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 aplication, 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].

$$\begin{cases} Y = 0.2989 \times R + 0.5866 \times G + 0.1145 \times B \\ Cb = -0.1688 \times R - 0.3312 \times G + 0.5 \times B \\ Cr = 0.5000 \times R - 0.1181 \times G - 0.0816 \times B \end{cases} \quad (1)$$

$$\begin{cases} R = 1.0 \times Y + 0.0 \times Cb + 1.403 \times Cr \\ G = -0.1688 \times Y - 0.3312 \times G + 0.5 \times B \\ B = 0.5000 \times Y - 0.1181 \times G - 0.0816 \times B \end{cases} \quad (2)$$

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:

$$F(u,v) = c(u)c(v) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \times \cos \frac{\pi u(2x+1)}{2M} \cos \frac{\pi v(2y+1)}{2N} \quad (3)$$

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

$$c(u), c(v) = \begin{cases} \frac{1}{\sqrt{2}} & \text{si } u, v = 0 \\ 1 & \text{si } otherwise \end{cases} \quad (4)$$

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

$$f(x,y) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} c(u) \times c(v) F(u,v) \times \cos[\frac{\pi}{M} u(x+\frac{1}{2}] \cos[\frac{\pi}{N} v(y+\frac{1}{2}] \quad (5)$$

ISBN 978-80-86943-41-1

With images, most of the energy prevails in low frequency. While the high frequency can be neglected as it results 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 techniques 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:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N} \quad (6)$$

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.

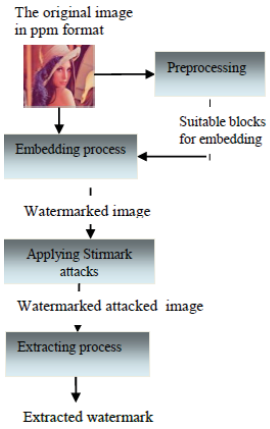


Figure 1: The flow chart of the watermarking approach

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 elicit matrix whose size is M*M, Y is chosen because it is tolerant to the wellknown attack JPEG compression

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

Step6: All pixels of the blocks are substracted 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

ISBN 978-80-86943-41-1

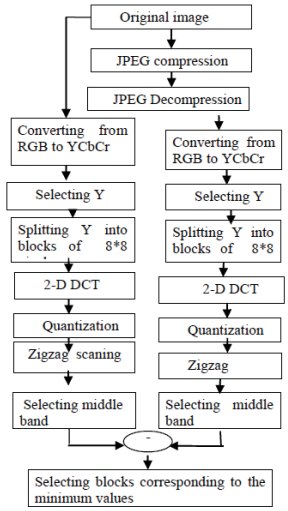


Figure 2: The flow chart of the preprocessing step

addition to Y, Cb is selected to resist to the cropping attack.

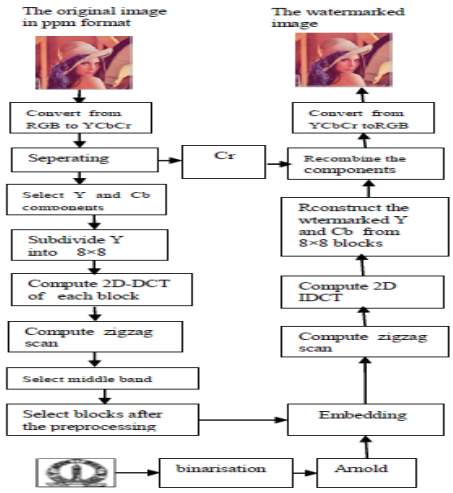


Figure 3: The flow chart of the embedding process

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.

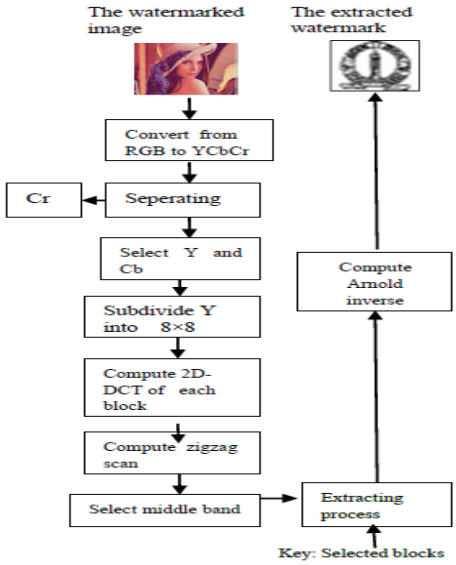
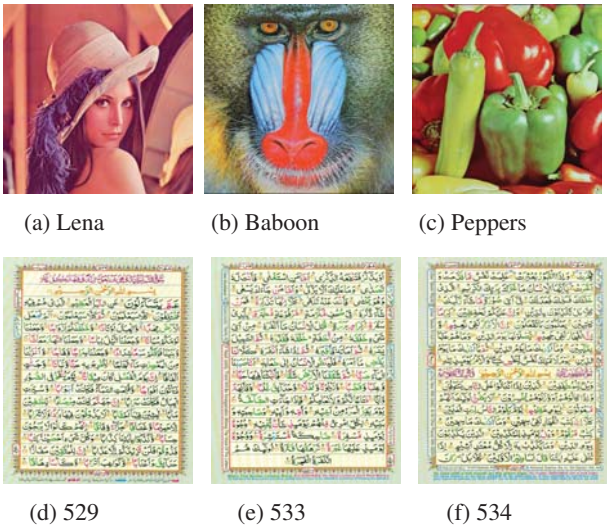


Figure 4: The flow chart of the extraction process

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.



(a) Lena (b) Baboon (c) Peppers

(d) 529 (e) 533 (f) 534

Figure 5: The original images

Figure 6 shows the original image watermark and the results after binarisation step and applying Arnold

ISBN 978-80-86943-41-1

(a) The original watermark

(b) The watermark after binarisation

(c) The watermark after Arnold Transform

Figure 6: The watermark processing

transform 8 times.

The key of our scheme is composed of the number of iteration of the Arnold transform and the index of the chosen blocks in the insertion step.

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:

$$PSNR = 10 \times \log_{10}(L \times \frac{L}{MSE}) \quad (7)$$

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]:

$$NC = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} W(i,j)W'(i,j)}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N} W(i,j)^2}\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N} W'(i,j)^2}} \quad (8)$$

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].

$$BER = \sum_{i=1}^{n}\sum_{j=1}^{m} \frac{W(i,j) \oplus W'(i,j)}{m*n} \quad (9)$$

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.

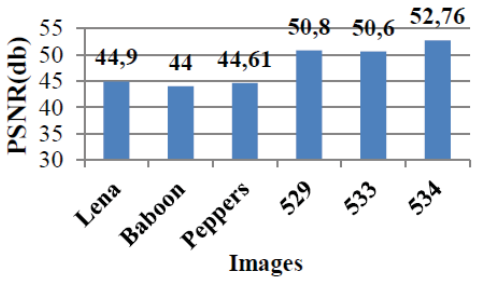


Figure 7: PSNR values of several watermarked images

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

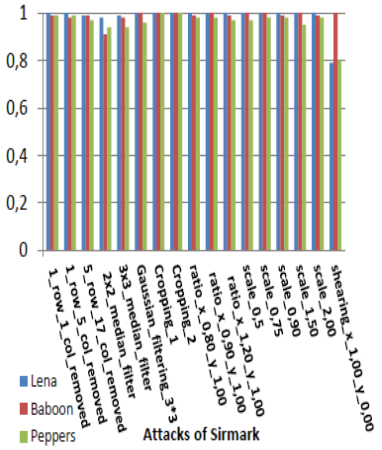
The watermarked images are in ppm formats, the Stirmark generates attacked images in ppm and jpeg formats. The ones with ppm are the unique attacks of Stirmark.

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 imageS which are '529.ppm','533.ppm','534.ppm'.

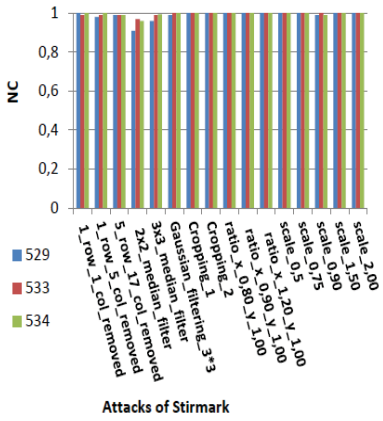
ISBN 978-80-86943-41-1

Image / Quality Factor	Lena		Baboon		Peppers		529		533		534	
	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
15	1	0	1	0	0.99	0.0009	1	0	0.99	0.001	0.99	0.001
20	1	0	1	0	1	0	1	0	1	0	0.99	0.001
25	1	0	1	0	1	0	1	0	0.98	0.005	0.98	0.006
30	1	0	1	0	0.98	0.006	1	0	0.96	0.013	0.96	0.013
35	1	0	1	0	0.98	0.006	1	0	0.95	0.019	0.99	0.001
50	1	0	0.99	0.003	0.98	0.006	1	0	0.99	0.003	0.98	0.006
70	1	0	1	0	0.99	0.0009	1	0	0.99	0.001	0.99	0.001
80	1	0	1	0	1	0	1	0	1	0	1	0
90	1	0	1	0	1	0	1	0	1	0	1	0

Table 1: Evaluation of the robustness against JPEG compression



(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

Figure 8: The NC values against unique attacks of Stirmark

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 TNC = 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 BER are less than the predefined threshold value TBER = 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 TBER = 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

ISBN 978-80-86943-41-1

Attacks \ Image name(.ppm)	Lena	Baboon	Peppers	529	533	534
1_row_1_col_removed	0	0	0.0010	0	0.0009	0
1_row_5_col_removed	0	0	0.003	0.008	0.0009	0
5_row_17_col_removed	0.001	0.001	0.008	0.004	0.001	0.0009
2x2_median_filter	0.004	0.03	0.022	0.03	0.03	0.016
3x3_median_filter	0.001	0.008	0.024	0.01	0.0009	0.001
Gaussian_filtering_3*3	0	0	0.012	0.0009	0	0
Cropping_1	0	0	0	0	0	0
Cropping_2	0	0	0	0	0	0
ratio_x_0.80_y_1.00	0	0.0009	0.008	0	0	0
ratio_x_0.90_y_1.00	0	0	0.004	0	0	0
ratio_x_1.20_y_1.00	0	0.0009	0.008	0	0	0
scale_0.75	0	0	0.004	0	0.001	0
scale_0.90	0	0	0.003	0.0009	0	0.009
scale_2.00	0	0	0.002	0	0	0
shearing_x_1.00_y_0.00	0.07	0.07	0.07	0.08	0.08	0.08

Table 2: Evaluation of the robustness against unique attacks of Stirmark

Attacks \ Image name(.jpg)	Lena	Baboon	Peppers	529	533	534
1_row_1_col_removed	0.02	0.03	0.02	0.054	0.07	0.054
1_row_5_col_removed	0.038	0.06	0.04	0.084	0.08	0.083
5_row_1_col_removed	0.041	0.05	0.03	0.074	0.09	0.074
3x3_median_filter	0.05	0.06	0.04	0.057	0.1	0.057
Gaussian_filtering_3*3	0.07	0.078	0.1	0.076	0.2	0.076
FMLR	0.01	0.006	0.03	0.016	0.1	0.016
ratio_x_0.80_y_1.00	0.0068	0.05	0.01	0.075	0.02	0.075
ratio_x_0.90_y_1.00	0.0087	0.02	0.004	0.07	0.03	0.07
ratio_x_1.20_y_1.00	0.006	0.019	0.02	0.025	0.02	0.025
scale_1.10	0.044	0	0.09	0.059	0.1	0.059
scale_1.50	0.003	0	0.01	0.003	0.03	0.003
scale_2.00	0	0	0.006	0	0.01	0

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

Attacks \ Methods	Proposed method **PSNR=49**		[Man15] **PSNR=44**	[Job17] **PSNR=38**	
	NC	BER	BER	NC	BER
No attack	1	0	0	1	0
Scale_0.5	0.99	0.001	0.02	0.86	0.16
Scale_2	0.99	0.009	0.02	0.86	0.16
Aspect ratio(1.2, 1.0)	0.99	0.001	0	-	-
JPEG (Q=20)	0.99	0.001	0.003	0.73	0.34
JPEG (Q=50)	0.99	0.001	0.001	0.83	0.22
JPEG (Q=60)	0.99	0.001	-	0.75	0.32

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

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.

 ISBN 978-80-86943-41-1

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 compresion , 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

[Aro15] A.Roy, A. K. Maiti, and K. Ghosh, A perception based color image adaptive watermarking scheme in YCbCr space, in Signal Processing and Integrated Networks, 2nd International Conference, 2015.

[Ali10] Ali Wali, Najib Ben Aoun, Hichem Karray, Chokri Ben Amar, Adel M. Alimi: A New System for Event Detection from Video Surveillance Sequences. Advanced Concepts for Intelligent Vision Systems International Conference, ACIVS, 2010.

[Bou11] Boulbaba Guedri, Mourad Zaied, Chokri Ben Amar: Indexing and images retrieval by content. High Performance Computing and Simulation (HPCS), 2011.

[Fat15] Faten Chaabane, Maha Charfeddine,William Puech,Chokri Ben Amar, A qr-code based audio watermarking technique for tracing traitors, EUSIPCO, 2015.

[Hai13] Hai Tao, Li Chongmin, Jasni Mohamad Zain1, Ahmed N. Abdalla,Robust Image Watermarking Theories and Techniques: A Review,Journal of Applied Research and Technolog, 2014

[Job17] Jobin Abraham ,Varghese Paul, An imperceptible spatial domain color image watermarking scheme, Journal of King Saud University – Computer and Information Sciences, 2017.

[Lam15] Lamri Laouamer and Omar Tayan, A Semi-Blind Robust DCT Watermarking Approach for Sensitive Text Images, Arab J Sci Eng, 2015.

[LIG17] LIGM, Laboratoire d'Informatique Gaspard-Monge,1990 http://igm.univmlv.fr/ incerti/IMAGES/PPM.htm. Online accessed April 2017.

[Mah12] Maha Charfeddine, Maher El'arbi and Chokri Ben Amar, A new DCT audio watermarking scheme based on preliminary MP3 study , Multimed Tools Appl, 2012.

[Man16] Manpreet Kaur, Vinod Kumar Sharma, Encryption based LSB Steganography Technique for Digital Images and Text Data, International Journal of Computer Science and Network Security, 2016

[Man15] Manuel Cedillo-Hernandez , Antonio Cedillo- Hernandez Francisco Garcia-Ugalde, Mariko Nakano-Miyatake, Hector Perez-Meana, Copyright Protection of Color Imaging Using Robust-Encoded Watermarking, Radioengineering, 2015.

[Mas10] Masmoudi Salma, Charfeddine Maha, Chokri Ben Amar A robust audio watermarking technique based on the perceptual evaluation of audio quality algorithm in the multiresolution domain,Signal Processing and Information Technology (ISSPIT), 2010

[Meh16] Mehdi Khalili and Mahsa Nazari, Non Correlation DWT Based Watermarking Behavior in Different Color Spaces , International Journal of Advanced Computer Science and Applications, 2016.

[Mel11] M.El'Arbi, M.Charfeddine,S. Masmoudi M.Koubaa and C. Ben Amar,Video watermarking algorithm with BCH error correcting codes hidden in audio channel,IEEE symposium series in computational intelligence, 2011

[Mku] M.Kutter and F. Petitcolas, A fair benchmark for image watermarking systems,SPIE, 1999

[Moh16] Mohammad Moosazadeh and Gholamhossein Ekbatanifard, Robust Image Watermarking Algorithm Using DCT Coefficients Relation in YCoCg-R Color Space ,Eighth International Conference on Information and Knowledge Technology (IKT), Hamedan, Iran,2016.

[Nam17] Namita Tiwari1 and Sharmilaand, Digital Watermarking Applications, Parameter Measures and Techniques, International Journal of Computer Science and Network Security, 2017.

[Pooj15] Pooja Rani , Apoorva Arora, Image Security System using Encryption and Steganography, International Journal of Innovative Research in Science, Engineering and Technology,2015.

[Rea17] Reading Al Quran, 2017, http://readingalquran.com/alquran.php?part=30, Accessed April 2017

 ISBN 978-80-86943-41-1

[Sra17] S. Rashmi, Priyanka and Sushila Maheshkar,Robust Multiple Composite Watermarking Using LSB Technique , Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications, Advances in Intelligent Systems and Computing, 2017

[Ssh14] S.Shanmugaprabha and N.Malmurugan, A New Robust Image Watermarking Scheme Based On DWT With SVD , International Journal of advanced studie in Computer Science and Engineering, 2014.

[Son16] Sonam Tyagi, Harsh Vikram Singh, Raghav Agarwal and Sandeep Kumar Gangwar,Digital Watermarking Techniques for Security Applications,International Conference on Emerging Trends in Electrical, Electronics and Sustainable Energy Systems, 2016.

[Sub17] Subin Bajracharya and Roshan Koju, An Improved DWT-SVD Based Robust Digital Image Watermarking for Color Image International Journal Engineering and Manufacturing, pp 49-59, 2017

[Sur17] Suraj Kumar Dubey, Vivek Chandra, Steganography, Cryptography and Watermarking: A Review , International Journal of Innovative Research in Science, Engineering and Technology, 2017.

[Wke15] W.K. ElSaid, Watermarking Digital Artworks , International Journal of Computer Applications,2015.

 ISBN 978-80-86943-41-1