

# Authentication System for Medical Watermarked Content Based Image

Y. I. KHAMLICH, Y. ZAZ, and K. AFDEL

**Abstract**—An efficient digital watermarking scheme to transmit the medical image which embeds an encrypted data is proposed in this paper. We substitute the non-significant LSB bitplane of the image with encrypted data composed of the patient data and a digest. The latter is composed of two numbers representing the sum of detected image edge pixels without LSB bitplane, using Canny and Laplacien of Gaussian (LoG) operators respectively.

On the receiving side, after decrypting data contained in the LSB bitplane, a comparison of the digest number saved on the watermarked image and the digest computed on the received image without LSB bitplane. The equality of the two digests, saved in the LSB bitplane and computed on the received image, proves the integrity and the authenticity of the medical image.

**Key words:** Medical image, Digital watermarking, Canny, LoG, digest, LSB bitplane.

## I. INTRODUCTION

For the purpose of diagnosis, medical images must be utilized in association with ancillary data, such as demographic information (patient identity, age, gender, etc.), data acquisition parameters, and comments and notes from medical personnel.

Solomon [1] provided standard of image, called DICOM, which can integrate patient information onto the image data header section.

On the other hand, the advances in communication technologies provide a new ways to store and distribute medical data in a digital format. But these advances have introduced new risks for inappropriate use of medical information circulating in open networks, and then use of DICOM standard presents a high risk of tampered with, because the information can be easily obtained from the image file.

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 of authentication and copyright protection [2] [3] [4].

Y. I. Khamlichi is with the Acquisition team, Modeling and information treatment, Laboratory of Instrumentation and Measures, Ibn Zohr University, Faculty of Science, BP 28/S, Agadir 80000, Morocco (phone: 212-64-166630; fax: 212-48-242243 ; e-mail : ykhamlichi@yahoo.com)

Y. Zaz is with the Laboratory of Electronic, Signals-Systems, and Informatics (L.E.S.S.I.), Department of Physic, Faculty of Sciences, B.P. 1796-30000, Fez, Morocco (e-mail : youssef\_zaz@yahoo.fr)

K. Afdel is with the Acquisition team, Modeling and information treatment, Laboratory of Instrumentation and Measures, Ibn Zohr University, Faculty of Science, BP 28/S, Agadir 80000, Morocco (e-mail : kafdel@yahoo.fr).

Robust watermarks are designed to be hard to remove and to resist 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 ideal for image authentication applications (in our case medial images), where the objective is to determine if the watermarked image has been tampered with or modified.

Early fragile watermarking systems embedded checksums [5] or pseudo-random sequences [6], [7] in LSB bitplane of an image. Zhao et al.[8] presented a method to integrate and encrypt medical data using a bipolar multiple-number based algorithm for transmission of electronic medical records between hospitals. Rajendra et al.[9] combined medical images with encrypted patient data by interleaving different sources of information. These methods have been successful in specific applications. However, they integrate data using a packaging process without exploring the fundamental properties of the image features.

To solve this problem, we present a new approach to ensure the authenticity and the integrity of data, by integrating a digest, computed from image features. The digest is composed of the edges sums, extracted from the image without LSB bitplane using Canny [10] and Laplacian of Gaussian (LoG) [11] detectors respectively. In fact, the LSB bitplane is substituted by encrypted data composed by patient information and the digest.

## II. WATERMARKING TECHNIQUES FOR MEDICAL IMAGES

Medical imagery is a field where the protection of the integrity and confidentiality of content is a critical issue due to the special characteristics derived from strict ethics, legislative and diagnostic implications. It is very important to prevent unauthorized manipulation and misappropriation of such digitized images. The risks are increased when dealing with an open environment like the internet. Medical images should be kept intact in any circumstance and before any operation they must be checked for:

- Integrity: the image has not been modified by non authorized people.
- Authentication: the image belongs indeed to the correct patient.

Before applying watermarking techniques developed for multimedia applications to medical imagery applications, it is important that the requirements imposed by medical

images are carefully analyzed to investigate whether they are compatible with existing watermarking techniques.

Different watermarking schemes have been proposed to address the problems of medical confidentiality protection and both origin and data authentication [12].

### III. AUTHENTICATION SYSTEM FOR MEDICAL WATERMARKED CONTENT BASED IMAGE

The ill posed problem is the authentication and the integrity of both image data and its associated patient data. Fragile watermark are designed to be easily destroyed if the watermarked image is manipulated in the slightest manner. This method is ideal for image authentication, where the objective is to determine if the watermarked image has been tampered with or modified.

LSB technique is fragile and well known method for embedding data with a high embedding capacity. The least significant bits (LSB bitplane) of each pixel of the image are generally considered as noise caused by the imaging device. So, these bits can be used for embedding secret message and patient information without disturbing greatly the appearance of the image.

To ensure confidentiality of data embedded, we encrypt it using highly secured algorithm called as Advanced Encryption Standard (AES) [13]. On the other hand, in order to detect any malicious attacks that can be happened we use edge map, the logic is that local features such as contours, edges, or zero-crossings are unique to each image, and therefore, can act as a signature of the image. 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 neighbouring objects in terms of gray level or texture property. Therefore, it is useful to compute the digest according to image edge map. The digest is given by the sum edge map pixels of original image. To obtain map edge we use Canny and LoG Detectors witch uses second derivative operator instead of first derivative operator, this characteristic makes the operator sensitive to any small variation, and then it is useful to detect any eventual malicious attack.

### IV. TECHNICAL DESCRIPTION

#### A. Emission side

The first step of this technique is to extract an edge map from the original image without LSB bitplane and we compute the digest from the image. The digest is composed by two numbers representing the sum map edge pixel obtained by Canny and LoG operators respectively. Step two, we substitute the LSBs bitplane of the image with encrypted data composed by patient's information and the digest using AES encryption algorithm and we submit the watermarked image on Internet network.

#### B. Reception side

In reception side we decrypt data stored in the LSB's bitplane of the image and we compute the digest from the image without LSB bitplane using Canny and LoG operators respectively under the same conditions. We compared the digest to the one obtained from decrypted data. If the image will be not tampered, the digest will be not modified and the integrity and authenticity of the image during the transmission will be preserved. The Figure 1 describes clearly the procedure.

### V. EXPERIMENTATIONS

We use breast images, taken from mammography database [14], to test the watermarking procedure. In the emission side, the mammography image (fig. 2a) was watermarked using the method described. The digest, representing the sum of edge map pixel obtained by Canny and LoG operators respectively, is made up by the sum of two values 4677 and 7283. The LSB's bitplane of the image is substituted by encrypted data composed by patient's information and the digest (fig. 2b). In the received side, when the image is not tampered (fig. 2c), the computation of the digest from the obtained image ensures that it is not attacked during the transmission. In contrary, when the image is tampered by a stain in the breast teat (fig. 2d), the digest is different from the one saved in the encrypted data on the LSB's bitplane (4109 and 6562). This gives indication that the image was tampered during the transmission.

The proposed method is a good tool to demonstrate any modification of the transmitted images. Any attack destroys the whole data or at least modify the original values of Canny and LoG sums, as illustrated by Table 1. It appears from obtained data that any modification of the images resulted in different values of Canny and LoG.

### VI. CONCLUSION

We proposed a fragile and efficient digital watermarking scheme to transmit the medical image which embeds an encrypted data. LSBs bitplane is substituted by encrypted data composed of the patient data and a digest which is composed by two numbers representing the sums of detected edge of the image without LSB bitplane, using Canny and Laplacian of Gaussian (LoG) operators respectively.

The proposed method ensures the authenticity, integrity of the image, and the confidentiality of the patient's data.

### REFERENCES

- [1] H.P. Solomon, "Integration of haemodynamic and electrocardiographic waveform data with DICOM images," *Int J Card Imaging*, vol. 14(5), 1998, pp. 301-3066.
- [2] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *IEEE Proceeding*, vol. 87, no. 7, July 1999, pp.1079 -1107.
- [3] F. A. P. Peticolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," *IEEE Proceeding*, vol. 87, no. 7, July 1999, pp. 1062 -1078.

- [4] C. I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," *IEEE Transactions on Selected Areas in Communications*, vol. 16, no. 4, May 1998, pp. 525-539.
- [5] S. Walton, "Information authentication for a slippery new age," *Dr Dobbs Journal*, vol. 20, no. 4, April 1995, pp. 18-26.
- [6] R. Wolfgang and E. J. Delp, "A watermark for digital images," *Proceedings of the IEEE International Conference on Image Processing*, vol. 3, 1996, pp. 219-222.
- [7] R. Wolfgang and E. J. Delp, "Fragile Watermarking Using the VW2D Watermark," *Proceedings of the SPIE/IS&T International Conference on Security and Watermarking of Multimedia Contents*, vol. 3657, January 25 - 27, San Jose, CA, 1999, pp. 204-213.
- [8] H-M. Zhao, C-M. Hsu, and S-G Miaou, "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records," *IEEE Trans. Information Technology in Biomedicine*, Vol. 6, 2002, pp. 46-53.
- [9] A. U. Rajendra, A. Deepthi, B. P. Subbanna, and U. C. Niranjana, "Compact storage of medical images with patient information," *IEEE Trans. Information Technology in Biomedicine*, Vol. 5, No. 4, 2001, pp. 320-323.
- [10] J. Canny. "A Computational Approach to Edge Detection," *IEEE Trans. Pattern Anal. & Machine Intell.*, vol. 8, 1986, pp. 679-698.
- [11] Hildreth, E. C. "The Detection of Intensity Changes by Computer and Biological Vision Systems," *Computer Vision, Graphics, and Image Processing*, vol. 22, 1983, pp. 1-27.
- [12] 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, pp. 250-255.
- [13] J. Daemen, V. Rijmen, (1999, September 03). AES Proposal Rijndael, Networks (2nd ed.) [Online]. Available: <http://csrc.nist.gov/CryptoToolkit/aes/index.html>
- [14] Digital Database for Screening Mammography. Available: <http://marathon.csee.usf.edu/Mammography/Database.html>

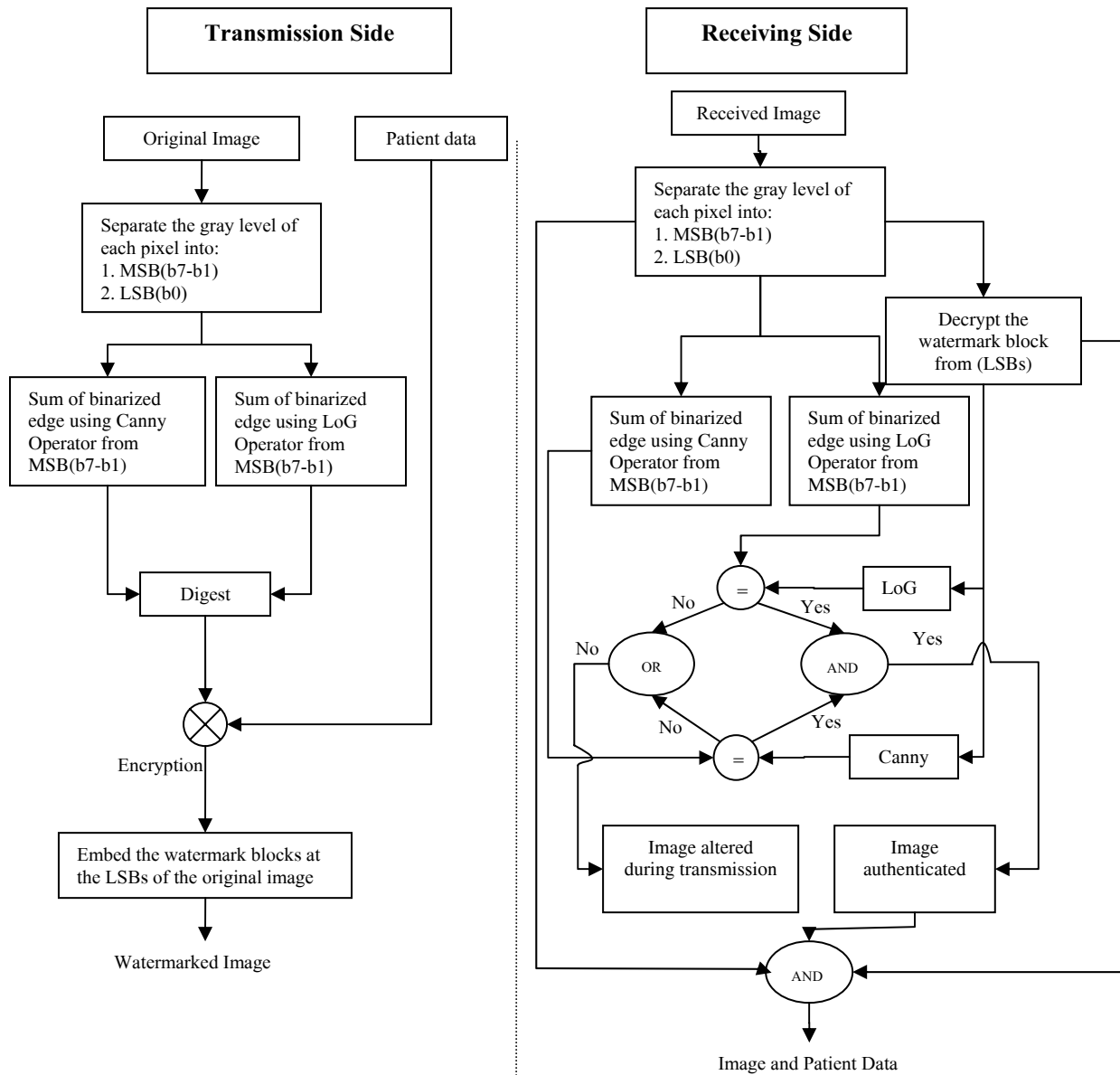


Fig. 1. Flow Diagram of the content-based watermarking scheme

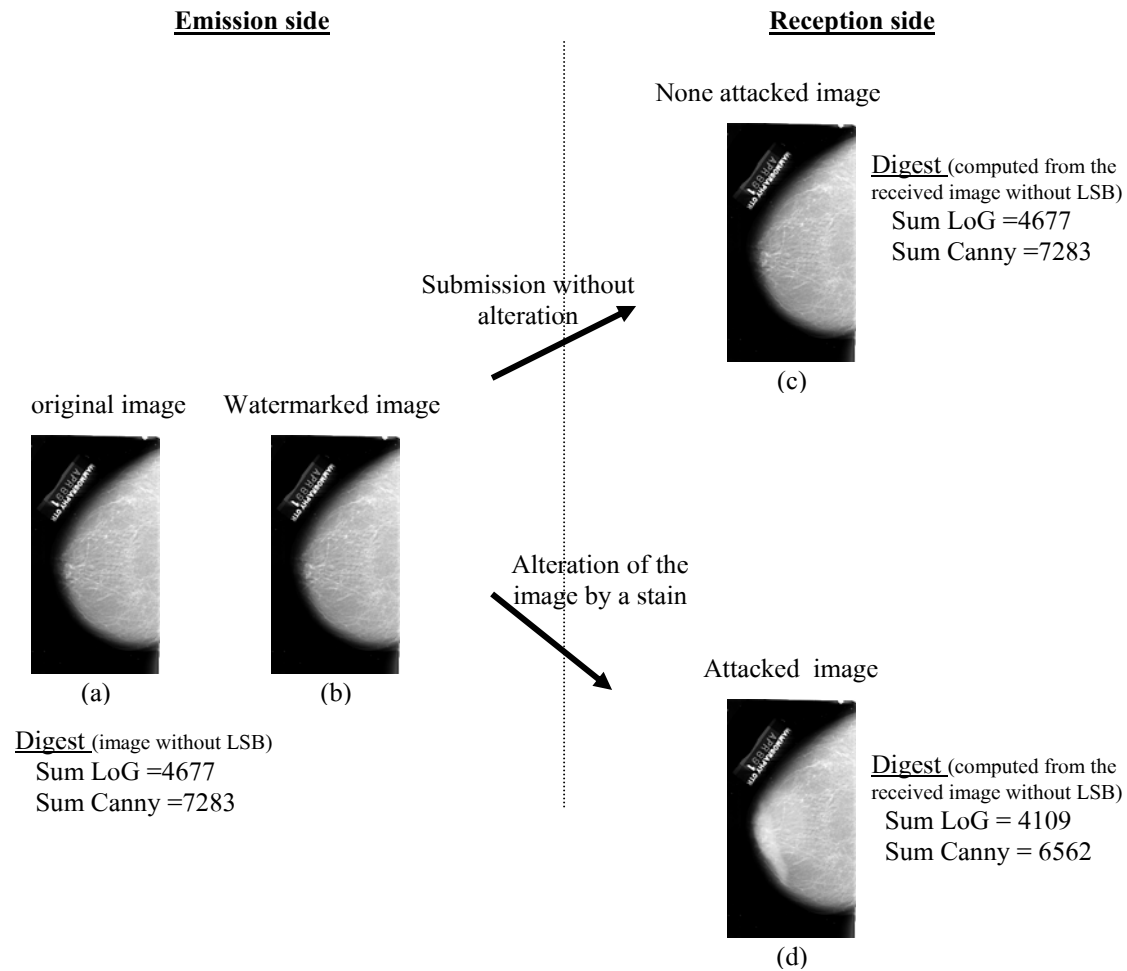


Fig. 2. Image of the breast using content-based watermarking scheme.

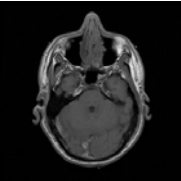
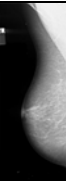
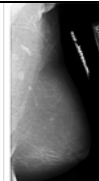
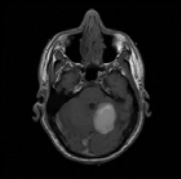
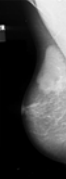

		
head_mri	A_0003_1.LEFT_MLO	A_0012_1.RIGHT_MLO
Sum LoG = 3272 Sum Canny = 4215	Sum LoG = 2461 Sum Canny = 3555	Sum LoG = 2577 Sum Canny = 6897
		
head_mri Stain added	A_0003_1.LEFT_MLO Stain added	A_0012_1.RIGHT_MLO Histogram Equalized
Sum LoG = 3321 Sum Canny = 4368	Sum LoG = 2384 Sum Canny = 3883	Sum LoG = 2930 Sum Canny = 5542

Table 1 – Examples of images with the values of LoG and Canny sums