International Journal of Medical, Medicine and Health Sciences
ISSN: 2517-9969
Vol:1, No:1, 2007

A Lossless Watermarking Based Authentication System For Medical Images

Samia Boucherkha and Mohamed Benmohamed

Abstract**—** In this paper we investigate the watermarking authentication when applied to medical imagery field. We first give an overview of watermarking technology by paying attention to fragile watermarking since it is the usual scheme for authentication. We then analyze the requirements for image authentication and integrity in medical imagery, and we show finally that invertible schemes are the best suited for this particular field. A well known authentication method is studied. This technique is then adapted here for interleaving patient information and message authentication code with medical images in a reversible manner, that is using lossless compression. The resulting scheme enables on a side the exact recovery of the original image that can be unambiguously authenticated, and on the other side, the patient information to be saved or transmitted in a confidential way. To ensure greater security the patient information is encrypted before being embedded into images.

Keywords**—**Medical Imaging, Invertible Watermarking, Authentication, Integrity.

I. Introduction

The advances in multimedia and communication technology have provided new ways to store, access and distribute medical data in a digital format. On the other hand, these advances have introduced new risks for inappropriate use of medical information circulating in open networks , given the ease with which digital content can be manipulated. It is well known that the integrity and confidentiality of medical folders is a critical issue for ethical as well for legal reasons. Classical encryption technology is an important tool that can be used to protect data transmitted over computer networks but it doesn't solve all digital data protection problems. At the receiver's side, decrypted content may be subject to unauthorized use or manipulation. Digital watermarking is an emerging technology for digital image authentication and copyright protection. Copyright protection is achieved by robust watermarking while image authentication is usually achieved by fragile schemes. A fragile watermarking scheme detects any manipulation made to a digital image to guarantee the content integrity while a robust scheme prevents the watermark removing unless the quality of the image is greatly reduced. In general, fragile schemes modify the LSB planes of the original image in an irreversible way. This is not acceptable in medical imagery where the least modification can lead to an erroneous diagnosis as well for legal reasons. Invertible watermarking is a new paradigm which enables the exact recovery of the original image upon extraction of the embedded information. In this work, a watermarking technique is adapted to provide both authentication and confidentiality in a reversible manner without affecting the image in any way. The patient information is interleaved with the corresponding medical image using a quite simple data compression method. To ensure greater security the patient information is encrypted before being embedded into images. LSB is used as embedding method and RLE technique is employed for data compression. A derived form of Vigenere algorithm [8] is adapted here for encryption. Results are tabulated for a specific example.

In section 2, we present an overview of watermarking technology by paying attention to fragile watermarking since it is the usual scheme for authentication. In section 3, the desired functionalities of watermarking techniques are discussed in terms of medical images and the new "invertible" watermarking paradigm is presented as a well designed scheme for the medical field. In section 4 we give the main functionalities of our authentication system based on invertible watermarking. In section 5 some experiments are shown demonstrating the impact that the presence of the watermark has on the HVS (Human Visual System) and we give finally our conclusion.

II. SHORT REVIEW OF WATERMARKING TECHNOLOGY

A digital watermark is a secret key dependant signal inserted into digital data (images, sound, texts) and which can be later detected/extracted in order to make an assertion about the data (identification, authentication…) [6]. Technically, the digital watermark is represented as a kind of 'natural' noise. The identification information is encoded into the original unwatermarked data by adding more 'natural' noise and/or rearranging existing noise. The locations for embedding the watermark as well as the value of the watermark are determined by secret elements. In this work we are first interested in image watermarking.

Manuscript received November, 2004.

S. Boucherkha is with the Vision & Infography group, LIRE Lab, Computer Science Department, Mentouri University, Route de Ain El Bey, Constantine, 25000 Algeria (phone: 213031963833; fax: 213031963833; e-mail: sboucherkha@yahoo.com).

M. Benmohamed is with the Vision & Infography group, LIRE Lab, Computer Science Department, Mentouri University, Route de Ain El Bey, Constantine, 25000 Algeria.

Watermarks can either be visible or invisible.
- A visible watermark is commonly used in applications such as photograph catalogs, allowing the viewer to see what the image is like before ordering a good copy. A visible logo or label is placed at the corner of the image or overlays a transparent pattern over the image. This renders the viewed image useless for reproduction or commercial use.
- Invisible watermarks are used in public information settings such as digital images libraries , museums and art galleries.
The location of watermark embedding determines two kinds of methods:
- The spatial domain methods embed watermark information directly into images pixels.
- The frequency domain methods embed watermark information in the transform domain. The general approach used in these methods is to divide the image into blocks. Each block is mapped into the transform domain using either the Discrete Cosine Transform (DCT) [9], the Discrete Fourier Transform (DFT), or the Wavelet Transform. Embedding the watermark in the frequency domain can provide more robustness than in the spatial domain. It is strong against attacks like compression where spatial domain is not.
Image watermarking techniques can be distinguished according to the way the watermark is revealed from the watermarked image. One way is by comparing this image to the original one, while the other doesn't resort to this comparison. The second are usually referred to as *blind* watermarking techniques and are preferable.
A watermarking scheme can also be classified as either robust or fragile:
- The robust watermarks are generally used for copyright and ownership verification. In this case it is important that the mark, that contains the proof of property, can survive all types of attacks so much that the image remained exploitable. - The fragile watermarks are useful for purposes of authentication and integrity attestation. They provide a guarantee that the image has not been tampered with and came from the right source. The watermark must be characterized by strong sensitivity to all modification of the image, even lightest, in order to prove that there was tentative of attack. Fragile watermarking is of great importance in courtroom defence, reliable e-business, medical image databases, etc. When the content of multimedia is suspected, the extraction of fragile watermark can be used to detect and localize tampers, even present the category of tampering.

III. Requirements for Medical Imaging

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: that is the image has not been modified by non authorized people;
- authentication : that is the image belongs indeed to the correct patient.

Watermarking is a new technology which hopefully can help in that aim. 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 [2]. Examples are robust watermark containing the doctor's digital signature for authentication, and fragile watermark for the purpose of data integrity control. Classical watermarking schemes impose more or less distortions to the original data due to quantization, bit-replacement, truncation, etc…

For most applications some distortion in the image content might be acceptable, but for medical applications, the images must be kept perfectly without any loss of information, that is, the watermark should not introduce visible distortion in the image. For example, the typical shape of a healthy ECG signal is well known to cardiologists. Any deviation from that shape is usually considered to be a symptom of a pathological case [3]. This render traditional schemes inapplicable to medical imagery. The latest years a new paradigm of watermarking authentication has been presented [1],[3],[4] involving the insertion of a watermark into the host image in a lossless manner, i.e., enabling the exact recovery of the original image upon extraction of the embedded watermark. This property matches exactly the requirements imposed by manipulating medical images. In this work we combine cryptographic tools (encryption and message authentication code or MAC) [8] with invertible watermarking scheme, to provide confidentiality and authentication in the same time and in a reversible way. The confidentiality is achieved by interleaving the encrypted form of patient information with the corresponding medical image while the authentication is achieved by inserting the message digest. In the verification step, removing the MAC and the patient information will reveal the original image in its integrality. Computing the MAC of this latter and comparing it with the extracted one will authenticate unambiguously the image. If the image is altered in some way, the verification program will alert the user (the doctor). There are several advantages in watermarking a medical image in such a way:
- A patient doesn't necessarily wants his/her medical image open to the public, nor his name appended to a publicly available image. In this point of view, medical image can be viewed as the copyright of this patient.
- Sometimes the link between image and patient is lost, thus, embedding the patient info in the image could be a useful safety measure.

- When an archiver in a HIS (Hospital Information System) save an image for a long time, and a different person refers to the image, this latter must confirm its integrity before using it (e.g, for a comparative study with similar cases).
- images may refer to a newly discovered medical case, therefore it is desirable that the copyright and integrity of the medical image are protected by digital watermarking.
- embedding the authentication code in the image rather than appending it to the end makes it less sensitive to attacks.

In the next section we outline the principles of the invertible data embedding method.

IV. AUTHENTICATION USING INVERTIBLE WATERMARKING

In classical image authentication, a short image digest, such as the cryptographic checksum or MAC (Message Authentication Code), is attached to the image file in a header or a separate file. Checksums or MACs [8] are based on the fact that it is unlikely that two different natural images have the same signature, and even if a single bit of image data changes, the signature may be totally different. In image authentication using watermarking, the MAC is invisibly embedded in the image itself [6]. This has the advantage that the image can authenticate itself without accessing any side information and makes the MAC less sensitive to attacks.

Invertible watermarking selects pixels or transformation coefficients, and then losslessely compresses them so as to save space for the watermark. Therefore, it has the property that the embedding distortion can be completely removed from the watermarked image without any side channel [4]. At the detector side, the original host image can be recovered in its integrality.

Authentication and data embedding, are, in practice, time and memory consuming operations. To achieve good performance for our proposed scheme, we opted for a quite simple lossless compression method, namely RLE (Run Length Encoding). The ratio currently reported by the technique in the literature is about 40%, which covers broadly our embedding needs. It is a lossless algorithm and merely simple to implement. RLE algorithm acts by replacing repeating strings of same symbol by a single instance of the repeated symbol along with a count of the number of times it is repeated. It is particularly efficient for binary files where it takes advantage of the fact that the runs alternate between 0 and 1 avoiding storing the 0's and 1's themselves. So, this compression algorithm is suitable for our digital watermarking authentication system.

Similarly, we adopt HMAC, a keyed-hash authentication code as the MAC for authentication with MD5 as a one-way hash function [8]. The same secret key K is used for the MAC computing and for encryption. MD5 uses 64 bytes input blocks and produces a 16 bytes digest (128 bits). Two strings are first defined, ipad and opad where ipad is the byte (0 X 36) duplicated 64 times and opad is the byte (0 X 5C) duplicated 64 times. The MAC is then

$$HMAC_K(M) = MD5(K+opad,MD5(K+ipad,M))$$

where M is the image to sign.

Bearing in mind the particularity of the images in the medical field and for simplicity purpose, we opted for the use of the LSB domain watermarking technique [6]. LSB is a simple non robust embedding technique with a high embedding capacity and small embedding distorsion The least-significant bits of each pixel of the image are generally considered as noise caused by the imaging device. So, these bits can be used for secret message embedding without disturbing greatly the appearance of the image.

Embedding process:

In the embedding process, we scan the image by rows and losslessly compress the bit-stream of LSB values as the image is scanned. Once this compressed bit-stream is obtained, we concatenate it with the patient information and the hash and embed it into the LSBs by scanning the image in the same pattern. The overall procedure is then a four steps process:

(1) Calculate the authentication code (MAC) of the image using MD5 algorithm;

(2) Concatenate the authentication code and patient information and encrypt the resulting string ;

(3) Select the LSBs of all pixels and compress the resulting string using RLE algorithm.

(4) Concatenate the compressed string and the encrypted string and insert them back into the LSB locations by adding blanks if necessary.

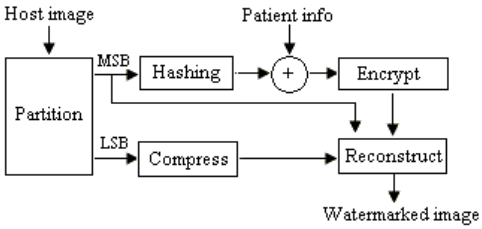


Fig.1 Embedding phase

Extraction and verification process:

The message extraction proceeds by scanning the image in the same manner as during the embedding, extracting the concatenated bit-stream from all LSBs and calculating the actual MAC from MSBs. The extracted bit stream is partitioned in two parts, the encrypted patient information and the MAC, and the compressed LSBs of original image. Once the decompressed bit-stream is obtained by RLE decompressing algorithm, we scan the image in the same defined pattern as we did during the embedding and restore the original values to their appropriate places in the image's LSBs. On the other hand, the second part of extracted bit-stream is decrypted, obtaining the patient information and the original MAC. Comparing it with the actual MAC will authenticate or reject the image.

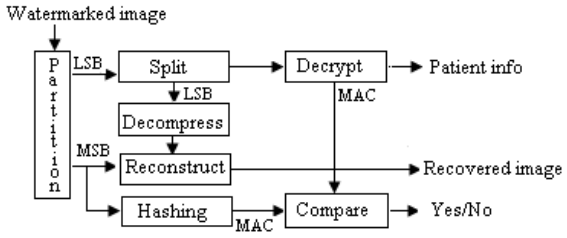


Fig.2 Extraction and verification phase

V. Results and Conclusion

In experiments, we tested three ultrasounds images that had been saved in BMP format via the Microsoft Paintshop Program. We used a PIV machine with 256 Mo memory and the Windows XP operating system. The images had been acquired from the obstetrical ultrasound site of Dr.J. Woo.

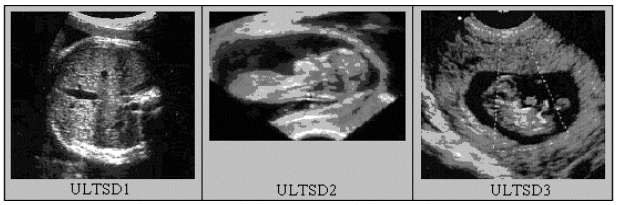


Fig.3 grayscale images used for testing

About 32 ASCII characters of patient information and a 128 bits MAC are embedded into each image. The patient information has the following format:

Fist name	Family name	Age	Sex
14	14	3	1

Table.1 shows the PSNR (Peak Signal to Noise Ratio) between the original and the watermarked image expressed in dB and indicating the energy of inserted watermark. The PSNR depends on the mean squared error (MSE) which is calculated according to Eq. (1) where *p* and q are the original and watermarked images, and *M* and *N* are image dimensions.

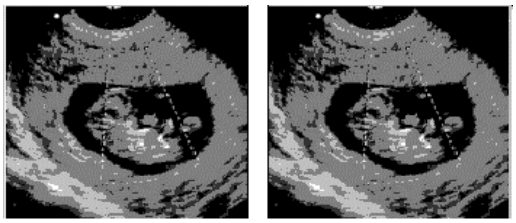
$$MSE = \frac{1}{N}\sum_{i=0}^{i=N-1}\sum_{j=0}^{j=M-1}(p(i,j) - q(i,j))^2 \quad (1)$$

$$PSNR = 10\log_{10}(\frac{255^2}{MSE}) \quad (2)$$

TABLE.1 WATERMARK EMBEDDING EFFECT

Test image	Dimensions	PSNR (dB)
ULTSD1	256x256	39.72
ULTSD2	400x268	52.27
ULTSD3	512x512	41.33

As expected, experiments confirmed that all the images hide the patient information so that it was unnoticeable, and successfully decoded. (Fig. 4)



(a) (b)

Fig.4 Original (a) and watermarked (b) images

The experimental results provide an indication of the potential of the approach and there are several advantages that make it suitable for practical use:

- no additional file is sent, so storage and transmission overheads are reduced.
- the patient information is hidden for innocuous eyes, and stays with the related image.
- the image can be unambiguously authenticated.
- the image can be recovered in its integrality for a reliable diagnosis.
- the embedding process doesn't increase the image file size.

Our future work will proceed in two directions. First, we shall focus on the issue of how to highlight the area of the image that has been maliciously tampered with, by using more sophisticated embedding algorithm. Secondly, we will extend the secret key based watermarking approach to public-key detection since it is generally believed that secret key detection will encumber the automation and portability of authentication systems.

REFERENCES

[1] P. Campisi, D. Kundur, D. Hatzinakos and A.Neri, "Compressive Data Hiding: An Unconventional Approach for Improved Colour Image Coding,"EURASIP Journal on Applied Signal Processing, special issue on Emerging Applications of Multimedia Data Hiding, vol. no. 2, pp. 152-163, February 2002.

[2] 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, p. 250-255, Nov. 2000.

[3] J. Fridrich et al, Lossless Data Embedding for All Image Formats, Proc. SPIE Photonics West, Security and Watermarking of Multimedia Contents, pp. 572–583, 2002.

[4] J. Fridrich, M. Goljan and R. Du, Invertible Authentication, Proc. SPIE Photonics West, vol. 3971, Security and Watermarking of Multimedia Contents III, pp. 197-208, 2001.

[5] J. Fridrich, M. Goljan, and R. Du. "Invertible Authentication Watermark for JPEG Images." ITCC 2001, Las Vegas, Nevada, April 2–4, 2001.

[6] F. Hartung and M. Kutter, "Multimedia watermarking techniques," Proceedings of the IEEE, vol. 87, no. 7,pp. 1079–1107, July 1999.

[7] C.-S. Lu, H.-Y.M. Liao and C.-J. Sze, "Combined Watermarking for Image Authentication and Protection," Proc. IEEE Int. Conf. on Multimedia and Expo, vol.3, pp. 1415–1418, August 2000.

[8] A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1997.

[9] Juan RHMA, Perez-Gonzalez F: DCT-Domain Watermarking Techniques for Still images: Detector Performance Analysis and a New Structure. IEEE Transactions on Image Processing 2000, 9:55-68.

[10] http:// www.ob-ultrasound.net/joewoo