Multiple Watermark for Authentication and Tamper Detection using Mixed scales DWT

M.El Hajji
IRF-SIC Laboratory
University Ibn Zohr
Agadir
MOROCCO

H. Ouaha
Laboratory Computing Systems & Vision LabSiv
Agadir
MOROCCO

K. Afdel
Laboratory Computing Systems & Vision LabSiv
Agadir
MOROCCO

H.Douzi
IRF-SIC Laboratory
University Ibn Zohr Agadir
Agadir
MOROCCO

ABSTRACT
Authentication of multimedia contents is introduced as a tool to improve the security against unauthorized manipulation and misappropriation. The risks increased when dealing with an open environment like the Internet. This paper proposes a multiple watermarking techniques using dominant blocks of wavelet coefficients in mixed scales and moment invariant methods as a complementary safety measure. The logic of use the blocks dominants map is that local features such as contours or edges are unique to each image. In addition, these dominants blocks have proven to be useful in detecting possible alteration in the temperate region of the image-based data.

Keywords
Watermarking, Authentication, Content-Based, Wavelet.

1. INTRODUCTION
Digital watermarking is a technology for embedding digital information in digital content (audio, images, video…) [1] [2] [3]. It has introduced as a tool to improve the security. Watermarking techniques are divided in two 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).

Integrity and confidentiality are critical issues in some imagery application such as medical imagery. Different watermarking schemes have been proposed to address the problems of medical privacy and security [4] [5]. 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.

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 [6] [7]. 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.

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 data under digital formats. However, the use of these technologies is not always safe as the medical records are freely circulated in open networks and thus subjected to alterations and misuses.

In this paper we propose to combine moment invariant and dominant blocks of mixed scales-wavelet coefficient, this will allow adding a supplementary security level, which is suitable for transmission in open network as Internet and location of the tempered area accurately.

The scheme use the parameterize integer wavelet transform which is the fast approach of Discrete Wavelet Transform formulated using lifting scheme [8]. It's an effective method to improve the processing speed of DWT. Integer wavelet transform allows to construct lossless wavelet transforms.

This paper is organized as follows. In section 2, we present the mixed scale DWT. Section 3 is devoted to the presentation of the proposed approach. In section 4, experimental results are given. The conclusion and future works are described in the last section.

2. DWT MIXED SCALES
Wavelets have been found to be extremely useful in digital watermarking. It has a growing impact in signal and image processing, mainly due to multistage and time-frequency localization of the image and their good performance in decorrelating information.

Traditionally, the original image is transformed using DWT multiresolution wavelet decomposition. In our watermarking algorithm, we prefer to use a mixed-scales representation using Faber-Schauder basis which permits to distinguish very particular regions of the image as shown in Figure.2, where we have a high density of dominant wavelet coefficients. Faber-Schauder DWT (FSDWT) [10] has the same construction principle and some properties of the S.Mallat wavelet transform [9] except the fact that the FSDWT basis is not orthogonal. This transformation is also well adapted to contour detection because it eliminates constant and linear correlation of smooth regions and use only the first neighbouring coefficients and gives more precise edge detection than higher order spline wavelets [8].

This wavelet transform is obtained by lifting scheme formulation with only arithmetic operation and no boundary treatment in three steps as shown in the following figure:

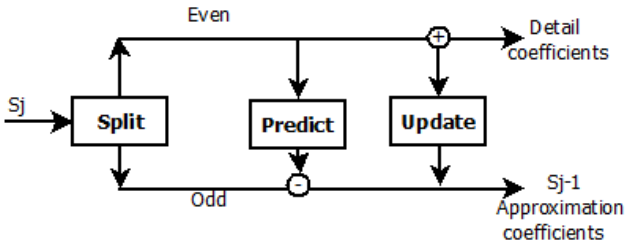


Fig 1: DWT by lifting scheme

The multiresolution transform is a linear transformation, from the canonical basis to the Faber-Schauder one; it redistributes differently the information contained in the original image [10]. In each sub-band, the dominant coefficients represent the most characteristics of image. The non-dominant coefficients in a given sub-band are the projection of dominant coefficients in the other sub-bands. In the order to facilitate the selection of the majority of dominants coefficients in all sub-bands, we use mixed-scales representation which is put each coefficient at the point where its related basis function reaches its maximum (cf. Figure 2).

Fig 2: mixed scales representation

So, we have visually coherent image which look like to a regions around the edges and textured zones. These regions are represented by a high density of dominant coefficients and they are a priori the most stable ones for any transformation keeping visual characteristics of the image.

The lifting Scheme of the FSWT is given by the following algorithm:

$$\begin{cases} f_{ij}^{0} = f_{ij} \quad for\ i,j \in Z \\ for \quad 1 \le k \le N \\ f_{ij}^{0} = f_{2i,2j}^{k-1} \\ g_{ij}^{k1} = \left(g_{ij}^{k-1}, g_{ij}^{k2}, g_{ij}^{k3}\right) \\ g_{ij}^{k1} = f_{2i+1,2j}^{k-1} - \frac{1}{2}\left(f_{2i,2j}^{k-1} + f_{2i+2,2j}^{k-1}\right) \\ g_{ij}^{k2} = f_{2i,2j+1}^{k-1} - \frac{1}{2}\left(f_{2i,2j}^{k-1} + f_{2i+2,2j+2}^{k-1}\right) \\ g_{ij}^{k3} = f_{2i+1,2j+1}^{k-1} - \frac{1}{4}\left(f_{2i,2j}^{k-1} + f_{2i,2j+2}^{k-1} + f_{2i+2,2j}^{k-1} + f_{2i+2,2j+2}^{k-1}\right) \end{cases} \quad (1)$$

The reconstruction of the original images is performed by a similar recursive algorithm.

3. WATERMARK EMBEDDING

Fragile watermark are designed to be easily used as tamper detection tool. This method is based on LSB technique which 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 dominants Blocks 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 logic of use the dominants blocks 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 [11]. Attacks or manipulations, such as removal of sensitive parts or addition of foreign objects or features, result in significant changes to the dominants blocks 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 Dominant blocks

As shown in figure 3, the non dominant coefficients have amplitude near to zero and it has small deviation values. The selection of blocks is based on two thresholds:

- SC is fixed to separating the dominant coefficients from non dominant ones in mixed scales: if the coefficient is greater than SC, it is chosen.
- SD fixed to select the percentage of dominant coefficient in block: SD% of coefficients is retained.

The choice of parameters SC and SD is based on studying the histogram of the wavelet coefficients of the images. So, the coefficients of the dominants blocks are located mainly around the image contour and characterize the textured zones as shown in figure 4. The logic of use the blocks dominants 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 [11]. 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.

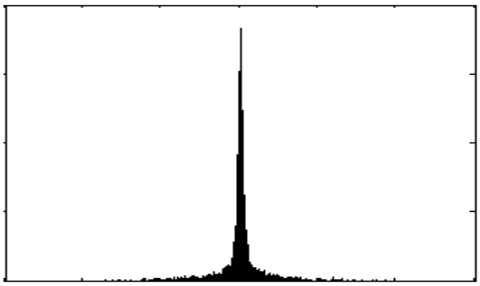


Fig 3: Histogram of wavelet coefficients

Fig 4: The important blocks that has a high-density of the dominant coefficients. (For Lena image: 8x8 blocks, SC = 10, SD = 20%).

3.2 Watermark construction

The embedding algorithm is illustrated in figure7. The first step in constructing watermark is to compute the mean of the second and third order moments of image without LSB bitplane. Then, the image is transformed by Faber-Schauder wavelet transform (FSWT) through lifting scheme. We extracting the dominants blocks map. The dominant blocks should be arranged in a way to make its rebuilding difficult for a no-authorized user. The LSB's bitplane of the image is substituted with watermark data composed by:

- Encrypted the message to be embed and mean value of the second and third order moments, The AES is used as encryption algorithm [12].

- Dominant blocks map built as mentioned above.

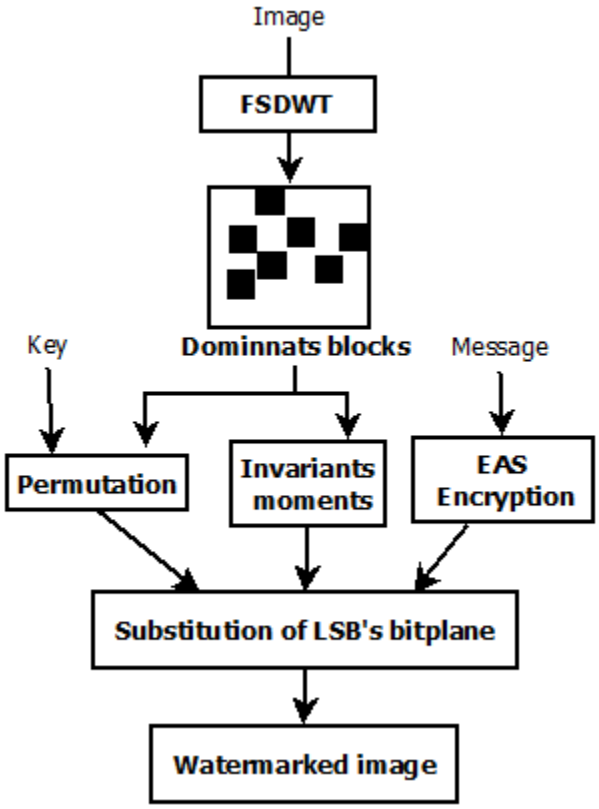


Fig 5: The proposed embedding algorithm

3.3 Locating of tamper region

At the reception side, the user starts with extracting the message 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 dominant blocks 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 dominant blocks maps permits to locate the modified tamper region whatever the degree of alteration.

4. EXPERIMENTAL RESULTS

We have tested our scheme on Lena image. In our work, The Lena image (Figure 6-a) was watermarked (Figure 6-b) using the method described previously. The mean value of invariants moments is 0. 2698. We apply FSDWT- mixed scales then we select the domiant blocks map The LSB's bitplane of the image is substituted by watermark composed by Domiant blocks map, encrypted message and the mean value of invariants moments.

In the reception side the image was slightly altered (Figure 7-b). This modification gives different reading of the mean value of the invariants on the tampered image which was 0.2698 against 0.2607 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 transformed by DWT in mixed scales and then select the dominants blocks to get edge map. The later was compared to

the one extracted from the LSB's bitplane. The comparison between these two dominant blocks maps coupled with contrast modification permits to identify the altered region. In case of no tampering, the comparison shows a totally black map (Figure 5-c).

Results obtained after tampering which are not visible as shown in Figure.5.c. The Lena image is tampered invisibly. The scheme recovers the approximated image and also locates the tampered area accurately.

The Peak Signal to Noise Ratio (PSNR) is used as distortion measurement between the original and a watermarked image. It is define as

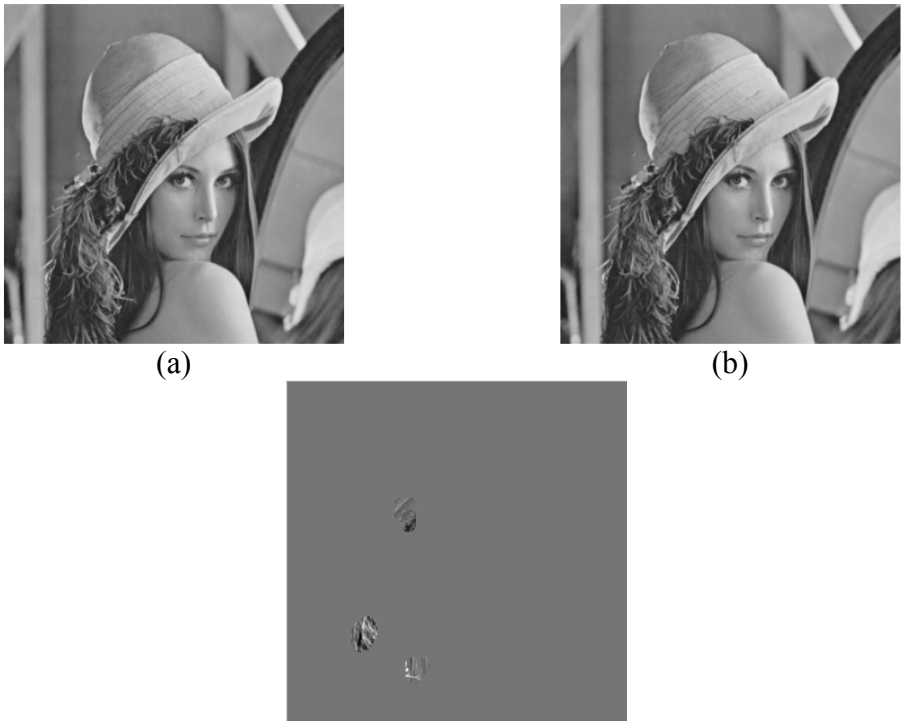
$$PNSR = 10\log_{10}\left(\frac{255^2}{\frac{1}{N}\sum_{n=1}^{N}(w_n)^2}\right) \quad (2)$$

Where N is the total number of the pixels, $w_n = s_n - y_n$, s represents the original image, and y is the watermarked image.

The PSNR of the watermarked image is 50.55db, which is quite reasonable. The watermarks are perceptually invisible. Figure.4 shows the original and watermarked images of Lena and a binary signature, which is embedded in Lena image.

(a) (b)

Fig 6: (a) The original Lena Image (b) he watermarked Image (PSNR 50.55db)



(a) (b)

Fig 7: (a) Original image (b) Watermarked image, (c) Scaled difference which shows those areas which are tampered

In order to identify the altered region, one should rebuild the dominant blocks 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 Dominant blocks maps permits to locate the modified tamper region whatever the degree of alteration.

5. CONCLUSION

This article proposed an efficient digital watermarking scheme to increase security, confidentiality and integrity of image such as medical and press agencies images. Firstly, we verify if the image is not attacked using a mean value of the second and third order moments as effectiveness tamper detection. The dominant blocks map of DWT coefficient in mixed scales is used to localize the altered region. The proposed watermarking algorithm can be used to introduce the patient's information in a private and sure manner all while preserving the visual quality of watermarked image. It is highly secure because of inclusion of private keys at various stages of watermark generation.

6. REFERENCES

[1] Jagadish Nayak, P Subbanna Bhat, Rajendra Acharya and Niranjan 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 Fransisco, CA: Morgan Kauffman, 2002.

[3] Knopp R, Robert A: Detection Theory and Digital Watermarking. Proceedings of SPIE, 2000, 3971:14-23.

[4] 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.

[5] Y. I. Khamlichi, M. Machkour, K. Afdel and A. Moudden, Multiple watermark for tamper detection in mammography image, WSEAS Trans. on Computers, Issue 6, Vol. 5, ISSN 1109-2750, pp. 1222-1226, June 2006.

[6] 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.

[7] 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.

[8] H. Douzi, D. Mammass, F. Nouboud, Faber-Schauder wavelet transformation application to edge detection and image characterization, Journal of Mathematical Imaging and Vision, Kluwer Academic Press, pp 91-102 ,Volume 14, no2, (2001).

[9] S. G. Mallat. Multifrequency channel decompositions of images and wavelet models. IEEETrans. Acoust. Speech Signal Process., 37(12):2091, 2110, 1989.

[10] M. El hajji, H. Douzi, R. Harba , Watermarking based on the density coefficients of Faber-Schauder wavelets, ICISP 2008: Lecture Notes in Computer Science, 455-462.

[11] 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.

[12] J. Daemen, V. Rijmen, (1999, September 03). AES Proposal Rijndael, Networks (2nd) [Online].Available: http://csrc.nist.gov/CryptoToolkit/aes/index.html.