Journal of Electrical and Electronics Engineering Research Vol. 2(5), pp. 114-121, November 2010
Available online at http://www.academicjournals.org/jeeer
ISSN – 2141 - 2367 ©2010 Academic Journals

Full Length Research Paper

A new scheme of image watermarking based on fuzzy clustering theory

Sameh Oueslati[1,2]*, Adnane Cherif[1] and Bassel Solaiman[2]

[1]Department of Physics, Laboratory of Signal Processing, Faculty of Sciences, University Tunis, El Manar 1060, Tunis.
[2]Department: Image and Information Processing, Higher National School of Telecommunication of Bretagne,
Technopole of Brest Iroise, 29285 Brest – France.

Accepted 31 July, 2010

Digital watermarking technology has the advantages of easy implementation and capability of providing wide security services such as copyright protection, authentication and secret communication. In this paper, a novel image watermarking approach based on embedding watermarks in different domains, without any distortion of the watermarked image is used. In the spatial domain, the processing method is based on study of segmentation by fuzzy c-means clustering method (FCM) that outputs the zones of watermark embedding and respectively the associated appropriate embedding gain factors. However, in the DCT, we embedded the watermark into the coefficients in mid-band frequency of the selected blocks with different embedding strength. Experimental results show that the proposed scheme has good imperceptibility and high robustness to common image processing operators.

Key words: Image watermarking, insertion force, Image segmentation, fuzzy C-mean (FCM), statistical features.

INTRODUCTION

With the rapid development of Intemet and multimedia technology, more and more digital media including images, texts, and video are transmitted over the Intemet (Barni et al., 2009). However, as far as we know, transmitting information on computer networks is not safe and the valuable data is easy to be copied, thus, providing copyright protection for digital media is becoming increasingly important (Davoine et al., 2004). A solution to alleviate this problem is to insert watermarks into the media particularly in images, so it can be detected and used as evidence of copyright.

There are three important requirements that are mostly needed for a well-designed watermarking scheme described as follows (Patrick et al., 2007; Anne, 2001; Azza, 2009).

1) Imperceptibility: The host image or original image should not be visibly degraded by the watermark. In other words, we must ensure that an unauthorized user do not perceive the existence of the watermark. Imperceptibility ensures the excellent perceptual quality of the protected image.
2) Robustness: The hidden watermark must survive image processing or operations such as clipping, filtering, and enhancement. The watermark should be retrieved after been compressed by lossy compression techniques such as JPEG. It also must be against the malicious attack that denotes the manipulation of destroying or removing the watermark.
3) The third important factor that allows a watermarking method to be commercially interesting is the watermarking capacity that permits a bigger amount of data embedding in the image.

In this paper, we propose to exploit the robustness of respectively the spatial and frequency domain in the same time (Shih et al., 2003). A set of watermarks is embedded in the DCT frequency domain (Barni et al., 1998; Cox et al., 1997) in different selected blocks coefficients with respect to the JPEG quantization values table. The choice of these coefficients is based on a strategy to minimize the vulnerability of the embedding scheme by the redundancy of the different embedded

*Corresponding author. E-mail: sameh.oueslati@telecom-bretagne.eu.

watermarks (Patrick et al., 2002). In the same time, a second set of watermarks is embedded in the spatial domain.

A study of segmentation by fuzzy c-means method is carried out in order to determine the best embedding locations and the highest usable gain factor with respect to the image zones characteristics. This embedding approach proved that the watermarked image become more robust mutually to the JPEG compression (Wallace, 1992) and wide kinds of synchronous and asynchronous attacks. In addition, because of the recurrence resulting from the multiple embedded watermarks in these two domains, at least all or some of these inserted watermarks survived in each of the applied attacks.

EMBEDDING PROCESS IN THE FREQUENCY DOMAIN

The first step of this approach is to insert several identical marks in the field of DCT. The watermarks are presented as different binary images, containing data about the author's data about the patient as: The name, medical diagnose…etc. With $P \times P$ size described as the following:

$$M_L = \{M_L(i, j), 0 \le i, j \le P\}\ M \in \{0,1\}\ L \in .\{1,2......, L_{\max}\} \quad (1)$$

Among the work of watermarking, the algorithm proposed by Zhao (1995) is coded on a pair of frequency values (0, 1). The use of DCT frequency domain can fulfill not only the invisible through the study of optimizing the insertion gain used, but also security by providing a blind algorithm which use the original image which is not essential and the extraction of the mark made by a secret key (Patrick, 2005; Wolfgang, 1997). In order to invisibly embed the watermark that can survive lossy data compressions, a reasonable

$$C_1(i_1,\ j_1) - C_2(i_2, j_2) \ge \alpha \quad (2)$$

C_1, C_2 are the DCT coefficients, $(i_1,\ j_1)$, (i_2, j_2) are respectively the positions of the two selected coefficients with same quantization values and α is the gain factor resultant from this equation.

The redundancy introduced by the insertion of multiple watermarks encoded in the described coefficients, proved through experimental results, that it introduces a higher robustness after different attacks. An explanation of the robustness increase is that some or at least one of the embedded watermarks survives in each time the attack is applied. By applying an inverse DCT transform, we obtain a spatial representation of a watermarked image $I_{DCT^{-1}}$. Trade-off is to embed the watermark into the middle-frequency range of the image. In this paper, the DCT coefficients where the watermark bits will be encoded are chosen from the medium frequency band in order to provide additional resistance to lossy compression while avoiding significant modifications or distortions to the cover image (Bruyndonckx et al., 1995). Instead of choosing arbitrarily the coefficients locations, we can increase the robustness to compression by basing our choice on the recommended JPEG table. In fact, if two locations are chosen as they present identical quantization values, any scaling of the first coefficient will scale the second by the same factor preserving their relative size (Davoine et al., 2004). Furthermore, to augment the survival chances of the embedded watermarks against a large set of attacks and to reduce the probability of detection errors, an additional gain factor noted α is used in the watermark embedding process. Some criteria are presented for the choice of α as shown in the Equation (2), in order to respect the imperceptibility threshold shown by the image distortions. It is found that the computed gain factor value is approximately equal to that given by this equation (Davoine et al., 2004).

STATISTICAL SEGMENTATION FOR ZONES DETERMINATION

Spatial insertion procedure is preceded by a step of determining zones of insertion. Indeed, a heterogeneous image is composed by different zones (homogeneous textures, low intensity...) (Khaled et al., 2009). This diversity implies that the insertion in these different zones may not be identical. Hence the classification stage of the image used in different zones according to the characteristics of each is indispensable (Lotfi et al., 2009). To enhance the robustness against various image distortions that can be subjected, we use a force insertion α of watermark. This force must be below a predefined threshold of visual perceptibility which depends on the characteristics of the zones of insertion. This force is not always uniform on all components of the inserted watermark, but depends on the characteristics of the zones of insertion (textured, uniform ...), because the eye is less sensitive to noise in regions of the image where the brightness is very high or very low and the human eye is less sensitive to regions of the image with strong texture, more specifically, to zones near the edges. These aspects have been implemented in this article; so the key point to embed a watermark is to determine where the watermark can be embedded and how much strength can be added.

Fuzzy C-means clustering based on the image statistical features

The most widely used clustering method is probably the fuzzy C-means (Ruspini, 1969; Dunn, 1974; Bezdek, 1981; Mukherjee et al., 1996), called FCM algorithm, which is a "fuzzy relative" to the simple C-means technique (Haralick et al., 1973). FCM is an unsupervised clustering technique which has been utilized in a wide variety of image processing applications such as medical imaging (Hsiang et al., 1999; Bezdek et al., 1993) and remote sensing (Rignot et al., 1992; Chumsamrong et al., 2000; Yang et al., 2005). Its advantages include a straightforward implementation, fairly robust behavior, applicability to multichannel data, and the ability to model uncertainty within the data. A major disadvantage of its use in imaging applications, however, is that FCM does not incorporate information about spatial context, causing it to be sensitive to noise and other imaging artifacts. In fact, an image can be represented in terms of pixels, which are associated with a location and a gray level value. It can also be represented by its derivatives, e.g., regions with statistical features like average grayscale value (Ag), standard deviation (Sd), variance (Va), entropy(E), skewness (Sk), kurtosis(Ku) given in Table 1.

Therefore, a proposed segmentation approach combining pixel characterization by a set of statistical features and fuzzy clustering approach, FCM, is discussed. The proposed approach can be divided into two principal steps. The first consists to characterize each image pixel by a feature vector. Features can be extracted from regions masked by $(n \times n)$ window. The second step is a clustering procedure of the feature vector, initially extracted, using FCM clustering algorithm. By applying FCM, a partition of the feature vectors into new regions can be found. As depicted in Figure 1, the system scans the image using a sliding window and extracts a feature vector for each $(n \times n)$ block. The c-means algorithm is used to cluster the feature vectors into several classes with every class corresponding to one region in the segmented image (Bezdek et al., 1981). An alternative to the block-wise

Table 1. A set of statistical features.

$$A_g = \frac{1}{MN}\sum_{i=1}^{M}\sum^{N} g(i,j) \tag{3}$$

$$S_d = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} (g(i,j)-M_e)^{1/2} \tag{4}$$

$$V_a = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} (g(i,j)-M_e)^{2} \tag{5}$$

$$E = -\sum_{i=1}^{M}\sum^{N} g(i,j)\log(g(i,j)) \tag{6}$$

$$S_K = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} (g(i,j)-M_e)^{3} \tag{7}$$

$$K_u = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} (g(i,j)-M_e)^{4} \tag{8}$$

Note $g(i,j)$ is the grey level of pixel (i,j).

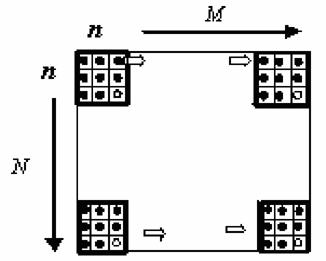


Figure 1. Scan an image ($M \times M$) by a window ($n \times n$) with n

segmentation is a pixel wise segmentation by forming a window centered around every pixel. A feature vector for a pixel is then extracted from the windowed block. The spatial scanning order of an image ($M \times M$) is performed, as shown in Figure 1, from left to right and top to bottom, pixel by pixel.

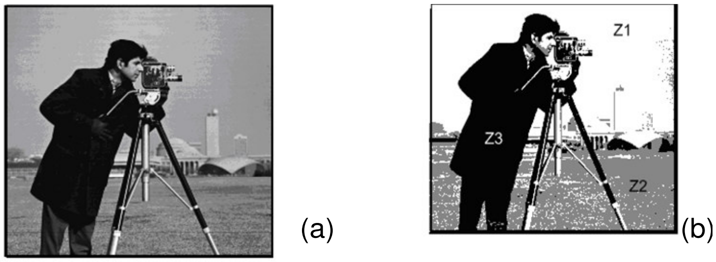


Figure 2. (a) Original image “cameraman”, (b) Three classified zones.

Spatial embedding procedure

Before embedding in the spatial domain, a study of the image characteristics is preliminary carried out in order to find out different images zones, where each one corresponds to specific image characteristics. In each of these zones, an automatic computation of the gain factor is used in the embedding equation in order to maintain watermark under the imperceptibility limits, this study fuzzy c-means clustering that takes into account the image statistics parameters. Using these parameters, we can identify the zones limits corresponding to the different images characteristics and computes the matching gains. This proposed method is found to be a fine tool of image segmentation with the characteristic been flexible and having the possibility to detect different programmed zones with acceptable accuracy. Using this method, the proposed technique does not allow a wrong classification output. A 2×2 pixel block is used to browse the DCT watermarked image to identify and mark the different existing zones. All the image matrix lines are consecutively processed and browsed by this block with an overlap of one line and one column pixel. The original is automatically classified and marked with different colors as shown in Figure 2. Three different zones are sorted with regards to their respective specificities where Z.1 represents the first zone marked in white that corresponds to a homogeneous zone in the host image (sky), Z.2, the second zone marked in black that corresponds to a textured zone (green), and the third zone called Z.3 corresponds to a dark zone in the host image (cameraman). For every zone, the appropriate gain factor called α, is automatically computed as detailed in Equations (10) basing on the Weber’s law to keep the watermark unperceivable as the following:

$$\frac{\Delta I(i,j)}{|I(i,j)|} = cte \tag{9}$$

Where cte denotes a constant, and $\Delta I(i,j)$ is the pixel difference between the watermarked and the original image. The Weber law can be written as the following:

$$(I_W(i,j) - I(i,j))/|I(i,j)| = cte \tag{10}$$

Once the gains computed, this imperceptibility limit is also protected as shown in Equation (11) by the use of a security factor that forbids the possibility to visualize some details of the embedded watermark even though the image size is zoomed many times.

$$\alpha = \alpha_c \times S_F \tag{11}$$

Where α the used gain factor, α_c is the computed and adjusted gain factor, S_F is the security factor. This factor used equals 0.75.

The general shape of the insertion procedure takes into account that the image was previously marked in the DCT frequency domain by a set of labels introduced as the following equation:

$$I_{MML}(i,j) = I_{M,L,n}(i,j)[1 + \alpha M_{L,n}(i,j)] \tag{12}$$

Where L denotes the watermark index, N the number of the segmented zones; n varies with the indexed zones and respectively $L \in \{1,2,...,L_{\max}\}$ and $n \in \{1,2,....N\}$. In this equation I_{MM} denotes the double watermarked image in the spatial and frequency domain, I_{MML} is the watermarked image by L watermarks in the two domains, $I_{M,L,n}$ is the frequency

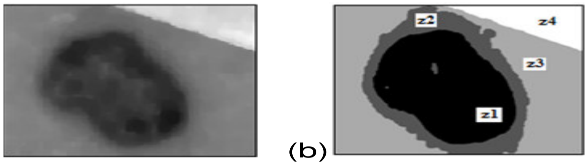


Figure 3. (a) Original image: (b) Four classified zones.

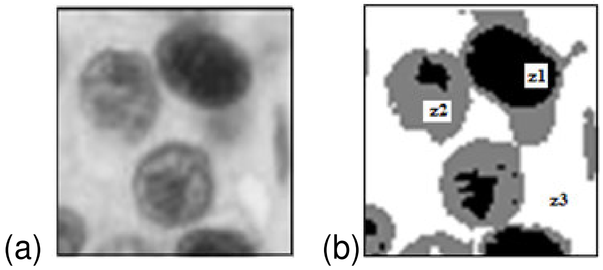


Figure 4. (a)Original image; (b) Three classified zones.

watermarked image going to be watermarked in the second time by the watermark number L in the n^{th} spatial classified zone, $M_{L,n}$ is the watermark number L going to be embedded in the n^{th} Zone and α is the variable gain factor determined by the segmentation process. The total embedded watermarks in the spatial and frequency domain are then considered equal to eleven.

Different other images are used in the carried experiments in all the watermarking process, with different classified zones numbers as shown in Figures 3 and 4. These figures show medical images with textures. Figure 3 shows an image of malignant melanoma, a skin cancer seen in France as the leading cause of death among women between 25-29 years 6,000 new cases each year, partitioned into four zones where the watermark can be embedded with several different gain factors. Figure 4 is divided into three different zones. In each image, the position where the watermark is to be embedded changes with the different zone.

EXPERIMENTAL RESULTS

The watermarking algorithm was tested using a 256 × 256 gray scale images. The peak signal to noise ratio (PSNR) is used to measure the imperceptibility of the watermarked image. By using the proposed scheme, the watermark is almost imperceptibility to the human eyes, as shown in Table 2.

The PSNR is defined as follows:

$$PSNR = 10\log_{10}\left(\frac{X_{\max}^2}{MSE}\right) = PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \qquad (13)$$

$X_{\max}$: The maximum luminance.
The MSE is defined as follows:

$$MSE = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}\left(I_{ij} - I_{ij}^{*}\right)^2}{n \times m} \qquad (14)$$

I and I^* are respectively the original image and the image watermarked size $m \times n$ where I_{ij} and I_{ij}^* are their components.

This error is mainly due to the addition of the mark. In the bibliography, quality of the watermarked image is good if the PSNR is equal to or higher than 30 dB. We note from Table 2 that for a given image and following the insertion of the first mark will be worth significantly more than 30 dB PSNR. We note from Table 2 that the greater the number of signatures, PSNR decreases. In fact, the insertion of signatures in the image returns to introduce new information and therefore a degradation of image quality, and every time we increase the number of the mark image, quality decreases.

Robustness against attacks

Furthermore, several experiments were performed in order to demonstrate the robustness of the algorithm under various attacks, including lossy JPEG compression, Noises attacks, as well as filtering attacks.

JPEG compression attack

Lossy compression algorithms such as JPEG are commonly used for efficient storage and transmission of images over the Internet. It is therefore crucial to examine whether the proposed watermarking scheme can survive JPEG compression attacks. In order to perform this experiment, the watermarked image shown in Figure 5(c) was compressed using different quality factors. As shown in Table 3, in each experiment, the correlations values are gathered corresponding to the embedded watermarks in the two domains. High correlations are obtained using this method which proves that all or some of the embedded watermarks have survived to the applied attacks. The watermarked image indicates a good perceptual quality and the extracted watermark is similar to original one. As shown in Figure 6, the extracted watermark is still visually acceptable after the watermarked image had undergone several common attacks such as JPEG lossy compression and destructive signal processing; some results are shown in Table 3.

Fidelity against noise attacks

It is quite relevant to evaluate the robustness of the suggested method against noise. In fact, we have tested our new approach using 10 different noise generations and by modifying variances at each time. From Figure 7, we can observe values of PSNR that are always higher than 30 *dB*. This makes it obvious that the image quality is good and these new watermarked images algorithm is powerful to keep image fidelity even after noise attack.

The watermark detector response when the watermarked image is introduced to additive Gaussian noise with different variance values is shown in Figure 8(a).

Table 2. PSNR of watermarking images.

Number of watermark	Watermark 1	Watermark 2	Watermark 3	Watermark 4
PSNR (dB)	49.08	41.17	38.15	34.40

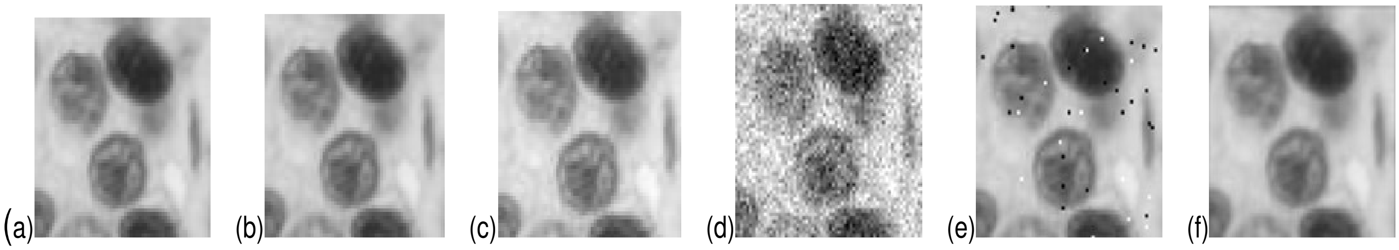


Figure 5. The watermarked image introduced to various attacks. (a) Original image (b) Watermarked image, (c) JPEG compression, (d) additive Gaussian noise, (e) Salt and paper noise, (f) Gaussian filter.

Table 3. Presentation of the correlation values after attack of JPEG compression 60 between the watermarks obtained in the spatial domain and frequency and the original.

Number of watermarks	Spatial domain	Frequency domain
Watermark 1	0.9080	0.9798
Watermark 2	0.9862	0.9953
Watermark 3	0.8523	0.9745

Watermarks detection

In this section we present experimental results carried out on a database of 800 marks in which the extracted marks are tested. The test technique is made by correlation between the extracted marks and the dictionary. Figures 8 demonstrate that the marks are correctly detected from our simulation results from Watermarked images after Noises attacks, JPEG Compression and Filtering attacks. Figure 8(b) shows that the detection results are satisfactory, even if the watermarked image has deteriorated considerably during the compression of a quality factor as low as 20. We have tested the robustness of our proposed method face to Gaussian filter Figure 8(c) displays the watermark detector response when the watermarked image is attacked by Gaussian filter.

Rotation attack

This attack can be seen as an innocent attack or malicious attack. In fact, the analog-digital conversion (scanning) sometimes involves the need for a relationship on the image to better exploit. This same attack can be considered malicious if the attacker makes a slight turn invisible on the image (of the order of several degrees or radians). This rotation, imperceptible to the naked eye will cause desync total image when looking for the signature and a change in the coefficients related to the image especially in the areas processed (frequency, multi-resolution ...). Regarding the attack by rotating the image, the angles chosen are 2, 5, 10 and 12°. The large angles of rotation have degraded the quality of digital image. However, these values do not pose problems for the extraction of the mark. The marks obtained after this attack showed a similarity with the original image showing that the mark inserted was not damaged by the attack carried.

Conclusion

In this paper, a novel image watermarking approach based on a multiple domain watermarking with several watermarks embedding in the spatial and frequency domains. The watermarking process is divided in two separated steps: Embedding in the DCT frequency domains and the spatial domain. In the DCT frequency domain, a strategy to choose the DCT coefficients where the watermarks are embedded in order to minimize the image distortion and obtain the maximum robustness of the different inserted watermarks is carried out. Whereas in the spatial domain, a method fuzzy c-means clustering based on the image statistical features leading to the image classification into different zones. In these zones, an automatic computing of the gain factor used to embed the watermark based on the Weber's law is also considered. The simulation results proved that the proposed technique is robust against different synchronous and asynchronous attacks such as JPEG compression, different filtering and geometrical transformations. In the watermark detection process we proved that between the embedded watermarks, a

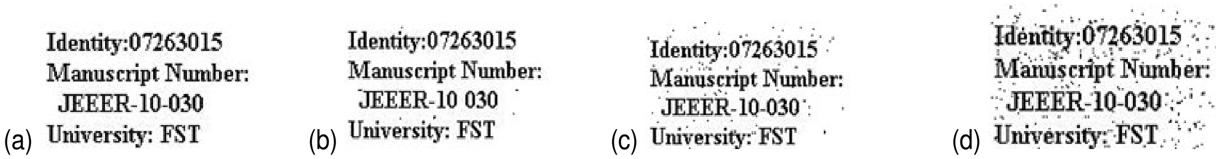

(a)
Identity:07263015
Manuscript Number:
JEEER-10-030
University: FST
(b)
Identity:07263015
Manuscript Number:
JEEER-10 030
University: FST
(c)
Identity:07263015
Manuscript Number:
JEEER-10-030
University: FST
(d)
Identity:07263015
Manuscript Number:
JEEER-10-030
University: FST

Figure 6. Original and extracted watermarks: (a): original (b): JPEG 90% (c): JPEG 50% (d): JPEG 20%.

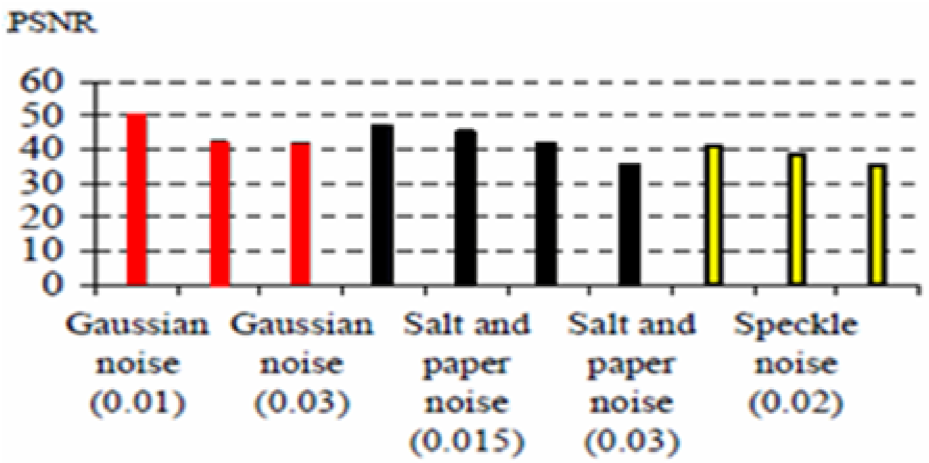
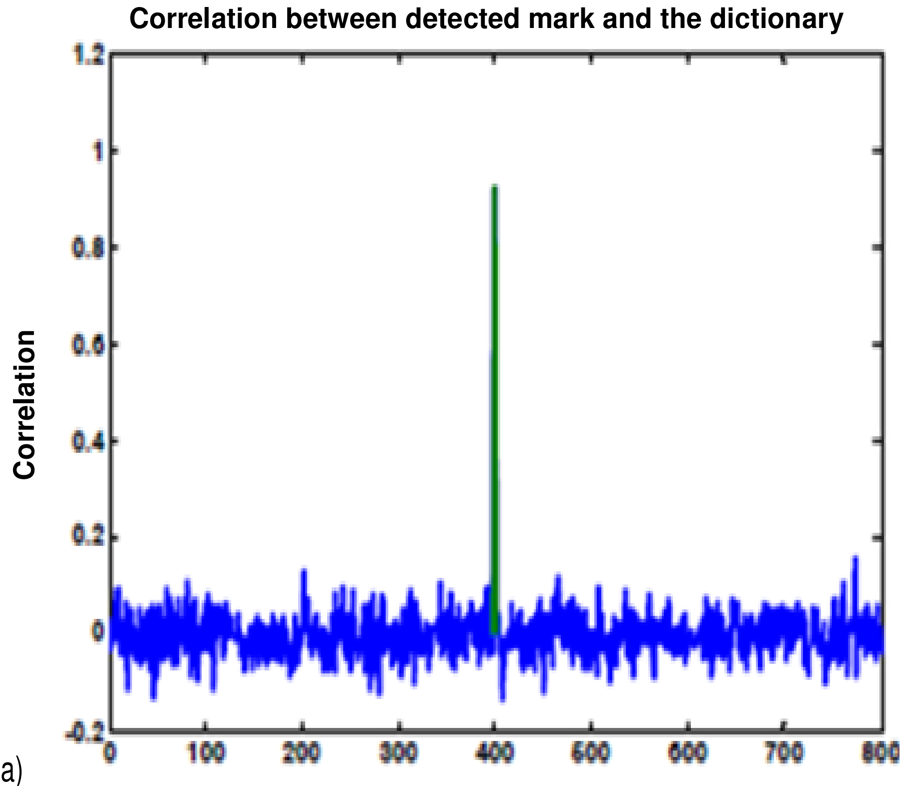
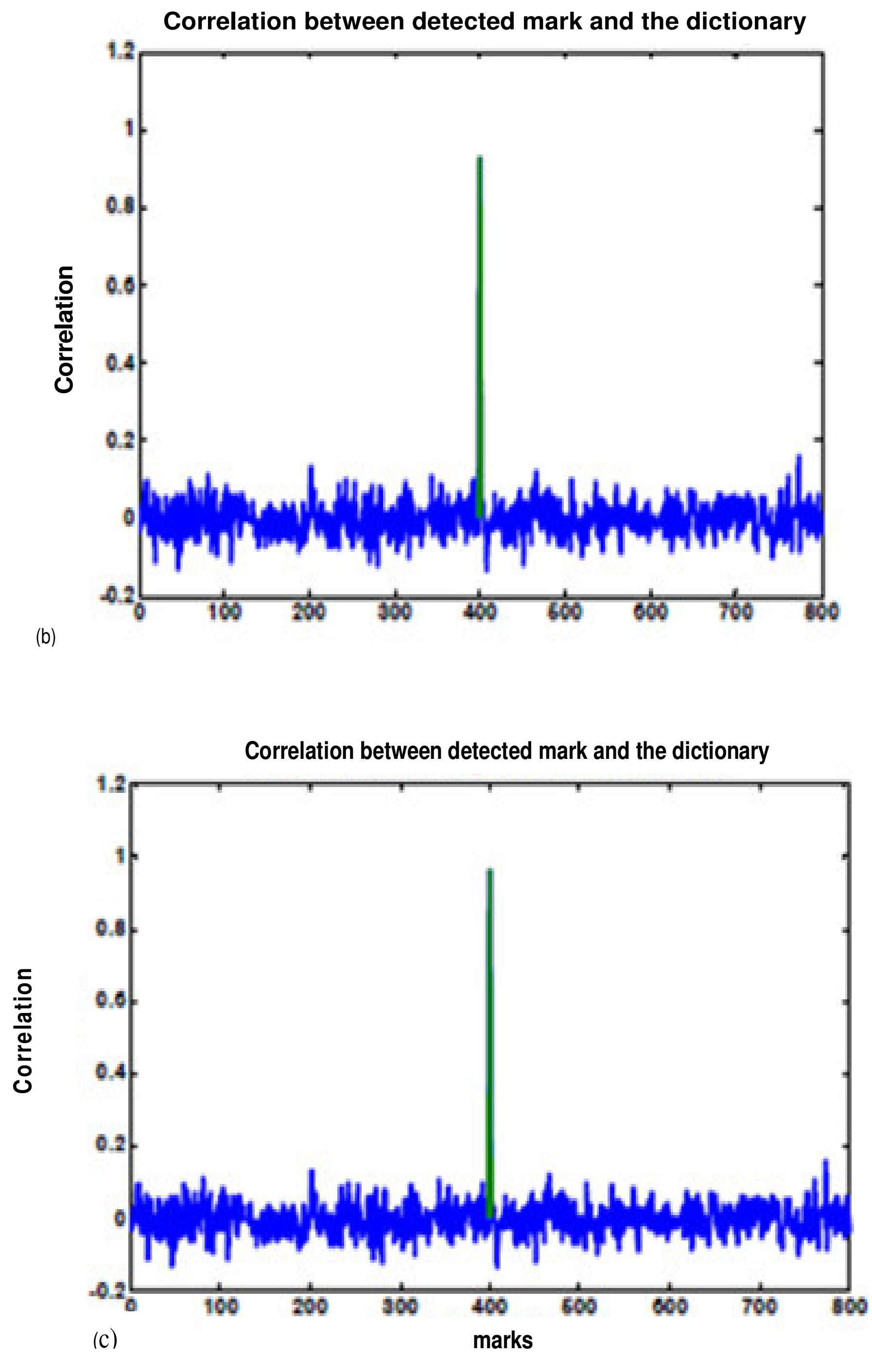


Figure 7. Mean values of PSNR images Watermarked and attacked by different types of noises.



(a)



(b)

(c)

Figure 8. (a) Watermark detector response of attacked by Gaussian noise (0.05), (b) Watermark detector response of attacked by JPEG compression of quality 50, (c) Watermark detector response of attacked by Gaussian filter.

different watermark had survived to a large set of the applied attacks kinds. In addition, the redundancy caused by the multiple insertions has not altered our algorithm robustness. High correlations values after the attacked watermarked image are found in all the applied attacks kinds.

REFERENCES

Anne MAN (2001). Tatouage d'images numériques par parquets d'ondelettes, thesis, Nantes.

Azza OZ (2009). Compression et tatouage d'images à des fins d'archivage et de transmission : application aux images médicales Habilitation University, Tunis El Manar.

Barni M, Bartolini F, Cappellini V, Piva A (1998). A DCT domain system for robust image watermarking, Signal Process., 66(3): 357-372.

Bezdek JC, (1981). Pattern recognition with fuzzy objective function algorithms, Pleunum, New York.

Bezdek JC, Hall LO, Clarke LP (1993). Review of MR image segmentation techniques using pattern recognition. Med. Phys., 20, 1033–1048.

Bruyndonckx O, Quisquater JJ, Macq B (1995). Spatial method for copyright labeling of digital images", IEEE Workshop Non-linear Signal Image Process., Thessaloniki, Greece, pp. 456 - 459.

Chumsamrong W, Thitimajshima P, Rangsanseri Y (2000). Syntetic aperture radar (SAR) image segmentation using a new modified fuzzy c-means algorithm. Proc. Geosci. Remote Sens. Symp., 2: 624–626.

Cox IJ, Kiliani J, Leighton T, Shamoon T (1997). Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process., pp. 1673-1687.

Davoine F , Pateux S (2004). Tatouage de documents audiovisuels numériques, Edition Hermes science, Lavoisier.

Dunn JC (1974). A fuzzy relative of the ISODATA process and its use in detecting compact well separated clusters. J. Cybernet., Vol. 3 : 32-57.

Haralick RM, Shanmugam K, Dinstein (1973). Textural Features for Image Classification, IEEE Trans. Syst., Man Cybernet., 3(6), pp. 610-621.

Hsiang K, Ming-Jang C, Chung-Chih L (1999). Model-Free Functional MRI Analysis Using Kohonen Clustering Neural Networks and Fuzzy C-Means, IEEE Trans. Med. Imaging, 18(12), pp. 1025-1036.

Khaled SA, Nizar AB, Ahmed BH (2009). Segmentation statistique non supervisée des images Code 2D par modèle de Markov Caché, 5th International Conférence of Sciences of Electronic, Technologies of Information and Telecommunications.

Lotfi TL (2009). A Fuzzy Segmentation Approach for Images Application, 5th International Conference of Sciences of Electronic, Technologies of Information and Telecommunications.

Mukherjee DP, Pal P, Das J (1996). Sonar image segmentation using fuzzy c-means. Signal Process., 54(3): 295–302.

Patrick BA (2005). Méthodes de tatouage d'images Fondées sur le contenu. Thesis, Institut National Polytechnique, Grenoble.

Patrick BA, Chassery JM, Macq B (2002). Geometrically invariant watermarking using feature points, IEEE Trans. Image Process., 11(9): 1014-1028.

Patrick BA, Furon T, Cayre F, Doërr G (2007). Practical security analysis of dirty paper trellis watermarking. In Information Hiding: 9th international workshop, Saint-Malo, vol. 4567 of Lecture Notes in Computer Science, Springer Verlag.

Rignot E, Chellappa R, Dubois P (1992). Unsupervised segmentation of polarimetric SAR data using the covariance matrix. IEEE Trans. Geosci. Remote Sens., 30(4): 697–705.

Ruspini EH (1969). A new approach to clustering, Inf. Control, 15(1): 22–32.

Shih FH, Wu FYT (2003). Combinational image watermarking in the spatial and frequency domain, Patt. Recognit., 36(4): 969-975.

Wallace GK (1992). The JPEG still picture compression standard. IEEE Trans. Consumer Electronics, 38(1): 18-34.

Wolfgang R, Delp E (1997). A Watermarking Technique for digital imagery: Further studies, International Conference on Imaging Science, Systems and Technology, Los Vegas, Nevada.

Yang Y, Zheng CH, Lin P (2005). Fuzzy C-means clustering algorithm with a novel penalty term for image segmentation. Opto- Electron. Rev., 13(4).

Ying LI (2003). Texture segmentation based on features in wavelet domain for image retrieval, Visual Communications and Image Processing, Lugano, Switzerland.

Zhao J, Koch E (1995). Towards robust and hidden image copyright labelling. IEEE Workshop on Nonlinear Signal Image Processing.