ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Medical Image Authentication Through Watermarking

[I]Abhinav Shukla, [II]Chandan Singh
[I]M.Tech, Dept. of Computer Science, Mangalaytan University
[II]Asst. Professor, Dept. of Computer Science, Mangalaytan University
E-mail : [I]abhinavshukla007@gmail.com, [II]Chandan.singh@mangalayatan.edu.in

Abstract
Medical image is usually comprised of region of interest (ROI) and region of non interest (RONI). ROI is the region that contains the important information from diagnosis point of view so it must be stored without any distortion. We have proposed a digital watermarking technique which avoids the distortion of image in ROI by embedding the watermark information in RONI. The watermark is comprised of patient information.

Keywords
BCH Encryption, Data authentication, Electronic Patient Record, Medical Images, Spatial domain watermarking data to the adversaries.

I. Introduction

Due to the development of latest technology in communications and computer networks, exchange of medical images between hospitals has become a usual practice now days [1]. These medical images are exchanged for number of reasons. For example teleconference among clinicians, interdisciplinary exchange between clinicians and radiologists for consultative purposes or to discuss diagnostic and therapeutic measures and for distant learning of medical personnel [2]. However these applications require more attention towards image protection (availability, confidentiality and reliability) [3]. To facilitate sharing and remote handling of medical images in a secure manner watermarking guarantee attractive properties [4, 5]. It allows permanent association of image content with proofs of its reliability by modifying the image pixel values, independently of the image file format. For protecting the digital images two categories of watermarking have been developed: Robust Watermarking [6] and Fragile Watermarking [7, 8]. Robust watermarks are those which are difficult to remove from the digital content. Withstand intentional or incidental distortions like compression, scaling, cropping, filtering, A/D or D/A conversion, etc. and therefore are used for copyright applications. Fragile watermarks are those that are easily destroyed by tampering or modifying the watermarked content hence the absence of watermark to the previously watermarked content points to the conclusion that data has been tampered with, and thus are used for data authentication applications.

One can use the fragile watermarking for authentication of medical images. In this case, the robustness of watermark in the image is less concerned, while detection and localization of the slight changes of the images are more important [1].

In this paper we have extended our work [19] and have proposed a blind fragile watermarking scheme that does not require the original host image during the extraction of watermark. First the image has been segmented which separates the region of interest (ROI) from original image then three different types of watermarks are embedded in the host image by reading the information from the patient file and converting the text in to binary. After that apply the 4 level haar lifting wavelet transform to decompose the image. On each decomposition watermark bit is embedded according to some specific conditions The Scheme serves for both the purposes of medical image Authentication and hiding electronic patient record. The portions of formation image that contains significant information for diagnosis are called region of interest (ROI) and must be stored without distortion. Usually it is desirable to embed data outside of ROI to give better protection [10] without compromising with the diagnosis information.

II. Literature Review

Different groups of authors have contributed number of medical image watermarking techniques. A technique of embedding electronic patient record (EPR) data in medical images is suggested by Acharya et al. [11]. 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. In another technique proposed by Nayak et al. [12], the ASCII characters in EPR text are encrypted using Rijndael algorithm before hiding it in image. Signal graphs (ECG, EEG, EMG etc.) are compressed using differential pulse code modulation (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) code. 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 Characters Altered (NOCA) for text data and percentage distortion (PDST) for the signal graph are evaluated. Xuanwen et al. [13] utilizes compressed binary bit-plane to embed EPR data.

Since there are 8 bit planes for gray scale images with pixel values ranging from 0 to 255. So in order to obtain the sufficient embedding capacity, each binary bit plane is compressed losslessly and data is embedded into saved space. In reverse direction, the embedded data is extracted and the compressed image is decompressed. The original image is recovered because the compression was lossless. Odriquez et al. [14] searches for the suitable pixels to embed information using the spiral scan starting from the centroid of the image. Then obtain a block with its center at the position of the selected pixel. If the bit to be embedded is 1, change the luminance value of the central pixel by adding the gray-scale level mean of the block with luminance of the block. If the bit to be embedded is 0, change the luminance value of the central pixel by subtracting the luminance of the block from the grayscale level mean of the block. In the extraction procedure, marked pixels are located using the spiral scan starting in the centroid of the image. If the luminance value of the central pixel is greater than the gray

scale level mean of the block, then the embedded bit is identified as 1, otherwise as 0.
This algorithm has the limitations that the region of interest (ROI) which is diagnostically important area in medical images has not been implemented in data embedding methods. Some of the important requirements in medical field are to recover the EPR with zero BER, to have the cover image without any distortion. Another requirement is that the ROI should be protected [15].

III. Proposed Scheme

Our approach focuses on embedding watermark in RONI region of medical image by preserving ROI. This approach helps in isolating ROI region i.e. not to distort the critical area of medical image, which will be referred by physician for the diagnosis. The system diagram for this approach is shown in Figure 1. The system process carried away in three stages:

1. Watermark embedding process
2. Watermark extraction process
3. Watermark authentication process

In first phase of system separating the ROI from the original medical image provides RONI region for embedding watermark. This step isolates ROI from embedding process. In this phase multiple watermarks are embedded into the RONI area of medical image. Embedding multiple watermarks ensure high security of Medical image as it carries high payload and it will be more complex to break the system. Here fragile watermarking system is used to get the benefit of identifying whether a medical image is tampered or not? After the completion of embedding process the separated ROI is combined with the produced watermarked medical image. The resultant watermarked medical image is then sent to the receiver.
In watermark extraction phase, first step is separating the ROI from the watermarked medical image. The remaining watermark extraction process is exact reverse of embedding process, where the embedded watermark will be extracted from the watermarked medical image. The watermark authentication is achieved by comparing the extracted watermark with the original watermark. This process helps in identifying if any tampering or manipulation to the watermarked medical image over the public network.

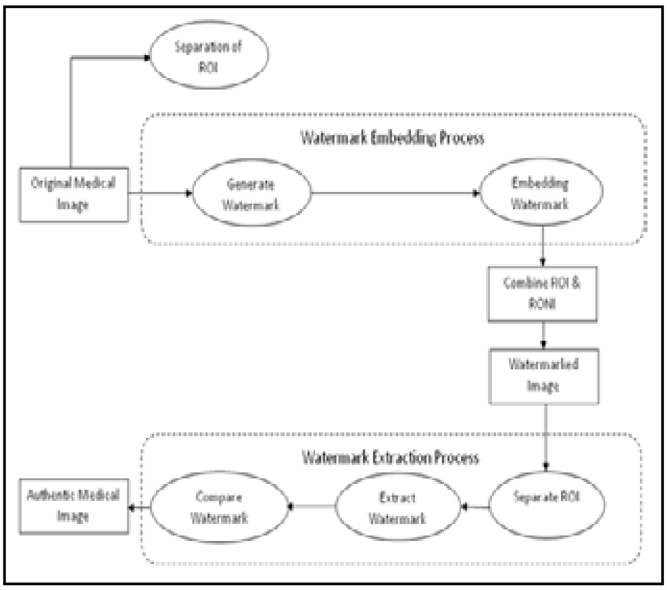


Fig.1: Medical Image Watermarking Approach Preserving ROI

IV. Algorithm

In this algorithm the multiple watermarks embedding technique is used. Where, depending on the quantization of selected coefficients the multiple watermarks embedding procedure is used. This prevents any modification to the watermark bits by granting integer changes in spatial domain of medical image. This can be achieved by applying 4-level haar wavelet transform to decompose the host medical image. Moreover it gives the output as coefficients, which are in the form of dyadic rational numbers. These coefficients denominators are in powers of 2. The multiple of 2l (l is decomposition level) number adding or subtracting to the produced coefficient value, assures that the inverse DWT provide integer pixel values. Wavelet transform generally provides the coefficients which are real numbers. By applying the quantization function it assigns the binary number to every coefficient. This quantization function is defined as

$Q(f) = 0$; if $[f-s]/\Delta$ is even …………….. (1).

$Q(f) = 1$; if $[f-s]/\Delta$ is odd……………… (2).

Where s is a user-defined offset for increased security, f is frequency coefficient produced by haar wavelet transform and, the quantization parameter, is a positive real number. Moreover is defined as $\Delta = 2^l$.
As explain earlier, addition or subtraction of a multiple of 2l value to the haar wavelet coefficient results in integer pixel values, after applying inverse DWT. During the embedding process the algorithm add or subtract an appropriate constant to the haar coefficient chosen for watermark casting.

The algorithm for embedding multiple watermarks is explained below:
Step 1: Separate the ROI region from the host medical data using GUI based mouse clicking approach. Which results in image of RONI region, name it as original medical image.
Step 2: Save the removed ROI from medical image.
Step 3: The multiple watermarks to be embed into an original image is generated by reading the patient's information file from text document, and converting it into binary.
Step 4: Apply the 4-level Haar-lifting wavelet transform to original medical image, to obtained a gross image approximation n at the lowest resolution level and a sequence of detail images corresponding to the horizontal, vertical, and diagonal details at each of the four decomposition levels.
Step 5: On each decomposition level the watermark bit wi is embedded into the key determined coefficient f, which is obtained by applying wavelet transform according to the following condition:
1. If Q (f) = wi, the coefficient is not modified
2. Otherwise, the coefficient is modified so that Q (f) = wi, using the following equation:

$f = f + \Delta \quad \text{if } f \leq 0$ (4.6)

$f = f - \Delta \quad \text{if } f > 0$ (4.7)

Step 6: The pre watermarked image is produced by performing the corresponding four level inverse wavelet transform.
Step 7: The resultant watermarked image is obtained by combining the saved ROI with the pre watermarked image.
The watermark extraction process is similar to that of embedding one except that at the receiving end extractor should have the knowledge of location of the embedded watermark. This can achieve by the key-based embedding and detection. With this type of method access to the watermark by unauthorized users

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

is prevented. The algorithm for extraction process to recover the host medical image is explained below.

Step 1: Remove the ROI region from the received watermarked image with the help of Xmax, Xmin, Ymin and Ymax parameter provided with watermarked image.

Step 2: Apply the 4-level lifting-haar wavelet transform to the image which is created from step 1, which results in a image approximation at level four and sequence of images corresponding to the horizontal, vertical, and diagonal details at each of the four decomposition levels.

Step 3: Identify the location of watermark by key-based detection.

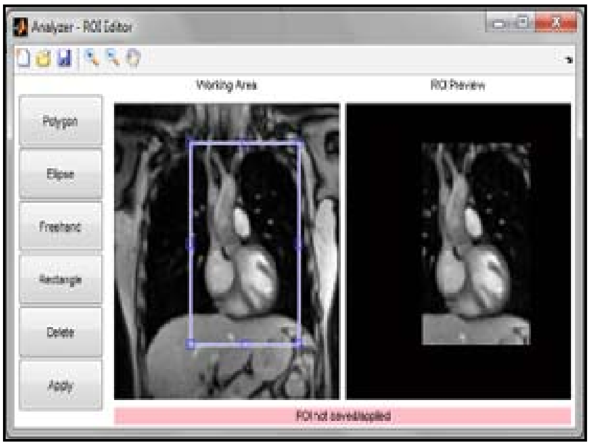
Step 4: Extract the watermarks by applying quantization function defined in equation 1 and 2 which recovers the original coefficient. Convert the extracted binary watermark to text watermark.

Step 5: The pre output image is obtained by applying inverse 4-level haar wavelet transform.

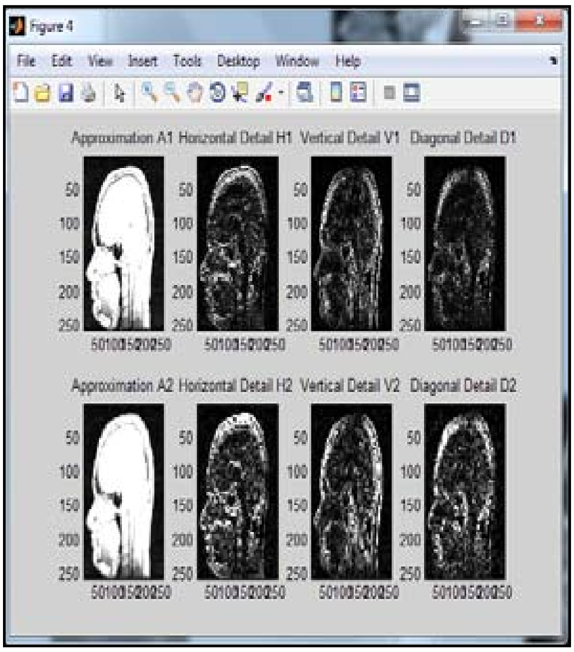
Step 6: combine the separated ROI region to the pre output image to get the original host medical image

V . Experiments and Results

1. Select the Region of Interest



2. Apply the 4-level Haar-lifting wavelet transform to original medical image.



The number of rows in input image is: 256
The number of coloums in input image is: 256
Enter the decomposition level 4 :n = 4
Decomposition vector of size 1*524288 is stored in c.
Corresponding book keeping matrix

16	16	3
16	16	3
32	32	3
64	64	3
128	128	3
256	256	3

Level-dependent thresholds: 6.3500
The entropy used is: threshold
The type of thersholding is: Hard Thresholding

Approximation coefficients are: 1

Wavelet packet best tree decomposition of XD

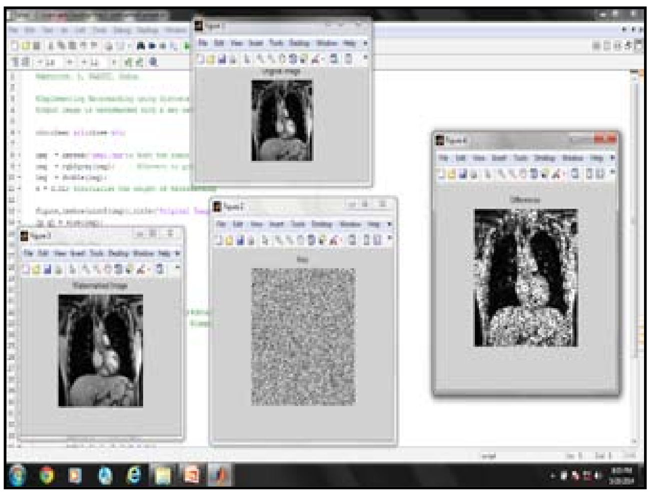
Wavelet Packet Object Structure
=================================
Size of initial data : [256 256]
Order : 4
Depth : 2
Terminal nodes : [5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20]

Wavelet Name : haar
Low Decomposition filter : [0.7071, 0.7071]
High Decomposition filter: [-0.7071, 0.7071]
Low Reconstruction filter: [0.7071, 0.7071]
High Reconstruction filter: [0.7071, -0.7071]

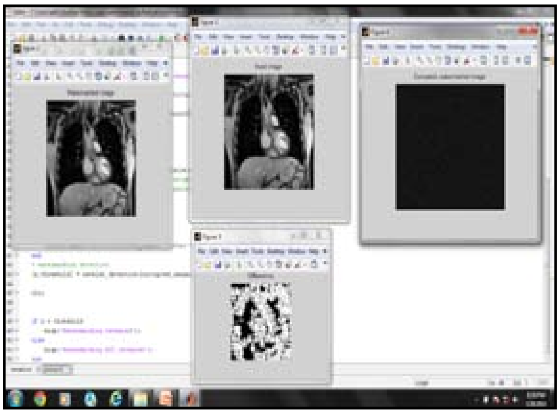
Entropy Name : threshold
Entropy Parameter : 6.35

The L^2 recovery: 99.9539
The compression scores in percentages: 64.6088
The numbers of rows in compressed image are: 256
The numbers of coloums in image are: 768

3. Watermarking Medical image



4. Medical Image Authentication



Watermarking NOT revealed

IV. Conclusion

There exist various medical image watermarking algorithms which provide the confidentiality of medical data, recovering original image without any distortion, data integrity, authentication and efficient data management. Also the different segmentation algorithms are in place, which vary for the types of medical images such as MRI, CT scan, X-ray and Ultrasounds etc. Here the proposed system used an algorithm to separate ROI from the host medical image that will be applicable for all types of medical images. Separated ROI can be stored with Xmin, Xmax, Ymin, and ymax value so that at the end of embedding process before transmitting watermarked image, the segmented ROI can be attached with watermarked image. And the ROI region which is considered as a critical data and used as a reference by the physician for the treatment will be safe.

References

[1] *Na Li; Xiaoshi Zheng; Yanling Zhao; Huimin Wu; Shifeng Li Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform", Electronic Commerce and Security, International Symposium ,Volume, Issue , 3-5 Aug. 2008 , Page(s):942.*

[2] *D. Osborne, D. Rogers, J. Mazumdar, R. Coutts, D. Abbott, "An Overview of Wavelets for Image Processing for Wireless Applications", Proceedings of SPIE: Smart Structures, Devices and Systems, University of Melbourne, Australia, Vol. 4935, pp.427.*

[3] *Nisar Ahmed Memon,"Watermarking of Medical Images for Content Authentication and Copyright protection",PhD Thesis, GIK Institute of Engineering Sciences and Technology Topi, Swabi, Khyber Pakhtunkhwa, Pakistan, May 2010.*

[4] *D. Osborne," Embedded Watermarking for Telemedicine", PhD Thesis, University of Adelaide, 2005*

[5] *Malay Kumar Kundu, Sudeb Das,"Lossless ROI Medical Image Watermarking Technique with Enhanced Security and High Payload Embedding", International conference on Pattern Recognition pages: 1457-1460.*

[6] *Ahmad Nilchi1, Ayoub Taher," A New Robust Digital Image Watermarking Technique based on the Discrete Cosine Transform and Neural Network", pp:1 – 7, April 2008.*

[7] *M.S. Hsieh, and D.C. Tseng, "Hiding digital watermarks using multiresolution Wavelet transform", IEEE Transactions on industrial electronics, vol:48, No:5, pp:875-882, Oct, 2001. May, 2002.*

[9] *Wang, S. and Y. Lin, "Wavelet Tree Quantization for Copyright Protection Watermarking," IEEE Trans. Image Processing, vol. 1 no. 2, pp: 154-164, 2004.*

[10] *Ramani K.; Prasad E.V, Varadarajan S.; Subramanyam A,"A Watermarking Scheme for information Hiding and Communications, 16th International Conference, 14 pp:58 – 64.*

[11] *V.R. Ratnaparkhe, R.R.Manthalkar and Y.V.Joshi, " Characterization of CT images Based on Ridgelet Transform" International Journal on Graphics, Vision and Image Processing, GVIP, Volume 8, 2008, pages:43-50. [12] M.S. Joshi, R.R. Manthalkar, Y.V.Joshi,' Image Comp Curvelet, Wavelet and Ridgelet Transform: A Comparative study' ,ICGST GVIP, ISSN 1687-398X, Volume 8, Issue III, October 2008, Pages: 25-34.*

[13] *Na Li; Xiaoshi Zheng; Yanling Zhao; Huimin Wu; Shifeng Li ," Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform", Electronic Commerce and Security, International Symposium ,Volume, Issue , 3-5 Aug. 2008 , Page(s):942*

[14] *Wang Hongjun, Li Na," An algorithm of digital image watermark based on multiresolution wavelet analysis", International Workshop on VLSI Design and Video Technology, Proceedings, 28 275*

[15] *Krishnan, N. Selvakumar, R.K. Rajapandian, S. Arul Mozhi, K. Nelson Kennedy Babu, "A Wavelet Transform Based Digital Image Watermarking and Authentication", Annual IEEE Conference, in India, 15-17 Sept. 2006, pp: 1-6*

[16] *Abu-Errub, A., Al-Haj, A.,"Optimized DWT watermarking", First International Conference on Applications of Digital Information and Web Technologies, IEEE,2008,*

[17] *Ramani, E Prasad, S Varadarajan, "integer wavelet transform", IJCSNS international journal of Computer science and network security, vol No: 7 July 2007*

[18] *Saied Amirgholipour Kasmani, Ahmadreza Naghsh Robust Digital Image Watermarking Technique Based on Joint DWT DCT Transformation", Convergence and Hybrid Information Technology, 2008. ICCIT '08. Third International Conference, 11 Nov. 2008, Volume: 2, pp: 539*