International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 01, January-June 2016
www.arresearchpublication.com
IJEEE
ISSN 2321 - 2055

APPLICATION OFWATERMARKING TECHNIQUES INMEDICAL DATA

Swati Mishra[1], G.R Mishra[2]

[1, 2] *Department of Electrical and Electronics Engineering*

Amity School of Engineering and Technology, Amity University, Lucknow, (India)

ABSTRACT

In hospitals medical images are generated, presented, transmitted and stored in digital form. As they are in the digital form they are vulnerable to attacks, thus there has been a rising interest to provide protection to the medical images against internal/externalattacks. Digital Watermarking for medical image has been employed as a method to enhance medical data security, secrecy and authenticity. Medical image watermarking necessitates extensive attention while embedding secondary data within the medical images (primary/host/cover image) because this process of embedding data into cover data should not affect the quality and originality of the medical image. Exploration systems utilized for medical diagnosis of the patient depends upon the assessment of medical images. CR, CT and MR, obtains images that can be stored in digital formats such as (DICOM files) which are related with data of patients and information about the study. The aim of this paper is to briefly describe the schemes for the protecting and preserving the authenticated medical records of patient in the hospitals utilizing concept of watermarking on the medical data.

Keywords: Digital Watermark, Information Hiding, Medical Imaging,Media Security, Mobile Security

I. INTRODUCTION

Image watermarking has emerged as a significant research area in data security, privacy and image integrity. Medical image watermarking entails extreme attention while embedding additional data within the cover medical images, because this embedding of data should not affect the quality of image. Medical images are stored for different purposes such as diagnosis, long time storage and research database. The significance of the security of medical data has been emphasized in the medical field, especially pertaining to information concerning patients (diagnosis, personal data and studies) [1].

The rapid increase in transmission of medical data over internet has been witnessed and the need of fast and secure diagnosis in the medical field has been realized. The secure diagnosis found its solution with the watermarking and made medical image transmissions secure. Many of the examination systems used in the medical diagnosis are centered on the study images. The conventional radiology, CT and MR, obtains images that are stored in digital formats which are related with patient data and information about the study, e.g.: patient name, study type and date, among others. Digital Imaging and Communications in Medicine (DICOM) is one of the digital formats that was created by the National Electrical Manufacturers Association (NEMA) to

provide assistance in the distribution and inspecting medical images and other data [2].DICOM file contains a header, and in the header information like patient's name, the type of scan, image dimension, etc. are stored.

Due to the recent increase in identity theft cases, the protection of private data has been the focus of many scientific efforts. In the years to come, healthcare systems are expected to experience a drastic change in its structure and organization as indicated, for example, in the Healthcare 2015 report showing that governments, health regions, hospitals are allotting billions of dollars into multiple medical initiatives [1]. As the volume of health care data increases, more complex, storage and accessibility of medical information is not only invaluable but also necessary. Protection against unauthorized access on personal patient data and medical history data is something that can protect a patient's sensitive data from identity theft schemes and can also protect the healthcare as well as insurance system from deceitful claims. Watermarking is implemented both onimages,audio as well as on video by using various methods likewavelet transform,Fourier transform and approaches based on independent component analysis [3, 4,5].

This rest of the paper is organized as follows: section II outlines the characteristics of medical information records.In section III the watermarking schemes applied in medical images and the watermarking requirement against the attacks has been discussed, which is followed by the section IV which concludes the objective of the study.

II. CHARACTERISTICS OF MEDICAL INFORMATION RECORDS

Medical Imaging is a field of the protecting integrity and confidentiality of the medical information, which is originated from ethics and legislatives rules. Patient's medical record is an assemblage of clinical examinations, prescriptions, diagnosis and images in several modalities. The information provided by the records are used for different purposes like: epidemiological studies and clinical research. All the medical records, whether it be electronic or not, are associated with the medical secrecy, and thus these records must be kept confidential.The medical information records must reflects characteristics like confidentiality, reliability, integrity, authenticity and availability. By confidentiality we mean to say that the access to the medical record of the patient should be given to the authorized user. The access to the patient's medical record should not be given to unauthorized person, as this act can emerge as threat. The record should be reliable and should possess integrity i.e. the information contained in the records should not be modified by the unauthorized user. Authentication i.e. the proof that the medical information belongs to the intended patient only is another characteristic that should be contributed by the medical information records.

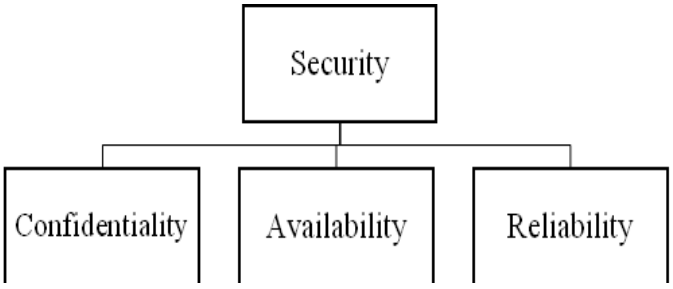

Figure 1 Security components in medical information

III. WATERMARKING TECHNIQUES IN MEDICAL IMAGE

There has been augmenting interest in watermarking techniques to offer protectionto the intellectual property in digital formats e.g. images, video, audio, software. As result of this rising interest in the field of watermarking several techniques have been developed. Data hiding techniques i.e. steganography and watermarking are techniques for the secured communication. Steganography describes a technique to secrete point to point communication concerning two parties.However a watermarking system, would embed information that could not be extracted or modified without entirely formulatingthe object intoinoperable. There are some steganography approaches that does not offers robustness against attacks andalterationsof data duringstorage,transmissionor format conversions [6].

3.1 Watermarking Requirements Against Attacks

Contrary to steganography, watermarking has some additional requirements against all possible attacks which can be termed as follows:

- Robustness: Robustness means that the watermarking structure should be able to preserve the watermark under numerous attacks like rotation, scaling, translation, additive noise, compression, filtering etc. [7].
- Imperceptibility (Quality): Watermarking approach should not affect the quality of the cover image or the embedded data after watermarking. The degradation in quality of host image should not be perceptible to the human vision [7].
- Capacity: It is significant to determine the sum of information that one can embed in a primary image, the amount of information to be embedded into depends on the application (copyright protection, medical safety, fingerprinting etc.) [7], as this information may be anumber, a logo, hash code, etc.

3.2 Application of Watermarking in Medical Data

There are several studies in the literature which are dedicated to application of watermarking in medical images. Anand *et al*. [8],proposedan approach to insert an encrypted version of the EPR (Electronic Patient Record) in the LSB (Least Significant Bit) in medical image's gray scale level. Even thoughthe degradation caused in the quality of image is minimum, the limitations and tenuousnessof LSB watermarking are well-known. Miaou*et al*. [9] put forward an approach to validatethe origin of the transmission.

Macq and Dewey [10]proposed method in which they insert useful information in the headers of medical images. The approaches proposeddoes not reflect characteristic of robustness against attacks such ascompression,filtering, additive noise, as well as against geometrical attacks such as scaling or rotation transformations. Toovercome the limitations,Rodríguez-ColínRaúl et al.utilized the image moment theory to normalize the image to ensure robustness against active attacks. In this paper they [11] proposed a watermarking approach that combinesencryption,data compression and watermarking techniques and then applied image moment theory to radiological medical images. They have utilizedDICOM data as a watermark, which is supposed to be embedded in medical images.The blind watermarking scheme has been utilized,where in the extraction process it only requires the secret key used in the cryptographic step.

Sung Jin Lim*et al.*[12]proposed a Dual Watermarking Method(DWM) for integrity of medical image. The proposed DWM offers robustness with the embedded watermark, it ensures the integrity of the medical image

being transmitted and/or stored. DWM, watermarks are carefully embedded circumventingthe area of ROI (Region of Interest)and the edge of the significant contents to safeguard the integrity of the medical image. And concluded that DWM is capable of detecting the robust watermark preciselyand discoverintentional/unintentional leakage of the stored or transmitted medical image.

Suneet Kaur et al. "Digital watermarking of ECG data for secure wireless communication"[13].Use of wireless technology has made the bio-medical data vulnerable to attacks like tampering, hacking etc. This paper proposes the use of digital watermarking to increase the security of an ECG signal transmitted through a wireless network. A low frequency chirp signal is used to embed watermark which is patient's identification taken as 15 digit code. The characteristic of the proposed watermarking scheme is that the blind recovery of the watermark is possible at the receiver and the embedded watermark can be fully removed. Hence, ECG can be viewed by a clinician with zero distortion which is an essential requirement for bio-medical data. Further, tampering such as noise addition and filtering attack can also be detected at the receiver.

IV. CONCLUSION

The medical data are vulnerable to external attacks like hacking, tampering etc. Data hiding techniques are the solution to this question on the protection and preservation of medical data. Amongst the traditional approaches of data hiding i.e. cryptography, steganography and watermarking, the most apposite approach is watermarking.Blind watermarking adapted in protecting medical images is robust against attacks like contrast modification. It has been observed that use of image moments permitsto obtain suitableresults in the extraction process even after geometrical attacks like translation and scaling. Dual watermarking method is the method for secured medical image transmission. The integrity of the medical images during transmission is assured by embedding fragile watermark after process of embedding robust watermark into the medical image.

V. ACKNOWLEDGEMENTS

The authors are thankful to Hon'able C – VI, Mr. Aseem Chauhan (Additional President, RBEF and Chancellor AUR, Jaipur), Maj. General K. K. Ohri (AVSM, Retd.) Pro-VC Amity University, Uttar Pradesh Lucknow Campus, Wg. Cdr. (Dr.) Anil Kumar, Retd. (Director, ASET), Prof. S. T. H. Abidi (Professor Emeritus), Brig. U. K. Chopra, Retd. (Director AIIT), and Prof O. P. Singh (HOD, Electrical & Electronics Engg.) for their motivation, kind cooperation, and suggestive guidance.

REFERENCE

[1] Vlachos, Michail, Yu, S. Philip, "Systems and Methods for Metadata Embedding in Streaming Medical Data" 9August 2009

[2] N. F. Johnson, S. Jajodia Z. Duric. "Information hiding: Steganography and watermarking attacks and countermeasures", *Kluwer academic Publishers* 2000.

[3] B. S. Ko, R. Nishimura and Y. Suzuki, "Time-spread Echo Method for Digital Audio Watermarking", *IEEE Transactions on Multimedia*, 7(2), 2005,pp. 212-221.

[4] H. O. Oh, J. W. Seok, J. W. Hong and D. H. Youn, "New Echo Embedding Technique for Robust and Imperceptible Audio Watermarking*", Proc. ICASSP* 2001,pp.13411344.

[5] Bao P, Xiaohu M. ''Image adaptive watermarking using wavelet domain singular value decomposition'', *IEEE Trans. Circuits Syst. Video Technol*2005; Vol 15(1), pp. 96-102.

[6] S. Katzenbeisser, F. A. P. Petitcolas. "Information hiding techniques for steganography and digital watermarking", Artech House Publishers, 2000.

[7] W. Puech, J. M. Rodrigues. "A new crypto-watermarking method for medical images safe transfer". *In Proceedings of the 12th European Signal Processing Conference*, Vienna, Austria, 2004, pp. 1481-1484.

[8] D. Anand and U. C. Niranjan. "Watermarking Medical Images with Patient Information". In *Proceedings IEEE/EMBS Conference*, Hong Kong, China, October 1998, pp. 703-706.

[9] S. G. Miaou et al. "A Secure Data Hiding Technique with Heterogeneous Data-Combining Capability for Electronic Patient Record". *In Proceedings of the World Congress on Medical Physics and Biomedical Engineering, Session Electronic Healthcare Records*, USA, July 2000.

[10] Macq B. and Dewey F.: Trusted Headers for Medical Images. *In DFG VIII-DII Watermarking Workshop*, Erlangen, Germany, October (1999).

[11] Rodríguez-ColínRaúl, Feregrino-Uribe Claudia, Trinidad-Blas Gershom de J. ," Data Hiding Scheme for Medical Images ", *17th International Conference on Electronics, Communications and Computers (CONIELECOMP'07),*2007

[12] Sung Jin Lim, Hae Min Moon, Seung-HoonChae, Sung Bum Pan,Yongwha Chung,Min Hyuk Chang,"Dual Watermarking Method for Integrity of Medical Images ", *Second International Conference on Future Generation Communication and Networking,IEEE* 2008

[13] Suneet Kaur ,Riya Singhal ,Dr. Omar Farooq , Bhavneet Singh Ahuja ,"Digital watermarking of ECG data for secure wireless communication ", *International Conference on Recent Trends in Information, Telecommunication and Computing,1EEE* 2010

[14] L. Knudsen et al. "Analysis Methods for (Alleged) RC4". Advances in Cryptology-*ASIACRYPT proceedings, Vol. 1514 of LNCS Springer Verlag*, 1998, pp. 327-341.

[15] D. Osborne, D. Abbott, M. Sorell, and D. Rogers, "Multiple embedding using robust watermarks for wireless medical images," in *MUM '04:Proceedings of the 3rd international conference on Mobile and ubiquitousmultimedia*. New York, NY, USA: ACM, 2004, pp. 245–250.

[16] H. Trichili, M. Bouhlel, and B. Solaiman, "A new image watermarking scheme for medical image archiving," in *Information and CommunicationTechnologies, 2006. ICTTA '06. 2nd*, vol. 1, 0-0 2006, pp. 1498–1503.

[17] Y.-G. Wang and Y.-Q. Lei, "A robust content in dct domain for image authentication," *Intelligent Information Hiding and Multimedia SignalProcessing, International Conference on*, vol. 0, pp. 94–97, 2009.

[18] A. Giakoumaki, K. Perakis, A. Tagaris, and D. Koutsouris, "Digital watermarking in telemedicine applications - towards enhanced data security and accessibility," in *Engineering in Medicine and BiologySociety, 2006. EMBS '06. 28th Annual International Conference of theIEEE*, 30 2006-Sept. 3 2006, pp. 6328–6331.

[19] A. Tagaris, A. Giakoumaki, L. Karle, and D. Koutsouris, "Watermarking sdk implementation to facilitate integration in a secure healthcare environment," in *Engineering in Medicine and Biology Society, 2006.EMBS '06. 28th Annual International Conference of the IEEE*, 30 2006- Sept. 3 2006, pp. 3262–3265.

[20] P. Viswanathan and P. Venkata Krishna, "Text fusion watermarking in medical image with semi-reversible for secure transfer and authentication," in *Advances in Recent Technologies in Communication andComputing, 2009. ARTCom '09. International Conference on*, Oct. 2009, pp. 585–589.

[21] J. M. Zain, A. R. M. Fauzi, and A. A. Aziz, "Clinical evaluation of watermarked medical images," *Proceedings of the 28th IEEE EMBSAnnual International Conference New York City*, vol. 28, pp. 5459–5462,2006.

[22] L. Tung-Lam, N. Thi-Hoang-Lan. "Digital Image Watermarking with Geometric Distortion Corrections Using the Moment Image Theory", *International Conference on Research, Innovation & Vision for the Future (RIVF)*, February 2004.

[23] P. Dong et al. "Digital Watermarking Robust to Geometric Distortions", *in IEEE Transactions on Image Processing*, Vol. 4, No. 12, December 2005.

[24] Y. Wang, A. Pearmain. "Blind image data hiding based on self-reference", *in Pattern Recognition Letters*, Vol. 2 No. 15 November 2004, pp. 1681-1689.

[25] B. Plaintz, A. Maeder. "Medical Image Watermarking: A Study on Image Degradation", *in proceedings of the Australian Pattern Recognition Society (APRS) Workshop on Digital Image Computing (WDIC*), Brisbane Australia, February 2005.

[26] S. Voloshynovskiy, S. Pereira, V. Iquise, and T. Pun. "Attack modelling: Towards a second generation watermarking benchmark". *Signal Processing, Special Issue on Information Theoretic Issues in Digital Watermarking*, 81(6), June 2001.