RESEARCH ARTICLE OPEN ACCESS

DFRFT Domain Digital Watermarking On Medical Images for Wireless Networks

K. Jayaram M.E., MISTE[1], G. Ramachandran M.Tech, MISTE [2], S. Kannan M.E MISTE [3], L. Vasanth M.E MISTE [4], P.M Murali M.E MISTE [5]
Assistant Professor, Electronics and Communication Engineering
[1]Madurai Institute of Engineering & Technology, Madurai.
[2,3,5]VMKV Engineering College, Salem.
[4]Tejaa Shakthi Institute of Technolgy, Coimbatore

ABSTRACT
The wireless networks have been increasingly used both inside hospitals and in patients homes to transmit medical information. In general, wireless networks endure from decreased security.In this work, combining wireless transmission and digital watermarking technologies to better secure the transmission of medical images within and outside the hospital. 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 applying DFRFT domain digital watermarking to the medical images before transmitting them through the wireless channel. The DFRFT digital watermarking provides two additional freedom like DFRFT powers and watermark location that results in the possibility to embed more number of watermark bits than watermarking domains. The DFRFT powers and watermark location can be used as secret keys for such type watermarking technique. 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. This system can enhance security during the transmission of medical images through a wireless channel.

I. INTRODUCTION

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.2The 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 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.9In 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.

II. 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.

III. WIRELESS NETWORK

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.2For 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, whereas the other modalities were retrieved from the laptop's hard drive. Nevertheless, the same procedure was applicable for these modalities as well.

IV. DIGITAL WATERMARKING

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. 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.

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.

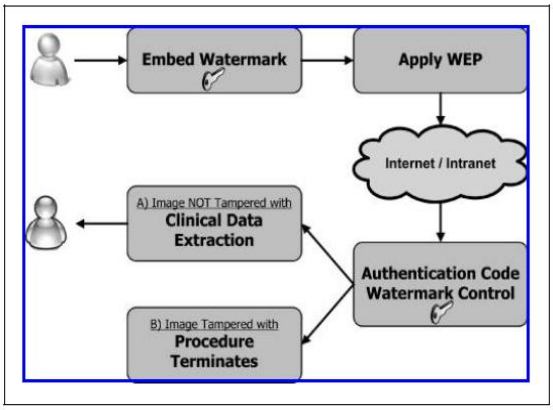


Fig-Combining Wired Equivalent Privacy (WEP) encryption with digital watermarking to enhance security in wireless medical image transmission.

Each Digital watermarking is a technology of protecting multimedia contents from intellectual piracy. It is achieved by embedding some information, called watermark, into original host media with minimum perceptual degradation. The watermark is detected or extracted to prove the ownership of multimedia content when an ownership dispute occurs.A watermarking algorithm is implemented for gray-scale images using 2D-DFRFT. A normal distributed random sequence is used as a watermark. This watermark is used to modify the DFRFT coefficients of an image for various locations and various length of watermark. . Then the inverse DFRFT is applied to give the watermarked image. The detection of watermark is performed through same transform operation. Then we compute the detection value from the DFRFT coefficients of watermarked image. We also find threshold value from some randomly generated sequences. Then comparison between the detection value and the threshold value is performed. It is decided that a watermark has been detected if the detection value is larger than the threshold value. There is a criterion given in [3] that a watermark has been detected if the detection value i.e. computed value of d is larger than a threshold, which is set to *E [d]/2*.

V. OVERVIEW OF DFRFT

The Fractional Fourier transform (FRFT) is the generalized form of the classical Fourier transform (FT). The FRFT is a powerful and potential tool for time-varying and non-stationary signal processing [4-6]. The FT corresponds to a rotation in the time-frequency plane over an angle equal to $\alpha = \pi/2$. But, the FRFT corresponds to a rotation over some arbitrary angle i.e. $\alpha = p\pi/2$. The *p*th order FRFT of a signal *f (x)* is defined as

$$F^{p}[f(x)] = \int_{-\infty}^{\infty} K_p(x,u) f(x)\,dx, 0 \le |p| \le 2 \qquad (1)$$

where, *Kp (x, u)* is the kernel function of the FRFT, and is given as:

$$K_p(x,u) = \begin{cases} \sqrt{\frac{i - j\cot\alpha}{2\pi}}\, \exp\left(j\frac{x^2+u^2}{2}\cot\alpha - j\frac{xu}{\sin\alpha}\right), & \text{if } \alpha \neq n\pi \\ \delta(u-x), & \text{if } \alpha = 2n\pi \\ \delta(u+x), & \text{if } \alpha = (2n+1)\pi \end{cases} \qquad (2)$$

where *p* is the FRFT order or power, α is the FRFT rotation angle. The relationship between p and α is given as $\alpha = p\pi/2$. The inverse of an FRFT with an order *p* is the FRFT with order p.

$$f(x) = F^{-p}\left[F^{p}(f(x))\right] \qquad (3)$$

VI. WATERMARK EMBEDDING

Digital image watermarking in DFRFT domain was also attempted earlier in [3]. In our digital image watermarking technique, first the DFRFT of the host image is computed. Then the DFRFT coefficients are sorted according to their magnitude in ascending order and the sorted array is denoted as *Zi=Xi+jYi.* Then the watermark is embedded into the DFRFT coefficients *Zi, i =L+1, ... , L+M.* The watermark itself is a normal distributed random sequence of M complex numbers.

Embedding of watermark modifies the sorted vector Zi as:

$$Z_i^{w} = Z_i + u_i |X_i| + j v_i |Y_i|, i = L+1,\ldots,L+M \qquad (4)$$

Then the modified array *Ziw* is rearranged in the original 2D array and the watermarked image is obtained by computing the inverse DFRFT.

VII. WATERMARK DETECTION

Watermarked image is first transformed by using DFRFT with same powers, and DFRFT coefficients are put in the same order as was used for embedding. Next the detection value (*d*) from the DFRFT coefficients of the watermarked image is computed as:

$$d = \sum_{i=L+1}^{L+M} [u_i - j v_i] Z_i^{w} \qquad (5)$$

The expected value of *d* is given as

$$E[d] = \frac{\sigma^2}{2} \sum_{i=L+1}^{L+M} \left(|X_i| + |Y_i|\right) \qquad (6)$$

The presence or absence of the watermark is decided based on the decision whether the computed value of *d* is greater/smaller than threshold, which is set to *E*[*d*]*/2* [3]. This seems reasonable since an image without a watermark has *E [d] =0.* The value d

for the correct watermark should stand out above this average. Here stand out can be defined as being larger than $\tau = \mu + 4\sigma$.

VIII. RESULTS AND DISCUSSION

Parameters used in watermark embedding and detection are DFRFT powers (p), watermark location (L), watermark length (M), and watermark variance ($\sigma 2$). Parameters used for performance measurement of this algorithm are PSNR and imperceptibility.

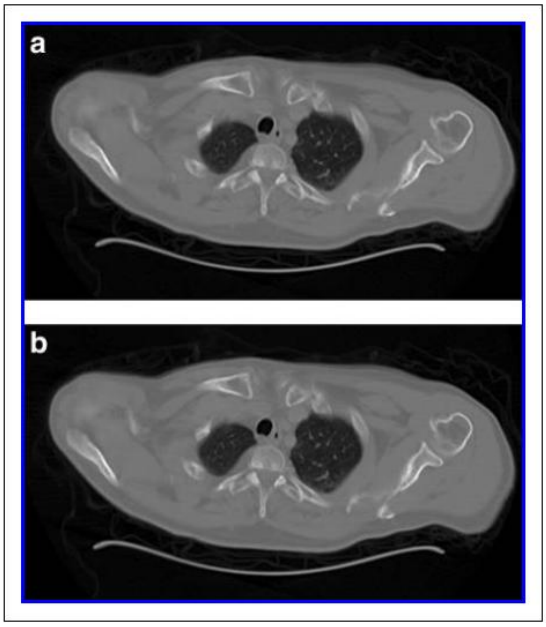
PSNR: PSNR is used to measure the objective quality of watermarked images. It is defined as

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \quad (7)$$

Where MSE is the mean square error of watermarked image with host image. MSE is defined as

$$MSE = \frac{1}{512\times 512}\sum_{x=1}^{x=512}\sum_{y=1}^{y=512}\left[p(x,y) - p'(x,y)\right]^2 \quad (8)$$

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
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.



(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.

IX. 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.

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] 10.X. Huang, Y. Luo, M. Tan, and D. Lin, "A Image Digital Watermarking based on DWT in Invariant Wavelet Domain," Proceedings of IEEE International Conference on Images and Graphics, ICIG 2007, pp. 329-336, 22-24 Aug.2007.

[11] G. Gui, L. Jiang, and C. He, "A New Watermarking System for Joint Ownership Verification," Proceedings of IEEE International Symposium on Circuits and Systems, ISCAS 2006, Page(s): 4 pp. 21-24 May 2006.

[12] I. Djurovic, S. Stankovic, and I. Pitas, "Digital Watermarking in the Fractional Fourier Transformation Domain," Journal of Network and Computer Applications, Vol.24, pp. 167-173, 2001.

[13] S.C. Pei and M.H. Yeh, "A Novel Method for Discrete Fractional Fourier Transform Computation," Proceedings of IEEE International Symposium on Circuits and Systems, ISCAS 2001, Vol. 2, pp. 585-588, 6-9 May 2001.

[14] C. Candon, M.A. Kutty, and H.M. Ozaktas, "The Discrete Fractional Fourier Transform," IEEE Transaction on Signal Processing, Vol. 48, No. 5, pp. 1329-1337, May 2000.

[15] F.Q.Yu, Z.K. Zhang, and M.H. Xu, "A Digital Watermarking Algorithm for Image Based on Fractional Fourier Transform," Proceedings of 1st IEEE International Conference on Industrial Electronics and Applications, ICIEA 2006, pp. 1-5, 2006.