


Toward a Robust Image Watermarking Method: Exploiting Human Visual System Properties in the Spatial Domain



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.400327>

ABSTRACT

Received: 22 February 2023

Accepted: 18 May 2023

Keywords:

robustness, informed watermarking, local binary pattern (LBP), imperceptibility

The need for secure and reliable methods to protect digital content from unauthorized manipulation has become increasingly critical. Although cryptography has been instrumental in addressing digital content security, it is not without shortcomings. In particular, symmetrical cryptographic systems exhibit significant vulnerabilities in encryption key protection, while asymmetric cryptosystems demand high computational time. Consequently, there is an urgent need to explore alternative security solutions to address these limitations. Watermarking has emerged as a promising candidate for ensuring integrity, authenticity, and digital rights protection. In this study, a novel, robust, and informed watermarking approach for color digital images in the spatial domain is proposed, leveraging Local Binary Pattern (LBP) operators for watermark generation. The embedding of the watermark is achieved in the blue channel of the Red, Green, Blue (RGB) image on its corresponding LBP image, owing to the low sensitivity of the blue color in relation to the imperceptibility of the embedded watermark. The proposed approach is evaluated against a diverse range of geometric and non-geometric attacks to demonstrate its reliability. In order to assess the performance of the proposed method in terms of imperceptibility and robustness, watermarked images are subjected to various attacks and analyzed using well-established metrics. The results obtained are highly encouraging, both in terms of the imperceptibility of the embedded watermarks and their robustness against different attack scenarios.

1. INTRODUCTION

In the realm of secure image transmission, cryptography is widely acknowledged as the art of secret codes, while steganography remains relatively obscure. Cryptography entails rendering text or multimedia content indecipherable (and thus secret), whereas steganography focuses on concealing a message within content, making it not indecipherable, but indistinguishable [1]. Watermarking, which involves hiding information, offers technical solutions to address challenges related to rights protection, integrity, and authenticity.

Despite the prevalence of cryptography in security, it exhibits significant weaknesses, particularly in terms of securing keys used in symmetric cryptographic systems and the high computational time required for asymmetric cryptographic systems [2, 3]. These limitations necessitate the exploration of alternative perspectives that provide greater security with reduced computational time, suitable for real-time applications. Research has indicated that data exchange makes data susceptible to unauthorized users who might alter it and infringe on privacy and copyright. Watermarking has the potential to mitigate this vulnerability.

Image watermarking can be classified into two types of schemes: fragile and robust. Fragile watermarking [4, 5] is used solely to verify the authenticity of documents and data integrity. Since protection of the watermark is weak, the conveyed message is of little importance. The watermark is

part of the document, and when modified, the embedding is also fragile. This type of watermarking still poses a problem, as it does not prove the authorship of the document, even if it confirms that a document has been altered. Robust watermarking [6-8], on the other hand, must withstand various attacks and have two key properties: 1) resistance to known attacks such as resampling, JPEG compression, cropping, and noise, and 2) easy recognizability of the watermark after extraction, despite damage inflicted by various attacks.

Watermarking schemes can be implemented based on the domain of watermark insertion/extraction (spatial or frequency) and the method of watermark extraction post-attack (blind, semi-blind, or non-blind). In spatial watermarking [9], the watermark is directly embedded in the host image's pixels without prior preprocessing, unlike in the frequency domain [10, 11], where the host image must undergo spectral transformations. Watermark extraction can occur in three primary ways: a) blind watermarking [12], where only the watermarking key is used to extract the attacked watermark, b) semi-blind [13], where the original watermark is needed in the extraction process, and c) non-blind [14], where the host image is required for watermark extraction.

This paper proposes a novel spatial image watermarking scheme based on a key feature of the human visual system (HVS) — the blue component of an RGB image — using local binary patterns (LBP). Embedding the watermark in the

blue component is chosen due to the human eye's lower sensitivity to blue color changes, minimizing perceptual alterations in the watermarked image. The choice to use the blue component and LBP is motivated by their relationship with the HVS, as embedding the watermark in textured regions of the corresponding blue components in RGB images enhances the imperceptibility of embedded watermarks and significantly contributes to robustness. It is well-established that watermarking in textured zones guarantees high watermark imperceptibility (as in the case of using LBP) and that the blue component in any RGB image is less sensitive to changes compared to red and green colors.

Exploiting the blue component of the RGB image and its corresponding LBP allows for the assessment of imperceptibility between the host image and the watermarked image. The approach also enables a reduction in computational time and memory consumption versus data payload while maintaining a high degree of imperceptibility and robustness.

This paper is organized as follows. Section 2 presents recent watermarking techniques in the literature regarding image content security. Section 3 provides an overview of the HVS. Section 4 details the local binary pattern (LBP) and its relationship with the HVS. Section 5 outlines the proposed watermarking scheme for watermark embedding and extraction. Section 6 discusses the experimental results in terms of the proposed approach's imperceptibility and robustness. Finally, Section 7 concludes the paper.

2. RELATED WORK

In this section, a state of the art of the most recent and relevant image security techniques presented in the literature is introduced. It should be noted that the problem of image security covers several aspects including image content protection, integrity of the exchanged data, authentication, and robustness of watermarks against attacks applied to digital images, 3D images, medical images, videos, etc.... The most widespread techniques related to these aspects are symmetric and asymmetric encryption techniques; homomorphic encryption techniques in case the image is hosted in the cloud; and information hiding techniques where the data payload is an important element. The focus in this section will be more on image watermarking techniques which are related to the subject of this paper.

Image encryption is a science with the goal of making the content of an image unreadable, which increases the protection of its content against illegal manipulation. Symmetric encryption essentially relies on one key for encryption and decryption. This type of encryption can take several forms, like for example the case of chaotic maps. Authors [15] present a new 3D chaotic logistical map with DNA encoding approach both for confusion and diffusion of image pixels. The proposed approach generates three keys of 32-bit size. First, the approach is based on the generation of initial conditions to build the chaotic map from the three symmetric keys proposed to be used in image row and column permutation. DNA encoding is used for the dissemination of these random pixels and applying the XOR operation between DNA encoded input image and key image. The proposed approach produces a remarkable result regarding the security of the images content but requires a high computation time.

Asymmetric encryption systems show more efficiency and power than symmetric encryption systems. This power lies in the uses of relation to the keys since it uses two keys, one for encryption and the other one for decryption as well as in the considerable sizes of the keys. A new technique proposed in study [16], is based on improving the equal modulus decomposition security (EMD) by combining EMD in the Fresnel transform domain and a sparse sampling to authenticate any image. A nonlinear correlation is exploited to authenticate the decrypted image with the plaintext. The percentage of extracted pixels does not have to be determined deliberately and a numerical simulation has been applied to validate the proposed technique.

Authors [17] address the problem of data capacity to be embedded in an image with less distortion in the host image's quality. To this end, they propose an algorithm based on ridge regression for reversible data hiding which predicts errors with high precision. The authors, prove that the predictor based on ridge regression is more accurate and provides smaller prediction errors compared to the predictor based on least squares. Through their experimental results, they show that the proposed method outperforms the existing adaptive reversible data hiding method in terms of prediction accuracy and embedding performance. Despite its high accuracy, the proposed approach requires more execution time than some existing predictors.

Another approach regarding reversible data hiding was proposed in study [18]. The approach consists of a novel code division multiplexing (CDM) algorithm based on reversible data hiding where the cover data are designated by different orthogonal spreading sequences and which will be embedded in an overlapping manner. The orthogonal spreading sequences are generated from the Walsh Hadamard matrix. A multilevel data embedding will be allowed which significantly increase the data embedding capacity by keeping the quality of the host image. The authors show that the obtained results can achieve better performance by increasing data embedding capacity compared to some existing methods. The security of the proposed approach not only relies on the method itself but also on the spreading sequence.

For securing 3D images, a new approach has been proposed in study [19]. The approach is based on multi-parameter cosine number transform. This transform is calculated based on three-dimensional cosine number transform (3D-CNT) which constitutes a possible Eigen-basis for the Laplacian of the cubical lattice graph evaluated in a finite field. 3D-CNT is known by rotating the 3D-CNT basis vectors, using a finite field rotation operator. A medical image is encrypted using 3D-CNT by exploring the rotation angles as secret parameters. Based on the results they obtained, authors conclude that the proposed scheme is resistant against the main cryptographic attacks.

The authors in study [20] proposed an approach for color image watermarking based on genetic and gray wolf techniques. The proposed approach focuses on the invisible regions of the host image by embedding more watermark information which significantly increases the payload of the hidden data. The objective is to achieve a better imperceptibility of the watermark and a better robustness against geometric and non-geometric attacks. The authors show based on their experiments that their approach requires more computation for both watermark embedding and extraction than to Local Binary Pattern (LBP) and fractal

estimates. The approach however presents some weaknesses against Filtering and JPEG compression attacks.

In study [21], the authors proposed an approach for color watermarking images in the spatial domain based on fuzzy rough sets. The main goal of the proposed approach is to select the accurate blocks which will be considered for watermark embedding by keeping high watermark imperceptibility. The proposed approach is based on one of the main characteristics of the HVS which is the eye color sensitivity. Realizing watermark embedding was focused mainly on the textured and semi smooth blocks by taking into consideration the main three channels of color distribution especially the blue component. The measured Bit Error Ratio (BER) between the original watermarks and the extracted ones presented some weakness particularly against adding noise attacks.

An Elliptic Curve Cryptography (ECC) is proposed in study [22]. The approach is semi-blind which consist of achieving watermarking with a binary watermark. The embedding and extraction processes were achieved using Discrete Wavelet Transform (DWT)- Singular Value Decomposition (SVD) transforms. Exploiting the HVS based on entropy was proposed to designate the appropriate blocks in spatial domain considered for watermarking. DWT is computed for the chosen blocks and the watermark embedding is realized in singular values of each DWT block. The use of DWT-SVD with ECC achieves better performance. Moreover, the HVS based on entropy was implemented to incrust the ECC encrypted binary watermark in host images. Luminance, Contrast and Edge Sensitivity, perform better both in terms of imperceptibility and robustness.

The authors in study [23], suggest a novel HVS based spread spectrum method to scalable image watermarking. A Discrete Wavelets Transforms (DWT) was applied to scalable watermark into the whole frequency sub-bands of the wavelet decomposed host image. The watermark is embedded in each DWT sub-band by selecting only the highly textured, highly contrasted and very dark/bright areas of the image. In the low frequencies sub-bands, an independent analysis of texture is achieved to select the concerned low sub-bands based on coefficients amplitude and local entropy to embed the watermark. The proposed approach can ensure authenticity, especially in heterogeneous networks.

In study [24], a robust image watermarking approach has been proposed against geometric attacks. A color watermarking approach with a blind manner was detailed combining Discrete Cosine and Discrete Wavelets Transforms (DCT and DWT respectively). The host image is transformed into the Y: Luminance, Cb: blue difference, Cr: red difference (YCbCr) color channels. The watermark is incrust in those three channels. It is embedded regarding the HVS on the applied Discrete Cosine Transform (DCT) and DWT coefficients of the host image. To correct the rotation, Zernike moments are applied. The obtained results are significant only against some limited geometric attacks.

The authors in study [25], suggested a new intelligent image watermarking approach based on singular values decomposition (SVD) and discrete wavelet transform (DWT) exploiting HVS characteristics and particle swarm optimization (PSO). A DWT of level 1 has been applied to the host image by selecting only the LL sub-band of the DWT transformed image to embed the watermark. The

selected LL sub-band is based on HVS. The SVD is used on the selected DWT LL sub-bands blocks, and every two watermark bits are embedded indirectly into the U and Vt matrices of the SVD decomposition. Scaling factors are chosen automatically by (PSO) In order to increase the robustness.

3. HUMAN VISUAL SYSTEM

To properly hide a watermark in an image, it would be helpful to exploit the weaknesses of the human visual system (HVS). However, HVS is extremely complex, and many of its properties are still not well understood. Many important aspects related to HVS such the variation of contrast sensitivity, the masking phenomenon etc. have been studied.

Contrast Sensitivity [26] is a measure of the relative variation in luminance. Unfortunately, there is no definition of contrast that is appropriate for all kinds of visual stimuli. In psycho-visual experiments, periodic patterns are often used, for example sinusoids, whose luminance varies between two bounds. Masking [27] is a very important visual phenomenon describing the interactions between stimuli. The meaning of masking is when a stimulus, which is visible alone, cannot be perceived because of the presence of another stimulus. In the context of digital watermarking, the proposed approach considers the watermark as the stimulus that is masked by the host image, which therefore functions as the background. This masking explains why the noise of the watermark is unpleasant in certain regions of an image while it is barely noticeable elsewhere. In other words, masking increases the threshold of visibility depending on the contrast of the mask.

The human eye is less sensitive to changes that an image may undergo, especially in the textured areas and the blue color channel [28]. Embedding ac watermark in the blue component minimizes the perceptual changes of the watermarked image. This operation is a part of the masking techniques since it consists of performing watermarking on an invisible component which is less sensitive to any changes within a color image. Figure 1 illustrates the main three components (red, green and blue) of a color image.

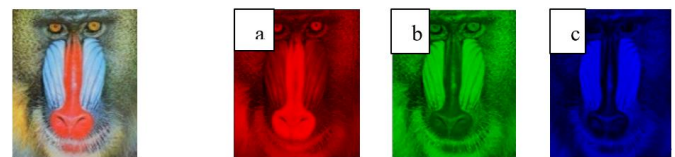


Figure 1. Host image Baboon and its three components: a) red channel, b) green channel and c) blue channel

4. LOCAL BINARY PATTERN

The Local Binary Pattern (LBP) is a well-known technique in computer vision and in particular for image classification. This technique substantially describes the content of an image through its textural regions. It describes remarkably the image content through its texture. Similarly, LBP is efficient, robust to monotonic gray-scale changes caused, for example by illumination variations [29, 30].

Local binary patterns (LBP) are features used in computer vision to recognize textures or for object extraction in digital

images. The idea of the Local binary pattern texture operator is to assign each pixel a code depending on the gray levels of its neighborhood. The gray level of the central pixel (g_c) with coordinates (x_c, y_c) is compared to that of its neighbors (g_p) according to Eq. (1) [31]. where p is the number of neighboring pixels. It is considered for the calculation of the LBP a neighborhood of 3×3 from where $p=8$ neighbors which gives as a result an image in gray levels, a matrix containing values of the LBP ranging between 0 and 255 for each pixel. Local primitives extracted by LBPs include detection of line end spot, edge, spot/flat, corner, etc.

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

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

The calculation of the local binary pattern is well described in Figure 2.

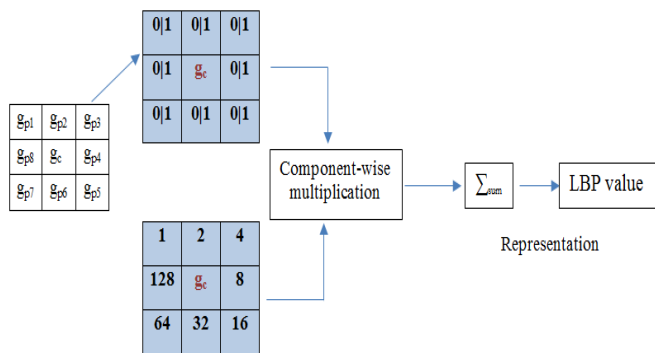


Figure 2. LBP operator computation

5. IMAGE WATERMARKING MODEL DESCRIPTION

The watermarking model proposed in this paper consists mainly of three essential steps: watermark embedding, attacks on the watermarked images and watermark extraction. These steps are described in detail below. The model's description is illustrated in Figure 3.

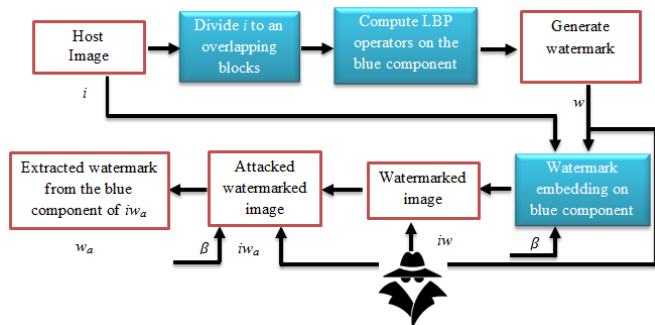


Figure 3. Image watermarking description model

The proposed watermarking scheme operates only on color images since the watermark embedding is achieved on only the blue component after coming out its Local Binary Patterns (LBP). This advantage can be explained by the fact that the LBP represents the textured areas of the image and using only the blue color is due to the fact that changes that

an image can have during watermark embedding are less sensitive to the human eye in the blue channel and textured areas.

5.1 Embedding of watermark

To achieve the watermark embedding, it is imperative firstly to calculate the local binary pattern LBP only for the blue component of the host image. The LBP image will be embedded within the blue component of the host image. The watermark embedding is achieved with a linear interpolation as illustrated in Eq. (2) [32]. With the parameter β , it will be possible to control the visibility/invisibility of the incusted watermark can be managed by varying the values of β .

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

where, i_w , i , w are the watermarked, host and watermark images respectively. Knowing that $\beta \in]0, 1[$. The watermark embedding process and generating the watermark from the blue component of the host image based on the local binary pattern operators is illustrated in Figure 4.

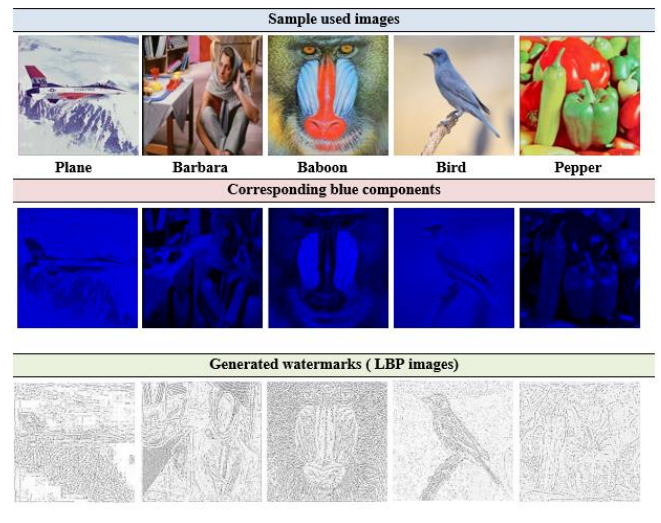


Figure 4. Generating watermark and the embedding process

5.2 Attacks

To assess the performance of our model, geometric and non-geometric attacks have been simulated using one of the popular benchmarks in digital image watermarking called Stirmark [33]. Stirmark contains a variety of attacks such as JPEG compression, adding noise, rotation, filtering, convolution, affine attacks, etc. These attacks are aimed at influencing the embedded watermark and not the watermarked image in itself. Figure 5 illustrates some of these attacks on the five images (Plane, Barbara, Baboon, Bird and Peppers).

The description of the illustrated attacks is summarized in Table 1.

The watermark extraction is done by an inverse operation of Eq. (1) (watermark embedding) as shown in Eq. (3) [32].

$$w_a = \frac{1}{\beta} w - \frac{1 - \beta}{\beta} i_{w_a} \quad (3)$$

where, w_a , w and i_{w_a} are respectively the attacked watermark,

the original watermark and the attacked watermarked image. Knowing that $0 < \beta < 1$.

Table 1. A brief description of the used attacks

Attack name	Description
JPEG_90	JPEG compression with quality factor=90
Conv_2	Convolution with factor=2
Rotate_45	Rotation with 45 degrees
Noise_80	Adding noise with density degree=80
Median_9	Median filtering by 3×3
RML_90	Removing lines (3×3)
Affine_2	Affine transform (changing image size)
Cropping_25	Cropping image

imperceptibility between the host image and the watermarked image. The approach also makes possible to reduce the computational time/ memory consumption Vs data payload while maintaining a high degree of imperceptibility and robustness.

6.1 Imperceptibility and robustness

Evaluating the performance of the proposed model consists of measuring metrics, the Peak Signal Noise Ration PSNR [32] metric (see Eq. (4)) between the original images and their corresponding watermarked images. A PSNR exceeding 34 dB means that the watermarked image and the host image are visually the same, which means that the imperceptibility is quasi-guaranteed.

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

Figure 6 illustrates the PSNRs of the different used images.

Attacks	Watermarked images i_w				
Jpeg_90					
Noise_80					
Rotation_45					
Median_9					
Conv_2					
RML_90					
Affine_2					
Cropping_25					
PSNR between image i and i_w					
	60.2541	50.5819	50.9423	63.3791	49.3431

Figure 6. PSNR between the host images and their corresponding watermarked images

It should be noted that the PSNR values for all the images used are considerably high and greatly exceed 34dB. These results reflect that the criterion of imperceptibility between host images and their corresponding watermarked images is well verified. This strong imperceptibility is due to the watermarking in the textured areas using the LBP operators where the human eye is less sensitive to modifications.

The robustness criterion can be measured by calculating the correlation coefficients (CC) and the Bit Error ratio (BER) between the original watermark and its corresponding extracted one. The principle of digital image correlation [30] is based on tracking information from a so-called reference image with the modified or interfered images, often called distorted images. This means that the correlation coefficient enables pixel tracking over the set of observed pixels. The correlation coefficient between two images is calculated according to Eq. (5). If the CC value is close to 1, it means that the two images are similar. Otherwise, if the CC value is close to 0, this reflects the dissimilarity between these two images.

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

6. RESULTS INTERPRETATION

The exploitation of the blue component of the RGB image and its corresponding LBP allow us to verify the

where, w and w_a are respectively the original watermark and the extracted one.

The loss of information within the image occurs when one or more data packets passing through a network fail to reach their destination correctly. Packet loss is considered to be one of the main types of errors encountered in digital communications. The Bit Error Rate (BER) [32, 34] expresses the erroneous bits and spurious packets caused by noise. These erroneous bits from the total bits of a sent image can be expressed by calculating the BER as defined in Eq. (6).

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

The values of the correlation coefficients as well as the BER between the original watermarks w and the extracted ones w_a are well illustrated in Figure 7. The calculated CCs are in all cases close to 1, while the BERs represent low values in most cases. These results endorse the robustness of watermarks against multiple attacks used.

It should be noted that the values of the correlation coefficients (CC) are in their majority around the value 1 and this for various attacks applied to the watermarked images namely JPEG compression, convolution, rotation, adding noise, median filtering, removing lines, affine transformation, and cropping. These results signify the effectiveness of the proposed watermarking scheme.

6.2 Performances comparison

In this research, a comparison of the proposed approach with other relevant and recent approaches has been conducted focusing on terms of imperceptibility and robustness represented by the PSNR and CC correlation metrics. The results obtained through our assessment are very encouraging compared to the work presented in studies [35-37]. Our approach operates in the spatial domain and despite that, we compared it with other research that operates in the frequency domain to evaluate the strength of our approach. Indeed, it is well known that watermarking approaches in the frequency domain are more robust in resisting attacks compared to watermarking approaches in the spatial domain. Table 2 and Table 3 summarize the comparison in terms of imperceptibility as measured by PSNR and robustness as measured by CC.

Furthermore, this research performs a comparison of the proposed approach with recent approaches in terms of imperceptibility as measured by the PSNR metric for commonly used images (Baboon, Barbara and pepper). This research is better in terms of PSNR compared to the work in in study [37] which also operates in the spatial domain. Our results are close to the results obtained in study [36] but worse than the proposed approach in in study [35]. The results obtained in in study [35] are more encouraging because the approach operates in the frequency domain, and this is quite normal since the methods based on watermarking in the frequency domain are more efficient than those in the spatial domain, and they require more time in watermark embedding/extracting than the spatial methods.

Similarly, to compare the robustness of the proposed approach with other methods against the attacks described earlier, the CC of the proposed approach is compared to CC of the approaches in studies [32, 34, 35]. In most cases for the commonly used attacks (median filtering, Gaussian noise, cropping and rotation), our approach yields better results that are almost as good as the approach proposed in study [32]. Our obtained values are very close to 1, which means a significant robustness against attacks in question.






Attacks	Watermark images w				
					
JPEG_90	CC=0.9999	CC=0.9999	CC=0.99995	CC=0.99997	CC=0.9982
	BER=3.22%	BER=10.17%	BER=8.29%	BER=3.53%	BER=12.33%
Conv_2	CC=0.985	CC=0.997	CC=0.9967	CC=0.9999	CC=0.9999
	BER=18.23%	BER=19.81%	BER=19.15%	BER=17.23%	BER=20.03%
Rotate_45	CC=0.9997	CC=0.9994	CC=0.9999	CC=0.9999	CC=0.9993
	BER=10.39%	BER=15.01%	BER=13.73%	BER=10.26%	BER=16.57%
Noise_80	CC=0.9999	CC=0.9999	CC=0.9999	CC=0.99993	CC=0.9999
	BER=13.4%	BER=15.3%	BER=14.76%	BER=13.06%	BER=15.64%
Median_9	CC=0.9999	CC=0.9998	CC=0.9999	CC=0.9999	CC=0.9997
	BER=3.07%	BER=10.16%	BER=8.48%	BER=3.43%	BER=12.51%
RML	CC=0.9999	CC=0.9999	CC=0.9996	CC=0.9998	CC=0.9994
	BER= 11.4%	BER= %9.87	BER= %6.23	BER= %9.81	BER= %11.34
Affine	CC=0.9998	CC=0.9998	CC=0.9997	CC=0.9996	CC=0.9996
	BER=10.56%	BER=10.14 %	BER= %7.58	BER= %10.33	BER= %13.24
Cropping	CC=0.9989	CC=0.9988	CC=0.9987	CC=0.9986	CC=0.9985
	BER= 15.8%	BER=16.35 %	BER= 12.69%	BER=13.58 %	BER= 14.84%

Figure 7. CC and BER between the original watermarks and their corresponding extracted watermarks

Table 2. PSNR comparison for commonly used images

Methods Used domain	Frequency domain [35]	Spatial domain [36]	Frequency domain [37]	Proposed approach Spatial domain
Baboon image	54.84	56.2988	42.9159	50.9423
Barbara image	-	56.3031	-	50.5819
Pepper image	54.29	56.0917	42.9477	49.3431

Table 3. Robustness comparison using NC metric with commonly used images

Methods	Algorithm [32]	Algorithm [34]	Algorithm [35]	Proposed approach
Median filtering	0.99710	0.8991	0.9263	0.9998
Cropping	0.99709	0.989	0.8125	0.9997
Salt & pepper noise	0.99704	0.9895	0.9816	0.999
Rotation 45°	0.99701	0.98	0.7701	0.9995

7. CONCLUSIONS

This paper addresses an important topic in information security which consists of protecting an image's contents in terms of integrity, copyright, and authenticity through to main factors which are: imperceptibility and watermark robustness. A new approach for color images watermarking has been proposed exploiting some human visual system weaknesses by selecting only image regions concerned by the watermark embedding; namely the sensitivity to the blue color component as well as the texture expressed by the local binary pattern (LBP). This represents an improvement over some related approaches in the literature. The approach consists of watermarking the blue component by generating an informed watermark through its local binary pattern (LBP). This choice is due to the fact that the textured areas and the blue component of the RGB image are less sensitive to changes when inserting a watermark in the host image. The performance of the proposed approach has also been assessed by measuring the imperceptibility and robustness of the watermark against several scenarios of attacks. The imperceptibility was measured by the PSNR metric (Peak Signal Noise Ratio). Whereas, robustness was measured by two known metrics such: Correlation Coefficients (CC) and Bit Error Ratio (BER). The approach shows remarkable efficiency through the obtained results of PSNR, CC and BER metrics.

In future works, we will exploit other tracks while pressing the characteristics of the human visual system (HVS) in order to find other factors related to the textures within the image or the contrast sensitivity function (CSF) requiring less watermark data payload while selecting the most relevant areas of interest within image. Of course, these perspectives should not affect the imperceptibility and robustness of the watermark against attacks.

ACKNOWLEDGMENT

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-2-4-1-27596). The authors also thank Qassim University for technical support.

REFERENCES

- [1] Qi, L., Wang, X., Ma, B., Wang, X., Wang, C., Gao, S., Shi, Y. (2022). Concealed attack for robust watermarking based on generative model and perceptual Loss. *IEEE Transactions on Circuits and Systems for Video Technology*, 32(8): 5695-5706. <https://doi.org/10.1109/TCSVT.2021.3138795>
- [2] Gao, S., Wu, R., Wang, X., Wang, J., Li, Q., Wang, C., Tang, X. (2023). A 3D model encryption scheme based on a cascaded chaotic system. *Signal Processing*, 202: 108745. <https://doi.org/10.1016/j.sigpro.2022.108745>
- [3] Wu, R., Gao, S., Wang, X., Liu, S., Li, Q., Erkan, U., Tang, X. (2022). AEA-NCS: An audio encryption algorithm based on a nested chaotic system. *Chaos, Solitons & Fractals*, 165: 112770. <https://doi.org/10.1016/j.chaos.2022.112770>
- [4] Huang, L., Kuang, D., Li, C.L., Zhuang, Y.J., Duan, S.H., Zhou, X.Y. (2022). A self-embedding secure fragile watermarking scheme with high quality recovery. *Journal of Visual Communication and Image Representation*, 83: 103437. <https://doi.org/10.1016/j.jvcir.2022.103437>
- [5] Lefèvre, P., Carré, P., Fontaine, C., Gaborit, P., Huang, J. Efficient image tampering localization using semi-fragile watermarking and error control codes. *Signal Processing*, 190: 108342. <https://doi.org/10.1016/j.sigpro.2021.108342>
- [6] Artiles, J.A.P., Chaves, D.P.B., Pimentel, C. (2022). Robust image watermarking algorithm using chaotic sequences. *Journal of Information Security and Applications*, 68: 103219. <https://doi.org/10.1016/j.jisa.2022.103219>
- [7] Wang, C., Ma, B., Xia, Z., Li, J., Li, Q., Shi, Y.Q. (2022). Stereoscopic image description with trinion fractional-order continuous orthogonal moments. *IEEE Transactions on Circuits and Systems for Video Technology*, 32(4): 1998-2012. <https://doi.org/10.1109/TCSVT.2021.3094882>
- [8] Su, Q., Liu, D., Sun, Y. (2022). A robust adaptive blind color image watermarking for resisting geometric attacks. *Information Sciences*, 606: 194-212. <https://doi.org/10.1016/j.ins.2022.05.046>
- [9] Yuan, Z., Su, Q., Liu, D., Zhang, X., Yao, T. (2021). 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>
- [10] Singha, R., Ashokb, A. (2021). An optimized robust watermarking technique using CKGSA in frequency domain. *Journal of Information Security and Applications*, 58: 102734. <https://doi.org/10.1016/j.jisa.2020.102734>
- [11] Kalpanasonika, R., Agnes, S.A. (2014). A Resilient digital watermarking exploiting spatial and frequency domain against image hackers. 2014 Informatics and Communication Technologies for Societal Development Conference, Kochi, Kerala, India, pp. 167-172. https://doi.org/10.1007/978-81-322-1916-3_17
- [12] Sinhal, R., Ansari, I.A., Ahn, C.W. (2020). Blind image watermarking for localization and restoration of color images. *IEEE Access*, 8: 200157-200169. <https://doi.org/10.1109/ACCESS.2020.3035428>
- [13] Koju, R., Joshi, S.R. (2016). Semi blind color image watermarking using Slant transform. 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics, Chennai, India. <https://doi.org/10.1109/AEEICB.2016.7538342>
- [14] Anbarjafari, G., Ozcinar, C. (2018). Imperceptible non-blind watermarking and robustness against tone mapping operation attacks for high dynamic range images. *Multimedia Tools and Applications*, 77: 24521-24535. <https://doi.org/10.1007/s11042-018-5759-1>
- [15] Patel, S., Bharath, K.P., Kumar, R.M. (2020). Symmetric keys image encryption and decryption using 3D chaotic maps with DNA encoding technique. *Multimedia Tools and Applications*, 79: 31739-31757. <https://doi.org/10.1007/s11042-020-09551-9>
- [16] Luan, G., Li, A., Zhang, D., Wang, D. (2019). Asymmetric image encryption and authentication based on equal modulus decomposition in the fresnel

- transform domain. *IEEE Photonics Journal*, 11(1): 6900207. <https://doi.org/10.1109/JPHOT.2018.2886295>
- [17] Wang, X., Wang, X., Ma, B., Li, Q., Shi, Y.Q. (2021). High Precision Error Prediction Algorithm Based on Ridge Regression Predictor for Reversible Data Hiding. *IEEE Signal Processing Letters*, 28: 1125-1129. <https://doi.org/10.1109/LSP.2021.3080181>
- [18] Ma, B., Shi, Y.Q. (2016). A reversible data hiding scheme based on code division multiplexing. *IEEE Transactions on Information Forensics and Security*, 11(9): 1914-1927. <https://doi.org/10.1109/TIFS.2016.2566261>
- [19] Lima, V.S., Madeiro, F., Lima, J.B. (2020). Encryption of 3D medical images based on a novel multiparameter cosine number transform. *Computers in Biology and Medicine*, 121: 1-13. <https://doi.org/10.1016/j.combiomed.2020.103772>
- [20] Favorskaya, M.N., Pakhirka, A.I. (2021). Adaptive HVS objectivity-based watermarking scheme for copyright protection. *Procedia Computer Science*, 192: 1441-1450. <https://doi.org/10.1016/j.procs.2021.08.148>
- [21] Ghadi, M., Laouamer, L., Nana, L., Pascu, A. (2016). Fuzzy rough set based image watermarking approach. *Proceedings of the International Conference on Advanced Intelligent Systems and Informatics*, Cairo, Egypt, pp. 234-245.
- [22] Gupta, R., Mishra, A., Jain, S. (2018). A semi-blind HVS based image watermarking scheme using elliptic curve cryptography. *Multimedia Tools and Applications*, 77: 19235-19260. <https://doi.org/10.1007/s11042-017-5351-0>
- [23] Amiri, M.D., Meghdadi, M., Amiri, A. (2019). HVS-based scalable image watermarking: A novel approach to image copyright protection against scalable compression. *Multimedia Tools and Applications*, 78: 7097-7124. <https://doi.org/10.1007/s11042-018-6419-1>
- [24] Bei, Y.L., Qiao, S., Liu, M.X., Zhu, X.R., Zhang, Q. (2018). A color image watermarking scheme against geometric rotation attacks based on HVS and DCT-DWT. *2018 International Conference on Security, Pattern Analysis, and Cybernetics*, Jinan, China. <https://doi.org/10.1109/SPAC46244.2018.8965467>
- [25] Ahmadi, S.B.B., Zhang, G., Wei, S., Boukela, L. (2021). An intelligent and blind image watermarking scheme based on hybrid SVD transforms using human visual system characteristics. *The Visual Computer*, 37: 385-409. <https://doi.org/10.1007/s00371-020-01808-6>
- [26] Triantaphillidou, S., Jarvis, J., Psarrou, A., Gupta, G. (2019). Contrast sensitivity in images of natural scenes. *Signal Processing: Image Communication*, 75: 64-75. <https://doi.org/10.1016/j.image.2019.03.002>
- [27] Li, D., Zhai, G., Yang, X., Hu, M., Liu, J. (2017). Perceptual information hiding based on multi-channel visual masking. *Neurocomputing*, 269: 170-179. <https://doi.org/10.1016/j.neucom.2017.04.072>
- [28] Thongkor, K., Amornraksa T. (2014). Digital image watermarking with partial embedding on blue color component. *Signal and Information Processing Association Annual Summit and Conference*, Cambodia. <https://doi.org/10.1109/APSIPA.2014.7041667>
- [29] Bhagat, P.K., Choudhary, P., Singh, K.M. (2019). A comparative study for brain tumor detection in MRI images using texture features. *Advances in ubiquitous sensing applications for healthcare, Sensors for Health Monitoring*, Academic Press, 5: 259-287. <https://doi.org/10.1016/B978-0-12-819361-7.00013-0>
- [30] Jegan, R., Jayagowri, R. (2023). Windowed modified discrete cosine transform based textural descriptor approach for voice disorder detection. *Implementation of Smart Healthcare Systems using AI, IoT, and Blockchain, Intelligent Data-Centric Systems*, Academic Press, pp.147-167. <https://doi.org/10.1016/B978-0-323-91916-6.00007-2>
- [31] Bedi, A.K., Sunkaria, B.K., Randhawa, S.K. (2018). Local Binary Pattern Variants: A Review. *2018 First International Conference on Secure Cyber Computing and Communication*, Jalandhar, India. <https://doi.org/10.1109/ICSCCC.2018.8703326>
- [32] Ghadi, M., Laouamer, L., Nana, L., Pascu, A.C. (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>
- [33] Petitcolas, F.A.P., Anderson, R.J., Kuhn, M.G. (1998). Attacks on copyright marking systems. In: David Aucsmith (eds), *Information Hiding*, Second International Workshop, Portland, Oregon, U.S.A. <https://www.petitcolas.net/watermarking/stirmark/>.
- [34] Alshoura, W.H., Zainol, Z., Teh, S., Alawida, M., Alabdulatif, A. (2021). Hybrid SVD-based image watermarking schemes: A review. *IEEE Access*, 9: 32931-32968. <https://doi.org/10.1109/ACCESS.2021.3060861>
- [35] Alshoura, W.H., Zainol, Z., Teh, J.S., Alawida, M. (2022). An FPP-resistant SVD-based image watermarking scheme based on chaotic control. *Alexandria Engineering Journal*, 61: 5713-573. <https://doi.org/10.1016/j.aej.2021.10.052>
- [36] Rinki, K., Verma, P., Singh, R.K. (2022). A novel matrix multiplication based LSB substitution mechanism for data security and authentication. *Journal of King Saud University – Computer and Information Sciences*, 34(8): 5510-5524. <https://doi.org/10.1016/j.jksuci.2021.01.013>
- [37] 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>