IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 39, No. 5, October, 2022, pp. 1851-1856
Journal homepage: http://iieta.org/journals/ts

New Informed Non-Blind Medical Image Watermarking Based on Local Binary Pattern

Lamri Laouamer

Department of Management Information Systems & Production Management, College of Business & Economics, Qassim University, P.O. Box 6633, Buraidah 51452, KSA

Corresponding Author Email: laoamr@qu.edu.sa

https://doi.org/10.18280/ts.390545

Received: 8 August 2022
Accepted: 12 October 2022

Keywords:
medical image, image watermarking, Informed watermarking, LBP, robustness

ABSTRACT

Medical image watermarking represents a promising alternative tool regarding many security aspects such: digital rights, authenticity and integrity and content protection issues. Achieving a successful watermarking should be achieved by choosing the most significant and important patterns describing the image. This strategy should also ensure a tradeoff between the robustness of the watermark against attacks and the computational time both for watermark embedding and extracting processes. In this paper, an informed medical image watermarking scheme is proposed based on local binary pattern LBP. Local Binary Pattern (LBP) is an effective texture descriptor for images by providing the texture regions of interests concerned by watermarking. A watermark is built based on the significant information extracted from the host image by through the LBP descriptor. LBP image will be addressed to be embedded using a linear interpolation. Scenarios of geometric and non-geometric attacks have been realized on the watermarked images to evaluate the robustness of the embedded watermark in the extraction process. Furthermore, the obtained experiment results show the effectiveness of the proposed approach regarding the watermark imperceptibility and robustness.

1. INTRODUCTION

The digital technologies, the explosion of communication networks and the ever-growing enthusiasm of the general public for new information technologies are leading to an increased traffic of multimedia (images, videos, texts, sounds, etc.). The extent of this phenomenon is such that essential concerns now arise regarding the protection and control of the exchanged data. Indeed, by their digital nature, multimedia documents can be duplicated, modified, transformed and distributed easily. Under these conditions, it becomes therefore necessary to develop systems to enforce copyright, protecting the integrity of documents and authentication [1]. In this context, digital watermarking very quickly appeared as the alternative solution to reinforce the security of multimedia contents.

The main idea of image digital watermarking is to hide in digital image subliminal information (i.e. invisible or imperceptible) to ensure a security level (copyright, integrity, authenticity purposes, etc.). One of the specificities of digital watermarking compared to other techniques, such as for example simple information storage in the header of file, is that the watermark is intimately to data. Therefore, the watermarking is theoretically independent from the format of file and can be detected or extracted even if the image has undergone modifications or is incomplete.

Watermark embedding techniques can be classified into two main categories depending on the targeted objective: the watermarking domain and the type of watermarking. For the watermarking domain, two essential domains are distinguished: 1) the spatial domain in which directly modifies the pixels without any preliminary processing [2, 3] to embed the watermark; and 2) the frequency domain [4, 5] which requires transforms before embedding the watermark such as the Discrete Cosine Transform [6, 7], Discrete Wavelet Transform [8, 9], Singular Value Decomposition [10, 11], etc. For the second category which consists of the type of watermarking, we define three types: Blind watermarking [12] in which we need only the watermarking key to extract the attacked watermark; semi-blind watermarking [13] where the host image is required to extract the attacked watermark and finally the non-blind watermarking [14] while the original watermark is needed to extract the attacked watermark.

A watermarking scheme must be robust against different scenarios of geometric and/or non-geometric attacks which mean that the watermark can be extracted even if the watermarked image is attacked. Similarly, the computational time parameter should not be neglected, especially with the growth of data, which means that this parameter must also be taken into consideration for the watermarking scheme to be applicable in real time.

We present through this paper, a new medical watermarking scheme both for embedding and extracting watermark. The proposed scheme is based on local binary pattern LBP to be involved to build an informed watermarks based on the LBP operators. A different scenario of attacks has been applied on the watermarked images to evaluate the robustness of the embedded watermarks. The obtained results are well discussed and evaluated.

2. RELATED WORK

Su and Chen [15] propose a watermarking approach with a blind manner which consist to incrust watermark directly and without any transform to the blue component in the RGB image. The approach exploits the DC coefficient to realize embedding watermark in different regions of the host image. The extraction process is based on the same way when embedding watermark on the watermarked image and the key-based quantization. Authors show that the proposed approach gain an acceptable invisibility factor when embedding watermark and resist against some kind of attacks such cropping, and noise JPEG compression.

A spatial domain watermarking technique has been proposed [16]. The technique is based on combining the DC behavior in its original value and its value when applying a Fourier transform. Embedding and extracting watermarks is basically based on the changed value of the DC component of each block. Authors illustrates that the proposed technique have shown the invisibility of the watermark on the watermarked images. The technique was tested against a few numbers of attacks such JPEG compression and adding noises. The main contribution of this technique is its low computational time.

In the watermarking scheme proposed by Abraham and Paul [17], authors suggested to achieve the watermark embedding on specific regions in the host image. The approach is principally based on using two masks which are used to distribute the watermark information to the neighboring pixels in the selected region. The firs mask modulates blue component of the RGB image and has a role to the tune of the watermark bit. While the second mask which is considered as a compensating mask that adjusts red and green color channels.

Faheem et al. [18] proposed a Least Significant Bits (LSB) spatial watermarking approach through an image gradient and chaotic map. The image is divided into non overlapping blocks, and the gradient of each block is calculated. As known, the gradient expresses a good information regarding changes in an image. A chaotic substitution box (S-Box) is used to scramble the watermark according to a piecewise linear chaotic map (PWLCM). The embedding payload introduces a compromise between robustness and watermark invisibility. The tests achieved through this approach show a satisfactory enhancement in term of watermark robustness against geometrical attacks. The approach maintains also an acceptable imperceptibility of the watermark.

3. LOCAL BINARY PATTERN

Local Binary Pattern (LBP) is a technique in which many image features can be expressed such local texture (spot, Spot/flat, line end, edge, corner, etc.) operator for a gray-level changes. This technique is obtained from information regarding texture in a local neighbourhood. The LBP operator thresholds is a neighbourhood gray value centre, by presenting the outputs as a sequence of binary code that defines the local texture pattern as shown in Eq. (1). The LBP performs remarkably with applications needing fast feature extraction and texture classification due to its discriminative power and computational simplicity. The value of LBP code of a pixel (*xc*, *yc*) is given by:

$$LBP_{R,P} = \sum_{p=0}^{P-1} s(g_p - g_c)\, 2^p \qquad (1)$$

$$s(x) = \{1, if\ x \geq 0 | 0, otherwise\}$$

Figure 1 illustrates the process in how to calculate the local binary pattern of any gray-level image.

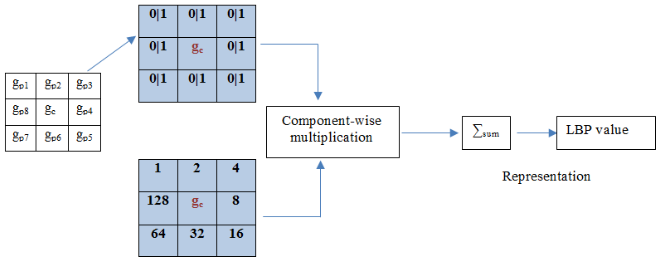


Figure 1. LBP operator computation

The different steps to calculate the local binary pattern LBP for an image are illustrated in the following algorithm I.

Algorithm I

Step 1. Converting the input image into graylevel.

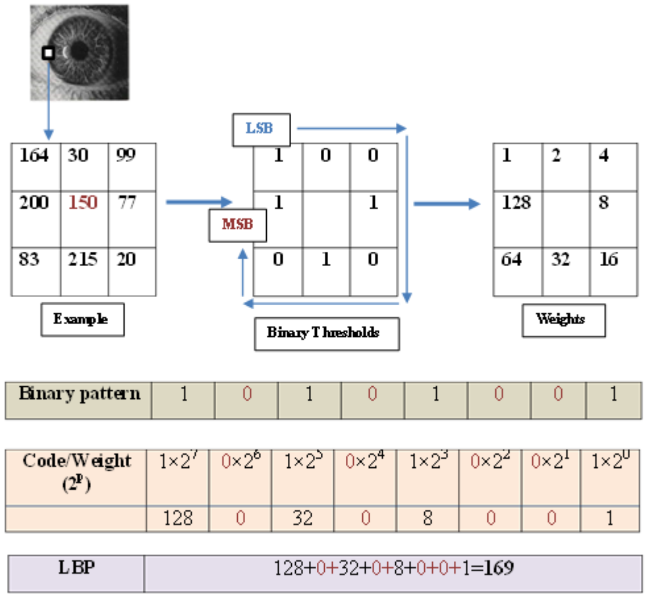
Step 2. Selecting the Q neighborhoods For each pixel (g_Q), select the *P* neighborhoods surrounding the central pixel.

Step 3. set center pixel (g_c) as a threshold for its Q neighbors.

Step 4. Set to 1 if the adjacent pixel value is >= to the value of the center pixel, 0 else.

Step 5. Calculate the LBP operator with a sequentially and counterclockwise manner, write a binary number consisting of digits adjacent to the center pixel according to Eq. (1).

For a given gray-level image, we illustrate how to compute an LBP operator for a given block of size 3×3 as shown in Figure 2.



164	30	99
200	150	77
83	215	20

1	0	0
1		1
0	1	0

1	2	4
128		8
64	32	16

Binary pattern	1	0	1	0	1	0	0	1
Code/Weight (2^P)	1×2^7	0×2^6	1×2^5	0×2^4	1×2^3	0×2^2	0×2^1	1×2^0
	128	0	32	0	8	0	0	1
LBP	128+0+32+0+8+0+0+1=169							

Figure 2. Example of computing the LBP operator for a given 3×3 block

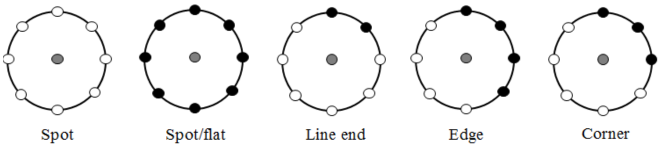


Figure 3. Different texture primitives detected by the LBP

Through LBP we can define many local primitives of an image such curves, spots, edges, etc. Figure 3 illustrates some of these primitives with LBP8, R operator. Circle with black background represents the value 1 in the image, 0 for white otherwise. Detecting such primitives using LBP is widely used in recognizing a wide variety of texture types.

Through Figure 4, we present a sample of images and the corresponding local binary pattern images. The used images are gray-level and of size 255×255.

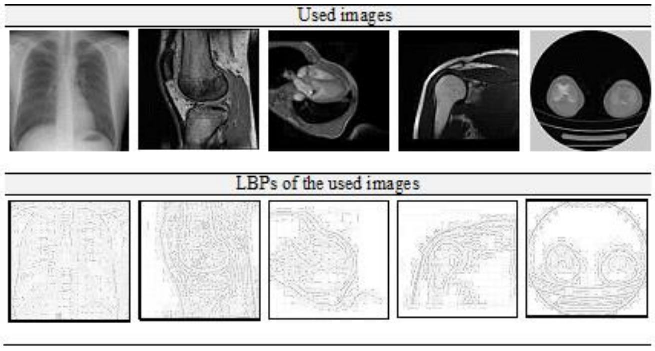


Figure 4. A sample of images and the corresponding LBP images

4. PROPOSED ATERMARKING PROCESS

The watermarking scheme that we propose through this paper consists of three essential phases. The first phase concerns watermarking embedding within a host image in an imperceptible way to guarantee its robustness. The second phase consists of applying geometric and non-geometric attacks on the images watermarked. The role of the third phase is to extract the watermark after applying attacks. The images used in our tests are illustrated in the Figure 5 and are of size 255×255 and in gray-level [19]. The medical images dataset represents a computerized tomography images combining a series of X-ray images taken from different angles. We detail the three steps in the following.

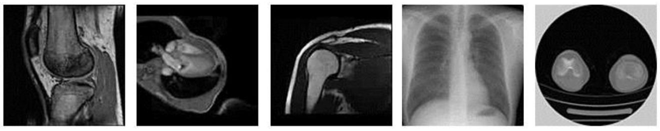


Figure 5. The used images in tests

4.1 Watermark embedding steps

To guarantee the robustness of the watermark against different kinds of attacks, the watermark must imperatively be invisible (imperceptible). The imperceptibility is manipulated by a linear interpolation as shown in Eq. (2). Whether the parameter α closer to 1 more the watermark is invisible. More α is close to 0, more the watermark becomes visible. Figure 6 illustrates the visibility/invisibility of the watermark by changing the values of the watermarking key α.

$$i_w = (1-\alpha)w + \alpha i \tag{2}$$

where, i_w, w, i are respectively the watermarked image, the watermark and the host image.

And $\alpha \in [0,1]$.

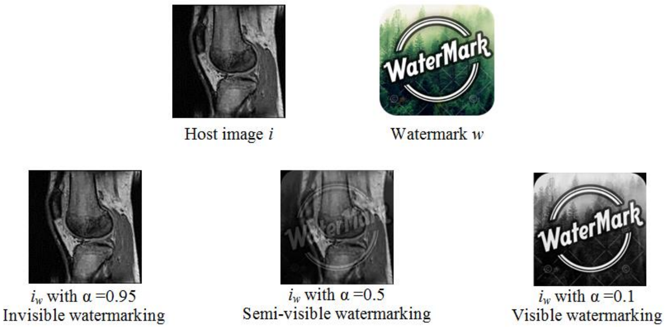


Figure 6. Control of watermark visibility/invisibility with different values of α

Each medical image has been embedded by its corresponding LBP image. Note that the LBP matrix is calculated with an overlapping blocks of size 3×3.

4.2 Scenario of attacks

We tested the proposed approach on a database of 25 images in gray-level and of size 255×255.The watermarked images were a subject of many attacks through Stirmark benchmark [20]. Stirmark is a well-known evaluation tool for watermarking schemes. It contains many attacks both in their two types (geometric and non-geometric) which help to evaluate the robustness of any image watermarking approach.

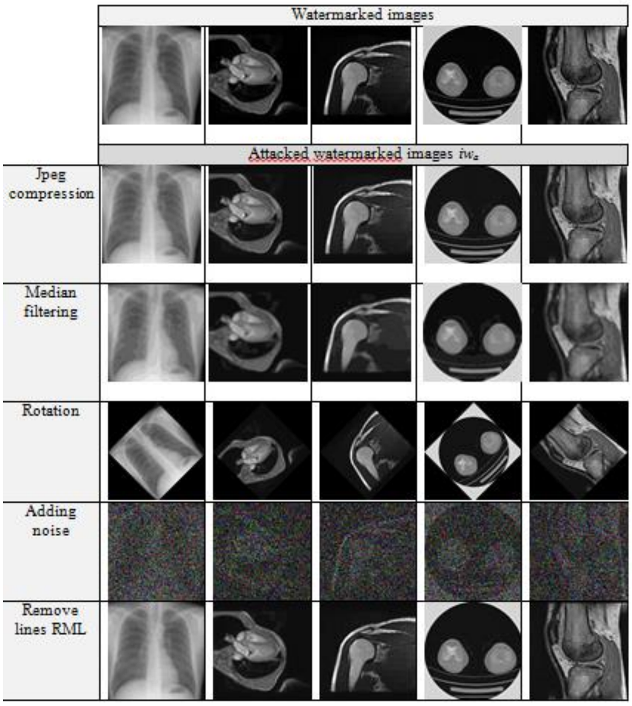


Figure 7. Some of applied attacks on the watermarked images

As mentioned previously, geometric and non-geometric attacks as shown in Figure 7 have been applied to different watermarked images such: chest, heart, shoulder, ORT and knee. We summarize here some attacks like JPEG compression, Median filtering, rotating with a chosen angle, adding noise and removing lines (vertically and horizontally). Attacking the watermarked images will be useful in the next section (watermark extraction) in order to decide about the watermark resistance against such attacks.

4.3 Watermark extraction steps

In this step, we try to extract the attacked watermark w_a from the attacked watermarked image iw_a. This process is the reverse operation of watermark embedding. The extraction of the attacked watermark is achieved in a non-blinded way as defined in Eq. (3).

$$w_a = \frac{1}{\alpha} w - \frac{1-\alpha}{\alpha} iw_a \tag{3}$$

where w_a, w, iw_a are respectively the extracted watermark, the original watermark and the attacked watermarked image.

And $\alpha \in [0,1]$.

The general watermarking scheme covering embedding, attacks and extracting watermark is shown in Figure 8.

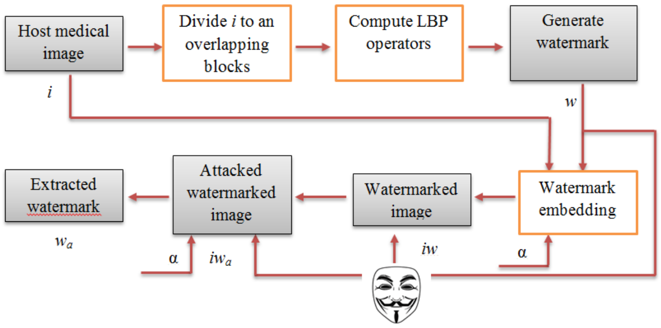


Figure 8. General watermarking scheme

We extracted the different watermarks from their corresponding attacked watermarked images against every attack as shown in Figure 9. The extracted watermarks will be a subject of discussion in the next section regarding their robustness.

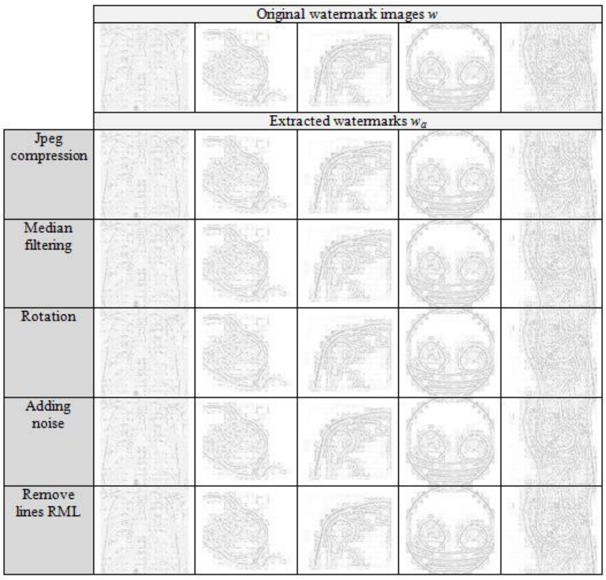


Figure 9. Extracted watermarks from the attacked watermarked images

5. RESULTS AND DISCUSSION

The evaluation of the results obtained will be defined on the calculation of three widely used metrics in image watermarking: Peak Signal Noise Ratio (PSNR), Correlation coefficient (CC) and the Bit Error Ratio (BER).

PSNR [21] is a logarithmic function of Mean Square Error (MSE) interpreted as a corrected version of the Signal-to-Noise Ratio. A PSNR value that exceeds 34db means a similarity between two images. A high similarity between two given images is expressed when $PSNR \rightarrow \infty$. The PSNR is calculated using Eq. (4):

$$PSNR = 10log_{10}\left(\frac{255^2}{\frac{1}{M \times N}\sum_{p=1}^{M}\sum_{q=1}^{N}\left(i(p,q) - iw(p,q)\right)^2}\right) dB \tag{4}$$

where, $i(p,q)$ and $i_w(p,q)$ are the pixels (p,q) in the original image i and the watermarked image i_w respectively. $M \times N$ is the size of the image.

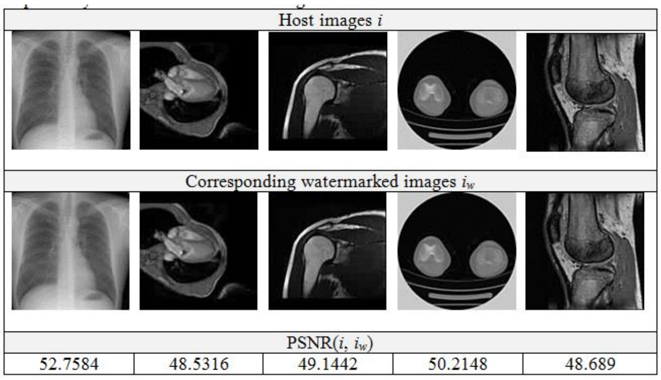


Figure 10. PSNR between the host images and their corresponding watermarked images

5.1 Imperceptibility

From the obtained results, we notice that all the PSNR values are very high and exceed the 34dB. This means that host images and their corresponding watermarked images are visually very similar and the difference cannot be detected by the human visual system. From the PSNR values we can confirm that the approach is imperceptible as shown in Figure 10. Table 1 illustrates a comparison between the proposed approach and some relevant works [22-24] in terms of imperceptibility.

From Table 1 we can conclude that the values of PSNR in the proposed approach are more better that obtained ones regarding approaches proposed in references [22-24].

5.2 Robustness

Now, to evaluate the robustness of the proposed approach, we rely on the correlation coefficients and the Bit Error Ratios between the original watermarks and their corresponding extracted watermarks.

Correlation Coefficient CC [21] represents the similarity between the original image and the attacked one. This coefficient is ranged in [1,-1]; if CC=1 this means that two images are highly identical, if CC=0 this means that two images are completely different. This metric is computed according to Eq. (5):

$$CC(w,wa) = \frac{\sum_{p=1}^{M}\sum_{q=1}^{N}(w(p,q) - \overline{w}(p,q))(w(p,q) - \overline{w_a}(p,q))}{\sqrt{(\sum_{p=1}^{M}\sum_{q=1}^{N} w(p,q) - \overline{w}(p,q)^2)(\sum_{p=1}^{M}\sum_{q=1}^{N} w_a(p,q) - \overline{w_a}(p,q)^2)}} \tag{5}$$

where, w_{ij}, w_{aij} are intensities of pixel (i, j) in the original watermark image w and the extracted watermark w_a respectively. The images w, w_a are the means intensities of respectively the watermark image w and the extracted watermark w_a.

BER [21] (Bit Error Rate) is the quotient of erroneous attacked image bits on the total number of original image bits. It is expressed in percentage as defined in Eq. (6).

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

Table 2 illustrated the correlation coefficients obtained between the original watermarks w and their corresponding attacked watermarks w_a. We notice that in almost cases, the CC values are very close to 1 which means that there is a high similarity between the watermark and its corresponding extracted one.

Table 3 illustrated also the different values of BER obtained between the original watermarks w and their corresponding attacked watermarks w_a. We notice that in almost cases, the BER values are very low in percentage which means that there is also a high similarity between the watermark and its corresponding extracted one.

Performance analysis is conducted to compare the results obtained from the proposed approach with works presented in [22-24] in terms on correlation coefficients as shown in Table 4. The correlation coefficients values in the proposed approach are closer to 1 regarding the compared works. This comparison is achieved for common attacks despite the proposed approach is performed in spatial domain.

Table 1. Comparison between the proposed approach and works [22-24] in terms of PSNR values

	Zhu et al. [22]	Mellimi et al. [23]	Kaibou et al. [24]	Proposed approach
PSNR values	~ 37.5	~44.08	~49.3	~50

Table 2. CC values between the original watermarks and the corresponding extracted ones

	Chest	Heart	Shoulder	Ort	Knee
Jpeg compression	0.9985	0.9992	0.9992	0.9991	0.9992
Median filtering	0.9985	0.9991	0.9992	0.9991	0.9991
Rotation	0.9984	0.9991	0.9992	0.9991	0.9992
Adding noise	0.9985	0.9992	0.9992	0.9992	0.9992
Remove lines RML	0.9985	0.9992	0.9992	0.9991	0.9992

Table 3. BER values between the original watermarks and the corresponding extracted ones

	Chest	Heart	Shoulder	Ort	Knee
Jpeg compression	9.21%	8.63%	9.57%	11.45%	13.05%
Median filtering	10.31%	9.31%	9.80%	11.70%	13.85%
Rotation	14.17%	9.71%	10.35%	11.20%	14.14%
Adding noise	15.58%	9.28%	9.84%	10.44%	13.32%
Remove lines RML	9.77%	8.82%	9.59%	11.43%	13.23%

Table 4. Comparison of robustness between the proposed approach and works [22-24] in terms of correlation coefficients

	Zhu et al. [22]	Mellimi et al. [23]	Kaibou et al. [24]	Proposed approach
Gaussian noise	0.958	0.6736	0.99	**0.9987**
Rotation 30°	0.927	-	-	**0.99**
JPEG compression QF=77	0960	0.98	-	**0.998**
Copping_10	-	0.9998	0.4567	**0.993**

6. CONCLUSION

Providing evidence on medical images ownership became necessary to protect medical images content rights. We have developed through this paper an innovative approach in the medical watermarking field. The approach is purely informed in the sense that the watermark is built from significant features of the host image. This feature is called Local Binary Pattern LBP. The approach was evaluated by applying different kind of attacked on the watermarked images to extract the attacked watermark which help to decide on the robustness of the proposed approach. The evaluation of the obtained results was achieved through well-known metrics in such Correlation coefficients CC and Bit Error Ratio BER. The results obtained are very encouraging and confirm the robustness of the approach.

ACKNOWLEDGEMENT

The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education, Saudi Arabia for funding this research work through the project number (QU-IF-2-4-1-27599). The authors also thank to Qassim University for technical support.

REFERENCES

[1] Ganesh, S.M., Manikandan, S.P. (2020). An efficient integrity verification and authentication scheme over the remote data in the public clouds for mobile users. Security and Communication Networks, 2020: 9809874. https://doi.org/10.1155/2020/9809874

[2] 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

[3] Yuan, Z., Su, Q., Liu, D., Zhang, X., Yao, T. (2020). Fast and robust image watermarking method in the spatial domain. IET Image Processing, 14(15): 3829-3838. https://doi.org/10.1049/iet-ipr.2019.1740

[4] Yuan, Z., Su, Q., Liu, D., Zhang, X. (2021). A blind image watermarking scheme combining spatial domain and frequency domain. The Visual Computer, 37(7): 1867-1881. https://doi.org/10.1007/s00371-020-01945-y

[5] Sisaudia, V., Vishwakarma, V.P. (2022). A secure gray-scale image watermarking technique in fractional DCT domain using zig-zag scrambling. Journal of Information Security and Applications, 69: 103296. https://doi.org/10.1016/j.jisa.2022.103296

[6] Jana, M., Jana, B. (2022). A new DCT based robust image watermarking scheme using cellular automata. Information Security Journal: A Global Perspective, 31(5): 527-543. https://doi.org/10.1080/19393555.2021.1956023

[7] Ariatmanto, D., Ernawan, F. (2020). Adaptive scaling factors based on the impact of selected DCT coefficients for image watermarking. Journal of King Saud University-Computer and Information Sciences, 34(3): 605-614. https://doi.org/10.1016/j.jksuci.2020.02.005

[8] Kumar, S., Singh, B.K. (2021). DWT based color image watermarking using maximum entropy. Multimedia Tools and Applications, 80(10): 15487-15510. https://doi.org/10.1007/s11042-020-10322-9

[9] Gao, H., Chen, Q. (2021). A robust and secure image watermarking scheme using SURF and improved Artificial Bee Colony algorithm in DWT domain. Optik, 242: 166954. https://doi.org/10.1016/j.ijleo.2021.166954

[10] Zhu, T., Qu, W., Cao, W. (2022). An optimized image watermarking algorithm based on SVD and IWT. The Journal of Supercomputing, 78(1): 222-237. https://doi.org/10.1007/s11227-021-03886-2

[11] Hu, H.T., Hsu, L.Y., Chou, H.H. (2020). An improved SVD-based blind color image watermarking algorithm with mixed modulation incorporated. Information Sciences, 519: 161-182. https://doi.org/10.1016/j.ins.2020.01.019

[12] 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

[13] Kumar, S., Rajpal, A., Sharma, N. K., Rajpal, S., Nayyar, A., Kumar, N. (2022). ROSEmark: Robust semi-blind ECG watermarking scheme using SWT-DCT framework. Digital Signal Processing, 129: 103648. https://doi.org/10.1016/j.dsp.2022.103648

[14] Minamoto, T., Ohura, R. (2011). A non-blind digital image watermarking method based on the dyadic wavelet transform and interval arithmetic. In International Conference on Signal Processing, Image Processing, and Pattern Recognition, Jeju Island, Korea, pp. 170-178. https://doi.org/10.1007/978-3-642-27183-0_18

[15] Su, Q., Chen, B. (2018). Robust color image watermarking technique in the spatial domain. Soft Computing, 22(1): 91-106. https://doi.org/10.1007/s00500-017-2489-7

[16] Su, Q., Liu, D., Yuan, Z., Wang, G., Zhang, X., Chen, B., Yao, T. (2019). New rapid and robust color image watermarking technique in spatial domain. IEEE Access, 7: 30398-30409. https://doi.org/10.1109/ACCESS.2019.2895062

[17] Abraham, J., Paul, V. (2019). An imperceptible spatial domain color image watermarking scheme. Journal of King Saud University-Computer and Information Sciences, 31(1): 125-133. https://doi.org/10.1016/j.jksuci.2016.12.004

[18] Faheem, Z.B., Ali, M., Raza, M.A., Arslan, F., Ali, J., Masud, M., Shorfuzzaman, M. (2022). Image Watermarking Scheme Using LSB and Image Gradient. Applied Sciences, 12(9): 4202. https://doi.org/10.3390/app12094202

[19] https://barre.dev/medical/sample, accessed on 12 June 2022.

[20] https://www.petitcolas.net/watermarking/stirmark/, accessed on 12 June 2022.

[21] Ghadi, M., Laouamer, L., Nana, L., Pascu, A. (2016). A novel zero-watermarking approach of medical images based on Jacobian matrix model. Security and Communication Networks, 9(18): 5203-5218. https://doi.org/10.1002/sec.1690

[22] 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

[23] 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

[24] Kaibou, R., Azzaz, M.S., Benssalah, M., Teguig, D., Hamil, H., Merah, A., Akrour, 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