World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:2, No:5, 2008

A Watermarking System Using the Wavelet Technique for Satellite Images

I. R. Farah, I. B. Ismail, and M. B. Ahmed

Open Science Index, Information and Communication Engineering Vol:2, No:5, 2008 publications.waset.org/5112/pdf

***Abstract*—**The huge development of new technologies and the apparition of open communication system more and more sophisticated create a new challenge to protect digital content from piracy. Digital watermarking is a recent research axis and a new technique suggested as a solution to these problems. This technique consists in inserting identification information (watermark) into digital data (audio, video, image, databases…) in an invisible and indelible manner and in such a way not to degrade original medium's quality. Moreover, we must be able to correctly extract the watermark despite the deterioration of the watermarked medium (i.e attacks). In this paper we propose a system for watermarking satellite images. We chose to embed the watermark into frequency domain, precisely the discrete wavelet transform (DWT). We applied our algorithm on satellite images of Tunisian center. The experiments show satisfying results. In addition, our algorithm showed an important resistance facing different attacks, notably the compression (JEPG, JPEG2000), the filtering, the histogram's manipulation and geometric distortions such as rotation, cropping, scaling.

***Keywords*—**Digital data watermarking, Spatial Database, Satellite images, Discrete Wavelets Transform (DWT).

I. Introduction

IN spite of its multiple advantages, digital technologies have increased counterfeiting and made easy the illegal use of digital data. And nowadays, the classical techniques of data protection have proven their insufficient and ineffective towards these problems [1] [2]. In fact, often data is stored in digital format, consequently, it become so easy to copy, to modify or to deform it with appropriate software.

Digital watermarking is a recent research axis considered as the best technique that provides reasonable and robust solution to this issue [4]; for this reason it became a very active and attractive area of research. The principal of watermarking consists in embedding information into digital data. We often call this hidden information the *watermark* or *payload*, and we designate by *cover work* the original data, where the watermark is to be inserted. This cover work may be any digital data that can be watermarked, like images, audio, video, formatted text, and others. The watermark can be an image, an identification text, a secret message…

The constraints required by a watermarking system are various. First, watermark should be imperceptible and it must be robust against attempts of replacing or removing it. Then, the original data's quality should not be lost or degrade. Moreover, we must be able to correctly extract the watermark despite the deterioration of the cover work. Finally, the watermark's presence must not be detected only by an authorized person (owner of private detection key, for instance).

In this paper, we present a robust watermarking scheme for hiding information into spatial database. We conceived this scheme particularly for satellite images. The proposed approach provides frequency domain information; precisely we adapted the Discret Wavelet Transform (DWT) to embed watermarks. Indeed, DWT consists in splitting the signal in low and high frequencies [7] [8]. The least significant coefficients are located typically in high frequency. Considering the fact that humain visual system is not sensitive to small changes in high frequencies of the images, the watermark was hidden into the high frequency zones. To enfonce security in our system, two keys (private and public) are used.

II. Digital Watermarking

A. Definitions and Concepts

Digital watermarking belongs to steganography, but their finality differs and their processes stand out mainly by their roles. Indeed, steganography consists generally in the exchange of a secret message between correspondents; however, watermarking systems try to insert imperceptible mark in a digital content without obvious deterioration of this cover work.

As said before, digital watermarking is suggested as an ultimate solution to protect digital content from piracy. This technique amounts to insert an imperceptible and permanent information or signature into an image, digital document, video sequence…This embedded information must be able to be detected only by the data owner, and must resist any kind of attacks aiming to remove it; we speak then of watermarking scheme robustness.

The watermark can contain permession information relative to the cover work. Also, it can be used to ensure the thruthfulness of document content and its integrity, and here we speak about document authentication [4]. Watermark can also indicate the document's owner; this embedded information can be either a unique code specifying the author or an originator of the cover-data [1]. Three general properties must be taken into consideration in order to assure a real-world robust marking system. First, the mark must be *imperceptible*, therefore, the existence of the hidden information should not be perceived by humain visual system, not only this, but also the embedding system must not produce a remarkable degradation in the cover work and must not reduce its quality value. Secondly, watermark must be *clearly*

Open Science Index, Information and Communication Engineering Vol:2, No:5, 2008 publications.waset.org/5112/pdf

identified by the detection system, we speak here of unambiguity or specificity, indeed, detected mark should unambigously identify the owner [1]. Thirdly, mark must be *robust*, so removing it must be a very difficult act for any unauthorized user. Moreover, the destruction of the watermark should damage the cover work quality.

B. Watermarking System Process

Watermarking system is composed of two basic parts, the embedding part and the recovery part. As an input, the first part requires the watermark (*w*), the cover work (*c*) in which *"w"* is to be inserted and may also require key(s), in fact, The embedding process can take place using a secret key that will be therefore necessary for mark detection. Watermarked work is the output of the embedding system [2] (Fig. 1).

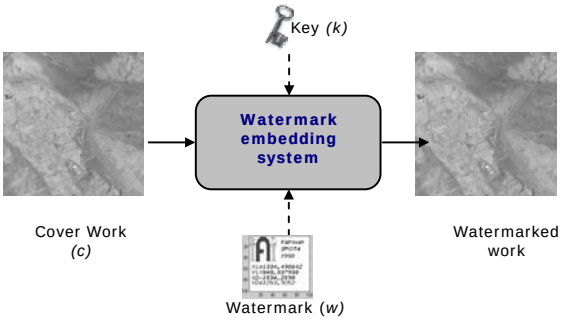


Fig. 1 Watermark embedding process

As for the second part, that is the recovery system – which aims to extract the mark- it takes the test work (t) which is possibly distorted, also it takes key and original cover work. As output, and if the test work was not attacked, it returns the watermark or an indication of presence [3] that characterizes the mark presence probability. It does not return anything in the contrary case (Fig. 2).

C. Watermarking Techniques

Watermarking methods started by simple and fragile solutions, nevertheless the evolution of the complexity of attack techniques extends watermarking methods to become sophisticated and more robust. In most work, different watermarking methods are classified according to the domain in which the watermarking scheme took place. We distinguish two main domain classes: Spatial domain and Frequency domain.

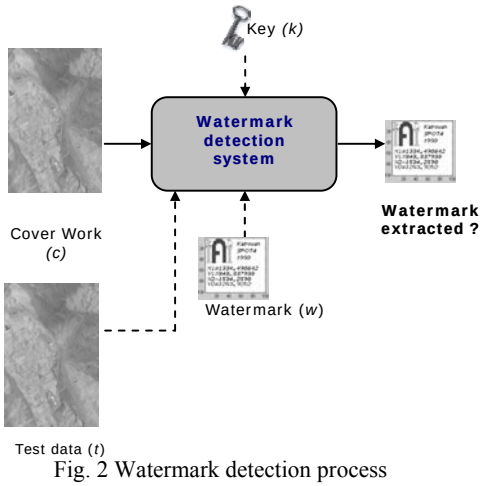


Fig. 2 Watermark detection process

However, in some cases, authors differentiate these methods according to the embedding mark way [4]. In such situation, we distinguish the additive methods, in which we add the mark to the cover mark features, and the substitutive ones which consists in replacing some cover work coefficients.

Spatial domain: The spatial methods involve direct modification of pixel's value. These techniques are qualified rapids, but they do not ensure a robust protection against various attacks or common operations applied to watermarked cover, especially the compression data, for example JPEG compression destroyed easily the mark. There are many variants of such techniques, among these methods we distinguish mainly: The LSB modification method, the blocks modification method and patchwork method [4].

Frequency domain: These techniques improved the resistance and robustness facing numerous operations and attacks [5]. In this domain, the embedding scheme consists in three steps (Fig. 3).

First we apply a transformation on the cover work. This transformation can be DCT (Discret Cosinus Transform), it can be also DFT (Discret Fourier Transform) or recently DWT (Discret Wavelet Transform). The second step consists in embedding watermark by modifying some coefficients value of the transformed cover work; thus, we get a watermarked and transformed work. At last we apply to this new work, the reverse transformation in order to obtain watermarked work.

D. Watermarking Applications

Watermarking application domains are numerous. We distinguish the protection of intellectual property, the documents follow-up, the non-authorized distribution prevention, the copyrights protection, the authentication and integrity of the content [6].

Open Science Index, Information and Communication Engineering Vol:2, No:5, 2008 publications.waset.org/5112/pdf

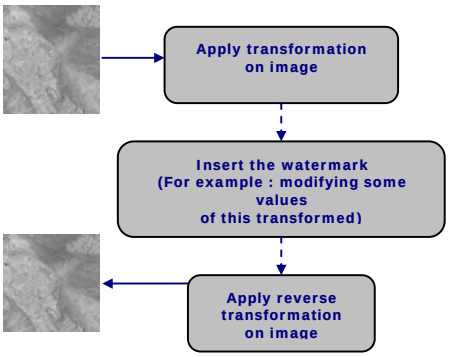


Fig. 3 General watermarking process in frequentiel domain

III. Discreet Wavelet Transform (DWT)

It is difficult to treat this immense subject with all mathematical proofs and associated theoretical concepts in some paragraphs. Wavelet analysis is a new and promising method of signal processing, considered as extention to the Fourier analysis [8]. Applied to a signal, wavelet transform make possible the simultaneous apparition of both temporal and frequencial information.

A. Definitions

Wavelet analysis allows *"the use of long time intervals where we want more precise low-frequency information, and shorter regions where we want high-frequency information "* [7][8].

A function $\psi(t) \in L^2(R)$ is considered as wavelt only if it verifies the admissibility condition (1) :

$$\int_{-\infty}^{+\infty} \frac{|\hat{\psi}(\omega)|}{|\omega|} d\omega < \infty \quad (1)$$

This condition makes the signal analysis easy, and makes possible to rebuild it without a loss of information [10].

Precisely, wavelet transform consists in splitting signal into shifted and dilated versions of a window, called *mother* wavelet [10][7]. This dilation and this shift of mother wavelet generate what we call *wavelet family* (2).

$$\forall u,s \in Rx[0;+\infty[\quad \psi_{u,s}(t) = \frac{1}{\sqrt{s}} \psi\left(\frac{t-u}{s}\right) \quad (2)$$

Wavelet transform takes two arguments: time and scale; and it is defined by (3):

$$W(f)(u,s) = \int_{-\infty}^{+\infty} f(t) \frac{1}{\sqrt{s}} \psi^*\left(\frac{t-u}{s}\right) dt \quad (3)$$

the discret wavelet transform DWT uses a discrete sequence of scales s^i. Discret wavelet consists in sampling the scale at s^i and time at its integer values (4), the discret wavelet transform of f is (5)

$$\psi_i[n] = \frac{1}{\sqrt{s_i}} \psi\left(\frac{n}{s_i}\right) \quad (4)$$

$$Wf[n,s_i] = \sum_{m=0}^{n-1} f[m] \psi_i^*[m-n] \quad (5)$$

B. Image Wavelet Decomposition

It deals with Mallat algorithm or multiresolution analysis [8], it is a classical scheme known in the signal processing community as a two-channel subband coder. In image wavelet decomposition we often speak of approximations and details. The approximations are the high-scale, low-frequency signal components; it contains most of the information from the original signal. The details are the low-scale, high-frequency components.

So, the image will be decomposed for each resolution level into a high-high (HH), high-low (HL), and low-high (LH) sub-image, and a low-low (LL) sub-image for the coarest resolution level. The LL sub-image is the approximation (**A**). The HH, HL and LH sub images are the details (**D**) containing the diagonal, horizontal and vertical details [4][6][12] (Fig. 4).

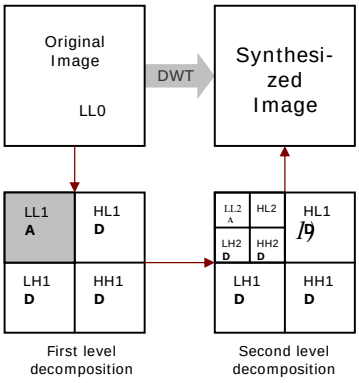


Fig. 4 2D-Wavelet decomposition (Resolution level 2) (A : approximation, D : Details)

IV. Our Contribution

In addition to its robust character, the watermarking system proposed in this paper is suitable for both copyright protection and authentication data**.** The first application is based on private key whereas the second is based on public key. It operates in the frequentiel domain and it is based on wavelet technique (*DWT*).

Moreover, our algorithm does not require prior knowledge of the original cover work. It resists all types of scaling and geometric distortion attacks, compression (In particular JPEG, JPEG2000), filtering, and the histogram's manipulation.

V. Proposed Architecture

The proposed architecture is composed of three parts or sub-systems [13] (Fig. 6): The *spatial references system*, containing information system essentially the satellite images base and the watermark set. The second part, which we call *user interface,* is a Web interface that makes easy, to any user, the access to the spatial database and offer the possibility to consult or download available satellite images. The third part is the most important architecture's component, the *watermarking system*. It includes essentially the embedding watermark scheme and the detecting watermark scheme. We add to this component a valuation module to make possible the marking process verification and to value system quality by following-up the marking step. This component is

Open Science Index, Information and Communication Engineering Vol:2, No:5, 2008 publications.waset.org/5112/pdf

manipulated by the database's owner. In this paper we will concentrate on the third component from now on.

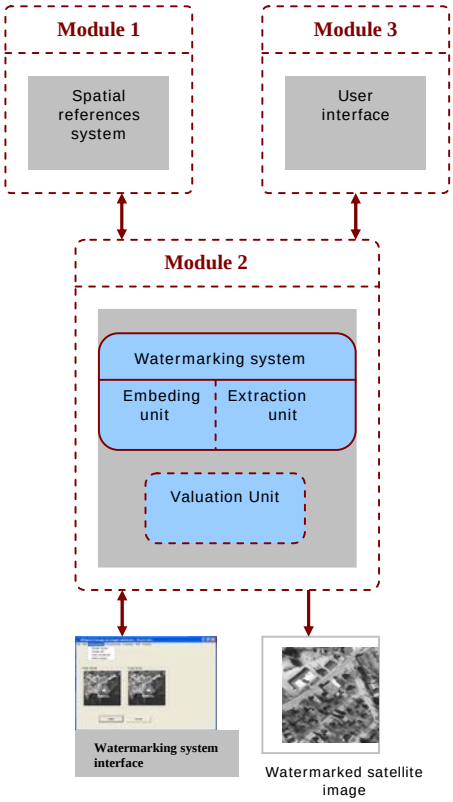


Fig. 5 Proposed architecture

VI. Watermarking Technique

A. Embedding Scheme

For the embedding scheme, we chose to insert the watermark in the details (sub-images). In fact, the main interest of wavelet based techniques is that it ensures the imperceptibility's constraint and makes it possible. In addition, taking into consideration that the human visual system is not sensitive to small changes in high frequency [4][6] that is, details, we proceed to insert watermark in these part of decomposed image. To ensure robustness, we used keys to embed and detect watermark.

The following figure (Fig. 6) shows the adopted procedure to embed the mark. First, we use the key k1 to choose sub-images in which we are going to insert the mark. then, we insert the mark in these details while constructing key k2 progressively. Finally, we rebuild image with the tattooed details.

The proposed embedding algorithm consists in inserting the watermark pixel by pixel. Before inserting any watermark pixel, we compare its value (p_w) to the sub-image selected pixel value (p_{si}):

$$pw \in [psi-\lambda_1, psi+\lambda_1] \text{ or } psi <= \lambda_2$$

We substitute these two pixels while saving pw new position, pw value and sub-image type (*HH, LH or HL*) in a matrix (k2).

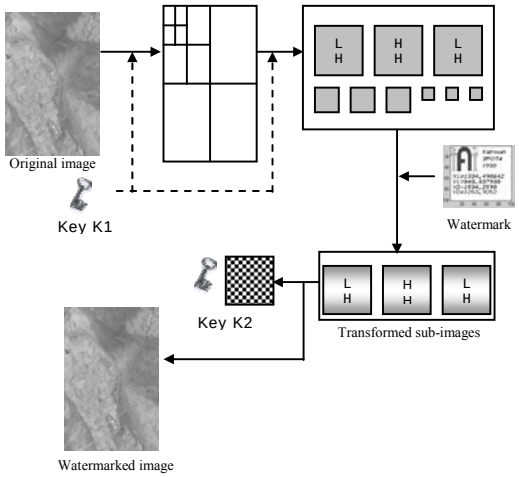


Fig. 6 Embedding scheme

We repeat this procedure for each watermark pixel, we note that if the sub-image pixels are finished, we take the following sub-image. If all watermark pixels are embedded, we apply the Reverse Discreet Wavelet Transform DWT-1 to the new sub-images.

As output, this scheme returns k2 and the watermarked image. (k1, k2) represent the detection key, or the secret key.

B. Detecting Scheme

The recovery watermark algorithm is similar to the embedding one while in a reverse order and process (fig. 7). The extraction of a watermark requires only the detection key (k1, k2) and obviously the test image. As in embedding scheme, we start by applying the Discreet Wavelet Transform to the test work, and then for each k2 value (t, pos, val) we select the sub-image type specified by t, we search the pixel position specified by pos and we construct the watermark pixel by pixel.

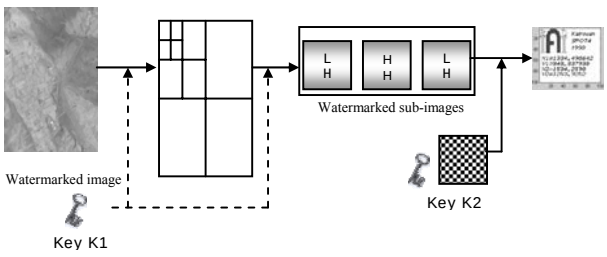


Fig. 7 Detecting scheme

VI. Results

To make tests, we start with embedding the watermark into the original cover work, and then we proceed to attack the watermarked image (Fig. 8). After, we calculate the PSNR between the original image and the watermarked one, and then we calculate the PSNR between the original mark and the mark extracted in order to discern the watermark resistance facing attacks.

Open Science Index, Information and Communication Engineering Vol:2, No:5, 2008 publications.waset.org/5112/pdf

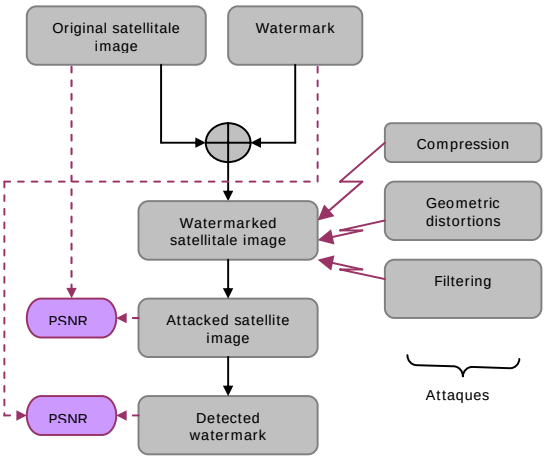


Fig. 8 Test process

The algorithm was applied on satellite images (SPOT). The image used in this paper represents Tunisian Center (Kairouan) and RIADI's logo is used as watermark (Fig. 9). The experiments show satisfying results (Fig. 10 and Fig. 11).

In addition, our algorithm showed an important resistance facing different attacks, notably the compression (JEPG, JPEG2000), the filtering, the histogram's manipulation and same geometric attacks (Rotation, cropping). The following table (Table I) shows the main gotten results.

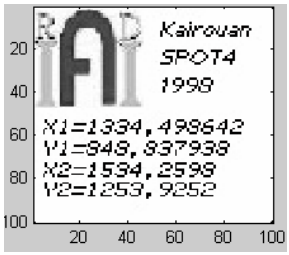


Fig. 9 Example of Watermark

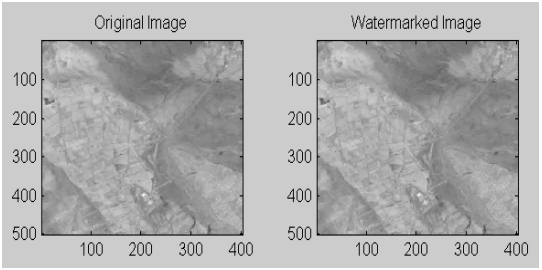


Fig. 10 Watermark imperceptivity proof

TABLE I
RESULTS OF RESISTANCE FACING DIFFERENT ATTACKS

Deformations		PSNR between watermarked image and original one (dB)	PSNR between extracted mark and original one (dB)
Filtering	Median 5x5	41.20	39.56
	Median 16x16	40.11	36.12
Speciel filtering	Disk	41.12	36.10
	Gaussian	40.09	35.44
	Laplacian	40.3	36.54
	Motion	41.21	36.12
	Sobel	39.03	34.10
	Unsharp	41.90	39.00
Rotation	5°	41.6	35.67
	15°	41.48	35.49
	45°	41.46	35.44
	75°	40.38	34.87
Cropping	+50%	41.13	35.12
Histogramme		41.47	38.33
Compression	Jpeg	42.15	39.45
	Jpeg2000	42.18	38.66
	Tiff	41.98	38.13
	Gif	42.01	37.12

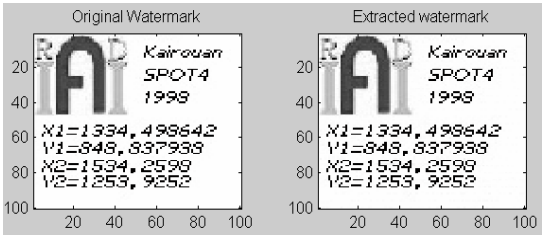


Fig. 11 Well extracted Watermark

VII. CONCLUSION

In this paper, we presented a wavelet based method for satellite image watermarking. We proposed a *blind marking* algorithm which can be applied both in the copyright protection and the content authentication domaine.

Even though we obtained satisfying results and showed that our system can resist different geometric distortions, filtering, various compression and many others attacks, we cannot prove that it will resist all attacks particularly malicious ones. Indeed, it is true that technical watermarking researches progress and try to reach high performance, but on the other hand, the attack's techniques have become more and more sophisticated and pirates are progressing as well.

REFERENCES

[1] Stefan Katzenbeisser et Fabien A. P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*. Security Technologies for the World Wide Web, Artech House Computer Security Series, 2000.

[2] Matthieu Brunet et Frédéric Raynal. "*La problématique du watermarking"*. Site : www-rocq.inria.fr/codes/Watermarking Dernière mise à jour 2000.
[3] Christine Cavaro-Menard. "*Codage, Compressiont Echanges d'images"*. Unité de Traitement d'Images Médicales - Équipe Signal et Image - Service de Médecine Nucléaire et de Biophysique - CHU d'Angers.
[4] Anne Manoury. "*Tatouage d'images numériques par paquets d'ondelettes"*, Thèse de Doctorat, Spécialité: Automatique et informatique appliquée. Ecole Centrale de Nantes, Décembre 2001.
[5] David Gross-Amblard. "*Tatouage: appliqué aux bases de données"*. Laboratoire Cedric – CNAM, 2003.
[6] Nafornita Corina. "*Watermarking in the wavelet domain"*. Mémoire de diplôme pour obtenir le degré de M.Sc. Université ″Politechnica″ Timisora, Faculté d'Electronique et Télécommunication. TIMISOARA-2004.
[7] S. Mallat. *Une exploration des signaux en ondelettes*. Les Éditions de l'École Polytechnique, Ellipses edition, 2000.
[8] S. Mallat. *A wavelet tour of signal processing*. Academic Press, 1998.
[9] Ingemar J. Cox, Matthew L. Miller, et Jerey A. Bloom. "*Digital Watermarking"*. Morgan Kaufmann Publishers, Inc., San Francisco, 2001.
[10] Demaeyer Jonathan, Bebronne Michael et Forthomme Sébastien. "*Les Ondelettes"*. Université Libre de Bruxelles, Faculté des Sciences, Département de Physique : Deuxième Candidature en Sciences Physiques, Printemps des sciences 2003.
[11] Caroline Fontaine. "*Le tatouage des images numériques"*. Laboratoire d'Informatique Fondamentale de Lille. Pour la science N°270 - Avril 2000.
[12] Guillaume Savaton. "*Méthodologie de Conception de Composants Virtuels Comportementaux pour une Chaîne de Traitement du Signal Embarquée"*. Laboratoire d'Electronique des Systèmes Temps Réel (*LESTER*) Université de Bretagne Sud, Lorient décembre 2002.
[13] I.B.Ismail, I. R. Farah and M. B. Ahmed "Satellite images watermarking based on wavelet techniques*"*. IEEE The 2 International Conference en Information and Communication Technologies ICTTA'06 Syria, 2006.

Farah Imed Riadh received the M.D. and Dr. Eng. degrees, from ISG Inst. of computer sciences in 1995 and ENSI Sch. in 2003, respectively. After working as a research assistant (from 1996) and a permanent researcher at laboratory RIADI, ENSI National School of Computer Sciences engineering (since 1995), he has been an assistant professor at University of Jendouba, since 2004. His research interest includes image processing, pattern recognition, artificial intelligent, and their application to remote sensing. He is a member of Arts-Pi Tunisia.

Ben Ismail Imen received the M. E., from ENSI National School of Computer Sciences Engineering in 2006. She is a permanent researcher at laboratory RIADI, ENSI National School of Computer Sciences engineering (since 2004). She's research interest includes image processing, artificial intelligent and pattern recognition.

Ben Ahmed Mohamed is emeritus professor.

Open Science Index, Information and Communication Engineering Vol:2, No:5, 2008 publications.waset.org/5112/pdf