IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 23, 2022, accepted April 1, 2022, date of publication April 8, 2022, date of current version April 15, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3165813

Multiple Zero-Watermarking of Medical Images for Internet of Medical Things

MAHMOUD MAGDY[1], NEVEEN I. GHALI[1], SAID GHONIEMY[2], AND KHALID M. HOSNY[3], (Member, IEEE)

[1]Department of Digital Media Technology, Future University in Egypt (FUE), New Cairo 11835, Egypt
[2] Department of Computer Systems, Faculty of Computer and Information Sciences, Ain Shams University, Cairo 11566, Egypt
[3]Department of Information Technology, Zagazig University, Zagazig 44519, Egypt

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

ABSTRACT The Internet of Medical Things (IoMT) plays a vital role in healthcare systems to increase electronic devices' accuracy, reliability, and productivity. This paper presents fast multiple zero-watermarking methods based on Multi-channel Fractional Legendre Fourier moments (MFrLFMs) for medical image security and copyright protection in IoMT applications without deforming the original medical images. The MFrLFMs are utilized due to their high accuracy, numerical stability, geometric invariances, and high resistance to various attacks. Based on the most significant features generated from MFrLFMs, after scrambling using a two-dimensional Discrete Henon Map, then XORed with binary scrambled watermark to construct owner share. The proposed watermarking method is implemented using a low-cost Raspberry Pi Linux microprocessor, which ensures the suitability of medical devices in the IoMT environment. We evaluated the robustness of the proposed algorithm against different geometric and common signal processing attacks using various medical images. The proposed method gives better BER, NC, and SSIM values than existing methods.

INDEX TERMS Color medical images, zero-Watermarking, IoMT, fractional-order moments, Raspberry-Pi.

I. INTRODUCTION

Nowadays, data transmission technologies and telemedicine applications have been developed. Medical image security and copyright protection become challenging, especially after the COVID-19 pandemic and quarantine [1]. Researchers are directed toward an online healthcare system that must transmit the patients' medical information and scan images and medical reports through a secure network. Protection of these medical images is a big challenge. Many techniques have been used to secure this data as cryptography [2], [3], steganography [4], and watermarking [5]. Digital watermarking is widely used in image security which can be classified as a traditional watermarking model based on embedding an information watermark into the original image, then the watermark extracted to prove copyright. The embedding and extraction operations lead to image degradation, a lossless technique [6] has been proposed to solve these challenges.

Due to the shortage of traditional watermarking schemes, Quan *et al.* [7]. Robust features are extracted and combined with the watermark. The zero-watermark is stored in a trusted authority for future usage. So, extracting robust features from the image is challenging in such approaches.

Due to the continued growth in image processing applications in various fields, feature extraction and image mapping have become two critical challenges in computer vision and image security. Feature extraction is the process of detecting the essential information of the image at every pixel, which must be robust to different geometric [8] and image processing attacks [9]. Many feature extraction algorithms have been proposed. However, the main challenge is how to extract features robust against various image attacks. Feature extraction is classified into traditional [10] and moment-based. The traditional feature extraction algorithms can resist common attacks but give poor results against geometric attacks like flipping, rotation, and translation.

Moments [11] is a new feature extraction approach used in many applications such as medical image security, object identification, image reconstruction, and invariant pattern recognition. Moments-based algorithms have this valued property of geometric invariance, which motivates scientists and researchers to utilize the moments in constructing

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaolong Li.

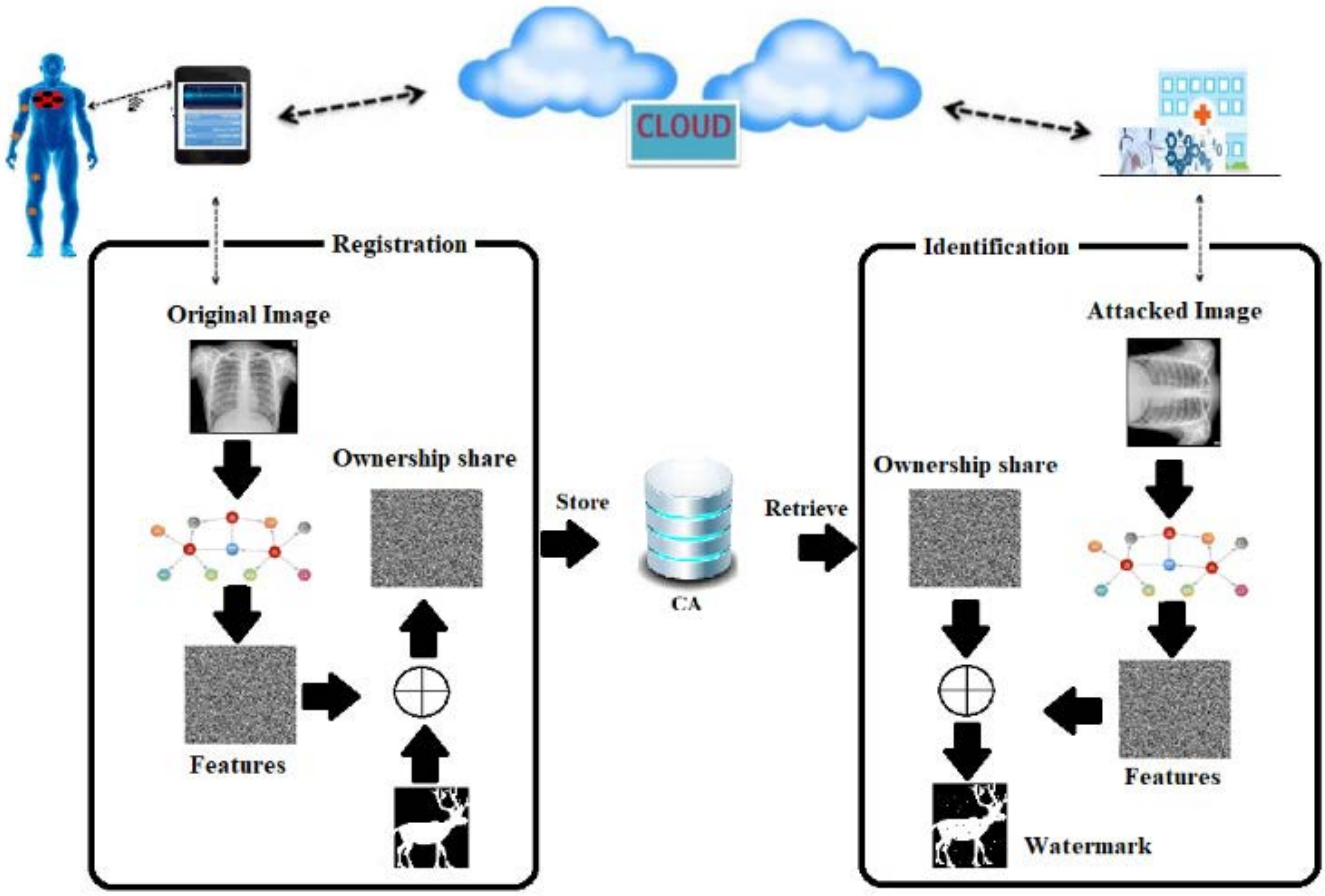


FIGURE 1. Zero-watermarking in telemedicine application.

zero watermarking algorithms and other image processing applications that need accurate and robust features against geometric attacks such as invariant patterns recognition, medical image security, image reconstruction, and object identification.

Medical images have some special requirements [12], so many robust zero-watermarking techniques have been developed which focus on the region of interest (ROI) to combat mentioned problems and successfully solve these specific requirements.

Due to the medical image security challenges [13], a zero watermarking technique is proposed to overcome these challenges. The authors used Fractional Legendre Fourier Moments (FrLFMs) with a Two-Dimensional Discrete Henon Map for enhancing security. The proposed approach encompasses five main steps. First, the Legendre moments are computed from the original medical image. Second, choose the most accurate moments and build the master share representing the host image. Third, master share and binary scrambling. Fourth is the binarization process for both the watermark and the selected features, then XORed to generate the zero watermark after scrambling.

The Zero-watermark technique [14] encompasses two main phases, the registration and identification phase, as shown in Fig. 1.

Since then, various research groups have utilized orthogonal moments as well as moment invariants; some of this research is presented below:

Xia *et al.* [14] presented a zero watermarking technique based on the continuous orthogonal radial harmonic Fourier moments (FrRHFMs) to protect the copyright of medical images. A fractional-order overcomes the numerical instability to improve the security results.

Zhang *et al.* [15] proposed robust zero watermarking schemes for colored medical data to protect the copyright of many medical images based on the quaternion generalized Fourier descriptor (QGFD) algorithm and QR code. The most robust features are computed from each color image using QGFD and binarized, then XORed with the scrambled watermark image. This study [16] introduced a new imperceptible zero watermarking method using Tchebichef Moments for the medical images. This method applied quantization using dither modulation to increase the watermark imperceptibility.

TABLE 1. Raspberry Pi 4 model B specifications.

CPU	Quad-core Cortex-A72 -64-bit CPU with a speed of 1.5 GHz	Wireless Communication	5.0 GHz wifi
RAM	1 GB	Bluetooth	V 5.0
VGA	Two micro-HDMI ports with 4K video resolution	LAN port	High-speed ethernet
USB	Multiple USB 3.0 ports		

In this paper [17], the authors utilized fractional orders of Gegenbauer moments (FrMGMs) in their scheme. Xia *et al.* [18] proposed a lossless watermarking scheme to prove the copyright of colored medical images by extracting the accurate coefficients extracted using quaternion polar harmonic transforms (QPHTs).

Wang *et al.* [19] used polar complex exponential transform (PCET) in their algorithm for medical images. Wang *et al.* [20] presented a robust model using polar complex exponential transform (PCET) medical image security to overcome the challenge of watermark discrimination ignored by many researchers in which original host image and fake host image. It cannot be distinguished.

This paper is organized as follows. Section 2 presents the concept of the internet of medical things, the Raspberry-pi platform, the two-dimensional discrete Henon map, and MFrLFMs. Section 3 presents our proposed scheme. Section 4 shows the experimental results. Section 5 discusses the results. Finally, Section 6 concludes the work.

II. PRELIMINARIES

A. INTERNET OF MEDICAL THINGS (IoMT)

IoMT [21] shares an important role in healthcare applications. The development of communication protocols and smart devices made connecting medical things easier for diagnoses operations. Researchers are interconnecting healthcare services and medical devices to contribute to a healthcare system. Medical images and data need to be secured before transmission over the network. Our focus in this study is on securing these data in the healthcare domain [22].

The C++ language's powerful libraries and packages [24]. Raspberry Pi is a portable Linux-based embedded system board that has been used in many computer vision, image classification, and machine learning applications [23]. Some versions of Raspberry Pi have a Quad-core CPU, support the parallel processing implementations using OpenMP [25] and MPI [26] as discussed in [27] also in [28] to solve edge detection problems and utilize the cluster to accelerate the wavelet transform in 3D. Our implementation used the Raspberry Pi 4 Model B kit shown in Fig. 2. Table 1 the properties of the used board.

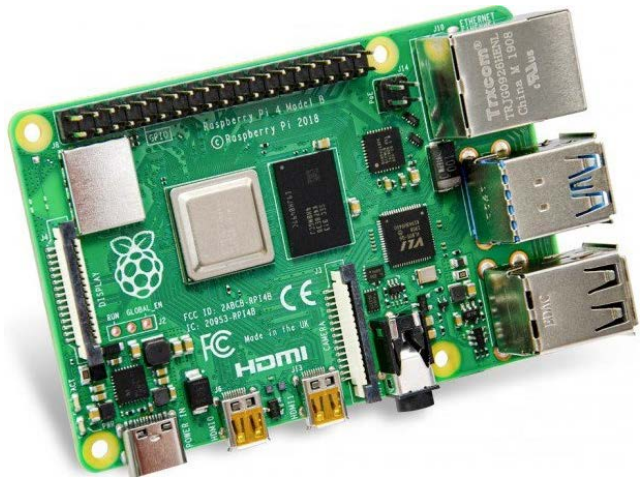


FIGURE 2. The raspberry Pi 4 model B of x86 PC.

All these possibilities described in Table 1 support the choice of this board in our telemedicine application, which allows multiple other devices to connect with the Raspberry Pi.

B. MULTICHANNEL LEGENDRE-FOURIER MOMENTS OF FRACTIONAL-ORDER (MFrLFMs)

The color medical images are reshaped as a polar form g(r, θ) [29]. In which each image is represented by its channels using the intensity function.

$$f_c(\mathrm{r},\theta) = f_R(\mathrm{r},\theta), f_G(\mathrm{r},\theta), f_B(\mathrm{r},\theta)$$

The moments are computed with the following equation:

$$FrM_{pq}(f_c) = \frac{(2p+1)}{2\pi}\int_0^{2\pi}\int_0^1 f_c(r,\theta)[W_{pq}(r,\theta)] * rdrd\theta \tag{1}$$

The letter c represents each R, G, or B channel.

p : represent moment order, such that $|p| = 0, 1, 2, 3, \ldots.\infty$,

q : denotes the repetition, such that $|q| = 0, 1, 2, 3, \ldots\ldots\infty$. The function is

$$W_{pq}(r,\theta) = L_p(\alpha, r)e^{\hat{iq\theta}} \tag{2}$$

The functions $L_p(\alpha, r)$ refer to the fractional-order Legendre polynomials:

$$L_p(\alpha, r) = \sqrt{\alpha}\sum_{k=0}^{p} -1^{(p+k)}\frac{(p+k)!r^{\alpha k\frac{\alpha-2}{2}}}{(p-k)!\,(k!)^2} \tag{3}$$

Using equation (3) is time-consuming. Since,

The fractional-order Legendre rotation invariants forms are:

$$MFrM_{pq}(Rot) = e^{-iq\beta}MFrM_{pq}(Base) \tag{4}$$

From Equation (4):

$$\left|M_{(p,q)}f_c^{rot}\right| = \left|M_{p,q}f_c\right|, \quad C \in R, G, B \tag{5}$$

Equation (5) shows that the magnitude values of MFrLFMs do not affect by rotation.

The MFrLFMs scale invariants forms are:

$$\sum_{k=0}^{n} (FrM_{00}(F_c)^{(-(2i+3)/3)} C_{pi} d_{ik}) FrM_{kq}(f_c) \quad (6)$$

where coefficients C_{pi} and d_{ik} are [30]:

$$C_{pi} = (-1)^{(p+i)} \frac{(p+1)!}{(p-i)!\,(i!)^2} \quad (7)$$

$$d_{ik} = \frac{(2k+1)\,(i!)^2}{(i+k+1)!\,(i-k)!} \quad (8)$$

An accurate kernel-based framework presented in [31] was utilized to calculate MFrLFMs using the following equation:

$$FrM_{pq} = \frac{(2p+1)}{2\pi} \sum_i \sum_j I_p(r_i)\, J_q(\theta_{ij})\, \hat{f}_c(r, \theta_{ij}) \quad (9)$$

The interpolated function $\hat{f}_c(r, \theta_{ij})$ is calculated using cubic interpolation and intensity functions [32].

The radial and polar kernels in equation (10) are calculated based on equation (9):

$$J_q(\theta_{ij}) = \int_{V_{i,j}}^{V_{i,j+1}} e^{-\hat{i}q\theta} d\theta \quad (10)$$

$$I_p(r_i) = \int_{U_i}^{U_{i+1}} L_p(\alpha, r)\, rdr = \int_{U_i}^{U_{i+1}} R(r) dr \quad (11)$$

The kernel $Jq(\theta_{ij})$ is applied using integration:

$$J_q(\theta_{ij}) = \begin{cases} \frac{\hat{i}}{q}(e^{-\hat{i}qV_{i,j+1}} - e^{-\hat{i}qV_{i,j+1}}), & q \neq 0 \\ V_{i,j+1} - V_{i,j}, & q = 0 \end{cases} \quad (12)$$

C. TWO-DIMENSIONAL DISCRETE HENON MAP

It is considered an efficient scrambling algorithm to scramble the pixels of a given image. This scrambling algorithm utilizes the simplified model of the Lorenz model mentioned in [33], represented in the following equation:

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \quad (13)$$

where:

x, y represents continuous state variables.

a, b denotes control parameters.

n: no of iterations, such that n = 0, 1, 2 . . . .

A discrete Henon map was used by applying (2) to facilitate the processing.

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \; mod\; N \\ y_{n+1} = bx_n + c \; mod\; N \end{cases} \quad (14)$$

Such that:

x, y $\in \{0, 1, 2, \ N-1\}$ represents discrete state variables.

a, b, c denotes the control parameters.

N: is the order of the matrix

Equation (2) represents the equation used in the scrambling process, so the inverse scrambling of the Henon map is formulated in the following equation:

$$\begin{cases} x_n = y_{n+1} = bx_n - c \; mod\; N \\ y_n = x_{n+1} - 1 - ax_n^2 + y_n \end{cases} \quad (15)$$

III. PROPOSED ZERO-WATERMARKING SCHEME

The proposed model consists of two main phases: construction and verification. The moments are calculated for the original image to extract the most robust features in the construction phase and create the ownership share (zero watermarks). In the verification phase, the copyright is verified by comparing the extracted watermark and the stored copyright watermark. A detailed description of the proposed model phases is illustrated in this section.

A. ZERO WATERMARK CONSTRUCTION PHASE

The construction phase described in Fig. 3 is considered the first step in which the most important features are computed from the cover image to create the master share and then build the ownership share [12]. The generated ownership is stored in the certification authority (CA) to prove copyright in the future.

Master Share Construction:

Step 1: Split the original image into three R, G, and B channels to be ready for feature extraction.

Step 2: The moments' Calculation. Calculating the moments using Equation (1) [34] with Maximum moment = 45, and fractional parameter = 0.3. Applied for each channel of R, G, and B.

Step 3: Construct the feature vector ($F^{\rightarrow}$). After selecting the accurate MFrLFMs coefficients based on Xin *et al.* [35], they pointed out in their research that circular moments (m) with a negative value ($m < 0$) are not convenient for use in watermarking, the feature vector generated with size equal to the selected watermark image. Then, the feature vector is: generated with size $P \times Q$ the same size as the watermark image:

$$F^{*\rightarrow}{}_{R,G,B} = \{F^*{}_1, F^*{}_2, F^*{}_3, \ldots, F^*{}_{pxq}\}$$

Step 4: Feature Binarization, a binary feature vector $B^{\rightarrow}$ constructed using the selected feature matrix binarization.

$$B_{R,G,B}{}^{\rightarrow} = \{B_1, B_2, B_3, \ldots, B_{pxq}\}$$

Using the following binarization formula applied on the feature vector $F^{\rightarrow}$:

$$B_i = \begin{cases} 0, & A_i < T \\ 1, & A_i \geq T \end{cases}$$

Such that I = 1, 2, 3. . . . . , pxq, T: denotes the calculated threshold value (mean value of $F^{\rightarrow}$).

Step 5: Master share construction. The binarized vector is reformulated into a 2D feature image equal to the

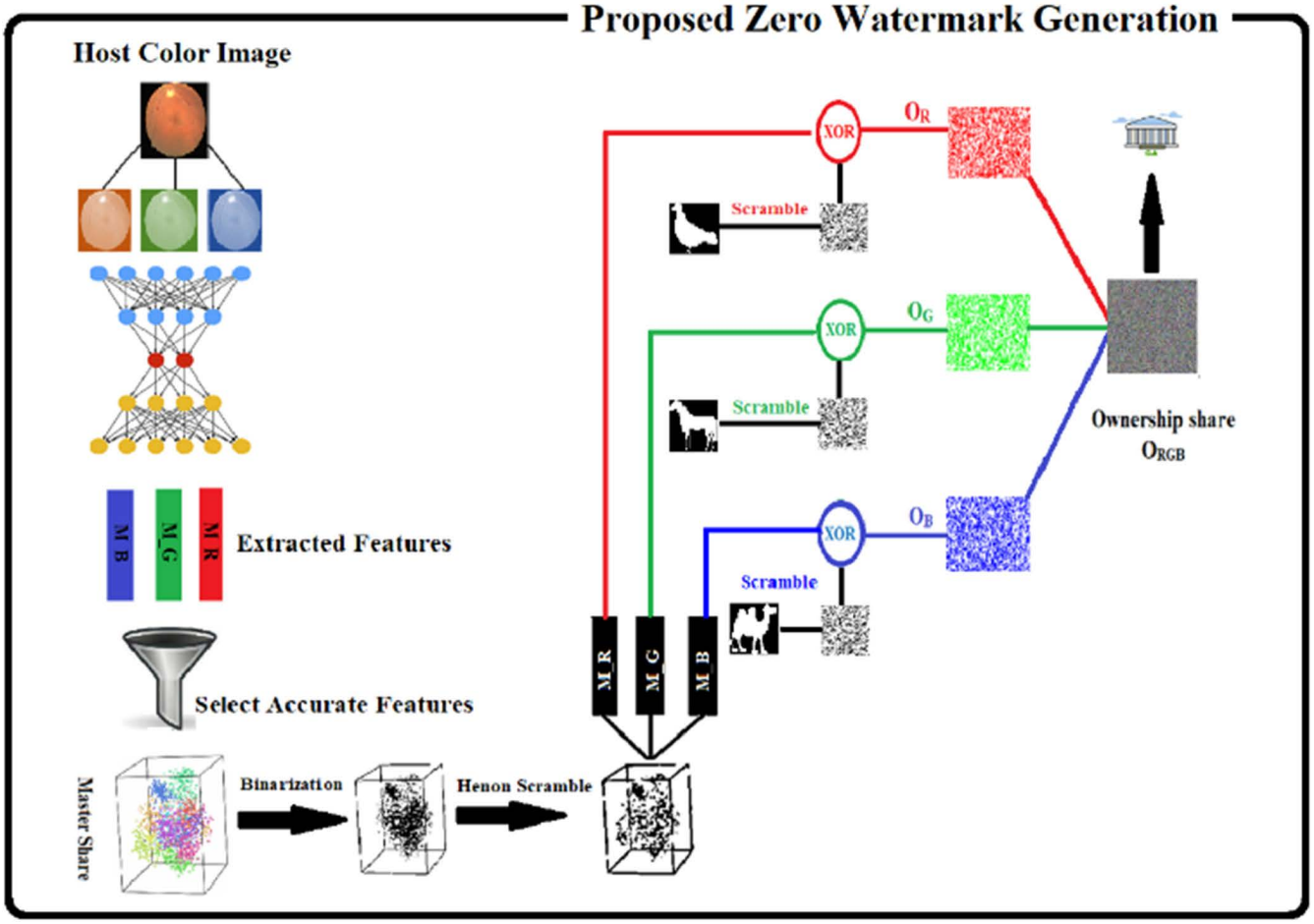


FIGURE 3. Proposed framework zero watermark generation phase.

binary watermark $P \times Q$, called the master share M_R, M_G, M_B.

Step 6: Scrambling the master share to remove the relation between the values of the moment matrix using Henon Map, M'_R, M'_G, M'_B.

Ownership Share Construction:

Step 7: Scrambling the binary watermark images for each channel to generate W'_R, W'_G, and W'_B. We choose three different binary watermark images for each channel using Discrete Henon Map as a scrambling algorithm to convert the watermark into an indistinct format. After checking whether the image is of size NxN or not. Set the discrete control parameter of:
a: an integer value not multiple of N and between 1 and 2^{128}.
b: is equal to 1.
c: value between 0 and 2^{128}.
t: the iteration time until we obtain the final 'scrambled image W'.

Step 8: Constructing the ownership (O_{RGB}). The scrambled master share XORed with scrambled watermark image.

$$O_{RGB} \begin{cases} M'_R \oplus W'_R \\ M'_G \oplus W'_G \\ M'_B \oplus W'_B \end{cases}$$

Finally, the ownership shares are stored in CA for copyright identification [36].

B. ZERO WATERMARK VERIFICATION PHASE

When the copyright proving is required, the watermark extracted from the disputed image is compared with the stored in certification authority, as shown in Fig. 4. The proposed algorithm considered a blind zero watermarking as only the attacked image is required to extract the watermark.

Step 1: Split the disputed image into three R, G, and B channels.

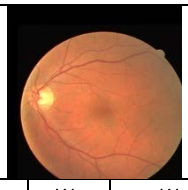
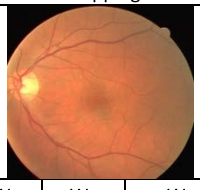
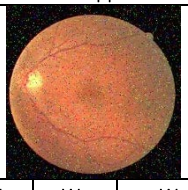
Step 2: MFrLFMs moments Calculation. Calculating the moments of the disputed image using the same construction equation.

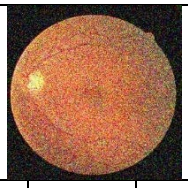
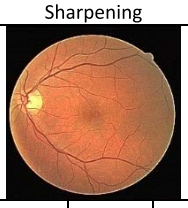
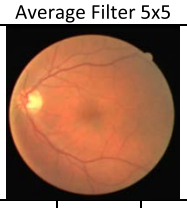
Step 3: Construct the disputed image's feature vector ($F^{*\rightarrow}$). Selecting the accurate MFrLFMs

TABLE 2. Binary watermark extraction and evaluation for fundus images.

Original Image

Attack	Rotation -90			Rotation 60			JPEG Compression 90			JPEG Compression 70		
Disputed Image												
Extracted Watermark	W_R	W_G	W_B	W_R	W_G	W_B	W_R	W_G	W_B	W_R	W_G	W_B
												
Average BER	0.00160			0.00163			0.00195			0.00216		
Average NC	0.99819			0.99796			0.99711			0.99174		
Average SSIM	0.99997			0.99996			0.99995			0.99979		
PSNR	26.8219			26.7956			30.5157			29.9941		

Attack	Translation			Cropping			Salt and Peppers 0.05			Median Filter 5x5		
Disputed Image												
Extracted Watermark	W_R	W_G	W_B	W_R	W_G	W_B	W_R	W_G	W_B	W_R	W_G	W_B
												
Average BER	0.00627			0.00394			0.00439			0.00752		
Average NC	0.95089			0.97855			0.98454			0.98571		
Average SSIM	0.99312			0.99852			0.99922			0.99914		
PSNR	29.0514			28.9720			36.4016			31.7259		

Attacks	Gaussian Noise 0.05			Speckle			Sharpening			Average Filter 5x5		
Disputed Image												
Extracted Watermark	W_R	W_G	W_B	W_R	W_G	W_B	W_R	W_G	W_B	W_R	W_G	W_B
												
Average BER	0.00472			0.00335			0.00157			0.00293		
Average NC	0.97844			0.9980			0.99785			0.99587		
Average SSIM	0.99571			0.99981			0.99912			0.99991		
PSNR	28.3718			27.2237			28.2100			29.8658		

coefficients.

$$F^{*\rightarrow}{}_{R,G,B} = \{F^*{}_1, F^*{}_2, F^*{}_3, ., F^*{}_{pxq}\}$$

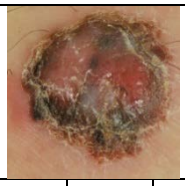
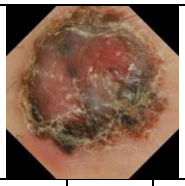
Step 4: Disputed Feature vector Binarization, generate the binary feature vector $B^{*\rightarrow}$ for the attacked image, same as the construction phase.

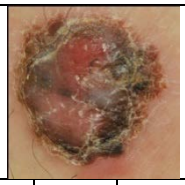
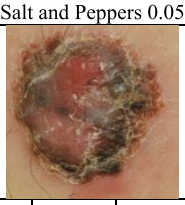
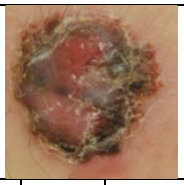
$$B^*{}_{R,G,B}{}^{\rightarrow} = \{B^*{}_1, B^*{}_2, B^*{}_3, \ldots\ldots\ldots, B^*{}_{pxq}\}$$

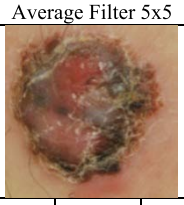
Step 5: Disputed Master share construction M'_R, M'_G, M'_B with size $P \times Q$.

TABLE 3. Binary watermark extraction and evaluation for melanoma images.

Original Image

Attack	Rotation -90			Rotation -45 with cropping			JPEG Compression 90			JPEG Compression 70		
Disputed Image												
Extracted Watermark	W_R	W_G	W_B	W_R	W_G	W_B	W_R	W_G	W_B	W_R	W_G	W_B
												
Average BER	0.00391			0.00479			0.00257			0.00223		
Average NC	0.99510			0.98624			0.99841			0.99755		
Average SSIM	0.99971			0.99876			0.99981			0.99954		
PSNR	26.0819			25.5697			29.0682			28.1661		

Attack	Translation			Cropping			Salt and Peppers 0.05			Median Filter 5x5		
Disputed Image												
Extracted Watermark	W_R	W_G	W_B	W_R	W_G	W_B	W_R	W_G	W_B	W_R	W_G	W_B
												
Average BER	0.00637			0.00354			0.00429			0.00792		
Average NC	0.95189			0.98855			0.98354			0.97571		
Average SSIM	0.99212			0.99752			0.99932			0.99814		
PSNR	26.7680			25.6087			35.2298			28.2575		

Attacks	Gaussian Noise 0.05			Speckle Noise			Sharpening			Average Filter 5x5		
Disputed Image												
Extracted Watermark	W_R	W_G	W_B	W_R	W_G	W_B	W_R	W_G	W_B	W_R	W_G	W_B
												
Average BER	0.00463			0.00325			0.00156			0.00291		
Average NC	0.98744			0.9960			0.99773			0.99677		
Average SSIM	0.99471			0.99971			0.99944			0.99981		
PSNR	27.2361			25.9404			26.1643			27.1923		

Step 6: Scrambling the disputed master share $M'_R{}^*$, $M'_G{}^*$, $M'_B{}^*$.

Step 7: A scrambled watermark extraction. (XOR) operation is applied between the scrambled master

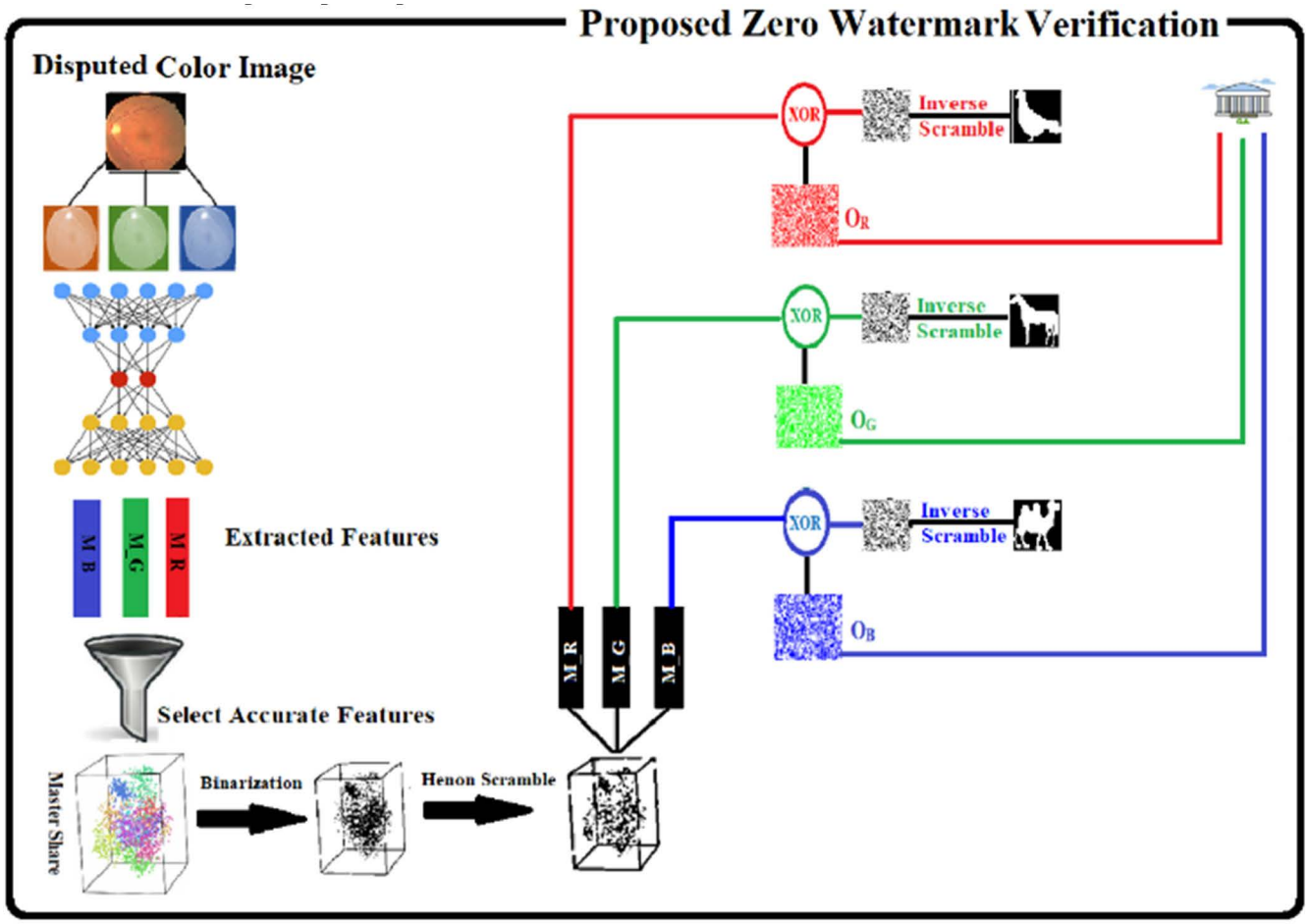


FIGURE 4. Proposed framework zero watermark verification phase.

share of disputed and the retrieved ownership share from CA.

$$\begin{matrix} W'_R{}^* \\ W'_G{}^* \\ W'_B{}^* \end{matrix} \begin{cases} M'_R{}^* \oplus O_R \\ M'_G{}^* \oplus O_G \\ M'_B{}^* \oplus O_B \end{cases}$$

Step 8: Recover of verifiable watermark image. In this step, the invertible Henon map is applied, which is inverse scrambling defined by Equation (3) by the same number of scrambling iterations.

IV. EXPERIMENTS AND RESULT

The authors executed all experiments on a Model B Raspberry Pi 4; our algorithm was applied to color medical images with 256 × 256 shown in Fig. 5. Nine binary images of size 32 × 32 are shown in Fig. 6 used as watermarks.

Each color medical image has different features. So, the color medical image, ''Fundus,'' of size 256 × 256, is considered the base image. Fundus images contain fine details such as optic disks, macula, and blood vessels, essential in diagnosis. The binary images ''Horse,'' ''Camel,'' and ''Elephant'' of 32 × 32 were selected as the watermark for R, G, and B channels, respectively. The results of each attack are shown in Table 2. Additional experiment applied on ''melanoma'' medical image of size 256 × 256 in Fig. 5, with same watermark images, and the results are presented in Table 3.

TABLE 4. Comparison of computation time for the proposed scheme and existing methods.

Algorithm	Average generation time(sec)	Average verification time(sec)
Xia et al [40]	32.631	33.205
Xiaoping et al [18]	43.079	43.815
Xiaoping et al [41]	42.186	42.761
Proposed Method	22.716	23.234

A. PERFORMANCE EVALUATION METRICS

For evaluation, the robustness of the proposed algorithm is measured by the normalized correlation (NC) [37]. NC is used in calculating the similarity between the original and the extracted watermark image. It can be mathematically

TABLE 5. BER and NC values of distorted watermark.

Attacks		Evaluation Metric	Xia et al [40]	Xiaoping et al [18]	Xiaoping et al [41]	Proposed Method
Rotation	35°	BER	0.0153	0.0268	0.0273	0.00260
		NC	0.9810	0.9648	0.9645	0.99653
	25°	BER	0.0213	0.0283	0.0285	0.00391
		NC	0.9738	0.9645	0.9639	0.99478
	15°	BER	0.0135	0.0190	0.0192	0.00163
		NC	0.9836	0.9739	0.9736	0.99766
Translation	(3,3)	BER	0.0114	0.0204	0.0206	0.00536
		NC	0.9739	0.9579	0.9576	0.98231
Compression	90%	BER	0.0089	0.0113	0.0119	0.00257
		NC	0.9896	0.9866	0.9862	0.99841
	70%	BER	0.0097	0.0115	0.0118	0.00223
		NC	0.9886	0.9856	0.9853	0.99755
Salt and Pepper	0.03	BER	0.0131	0.0143	0.0145	0.00429
		NC	0.9843	0.9804	0.9801	0.98354
Gaussian Noise	0.03	BER	0.0128	0.0254	0.0258	0.00443
		NC	0.9838	0.9675	0.9669	0.98744
Median Filter	5x5	BER	0.0134	0.0183	0.0186	0.00792
		NC	0.9842	0.9778	0.9774	0.97571

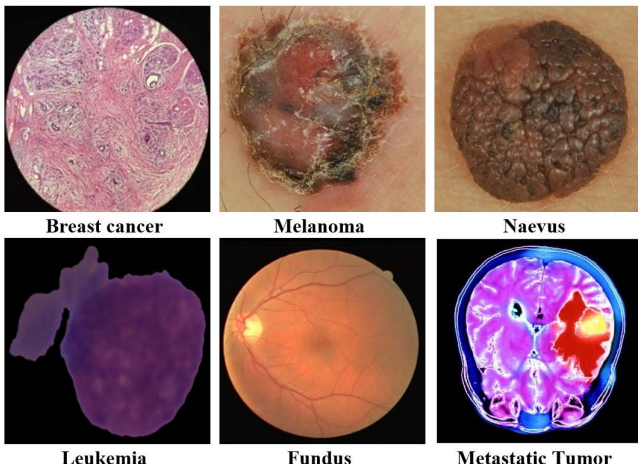


FIGURE 5. Selected color medical images used in experiments.

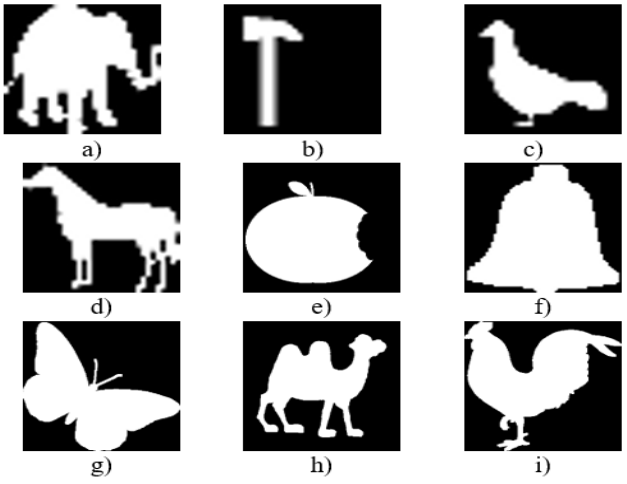


FIGURE 6. 32 × 32 binary watermark images.

represented as

$$NC = \frac{\sum_{I=1}^{X}\sum_{J=1}^{Y}\left(W_{orgij} \times W_{recij}\right)}{\sum_{I=1}^{X}\sum_{J=1}^{Y}\left(W_{org-ij^2}\right)}$$

The bit error rate (BER) [38] used in the evaluation coefficient values small as possible. Ideally = 0. It can be mathematically represented as

$$BER = \frac{\text{number of incorrectly decodedbits}}{\text{Total number of bits}}$$

The structural similarity index measure (SSIM) [39] measures the similarity between the original and the extracted

watermark coefficient values ranging from 0 to +1. Ideally = 1, its mathematical equation represented as

$$SSIM\ (x, y) = \frac{(2\mu_x\mu_y c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

Also, the Peak Signal to Noise Ratio (PSNR) [37] criteria are used to know how the watermarked image and the original image are similar. A high PSNR value means a high similarity. It is represented as,

$$\text{PSNR} = 10_{\log}\frac{(255)^2}{\text{MSE}}$$

where

$$\text{MSE} = \frac{1}{\text{X} \times \text{Y}}\sum_{\text{i}=1}^{\text{X}}\sum_{\text{j}=1}^{\text{Y}}(\text{I}_{\text{ij}} - \text{W}_{\text{ij}})^2$$

B. WATERMARK EXTRACTION

V. DISCUSSION

A. SIMILAR ZERO WATERMARKING ALGORITHMS

The experimental results showed that the extracted watermarks from the attacked images are successfully extracted with the least distortion and very close to the original one, and the SSIM, BER, and NC values tend to be the ideal values, which indicates that our scheme can prove the copyright even if the image is exposed to different significant distortions.

B. COMPUTATIONAL TIME

The computational time of the proposed algorithm is measured for the watermark construction and verification process. The average computation times for the six test images (shown in Fig. 5) with a size of 256 × 256 are presented in Table 4 and compared with existing methods. It was observed that the time consumed by the proposed scheme is less than others in both construction and verification and is highly recommended for a real-time telemedicine application.

VI. CONCLUSION AND FUTURE WORK

This paper proposed a low-cost multiple zero watermarking model to secure medical images in telemedicine applications. Our proposed algorithm is based on extracting the most robust and accurate MFrLFMs moments and scrambling with a Two-Dimensional Discrete Henon Map algorithm. The proposed model was operated on a Raspberry Pi system kit.

The proposed model was tested on some medical images. Experimental results verified that the proposed model is robust, which gives low BER values and high N.C and SSIM values compared with other techniques. In the future, we will use a selection algorithm to select more accurate moments, using machine learning techniques for feature extraction. Also, using an encryption algorithm may increase the robustness. Some common image processing and geometric attacks are applied for algorithm evaluation.

REFERENCES

[1] M. Ciotti, M. Ciccozzi, A. Terrinoni, W. C. Jiang, C. B. Wang, and S. Bernardini, "The COVID-19 pandemic," *Crit. Rev. Clin. Lab. Sci.*, vol. 57, no. 6, pp. 365–388, 2020.
[2] M. Ali, "A survey of the most current image encryption and decryption techniques," *Int. J. Adv. Res. Comput. Sci.*, vol. 10, no. 1, pp. 9–14, Feb. 2019.
[3] Y. Tan, J. Qin, L. Tan, H. Tang, and X. Xiang, "A survey on the new development of medical image security algorithms," in *Proc. Int. Conf. Cloud Comput. Secur.*, in Lecture Notes in Computer Science, vol. 11065. Cham, Switzerland: Springer, 2018, pp. 458–467.
[4] S. Dhawan and R. Gupta, "Analysis of various data security techniques of steganography: A survey," *Inf. Secur. J., Global Perspective*, vol. 30, no. 2, pp. 63–87, Mar. 2021.
[5] B. Meryem and M. Samira, "A short survey on image zero-watermarking techniques based on visual cryptography," in *Proc. 9th Int. Symp. Signal, Image, Video Commun. (ISIVC)*, Nov. 2018, pp. 157–162.
[6] K. M. Hosny, M. M. Darwish, and M. M. Fouda, "New color image zero-watermarking using orthogonal multi-channel fractional-order Legendre–Fourier moments," *IEEE Access*, vol. 9, pp. 91209–91219, 2021.
[7] W. Quan, S. Tanfeng, and S.-X. Wang, "Concept and application of zero-watermark," *Acta Electron Sinica*, vol. 31, no. 2, pp. 214–216, 2003.
[8] L. Vinicius and R. Jordan, "Geometric attacks on image watermarking systems," *IEEE Multimedia*, vol. 12, no. 3, pp. 68–78, Jul. 2005.
[9] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su, "Attacks on digital watermarks: Classification, estimation based attacks, and benchmarks," *IEEE Commun. Mag.*, vol. 39, no. 8, pp. 118–126, Aug. 2001.
[10] D. Storcheus, A. Rostamizadeh, and S. Kumar, "A survey of modern questions and challenges in feature extraction," in *Proc. Feature Extraction, Mod. Questions Challenges*, Dec. 2015, pp. 1–18.
[11] P. Kaur, H. S. Pannu, and A. K. Malhi, "Comprehensive study of continuous orthogonal moments—A systematic review," *ACM Comput. Surv.*, vol. 52, no. 4, pp. 1–30, Jul. 2020.
[12] H. Nyeem, W. Boles, and C. Boyd, "A review of medical image watermarking requirements for teleradiology," *J. Digit. Imag.*, vol. 26, no. 2, pp. 326–343, Apr. 2013.
[13] S. G. Shini, T. Thomas, and K. Chithraranjan, "Cloud based medical image exchange-security challenges," *Proc. Eng.*, vol. 38, pp. 3454–3461, Jan. 2012.
[14] 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," *Appl. Intell.*, vol. 52, pp. 1–15, May 2021.
[15] H. Zhang, Z. Li, and Y. Liu, "Fractional orthogonal Fourier–Mellin moments for pattern recognition," in *Proc. Chin. Conf. Pattern Recognit.* Singapore: Springer, 2016, pp. 766–778.
[16] 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.
[17] 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.
[18] 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.
[19] 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.
[20] W. Wang, Y. Li, and S. Liu, "A polar complex exponential transform-based zero-watermarking for multiple medical images with high discrimination," *Secur. Commun. Netw.*, vol. 2021, pp. 1–13, Mar. 2021.
[21] G. J. Joyia, R. M. Liaqat, A. Farooq, and S. Rehman, "Internet of medical things (IOMT): Applications, benefits and future challenges in healthcare domain," *J. Commun.*, vol. 12, no. 4, pp. 240–247, 2017.
[22] S.-Y. Ge, S.-M. Chun, H.-S. Kim, and J.-T. Park, "Design and implementation of interoperable IoT healthcare system based on international standards," in *Proc. 13th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2016, pp. 119–124.
[23] N. John, R. Surya, R. Ashwini, S. S. Kumar, and K. P. Soman, "A low cost implementation of multi-label classification algorithm using mathematica on Raspberry Pi," *Proc. Comput. Sci.*, vol. 46, pp. 306–313, Jan. 2015.
[24] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, and D. Cournapeau, "Scikit-learn: Machine learning in Python," *J. Mach. Learn. Res.*, vol. 12, no. 85, pp. 2825–2830, 2011.

[25] R. Chandra, L. Dagum, D. Kohr, R. Menon, D. Maydan, and J. McDonald, *Parallel Programming in OpenMP*. San Mateo, CA, USA: Morgan Kaufmann, 2001.
[26] W. Gropp, R. Thakur, and E. Lusk, *Using MPI-2: Advanced Features of the Message Passing Interface*. Cambridge, MA, USA: MIT Press, 1999.
[27] V. Govindaraj, "Parallel programming in Raspberry Pi cluster. A design project report," M.S. thesis, Dept. Elect. Comput. Eng., School Elect. Comput. Eng., Cornell Univ., Ithaca, NY, USA, Tech. Rep., 2016.
[28] G. Bernabé, R. Hernández, and M. E. Acacio, "Parallel implementations of the 3D fast wavelet transform on a Raspberry Pi 2 cluster," *J. Supercomput.*, vol. 74, no. 4, pp. 1765–1778, Apr. 2018.
[29] 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.
[30] K. M. Hosny and M. M. Darwish, "Invariant color images representation using accurate quaternion Legendre–Fourier moments," *Pattern Anal. Appl.*, vol. 22, no. 3, pp. 1105–1122, Aug. 2019.
[31] K. M. Hosny and M. M. Darwish, "A kernel-based method for fast and accurate computation of PHT in polar coordinates," *J. Real-Time Image Process.*, vol. 16, no. 4, pp. 1235–1247, 2019.
[32] K. M. Hosny, M. A. Shouman, and H. M. A. Salam, "Fast computation of orthogonal Fourier–Mellin moments in polar coordinates," *J. Real-Time Image Process.*, vol. 6, no. 2, pp. 73–80, Jun. 2011.
[33] M. Henon, "A two-dimensional mapping with a strange attractor," *Commun. Math. Phys.*, vol. 50, no. 1, pp. 69–77, 1976.
[34] 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.
[35] 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.
[36] A. Roček, M. Javorník, K. Slavíček, and O. Dostál, "Zero watermarking: Critical analysis of its role in current medical imaging," *J. Digit. Imag.*, vol. 34, no. 1, pp. 204–211, Feb. 2021.
[37] J. D. Faires and R. L. Burden, *Numerical Methods*, 3rd ed. Pacific Grove, CA, USA: Brooks Cole Publication, 2002.
[38] 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.
[39] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *J. Sel. Areas Telecommun.*, vol. 1, pp. 31–38, Apr. 2011.
[40] 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.
[41] Z. Xia, X. Wang, B. Han, Q. Li, X. Wang, C. Wang, and T. Zhao, "Color image triple zero-watermarking using decimal-order polar harmonic transforms and chaotic system," *Signal Process.*, vol. 180, Mar. 2021, Art. no. 107864.