Secure fragile watermarking based on Huffman encoding and optimal embedding strategy

Mourad Zairi, Tarik Boujiha, Abdelhaq Ouelli
Department of Electrical Engineering, Networks and Telecommunication Systems-Engineering Science Laboratory,
Ibn Tofail University, Kenitra, Morocco

Article Info

Article history:

Received May 25, 2022
Revised Oct 19, 2022
Accepted Oct 31, 2022

Keywords:

Embedding strategy
Fragile watermarking
Huffman encoding
Information security
Scrambled watermark

ABSTRACT

Image watermarking is one of the most popular techniques used to assure information security, integrity, and authenticity. Watermarking algorithms can be categorised, according to the domain of insertion, as either spatial or spectral domain-based watermarking approaches. The resulted watermark can also be classified as either strong designed to withstand malicious attacks or fragile designed to detect every possible alteration. In order to combine the advantages of the two categories of watermarking algorithms, this paper proposes a new fragile hybrid domain-based watermarking scheme to get both robustness and imperceptibility using an optimal embedding strategy according to the entropy values of the host images blocs. To enhance security and safety, the watermark undergoes an encryption using Huffman encoding to produce a scrambled watermark. This scheme is evaluated based on different metrics like the peak signal to noise ratio, the structural index similarity, and the normalized correlation coefficient, satisfactory results are attained. The experimental results show that Huffman encryption and optimal blocs selection offer good features of security and imperceptibility.

Corresponding Author:

Mourad Zairi
Department of Electrical Engineering, Networks and Telecommunication Systems-Engineering Science Laboratory, Ibn Tofail University
B.P 241, Kenitra, Morocco
Email: mouradzairi@gmail.com

1. INTRODUCTION

Nowadays, digital networks are so developed that they have become an essential communication mechanism. They allow the transmission of all kinds of digital data: text, sound, and mainly images. The increased use of multimedia applications raises more and more problems concerning the preservation of the confidentiality and authenticity of these digital data, in particular images which must be protected from any falsification [1]. The appropriate solution to this problem is the use of the fragile watermarking methods. These methods are suitable for verifaying the integrity and awner authenticity. The fragile watermark can be distorted and the hidden information is lost or modified as soon as the host image undergoes a modification [2]. Thereby, the loss of the watermark or its alteration will be taken as a proof that the data has been modified, while the recovery of the watermark is used to demonstrate the integrity of data. The watermarking algorithms found in the literature can be divided according to the domain of insertion into two categories [3]: watermarking in spatial domain and watermarking in spectral domain.

In the spatial domain, the watermark is inserted by directly modifying the pixel values of the host image [4]. Several approaches have been developed in this domain. Among these algorithms we find the conventional least significant bit (LSB) method [5], which is used because of its simplicity and its little effect on the image [6]; the LSB of the host image is replaced by the most significant bit (MSB) of the watermark, these changes cannot be perceived by the human visibility system. While in the approaches related to the spectral domain, the embedding part is carried out after the transformation of the host image using one of the following transforms or a combination between them [7], [8]: discrete fourier transform (DFT), discrete cosine transform (DCT), and discrete wavelets transform (DWT).

Spectral domain-based watermarking approaches are known for their good robustness against multiple attacks [9], [10]. Many research works have been carried out, Al-ardhi *et al.* [11] used a watermarking scheme based on linear cellular automata transform (LCAT) algorithm operating in the spectral domain to protect the vector maps under copyright, the proposed scheme presents robustness against geometric attacks, namely, translation, scaling, and rotation. To reach the same goal, Neyman *et al.* [12] proposed a watermarking algorithm based on the fast fourier transform (FFT) to embed a copyright marker into vector map.

However, the spatial domain watermarking techniques are computationally simpler, they offer a good impercptability but they provide less protection against attacks, namely, geometric attacks such as scaling, printing and scanning, changing ratio, and cropping. Several algorithms were previously presented regarding this matter; Many watermarking methods developed in the past employed the singular value decomposition (SVD) [13], [14]. Shehab *et al.* [15] proposed an SVD based fragile watermarking scheme using grouped block method offering more security and providing the possibility to locate the attacked areas inside different medical images. Bal *et al.* [16] presented an LSB watermarking procedure based on bit pair similarity, to make the watermark more secure the authors utilized symmetric key cryptography. Kumar and Singh [17] proposed a novel scheme based on the encryption of the watermark image by using the Hill Cipher method before the embedding procedure, the robustness of this method was demonstrated by testing multiple attacks. Zhang *et al.* [18] proposed a robust image watermarking scheme based on mathematical features of SVD in the spatial domain and Arnold's transformation to encrypt the watermark. To secure medical images in digital imaging and communications in medicine (DICOM) format, Ayu *et al.* [19] proposed a digital watermarking technique based on the encryption of the DICOM confidentiality tags using the AES256 encryption algorithm and the insertion into the 2nd LSB of the medical image, the proposed technique maintains image quality and resist to several malicious attacks. In order to provide a full security system for medical information (imaging and report) in terms of confidentiality, authentication and integrity, Boussif *et al.* [20] proposed an approach which combine a semi reversible build watermarking method robust to JPEG compression, build fragile watermarking, and a stream cipher symmetric encryption algorithm. Joshi *et al.* [21] presented a detailed study of LSB method using different secret message sizes to analyze its impact on the PSNR and MSE metrics. Rinki *et al.* [22] proposed a new LSB digital watermarking scheme based on the selection of the non-consecutive matrix of pixels to replace the last three bits of each RGB components of the host image by the bits of the watermark image, the authors claimed that this scheme enhance robustness, imperceptibility, and security. Sowmya *et al.* [23] proposed an algorithm based on the embedding of a watermark into another watermark in addition to encrypting the main watermark using A5/1 encryption algorithm, then the encrypted watermark is inserted into the two LSBs of the host image green and blue components. This scheme enabled increasing embedding capacity and safety.

In order to combine the good features of the two previous categories, hybrid domain-based watermarking approaches are investigated to get both robustness and imperceptibility. Kumar *et al.* [24] proposed a method combining embedding in wavelet domain and spatial domain to improve authenticity, security and copyright protection. In addition to classify watermarking algorithms according to the domain of insertion, watermarking methods may be also classified as strong watermarking [14] and fragile watermarking [15]. The strong watermarking method allows extraction of hidden watermarks from watermarked images, even after image processing such as image compression and filtering; thus, it can be exploited to verify copyright. The fragile watermarking technique produces a very sensitive watermark designed to detect every possible change in marked image; thus, it can accurately detect the tampered area and assure integrity verification and authenticity. As far as we know, Walton [25] was the first to propose a complete fragile watermarking scheme for image tampering detection. The author has chosen to insert "checksums" control values into the least significant bits of each pixel. This technique presents a high probability of tamper detecting but it is vulnerable to the block swap attacks

This paper proposes a new fragile watermarking scheme based on LSB substitution, optimal block selection strategy, and Huffman encoding. Our proposed method can be classified as a fagile hybrid domain-based watermarking technique. The experimental results show that Huffman encryption and optimal blocs selection offer good features of security and imperceptibility. The remainder of this paper is organized as follows. Section 2 presents the proposed method in detail. Section 3 clarifies experiment results as well as some discussions. Conclusions are given in section 4.

2. METHOD

In this section, we propose a novel scheme for digital image watermarking based on combining Huffman encoding with optimal embedding strategy to improve both security and imperceptibility. Security of the watermark is maintained since it cannot be extracted without knowing the decoding rules and Huffman table. Furthermore, specifics blocks were selected for embedding according to the maximum entropy value.

2.1. Huffman coding

Huffman coding is a lossless data compression algorithm developed by Huffman [26] in 1952. It uses a variable length code to represent a source symbol (pixels of the watermark in our case). The most frequent characters (with the highest occurrence) are encoded with the smallest binary codes, so the space used to encode them is minimal, which increases the compression rate. The purpose of the Huffman algorithm is to reduce the number of bits used for encoding frequent characters and to increase this number for unfrequented ones [27]. As shown in Figure 1, using Huffman encoding and the Huffman table, the watermark (logo image) is transformed into a bitstream of 0 and 1 values that can be represented as an image to produce a scrambled watermark.

The scrambled watermark and the secret key (Huffman encoding and the Huffman table) are used to restore the pixel values to their original values in the watermark as shown in Figure 2, which is then used to verify the suspected digital image. The encryption step using Huffman encoding has two advantages; the first is securing the watermark and the second is the compression of the watermark before embedding to reduce the distortion. Furthermore, embedding in specif blocs of the image may improve the impercibility and the quality of the watermarked image.

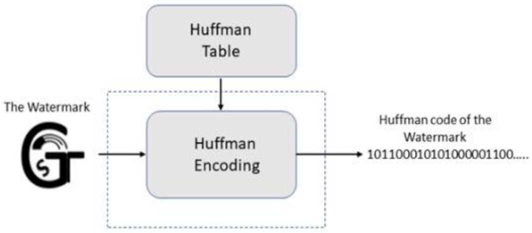


Figure 1. Huffman encoding

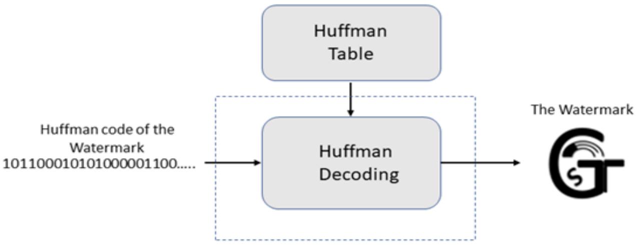


Figure 2. Huffman decoding

2.2. Optimal embedding strategy

Considering the characteristics of the human eyes visual system, we invistigated embedding the scrambled watermark information in specific blocs of the host image according to the entropy value. The entropy measures the degree of randomness in the image [28], [29]. It describes how much uncertainty or randomness there is in an image. It is given as:

$$E(x) = -\sum p(x) log p(x) \quad (1)$$

Here p(x) is the probability of occurrence of ‘x’ in image E(x). Human eyes are less sensitive to high entropy region so optimal perceptibility is obtained when embedding is performed in the bloc with maximum entropy value.

The overall process of the proposed watermarking scheme is presented in Figure 3. First, the host image (standard Lena image) is divided into nonoverlapping blocks to select the most suitable one for embedding according to the maximum entropy value. Secondly, the scrambled watermark is embedded in the first LSB of the host image bloc, then eventually in the second and third LSB as needed depending on the length of the bitstream. Finally, the watermark extraction procedure is the direct reversal of the watermark embedding procedure; the scrambled watermark image is recovered, then using the Hoffman decoding rules we extract the original watermark image.

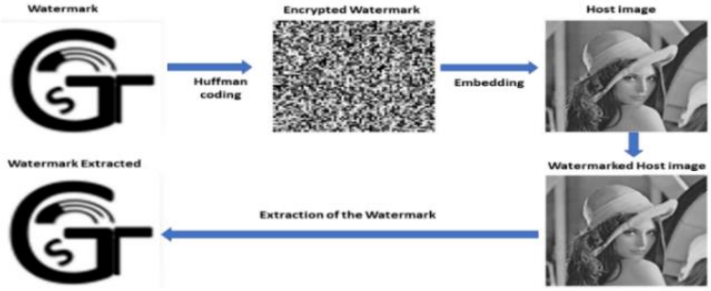


Figure 3. Watermark encryption, embedding, and extraction flow diagram

3. RESULTS AND DISCUSSION

In order to evaluate the effectiveness of the proposed scheme and mesure the effect of combining Huffman encoding with optimal embedding strategy, peak signal to noise ratio (PSNR), structural index similarity (SSIM), and normalized correlation coefficient (NC) of the extracted watermark with respect to the original watermark were calculated. The perceptibility is evaluated through PSNR that measures the degree of similarity between the original image and the watermarked image, the PSNR is defined as (2).

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right) \tag{2}$$

The MSE (mean squared error) is obtained using the (3):

$$MSE = \frac{\sum_{M,N}[I1(m,n)-I2(m,n)]^2}{M*N} \tag{3}$$

where M and N are the number of rows and columns in the input images respectively and I1(m, n) is the original image, I2(m, n) is the watermarked image.

The SSIM is defined in RGB color images as (4):

$$SSIM(i,i') = l(i,i')c(i,i')s(i,i') \tag{4}$$

where i is the original image and i’ is the distorted image. $l(i,i')$, $c(i,i')$ and $s(i,i')$ are respectively the functions that compare luminance, contrast and structures of image i and image i’ [30].

The idea behind SSIM is to measure the structural similarity between the two images, rather than a pixel to pixel difference like the PSNR does [31], [32]. SSIM value should ideally be similar to unity. The robustness of the proposed algorithm is analyzed by using normalized cross correlation (NC), it is a metric to evaluate the degree of similarity between the original watermark and the extracted watermark. The equation to compute NC is given in (5):

$$NC = (\sum_{i=0}^{M}\sum_{j=0}^{N} OW * EW)/(\sum_{i=0}^{M}\sum_{j=0}^{N} OW * OW) \tag{5}$$

OW and EW are, respectively, the original watermark and the extracted watermark.

We start our experiments by testing the proposed scheme using the 512x512 size standard Lena image as host image and the 64x64 size logo, thorax, leaf, and floor images, respectively, as watermarks (Figure 4). Table 1 shows the good values of PSNR, SSIM, and NC, they reach values of 63.12dB, 0.9999, and 0.998, respectively, for the embedding of the thorax image. It is due to the optimal embedding strategy that selects bloc with maximum value of entropy; human eyes are less sensitive to high entropy region. Furthermore, transforming the watermark into a bitstream of 0 and 1 values and inserting them in LBS of the selected bloc reduce severely the distortion of the host image. Embedding in the first LSB can modify the value of the pixel at most by 1. Depending on the length of the bitstream, if we need to continue embedding in the second or in the third LSB of the host image, pixels values can be modified only and at most by 3 and 7 respectively.

Table 1. The three metrics values of embedding the four watermarks in the host image Lena

Watermark	PSNR (dB)	SSIM	NC
Logo	56.2	0.9993	0.975
Thorax	**63.12**	**0.9999**	**0.998**
Leaf	57.03	0.9995	0.937
Floor	58.24	0.9997	0.943

In order to assess the image distortion or more specifically the modification of pixels values in the host image, we calculate the image histogram. It is defined as the plot of the frequency of each intensity value in the image. The image histogram can be written as (6):

$$H_i(k) = J\ ;\ k \in \{0{,}255\} \tag{6}$$

where i is an image of MxN dimension and J represent how many times the gray level k occurs.

$$NC = (\sum_{i=0}^{M}\sum_{j=0}^{N} OW * EW)/(\sum_{i=0}^{M}\sum_{j=0}^{N} OW * OW) \tag{7}$$

Three standard images (shown in Figure 4) have been chosen from the USC-SIPI image database [33], the same previous watermarks are used for embedding to investigate furthermore the proposed scheme.

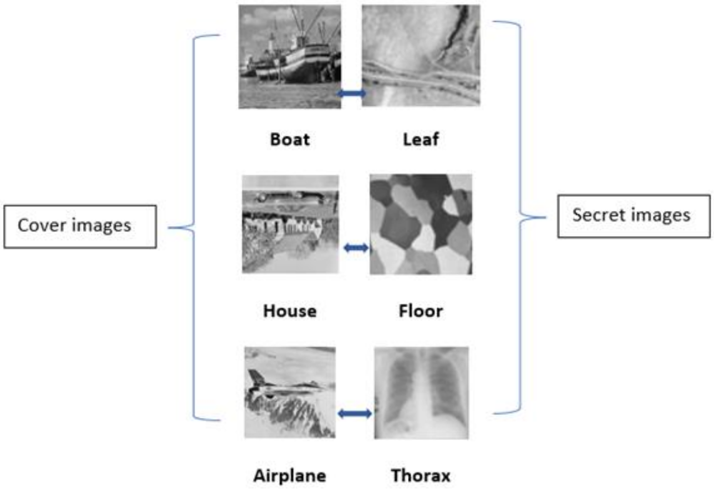


Figure 4. Host images and watermark images

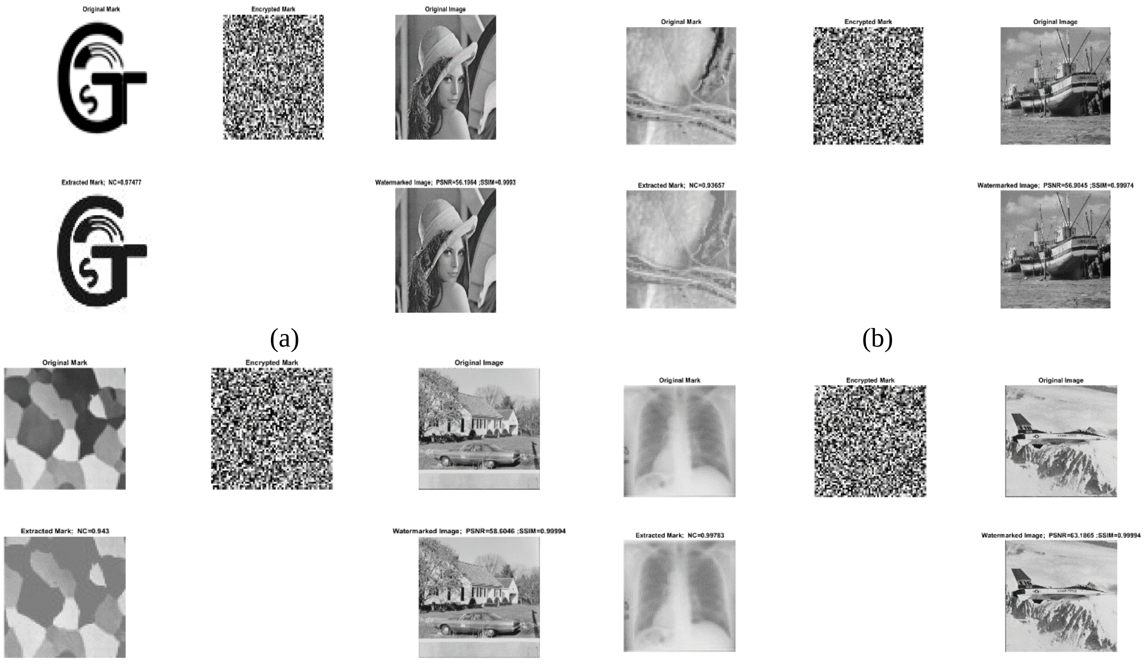
Table 2 shows the high values of PSNR and SSIM that are greater than 56 dB and 0.9993 respectively which indicate that the quality of the watermarked images is very good and the degradation suffered due to the embedding process is generally imperceptible. Furthermore, the values of NC are greater than 0.937, NC is used to calculate the correlation of the original watermark with the extracted watermark. NC results are very close to 1 when no attack is applied and close to 0 when applying any perturbation. This means that the proposed algorithm is very fragile to any perturbation that can affect it.

Figure 5 shows the good imperciptibility of the produced images using the proposed method by comparing visual quality of the original images to the watermarked images and the original watermarks to the extracted watermarks using Lena/logo Figure 5(a), boat/leaf Figure 5(b), house/floor Figure 5(c), and airplane/thorax Figure 5(d) as host images and watermarks respectively. The high visual quality is due to the little modification carried out during embedding process; only few pixels are modified and at most by 7 if we need to embed in the third LSB.

Table 2. PSNR, SSIM, and NC

Host image/watermark	PSNR (dB)	SSIM	NC
Boat/leaf	56.9	0.9997	0.937
House/floor	58.61	**0.9999**	0.943
Airplane/thorax	**63.19**	**0.9999**	**0.998**

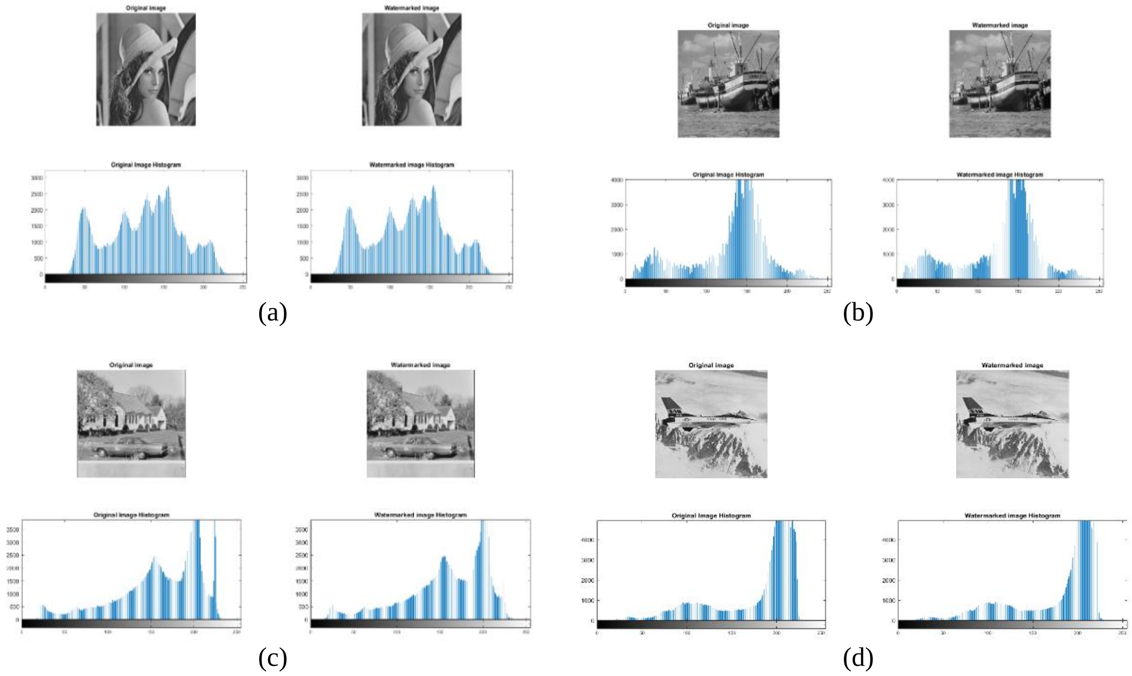
The image histogram plots the frequency of each intensity value in the image. Figure 6 shows that all histograms of watermarked images are similar to those of host images using Lena Figure 6(a), Boat Figure 6(b), house Figure 6(c), and airplane Figure 6(d) as host images. This close similarity indicates that the proposed method preserves the image quality without distortion.


Original Mark
Encrypted Mark
Original Image
Extracted Mark; NC=0.97477
Watermarked Image; PSNR=56.1964 ;SSIM=0.9993
Original Mark
Encrypted Mark
Original Image
Extracted Mark; NC=0.93657
Watermarked Image; PSNR=56.9045 ;SSIM=0.99974
Original Mark
Encrypted Mark
Original Image
Extracted Mark; NC=0.943
Watermarked Image; PSNR=58.6046 ;SSIM=0.99994
Original Mark
Encrypted Mark
Original Image
Extracted Mark; NC=0.99783
Watermarked Image; PSNR=63.1865 ;SSIM=0.99994

(a) (b)

(c) (d)

Figure 5. Comparing visual quality of the original images to the watermarked images and the original watermarks to the extracted watermarks using (a) Lena/logo, (b) boat/leaf, (c) house/floor, and (d) airplane/thorax



(a) (b)

(c) (d)

Figure 6. Comparing histograms of the original host image to those of the watemerked image for (a) Lena, (b) boat, (c) house, and (d) airplane

4. CONCLUSION

In this paper, we present a novel secure fragile watermarking method based on Huffman encoding and optimal embedding strategy. First, we encrypt the watermark image using Huffman encoding to produce a scrambled watermark. Then the host image is divided into nonoverlapping blocks to select the most suitable one for embedding according to the maximum entropy value. The scrambled watermark is embedded in the LSB of the selected bloc of the host image depending on the length of the bits stream. Since the proposed method is a fragile watermarking method, the watermark information will be destroyed by any image processing such as compression or filtering. The main goal of encrypting the watermark before embedding is increasing safety and security.

In this scheme, the requirements are achieved by embedding encrypted watermarks in higher entropy area of host images. The experimental results prove that this proposed technique provides high security and high imperceptibility. The future work will be focused on video watermarking using the extension of this method to differents frames of videos.

REFERENCES

[1] J. Bloom, I. J. Cox, and M. Miller, *Digital watermarking and steganography*, 2nd ed. New York, Ipswich: Elsevier, 2009, doi: 10.1016/B978-0-12-372585-1.X5001-3.

[2] R. Naskar and R. S. Chakraborty, "Reversible digital watermarking: theory and practices," *Synthesis Lectures on Information Security, Privacy, and Trust*, vol. 5, no. 1, pp. 1–130, 2014, doi: 10.2200/S00567ED1V01Y201401SPT010.

[3] O. Evsutin, A. Melman, and R. Meshcheryakov, "Digital steganography and watermarking for digital images: a review of current research directions," *IEEE Access*, vol. 8, pp. 166589–166611, 2020, doi: 10.1109/ACCESS.2020.3022779.

[4] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE Transactions on Image Processing*, vol. 14, no. 2, pp. 253–266, 2005, doi: 10.1109/TIP.2004.840686.

[5] O. C. Abikoye and R. O. Ogundokun, "Efficiency of LSB steganography on medical information," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 5, pp. 4157–4164, 2021, doi: 10.11591/ijece.v11i5.pp4157-4164.

[6] S. Katzenbeisser and F. Petitolas, "Information hiding techniques for steganography and digital watermaking," *EDPACS*, vol. 28, no. 6, pp. 1–2, 2000, doi: 10.1201/1079/43263.28.6.20001201/30373.5.

[7] B. Marques, B. Sim, and L. Cheng, "Spatial-spectral watermarking scheme for JPEG steganography," *SAIEE Africa Research Journal*, vol. 104, no. 4, pp. 154–160, 2013, doi: 10.23919/SAIEE.2013.8531900.

[8] A. O. Mulani and P. B. Mane, "Watermarking and cryptography based image authentication on reconfigurable platform," *Bulletin of Electrical Engineering and Informatics*, vol. 6, no. 2, pp. 181–187, 2017, doi: 10.11591/eei.v6i2.651.

[9] L. Lidyawati, A. R. Darlis, L. Jambola, L. Kristiana, and R. R. Jayandanu, "Digital watermarking image using three-level discrete wavelet transform under attacking noise," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 1, pp. 231–238, 2022, doi: 10.11591/eei.v11i1.3565.

[10] D. B. Taha, T. B. Taha, and N. B. Al Dabagh, "A comparison between the performance of DWT and LWT in image watermarking," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 3, pp. 1005–1014, 2020, doi: 10.11591/eei.v9i3.1754.

[11] S. AL-ardhi, V. Thayananthan, and A. Basuhail, "RST invariant watermarking technique for vector map based on LCA-transform," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 1, pp. 500–510, 2020, doi: 10.12928/telkomnika.v18i1.15020.

[12] S. N. Neyman, I. N. P. Pradnyana, and B. Sitohang, "A new copyright protection for vector map using FFT-based watermarking," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 12, no. 2, pp. 367–378, 2014, doi: 10.12928/telkomnika.v12i2.1975.

[13] C.-C. Lai, "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm," *Digital Signal Processing*, vol. 21, no. 4, pp. 522–527, 2011, doi: 10.1016/j.dsp.2011.01.017.

[14] I. A. Ansari, M. Pant, and C. W. Ahn, "Robust and false positive free watermarking in IWT domain using SVD and ABC," *Engineering Applications of Artificial Intelligence*, vol. 49, pp. 114–125, 2016, doi: 10.1016/j.engappai.2015.12.004.

[15] A. Shehab *et al.*, "Secure and robust fragile watermarking scheme for medical images," *IEEE Access*, vol. 6, pp. 10269–10278, 2018, doi: 10.1109/ACCESS.2018.2799240.

[16] S. N. Bal, M. R. Nayak, and S. K. Sarkar, "On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 5, pp. 552–561, 2021, doi: 10.1016/j.jksuci.2018.04.006.

[17] S. Kumar and B. K. Singh, "Entropy based spatial domain image watermarking and its performance analysis," *M Multimedia Tools and Applications*, vol. 80, no. 6, pp. 9315–9331, 2021, doi: 10.1007/s11042-020-09943-x.

[18] H. Zhang, C. Wang, and X. Zhou, "A Robust image watermarking scheme based on SVD in the spatial domain," *Future Internet*, vol. 9, no. 3, 2017, doi: 10.3390/fi9030045.

[19] M. A. Ayu, T. Mantoro, and I. M. A. Priyatna, "Advanced watermarking technique to improve medical images' security," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 5, pp. 2684–2696, 2019, doi: 10.12928/telkomnika.v17i5.13292.

[20] M. Boussif, N. Aloui, and A. Cherif, "New Watermarking/encryption method for medical imaging FULL protection in m-health," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 6, pp. 3385–3394, 2017, doi: 10.11591/ijece.v7i6.pp3385-3394.

[21] K. Joshi, R. Yadav, and S. Allwadhi, "PSNR and MSE based investigation of LSB," *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*, 2016, pp. 280–285. doi: 10.1109/ICCTICT.2016.7514593.

[22] K. Rinki, P. Verma, and R. K. Singh, "A novel matrix multiplication based LSB substitution mechanism for data security and authentication," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 8, pp. 5510–5524, 2022, doi: 10.1016/j.jksuci.2021.01.013.

[23] Sowmya S, S. Karanth, and S. Kumar, "Protection of data using image watermarking technique," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 386–391, 2021, doi: 10.1016/j.gltp.2021.08.035.

[24] V. A. Kumar, C. Dharmaraj, and Ch. S. Rao, "A hybrid digital watermarking approach using wavelets and LSB," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 5, pp. 2483–2495, 2017, doi: 10.11591/ijece.v7i5.pp2483-2495.

[25] S. Walton, "Information authentication for a slippery new age," *Dr. Dobbs Journal*, vol. 20, no. 4, pp. 18–26, 1995.

[26] D. Huffman, "A method for the construction of minimum-redundancy codes," *Proceedings of the IRE*, vol. 40, no. 9, pp. 1098–1101, 1952, doi: 10.1109/JRPROC.1952.273898.

[27] K. Sayood, *Introduction to data compression*, Fifth edition. Cambridge: Morgan Kaufmann Publishers, 2018.

[28] S. Kumar and A. Dutta, "A novel spatial domain technique for digital image watermarking using block entropy," *2016 International Conference on Recent Trends in Information Technology (ICRTIT)*, 2016, pp. 1–4. doi: 10.1109/ICRTIT.2016.7569530.

[29] F. Ernawan, "Tchebichef image watermarking along the edge using YCoCg-R color space for copyright protection," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 3, pp. 1850–1860, 2019, doi: 10.11591/ijece.v9i3.pp1850-1860.

[30] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004, doi: 10.1109/TIP.2003.819861.

[31] A. Horé and D. Ziou, "Is there a relationship between peak-signal-to-noise ratio and structural similarity index measure?," *IET Image Processing*, vol. 7, no. 1, pp. 12–24, 2013, doi: 10.1049/iet-ipr.2012.0489.

[32] A. Hore and D. Ziou, "Image quality metrics: PSNR vs. SSIM," *2010 20th International Conference on Pattern Recognition*, 2010, pp. 2366–2369. doi: 10.1109/ICPR.2010.579.

[33] "USC-SIPI image database." USC University of Southern California, USC Viterbi School of Engineering, Signal and Image Processing Institute., 1977. [Online]. Available: https://sipi.usc.edu/database/ (Accessed Jun 12, 2022).

BIOGRAPHIES OF AUTHORS

Mourad Zairi received the B.Sc. degree in electronical engineering from Ibn Tofail University, in 2002. Received the M.Sc. degree in physics and nuclear techniques from Cadi Ayyad University, in 2005. Received the M.Sc. degree in applied physics from Huelva University, in 2009. Now he is a Ph.D. student at the National School of Applied Sciences, Ibn Tofail University. His research interests include image processing, steganography and data analysis. He can be contacted at email: mouradzairi@gmail.com.

Tarik Boujiha received the Ph.D. from the University of Kenitra in 2011. Since, he is an associate professor in the National School of Applied Sciences, Ibn Tofail University. His research topic concerns image processing, data analysis, dynamic texture analysis, steganography and steganalysis. He can be contacted at email: ftarik6@gmail.com.

Abdelhaq Ouelli was born in Morocco, in 1975. He received the B.Sc. degree in electronical engineering from Cadi Ayyad University, in 2006. Received the M.Sc. degree in signal processing from Mohammed 5 University, in 2009. Received the Ph.D. degree from Sultan Moulay Slimane University, in 2015. His research interests include computer vision, signal processing, as well as speech and image processing. He can be contacted at email: ouelli2014@gmail.com.