Hindawi
International Journal of Biomedical Imaging
Volume 2018, Article ID 2572431, 11 pages
https://doi.org/10.1155/2018/2572431

Research Article

Medical Image Blind Integrity Verification with Krawtchouk Moments

Xu Zhang[1], **Xilin Liu**[1,2] **Yang Chen**[1] **and Huazhong Shu**[1,3,4]

[1]*Laboratory of Image Science and Technology, Southeast University, Nanjing 210096, China*
[2]*College of Data Science, Taiyuan University of Technology, Taiyuan 030024, China*
[3]*Centre de Recherche en Information Biomédicale Sino-Français, Nanjing 210096, China*
[4]*International Joint Research Laboratory of Information Display and Visualization, Southeast University, Ministry of Education, Nanjing 210096, China*

Correspondence should be addressed to Huazhong Shu; shu.list@seu.edu.cn

Received 15 August 2017; Revised 19 November 2017; Accepted 31 May 2018; Published 2 July 2018

Academic Editor: Lizhi Sun

A new blind integrity verification method for medical image is proposed in this paper. It is based on a new kind of image features, known as Krawtchouk moments, which we use to distinguish the original images from the modified ones. Basically, with our scheme, image integrity verification is accomplished by classifying images into the original and modified categories. Experiments conducted on medical images issued from different modalities verified the validity of the proposed method and demonstrated that it can be used to detect and discriminate image modifications of different types with high accuracy. We also compared the performance of our scheme with a state-of-the-art solution suggested for medical images—solution that is based on histogram statistical properties of reorganized block-based Tchebichef moments. Conducted tests proved the better behavior of our image feature set.

1. Introduction

With the development of eServices such as eHealth, eCommerce, and eLearning, a huge amount of digital information, such as images and videos, is transmitted over the internet. However, as data sharing is facilitated and accelerated, data security needs also increase. In particular, data reliability is of major concern. It is the key of trust one can have in the data he or she received. Taking eHealth as an example, a lot of medical information and images are exchanged through the internet between health professionals [1]. Herein, medical images already play an important role in teleradiology and telesurgery applications, for the identification of potential diseases as well as for therapy. Indeed, medical images convey many details and specific pieces of image information that can be raised up to physicians via the tools of image processing techniques [2]. However, such frameworks are often sensitive to various kinds of threats. Particularly, data can be intercepted and modified for illegal and malevolent purposes ranging from the patient life endangerment to the wrongful accusation of health professionals or medical institutions [3]. Therefore, data should be proven trustworthy before being exploited.

Regarding the trustworthy of medical images, two aspects are usually considered. One is the image integrity and the other is image authenticity. The image integrity verification consists in the detection (and even prevention or correction) of image degradation or alteration, while the authenticity verification allows for determination of authorship of medical images [4]. Various strategies have been applied to verify the integrity and authenticity of images. One class of techniques is based on image signature [5–7]. To verify the integrity, one just has to compare the signature shared along with the image with the one computed by the user from the image he received. Any difference would alert the user about an integrity loss. An aspect of consideration for such an approach is where to store the signature. One strategy stands in using image file headers, as proposed in the DICOM standard Part 15 [8]. However, commercial implementation of the DICOM standard is not always in compliance with Part 15 specification. Moreover, trustworthy

verification might fail if image signature is deleted from the image DICOM file [4]. Another approach is based on watermarking, which allows embedding the signature into the image itself by imperceptibly modifying the gray values in images. The main drawback of watermarking methods is the possible induced image degradation that can endanger the image's diagnostic value [5]. The last class employs blind forensics techniques. These techniques do not require any additional image information besides the image itself to detect whether it has been modified or not [9]. Many blind forensics methods have been proposed for the detection of various modifications of natural images including noise addition [10], median filtering [11], copy-move modification [12, 13], JPEG compression [14]. Notice that blind forensics techniques can also be used for image steganalysis purpose, that is, to detect whether an image has been modified so as to dissimulate a secret message in between spies [15–18]. These methods can thus detect subtle image modifications if correctly designed. For verifying medical image integrity and further identifying the type of modification, very few methods have been proposed for medical images. Huang et al. [19] recently proposed a scheme in which a set of image features that are sensitive to modification is generated before being submitted to a classifier for image integrity verification. These features are derived from the histogram statistical properties of reorganized block-based Tchebichef moments (HRBT).

It is known that Krawtchouk moments have better image reconstruction performance than Tchebichef moments [20, 21] and have already find applications in image recognition [22] and fractional transform domain construction [23]. Therefore, in this work, we propose to take advantage of them so as to build a new feature set in which the features are extracted from the histogram statistical properties of reorganized block-based Krawtchouk moments (HRBK). The proposed features can be applied for medical image integrity verification and further applied for image modification classification with better accuracy than with Tchebichef moments. The rest of this paper is organized as follows. Section 2 reviews the definition and some properties of the Krawtchouk moments. The HRBK feature generation procedure is described in Section 3. Some experimental results on image integrity verification with HRBK and its comparison with HRBT are given in Section 4. Section 5 concludes the paper.

2. Krawtchouk Moments

Let $f(x)$ be one-dimensional signal in length N, the 1D Krawtchouk transform in terms of weighted Krawtchouk polynomial is defined as in [21]:

$$\mathbf{Q}_n = \sum_{x=0}^{N-1} K_n(x; p, N-1)\, f(x), \quad n = 0, 1, \ldots, N-1, \tag{1}$$

where $K_n(x; p, N-1)$ is the nth order weighted Krawtchouk polynomial, defined as

$$K_n(x; p, N-1) = \kappa_n(x; p, N-1) \sqrt{\frac{w(x; p, N-1)}{\rho(n; p, N-1)}}. \tag{2}$$

Here, the weighting coefficient $w(x;p,N\text{-}1)$ and normalization coefficient $\rho(n;p,N\text{-}1)$ are defined as

$$w(x; p, N-1) = \binom{N-1}{x} p^x (1-p)^{N-1-x}. \tag{3}$$

$$\rho(n; p, N-1) = \left(\frac{p-1}{p}\right)^n \frac{n!}{(-N+1)_n} \tag{4}$$

$\kappa_n(x; p, N-1)$ is the classical Krawtchouk polynomial:

$$\kappa_n(x; p, N-1) = {}_2F_1\left(-n, -x; -N+1; \frac{1}{p}\right), \quad p \in (0, 1). \tag{5}$$

${}_2F_1$ is the hypergeometric function:

$${}_2F_1(a, b; c; z) = \sum_{k=0}^{\infty} \frac{(a)_k (b)_k}{(c)_k} \frac{z^k}{k!}. \tag{6}$$

$(a)_k$ is the Pochhammer symbol:

$$(a)_k = a(a+1)\cdots(a+k-1) = \frac{\Gamma(a+k)}{\Gamma(a)}. \tag{7}$$

The weighted Krawtchouk polynomial $K_n(x; p, N-1)$ satisfies the following orthogonality property:

$$\sum_{x=0}^{N-1} K_n(x; p, N-1)\, K_m(x; p, N-1) = \delta_{nm}. \tag{8}$$

With the above orthogonality property, the signal can be reconstructed with the following inverse transform:

$$f(x) = \sum_{n=0}^{N-1} \mathbf{Q}_n K_n(x; p, N-1). \tag{9}$$

For an $N\times N$ image $g(x, y)$, the two-dimensional Krawtchouk moments are defined as

$$\mathbf{Q}_{nm} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} K_n(x; p, N-1)\, K_m(y; q, N-1)\, g(x, y) \tag{10}$$

and its inverse transform is given by

$$g(x, y) = \sum_{n=0}^{N-1} \sum_{m=0}^{N-1} \mathbf{Q}_{nm} K_n(x; p, N-1)\, K_m(y; q, N-1). \tag{11}$$

3. Proposed Blind Image Forensics

In order to blindly detect whether a medical image has been modified by some global image processing techniques (e.g., filtering, lossy image compression) and further identify the

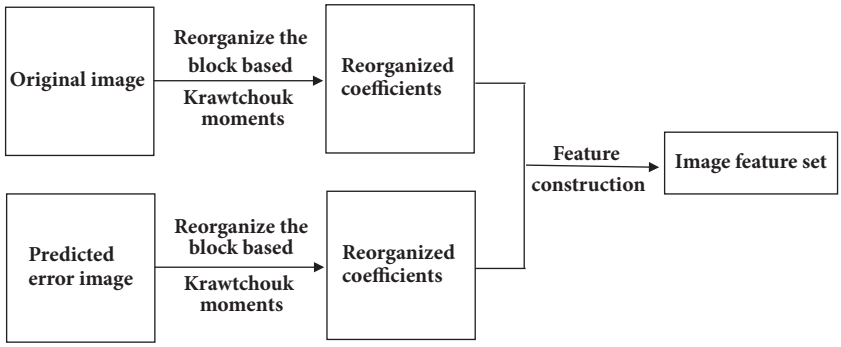

Figure 1: Proposed image feature generation procedure.

type of modification, two issues should be addressed: (1) a set of image features should be designed to distinguish original images from modified ones; (2) a classifier model needs to be built to predict the integrity of an input image. In our work, the support vector machine (SVM) is used as classifier mainly because it has been shown that, for classification problems, SVM based solutions outperform traditional neural network approaches, such as multilayer perceptron (MLP) and radial basis functions [24, 25]. The remaining issue is thus to construct an image feature set that is sensitive to the image modifications one wants to detect and identify. In this work, histogram statistical properties of reorganized block-based Krawtchouk moments are exploited to design this feature set. This approach is developed based on the fact that low order Krawtchouk moments often have better image reconstruction performance than Tchebichef moments [21, 22] do, indicating as a consequence that most of the image energy is compacted into these low order moments. As a result, it is reasonable to extend the strategy proposed in [19] to Krawtchouk moments with some improvements taking advantage of the specificities of Krawtchouk moments. Figure 1 shows the schematic diagram of the extraction process of our features, which we elaborate in detail in the following part of this section.

Firstly, the image is divided into $n \times n$ nonoverlapping blocks and the Krawtchouk moments of each block are computed. In each block, Krawtchouk moments are partitioned into $3L+1$ ($n = 2^L$) subbands. Then the coefficients of the same subband in each block are grouped together to generate an L-scale coefficient tree for the whole image. In our experiments, we considered $n = 8$. As shown in Figure 2, one moment block is thus divided into 10 subbands. Figure 3 illustrates the corresponding L-scale coefficient tree for the whole image, where the coefficients of the same subband i ($i = 0, 1, \ldots, 9$) from all blocks are reorganized into the group G_i.

Contrarily to [19], in order to emphasize the Krawtchouk moment statistical variations under modifications, we further divide coefficients groups G_7, G_8, and G_9 as illustrated in Figure 4. At last, all the block-based Krawtchouk moments are reorganized into 25 groups. The detailed way of reorganizing the Krawtchouk moment block can be found in [18].

Once Krawtchouk moments are reorganized, the image features can be generated. The first class of features we use

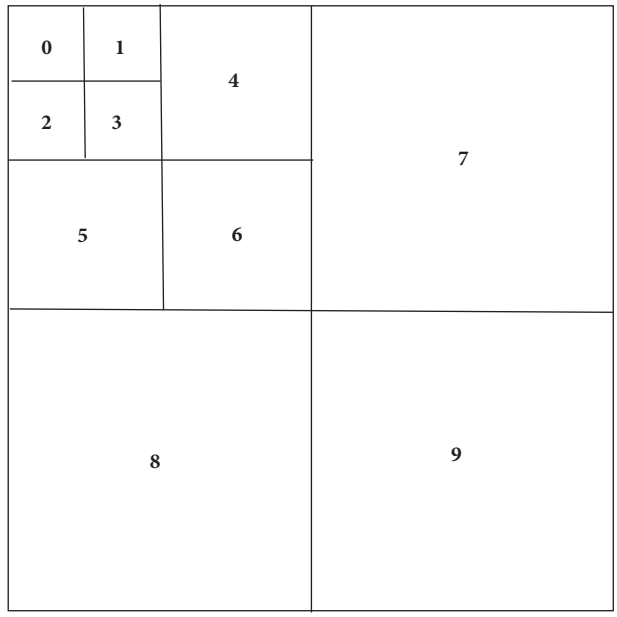

Figure 2: Ten subbands of Krawtchouk moments for one image block of 8×8 pixels.

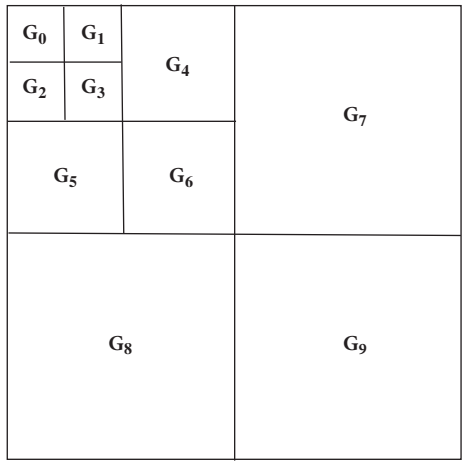

Figure 3: Reorganized coefficients of all 8×8 Krawtchouk moment blocks for the whole image.

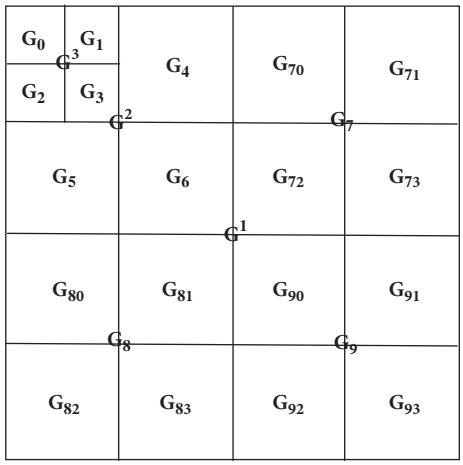

Figure 4: Reorganized Krawtchouk moment coefficients.

corresponds to the statistical moments of the discrete Fourier transform (DFT) of histogram of one Krawtchouk moment subband [15]:

$$M_1 = \frac{\left(\sum_{k=0}^{K/2} k\,|H(k)|\right)}{\sum_{k=0}^{K/2} |H(k)|} \tag{12}$$

$$M_2 = \frac{\left(\sum_{k=0}^{K/2} k^2\,|H(k)|\right)}{\sum_{k=0}^{K/2} |H(k)|} \tag{13}$$

$$M_3 = \frac{\left(\sum_{k=0}^{K/2} k^3\,|H(k)|\right)}{\sum_{k=0}^{K/2} |H(k)|} \tag{14}$$

where $H(k)$ is the DFT coefficient at frequency k in the histogram of one subband of reorganized Krawtchouk moment transform coefficients. As it can be seen, features defined in (12)-(14) act as high-pass filters for the histogram. In order to take advantage of the rest of frequency information of the histogram, the second class of features obtained is defined as [26]

$$F_1 = \sum_{k=0}^{K/2} |H(k)| \sin\left(\frac{\pi k}{K}\right) \tag{15}$$

$$F_2 = \sum_{k=0}^{K/2} |H(k)| \sin^2\left(\frac{\pi k}{K}\right) \tag{16}$$

$$F_3 = \sum_{k=0}^{K/4} |H(k)| \sin\left(\frac{\pi k}{K}\right). \tag{17}$$

In addition to these two classes of features generated from the original image, features are also generated from the prediction error image. The basic idea is to achieve a second set of features that is more image content independent. Let $g_{i,j}$ be an image pixel at position (i, j). In this work, its predicted value $g_{i,j}$ is defined as [27]

$$g'_{i,j} = \begin{cases} \max\left(g_{i,j+1}, g_{i+1,j}\right), & g_{i+1,j+1} \le \min\left(g_{i,j+1}, g_{i+1,j}\right) \\ \min\left(g_{i,j+1}, g_{i+1,j}\right), & g_{i+1,j+1} \ge \max\left(g_{i,j+1}, g_{i+1,j}\right) \\ g_{i,j+1} + g_{i+1,j} - g_{i+1,j+1}, & \text{otherwise.} \end{cases} \tag{18}$$

Afterwards, the prediction error image is constructed by subtracting the predicted image from the original one, that is, $g - g'$.

Finally, the feature set $\{M_1, M_2, M_3, F_1, F_2, F_3\}$ are extracted from the 25 groups of the reorganized Krawtchouk moments of the original image, giving access to a first set of 150 features. Regarding the prediction error image, the twelve subbands, $G_{70} \sim G_{73}$, $G_{80} \sim G_{83}$, $G_{90} \sim G_{93}$, are not exploited because the coefficients in these subbands are of very small values and are insignificant for image description purpose, so only 78 image features are extracted from the prediction error image. To conclude, one image will be represented or summarized by a feature vector of 228 components which are used to train the SVM classifier for discriminating the original images from the modified ones, as well as to identify the kind of modification (e.g., filtering, lossy compression).

4. Experimental Results and Discussion

In order to verify the validity of the proposed image feature set for medical image blind verification, two medical image datasets in different imaging modalities were used. The performance of our features is compared with performance of those features proposed in [19] which are based on Tchebichef moments. We detail and discuss some experimental results in this section.

4.1. Test Data, Modifications, and Test Parameterization. Our image datasets consist of medical images issued from two modalities: (1) 100 computed tomography (CT) images of size 512×512, 12 bits encoded; (2) 100 magnetic resonance (MR) images of size 181×181, encoded onto 12 bits [28, 29]. Some samples of these two test datasets are illustrated in Figure 5. Notice that the features are generated from the 128×128 image block centered in each image. To make a fair comparison with the method proposed in [19], we used the same types of image modifications. That is, seven types of common image modifications were considered: JPEG2000 compression, Gaussian filtering, Laplacian filtering, brightening, scaling up, histogram equalization, and JPEG compression. For each type of modifications, five different modification intensities were considered. The detailed parameters that correspond to each modification type are listed in Table 1.

In the following experiments, the 100 original images of each modality along with their modified versions were divided into two groups. One group was used as the training set of SVM classifier and the other used for SVM testing. Training and testing sets were randomly generated. It is

Table 1: Image modification types and their parameterizations.

Modification	Values of parameters
JPEG2000	Compression rate: 2:1, 4:1, 6:1, 8:1, 10:1
Gaussian filtering	Standard deviation: 0.3, 0.5, 1, 2, 3
Laplacian filtering	Shape parameter: 0.1, 0.3, 0.5, 0.7, 0.9
Brightening	Ratio: 0.1, 0.3, 0.5, 0.7, 0.9
Scaling up (%)	Scaling up parameter: 5, 10, 15, 20, 25
Histogram equalization	Discrete level: 2^{11}, 2^{10}, 2^{9}, 2^{8}, 2^{7}
JPEG	Quality factor: 95, 90, 85, 80, 75

Table 2: Modification detection rates (%) with HRBT and HRBK features.

	CT image dataset		MR image dataset	
Modification	HRBT	HRBK	HRBT	HRBK
JPEG2000	67.13	67.17	74.07	76.77
Gaussian filtering	80.23	80.37	77.77	78.60
Laplacian filtering	100	100	100	100
Brightening	97.67	98.90	97.57	97.50
Scaling	99.33	100	97.63	99.20
Histogram equalization	100	100	100	100
JPEG compression	82.10	100	89.43	87.47
All attacks	96.70	96.80	97.03	97.07

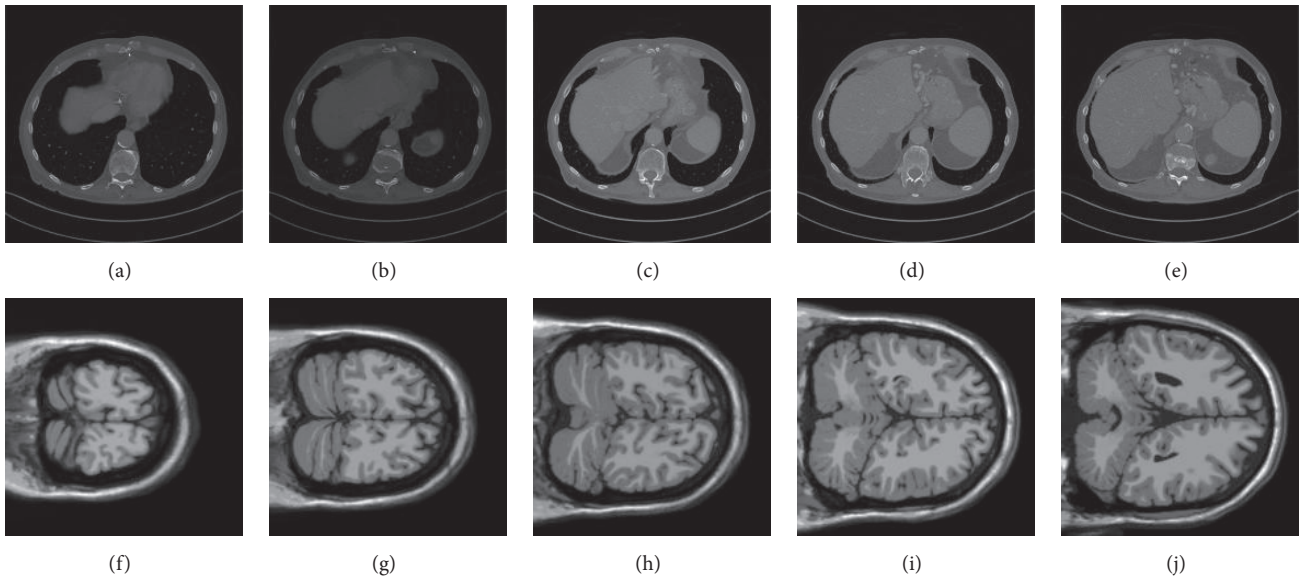

Figure 5: Image samples from our experiments: (a)–(e) CT images, (f)–(i) MR images.

important to notice that the following experimental results are given in average after ten rounds of training and testing.

4.2. Detection of Image Modification. In this experiment, the objective was to discriminate the original images from the modified ones using the proposed HRBK features. In the first test, each modification type described in Section 4.1 was treated separately. For each modification type, fifty original test images and their modified ones, that is to say, three hundred images (50 originals and 250 modified images corresponding to 5 different intensities; see Table 1), were used to train an SVM classifier. The rest of the original images and their corresponding modified images were then exploited as the test set. The detection rates for each type of modifications are provided in Table 2. As it can be seen, the proposed scheme was able to detect all types of modifications with higher accuracy than the cases with HRBT features.

In the second test, all types of modifications were considered together, the objective was to discriminate the original images from the modified ones. Again, fifty original test

Table 3: Detection rates (%) with HRBT and HRBK features for different modification parameterizations (MR image dataset).

Modification		Modification detection rates (%)				
JPEG2000	HRBT:	43.33	54.93	60.60	71.07	73.87
	HRBK:	43.47	64.20	76.13	85.13	89.80
Gaussian filtering	HRBT:	46.40	91.13	99.53	99.47	99.33
	HRBK:	44.93	92.93	99.07	99.60	99.33
Laplacian filtering	HRBT:	100	100	100	100	100
	HRBK:	100	100	100	100	100
Brightening	HRBT:	100	100	100	99.73	95.13
	HRBK:	100	100	100	99.20	96.13
Scaling	HRBT:	92.80	97.13	98.27	99.20	99.33
	HRBK:	96.20	98.33	99.00	99.53	99.87
Histogram equalization	HRBT:	100	100	100	100	100
	HRBK:	100	100	100	100	100
JPEG compression	HRBT:	68.73	73.87	82.40	85.40	83.87
	HRBK:	62.80	66.73	68.40	72.13	69.00

Table 4: Detection rates (%) with HRBT and HRBK features for different modification parameterizations (CT image dataset).

Modification		Modification detection rates (%)				
JPEG2000	HRBT:	41.00	47.00	49.00	46.00	56.00
	HRBK:	41.00	51.00	71.00	60.00	69.00
Gaussian filtering	HRBT:	46.00	99.00	100	100	100
	HRBK:	44.00	100	100	100	100
Laplacian filtering	HRBT:	100	100	100	100	100
	HRBK:	100	100	100	100	100
Brightening	HRBT:	100	100	100	100	98.00
	HRBK:	100	100	100	100	100
Scaling	HRBT:	98.00	100	100	100	100
	HRBK:	100	100	100	100	100
Histogram equalization	HRBT:	100	100	100	100	100
	HRBK:	100	100	100	100	100
JPEG compression	HRBT:	55.00	74.00	96.00	98.00	100
	HRBK:	100	100	100	100	100

images and all their modified versions were used so as to generate the SVM model for classification. This training set was thus composed of the features of 1800 images. Then the rest of the original images and their corresponding modified images were fed to the trained SVM model to determine whether an input image was modified or not. The modification detection rates for this setup are recorded in the last row of Table 2. As it can be seen from this table, HRBK detection rates are better than HRBT ones.

The third test was conducted to compare the performance of the two feature sets under different modification parametrization settings. In this test, for each modification type and parameter, the training dataset was composed of fifty original images and their modified ones, which are modified according to the corresponding modification type and parameter; the test set included the remaining fifty original images and their modified ones. The training and testing of SVM model were similarly done as in aforementioned tests. The results of this test are recorded in Tables 3 and 4 for the two image datasets. As it can be seen from these two tables, HRBK outperforms HRBT in most cases.

4.3. Identification of the Image Modification Type. In this second experiment, the objective was not only to detect whether an image had been modified, but also to determine the type of the image tampering. To do so, a multiclass SVM was constructed based on one-versus-one binary classifier, and pairwise coupling [30] was employed to combine results from all binary classifiers. As previously, fifty original images along with all their modified versions, that is to say, 1800 images, were used as training set. The rest of the images, original and modified, were used as the test set for the evaluation of the trained classifier. Detection rates are provided in Table 5 for different modification types considering CT images and MR images. As it can be seen, for each modification type, the detection rates of HRBK features are higher than those of HRBT features in most situations. This is due to the better image representation of the Krawtchouk moments

Table 5: Multiclass detection rates (%) with HRBT and HRBK features.

	CT image dataset		MR image dataset	
Modification	HRBT	HRBK	HRBT	HRBK
JPEG2000	87.32	92.72	78.32	79.40
Gaussian filtering	69.00	69.24	64.36	66.68
Laplacian filtering	100	100	99.28	99.44
Brightening	96.20	97.12	88.76	90.64
Scaling	86.92	89.32	85.44	85.48
Histogram equalization	100	100	100	100
JPEG compression	76.64	96.84	81.84	81.68

Table 6: Multiclass detection rates (%) of HRBK with different training and testing sets ratios.

	CT image dataset		MR image dataset	
Modifications	1:1	7:3	1:1	7:3
JPEG2000	92.72	96.07	79.40	70.67
Gaussian filtering	69.24	71.87	66.68	71.07
Laplacian filtering	100.00	100.00	99.44	99.60
Brightening	97.12	96.60	90.64	92.67
Scaling	89.32	87.53	85.48	93.60
Histogram equalization	100	100.00	100	100.00
JPEG compression	96.84	96.53	81.68	89.07

than that of Tchebichef moments. It can be observed that HRBK achieved much better results for CT images with JPEG compression than HRBT did, but worse results for MR images with JPEG compression. This could be due to the fact that MR images have more image details than CT images do. After JPEG compression, more image discriminative information is lost for MR images, which leads to lower modification detection rates.

4.4. Evaluation of the Influence of Block Size on Integrity Verification Performance. In this last experiment, the objective was to determine the influence of the centered block size (size of the image block used to generate features) on detection rates for the different modification types described in Section 4.1. Let us recall that the number of Krawtchouk moments in a subband depends on the block size. In this test, three different block sizes were considered; i.e., 128×128, 64×64, and 32×32 were chosen to generate the image features while considering the same ten subbands (see Section 3). As before, for each modification type, fifty original images and their modified images were used as training set and the others as test set, and multiclass SVM was used as classifier. The plots in Figures 6 and 7 show the relations between detection rates and block sizes for CT and MR images, respectively. As it can be seen, detection rates decrease as the block sizes reduce. However, the HRBK method has better detection rates in most cases, and this superiority is much obvious for small block sizes. This phenomenon can be explained as the result of better description power of Krawtchouk moments compared to Tchebichef moments and their ability to keep essential discriminative image information as block size decreases.

In previous experiments, the ratio between the size of training set and that of the testing set was 1:1. The influence of the ratio value on the performance of the proposed method was also tested. In this test, we used seventy original images along with all their modified versions as the training set. The rest of the images, original and modified, were used as the test set to evaluate the performance of the trained classifier for modification classification. This leads the ratio between training set size and testing set size to be 7:3. Table 6 shows the detection rates of HRBK with 128×128 block size for different modification types. As it can be seen, the detection rates with the HRBK features increased in most cases. However, the choice of the optimal value of the ratio needs further study; this will be part of our further work.

4.5. Discussion. For the purpose of verifying the integrity of medical images, a new set of image features was proposed, which was developed based on the histogram statistical properties of reorganized block-based Krawtchouk moments. Higher image modification detection rates are achieved when the proposed method is used in most modification situations. However, our method can only be used to detect modifications with "a priori knowledge." More clearly, the possible types of modification an image may undergo are identified before the SVM training. In the case of an "unforeseen attack," the proposed method will identify the modification as the closest or most similar a priori known modification type. Moreover, we considered only global image modification types; further study should be done to investigate the image integrity verification problem with local image modification types. To further improve the performance of our method, one way could be to use other prevalent machine

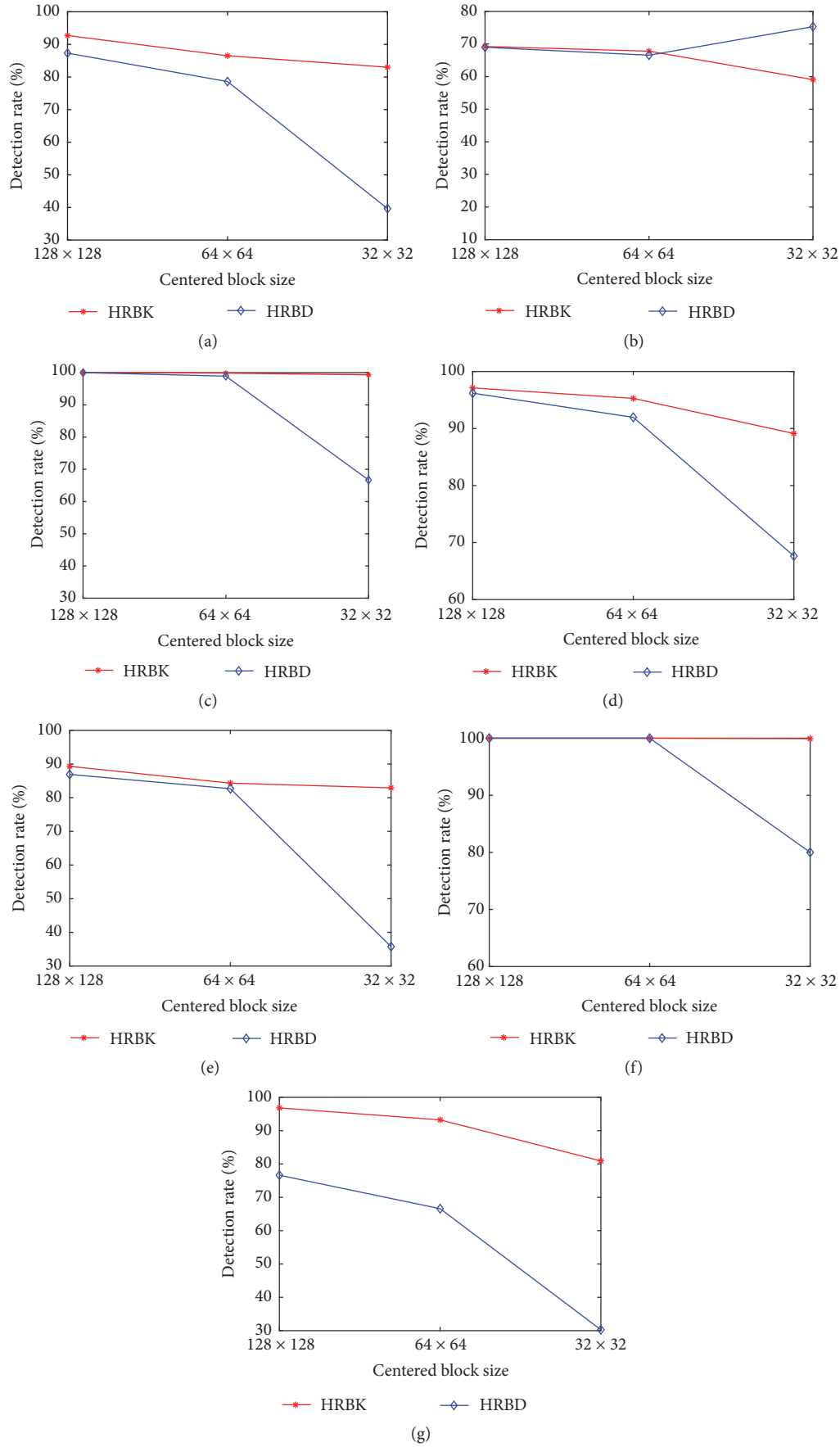

Figure 6: CT image modification detection rates for different centered block sizes and various modification types: (a) JPEG2000, (b) Gaussian filtering, (c) Laplacian filtering, (d) brightening, (e) scaling, (f) histogram equalization, (g) JPEG compression.

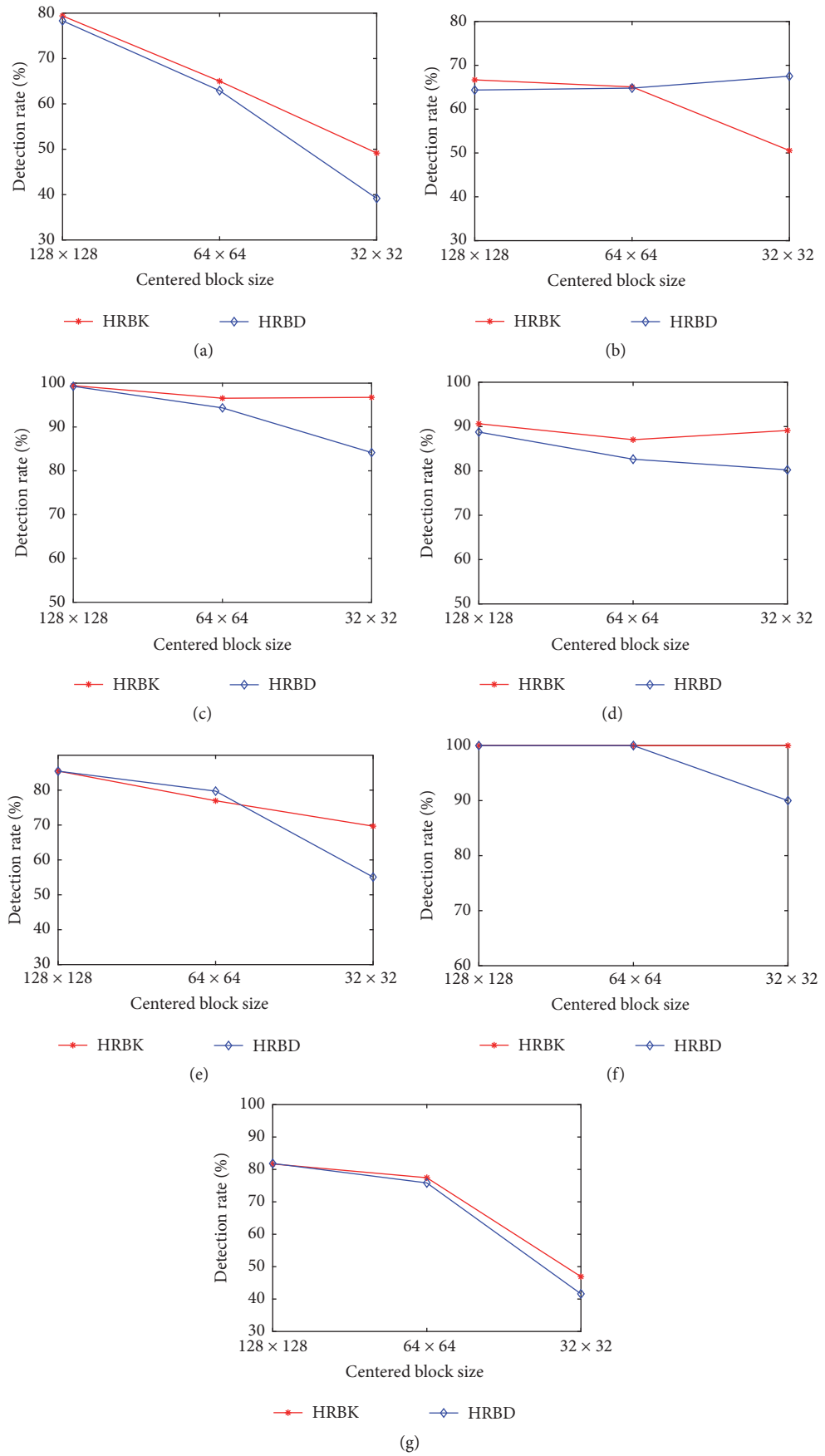

FIGURE 7: MR image modification detection rates for different centered block sizes and various modification types: (a) JPEG2000, (b) Gaussian filtering, (c) Laplacian filtering, (d) brightening, (e) scaling, (f) histogram equalization, (g) JPEG compression.

learning methods, such as deep leaning, to construct the classification model.

5. Conclusions

In this paper, we have proposed a new set of image features based on Krawtchouk moments. These HRBK features are used to detect medical image modifications and also to distinguish the types of the image modifications through a classification-based strategy. Compared with the existing HRBT features, HRBK achieves better detection rates for almost all kinds of image modification types and is more robust with respect to feature extraction area size. The proposed integrity verification method relies on the ability of the image features to describe the differences between unmodified and modified images. Future works include exploiting image moment properties to construct more selective image features and speeding up the feature extraction process by taking advantage of parallelism in the computation.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] M. Ghadi, L. Laouamer, and T. Moulahi, "Enhancing digital image integrity by exploiting JPEG bitstream attributes," *Journal of Innovation in Digital Ecosystems*, vol. 2, no. 1-2, pp. 20–31, 2015.

[2] A. P. Dhawan, *Medical Image Analysis*, IEEE Press, Hoboken, NJ, USA, 2nd edition, 2011.

[3] D. Bouslimi, G. Coatrieux, M. Cozic, and C. Roux, "A telemedicine protocol based on watermarking evidence for identification of liabilities in case of litigation," in *Proceedings of the IEEE 14th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 506–509, October 2012.

[4] L. O. M. Kobayashi and S. S. Furuie, "Proposal for DICOM multiframe medical image integrity and authenticity," *Journal of Digital Imaging*, vol. 22, no. 1, pp. 71–83, 2009.

[5] H. Huang, G. Coatrieux, H. Z. Shu, L. M. Luo, and C. Roux, "Medical image integrity control and forensics based on watermarking – approximating local local modifications and identifying global image alterations," in *Proceedings of the 33rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 8062–8065, Boston, MA, USA, August 2011.

[6] A. N. Azmi, D. Nasien, and F. S. Omar, "Biometric signature verification system based on freeman chain code and k-nearest neighbor," *Multimedia Tools and Applications*, vol. 76, no. 14, pp. 15341–15355, 2017.

[7] G. Coatrieux, H. Maitre, and B. Sankur, "Strict integrity control of biomedical images," in *Proceedings of SPIE*, vol. 4314, pp. 229–240, 2011.

[8] "Part 15: Security and System Management Profiles," in *Digital Imaging and Communications in Medicine, DICOM PS 3.15*, 2004.

[9] C. Chen, J. Ni, Z. Shen, and Y. . Shi, "Blind forensics of successive geometric transformations in digital images using spectral method: theory and applications," *IEEE Transactions on Image Processing*, vol. 26, no. 6, pp. 2811–2824, 2017.

[10] G. Cao, Y. Zhao, R. Ni, B. Ou, and Y. Wang, "Forensic detection of noise addition in digital images," *Journal of Electronic Imaging*, vol. 23, no. 2, p. 023004, 2014.

[11] Z. Shen, J. Ni, and C. Chen, "Blind detection of median filtering using linear and nonlinear descriptors," *Multimedia Tools and Applications*, vol. 75, no. 4, pp. 2327–2346, 2016.

[12] M. Jenadeleh and M. Ebrahimi Moghaddam, "Blind Detection of Region Duplication Forgery Using Fractal Coding and Feature Matching," *Journal of Forensic Sciences*, vol. 61, no. 3, pp. 623–636, 2016.

[13] J.-C. Lee, C.-P. Chang, and W.-K. Chen, "Detection of copy-move image forgery using histogram of orientated gradients," *Information Sciences*, vol. 321, pp. 250–262, 2015.

[14] Q. Wang and R. Zhang, "Double JPEG compression forensics based on a convolutional neural network," *EURASIP Journal on Information Security*, vol. 2016, no. 1, 2016.

[15] Y. Q. Shi, G. Xuan, D. Zou et al., "Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image," in *Proceedings of International Conference on Multimedia Expo*, p. 1, 2005.

[16] S. K. Jena and G. V. V. Krishmna, "Blind steganalysis: estimation of hidden message length," *Journal of Computers, Communications, and Control*, vol. 2, pp. 149–158.

[17] N. Provos and P. Honeyman, "Hide and seek: an introduction to steganography," *IEEE Security & Privacy*, vol. 1, no. 3, pp. 32–44, 2003.

[18] Y. Sheng, Z. Xin, C. Jian-guo, X. Yong-liang, and L. Qiang, "A blind image detection method for information hiding with double random-phase encoding," *Optics & Laser Technology*, vol. 41, no. 5, pp. 590–595, 2009.

[19] H. Huang, G. Coatrieux, H. Shu, L. Luo, and C. Roux, "Blind integrity verification of medical images," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 6, pp. 1122–1126, 2012.

[20] P. T. Yap, R. Paramesran, and S. H. Ong, "Krawtchouk moments as a new set of discrete orthogonal moments for image reconstruction," in *International Joint Conference on Neural Networks*, vol. 1, pp. 908–912, 2002.

[21] P.-T. Yap, R. Paramesran, and S.-H. Ong, "Image analysis by Krawtchouk moments," *IEEE Transactions on Image Processing*, vol. 12, no. 11, pp. 1367–1377, 2003.

[22] B. Kaur and G. Joshi, "Lower Order Krawtchouk Moment-Based Feature-Set for Hand Gesture Recognition," *Advances in Human Computer Interaction*, vol. 2016, 2016.

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

[24] H.-H. Tsai and D.-W. Sun, "Color image watermark extraction based on support vector machines," *Information Sciences*, vol. 177, no. 2, pp. 550–569, 2007.

[25] V. S. Verma, R. K. Jha, and A. Ojha, "Digital watermark extraction using support vector machine with principal component analysis based feature reduction," *Journal of Visual Communication and Image Representation*, vol. 31, pp. 75–85, 2015.

[26] Y. Wang and P. Moulin, "Perfectly secure steganography: capacity, error exponents, and code constructions," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 54, no. 6, pp. 2706–2722, 2008.

[27] D. Zhao, W. Gao, and Y. K. Chan, "Morphological representation of DCT coefficients for image compression," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 12, no. 9, pp. 819–823, 2002.

[28] C. A. Cocosco, V. Kollokian, R. K.-S. Kwan, A. C. Evans, and BrainWeb, "Online interface to a 3D MRI simulated brain database," in *Proceedings of the Proceeding of 3rd International Conference on Functional Mapping of the Human Brain*, vol. 5, p. 475, 1997.

[29] R.-S. Kwan, A. C. Evans, and G. B. Pike, "MRI simulation-based evaluation of image-processing and classification methods," *IEEE Transactions on Medical Imaging*, vol. 18, no. 11, pp. 1085–1097, 1999.

[30] T.-F. Wu, C.-J. Lin, and R. C. Weng, "Probability estimates for multi-class classification by pairwise coupling," *Journal of Machine Learning Research (JMLR)*, vol. 5, pp. 975–1005, 2004.