Lossless ROI Medical Image Watermarking Technique with Enhanced Security and High Payload Embedding

Malay Kumar Kundu
Indian Statistical Institute
Machine Intelligence Unit
203, B. T. Road, Kolkata 700 108, India
malay@isical.ac.in

Sudeb Das
Indian Statistical Institute
Machine Intelligence Unit
203, B. T. Road, Kolkata 700 108, India
to.sudeb@gmail.com

***Abstract*—In this article, a new fragile, blind, high payload capacity, ROI (Region of Interest) preserving Medical image watermarking (MIW) technique in the spatial domain for gray-scale medical images is proposed. We present a watermarking scheme that combines lossless data compression and encryption technique in application to medical images. The effectiveness of the proposed scheme, proven through experiments on various medical images through various image quality measure matrices such as PSNR, MSE and MSSIM enables us to argue that, the method will help to maintain Electronic Patient Report (EPR)/DICOM data privacy and medical image integrity.**

***Keywords*-Image Watermarking; Electronic Patient Report; Fragile watermarking, Region of Interest.**

I. Introduction

During the last few years as a consequence of the fast and significant advancements in information and communication technologies, medical data management systems have changed immensely. Hospital Information Systems (HIS) and Picture Archiving and Communication Systems (PACS) based on DICOM as advised by NEMA, form the base of the modern integrated health-care delivery systems. These systems provide easier access, manipulation and distribution of medical data. On the other hand, these advances have introduced new risks for inappropriate use of medical information, given the ease with which digital data can be manipulated. It is important to prevent unauthorized accesses and protect medical confidentiality, source authentication should take place, medical data integrity must be safeguarded, as tampering of the medical data might result in misdiagnosis.

MIW is a particular subset of image watermarking, where medical information is embedded in the medical images. The sensitive nature of the medical image data requires that any additional information that is stored within a medical image must not affect the perceptual integrity of the image [2]. MIW is one of the most important fields that need lossless watermarking techniques where distortion may cause misdiagnosis [1].

Many MIW techniques have been proposed by various researches. Zain *et al.* [3] proposed an LSB-based reversible scheme to verify the integrity and authenticity of DICOM ultrasound images. Another spatial domain technique was proposed by Zain *et al.* [4] to improve the security of medical images by involving the ability to detect tamper and subsequently recover the image. Zhou *et al.* [5] presented a watermarking method for verifying the authenticity and integrity of digital mammography images. An LSB technique of embedding EPR data in medical images is suggested by Acharya *et al.* [8]. A frequency domain technique based on discrete wavelet transformation (DWT) combined with a proper quantization method was proposed by Giakoumaki *et al.* [6]. Chao *et al.* [9] proposed a discrete cosine transform (DCT) based data hiding scheme, which is capable of hiding EPR-related data in the quantized DCT coefficients into a marked image. Wu *et al.* [7] proposed two schemes based on Modulo 256 and DCT, for tamper detection and recovery purpose. Woo *et al.* [10] proposed a multiple digital image watermarking method which is suitable for privacy control and tamper detection in medical images.

In all these previous works, either the methods work on a particular modality of medical images, or their imperceptibility decreases very fast with higher payload, or they are less secure. In this article we have proposed a watermarking method that can be used to enhance security, content verification, confidentiality and integrity of medical information. Our method is highly imperceptible, with very high payload capacity. Experimental results show that as much as 10000 characters embedded in the image causes PSNR value to be well over 40 dB. The method works equally well on different modalities of medical images (CT, MRI, angiogram, mammography, barium study, xray etc.) as well as on different image formats (jpg, bmp, gif, tif, DICOM etc). e-health insurance is another field where our method will be helpful in maintaining authenticity and secrecy of medical information.

The rest of the article is organized as follows. Section II. describes the proposed watermarking embedding and extraction algorithms. Experimental results and comparison are presented in Section III. and we draw conclusion in Section IV.

1051-4651/10 $26.00 © 2010 IEEE
DOI 10.1109/ICPR.2010.360

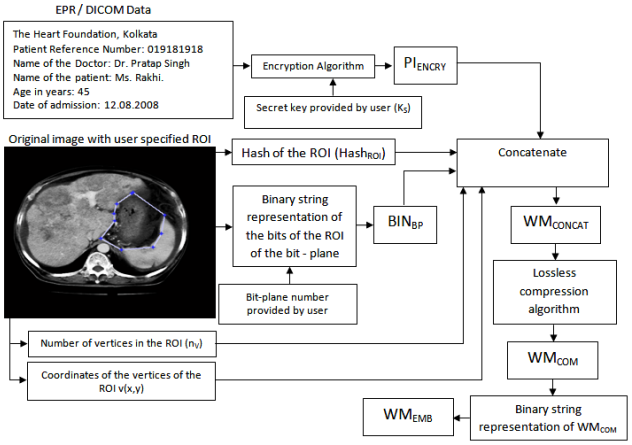


Figure 1. Block diagram of watermark generation process.

II. Proposed Scheme

We have combined spatial domain watermarking technique with lossless data compression and encryption technique in our method. The various steps of the propose scheme is described here:

A. Selection of ROI and finding the hash of the ROI

In our scheme a polygonal ROI can be defined by the Doctor interactively. We chose polygonal ROI because, in most of the cases ROI in a medical image is irregularly shaped. A polygon is completely characterized by the number of vertices n_v, and the vertex coordinates $v(x, y)$. We have used SHA-256 hashing algorithm to calculate an one-way hash value of the ROI (other hashing techniques can also be used) of the original image. This hash value can be used as a Message Authentication Code (MAC). Let the hash value of the ROI be $Hash_{ROI}$.

B. Watermark generation

To generate the watermark, we follow the next procedure:

1) Encrypt the EPR data to enhance the security of the algorithm. If the image format is DICOM, then we first extract the image and the DICOM data from the DICOM file and then encrypt the DICOM data. We have applied Advanced Encryption Standard (AES) method to encrypt the EPR/DICOM data using a secret key K_s. Let the encrypted data be PI_{ENCRY}.
2) Represent the bits of the ROI of the bit-plane specified by the user as a binary string BIN_{BP}.
3) Concatenate n_v, coordinates $v(x, y)$, $Hash_{ROI}$, PI_{ENCRY} and BIN_{BP} to WM_{CONCAT}.
4) Compress WM_{CONCAT} losslessly to WM_{COM}. We have used arithmetic integer compression technique.
5) Represent WM_{COM} as a binary string WM_{EMB}. WM_{EMB} is the watermark to be embedded in the image.

Figure 1. describes the watermark generation process.

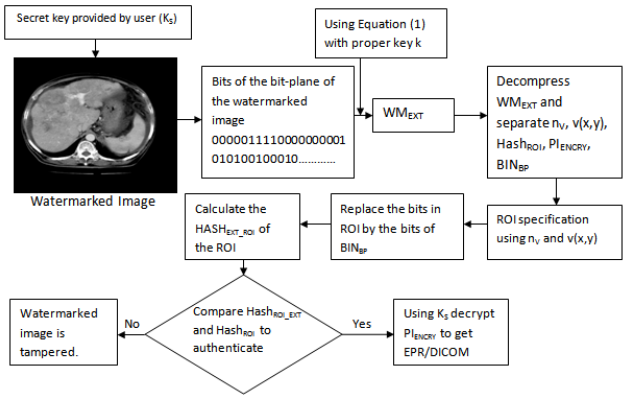


Figure 2. Block diagram of watermark extraction and verification process.

C. Watermark embedding

In our method, the user has the provision to specify the bit-plane number in which he/she wish to embed the watermark. Given a medical image, the algorithm first provides a table which shows the change in visual quality (measured by PSNR) for every bit plane with a predefined payload. Another reason of choosing bit-plane modification technique is the high embedding capacity. The embedding process is described as follows:

1) Separate the original image into ROI and Non Region Of Interest (NROI) by the technique described in section II.A.
2) Generate the watermark WM_{EMB} as described in section II.B.
3) Embed WM_{EMB} in the bit-plane specified by the user. To increase security, we randomize the mapping of WM_{EMB} bit values into the embedding region using the following equation (1).

$$f(x) = kx \ mod \ n + 1 \tag{1}$$

Here, k is a secret prime key (we have taken k as 23) and $k \in [1, n]$; x is the bit position in WM_{EMB} and $x \in [1, length\ of\ watermark]$; n is the total number of pixels available for embedding (in our case this is equal to the total number of pixels in a bit plane). During embedding, first 524 bits of the specified bit plane is used to embed side information which is required during the watermark extraction process.

D. Watermark extraction and verification

The salient steps of the extraction and verification process can be enumerated as follows:

1) All the bits from the bit-plane where the WM_{EMB} is embedded is extracted.
2) From the side information, and using the equation (1). with proper key k, the bit-string representation

Table I
IMPERCEPTIBILITY AND SIMILARITY MEASURE USING MSE, PSNR AND MSSIM

Original Image	Distorted Image	MSE	PSNR	MSSIM
abdomenCT	WMEm	0.16	56.09	0.99
512 × 512	WMEx	0.15	56.38	0.99
brainCTg	WMEm	0.17	55.95	0.99
400 × 400	WMEx	0.15	56.26	0.99
brainMRIg	WMEm	0.21	54.84	0.99
330 × 330	WMEx	0.20	55.08	0.99
usg	WMEm	0.12	57.52	0.99
768 × 562	WMEx	0.11	57.68	0.99
CTMono	WMEm	0.12	57.40	0.99
512 × 512	WMEx	0.11	57.54	0.99

WMEm = Watermark Embedded Image, WMEx = Watermark Extracted Image, Bit plane =2

of WM_{EMB} is constructed. Let it is denoted by WM_{EXT}.

3) Decompress WM_{EXT}.
4) Separate n_v, coordinates $v(x, y)$, $Hash_{ROI}$, PI_{ENCRY} and BIN_{BP}.
5) Using n_v and coordinates $v(x, y)$, the proposed scheme automatically specify the ROI.
6) Replace the bits of the bit-plane in ROI by the bits of BIN_{BP}.
7) Calculate the hash $Hash_{ROI_EXT}$of the ROI using the same hashing algorithm used in embedding process.
8) If $Hash_{ROI}$ and $Hash_{ROI\_EXT}$ is equal, the image is authenticated. Otherwise the the watermarked image is tampered with.
9) If authenticate then using the secret key K_s decrypt the PI_{ENCRY} to get the EPR/DICOM data.

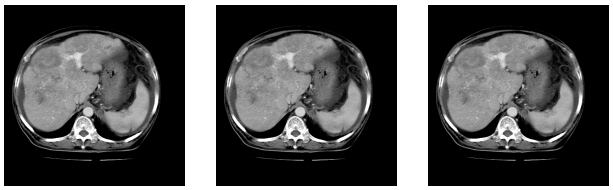
Figure 2. describes the extraction and verification process.

III. EXPERIMENTAL RESULTS AND COMPARISON

5 medical images, of different modalities (CT, MRI, USG) , sizes (smallest 330 × 330 - biggest 768 × 562 etc.), file types (BMP, JPEG, TIF, GIF) and bit depths (8, 12, 16) were used to test our scheme. Table I. and Figure 3. shows the results of embedding and extraction processes.We have used PSNR (Peak Signal-to-Noise Ratio) and MSE (Mean Square Error) metrics to measure the distortion produced after the embedding and extraction processes. We have also used MSSIM (Mean Structural SIMilarity index) to measure the similarity between the original image and watermark embedded image as well as the original image and watermark extracted image.

$$MSE = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (f(x, y) - f'(x, y))^2, \quad (2)$$

where $M \times N$ is the size of the image, $f(x, y)$ is the pixel intensity of original image and $f'(x, y)$ is the pixel intensity



(a) (b) (c)

Figure 3. Results of watermark embedding and extracting. (a) original abdomenCT image, (b) watermarked abdomecCT image, (c) watermark extracted abdomenCT image.

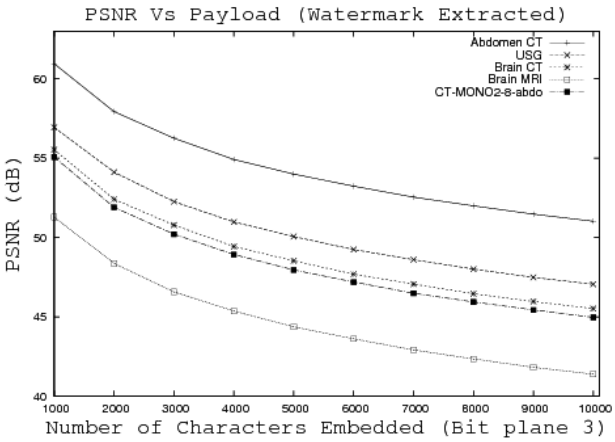


Figure 4. PSNR v/s Payload graph for original v/s watermark extracted images of 5 different modalities (Bit plane = 2).

of watermark embedded or watermark extracted image.

$$PSNR = 10 \times \log_{10} \frac{B^2}{MSE}, \quad (3)$$

where B = Maximum luminance in the image. Values over 36 dB in PSNR are acceptable in terms of degradation [11].

SSIM is ideal for testing for similarities in medical images because it focuses on local rather than global image similarity. SSIM performs a luminance comparison (LC), contrast comparison (CC), and structure comparison (SC) between two image regions. The structural similarity of two images regions R_x and R_y, which are on images x and y respectively, is given by

$$SSIM(R_x, R_y) = LC(R_x, R_y)^{\alpha}.CC(R_x, R_y)^{\beta}.SC(R_x, R_y)^{\gamma}, \quad (4)$$

where α, β, $\gamma \geq 1$ and are used to weight the importance of each of the three components. In the perceptual model used in the experiments presented in this article, each of the three SSIM components was weighted equally i.e., $\alpha = \beta = \gamma = 1$. SSIM values > 0.95 are typically regarded as visually imperceptible for the parameter choices indicated.

Figure 4. shows the degradation (in terms of PSNR) in vi-

Table II
A COMPARISON BETWEEN OUR SCHEME AND OTHER SCHEMES MENTIONED IN SECTION I.

Scheme	Objectives	Hiding Capacity	Security Measures Used	ROI Based	Lossless or Lossy	Non-blind or Blind
Chao[9]	Authentication, integrity and confidentiality of EPR	Low	Using Mark image as a key	No	Lossy	Non-Blind
Zain[3]	Authentication	Low, only authentication data are embedded, no patient's data are embedded	Using hash value of the whole image	Yes	Lossless	Blind
Wu (1,2)[7]	Authentication	Low, no patient's data can be embedded	No	No/Yes	Near Lossless	Blind
Our scheme	Authentication, integrity content verification, security and confidentiality of medical information	High, 10000 characters inserted with PSNR value $>$ 40 dB	Hashing, Secret key for encryption, bit-plane number and prime key to randomized the embedding locations	Yes	ROI Lossless	Blind

sual quality of the watermark extracted images with respect to the original images by embedding watermarks of varying strengths in 5 different modalities of medical images. It is clear from Figure 4. that our scheme is capable of very high payload, with good imperceptibility. The security of the proposed scheme is also enhanced because one have to know the value of k and K_s both to get the correct EPR/DICOM data. The MSSIM value (0.99), observed from Table I. shows that our method is a good candidate for MIW.

Table II. shows the comparison between our scheme and some of the schemes mentioned in section 1. which clarifies the advantages of our scheme over those schemes.

IV. CONCLUSIONS

We have presented a blind, fragile watermarking scheme applied to medical images with good imperceptibility, high payload and enhanced security. Our scheme can be used for different medical image modalities. The experimental results indicate that the proposed scheme is feasible and given its relative simplicity, it can be applied to the medical images at the time of acquisition to serve in many medical applications concerned with privacy protection, safety, and management.

REFERENCES

[1] M. Awrangjeb, *An Overview of Reversible Data Hiding*, 6th International Conference on Computer and Information Technology, pp. 75-79, December 2003.

[2] G. Coatrieux and H. Maitre and B. Sankur and Y. Rolland and R. Collorec, *Relevance of watermarking in medical imaging*, IEEE EMBS International Conf. On Information Technology Applications in Biomedicine, pp. 250-255, Arlington, VA, USA, 2000.

[3] J. M. Zain and L. P. Baldwin and M. Clarke, *Reversible watermarking for authentication of* DICOM *images*, in Proc. 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 3237-3240, 2004.

[4] J. M. Zain and A. R. M. Fauzi, *Medical Image Watermarking with Tamper Detection and Recovery*, Proc. 28th IEEE EMBS Annual International Conference, pp. 3270-3273, 2006.

[5] Xiaoqiang Zhou and H. K. Huang and Shieh Liang Lou, *Authenticity and integrity of digital mammography images*, IEEE Trans. Med. Imaging, Vol.20, No.8, pp. 784-791, 2001.

[6] A. Giakoumaki and S. Pavlopoulos and D. Koutsouris, *A medical image watermarking scheme based on wavelet transform*, in Proc. 25" Annual Intemational Conference of the IEEE Engineering in Medicine and Biology Society, pp. 856-859, 2003.

[7] J. H. K. Wu and R.-F. Chang and C.-J. Chen and C.-L. Wang and T.-H. Kuo and W. K. Moon and D.-R. Chen, *Tamper Detection and Recovery for Medical Images Using Near-lossless Information Hiding Technique*, Journal of Digital Imaging, Vol. 21, pp. 59-76, 2008.

[8] R. Acharya and P. Subhanna Bhat and S. Kumar and C. Min, *Transmission and storage of medical images with patient information*, Journal of Computers in Biology and Medicine, Vol. 33, pp. 303-310, 2003.

[9] H.M. Chao and C.M. Hsu and S.G. Miaou, *A data-hiding technique with authentication, integration, and confidentiality for electronic patient records*, IEEE Trans Inf Technol Biomed, Vol. 1, pp. 46-53, March 2002.

[10] C.-S. Woo and J. Du and B. Pham, *Multiple Watermark Method for Privacy Control and Tamper Detection in Medical Images*, in Proc. APRS Workshop on Digital Image Computing Pattern Recognition and Imaging for Medical Applications, pp. 43-48, 2005.

[11] Xuanwen Luo, Qiang Cheng, Joseph Tan, *A Lossless Data Embedding Scheme For Medical in Application of e- Diagnosis*, Proceedings of the 25th Annual International Conference of the IEEE EMBS Cancun, Mexico. September 17-21, 2003.