**SETIT 2007**
4rth International Conference: **S**ciences of **E**lectronic, **T**echnologies of **I**nformation and **T**elecommunications
March 25-29, 2007 – TUNISIA

# Survey of Medical Image Watermarking Algorithms

K. A Navas* and M. Sasikumar**

*K. A. Navas
*Asst. Professor, College of Engineering, Trivandrum-16, Kerala, India*
**kanavas@rediffmail.com**
** M. Sasikumar
*Professor, Marian Engineering College, Trivandrum, Kerala, India*

**Abstract:** Watermarking in medical images is a new area of research and some works in this area have been reported world wide recently. Most of the works are on the tamper detection of the images and embedding of the Electronics Patient Record (EPR) data in the medical images. Watermarked medical images can be used for transmission, storage or telediagnosis. Tamper detection watermarks are useful to locate the regions in the image where some manipulations have been made. EPR data hiding in images improves the confidentiality of the patient data, saves memory storage space and reduce the bandwidth requirement for transmission of images. This paper discusses various aspects of medical image watermarking and makes a review of various watermarking algorithms originally proposed for medical images.
**Key words:** Medical image watermarking (MIW), DICOM, Electronic patient record (EPR)
.

## INTRODUCTION

Watermarking patient data in the medical image has become an interesting topic recently among the researchers. Though the watermarking is originally proposed for authentication of the images, the technology is adapted for hiding the EPR in it. Almost all the earlier works in medical image watermarking focused mainly on two areas; 1. tamper detection and authentication and 2. embedding EPR in medical images. Tamper detection watermarks are used for the probable manipulations done by the hostile people. Embedding of EPR in medical images will save storage space of the Hospital Information System (HIS), enhance confidentiality of the patient data, avoid detachment of the Electronic Patient Record (EPR) data from the image and save bandwidth for transmission [ 1, 2, 3, 4].

Authentication, integration and confidentiality are the most important issues concerned with EPR data exchange through internet [6, 9]. All these requirements can be achieved using suitable watermarks. The three requirements of general watermarks (robustness, imperceptibility and capacity) are of specific importance to medical images also. Since the medical images have region of interest (ROI), achieving the above requirements without adversely affecting the ROI is a real challenge to the researchers.

Coatrieux et al [8] asserts the relevance of the watermarking in medical images.

Though Piva et al [22] made a general analysis of watermarking techniques in medical imaging, they have not done an exhaustive search and discussion on different algorithms presented recently. This paper makes a search on different works done in MIW context. It will be of immense use for the researchers to understand the state of the art technology in this field. We also exhorts the need of an exclusive benchmarking for MIW. Section 2 discusses the application of MIW, section 3 discusses the advantages and the need of MIW. Section 4 describes the requirements of MIW, section 5 attacks on watermarked images section 6 benchmarking requirements, section 7 watermarking algorithms and section 8 conclusions of the work.

## 1. Applications of MIW

### 1.1 Integration and storage of medical data with images

Millions of medical images are being produced in various radiology departments of hospitals and research institutes around the world. These are invaluable source of information for medical students, practicing doctor and researchers. A lot of efforts are being made around the globe to integrate these images and corresponding metadata such as first information report and detailed diagnosis report about the patient. Munch et al [3] designed a web based method to integrate the data and images. The best way of integration of EPR and medicaln images is the hiding EPR in images.

**1. 2 Telediagnosis through www and e-mail**

Popularity of internet has become a boon to patients and low capital hospitals to utilize the facility to communicate with the clinicians for the diagnosis of the medical images. The medical images of different modalities can be sent to the clinicians residing at any corner of the globe for the diagnosis through internet. Earlier the first information reports (FIR) were sent by e-mail and medical images as an attached file with the e-mail to the remote clinicians. The watermarking techniques are adapted to attach the FIR with a Medical image thus saving any chance of detachment of the data from the image, in addition to the maintenance of the confidentiality of the data.

Watermarks are of great importance to telediagnosis because it functions as a mechanism to the authenticity of the image, nonrepudiation by the sending party, detection of the tampering of the data, memory and bandwidth saving, integrity of the image and so on.

Block diagrams of the watermarking system for telediagnois are shown in the figures 1 and 2. Figure 1 shows the transmission system and figure 2 receiver system. In the block diagrams I represents original image, PID patient identification details, PDR patient's diagnosis report, WMI watermarked image and AWMI attacked watermarked image. In a practical telediagnosis system a medical image watermarked with the PID will be sent by the hospital personnel to a remote clinician for analysis. PID is encrypted in the original image using a key before embedding for security and confidentiality. When the watermarked image gets transmitted through the internet clinician receives the attacked watermarked image. Clinician dewatermarks to separate the PID and I, analyses the image and embeds the encrypted PDR in the image and transmit back to the hospital using. The same transmit-receive system can be duplicated for the transmission of the data to hospital.

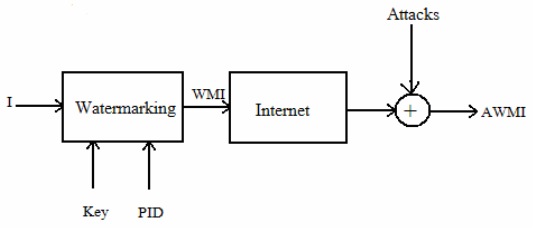


Fig 1. Block diagram of transmission system from hospital to clinician

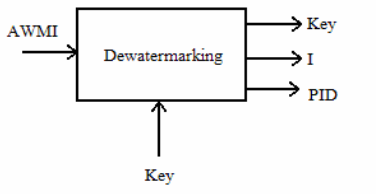


Fig 2. Block Diagram for transmission system from clinician to hospital

**1.3. Web based teleconferencing**

A team of doctors residing at different parts of the world can discuss and diagnose the medical image at hand. So much amount of funds are being spent by the governments world wide for setting up of effective web based telediagnosis systems. In such systems medical images are attached with EPR data. The watermarking techniques can be utilized in this application also. The work done by Munch et al [3] claims that the work done by them can be extended for web based teleconferencing for diagnosis.

**1.4. Annotation, authentication and tamper detection**

The important details can be stored in images imperceptibly, causing no harm to the ROI of the images. This kind of brief descriptions can be hidden in images immediately after the production of the images in the radiology departments. This kind of annotation hiding can be done by incorporating the watermarking mechanism in the different modality machines namely, CT or MRI scanners. Authentication watermarking is used to assure that any tampering has not been done by a hostile party. Telltale and fragile watermarking techniques can be used for this purpose.

## 2. Advantages of MIW

Though the watermarking was initially proposed for the authentication purpose, in medical imaging it is adapted for tapping many benefits. Important advantages are listed below.

**2.1 Memory saving**

Storage space required for the image and the patient record is very voluptuous. For small hospitals financial economy is an important decisive factor. Embedding the data in the corresponding images will save so much of the storage space. The memory for storage can be saved in HIS by embedding the EPR in the image because the image and the data become a single entity after watermarking.

**2.2 Bandwidth saving**

Huge amount of bandwith is required for the transmission of the image data for telemedicine purposes. The addition requirement of bandwidth for the transmission of the metadata can be avoided if the data is hidden in the image itself. Since the EPR and the image integrated into one, bandwidth for the transmission can be reduced in telemedicine applications.

**2.3 Avoiding detachment**

Millions of medical images are being produced in radiology departments around the world. Researchers in this field have done some works to embed patient data to medical images. The medical images generated in radiology departments have immense value to practicing medical professionals, medical researchers and students. Pengyu et al [20] developed a web based integrated medical image database and retrieval system for a convenient access by medical staff. Any

chance of detachment or access to wrong data may lead to a fiasco.

If the electronic patient record data and the image are separate, the chance of detachment of patient data from the image is too high. Misplacing a data will be very crucial in the case of medical image. To avoid this misplacing or detachment, data should be either integrated with the images using any software or hide it in the image itself.

**2.4 Confidentiality**
Normally a patient does not like to expose his medical report to public; especially if the disease is of clandestine nature. The utmost confidentiality can be maintained by hiding the data in the image.

**2.5 Security**
When the patient data text and image are sent separately, if a tampering is done on the text or image, the after-effects may even cost a life due to wrong diagnosis. Most of the internet users are ignorant of the esoteric terms of watermarking techniques. When the patient data is hidden in medical image, such people will not try to tamper it. If tampered, it can be made out by using appropriate watermarking technique.

**2.6 Nonrepudiation**
The marked images are distributed through internet or intranets between the Hospital Information Systems (HIS) for diagnosis or general telemedicine applications. Both the parties involved in the telediagnosis (hospital personnel and clinician) may repudiate that the data was not sent by them. This kind of situation may occur if the understanding between them gets vitiated or any breach of contract by any of them. Once the data is analysed by the clinician, the hospital is bound to pay the fees. Both parties could be in safer side by using keys. Key used by the hospital could be their logo and that by the clinician his digital signature.

## 3. Requirements of MIW

General watermarking method needs to keep the three factors (capacity, imperceptibility and robustness) reasonably very high. Robustness is the ability to recover the data in spite of the attacks in the marked image, imperceptibility is the invisibility of the watermark and capacity is the amount of data that can be embedded. These requirements are hindering each other. There must be some trade off among these requirements according to the applications. For medical images, in addition to the requirement on these factors, the region of interest (ROI) of the image must be particularly kept intact. This is an additional challenge to the researchers in this field.

**3.1 Imperceptibility** Watermark embedded in the image must be invisible to humane eye for the secrecy and confidentiality.

**3.2 Robustness** Robustness of the watermark is its ability to survive various image processing attacks. A secure watermark withstands against any purposeful attacks incurred on that. It should be able to recover PID and Patient Diagnosis Report (PDR) from the images for infallible diagnosis.

**3.3 Capacity** The data pay load that can be hidden must be as high as possible. This will make the analyst free from the restriction on the availability of space to write the detailed PDR.

**3.4 Authenticity** The data must be accessible only by the authentic users. Authentic users are the patients, HIS personnel and clinicians. Secret keys are used for this purpose. Umut et al suggested a biometric key based watermarking [21].

**3.5 Reversibility** The reverse should exist for the system of embedding to decipher the data from the image by the authentic user.

**3.6 Intactness of ROI** Medical image have region of interest. The watermarking schemes should not affect the ROI adversely. Distorted ROI will lead to wrong diagnosis. The enhancement of the requirement parameters should be done keeping the ROI intact.

**3.7 Complexity** The algorithm should be less complex to save execution time. For telediagnosis the speed becomes an important factor if the situation demands.

## 4. Attacks on MIW

When the image is transmitted through the internet, the probability of attacks is manifold. The attacks could be either purposeful or inadvertent.

**4.1 Geometrical attacks** The affine transformation such as rotation; scaling and translation (RST) of the image may lead to the distortion of the ROI and in turn to wrong analysis of the data in some cases. Geometric attack is considered as one of the most dangerous attacks on watermarks.

**4.2 Noise** If the images are kept for long time storage it may yield to speckle noise and if the images are transmitted Gaussian noise will affect the image adversely.

**4.3 Compression** Compression is normally done to any image for saving storage space. Watermark should be designed such that it will survive new compression algorithms.

**4.4 Collusion** If several similarly watermarked copies are available to the hostile person, s/he can recognize or remove the watermark or manipulate the data.

**4.5 Filtering** If the watermarked image is filtered, the patient data may get destroyed if the data is hidden in frequency band that is filtered out. High pass filtering is a normal signal processing attack to watermarks. Due to this reason, high frequency components are not used for watermarking purpose.

## 5. Benchmarking

If a watermarking system is to be used for a particular application, there must be a standard mechanism for the evaluation of the system Benchmark involves examining a set of mutually dependent performance factors. But there are no universally accepted performance measures applicable for every watermarking system. This calls for a benchmark exclusively for medical image watermarking. In addition to the existing evaluation parameters (visual quality, robustness, capacity) medical image watermarking evaluation must include ROI in the medical image as another parameter. The robustness of the system must be checked against all the possible transmission and storage attacks. Rather than performing the evaluation on images of different formats, the medical image format can be confined to the DICOM standard. The EPR diffusion into medical images requires more concentration into the capacity of data hiding without affecting visual quality of the image. The evaluation of imperceptibility of the mark must consider the properties of Human Visual System. The security of the system is dependent on the watermarking key and the performance evaluation of the system must be done by varying the embedding strength and different type of keys. The delay encountered during embedding and recovery of the watermark is also an important factor in telemedicine applications.

To our knowledge, no works have been reported on a formulation of benchmarking exclusively for MIW.

## 6. Watermarking algorithms

The works on watermarking medical images are classified into two. 1) tamper detection and authentication and 2) EPR data hiding. Tamper detection watermarks are able to locate the regions or pixels of the image where tampering was done. Authentication watermarks are used to identify the source of image. EPR data hiding techniques gives more importance in hiding high payload data in the images keeping the imperceptibility very high.

### 6.1 Tamper detection and authentication algorithms

The priority order of tamper detection and authentication watermarking methods is imperceptibility, robustness and capacity.

#### 6.1.1 Hyung et al algorithm[11]

To avoid illegal forgery, ROI information is embedded in the no-ROI region. This technique is implemented in wavelet transform for high robustness. Initially, the medical image is separated into two parts, ROI and non-ROI. Then the ROI image is embedded into the non-ROI part. ROI image is transformed into three level DWT and the wavelet coefficients in third level approximation coefficients are represented to 8bit plane. Then each of bit-plane information is matched to the size of non-ROI region and it is used as the watermark in the non-ROI using the embedding equation.

.

#### 6.1.2 Giakoumaki et al algorithm[12]

Simultaneous embedding of three types of watermarks is proposed by giakoumaki et al. A robust watermark containing doctor's identification code to achieve confidentiality and authentication, a caption watermark conveying patient's information and a fragile watermark for tamper detection. The method is implemented in wavelet transform domain. Watermarks are embedded in selected detail coefficients based on a key.

#### 6.1.3 Hiral et al algorithm[13]

This method provides exact authentication to medical image through reversible or erasable watermark. This method provides exact recovery of the original image at recipient end after the removal of watermark from the image. The technique discussed is based on correlation watermarking. The merits of this method are very good perceptual transparency for watermarked image, recovery of the original cover image, and high value of PSNR**.** The digital signature is computed using all information in image and then embeds signature in an erasable manner within the image. This signature is unique for each image. At the receiving side the recipient computes a one way Hash and compare it with a Hash decoded from the signature. If the two hashes are identical received image is considered authentic.

#### 6.1.4 Wakatani algorithm[5]

The distortion of the ROI is avoided in this technique by embedding signature information into other area than the ROI. Signature image compressed by a progressive coding algorithm is used as the signature information. The most significant information of the signature information is embedded in the nearest area to the ROI. Authors claimed that the method can detect the signature image with moderate quality from a clipped image including the ROI. The signature image with moderate quality can be acquired from a clipped image including only part of the ROI. Wavelet transform is used.

#### 6.1.5 Wang and Rao algorithm[14]

This is a fragile watermarking algorithm suitable for real-time diagnosis based on least significant bit (LSB), hash function and chaotic sequence. To resist counterfeiting attack, the watermark signal is extracted from the original image. The watermark signal is then processed by exclusive-OR (XOR) operation with the chaotic sequence in order to increase the security of the watermarking algorithm. Further it is embedded in the LSB of the host image. The experimental results showed that the watermark is imperceptible and robust.

#### 6.1.6 Zain et al algorithm[15]

The purpose of this method is to verify the integrity and authenticity of DICOM images. They used 800x600x8 bits ultrasound images in their

experiments. Hash of the whole image is embedded in the least significant bits of the RONI (Region of Non-Interest). If the image has not been altered, the watermark will be extracted and the original image will be recovered. Hash of the recovered image will be compared with the extracted watermark for authentication**.**

**6.1.7 Birgit et al algorithm** [16]
The image is separated into regions and characterizes each region according to some features. Each region is then watermarked with a particular watermark method and payload capacity such that perceptual degradation is limited. Results on MR and CT images demonstrated that less visually sensitive areas on images can be watermarked using more robust techniques and more sensitive areas can be watermarked using lighter or no embedding.

**6.2 EPR Data hiding algorithms**
The priority order of requirements of EPR data hiding is imperceptibility, capacity and robustness. Primary EPR data, diagnosis report and digital signatures of radiologist and clinician are to be embedded in the medical image. Hence the capacity becomes an important requirement.

**6.2.1 Deepthi and Niranjan algoritm** [10]
LSB technique of datahiding in spatial domain is proposed in [2]. Text file that to be hidden consisting of ASCII characters is encrypted using a log function

The bits in the equivalent binary number of the resulting digit are interleaved in the LSB of the gray level values. Graphical data such as ECG or EEG signals are also hidden in the image after the conversion into binary DPCM. The assessment of the method is done using Normalised Root Mean Square Error (NRMSE) parameter. Authors claim that the watermarked image was found perceptually good proximity to the original image. The histograms of the original and watermarked were also found similar to each other.

The technique is very simple and hence the implementation time is very less. This technique is suitable in the situations like immediate diagnosis is required. This technique is not robust against image processing attacks. Tampering of the watermarks is also possible.

**6.2.2 Acharya et al algorithm** [4]
With an intention to reduce the storage space and transmission bandwidth, a technique of embedding EPR data in medical images is suggested by Acharya et al. EPR data consist of text file and graphs. Text file is the preliminary report about the patient from the radiology department of the hospital and graphs are ECG or EEG. It is an LSB technique implemented in spatial domain. The ASCII characters in EPR data are encrypted before interleaving in medical images to improve the security of the data using Rijndael algorithm.

During transmission or storage the data are susceptible to Gaussian noise. To encounter the noise effect substantially, channel coding technique has been used. Each LSB of the medical image pixels are replaced by the bits in the binary equivalent of the encrypted and error correcting coded ASCII characters. Hamming code was found to be superior to repetition code against Gaussian noise.

The complexity is less and hence execution time is less. This technique is suitable for speedy embedding and retrieving of the watermark. This makes it suitable for low budget hospitals to send the medical images to remote clinicians for the diagnosis, especially if the situation demands urgent diagnosis of the image. Mediocre systems are enough to embed and recover the patient report. LSB technique is not robust to even intentional image processing attacks like compression. This method is susceptible to noise and cropping attack.

**6.2.3 Acharya et al algorithm-2** [2]
LSB technique of datahiding in frequency domain is proposed in [2]. The image is transformed to frequency domain using DCT. The coefficients are run length encoded. Variable length Huffman encoding is used to save memory space. Text file that to be hidden consisting of ASCII characters is encrypted and the bits in the equivalent binary number are interleaved in the LSB of high frequency DCT coefficients. Graphical data such as ECG or EEG signals are also hidden in the image after the conversion into binary DPCM. The assessment of the method is done using Normalised Root Mean Square Error (NRMSE) parameter. Authors claim that the watermarked image was found perceptually good proximity to the original image. The histograms of the original and watermarked were also found similar to each other.

The technique is more robust than spatial domain LSB technique. If any manipulation is done on the image to tamper or remove the watermark, watermark and the cover image will be equally affected.

**6.2.4 Fan and Honghin algorithm**[18]
This is a high capacity method exploiting the limitations of human vision system. Watermarking is done using noise visibility function (NVF). The cover image adaptive watermarking embeds strongly and invisibly. The implementation is done in spatial domain. Though intended for a high capacity, this method is not enough to hide complete EPR and digital signatures.

**6.2.5 Jagadish et al algorithm**[19]
The ASCII characters in EPR text are encrypted using Rijndael algorithm before hiding it in images. Signal graphs (ECG, EEG EMG etc.) are compressed using DPCM technique before hiding. To enhance the robustness of the embedded information, the patient information is coded by Error Correcting Codes such as (7, 4) Hamming, Bose-Chaudhuri-Hocquengham (BCH) and Reed Solomon (RS) codes. The noisy scenario is simulated by adding salt and pepper noise to the embedded image. For different Signal to Noise Ratio (SNR) of the image, Bit Error Rate (BER) and

Number of Character Altered (NOCA) for text data and percentage distortion (PDIST) for the signal graph are evaluated.

**6.2.6 Xuanwen et al algorithm**[17]
In order to increase the embedding capacity the eight bit planes are loselessly compressed and the data are embedded in the saved space. In the reverse process, decompression is done after extracting the data. Authors claimed to increase maximum number of embedded bits (MNEB) tolerating the distortion.

**7. Conclusions**
The philosophy, methodology, characteristics and requirements of medical image watermarking have been given in detail. We raise the need of benchmarking exclusively for MIW. For the novice researchers in this field this survey will be of immense use. Presently the authors are working to stipulate the benchmarking standard exclusively for MIW.

## REFERENCES


[1] Ingemar J. Cox, Matthew L. Miller, Jefrey A. Bloom, *Digital watermarking*, (Morgan Kaufmann Publishers, 340 Pine Street, Sixth floor, Sans Francisco, CA, USA, 2004)

[2] Rajendra Acharya U., U. C. Niranjan, S.S. Iyengar, N. Kannathal, Lim Choo Min "Simultaneous storage of patient information with medical images in the frequency domain, C*omputer Methods and Programs in Biomedicine*, Vol. 76, 2004, pp.13-19.

[3] H. Munch, U. Englemann, A. Schroter, H.P. Meinzer "The integration of medical images with the patient record and their web based distribution*" Journal of Academic Radiolog*, 11(6), June 2004, 1995, pp.661-668.

[4] Rajendra Acharya U., P. Subhanna Bhat, Sathish Kumar, Lim Choo Min, Transmission and storage of medical images with patient information, *Journal of Computers in Biology and Medicine,.33*, 2003, pp.303-310.

[5] Akiyoshi Wakatani, Digital watermarking for ROI medical images by using compressed signature image" *Proc. of the 35th Int. Conference on System Sciences-2002*.

[6] Hui-Mei chao, Chin-Ming Hsu, Ahaou-Gang Miaou, A data hiding technique with authentication, integration and confidentiality for electronic patient records, *IEEE trans. Inf. Tech. in biomedicine, 6(1)*, March 2002, 46-53

[7] Dan Yu, Farook Sathar, Kai-Kuang Ma Watermark detection and extraction using independent component analysis, *EURASIP J. on Applied Signal Processing* 2002, 92-104.

[8] Coatrieux G, H. Maitre, B. Sankur, Y. Rolland, R. collorec, Relevance of watermarking in medical imaging, *Proc. IEEE EMBS int. conf. on Inf. Tech. applications in Bio-medicine*, 2000,250-255

[9] Xuang Kong, Watermarking medical signals for telemedicine, *IEEE trans. Inf. Tech. in Bio-medicine, 5(3)*, 2001, 195-201.

[10] Deepthi Anand., U. C. Niranjan "Watermarking medical images with patient information", *Proc. 20th Annual Int. Conf. of IEEE engineering in medicine and biology*, vol. 20, No. 2, 1998.

[11] Hyung-Kyo Lee, Hee-Jung Kim, Ki-Ryong Kwon, Jong-Keuk Lee, ROI Medical Image Watermarking using DWT and Bit-plane, 2005 *Asia-Pacific Conference on Communications, Perth, Western Australia*, 3 - 5 October 2005.

[12] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris Proceedings of the 25th *Annual Intemational Conference of the IEEE EMBS*, Cancun, Mexico September 17-21,2003

**[13]** Hiral M Desai, Mehul S Raval, Ajay I Trivedi Correlation-based Reversible Watermarking technique for Medical Images.

[14] Wang Gang, Rao Ni-ni A Fragile Watermarking Scheme for Medical Image *Proc. of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference* Shanghai, China, 2005

[15] J. M. Zain, L.P Baldwin, M. Clarke Reversible watermarking for authentication of DICOM images *Proc. of the 26th Annual International Conference of the IEEE EMBS* San Francisco, CA, USA, September 1-5, 2004

[16] Birgit M. Planitz and Anthony J. Maeder A Study of Block-based Medical Image Watermarking Using a Perceptual Similarity Metric

[17] Xuanwen Luo, Qiang Cheng, Joseph Proceedings of the A Lossless Data Embedding Scheme for Medical Images in Application of e-Diagnosis *25th Annual Intemational Conference of the IEEE EMBS*, Cancun, Mexico, September 17-2 1,2003

*[18]* Fan Zhang and Honghin Zhang, Digital Watermarking Capacity Research *Proc. Circuits and systems, ICCAS* 2004

[19] Jagadish Nayak, P. Subbanna Bhat, M Sathish Kumar, Rajendra Acharya Reliable And Robust Transmission And Storage Of Medical Images With Patient Information Proc. *International Conference on Signal Processing & Communications (SPCOM)*, 2004,91-95

[20] Pengyu Caoa, Masao Hashibab, Kouhei Akazawaa,b, Tomoko Yamakawaa, Takayuki Matsuto, An integrated medical image database and retrieval system using a web application server *International Journal of Medical Informatics* (2003) 71, 51-55

[21] Umut Uludag, Sharath Pankanti, Salil Prabhakar, Anil K. Jain, biometric cryptosystems: issues and challenges, *Proceedings of theIEEE*, 92(6), 2004.

[22] Alessandro Piva, Franco Bartolini, Iuve Coppini, Alessia De Rosa, Elena Tamburini, Analysis of data hiding technologies for medical images, *Proceedings of SPIE-IS&T Electronic Imaging, SPIE* Vol. 5020 (2003).