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

Watermarking SDK Implementation to Facilitate Integration in a Secure Healthcare Environment

Anastassios Tagaris, *Member, IEEE,* Aggeliki Giakoumaki, *Member, IEEE,* Lars Karle, and Dimitris Koutsouris, *Senior Member, IEEE*

***Abstract*—The implementation of digital watermarking technology in healthcare applications is still in its infancy; however, the benefits of exploring this technology towards secure and efficient health data management are steadily propagated and realized by the research community. The paper presents the architecture of a watermarking Software Development Kit (SDK), which provides multiple watermarking functionality and can be customized according to the targeted medical application, in order to address security of sensitive data, origin and data authentication, image archiving and retrieval. Two use cases of the proposed watermarking SDK are presented, the one involving access to the watermarking engine through a user interface, and the other referring to the case that the engine is embedded into the image acquisition device. The nature of the embeddable information that is applicable in each use case is also described.**

I. Introduction

THE rapid advances that have recently taken place in information and communication technologies have greatly affected the landscape of healthcare delivery and medical data management. Healthcare information is nowadays widely distributed and easily accessed, a fact that raises a number of pivotal issues relating to security and efficient management of sensitive data. The research community constantly seeks complementary and/or alternative solutions to the existing ones, in order to confront the new challenges. Digital watermarking is a rather new technology, which has already been explored in a variety of application fields; however, its potential to provide value-added services to healthcare information management and distribution, has only recently started to be realized. Watermarking medical images with the appropriate set of data provides the capability of effectively addressing issues including origin and data authentication, image archiving and retrieval, and sensitive data protection. This paper describes the architecture of a watermarking Software Development Kit (SDK), which delivers multiple watermarking functionality towards secure and efficient health data management. Furthermore, two use cases of the proposed watermarking SDK are presented.

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 (phone: +30 210 7722483; fax: +30 210 7722431; e-mail: tassos@biomed.ntua.gr)

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 (e-mail: agiakoum@biomed.ntua.gr).

L. Karle is with Eumdx, 33 Klimentos str., 1061, Nicosia, Cyprus (e-mail: lkarle@eumdx.com)

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).

II. Medical Image Watermarking

A range of medical data management and distribution issues, including among others data access and integrity control, origin identification, and efficient archiving and retrieval, can be addressed by medical image watermarking. A review of medical-oriented watermarking approaches found in the literature is presented in [1]. Due to the diverse characteristics and requirements of the watermarks depending on the specific application, multiple watermarks with varying robustness and capacity requirements need to be independently embeddable and retrievable, in order for a single watermarking scheme to simultaneously address a range of applications.

The multiple watermarking scheme that has been described in detail in [2], addresses several issues relating to security in contemporary health information systems, and also provides value-added services for efficient medical data management. Specifically, the scheme addresses a set of objectives including origin and data authentication, enhanced security of sensitive data and efficient image archiving and retrieval, by providing the option of embedding four types of watermarks; the watermark embedding and extraction procedures are based on wavelet image decomposition and quantization of coefficients. The four application-dependent types of watermarks that can be embedded are as follows:

i) Signature watermark: it may convey data to be used for origin authentication purposes; depending on the application, it could include the identification code of a remote telemedical unit or an image acquisition device, the name of the medical institution and/or the laboratory, the physician's digital signature, etc.

ii) Index watermark: it carries keywords that can be used for efficient data archiving and retrieval by hospital database management systems. These keywords may include diagnostic codes (e.g. ICD9/10 codes), the patient's identifier – for instance his/her Social Security (SSN) or Medical Record Numbers (MRN), or the code of the examination.

iii) Caption watermark: it may convey patient's personal

data (name and demographics) and information about the examination (date and time, examination report, diagnosis, etc.); besides, additional helpful information could be included by this type of watermark, such as the patient's medical summary, comments about the patient's status or examination, highlighting of diagnostically significant regions, or any other metadata that would assist in future reference or other physicians' guidance. The embedding of the above information in the image not only enhances medical confidentiality protection, but also guarantees a permanent link between the patient and his/her medical data.

iv) Reference watermark: it comprises a bit array that is known a priori at the recipient's site and allows the integrity control of the distributed images [3]. The extraction of the reference watermark from the image and its subsequent comparison with the originally embedded one provides the user with the capability to check whether the image has been tampered with during transmission or after storage; additionally, in the case of tamper detection, the user can check the possibly distorted image parts and decide whether the image is trustworthy or not.

Depending on the nature and size of the information that a watermark carries, distinct characteristics and requirements in terms of robustness and capacity arise. Indicatively, the signature watermark has limited payload needs, but on the other hand strict robustness requirements, due to its intolerance to even one error bit. The index and caption watermarks need also to be robust, however their capacity needs are much higher than that of the signature, especially in the case of the caption watermark. These demands along with the robustness and capacity that each decomposition level and subband provide, have been taken into account in the distribution of the watermarks within the images.

In order to guarantee that the quality and diagnostic value of the image are preserved throughout the watermarking process, the SDK provides the option of defining a Region of Interest (ROI); this ROI includes the diagnostically significant data and can be either excluded from the watermarking procedure or used only for integrity-checking reference watermarking. The SDK provides the means to customize watermarking according to the specific targeted application, thus providing the option of embedding the watermarks that are appropriate for each use case; in Section IV, different use cases of the watermarking module are described.

III. Watermarking SDK Architecture

The watermarking functionality may be delivered by the architecture that is presented in Fig. 1. The core of the system is the watermarking engine along with the API which can act both as watermark embedder and extractor.

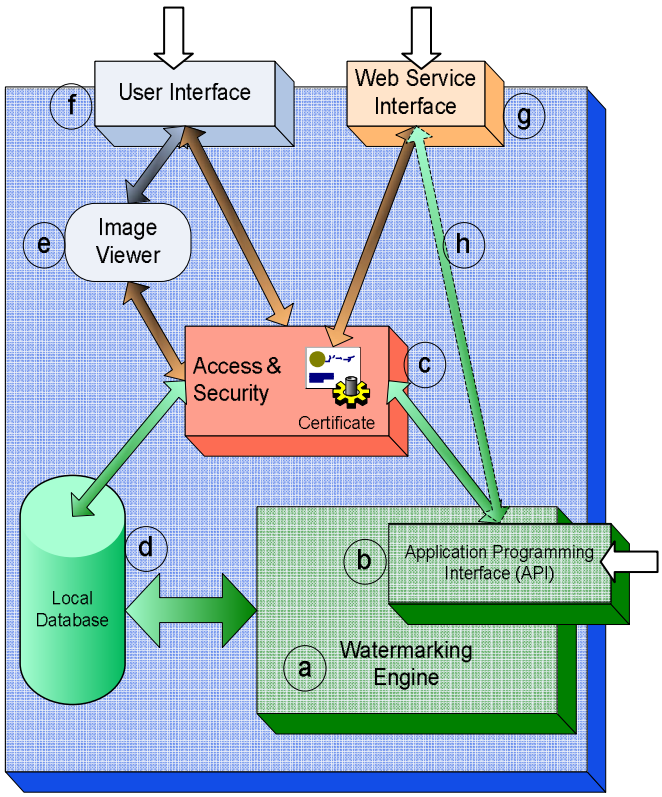

Fig. 1. Watermarking SDK architecture

The different components shown in Fig. 1 are defined below:

(a). Watermarking Engine: It is the core component of the SDK which implements the embedding and extraction of the multiple watermarks (signature, index, caption and reference).

(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 external SW to communicate directly with it. We foresee two basic use cases of the watermarking engine:

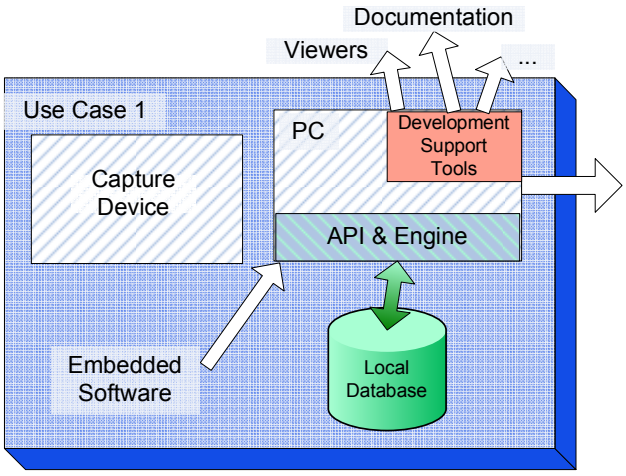

Fig. 2. Use case 1

i) Use case 1 (engine used through the SDK): In this use case the SDK may be installed in a normal PC. A set of development tools has been created in order to facilitate the integration of the watermarking SW with other applications. In that scenario the API of the engine is accessed through the User Interface and the Image Viewer. 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 API of the watermarking engine.

ii) Use case 2 (engine embedded in the device): This is the case where the engine along with the API is embedded into the medical device that captures the images.

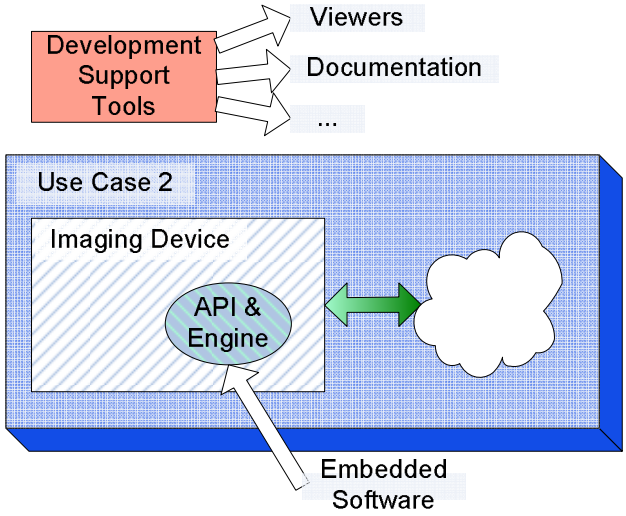

Fig. 3. Use case 2

In that case there is no use of other interfaces or security components as the whole procedure is automated and predefined by the device specifications. This approach enables device manufacturers to use watermarking procedures directly from their devices. The above two use cases are presented in more detail in Section IV.

An indicative list of the basic methods of the API is presented below:

fWRMRK_AuthenticateUser(un, pwd):Boolean

This method accepts a UserName and a Password and returns TRUE if the User Credentials are accepted or FALSE in the opposite case.

fWRMRK_ImageSIGNWTM(Img, ROI, data, var ErrNo, ErrStr): Img

This method accepts an image, an optionally selected Region of Interest (as an array of Coordinates), and the data to be embedded and returns the image watermarked with the signature. In case of an error it returns also an error ID and the corresponding string (message).

fWRMRK_ImageINDXWTM(Img, ROI, data, var ErrNo, ErrStr): Img

This method accepts an image, an optionally selected Region of Interest, and the data to be embedded and returns the image watermarked with the indices. In case of an error it returns also an error ID and the corresponding string (message).

fWRMRK_ImageCAPTWTM(Img, ROI, data, var ErrNo, ErrStr): Img

This method accepts an image, an optionally selected Region of Interest, and the data to be embedded and returns the image watermarked with the metadata. In case of an error it returns also an error ID and the corresponding string (message).

fWRMRK_ImageREFWTM(Img, ROI, var ErrNo, ErrStr): Img

This method accepts an image and an optionally selected Region of Interest and returns the image watermarked with the reference watermark. In case of an error it returns also an error ID and the corresponding string (message).

Similarly, there are methods to retrieve an image with different options, to proof that a watermarked image is still valid and not tampered with etc.

(c). Access & Security Component: This component authenticates users in order to use the API of 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. We may define two modes of operation:

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

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

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

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

ii) The users of the SDK as well as their access rights.

The local database could be extended in order to support storing of medical as well as demographic data of the patients. In that case the engine, the user interface and the viewer, make use of the database to store and find data (patient's data, images etc).

(e). Image Viewer: This component is a tool to display both the original and the watermarked images. The basic image manipulation functions are available to the user (brightness, contrast etc). The image viewer may be authenticated in an internal application level in order to have direct access to the engine's API. It may be considered also as part of the next component which is the User Interface.

(f). User Interface: The User Interface apart from the Image viewer, includes also the required controls to embed as well as to extract watermarks from images:

- Embed

i. Define which is the original image to be watermarked (either from the file system or the local database)
ii. Define the types of the watermarks to be used
iii. Define the group of data to be embedded
iv. Inform the user about the encoding (embedding) process of watermarking

- Extract

i. Select an already watermarked image
ii. Inform the user about the extraction procedure
iii. Display the extracted information

(g). Web Service Interface*:* This interface could be developed in order to "expose" the engine's API via the WWW and enable remote watermarking services.

All of the above described components are currently implemented using Microsoft's .NET Framework (v2.0). The local database is SQL Server 2005 but could be any other available RDBMS. Finally, the engine along with the API is implemented using C++ in order to achieve both efficiency (in terms of algorithm execution times) and portability (to facilitate Use Case 2).

IV. USE CASES

The two use cases of the proposed watermarking software that were presented in Section III, are described in more detail below.

The first use case involves accessing the watermarking engine through a user interface; after the image is captured by a medical image acquisition device, it is transmitted to a computer, where the watermarking SDK (Engine, UI, Viewer, Database) is installed. The user interface provides the user with a range of options including: a) definition of a ROI that should be either excluded from the watermarking procedure or used only for reference watermarking, b) selection of the types of the watermarks that should be used in a specific application, and c) manual entry of the data to be embedded. The embeddable information is application-dependent; indicatively, in case of a teleconsultation request by a remote health provision center, the patient's images to be sent to the expert physician could be watermarked with data such as: the identification code of the healthcare center, the doctor's digital signature, the patient's name and personal data. Other embeddable data could include the preliminary diagnosis, highlighting of diagnostically significant regions, comments about the patient's clinical status, and other metadata that would contribute in a trustworthy diagnosis. Apart from the origin identification data (contained in the signature watermark) and the patient's data (comprising the caption watermark), the user interface allows the option of embedding keywords to be used for efficient image indexing, archiving, and retrieval in Picture Archiving and Communication Systems (PACS). Finally, the reference watermark aiming at providing image integrity control, is also applicable in this use case.

The second use case involves the integration of the watermarking software in a medical image acquisition device (e.g. CT, MRI, ultrasound), which allows real-time embedding of information in the image, without the need of human intervention. In order for this on-line watermark embedding to take place, the watermarking engine along with its API are embedded into the medical image capturing device, thus enabling the automatic embedding of predefined watermarks in the images at the time of their acquisition. Due to the fact that in this use case the watermarking procedure is executed directly in the image acquisition device, the embeddable data may include the identification code of the imaging device, the name of the medical institution and/or the laboratory, and the date and time of the examination. Besides, in the case that the image capturing system provides the option of storing the patient's name or unique identifier (e.g. social security number or medical record number), these data could also be embedded in the image at the point of acquisition. Indicatively, this use case is applicable in emergency telemedicine and homecare incidents, where real-time watermarking without any manual data entry should be implemented; the nature and size of information to be embedded in these cases is predetermined and application-dependent. For instance, the mobile station ID and the time and date of an emergency treatment are adequate for the origin identification and the proper incident registration at the base station. On the other hand, in the case of homecare applications, the origin identification data could comprise a unique identifier of the patient and/or the registration name of the computer located at his/her home. The specific use case may also involve medical image acquisition devices located at laboratories within a hospital; in this case, the identification code of the laboratory and/or the device could be used as origin identification watermarks. Apart from the application-dependent source identification data, the integrity-checking reference watermark is applicable in all the application scenarios of the watermarking SDK.

V. DISCUSSION

The paper presents the architecture of a watermarking SDK that provides multiple watermarking functionality, aiming to enhance security and facilitate data management in healthcare information systems; furthermore, two use cases of the proposed watermarking SDK are presented. The current implementation of the watermarking engine supports only grayscale images. Nevertheless, there are plenty of medical devices nowadays that produce color images and/or video as output. Therefore, future work involves enrichment of the engine with watermarking algorithms that will support color images at first and video (image sequences) as the next step.

REFERENCES

[1] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Secure and efficient health data management through multiple watermarking on medical images," *Medical & Biological Engineering & Computing*, to be published.

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

[3] 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.