A New Robust Blind Watermarking Scheme Based on Steerable pyramid and DCT using Pearson product moment correlation

Azz El Arab El Hossaini*, Mohamed El Aroussi*, Khadija Jamali#, Samir Mbarki*, Mohammed Wahbi*

*Deptartment of Computer Science, Faculty of Science, Ibn Tofail University, Kenitra, Morocco
#Department of Electrical Engineering, Ecole Hassania des Travaux Publics, BP 8108 Oasis-Casablanca, Morocco

Abstract—In this paper, we present a new, robust digital watermarking scheme for ownership protection. The scheme is based on Steerable Pyramid (SP) and discrete cosine transform (DCT) using Pearson product moment correlation. During the process of watermark embedding, SP is performed on original host image, and corresponding oriented sub-band is selected to carry the watermark. DCT is applied to each block of size 8x8 of the selected sub-band. Two independent streams representing the watermark are embedded in low and mid-frequency of DCT components. Watermark detection is based on comparison result between Pearson product moment correlations of the two independent streams with each watermarked block. The experimental results demonstrate good visual imperceptibility and resiliency of the proposed scheme against an intentional and un-intentional variety of attacks.

Index Terms—Robust image watermarking, Steerable pyramid, Pearson product moment correlation, discrete cosine transform, Geometric attacks.

I. INTRODUCTION

With the rapid progress of the Internet and the potential problem of illegal distribution of multimedia, there is an urgent need for protecting the copyright of digital content against piracy and malicious manipulation like unauthorized copying, cheap distribution, editing, copyright protection, etc. In order to overcome these problems, digital watermarking has been developed as one of several potential solutions to achieve data security in the digital watermarking technology.

Digital watermarking consists of embedding the owner’s mark called watermark into the protected data so that intellectual property rights can be identified. The watermark should be detectable even if the digital content has been modified by a variety of intentional and unintentional manipulations and attacks. Nowadays, techniques in the field of watermarking grow rapidly; on the other hand, attacks aimed to modify or delete secret information hidden in the host image have become more sophisticated. Signal processing (JPEG compression, median filtering, noise adding, and sharpening, etc.) and geometric attacks (translation, scaling, rotation etc) are the two main categories of these attacks. Common signal processing attacks aim to reduce the watermark energy, while general geometric attacks cause synchronization errors between the original and the embedded watermark, and that may cause a poor extraction of the watermark during the detection process.

Invisibility, robustness, and capacity are the main requirements for image watermarking. Capacity is the amount of information that can be embedded in the host signal. Invisibility means that human eyes should not perceive changes of the host data after the embedding process to maintain a good quality of the watermarked signal. Robustness means that watermark should be able to resist to common attacks (rotation, resizing, cropping, noise, and JPEG compression) even if these attacks are deliberately made [1]. Increasing the intensity of watermark embedding will improve the robustness, but the visual quality of the watermarked signal can be affected. Trade-off between imperceptibility, robustness, and capacity is a challenging problem. Many research works are related to these requirements of a digital watermarking system [2, 3].

Depending on information required for the watermark extraction process, watermarking schemes could be classified into three categories: non-blind, semi-blind, and blind categories. A watermarking scheme that requires original images during watermark recovery is called Non-blind. Semi-blind watermarking needs the watermark information and secret keys to extract the embedded watermark. Finally, a scheme that recovers the watermark without referring to the original image is called blind watermarking. Spatial domain and transform domain techniques are two main categories of watermarking techniques [4] according to the domain in which the watermark is embedded. In the spatial domain techniques [5, 6], the watermark is embedded by directly manipulating the pixel values of the host image. These
techniques are not extensive in time and computation but are more fragile (not robust). On the other hand, in transform domain techniques the watermark is embedded by manipulating the transform coefficients. These techniques are more complex, numerically demanding, and more robust against image processing and geometric attacks. Discrete Fourier Transform (DFT) [7], Discrete Cosine Transform (DCT) [8, 9, 10, 11], Discrete Wavelet Transform (DWT) [12, 13, 14], Redundant Discrete Wavelet Transform (RDWT) [15], Finite Ridgelet Transform (FRIT) [16], Singular Value Decomposition (SVD) [12, 13, 17, 18] are the most popular examples of transforming domain techniques. Recently in the literature, hybrid watermarking schemes have been suggested. These watermarking methods are based on more than one transform domain [12, 17, 19, 20].

Ganic et al. [19] proposed a hybrid watermarking scheme based on DWT and SVD that embed the singular values of the gray scale watermark into the singular values of all sub-bands wavelet transformed host image. Lagzian et al. [15] presented the same watermarking scheme as Ganic et al. [19], the only difference is that they are applying RDWT to cover image instead of DWT. Pun [21] has proposed a watermarking scheme for image copyright protection based on DFT. After decomposing the host image into Fourier domain, DFT coefficients with highest magnitudes are selected except for those in the lowest one. The embedding process inserts the watermark data in these selected DFT coefficients. Similarity measure between the input watermark and the DFT coefficients of the watermarked image is used by the extraction process to detect the watermark. Xia et al. [22] used pseudo-random codes as a watermark to be embedded into the large coefficients at high- and middle-frequency bands of the DWT of an image. The embedding process takes into account perceptual considerations by adjusting the amount of change proportional to the intensity of the coefficient itself. In the extraction process a comparison with the original image is used to detect the embedded watermark. Tsai et al. [23] proposed a watermarking scheme based on feature region selection with two main objectives, robustness against several attacks, and preserving image quality of the watermarked image as much as possible. Experimental results show that the primary feature set is robust to all predefined attacks and its extension can enhance the robustness against undefined attacks. Dawei et al. [24] have developed a new watermarking method for still images in wavelet domain that uses a chaotic map, called logistic map. The image is divided into non-overlapping 8x8 blocks and some of them are selected based on the chaotic logistic map. Wavelet transform is applied locally to these selected blocks, and then the chaotic watermark is embedded into parts of the sub-band coefficients. Correlation between the watermarked coefficients and the watermarking signal is used to extract the embedded watermark. Experimental results of this method show high robustness to geometric attacks, but it is sensitive to common attacks. Tsai et al. [25] proposed a new watermarking technique called SVM-based color image watermarking (SCIW) for the authentication of color images in which a binary data is used as a watermark to be embedded in host image. This technique uses a set of training patterns to train the SVM and then applies the trained SVM to classify a set of testing patterns. By using classifier results, detection of the embedded watermark is achieved without the original image. In [26], the authors proposed a watermarking scheme for copyright protection of digital image in which a visually meaningful gray scale logo is used as a watermark. Transformation in wavelet domain of the host image and the watermark is used for the embedding process, taking into account the consideration of human visual system (HVS) characteristics to select the significant coefficients where the watermark will be embedded. Calculation of the weight factors for wavelet coefficients of the original image is based on the model proposed by Barni et al. [27]. Distortion caused by the different attacks is taken into account for a reliable extraction of the watermark. Kang et al. [28] proposed a watermarking scheme based on DWT and DFT to achieve the robustness to both, affine transform and JPEG compression. In this method, the coefficients of the LL sub-band in the DWT are modified by a spread-spectrum-based informative watermark, while middle-frequency components in the DFT are modified by a template. Zhao et al. [29] proposed an approach for the protection and compression of cultural heritage imagery that uses DCT and DWT as dual domain algorithm. In Niu et al. [30] a method of embedding a gray-level digital watermark into an image is proposed based on DCT. The embedding process decomposes the watermark into a series of binary bit planes. Some of them are used to be embedded into the middle DCT coefficients of the host image, and the rest are used as a secret key. Voyatzis and Pitas [31] first proposed a chaotic watermarking scheme in spatial domain, which embeds a mixed watermark using automorphisms as chaotic 2-D integer vector generators into the host image.

In this paper, a new robust copyright protection scheme based on Steerable Pyramid (SP) and discrete cosine transform (DCT) using Pearson product moment correlation is proposed. The original host image is transformed with SP, and the oriented sub-band is extracted in order to be divided into non-overlapping blocks of size 8x8, to which the DCT is applied. Two independent streams are generated with a key to represent the watermark. One stream represents watermark’s bit 1, and the other represents watermark’s bit 0. Depending on the value of watermark’s bit, a stream is selected to be embedded in low and mid frequency of DCT components. Pearson product moment correlations’ comparison result between the two independent streams and each watermarked block is used to extract the embedded watermark. Experimental results demonstrate good visual imperceptibility and resiliency of the proposed scheme against an intentional and unintentional variety of attacks.

The remaining sections of the paper are organized as follows: Section 2 describes our proposed watermarking
scheme using Pearson product moment correlation, Steerable Pyramid (SP) and discrete cosine transform (DCT), followed by Section 3 where experimental results are presented, and finally Section 5 concludes this paper.

II. PROPOSED METHOD

In this section, the proposed watermarking scheme is described, which consists of a watermark embedding and watermark detection procedures using Pearson product moment correlation, steerable pyramid and discrete cosine transform.

A. Steerable Pyramid Decomposition

DWT is playing an increasingly important role in watermarking due to its good spatial-frequency characteristics, and its wide applications in the image/video coding standards [32]. DWT based watermarking schemes demonstrate a very good performance to common signal processing attacks. However, an important problem with the standard wavelet transform is that it lacks the translation and rotation invariant properties, which are very desirable in watermarking scheme. This problem makes DWT watermarking scheme sensitive to the geometric distortion such as translation and rotation. If the image is rotated, then in the wavelet domain, the wavelet coefficients change completely. In fact, the wavelet coefficients of the rotated image are not just be simply rotated, but are also modified [33]. A way to overcome this problem is to replace the standard wavelet transform with a steerable pyramid transform [34, 35].

![Figure 1](image1.png)

**Figure 1.** 3 scales and 4 orientations steerable pyramid transform.

![Figure 2](image2.png)

**Figure 2.** Tree representations of one-level 2D steerable pyramid transform.

The Steerable pyramid is among multi-resolution algorithms like the contourlet transform, which is a discrete extension of the curvelet transform that aims to capture curves instead of points. The construction of contourlet transform is mainly based on the Laplacian pyramid and the directional filter banks.

The Steerable Pyramid Decomposition is a linear multi-resolution image decomposition method, by which an image is sub-divided into a collection of sub-bands localized at different scales and orientations [34], that provides a useful tool for image processing applications based on combining differential measurements (e.g., differences of neighborhoods) and multi-scale decompositions. The implementation is generally computed recursively using convolution and decimation operations, and possesses the advantage that the sub-bands are translation and rotation-invariant. In steerable pyramid decomposition, the image is preprocessed by a high-pass pre-filter and a low-pass pre-filter, to produce low and high sub-bands. The low-pass sub-band is then divided into a set of oriented band-pass sub-bands and a low-pass sub-band. This procedure is continued recursively by sub-sampling the lower low-pass sub-band by a factor of 2 along the rows and columns. If there are k band-pass filters, then the pyramid is overcomplete by a factor of 4k/3. The structure of the steerable pyramid in the frequency domain is shown in Fig. 1, and an example of 3 scales and 4 orientations steerable pyramid transform, applied to mandrill image is shown in Fig. 2.

Requirement for the recursive multi-scale SP had been evaluated in [36] to achieve the perfect construction, these requirements are defined as:

Unity system response amplitude:

\[
|H_0(\omega)|^2 + |L_0(\omega)|^2 \left( |L_1(\omega)|^2 + \sum_{k=0}^{K-1} |B_k(\omega)|^2 \right) = 1
\]  

(1)

Recursion relationship:

\[
|L_q(\omega)|^2 + \left| L_q(\omega) \right|^2 \left( |L_{q+1}(\omega)|^2 + \sum_{k=0}^{K-1} |B_k(\omega)|^2 \right) = |L_q(\omega)|^2
\]

(2)

Aliasing cancellation

\[
|L_q(\omega)| = \begin{cases} 0, & |\omega| > \frac{\pi}{2} \\ 1, & \text{otherwise} \end{cases}
\]

(3)

Where $\omega$ represent the frequency vector in the Fourier domain, $H_0(\omega)$ indicate the non-oriented high-pass, $L_0(\omega)$ indicate the low-pass filters, $L_1(\omega)$ represent the narrow-band low-pass filter and $B_k(\omega)$ represent the oriented band-pass filter.

And finally to achieve Steerability the following requirement must be satisfied:

\[
|B_k(\omega)| = |B(\omega)| \left| -j\cos(\theta - \theta_k) \right|^{K-1}
\]

(4)

Where $\theta = \text{arg}(\omega), \theta_k = \frac{\pi k}{K}$ and $B(\omega) = \sqrt{\sum_{k=0}^{K-1} |B_k(\omega)|^2}$

(5)
where $\alpha_K = 2^{(k-1)} \frac{(K-1)!}{\sqrt{K(2^K-K-1)!}}$.

**B. Discrete Cosine Transform**

In the literature, DCT-based watermarking schemes are done by applying directly the DCT transform to the entire image, or by segmenting the image to non-overlapping blocks, then applying DCT to each block. Three frequencies are produced with this transformation: low-frequency sub-band, mid-frequency sub-band, and high-frequency sub-band. For a good robustness, the watermark should be embedded into the low-frequency sub-band. On the other hand, this results in a poor quality of the watermarked image, because most of the signal information is concentrated in the low-frequency sub-band which contains the most important visual parts of the image. Embedding the watermark in the high-frequency sub-band results in a good image quality, but the watermark can be removed by attacks like compression and noise addition. For these two reasons, most proposed watermarking schemes embed the watermark in the mid-frequency sub-band, to achieve a balance between imperceptibility and robustness.

The formula of calculating DCT regarding an image block of size NxN pixels is given by equation 12, and inverse DCT is given by equation 13. $A(i, j)$ represents the coefficient at coordinate $(i, j)$ in the DCT-transformed block and $B(x, y)$ represents the intensity of the pixel at coordinate $(x, y)$ in the original block.

$A(i, j) = C(i) \times C(j) \times \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} B(x, y) \cos \left( \frac{(2x+1)i\pi}{2N} \right) \cos \left( \frac{(2y+1)j\pi}{2N} \right) / 2N$  \hspace{1cm} (12)

$B(x, y) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} C(i) \times C(j) \times A(i, j) \times \cos \left( \frac{(2x+1)i\pi}{2N} \right) \cos \left( \frac{(2y+1)j\pi}{2N} \right) / 2N$  \hspace{1cm} (13)

Where $C(i), C(j)$ is given by:

$C(i), C(j) = \begin{cases} \frac{1}{\sqrt{N}} & \text{for } i = 0, j = 0 \\ \frac{1}{\sqrt{N}} & \text{for } i = 1, 2, \ldots, N-1 \\ 0 & \text{otherwise} \end{cases}$  \hspace{1cm} (14)

**C. Pearson Product Moment Correlation**

In this paper, the main idea to extract an embedded watermark is based in the relationship between the embedded and the watermarked signals. The association of two or more variables is often of interest. Researchers are often interested in whether the variables of interest are related, and how strong the association is. Correlation coefficient is one of the descriptive statistical analyzed techniques that are used to study the relationship that may exist between two or more variables, and what the strength of this relationship is [38]. Correlation coefficients reflect a monotone association between variables. Positive or negative signs of the correlation coefficient between two variables X and Y indicate the direction of the relationship. A positive correlation occurs when X and Y vary exactly in the same direction (e.g. when the value of X increases, the value of Y increases, and vice-versa). A negative correlation occurs when X and Y vary exactly in the opposite direction (e.g. when the value of X increases, the value of Y decreases, and vice-versa).
coefficient occurs when X and Y vary inversely (e.g. when the value of X increases, the value of Y decreases, and vice-versa). In the literature, different types of correlation coefficients are used to demonstrate the degree of the relationship between two variables. The most popular correlation coefficients are Pearson product moment correlation, Spearman’s rank-order correlation, and Kendall’s tau correlation. Using the appropriate correlation depends on several criteria, among them the type of data analyzed. For ordinal or interval data, Spearman’s rank-order correlation and Kendall’s tau correlation could be used while Pearson product moment correlation coefficient is appropriate only for interval data. Other criteria propose which correlation could be more adapted for data that incorporate several types of variables [39]. According to the authors in [40], Kendall’s tau correlation is more adapted for data that contains at least one ordinal variable. For the same criteria Spearman’s correlation coefficient is proposed by other authors in [41,42,43]. However, Pearson product moment correlation, Spearman’s rank-order correlation, and Kendall’s tau correlation could be used for interval data [44]. In this paper, we use the Pearson product moment correlation in our watermarking scheme to indicate a predictive relationship that can be exploited in the extraction process. Two independent streams are used to watermark the host image. One stream represents a watermark bit of value 1 and the other represents a watermark bit of value 0. Extraction decision of a watermark bit is based on comparison of relationship strength between the watermarked block and each independent stream. A watermark bit value is considered to be 1 if the strength of the relationship with the first stream is higher than the strength of the relation with the second stream; otherwise the watermark bit value is considered to be 0. The two independent streams were chosen to be independent to reduce the probability of having incorrect extracted watermark bit value, because there is an absence of the relationship between them as shown in the Fig. 4(b). Pearson product moment correlation can be called Pearson’s correlation for short. It was developed by Karl Pearson from a related idea introduced by Francis Galton in the 1880s [45, 46]. It represents the most common measure of correlation, and it is widely used in the sciences as a measure of the strength of linear dependence. Pearson’s correlation is defined as the ratio of the covariance of the two variables to the product of their respective standard deviations, and it is commonly represented by the Greek letter $\rho$ (rho).

$$\rho = \frac{\text{Cov}(X,Y)}{\sigma_x\sigma_y}$$

(15)

When applied to a sample is commonly represented by the letter “r”.

$$r = \frac{\sum_{i=1}^{n} ((x_i - \bar{x})(y_i - \bar{y}))}{\sqrt{\sum_{i=1}^{n} (x_i - \bar{x})^2 \sum_{i=1}^{n} (y_i - \bar{y})^2}}$$

(16)

Where

$$x = \frac{\sum_{i=1}^{n} x_i}{n}; y = \frac{\sum_{i=1}^{n} y_i}{n}$$

(17)

Possible values for the Pearson Correlation are between +1 and -1. A value of +1 demonstrates a perfect positive correlation between variables as shown in Fig. 4 (a), while a value of -1 demonstrates a perfect negative correlation between variables as shown in Fig. 4 (c). A correlation of a value 0 indicates the absence of linear relationship between the variables as shown in Fig. 4 (b).

D. Watermark Embedding

The process of watermark embedding is shown in Fig. 5(a), and the detailed algorithm is given as follows:

- **Step 1.** The host image is transformed into steerable pyramid coefficients using one scale and one orientation.
- **Step 2.** Oriented sub-band is extracted and divided into 8x8 non-overlapping blocks.
- **Step 3.** After performing discrete cosine transform on all the 8x8 blocks, low- and mid- frequencies of DCT components are selected to carry the watermark signal as shown in Fig. 3.
- **Step 4.** Within the 8x8 blocks, a number $R$ of distributed blocks is selected to carry one bit of the watermark.

$$R = \frac{\text{Total number of 8x8 blocks}}{\text{size of the watermark}}$$

(18)

- **Step 5.** Using a key, two independent streams are generated. The first stream represents the watermark bit of value 1 and the second stream represents the watermark bit of value 0.
- **Step 6.** Equation 19 is used to embed the watermark’s bit of value 1 and equation 20 is used to embed the watermark’s bit of value 0.
Figure 5. (a) Block diagram of the proposed watermark embedding; (b) Block diagram of the proposed watermark extraction.

Figure 6. (a) to (d) Host images; (a) Lena; (b) Einstein; (c) Peppers; (d) Pirate; (e) to (h) Watermarked images obtained by the proposed scheme; (e) Lena; (f) Einstein; (g) Peppers; (h) Pirate; (i) Embedded watermark; (j) to (m) Extracted watermark under free attacks; (j) From Lena; (k) From Einstein; (l) From Peppers; (m) From Pirate.

\[ wlm = lm + \alpha \times fs \]  \hspace{1cm} (19)  
\[ wlm = lm + \alpha \times ss \]  \hspace{1cm} (20)

Where \( lm \) represents the selected low- and mid-frequency of DCT components, \( \alpha \) is the watermark strength, \( fs \) is the first stream and \( ss \) is the second stream.

- **Step 7.** Step 6 is repeated on each 8x8 block until the number of 8x8 blocks is reached.
- **Step 8.** Watermarked 8x8 blocks are obtained by applying the inverse discrete cosine transform to each block.
- **Step 9.** Watermarked image is obtained by performing the inverse steerable pyramid transform.

**E. Watermark Extraction**

The process of watermark extraction is shown in Fig. 5(b), and the detailed algorithm is given as follows:

- **Step 1.** The watermarked image is transformed into steerable pyramid coefficients using one scale and one orientation.

- **Step 2.** Oriented sub-band is extracted and divided into 8x8 non overlapping blocks.

- **Step 3.** After performing discrete cosine transform on all the 8x8 blocks, low- and mid-frequencies of DCT components are selected.

- **Step 4.** Using the same key for the embedding process, the two independent streams $f_s$ and $s_s$ are generated.

- **Step 5.** Construct two matrices $f_{Mat}$ and $s_{Mat}$ of the same size as the watermark. The degree of the relation between selected DCT components and the two independent streams is computed using Pearson product moment correlation, and it is stored in the corresponding matrix. Each element of the $f_{Mat}$ and $s_{Mat}$ is calculated as bellow.

$$f_{Mat}(i, j) = \sum_{r=1}^{R} PPMC(lm_r', f_s)$$

$$s_{Mat}(i, j) = \sum_{r=1}^{R} PPMC(lm_r', s_s)$$

(21) (22)

Where $PPMC$ is the Pearson product moment correlation function as described in section II.B. $R$ represents distributed 8x8 blocks as the step 4 in watermark embedding section, and $lm_r'$ is the corresponding low- and mid frequencies of DCT components.

- **Step 6.** Comparison between the two degrees of relation is performed to determine the value of the extracted watermark’s bit. A watermark’s bit value is considered to be 1 if the degree of the relation with the first stream is higher than the degree of the relation with the second stream; otherwise the watermark’s bit value is considered to be 0.

$$\text{watermark}(i, j) = \begin{cases} 1, & \text{if } f_{Mat}(i, j) > s_{Mat}(i, j) \\ 0, & \text{otherwise} \end{cases}$$

(23)

### III. EXPERIMENTAL RESULTS

The proposed watermarking scheme is implemented using MATLAB platform and different-standard gray scale test images, namely Lena, Einstein, Peppers, and Pirate shown in Fig. 6 (a) to (d) of size 512x512 are used as the host images. In our tests we used a binary watermark of size 16x16. We test the proposed algorithm using some necessary parameters to determine optimal configuration values for the proposed watermarking scheme. These tests, namely SP1(1,1), SP2(1,1), SP3(2,1), SP4(2,1), SP5(2,1), are shown in Table 1. Taking into account the visual quality of the watermarked image, the intensity of watermark embedding is chosen where the PSNR value is around 40db. The PSNR values for different tests SP1(1,1), SP2(1,1), SP3(2,1), SP4(2,1) and SP5(2,1) using Lena image are 40.0848, 40.2403, 40.2308, 40.7012 and 40.8731 respectively.

<table>
<thead>
<tr>
<th>test name</th>
<th>Scale</th>
<th>Orientation</th>
<th>alpha</th>
<th>Selected sub-band</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP1(1,1)</td>
<td>1</td>
<td>1</td>
<td>6</td>
<td>High sub-band.</td>
</tr>
<tr>
<td>SP2(1,1)</td>
<td>1</td>
<td>1</td>
<td>7.5</td>
<td>Oriented subband.</td>
</tr>
<tr>
<td>SP3(2,1)</td>
<td>1</td>
<td>2</td>
<td>8</td>
<td>High sub-band.</td>
</tr>
<tr>
<td>SP4(2,1)</td>
<td>1</td>
<td>2</td>
<td>8</td>
<td>The first oriented sub-band</td>
</tr>
<tr>
<td>SP5(2,1)</td>
<td>1</td>
<td>2</td>
<td>8</td>
<td>The second oriented sub-band</td>
</tr>
</tbody>
</table>

![Figure 7. NC results using different parameters and under different attacks to determine optimal configuration: (a) Sharpening; (b) gamma correction (0.05); (c) Histogram equalization; (d) Resize (384x384); (e) Resize (256x256); (f) Resize (192x192); (g) JPEG compression Q=70; (h) JPEG compression Q=50; (i) JPEG compression Q=40; (j) JPEG compression Q=30; (k) JPEG compression Q=25; (m) JPEG compression Q=20; (n) Rotation (angle=10); (o) Rotation (angle=20); (p) Rotation (angle=30); (q) Rotation (angle=40); (r) Rotation (angle=45); (s) Rotation (angle=50); (t) Rotation (angle=60); (u) Rotation (angle=70); (v) Rotation (angle=80).](image-url)
Based on result tests shown in Fig. 8 and Fig. 7, we notice that SP2(1,1) test represents the most optimal configuration values, and its parameters will be used for further tests from now on.

In this work, the quality of the watermarked image is measured using PSNR (Peak Signal to Noise Ratio). By using the proposed watermarking scheme, the tested watermarked images Lena, Einstein, Peppers and Pirate are having PSNR values 40.0848, 39.9183, 39.3452 and 40.0980, respectively. From Fig. 6, it is clear that there is no perceptible degradation between the watermarked images in Fig. 6 (e) to (h) and the original images in Fig. 6 (a) to (d) according to human perception. The PSNR is defined as:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}$$

Where MSE (Mean Square Error) is defined as:

$$MSE = \frac{1}{N} \sum_{i=1}^{N} (I_i - \tilde{I}_i)^2$$

Figure 8. NC results using different parameters and under different attacks to determine optimal configuration: (a) Without any attack; (b) Salt & pepper (density 0.01); (c) Salt & pepper (density 0.05); (d) Salt & pepper (density 0.1); (e) Salt & pepper (density 0.15); (f) Salt & pepper (density 0.2); (g) Speckle noise (var=0.01); (h) Speckle noise (var=0.05); (i) Speckle noise (var=0.1); (j) Speckle noise (var=0.15); (k) Speckle noise (var=0.2); (l) Gaussian noise (density 0.01); (m) Gaussian noise (M = 0, var=0.05); (n) Gaussian noise (M = 0, var=0.1); (o) Gaussian noise (M = 0, var=0.15); (p) Gaussian noise (M = 0, var=0.2); (q) Median filtering (3x3); (r) Median filtering (4x4); (s) Median filtering (5x5); (t) Median filtering (6x6); (u) Wiener filtering (3x3); (v) Wiener filtering (4x4); (w) Wiener filtering (5x5); (x) Wiener filtering (6x6).

Figure 9. watermarked images under attacks: (a) Speckle noise (var=0.05); (b) Pepper & salt noise (density 0.05); (c) Average filter (5x5); (d) Median filtering (5x5); (e) JPEG compression (Q=30); (f) Gamma correction (0.05); (g) Histogram Equalization; (h) Increasing contrast (40%); (i) Decreasing contrast (40%); (j) Resizing (192x192); (k) Cropping 1/2th from the right; (l) Rotation (angle=40).
Where N represents the number of pixels in the original (I) and the watermarked (J) image. Besides the imperceptibility test, the robustness of the proposed watermarking scheme is evaluated by applying various attacks on the tested benchmark images. Table II and Table III show the similarity results between the extracted watermark and the original embedded watermark. This similarity is measured using normalized correlation (NC). The normalized correlation (NC) may take values between 0 (random relationship) to 1 (perfect linear relationship).

\[
NC = \frac{\sum_{i=1}^{M} w_i j_i}{\sqrt{\sum_{i=1}^{M} w_i^2 \sum_{i=1}^{M} j_i^2}}
\]  

(8)

Where M represents the number of pixels in the original (w) and the extracted (j) watermark image.

### TABLE II.
**OBTAINED NC RESULTS AFTER DIFFERENT ATTACKS ON THE PROTECTEDlena, Einstein, Peppers, and Pirate Images***

<table>
<thead>
<tr>
<th>Attacks &amp; salt noise</th>
<th>Pepper</th>
<th>Salt</th>
<th>0%</th>
<th>10%</th>
<th>20%</th>
<th>30%</th>
<th>40%</th>
<th>50%</th>
</tr>
</thead>
<tbody>
<tr>
<td>density=0.01</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
</tr>
<tr>
<td>density=0.02</td>
<td>1.000</td>
<td>0.997</td>
<td>0.997</td>
<td>0.997</td>
<td>0.997</td>
<td>0.997</td>
<td>0.997</td>
<td>0.997</td>
</tr>
<tr>
<td>density=0.05</td>
<td>0.976</td>
<td>0.962</td>
<td>0.962</td>
<td>0.962</td>
<td>0.962</td>
<td>0.962</td>
<td>0.962</td>
<td>0.962</td>
</tr>
<tr>
<td>density=0.08</td>
<td>0.890</td>
<td>0.918</td>
<td>0.940</td>
<td>0.919</td>
<td>0.919</td>
<td>0.919</td>
<td>0.919</td>
<td>0.919</td>
</tr>
</tbody>
</table>

### TABLE III.
**OBTAINED NC RESULTS AFTER DIFFERENT ATTACKS ON THE PROTECTED Lena, Einstein, Peppers, and Pirate Images***

<table>
<thead>
<tr>
<th>Increasing brightness</th>
<th>Q=80</th>
<th>Q=70</th>
<th>Q=60</th>
<th>Q=50</th>
<th>Q=40</th>
<th>Q=30</th>
<th>Q=25</th>
<th>Q=20</th>
<th>Q=10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increasing contrast</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
</tr>
<tr>
<td>1%</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
</tr>
<tr>
<td>2%</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
</tr>
<tr>
<td>3%</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
</tr>
<tr>
<td>4%</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
</tr>
</tbody>
</table>

© 2014 ACADEMY PUBLISHER
As shown in Fig. 6 (i) to (m), the extracted watermark under free attacks is 100% identical to the embedded watermark, while under some attacks it is still very recognized. We have also shown some watermarked Lena images that were affected by some attacks in Fig. 9.

Geometric and non-geometric attacks were considered in Table II and Table III, where 86 attacks were applied to each tested image (Lena, Einstein, Peppers, and Pirate) to verify the robustness of the proposed method. These attacks include JPEG compression, Pepper & salt noise, Speckle noise, Gaussian noise, Average filtering, Median filtering, Weiner filtering, Gamma correction, Histogram Equalization, Sharpening, Increasing contrast, Decreasing contrast, Increasing brightness, Decreasing brightness, Resizing, Rotation and Cropping. NC results in Table II and Table III, demonstrate the robustness of the proposed watermarking scheme against a variety of attacks, despite the watermarked image being seriously distorted.

### A. Geometric attacks

In this experiment, the watermarked images are cropped, rotated with an angle degree from 5 to 80 and

![Image of watermarked images](image_url)

**Figure 10.** Extracted watermark under attacks: (a) Speckle noise (var=0.01); (b) Speckle noise (var=0.05); (c) Pepper & salt noise (density 0.01); (d) Pepper & salt noise (density 0.05); (e) Average filtering (3x3); (f) Average filtering (5x5); (g) Median filtering (3x3); (h) Median filtering (5x5); (i) Weiner filtering (3x3); (j) Weiner filtering (5x5); (k) Gamma correction (0.7); (l) Gamma correction (0.05); (m) Increasing contrast (50%); (n) Decreasing contrast (20%); (o) Increasing brightness (50%); (p) Decreasing brightness (50%); (q) Resize (192x192); (r) Resize (256x256); (s) JPEG compression (Q=30); (t) JPEG compression (Q=40); (u) JPEG compression (Q=50); (v) Cropping 1/2th from the right; (w) Cropping 1/2th from the top; (x) Rotation (angle=10); (y) Rotation (angle=40); (z) Rotation (angle=45).

### TABLE IV.

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Proposed scheme</th>
<th>Wang et al. [47]</th>
<th>Run et al. [48]</th>
<th>Agarwal et al. [49]</th>
<th>Ranjbar et al. [50]</th>
<th>Horng et al. [51]</th>
</tr>
</thead>
<tbody>
<tr>
<td>JPEG compression (Q=90)</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>JPEG compression (Q=80)</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>JPEG compression (Q=70)</td>
<td>1.0000</td>
<td>0.99</td>
<td>0.99</td>
<td>1.0000</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>JPEG compression (Q=60)</td>
<td>1.0000</td>
<td>0.99</td>
<td>0.99</td>
<td>1.0000</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>JPEG compression (Q=50)</td>
<td>1.0000</td>
<td>0.99</td>
<td>0.99</td>
<td>1.0000</td>
<td>-</td>
<td>0.7041</td>
</tr>
<tr>
<td>JPEG compression (Q=40)</td>
<td>1.0000</td>
<td>0.97</td>
<td>0.93</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>JPEG compression (Q=30)</td>
<td>0.9922</td>
<td>0.90</td>
<td>0.85</td>
<td>-</td>
<td>-</td>
<td>0.7215</td>
</tr>
<tr>
<td>JPEG compression (Q=25)</td>
<td>0.9500</td>
<td>0.87</td>
<td>0.77</td>
<td>-</td>
<td>0.9914</td>
<td>-</td>
</tr>
<tr>
<td>JPEG compression (Q=20)</td>
<td>0.8911</td>
<td>0.74</td>
<td>0.68</td>
<td>-</td>
<td>0.7309</td>
<td>-</td>
</tr>
<tr>
<td>JPEG compression (Q=10)</td>
<td>0.7636</td>
<td>0.41</td>
<td>0.32</td>
<td>0.8455</td>
<td>-</td>
<td>0.7240</td>
</tr>
<tr>
<td>Median filtering (3x3)</td>
<td>1.0000</td>
<td>0.95</td>
<td>0.93</td>
<td>0.9013</td>
<td>0.531</td>
<td>0.6706</td>
</tr>
<tr>
<td>Median filtering (5x5)</td>
<td>0.9948</td>
<td>0.86</td>
<td>0.84</td>
<td>0.8798</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Average filtering (3x3)</td>
<td>1.0000</td>
<td>0.97</td>
<td>0.95</td>
<td>-</td>
<td>-</td>
<td>0.7571</td>
</tr>
<tr>
<td>Average filtering (5x5)</td>
<td>0.9747</td>
<td>0.86</td>
<td>0.80</td>
<td>-</td>
<td>-</td>
<td>0.7043</td>
</tr>
<tr>
<td>Weiner filtering (3x3)</td>
<td>1.0000</td>
<td>-</td>
<td>-</td>
<td>0.934</td>
<td>0.972</td>
<td>-</td>
</tr>
<tr>
<td>Weiner filtering (5x5)</td>
<td>1.0000</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Histogram Equalization</td>
<td>1.0000</td>
<td>0.82</td>
<td>0.86</td>
<td>0.9858</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Sharpening</td>
<td>1.0000</td>
<td>0.99</td>
<td>-</td>
<td>1.0000</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Resizing (256x256)</td>
<td>1.0000</td>
<td>0.91</td>
<td>0.86</td>
<td>1.0000</td>
<td>1.0000</td>
<td>0.7655</td>
</tr>
<tr>
<td>Cropping 1/4</td>
<td>1.0000</td>
<td>0.76</td>
<td>0.68</td>
<td>0.7554</td>
<td>0.9908</td>
<td>0.7364</td>
</tr>
<tr>
<td>Speckle noise (var=0.01)</td>
<td>1.0000</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0.971</td>
<td>-</td>
</tr>
<tr>
<td>Salt &amp; Pepper noise (density=0.01)</td>
<td>1.0000</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0.869</td>
<td>0.5674</td>
</tr>
<tr>
<td>Gaussian noise (M=0,var=0.001)</td>
<td>1.0000</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0.985</td>
<td>-</td>
</tr>
<tr>
<td>Gaussian noise (M=0,var=0.01)</td>
<td>0.9629</td>
<td>0.94</td>
<td>0.89</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Gaussian noise (M=0,var=0.02)</td>
<td>0.9160</td>
<td>0.70</td>
<td>0.52</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Gaussian noise (M=0,var=0.03)</td>
<td>0.8814</td>
<td>0.51</td>
<td>0.39</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Rotation (angle=0.25)</td>
<td>1.0000</td>
<td>0.75</td>
<td>0.65</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Rotation (angle=0.25)</td>
<td>1.0000</td>
<td>0.74</td>
<td>0.70</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Rotation (angle=0.3)</td>
<td>1.0000</td>
<td>0.68</td>
<td>0.58</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Rotation (angle=0.3)</td>
<td>1.0000</td>
<td>0.70</td>
<td>0.65</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Rotation (angle=180)</td>
<td>1.0000</td>
<td>-</td>
<td>-</td>
<td>0.934</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

The bold values indicate the best values comparing with the others.

© 2014 ACADEMY PUBLISHER
finally resized to 384x384, 256x256 and 192x192 as shown in Table III. Attacked Lena image by resizing (192x192), cropping 1/2th from the right and rotation (angle=40) are shown in Fig. 9 (j) to (l), respectively. Samples of extracted watermarks after applying geometric attacks are shown in Fig. 10 (q) to (z). From these results, the extracted watermarks are identified at a single glance and this demonstrates the effectiveness of the proposed scheme against geometric attacks.

B. JPEG Compression

JPEG Compression is a commonly used method to compress digital content, allowing a selectable trade-off between storage size and image quality. In our test against jpeg compression, the watermarked image is attacked by a lossy compression. It means that the quality of the watermarked image could be affected, because some information will be lost and cannot be restored when the image is uncompressed. In Table III, different quality factors ranging in the range [10, 80] are used to test the performance of the proposed watermarking scheme. A high value of quality factor indicates low compression and vice versa. Compressed Lena image by quality factor of 30 is shown in Fig. 9(e), and extracted watermarks for different quality factor from 30 to 50 are shown in Fig. 10(s) to (u). Experimental results in Table III demonstrate that the proposed watermarking scheme can resist JPEG compression, even at a very low quality factor.

C. Noise attacks

To test the robustness against additive noise, watermarked images are attacked by zero mean Gaussian, Pepper & salt and speckle noises of different variances from 0.01 to 0.1. NC values of extracted watermarks from different attacked images are shown in Table II, and some extracted watermarks are shown in Fig. 10 (a) to (d). From Table II and Fig. 9 (a) to (d), we can see that the proposed scheme is resistant to noise attacks.

D. Filtering and enhancement attacks

Various types of filtering and enhancement techniques including average filtering, median filtering, wiener filtering, un-sharp filtering, histogram equalization, increasing/decreasing contrast and brightness, and gamma correction are used to assess the robustness of the proposed method. Some distorted Lena images by these attacks are shown in Fig. 9 and their extracted watermarks are given in Fig. 10 (a) to (p). Detailed results are given in Table II and III. As we can see from these results, the proposed watermarking scheme demonstrates an excellent robustness against all the mentioned attacks, even if the watermarked image being seriously distorted.

E. Comparison results with other related schemes.

In order to assess the efficiency of the proposed watermarking scheme, five recently related watermarking schemes are incorporated for the comparison including Wang et al. [47], Run et al. [48], Agarwal et al. [49], Ranjbar et al. [50] and Horng et al. [51]. The first comparison is done based on the quality of the resulting watermarked image. The PSNR values reported by other schemes are given in Table V, in which the PSNR value of Wang et al. [47] and Run et al. [48] is better than us. But we have to mention that the obtained PSNR value (40dB) in our proposed watermarking scheme is considered to be very good. From Fig. 6 we can see that there is no difference between each original image and its watermarked version based on the human visual system.

The second comparison considers the robustness against various attacks. As shown in Table IV, a comparison is done based on 30 attacks with different parameters. These attacks are JPEG compression, Median filtering, Average filtering, Weiner filtering, Histogram Equalization, Sharpening, Resizing, Cropping, Speckle noise, Pepper & salt noise, Gaussian noise and Rotation. Table IV demonstrates that the robustness of the proposed algorithm is far better and proves superiority over the other existing algorithms.

IV. CONCLUSION

In this paper, a robust blind watermarking scheme based on SP and DCT using Pearson product moment correlation is proposed. Our experimental results showed that the proposed scheme is robust against geometric and non-geometric attacks. Comparison with some recent previous schemes demonstrates the effectiveness of the proposed scheme. In addition to robustness, our scheme achieves a good imperceptibility where human eyes cannot perceive changes of the resulting image after the embedding process.

REFERENCES


J. Portilla, E. P. Simoncelli, A parametric texture model based on joint statistics of complex wavelet coefficients,
Azz el arab El hossaini: currently he is a PhD student at the Faculty of Science, Ibn Tofail University. He received a Master’s degree in Network and System Administration from the same faculty. He received his Bachelor’s degree in administration of Computer Park from Faculty of Sciences Mohamed V-Agdal, Rabat. His research interest includes watermarking technologies, fingerprinting and data authentication.

Mohamed El aroussi: has obtained his PHD degree in computer science and telecommunication from the Faculty of Sciences, University Mohamed V-Agdal, Rabat, Morocco, 2009. Since then he has worked in different projects in the field of WSN Biometric embedded systems. He is the author of several articles published in reputed journals.

Khadija Jamali: she received her Bachelor’s degree in java and c++ development, she received a Master’s degree in Network and System Administration and she is a Phd student at the Faculty of Science, Ibn Tofail University, Kenitra, Morocco. Her interest is watermarking technologies.

Samir Mbarki: received the B.S. degree in applied mathematics from Mohammed V University, Morocco, 1992, and Doctorat of High Graduate Studies degrees in Computer Sciences from Mohammed V University, Morocco, 1997. In 1995 he joined the faculty of science Ibn Tofail University, Morocco where he is currently a Professor in Department of computer science. His research interests include software engineering, model driven architecture, software metrics and software tests. He obtained an HDR in computer Science from Ibn Tofail University in 2010.

Mohamed Wabbi obtained the diploma of engineer and the Ph.D. from ENSEEINT - INP Toulouse in May 1983 and the Docteur Es-Science diploma in December 1986 from the same institution. He is since Professor in the EHTP engineering school. He is the head of its Electrical Engineering and Telecommunications department and the SIR2C2S/LaGeS-EHTP research team. His research interests relate to Physics Electronics & Optoelectronics. He is author of a large number of regular and invited papers in international conferences and journals.