RESEARCH ARTICLE

New Blind Image Moments Watermarking Method Based on Evolutionary Optimization of Embedding Parameters

CHAIMAE CHEKIRA [1], **MANAL MARZOUQ**[1], **IMAD BATIOUA**[2], **HAKIM EL FADILI**[1], **ZAKIA LAKHLIAI**[1], **AND KHALID ZENKOUAR**[2]

[1]Computer Science and Interdisciplinary Physics Laboratory (LIPI), Sidi Mohamed Ben Abdellah University, Fez 30003, Morocco
[2]Laboratory of Intelligent Systems and Applications (LSIA), Sidi Mohamed Ben Abdellah University, Fez 30003, Morocco

Corresponding author: Chaimae Chekira (chaimae.chekira@usmba.ac.ma)

ABSTRACT In image watermarking, the locations where the watermark is embedded in the frequency domain and the embedding strength influence the overall performance of the blind watermarking procedure. The present paper aims to propose a new blind watermarking method based on the dither modulation by developing an automatic selection of the optimum embedding parameters that guarantee high-quality watermarked images and low bit error rates during the extraction process. The proposed automatic search method for the best discrete moments subsets is based on an evolutionary algorithm and adopts a specific coding strategy with a group of genes representing the embedding positions. The second part of the chromosome is reserved for the embedding strength coding, followed by the application of different evolutionary operators on the evolution pool. Our study explores the impact of maximum generation, population size, and cutting-point positions with different crossover and mutation rates. The performances under different attack conditions are evaluated, and a comparative study is established with other conventional selection methods and other discrete transforms. Results show that our proposed optimization algorithm baptized EWIMps achieves the best trade-off between robustness and imperceptibility with a peak signal-to-noise ratio varying from 28.33 dB to 59.87 dB and a normalized cross-correlation value from 0.707 to 1.

INDEX TERMS Data hiding, blind image watermarking, orthogonal discrete moments, discrete transforms, dither modulation, evolutionary algorithm.

I. INTRODUCTION

Data can be easily duplicated and illegally distributed via communication networks nowadays. Therefore, finding a secure and private method of communication is crucial for both commercial and military goals connected to market strategy, copyright protection, and other factors. For this purpose, data-hiding techniques have evolved as a solution for the aforementioned issues [1]. Digital image watermarking, as a data hiding form, is employed to embed a watermark inside the image to achieve copyright protection, prevent unauthorized copying, and secure data via transmission channels. The blind watermarking process must simultaneously ensure resistance to attacks and maintain recovered image quality.

The associate editor coordinating the review of this manuscript and approving it for publication was Joewono Widjaja [ID].

Typically, spatial and frequency domains can be used for embedding the watermark [2]. The goal of spatial domain based on blind watermarking is to directly alter the pixels in images. Spatial domain approaches are consequently less resistant to normal image processing and attacks that could easily remove the watermark. Alternatively, the frequency domain (where image coefficients are altered to incorporate a watermark) is more used because of its resistance to compression and geometrical alterations [3]. Moments as a specific case of frequency transformation were largely used in watermarking since their first introduction in [4] where an iterative watermarking approach based on Hu's geometric moments is presented.

An important issue rarely addressed in watermarking literature is the selection of the frequency locations for embedding the watermark. In fact, image transformation in the frequency

domain is composed of high-frequency, low-frequency, and middle bands. The high-frequency band of an image contains information about its contour and it is vulnerable to the most common image processing attacks, which may cause data loss. Embedding a watermark in the higher frequency band, therefore, does not achieve good robustness, even if it ensures a satisfied watermarked image quality [5]. On the other hand, the majority of the image energy is concentrated in the low-frequency band. Thus, any embedding made in this band negatively impacts the quality of the watermarked image while securing the watermark against typical image processing attacks [5], [6]. Finally, embedding randomly the watermark in the middle-frequency domain that contains the texture of the image may also affect the watermarking performances [6]. In this context, most authors used the trial and error method or the zigzag operation to select the frequency moments coefficients highly securing the watermark, or choose the positions arbitrarily in such a way that they have no effect on the Peak Signal-to-Noise Ratio (PSNR) between original and watermarked images [7] and [8]. In fact, authors in [9], [10], [11], [12], [13] exclude Zernike moments (ZMs) with orders higher than a certain threshold, as the rounding errors become more significant. Then, depending on the length of the watermark bit sequence, they use a secret key to select randomly a number of the considered ZMs [11], [12], [13]. Authors in [14], [15], and [16] adopt the same selection criteria taking into account the intrinsic properties of continuous moments used. In the case of discrete moments, few papers addressed this issue. For instance, authors in [17] select randomly a vector of local Tchebichef moments (TMs) from a set of moments where the maximum order is determined experimentally to balance invisibility and robustness. In [18], [19], and [20], only a necessary number of moments equal to the inserted message length is adopted to satisfy the capacity requirement. In [6], a zigzag scanning is adopted to select the first produced lower-order of TMs. Authors in [21] take into account the first QRFrCMs moments of lower order justifying this choice by their ability to represent the significant features of the image and by their robustness against image processing attacks. Recently, the watermarking works converged to find near-optimum embedding parameters that guarantee a good trade-off between the two most essential requirements of image watermarking [22]. Hence, research focuses mainly on the imperceptibility of the watermarked and the robustness of the extracted watermark because they often prove to be mutually exclusive.

In this paper, image watermarking is considered an optimization issue. This problem is addressed using a new watermarking technique based on Evolutionary Algorithms [23], [24] that can simultaneously improve the robustness and imperceptibility. Our proposed selection methodology consists of an evolutionary algorithm based on an automatic search of the optimal frequency moments subset among image moments to insert the watermark bits individually. In this work, each evolutionary population has a set of

TABLE 1. List of abbreviations parameters adopted in our work.

Nomenclature	
IL	Size of the original image I
WL	Size of the watermark W
N	Arnold encryption period
n	Moments order
m	Moments repetition
p_1-p_2	Locality parameters of Krawtchouk moments
Δ	Quantization step of dither modulation
K_1	Key of encryption and decryption watermark
K_2	Key of the embedding and extraction processes
MG	Maximum generation
PS	Population size
L	Individual length
L_b	Chromosome length
G_i	The ith gene of the embedding positions
Gb_i	The ith binary gene of the embedding positions
l	Binary gene length of the embedding positions
G'	Added gene of the embedding strength
Gb'	Binary added gene of the embedding strength
l'	Binary added gene length of the embedding strength
CR	Crossover rate
CP	Cutting point of the crossover operator
MP	Mutation percentage
MR	Mutation rate
FF	Fitness Function

chromosomes that represents the embedding locations. A new coding strategy is used before applying the evolutionary operators to provide valid phenotypes. As a result, we preserve promising areas of the search space where an optimal solution can be discovered over generations. Additionally, as the dither modulation highly impacts the performance of the blind watermarking process, the quantization step is also included and coded in the second part of our final adopted chromosome to explore the best combination between positions and embedding strength. In the literature, this parameter is often chosen randomly [13], [14], experimentally [12], [17] or such that the PSNR of the watermarked and original image is close to a threshold that ensures a good imperceptibility [10].

As a summary, the main contribution of our method baptized EWIMps (Evolutionary Watermarking Image Moments method for embedding positions and strength) is to automatically explore simultaneously the embedding moments where the watermark data will be inserted and the embedding strength, knowing that the choice of those parameters greatly influences the resulting embedding algorithm performances. In this work, our EWIMps method uses Krawtchouk, Tchebichef, Dual Hahn, and Racah moments which do not require any numerical approximation processes compared with continuous orthogonal moments [25]. Nevertheless, the proposed method is also applicable to any moment family and can either be used in the case of continuous or discrete moments. In order to assess the validity of our method, a comparison study is performed with other conventional selection methods, and between moments and discrete transform using standard testing images. The performances against different attacks are also explored including salt and pepper, poisson, speckle, rotation, gaussian, and JPEG compression attacks.

The rest of the paper is organized as follows: section II points out related works about watermarking using moments. Then, a theoretical background about discrete image moments is presented in section III. The Evolutionary Watermarking Image Moments method for embedding positions and strength (EWIMps) is proposed in section IV. Section V is dedicated to the experimental study, results, and discussion of imperceptibility and robustness analysis. Finally, section VI concludes the present work and suggest prospects.

II. RELATED WORKS

In the following review study, an automatic search in well-known databases is set up to find the most important works on watermarking using orthogonal image moments in different coordinate spaces (cartesian and polar) in order to make a relevant and useful synthesis of previous studies that aim to find the gaps and issues in this field. The works presented in Table 2 are ordered chronologically by specifying the main author, moments used, and corresponding performance indicators of the watermarking schemes that evaluate the impact of the moments and the efficiency of the adopted methods. The last column indicates the optimized parameters if used in each work. The presented papers are the result of searching in digital libraries: IEEE Xplore, Science Direct, ResearchGate, Elsevier, and the Google Scholar search engine, published between 2007 and 2022. Conference papers and books are excluded from our search.

From this review study, we have noted that the properties of continuous orthogonal moments have been used in both polar and cartesian spaces. One of the first and most important papers devoted to polar space is the work presented in [26] where the authors suggest an octonion continuous orthogonal moments (OCOMs) applicable to color stereoscopic images by fusing the octonion theory with the continuous orthogonal moments in the polar coordinate system. According to experimental results, the zero-watermarking technique used by OCOMs satisfies the robustness condition. A non-unit mapped radial moment has been developed in [27] to produce a robust watermarking technique against signal processing and both local and global geometric attacks. Many previous studies have focused on Zernike moments. In fact, Xin et al. proposed the first resilient image watermarking technique using Zernike and pseudo-Zernike moments (PZMs) [9]. Authors embed a multi-bit watermark signal by dither modulating the magnitudes of chosen moments, which offers outstanding watermark resistance to several geometric and signal processing techniques. Feature-based robust image watermarking has been proposed in [10] and [28] where feature point-based regions are first marked by the Harris detector, then the watermark is locally encoded into local Zernike moments ZMs (LZMs) to successfully be robust against attacks. Accurate Zernike moments were adopted in [13] to enhance the robustness and imperceptibility of watermark embedding. An alternative framework was presented in [12] which is based on an accurate and fast approach for computing Zernike moments. The authors suggest a novel image-adaptive watermarking scheme for geometrically invariant and high-capacity data embedding. Furthermore, authors in [29] suggested using local frequency-domain Exponent-Fourier moments (EFMs) modeling to create a statistical image watermark decoder. Bessel-Fourier moments are another type of orthogonal moment used to extract feature images and build the zero-watermark [30]. The goal of the previous study is to suggest a reliable visual zero-watermarking approach resistant to a variety of attacks, including rotation, scaling, Gaussian noise, and blurring. Recently, harmonic Fourier moments (HFMs) have been used to find new groups of moments in polar space. For a robust watermarking of gray-level images and to increase security, authors in [31] combined accurate polar harmonic Fourier moments (PHFMs) with chaotic mapping. Geranion polar harmonic Fourier moments (GPHFMs) are constructed based on geranion theory and polar harmonic Fourier moments and applied for embedding and extraction process of light-field image watermarking in [32]. A promising area of research has been initiated using quaternion moments-based watermarking methods for color images. Niu et al. [15] proposed a color image watermarking scheme based on quaternion radial harmonic Fourier moments (QRHFMs) invariant against geometric distortions. Xia et al. [33] have then developed a modified zero-watermarking scheme based on the quaternion polar harmonic Fourier moment (QPHFMs). Those moments have been used by authors in [34] where a robust zero-watermarking algorithm that simultaneously provides copyright protection for three CT images is proposed. Additionally, authors utilized in [35] a local quaternion polar harmonic Fourier moments to introduce a multiple-zero watermarking scheme for color medical images. Wang et al. [36] studied the local quaternion exponent moments (QEMs) for color image watermarking to improve robustness against desynchronization and image processing attacks. Authors in [37] inserted the watermark into host color images by modifying the quaternion radial substituted Chebyshev moments (QSRCMs) magnitudes for a resilient color image watermarking. In order to calculate the Quaternion Legendre-Fourier moments (QLFMs) in polar coordinates, the same authors developed a precise and numerically stable method in [16] where a geometrically invariant color image watermarking scheme is proposed. Wang et al. [38] presented a new technique for color image zero-watermarking making use of precise quaternion generalized orthogonal Fourier-Mellin moments (AQGOFMMs). Particularly, Quaternion polar harmonic transforms (QPHTs) were proposed by other authors. In fact, Xia et al. [39] presented a strong zero-watermarking approach for color medical images, based on precise QPHT magnitudes and a chaotic system of a mixed linear-nonlinear coupled map lattice. Simultaneously, authors in [40] and [41] proposed robust color image watermarking schemes by using an

approximated quaternion polar harmonic transform resistant against geometric distortions and some image processing attacks. An attempt is made by some authors to enhance the watermarking performances using polar complex exponential transform (PCETs). Wang et al. in [42] suggested a zero-watermarking method for grayscale images based on polar complex exponential transform and logistic mapping to increase scheme security. Other types of moments belonging to the same family have been explored. Work in [43] presented a fast quaternion generic polar complex exponential transform (FQGPCETs) for a color image zero-watermarking algorithm that could successfully withstand geometrical attacks like rotation, scaling, and cropping. Xia et al. [44] introduced a novel quaternion polar complex exponential transform (NoQPCETs) based on a robust zero-watermarking algorithm for lossless copyright protection of color images. Other authors investigated the ternary number theory in the same context. A new kind of polar harmonic transform called ternary accurate polar complex exponential transforms (TAPCETs) was given by Ma et al. [45], where the authors proposed a zero-watermarking algorithm for protecting two similar medical images. In this work, the essential features are extracted using the gaussian numerical integration method and chaotic mapping. Experimental results show the algorithm's robustness against common and geometric attacks. Furthermore, Wang et al. [46] designed ternary radial harmonic Fourier moments (TRHFMs) to process a robust stereo image zero-watermarking algorithm robust against various asymmetric and symmetric attacks. Recent research demonstrated that polynomials with fractional orders represent functions more effectively than those with equivalent integer orders. Authors in [47] developed a reliable zero-watermarking system for lossless copyright protection of medical images using fractional-order radial harmonic Fourier moments (FoRHFMs). Hosny et Darwish in [48] proposed a novel robust color image-watermarking algorithm based on new multiple fractional multi-channel orthogonal moments: fractional-order exponent moments (MFrEMs), fractional-order polar harmonic transforms (MFrPHTs), and fractional-order radial harmonic Fourier moments (MFrRHFMs). In the same context, fractional orders have been combined with several types of Charlier moments, such as fractional Charlier polynomials (FrCPs) presented by Yamni et al. [49] for reconstructing and watermarking gray-level images. The same author proposed in [21] a set of moments called quaternion radial fractional Charlier moments (QRFrCMs) for copyright protection of color medical images in a zero-watermarking scheme and a separable fractional Charlier–Meixner moments (FrCMMs) in [50].

In cartesian space, many other studies have been dedicated to using continuous orthogonal moments in image watermarking. Zhang et al. [51] used affine Legendre moments (AFMs) to detect and extract watermarks from images being attacked by affine transformations. Authors in [52] explored a set of multi-channels shifted Gegenbauer moments of

fractional orders (FrMGMs) to extract invariant features from color medical images.

In recent papers, attempts have been made to explore the advantages of discrete orthogonal moments in cartesian space. The basic functions of discrete moments do not require any numerical approximation processes. Consequently, image reconstruction using discrete moments performs better [25]. In this context, Tchebichef moments (TMs) have been used in various works. Authors presented in [53] a secure high-capacity information hiding scheme, and in [54] an empirical comparative study between the noise sensitivity of Tchebichef and Zernike moments in image watermarking applications. In addition, Deng et al. in [17] developed a method based on Tchebichef moments where the reliable feature point is determined using the Harris Laplace detector recognizing different non-overlapped disks. A new imperceptible zero watermarking method using Tchebichef moments for medical images was introduced by authors in [55]. Krawtchouk moments (KMs) are then proposed in [56] where a new method is presented to protect 3D video content against pirating. The same moments were used in [57] where a local affine transform invariant image blind watermarking is designed and tested against attacks. Papakostas et al. [19] proposed an important approach of digital image watermarking using Krawtchouk moments based on a genetic algorithm for searching an appropriate set of parameters (locality parameters, dither modulation quantization step, and moment coefficients) achieving high robustness and imperceptibility performances. The same authors proposed the fuzzy inference as an optimization method in [20]. Furthermore, Dual Hahn moments (DHMs) were adopted in image watermarking by Daoui et al. [58] where a Sine Cosine Algorithm is used to optimize the local parameters of Dual Hahn moments. The same optimization algorithm was presented by authors for local zero-watermarking of color stereo images in [59]. Another important work was done by Tsougenis et al. [18] where the authors proposed a new approach called separable moments (SMs) that generates a series of new discrete moments families applicable to image watermarking. The fractional method was tested in [60] using Tchebichef moments (FrDTMs), and using Krawtchouk transforms (FrKTs) in [61].

It is important to note that a robust image watermarking system must meet the two most important requirements: imperceptibility and robustness. Imperceptibility indicates that the host and watermarked images must appear the same to the human visual system. In some watermarking applications, minor distortions are, nevertheless, permitted to reduce costs [62]. Robustness denotes that during the transmission of the watermarked image across an unsecured channel, the extracted watermark must resist extreme malicious attacks [62]. Therefore, watermarking schemes must have a compromise between these two requirements [21]. To assess the watermarking performances, we generally use the PSNR and SSIM (Structural Similarity Index Metric) indices to

TABLE 2. Our state-of-the-art of watermarking techniques using image moments.

Ref	Moments used	Performance Indicators	Optimized parameters
[9]	Zernike and pseudo-Zernike moments	PSNR, BER	—
[57]	Krawtchouk moment invariants	PSNR, NC	—
[28]	Local Zernike moments	Detection Ratio (DR), PSNR	—
[10]	Local Zernike moments	Average Detection Ratio, PSNR	—
[11]	Pseudo-Zernike moments	Correlation coefficient, PSNR	—
[17]	Local Tchebichef moments	False positive error probability, PSNR	—
[13]	Zernike Moments	BER	—
[51]	Affine Legendre moment invariants	PSNR	—
[53]	Tchebichef moments	PSNR	—
[54]	Tchebichef and Zernike moments	Accumulative Relative Error (ARE)	—
[19]	Krawtchouk moments	BER, PSNR	$p_1, p_2, \Delta_k, n_i, m_i$
[12]	Zernike moments	Data Hiding Ratio, PSNR, BER	—
[36]	Local quaternion exponent moments	PSNR, DR	—
[18]	Separable moments	BER, PSNR, SSIM	—
[30]	Bessel-Fourier moments	The average accuracy rate (AAR), PSNR	—
[40]	Quaternion polar Harmonic transforms	PSNR, BER	—
[15]	Quaternion radial harmonic Fourier moments	PSNR, BER	—
[20]	Tchebichef and Krawtchouk moments	Reduction Factor (RF), PSNR, BER	Fuzzy inference parameters
[41]	Local quaternion polar Harmonic transforms	PSNR, DR	—
[61]	Fractional Krawtchouk transforms	PSNR, MSE, BER	—
[42]	Polar complex exponential transform	PSNR, BER, SSIM	—
[16]	Quaternion Legendre-Fourier moments	PSNR, SSIM, BER	—
[27]	Radial moments	PSNR, BER	—
[39]	Quaternion polar harmonic transforms	PSNR, MSE, BCR	—
[37]	Quaternion radial substituted Chebyshev moments	PSNR, NC, SSIM	—
[46]	Ternary radial harmonic Fourier moments	PSNR, MSE, BER	—
[34]	Quaternion polar harmonic Fourier moments	PSNR, Accuracy Rate	—
[33]	Precise quaternion polar harmonic Fourier moments	PSNR, Bit Correct Ratio (BCR)	—
[6]	Tchebichef Moments	PSNR, SSIM, NC, BER	—
[43]	Fast Quaternion generic polar complex exponential transforms	PSNR, BER	—
[60]	Fractional discrete Tchebyshev moments	PSNR, BER	—
[31]	Polar harmonic Fourier moments	BER	—
[55]	Tchebichef moments	PSNR, NC	—
[49]	Fractional Charlier polynomials	MSE, PSNR, BER	—
[56]	Krawtchouk moments	PSNR, SSIM, NC, BER	—
[45]	Ternary Accurate polar complex exponential transform	PSNR, SSIM, NC, BER	—
[38]	Accurate quaternion generalized orthogonal Fourier–Mellin moments	PSNR, BER, BCR, Capacity, the False Positive Ratio	—
[26]	Octonion continuous orthogonal moments	Mean Relative Error (MRE), BCR	—
[29]	Exponent-Fourier moments	BER, NC, SSIM, PSNR, Time	—
[35]	Local quaternion polar harmonic Fourier moments	BCR	—
[47]	Fractional-order radial harmonic Fourier moments	MRE, BER, PSNR	—
[50]	Separable fractional Charlier–Meixner moments	PSNR, BER, computational complexity	—
[21]	Quaternion Radial Fractional Charlier moments	MSE, PSNR, BCR	—
[44]	Quaternion polar complex exponential transform	PSNR, BCR, ETIR	—
[52]	fractional-order Gegenbauer moments	PSNR, BER, NC	—
[59]	Octonion hahn moments	PSNR, MSE	Local zero-watermarking
[58]	Dual hahn moments	PSNR, BER, NCC, SSIM	Local parameters of DHPs
[48]	Fractional-order: polar harmonic transforms, exponent radial harmonic Fourier moments	PSNR, BER, NC	—
[32]	Geranion polar harmonic Fourier moments	PSNR, BCR	—

evaluate the imperceptibility and the BER (Bit Error Rate) and NC (Normalized cross-Correlation) indices to evaluate the robustness.

Great improvements have been made in the research on watermarking using different moment families. It should be pointed out that, to our knowledge, even though the optimization process of some watermarking parameters has been used in the literature, embedding positions are still chosen at random or through the trial-and-error or zigzag methods. From our perspective, special attention is needed to control the locations where the watermark data must be inserted. Consequently, the present work constitutes an attempt to optimize the embedding locations in a discrete moments-based watermarking scheme.

III. THEORETICAL BACKGROUND - DISCRETE IMAGE MOMENTS

Image moments are an effective method to characterize image content. Thus, they have been successfully utilized in diverse engineering research areas, including pattern recognition, image watermarking, medical analysis, and computer vision [63], [64]. Discrete moments present multiple advantages as they assure a strong image representation capacity with minimal computing complexity. Moreover, they

completely reconstruct the described image with minimum errors and great robustness against noise [65]. In particular, image moments are a useful technique in watermarking applications, due to the minimal reconstruction error of the watermarked image after embedding the data at the moment domain, and the good watermark extraction quality in the presence of attacks [19]. The following subsections include a brief presentation of the discrete orthogonal polynomials used in this paper. Krawtchouk polynomials are first presented, followed by Tchebichef, Dual Hahn, and Racah polynomials. More details can be found in [66], [67], [68], and [69].

A. KRAWTCHOUK DISCRETE ORTHOGONAL POLYNOMIAL
Yap et al. employed the Krawtchouk discrete orthogonal polynomials in image analysis [68]. They have been defined as follows [70]:

$$k_n(x; p, N) = \sum_{k=0}^{N} a_{k,n,p} x^k = {}_2F_1\left(-n, -x; -N; \frac{1}{p}\right) \quad (1)$$

where the hypergeometric function is expressed by the variables $x, n = 0, 1, N, 0 < p < 1$ and defined as follows:

$$_2F_1(a, b; c; z) = \sum_{k=0}^{\infty} \frac{(a)_k (b)_k z^k}{k!(c)_k}. \quad (2)$$

In order to prevent the numerical instability of the classic Krawtchouk polynomials, a group of normalized Krawtchouk polynomials has been discussed in [68] by the following formula:

$$\bar{k}_n(x; p, N-1) = k_n(x; p, N-1)\sqrt{\frac{w_k(x; p, N-1)}{\rho_k(n; p, N-1)}} \quad (3)$$

We apply the recursive formula published in [68] in our research, which is denoted by:

$$\bar{k}_n(x; p, N-1) = A_n\bar{k}_{n-1}(x; p, N-1) - B_n\bar{k}_{n-2}(x; p, N-1),$$
$$\bar{k}_0(x; p, N-1) = w_k(x; p, N-1),$$
$$\bar{k}_1(x; p, N-1) = w_k(x; p, N-1)\frac{(N-1)p - x}{\sqrt{(N-1)p(1-p)}}, \quad (4)$$

with

$$A_n = \frac{(N-1p - 2(n-1)p + n - 1 - x)}{\sqrt{p(1-p)n(N-n)}} \quad and$$
$$B_n = \sqrt{\frac{(n-1)(N-n+1)}{(N-n)n}}$$

B. TCHEBICHEF DISCRETE ORTHOGONAL POLYNOMIAL
In [66], authors have presented their approach to computing discrete Tchebichef orthogonal moments. The nth order of classical Tchebichef polynomials is expressed in the following formula [70]:

$$t_n(x; N) = (1-N)n_3F_2(-n, -x, 1+n; 1, 1-N; 1), n, x, y$$
$$= 0, 1, \ldots N - 1 \quad (5)$$

where the generalized hypergeometric function $_3F_2$ can be defined as:

$$_3F_2(a_1, a_2, a_3; b_1, b_2; z) = \sum_{k=0}^{\infty}\left(\frac{(a_1)_k (a_2)_k (a_3)_k z^k}{(k!)(b_1)_k (b_2)_k}\right) \quad (6)$$

and $(a)_k$ presents the Pochhammer symbol defined as:

$$(a)_k = a(a+1)(a+2)\ldots(a+k-1)$$
$$= \frac{\Gamma(a+k)}{\Gamma(a)}, k \geq 1, \text{ and } a_0 = 1 \quad (7)$$

where $\Gamma(\cdot)$ is the Gamma function.

Mukundan et al. established a set of normalized Tchebichef polynomials in [66] by the following formula to prevent the numerical instability of classical Tchebichef polynomials produced by the hypergeometric function in equation (5):

$$\bar{t}_n(x; N) = \frac{t_n(x; N)}{\beta(n, N)} \quad (8)$$

where, as stated in [66], $\beta(n, N)$ is a suitable constant that is independent of x:

$$\beta(n, N) = \sqrt{\rho(n, N)} \quad (9)$$

Authors in [66] suggest a recursive formula for the normalized Tchebichef polynomials in order to reduce the high computing cost of equation (8) represented by:

$$\bar{t}_n(x; N)$$
$$= \frac{(2n-1)\bar{t}_1(x; N)\bar{t}_{n-1}(x; N) - (n-1)\left(1 - \frac{(n-1)^2}{N^2}\right)\bar{t}_{n-2}(x; N)}{n}$$
$$\bar{t}_0(x; N) = 1$$
$$\bar{t}_1(x; N) = \frac{2x + 1 - N}{N} \quad (10)$$

C. DUAL HAHN DISCRETE ORTHOGONAL POLYNOMIAL
Authors in [69] introduced the dual Hahn polynomials for image analysis. The non-uniform lattice serves as the definition for this family of discrete orthogonal polynomials. The nth order is given by [70]:

$$dh_n^{(c)}(s, a, b)$$
$$= \frac{(a-b+1)_n(a+c+1)_n}{n!}$$
$$\times {}_3F_2(-n, a-s, a+s+1; a-b+1, a+c+1; 1), \quad (11)$$

where the parameters a, b, c, n, and s are restricted to $-\frac{1}{2} < a < b, b = a + N, |c| < a + 1, n = 0, 1, \ldots N - 1$, and $s = a, a+1, \ldots b-1$. $_3F_2$ is the generalized hypergeometric function given in equation (6).

The dual Hahn polynomials are scaled using the weighting function and square norm to prevent numerical instability in polynomial computation. The group of normalized dual Hahn polynomials is given by:

$$\overline{dh}_n^{(c)}(s, a, b) = dh_n^{(c)}(s, a, b)\sqrt{\frac{w_{dh}(s)}{\rho_{dh}(n)}\left[\Delta X\left(s - \frac{1}{2}\right)\right]}$$
$$n = 0, 1, \ldots, N - 1 \quad (12)$$

We adopt the recursive formula with respect to n as suggested in [69] to reduce the computing cost in equation (11), which is based on a generalized hypergeometric function. This formula is indicated by the following notation:

$$
\overline{\mathrm{dh}}_n^{(c)}(s, a, b) = A \sqrt{\frac{\rho_{\mathrm{dh}}(n-1)}{\rho_{\mathrm{dh}}(n)}} \overline{\mathrm{dh}}_{n-1}^{(c)}(s, a, b)
$$
$$
+ B \sqrt{\frac{\rho_{\mathrm{dh}}(n-2)}{\rho_{\mathrm{dh}}(n)}} \overline{\mathrm{dh}}_{n-2}^{(c)}(s, a, b)
$$
$$
\overline{\mathrm{dh}}_0^{(c)}(s, a, b) = \sqrt{\frac{w_{\mathrm{dh}}(s)}{\rho_{\mathrm{dh}}(0)} \left[\Delta X \left(s - \frac{1}{2} \right) \right]}
$$
$$
\overline{\mathrm{dh}}_1^{(c)}(s, a, b) = -\frac{1}{w_{\mathrm{dh}}(s)} \frac{w_1(s) - w_1(s-1)}{X \left(s + \frac{1}{2} \right) - X \left(s - \frac{1}{2} \right)}
$$
$$
\sqrt{\frac{w_{\mathrm{dh}}(s)}{\rho_{\mathrm{dh}}(1)} \left[\Delta X \left(s - \frac{1}{2} \right) \right]}, \qquad (13)
$$

where:

$$
A = \frac{1}{n}[s(s+1) - ab + ac - bc - (b - a - c - 1)(2n - 1) + 2(n-1)^2]
$$
$$
B = -\frac{1}{n}(a + c + n - 1)(b - a - n + 1)(b - c - n + 1),
$$

and

$$
w_n(s) = \frac{\Gamma(a+s+n+1)\Gamma(c+s+n+1)}{\Gamma(s-a+1)\Gamma(b-s-n)\Gamma(b+s+1)\Gamma(s-c+1)}.
$$

D. RACAH DISCRETE ORTHOGONAL POLYNOMIAL

The Racah polynomials defined in the non-uniform lattice will be discussed in this subsection. Authors in [69] employed this group of discrete orthogonal polynomials for image analysis for the first time, where the nth-order Racah polynomials are defined by the following formula [70]:

$$
r_n^{(\alpha, \beta)}(s, a, b) = \frac{(a - b + 1)_n (\beta + 1)_n (a + b + \alpha + 1)_n}{n!}
$$
$$
\times {}_4F_3(-n, \alpha + \beta + n + 1, a - s, a + s + 1; \beta + 1, a + 1 - b, a + b + \alpha + 1; 1)
$$
$$
\tag{14}
$$

where the parameters $a, b, \alpha, \beta, n,$ and s are restricted to $-\frac{1}{2} < a < b, \alpha > -1, -1 < \beta < 2a + 1, b = a + N,$ $n = 0, 1, \ldots n - 1,$ and $s = a, a + 1, \ldots, b - 1$ and ${}_4F_3$ is the generalized hypergeometric function given by:

$$
{}_4F_3(a_1, a_2, a_3, a_4; b_1, b_2, b_3; z)
$$
$$
= \sum_{k=0}^{\infty} \left(\frac{(a_1)_k (a_2)_k (a_3)_k (a_4)_k z^k}{(k!) (b_1)_k (b_2)_k (b_3)_k} \right). \qquad (15)
$$

The Racah polynomials are scaled using the square norm and weighting function to prevent numerical instability in polynomial computing. The following definition applies to the set of normalized Racah polynomials:

$$
\bar{r}_n^{(\alpha, \beta)}(s, a, b) = r_n^{(\alpha, \beta)}(s, a, b) \sqrt{\frac{w_r(s)}{\rho_r(n)} \left[\Delta X \left(s - \frac{1}{2} \right) \right]},
$$
$$
n = 0, 1, \ldots, N - 1. \qquad (16)
$$

The recursive formula with respect to n suggested in [69] is used to decrease the issue of the high computation cost of Racah polynomials when employing equation (14), and is indicated by the following formula:

$$
A_n \bar{r}_n^{(\alpha, \beta)}(s, a, b) = B_n \sqrt{\frac{\rho_r(n-1)}{\rho_r(n)}} \bar{r}_{n-1}^{(\alpha, \beta)}(s, a, b)
$$
$$
+ C_n \sqrt{\frac{\rho_r(n-2)}{\rho_r(n)}} \bar{r}_{n-2}^{(\alpha, \beta)}(s, a, b)
$$
$$
\bar{r}_0^{(\alpha, \beta)}(s, a, b) = \sqrt{\frac{w_r(s)}{\rho_r(0)} \left[\Delta X \left(s - \frac{1}{2} \right) \right]}
$$
$$
\bar{r}_1^{(\alpha, \beta)}(s, a, b) = -\frac{1}{w_r(s)} \frac{w_1(s) - w_1(s-1)}{X \left(s + \frac{1}{2} \right) - X \left(s - \frac{1}{2} \right)}
$$
$$
\sqrt{\frac{w_r(s)}{\rho_r(1)} \left[\Delta X \left(s - \frac{1}{2} \right) \right]} \qquad (17)
$$

where:

$$
A_n = \frac{n(\alpha + \beta + n)}{(\alpha + \beta + 2n - 1)(\alpha + \beta + 2n)}
$$
$$
B_n = x - \frac{(a^2 + b^2 + (a - \beta)^2 + (b + a)^2 - 2)}{4}
$$
$$
+ \frac{(\alpha + \beta + 2n - 2)(\alpha + \beta + 2n)}{8}
$$
$$
- \frac{(\beta^2 - \alpha^2) \left[\left(b + \frac{\alpha}{2} \right)^2 - \left(a - \frac{\beta}{2} \right)^2 \right]}{2(\alpha + \beta + 2n - 2)(\alpha + \beta + 2n)},
$$
$$
C_n = \frac{(\alpha + n - 1)(\beta + n - 1)}{2(\alpha + \beta + 2n - 2)(\alpha + \beta + 2n)} \left[\left(a + b + \frac{\alpha - \beta}{2} \right)^2 \right.
$$
$$
\left. - \left(n - 1 + \frac{\alpha + \beta}{2} \right)^2 \right] \left[\left(b - a + \frac{\alpha + \beta}{2} \right)^2 \right.
$$
$$
\left. - \left(n - 1 - \frac{\alpha + \beta}{2} \right)^2 \right].
$$

and

$$
w_n(s) = \frac{\Gamma(a+s+n+1)\Gamma(s-a+\beta+n+1)\Gamma(b+\alpha-s)\Gamma(b+\alpha+s+n+1)}{\Gamma(a-\beta+s+1)\Gamma(s-a+1)\Gamma(b-s-n)\Gamma(b+s+1)}.
$$

IV. THE PROPOSED EVOLUTIONARY WATERMARKING IMAGE MOMENTS METHOD FOR EMBEDDING POSITIONS AND STRENGTH (EWIMps)

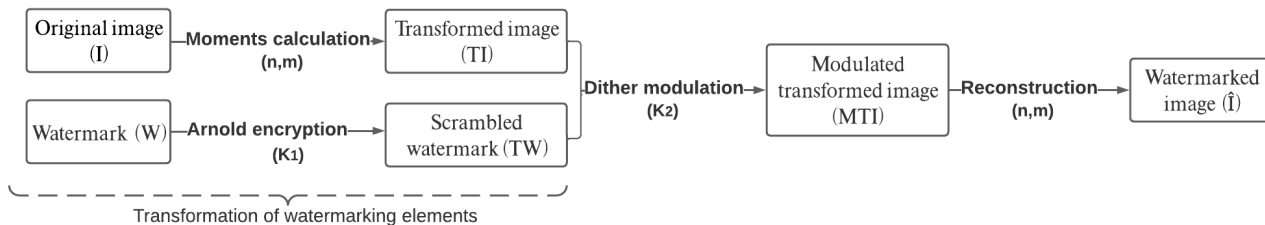The proposed optimization method allows an automatic selection of the best moments where the watermark data

FIGURE 1. The flowchart of the proposed EWIMps.

will be inserted while intelligently optimizing the embedding strength value. This optimization is performed by an evolutionary algorithm, which starts by generating an initial population (P_0) containing a set of randomly chosen individuals representing the population size (PS), each one forms a set of unique variables composed of embedding positions numbers and embedding strength. The imperceptibility and robustness performances of each individual are then assessed by exploring its variables in watermarking embedding and extraction procedures. In fact, after the calculation of image moments and the encryption of the watermark, the dither modulation technique is applied using the embedding strength variable to embed the binary scrambled watermark into moments coefficients whose numbers correspond to the embedding position variables of the individual, taking into consideration that one bit can be assigned to one-moment coefficient. The reconstruction process is afterward used to obtain the

final watermarked image. Employing the same parameters, the extracted watermark is obtained from moments of the attacked watermarked image applying the same dither modulation technique. Indicators of performance are finally calculated according to the quality of the watermarked image and the fidelity of the extracted watermark. Steps are repeated for each individual until the population size is reached, then the best one is chosen based on the highest performance. To generate the next population, we utilize a coding strategy that converts individuals into chromosomes composed of genes containing the embedding variables. Different evolutionary operators (selection-crossover-mutation) are then adopted for recombination purposes to enable altering the composition of genes and producing new chromosomes leading to a new population (P_k). Watermarking embedding and extraction procedures re-applied to individuals in order to assess their performance, and the fittest is then selected. The entire

FIGURE 2. Watermark embedding procedure.

process is repeated for each subsequent population (P_{k+1}) until a specific maximum number of generations ($k = MG$) with satisfactory results is reached. The flowchart of the EWIMps method is shown in Figure 1.

A. WATERMARKING EMBEDDING
The first step of the embedding procedure is the transformation of the blind watermarking elements. The original image (I) is transformed using orthogonal discrete moments with the order (n) and repetition (m). In addition, the watermark (W) is scrambled such that, even if a hacker is successful in extracting it, he will still only be able to acquire some random bits without the secret key (K_1) [62]. In the second step, dither modulation using a secret key (K_2) is applied to embed the binary scrambled watermark (TW) within the transformed image (TI) to obtain the modulated transformed image (MTI). Finally, the watermarked image ($\tilde{I}$) is reconstructed using the same coefficients (n, m)(See Figure 2).

1) MOMENTS CALCULATION
Discrete orthogonal moments: Krawtchouk (KMs), Tchebichef (TMs), Dual Hahn (DHMs), and Racah moments (RMs) presented previously are applied on a grayscale original image (I) with its corresponding size $IL = [HI \times WI]$ obtaining the transformed image (TI) constituted of moments (M_{nm}) calculated using the coefficients (n, m).

2) ARNOLD ENCRYPTION OF THE WATERMARK
The binary digital watermark (W) with its corresponding size $WL = [HW \times WW]$ needs to be scrambled in order to increase its security and improve its resistance to frequent and varied attacks. Since Arnold transform is intuitive, easy, periodic, and simple to use, it was chosen for this work as the pre-treatment approach for the watermark signal [6], [40].

The Arnold transformation and the inverse Arnold transformation are given by equations (18) and (19) respectively:

$$\begin{pmatrix} tw_x \\ tw_y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} w_x \\ w_y \end{pmatrix} mod\ N \qquad (18)$$

$$\begin{pmatrix} w_x \\ w_y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} tw_x \\ tw_y \end{pmatrix} mod\ N \qquad (19)$$

where (w_x, w_y) is the original pixel position of the watermark and (tw_x, tw_y) is the pixel position post-transformation, N is the period of the Arnold transform for the modulus operation that represents the key (K_1). The scrambled watermark denoted by (TW) is then transformed into a one-dimensional sequence of ones and zeros as follows:

$$TW = \{tw_i \in [0, 1]\} \quad i = 1, \ldots, WL \qquad (20)$$

3) DITHER MODULATION
The scrambled watermark is embedded by altering the magnitudes of the moments with the dither modulation function which is a crucial technique for signal encoding that maximizes embedding rates while minimizing the original signal distortion and guarantees durability in attack conditions environment [16]. Watermarking techniques have used the dither modulation embedding approach successfully as a particular kind of quantization index modulation suggested for information hiding [9], [19].

$$MM_{n_i m_i} = \left[\frac{M_{n_i m_i} - d_i\ (tw_i)}{\Delta} \right] \Delta + d_i\ (tw_i) \qquad (21)$$

In this study, the *WL*-bit length binary watermark ($tw_1, tw_2, \ldots, tw_{WL}$) is inserted using equation (21) in a set of moments ($M_{n_i m_i}$) whose numbers correspond to the embedding positions variables of each individual, to obtain the modified moments ($MM_{n_i m_i}$) that compose the modulated transformed image (MTI). [.] represents the rounding operator, Δ is the quantization step that refers to the embedding strength, and $d_i(.)$ is the ith dither function satisfying $d_i(1) = \Delta/2 + d_i(0)$ where the dither vector $d_i(0)$ has a uniform distribution in the [0, Δ] range [19]. We note that the security key (K_2) used in this step is composed of ([$d(0)$], [$d(1)$], Δ).

4) RECONSTRUCTION PROCESS
Reconstructing the entire image with small errors requires a large number of moments making it a laborious and long process. Therefore, we proposed to minimize the computing time by isolating the data quantity (D) in its frequency domain, reconstructing it, and adding to the original image in its
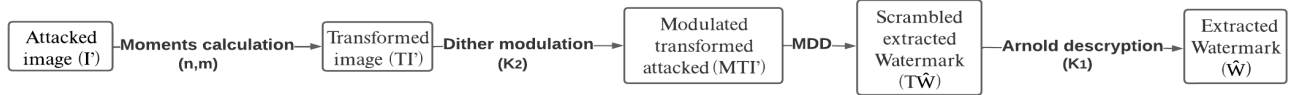
FIGURE 3. Watermark extracted procedure.

spatial domain, as proved in the equation (22). The first part represents the original image, while the second represents the data quantity in the frequency domain, which is equal to the difference between the modulated moments and the original ones ($D_{nm} = MM_{nm} - M_{nm}$). Instead of reconstructing the whole modulated transformed image (MTI), we only reconstruct the quantity (D_{nm}) to obtain the watermarked image ($\tilde{I}$) [19].

$$\tilde{I} = \sum_{n=1}^{HI} \sum_{m=1}^{WI} MM_{nm}P_n(x)P_m(y)$$

$$= \sum_{n=1}^{HI} \sum_{m=1}^{WI} (M_{nm} + D_{nm})\, P_n(x)P_m(y)$$

$$= \sum_{n=1}^{HI} \sum_{m=1}^{WI} M_{nm}P_n(x)P_m(y) + \sum_{n=1}^{HI} \sum_{m=1}^{WI} D_{nm}P_n(x)P_m(y)$$

$$= I + D \tag{22}$$

B. WATERMARKING EXTRACTION

In the suggested technique, the watermark extraction process under various attacks does not require the original image or any additional side information. The main difference between embedding and watermark extraction is the adoption of the Minimum Distance Decode (MDD) module used to extract the hidden binary watermark from the attacked image (I') (See Figure 3).

Moments are first performed on the attacked image (I') with the same order (n) and repetition (m). Then, the transformed attacked Image (TI') constitutes of moments ($M'_{n_i m_i}$) is resulted. These moments are quantized considering a bit value of $j \in [0, 1]$ to obtain the moments ($|M'_{n_i m_i}|_j$).

The operation of the Minimum Distance Decoder (MDD) is defined by the following formula:

$$t\hat{w}_i = arg\, min_{j\in[0,1]}(|M'_{n_i m_i}|_j - M'_{n_i m_i})^2 \quad i = 1, \ldots, WL \tag{23}$$

We calculate the distance between ($|M'_{n_i m_i}|_j$) and ($M'_{n_i m_i}$), depending on this distance, the extracted bit ($t\hat{w}_i$) is decided to be 0 or 1 [19]. The one-dimensional binary sequences are rearranged to form the binary watermark which is then decrypted by inverse Arnold with the same key (K_1) used in the encryption process. Finally, the extracted watermark ($\hat{W}$) is obtained.

Symbols of different embedding and extraction watermarking elements are listed in Table 3.

TABLE 3. Embedding and extraction elements.

	Symbol
Original image	I
Watermark	W
Transformed image	$TI\,[M_{nm}]$
Scrambled watermark	TW
Modulated transformed image	$MTI\,[MM_{nm}]$
Watermarked Image	$\tilde{I}$
Attacked image	I'
Transformed attacked image	$TI'\,[M'_{nm}]$
Modulated transformed attacked I	$MTI'\,[MM'_{nm}]$
Scrambled extracted watermark	$T\hat{W}$
Extracted watermark	$\hat{W}$

C. FITNESS FUNCTION AND ENCODING STRATEGY

1) FITNESS FUNCTION

The major challenge of creating an image watermarking method is to meet the two main factors that determine how well the watermarking algorithm performs: imperceptibility evaluated by The Peak Signal to Noise Ratio (PSNR) and robustness evaluated by the Normalized Correlation (NC). Hence, each candidate solution in our EWIMps is evaluated using the fitness function created by combining the two metrics of watermarking performance to achieve the optimal balance between these most important watermarking requirements [71]. This function is expressed as:

$$FF_j = PSNR_j + 100 \times NC_j \quad j = 1, \ldots, PS \tag{24}$$

The fittest individual of the population P_k with size PS is then retained:

$$Best\, indiv^{(P_k)} = \int_1^{PS} indiv_j(\max FF_j)^{(P_k)} \tag{25}$$

2) CHROMOSOME ENCODING STRATEGY

In the representation of our EWIMps algorithm, each individual with length (L) represents a set of variables called genes, these genes are the embedding positions (G_i) of the watermark with size (WL), concatenated with the representation of the embedding strength parameter (G'). Consequently, the final individual length is $L = WL + 1$. In the adopted binary encoding system, each gene is coded in a finite sequence of 0 and 1 to generate binary genes composed of the binary embedding positions of the watermark (Gb_i), and the binary strength embedding parameter (Gb'). The choice of the binary encoding scheme guarantees more diversity in our evolution pool while applying EWIMps operators. The
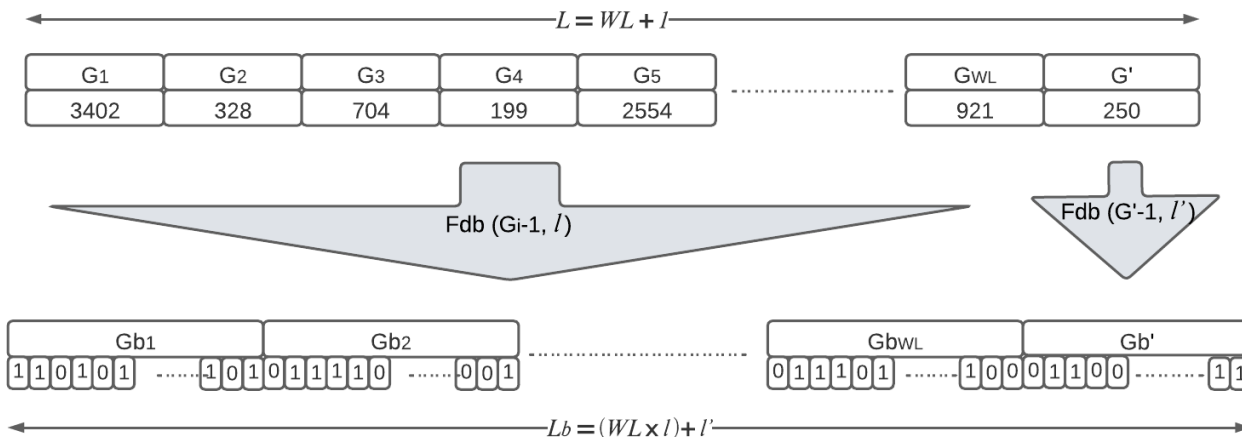
FIGURE 4. The proposed encoding strategy of the EWIMps method.

representation of the chromosome encoding strategy is shown in Figure 4.

Firstly, we optimize the embedding position (moments) of the transformed image with size (IL) where the watermark is inserted. Initially, values of variables needed in each individual are generated randomly:

$$G_i \in [2, \ldots, IL] \quad i = 1, \ldots, WL \quad (26)$$

The following requirements must be respected in relation to the framework parameters:

- The image size must respect the criterion: $2^{l-1} < IL \leq 2^l$
- Each gene (G_i) is encoded on l bits (length of a binary gene)
- The conversion function from decimal to binary basis system on l bits is given by:
  $Gb_i = Fdb(G_i - 1)$ where $G_i \neq 1$ and $Gb_i \in [0, 1]$

Secondly, we optimize the embedding strength parameter (Δ) represented by (G') in our chromosome. Initially, (G') is a positive value generated randomly and added to the chromosome genes (G_i), in such a way that:

$$G' \in [\Delta_{min}, \Delta_{max}] \quad (27)$$

where Δ_{min} and Δ_{max} are fixed experimentally. The following requirements must be respected in relation to the framework parameters:

- Δ_{max} must respect the criterion: $\Delta_{max} \leq 2^{l'}$
- The gene (G') is coded on l' bits (length of the binary gene)
- The conversion function from decimal to binary basis system on l' bits is given by:
  $Gb' = Fdb(G' - 1)$ where $G' \neq 1$ and $Gb' \in [0, 1]$

This encoding method eliminates the invalid individuals that may be produced in the following phases, with embedding positions greater than the transformed image size ($G_i > IL$), and embedding strength greater than Δ_{max} ($G' > \Delta_{max}$).

The length of the chromosome is then given by: $L_b = (WL \times l) + l'$.

D. EWIMps OPERATORS
1) SELECTION OPERATOR

The principle of "survival of the best" underlies the selection process: the better chromosome's fitness function is, the more likely to be selected. It determines in a population which individuals are selected as parents to produce fitter offspring.

The roulette wheel (known also as fitness proportionate) is the most widely employed selection method, where each individual has a selection probability associated with his fitness function value, giving higher probabilities to fitter individuals [72]. Even though this selection method ensures randomness due to the random generation of the probabilistic sequence, it cannot guarantee that the best individual will be able to take part in inheritance [73]. In order to improve the performances of our selection operator using the roulette wheel method, the best individual of the population P_k is assigned to the first position of the next population P_{k+1} without participating in the crossover and mutation procedures [73].

2) CROSSOVER OPERATOR

Crossover is carried out by exchanging segments of two chromosomes (parents) by cutting the strings at different positions called cutting points (CP). In our work, the crossover operator is applied to each binary gene of the two chromosomes by exchanging their segments at one or more cutting points in fixed or random positions. Hence, the offspring are then generated as represented in Figure 5. As the crossover may not be applied to every selected pair of parents, its application is controlled by the probability called the crossover rate (CR) [74]. $CR = 100\%$ means that all offspring are produced through
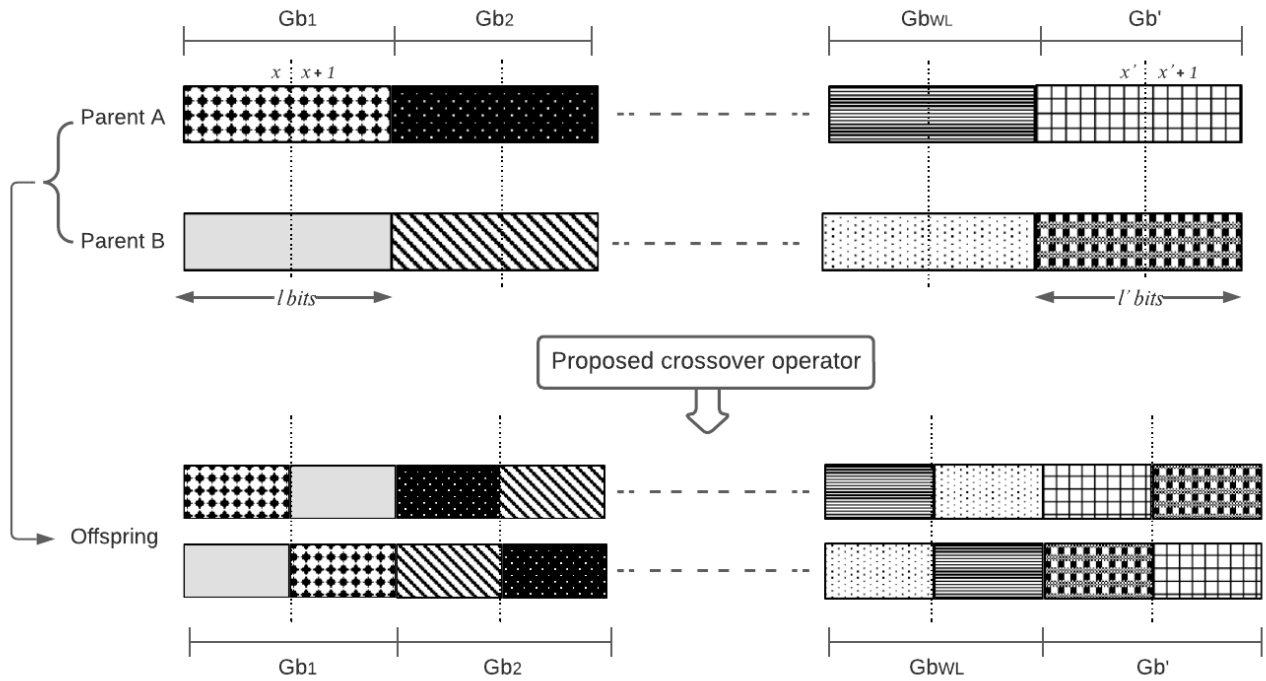
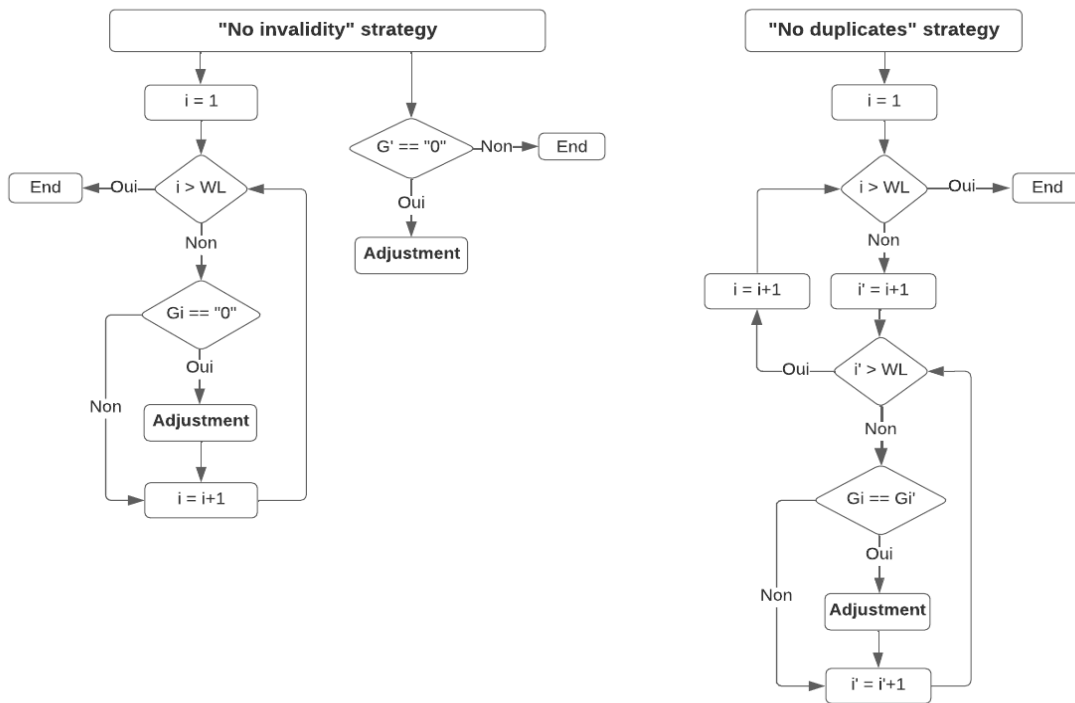**FIGURE 5.** Example of a single cutting point crossover.

FIGURE 6. Adjustment tests of the chromosome genes.

crossover, while $CR = 0\%$ means that the new generation is copied from the older one [72].

3) MUTATION OPERATOR

The mutation operator attempts to generate variations in the structure of possible solutions to guarantee variety. Since mutation can lead to major modifications in the composition of individuals, its application must be suitably adjusted using the appropriate mutation rate (MR) to maintain inheritance between parents and their offspring. This mutation rate is often very low compared with the crossover rate [75]. The mutation operator applies random changes by flipping a set of chosen bits from zero to one or vice versa [72]. The number of altered bits is specified by the mutation percentage (MP).

E. CHROMOSOME DECODING AND STOPPING CRITERIA

At the end of the mutation process, the decoding operation is performed. In order to improve our EWIMps algorithm effectiveness, we use the "No invalidity" strategy to avoid invalid individuals produced in the new generation with a gene (G_i or G') equal to zero. Additionally, because embedding position could not occur twice in the same individual, the "No duplicates" strategy is used to eliminate identical genes [76]. In both strategies, the gene is adjusted replacing it with a random value different from the existing ones. Therefore, this test is described in Figure 6.

The next population P_{k+1} takes over from P_k containing new individuals composed of embedding positions and embedding strength, and the EWIMps process is repeated until a stopping criterion is reached. The most used stopping criteria in the literature are: A fixed number of generations is reached, a satisfied fitness is attained, or no further increase in the best fitness function value [72]. In our study, a fixed maximum generation ($k = 0, 1, \ldots, MG$) is used as the stopping criterion. The best individual over generations is then given by:

$$\int_0^{MG} Best\ indiv = \int_1^{PS} indiv_j (\max FF_j)^{P_{MG}} \qquad (28)$$

F. ALGORITHM OF THE PROPOSED EWIMps

This subsection describes the proposed algorithm (algorithm 1) detailing the different EWIMps steps, starting with the initialization of the first generation and ending with the selection of the fittest individual over all generations.

V. EXPERIMENTAL STUDY

A set of pertinent experiments have been developed to validate the effectiveness of our EWIMps suggested model. These experiments were carried out using the standard MATLAB software and executed in an Intel Core i5-10th GEN under Windows 10 operating system. Three well-known images with the same size [HI x WI] that have been used in the following experimental study in addition to the binary watermark are shown in Figure 7. In the first subsection,

---

Algorithm 1 The Proposed Algorithm of Our Evolutionary EWIMps Method for the Embedding Parameters Selection

Input: Original image and watermark
Output: Watermarked and extracted watermark using the best positions and strength.
  Pre-processing:
  Original image I with size $IL = [HI$ x $WI]$
  Binary watermark W with size $WL = [HW$ x $WW]$
  Initialisation:
  Initialization of the first population P_0 contains PS number of individuals $Indiv_j$ with individual length L.
  Each individual contains WL number of embedding positions G_i and the embedding strength G' where $L = WL + 1$
  Image transformation:
  Moments calculation on original image I using the order (n) and repetition (m)
Output: Transformed image TI [M_{nm}]
  Watermark transformation:
  Arnold transform using the key K_1
  Reshape into one-dimensional vector form
Output: Scrambled watermark TW
  For each population P_k:
  for $k \leftarrow 0$ **to** MG **do**
    for $j \leftarrow 1$ **to** PS **do**
      Embedding process:
      for $i \leftarrow 1$ **to** WL **do**
        Applying dither modulation on each M_{nm} whose numbers correspond to the embedding position G_i, using the key $K_2 = (d_i(0), d_i(1), G')$
      end for
Output: Modulated transformed image MTI [MM_{nm}]
    Reconstruction process using the order (n) and repetition (m)
Output: Watermarked image $\tilde{I}$
    Extraction process:
    Moments calculation on attacked image I' using the order (n) and repetition (m)
Output: Transformed attacked image TI' [M'_{nm}]
    for $i \leftarrow 1$ **to** WL **do**
      Applying the dither modulation and the Minimum Distance Decoder (MDD) using the key K_2
    end for
    Inverse reshape into two-dimensional vector form
    Applying inverse Arnold transform using the key K_1
Output: Extracted watermark ($\hat{W}$)
    Calculate the fitness function (FF_j):
    end for
    Choice of the best individual: $Best\ indiv^{(P_k)} = indiv_j(\max FF_j)$
    Evolutionary operators: selection, crossover, mutation
Output: New population P_{k+1}
  end for
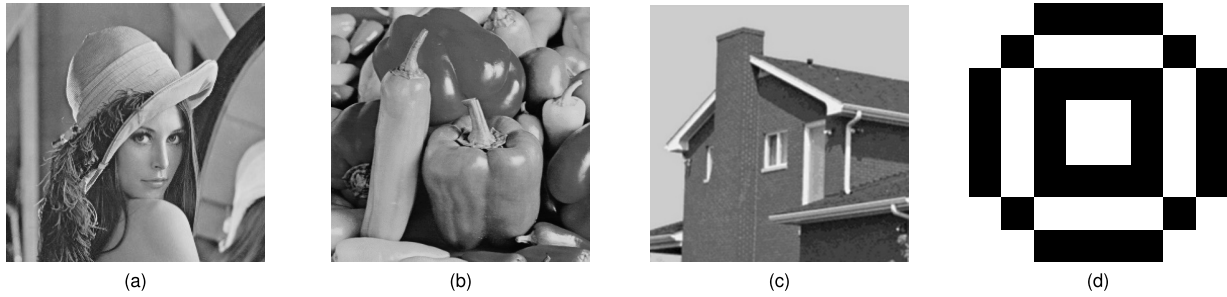 Selection of the final fittest individual: $Best\ indiv = indiv_j(\max FF_j)^{(P_{MG})}$

FIGURE 7. Original images: (a) Lena, (b) Pepper, (c) House and (d) Original binary watermark.

TABLE 4. Different attacks used in the EWIMps method for evaluating the robustness.

Abbreviation	Description
PSN 1	Salt and pepper (var=0.001)
PSN 2	Salt and pepper (var=0.01)
PN	Poisson noise
SN 1	Speckle (var=0.03)
SN 2	Speckle (var=0.02)
RT	Rotation (ang=-1)
GN 1	Gaussian (var=0.001)
GN 2	Gaussian (var=0.01)
JPEG 5	JPEG (Q=5%)
JPEG 50	JPEG (Q=50%)
JPEG 100	JPEG (Q=100%)

TABLE 5. Initial values of the evolutionary parameters of the EWIMps method.

Parameter	Value
MG	10
PS	100
CP	8 and 6 as fixed positions for Gb_i and Gb' respectively
CR	$(PS - 1)/PS$
MP	$2L/L_b$
MR	$4/PS$

TABLE 6. Effect of the maximum generation on the EWIMps performances.

MG	Performance Indicators			
	PSNR	NC	UIQI	BER
10	34.99	1	0.9954	0
20	35.09	1	0.9955	0
30	34.97	1	0.9954	0
40	35.19	1	0.9956	0
50	35.24	1	0.9956	0
60	35.16	1	0.9955	0
70	35.84	1	0.9962	0
80	35.23	1	0.9956	0
90	35.50	1	0.9958	0
100	35.44	1	0.9958	0

we will present the performance indicator adopted to assess the imperceptibility and robustness under different attacks, these attacks are described in the second subsection. Then, we will explore the evolutionary parameters used in the remaining exposed results. The adopted configuration parameters of our EWIMps method are listed in the next subsection. The final subsection is dedicated to the experimental results: the first part discusses the optimization of the embedding positions, while the second part performs the optimization of both embedding positions and embedding strength.

A. PERFORMANCE INDICATORS

To evaluate the effectiveness of our method under various attacks, different usual indicators will be used. Peak Signal-to-Noise Ratio and Universal Image Quality Index are two imperceptibility metrics used to assess the quality of the watermarked image $\tilde{I}(x, y)$ compared to the original image $I(x, y)$, while the Bit Error Rate and Normalized cross-Correlation are used to evaluate the robustness of the extracted watermark $\hat{W}(x, y)$ under attacks compared to the embedded watermark $W(x, y)$.

The PSNR is a mathematical measurement of image quality based on the pixel difference between two images. In our case, it compares the quality of the watermarked image with the original one [77]. The PSNR indicator is calculated by equation (29):

$$PSNR = 10 \log \frac{255^2}{MSE} \qquad (29)$$

where Mean Square Error (MSE) is determined by averaging the squared intensities of the pixels from the original image and the resulting watermarked image. This metric is given by equation (30):

$$MSE = \frac{1}{HI \times WI} \sum_{x=0}^{HI-1} \sum_{y=0}^{WI-1} [\tilde{I}(x, y) - I(x, y)]^2 \qquad (30)$$

To evaluate the Universal Image Quality Index (UIQI), three components are used to compare the original image to the watermarked one: loss of correlation, luminance distortion, and contrast distortion respectively [78], as defined in equation (31).

$$UIQI = \frac{\sigma_{I\tilde{I}}}{\sigma_I \sigma_{\tilde{I}}} \cdot \frac{2\mu_I \mu_{\tilde{I}}}{\mu_I^2 + \mu_{\tilde{I}}^2} \cdot \frac{2\sigma_I \sigma_{\tilde{I}}}{\sigma_I^2 + \sigma_{\tilde{I}}^2} \qquad (31)$$

μ_I and $\mu_{\tilde{I}}$ are the mean values of the original and watermarked images respectively.

σ_I and $\sigma_{\tilde{I}}$ are the standard deviations of the original and watermarked images respectively.
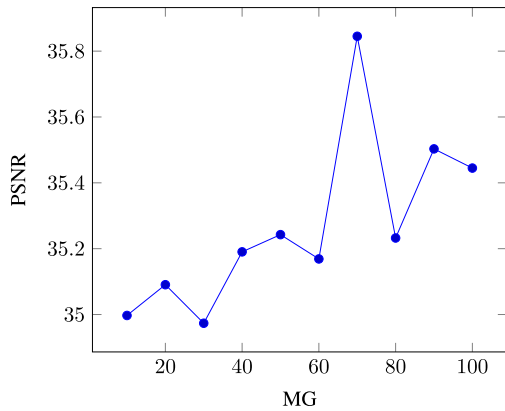
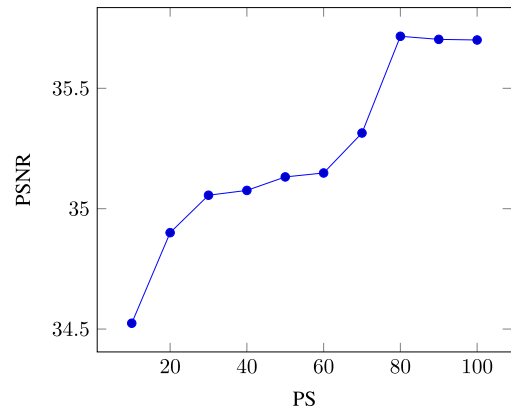**FIGURE 8.** PSNR performance of different MG values for the EWIMps method.

FIGURE 9. PSNR performance of different PS values for the EWIMps method.

TABLE 7. Effect of the population size on the EWIMps performances.

PS	Performance Indicators			
	PSNR	NC	UIQI	BER
10	34.52	1	0.9949	0
20	34.90	1	0.9953	0
30	35.05	1	0.9954	0
40	35.07	1	0.9955	0
50	35.13	1	0.9955	0
60	35.14	1	0.9955	0
70	35.31	1	0.9957	0
80	35.71	1	0.9961	0
90	35.70	1	0.9961	0
100	35.70	1	0.9961	0

$\sigma_{I\tilde{I}}$ is the covariance of both images.

The Normalized cross-Correlation is calculated based on equation (32) using the original and the extracted watermark pixel value at location (x, y). The extracted watermark is identical to the original when the NC value converges to one [6].

$$NC = \frac{\sum_{x=1}^{HW} \sum_{y=1}^{WW} W(x, y).\hat{W}(x, y)}{\sqrt{\sum_{x=1}^{HW} \sum_{y=1}^{WW} W(x, y)^2 \sum_{x=1}^{HW} \sum_{y=1}^{WW} \hat{W}(x, y)^2}} \quad (32)$$

Equation (33) is used to calculate the Bit Error Rate indicator. It should be highlighted that a lower BER value indicates good robustness of the watermark.

$$BER = \frac{\sum_{x=1}^{HW} \sum_{y=1}^{WW} W(x, y) \oplus \hat{W}(x, y)}{HW \times WW} \quad (33)$$

B. APPLIED ATTACKS

A well-performing watermarking system must resist different types of attacks that can occur during the transmission. Therefore, proving the invariance of the adopted image moments against attacks is crucial. Hence, attacks presented in Table 4 are applied to our watermarked image to evaluate the robustness of the proposed method. It should be noted that other geometric attacks are not selected since they can be easily treated by an image normalization pre-processing step [19].

C. EFFECT OF THE EVOLUTIONARY PARAMETERS ON THE PERFORMANCES OF OUR EWIMps METHOD

The choice of the evolutionary parameters of our EWIMps method is crucial to obtain optimal or nearly optimal solutions [72]. Therefore, a first set of experiments is run to select the optimum parameters: maximum generation (MG), population size (PS), cutting points (CP) number and nature (fixed or random position), and the mutation percentage (MP). The best-obtained values of these parameters (based on their performance indicators) will be used in the remaining experimental results. These experiments are applied to a gray-level Lena image using Krawtchouk moments, attacked by salt and pepper noise (variance 0.01), with a crossover rate $CR = (PS-1)/PS$ (since the first individual in the population does not take part in the crossover operation), and a mutation rate $MR = 0.05$.

Initial values of used parameters are presented in Table 5.

1) CHOICE OF THE MAXIMUM GENERATION

To determine the maximum number of generations, experiments were conducted over a range of 10 to 100 generations. Table 6 and Figure 8 illustrate the performance indicators obtained by varying the number of maximum generations used in our algorithm. We can see that with $MG = 70$ we obtain at the same time the maximum robustness (NC = 1) and the higher imperceptibility (PSNR = 35.84, UIQI = 0.9962). Consequently, for the remaining experiments, a maximum generation of 70 is adopted.

2) CHOICE OF THE POPULATION SIZE

A second set of tests was performed to examine the critical impact of population size. Indeed, a small population size reduces the search space and a large one increases the computation time. For this reason, the population size should be reasonable [72]. Table 7 and Figure 9 show the results of experiments where the population size varies between 10 and 100 individuals. According to the obtained results, the imperceptibility increases until a population size of 80 (PSNR = 35.71 dB) where it remains approximately the

TABLE 8. Effect of the cutting point crossover on the EWIMps performances.

	Gb_i	Gb'	PSNR	NC	UIQI	BER
			Performance Indicators			
One CP	$(x, x+1) = (3, 4)$	$(x', x'+1) = (2, 3)$	35.14	1	0.9955	0
	$(x, x+1) = (6, 7)$	$(x', x'+1) = (4, 3)$	35.70	1	0.9961	0
	$(x, x+1) = (9, 10)$	$(x', x'+1) = (6, 7)$	35.30	1	0.9957	0
	Rand	Rand	35.05	1	0.9954	0
Two CP	$(x, x+1) = (3, 4) ; (y, y+1) = (7, 8)$	$(x', x'+1) = (2, 3) ; (y', y'+1) = (5, 6)$	35.35	1	0.9957	0
	$(x, x+1) = (4, 5) ; (y, y+1) = (8, 9)$	$(x', x'+1) = (3, 4) ; (y', y'+1) = (6, 9)$	34.54	1	0.9949	0
	$(x, x+1) = (6, 7) ; (y, y+1) = (10, 11)$	$(x', x'+1) = (4, 5) ; (y', y'+1) = (7, 8)$	35.10	1	0.9945	0
	Rand	Rand	34.14	1	0.9945	0

TABLE 9. Effect of the mutation percentage on the EWIMps performances.

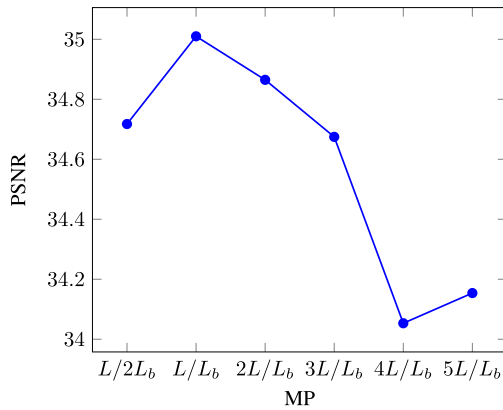| MP	Performance Indicators			
	PSNR	NC	UIQI	BER
$L/2L_b$	34.71	1	0.9952	0
L/L_b	35.01	1	0.9954	0
$2L/L_b$	34.86	1	0.9952	0
$3L/L_b$	34.67	1	0.9952	0
$4L/L_b$	34.05	1	0.9943	0
$5L/L_b$	34.15	1	0.9945	0

FIGURE 10. PSNR performance of different MP values for the EWIMps method.

TABLE 10. Original image and watermark configuration.

	2D size	1D length	Encoding parameter
Original Image	$[HI \times WI] = 64 \times 64$	$IL = 4096$	-
Watermark	$[HW \times WW] = 8 \times 8$	$WL = 64$	$N = 20$

TABLE 11. Image moments configuration.

	Krawtchouk	Tchebichef	Racah	Dual Hahn
n	64	62	64	64
m	64	62	64	64
p_1	0.5	-	-	-
p_2	0.5	-	-	-

same. Moreover, we can see that higher population sizes allow more possible combinations, giving a chance to a large number of individuals to become potential solutions, which guarantees a higher genetic diversity and allows reaching more accurate performance [75]. Therefore, $PS = 80$ allows a good compromise between diversity and computation time.

TABLE 12. Watermarking embedding and extraction configuration.

	Optimization of the embedding positions	Optimization of the embedding positions and strength
Δ	253 (experimentally chosen)	Unknown (varies between 100 and 400)
K_1	N	N
K_2	$([d(0)], [d(1)], \Delta)$	$([d(0)], [d(1)], \Delta)$

TABLE 13. Evolutionary algorithm configuration.

	Type or value
MG	70
PS	80
L	64 in the case of the embedding positions optimization 65 in the case of the embedding positions and strength optimization
l	12
l'	8
L_b	(64×12) in the case of the embedding positions optimization $(64 \times 12) + 8$ in the case of the embedding positions and strength optimization
CP	Single fixed positions at 6 and 4 for Gb_i and Gb' respectively
CR	$(80 - 1) / 80$
MP	L/L_b
MR	$4/PS = 0.05$
FF	$PSNR + 100 \times NC$

3) CHOICE OF THE CUTTING POINT NUMBER AND NATURE

This subsection investigates the effect of the cutting point crossover by exploring its number (one or two) and nature (fixed or random) for a population size of 80 with a maximum of 70 generations. Our chromosome is composed of WL binary genes Gb_i coded on $l = 12$ bits concatenated with the binary gene Gb' coded on $l' = 8$. Thus different numbers and natures of cutting points will be applied to each gene separately. The one cutting point is applied on Gb_i between $(x, x+1)$ positions, and on Gb' between $(x', x'+1)$ positions. On the other hand, two cutting point positions are applied between $(x, x+1)$, $(y, y+1)$ and $(x', x'+1)$, $(y', y'+1)$ on Gb_i and Gb' respectively. Table 8 presents the explored positions of the cutting points crossover where the following condition must be respected: $[(x, y) \neq (1, l)$ and $(x', y') \neq (1, l')]$. It is shown that the best performance indicators (PSNR $= 35.70$ dB, NC $= 1$) are obtained using one fixed CP at position 6 for each Gb_i and position 4 for Gb'.

4) CHOICE OF THE MUTATION PERCENTAGE

In order to explore the effect of mutation percentage on the efficiency of the proposed model, different values of MP are

applied using 80 individuals and a maximum generation of 70, with a fixed single cutting point at positions 6 and 4 for Gb_i and Gb' respectively. According to the resulting values shown in Table 9 and Figure 10, the best performances are obtained with $MP = L/L_b$ (PSNR = 35.01 dB, NC = 1) where L_b represents the length of the chromosome: $L_b = (WL \times l) + l'$ and L the size of the individual: $L = WL + 1$. We note that the best mutation percentage value allows a compromise between diversity and the parent-offspring link. The optimal evolutionary settings resulted are displayed in Table 13 and utilized in subsequent experiments.

D. CONFIGURATION PARAMETERS OF THE EWIMps METHOD

The selected parameters that will be used in our method concerning: the original image and the watermark, the image moments, the embedding and extraction procedures, and the evolutionary algorithm are listed in Tables [10 - 13] respectively.

E. EXPERIMENTAL RESULTS

In this subsection, we present the experimental results to validate the effectiveness of our EWIMps method. The obtained performances using image moments are compared to other image transformations in the frequency domain. Indeed, we apply the standard and widely used DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform) in the image transformation step before the watermarking embedding. For a pertinent comparison, the same techniques and parameters used with image moments in the evolutionary process, the watermarking embedding, and the watermarking extraction are reapplied with DCT and DWT transformations. First, we present the obtained results with the ideal embedding moments when various performance quality indices are incorporated into the fitness function. Thus, the number of variables in this part is adjusted to the watermark size (WL). Next, we demonstrate the relevance of the optimum embedding strength in addition to the optimum embedding moments. Therefore, the number of unknown variables becomes (WL+1) in this part. This will yield two parts of the experimental study that define a watermarking parameter optimization challenge.

1) COMPARISON OF PERFORMANCES WITH STATE-OF-THE-ART METHODS OF POSITIONS SELECTION

In this subsection, an experiment was performed to prove the superiority of the proposed EWIMps method for selecting the best embedding positions, compared with other traditional methods that choose the coefficients from the high, low, and middle-frequency bands [3], or use the zig-zag and the random methods [6], [17]. For a fair comparison, these selection methods were implemented using the same adopted dither modulation technique to embed the watermark in the Lena cover image using Krawtchouk and Dual Hahn moments. Table 14 outlines the PSNR and NC values computed for each watermarked image and extracted watermark respectively,

TABLE 14. Watermarking performances comparison between the proposed algorithm and other selection bands under SN 2 attack.

Selection bands	KMs		DHMs	
	PSNR	NC	PSNR	NC
Low frequency positions	32.71	0.981	31.14	0.993
Middle frequency positions	35.68	0.975	34.41	0.981
High frequency positions	35.01	0.867	33.65	0.891
Random positions	36.67	0.953	34.87	0.961
Zig-zag ordered positions	33.15	1	32.47	0.988
EWIMps positions	38.05	1	36.20	1

under salt and pepper noise with a variance of 0.01. It can be seen from the obtained experimental results that the proposed blind watermarking method based on the automatic selection of the embedding positions has a significantly better performance compared to other methods. This result occurs because of the robustness of the genetic algorithm to find the optimum positions that provide satisfactory results. We can conclude that the proposed EWIMps method is more resilient against image attacks and gives the best performances in terms of robustness and imperceptibility.

2) OPTIMIZATION OF THE EMBEDDING POSITIONS

This first set of experiments aims to discover the ideal image region to insert the watermark data. First, we show the imperceptibility and robustness results of the EWIMps model applied to Lena, Pepper, and House images. Our experiments include 11 scenarios corresponding to the 11 attacks listed in Table 4, where each scenario involves a cycle of watermarking embedding and extraction process. Then, we demonstrate the high performances of the investigated transformation families. Finally, we perform the improvement of the fitness function along the process and the distribution of the best embedding positions.

- **Imperceptibility analysis**

The imperceptibility is evaluated by comparing the produced watermarked image generated at each scenario with the original one. Even though imperceptibility is independent of the attacks applied before the extraction phase, here the imperceptibility is reevaluated at each scenario to expand the diversity area and explore the largest number of coefficients possible. Tables 15, 16 and 17 report the imperceptibility performance using the three tested images respectively where the PSNR and UIQI results for different image transformations in each scenario are presented. From these tables, we observe that we obtain similar PSNR and UIQI values across scenarios for each transformation. Therefore, the evaluation will be based on the obtained average (MEAN) to analyze the deformation produced after the embedding process. The average values presented in Tables 15, 16 and 17 clearly show that the model achieves good imperceptibility (the average value of PSNR varies between 31.85 and 44.13 dB) indicating the high quality of the watermarked image. The obtained results demonstrate that discrete transforms (DCT and DWT) produce the highest quality of the watermarked images

TABLE 15. Imperceptibility indicators of embedding positions optimization for Lena image.

Scenario	PSNR						UIQI					
	KMs	TMs	RMs	DHMs	DCT	DWT	KMs	TMs	RMs	DHMs	DCT	DWT
Sc 1	38.77	34.14	38.42	36.75	44.84	44.82	0.997	0.994	0.997	0.996	0.999	0.999
Sc 2	38.19	34.12	38.01	36.35	43.26	44.82	0.997	0.994	0.997	0.996	0.999	0.999
Sc 3	38.54	32.73	38.18	36.48	42.69	44.60	0.997	0.992	0.997	0.996	0.999	0.999
Sc 4	37.77	34.44	37.14	34.85	42.84	43.92	0.997	0.994	0.997	0.995	0.999	0.999
Sc 5	36.87	30.29	37.51	35.87	42.80	43.62	0.996	0.986	0.997	0.996	0.999	0.999
Sc 6	37.95	34.10	38.70	36.17	43.26	44.18	0.997	0.994	0.997	0.996	0.999	0.999
Sc 7	39.09	29.58	38.88	36.47	42.94	43.29	0.998	0.979	0.998	0.996	0.999	0.999
Sc 8	37.14	28.33	37.85	35.65	42.85	43.08	0.997	0.984	0.997	0.996	0.999	0.999
Sc 9	37.43	31.72	37.93	36.08	43.27	43.82	0.997	0.990	0.997	0.996	0.999	0.999
Sc 10	38.33	33.24	37.77	35.93	42.53	43.88	0.997	0.993	0.997	0.996	0.999	0.999
Sc 11	39.01	34.11	38.72	36.60	43.26	44.92	0.998	0.994	0.997	0.996	0.999	0.999
MEAN	38.10	31.85	38.11	36.11	43.14	44.09	0.997	0.989	0.997	0.996	0.999	0.999

TABLE 16. Imperceptibility indicators of embedding positions optimization in Pepper image.

Scenario	PSNR						UIQI					
	KMs	TMs	RMs	DHMs	DCT	DWT	KMs	TMs	RMs	DHMs	DCT	DWT
Sc 1	38.47	35.41	38.8	36.16	44.79	45.14	0.998	0.996	0.998	0.997	0.999	0.999
Sc 2	37.26	33.76	38.03	35.67	42.53	44.93	0.986	0.995	0.997	0.996	0.999	0.999
Sc 3	38.3	36.56	38.36	35.87	43.18	43.52	0.998	0.997	0.998	0.996	0.999	0.999
Sc 4	37.18	34.65	36.67	34.88	43.03	43.47	0.997	0.996	0.997	0.996	0.999	0.999
Sc 5	37.44	31.95	37.36	34.91	42.55	43.71	0.997	0.992	0.997	0.996	0.999	0.999
Sc 6	37.21	34.65	37.47	35.04	43	44.88	0.997	0.996	0.997	0.996	0.999	0.999
Sc 7	38.31	33.84	38.79	36.28	42.96	43.66	0.998	0.995	0.998	0.997	0.999	0.999
Sc 8	37.22	30.47	37.33	34.76	43.69	43.58	0.997	0.989	0.997	0.996	0.999	0.999
Sc 9	37.4	31.61	37.32	35.65	43.07	44.17	0.997	0.992	0.997	0.996	0.999	0.999
Sc 10	37.57	30.69	37.74	35.69	43.84	43.64	0.997	0.99	0.997	0.996	0.999	0.999
Sc 11	38.09	35.98	38.66	36.11	44.8	44.82	0.998	0.997	0.998	0.997	0.999	0.999
MEAN	37.67	33.59	37.86	35.54	43.4	44.13	0.996	0.994	0.997	0.996	0.999	0.999

TABLE 17. Imperceptibility indicators of embedding positions optimization for House image.

Scenario	PSNR						UIQI					
	KMs	TMs	RMs	DHMs	DCT	DWT	KMs	TMs	RMs	DHMs	DCT	DWT
Sc 1	38.4	32.6	38.79	36.87	44.8	44.91	0.998	0.994	0.998	0.997	0.999	0.999
Sc 2	37.55	32.25	38.21	36.51	43.4	44.43	0.998	0.994	0.998	0.997	0.999	0.999
Sc 3	38.97	33.71	38.36	36.7	43.3	43.73	0.998	0.995	0.998	0.997	0.999	0.999
Sc 4	37.36	32.26	36.32	35.17	42.86	43.38	0.998	0.994	0.997	0.996	0.999	0.999
Sc 5	38.1	32	36.74	35.23	43.4	44.57	0.998	0.993	0.997	0.996	0.999	0.999
Sc 6	38.39	30.77	38.01	36.41	43.27	44.96	0.998	0.992	0.998	0.997	0.999	0.999
Sc 7	38.4	30.23	38.73	37.12	42.74	44.37	0.998	0.991	0.998	0.997	0.999	0.999
Sc 8	37.62	33.87	37	36.25	43.14	42.98	0.998	0.995	0.997	0.997	0.999	0.999
Sc 9	38.19	33.01	37.88	36	42.66	43.95	0.998	0.995	0.998	0.997	0.999	0.999
Sc 10	37.55	33.05	38.34	36.2	43.38	43.74	0.998	0.995	0.998	0.997	0.999	0.999
Sc 11	38.48	35.17	39.16	37.04	44.74	45.07	0.998	0.996	0.998	0.997	0.999	0.999
MEAN	38.09	32.62	37.95	36.27	43.42	44.09	0.998	0.994	0.997	0.996	0.999	0.999
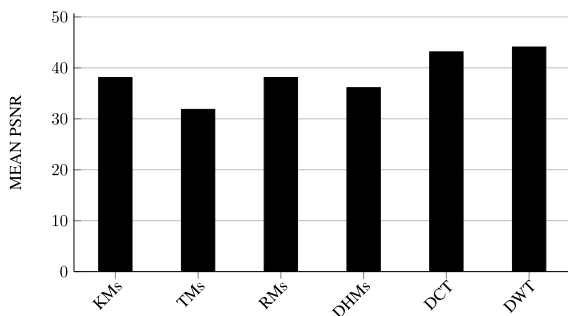
FIGURE 11. Average PSNR values by image transformations for the optimization of embedding positions using Lena image.

(the mean of PSNR varies between 43.14 and 44.13 dB), while some discrete orthogonal moments do not satisfy the imperceptibility, which is one of the crucial factors of image watermarking. Using Krawtchouk and Racah moments in embedding watermarking on the Lena, Pepper, and House images, provides an approximate high level of imperceptibility shown by their corresponding PSNR mean values of 38.1 and 38.11 dB, 37.67 and 37.86 dB, 38.09 and 37.95 dB for both moments respectively. On the other hand, a significant distortion is noted when embedding the watermark in Tchebichef moments that damages the quality of the obtained watermarked with average PSNR values of 31.85, 33.59, and 32.62 dB of the three tested images respectively. Although, the UIQI metric which considers the Human Visual System proves a good quality of the produced watermarked images and a similar behavior for all the adopted image transformations by producing average values between 0.989 and 0.999.

TABLE 18. Watermarked images in SC 3 in the case of the embedding positions optimization for different transformations.

	Lena	Pepper	House
KMs (Krawtchouk moments)			
TMs (Tchebichef moments)			
RMs (Racah moments)			
DHMs (Dual Hahn moments)			
DCT			
DWT			

TABLE 19. Robustness indicators against attacks of embedding positions optimization for Lena image.

		NC						BER					
		KMs	TMs	RMs	DHMs	DCT	DWT	KMs	TMs	RMs	DHMs	DCT	DWT
Sc 1	PSN 1	1	0.923	1	1	1	1	0	0.078	0	0	0	0
Sc 2	PSN 2	1	0.854	1	1	0.886	1	0	0.156	0	0	0.109	0
Sc 3	PN	1	0.968	1	1	0.923	0.926	0	0.0313	0	0	0.078	0.078
Sc 4	SN 1	0.939	0.839	0.906	0.926	0.757	0.766	0.062	0.156	0.093	0.078	0.218	0.250
Sc 5	SN 2	0.952	0.825	0.954	0.953	0.762	0.812	0.046	0.187	0.046	0.046	0.234	0.187
Sc 6	RT	1	0.818	1	1	0.923	1	0	0.187	0	0	0.078	0
Sc 7	GN 1	1	0.889	1	1	1	0.984	0	0.109	0	0	0	0.015
Sc 8	GN 2	0.866	0.820	0.875	0.886	0.717	0.736	0.140	0.171	0.125	0.109	0.296	0.296
Sc 9	JPEG 5	0.745	0.757	0.736	0.717	0.747	0.726	0.296	0.2500	0.296	0.328	0.265	0.296
Sc 10	JPEG 50	0.954	0.825	0.954	0.984	0.747	0.836	0.046	0.171	0.046	0.015	0.265	0.171
Sc 11	JPEG 100	1	0.906	1	1	0.923	1	0	0.093	0	0	0.078	0
MEAN		0.950	0.874	0.947	0.951	0.853	0.889	0.053	0.126	0.055	0.052	0.147	0.117

TABLE 20. Robustness indicators against attacks of embedding positions optimization for Pepper image.

		NC						BER					
		KMs	TMs	RMs	DHMs	DCT	DWT	KMs	TMs	RMs	DHMs	DCT	DWT
Sc 1	PSN 1	1	0.857	1	1	1	1	0	0.14	0	0	0	0
Sc 2	PSN 2	1	0.843	1	1	0.913	1	0	0.156	0	0	0.093	0
Sc 3	PN	1	0.896	1	1	0.936	0.93	0	0.109	0	0	0.062	0.078
Sc 4	SN 1	0.848	0.75	0.92	0.923	0.736	0.793	0.156	0.25	0.078	0.078	0.296	0.203
Sc 5	SN 2	0.906	0.825	0.968	0.984	0.755	0.806	0.09	0.187	0.031	0.015	0.265	0.203
Sc 6	RT	0.984	0.848	1	1	0.86	1	0.015	0.156	0	0	0.156	0
Sc 7	GN 1	1	0.857	1	1	0.984	0.984	0	0.14	0	0	0.015	0.015
Sc 8	GN 2	0.784	0.82	0.892	0.892	0.727	0.714	0.234	0.171	0.109	0.109	0.328	0.265
Sc 9	JPEG 5	0.726	0.755	0.727	0.736	0.736	0.717	0.296	0.265	0.281	0.312	0.296	0.296
Sc 10	JPEG 50	0.968	0.861	0.968	0.968	0.745	0.718	0.031	0.14	0.031	0.031	0.296	0.281
Sc 11	JPEG 100	1	0.909	1	1	1	1	0	0.093	0	0	0	0
MEAN		0.928	0.838	0.952	0.954	0.853	0.878	0.074	0.164	0.048	0.049	0.164	0.121

TABLE 21. Robustness indicators against attacks of embedding positions optimization for House image.

		NC						BER					
		KMs	TMs	RMs	DHMs	DCT	DWT	KMs	TMs	RMs	DHMs	DCT	DWT
Sc 1	PSN 1	1	0.896	1	1	1	1	0	0.109	0	0	0	0
Sc 2	PSN 2	1	0.813	1	1	0.896	1	0	0.203	0	0	0.109	0
Sc 3	PN	1	0.923	1	1	0.92	0.926	0	0.078	0	0	0.078	0.078
Sc 4	SN 1	0.843	0.787	0.902	0.892	0.736	0.755	0.156	0.203	0.093	0.109	0.296	0.265
Sc 5	SN 2	0.861	0.8	0.936	0.952	0.736	0.793	0.14	0.203	0.062	0.046	0.312	0.203
Sc 6	RT	1	0.836	1	1	0.926	1	0	0.171	0	0	0.078	0
Sc 7	GN 1	1	0.875	1	1	1	0.984	0	0.125	0	0	0	0.015
Sc 8	GN 2	0.774	0.773	0.92	0.707	0.717	0.745	0.25	0.265	0.078	0.312	0.296	0.281
Sc 9	JPEG 5	0.727	0.769	0.726	0.717	0.717	0.736	0.281	0.234	0.296	0.296	0.328	0.281
Sc 10	JPEG 50	0.937	0.83	0.968	0.97	0.727	0.875	0.062	0.171	0.031	0.031	0.281	0.125
Sc 11	JPEG 100	1	0.889	1	1	1	1	0	0.109	0	0	0	0
MEAN		0.922	0.835	0.929	0.934	0.852	0.892	0.08	0.17	0.073	0.069	0.161	0.113

Table 18 shows the watermarked images resulting when the chosen embedding coefficients are optimized using our proposed method in different types of transformations in the case of the third scenario (Sc 3). Figure 11 illustrates the average PSNR for each image transformation. According to Table 18 and Figure 11, we can conclude that the watermarking application using our proposed EWIMps method largely satisfy the imperceptibility property with the optimization selection of embedding moments. Overall, we have proved that discrete transforms reach the best level of quality according to the watermarked images, followed by KMs and RMs, while TMs produce a remarkable distortion phenomenon.

- **Robustness analysis**

In this subsection, the same attacks are applied to the watermarked images. The robustness property is then examined to describe the similarity between the original and the extracted watermark using the NC and BER metrics. These metrics are inversely proportional (the larger the NC, the lower the BER) and the watermarking algorithm reach the highest level of robustness when the NC and BER values are 1 and 0 respectively. Tables 19, 20 and 21 present the results of the robustness indicators under the specified attacks where the embedding positions are selected using the EWIMps optimization method, in the case of Lena, Pepper, and House images respectively.

TABLE 22. Extracted watermarks from Lena watermarked in the case of the embedding positions optimization.

Attacks	KMs	TMs	DHMs	RMs	DCT	DWT
PSN 1						
PSN 2						
PN						
SN 1						
SN 2						
RT						
GN 1						
GN 2						
JPEG 5						
JPEG 50						
JPEG 100						

FIGURE 12. Average NC values of embedding positions optimization using Lena image against various attacks.

According to these tables, it's clear that the proposed Racah and Dual Hahn moments keep satisfying mean values of BER (0.055, 0.048, 0.073 with RMs and 0.052, 0.049, 0.069 with DHMs) and a mean values of NC (0.947, 0.952, 0.929 with RMs and 0.951, 0.954, 0.934 with DHMs) for Lena, Pepper and House respectively. These values indicate that RMs and DHMs can be useful for the secure transport of the watermark under the majority of attacks. Thus, they could present the best choice of image transformations since they achieve an outstanding performance of robustness. Furthermore, Krawtchouk moments perform well throughout the experiments and provide good robustness (Mean NC of 0.950, 0.928, 0.922 for Lena, Pepper, and House images respectively, Mean BER < 0.08). Otherwise, Tchebichef moments seem to have the lowest resistance to most attacks (Mean NC < 0.874 and Mean BER > 0.126) which proves that the optimized Tchebichef coefficients used for embedding the watermark could not provide strong robustness performance. On the other hand, we notice that the discrete transforms do not satisfy the robustness requirement (Mean NC < 0.892 and Mean BER > 0.113). The extracted watermark resulting in each transformation type is given in Table 22 in the case of embedding positions optimization using Lena image, while Figure 12 shows the average NC values against different attacks. According to all previous results, we conclude that, unlike the imperceptibility criterion results, using image moments for the watermarking process with the optimization of embedding locations is generally more efficient and robust than discrete transforms. Indeed, DHMs, RMs, and KMs can resist different types of attacks, indicating their superiority in terms of securing the transmission of the watermark.

As previously noted, the main goal of image watermarking applications is to meet both imperceptibility and robustness requirements. Nevertheless, from the previously obtained results, we conclude that each transformation type performs better on one of the two performance factors (imperceptibility and robustness) for watermarking, but not necessarily both. Consequently, our evaluation of the image transformations will be based on the adopted fitness function which takes into consideration the two performance factors.

TABLE 23. Performances based on the fitness function in the case of the embedding positions optimization.

		Fitness function					
		KMs	TMs	RMs	DHMs	DCT	DWT
Sc 1	PSN 1	+++		+++	+++	+++	+++
Sc 2	PSN 2	+++		+++	+++	+++	+++
Sc 3	PN	+++	+	+++	+++	+++	+++
Sc 4	SN 1	+					
Sc 5	SN 2	+		+++	+++		
Sc 6	RT	+++		+++	+++	+++	+++
Sc 7	GN 1	+++		+++	+++	+++	+++
Sc 8	GN 2			+			
Sc 9	JPEG 5						
Sc 10	JPEG 50	+++		+++	+++		+
Sc 11	JPEG 100	+++		+++	+++	+++	+++
SUM		23	1	25	24	18	19

- **Effect of the image transformations on the fitness function in the case of the embedding positions optimization**

To select the appropriate image transformations among all available image transformation families, we adopt a similar evaluation method as described by Tsougenis et al. [18]. Table 23 reports the best fitness function values where FF > 128.84 dB. This minimum fitness function value is calculated using equation 24 and based on the mean value of imperceptibility (PSNR = 38.66 dB) and the mean value of robustness (NC = 0.90) of all images.

It is worth mentioning that each symbol (+) under a specific attack indicates if the image transformation reaches the fixed fitness function threshold for Lena, Pepper, and House images respectively, i.e., for scenario 5 under Speckle noise with (var=0.02), RMs achieve the best fitness function for the three tested images, KMs reach the best fitness function only for House image, while TMs do not satisfy the adopted threshold fitness function. The SUM value is the sum of all (+) symbols obtained for each image transformation over the 11 scenarios. Based on the obtained results in Table 23, it can be concluded that Racah moments outperform other image transformations. Furthermore, Krawtchouk and Dual Hahn moments provide a good trade-off between robustness and imperceptibility. However, DWT seems to perform better compared with DCT transform. On the other hand,
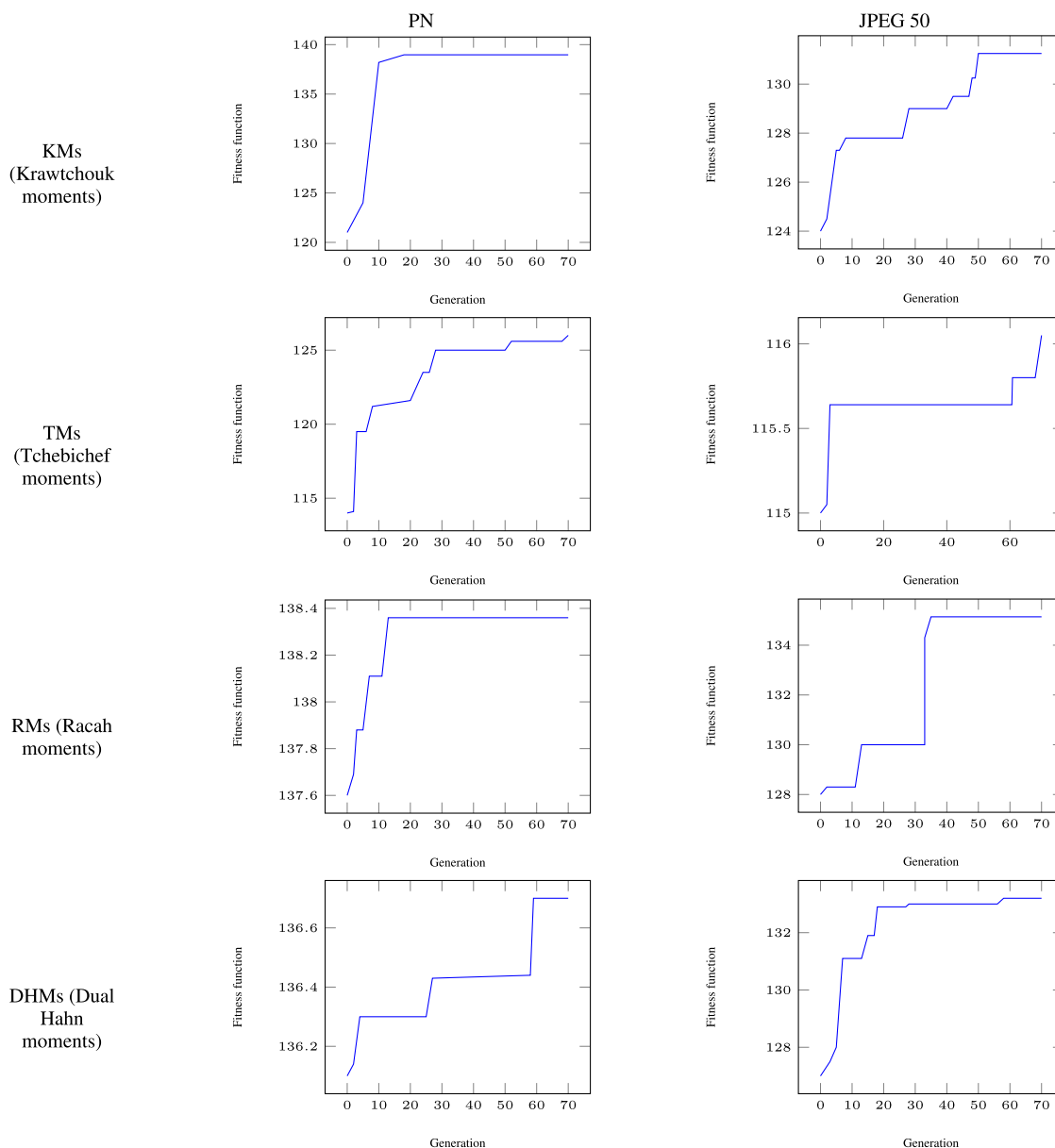
FIGURE 13. Evolution of the fitness function through generations using House image under PN and JPEG 50 attacks in the case of embedding positions optimization.

Tchebichef moments damage the quality of the watermarked image and could be easily affected by the insecure channel.

- **Effect of the adopted selection operator on the EWIMps performance**

In order to visualize the impact of the adopted selection operator of our proposed EWIMps method, the fitness function of the best individual in each generation is represented in Figure 13 for each image transformation under PN attack and JPEG 50 compression using House image. From the illustrated figure, we can infer that the obtained performance evolves after a few generations and continues to improve over iterations (from FF=124 in P_1 to FF=131.25 in P_{50} for KMs under JPEG 50, and from FF=136.1 in P_1 to FF=136.7 in P_{59}

for DHMs under PN). This improvement is due to the diversification obtained with the selection operator used besides the evolutionary operators that allow getting the most satisfactory positions.

- **Distribution of the embedding positions of the best individual**

In this subsection, we describe the obtained position of the best embedding moments allowing the highest performances. Figure 14 shows the distribution of these positions for Lena image moments under PSN 1 and SN 2 attacks for different adopted discrete moment families. According to this figure, we can observe that the best resulting locations are not condensed in a precise portion of the image moments
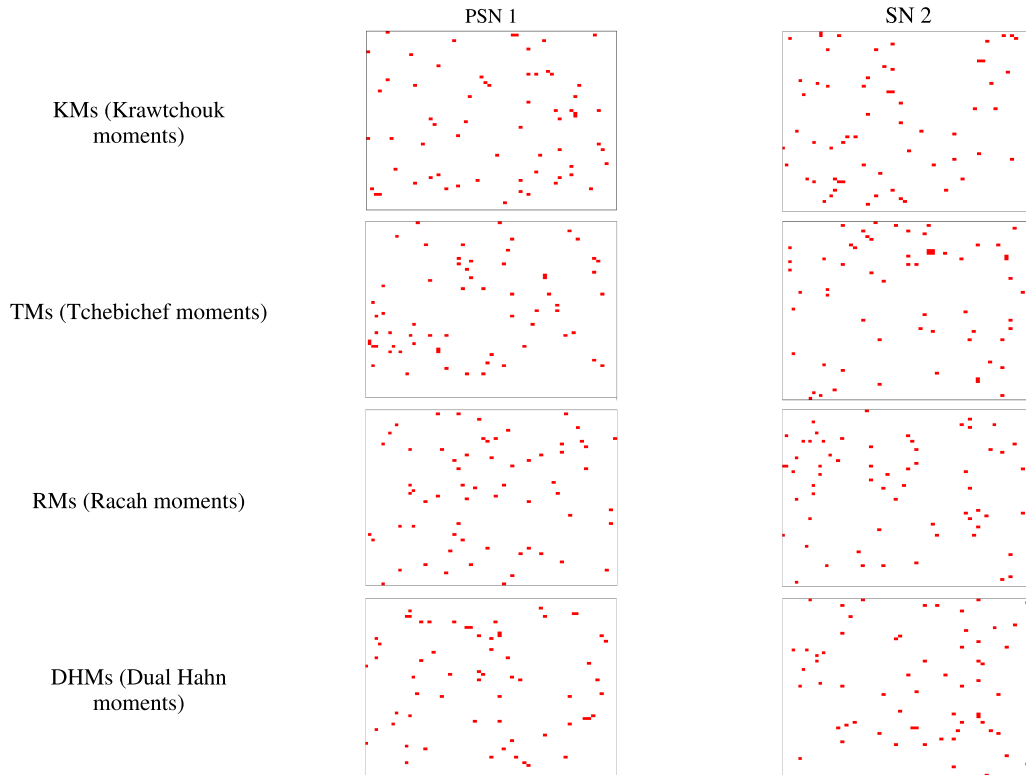
FIGURE 14. Distribution of the best embedding moments using Lena image under PSN 1 and SN 2 attacks.

TABLE 24. Imperceptibility indicators of embedding positions and strength optimization for Lena image.

	PSNR						UIQI					
	KMs	TMs	RMs	DHMs	DCT	DWT	KMs	TMs	RMs	DHMs	DCT	DWT
Sc 1	52.14	35.37	47.49	37.83	48.66	57.85	0.999	0.995	0.999	0.997	0.999	0.999
Sc 2	38.81	31.25	37.81	35.58	38.21	54.90	0.997	0.989	0.997	0.995	0.997	0.999
Sc 3	53.37	34.46	38.82	36.52	38.71	39.90	0.999	0.994	0.998	0.996	0.997	0.998
Sc 4	34.80	29.42	35.45	34.57	36.84	35.90	0.995	0.983	0.995	0.994	0.996	0.996
Sc 5	36.04	32.77	35.90	34.23	36.44	34.97	0.996	0.992	0.996	0.994	0.996	0.995
Sc 6	40.20	30.42	38.08	36.92	38.32	57.89	0.998	0.987	0.997	0.996	0.997	0.999
Sc 7	41.41	34.67	40.96	37.64	41.30	40.64	0.998	0.995	0.998	0.997	0.998	0.998
Sc 8	35.71	35.42	36.20	34.07	35.76	35.86	0.996	0.995	0.996	0.994	0.996	0.996
Sc 9	39.60	35.33	52.78	35.68	36.76	36.53	0.998	0.995	0.999	0.996	0.996	0.996
Sc 10	38.72	32.05	37.51	35.02	39.45	36.25	0.997	0.991	0.997	0.995	0.998	0.996
Sc 11	53.73	31.70	41.71	37.86	59.87	59.04	0.999	0.990	0.998	0.997	0.999	0.999
MEAN	42.23	32.98	40.24	35.99	40.94	44.52	0.997	0.991	0.997	0.996	0.997	0.997

but they are distributed all over the image bands in their frequency domain. We conclude that the use of an evolutionary approach in our proposed EWIMps method allows us to benefit at the same time from the advantages of the low, high, and middle-frequency bands obtaining the best compromise between imperceptibility and robustness requirements with the fittest individuals selected for the watermarking embedding.

3) OPTIMIZATION OF THE EMBEDDING POSITIONS AND THE EMBEDDING STRENGTH

This second set of the experimental study discusses the impact of optimizing the embedding strength along with the optimization process of embedding positions using our

TABLE 25. The optimized embedding strength using Lena image.

Scenario	Quantization step					
	KMs	TMs	RMs	DHMs	DCT	DWT
Sc 1	75	109	32	73	26	11
Sc 2	329	445	106	110	102	15
Sc 3	74	337	98	102	86	83
Sc 4	505	277	126	116	110	121
Sc 5	506	435	127	127	125	126
Sc 6	279	329	106	91	107	10
Sc 7	287	506	75	78	73	74
Sc 8	510	302	125	122	122	127
Sc 9	339	171	15	115	109	121
Sc 10	372	461	94	115	109	121
Sc 11	76	473	73	15	9	9

EWIMps method on the watermarking performance. The selection of the quantization step (Δ) used in the dither

FIGURE 15. Watermarked images in Sc 3 in the case of the embedding positions and strength optimization for different transformations.

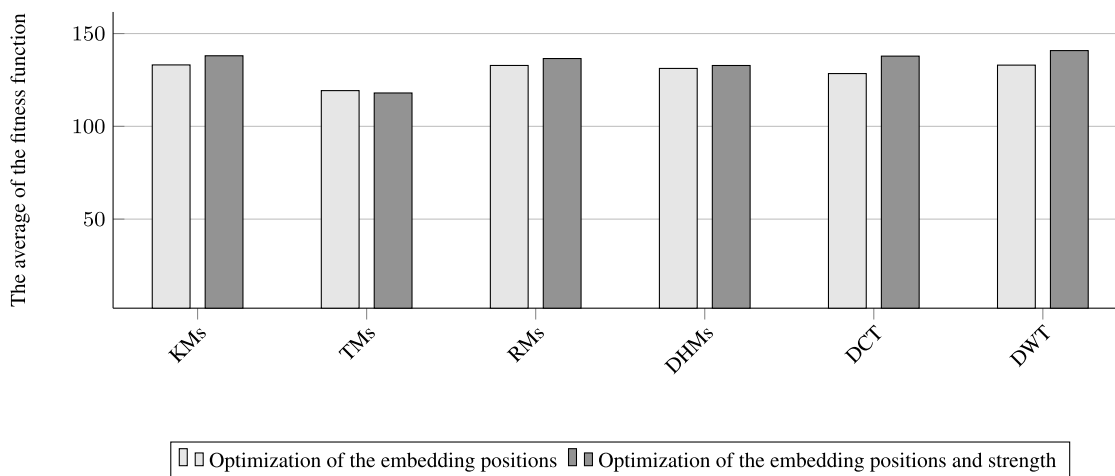Optimization of the embedding positions   Optimization of the embedding positions and strength

FIGURE 16. The average fitness function with image transformations in the case of the optimization of the embedding positions, and the optimization of the embedding positions and embedding strength.

TABLE 26. Robustness indicators against attacks of embedding positions and strength optimization in Lena image.

		NC						BER					
		KMs	TMs	RMs	DHMs	DCT	DWT	KMs	TMs	RMs	DHMs	DCT	DWT
Sc 1	PSN 1	1	0.939	1	1	1	1	0	0.062	0	0	0	0
Sc 2	PSN 2	1	0.857	1	1	1	1	0	0.140	0	0	0	0
Sc 3	PN	1	0.984	1	1	1	1	0	0.015	0	0	0	0
Sc 4	SN 1	0.968	0.830	0.984	0.970	0.968	0.952	0.031	0.171	0.015	0.031	0.031	0.046
Sc 5	SN 2	0.984	0.830	1	1	1	1	0.015	0.071	0	0	0	0
Sc 6	RT	0.984	0.889	1	1	1	0.984	0.015	0.109	0	0	0	0.015
Sc 7	GN 1	1	0.820	1	1	1	1	0	0.203	0	0	0	0
Sc 8	GN 2	0.920	0.757	0.937	0.956	0.952	0.937	0.078	0.250	0.062	0.046	0.046	0.062
Sc 9	JPEG 5	0.747	0.727	0.709	0.742	0.788	0.736	0.265	0.281	0.343	0.250	0.218	0.281
Sc 10	JPEG 50	0.939	0.806	0.968	0.984	0.952	0.984	0.062	0.203	0.031	0.015	0.046	0.015
Sc 11	JPEG 100	1	0.920	1	1	1	1	0	0.078	0	0	0	0
MEAN		0.958	0.85	0.963	0.968	0.969	0.963	0.042	0.143	0.041	0.031	0.031	0.038

modulation operation based on the watermarking techniques is generally based on the trial and error method. However, intending to meet the imperceptibility criteria, it is extremely important to choose the appropriate (Δ) value since it controls
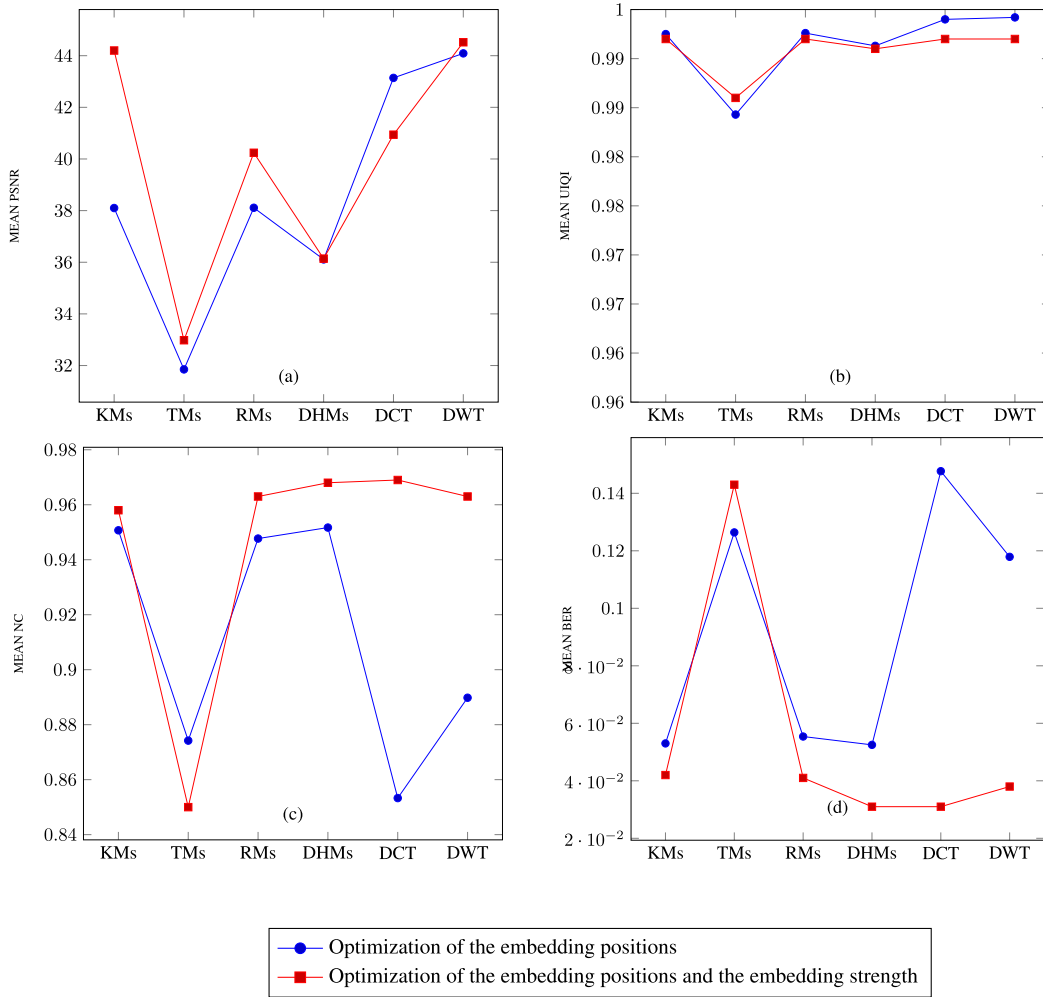
FIGURE 17. The mean performance in the case of the optimization of the embedding positions, and the optimization of the embedding positions and strength: (a) MEAN PSNR, (b) MEAN UIQI, (c) MEAN NC, (d) MEAN BER.

how much information is embedded and, as a result, affects the quality of the watermarked image [19]. Therefore, this embedding strength is combined with the embedding positions to define each individual in the population pool. Given the similar behavior of Lena, Pepper, and House images as demonstrated in the previous subsection, the remaining experimental results will be only shown for Lena image.

- **Imperceptibility analysis**

The results presented in Table 24 indicate the imperceptibility indicators values when the embedding positions and the embedding strength are optimized for the 11 scenarios, while Figure 15 shows the watermarked Lena image resulting in the third scenario for different image transformations. From the shown results, we can deduce that adding the quantization step to the optimization procedure increases the quality of the watermarked Lena images. In fact, comparing the average PSNR values obtained in Table 15 where only the embedding positions are optimized, with those obtained in Table 24 where the embedding positions and strength are both optimized, we can see that the mean PSNR values have increased

TABLE 27. Performances based on the fitness function in the case of the embedding positions and strength optimization.

		Fitness Function					
		KMs	TMs	RMs	DHMs	DCT	DWT
Sc 1	PSN 1	+		+	+	+	+
Sc 2	PSN 2	+		+	+	+	+
Sc 3	PN	+		+	+	+	+
Sc 4	SN 1			+		+	
Sc 5	SN 2	+		+	+	+	+
Sc 6	RT	+		+	+	+	+
Sc 7	GN 1	+		+	+	+	+
Sc 8	GN2						
Sc 9	JPEG 5						
Sc 10	JPEG 50			+		+	+
Sc 11	JPEG 100	+		+	+	+	+
SUM		7	0	9	7	9	8

from 38.10 to 42.23 dB, from 31.85 to 32.98 dB, and from 38.11 to 40.24 dB in the case of Krawtchouk, Tchebichef and Racah moments respectively.

- **Robustness analysis**

A deep inspection of the NC and BER values presented in Table 26 and at the extracted watermarks shown in

TABLE 28. Extracted watermarks from Lena watermarked image in the case of the embedding positions and strength optimization.

Attacks	KMs	TMs	DHMs	RMs	DCT	DWT
PSN 1						
PSN 2						
PN						
SN 1						
SN 2						
RT						
GN 1						
GN 2						
JPEG 5						
JPEG 50						
JPEG 100						

Table 28, while the embedding positions and strength are both optimized under different attacks using adopted image transformations, demonstrates that optimizing the embedding strength (Δ) improves the robustness requirement of the

discrete transforms (DCT and DWT). The mean NC increases from 0.951 to 0.968, from 0.853 to 0.969, and from 0.889 to 0.963, while the mean BER is reduced from 0.052 to 0.031 (reduction of 40.38%), from 0.147 to 0.031 (reduction of 78.91%) and from 0.117 to 0.038 (reduction of 67.52%) for DHMs, DCT, and DWT respectively. We can conclude that including this second optimization parameter enhances the resulting imperceptibility and robustness of image moments and discrete transforms respectively. Table 25 indicates the best obtained embedding strength values for all scenarios and all image transformations leading to the highest performances, varying between $\Delta_{min} = 9$ and $\Delta_{max} = 510$. From all the above, we can point out two important conclusions:

- we achieved good robustness using image moments without necessarily affecting the quality of the watermarked image.

- we maintained a good level of imperceptibility using discrete transforms and obtained at the same time good resistance over an insecure network.

Thus, selecting the appropriate embedding coefficients along with optimum embedding strength using our EWIMps algorithm highly satisfies both the robustness and imperceptibility requirements.

- **Effect of image transformations on the fitness function in the case of embedding positions and strength optimization**

To properly assess the performance of image transformations according to fitness function criteria. Table 27 reports the best fitness function values where FF > 133.5 dB is calculated based on the mean value of imperceptibility (PSNR = 39.48 dB), and the mean value of robustness (NC = 0.94) of all image transformations using Lena image, when the embedding positions and strength are both optimized. Based on the obtained results, we can conclude that Racah moments maintain good performances among other moments. In addition, we can observe an increase in the performances of discrete transforms thanks to the adopted optimization process.

- **Optimization impact of the embedding positions and strength parameters on the performance indicators**

Figure 17 illustrates the obtained average values of imperceptibility metrics (PSNR and UIQI) and robustness metrics (NC and BER) in the case of the embedding location optimization, and the embedding location and strength optimization, where each metric is illustrated according to the used image transformations. From this figure, we can see that optimizing the embedding positions and the embedding strength using our EWIMps method has generally increased the imperceptibility performance evolution and allowed an important reduction of the bit error rate ensuring high robustness.

- **Impact of the embedding parameters optimization on the fitness function**

Figure 16 shows the average of all best fitness function values resulting under several attacks in the first and second aforementioned optimization parts for each image transformation. From this figure, we can conclude that adding the embedding
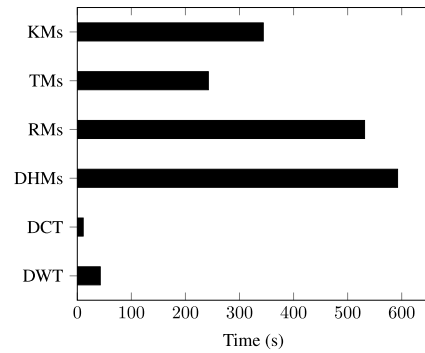

FIGURE 18. Computational cost for different transformation types.

strength parameter to the optimization process increases the accuracy for KMs, RMs, DHMs, DCT, and DWT which proves the efficiency of our EWIMps method.

- **Computational cost effect**

To analyze the computational cost of the proposed system, we performed a comparative study of the computational time required by the image transformations for embedding and extracting the watermark using the evolutionary algorithm under the same noise (poisson). The obtained results in seconds (s) are depicted in Figure 18. We note that discrete transforms have a lower computational time than discrete moments requiring more complex mathematical operations, resulting in relatively higher computational time. Consequently, this factor needs to be investigated in future works.

VI. CONCLUSION

The proposed paper presents a new blind image watermarking method based on an automatic selection of the appropriate embedding moments and strength, baptized EWIMps. Our approach ensures a good trade-off between the imperceptibility with the high quality of the watermarked image and good robustness against different attacks. Discovering the positions where hidden data will be inserted and the embedding strength is a crucial issue that can be viewed as an optimization challenge since these parameters influence the behavior of the blind watermarking algorithm. Contrarily to the unstructured manual selection methods presented in the literature, the proposed automatic search method is based on an evolutionary algorithm with a specific encoding strategy and adapted evolutionary operators. For this, the embedding parameters are coded by a simple and compact chromosome, evolved through adapted selection, crossover, and mutation operators to keep the fittest solutions over the generations of our evolutionary process.

Results of the evolutionary parameters effect firstly show that one fixed cutting point of the crossover operator in the middle of each gene of the chromosome is the best choice since it allows more exchange of the building blocks of the parent chromosomes improving hence the final performance of the offspring. The proposed mutation operator preserves

a good compromise between diversity and the behavioral link between parents and offspring. Krawtchouk, Tchebichef, Dual Hahn, and Racah moments are used to transform the original image before using the dither modulation as an embedding technique to generate the watermarked image. Our blind watermarking method EWIMps is then evaluated in terms of the imperceptibility and robustness against image processing attacks. To validate the efficiency of the proposed method, a comparison study was performed with two discrete transforms (DCT and DWT) applying the same evolutionary process and watermarking techniques. The first experiments explore the results of the watermarking performances using the embedding positions optimization. In fact, optimizing the moments coefficients used for the embedding process shows a great improvement in the fitness function values over generations. For instance, using KMs under PN attack on House image produces a fitness function varying from 121 in the first generation to 138.97 in the last one. Using Lena reference image, the proposed EWIMps method gives an imperceptibility performance (Mean PSNR) of 38.1, 31.85, 38.11, and 36.11 dB, and robustness (Mean NC) values of 0.95, 0.874, 0.947, and 0.951 for KMs, TMs, RMs, and DHMs respectively. For DCT and DWT, the imperceptibility performances are 43.14 and 44.09 dB, and the robustness performances are 0.853 and 0.889 respectively. Therefore, discrete moments perform well in terms of robustness while discrete transforms in terms of imperceptibility. Moreover, our testing results demonstrated that RMs, among all other image transformations, produce more accurate and reliable watermarking performance with high quality of the watermarked image as well as the recovered watermark under different attack conditions. Furthermore, it appears that the optimization of the embedding strength as an additional parameter significantly improved the entire watermarking process. In fact, the performance of imperceptibility was additionally enhanced to 42.23, 32.98, 40.24, and 35.99 dB for KMs, TMs, RMs, DHMs, and the robustness performance to 0.969 and 0.963 for DCT and DWT respectively, with the same aforementioned image. According to the adopted fitness function performance, it is also noticeable that, with the optimization of this additional parameter, DCT and DWT performances have been improved while RMs preserve their superiority compared to other moments. Consequently, obtained results reveal that the proposed automatic selection method of the best embedding parameters recorded an excellent performance simultaneously in terms of robustness and imperceptibility. It is worth noting that the EWIMps method is applicable to different kinds of gray-level original images and any other moments family.

The present work offers new perspectives to investigate the proposed method in the emerging Internet of Medical Things (IoMT) applications in order to resolve patient privacy protection issues, taking into account our good performances obtained in terms of the robustness of the extracted watermark that could preserve sensitive patient health data.

REFERENCES

[1] O. N. A. AL-Allaf, "Particle swarm optimization algorithm vs. Genetic algorithm for image watermarking based discrete wavelet transform," *Int. J. Comput. Inf. Eng.*, vol. 11, no. 9, p. 7, 2017.

[2] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[3] Y. Qianli and C. Yanhong, "A digital image watermarking algorithm based on discrete wavelet transform and discrete cosine transform," in *Proc. Int. Symp. Inf. Technol. Med. Educ.*, Aug. 2012, pp. 1102–1105.

[4] M. Alghoniemy and A. H. Tewfik, "Image watermarking by moment invariants," in *Proc. Int. Conf. Image Process.*, vol. 2. Vancouver, BC, Canada: IEEE, 2000, pp. 73–76.

[5] C.-S. Shieh, H.-C. Huang, F.-H. Wang, and J.-S. Pan, "Genetic watermarking based on transform-domain techniques," *Pattern Recognit.*, vol. 37, no. 3, pp. 555–565, Mar. 2004.

[6] F. Ernawan and M. N. Kabir, "An improved watermarking technique for copyright protection based on tchebichef moments," *IEEE Access*, vol. 7, pp. 151985–152003, 2019.

[7] A. Bahrushin, G. Bahrushina, R. Bazhenov, K. Kim, and R. Tsoy, "Robust image watermarking technique based on genetic algorithm optimization and even odd modulation," in *Proc. 9th Int. Conf. Discrete Optim. Oper. Res. Sci. School (DOOR)*, Dec. 2016, pp. 415–427.

[8] E. D. Tsougenis, G. A. Papakostas, D. E. Koulouriotis, and V. D. Tourassis, "Performance evaluation of moment-based watermarking methods: A review," *J. Syst. Softw.*, vol. 85, no. 8, pp. 1864–1884, Aug. 2012.

[9] Y. Xin, S. Liao, and M. Pawlak, "Circularly orthogonal moments for geometrically robust image watermarking," *Pattern Recognit.*, vol. 40, no. 12, pp. 3740–3752, Dec. 2007.

[10] N. Singhal, Y.-Y. Lee, C.-S. Kim, and S.-U. Lee, "Robust image watermarking using local Zernike moments," *J. Visual Commun. Image Represent.*, vol. 20, no. 6, pp. 408–419, Aug. 2009.

[11] J.-G. Sun and W. He, "RST invarian watermarking scheme based on SIFT feature and Pseudo-Zernike moment," in *Proc. 2nd Int. Symp. Comput. Intell. Design*. Changsha, China: IEEE, Dec. 2009, pp. 10–13.

[12] C. Singh and S. K. Ranade, "Image adaptive and high-capacity watermarking system using accurate Zernike moments," *IET Image Process.*, vol. 8, no. 7, pp. 373–382, Jul. 2014.

[13] I. A. Ismail, M. A. Shuman, K. M. Hosny, and H. M. Abdel Salam, "Invariant image watermarking using accurate Zernike moments," *J. Comput. Sci.*, vol. 6, no. 1, pp. 52–59, Jan. 2010.

[14] X.-Y. Wang, Y.-P. Yang, and H.-Y. Yang, "Invariant image watermarking using multi-scale Harris detector and wavelet moments," *Comput. Electr. Eng.*, vol. 36, no. 1, pp. 31–44, Jan. 2010.

[15] P.-P. Niu, P. Wang, Y.-N. Liu, H.-Y. Yang, and X.-Y. Wang, "Invariant color image watermarking approach using quaternion radial harmonic Fourier moments," *Multimedia Tools Appl.*, vol. 75, no. 13, pp. 7655–7679, Jul. 2016.

[16] K. M. Hosny and M. M. Darwish, "Robust color image watermarking using invariant quaternion legendre-Fourier moments," *Multimedia Tools Appl.*, vol. 77, no. 19, pp. 24727–24750, Oct. 2018.

[17] C. Deng, X. Gao, X. Li, and D. Tao, "A local Tchebichef moments-based robust image watermarking," *Signal Process.*, vol. 89, no. 8, pp. 1531–1539, Aug. 2009.

[18] E. D. Tsougenis, G. A. Papakostas, and D. E. Koulouriotis, "Image watermarking via separable moments," *Multimedia Tools Appl.*, vol. 74, no. 11, pp. 3985–4012, Jun. 2015.

[19] G. A. Papakostas, E. D. Tsougenis, and D. E. Koulouriotis, "Moment-based local image watermarking via genetic optimization," *Appl. Math. Comput.*, vol. 227, pp. 222–236, Jan. 2014.

[20] G. A. Papakostas, E. D. Tsougenis, and D. E. Koulouriotis, "Fuzzy knowledge-based adaptive image watermarking by the method of moments," *Complex Intell. Syst.*, vol. 2, no. 3, pp. 205–220, Oct. 2016.

[21] M. Yamni, H. Karmouni, M. Sayyouri, and H. Qjidaa, "Robust zero-watermarking scheme based on novel quaternion radial fractional charlier moments," *Multimedia Tools Appl.*, vol. 80, no. 14, pp. 21679–21708, Jun. 2021.

[22] C. Agarwal, A. Mishra, and A. Sharma, "Gray-scale image watermarking using GA-BPN hybrid network," *J. Vis. Commun. Image Represent.*, vol. 24, no. 7, pp. 1135–1146, Oct. 2013.

[23] D. Câmara, "Evolution and evolutionary algorithms," in *Bio-Inspired Networking*. Cham, Switzerland: Springer, 2015, pp. 1–30.

[24] C. Gondro and B. Kinghorn, "Application of evolutionary algorithms to solve complex problems in quantitative genetics and bioinformatics," Centre GeneticImprovement Livestock, Univ. Guelph, 2008.

[25] B. He, J. Cui, B. Xiao, and Y. Peng, "Image analysis using modified exponent-Fourier moments," *EURASIP J. Image Video Process.*, vol. 2019, no. 1, p. 72, Dec. 2019.

[26] C. Wang, Q. Hao, B. Ma, X. Wu, J. Li, Z. Xia, and H. Gao, "Octonion continuous orthogonal moments and their applications in color stereoscopic image reconstruction and zero-watermarking," *Eng. Appl. Artif. Intell.*, vol. 106, Nov. 2021, Art. no. 104450.

[27] S. Golabi, M. S. Helfroush, and H. Danyali, "Non-unit mapped radial moments platform for robust, geometric invariant image watermarking and reversible data hiding," *Inf. Sci.*, vol. 447, pp. 104–116, Jun. 2018.

[28] N. Singhal, Y.-Y. Lee, C.-S. Kim, and S.-U. Lee, "Robust image watermarking based on local Zernike moments," in *Proc. IEEE 9th Workshop Multimedia Signal Process.* Crete, Greece: IEEE, 2007, pp. 401–404.

[29] X.-Y. Wang, X. Shen, J.-L. Tian, P.-P. Niu, and H.-Y. Yang, "Statistical image watermark decoder based on local frequency-domain exponent-Fourier moments modeling," *Multimedia Tools Appl.*, vol. 80, no. 18, pp. 27717–27755, Jul. 2021.

[30] G. Gao and G. Jiang, "Bessel-Fourier moment-based robust image zero-watermarking," *Multimedia Tools Appl.*, vol. 74, no. 3, pp. 841–858, Feb. 2015.

[31] B. Ma, L. Chang, C. Wang, J. Li, X. Wang, and Y.-Q. Shi, "Robust image watermarking using invariant accurate polar harmonic Fourier moments and chaotic mapping," *Signal Process.*, vol. 172, Jul. 2020, Art. no. 107544.

[32] C. Wang, Q. Zhang, B. Ma, Z. Xia, J. Li, T. Luo, and Q. Li, "Light-field image watermarking based on geranion polar harmonic Fourier moments," *Eng. Appl. Artif. Intell.*, vol. 113, Aug. 2022, Art. no. 104970.

[33] Z. Xia, X. Wang, M. Wang, S. Unar, C. Wang, Y. Liu, and X. Li, "Geometrically invariant color medical image null-watermarking based on precise quaternion polar harmonic Fourier moments," *IEEE Access*, vol. 7, pp. 122544–122560, 2019.

[34] Z. Xia, X. Wang, X. Li, C. Wang, S. Unar, M. Wang, and T. Zhao, "Efficient copyright protection for three CT images based on quaternion polar harmonic Fourier moments," *Signal Process.*, vol. 164, pp. 368–379, Nov. 2019.

[35] Z. Xia, X. Wang, C. Wang, B. Ma, M. Wang, and Y.-Q. Shi, "Local quaternion polar harmonic Fourier moments-based multiple zero-watermarking scheme for color medical images," *Knowl.-Based Syst.*, vol. 216, Mar. 2021, Art. no. 106568.

[36] X.-Y. Wang, P.-P. Niu, H.-Y. Yang, C.-P. Wang, and A.-L. Wang, "A new robust color image watermarking using local quaternion exponent moments," *Inf. Sci.*, vol. 277, pp. 731–754, Sep. 2014.

[37] K. M. Hosny and M. M. Darwish, "Resilient color image watermarking using accurate quaternion radial substituted Chebyshev moments," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 15, no. 2, pp. 1–25, May 2019.

[38] X.-Y. Wang, L. Wang, J.-L. Tian, P.-P. Niu, and H.-Y. Yang, "Color image zero-watermarking using accurate quaternion generalized orthogonal Fourier–Mellin moments," *J. Math. Imag. Vis.*, vol. 63, no. 6, pp. 708–734, Jul. 2021.

[39] Z. Xia, X. Wang, W. Zhou, R. Li, C. Wang, and C. Zhang, "Color medical image lossless watermarking using chaotic system and accurate quaternion polar harmonic transforms," *Signal Process.*, vol. 157, pp. 108–118, Apr. 2019.

[40] H.-Y. Yang, X.-Y. Wang, P.-P. Niu, and A.-L. Wang, "Robust color image watermarking using geometric invariant quaternion polar harmonic transform," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 11, no. 3, pp. 1–26, Feb. 2015.

[41] X.-Y. Wang, Y.-N. Liu, M.-M. Han, and H.-Y. Yang, "Local quaternion PHT based robust color image watermarking algorithm," *J. Vis. Commun. Image Represent.*, vol. 38, pp. 678–694, Jul. 2016.

[42] C.-P. Wang, X.-Y. Wang, X.-J. Chen, and C. Zhang, "Robust zero-watermarking algorithm based on polar complex exponential transform and logistic mapping," *Multimedia Tools Appl.*, vol. 76, no. 24, pp. 26355–26376, Dec. 2017.

[43] H.-Y. Yang, S.-R. Qi, P.-P. Niu, and X.-Y. Wang, "Color image zero-watermarking based on fast quaternion generic polar complex exponential transform," *Signal Process., Image Commun.*, vol. 82, Mar. 2020, Art. no. 115747.

[44] Z. Xia, X. Wang, C. Wang, B. Ma, H. Zhang, and Q. Li, "Novel quaternion polar complex exponential transform and its application in color image zero-watermarking," *Digit. Signal Process.*, vol. 116, Sep. 2021, Art. no. 103130.

[45] B. Ma, L. Chang, C. Wang, J. Li, G. Li, Z. Xia, and X. Wang, "Double medical images zero-watermarking algorithm based on the chaotic system and ternary accurate polar complex exponential transform," *J. Math. Imag. Vis.*, vol. 63, no. 9, pp. 1160–1178, Nov. 2021.

[46] C. Wang, X. Wang, Z. Xia, and C. Zhang, "Ternary radial harmonic Fourier moments based robust stereo image zero-watermarking algorithm," *Inf. Sci.*, vol. 470, pp. 109–120, Jan. 2019.

[47] Z. Xia, X. Wang, C. Wang, C. Wang, B. Ma, Q. Li, M. Wang, and T. Zhao, "A robust zero-watermarking algorithm for lossless copyright protection of medical images," *Int. J. Speech Technol.*, vol. 52, no. 1, pp. 607–621, Jan. 2022.

[48] K. M. Hosny and M. M. Darwish, "Robust color image watermarking using multiple fractional-order moments and chaotic map," *Multimedia Tools Appl.*, vol. 81, no. 17, pp. 24347–24375, Jul. 2022.

[49] M. Yamni, A. Daoui, O. El Ogri, H. Karmouni, M. Sayyouri, H. Qjidaa, and J. Flusser, "Fractional charlier moments for image reconstruction and image watermarking," *Signal Process.*, vol. 171, Jun. 2020, Art. no. 107509.

[50] M. Yamni, H. Karmouni, M. Sayyouri, and H. Qjidaa, "Image watermarking using separable fractional moments of Charlier–Meixner," *J. Franklin Inst.*, vol. 358, no. 4, pp. 2535–2560, Mar. 2021.

[51] H. Zhang, H. Shu, G. Coatrieux, J. Zhu, Q. M. J. Wu, Y. Zhang, H. Zhu, and L. Luo, "Affine legendre moment invariants for image watermarking robust to geometric distortions," *IEEE Trans. Image Process.*, vol. 20, no. 8, pp. 2189–2199, Aug. 2011.

[52] K. M. Hosny and M. M. Darwish, "New geometrically invariant multiple zero-watermarking algorithm for color medical images," *Biomed. Signal Process. Control*, vol. 70, Sep. 2021, Art. no. 103007.

[53] S. M. Elshoura and D. B. Megherbi, "A secure high capacity full-gray-scale-level multi-image information hiding and secret image authentication scheme via Tchebichef moments," *Signal Process., Image Commun.*, vol. 28, no. 5, pp. 531–552, May 2013.

[54] S. M. Elshoura and D. B. Megherbi, "Analysis of noise sensitivity of Tchebichef and Zernike moments with application to image watermarking," *J. Vis. Commun. Image Represent.*, vol. 24, no. 5, pp. 567–578, Jul. 2013.

[55] A. Bastani and F. Ahouz, "High capacity and secure watermarking for medical images using Tchebichef moments," *Radioengineering*, vol. 29, no. 4, pp. 636–643, Dec. 2020.

[56] S. Ben Jabra and E. Zagrouba, "Robust anaglyph 3D video watermarking based on cyan mosaic generation and DCT insertion in Krawtchouk moments," *Vis. Comput.*, vol. 38, no. 11, pp. 3611–3625, Nov. 2022.

[57] L. Zhang, W. W. Xiao, and Z. Ji, "Local affine transform invariant image watermarking by Krawtchouk moment invariants," *IET Inf. Secur.*, vol. 1, no. 3, pp. 97–105, Apr. 2007.

[58] A. Daoui, H. Karmouni, M. Sayyouri, and H. Qjidaa, "Robust 2D and 3D images zero–watermarking using dual Hahn moment invariants and sine cosine algorithm," *Multimedia Tools Appl.*, vol. 81, no. 18, pp. 25581–25611, Jul. 2022.

[59] A. Daoui, M. Yamni, H. Karmouni, M. Sayyouri, H. Qjidaa, M. Ahmad, and A. A. Abd El-Latif, "Color stereo image encryption and local zero-watermarking schemes using octonion Hahn moments and modified Henon map," *J. King Saud Univ. -Comput. Inf. Sci.*, vol. 34, no. 10, pp. 8927–8954, Nov. 2022.

[60] B. Xiao, J. Luo, X. Bi, W. Li, and B. Chen, "Fractional discrete Tchebyshev moments and their applications in image encryption and watermarking," *Inf. Sci.*, vol. 516, pp. 545–559, Apr. 2020.

[61] X. Liu, G. Han, J. Wu, Z. Shao, G. Coatrieux, and H. Shu, "Fractional Krawtchouk transform with an application to image watermarking," *IEEE Trans. Signal Process.*, vol. 65, no. 7, pp. 1894–1908, Apr. 2017.

[62] S. B. B. Ahmadi, G. Zhang, M. Rabbani, L. Boukela, and H. Jelodar, "An intelligent and blind dual color image watermarking for authentication and copyright protection," *Int. J. Speech Technol.*, vol. 51, no. 3, pp. 1701–1732, Mar. 2021.

[63] I. Batioua, R. Benouini, and K. Zenkouar, "Image recognition using new set of separable three-dimensional discrete orthogonal moment invariants," *Multimedia Tools Appl.*, vol. 79, nos. 19–20, pp. 13217–13245, May 2020.

[64] R. Benouini, I. Batioua, K. Zenkouar, S. Najah, and H. Qjidaa, "Efficient 3D object classification by using direct Krawtchouk moment invariants," *Multimedia Tools Appl.*, vol. 77, no. 20, pp. 27517–27542, Oct. 2018.

[65] R. Benouini, I. Batioua, I. Elouariachi, K. Zenkouar, and A. Zarghili, "Explicit separable two dimensional moment invariants for object recognition," *Proc. Comput. Sci.*, vol. 148, pp. 409–417, 2019.

[66] R. Mukundan, S. H. Ong, and P. A. Lee, "Image analysis by Tchebichef moments," *IEEE Trans. Image Process*, vol. 10, no. 9, pp. 1357–1364, Sep. 2001.

[67] H. Zhu, H. Shu, J. Liang, L. Luo, and J.-L. Coatrieux, "Image analysis by discrete orthogonal Racah moments," *Signal Process.*, vol. 87, no. 4, pp. 687–708, Apr. 2007.

[68] P.-T. Yap, R. Paramesran, and S.-H. Ong, "Image analysis by Krawtchouk moments," *IEEE Trans. Image Process.*, vol. 12, no. 11, pp. 1367–1377, Nov. 2003.

[69] H. Zhu, H. Shu, J. Zhou, L. Luo, and J. L. Coatrieux, "Image analysis by discrete orthogonal dual Hahn moments," *Pattern Recognit. Lett.*, vol. 28, no. 13, pp. 1688–1704, Oct. 2007.

[70] I. Batioua, R. Benouini, K. Zenkouar, and H. E. Fadili, "Image analysis using new set of separable two-dimensional discrete orthogonal moments based on Racah polynomials," *EURASIP J. Image Video Process.*, vol. 2017, no. 1, p. 20, Dec. 2017.

[71] T. Naheed, I. Usman, T. M. Khan, A. H. Dar, and M. F. Shafique, "Intelligent reversible watermarking technique in medical images using GA and PSO," *Optik*, vol. 125, no. 11, pp. 2515–2525, Jun. 2014.

[72] A. Hassanat, K. Almohammadi, E. Alkafaween, E. Abunawas, A. Hammouri, and V. B. S. Prasath, "Choosing mutation and crossover ratios for genetic algorithms—A review with a new dynamic approach," *Information*, vol. 10, no. 12, p. 390, Dec. 2019.

[73] X. Zhou, C. Cao, J. Ma, and L. Wang, "Adaptive digital watermarking scheme based on support vector machines and optimized genetic algorithm," *Math. Problems Eng.*, vol. 2018, pp. 1–9, 2018.

[74] X. Yao, "Global optimisation by evolutionary algorithms," in *Proc. 2nd Int. Symp. Parallel Algorithms/Architecture Synth.* London, U.K.: IEEE Computer Society Press, Dec. 1997, pp. 282–291.

[75] M. Marzouq, H. El Fadili, K. Zenkouar, Z. Lakhliai, and M. Amouzg, "Short term solar irradiance forecasting via a novel evolutionary multimodel framework and performance assessment for sites with no solar irradiance data," *Renew. Energy*, vol. 157, pp. 214–231, Sep. 2020.

[76] V. Álvarez, J. A. Armario, M. D. Frau, F. Gudiel, M. B. Gäemes, E. Martín, and A. and Osuna, "Based robust blind digital watermarking," *Electron. Notes Discrete Math.*, vol. 68, pp. 149–154, Jul. 2018.

[77] Y. A. Y. Al-Najjar and D. D. C. Soong, "Comparison of image quality assessment: PSNR, HVS, SSIM, UIQI," *Int. J. Sci. Eng. Res.*, vol. 3, no. 8, pp. 1–5., 2012.

[78] Z. Wang and A. C. Bovik, "A universal image quality index," *IEEE Signal Process. Lett.*, vol. 9, no. 3, pp. 81–84, Mar. 2002.

MANAL MARZOUQ received the M.Sc. degree in industrial engineering, in 2015, and the Ph.D. degree in electrical engineering from the Sciences and Technologies Faculty, Sidi Mohammed Ben Abdallah University, Fez, Morocco, in 2021. Her current research interests include problem modeling, artificial intelligence, and machine learning.
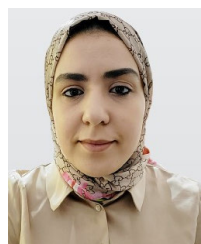
IMAD BATIOUA received the Ph.D. degree in intelligent systems and networks from the Faculty of Science and Technology, University of Sidi Mohammed Ben Abdellah, Fez, Morocco, in 2019. His research interests include pattern recognition and computer vision.
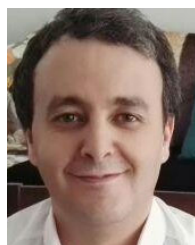
HAKIM EL FADILI was born in Azrou, Morocco, in 1976. He received the Ph.D. degree in image processing and machine intelligence from the Faculty of Science, Sidi Mohamed Ben Abdellah University, Fez, Morocco, in 2006. He was with the Moroccan Ministry of Justice as the Project Manager of Networking and Computer Science Projects, until 2010. He is currently a Professor with the Department of Electrical and Computer Engineering, National School of Applied Sciences (ENSA) of Sidi Mohamed Ben Abdellah University (USMBA), and he is affiliated to the Computer Science and Interdisciplinary Physics Laboratory (LIPI). His current research interests include machine intelligence models (neural networks and evolutionary algorithms) applied in pattern recognition and energy fields.

ZAKIA LAKHLIAI received the Ph.D. degree in physics from the University of Montpellier II, France, in 1987, and the Ph.D. degree from the University of Fez, Morocco, in 1996. She is currently a member of the Computer Science and Interdisciplinary Physics Laboratory (LIPI), ENSF, and a Professor with the Superior School of Technology (ESTF), Sidi Mohammed Ben Abdallah University (USMBA), Fez, Morocco. Her current research interests include signal and image processing and the indexation of old manuscripts.

CHAIMAE CHEKIRA received the degree in telecommunications and network engineering from the National School of Applied Sciences of Fez, in 2014. She is currently pursuing the Ph.D. degree with the Computer Science and Interdisciplinary Physics Laboratory (LIPI), Sidi Mohamed Ben Abdellah University, Fez. She is also an Engineer in networking and computer science with the Higher Education Ministry. Her research interests include image processing, evolutionary algorithms, and digital security.

KHALID ZENKOUAR was born in Meknes, Morocco, in 1971. He received the D.U.T. degree in mechanic and computer-integrated manufacturing from the High School of Technology, Fez, in 1993, the Gradate degree from the Faculty of Science, Sidi Mohamed Ben Abdellah University, Fez, and the D.E.S.A. degree in automatic and system analysis, in 2000. He is currently a Full Professor in image analysis and computer science with FST of Fez, Sidi Mohamed Ben Abdellah University.

• • •