Strict Attestation Of Medical Image Watermarking

Manish Madhava Tripathi
(TeerthankerMahaveer University, Moradabad)

Dr S P Tripathi
(I E T , Lucknow)

Image processing techniques have played an important role in the past decades in thefield of medical sciences for diagnosis and treatment of patients. During diagnosis important information is embedded into RONI part of the image to itsassure integrity of the image. We propose a fragile watermarking technique to ensure the integrity of medicalimage which avoids the distortion of image in ROI by embedding the watermark informationin RONI. The watermark is comprised of patient information, hospital logo and messageattestation code computed using hash function. Earlier encryption of watermark isperformed to ensure inaccessibility of embedded data to the adversaries.

1 Introduction

Recently, due to the development of latest technologies in the areas of communications andcomputer networks, exchange of medical images between hospitals has become a commonpractice. These medical images are exchanged for number of reasons among which are :

• Teleconferences among clinicians;

• Interdisciplinary exchange between clinicians and radiologists for consultative purposes

or to discuss diagnostic and therapeutic measures;

• For distant learning of medical personnel.

However, these applications require more attention towards image protection (availability, confidentiality and reliability). To facilitate sharing and remote handling of medicalimages in a secure manner watermarking guarantee attractive properties. It allows permanent association of image content with proofs of its reliability by modifying the image pixelvalues, independently of the image file format .

3 Proposed Scheme

In the proposed scheme, during the embedding phase the watermark is constructed fromthree different entities. Later on the watermark is embedded in the LSBs of RONI oforiginal image using proposed scheme. In the detection stage the embedded watermark isextracted. The process is the reverse of embedding process. The extracted logo is comparedwith the logo already known to the detector for subjective attestation. For objectiveattestation, the message attestation code (MAC) is calculated as was done at

thetime of embedding and is compared with the extracted attestation code for verifyingimage integrity.

3.1 Watermark generation

In order to generate the watermarks, following steps are implemented:

1. Read the hospital logo as shown in Fig. 1. Convert this gray intensity image into abinary image. We have used the following procedure to perform the above task:

(a) First resize the image to 32 × 32 pixels.

(b) Find mean value of gray scale image and call it threshold T.

(c) Based on this threshold value T, convert the grayscale image into binary by usingthe following formula:

1. if logo(x,y) > T, make the pixel white

else make the pixel black

where x and y are the row and column indices of logo image, such that $1 \le x \le 32$and $1 \le y \le 32$. Now convert this binary image into vector and call it W1 such that$W_1 = \{w_1(i) | w_1(i) \in [0,1], 1 \le i \le 1024\}$.

2. Read the text file containing the patient information, convert each character of textfile into its corresponding ASCII code [107];

3. Convert each ASCII code into its corresponding binary code and form the vector W2which may have length of M bits such that $W_2 = \{w_2(i) | w_2(i) \in [0,1], 1 \le i \le 1024\}$.

4. Set LSBs of all the pixels in the input image to zero and compute the hash functionof this image using MD5 algorithm. This gives 32 characters string comprised ofhexadecimal numbers;

5. Convert hexadecimal string obtained from step 4 into binary vector W3 in the sameway as described for patient information in step 3, such that $W_3 = \{w_3(i) | w_3(i) \in [0,1], 1 \le i \le 256\}$.;

6. Now concatenate all the watermarks W1, W2 and W3 and call it W having length sayN, such that $W = \{w(i) | w(i) \in [0,1], 1 \le i \le N\}$.

Fig 1 : Hospital logo used as watermark

3.2 Watermark pre-processing

A pseudo random binary vector P of the size same as W is generated by a secret keyk. The binary pseudo random vector P is represented as P={p(i)|p(i) ∈ [0,1],1 ≤ i ≤ N}. The following formula is used to get the ultimate watermark W∗

$W^* = W \oplus P$ (1)

where⊕ denotes the exclusive-OR operation. The W^* is the resultant watermark whichis to be embedded in the host image.

3.3 Selection of RONI for embedding the watermark

The proposed method selects the RONI for embedding the watermark in order to assurethe integrity of ROI and not to compromise with the diagnosis value of medical image. Toachieve this, it is necessary first to separate the original image into ROI and RONI areas.

Usually in radiological images the ROI is taken as a square. For example for theimages of size 512 × 512 pixels, square of size 256 × 256 is taken which almost cover theentire ROI. But in some cases especially for radiological MRI images of chest area,taking logical square for isolating the ROI eradicates some part of ROI as shown in Fig. 2.

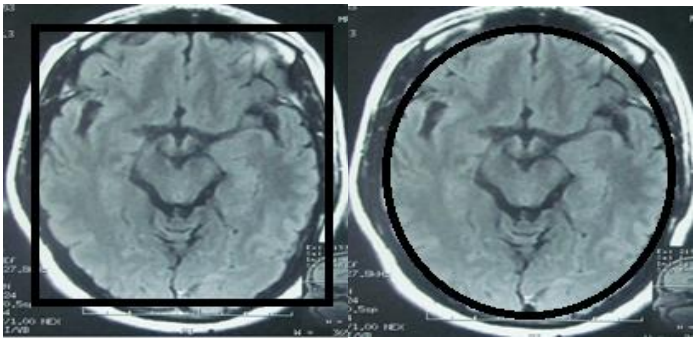

Fig 2: Isolating ROI using square Fig 3 using ellipse

This is because of the brain parenchyma on brain CT, which is elliptical in shape bynature and taking the square as logical boundary for isolating ROI eradicates some partof ROI. This technique though covers the entire brain parenchyma but it also takesthe area (like some part of thorax area and some other part lying between the two brainparts) as shown in Fig 3. Thus this technique of isolating ROI includes the image partswhich are not of the interest

for the physician for diagnosis point of view, thus can be usedfor embedding watermark information.

3.4 Separation of Brain Parenchyma

For isolating the brain parenchyma an optimal thresholding scheme is used which selects thethreshold based on the object and background pixel means. Once the threshold is selectedand applied, region growing and connectivity analysis are used to extract the exact cavityregion with accuracy The segmentation algorithm for segmenting the brain parenchyma fromthe input MRI image is described in more detail.

1. Read the input image;

2. Draw the black boundary on the input image;

3. Find the gray threshold of input image using the Otsu method and call it T_{final};

4. Based on threshold T_{final} found from step 3, turn all pixels white which have the grayvalues greater than the threshold;

5. Find the location of seed pixel and its value for starting the region growing process bysearching through all the boundaries leaving black boundary already drawn in step 2;

6. Find the tagged image by assigning 1 and 0 to the pixels as follows:

Itag(x,y) = 1 if f(x,y) = 255

0 if otherwise(2)

7. Turn those pixels and neighbours white which are not tagged. The resultant imagewill now contain the isolated brain parenchyma.

3.5 Increasing the embedding capacity

By isolating the brain parenchyma with the technique described in Section 3.6 above, onemay increase embedding capacity for the watermark insertion. By taking the square forisolating the brain parenchyma from the input MRI image with size 256 × 256 pixels, itwas necessary to take at least square of size 192 × 192 pixels in order to cover the wholebrain parenchyma as shown in Fig. 4(a). This gives [(256 × 256) − (192 × 192)] = 28672pixels for embedding the watermark information. Similarly drawing the ellipse as shownin Fig. 4(b) gives [(256 × 256) − 33749] = 31787 pixels as embedding capacity. With theproposed scheme shown in Fig. 4(c), [(256×256)−17114] = 48422 pixels are obtained forembedding watermark information.

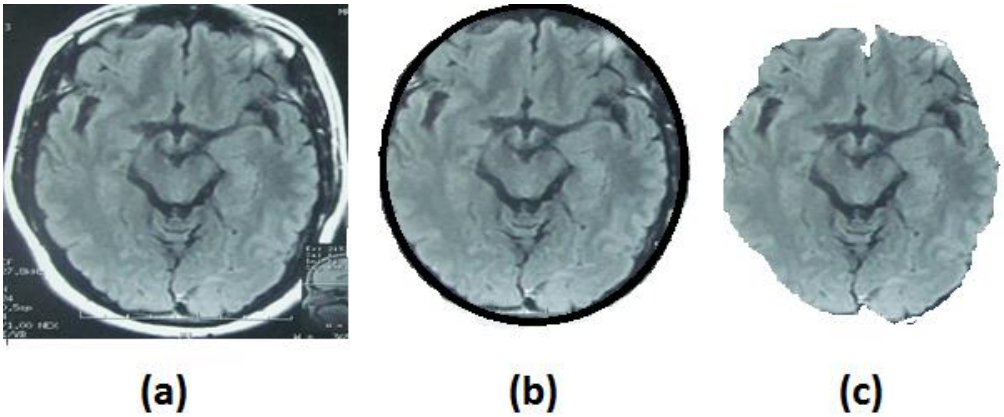

Figure 4: (a) ROI (b) ROI as in (c) Proposed Algorithm

3.6 Embedding process

The embedding process starts with the generation of watermarks as described in Section 3.3, then the host image is divided into ROI and RONI. Later on the watermarkis embedded in RONI. The process is described step by step as follows:

1. Generate the watermark;

2. Encrypt the watermark W with pseudo random binary vector P to produce W∗;

3. Separate the image into ROI and RONI;

4. Scramble the pixels in RONI using the secret key;

5. Embed the watermark in the scrambled pixels in LSBs of RONI;

6. Re-scramble the pixels in RONI to take them back to original position;

7. Combine ROI and RONI to get the watermarked image.

The block diagram of embedding process is shown in Fig. 5.

3.7 Extraction process

Number of steps of the extraction process are same as embedding process. Since proposedscheme is blind so there is no need of original image to extract the embedded watermark.The extraction process has the following steps:

1. Separate the watermarked image into ROI and RONI by using segmentation algorithm;

2. Scramble the pixels in RONI using the same secret key as was used for embedding;

3. Extract the LSBs from all the selected pixels;

4. Decrypt the extracted watermark W∗ using the P to get W;

5. Split the extracted watermark W∗ into W∗1 , W∗ 2 and W∗ 3 .

6. Compare the extracted watermark W∗ 3 (hash value) to the computed hash. If both aresame, received image is attested, otherwise declare it as unattested.

The block diagram of extraction process is shown in Fig. 6.

4 Experimental Results

This section describes the experimental results of proposed scheme. The experiments werecarried out using the dataset of 11 patients received from Integral University, Lucknow. Each patient's dataset contained about 60 to 100 slices of MRI images with

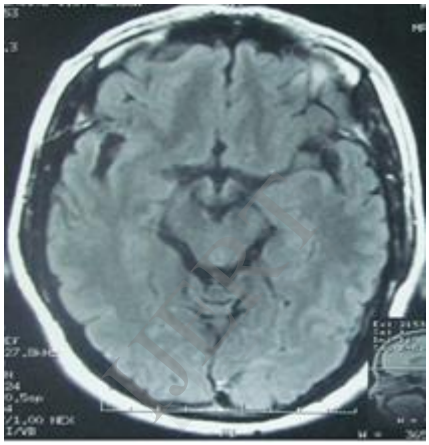

Figure 7: Image used in our research experiments (a) MRI image of start of brain

(b) MRI image of Middle of brain (c) MRI image of end of brainvarying slice thicknesses. The further details about how the medical images were got forexperimental work is given in Appendix B. All the images are resized to 256 × 256 pixelsand are 8-bit gray level images. The start, middle and end of the brainMRI slices of onepatient are shown in Fig. 7.

4.1 Imperceptibility

As a first step watermarks are generated and concatenated to form a single watermarkas described in Section 3.3. Later on this watermark is encrypted with pseudo randombinary vector generated by using the secret key in order to increase the robustness of embedded data . Table 1 shows the size of different watermarks generated and used insimulations of this work.

Fig.8(a) shows the ROI and Fig. 8(b) shows the RONI after dividing the MRIimage of middle part of brain into two regions. Fig. 8(c) shows the scrambled coefficientsof RONI. Fig. 9(a)

shows the watermarked image and Fig. 9(b) shows the differencebetween the cover image and the watermarked image.

The degradation introduced in watermarked image with respect to original one is determined

Watermark Type	Size	Binary Conversion	Total (Bits)
Logo	64 X 64	4096	4096
EPR	1024 (Char)	1024 X 8	8192
MAC	32 (Char)	32 X 8	256

Table 1: The size and type of each watermark

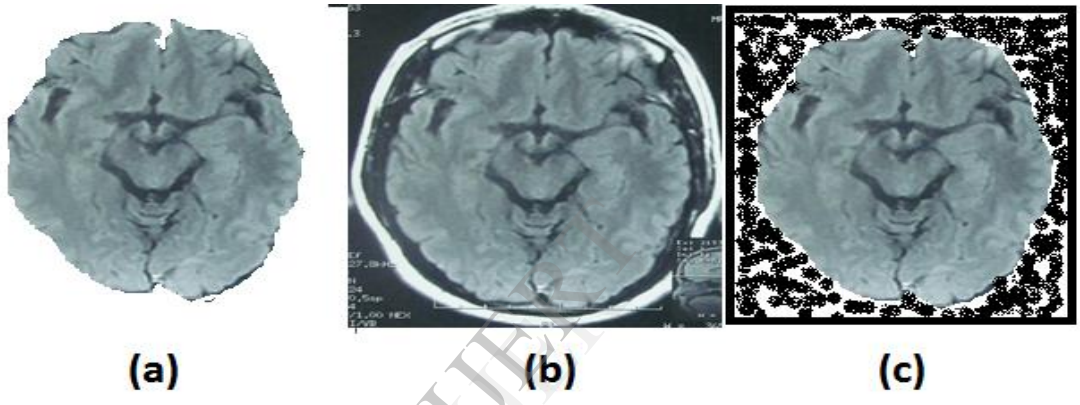

Figure 8: (a) Region of interest (b) Region of non- interest (c) Pixels scrambled inregion of non-interest

by using Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) metricsas described in the Eq. 3 and Eq. 4 respectively;

$$PSNR = 10\log_{10}\frac{R^2}{MSC} \quad (3)$$

where R is the maximum fluctuation of intensity in the input image data type. For example,if image has double precision floating point data type then R is 1 and if input image has an8 bit unsigned integer data type R is 255; and

$$MSE = \frac{\sum_{M,N}[I_1(m,n)-I_2(m,n)]^2}{MXN} \quad (4)$$

where M and N are number of rows and number of columns in both the cover (I1) andwatermarked image (I2). The degradation in terms of PSNR and MSE in the cover imageand watermarked image for different images are shown in Table 2.

For the image of size 256 × 256, 73.88% of total image pixels were found as RONI. Thewatermarks of different strengths were embedded in these RONI pixels. Table 3 shows thedegradation in visual quality of the watermarked image with respect to the original imageby embedding watermarks of varying strengths in terms of PSNR and MSE.

Image Type	Size(pixels)	PSNR(dB)	MSE
Start ofbrain	256X256	58.35	0.0940
Middle of brain	256X256	58.30	0.0960
End of brain	256X256	58.30	0.0960

Table 2: The imperceptibility of watermarked images in terms of PSNR and MSEImage Type

5 Summary

A blind fragile watermarking technique is proposed in the spatial domain to preserve thehistory of medical image by embedding the medical diagnosis report. While embedding thedata, ROI of medical image is avoided to ensure the integrity of ROI. The scheme allowsthe simultaneous storage and transmission of electronic patient record along with imageattestation information which can be extracted at the receiving end without the originalimage. Encryption of the embedded data is done to provide additional security. It alsoprovides sufficient capacity for storing about more than half of Kilo bytes of patient datafor the images of size 256 × 256. The scheme can easily be used in e-diagnosis applications

5. References:

[1] V. Fotopoulos, M. L. Stavrinou, A. N. Skodras, ”Medical Image Authentication and Self-Correction through an Adaptive Reversible Watermarking Technique”, Proceedings of 8th IEEE International Conference on Bio-Informatics and Bio-Engineering (BIBE-2008), pp. 1-5, October 2008.

[2] J. B. Feng, I.-C. Lin, C. S. Tsai, P. Chu, ”Reversible Watermarking: Current Status and Key Issues”, International Journal of Network Security, Vol. 2, pp. 161-171, May 2006.

[3] S. Weng, Y. Zhao, J. S. Pan, R. Ni, ”A Novel Reversibel Watermarking based on Integer Wavelet Transform”, Proceedings of IEEE International Conference (ICIP-2007, pp. 241-244, 2007.

[4] H.-W. Tseng, C.-C. Chang, ”An Extended Difference Expansion Algorithm for Reversible Watermarking”, Image and Vision Computing, Elsevier, Vol. 26, pp. 1148-1153, 2008.

[5] S. I. Fraser, A. R. Allen, ”A High Capacity Reversible Watermarking Techniques Based on Difference Expansion”, Proceedings of Signal and Image Processing (SIP-2008, Kailua-Kona, HI, USA, August 18-20, 2012.

[6] A. Giakoumaki, S. Pavlopulos, D. Koutsouris, ”Multiple Image Watermarking Applied to Health Information Management”, IEEE Transactions on Information Technology

in Bio-Medicine, Vol. 10, No. 4, October 2011.

[7] K. A. Navas, M. Sasikumar, ”Survey of Medical Image Watermarking Algorithms”,

Proceedings of the 4th International Confernce on Sciences of Electronic Technologies of Information and Telecommunications (SETIT-2007), pp. 1-6, March 25-29, 2011.

[8] N. A. Memon, S.A.M. Gilani, ”NROI Watermarking of Medical Images for Content

Authentication”, Proceedings of 12th IEEE International MultitopicConfernce (IN-MIC’2008), Karachi, Pakistan, pp. 106-110, December 23-24, 2008.

[9] P. Chang-Ri, W. Dong Min, P. Dong-Chul, H. SeungSoo, ”Medical Image Authentication Using Hash Function and Integer Wavelet Transform,” Proceedings of IEEE 2008 Congress on Image and Signal Processing, Snaya, Hainan, China, pp.7-10, May 27-30, 2008.

[10] K. A. Navas, S. ArchanaThampy, M. Sasikumar, ”EPR Hiding in Medical Imagers for Telemedicine,” Proceedings of World Academy of Science, Engineering and Technology, Vol. 28, April 2008.

[11] I. Usman, A. Khan, ”BCH Coding and Intelligent Watermark Embedding: Employing both Frequency and Strength Selection”, Applied Soft Computing, Vol. 10, No. 1, pp. 332-343, 2010.

[12] Z. Yuehua, C GuiXuan, D. Yunhai, ”A Image Watermarking Algorithm based on Discrete Cosine Transform Block Classifying,” Proceedings of 3rd International Conference on Information Security, Shanghai vol. 85, pp. 234-235, 2004.

[13] D. A. Karras ”A Second order Spread Spectrum Modulation Scheme for Wavelet based Low Error Probability Digital Image Watermarking”, ICGST International Journal on Graphics, Vision and Image Processing (GVIP), Vol. 3, No. 5, February 2005.

[14] S. Hai-mei, M. Tian-can, Q. Qian -ging, ”Spread Spectrum Watermark based on Wavelet Transform for Still Digital Image”, Wuhan University Journal of Natural Sciences, Vol. 9, No. 2, pp. 203-208, 2004.

[15] A. Khan, A.M. Mirza, ”Genetic perceptual shaping: utilizing cover image and conceivable attack information during watermarking embedding”, Information Fusion; Vol. 8, pp. 354-365, 2007.