A New Robust and Blind Image Watermarking Scheme In Frequency Domain Based On Optimal Blocks Selection

Nesrine Tarhouni
REsearch Groups in Intelligent Machines, National Engineering School of Sfax
Sfax, 3038, Tunisia
nesrine.tarhouni@enis.tn

Maha Charfeddine
REsearch Groups in Intelligent Machines, National Engineering School of Sfax
Sfax, 3038, Tunisia
maha.charfeddine@enis.tn

Chokri Ben Amar
REsearch Groups in Intelligent Machines, National Engineering School of Sfax
Sfax, 3038, Tunisia
chokri.benamar@enis.tn

ABSTRACT
Image, audio and video are the first media affected by hacking due to the availability of the internet and to the high speed connection. One of the solutions to solve such problems is watermarking. Digital watermarking is the process of embedding an imperceptible and a robust signature into a digital signal. In this paper, we focus on image watermarking. We have embedded the watermark in the frequency domain using Discrete Cosine Transform. The choice of the blocks where we insert the watermark bits depends on a preprocessing study on the original and compressed-decompressed image. Then we have implemented a blind detection algorithm. We tried to enhance the security of our technique by applying an Arnold transform to the embedded watermark. Finally, we have tested the robustness of our method by applying many attacks to the watermarked images using Stirmark 3.1. The results demonstrate that our method yields a high level of imperceptibility and robustness against JPEG compression, unique and double Stirmark attacks.

Keywords
Image watermarking, Discrete Cosine Transform, Arnold.

1 INTRODUCTION
The appearance of digital data is a recent revolution in the world of signal processing. Indeed, switching from analogue to digital has made handling more convenient. The transmission is faster, the storage more economical, the indexing more efficient and the copying easier.

Certainly, simplifying the access to the identical copy has facilitated hacking. Image, audio and video are the first media affected by this serious problem, as such data can be tampered and used without authorization, can be copied with preserving the image quality and with unlimited number of copies.

Several researchers have tried different methods to prevent or at least slow down the copying of these multimedia data. For example, steganography, which aims to hide a message into a data in such a way that an eavesdropper cannot detect the presence of the message [Pooj15]. Also, the cryptography, which attempts to protect the content by making it unreadable and the output is inexplicable without the knowledge of the key [Sur17]. Besides, the digital watermarking is the technique of hiding information into a digital content (image, audio, video, etc) to protect it from dishonest manipulations. In contrast to steganography and cryptography, the watermarked data are available, exploitable and the presence of the hidden message is known [Man16].

Digital watermarking was proposed for many applications: Tracing traitors, content authentication, indexing and event detection from video sequences and essentially for copyright protection [Fch15] [Nam17] [Bou11] [Ali10].

The techniques of digital watermarking have particular characteristics regarding to the given application. Therefore, the watermarking systems don’t follow the same properties. Generally, there are three important features that are usually treated in the most applications:

Imperceptibility: This property is related to the insertion scheme where the embedded watermark not degrade the media quality. The watermarks do not create visible artifacts in images and also don’t alter the bit rate of the video or introduce audible noises in audio signals [Wke15].

Robustness: It means the resistance of the digital
watermarking technique against changes made to the watermarked media. It depends on the application, if the watermarking is used for copyright protection, then the watermark has to be available after different modifications. The watermarks should not get destroyed as a result of unintentional or malevolent distortions like cropping, resampling, rotation, scaling and compression. On the other hand, if it is used for content authentication, the watermarks get disappeared whenever the content is modified so that the loss of integrity of document must be detected [Hai13].

**Capacity:** The capacity of insertion represents the quantity of information inserted in the content. More the capacity is low more the imperceptibility and robustness are relevant [Son16].

The digital watermarking scheme consists of two steps: the embedding process and the detection process. The techniques according to the embedding domain are classified into two categories: insertion domain without transformation and with transformation where we hide the watermark in the frequency domain [Mas10] or the multiresolution one [Mel11]. An example for the first class, in [Sra17] which proposed a watermarking approach in spatial domain based on LSB. Color watermark is composed of three different binary watermarks. The composite color watermark is embedded by substituting the least significant bit of the intensity values of the cover image. Its detection scheme is blind. For the second class, [Moh16] focused on image watermarking in YCoCg-R color space. In the proposed method, DCT is applied to Y of the host image and each bit of watermarks is embedded in three different blocks. Also, Arnold transformation is used to scramble Y and the watermark. The authors in [Lam15], proposed a semi blind approach based on DCT and linear interpolation to protect and authenticate the source such as quran text image. The RGB image is transformed to YUV then, applying DCT and quantification to each 8*8 block of the original image and the watermark. Finally, generating the watermarked image by applying the linear interpolation equation. The watermark could be detected in most cases under various types of attacks when the parameter t of the equation was set near to one. PSNR value is over than 34 dB while SSIM, VIF and UQI values are close to 1, and the NQM exceeds 30 dB. [Ssh14] proposed a method for authentication and copyright protection, the authors applied DWT and SVD to the low frequency subband LL of both cover and watermark images. Then, they embedded the singular values of the watermark image in singular values of the host image. The detection scheme uses the cover image to extract the watermark. In this paper, a blind and robust image watermarking scheme resistant against many different types of attacks such geometric distortions, common signal processing and JPEG compression.

The main contributions include:
1. The spatial domain based on LSB provides low degradation of image quality and important capacity but it is not robust. Hence, we decided to substitute the watermark in the LSB but in the frequency domain.
2. The choice of the suitable blocks to insert the watermark bits depends on a preprocessing study on the original and compressed-decompressed image.
3. The watermark is scrambled using Arnold transformation to ameliorate the security level.
4. The detection of the watermark is directly from the attacked image.
5. Our method resists to double attacks of Stirmark.

## 2 Preliminaries

### 2.1 YCbCr color space

YCbCr is the well known space used for video and digital photography system, where Y is the luminance component, Cb and Cr are respectively the blue-difference and red-difference components. The transformation from RGB space to YCbCr is in the equation (1) and the conversion from YCbCr to RGB is done by using the formula (2) [Sub17].

$$
\begin{align*}
Y &= 0.2989 \times R + 0.5866 \times G + 0.1145 \times B \\
Cb &= -0.1688 \times R - 0.3312 \times G + 0.5 \times B \\
Cr &= 0.5000 \times R - 0.1181 \times G - 0.0816 \times B \\
R &= 1.0 \times Y + 0.0 \timesCb + 1.403 \times Cr \\
G &= -0.1688 \times Y - 0.3312 \times G + 0.5 \times B \\
B &= 0.5000 \times Y - 0.1181 \times G - 0.0816 \times B
\end{align*}
$$

(1)

(2)

### 2.2 DCT and IDCT transforms

The DCT transform is used in this work, in order to convert the original signal from spatial domain to frequency domain. For the original image f(x, y), DCT transform could be shown as follows:

$$
F(u,v) = c(u)c(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \times \cos\left(\frac{\pi u (2x + 1)}{2M}\right) \cos\left(\frac{\pi v (2y + 1)}{2N}\right)
$$

(3)

Here M and N are the rows and columns. The c(u) and c(v) could be shown as follows:

$$
c(u), c(v) = \begin{cases} 
1/v^2 & \text{si } u, v = 0 \\
1 & \text{si } otherwise
\end{cases}
$$

(4)

The inverse of DCT is IDCT, is used to convert the signal from the frequency domain to the spatial domain.

$$
f(x,y) = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} c(u) \times c(v) F(u,v) \times \cos\left(\frac{\pi u (x + \frac{1}{2})}{2M}\right) \cos\left(\frac{\pi v (y + \frac{1}{2})}{2N}\right)
$$

(5)
With images, most of the energy prevails in low frequency. While the high frequency can be neglected as it results in little visible distortion such as JPEG compression.

2.3 Arnold transform

One of the purposes of our method is to improve the security level by scrambling the watermark. One such scrambling technique is the Arnold transformation. The specificity of this transformation is that the image will not be affected after certain iterations. The number of iteration is called also 'Arnold period'. The Arnold Transform of the image is as follows:

\[
\begin{bmatrix}
 x' \\
 y'
\end{bmatrix} = \begin{bmatrix}
 1 & 1 \\
 1 & 2
\end{bmatrix} \begin{bmatrix}
 x \\
 y
\end{bmatrix} \pmod{N}
\]  

3 THE PROPOSED IMAGE WATERMARKING SCHEME

The proposed image watermarking technique consists of three parts: the embedding process, the application of Stirmark attacks and extracting the watermark. These parts are depicted in Figure 1.

![Figure 1: The flow chart of the watermarking approach](image)

3.1 DCT-LSB-Arnold watermark embedding algorithm

In this section, we clarify in details the inserting steps of the watermark and these steps are described in figure 3.

**Step1**: Reading the watermark, transform it to binary image and scramble it by Arnold transform eight times. This number is related to the image size and based on experimental results.

**Step2**: Loading the host RGB image.

**Step3**: Converting the RGB image to YCbCr color space. YCbCr is chosen because its components offer minimum correlations [Aro15]. The YCbCr color space is used in the JPEG standard, therefore, the use of this color space allows us to improve the robustness results.

**Step4**: Separating the Y, Cb and Cr components and Choosing the 'Y' component and eliciting matrix whose size is M*M, Y is chosen because it is tolerant to the well-known attack JPEG compression.

**Step5**: Splitting Y into 8x8 blocks so that we have a total of (M*M)/64 blocks.

**Step6**: All pixels of the blocks are subtracted by 128 then transformed into frequency domain using DCT transform, then quantized and scanned by applying zigzag to all 64 DCT coefficients.

**Step7**: Selecting the middle band frequency coefficients to embed the watermark for the following reasons: Embedding in the low frequency will affect the visual quality of the image because the most energy is situated there. So, the requirement for imperceptibility will not be reached. Besides, the high band frequency is the most easily removed region after applying lossy compression, low pass filter and image noise. So choosing that band won’t meet the robustness requirement. Therefore, middle band frequency is chosen to embed the mark as long as it usually provides good imperceptibility and robustness results in different watermarking schemes with several data (audio, images) [Mah12].

The previous steps are inspired from the algorithm of the JPEG standard. We adopt this idea to assure that our watermarking technique will be robust to JPEG compression attack directly without operating a decompression phase before the extraction process is triggered, which makes our approach original comparing with others [Job17].

**Step8**: Studying and selecting the suitable blocks assuring the best robustness and imperceptibility. The blocks are selected after performing a treatment algorithm. These blocks are the key of our algorithm. The steps of this pre-treatment are explained in figure 2.

The preprocessing consists in computing the step 1 to 6 on both the original and compressed-decompressed image. Then, we subtract the middle band of compressed image from the middle band of the original and we select the blocks corresponding to the minimum values. These blocks are the key of our watermarking scheme.

**Step9**: Inserting the watermark in the LSB of the middle band frequency of the chosen coefficients of the calculated blocks.

In our approach, LSB of these coefficients are substituted by the bits of the watermark after applying Arnold transform.

**Step10**: Running zigzag inverse, then IDCT to each block to obtain the block data containing the watermark information in the spatial domain.

**Step11**: Repeating steps 5 to 12 to 'Cb' component. In
addition to Y, Cb is selected to resist to the cropping attack.

3.2 DCT-LSB-Arnold watermark extracting

The proposed watermarking scheme is a blind approach since the watermark detection doesn’t need the original image. The extraction process is depicted in figure 4 and described as below:

Step1: Loading the watermarked RGB image.

Step2: Converting the RGB image to YCbCr color space and separating the Y, Cb and Cr components.

Step3: Choosing the ‘Y’ component.

Step4: Splitting Y into blocks of 8*8 pixels.

Step5: Each block pixel is subtracted by 128 then transformed into frequency domain using DCT, then quantized and finally scanned by applying zigzag to all 64 DCT coefficients.

Step6: Selecting the middle band frequency coefficients.

Step7: Performing the extraction operation using the same key as in the insertion step which is the chosen blocks after pre-treatment.

Step8: Combining the extracted bits together.

Step9: Running the Arnold inverse to obtain the watermark.

Step10: Repeating steps 5 to 9 to ‘Cb’ component.

4 EXPERIMENTAL RESULTS

For test evaluation purpose, the experiments are tested on 512x512 standard color images and on 816*1261 Quranic images, available respectively in [LIG17] and [Rea17]. We present some of these images in figure 5.
4.1 Evaluation metrics

The performance of the proposed watermarking scheme is examined and analyzed with three metrics. These metrics are used with reference to the most important requirements of the digital image watermarking: imperceptibility and robustness. The first metric is peak Signal to Noise Rate (PSNR) which is used to measure the quality of the watermarked image with regard to the original one [Nam17]. PSNR in decibels (dB) is given by the following equations:

$$\text{PSNR} = 10 \times \log_{10}(L \times \frac{L}{\text{MSE}})$$

In which L is the peak signal amount in the host image and MSE is the mean square error. To distinguish host and watermarked image is usually hard for the human eye. In general, acceptable PSNR values > 36dB [Wke15].

According to (8), the normalized correlation (NC) is used to check the similarity between the original and the extracted watermark bits [Nam17]:

$$\text{NC} = \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} W(i,j)W'(i,j)}{\sqrt{\sum_{i=1}^{N} \sum_{j=1}^{N} W(i,j)^2} \sqrt{\sum_{i=1}^{N} \sum_{j=1}^{N} W'(i,j)^2}}$$

In which W (i,j) and W’(i,j) are original and extracted watermark respectively. The original and extracted watermark are similar when NC> 0.75 [Wke15].

According to (9), the bit error ratio (BER) is the ratio showing how many bits are received in error over the number of the total bits received. It is calculated by comparing bit values of both the embedded and the extracted watermark [Nam17].

$$\text{BER} = \frac{\sum_{i=1}^{n} \sum_{j=1}^{m} W(i,j) \oplus W'(i,j)}{m \times n}$$

In which W and W’ are original and extracted watermark image respectively, with size of n* m and \(\oplus\) means xor operation.

4.2 Imperceptibility results

To test the imperceptibility of our approach we calculate the PSNR. The results of the proposed watermarking scheme for different images are listed in Figure 5. It can be seen from the PSNR values which are over 36 db that the watermarked images have a good quality.

4.3 Robustness results

A robust watermarking algorithm should resist to different signal distortions and attacks.

To evaluate the performance of the proposed watermark detector against signal manipulations and degradations, we used Stirmark bench 3.1 [Mku] and we calculate the NC and BER values after detection step.

4.3.1 Robustness against JPEG compression

Table 1 shows experimental results from JPEG attacks of Stirmark to the watermarked images ‘Lena’, ‘Baboon’, ‘Peppers’ and to the Quranic images ‘529’, ‘533’, ‘534’. These images are in ‘.ppm’ format before applying JPEG compression. As shown, our method resists to JPEG attack for rates from 15 to 90. In fact, the NC values are between 0.98 and 1 and the BER values are between 0.01 and 0.

We detect the watermark directly from the compressed images without decompressing them contrary to other techniques which decompress the images before detection [Sra17]. This fact is an important advantage that highlights the originality of our approach.

4.3.2 Robustness against unique attacks of Stirmark

The watermarked images are in ppm formats, the Stirmark generates attacked images in ppm and jpeg formats. The ones with ppm are the unique attacks of Stirmark.

Figure 8 exhibits the values of the NC of the attacked images obtained after applying geometric and combined distortions, the attacked images are ‘Lena.ppm’, ‘Baboon.ppm’ and ‘Peppers.ppm’ and the Quranic image5 which are ‘529.ppm’, ‘533.ppm’, ‘534.ppm’.
Analyzing the results in Figure 8 we show that our method is robust against several geometric distortions including scaling from 0.5 to 2, symmetric and asymmetric line and column removal, shearing, cropping attack with 1% and 2% and common signal processing including median filter and gaussian filter. In all cases we have obtained NC values greater than the predefined threshold value $T_{NC} = 0.75$ [Man15] and we detect the watermark without managing to ameliorate the attacked images unlike with other methods [Sra17].

Table 2 confirms the results shown Figure 8, all the values of $T_{BER} = 0.2$ [Wke15].

4.3.3 Robustness against double attacks of Stirmark

In addition to unique attacks, we evaluate our algorithm against double attacks. Stirmark Bench combines the distortions with JPEG compression which is known that is very destructive. This brand of combination called double attacks. In table 3, we present the results of our approach against scaling from 0.5 to 2, symmetric and asymmetric line and column removal, common signal processing including median filter, gaussian filter and Frequency mode Laplacian removal (FMLR).

Our proposed scheme successfully resists to double attacks, the highest value of BER values is equal to $T_{BER} = 0.2$ and we extract the watermark from the attacked image in JPEG format without decompressing it as other methods [Sra17].

4.4 Comparison with existing Algorithms

In this section we present comparison between our method and [Man15] and [Job17] methods. Analyzing the results in Table 4, we show that our algorithm and the work of [Man15] present good robustness against several common signal processing operations, including scaling, aspect ratio and JPEG compression with several quality factors ranging such as 20 and 50. In addition, our proposed method obtains BER values better than [Man15]. For scaling attack, we obtain BER equal to 0.001 and 0.009 respectively for scale_0.5 and

<table>
<thead>
<tr>
<th>Image</th>
<th>Lena</th>
<th>Baboon</th>
<th>Peppers</th>
<th>529</th>
<th>533</th>
<th>534</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality Factor</td>
<td>NC</td>
<td>BER</td>
<td>NC</td>
<td>BER</td>
<td>NC</td>
<td>BER</td>
</tr>
<tr>
<td>15</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0.99</td>
<td>0.0009</td>
</tr>
<tr>
<td>20</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0.98</td>
<td>0.005</td>
</tr>
<tr>
<td>25</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0.98</td>
<td>0.006</td>
</tr>
<tr>
<td>30</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0.98</td>
<td>0.006</td>
</tr>
<tr>
<td>35</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0.98</td>
<td>0.006</td>
</tr>
<tr>
<td>50</td>
<td>1</td>
<td>0</td>
<td>0.99</td>
<td>0.003</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>70</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0.99</td>
<td>0.0009</td>
</tr>
<tr>
<td>80</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>90</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 1: Evaluation of the robustness against JPEG compression

Figure 8: (a) The NC values of Lena, Baboon, Peppers images against unique attacks of Stirmark (b) The NC values of 529, 533, 534 images against unique attacks of Stirmark
Table 2: Evaluation of the robustness against unique attacks of Stirmark

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Lena</th>
<th>Baboon</th>
<th>Peppers</th>
<th>529</th>
<th>533</th>
<th>534</th>
</tr>
</thead>
<tbody>
<tr>
<td>1_row_1_col_removed</td>
<td>0</td>
<td>0</td>
<td>0.0010</td>
<td>0</td>
<td>0.0009</td>
<td>0</td>
</tr>
<tr>
<td>1_row_5_col_removed</td>
<td>0</td>
<td>0</td>
<td>0.003</td>
<td>0.008</td>
<td>0.009</td>
<td>0</td>
</tr>
<tr>
<td>5_row_17_col_removed</td>
<td>0.001</td>
<td>0.001</td>
<td>0.008</td>
<td>0.004</td>
<td>0.001</td>
<td>0.0009</td>
</tr>
<tr>
<td>2x2_median_filter</td>
<td>0.004</td>
<td>0.03</td>
<td>0.022</td>
<td>0.03</td>
<td>0.03</td>
<td>0.016</td>
</tr>
<tr>
<td>3x3_median_filter</td>
<td>0.001</td>
<td>0.008</td>
<td>0.024</td>
<td>0.01</td>
<td>0.0009</td>
<td>0.009</td>
</tr>
<tr>
<td>Gaussian_filtering_3*3</td>
<td>0</td>
<td>0</td>
<td>0.012</td>
<td>0.0009</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Cropping_1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Cropping_2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ratio_x_0.80_y_1.00</td>
<td>0.02</td>
<td>0.0009</td>
<td>0.008</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ratio_x_0.90_y_1.00</td>
<td>0</td>
<td>0</td>
<td>0.004</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ratio_x_1.20_y_1.00</td>
<td>0</td>
<td>0.0009</td>
<td>0.008</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>scale_0.75</td>
<td>0</td>
<td>0</td>
<td>0.004</td>
<td>0</td>
<td>0.001</td>
<td>0</td>
</tr>
<tr>
<td>scale_0.90</td>
<td>0</td>
<td>0</td>
<td>0.003</td>
<td>0.0009</td>
<td>0</td>
<td>0.009</td>
</tr>
<tr>
<td>scale_2.00</td>
<td>0</td>
<td>0</td>
<td>0.002</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>shearing_x_1.00_y_0.00</td>
<td>0.07</td>
<td>0.07</td>
<td>0.07</td>
<td>0.08</td>
<td>0.08</td>
<td>0.08</td>
</tr>
</tbody>
</table>

Table 3: Evaluation of the robustness against double attacks of Stirmark

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Lena</th>
<th>Baboon</th>
<th>Peppers</th>
<th>529</th>
<th>533</th>
<th>534</th>
</tr>
</thead>
<tbody>
<tr>
<td>1_row_1_col_removed</td>
<td>0.02</td>
<td>0.03</td>
<td>0.02</td>
<td>0.054</td>
<td>0.07</td>
<td>0.054</td>
</tr>
<tr>
<td>1_row_5_col_removed</td>
<td>0.038</td>
<td>0.06</td>
<td>0.04</td>
<td>0.08</td>
<td>0.08</td>
<td>0.083</td>
</tr>
<tr>
<td>5_row_1_col_removed</td>
<td>0.041</td>
<td>0.05</td>
<td>0.03</td>
<td>0.074</td>
<td>0.09</td>
<td>0.074</td>
</tr>
<tr>
<td>3x3_median_filter</td>
<td>0.05</td>
<td>0.06</td>
<td>0.04</td>
<td>0.057</td>
<td>0.1</td>
<td>0.057</td>
</tr>
<tr>
<td>Gaussian_filtering_3*3</td>
<td>0.07</td>
<td>0.078</td>
<td>0.1</td>
<td>0.076</td>
<td>0.2</td>
<td>0.076</td>
</tr>
<tr>
<td>FMLR</td>
<td>0.01</td>
<td>0.006</td>
<td>0.03</td>
<td>0.016</td>
<td>0.1</td>
<td>0.016</td>
</tr>
<tr>
<td>ratio_x_0.80_y_1.00</td>
<td>0.0068</td>
<td>0.05</td>
<td>0.01</td>
<td>0.075</td>
<td>0.02</td>
<td>0.075</td>
</tr>
<tr>
<td>ratio_x_0.90_y_1.00</td>
<td>0.0087</td>
<td>0.02</td>
<td>0.004</td>
<td>0.07</td>
<td>0.03</td>
<td>0.07</td>
</tr>
<tr>
<td>ratio_x_1.20_y_1.00</td>
<td>0.006</td>
<td>0.019</td>
<td>0.02</td>
<td>0.025</td>
<td>0.02</td>
<td>0.025</td>
</tr>
<tr>
<td>scale_1.10</td>
<td>0.044</td>
<td>0</td>
<td>0.09</td>
<td>0.059</td>
<td>0.1</td>
<td>0.059</td>
</tr>
<tr>
<td>scale_1.50</td>
<td>0.003</td>
<td>0</td>
<td>0.01</td>
<td>0.003</td>
<td>0.03</td>
<td>0.003</td>
</tr>
<tr>
<td>scale_2.00</td>
<td>0</td>
<td>0</td>
<td>0.006</td>
<td>0</td>
<td>0.01</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 4: Comparison of robustness between the proposed approach and other existing image watermarking schemes

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NC</td>
<td>BER</td>
<td>BER</td>
<td>NC</td>
</tr>
<tr>
<td>No attack</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Scale_0.5</td>
<td>0.99</td>
<td>0.001</td>
<td>0.02</td>
<td>0.86</td>
</tr>
<tr>
<td>Scale_2</td>
<td>0.99</td>
<td>0.009</td>
<td>0.02</td>
<td>0.86</td>
</tr>
<tr>
<td>Aspect ratio(1.2, 1.0)</td>
<td>0.99</td>
<td>0.001</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>JPEG (Q=20)</td>
<td>0.99</td>
<td>0.001</td>
<td>0.003</td>
<td>0.73</td>
</tr>
<tr>
<td>JPEG (Q=50)</td>
<td>0.99</td>
<td>0.001</td>
<td>0.001</td>
<td>0.83</td>
</tr>
<tr>
<td>JPEG (Q=60)</td>
<td>0.99</td>
<td>0.001</td>
<td>0.001</td>
<td>0.83</td>
</tr>
</tbody>
</table>

scale_2, [Man15] obtain BER =0.02 for both attacks. On the other hand, the method proposed in [Job17] has a similar performance against the above mentioned common signal processing. However, the method seem to be not robust to JPEG compression, obtaining a BER =0.22, and 0.34. The two methods don’t deal with double attack problem like ours.
5 CONCLUSION
In this paper, we focused on image watermarking for copyright protection application. A DCT-based blind and robust image watermarking scheme using the least significant bit is presented. In order to increase the security, the Arnold transform is used to scramble the watermark. In the proposed scheme the Y and Cb components of the original image are substituted by the bits of the scrambled watermark.

The results demonstrate high imperceptibility and robustness against JPEG compression, unique and double attacks of Stirmark without ameliorating the watermarked attacked image before detection. At the end, our method is compared to other existing algorithms, the method presents good results.

6 ACKNOWLEDGMENTS
The research leading to these results received funding from the Tunisian Ministry of Higher Education and Scientific Research under the grant agreement number LR11ES48.

7 REFERENCES


