IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 27, 2021, accepted June 10, 2021, date of publication June 22, 2021, date of current version July 1, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3091614

New Color Image Zero-Watermarking Using Orthogonal Multi-Channel Fractional-Order Legendre-Fourier Moments

KHALID M. HOSNY[1], **(Member, IEEE), MOHAMED M. DARWISH**[2], **AND MOSTAFA M. FOUDA**[3], **(Senior Member, IEEE)**

[1]Department of Information Technology, Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Egypt
[2]Department of Computer Science, Faculty of Computers and Information, Assiut University, Assiut 71516, Egypt
[3]Department of Electrical and Computer Engineering, Idaho State University, Pocatello, ID 83209, USA

Corresponding author: Khalid M. Hosny (k_hosny@yahoo.com)

ABSTRACT Zero-watermarking methods provide promising solutions and impressive performance for copyright protection of images without changing the original images. In this paper, a novel zero-watermarking method for color images is envisioned. Our envisioned approach is based on multi-channel orthogonal Legendre Fourier moments of fractional orders, referred to as MFrLFMs. In this method, a highly precise Gaussian integration method is utilized to calculate MFrLFMs. Then, based on the selected accurate MFrLFMs moments, a zero-watermark is constructed. Due to their accuracy, geometric invariances, and numerical stability, the proposed MFrLFMs-based zero-watermarking method shows excellent resistance against various attacks. Performed experiments using the proposed watermarking method show the outperformance over existing watermarking algorithms.

INDEX TERMS Color images, zero-watermarking, orthogonal moments of fractional orders, attacks.

I. INTRODUCTION

Fast advancements of communication technologies increased the number of transmitted digital images. Image content protection and preserving the intellectual rights are challenging problems. Copyright protection of digital images is a vital security issue. Watermarking technology of digital images has been extensively studied and used as an emerged powerful copyright protection technologies and authentication of the content of digital images and software protection [1]–[4]. In general, the methods of digital watermarking can be classified into different ways [1], [5]: visible, invisible, blind, semi-blind, non-blind, Fragile, semi-fragile, and robust watermarking

In recent years, the well-known techniques for resolving the protection copyright of images are traditional technology for embedded watermarking [6], [7]. The main idea of traditional watermarking algorithms is to incorporate the watermark information to the base (original) image; once embedding the information of the watermark, the data extracted to enforce copyright protection [8]–[12]. However, these algorithms suffer from the limitations of degrading the base image quality and the contradiction between robustness and imperceptibility, which is always challenging for traditional watermarking methods. To overcome the limitations of these kinds of schemes, a zero-watermarking scheme, a kind of lossless watermarking technique, has been suggested in recent years to enhance the visual quality and protect the copyrights of digital multimedia content, particularly images [13]. According to zero-watermarking schemes' main idea, the watermark information does not embed within the original image. Instead, an essential verification of ownership (i.e., zero-watermark) is constructed based on the information watermark and the original image's vital features. Hence, the content of visual image quality has no degradation at all. On the other side of robust traditional watermarking, robust zero-watermarking can ultimately preserve the original image's excellent visual quality and have perfect imperceptibility. As the zero-watermarking algorithm can balance imperceptibility and robustness, it has become one of the digital watermarking research hotspots. According to the concepts of zero-watermarking and the image

The associate editor coordinating the review of this manuscript and approving it for publication was Mehul S. Raval.

feature construction, we can roughly classify the methods of zero-watermarking into three groups [13]:

(1) Features of spatial domain-based [14], [15],
(2) Features of frequency domain based [16]–[18],
(3) Moments based methods [19]–[21].

In the first one, the image features are obtained by directly employing the spatial domain features [14], [15]. However, the spatial-domain features are highly-sensitive to attacks (geometric & image processing), and no matter whether information of edge or texture is used. In the second group, the image features are generated by employing the frequency domain-features. However, the frequency domain features are suffering from the lack of scaling and rotation invariance, which led to poor performance [16]–[18]. In group (3), the image features are constructed using moments and moment invariants with helping properties of their invariance [19]–[21].

In [19], Gao *et al.* presented a new zero-watermarking scheme by employing the Bessel–Fourier moments (BFMs), which are robust to a myriad of security threats. However, these invariant methods-based watermarking are applied for gray-scale images. Since then, extensive research works for zero-watermarking emerged in the literature that utilized image moments as well as moment invariants. According to [19], Gao *et al.* [20] used the computed local phases of BFMs to present a robust zero-watermarking algorithm. Shao *et al.* [21] used Visual cryptography (V.C.) and invariance properties of quaternion moment to construct a zero-watermarking algorithm for color image data. The work in [22] introduced another zero-watermarking method targeting color images by employing geometric invariant quaternion exponent moments (QEMs). Later, researchers exploited polar complex exponential transforms (PCETs) and logistic maps to present an algorithm for zero-watermarking [23]. Additionally, ternary radial harmonic Fourier moments (TRHFMs) were used to design a zero-watermarking scheme specifically for stereo color images [24].

A different approach was adopted by Xia *et al.* [25] recently where they considered quaternion polar harmonic transforms (QPHTs) coupled with a chaotic system to devise a zero-watermarking algorithm to protect color medical images. Xia *et al.* [26] proposed a null watermarking medical image algorithm based on geometrically invariant quaternion polar harmonic Fourier moments (QPHFM). Again, based on QPHFM, the work in [27] realized the protection of three C.T. images' copyright. Kang *et al.* [28] used chaotic compound maps and polar harmonic transforms (PHTs) in zero-watermarking to protect the color images. Yang *et al.* [29] combine asymmetric tent maps, and fast quaternion generic polar complex exponential transforms (FQGPCETs) in a robust zero-watermarking method targeting color image contents.

Although extensive research work dedicated toward zero-watermarking were carried out, most existing methods encounter limitations and challenging problems. Most existing zero-watermarking algorithms can only resist common image processing attacks such as noise, filtering, JPEG compression and so forth effectively and cannot resist geometric attacks; however, these algorithms show less resistance against geometric operations (e.g., translation, rotation, scaling, and so forth). The combination of these geometric attacks with standard signal processing attacks increases the challenges.

In most of these methods, the traditional computing method is used to compute quaternion moments in Cartesian coordinates. Two types of errors are generated during the computation process: numerical integration errors and geometric errors. The first error is a result of the numerical approximation of the continuous double integrals to double summation, while the second is a result of square-to-circle mapping of image representation. These errors introduce numerical instabilities and increase calculation complexity, affecting the moment computation and the robustness of the quaternion moments-based zero-watermarking scheme. Particularly for the big moment orders, researchers observed numerical errors resulting in unstable performance issues. As a consequence, the aforementioned methods for facilitating the zero-image watermarking are rather constrained due to their heavy dependence on orthogonal moments of integer-orders. Furthermore, based on the fractional polynomial utilization in the orthogonal moments, recent studies verified that polynomials with fractional orders exhibit a superior performance in terms of their capability of representing images in contrast with their integer order counterparts [30]–[35].

Based on the above analysis, we can summarize some issues in the existing zero-watermarking methods as follows:

(1) Some methods have weak resistance to geometric distortion.
(2) Most existing methods don't address the equalization of zero-watermark.
(3) Some zero watermarking methods are implemented based on orthogonal moments of integer order.
(4) Most existing methods are used the direct computation of quaternion moments which lead to the common two errors, numerical integration and geometric errors. Therefore, these methods are inaccurate and numerically unstable especially with the high-order moments, which are more sensitive against attacks. The larger size of watermark image requires the larger moments' order, and lead to less these methods' performance.
(5) Most existing methods are used inaccurate computation method of moments for extraction the features of host images.

These issues have a significant impact on the time computation, equalization, and robustness of the moments-based zero watermarking methods.

These challenging problems motivate the authors to propose a new robust zero-watermarking method. The authors utilized the novel highly accurate MFrLFMs [31], which have excellent geometric invariances with a significant scrambling transform. The scrambling of the binary watermark image is performed using the generalized Arnold transform for removing the spatial relationships between the pixels of the watermark image and for enhancing the security and the equalization. This zero-watermarking approach comprises four main phases. First, the accurate MFrLFMs are computed for the original color image using Gaussian numerical and exact for radial and angular kernels, respectively. Second, we choose the most significant MFrLFM moments to build a robust and accurate moment feature for representing the host image. Third, we binarized the selected features. Fourth, we perform the bitwise XOR using the permuted binary watermark digits and the binarized image features to formulate the zero-watermark image. The introduced method was found to be significantly robust against various security threats including geometric attacks.

The empirical results also corroborate that the proposed zero-watermarking method is highly robust against most standard image processing and geometric attacks. It exhibits much more resilience to a number of attacks, particularly geometric operations, and is superior to the existing zero-watermarking variants.

The remainder of this paper is organized as follows: In section 2, the MFrLFMs, their geometric invariances, and the accurate computation are presented. Next, a detailed description of the new zero-watermarking algorithms showed in section 3. Section 4 describes the performed experiments. Finally, the paper is concluded in section 5.

II. MULTI-CHANNEL FRACTIONAL-ORDER LEGENDRE FOURIER MOMENTS OF COLOR IMAGES

A. THE DEFINITION OF MFrLFMS

The input color images are represented in polar coordinates (r, θ) using multi-channel approach [36]. In this approach, each input image $g_C(r,\theta)$ is represented by its primary channels, $g_C(r,\theta) = \{g_R(r,\theta), g_G(r,\theta), g_B(r,\theta)\}$ where $C \in \{R, G, B\}$.

The MFrLFMs are defined as [31]:

$$FrM_{pq} = \frac{2p+1}{2\pi}\int_0^{2\pi}\int_0^1 g_C(r,\theta)\left[E_{pq}(r,\theta)\right]^* r dr d\theta, \tag{1}$$

With $\mathrm{p} = 0, 1, 2, 3, \ldots \infty$, $|\mathrm{q}| = 0, 1, 2, 3, \ldots\ldots\ldots \infty$. $\hat{\mathrm{i}} = \sqrt{-1}$; the mathematical operator $[\cdot]^*$denotes the complex conjugate; $\mathrm{E_{pq}}(\mathrm{r}, \theta)$, indicates the MFrLFMs basis functions:

$$E_{pq}(r,\theta) = L_p(\alpha, r)\, e^{-\hat{i}q\theta} \tag{2}$$

where the fractional parameter is a positive real number, $\alpha \epsilon \mathbb{R}^+$ with, $\mathrm{L_p}(\alpha, \mathrm{r})$, refers to the radial shifted Legendre polynomials with fractional-order:

$$\begin{aligned} L_p(\alpha, r) &= \sqrt{\alpha}\sum_{k=0}^{p}(-1)^{p+k}\binom{p+k}{k}\binom{p}{k} r^{\alpha k+\left(\frac{\alpha-2}{2}\right)} \\ &= \sqrt{\alpha}\sum_{k=0}^{p}(-1)^{p+k}\frac{(p+k)!r^{\alpha k+\left(\frac{\alpha-2}{2}\right)}}{(p-k)!\,(k!)^2} \end{aligned} \tag{3}$$

$\mathrm{L_p}(\alpha, \mathrm{r})$ are orthogonal over $\mathrm{r} \in [0, 1]$ and met the relation of orthogonality as follows:

$$\int_0^1 L_p(\alpha, r)\, L_q(\alpha, r)\, \mathrm{rdr} = \frac{1}{(2\mathrm{p}+1)}\delta_{\mathrm{pq}} \tag{4}$$

δ_{pq} is the well-known Kronecker function.

The three-term recurrence relation of $\mathrm{L_p}(\alpha, \mathrm{r})$, is defined as follows:

$$\begin{aligned} L_{p+1}(\alpha, r) = {} & \frac{2\mathrm{p}+1}{\mathrm{p}+1}(2\mathrm{r}^{\alpha}-1)L_p(\alpha, r) \\ & - \frac{\mathrm{p}}{\mathrm{p}+1}L_{p-1}(\alpha, r) \end{aligned} \tag{5}$$

For $p \geq 1$, where the first terms are:

$$\begin{aligned} L_0(\alpha, r) &= \sqrt{\alpha r}^{\left(\frac{\alpha-2}{2}\right)}, \\ L_1(\alpha, r) &= \sqrt{\alpha r}^{\left(\frac{\alpha-2}{2}\right)}\left(2r^{\alpha}-1\right) \end{aligned} \tag{6}$$

B. GEOMETRIC INVARIANCE OF MFrLFMS

In the design of robust zero image watermarking methods, invariance to geometric distortion (e.g., translation, scaling, rotation, and so forth) is an essential characteristic. From here on, the MFrLFMs invariance is analyzed under rotation, scaling, and translation.

For rotation invariance, assuming that $g_C(r,\theta)$ and $g_C^{\beta}(r,\theta)$ respectively, denotes the base and the rotated color images, then MFrLFMs of $g_C^{\beta}(r,\theta)$ and $g_C(r,\theta)$, $MFrM_{pq}\left(g_C^{\beta}\right)$ and $MFrM_{pq}(g_C)$ respectively satisfy (7)

$$MFrM_{pq}\left(g_C^{\beta}\right) = e^{-iq\beta}MFrM_{pq}(g_C), C \in \{R, G, B\} \tag{7}$$

Equation (7) leads to:

$$|MFrM_{pq}\left(g_C^{\beta}\right)| = |MFrM_{pq}(g_C)|, C \in \{R, G, B\} \tag{8}$$

Thus, the magnitudes of the MFrLFMs are invariant with the rotation.

For scaling invariance, assuming that $g_C^S(r,\theta)$ and $g_C(r,\theta)$ respectively, denotes the scaled and original color images. Then, $MFrM_{pq}(g_C)$ and $MFrM_{pq}\left(g_C^S\right)$ indicate the MFrLFMs of the base (g_C) and scaled (g_C^S) images, respectively.

The scale invariants of MFrLFMs are constructed as follows:

$$\varphi_{pq} = \sum_{k=0}^{p}\frac{2p+1}{2k+1}\left(\sum_{i=k}^{p}(MFrM_{00}(g_C))^{-\frac{(2i+3)}{3}}C_{pi}d_{ik}\right) \tag{9}$$

where coefficients C_{pi} and d_{ik} are:

$$C_{pi} = (-1)^{p+i}\frac{(p+i)\,!}{(p-i)\,!\,(i!)^2} \tag{10}$$

$$d_{ik} = \frac{(2k+1)\,(i!)^2}{(i+k+1)\,!\,(i-k)\,!} \tag{11}$$

For translation invariance, the MFrLFMs are invariant with the translation when the center (x_c, y_c), coincides the origin of the coordinates [37], defined as follows:

$$\begin{aligned}\overline{MFrM}_{pq} &= \frac{2p+1}{2\pi}\int_0^{2\pi}\int_0^1 g_C\left(\bar{r},\bar{\theta}\right)\left[E_{pq}\left(\bar{r},\bar{\theta}\right)\right]^* \bar{r}d\bar{r}d\bar{\theta} \\ &= \frac{2p+1}{2\pi}\int_0^{2\pi}\int_0^1 g_C\left(\bar{r},\bar{\theta}\right)L_p\left(\alpha,\bar{r}\right)\mathrm{e}^{-iq\bar{\theta}}\bar{r}d\bar{r}d\bar{\theta}\end{aligned} \tag{12}$$

where $\left(\bar{r},\bar{\theta}\right)$ denotes the image pixel following the shifting of the origin to the centroid (x_c, y_c).

C. ACCURATE COMPUTATION OF MFrLFMS

An accurate MFrLFMs estimation is the core of our proposed algorithm for facilitating a robust zero-watermarking scheme. In this method, the kernel-based approach is utilized due to its well-known accuracy. Here, the interpolated color images $\hat{g}_C\left(r_i,\theta_{i,j}\right)$ are derived from the intensity functions of the original image using the cubic interpolation [38]. Equation (1) is rewritten as follows:

$$FrM_{pq} = \frac{2p+1}{2\pi}\sum_i\sum_j K_{pq}\left(r_i,\theta_{ij}\right)\hat{g}_C\left(r_i,\theta_{i,j}\right) \tag{13}$$

With:

$$K_{pq}\left(r_i,\theta_{ij}\right) = I_p\left(r_i\right)J_q\left(\theta_{ij}\right) \tag{14}$$

Next, both the angular and radial kernels are defined as follows:

$$J_q\left(\theta_{ij}\right) = \int_{V_{ij}}^{V_{i,j+1}} e^{-\hat{i}q\theta}d\theta \tag{15}$$

$$I_P\left(r_i\right) = \int_{U_i}^{U_{i+1}} L_p\left(\alpha,r\right)rdr = \int_{U_i}^{U_{i+1}} R\left(r\right)dr \tag{16}$$

With:

$$R\left(r\right) = L_p\left(\alpha,r\right)r \tag{17}$$

The limits, $\mathrm{V_{i,j+1}}$, $\mathrm{V_{i,j}}$, $\mathrm{U_{i+1}}$ & $\mathrm{U_i}$ are:

$$V_{i,j+1} = \theta_{i,j} + \frac{\Delta\theta_{i,j}}{2};\quad V_{i,j} = \theta_{i,j} - \frac{\Delta\theta_{i,j}}{2} \tag{18}$$

$$U_{i+1} = R_i + \frac{\Delta R_i}{2};\quad U_i = R_i - \frac{\Delta R_i}{2} \tag{19}$$

Based on the Calculus principles, $\mathrm{J_q}\left(\theta_{\mathrm{ij}}\right)$ is estimated in the exact form:

$$\mathrm{J_q}\left(\theta_{\mathrm{i,j}}\right) = \begin{cases}\dfrac{\hat{\mathrm{i}}}{\mathrm{q}}\left(\mathrm{e}^{-\hat{\mathrm{i}}\mathrm{qV_{i,j+1}}} - \mathrm{e}^{-\hat{\mathrm{i}}\mathrm{qV_{i,j}}}\right), & \mathrm{q}\neq 0\\ \mathrm{V_{i,j+1}} - \mathrm{V_{i,j}}, & \mathrm{q}=0\end{cases} \tag{20}$$

Based on the numerical integration method, accurate Gaussian integration [39], the $\mathrm{I_p}\left(\mathrm{r_i}\right)$ is evaluated as:

$$\begin{aligned}\mathrm{I_p}\left(\mathrm{r_i}\right) &= \int_{\mathrm{U_i}}^{\mathrm{U_{i+1}}}\mathrm{R}\left(\mathrm{r}\right)\mathrm{dr} \\ &\approx \frac{\left(\mathrm{U_{i+1}}-\mathrm{U_i}\right)}{2}\sum_{\mathrm{l}=0}^{\mathrm{c}-1}\mathrm{w_l R}\left(\frac{\mathrm{U_{i+1}}+\mathrm{U_i}}{2}+\frac{\mathrm{U_{i+1}}-\mathrm{U_i}}{2}\mathrm{t_l}\right),\end{aligned} \tag{21}$$

where $\mathrm{w_l}$ and $\mathrm{t_l}$ denote the weights and location $\mathrm{l} = 0, 1, 2, \ldots..\mathrm{c}-1$, respectively. Furthermore, the order of numerical integration is represented by c.

III. PROPOSED ZERO-WATERMARKING SCHEME

Similar to all methods of zero watermarking, our proposed scheme consists of two stages, namely (1) the generation and (2) the verification of zero watermark. In the generation of zero watermark stage, the essential MFrLFMs features of a base image are used to formulate the zero-watermark information. In contrast, in the verification stage of zero-watermark, the original image copyright is validated. The details of the two steps are presented in the remainder of the section. Let g be the original color image with dimension $N\times N$, and let $W = \{w(i,j) \in \{0,1\}, 0 \le i < P, 0 \le j < Q\}$, be the watermark image, with dimension $P \times Q$.

A. ZERO-WATERMARK GENERATION

The generation process of zero-watermark is displayed in Fig. 1, and the steps are described below.

Step 1: Scrambling the watermark image.

The generalized Arnold transform [26] is periodic, simple, intuitive transform and very convenient to use as a scrambling algorithm to remove the spatial relationships between the pixels of the watermark image data.

Therefore, the scrambling parameters and the number of iterations can be used as the key of the zero watermarking method to enhance the security of the zero-watermarking algorithm. For a square watermark image with size $P\times Q$ and $N_w = P = Q$, the generalized Arnold transform is defined as follows:

$$\begin{pmatrix}x'\\y'\end{pmatrix} = \begin{pmatrix}1 & b\\ a & ab+1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} mod(N_w) \tag{22}$$

where N_w is the size of image dependent parameter which decides the periodicity of transformation, a and b are scrambling parameters and NIt is the number of iterations. Here, (x, y) and (x', y') are the positions of the pixels before and after the transform, respectively.

First, the key is define as, $\mathrm{K}_2 = \{a = 2, b = 3, NIt = 10\}$, Then, according to K_2, the watermark image W is scrambled to derive $W_1 = \{w_1(i,j) \in \{0,1\}, 0 \le i < P, 0 \le j < Q\}$.

Step 2: Computing MFrLFMs moments

The MFrLFMs of the original image is assessed by using (13) based on the maximum moment order $(P \times Q)$ [40].

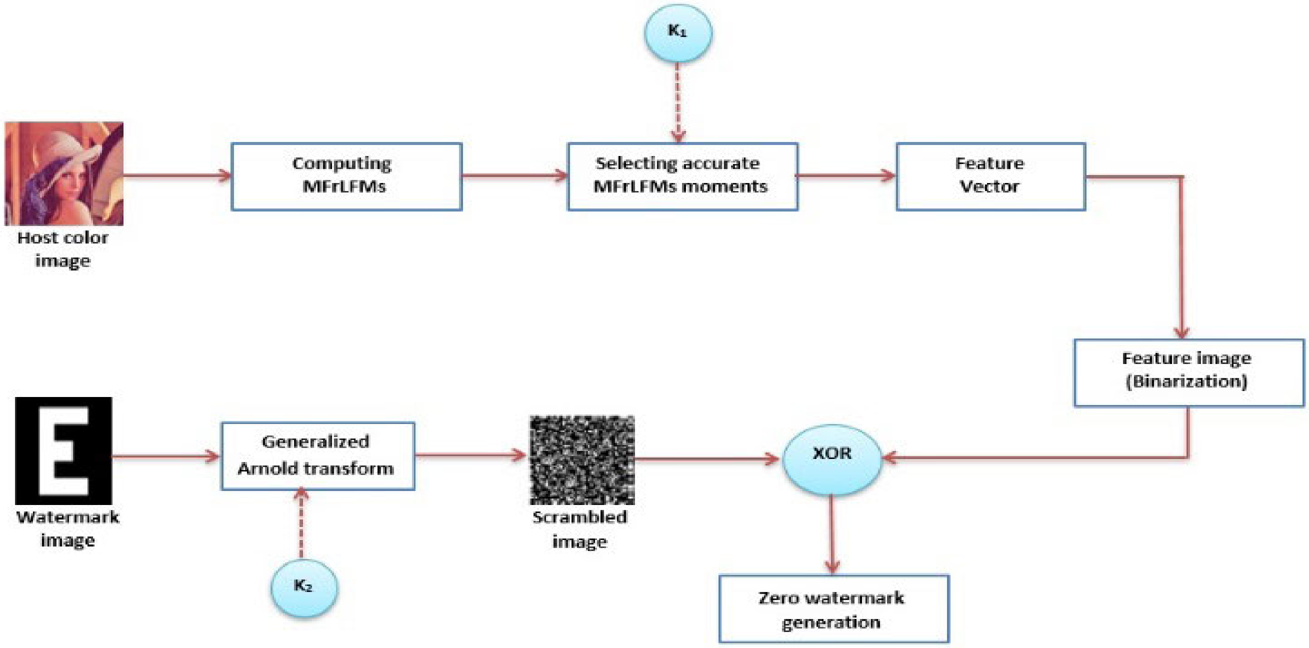

K₁
Host color image
Computing MFrLFMs
Selecting accurate MFrLFMs moments
Feature Vector
Feature image (Binarization)
Watermark image
Generalized Arnold transform
K₂
Scrambled image
XOR
Zero watermark generation

FIGURE 1. Zero-watermark generation.

Step 3: Selection of accurate MFrLFMs coefficients and construction of feature vector. In [41], Xin and his co-authors pointed out that circular moments with $q = 4m$, m ∈ Z (i.e., m = 0, m = 4, m = 8, m = 12, ...) are not suitable to embed the watermark bits. Also, the MFrLFMs with negative repetition q < 0 are not suitable to embed the watermark bits since these moments are dependent on the MFrLFMs with positive repetition q > 0. Therefore, we select MFrLFMs as follows:

$$S = \left\{ \left| MFrM_{pq} \right|, q \neq 4m, m \in Z \right\}, \tag{23}$$

where p, q, and m denote the order, repetition, and a non-negative integer, respectively. The symbol Z refers to the set of non-zero integers. By employing a secret key, K_1, $P \times Q$ coefficients MFrLFMs, are arbitrarily drawn from the accurate coefficients set S. Then, the feature vector is obtained based on the bits number of digital watermark as:

$$\vec{A} = \left\{ A_1, A_2, A_3, \ldots\ldots.., A_{P\times Q} \right\} \tag{24}$$

Step 4: Generation of binary feature image (Binarization).

The binary feature vector $\vec{B}$ is generated from the feature vector $\vec{A}$ as follows:

$$\vec{B} = \left\{ B_1, B_2, B_3, \ldots\ldots.., B_{P\times Q} \right\} \tag{25}$$

according to the following binarization formula:

$$B_i = \begin{cases} 1, & if\ A_i \geq T \\ 0, & if\ A_i < T \end{cases} \quad i = 1, 2, \ldots\ldots\ldots P \times Q \tag{26}$$

where T denotes a threshold, which is the mean value of the feature vector $\vec{A}$. The binarized feature vector $(\vec{B})$ is re-arranged into a 2D feature image, LF of $P \times Q$ size.

Step 5: Zero-watermark image generation

A bitwise Exclusive OR (XOR) operation is utilized, with the scrambled watermark image data, W_1 and the image feature, LF to construct the signal of zero-watermark W_{zero}, as follows.

$$W_{zero} = XOR\,(LF, W_1) \tag{27}$$

Therefore, the image of zero-watermark contains the watermark image.

B. ZERO-WATERMARK VERIFICATION

By using the verification of zero-watermark, the copyright of protected color is validated. Only reserved signal of zero watermarks and the protected image (or its attacked version) are required in the zero-watermark verification phase. Fig. 2 shows the verification of the zero-watermark flow chart, and the procedure is described as follows.

Step 1: Assessing MFrLFMs moments of the protected color image

The MFrLFMs of the protected color image data, g^*, are computed by using (13).

Step 2: Selection of accurate MFrLFMs coefficients and construction of the feature vector.

The accurate and robust MFrLFMs coefficients S^* are chosen to formulate the feature vector $\overrightarrow{A^*}$ (see the STEP-2 in Subsection A in Section III).

$$\overrightarrow{A^*} = \left\{ A_1^*, A_2^*, A_3^*, \ldots\ldots.., A_{P\times Q}^* \right\} \tag{28}$$

Step 3: Synthesis of binary feature image (Binarization).

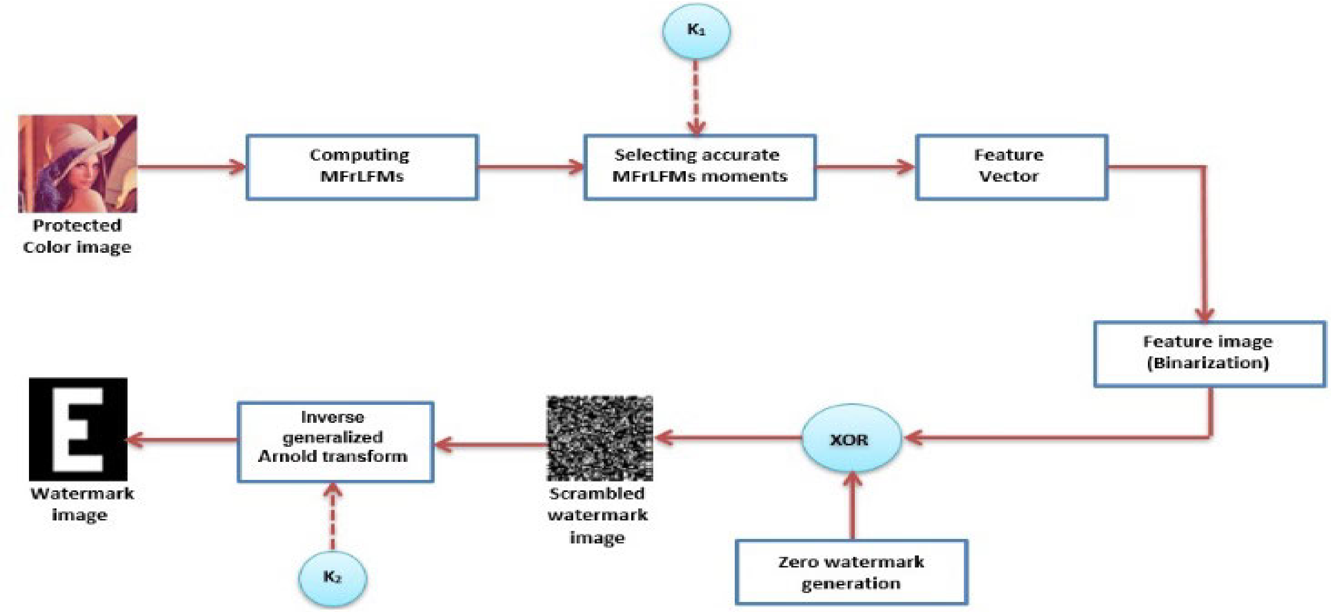

K₁
Protected Color image
Computing MFrLFMs
Selecting accurate MFrLFMs moments
Feature Vector
Feature image (Binarization)
XOR
Zero watermark generation
Scrambled watermark image
Inverse generalized Arnold transform
K₂
Watermark image

FIGURE 2. Zero-watermark verification framework.

TABLE 1. Equalizations of the zero-watermark signals produced from the ten base images.

Base images	Number of '0'	Number of '1'	Equalization
Image a	514	510	0.0039
Image b	522	502	0.0195
Image c	505	519	0.0137
Image d	509	515	0.0059
Image e	520	504	0.0156
Image f	506	518	0.0117
Image g	521	503	0.0176
Image h	508	516	0.0078
Image i	515	509	0.0059
Image j	507	517	0.0098
Mean of Equalization = 0.111			

The binary feature vector $\overrightarrow{B^*}$ is produced from the feature vector $\overrightarrow{A^*}$ as follows:
(see the STEP-3 in Subsection A in Section III for binarization process).

Next, the binarized feature vector $\overrightarrow{B^*}$ is re-arranged into a 2D feature image, LF^* of $P \times Q$ size.

Step 4: Synthesis of the scrambled watermark image

A scrambled image of the watermark W_1^* is produced by using XOR operation on the binary feature image L.F.* and the corresponding image of reserved zero-watermark $\mathrm{W}_{\mathrm{zero}}$ for the protected image.

$$\mathrm{W}_1^* = XOR\left(LF^*, W_{zero}\right) \tag{29}$$

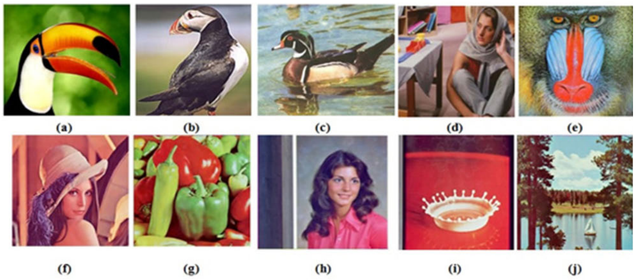


FIGURE 3. Standard color images.

Step 5: Recovering of verifiable the watermark image.

In this step, inverse generalized Arnold transform is used to obtain the retrieved watermark, which defined as:

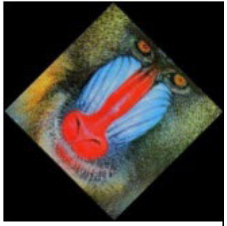
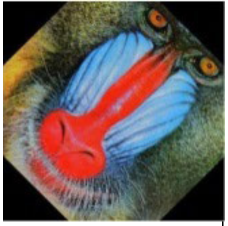
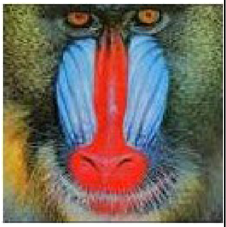
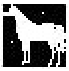
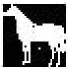
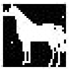
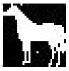
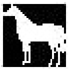
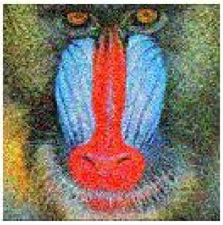
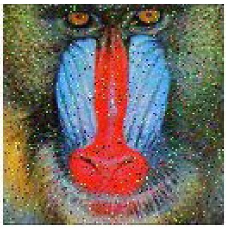
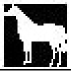
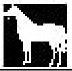
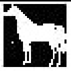
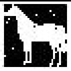
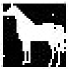
$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ab+1 & -b \\ -a & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} mod(N_w) \tag{30}$$

We need the key, K_2 to determine the scrambling parameter, the retrieved watermark, W* to be retrieved is denoted as $W^* = \{w^*(i,j) \in \{0,1\}, 0 \le i < P, 0 \le j < Q\}$.

IV. EXPERIMENTS

Various experiments demonstrate the proposed zero watermark algorithm's efficiency for color images and the results compared with other well-known zero watermark algorithms [22], [28], [29]. The authors conducted all experiments on selected standard color images with the same size of 512 × 512; they are shown in Fig. 3. Twelve images of the size 64 × 64 depicted in Fig. 4 are collected and utilized as binary watermarks.

TABLE 2. Binary watermark extraction with various distortions.

Attack	**Rotation with no cropping 45°**	**Rotation with cropping 45°**	**Scaling 0.5**	**Scaling 1.75**	**JPEG compression 70**
Attacked Image					
Retrieved watermark					
PSNR	10.9863	12.8772	32.6035	39.6315	39.4396
BER	0.0049	0.0029	0.0059	0.0020	9.7656e-04
NC	0.9931	0.9958	0.9917	0.9972	0.9986
Attack	**JPEG compression 90**	**Gaussian noise (0.04)**	**Salt & Peppers noise (0.04)**	**Median filtering 5x5**	**Gaussian filtering 5x5**
Attacked Image					
Retrieved watermark					
PSNR	41.4254	37.1775	38.7504	35.1962	35.2036
BER	0	0.0020	0.0029	0.0088	0.0059
NC	1	0.9972	0.9958	0.9876	0.9917

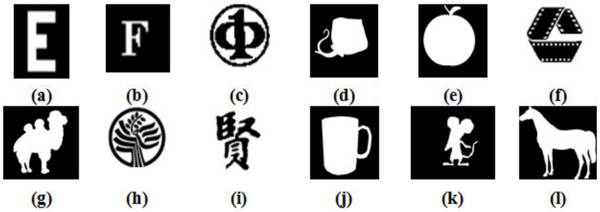


FIGURE 4. Binary watermarks images.

A. PERFORMANCE EVALUATION METRICS

For assessment measures, the quality of attacked images is assessed by using the computed peak signal-to-noise ratio (PSNR) between the base (original) and attacked (targeted) images.

The robustness against attacks is verified by the bit error rate (BER) and the normalized correlation (N.C.), which are employed to measure the closeness of the extracted and original watermarks.

The PSNR of the original image, g_c and its attacked version, g_c^w, is:

$$PSNR\left(g_c, g_c^w\right) = 10\,log_{10}\frac{255^2}{MSE} \tag{31}$$

where:

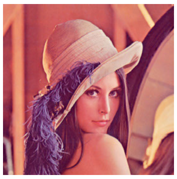
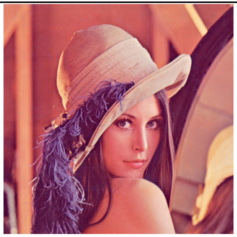
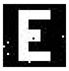
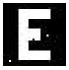
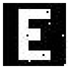
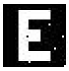
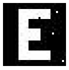
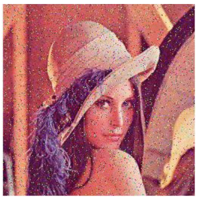
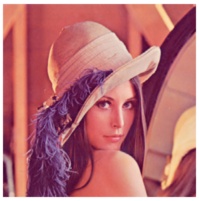
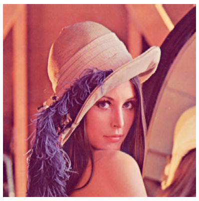
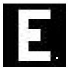
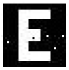
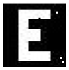
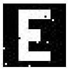
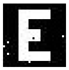
$$MSE = \frac{1}{N^2}\left(\sum_{i=1}^{N}\sum_{j=1}^{N}\left[g_c^w(i,j) - g_c(i,j)\right]^2\right) \tag{32}$$

The definition of the BER and N.C. of the base watermark, W and the extracted one W^*, respectively, are given by:

$$BER = \frac{1}{P \times Q}\left(\sum_{i=1}^{P}\sum_{j=1}^{Q}\left[w(i,j) - w^*(i,j)\right]^2\right) \tag{33}$$

$$NC = \frac{\sum_{i=1}^{P}\sum_{j=1}^{Q}\left[w(i,j) \times w^*(i,j)\right]}{\sum_{i=1}^{P}\sum_{j=1}^{Q}\left[w(i,j)\right]^2} \tag{34}$$

TABLE 3. Binary watermark extraction with various distortions.

Attack	**Rotation with no cropping 35°**	**Rotation with cropping 35°**	**Scaling 0.75**	**Scaling 1.5**	**JPEG compression 70**
Attacked Image					
Retrieved watermark					
PSNR	11.1728	13.7203	32.8205	39.8361	38.7396
BER	0.0059	0.0039	0.0068	0.0059	0.0039
NC	0.9892	0.9928	0.9873	0.9892	0.9928
Attack	**JPEG compression 90**	**Gaussian noise (0.05)**	**Salt & Peppers noise (0.05)**	**Median filtering 5x5**	**Gaussian filtering 5x5**
Attacked Image					
Retrieved watermark					
PSNR	41.9868	37.4127	38.9206	35.3518	36.1135
BER	9.7656e-04	0.0049	0.0039	0.0078	0.0059
NC	0.9982	0.9910	0.9928	0.9857	0.9892

The BER value lies between 0 and 1. The algorithm is more robust, where the BER value is closer to 0. The perfect extraction of the original watermark will lead to BER = 0. In that case, all the extracted watermark bits would be equal to those of the original watermark. On the other hand, if all the bits are extracted incorrectly, BER = 1.

B. ZERO-WATERMARK EQUALIZATION

For the sake of security, the numbers of 0 and 1 within the zero-watermark generated signal should be as close and balanced as possible as implied by the equalization. The numbers of ’0’ are equal or close to equal to the numbers of ’1’, leading to good equalization. This indicates that the corresponding zero-watermarking is endowed with a high level of security. The generated zero-watermarking equalization is measured by the evaluation parameter E.Q. which is defined as (35).

$$EQ = \frac{|N_0 - N_1|}{P \times Q} \tag{35}$$

The symbols N_0 and N_1 refer to the numbers of zeros, ’0’, and ones, ’1’, in the zero-watermark. The better equalization is achieved when the E.Q. is closer to 0. Fig. 5 shows the well-known “Lena” image, its matrix of extracted binary feature, and the generated zero-watermark.

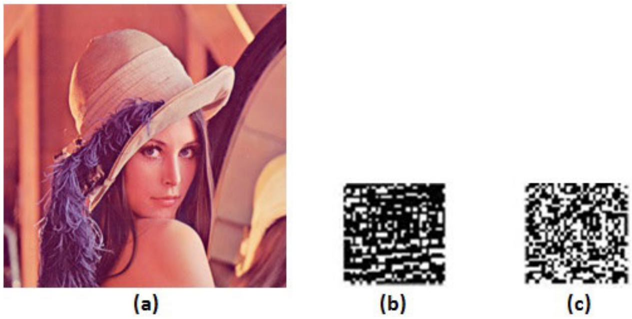


FIGURE 5. (a) The image of ’Lena’ (b) The extracted matrix of binary feature (c) the generated zero-watermark.

An experiment was performed using ten original images as illustrated in Fig. 3(a-j) to evaluate the proposed algorithm in terms of zero-watermark equalization (E.Q.).

The zero-watermark signal is generated for each image, and N0, N1, and E.Q. are computed in Table 1.

As shown in Table 1, the average equalizations of 10 zero-watermarks are 0.0111, which shows that the signal numbers '0' and '1' in the zero-watermarks are almost equal. These results ensure that the proposed scheme has high security and better equalization.

C. WATERMARK ROBUSTNESS

1) ROBUSTNESS TO VARIOUS ATTACKS

The robustness of the proposed algorithm is evaluated for the geometric as well as standard image processing attacks in this section. Each one of the host color images has different image feature. Therefore, different images lead to different results, but the obtained results from all images are very closer. In the conducted experiment, the color image, "baboon" of size 512 × 512, is selected from Fig. 3 as an example of the base (original) image. A binary image "horse" of 32 × 32 from Fig. 4 was selected and used as the watermark. In the additional conducted experiment, the color image, "Lena" of size 256 × 256 in Fig. 3 is selected and used as original image. A binary image "Letter E" of 32 × 32 Fig. 4 is selected and used as the watermark image.

A summary of each attack and its parameter setting are shown in Tables 2 and 3. For each attack, the corresponding extracted watermark image and its PSNR, BER, and N.C. values of the proposed algorithm are computed and presented in Tables 2 and 3. As shown in Tables 2 and 3, the proposed algorithm's extracted watermarks are closer to the original. The corresponding PSNR, BER, and N.C. values tend to optimum values. The obtained results clearly demonstrate that the watermarks which were retrieved remained recognizable even though a significant distortion of the original color image had been performed.

TABLE 4. BER values distorted watermark.

Various Attacks		Wang et al. [22]	Xiaobing et al. [28]	Yang et al. [29]	Proposed Method
Rotation	25°	0.0205	0.0195	0.0127	0.0059
	35°	0.0293	0.0244	0.0205	0.0098
	45°	0.0283	0.0166	0.0146	0.0078
Scaling factor	0.75	0.0215	0.0205	0.0186	0.0088
	1.5	0.0127	0.0107	0.0098	0.0039
Shift (Translation)	(H 4, V 4)	0.0215	0.0156	0.0107	0.0049
Reduction (0. 5) + Compression (JPEG, 80%)		0.0342	0.0293	0.0205	0.0098
Magnification (1.75) + Compression (JPEG, 80%)		0.0120	0.0098	0.0088	0.0049
Rotation (35°) + Compression (JPEG, 80%)		0.0305	0.0256	0.0210	0.0078
Compression	(JPEG, 70%)	0.0127	0.0107	0.0088	0.0039
	(JPEG, 90%)	0.105	0.0088	0.0078	0.0029
Noise, "Salt & Peppers, 0.04"		0.0156	0.0135	0.0123	0.0098
Noise, "Gaussian, 0.04"		0.0270	0.0142	0.0120	0.0078
Filtering (Gaussian , 3*3)		0.0143	0.0118	0.0105	0.0059
Filtering (Median , 3*3)		0.0198	0.0141	0.0123	0.0098

2) COMPARISON WITH SIMILAR ZERO-WATERMARKING ALGORITHMS

From here on, the proposed algorithm's robustness is examined against various attacks compared with the three existing similar zero-watermarking algorithms [22], [28], [29].

Several experiments were performed where various attacks (e.g., additive noise, filtering, JPEG compression, and geometric transforms (rotation, translation, and scaling)) were applied individually and in various combined forms.

The corresponding average values of BER and N.C. of twelve test images, as shown in Fig. 3 between the base and the recovered watermarks under the presence of these attacks are computed for the proposed and the existing methods [22], [28], [29] and summarized in Tables 4 and 5, respectively.

The zero-watermarking algorithms based on MFrLFMs-moments are superior to the algorithms [22], [28], [29]. regarding standard image processing and geometric attacks. In addition, for each attack listed in Tables 3 and 4, our proposed algorithm yielded the lowest BER values and the highest N.C. values. This indicates that our proposal is much more robust compared to the other considered methods. These results clearly demonstrate that our proposed approach can be effective against both common image processing and advanced geometric attacks, thereby emerging as a robust solution to the considered watermarking problem in this paper.

D. COMPUTATION TIME

In this subsection, the computational time of the proposed zero watermarking and the existing methods are evaluated for two main stages, zero watermark generation and verification stages. A set of experiments are performed for ten test images (shown in Fig. 3) with size of 512 × 512. The average computation times for the proposed method and the existing methods are displayed in Table 6. It can be observed from Table 6 that the average computation times for the proposed method is less than the other compared methods [22], [28], [29].

TABLE 5. N.C. values of the distorted watermarks.

Various Attacks		Wang et al. [22]	Xiaobing et al. [28]	Yang et al. [29]	Proposed Method
Rotation	25 °	0.9745	0.9759	0.9843	0.9928
	35 °	0.9643	0.9697	0.9745	0.9880
	45 °	0.9650	0.9794	0.9820	0.9904
Scaling factor	0. 5	0.9736	0.9747	0.9769	0.9893
	1.75	0.9843	0.9867	0.9880	0.9952
Shift (Translation)	(H 4, V4)	0.9737	0.9806	0.9867	0.9940
Reduction (0. 5) + Compression (JPEG, 80%)		0.9582	0.9643	0.9748	0.9880
Magnification (1.75) + Compression (JPEG, 80%)		0.9849	0.9880	0.9893	0.9940
Rotation (35°) + Compression (JPEG, 80%)		0.9638	0.9690	0.9736	0.9904
Compression	(JPEG, 70%)	0.9854	0.9872	0.9894	0.9952
	(JPEG, 90%)	0.9867	0.9893	0.9904	0.9978
Noise, "Salt & Peppers, 0.04"		0.9806	0.9764	0.9850	0.9880
Noise, "Gaussian, 0.04"		0.9665	0.9726	0.9849	0.9904
Filtering (Gaussian , 3*3)		0.9729	0.9857	0.9868	0.9928
Filtering (Median , 3*3)		0.9776	0.9724	0.9852	0.9880

TABLE 6. Average execution time of the proposed zero-watermark and the existing methods [22], [28], [29].

Average Execution Time (sec)	Wang et al.. [22]	Xiaobing et al. [28]	Yang et al. [29]	Proposed Method
Zero-watermark generation time	60.54	40.358	20.182	14.283
Zero-watermark verification	60.83	40.805	20.257	14.791

Therefore, the computation time of the proposed zero-watermarking method is suitable for a real application of watermarking.

V. CONCLUSION

This paper proposed a novel algorithm for achieving a robust zero-watermarking of color image contents. Our proposed robust zero-watermarking scheme is based on an accurate and stable MFrLFMs computation. The zero-watermarking scheme was found to be highly resistant against the complicated and straightforward combination of different common attacks of image processing and geometric attacks. Numerical simulations verified the robustness of our proposal to a myriad of attacks, including geometric distortions. Also, our proposed approach was demonstrated to outperform the existing watermarking methods. In the future, we will extend the proposed algorithm for protecting medical images in various Internet of Medical Things (IoMT) use-cases.

REFERENCES

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

[2] O. S. Faragallah, A. Afifi, H. S. El-Sayed, M. A. Alzain, J. F. Al-Amri, F. E. A. El-Samie, and W. El-Shafai, "Efficient HEVC integrity verification scheme for multimedia cybersecurity applications," *IEEE Access*, vol. 8, pp. 167069–167089, 2020.

[3] A. Zigomitros, A. Papageorgiou, and C. Patsakis, "Social network content management through watermarking," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 1381–1386, doi: 10.1109/TrustCom.2012.264.

[4] C. Iwendi, Z. Jalil, A. R. Javed, T. Reddy, R. Kaluri, G. Srivastava, and O. Jo, "Keysplitwatermark: Zero watermarking algorithm for software protection against cyber-attacks," *IEEE Access*, vol. 8, pp. 72650–72660, 2020.

[5] S. G. Rizzo, F. Bertini, and D. Montesi, "Fine-grain watermarking for intellectual property protection," *EURASIP J. Inf. Secur.*, vol. 2019, no. 1, Dec. 2019, Art. no. 10.

[6] W. H. Alshoura, Z. Zainol, J. S. Teh, and M. Alawida, "A new chaotic image watermarking scheme based on SVD and IWT," *IEEE Access*, vol. 8, pp. 43391–43406, 2020.

[7] C. Qin, P. Ji, C. C. Chang, J. Dong, and X. Sun, "Non-uniform watermark sharing based on optimal iterative BTC for image tampering recovery," *IEEE Multimedia*, vol. 25, no. 3, pp. 36–48, Oct. 2018, doi: 10.1109/MMUL.2018.112142509.

[8] H. Xu, X. Kang, Y. Chen, and Y. Wang, "Rotation and scale invariant image watermarking based on polar harmonic transforms," *Optik*, vol. 183, pp. 401–414, Apr. 2019.

[9] 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.

[10] 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. 24727–24750, 2019.

[11] Z. Shao, Y. Shang, Y. Zhang, X. Liu, and G. Guo, "Robust watermarking using orthogonal Fourier–Mellin moments and chaotic map for double images," *Signal Process.*, vol. 120, pp. 522–531, Mar. 2016.

[12] 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, doi: 10.1016/j.sigpro.2020.107544.

[13] Q. Wen, T. Sun, and S. Wang, "Concept and application of zero-watermark," *Acta Electron. Sinica*, vol. 31, pp. 214–216, Feb. 2003, doi: 10.3321/j.issn:0372-2112.2003.02.015.

[14] C.-C. Chang and J.-C. Chuang, "An image intellectual property protection scheme for gray-level images using visual secret sharing strategy," *Pattern Recognit. Lett.*, vol. 23, no. 8, pp. 931–941, Jun. 2002.

[15] C.-C. Chang and P.-Y. Lin, "Adaptive watermark mechanism for rightful ownership protection," *J. Syst. Softw.*, vol. 81, no. 7, pp. 1118–1129, Jul. 2008.

[16] X. Wu and W. Sun, "Robust copyright protection scheme for digital images using overlapping DCT and SVD," *Appl. Soft Comput.*, vol. 13, no. 2, pp. 1170–1182, Feb. 2013.

[17] H.-H. Tsai, H.-C. Tseng, and Y.-S. Lai, "Robust lossless image watermarking based on α-trimmed mean algorithm and support vector machine," *J. Syst. Softw.*, vol. 83, no. 6, pp. 1015–1028, Jun. 2010.

[18] H.-H. Tsai, Y.-S. Lai, and S.-C. Lo, "A zero-watermark scheme with geometrical invariants using SVM and PSO against geometrical attacks for image protection," *J. Syst. Softw.*, vol. 86, no. 2, pp. 335–348, Feb. 2013.

[19] 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.

[20] G. Gao and G. Jiang, "A lossless copyright authentication scheme based on Bessel–Fourier moment and extreme learning machine in curvature-feature domain," *J. Syst. Softw.*, vol. 86, no. 1, pp. 222–232, Jan. 2013.

[21] Z. Shao, Y. Shang, R. Zeng, H. Shu, G. Coatrieux, and J. Wu, "Robust watermarking scheme for color image based on quaternion-type moment invariants and visual cryptography," *Signal Process., Image Commun.*, vol. 48, pp. 12–21, Oct. 2016.

[22] C.-P. Wang, X.-Y. Wang, Z.-Q. Xia, C. Zhang, and X.-J. Chen, "Geometrically resilient color image zero-watermarking algorithm based on quaternion exponent moments," *J. Vis. Commun. Image Represent.*, vol. 41, pp. 247–259, Nov. 2016.

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

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] X. Kang, F. Zhao, Y. Chen, G. Lin, and C. Jing, "Combining polar harmonic transforms and 2D compound chaotic map for distinguishable and robust color image zero-watermarking algorithm," *J. Vis. Commun. Image Represent.*, vol. 70, Jul. 2020, Art. no. 102804.

[29] 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.

[30] R. Benouini, I. Batioua, K. Zenkouar, A. Zahi, S. Najah, and H. Qjidaa, "Fractional-order orthogonal chebyshev moments and moment invariants for image representation and pattern recognition," *Pattern Recognit.*, vol. 86, pp. 332–343, Feb. 2019.

[31] K. M. Hosny, M. M. Darwish, and T. Aboelenen, "New fractional-order Legendre-Fourier moments for pattern recognition applications," *Pattern Recognit.*, vol. 103, Jul. 2020, Art. no. 107324.

[32] K. M. Hosny, M. M. Darwish, and M. M. Eltoukhy, "Novel multi-channel fractional-order radial harmonic Fourier moments for color image analysis," *IEEE Access*, vol. 8, pp. 40732–40743, 2020.

[33] K. M. Hosny, M. M. Darwish, and M. M. Fouda, "Robust color images watermarking using new fractional-order exponent moments," *IEEE Access*, vol. 9, pp. 47425–47435, 2021.

[34] K. M. Hosny, M. M. Darwish, and T. Aboelenen, "Novel fractional-order polar harmonic transforms for gray-scale and color image analysis," *J. Franklin Inst.*, vol. 357, no. 4, pp. 2533–2560, Mar. 2020.

[35] K. M. Hosny, M. Abd Elaziz, and M. M. Darwish, "Color face recognition using novel fractional-order multi-channel exponent moments," *Neural Comput. Appl.*, vol. 33, no. 11, pp. 5419–5435, Jun. 2021.

[36] C. Singh and J. Singh, "Multi-channel versus quaternion orthogonal rotation invariant moments for color image representation," *Digit. Signal Process.*, vol. 78, pp. 376–392, Jul. 2018.

[37] T. Suk and J. Flusser, "Affine moment invariants of color images," in *Proc. 13th Int. Conf. Comput. Anal. Images Patterns* (Lecture Notes Computer Science), vol. 5702, Münster, Germany: Springer, 2009, pp. 334–341.

[38] Y. Xin, M. Pawlak, and S. Liao, "Accurate computation of zernike moments in polar coordinates," *IEEE Trans. Image Process.*, vol. 16, no. 2, pp. 581–587, Feb. 2007.

[39] J. D. Faires and R. L. Burden, *Numerical Methods*. Pacific Grove, CA, USA: Brooks Cole, 2002.

[40] K. M. Hosny and M. M. Darwish, "Invariant image watermarking using accurate polar harmonic transforms," *Comput. Electr. Eng.*, vol. 62, pp. 429–447, Aug. 2017.

[41] 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.

KHALID M. HOSNY (Member, IEEE) was born Zagazig, Egypt, in 1966. He received the B.Sc., M.Sc., and Ph.D. degrees from Zagazig University, Egypt, in 1988, 1994, and 2000, respectively. From 1997 to 1999, he was a Visiting Scholar with the University of Michigan, Ann Arbor, MI, USA, and the University of Cincinnati, Cincinnati, OH, USA. He is currently a Professor of information technology with the Faculty of Computers and Informatics, Zagazig University. He published three edited books and more than 80 articles in international journals. His research interests include image processing, pattern recognition, multimedia, and computer vision. He is a Senior Member of ACM. He is an editor and a scientific reviewer for more than 40 international journals.

MOHAMED M. DARWISH received the B.Sc. (Hons.) and M.Sc. degrees in computer science from the Faculty of Science, Assiut University, Assiut, Egypt. He is currently a Lecturer with the Department of Computer Science, Faculty of Computers and Information, Assiut University. His research interests include image processing and data mining.

MOSTAFA M. FOUDA (Senior Member, IEEE) received the Ph.D. degree in information sciences from Tohoku University, Japan, in 2011. He has worked as an Assistant Professor with Tohoku University, Japan. He was a Postdoctoral Research Associate with Tennessee Technological University, Cookeville, TN, USA. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, Idaho State University, Pocatello, ID, USA. He also holds the position of an Associate Professor with Benha University, Egypt. He has been engaged in research on cybersecurity, communication networks, wireless mobile communications, smart healthcare, smart grids, AI, blockchain, and the IoT. He has published more than 60 articles in prestigious peer-reviewed journals and conferences. He was a recipient of the prestigious 1st place award during his graduation from the Faculty of Engineering at Shoubra, Benha University, Egypt, in 2002. He has served as the Symposium/Track Chair of IEEE VTC2021-Fall conference. He has also served as the Workshops Chair, the Session Chair, a Technical Program Committee (TPC) Member, and a Designated Reviewer in leading international conferences, such as IEEE GLOBECOM, ICC, PIMRC, ICCVE, IWCMC, and 5G World Forum. He also served as a Guest Editor of some special issues of several top-ranked journals, such as IEEE Wireless Communications (WCM) and *IEEE Internet of Things Magazine* (IoTM). He also serves as a referee of some renowned IEEE journals and magazines, such as IEEE Communications Surveys and Tutorials, IEEE Wireless Communications (WCM), IEEE Transactions on Wireless Communications, IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Smart Grid, IEEE Access, IEEE Transactions on Network and Service Management, IEEE Transactions on Emerging Topics in Computing, and IEEE Network. He is an Editor of IEEE Transactions on Vehicular Technology (TVT) and an Associate Editor of IEEE Access.