International Conference on Computational Science and Information Management (ICoCSIM)
Vol. 1 (2012) 267-270

Tamper Localization and Recovery Medical Image Watermarking: A Review

Gran Badshah, Siau-Chuin Liew, Jasni Mohd Zain, Tutut Herawan

Faculty of Computer Systems and Software Engineering, Universiti Malaysia Pahang
Lebuh Raya Tun Razak, 26300 Gambang, Kuantan, Pahang, Malaysia

Abstract

Digital imaging technology development has improved the health care system, particularly improving digital medical imaging system used in the patient diagnoses, treatment and surgery. The remote access of digital medical images is also known as teleradiology, is an important unit of modern electronic health (eHealth) care system. Teleradiology is facing secrecy, fraud, misuses and security problems which encourage unauthorized users for copying, distributing and tampering images. Image tampering is one of the serious issues in hospital information system (HIS) based on online radiology information system (RIS) and picture archive and communication system (PACS). Medical decisions made on the basis of tampered images while diagnosing a patient can cause a non-recoverable loss. Watermarking technique is one of the best solutions to overcome this problem to locate and recover the tempered image in its original version before making any decision. This paper presents a survey of available important literature on digital image watermarking.

Keywords: Watermarking, Digital imaging, eHealth, Teleradiology, Security, RIS, HIS, PACS.

1. Introduction

The advancement of digital imaging technology has brought prominent change in hospital services. For example digital medical imaging has successfully replaced film based medical imaging. These changes have improved services reliability and cost reduction. X-ray, CT scan, Ultrasound (US) and Magnetic Resonance imaging (MRI) are popular imaging modalities. These modalities have proved their best performance in medical imaging. Hospital information system (HIS) has been integrated by DICOM (Digital image communication in medicine) for supporting radiology information system (RIS) and picture archive and communication system (PACS). RIS and PACS insure digital medical images storage and availability in remote accessible electronic patient record (EPR) system. DICOM is the standard set of rules or instructions which make possible the digital image communication among imaging tools, computers and other components which comprise the hospital network [1]. Problems related to copyright protection and authentication are the problems faced by digital images during communication. These problems include images illegal reproduction, tempering and any other type possible alteration. Digital watermarking is a best solution to overcome these problems [2].

2. LiteratureReview

Cryptography is the early version of steganography, which is a Greek word meaning secret writing. Cryptography was being used for secret data communication like medical images and military purposes. Medical images were protected by digital signature and transmitted with the image in a separate file or in an image header which sometimes ascended loosing of signature at the time of changing the file format or during the normal communication. Steganography was being used to resolve this problem. Steganography was an advance version of encryption means covered writing, used to hide communicating information but data communicated via internet had still problems such as communication errors due to noisy channels, different attacks and internet files compression process which ascended an intense need of some better security mechanism for safe communication. To fill up that security gape watermarking technique was proposed and developed. Most of researchers know watermarking a synonym of steganography in literature [3].

2.1 Characteristics and Security of Watermark

Watermark may be a visible symbol such as logo, monogram or an embedded non-visible digital information code in an image. A watermark available on the paper like passport, paper currency and matric card or citizen identity cards are the examples of visible watermark also known as non-digital watermark. Whereas digitally coded watermark added to an audio, video, image or any other digital product is an example of non-visible or digital watermark. Digital watermark is detectable only from the watermarked product and it is impossible or hard to be removed by an unauthorized person [4], [5]. This is the basic

quality of digital watermark that can be detected in original status even the image is tampered. Data hiding, security and authentication are the most important properties of digital watermarking [6]. EPR treatment procedures information, diagnostic results, graphical data at various stages are hidden into the images can validate better security and image tamper detection process [7]. Robustness is that quality of watermark which defends it from attacks. Watermarks are very sensitive to attacks because attacks degrade the quality of watermarked images [8].Kutter M. et al, classify watermark attacks into removal, geometrical, cryptographic and protocol categories whereas Voloshynovskiy S., revises these attacks in more detail [9]. Removal attacks are those which access the watermark data and remove it without disturbing the watermarking key. The geometrical attacks do not remove watermark but disturb the watermark detector. Watermark detector is a tool which tells about the presence of watermark and its decoding [10]. The cryptographic attacks break the watermark security and remove the embedded watermark information ormake some changes to the information to mislead the detection process. The protocol attacks are those which change the ownership of watermarked product by accessing the real watermark and making some desirable changes to claim the ownership. Cayre F. et al, also discuss digital watermark security as part I and part II [11], [12]. Watermark data integrity control, hiding and authentication are three main objectives of the digital watermarking [13]. Digital watermarking has three major steps before and after transmission; embedding, detection and extraction. A certain key is used to encrypt the watermark to be transmitted on digital media and to decode after extraction [14].

2.2 Embedding, detecting and extracting a watermark

Watermarking mean inserting information into multimedia,an original media after watermarking gets some changes. Watermarked product can be communicated through internet, mobile or any other transmission channel. At the receiver side the process in reverse of watermark is detected and extracted. Mathematically these processes can be represented by equation (1) , (2) and (3) respectively.

$$X' = E(X, W, [K]) \quad (1)$$

$$\{\text{yes or no}\} = d(X', [X], W, [K]) \quad (2)$$

$$W' = D(X', [X], [K]) \quad (3)$$

Where E, d and D, are functions used for watermarking, watermark detection and its extraction, while X, X′, W, W′ and K are the original and watermarked media such as a medical image, watermark, extracted watermark and a key respectively. A watermark extraction may be non-oblivious or oblivious. The non-oblivious extraction algorithms require the presence of original image [15] [16] [17] while the oblivious extraction algorithms do not need the presence of original image [18] [19]. The key is a sequence of random numbers may be public or a secret used to produce more secure watermarks to prove the ownership and maintain integrity of an image [20]. Wu and Liu have extended this approach to compressed images [21].

2.3 Digital watermarking schemes

A digital watermark scheme can be exactly one of two available main categories, frequency or spatial domain.

2.3.1 Frequency Domain Watermarking

In frequency domain watermarking a coefficient of transform image is used for embedding watermark in the high level of frequency components [22], [23]. Pixels of the host image are transformed to corresponding frequency domain. This coefficient may be one of discrete Fourier transform (DFT), discrete wavelet transforms (DWT) or discrete cosine transforms (DCT). Robustness of this watermarking scheme can be improved by combining the DFT with the error correction codes [24]. DWT decomposition can be combined with binary image to have protection from unauthorized consumption and duplication of digital communication products [25]. C. Podilchuk et al, and Zhou et al, have focused on the DCT based watermarking maintaining its transparency, capacity, robustness of digital watermarked images and its JPEG compression [26], [27]. Joseph J. K Ruanaidh, and Trierry Pun have introduced a Fourier-Mellin transform-based invariant approach for watermark detection and extraction in which there is no need for the existence of the original image [28].

2.3.2 Spatial Domain Watermarking

In spatial or additive domain watermark is embedded in least significant bits (LSB) by changing the gray level of some pixels in host image. DeepthiAnand and U. C. Niranjan, have discussed the interchange of LSB of image pixels and the encryption of watermark to have its secure communication [29]. A spatial domain watermark can be coded reliably as authentication and

authorization code with copyright protection [30], [31].

2.3.2.1Tamper Localization and Recovery in Medical Images

Tamper localization in ultrasound (US) medical images and its recovery was successfully performed by [32]. However Jasni M. Zain and A. R. M. Fauzi have improved the technique by using watermarking temper detection and recovery (AW-TDR) technique [33]. The main disadvantage of this technique is that it only focuses on ROI while region of non-interest (RONI) which is an outside area of ROI has also some bits to support AW-TDR operations in completing the tamper detection and recovery process.

2.3.2.2Reversible Tamper Localization and Recovery in Medical Images

O. M. Al-Qershi and B. E. Khoo have used reversible ROI-based digital watermarking scheme [34]. Reversible tamper localization and recovery procedure have two main operations, watermark extraction and image restoration to its original status. This technique has the ability to reverse the image to its original version when the watermark is extracted [35]. Liew S. C. and Zain J. M., have also proposed a reversible tamper localization and recovery scheme for medical images [36]. Most of the least Significant Bits (LSB) in RONI pixels of a medical image has zero values so the default values are reversed after tamper detection. This technique divides the tampered image into three major components; ROI, RONI and image dividing blocks. To make more secure and solve the storage problems of watermarks, compression technique is useful. Compression may be lossy or lossless butlossy compression of images can cause loss of important data while lossless compression is better for the reasonit ensures nolossofintegral part of data.

2.3.2.3Lossless Compression Medical Image Watermarking

Lossless compression in digital watermarking is a very good solution to digital medical images efficient storage, communication and avoiding any alteration for correct diagnosis process [37]. The lossless watermarking technique has a good reputation in medical images security, readability with the concept that using this scheme an original image is recoverable from the watermarked one without any loss. The technique uses a high capacity reversible data hiding mechanism. O. M. Al-Qershi and B. E. Koo use lossless reversible watermarking technique for US images security [38]. S. C. Liew et al, have proposed ROI segmentation and multilevel authentication technique in tamper localization and lossless recovery watermarking scheme for time reduction in location and recovery process [39].

3 Conclusions

Digital medical imaging is a very important partof modern health care system for medical diagnosis and surgeries. Security of these images is a main problem while communicating in an e-health network. Watermarking is one of the best solutions of security problems faced in the teleradiology. A number of techniques had been developed and categorized into reversible, irreversible; lossy, lossless; ROI, RONI based; mainly into frequency and spatial domains. Each categorization has its own advantages to meet the target but no one brings the problem completely under control. A Spatial domain based technique, tamper localization and recovery is a technique which can efficiently address the problem by pointing out the tampered portion of the image and its original restoration. Lossless compression in tamper localization and recovery is seemed to be the most researched area in the future because this technique has the ability in solution of storage and communication problems, also reducing the processing time and progressive as well in terms of authentication and patient diagnostic process.

References

1. B. K. Sahu and Raghvendra Verma, “DICOM Search in Medical Image Archive Solution e-Sushrut Chhavi”, 978-1-4244-8679-3/11/$26.00 ©2011 IEEE.
2. Hyung-Kyo L., Hee-Jung K., Ki-Ryong K. and Jong-Keuk L., ”Digital watermarking of medical image using ROI information. In: Enterprise networking and computing in healthcare industry, 2005”. HEALTHCOM 2005, Proceedings of 7th International Workshop on, pp. 404–407, 2005.
3. Jeng S. P., Hsiang C. H. and Lakhmi C. J, a book on, “Intelligent Watermarking Techniques”, Series on Innovative Intelligence, Vol. 7, 2004.
4. Frank Hartung and Martin kutter, “Multimedia Watermarking Techniques”, Proceedings IEEE: Special issue on identification and protection of multimedia information, vol. 87, No. 7, 1079-1107, July 1999.
5. Hussain Nyeem, Wageeh Boles and Colin Boynd, “A Review of Medical Image Watermarking Requirements for Teleradiology”, J Digit Imaging DOI 10.1007/s10278-012-9527-x, Society for Imaging Informatics in Medicine, Sep. 2012.

6. Fallahpour M., Megias D., and Ghanbari M., “High capacity, reversible data hiding in medical images”, 16th IEEE International Conf: on Image Processing (ICIP), pp: 4241-4244, 2009.
7. Ulutas M., Ulutas G., and Nabiyev V. V., “Medical image security and EPR hiding using Shamir’s secret sharing scheme”, Journal of System and Software 84, 314-353, 2011.
8. Kutter M., Voloshynovskiy S. and Herrigel A., “Watermark copy attack”, IS&T/SPIEs 12th Annual Symposium, Electronic Imaging: Security and Watermarking of Multimedia Content II. 3971:23-28, 2000.
9. Voloshynovskiy S., “Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks”, IEEE Communications Magazine. 39(8):118–126, 2001.
10. Tanha, M.; Torshizi, S.D.S.; Abdullah, M.T. and Hashim, F., “An Overview of Attacks against Digital Watermarking and their Respective Countermeasures”, International IEEE Conference on Digital Object Identifier: 10.1109/CyberSec.2012.6246095, pp: 265 – 270, 2012.
11. Cayre F., Fontaine C. and Furon T., “Watermarking security, part I: theory” , In: Security, Steganography and Watermarking of Multimedia Contents VII, Proceedings of SPIE. 5681, 2005.
12. Cayre F., Fontaine C. and Furon T., “Watermarking security, part II: practice” , In: Security, Steganography and Watermarking of Multimedia Contents VII, Proceedings of SPIE. 5681, 2005.
13. Coatrieux G., Maitre H., Sankur B., Rolland Y. and Collorec R., “Relevance of watermarking in medical imaging”, In: Information Technology Applications in Biomedicine, 2000. Proceedings, 2000 IEEE EMBS International Conference on, 2000, pp. 250–255.
14. D. G. Stinson, a book on, “Cryptography theory and practice” , Discrete Mathematics and its applications, third edition, 2006.
15. Cox I. J., kilian J., Leighton T. and Shamoon T., “Secure spread spectrum watermarking for images, audio and video”, IEEE International conference on Image processing, Vol.3, pp: 243-246, 1996.
16. Podilchuk, C.I. and Zeng, W., “Image-adaptive watermarking using visual models” IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 525-539, May 1998.
17. Swanson, M., Zhu, B., and Tewfik, A., “Transparent robust image watermarking,” International Conference on Image Processing, pp. 21 1-214, 1996.
18. Holliman M. and Memon N., “Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes,” IEEE Trans. Image Processing, vol. 9 No. 3, pp. 432-441, March 2000.
19. Zeng, W. and Liu, B., “A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images,” IEEE Trans. Image Processing, vol. 8 No. 11, pp. 1534-1548, November 1999.
20. Ping Wah Wong and Nasir M., “Secret and Public Key Image Watermarking Scheme for Image Authentication and Ownership Verification”, IEEE Transactions on Image Processing Vol. 10 No 10, October 2001.
21. M. Wu and B. Liu, “Watermarking for image authentication”, in Proc, ICIP Chicago, IL, October 1998.
22. M. L. Miller and L. A. Bloom, "Computing the Probability of False Watermark Detection”, Proceeding of the Third International Workshop on Information Hiding. pp: 146-158, 1999.
23. I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, "Secure Spread Spectrum watermarking for Multimedia’’ , IEEE Transactions on Image Processing, vol. 6, no 12, pp. 1673-1687, 1997.
24. Youail, R. S., Khadhim, A-K. A-R. and Samawi, V. W., “Improved stegosystem using DFT with combined error correction and spread spectrum”, Proc. 2nd IEEE Conf. Industrial Electronics and Applications (ICIEA), pp. 1832-1836, 2007.
25. Tao, P. N and Eskicioglu, A. M, “A robust multiple watermarking scheme in the Discrete Wavelet Transform domain”, Proc. Internet Multimedia Management system Conference. 5601, pp: 133-144, 2004.
26. C. Podilchuk and W. Zeng, "Image Adaptive Watermarking Using Visual Models", IEEE Journal on Selected Area in Communication vol. 16, no. 4. pp. 525-539, 1998.
27. Zhou, H.T., Qi, C. and Gao, X. C., “Low luminance smooth blocks based watermarking scheme in DCT domain”, Proc. Int. Conf. Communications, Circuits and Systems, vol. 1, pp. 19-23, 2006.
28. Joseph J. K Ruanaidh, and Trierry Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking", IEEE ICIP pp: 536-539, 1997.
29. Deepthi Anand and U. C., Niranjan, “Watermarking medical images with patient information”, IEEE Proceedings in EMBS Conference, Hong Kong, pp 703-706, Vol. 20, No. 2, Oct 1998.
30. R. Schyndel, A. Z. Tirkel, and C. F. Osborne, “A digital watermark”, in IEEE Proc. Int. Conf. Image Processing, vol. 2, pp. 86–90, 1994.
31. R. B. Wolfgang and E. J. Delp, “A watermark for digital images”, in IEEE Proc. Int. Conf. Image Processing, vol. 3, pp. 219–222, 1996.
32. Jasni M. Zain and Fauzi A. R. M: “Medical image watermarking with tamper detection and recovery”. In: Engineering in Medicine and Biology Society (EMBS), 28th Annual International Conference of the IEEE, 2006, pp. 3270–3273, 2006.
33. Jasni M. Zain and A. R. M. Fauzi, "Evaluation of Medical Image Watermarking with Tamper Detection and Recovery (AWTDR)," in the 29th Annual International Conference of the IEEE EMBS, 2007, pp. 5661-5664.
34. O. M. Al-Qershi and B. E. Khoo, "Authentication and Data Hiding Using a Reversible ROI-based Watermarking Scheme for DICOM Images," in Proceedings of International Conference on Medical Systems Engineering (ICMSE), pp. 829-834, 2009.
35. M. Arsalan, S. A. Malik and A. Khan, “Intelligent reversible watermarking in integer wavelet domain for medical images”, The Journal of Systems and Software 85 (2012) 883– 894, 2011.
36. Liew S. C. and Zain J. M:, “Reversible medical image watermarking for tamper detection and recovery”. In 3rd IEEE International Conference on:

Computer Science and Information Technology (ICCSIT), pp. 417–420, 2010.

37. F. Y. Shih and Y. Wu., "Robust watermarking and compression for medical images based on genetic algorithms" , Information Science in Press, pp: 200-216, 2005.
38. O. M. Al-Qershi and B. E. Koo, “ROI-based Temper Detection and Recovery for Medical images using Reversible watermarking technique”, IEEE International Conference on information theory and information security (ICITIS), pp: 151 – 155, 2010.
39. S. C. Liew, S. W. Liew and J. M. Zain, “Tamper localization and lossless recovery watermarking scheme with ROI segmentation and multilevel authentication”, J Digit Imaging, DOI 10.1007/s10278-012-9484-4, 2012.