

Hough Transform-Based Robust Informed Watermarking Approach for Medical Images

Lamri Laouamer^{*}, Mohannad Alswaili^{}

Department of Management Information Systems & Production Management, College of Business & Economics, Qassim University, Buraidah 51452, KSA

Corresponding Author Email: laoamr@qu.edu.sa



Copyright: ©2024 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ts.410343>

ABSTRACT

Received: 12 June 2023
Revised: 16 November 2023
Accepted: 18 February 2024
Available online: 26 June 2024

Keywords:

medical image, attacks, robustness, imperceptibility, Hough transform

In digital image watermarking, robustness of watermarks against attacks has become a key issue, especially for real-time applications while maintaining high security with low complexity in terms of watermark embedding/extraction time. Through this motivation, we present in this paper a new approach based on Hough transform by detecting lines within the image reflecting the regions to be selected for watermarking. The main reason by choosing the Hough transform in our watermarking scheme is that watermarking will only be carried out in well-defined objects (represented by lines) in order to reduce the watermark payload and computational time. This choice is also because the Hough transform is based on the use of a parametric space, called Hough space, making it possible to simplify the complex problem of global shape detection in the image space. Indeed, in this parametric space, the detection is local and therefore simpler. Any curve that can be described by parameters is likely to be detected by the Hough transform. This transform represents many advantages, mainly its simplicity, speed (by stochastic sampling), and robustness to noise. Obviously, watermark will be embedded only in pixels located in all lines through a parameterized number depending on the lines to be detected. The evaluation of the proposed approach with regards to imperceptibility and robustness yielded encouraging, namely PSNR approximately equal to 65 dB, Correlation coefficients (CC) very close to 1, and Bit Error Rates (BER) with very low percentage in most cases.

1. INTRODUCTION

With the development of information technologies and the growth of devices connected to internet, the volume of medical data produced every day continues to increase significantly. Such large volumes of data need to be protected during storage, processing and exchange. Hence, it is necessary to find adequate and reliable security solutions with low computational time. In this context, the security of medical images exchanged by different computer networks becomes more and more essential and requires reliable and robust solutions with low processing time to be applicable in real-time medical applications.

Medical image watermarking can contribute to ensuring the authenticity, integrity, and robustness of medical images. The image watermarking application domains can be classified into two major categories: the spatial domain and the frequency domain. In the spatial domain image watermarking is directly done on the pixels of the host image and does not require any prior transform [1, 2]. In the frequency domain the host image undergoes a spectral transform before performing the watermarking [3, 4], i.e., the watermark will be embedded in the image's transformed coefficients space. It is well known that the frequency methods are more robust against attacks than the spatial methods [4].

Likewise, watermarking can be done in different ways, including blind watermarking, semi-blind watermarking, and

non-blind watermarking. Blind watermarking [5] is the most effective in terms of security since it only requires the key used in watermarking embedding to extract the attacked watermark. In semi-blind watermarking [6], the original watermark image is essential when extracting the attacked watermark, while in non-blind watermarking [7], the host image is required to extract the attacked watermark.

Choosing the type of watermarking depends on the purpose of the targeted watermarking scheme. Such purpose could be seeking robustness, integrity or authenticity. Robustness designates the almost perfect extraction of the attacked watermark to provide proof of ownership; integrity refers to evidence of non-change in the content of the watermarked image; and authenticity is about how to protect the integrity of the content of watermarked images.

Similarly important is the complexity aspect since medical images are usually represented by voluminous data. Therefore, the objective is to reduce the computational time as much as possible in terms of embedding and extracting watermark time. This aspect has become very important, especially for real-time applications that require fast interactions for responsiveness.

The following sections of this paper are organized as follows. Section 2 describes some relevant related works. Section 3 introduces the motivation for choosing the Hough transform through detecting lines to achieve the proposed watermarking framework. Section 4 addresses the proposed

watermark embedding and extraction processes. Section 5 interprets the obtained results regarding imperceptibility and robustness with a comparative study. Finally, Section 6 concludes this paper with some perspectives.

2. RELATED WORK

Roy and Pal [8] proposed an embedding approach of watermark bits on the blue/green channels. The approach consists of randomly modifying some middle significant AC coefficients based on repetition code. Many watermarks are embedded in the two channels following the DCT zigzag. The authors tested their approach against attacks such as cropping, scaling, rotation, etc. The recovered watermarks from the attacked watermarked images were close to the original watermarks for some attacks. Regarding JPEG compression attacks, the approach presents some difficulties in this regard since a small modification of the compression rate will completely change the DC component as well as the AC components of each image block.

Moad et al. [9] suggest a new embedding way to encrypt a watermark within the host image. The watermark in question is constructed from two operations; the first one is a part of a patient's fingerprint and the second one consists of the encrypted photography of the patient. The approach is based on the DWT four sub bands by deploying the watermark information (patient fingerprint and photography) on the middle frequency sub bands. Experiments have been achieved against attacks such as noising and JPEG compression. The results obtained against attacks such as rotation and median filtering were not as expected.

Two distinctive watermarking approaches have been introduced in the research [10] for RGB color channels. First, a watermark in a gray level has been embedded in the blue channel. Second, the blue watermark component was incrustated in the same channel color of the original image. The watermark was embedded in the singular values of the host image. The authors presented their approach as imperceptible where the original watermark and the extracted one after applying attacks were quasi similar to each other based on the calculated Normalized Correlation NC. The main disadvantage of this approach is that it requires more time for embedding the watermark when using the SVD transform.

A watermarking scheme based on the Number Theoretical Transform (NTT) has been proposed in the research [11] where the watermark is embedded in the NTT of a host image based on linear interpolation to control the visibility degree of the incrustated watermark. The strength of the proposed approach has been assessed by applying geometric and non-geometric attacks to measure the imperceptibility and the robustness of the watermark against different kind of attacks. This approach is interesting but requires heavy calculations since the calculation of the NTT is done twice and the appropriate choice of modulus must be made carefully.

Olanrewaju et al. [12] suggested a medical watermarking technique using Fast Fourier Transform and Complex Valued Neural Network (FFT-CVNN). The purpose of this technique is more focused on detecting tampered zones and falsification. The approach was evaluated using known metrics to judge the imperceptibility and the robustness of the watermark against a small number of attacks. Unfortunately, this approach was not tested against a variety of attacks which makes it hard to evaluate its effectiveness. Likewise, the approach requires a

high computational time when using FFT-CVNN.

In addition, hybrid methods combining different approaches of image watermarking in frequency transforms have been also proposed [13-15]. It should be noted that these methods reinforce the robustness of watermarks against malicious attacks by increasing significantly the computational complexity, which makes them unsuitable for real-time applications.

We summarize the advantages, disadvantages, and application scenarios of the approaches cited above in Table 1 to better understand the strong and weak points of each approach.

Table 1. Summarization of the related: Advantages, disadvantages, and application scenarios

	Advantages	Disadvantage	Application Scenarios
Approach in reference [8]	Robust against many geometric attacks	Weakness regarding JPEG compression attacks high computational time	Frequency domain
Approach in reference [9]	Robust against some geometric attacks	Weakness regarding rotation and median filtering attacks high computational time	Frequency domain Watermark encryption
Approach in reference [10]	Robust against almost geometric attacks	High computational time	Frequency domain
Approach in reference [11]	Robust against almost geometric attacks	High Sensitivity	Frequency domain
Approach in reference [12]	Detecting the altered zones and recovery	Robust against a few attacks	Frequency domain
Approach in references [13-15]	Hybrid	High computational time	Frequency domain

In this paper, we propose a new watermarking scheme based on the Hough transform to enhance watermark robustness against attacks and to verify the integrity of image contents exchanged through untrusted communication networks. The approach is interesting. The choice to realize a watermarking image scheme using the Hough transform is well justified by the fact that this transform offers a fast processing and noise-resistant against illegal manipulations. Through this approach we select only objects represented by lines in order to reduce the computational time both for watermark embedding/extraction by preserving a high degree of robustness.

3. HOUGH TRANSFORM

The generalized Hough transform makes it possible to

detect in the image the presence of parametric curves belonging to a known family (straight lines, circles, ellipses, etc.) by establishing a projection between the space of the image and a representative space of the desired shape (Hough space). We are interested in this paper to the Hough transform for lines detection. The straight line Hough transform is a method for detecting straight lines in an image, that is to say a set of more or less aligned points. This method is based on the parameterization of a straight line by an angle θ and a distance ρ as defined in Figure 1.

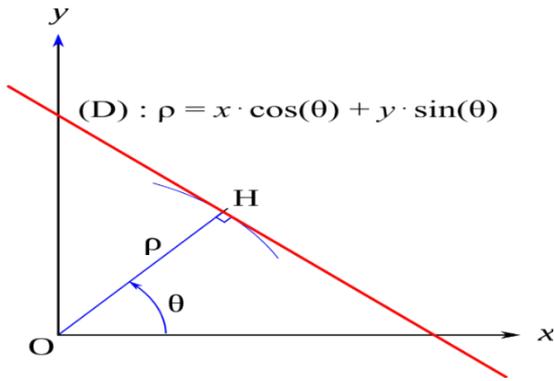


Figure 1. Hough transform for lines detection

The Cartesian equation of the line is defined in Eq. (1):

$$\rho = x \cos \theta + y \sin \theta \quad (1)$$

Hough's algorithm uses an accumulator matrix which represents the plane (ρ, θ) , of dimensions (p, q) where p is the number of possible values of ρ and q the number of values of θ .

For each point (x, y) of the processed binary image, each straight line (ρ, θ) passing through this point adds one unit to the corresponding element of the matrix. At the end of the accumulation, the points of the matrix with the highest value correspond to a large number of points aligned on the image. These lines are selected from an adjustable threshold.

Algorithm I: Image Hough transform to detect lines

```

Import: I % image
J ← Edge of I % by applying a Canny filter
Defining : δ % discrétisation pace
1. M ← 0 % accumulation matrice initialisation
2. For each pixel (x, y) of J do
3. For θ from 0 to 180 with δ pace
4. ρ ← x*cos(θ) + y*sin(θ)
5. M(ρ, θ) ← M(ρ, θ) + 1
6. End For
7. End For
Pics detection of M
    
```

By transforming all possible lines that pass through a point (i.e., by calculating the value of ρ for each θ), we obtain a single sinusoid called “Hough space”. If the curves associated with two points intersect, the area where they intersect in Hough space corresponds to the parameters of a straight line connecting these two points as illustrated in Figure 2.

The intersection of the curves in Hough space at point I represents the point in which the three points A, B and C lie on the same line. In point I, these three curves have the same value of the couple (θ, ρ) and this is how we detect all the

straight lines passing through all the pixels in the image. An example of how to transform a given image to its corresponding Hough image is shown in Figure 3.

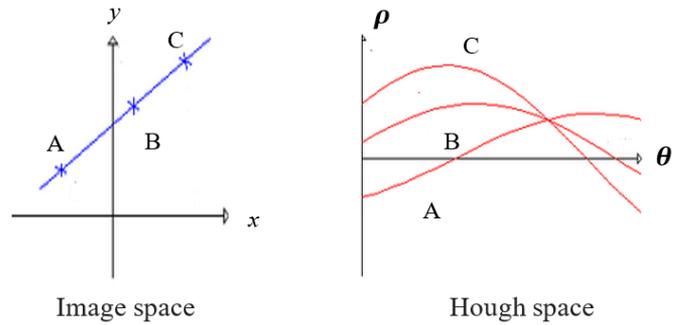


Figure 2. Image space and its Hough space

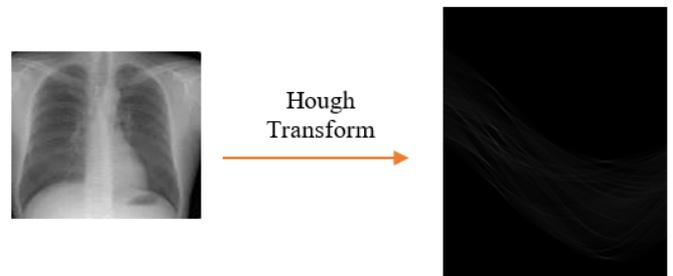


Figure 3. Example of a Hough image

It is quite clear that the Hough transform is strongly related to image segmentation by detecting objects represented by lines, circles, and other shapes. The choice of line detection for our watermarking scheme is mainly justified by the watermark embedding only on the detected lines instead of the entire image. This choice also makes it possible to reduce the time for carrying out the watermark embedding and extraction since it only consists objects represented by lines.

4. PROPOSED APPROACH AND MOTIVATION

4.1 Motivation

In medical image watermarking, the Hough transform involves less complexity than other transforms such as Discreet Cosine Transform (DCT), Wavelet Cosine Transform (DWT), Fast Fourier Transform (FFT), Singular Value Decomposition (SVD) since it only consists of making the watermark and/or extracting it only in specified and precise geometric shapes (case of Hough transform based-lines and circles detection). The major advantage of the Hough transform is its tolerance for discontinuities in the contours of the forms sought, as well as the noise of the image.



Figure 4. A sample of the used images in our tests

The proposed watermarking model is based mainly on three essential processes: watermark embedding, attacks on the

watermarked image and extracting the watermark from the attacked watermarked image. The used data set consists of 50 medical images of size 255×255 in grayscale [16]. Figure 4 represents a sample of the used images in our experimentation. We detail each process separately.

4.2 Watermark embedding

Before proceeding to watermark embedding, the detection of line segments in the images is necessary in order to detect curves that have the same value of the couple (θ, ρ) . In Figure 5, we illustrate an example of line detection represented by twenty straight lines for each image. The peaks of the lines passing through pixels will be considered as watermark data, which significantly reduces the computational time in the extraction phase. The number of lines shown can be less than the designated number depending on the effective segments existing within the image.

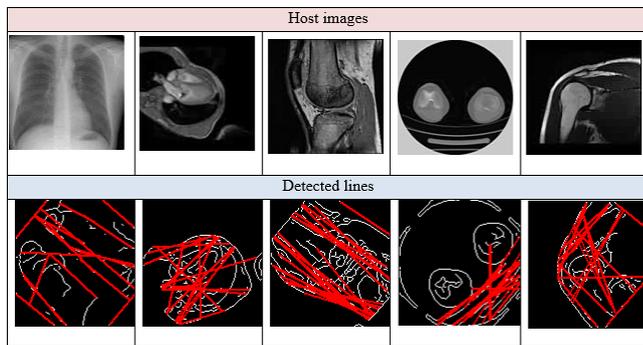


Figure 5. Example of detected lines segments (in red)

Figure 6 illustrates all the generated watermarks from the used images. The watermark images represent the peaks of the detected lines. That is to say that the black points in the watermarks reflect the peak position of each line existing in the host image.

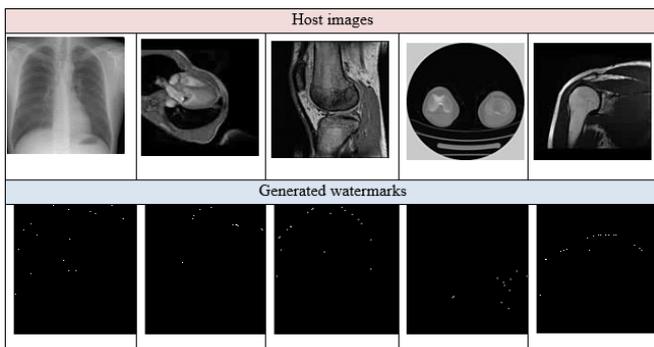


Figure 6. Generated watermarks for the used images

The watermark embedding will be carried out only on the pixels of the image located on the same line and this will be applied to all the lines detected by the Hough transform. The number of lines designed by the watermark embedding is parameterized (i.e., the user can define the number of lines to be taken into consideration for the watermarking). In other words, the pixels concerned by the watermarking are the pixels having the same pair (θ, ρ) for each line. This parameterization can greatly reduce the complexity of the watermarking process either for embedding or for extraction.

The watermark embedding process is defined by a linear

interpolation approach as defined in Equation 2. Choosing the linear interpolation for watermark embedding is mainly based on controlling the visibility/invisibility of the embedded watermark. This process is based on the value of δ . According to Eq. (2), If δ is close to 1, the watermark becomes invisible and if δ is closed to 0, the watermark becomes visible.

$$i_w = (1 - \delta)w + \delta i \quad (2)$$

where, i_w , and w are respectively the watermarked image and the original watermark. δ is the watermarking key such $\delta \in]0, 1[$. The parameter δ allows controlling the visibility/invisibility of the embedded watermark. Figure 7 Illustrates the used images and their corresponding watermarked images i_{ws} .

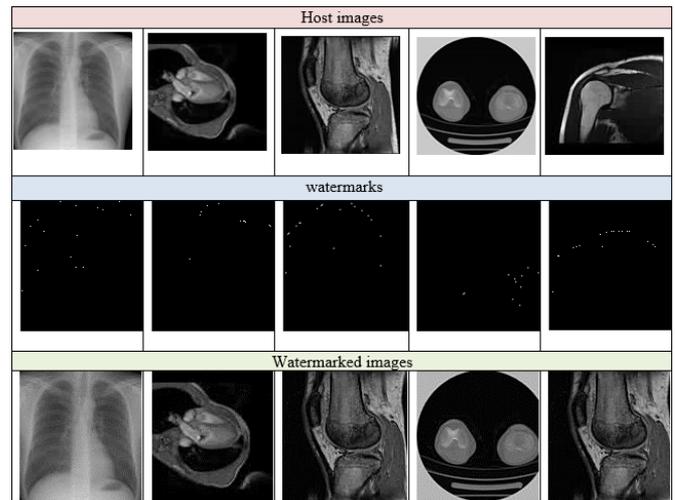


Figure 7. Watermark embedding phase

The embedding watermark phase can be summarized as illustrated in Algorithm II:

Algorithm II
Inputs: host image I (255×255 of size)
1. Detect curves with same value of the couple (θ, ρ) / angle θ and distance ρ
2. Choose the number of lines to be detected through
3. Generating watermark w from i (w represents the peaks of the detected lines in i)
4. Choose a value for $\delta \rightarrow 1$ ($\delta=0.95$ in our tests)
5. Embedding w in i according to Eq. (2)
Outputs: watermarked image i_w

4.3 Attacks on watermark

A number of attacks have been applied on different watermarked images including geometric and non-geometric attacks using one of the well-known benchmarks in the field of watermarking called Stirmark benchmark [17] such JPEG compression, Filtering by median, adding noise, convolution, cropping and rotation. These attacks aim to influence the watermark through the watermarked image and then make its extraction difficult. Figure 8 shows some attacks on a sample of watermarked images.

The attacks used in our tests are described in Table 2 as along with the description of each attack with the corresponding parameters.

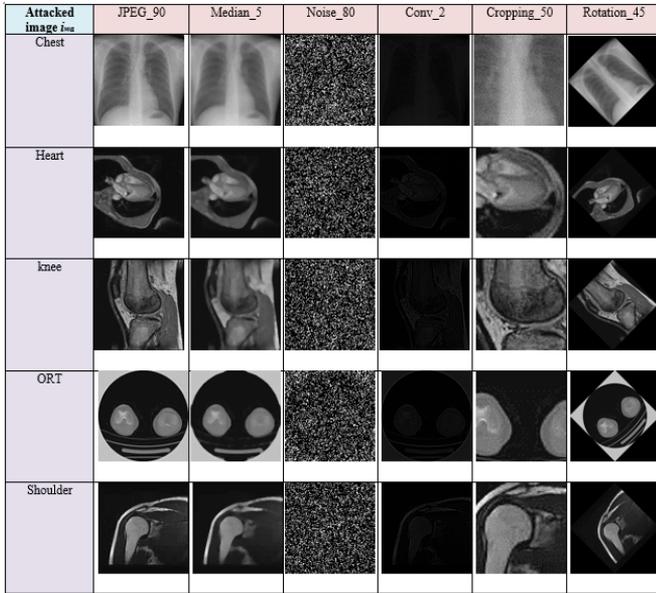


Figure 8. Example of attacks on watermarked images

Table 2. Some used attacks and their descriptions

Attack	Description
JPEG_90	Performs compression in jpeg format with compression rates ranging from 3 to 100 (in other words, the image is 3 to 100 times smaller than the original image).
Median_5	Modify the center pixel's value by the middle value of the arranged pixel. The used blocks size is 5×5.
Noise_80	Affects the pixels in the image with a specific percentage. White noise additive Gaussian is used by affecting 80% of pixels with mean equal to zero and a variance equal to σ^2 .
Conv_2	Aims to denoise an image and smooth textured areas by multiplication of two matrices of different sizes in 2D.
Cropping_50	Consists of removing part of an image defined by a specific rate either with the aim of improving it or for better framing, accentuation or removal of defects. The used rate is 50%.
Rotation_45	Rotate an image with a defined angle. The angle used in this attack is 45 degrees.

4.4 Watermark extraction

The watermark extraction process consists in extracting the watermark incusted in the host image after having undergone various geometric and non-geometric attacks. The extraction of the attacked watermark w_a is defined in Eq. (3).

$$w_a = \frac{1}{\delta} w - \frac{1 - \delta}{\delta} i w_a \quad (3)$$

where, w_a is the extracted watermark, $i w_a$ is the attacked watermarked image, δ is the same watermarking key used in the watermark embedding.

The watermark extraction phase can be summarized as illustrated in Algorithm III:

Algorithm III
Inputs: attacked watermarked image $i w_a$ (255×255 of size)
1. Detect curves with same value of the couple (θ , ρ) / angle θ and distance ρ

2. Choose the number of lines to be detected through HT/ the same in watermark embedding
3. Using watermark w of the embedding phase
4. Choose a value of $\delta \rightarrow 1$ ($\delta=0.95$ in our tests)/ the same value used in embedding process
5. Extract the attacked watermark w_a according to Eq. (3)

Outputs: attacked watermark w_a

Figure 9 shows the extracted watermarks from the different host images for each attack.

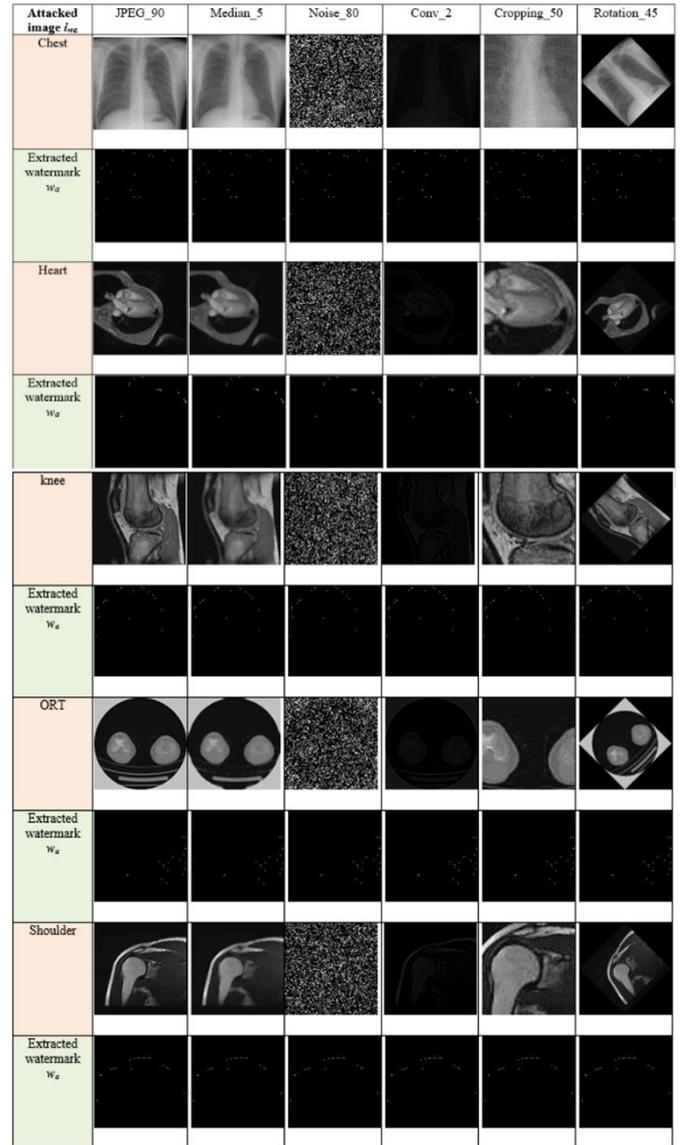


Figure 9. Watermarks extraction phase

5. RESULTS AND DISCUSSION

Through the proposed approach, we conducted several evaluations to assess the performance of the proposed model. This evaluation covers two main criteria: imperceptibility and robustness. Moreover, we compared our approach with other relevant watermarking models from the literature [18-20].

There are two ways to evaluate the performance of a watermarking scheme. The first one consists of measuring the imperceptibility between the host image and the watermarked image through the PSNR metric. It should be noted that the

value of the PSNR between two identical images tends towards infinity ($PSNR(i, i_w) \rightarrow \infty$), which means perfect resemblance. Typically, if the PSNR exceeds 40dB, the human eye does not visually detect the difference. The second one is the calculation of the correlation coefficient between the original watermark w and the extracted one w_a ; If $CC(w, w_a) = 1$ it means that w, w_a are identical.

The imperceptibility is evaluated in terms of resemblance between the host image and the watermarked one. Instead of measuring distortion, the value of Peak Signal to Noise Ratio (PSNR) [21] measures the fidelity between two images since it is proportional to quality. Likewise, PSNR is a function of Mean Square Error (MSE). Its definition and use come from the field of signal processing. For a given image, i max designate the maximum possible luminance value. An infinite PSNR value corresponds to a non-degraded image, and this value decreases as a function of the degradation. The PSNR leads the MSE to the maximum energy of the image. The PSNR calculation is defined in Eq. (4).

$$PSNR = 10 \log_{10} \left(\frac{i_{max}^2}{MSE} \right) dB \quad (4)$$

For all images used in our tests, we note that all PSNR values as illustrated in Table 3 between the host images i and their corresponding watermarked ones i_w exceed 40dB. This means that the criterion of imperceptibility is well verified. These results are quite logical since the watermark payload is

$$CC(w, w_a) = \frac{\sum_{p=1}^M \sum_{q=1}^N (w(p,q) - \bar{w}(p,q))(w_a(p,q) - \bar{w}_a(p,q))}{\sqrt{(\sum_{p=1}^M \sum_{q=1}^N (w(p,q) - \bar{w}(p,q))^2) (\sum_{p=1}^M \sum_{q=1}^N (w_a(p,q) - \bar{w}_a(p,q))^2)}} \quad (5)$$

Table 4. CC values between the original watermarks and their corresponding extracted ones

					
JPEG_90	0.9866	0.9996	0.9956	0.9935	0.9972
Median_5	0.9865	0.9983	0.9954	0.9937	0.9971
Noise_80	0.9928	0.9967	0.9953	0.9954	0.9951
Conv_2	0.9995	0.9996	0.9996	0.9996	0.9994
Cropping_50	0.9878	0.9965	0.9926	0.9928	0.9944
Rotation_45	0.9942	0.9996	0.9961	0.9953	0.9988

Table 5. BER values between the original watermarks and their corresponding extracted ones

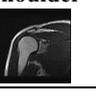
					
JPEG_90	12.3%	11.9%	11.8%	14.2%	11.7%
Median_5	11.7%	10.8%	10.4%	13.7%	10.6%
Noise_80	13.6%	12.2%	11.7%	13.9%	12.1%
Conv_2	9.2%	8.8%	8.9%	9.8%	9.0%
Cropping_50	14.8%	12.9%	12.1%	14.6%	12.7%
Rotation_45	11.4%	10.6%	9.9%	13.1%	10.4%

The bit error ratio (BER) [21] is defined as the expected statistical value of the ratio between the number of erroneous bits of the attacked watermark w_a data and the size of the original watermark data w itself. The BER is calculated in percentage, a lower percentage means that the original watermark and the extracted one are similar. The BER is calculated according to Eq. (6).

$$BER(w, w_a) = \frac{1}{N} \sum_{i=1}^N w(i) \oplus w_a(i) \times 100\% \quad (6)$$

weak as we only selected the pixels located on the same lines in the Hough transform. This embedding process increases the chances of high imperceptibility.

Table 3. PSNR values between the host images and their corresponding watermarked images

					
PSNR (i, i_w)	63.72	65.21	67.59	60.79	66.36

5.1 Robustness

One of the metrics used to calculate the resemblance between two images is the linear correlation (CC) [21]. The correlation technique relies on two images, one reference, the other corresponding to the deformed one with the same dimensions. The principle of image correlation is to recognize the same pattern of an image to another, and use it as a marker of a small area of the image. To match these two patterns and make them coincide, it is necessary to move this domain from one quantity which is then naturally identified with the local displacement. The correlation coefficient (Table 4) between the original watermark w and the extracted one w_a is defined in Eq. (5) as follow:

5.2 Performance analysis

In order to evaluate the effectiveness of the proposed watermarking method, a comparative study with three other watermarking algorithms published in studies [18-20] has been conducted. This comparison is based on two essential criteria used in any watermarking scheme: imperceptibility and robustness. Table 6 presents the obtained results of the PSNR values between the proposed approach and works cited in studies [18-20]. It should be noted that the proposed approach has better results since the average PSNR achieved in the proposed approach greatly exceeds those in approaches [18-20] with an average of 65dB.

Table 6. PSNR comparison between the proposed approach and approaches in studies [18-20]

	Zhu et al. [18]	Mellimi et al. [19]	Kaibou et al. [20]	Proposed Approach
PSNR Values	~ 37.5	~44.08	~49.3	~65

Regarding the robustness, we conducted a comparison of the results obtained from the correlation coefficients CCs between the proposed approach and the approaches cited in studies [18-20] as illustrated in Table 7. We conducted this comparison only with common attacks. A reading of the results obtained in terms of CC values shows that our approach generates better results than the other approaches [18-20] where the CCs values in the most cases are very close to 1.

Table 7. Correlation coefficients comparison between the proposed approach and approaches in studies [18-20]

	Zhu et al. [18]	Mellimi et al. [19]	Kaibou et al. [20]	Proposed Approach
Gaussian noise	~0.958	~0.6736	~0.99	~0.9945
Rotation 30°	~0.927	-	-	~0.9968
JPEG compression QF=77	~0.960	~0.98	-	~0.9946
Cropping 10	-	~0.9998	~0.4567	~0.9928

The advantage of the proposed approach is based on line detection through Hough transform. The lines represent the areas of contrast and texture while the human visual system (HVS) is less sensitive to any changes that an image can undergo and it is for this reason that the imperceptibility is better, which has a positive influence on the robustness of the watermark against attacks.

The proposed approach presents some shortcomings especially for images of a smooth or semi-smooth nature where the detection of shapes in general and lines in particular becomes a difficult task to implement. So our approach works well with images that contain textured or semi-textured regions.

Likewise, we did not measure the computational time of our approach nor of the other approaches since the used computer processors are different, which makes this criterion difficult to evaluate. But from a theoretical point of view, if the watermark payload is low, the computational time for watermark embedding and extraction will decrease.

6. CONCLUSIONS

A medical image watermarking approach has been proposed in this paper. The approach is essentially based on the Hough transform to achieve a watermark embedding/extraction through the straight lines detected by this transform. This approach is well indicated for securing medical images in real-time applications due to its relative minimal complexity with the other techniques operating in a transform domain, as well as its resistance to noise. We were interested in performing the watermarking only on the lines detected by the Hough transform which represent areas of texture in an image. This process helps to realize watermarking in areas with less sensitivity to human visual system, which guarantees imperceptibility and considerably reduces the payload of the watermark. The results obtained are very encouraging in terms of the imperceptibility of the watermark as well as its remarkable resistance to some geometric and non-geometric attacks. This conclusion was validated through results obtained regarding the three metrics: PSNR, CC and BER. The PSNR in the majority of its values is equivalent on average of 65dB, the CC is very close to 1 and the BER represents low rates in term of percentage in most cases. As perspectives regarding the proposed approach, attempting to create a watermarking scheme with other forms (circles, squares, etc.) based on Hough transform may provide interesting results and may improve the performance of the proposed watermarking scheme. Likewise, when reading the results obtained, we note that the proposed approach gives not better results, particularly against attacks such adding noise and cropping where the BER values are slightly increased.

REFERENCES

- [1] Kumar, S., Singh, B.K. (2021). Entropy based spatial domain image watermarking and its performance analysis. *Multimedia Tools and Applications*, 80(6): 9315-9331. <https://doi.org/10.1007/s11042-020-09943-x>
- [2] Wang, H., Su, Q. (2022). A color image watermarking method combined QR decomposition and spatial domain. *Multimedia Tools and Applications*, 81(26): 37895-37916. <https://doi.org/10.1007/s11042-022-13064-y>
- [3] Essaidani, D., Seddik, H. (2018). Invariant digital image watermarking scheme in the projected-frequency domain. In *Image and Signal Processing: 8th International Conference, ICISP 2018, Cherbourg, France*, pp. 45-54. https://doi.org/10.1007/978-3-319-94211-7_6
- [4] Thanh, T.M., Tanaka, K. (2016). The novel and robust watermarking method based on q-logarithm frequency domain. *Multimedia Tools and Applications*, 75: 11097-11125. <https://doi.org/10.1007/s11042-015-2836-6>
- [5] Soualmi, A., Alti, A., Laouamer, L. (2022). A novel blind medical image watermarking scheme based on Schur triangulation and chaotic sequence. *Concurrency and Computation: Practice and Experience*, 34(1): e6480. <https://doi.org/10.1002/cpe.6480>
- [6] Laouamer, L., Tayan, O. (2015). A semi-blind robust DCT watermarking approach for sensitive text images. *Arabian Journal for Science and Engineering*, 40: 1097-1109. <https://doi.org/10.1007/s13369-015-1596-y>
- [7] Mekarsari, Y.A., Sari, C.A., Rachmawanto, E.H. (2018). Non-blind RGB image watermarking technique using 2-level discrete wavelet transform and singular value

- decomposition. In 2018 International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, Indonesia, pp. 623-627. <https://doi.org/10.1109/ICOIACT.2018.8350793>
- [8] Roy, S., Pal, A.K. (2017). A blind DCT based color watermarking algorithm for embedding multiple watermarks. *AEU-International Journal of Electronics and Communications*, 72: 149-161. <https://doi.org/10.1016/j.aeue.2016.12.003>
- [9] Moad, M.S., Kafi, M.R., Khaldi, A. (2022). A wavelet based medical image watermarking scheme for secure transmission in telemedicine applications. *Microprocessors and Microsystems*, 90: 104490. <https://doi.org/10.1016/j.micpro.2022.104490>
- [10] Vaishnavi, D., Subashini, T.S. (2015). Robust and invisible image watermarking in RGB color space using SVD. *Procedia Computer Science*, 46: 1770-1777. <https://doi.org/10.1016/j.procs.2015.02.130>
- [11] Laouamer, L. (2017). Towards a robust and fully reversible image watermarking framework based on number theoretic transform. *International Journal of Signal and Imaging Systems Engineering*, 10(4): 169-177. <https://doi.org/10.1504/IJSISE.2017.086385>
- [12] Olanrewaju, R.F., Khalifa, O., Abdulla, A., Khedher, A.M. (2011). Detection of alterations in watermarked medical images using Fast Fourier Transform and Complex-Valued Neural Network. In 2011 4th International Conference on Mechatronics (ICOM), Kuala Lumpur, Malaysia, pp. 1-6. <https://doi.org/10.1109/ICOM.2011.5937131>
- [13] Dey, A., Mallick, P., Tunga, H. (2021). Hybrid algorithm based on DWT-DCT-RSA with digital watermarking for secure image transfer. In: Pan, I., Mukherjee, A., Piuri, V. (eds) *Proceedings of Research and Applications in Artificial Intelligence. Advances in Intelligent Systems and Computing*, vol 1355. Springer, Singapore. https://doi.org/10.1007/978-981-16-1543-6_2
- [14] Kang, X.B., Zhao, F., Lin, G.F., Chen, Y.J. (2018). A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength. *Multimedia Tools and Applications*, 77: 13197-13224. <https://doi.org/10.1007/s11042-017-4941-1>
- [15] Roy, S., Pal, A.K. (2019). A hybrid domain color image watermarking based on DWT-SVD. *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, 43: 201-217. <https://doi.org/10.1007/s40998-018-0109-x>
- [16] CT Medical Images. <https://www.kaggle.com/datasets/kmader/siim-medical-images>.
- [17] StirMark benchmark 4.0. (1998). <https://www.petitcolas.net/watermarking/stirMark/>.
- [18] Zhu, L., Wen, X., Mo, L., Ma, J., Wang, D. (2021). Robust location-secured high-definition image watermarking based on key-point detection and deep learning. *Optik*, 248: 168194. <https://doi.org/10.1016/j.ijleo.2021.168194>
- [19] Mellimi, S., Rajput, V., Ansari, I.A., Ahn, C.W. (2021). A fast and efficient image watermarking scheme based on deep neural network. *Pattern Recognition Letters*, 151: 222-228. <https://doi.org/10.1016/j.patrec.2021.08.015>
- [20] Kaibou, R., Azzaz, M.S., Benssalah, M., Teguig, D., Hamil, H., Merah, A., Akrou, M.T. (2021). Real-time FPGA implementation of a secure chaos-based digital crypto-watermarking system in the DWT domain using co-design approach. *Journal of Real-Time Image Processing*, 18(6): 2009-2025. <https://doi.org/10.1007/s11554-021-01073-3>
- [21] Laouamer, L. (2022). New informed non-blind medical image watermarking based on local binary pattern. *Traitement du Signal*, 39(5): 1851-1856. <https://doi.org/10.18280/ts.390545>