Volume 5, Issue 12, December 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Adaptation of Different Techniques on Digital Image Watermarking in Medical Domain: A Review

I. Assini, A. Badri, K. Safi
EEA & TI Laboratory Faculty of Science and Technology – Hassan II University of Casablanca,
B.P. 20650, Mohammedia, Morocco

Abstract— In the last couple of decade, multimedia documents become a central element into the different field of applications thanks to the development of the technologies related the computing science. This phenomenal development has not taken place without leading some concerns about illicit manipulations because anyone could easily copy, modify and distribute digital images without damaging them in any way. In this respect, digital watermarking can be seen as an alternative which could be efficient and complementary by affording additional security, ensuring an authorized access, facilitating content authentication or preventing unlawful reproduction. The aim of this paper is to present a literature survey of digital watermarking within an image. It describes the early work carried out on digital watermarks, including the brief analysis of various watermarking schemes and its potential applications.

Keywords— Image processing, security, digital watermarking, content authentication, Medical application.

I. INTRODUCTION

Digital watermarking is a process of embedding information into image or other digital documents (texts, video and audios), for various purposes such as the fight against fraud, hacking and the protection of copyright.
The general diagram of digital image watermarking system (***Figure 1***) can be described mainly by two basic phases: the insertion and extraction, however a third step can be considered: the transmission.

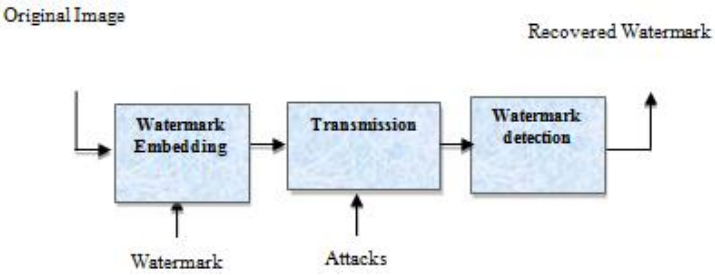

Fig 1: General diagram of insertion, transmission and extraction of digital image watermarking.

Requirements of watermarking process:
Capacity: represent the quantity of information that we want to insert into an image, this quantity varies depending on the application. On the other hand, it is necessary to hide several bits of information to enable authentication of images.
Robustness: The algorithms of digital watermarking of images can be classified according to their robustness. We can distinguish in this classification two categories of watermarking: robust and fragile. In robust watermark the system of watermarking should be robust against several attacks. However in fragile watermark the system of watermarking must be highly sensitive to any modifications or manipulations. Is generally used to verify the authenticity and integrity of the images.
Imperceptible: the digital watermark should not affect the quality of the original image after it is watermarked.

1. Insertion phase of watermarking

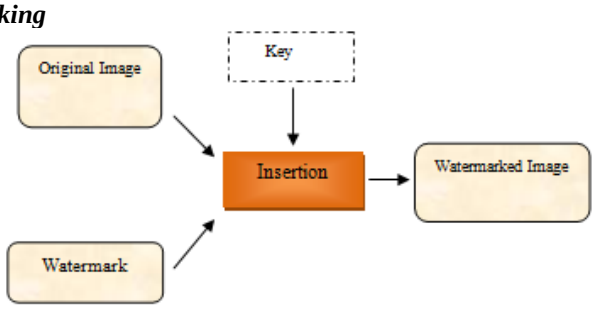

Fig 2: Diagram of insertion

This phase allows inserting the watermark into the original image for having a new image named image watermarked.
A third optional parameter can be added: the secret key which allows ensuring a certain level of security to the process of watermarking.

2. Detection phase of watermarking

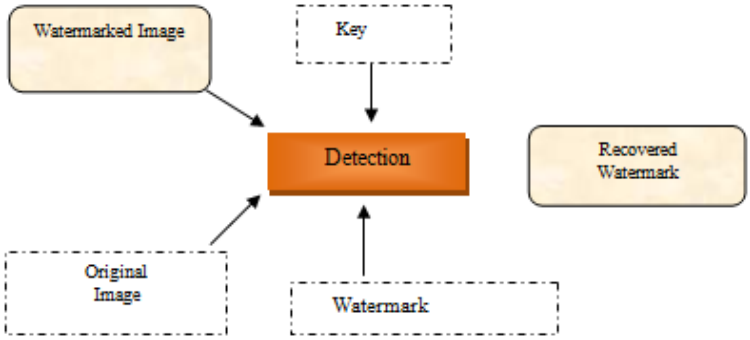

Fig 3: Diagram of detection

The detection of the watermark and the extraction of the embedded message have for role to certify if the watermark is or is not present in the image. According to the different algorithms, the original image and the secret key may or may not be necessary during the detection.

II. APPLICATION OF DIGITAL WATERMARKING

There are various applications of watermarking, we present here the main ones [1]:

A. Copyright Protection

When a new work is produced, copyright information can be inserted as a watermark. In case of dispute of ownership, this watermark can provide evidence.

B. Authentication and Integrity Verification

Content authentication is able to detect any change in digital content. This can be achieved through the use of fragile or semi fragile watermark which has low robustness to modification in an image.

C. Fingerprinting

Fingerprints are unique to the owner of digital content and used to tell when an illegal copy appeared.

D. Medical application

Name of the patients can be printed on the X-ray reports and MRI scans using techniques of watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster [2].

III. WATERMARKING TECHNIQUES

Watermarking techniques can be classified into two domains: Spatial domain watermarking and Frequency domain watermarking.

A. Spatial domain watermarking

In spatial domain technique the watermark embedding is achieved by directly modifying the pixel values of the host image. The most commonly used method in the spatial domain technique is the least significant bit (LSB).

- ***Least Significant Bit Coding (LSB)***

LSB [3] coding is one of the earliest methods of image watermarking. In this method the insertion of data is only done in the low-order bits of the image. For an image coded on 8 bits, the modification of the LSB causes a variation of the gray level of 1/256. This change in practice is invisible. If this method gets good results for what is the invisibility, it is not satisfactory for the robustness.

- ***Patchwork Technique***

Bender et al. [4] proposed watermarking scheme based on statistical method called patchwork.
In this technique, n pairs of image points (a, b) are randomly chosen. The image data in ‘a’ is lightened while that in ‘b’ is darkened in the same scale. Experimental results show that this algorithm is simple and easy, showing reasonably high resistance to most modifications. However there are some limitations such as extremely low embedded data rate and hence this technique is useful to low bit-rate applications only.

- ***Wong Technique***

The algorithm of Wong [5] allows watermarking the image in the spatial domain, it inserts two types of distinct data at the level of the LSB: the first is a binary logo, to identify the owner of the image, and the other a summary of the image derived from a hash function MD5 [6].

It is to divide the image and the logo by blocks of i * j pixels and calculate the summary of each block of the image. And then, the first bit of summary obtained are then added by an exclusive or to the block of the logo which will be then insert at the level of the LSB of the block of the image to watermark.

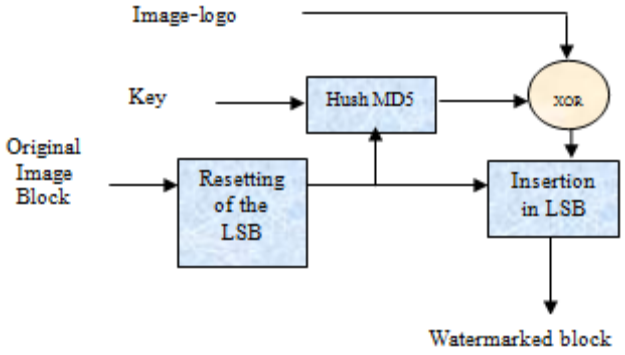

Fig 4: Wong technique

- ***Look Up Table (LUT) Technique***

Yeung [7] inserts the watermark by using a LUT for each pixel in the image, the LUT allows to obtain the corresponding binary value. If it is identical to the value of the bit to be inserted, the pixel of the image is not changed but if the value is different, the pixel is adjusted until the right value.

B. Frequency Domain Watermarking

This technique is also known as Transform domain. In this technique values of certain frequencies are changed from their original values. There are various methods which are used in transform technique such as DWT, DCT, DFT and SVD.

- ***Discrete Wavelet Technique (DWT)***

Discrete Wavelet transform (DWT) [1] is a mathematical tool for decomposing the image. The transform is based on small waves called wavelet of varying frequency. The wavelets transform decompose the image into three directions horizontal, vertical and diagonal. *Figure 5* shows the decomposition of image

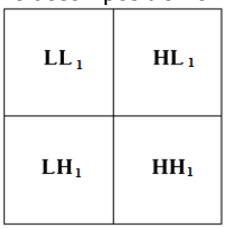

Fig5: Single Level Decomposition

Hence the magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and smaller for other bands (HH, LH and HL). DWT is preferred because it provide both a simultaneous spatial and frequency spread of watermark within the host image.

For embedding a watermark, we modify the DWT coefficients in the LL band:

$$LLw,i,\ j = LLi,j + \alpha kW\ i,j\ \ ,\ i,j = 1,.....,n$$

- ***Discrete Cosine Transform (DCT)***

Discrete Cosine Transform (DCT) [8] represents data in the form of frequency rather than an amplitude space. DCT watermarking techniques are robust compared to spatial domain techniques. The watermark is embedded into the coefficients of the middle frequency, so the visibility of image will not get affected and the watermark will not be removed by any kind of attack. Steps in DCT Block Based Watermarking Algorithm [9]:

1) Segment the image into non-overlapping blocks of 8x8,
2) Apply forward DCT to each of these blocks,

$$DCT\ (m,n) = \frac{1}{\sqrt{2N}} c(m).c(n) \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} x(k,l) \cos\left(\frac{(2k+1)m\pi}{2N}\right) \cos\left(\frac{(2l+1)n\pi}{2N}\right)$$

$$c(m) = \frac{1}{\sqrt{2}} \quad if\ i = 0\ \ and\ \ 1\ if\ i > 0$$

3) Apply some block selection criteria (HVS),
4) Apply coefficient selection criteria (highest),
5) Embed watermark by modifying the selected coefficients,
6) Apply inverse DCT transform on each block.

- ***Discrete Fourier Transform (DFT)***

The Fourier transform of an image allows going from a spatial representation to the frequency domain.
It is given by:

$$F(u,v) = \sum_{m-\infty}^{\infty} \sum_{n-\infty}^{\infty} f(m,n) e^{-jum} e^{-jvn}$$

F (u, v) is the Fourier transform of the matrix f (m, n), u and v represent the spatial frequencies of the image according to the directions Ox and Oy respectively.

In DFT [10], the insertion is performed in the mid-level frequency. The low frequency is not changed to avoid visual degradation too important, also the watermark is not inserted in the high frequency because then it would be sufficient to perform a low-pass filtering to remove it.

- ***Singular Value Decomposition (SVD)***

Singular Value Decomposition (SVD) [11] is a numeric analysis of linear algebra which is used to decompose a matrix to insert the bits of the watermark.

In fact, the decomposition in singular values based on the fact that there is a square matrix U per unit of size m and a matrix V per unit of size n such that:

$$\mathbf{U' \times I \times V = S}$$

S is a matrix whose first r diagonal terms are positive, all the other being void.

We note σi the singular values of I:

$$S = \begin{pmatrix} \sigma_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \sigma_n \end{pmatrix}$$

We used the matrix S of the singular values of the image to insert the bits of the watermark.

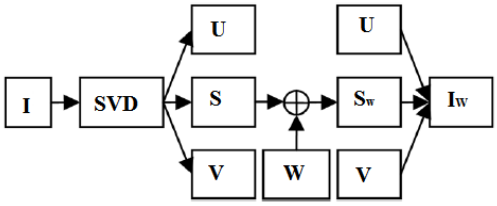

Fig 6: Diagram of watermarking with SVD

- I represent the original image
- W represent the watermark
- Iw represent the watermarked image

IV. APPLICATION ON MEDICAL IMAGING

Medical imaging is an important tool in management decisions and diagnostic. In this respect, several techniques and imaging modalities (IRM, Echographic, mammography, ultrasound, etc.). Currently, the transmission of medical information through public networks expands considerably, either in telemedicine, telediagnosis, telesurgery, distance learning, or even different applications related to consultation of databases. In effect, the images will undergo different attacks like transmission errors and the compressions loss. Hence the appearance of the watermarking in order to contribute to the security of medical images shared on the network. Digital watermarking images reinforce the reliability of medical images by the integrity control and confidentiality.

1. Integrity control

The control of the integrity and authentication of medical images is becoming ever more important within the Medical Information Systems (MIS). Is to verify that the image has not been degraded. Otherwise, the algorithm must be able to locate the degradations.

- ***Kundur Technique***

Kundur [12] proposed to use the transformed into wavelet transform (DWT) because it allows both to be a localization of damage and a spectral averaging of the watermark. The data (logo) are inserted by quantifying certain coefficients of images details of the first three levels. The choice of these coefficients is determined by a key. The quantification of these coefficients following the data to insert is carried out by cutting the space of the real with a step of quantizationΔ. Has each interval is associated alternately the binary value 0 or 1 (***Figure 7***).

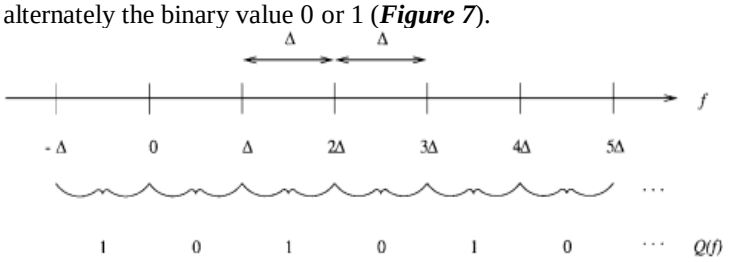

Fig7: Quantization in the method of Kundur

2. Confidentiality

The information required for to use medical images are presented in the header of the image such as the name of the patient, age, coordinates but also information about the doctor can be read by anyone with access to the image. This ease of reading poses a problem of confidentiality in the medical field.

The watermarking would then remove confidential information from the header to the insert directly in the image itself. This information would be more then directly accessible but obtaining them would require the use of the extraction software. It would be of even possible, thanks to the use of keys, to improve the control of access to such information.

- ***Xie Technique***

Xie [13] inserts the mark in the image approximation of a decomposition multi levels. The level of decomposition depends on the size of the information that we want to insert, the invisibility and robustness sought.

The insertion is performed by making evolve throughout the image approximation, without overlap, a window size of 3x1. For each position of the window, the three coefficients are stored in ascending order of their value.

\

V. CONCLUSION

In this paper reviews some of the watermarking techniques. It firstly provides a general description of the desirable characteristics of digital watermarking system. Consecutively, various watermarking techniques are discussed in brief with the potential applications of the watermarking methodology. Finally, we give some example of watermarking techniques applied in medical imaging.

This paper shows the different techniques and discusses the important of watermarking based on decomposition in wavelet domain which can be used in future work.

REFERENCES

[1] Vaishali S. Jabade, Dr. Sachin R. Gengaje "Literature Review of Wavelet Based Digital Image Watermarking Techniques", International Journal of Computer Applications (0975 – 8887) Volume 31– No.1, October 2011.

[2] G. Coatrieux, L. Lecornu, Member, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member IEEE, "a review of digital image watermarking health care"

[3] Mitchell D. Swanson, Mei Kobayashi, Ahmed H. Tewfik, Multimedia data-embedding and watermarking technologies in Proceedings of the IEEE, vol. 86(6), p. 1064-1087, June 1998.

[4] W. Bender, D. Gruhl, N. Morimoto, Techniques for Data Hiding in Proceedings of the SPIE Conference on Storage and Retrieval for Image and Video Databases III, San Jose, CA, vol. 2420, p. 164-173, February 1995.

[5] Wong,] P. W., A Public Key Watermark for Image Verification and Authentication Proceedings of the Int. Conf. Im. Proc, vol. I, p. 155-459, 1998.

[6] Mehmet U. Celik, Gaurav Sharma, A Hierarchical Image Authentication Watermark With Improved Localization And Security in Proceedings of the IEEE International Conference on Image Processing, vol. II, p. 502-505, Oct 2001.

[7] M. Yeung, F. Mintzer, An Invisible Watermarking Technique for Image Verification in Proceedings of the IEEE ICIP, Santa Barbara, Oct 1997.

[8] Prabhishek Singh, R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013.

[9] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, ―A Survey of Digital Image Watermarking Techniques‖, 2005 3rd IEEE International conference on Industrial Informatics (INDIN).

[10] Pereira, J. J. K., O Ruanaidh, F. Deguillaume, G. Csurka, T. Pun, Template based recovery of Fourier-based watermarks using Log-polar and Loglog maps in Proceedings of the IEEE Int. Conf. on Multimedia Computing and Systems, Special Session on Multimedia Data Security and Watermarking, Florence, Italy, June 1999.

[11] Henri Bruno Raza_ndradina, Paul Auguste Randriamitantsoa, Tatouage robuste et aveugle dans le domaine des valeurs singulières, JMAITS, 2008, pp.1-15.

[12] D. Kundur, D. Hatzinakos, Digital watermarking for telltale tamper proofing and authentication in Proceedings of the IEEE, vol. 87 (7), p. 1167-1180, July 1999.

[13] Xie, G. Arce L., A joint wavelet compression and authentication watermarking in Proceedings of the IEEE International Conference on Image Processing, Chicago, IL, Oct 1998.

