

# Medical Image Watermarked by Simultaneous Moment Invariants and Content-Based for Privacy and Tamper Detection

Y.I. KHAMLIHI, M. MACHKOUR, K. AFDEL, A. MOUDDEN

Department of Physic, Faculty of Science, Metrology and Information Processing

Laboratory

University Ibn Zohr of Agadir

Faculty of Science, BP 28/S, Agadir 80000

MOROCCO

*Abstract:* - Confidentiality is an ethical necessity in health care. As for teleconsulting and telediagnosis, the use of multimedia technologies for telemedicine purposes is now gaining the ground all over the world. The progress increased however the risk of violation of the authenticity and integrity of the patient's records as the circulation of data via Internet is hard to control. In this paper we suggest using watermarking techniques using simultaneous content-based and moment invariant methods as a complementary safety measure. Content-based techniques have proven to be useful in detecting possible alteration in the temperate region of the image-based data while invariant methods are now widely used for pint pointing changes in the medical imagery.

*Key-Words:* - MAMMOGRAPHY IMAGE, WATERMAKING, CONTENT-BASED, MOMENT INVARIANTS.

## 1 Introduction

Image watermarking is the process of embedding into image specific information that helps establishing the ownership of the image. Watermarking techniques are divided in tow categories.

**Spatial Domain Watermarking**, where the least significant bits is replaced with watermark, and **Frequency domain watermarking**, where the image is first transformed to frequency domain and then the low frequency components are modified to contain the watermark. Watermarking can be applied in frequency domain by applying transforms like Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) or Wavelet transform (DWT).

Recently there has been much interest in watermarking of all intellectual property in digital format such as multimedia products, images, video, graphics, etc. [1] [2] [3]. The present attempt consists of adapting such technique to embedding the patient's medical record in his personal images. In cancerlogy the link between the patient's image and his medical record is often lost. Thus, embedding the patient directly in mammography image

could be a useful tool as a complementary safety measure.

Watermarking is also critical for the exchange of data through internet. In the last ten years, a significant progress has been achieved in using communication technologies to store and distribute medical data under digital formats. However, the use of theses technologies is not always safe as the medical records are freely circulated in open networks and thus subjected to alterations and misuses.

Classical encryption technology is an important tool that can be used to protect data transmitted over computer networks but it does not solve all digital data protection problems. Nowadays, digital watermarking appears as an efficient mean to ensure integrity and authenticity verification [4] [5].

Robust watermarks are designed to be hard to remove and to resist to common image-manipulation procedures. They are useful for copyright and ownership assertion purposes.

Unlike robust watermark, fragile watermarks are designed to be easily destroyed if the watermarked image is manipulated in the slightest manner. This property is investigated for tamper detection.

In this paper we propose to combine moment invariant and content based watermarking methods, this will allow adding a supplementary security level, witch is suitable for transmission in open network as Internet and tamper detection in medical image.

## 2 Watermarking techniques for medical images

Integrity and confidentiality are critical issues in medical imagery. It is therefore of paramount importance to ensure the protection of the image content for strict ethics, legislative and/or diagnostic reasons. The ultimate objective is to prevent unauthorized manipulation and misappropriation of such digitized images. The risks increased when dealing with an open environment like the Internet.

Prior to applying watermarking techniques to medical imagery applications, it is important that the requirements imposed by medical images are carefully analyzed in order to investigate whether they are compatible with existing watermarking techniques or not. Different watermarking schemes have been proposed to address the problems of medical privacy and security [6].

## 3 Combination of watermarking methods

The ill-posed problem is the authentication and integrity of both image and its associated patient record. Fragile watermark are designed to be easily and used for tamper detection in medical image. This method is based on LSB technique witch is a well known method for embedding data with a high embedding capacity. The least significant bits (LSB) of each pixel of the image are generally considered as noise caused by the imaging device, therefore these bits can be used for embedding secret message and patient information without changing the visual quality of the image.

The watermark is composed of the edge map and the mean of several functions of the second

and third order moments. Invariant moments are designed to be not affected by scaling, rotating and/or orthogonal transformations; this has the advantage of making the watermark image dependent. The edge map is obtained by re-scaling the original image and using a LoG detector [7]. The logic of use the edge map is that local features such as contours or edges are unique to each image, and therefore, can act as a signature of the image [8]. Attacks or manipulations, such as removal of sensitive parts or addition of foreign objects or features, result in significant changes to the edge map because objects are supposed to be different from its background or neighboring objects in terms of gray level or texture property, therefore it is possible to locate de tampering regions.

### 3.1 Watermark construction

The first step in constructing watermark is to compute the mean of the second and third order moments of mammography image without LSB bitplane. Then, the image should be resized in order to increase the embedding capacity of LSB's bitplane prior to extracting the edge map using the LoG operator as shown in figure 1. The edge map should be subdivided in blocks and arranged in a way to make its rebuilding difficult for a no-authorized user. The technique consists of replacing the right part of the block by the left neighboring one along a circular path. The LSB's bitplane of the image is substituted with watermark data composed by:

- Encrypted patient's information and mean value of the second and third order moments, The AES is used as encryption algorithm [9]
- Edge map built as mentioned above.

0	1	0
1	-4	1
0	1	0

Fig.1. Operator de Laplacien of Gaussian (LoG)

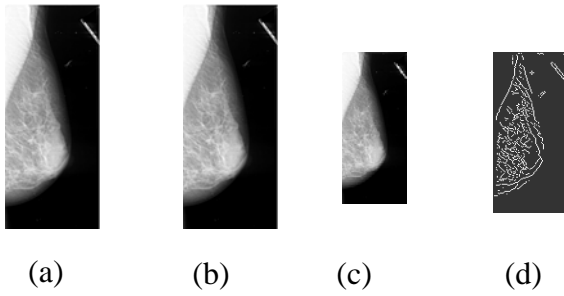


Fig.2 Creation edge map

(a) Original image (b) Original image without LSB, (c) image (b) resized, (d) Edge map of image (c) obtained by convolving image (c) with LoG operator

### 3.2 Locating of tamper region

At the reception side, the user starts with extracting the patient's data and the mean value of the second and third order moments from LSB's bitplane of the received image. If the image received is intact that means that the moment invariant value is still unchanged. If not, the value will change.

In order to identify the altered region, one should rebuild the edge map following the steps previously described and to compare it with the one embedded in the LSB's bitplane. A simple comparison of these two edge maps permits to locate the modified tamper region whatever the degree of alteration.

## 4 Experimental Results

Breast images, taken from mammography databases, were used to test the watermarking procedure shown above. The mammography image  $I(x,y)$  (Figure 3-a) was watermarked (Figure 3-b) using the method described previously. The mean value of invariants moments is 0.9489. Edge map pixel was obtained by convolving the mammography image  $I(x,y)$  with LoG operators. The LSB's bitplane of the image is substituted by watermark composed by edge map, encrypted patient's information and the mean value of invariants moments. In the reception side the breast mammography image was slightly altered at the teat level (Figure 3-c). This modification gives different reading of the

mean value of the invariants on the tampered image which was 0.9883 against 0.9489 saved in the LSB's bitplane indicating that the image was indeed tampered during the transmission. In order to locate the tampered region, the image received as first resized and then convolved with edge detector operator (LoG) to get edge map. The later was compared to the one extracted from the LSB's bitplane. The comparison between these two edge maps coupled with contrast modification permits to identify the altered region. In case of no tampering, the comparison shows a totally black map (Figure 3-e).

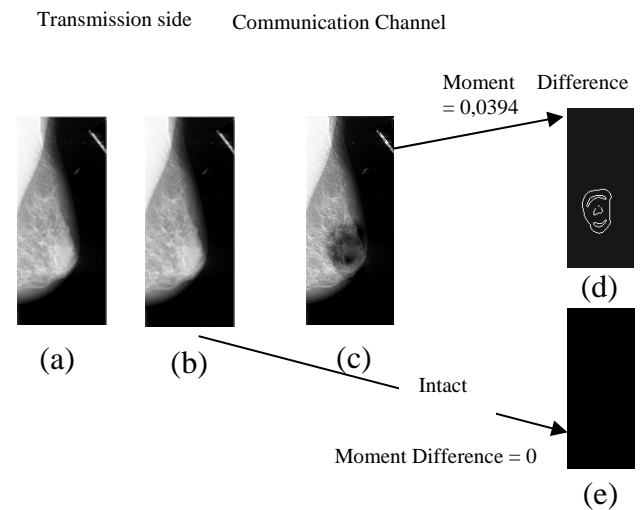


Fig.3 (a) original image, (b) image watermarked, (c) image tampered in the teat of breast (d) difference of these two edge map followed by a contrast modification

## 5 Visual quality evaluation

The evaluation was performed using the three commonly used parameters in visual image quality metric assessment [10]. These parameters are:

Relative entropy

$$Vq_e = \sum_k p_k \log_2 \left( \frac{p_k}{q_k} \right) \quad (1)$$

$Vq_e$  is expected to be low for similar images (0 if the images are equal) and high if the relative information differs significantly. where  $p$  and  $q$  are the probability distributions of  $I$  and  $I_w$  respectively, over all pixel intensities  $k$ .

**Peak Signal-To-Noise Ratio (PSNR)**

$$Vq_p = 10 \log_{10} \left( \frac{255}{RMS} \right)^2 \quad (2)$$

PSNR penalizes the visibility of noise in an image. Thus, two images that are exactly the same will produce an infinite PSNR value (RMS : Root Mean Square).

**Mean Square Error (MSE)**

$$Vq_s = \frac{1}{MN} \sum_i \sum_j (I_{ij} - Iw_{ij})^2 \quad (3)$$

MSE gives an indication of how much degradation was introduced at a pixel based level. The higher the MSE, the greater the level of degradation.

Table1: Metric Visual Quality Parameters

These parameters are used to quantify the quality of visualization of the image taken from the mammography image database. The table 2 gives an example of the image with values of the quantification parameters of the visualization quality. In our case, these values show that the visual aspect of image is well preserved.

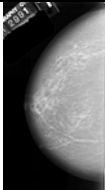
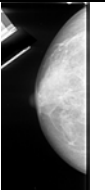
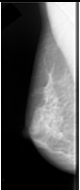
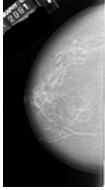
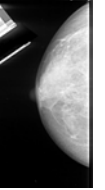
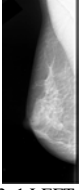
 A_0108_1.LEFT_CC	 A_0002_1.LEFT_CC	 A_0002_1.LEFT_MLO
 A_0108_1.LEFT_CC watermarked	 A_0002_1.LEFT_CC watermarked	 A_0002_1.LEFT_MLO Watermarked
<b>Vq<sub>c</sub> =0.0312</b> <b>MSE=2.4702e-007</b> <b>PSNR=81.1671</b>	<b>Vq<sub>c</sub> =0.0294</b> <b>MSE=1.9809e-007</b> <b>PSNR=81.6465</b>	<b>Vq<sub>c</sub> 0.0331</b> <b>MSE= 1.9594e-007</b> <b>PSNR = 81.6702</b>

Table 2 – Examples of mammography image with the values of the visualization quality quantification parameters

## 6 Conclusion

This article proposed an efficient digital watermark scheme to increase security, confidentiality and integrity of medical image to transmit it via internet by combining two

watermarking techniques. First technique uses a mean value of the second and third order moments as effectiveness tamper detection. Second technique uses the edge map of image to localize the altered region. The annotation watermark can be used to introduce the patient's information in a private and sure manner all while preserving the visual quality of watermarked image.

*References:*

- [1] Jagadish Nayak, P Subbanna Bhat, Rajendra Acharya and Niranjana UC, “Simultaneous storage of medical images in the spatial and frequency domain: A comparative study”, *BioMedical Engineering OnLine*, 2004.
- [2] Cox J, Miller ML, Bloom JA: Digital Watermarking. San Francisco, CA: Morgan Kaufman, 2002.
- [3] Knopp R, Robert A: Detection Theory and Digital Watermarking. *Proceedings of SPIE*, 2000, 3971:14-23.
- [4] Samia Boucherkha and Mohamed Benmohamed, “A Lossless Watermarking Based Authentication System For Medical Images”, *International Journal of signal processing*, Vol. 1 Num. 4, 2004, 278-281, ISSN:1304-4494
- [5] X. Q. Zhou, H. K. Huang, and S. L. Lou, Authenticity and Integrity of Digital Mammography Images, *IEEE Transactions on Medical Imaging*, Vol. 20, No. 8, August 2001, 784-791
- [6] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec, “Relevance of Watermarking in Medical Imaging”, in *Proceedings of the IEEE EMBS Conf. on Information Technology Applications in Biomedicine*, Arlington, USA, Nov. 2000, p. 250-255.
- [7] Hildreth, E. C. “The Detection of Intensity Changes by Computer and Biological Vision Systems,” *Computer Vision, Graphics, and Image Processing*, 22, 1-27, 1983.
- [8] Chang-Tsun Li, Der-Chyuan Lou, and Jiang-Lung Liu, “Image Integrity and Authenticity Verification via Content-Based Watermarks and a Public Key Cryptosystem”, in *Journal of Chinese Institute of Electrical Engineering*, vol 10, no. 1, 2003, pp 99-106.
- [9] J. Daemen, V. Rijmen, (1999, September 03). AES Proposal Rijndael, Networks (2nd ed.) [Online]. Available: <http://csrc.nist.gov/CryptoToolkit/aes/index.html>

- [10] B.M. Planitz, A.J. Maeder, Medical Image Watermarking: A Study on Image Degradation, *Australian Pattern Recognition Society (APRS) Workshop on Digital Image Computing (WDIC 2005)*, Brisbane, Australia, 12 February 2005; 2005: 3-8.