Data Hiding Scheme for Medical Images

Rodríguez-Colín Raúl, Feregrino-Uribe Claudia, Trinidad-Blas Gershom de J.
National Institute for Astrophysics, Optics and Electronics
Luis Enrique Erro No. 1, Sta. Maria Tonantzintla, Puebla, Mexico C.P. 72840
{raulrc, cferegrino, gtrinidad}@inaoep.mx

Abstract

Digital image watermarking has been proposed as a method to enhance medical data security, confidentiality and integrity. Medical image watermarking requires extreme care when embedding additional data within the medical images because the additional information must not affect the image quality. Many of the exploration systems used for medical diagnosis are based on the medical study images. CR, MR and CT, obtain images that can be stored in digital formats such as (DICOM files) which are related with data of patients and information about the study. In this paper we present a watermarking scheme that combines data compression, encryption and watermarking techniques and image moment theory applied to radiological medical images. In this work we use DICOM data as a watermark to embed in medical images. Image quality is measured with metrics which are used in image processing such as PSNR and MSE. Our results show good accuracy in the watermark extraction process.

1. Introduction

In recent years image watermarking has become an important research area in data security, confidentiality and image integrity. Medical image watermarking requires extreme care when embedding additional data within the medical images because the additional information must not affect the image quality.

Medical images are stored for different purposes such as diagnosis, long time storage and research.

In the medical field the importance of the medical data security has been emphasized, especially with respect to the information referring to the patients (personal data, studies and diagnosis) [1]. On the one hand the amount of digital medical images transmitted over the internet has increased rapidly, on the other hand the necessity of fast and secure diagnosis is important in the medical field, i.e. telemedicine, making watermarking the answer to more secure image transmissions. For applications that work with images, the watermarking aim is to embed a visible or invisibly message in an image [3].

Many of the exploration systems used for medical diagnosis are based on the study images. The conventional radiology, MR and CT, obtain images that can be stored in digital formats which are related with patient data and information about the study, e.g.: study type, patient name and date, among others. One of the digital formats is DICOM (Digital Imaging and Communications in Medicine) that was created by the National Electrical Manufacturers Association (NEMA) to aid the distribution and viewing of medical images and other data [12].

A single DICOM file contains a header (which stores information about the patient's name, the type of scan, image dimension, etc.) and all the images from studies. In this work, we propose the use of DICOM metadata as a watermark to embed in medical images extracted from the DICOM file.

This paper is organized as follows: section 2 outlines the background of watermarking schemes applied in medical images, in section 3 a brief description of image moments theory to obtain invariant image features is presented, the proposed digital watermarking scheme is presented in section 4; experimental results are shown in section 5; and finally, conclusions and future work are presented in section 6.

2. Background

Medical Imaginology is a field where the protection of integrity and confidentiality of the medical information is derived from strict ethics and legislatives rules. The medical information record of a patient is a complex expedient integrated of clinical examinations, diagnosis, prescriptions and images in several modalities. This information is used for different purposes such as: clinical research and epidemiological studies. All the medical records, electronic or not, are linked to the medical secrecy, for that reason, the records must be confidential.

17th International Conference on Electronics, Communications and Computers (CONIELECOMP'07)
0-7695-2799-X/07 $20.00 © 2007 IEEE

This imposes three characteristics for the medical information records (Figure 1).

Confidentiality: means that only authorized users have access to the information.

Reliability: This characteristic has two aspects:

- ***Integrity***: The information has not been modified by unauthorized users.
- ***Authentication***: Is a proof that the information belongs to the correct patient.

Availability: Is the ability of information systems to be used by authorized users.

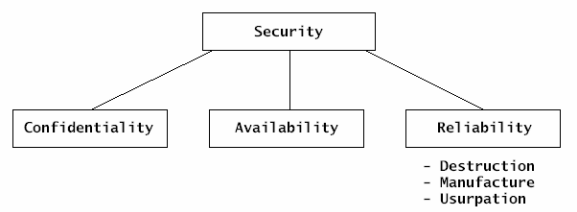


Figure 1 Security components in medical information

Recently there has been too much interest in watermarking techniques to protect intellectual property in digital formats e.g. images, audio, video, software. As a consequence of this interest several watermarking techniques have been developed.

Although steganography and watermarking both describe techniques for covert communications, steganography relates only to hide point to point communication between two parties [11].

A watermarking system, however, would embed an amount of information that could not be removed or altered without making the cover object entirely unusable. Some steganographic methods are not robust against attacks or modifications of data that might occur during transmission, storage or format conversions [2]. Watermarking, as opposed to steganography, has additional requirements against possible attacks:

- **Robustness**: Robustness means that the watermarking scheme should be able to preserve the watermark under some attacks. The attack could be anything like rotation, translation, scaling, additive noise, filtering, compression, etc. [3].
- **Imperceptibility (Quality)**: Watermarking should be done in such a way that it does not affect the quality of the host image or the hidden data after watermarking. The degradation in the image should not be noticeable to the human eye [3].
- **Capacity**: It is important to determine the amount of information that can be embedded in an image, this amount of information depends on the application (copyright protection, fingerprinting, medical safety, etc.) [3], as the information to embed may be a logo, a number, hash code, etc.

The number of studies in the literature dedicated to watermarking of medical images is not very extensive. Anand *et al*. [4], proposed to insert an encrypted version of the electronic patient record (EPR) in the LSB (Least Significant Bit) of the gray scale levels of a medical image. Although the degradation in the image quality is minimum, the limitations and fragility of LSB watermarking schemes is well-known. Miaou *et al*. [5] proposed a method to authenticate the origin of the transmission, the message embedded is an ECG, the diagnosis report and physician's information. Macq and Dewey [6] insert information in the headers of medical images.

These approaches are not robust against attacks such as filtering, compression, additive noise, etc. neither to geometrical attacks such as rotation or scaling transformations. To solve this problem, we use the image moment theory to normalize the image in order to obtain a watermarking scheme robust against active attacks (image manipulations).

3. Image Moments

The image moments are one of the techniques commonly used in feature extraction, where each order moment has different information for the same image [7]. For the digital images, the zeroth order is defined as:

$$m_{00} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \quad (1)$$

Where f is a data image matrix of size M x N. This formula is also known as the mass of matrix f. Similarly, first order image moment can be defined as:

$$m_{10} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} x \cdot f(x,y) \quad (2)$$

$$m_{01} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} y \cdot f(x,y) \quad (3)$$

The two first order moments, m_{10} and m_{01} [8], are used to locate the center of mass of the matrix *f*. The centroid of the image can be found as:

$$x_o = \frac{m_{10}}{m_{00}}; \qquad y_o = \frac{m_{01}}{m_{00}} \quad (4)$$

The centroid is invariant against geometrical attacks such as: rotation, scaling or translation and is used in both embedding and extraction processes.

4. Proposed Scheme

In this paper, we propose a blind watermarking scheme, i.e. in the extraction process it is not necessary the host image to recover the watermark, it is only necessary the secret key used in the cryptographic step (Figure 4).

This scheme is divided in two stages, in the first stage, the watermark is constructed (section 4.1); after that, the image is centered using x_0 and y_0 computed via (4); then the positions where the data will be embedded are obtained using the proposed scheme (section 4.2), this stage is shown in Figure 2.

The second stage (extraction step, section 4.4) is similar to the embedding process (section 4.3) using the watermarked image, the position of each modified pixel is calculated in the procedure *OBTAIN_PIXELS* (*IMG*, *cx*, *cy*) and the data are recovered, this stage is shown in Figure 3.

```
INPUT (IMG, DATA)
    // watermark generation.
    INFO = WATERMARK (DATA)
    // calculate the centroid of the host image.
    (cx, cy) = CENTROID (IMG)
    // center the image in basis of cx and cy.
    IMG_C = CENTER_IMAGE (IMG, cx, cy)
    // select the pixels in which the message will be
   // embedded.
    [P] = OBTAIN_PIXELS (IMG_C, cx, cy)
    // embed the message to obtain the stego image.
    WM_IMG = EMBED_DATA (P, INFO)
```

Figure 2 Embedding process

The procedure *OBTAIN_PIXELS* (*IMG*, *cx*, *cy*) calculates the pixels using an spiral scan starting in the centroid of the image, and uses the homogeneity of a block to determine if a pixel is "*good*" to embed information. The complete process is explained in following subsections, the algorithm selects *TP* pixels in the host image, where *TP* is the size of the data to embed.

```
INPUT (WM_IMG)
    // calculate the centroid of the watermarked image.
    (cx, cy) = CENTROID (WM_IMG)
    // select the pixels in which the information will be
   // extracted.
    [P] = OBTAIN_PIXELS (WM_IMG, cx, cy)
    // extract the message from the stego image.
    INFO = EXTRACT_DATA (P)
    // reconstruct the message.
    DATA = RECONSTRUCT_DATA (INFO)
```

Figure 3 Extraction process

The procedure *EXTRACT_DATA* (*P*) uses the gray-scale value of each pixel calculated in the watermarked image to obtain the information embedded; this procedure is explained in the extraction process (section 4.4). Finally, the procedure *RECONSTRUCT_DATA* (*INFO*) decrypts and decompresses the data extracted in order to obtain the original message. The following subsections describe some of these procedures in detail.

4.1. Watermark generation

To generate the watermark, we follow the next procedure:

- Extract the image and the DICOM data from a DICOM file.
- Compress the DICOM data; in our scheme we apply Huffman compression in order to reduce the amount of data to embed.
- Encrypt the compressed data to enhance the security of the DICOM data; in our scheme we use a RC4 method [14].
- Generate an image from the encrypted data that works as a watermark.

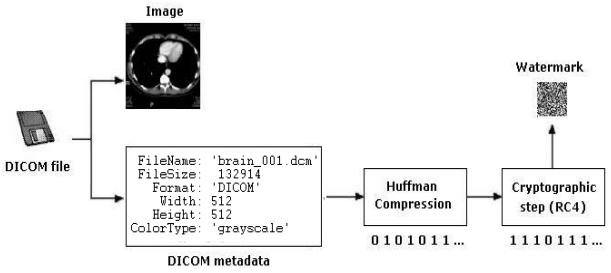


Figure 4 Watermark generation

4.2. Selection of the pixels for embedding the data

To select the pixels to be changed (embedding the message), we need to find regions with low homogeneity. To obtain these regions, we apply the next procedure:

- Scan the image in a spiral way using the centroid as the origin of this scan. This procedure selects the possible pixels where the data could be embedded (Figure 5).
- For each possible pixel, calculate the homogeneity using the variance (σ^2) of a block of (k x k) pixels, where k is the size of the window.

$$\sigma^2 = \frac{1}{k^2}\sum_{x=0}^{k-1}\sum_{y=0}^{k-1}\left(f(x,y)-\mu\right)^2 \quad (5)$$

where

$$\mu = \frac{1}{k^2}\sum_{x=0}^{k-1}\sum_{y=0}^{k-1} f(x,y) \quad (6)$$

- If $\sigma^2 \geq Th$ then the pixel is selected to embed data in this position according with formulas (5) and (6). Where Th is a threshold for the homogeneity and, both Th and k are given by the user (Figure 7).

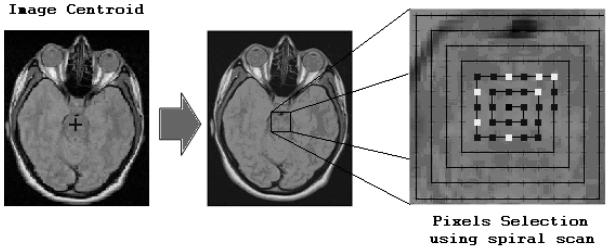
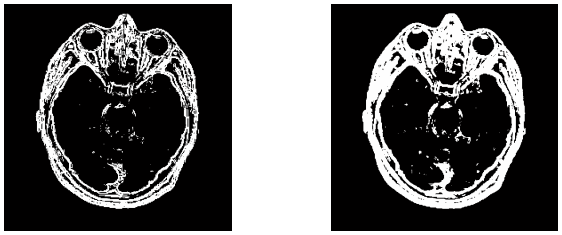


Figure 5 Process to select the pixels



A) **B)**

Figure 6 Examples of pixels selected for embedding data after a spiral scan with different window size. A) *k*=3 and B) *k*=5

4.3. Embedding process

The embedding process is similar that Wang *et al*. [9] it differs in the use of the method that is only for the selected pixels in section 4.2 and is described in the following procedure.

- Obtain a block of size (k x k) with center in the position of the selected pixel (Figure 7).
- If the bit to embed is "1" change the luminance value of the central pixel, to make sure that:

$$L_{real} \geq L_{mean} + \delta_1 \quad (7)$$

- If the bit to embed is "0" change the luminance value of the pixel, to make sure that:

$$L_{real} < L_{mean} - \delta_2 \quad (8)$$

Where δ_1 and δ_2 are calculated based on the homogeneity and luminance of the block (k x k), L_{real} is the gray-scale level of the pixel and L_{mean} is the gray-scale level mean of the block.

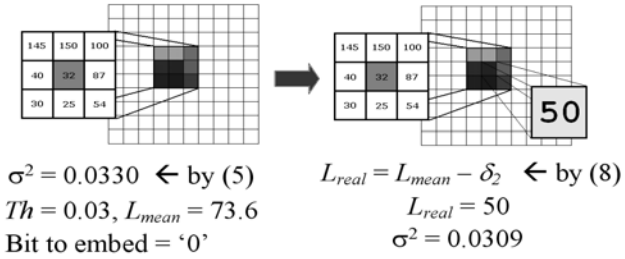


Figure 7 Example of pixel modification using formulas (5), (6), (7) and (8)

4.4. Extraction process

The extraction process is the following:

- Locate the changed pixels using the spiral scan starting in the centroid of the image.
- The decision threshold to extract the watermark is:
  - If $L_{real} \geq L_{mean}$ then the extracted bit is "1".
  - If $L_{real} < L_{mean}$ then the extracted bit is "0".

The values of δ_1 and δ_2 are not required to extract the watermark.

5. Experimental Results

In this section, we present the results obtained with our scheme. The experiments were carried out in three DICOM files. All the images are 512x512 gray scale medical images, as shown in Figure 8. In our experiments the homogeneity is calculated using a window of k x k pixels, with $k = 3$.

In order to determine the degradation in the stego-image with respect to the host image, in this stage we apply the PSNR metric (Peak Signal-to-Noise Ratio) and MSE (Mean Square Error) to measure the distortion produced after the embedding process [10], and NCC (Normalized Cross-Correlation) to evaluate the similarity between the original watermark and the extracted watermark.

Mean Square Error:

$$MSE = \frac{1}{M\,N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left(f(x,y) - f'(x,y)\right)^2 \quad (9)$$

Where M, N is the size of the image and contains M x N pixels, $f(x, y)$ is the host image and $f'(x, y)$ is the watermarked image.

This measure gives an indication of how much degradation was introduced in the stego-image, values near to zero indicate less degradation.

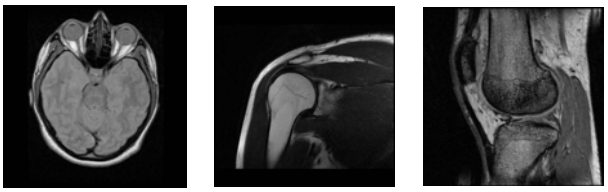
Peak Signal-to-Noise Ratio:

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

PSNR penalizes the visibility of noise in an image [13]. Values over 36 dB in PSNR are acceptable in terms of degradation, which means no significant degradation is observed by the human eye.

$$NCC = \frac{\sum_{x=0}^{R-1}\sum_{y=0}^{C-1} W(x,y)\cdot W'(x,y)}{\sum_{x=0}^{R-1}\sum_{y=0}^{C-1}\left|W(x,y)\right|^2} \quad (11)$$

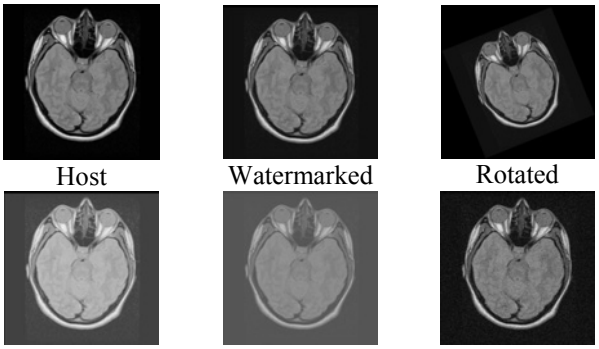
Where W is the original watermark and W' is the extracted watermark both with size R x C.



Brain Shoulder Knee

Figure 8 Medical images used in the experiments

After the watermark embedding process, we apply several attacks such as: additive noise, rotation, scaling and different contrast to comply the watermarking requirements. Figure 9 shows the attacks performed in the watermarked image.



Host Watermarked Rotated

Brighten Contrasted Gaussian noise

Figure 9 Different attacks in the watermarked image

Table 1. Imperceptibility in each image using PSNR (dB) and MSE metrics.

Image	PSNR	MSE
Brain	41.1	5.3
Knee	43.6	2.5
Shoulder	38.9	8.2

Table 2. Percentage of recovered data after brighten and a contrast modification.

Image	Brightened	Contrasted
Brain	94.5 %	94.8 %
Knee	92.2 %	92.0 %
Shoulder	95.0 %	95.5 %

Table 3. Percentage of recovered data after JPEG compression with quality factor Q=80 and rotation of 35 degrees.

Image	JPEG Compression	Rotation 35 degrees
Brain	94.5 %	90.2 %
Knee	96.5 %	88.4 %
Shoulder	91.5 %	91.7 %

The results obtained show that centering the image using the centroid gives us the advantage over geometrical attacks (rotation, scaling and translations), i.e. we can correct the geometrical distortions in order to recover the embedded watermark, and the use of homogeneity allow us to determine areas in the image which are better to embed data than other areas in order to obtain less degradation.

The results obtained show better accuracy in the extraction process. Although we can recover the most part of the message; some parts of the recovered message are illegible because we lost some bits in the extraction process; these bits can affect the result if for example we embed numerical data.

6. Conclusions and future work

In this paper, we have presented a new approach of blind watermarking scheme used in medical images that is robust some attacks like brighten or contrast modification. The use of image moments allows us to obtain good results in the extraction process after geometrical attacks such as translation and scaling. The obtained results show that the use of homogeneity allows getting better accuracy in the extraction process than the use of simple LSB method, because this approach selects the regions near to the borders. As future work; we will extend the algorithm in order to obtain less degradation in the watermarked image and obtain better accuracy in the recovered watermark.

References

[1] G. Coatrieux et al. “Relevance of watermarking in medical imaging”. In IEEE-embs Information Technology Applications in Biomedicine, Arlington, USA, 2000, pp. 250-255.

[2] S. Katzenbeisser, F. A. P. Petitcolas. “Information hiding techniques for steganography and digital watermarking”, Artech House Publishers, 2000.

[3] W. Puech, J. M. Rodrigues. “A new crypto-watermarking method for medical images safe transfer”. In Proceedings of the 12th European Signal Processing Conference, Vienna, Austria, 2004, pp. 1481-1484.

[4] D. Anand and U. C. Niranjan. “Watermarking Medical Images with Patient Information”. In Proceedings IEEE/EMBS Conference, Hong Kong, China, October 1998, pp. 703-706.

[5] S. G. Miaou et al. “A Secure Data Hiding Technique with Heterogeneous Data-Combining Capability for Electronic Patient Record”. In Proceedings of the World Congress on Medical Physics and Biomedical Engineering, Session Electronic Healthcare Records, USA, July 2000.

[6] Macq B. and Dewey F.: Trusted Headers for Medical Images. In DFG VIII-DII Watermarking Workshop, Erlangen, Germany, October (1999).

[7] L. Tung-Lam, N. Thi-Hoang-Lan. “Digital Image Watermarking with Geometric Distortion Corrections Using the Moment Image Theory”, International Conference on Research, Innovation & Vision for the Future (RIVF), February 2004.

[8] P. Dong et al. “Digital Watermarking Robust to Geometric Distortions”. In IEEE Transactions on Image Processing, Vol. 4, No. 12, December 2005.

[9] Y. Wang, A. Pearmain. “Blind image data hiding based on self reference”. In Pattern Recognition Letters, Vol. 2 No. 15 November 2004, pp. 1681-1689.

[10] B. Plaintz, A. Maeder. “Medical Image Watermarking: A Study on Image Degradation”. In Proceedings of the Australian Pattern Recognition Society (APRS) Workshop on Digital Image Computing (WDIC), Brisbane Australia, February 2005.

[11] N. F. Johnson, S. Jajodia Z. Duric. “Information hiding: Steganography and watermarking attacks and countermeasures”, Kluwer academic Publishers 2000.

[12] Digital Imaging and Communications in Medicine [http://www.medical.nema.org]

[13] S. Voloshynovskiy, S. Pereira, V. Iquise, and T. Pun. “Attack modelling: Towards a second generation watermarking benchmark”. Signal Processing, Special Issue on Information Theoretic Issues in Digital Watermarking, 81(6), June 2001.

[14] L. Knudsen et al. “Analysis Methods for (Alleged) RC4”. Advances in Cryptology-ASIACRYPT Proceedings, Vol. 1514 of LNCS Springer Verlag, 1998, pp. 327-341.

0-7695-2799-X/07 $20.00 © 2007 IEEE