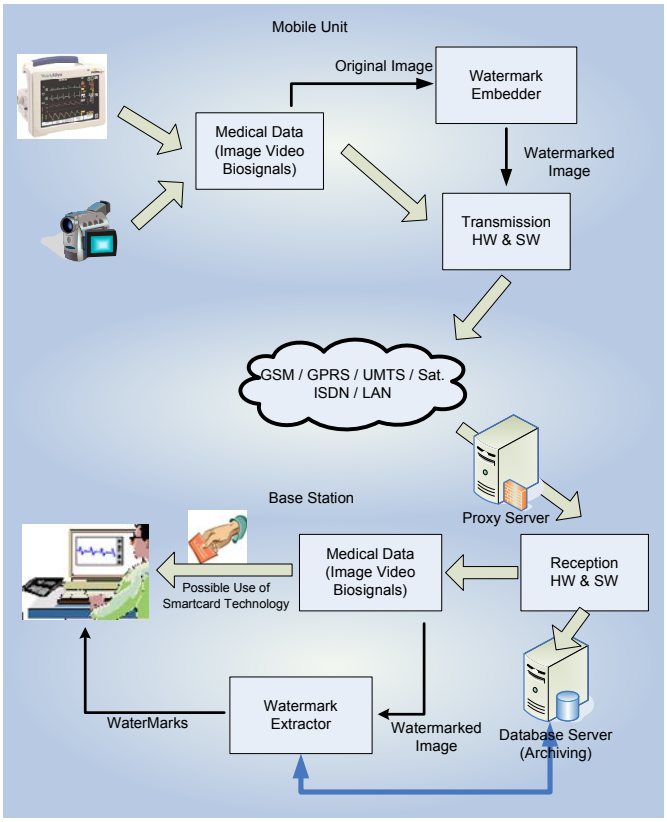

Fig. 1. Integration of the digital watermarking module with the telemedical system

B. Description of the Watermarking Module

Fig. 1 illustrates the architecture of integrating a digital watermarking module with the above described telemedical system. According to this, the mobile unit collects the images and the biosignals from the patient; the images are watermarked and subsequently transmitted along with the biosignals to the clinical station. There, the watermarks are extracted from the images and the appropriate handling of the information takes place, in order for the mobile healthcare providers to receive guidelines on how to cope with the incident.

The developed watermarking scheme provides value-added services to a range of health data management issues, such as enhancement of security and access control of sensitive information, source and data authentication, and efficient information retrieval. The scheme embeds in medical images multiple watermarks, with different characteristics and requirements, in order to simultaneously address the above issues. Besides the additional level of security obtained, the watermarking scheme is a value-added tool for efficient health data management, indexing, and archiving, that also facilitates the provision of accurate diagnoses and appropriate treatment planning. In order for the watermarking scheme to conform to the strict limitations regarding the acceptable modifications of the medical images, it allows the definition of a Region of Interest (ROI), which includes the diagnostically significant parts of the image and can optionally be ignored by the watermarking process, or just accommodate the minimum payload needed in order to allow integrity control.

In Fig. 1 the watermark embedder as well as the watermark extractor are in fact the same module which can act either as embedder or extractor. The watermarking functionality may be delivered by the architecture that is presented in Fig. 2. The core of the system is the watermarking engine along with the API which can act both as embedder or extractor.

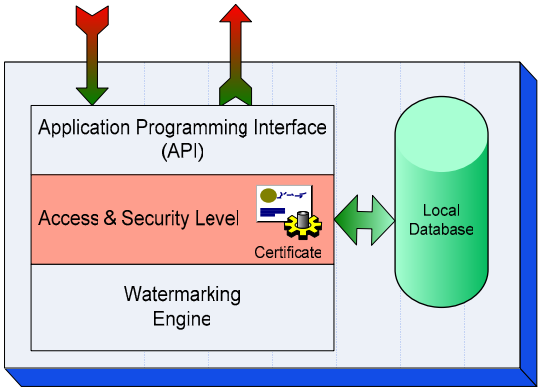

Fig. 2. Watermarking module architecture

The four basic components that assembly the watermarking module are described below:

(a). Watermarking Engine: It is the core component of

the module which implements the watermarking encoding and decoding. It applies multiple watermarking in medical images based on wavelet image decomposition. The embedding and extracting methods have been described in detail in [6]. The watermarking tool takes into account the different characteristics and requirements of the multiple embeddable watermarks, in terms of both robustness and capacity, and provides the option of being customized according to the specific targeted application. In general, it can embed the following four types of watermarks:

i) Signature watermark: it conveys data about the origin of the data and depending on the application it may include for instance the identification code of a remote telemedical unit or an image acquisition device, the name of the diagnostic centre, the physician's digital signature, and so on.

ii) Index watermark: it comprises of keywords to be used for efficient data archiving and retrieval. Indicatively, it may contain a unique identifier of the patient, e.g. his/her Social Security Number (SSN) or Medical Record Number (MRN), the examination code, or diagnostic codes (e.g. ICD9/10 codes).

iii) Caption watermark: it may include patient's name and demographics, date and time of the examination, the diagnosis and/or the examination report; moreover, it may include other helpful metadata, such as an electronic medical summary of the patient, or comments on special features and regions of diagnostic significance.

iv) Reference watermark: it comprises a watermark array – a priori known to the recipient – which aims at enabling integrity control of the transmitted images [7]. The comparison of the extracted reference watermark with the originally embedded one, not only provides information about whether an image has been modified during transmission or after storage, but also indicates the possibly tampered image regions.

(b). The API of the Engine: In fact, (a) and (b) are not two different components but they are represented as such here for clarity reasons. Component (b) is the API of the engine in order for the external SW to communicate directly with it. We foresee two basic use cases of the watermarking engine:

i) Use case 1 (engine used from the telemedicine software): The normal use case where the engine is accessed through the User Interface of the external application. The access to the engine is not straight forward but the access and security module filters who and at what level has access. In other words a user has first to be authenticated by that module in order to use the watermarking engine.

ii) Use case 2 (engine embedded in a medical device): This is the case where the engine along with the API is embedded into the medical device that captures the images. In that case there is no use of other interfaces or security components (i.e. the Access & Security level is missing) as the whole procedure is automated and predefined by the specifications of the device. This approach enables device manufacturers to use watermarking procedures directly from their devices.

(c). Access & Security Component: This component authenticates users in order to use the watermarking engine. In case of a version where images are stored in the local database, it could be extended to define access rights on those images. Two modes of operation may be defined:

i) Users and their access rights are stored in the local database.

ii) Integration with the Users Database of the Operating System (i.e. Active Directory). In that case the OS policy will define whether a user has access or not to the API of the watermarking engine.

(d). Local Database: The local database of the system will be used as a repository serving both:

i) Archiving of the images before and after their manipulation by the engine.

ii) The users of the system as well as their access rights (security credentials).

The local database could be extended in order to support storing of medical as well as demographic data of the patients.

III. Application Scenarios

The proposed system covers a wide range of telemedical applications. As described earlier, the system can support both homecare and emergency incidents, namely monitoring of patients at home or inside a moving vehicle (ambulance) via teleconsultation. Teleconsultation implies the use of computational systems and telecommunication infrastructure for medical data distribution in order to allow the provision of expert advice from a distance, and it can be applied in tele-radiology, tele-dermatology, tele-pathology and more. Three potential application scenarios are presented below.

In the scenario of emergency telemedicine, the paramedics apply the monitoring sensors upon the patient's body, and the biosignals are transmitted through the monitoring device to the computational unit of the system, and from there on to the medical experts. Still images of the patients can also be taken, in which digital watermarks can be embedded. In this application scenario, time and computational power is a major issue, so real-time watermarking, without human intervention, needs to be applied. Thereupon, the appropriate watermarks for the specific application should convey the mobile station ID and the date and time of the incident. At the time the data are received by the base station, the above information is extracted from the watermarked image and the whole set of the transmitted data is registered to the corresponding mobile station. Besides, an integrity-checking reference watermark could also be embedded at the time of image capture, in order to provide the physician located at the base station with the capability of examining the integrity of the received images.

In the scenario of homecare, time and computational power is not such an important issue, as in the case of

emergency telemedicine. In homecare applications, the medical images to be transmitted to the medical institution could be watermarked with the registration name of the computer located at the patient's home. Besides, a unique identifier of the patient could also be embedded, in order to enhance medical confidentiality protection and to guarantee a permanent link between the patient and the corresponding images. The integrity-checking watermark is also applicable in this case, as it allows the integrity control of the transmitted images.

As regards the scenario of remote health provision centers, rural doctors and nurses can make use of the proposed telemedical system in order to send biosignals of the patients to medical experts, as well as to transmit images acquired either by a digital camera or by a medical imaging device (e.g. X-Rays). In this scenario too, time and computational power requirements are not as strict as in the case of emergency telemedicine. This allows in practice the embedding of more watermarks and moreover the manual entry of additional helpful information. More specifically, in this case the embeddable data include the following: the identification code of the remote health provision center, the digital signature of the physician or the paramedic who handles the incident, the patient's name and personal data. Other watermarks conveying additional information regarding the patient's health history, highlighted regions of interest and any relevant comments, would also be applicable; this kind of information would assist the remotely located medical expert in obtaining a thorough patient status evaluation and consequently in making the primary diagnosis and recommending the appropriate healthcare treatment. The integrity-checking reference watermark that allows the tracing of possibly tampered parts of the transmitted images is applicable in this scenario too.

In all the above presented application scenarios, the recipient of the transmitted data is a base station, namely a hospital, a diagnostic centre, a medical institution etc, where a healthcare consultant is located. When the data are received, their origin is validated through the extraction of the signature watermark, which, depending on the application, may convey information about the identification code of the mobile station, the remote health provision center and/or the responsible healthcare provider. After the source authentication takes place, the whole data set is registered to the appropriate file; then, the healthcare professional located at the hospital supervises the incident, based on both the received data and the additional information that is retrieved by the watermarks. For instance, in the case that the transmitted data are watermarked with the patient's identifier, the physician can search the hospital database and retrieve the patient's record if it is available, thus gaining access to relevant data that would contribute to a thorough patient status evaluation. Furthermore, the physician may embed additional watermarks in the received images, before storing them in the hospital database; these watermarks could include his/her digital signature and a time stamp, the diagnosis, or even keywords (e.g. diagnostic codes) that could be used for efficient data indexing and retrieval.

IV. Discussion

Implementing telemedical solutions has become a trend amongst the various research teams at an international level. Nevertheless, the management and the dissemination as well as the exploitation of the sensitive personal data has raised significant issues that pose restraints to the teams involved in upgrading healthcare provision and enabling medical data management via web based platforms. The Internet Protocol has granted us with flexibility and efficiency, yet security remains an open issue.

The proposed paper has familiarized the readers with two systems that have already been developed by the research team of the Biomedical Engineering Laboratory of the NTUA, as well as with an architecture that will enable their integration. Such an integration of a telemedical system that enables remote monitoring of patients with a watermarking module which enhances security and access control of sensitive information and ensures source and data authentication, is bound to provide value-added services to a range of health data management issues. It is the authors' strong belief that the implementation of the conceived architecture will tackle the disbelief of the few as regards authentication, security and integrity of sensitive medical data, and will - in the near future – comprise the solution for robust telemedical systems.

References

[1] EU 2003, e-Health Ministerial Declaration, e-Health Ministerial Conference, May 2003.

[2] A. Horsch, "Telemedicine and e-Health in recent years: Meeting the challenges," *Proc. 3rd Intern. Conf. on Inform. Commun. Technol. in Health, ICICTH'05*, Samos, Greece, July 2005.

[3] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "A multiple watermarking scheme applied to medical image management," in *Proc. 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBC'04*, pp. 3241-3244, San Francisco, USA, September 1-5, 2004.

[4] S. Pavlopoulos, E. Kyriakou, A. Berler, D. Koutsouris, "Emergency telemedicine applications using mobile and internet communication links - The AMBULANCE Project," *Proceedings of EURO-MED NET 98 Conference*, Nicosia, Cyprus, pp. 281-282, 1998.

[5] K. Perakis, K. Banitsas, G. Konnis, D. Koutsouris, "3G networks in emergency telemedicine – An in-depth evaluation & analysis," in *Proc. 27th Annu. Intern. Conf. IEEE Engineering in Medicine and Biology Society, EMBC'05*, Shanghai, China, Sept. 1-4, 2005.

[6] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Multiple image watermarking applied to health information management," *IEEE Transactions on Information Technology in Biomedicine*, to be published.

[7] D. Kundur, D. Hatzinakos, "Diversity and attack characterization for improved robust watermarking," *IEEE Trans. Signal Processing*, vol. 49, no. 10, pp. 2383-2396, Oct. 2001.