ORIGINAL RESEARCH

Using Digital Watermarking to Enhance Security in Wireless Medical Image Transmission

Aggeliki Giakoumaki, Ph.D.,[1] Konstantinos Perakis, Ph.D.,[1] Konstantinos Banitsas, Ph.D.,[2] Konstantinos Giokas,[1] Sapal Tachakra, M.D.,[3] and Dimitris Koutsouris, Ph.D.[1]

[1]*Biomedical Engineering Laboratory, School of Electrical and Computer Engineering, National Technical University of Athens, Athens, Greece.*
[2]*School of Engineering and Design, E&CE, Brunel University, West London, England.*
[3]*A&E Department, North West London Hospitals, West London, England.*

Abstract

Objectives: *During the last few years, wireless networks have been increasingly used both inside hospitals and in patients' homes to transmit medical information. In general, wireless networks suffer from decreased security. However, digital watermarking can be used to secure medical information. In this study, we focused on combining wireless transmission and digital watermarking technologies to better secure the transmission of medical images within and outside the hospital.* ***Methods:*** *We utilized an integrated system comprising the wireless network and the digital watermarking module to conduct a series of tests.* ***Results:*** *The test results were evaluated by medical consultants. They concluded that the images suffered no visible quality degradation and maintained their diagnostic integrity.* ***Discussion:*** *The proposed integrated system presented reasonable stability, and its performance was comparable to that of a fixed network. This system can enhance security during the transmission of medical images through a wireless channel.*

Key words: *encryption, wireless telemedicine, image transfer, digital watermarking*

Introduction

As the technologies grow, wired networks are increasingly being replaced by their wireless counterparts, leaving the wired infrastructure to serve only as a backbone. People value their mobility and all the emerging applications that provide them with the ability to freely move around. The medical world is no exception: an increasing number of medical applications rely on the treating physician and/or the patient using wireless means to deliver or acquire medical information. Wireless networks are the status quo in modern hospitals and have helped speed up procedures, deliver medical expertise, and manage time and space much more efficiently.[1]

Unfortunately, nothing good comes without a price: an increasing concern has been raised lately about the security of wireless networks. Both patients and physicians feel that since the range of the network is not fixed, anyone outside the hospital's grounds can gain access to the network and tamper with the data sent. Understandably, this is a grim scenario because such an action may have a severe impact on the patients' lives and their privacy.[2]

The wireless networks industry suggested various ways of encrypting data sent in a wireless channel and also controlling the user access in that channel. These included Wired Equivalent Privacy (WEP),[3] Wi-Fi Protected Access, use of RADIUS servers, and IPSec, with WEP being the simplest and most commonly used method of encryption.[4] There are, however, increasingly publicized concerns about the effectiveness of the above-mentioned algorithms and especially that of WEP, the industry's default wireless security standard.[5] Exploiting vulnerabilities in the implementation of the security

DOI: 10.1089/tmj.2009.0054

algorithms or even performing brute force attacks can lead to an intruder taking control of the channel and compromising security.

In addition, wireless networks present a number of drawbacks, such as quality of service as compared with other means of electronic communication (namely, utilizing the fixed infrastructure), increased packet loss, increased latency, and jitter. Nevertheless, it is not the purpose of this article to go into depth regarding these issues, as they have been analyzed in other network-oriented and non-healthcare-oriented publications.

In this context, there is a critical need to resort to complementary measures to effectively address increasing security threats in the healthcare sector. Digital watermarking is a promising research area that can be exploited toward this direction. Among its numerous applications, ranging from copyright protection to integrity control, its value-added role in healthcare systems only recently started to be realized.[6–8] Digital watermarking involves insertion of additional information directly into the data; from a healthcare perspective, this attribute can be explored by means of inserting (1) patient's sensitive information into his/her examination data for increased security, (2) physician's and/or medical device identification number for authentication, (3) keywords (e.g., patient's unique identifier and examination or diagnostic codes) for efficient data indexing, archiving, and retrieval, and (4) control arrays for integrity check.[9]

In this context, it would make sense to introduce an integrated system that would be able to combine the security strengths of digital watermarking with the ease of use of wireless networks in medical scenarios. Such a system should be easy to use by both medical personnel and patients, secure enough to transfer vital medical information, integratable into standard pieces of software, and expandable to accommodate future needs and developments. This article presents a compact and integrated system that helps to ensure the safe transmission and receipt of medical images in a hospital environment that is run under wireless links. This has been achieved by combining the current wireless networking security (WEP) with an additional level of security provided by digital watermarking. As far as the authors are aware of, the concept of using digital watermarking as a complementary security solution in this context is still in its infancy, and its implementation in an integrated WEP-based security system has not yet been realized.

Methods

The suggested system essentially comprises two different units that are eventually combined together: (1) the wireless network that is partially secured using WEP encryption, and (2) the digital watermarking module that provides an additional level of security by enabling the insertion of patient/examination-specific information directly into the image, as well as the verification of the integrity of the image itself.

WIRELESS NETWORK

A wireless network consisting of two access points (APs) was established at the Central Middlesex Hospital in London, to cover both the majors and minors accidents and emergency (A&E) wards. Much like in any cellular configuration the power of the APs was adjusted so that the range of each partially overlapped the range of its neighboring one to provide roaming capabilities for the mobile client. *Figure 1* shows the intersection of the range of the two APs within the majors and minors A&E wards of the hospital. Each of the APs created an area of about 100–150 m^2 with a third of that overlapping with the area of the next cell. Both IEEE 802.11b and g technologies were used, which operate at the license-free band of 2.4 GHz; 802.11b achieved slightly better coverage at the expense of lower speed (802.11g and b had a practical top speed of 18 and 4 Mbps, respectively).

To facilitate the wireless transmission of medical images within the medical environment, a mobile trolley that could easily roam around the A&E area was utilized, incorporating all the necessary hardware that would be used during the experiments. A lightweight laptop, connected with a high-quality camcorder, which in turn had the ability to connect to a variety of other medical equipment around the A&E area through their video-out connectors, was mounted on a light trolley, and by having been connected to the WLAN, it was considered a part of the hospital's network.[2]

For compatibility purposes, WEP, being the default 802.11b/g encryption, was utilized. WEP supports 48-, 64-, or 128-bit encryption key. Unfortunately, owing to the implementation of its security algorithm (RC4), the overall security is compromised: improper use of the initialization vectors leaks out information about the key regardless of its length. An attacker can calculate the key by gathering and analyzing a sufficient number of packets. Using an 128-bit key would only linearly extend the attacking period, which nowadays takes no longer than 15–30 min, according to the distance of the attacker from the AP.[3] Using the above-mentioned trolley, the treating doctor could use any of the system's input (camera, video-in, etc.) to capture high-quality medical images, and apply the watermarking sequence before the image is transmitted through the wireless channel. The image would normally be directly transmitted to another site—in most cases a site where a medical consultant resides. As proof of concept, the authors utilized the high-quality camcorder to capture the dermatological images,

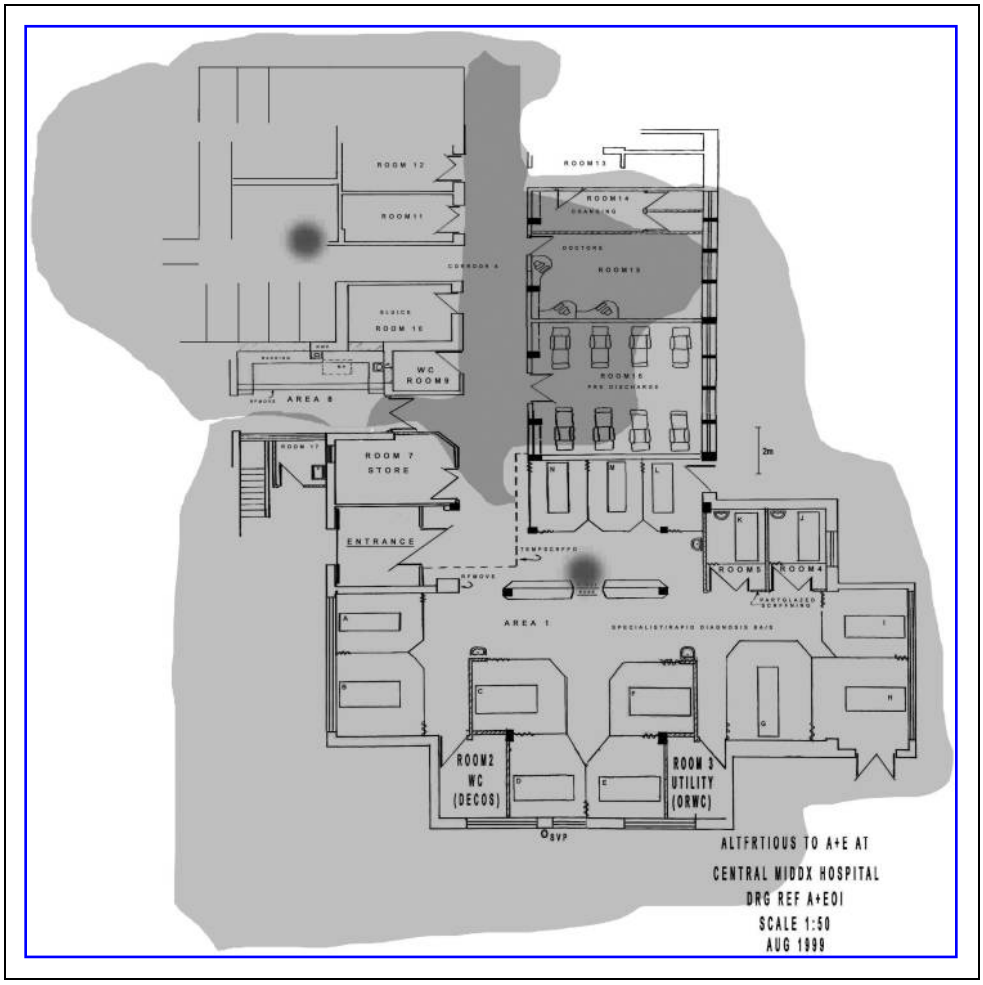

Fig. 1. Ground plan of the accidents and emergency (A&E) wards of the Central Middlesex Hospital indicating the intersection of the range of the two wireless access points.

whereas the other modalities were retrieved from the laptop's hard drive. Nevertheless, the same procedure was applicable for these modalities as well.

DIGITAL WATERMARKING MODULE

A digital watermarking software development kit was used to implement the digital watermarking module running at the roaming system within the A&E.[10] The underlying algorithm of the software development kit that was used applies discrete cosine transform for watermark embedding and is block based. The implemented digital watermarking module has a twofold role: on the one hand, it allows embedding of additional data regarding the patient, the examination, and the like, directly into the image; on the other hand, it enables verification of the image itself. As far as verification is concerned, the digital watermarking module generates an image-specific authentication code, which is embedded along with the additional patient's personal and examination data into the image during the embedding procedure. This authentication code may include a secure hash value or alternatively a digital signature, as well as a time-stamp, and is retrieved at the watermark extraction site for image verification. In addition, for security reasons, a secret key string is used during both watermark embedding and extraction, to allow for the retrieval of the embedded information by authorized users only.

During the customization of the watermarking module for the tests described in this article, the graphical user interface (GUI) was set to enable embedding of the following sequence of data in each image: (1) patient's first and last name, father's name, date of birth, and residence (street, municipality, city, and country), (2) image modality, (3) image time-stamp, (4) institute/clinic, and (5) general comments. As will be discussed in more detail in the Results section, the minimum number of characters that were embedded in each image in our trials was 160, which was the sum of all fields excluding the general comments. The maximum length of watermarks embedded was 2,000 characters, and there were also two intermediate embedding sequence lengths of 480 and 960 characters, respectively.

The GUI was utilized to embed the four different character sequences (160, 480, 960, and 2,000 characters) in sets of images of six different modalities, comprising computed tomography (CT), magnetic resonance angiography (MRA), magnetic resonance imaging (MRI), dermatological, radiological, and ultrasound images. Each

set included 5 images, thus reaching a total of 120 watermarked images for the evaluation phase. Regarding the acquisition of the aforementioned images, the high-quality camcorder, which was connected to the system, was utilized to capture the dermatological images, whereas the remaining images were retrieved from existing medical databases and were transferred to the system through a storage device. Three different image formats (JPEG, BMP, and TIF) were utilized for testing; however, the watermarking procedure is applicable to other formats as well, for example, to DICOM images, because the watermarking algorithm is applied only on the image pixels, not on the DICOM header, which is left intact by the whole process. Although it is beyond the scope of this article to go into detail about watermarking in DICOM images, it is noteworthy to mention that as far as DICOM images are concerned, watermarking can be exploited as follows: patient's sensitive data, for example, demographics, which are commonly included in the DICOM header, could instead be inserted as watermarks directly into the image; this would enhance security and would additionally provide a permanent link between the patient and the medical data, thus eliminating the risk of losing their association after a format change.[6–8]

After the transmission of the watermarked image and its reception at the consultant's site, the consultant utilizes the same GUI and inserts the secret key string to extract both the data and the authentication code for image verification (*Fig. 2*). Three different outcomes are possible:

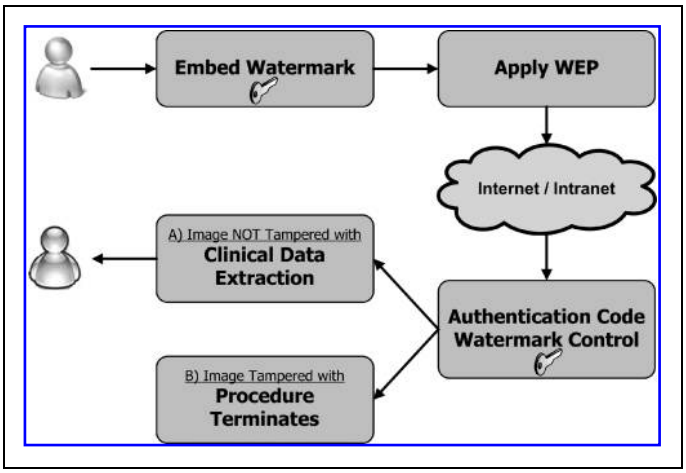

Fig. 2. Combining Wired Equivalent Privacy (WEP) encryption with digital watermarking to enhance security in wireless medical image transmission.

1. In case the secret key string is different from the one utilized during the embedding procedure, regardless of whether the authentication code could be successfully compared, the GUI returns an error message warning about the difference between the two key strings and prompts the user to insert the correct key string. In this case, the embedded information cannot be extracted until the correct key string is inserted.
2. In case the secret key string is correct and the authentication code is successfully compared, the extraction of the inserted data is also successful and the consultant gains access to them.
3. In case the secret key string is correct but the authentication procedure fails, the GUI informs the consultant that the image has been tampered with. In this case, the string sequence that was originally inserted cannot be extracted, and the GUI returns an error message providing the coordinates of the modified parts of the image.

A critical issue as far as watermarked images are concerned, especially in the case of medical images, is the evaluation of the image quality after watermarking. It is a common practice to use metrics such as peak signal–to–noise ratio (PSNR) to provide a numerical evaluation of the image quality after watermarking. For more completeness, we selected to calculate both PSNR and weighted PSNR (wPSNR) of the watermarked images; the latter is a quality metric that assigns varying weights to the perceptually different image regions, based on the noise visibility function (NVF), which reflects the masking properties of the human visual system.[6] The PSNR is measured in decibels and is defined as follows:

$$\mathrm{PSNR}\ (I,\hat{I}) = 10\log_{10}\left(\frac{\left[\max_{\forall(m,n)} I(m,n)\right]^2}{[1/N_I]\sum_{\forall(m,n)}\left[\hat{I}(m,n)-I(m,n)\right]^2}\right),$$

where I and $\hat{I}$ are the original and watermarked images, respectively, N_I is the number of pixels in the image, and $\max_{\forall(m,n)} I(m,n)$ is the maximum gray value of the original image. The denominator of the PSNR is the average sample mean squared error.

As mentioned above, the wPSNR is a quality metric that assigns different weights to the perceptually different image regions, based on the NVF. The NVF reflects the masking properties of the human visual system using a Gaussian model to estimate how much texture exists in any area of the image. For flat regions, the NVF value is close to 1, whereas for edge or textured regions, it is close to 0. The wPSNR is also measured in decibels and is defined as follows:

Table 1. Wireless Transmission Results of the Tested Medical Modalities

MODALITY	IMAGE DIMENSIONS (PIXELS)	AVERAGE SIZE (KB)	IMAGE FORMAT	TIME REQUIRED (AT 11 MBPS) (S)	TIME REQUIRED (AT 54 MBPS) (S)	ERRONEOUS PACKETS THAT NEEDED RETRANSMISSION (AVERAGE VALUE) (%)
CT	512×512	186	TIF	0.5	0.1	0.3
Dermatological	2,592×1,944	501	JPG	1.3	0.2	1.3
MRA	512×512	258	BMP	0.7	0.1	0.8
MRI	512×512	258	BMP	0.7	0.1	0.5
Radiological	500×640	314	BMP	0.7	0.2	0.6
Ultrasound	256×320	81	TIF	0.2	0.1	0.1

CT, computed tomography; MRI, magnetic resonance imaging; MRA, magnetic resonance angiography.

$$\mathrm{wPSNR}(I,\hat{I}) = 10\log_{10}\left(\frac{\left[\max_{\forall(m,n)} I(m,n)\right]^2}{[1/N_I]\sum_{\forall(m,n)}\left[(\hat{I}[m,n]-I[m,n])\bullet \mathrm{NVF}(m,n)\right]^2}\right),$$

where NVF(m, n) is the NVF value corresponding to the pixel (m, n), and the other variables are defined as in the PSNR formula.

Especially in the case of medical images being subjected to watermarking, it must be ensured that the watermarking process does not induce any degradation to them that would result in loss of diagnostic information and thus in the risk of misdiagnosis. Therefore, apart from addressing the issue of image quality evaluation based on the above-mentioned quality metrics, the watermarked images need to be evaluated by physicians as well. In the context of the work presented in this article, a blind review process took place; namely, two radiologists were provided with both the original and the watermarked images, without knowing which of them were the original ones, and were asked to evaluate their diagnostic information. The radiologists viewed the images in two ways before proceeding with their evaluation: for each medical modality test set, they first viewed the corresponding images, that is, the original images and the ones conveying watermarks of different sizes, individually, sequentially, and in a random order; then, they viewed them side by

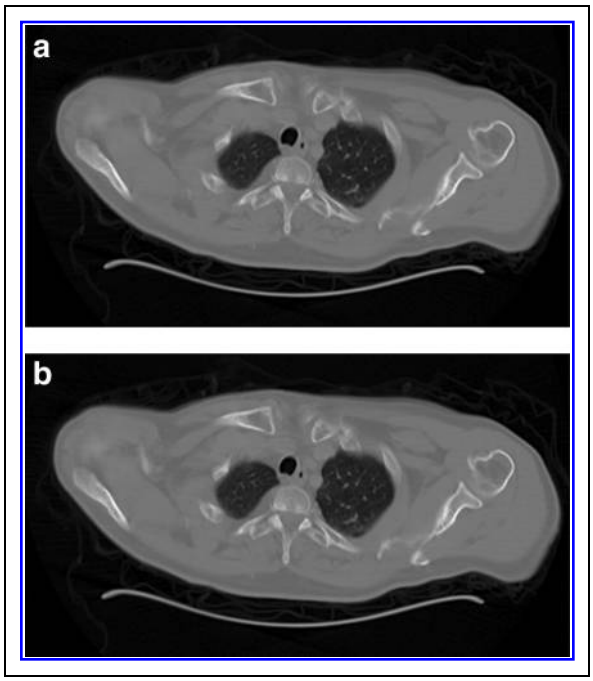

Fig. 3. (**a**) Original computed tomography test image. (**b**) Watermarked computed tomography test image.

Table 2. Average Peak Signal–to–Noise Ratio Values of the Watermarked Images for Each Tested Modality

MODALITY	PSNR (dB)			
	160 CHARS	480 CHARS	960 CHARS	2000 CHARS
CT	67.09 ± 0.04	63.37 ± 0.02	60.63 ± 0.01	57.78 ± 0.01
Dermatological	64.76 ± 0.30	60.41 ± 0.29	57.51 ± 0.37	54.56 ± 0.40
MRA	71.83 ± 0.07	68.15 ± 0.10	65.51 ± 0.11	62.47 ± 0.11
MRI	71.98 ± 0.10	68.15 ± 0.06	65.38 ± 0.05	62.32 ± 0.04
Radiological	72.64 ± 0.09	68.98 ± 0.08	66.27 ± 0.08	63.24 ± 0.10
Ultrasound	62.54 ± 0.03	58.48 ± 0.06	55.69 ± 0.07	52.78 ± 0.08

PSNR, peak signal–to–noise ratio; chars, characters.

side on flat-panel, 20-inch LCD monitors, with a resolution equal to 1,600 × 1,200. They were asked to report whether they were able to notice any difference among them, which would mean different diagnostic findings, or whether they would extract the same diagnosis regardless of the image that it would be based on. Given that the radiologists did not know which the original images were, they overcame the possibility of biased evaluation.

To test the integrity control capability of the watermarking module, we deliberately altered one image from each modality, namely, six images in total, after the watermarking procedure and before sending them to a consultant. The alterations were made using Photoshop and consisted of either blurring areas of the images (i.e., in the cases of MRI and ultrasound images) or painting areas of the images (i.e., in the cases of CT, dermatological, MRA, and radiological images). Those areas were deliberately very small in order not to be perceived by the human eye.

Results

In this research, we tested the hypothesis of further securing a WEP-enabled wireless network by adding digital watermarking in the medical data that it transmits through the air. For the first part of it, our tests showed that the established wireless network behaved very efficiently; the entire A&E ward was covered by two APs, and the mobile client, that is, the wireless trolley, could roam around that area without losing the connection. The system was tested for 7 days and a total of 50 h. It performed more than 35 handovers to the neighboring cell (roaming). It was also tested for real-time applications like carrying live streams (audio or video) or performing

Table 3. Average Weighted Peak Signal–to–Noise Ratio Values of the Watermarked Images for Each Tested Modality

MODALITY	WPSNR (dB)			
	160 CHARS	480 CHARS	960 CHARS	2000 CHARS
CT	82.14 ± 0.05	78.31 ± 0.02	75.31 ± 0.03	72.03 ± 0.04
Dermatological	72.47 ± 0.75	68.08 ± 0.46	65.23 ± 0.48	62.47 ± 0.50
MRA	86.98 ± 0.13	83.23 ± 0.03	80.52 ± 0.15	77.30 ± 0.29
MRI	87.13 ± 0.09	83.25 ± 0.06	80.35 ± 0.07	77.09 ± 0.05
Radiological	87.79 ± 0.06	84.06 ± 0.11	81.29 ± 0.18	78.12 ± 0.29
Ultrasound	77.42 ± 0.16	72.93 ± 0.37	69.53 ± 0.58	65.72 ± 0.87

wPSNR, weighted peak signal–to–noise ratio.

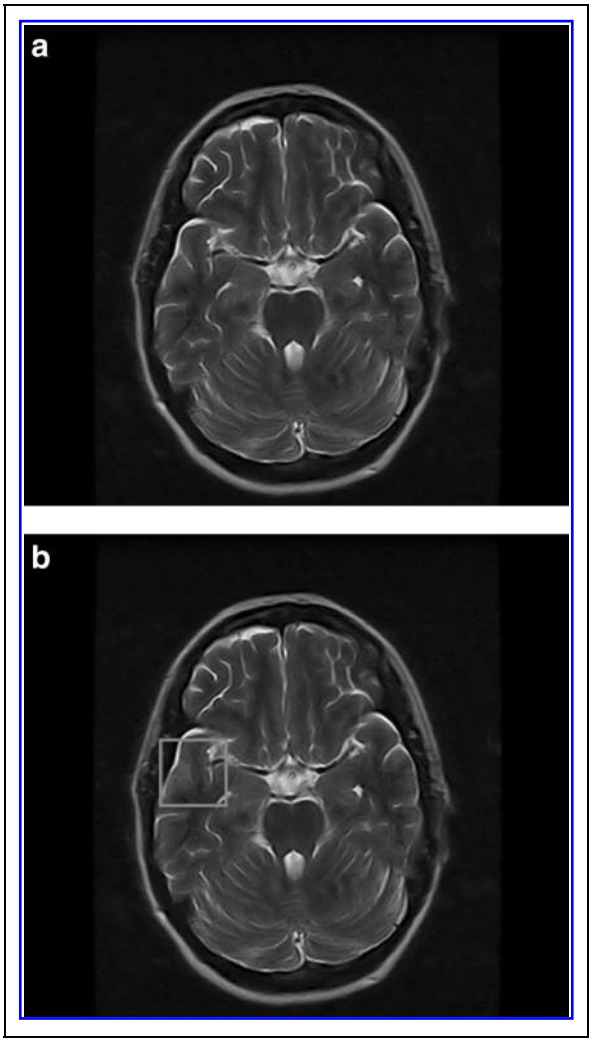

Fig. 4. (**a**) Watermarked magnetic resonance imaging test image. (**b**) The watermarking algorithm identified the part of the watermarked image (**a**) that was tampered with. The rectangle indicates the area of the original MRI test image (**a**) that was altered.

videoconferencing with an average required bandwidth of 400–500 kbps. While handing over from one AP to another, a small 1–4 s gap was introduced to the channel. Transmission control protocol/Internet protocol was used for image transfer; since transmission control protocol/Internet protocol guarantees reliable transmission, any kind of noise in the wireless channel that affected transmitted packets resulted in their retransmission, thus increasing the bandwidth occupied and/or the time to successfully send the file. *Table 1* summarizes the transmission times along with the average number of errors/packet retransmissions.

WEP use had negligible effect on the bandwidth occupied and on the number of erroneous packets. Even though the theoretical maximum transmission rates of IEEE 802.11b and IEEE 802.11g are much higher, during the testing activities the actual achieved maximum usable bandwidth was 3.8 and 18.2 Mbps, respectively. Finally, WEP cracking tools were used to test the vulnerability of the system. These tools took advantage of the weaknesses of WEP encryption and revealed the key in a matter of a few tens of minutes.

For the second part of the security solution, the digital watermarking module was utilized to embed four watermarks of different lengths, namely, 160, 480, 960, and 2,000 characters, in sets of images of six different modalities; each set consisted of five images, reaching a total of 120 watermarked images that were all transmitted and used for the evaluation phase. The modalities tested included CT, MRA, MRI, dermatological, radiological, and ultrasound images. The dimensions, format, and size of the tested images of each medical modality are presented in *Table 1*.

Figure 3 shows an original CT image and the resulting watermarked image, after the embedding of 2,000 characters. As illustrated in *Figure 3*, the watermarking procedure caused no visible degradation of the images, thus preserving their diagnostic significance. *Tables 2* and *3* present the average PSNR and wPSNR values obtained for each of the tested medical image modalities, respectively. As can be seen in these tables, the resulting PSNR and wPSNR values are high, thus indicating the negligible image distortion induced due to watermarking, in terms of numerical values.

Notwithstanding, such metrics cannot fully reflect the image degradation as it is perceived by the human eye; therefore, additional evaluation is needed. Particularly in the case of medical images, the most trustworthy results regarding perceptual quality can be obtained based on image evaluation conducted by medical experts, as mentioned above. For this reason, two radiologists from the A&E department of the North West London Hospitals were asked to evaluate the resulting watermarked images compared to the original ones, in terms of perceptual and diagnostic quality, following the evaluation approach described in the Methods section. According to the radiologists, no difference between the watermarked and the original images could be noticed in any of the images, thus avoiding any compromise on the quality of diagnostically significant parts. In general, as the size of the embedded information increases, the image is modified in a larger extent, thus resulting in larger degradation in quality; however, the evaluating radiologists did not notice any

difference even in the case of the maximum amount of additional information embedded (i.e., 2,000 characters), illustrating the efficiency of the addressed methodology.

As mentioned, the authors deliberately altered various images after the watermarking procedure and before sending them to a consultant, to test the integrity control capability of the watermarking module. In those cases, the authentication procedure failed and the GUI informed the consultant that the image had been tampered with; the string sequences that had been originally inserted could not be extracted, and the GUI returned an error message providing the coordinates of the modified parts of each of the distorted images. The result of such a case is graphically illustrated in *Figure 4b*, where the area of the original MRI test image (*Fig. 4a*) that was altered is pointed out with a rectangle.

Discussion

Regarding the wireless transmission, the proposed integrated system presented reasonable stability and its performance was comparable to that of a wired network. This system is capable of enhancing the security during the transmission of medical images through a wireless channel, in two ways: initially by using the default IEEE 802.11 security, WEP, and additionally by watermarking the medical images before transmitting them through the wireless channel. The integration of the watermarking functionality in a wireless network not only allows for additional information to be embedded in the patient's image, but also enables the receiving end to identify both whether the image has been tampered and whether the source of the image is an authenticated one. The proposed system is modular and easy to use: a GUI interface accepts two inputs, that is, image and data, and incorporates them into the wireless stream. The results of the tests showed the efficiency of the system in terms of both performance and image quality preservation. Future work involves large-scale tests of the proposed approach, using bigger and more representative data sets of different medical modalities commonly used in clinical practice. Further, more extended blind studies should take place regarding the radiologists' ability to reach an accurate diagnosis regardless of the watermarking process, before such an approach could be adopted in a clinical environment. Further clinical tests regarding user acceptability are also needed to have a more complete feedback by nonexpert users of the system.

Acknowledgments

This work has been supported by the General Secretariat for Research and Technology of the Hellenic Ministry of Development and the British Council.

Disclosure Statement

No competing financial interests exist.

REFERENCES

1. Tachakra S, Banitsas KA, Tachakra F. Performance of a wireless telemedicine system: MedLAN. *J Telemed Telecare* **2004;**12:298–302.
2. Banitsas KA, Tachakra S, Istepanian RSH. Operational parameters of a medical wireless LAN: Security, range and interference issues. *Conf Proc IEEE Eng Med Biol Soc* **2002;**1889–1890.
3. Earle AE. Wireless LAN security. In: *Wireless security handbook*. Boca Raton, FL: Auerbach Publications, **2006:**181–226.
4. IEEE Standard 802.11–1999. *Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*. Los Alamitos, CA: IEEE, **1999**.
5. Fluhrer S, Mantin I, Shamir A. Weaknesses in the key scheduling algorithm of RC4. In: Vandenay S, Youssef AM, eds. Selected areas in cryptography: 8th Annual International Workshop; Revised Papers/SAC 2001. London: Springer-Verlag, **2001:**1–24.
6. Giakoumaki A, Pavlopoulos S, Koutsouris D. Multiple image watermarking applied to health information management. *IEEE Trans Inf Technol Biomed* **2006;**10:722–732.
7. Coatrieux G, Lecornu L, Sankur B, Roux C. A review of image watermarking applications in healthcare. *Conf Proc IEEE Eng Med Biol Soc* **2006;**4691–4694.
8. Giakoumaki A, Pavlopoulos S, Koutsouris D. Secure and efficient health data management through multiple watermarking on medical images. *Med Bio Eng Comput* **2006;**44:619–631.
9. Giakoumaki A, Perakis K, Tagaris A, Koutsouris D. Digital watermarking in telemedicine applications—towards enhanced data security and accessibility. *Conf Proc IEEE Eng Med Biol Soc* **2006;**6328–6331.
10. MediaSec Technologies. *MediaSign digital—digital watermarking for authentication of digital media*. Available at www.mediasec.com/html/en/products_services/mediasigndigital.htm (last accessed September 12, 2008).

Address correspondence to:
Aggeliki Giakoumaki, Ph.D.
Biomedical Engineering Laboratory
School of Electrical and Computer Engineering
National Technical University of Athens
9, Heroon Polytechniou Str.
Athens 15773
Greece

E-mail: agiakoum@biomed.ntua.gr

Received: April 27, 2009
Revised: October 30, 2009
Accepted: October 31, 2009