International Journal of Multidisciplinary and Current Research

Research Article

ISSN: 2321-3124
Available at: http://ijmcr.com

Authenticating Medical Images with Lossless Digital Watermarking

Arathi Chitla*[1] and Chandra Mohan M[2]

[1*]Associate Professor Department of Computer Science & Engineering, Telangana University, Nizamabad, Andhra Pradesh, India.
[2]Associate Professor, Department of Computer Science and Engineering , JNTUH, Hyderabad, Andhra Pradesh, India.
[*]Corresponding author Fax:08421222212, Mobile:919491533907

Accepted 02 April 2014, Available online 15 April 2014, **Vol.2** (**March/April 2014 issue**)

Abstract

Wide spread of the Internet in the recent past has shown its impact in enhancing the growth in various fields such as in education, banking, commerce, medicine, military applications and many more. In the current e-health applications where images are stored, retrieved and transmitted over the internet, digital watermarking plays a vital role in authenticating the medical images, content verification, preserving the image quality and enhancing the data security. The present paper is a detailed discussion on watermarking techniques that are helpful in authenticating the medical images with a survey of latest research in the area. This paper also studies the simulation results of watermarking and recovery of watermark on several attacks on different medical images.

Keywords: *Authentication, Data security, Image fidelity, loss less watermarking, Medical imaging.*

1. Introduction

Digital Imaging and communication in Medicine (DICOM) is an industry standard image format to store medical images in digital format. Medical or clinical image database management systems helps in sharing patient data among medical practitioners and provide patients with easy access to their own information on health and diagnosis. As a result of the wide availability of both the internet and some powerful image processing software, it is often difficult to determine whether an image is authentic or not. But it is well known that the integrity and confidentiality of medical images is a critical issue for ethical as well as for legal reasons. Well known encryption technologies are good solution to protect data which is transferred over the internet. But sometimes, it may not solve the problem if the decrypted content may be subjected to unauthorized use at the receiver side. Hence digital watermarking techniques are one of the better solutions for both image authentication and copyright protection, where image authentication is achieved by fragile watermarking schemes while Copyright protection is achieved by robust watermarking schemes. Content integrity is guaranteed with fragile watermarking schemes as they sensitively detect any manipulations made in a digital image. Unless the quality of the image is greatly reduced, the watermark will not be affected in robust watermarking schemes.

Watermarking is a process of embedding information into a digital signal in a way that is difficult to remove. Watermark can be plain or in encrypted form of either text, or still image or a logo. Watermarking differs from steganography. In steganography, unlike watermarking, information which is not related to the host can be hidden in the given host. Cryptography enhances the security by embedding the encrypted watermark instead of the original watermark.

Watermarking can be broadly classified as two types depending on the domain of implementation. They are: Spatial domain and transform domain techniques. In spatial domain techniques, the watermark is embedded in the image pixels. They are less robust and simple to implement than the transform domain techniques. These techniques are best useful where there are fewer attacks on the image. LSB, ECC and Spread spectrum are some of the spatial domain techniques. In transform domain techniques, watermarks are added to the coefficients of transforms and there is a definite need to apply inverse transform in order to get the watermarked image. Singular Value Decomposition (SVD), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier transform (DFT) are some of the transform domain techniques. Many techniques based on DCT and DWT are implemented in medical image watermarking [1-33-5].

The rest of this paper is organized as follows: The relevance of watermarking in medical imaging, its objective and limitations in medical imaging is presented in section II. The security characteristics to be maintained and quality measures to assess the watermarked Image are also discussed. Recent advances in medical image watermarking are discussed in Section III. Simulation results are discussed in Section IV. Conclusions and future enhancement discussed in Section V.

2. Digital Watermarking In Medical Imaging

Digital watermarking also has proved to be beneficial in medical imaging. The main role of watermarking in medical imaging is to act as an interface to enhance the protection of its contents, without degrading the quality of data. Its role also extended to the traceability from the origin to the destination. DICOM header can accommodate any metadata but watermark enhances the security of the image, as it is expected to be a part of the image and at the same time is invisible.

Any particulars of the patient like his name, ID, age, address, hospital logo, doctor's remarks for diagnostic image; prescription etc can be used as watermarks in medical imaging. Textual characteristics are more fragile to attacks such as compression than image. So, image as watermark is more robust.

The two main objectives of watermarking in medical imaging are

i. Meta data is embedded as watermark in the images so that the image contains more useful information with a perfect linkage with the patient.

ii. Protection of the image is made possible with integrity control [4,1].

The limitations of watermarking in Medical Imaging are

i. **Payload limitations: -** The payload data such as patient information used as watermark which is embedded in medical image enhances the integrity and assures the correct linkage of information with image. But any alterations in the data due to payload of watermark may lead to distortion in original image.

ii. **Robustness constraints:** - In MI the data quality is most important as the diagnosis and treatment are the primary goals. So the watermark should be more robust against manipulations and malicious attacks. By controlling access rights, intentional modifications will be reduced. With that the robustness should be aimed at attacks such as data format conversion and compressions.

Ethical rules exist for the security and protection of medical information.HPB 517 in Japan, EC 95/46 Directives in Europe, Health Insurance Portability and Accountability Act (HIPAA) in United States etc are best examples of such regulations. Complex data set such as medical annotations, clinical examinations, diagnosis, doctor's findings, opinions and prescriptions with necessary scanned images related to patient's clinical examinations etc are the important information contained with any medical information system. So, in order to protect this data from malicious attacks, the mandatory security characteristics to be maintained are

[1]. **Integrity -** that is the image has not been modified by non authorized people.

Authentication: - that is the image belongs indeed to the correct person and originates from the right source [4,1].

[2]. **Confidentiality -** under normal conditions, only specified users have access to that data. There must be a high degree of confidence that the information is accurate [5, 2].

The quality of watermarked image with reference to the original image can be measured with the following measures.

i. **Mean Square Error (MSE) -** Used to find the degradation levels. Minimum MSE indicates the acceptable degradation.

ii. **Peak Signal to Noise Ratio (PSNR) -** Penalizes the visibility of noise in an image. In Multimedia applications, any image with more than 30db is acceptable. In Medical images, where the quality of the data is paramount, a PSNR around 50db is acceptable limit.

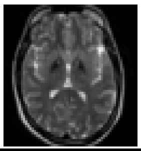
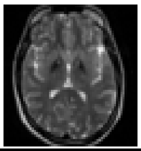
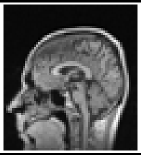
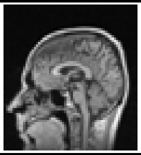
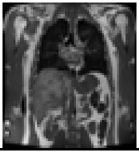
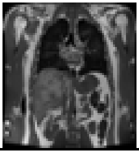
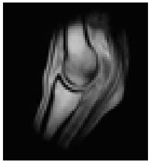
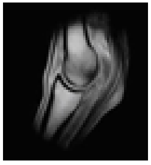
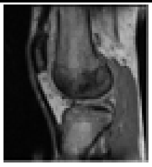
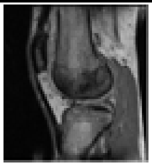
iii. **Normalized Correlation Coefficient (NCC)-** The correlation between original watermark which is embedded with the extracted watermark is computed with NCC. As it reveals the watermark that was embedded, NCC is called as measure of authenticity.

iv. **Structural Similarity Index Measure (SSIM) -** It is a method for measuring the similarity between two images. The SSIM index is a full reference metric. In other words, the measure of image quality is based on an initial distortion-free image as reference. SSIM is designed to improve on traditional methods like PSNR and MSE, which have proved to be inconsistent with human eye perception. The resultant SSIM index is a decimal value between -1 and 1, and where the value 1 is only reachable in the case of two identical sets of data. The SSIM metric is calculated on various windows of an image.

3. Advances In Medical Image Watermarking

With the increased communication of medical images through internet and other networks, and with the maintenance of digital image database management for medical diagnosis, more attention has been paid towards the application of digital watermarking in medical images to scatter the need of authentication and security of medical images. Authenticity and security were implemented by embedding watermark such as patient ID and institution ID in the cover medical images [6]. Block based embedding of watermarking and perceptual quality metrics [7] were used in analyzing suitable watermarking techniques. Comparative study on simultaneous storage of medical images in spatial and frequency domains was

Table1: Watermark embedding and resulting Quality metrics

Cover image (256X256)	Message image (16X16)	Watermarked image	PSNR in dB	SSIM
			42.34	0.988
Brain CT	M Logo	Watermarked Brain CT		
			41.81	0.978
Side Face	R Logo	Watermarked Side Face		
			41.51	0.985
Abdomen MRI	JS Logo	Watermarked Abdomen MRI		
	S		42.16	0.981
Ankle Joint X-Ray		Watermarked Ankle Joint X-Ray		
	K		41.19	0.969
Knee Joint MRI		Watermarked Knee Joint MRI		

also made in exploring suitable methods for medical image watermarking [3]. The objectives of watermarking were further extended through studies on application of watermarks on tamper detection and recovery [8] and enhancement of functionalities of shared medical images [9]. Transformations such as DFT, DCT and DWT were used in the watermarking methods [3]. In this way, the evolution of the digital watermarking in medical image is analyzed which shows its relevance in this study.

4. Simulation Results

The present tables are taken from Discrete Wavelet Transform based watermarking technique and analyzed the simulation results [10]. Five cases in which the logo has been used as watermarks are presented below. Discrete wavelet transform technique was used for watermarking. The simulation result shows the SSIM value, and PSNR value between the original image and the watermarked image.

It was observed that the PSNR value is above 40db in all the examples. SSIM value between the original cover image and the watermarked image is close to 1 which indicates the original and watermarked image are quite similar. SSIM value between original watermark and extracted watermark equal to 1 in case of there is no attacks which indicate that the original watermark and the extracted watermark are one and the same. In case of some attacks, it was also observed that the SSIM value resulted close to 1 which indicates that the quality of the original image is acceptable in medical imaging.

5. Conclusions

This research paper focused on the qualitative improvement in medical imaging with advancement in watermarking. The authors emphasized the significance of watermarking applications in medical imaging to attain privacy and security. It was shown that the watermarking assures the authenticity and integrity of a medical image. Watermarking in Medical imaging can be further enhanced in the direction of localizing the tamper with the malicious attacks.

Table2: Recovery of watermark from watermarked image without attack

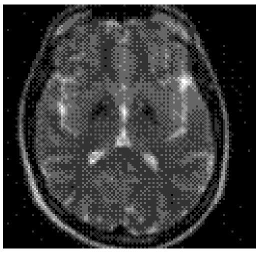
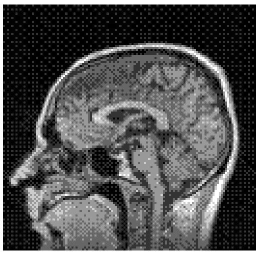
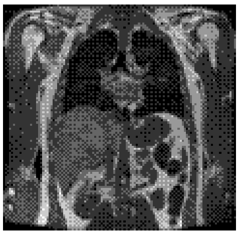
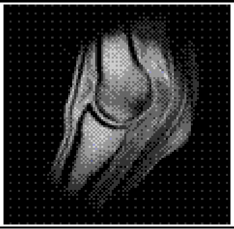
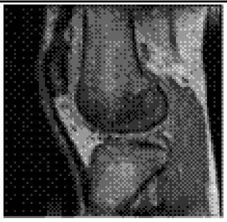
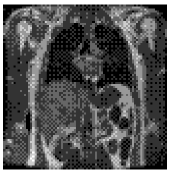
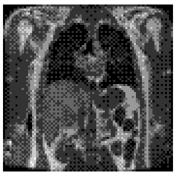
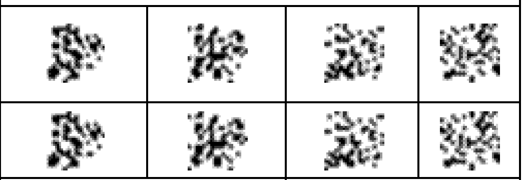
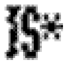
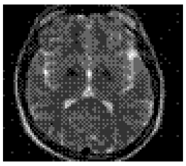
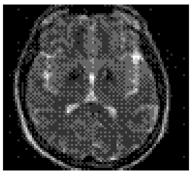
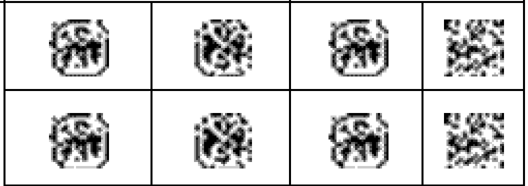
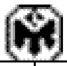
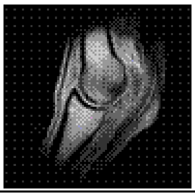
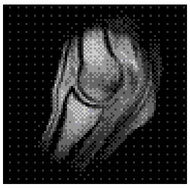
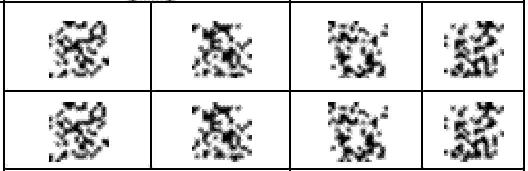
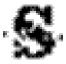
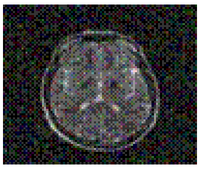
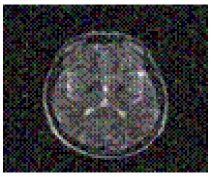
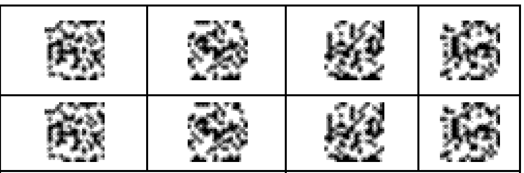
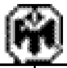
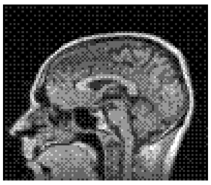
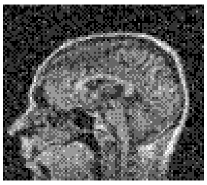
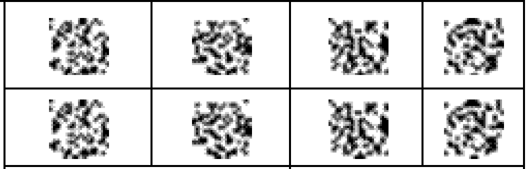
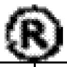
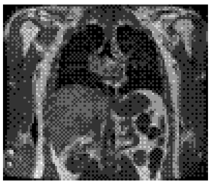
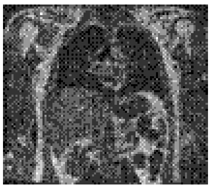
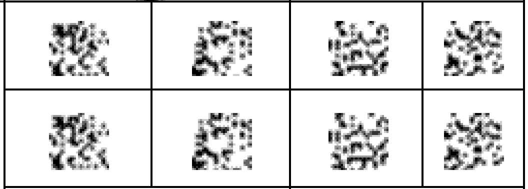
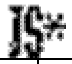
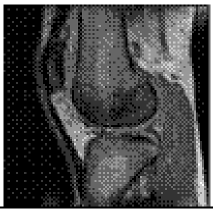
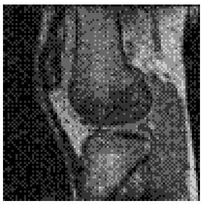
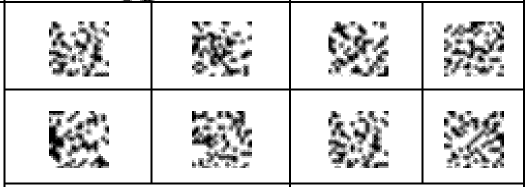
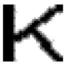
Watermarked Image	8 different recovered sets and derived final logo using bit majority algorithm			
	M	M	M	M
	M	M	M	M
Watermarked Brain CT	M		SSIM	
			1	
	®	®	®	®
	®	®	®	®
Watermarked Side Face	®		SSIM	
			1	
	JS	JS	JS	JS
	JS	JS	JS	JS
Watermarked Abdomen MRI	JS		SSIM	
			1	
	S	S	S	S
	S	S	S	S
Watermarked Ankle Joint X-Ray	S		SSIM	
			1	
	K	K	K	K
	K	K	K	K
Watermarked Knee Joint MRI	K		SSIM	
			1	

Table3: Recovery of watermark from watermarked image under several attacks

Watermarked image (256X256)	Altered or Attacked Watermarked image	8 different recovered sets and derived final logo using bit majority algorithm	
			
Watermarked Abdomen MRI	2% JPEG compression		SSIM 0.8574
			
Watermarked Brain CT	5%JPEG compression		SSIM 0.7842
			
Watermarked Ankle Joint X-Ray	5%JPEG compression		SSIM 0.7689
			
Watermarked Brain CT	20% salt & pepper noise		SSIM 0.9673
			
Watermarked Side Face	30% salt & pepper noise		SSIM 0.9351
			
Watermarked Abdomen MRI	40% Salt & Pepper noise		SSIM 0.79874
			
Watermarked Knee Joint MRI	20% Salt & Pepper noise		SSIM 0.9432

References

[1]. Jagadish, N.P., B. Subbanna, A. U. Rajendra and U. C. Niranjan. 2004. Simultaneous storage of medical images in the spatial and frequency domain: A comparative study. *Bio Medical Engineering*. 3: 17-23.

[2]. Rodrigues, J. M., W. Puech and C. Fiorio. 2004. Lossless Crypto data hiding in medical images without increasing the original image SIZE. 2nd *Medical Imaging and Signal Processing*. 2: 358-365

[3]. Syrine, E.K., E. K. Nabil and F. B. Abdelaziz . 2004. A watermarking method for medical digital images. *CSITEA*. 4: 27-29.

[4]. Coatrieux, G., L. Lecornu and B. Sankur. 2006. A review of image watermarking applications in health care. Proceedings of the 28th IEEE EMBS Annual International Conference.1:4691-4694.

[5]. National Electrical Manufacturers Association (NEMA) (2001). Security and privacy: An introduction to HIPPA. Website: www. Medical.nemd.org/privacy/education.pdf

[6]. Samia, B. and B. Mohamed. 2004. A lossless watermarking based authentication system for medical images. *Transactions on Engineering, Computing and Technology*. 6: 240-243.

[7]. Brigit, M.P. and J. M. Anthony. 2005. A study of block based medical image watermarking using a perceptual similarity metric. *Digital image computing: Techniques and Applications (DICTA')*. 5:70.

[8]. Plaintz, B.P. and A. J. Maeder. 2006. Perceptually limited modality adaptive medical image watermarking. *Medical Imaging*. 6146: 250-259.

[9]. Jansi, M.Z. and R.M.F. Abdul. 2006. Medical image watermarking with tamper detection and recovery. *Proceedings of the 28th IEEE - EMBS Annual International Conference*. pp.3270-3273.\

[10]. Pal, K., G. Ghosh and M. Bhattacharya. 2012. Biomedical Image Watermarking in Wavelet Domain for Data Integrity Using Bit Majority Algorithm and Multiple Copies of Hidden Information. *American Journal of Biomedical Engineering*. 2: 29-37.