Multimedia Tools and Applications (2020) 79:6623–6647
https://doi.org/10.1007/s11042-019-08281-x

Iris spoofing detection using discrete orthogonal moments

Bineet Kaur[1]

Received: 16 February 2019 / Revised: 2 September 2019 / Accepted: 22 September 2019 /
Published online: 17 December 2019

Abstract
Human iris being the most stable biometric modality suffers from presentation attacks like colored textured contact lenses and print attacks that obfuscate the natural iris texture. The paper presents discrete orthogonal moment-based invariant feature-set comprising of Tchebichef, Krawtchouk and Dual-Hahn moments which are extracted at localized iris regions to capture local intensity distributions of the iris texture. The orthogonal moment-based feature-set is made rotation, translation and scale-invariant in order to accommodate for geometric transformations when images are acquired in uncontrolled environment. The performance of the proposed techniques is evaluated using four publicly available iris spoofing databases: IIITD-Contact Lens Iris, IIITD Iris Spoofing, Clarkson LivDet 2015 and Warsaw LivDet 2015. The textured contact lens detection rate of 100% for IIITD-CLI and 99.48% for Clarkson datasets is achieved, respectively. Similarly, print+scan and print+capture attacks are detected with 99% and 98.93% accuracy for IIS datasets, respectively. The print attacks are detected with 99.63% and 98.89% accuracy for Clarkson and Warsaw datasets, respectively. The proposed techniques thus, prove to be effective in terms of contact lens and print attacks detection when acquired using multiple sensors.

Keywords Contact lens · Dual-Hahn moments · Iris spoofing · Krawtchouk moments · Orthogonal moments · Print attacks · Tchebichef moments

1 Introduction

Human iris identification is being used in various large-scale security applications like the Aadhar project in India [49] and in UAE border crossing [46]. Iris being the most stable biometric modality [17] because of its unique texture still suffers from presentation attacks

✉ Bineet Kaur
bineetkaur91@gmail.com

[1] Department of Electronics and Communication Engineering, Punjab Engineering College (Deemed to be University), Chandigarh 160012, India

where an imposter impersonates a genuine user. Iris texture was proposed as a biometric modality for the first time in 1987 by Flom and Safir [5]. After that, Daugman made first commercial biometric algorithm based on iris recognition which is still widely used in many commercial systems [3]. Iris is affected by various covariates like usage of colored textured contact lenses [51], consumption of alcohol [1] and pupil dilation [14]. However, the presence of textured contact lenses is more prevalent for Presentation Attack Detection (PAD) with the increase of 3–5% in the number of contact lens wearers worldwide [37]. They are used to obfuscate the natural iris texture by superimposing the pattern and color of the textured contact lens onto the natural iris which affects the overall iris recognition accuracy of the system. However, soft transparent contact lenses do not tamper the natural iris pattern. Other than this, print attacks are another way to iris spoofing where a printed iris image is presented to the biometric system for impersonating an already enrolled user [11, 25]. In this, either the iris pattern is first printed by a high-quality printer and then scanned which is called print+scan or the photo is captured by a scanner which is called print+capture [11]. Detection of iris spoofing is the first step to improve the reliability of an iris recognition system.

The manuscript deals with an important and challenging issue of Presentation Attack Detection (PAD) method for iris recognition. In today's scenario, biometric systems are being used in high-surveillance applications where security is the main concern. PAD is a challenge that researchers are working on these days to have more secure biometric systems. Recent research revealed that there are no existing methods that can significantly reduce spoofing attacks. Very few researchers have provided effective techniques which work for both iris spoofing attacks i.e. contact lenses and print attacks acquired using multiple sensors.

The manuscript deals with cross-sensor iris spoofing problem via contact lenses and print attacks when acquired using multiple sensors. Acquisition of iris images using multiple sensors also affects the overall performance of the iris recognition system. The first motive of the paper is thus, to develop a robust method that can detect any kind of iris spoofing attacks using different sensors. Thus, the focus of the paper is on iris spoofing detection acquired with multiple sensors using discrete orthogonal moment-based features which are invariant to noise and rotation. The paper introduces a novel method of constructing an orthogonal feature-set consisting of Krawtchouk, Tchebichef and Dual-Hahn moments extracted on localized 32 × 32 normalized iris texture regions. An orthogonal feature-set is deployed as these provide minimum information redundancy with sufficient number of features to discriminate between large number of subjects. For this, adequate number of features have been selected which can best represent the iris textural pattern. A critical analysis is done regarding the optimum selection of moment order and the number of features that can give best classification results.

With iris recognition systems being affected by various covariates like colored textured contact lenses and print attacks, there is a need of robust algorithms that can easily detect presentation attacks so as to make the system more reliable for use in large-scale applications. Acquiring iris samples using different sensors also affects the overall performance of the biometric system where samples acquired from one sensor are matched against another. Thus, the key motivation of the paper is to develop an effective technique that can easily detect presentation attacks acquired using different sensors. The main objectives of the paper are as follows:

(1) The paper proposes a robust method that can easily detect colored textured contact lenses as well as print attacks acquired using multiple sensors.
(2) The paper introduces a novel method of constructing an orthogonal feature-set consisting of Krawtchouk, Tchebichef and Dual-Hahn moments extracted on

localized 32 × 32 normalized iris texture regions. An orthogonal feature-set is deployed as these provide minimum information redundancy with sufficient number of features to discriminate between large number of subjects used in this work. For this, adequate number of features have been selected which can best represent the iris textural pattern. A critical analysis is done regarding the optimum selection of moment order and the number of features that can give best results. A feature-set constructed from discrete orthogonal moments can effectively represent local intensity variations which prove to be useful for iris spoofing attack classification. To the best of our knowledge, this is the first paper to exploit the property of developing a feature-set which is orthogonal, has invariance properties and represents local intensity variations that works best with iris texture patterns which is characterized by high-degree of randomness and irregularities.

(3) This feature-set has been made invariant to rotation, scale and translation as iris spoofed samples undergo geometric variations when acquired.

(4) The proposed method is evaluated using performance metrics namely Correct Classification Rate (CCR), Attack Presentation Classification Error Rate (APCER), Bonafide Presentation Classification Error Rate (BPCER), Average Classification Error Rate (ACER), DET (Decision Error Threshold) Curve and Detection Equal Error Rate (D-EER) and the performance is validated by comparing it with recently proposed algorithms available in the literature.

The paper has been organized as follows: Section II summarizes the research work done till date on iris spoofing. Section III discusses the details on the introduction of the discrete orthogonal moment-based polynomials along with the proposed technique used in the manuscript for detecting iris spoofing attacks. Section IV demonstrates experiments performed by taking various spoofed samples from multiple sensors using proposed methodology and a comparison is drawn with the techniques available in the literature. Section V concludes the manuscript along with possible future scope to make the proposed system more reliable and secure.

2 Related work

In 2003, Daugman introduced Fourier spectrum of the printed iris pattern which gave periodic iris pattern that occurs in dot matrix printing. These days the dot matrix printing is not used, thus making Fourier transform less reliable for PAD [2]. Recently, many researchers have implemented algorithms for iris spoofing detection. Yadav *et al.* proposed modified LBP (Local Binary Pattern) with SVM (Support Vector Machine) classification for textured contact lens detection using IIITD-Contact Lens Iris (IIITD-CLI) and Notre Dame Contact Lens databases. The textured contact lenses were detected with an accuracy of 95% and it was concluded that the removal and detection of contact lenses improves the reliability of the iris recognition system [51]. Hu *et al.* implemented regional features based on spatial pyramid for iris liveness detection on contact lens and print attack iris spoofing databases. The proposed methods gave minimum error rates when compared with other state-of-the-art methods [16]. Gupta *et al.* proposed LBP, HOG (Histogram of Oriented Gradients) and GIST with SVM classification for detection of iris spoofing via print attacks [11]. LBP was found to perform best giving PAD rate of above 95%. Kohli *et al.* implemented multi-order Zernike and LBP with variance for iris spoofing detection via contact lens and print attacks. The proposed method resulted in detection rate of 82.20% using combined iris spoofing database [31]. Kohli *et al.* analysed that colour cosmetic lenses degrade the performance of a biometric system with increase in false rejection using VeriEye. It was concluded that lens detection helps maintain the performance of the iris recognition system [30]. Menotti *et al.* proposed deep representation via convolutional networks and back-propagation for iris spoofing detection [34]. Silva *et al.* implemented deep representation through convolutional network with softmax regression for classification on IIITD-CLI database thus, achieving 30% performance gain as compared to other approaches [45]. Gragnaniello *et al.* proposed local descriptors based on microtextural features for iris liveness detection [9]. Nalla *et al.* proposed bi-spectral iris recognition which acquired both visible and near infrared with pixel-to-pixel correspondences. The Domain Adaption- Naïve Bayes Nearest Neighbor (DA-NBNN) with real-valued log-gabor phase features were extracted on IIITD-CLI database obtaining 89.92% accuracy [36]. Pala *et al.* implemented triplet convolutional network along with relative distance matching which proved to be effective for both photo-based and contact lens attacks [38]. Raghavendra *et al.* implemented deep convolutional neural network with fifteen layers for three-class classification of normal, soft and textured contact lenses on IIITD-CLI database. It showed an improvement of more than 10% in correct classification rate when compared to other state-of-the-art approaches [42]. Doyle *et al.* implemented modified LBP method which was applied to different iris regions at multiple scales for classifying no lens, soft lens and textured contact lens. Results gave 98% of textured contact lens detection rate on Notre Dame Contact Lens Database (NDCLD12) [4]. Sequeira *et al.* implemented a set of five features for liveness detection in a mobile scenario. These features included high frequency power, local contrast, global contrast, adapted frequency distribution rates and statistical texture analysis. The best features were selected using Sequential Forward Floating Selection (SFFS) which were classified using SVM, k-Nearest Neighbor (k-NN) and Discriminant Analysis (DA). The experiments were conducted on Biosec, Clarkson, NotreDame, MobBIOfake and Warsaw databases out of which Biosec gave best classification error of 2.0% using SVM [44]. Galbally *et al.* implemented 25 general image quality features to distinguish between fake and real iris images. The classification was done using Quadratic Discriminant Analysis (QDA). The experimental results were conducted on real images of CASIA-Iris V1 and WVU-Synthetic Iris databases along with self-developed ATVS-Fir database which consisted of 800 fake and 800 genuine iris samples. For ATVS-Fir database, 97% of samples were correctly classified. The synthetic iris samples gave False Fake Rate (FFR) of 4.2, False Genuine Rate (FGR) of 0.8 and Half Total Error Rate (HTER) of 2.1 [7]. Table 1 summarizes recent literature survey of promising algorithms for iris spoofing attack detection.

3 Proposed methodology

An iris recognition system has the following steps: 1) Image Acquisition 2) Iris Segmentation 3) Iris Normalization 4) Feature Extraction 5) Classification. The acquired iris sample is matched against the enrolled users resulting in either acceptance or rejection. The proposed methodology has been illustrated in Fig. 1.

Table 1 Recently proposed promising iris spoofing attack detection techniques

Ref.	Author and Year	Database	Feature Extraction	Results
[4]	Doyle *et al.* (2013)	Notre Dame Cosmetic Contact Lens 2012 database	Weighted LBP	CCR: 98% for detecting textured contact lenses
[30]	Kohli *et al.* (2013)	IIITD Contact Lens database	LBP with SVM classification	At 0.01% FAR, VeriEye simulator: 72.95% accuracy LBP with SVM classification, lens detection accuracy improves to 94.41%
[51]	Yadav *et al.* (2014)	IIIT-D Contact Lens Iris Database, Notre Dame Contact Lens Detection	Modified LBP	IIITD- No Lens: 62.14% Soft Lens: 61.63% Textured Lens: 94.74% ND Contact Lens: No Lens: 72.6% Soft Lens: 50% Textured Lens: 97%
[11]	Gupta *et al.* (2014)	IIITD iris spoofing database	LBP, HOG and GIST	Print+Scan Accuracy: LBP: 100% HOG: 97.22% GIST:65.19% LBP + HOG:92.32% Print+Capture Accuracy: LBP: 95.26% HOG:81.04% GIST:58.66% LBP + HOG:72.38%
[16]	Hu *et al.* (2015)	Warsaw (852 live iris images and 815 fake printouts collected in NIR illumination), Clarkson, Notre Dame and MobBIOfake database	LBP histogram, LBP correlogram, intensity histogram, intensity correlogram, Local Phase Quantization (LPQ) histogram	Error Rates: Warsaw: 1.05% MobBIOfake: 2.40% Clarkson: 2.43% Notre Dame: 0.41%
[9]	Gragnaniello *et al.* (2015)	Warsaw, Notre Dame and ATVS	LBP, SIFT, SID, BSIF (Binarized Statistical Image Features), Local Contrast-Phase Descriptor (LCPD), Multi-resolution LBP	Error Rates: SID: 0% for both Warsaw and ATVS. ND I: 0.1% ND II: 0.0% Cogent: 6.2% Vista: 3.5%
[38]	Pala *et al.* (2017)	Iris-2013-Warsaw and IITD	Deep Triplet Embedding network	Average Classification Error: Warsaw: 0.0 IIITD Cogent: 5.5 IIITD Vista: 0.7
[31]	Kohli *et al.* (2016)	Combined Iris Spoofing database	Multi-order Zernike moments, Local Binary Pattern Variance	Mean classification accuracy: 82.20%
[42]	Raghavendra *et al.* (2017)	IIITD and Notre Dame 2013	Deep Convolutional Neural Network	CCR (Multisensor): IIITD (Combined): 94.65% ND (Combined): 92.60%
This paper	This paper's proposed methodology	IIITD-CLI, IIS, Clarkson LivDet 2015, Warsaw LivDet 2015.	Discrete Orthogonal Moment-based Features (Tchebichef, Krawtchouk and Dual-Hahn Moments)	CCR: IIITD-CLI: 100% Clarkson: 99.48% (textured lens), Print+Scan: 99%, Print+Capture: 98.30%, Clarkson: 99.63% (Print attacks), Warsaw: 98.89% (Print Attacks)

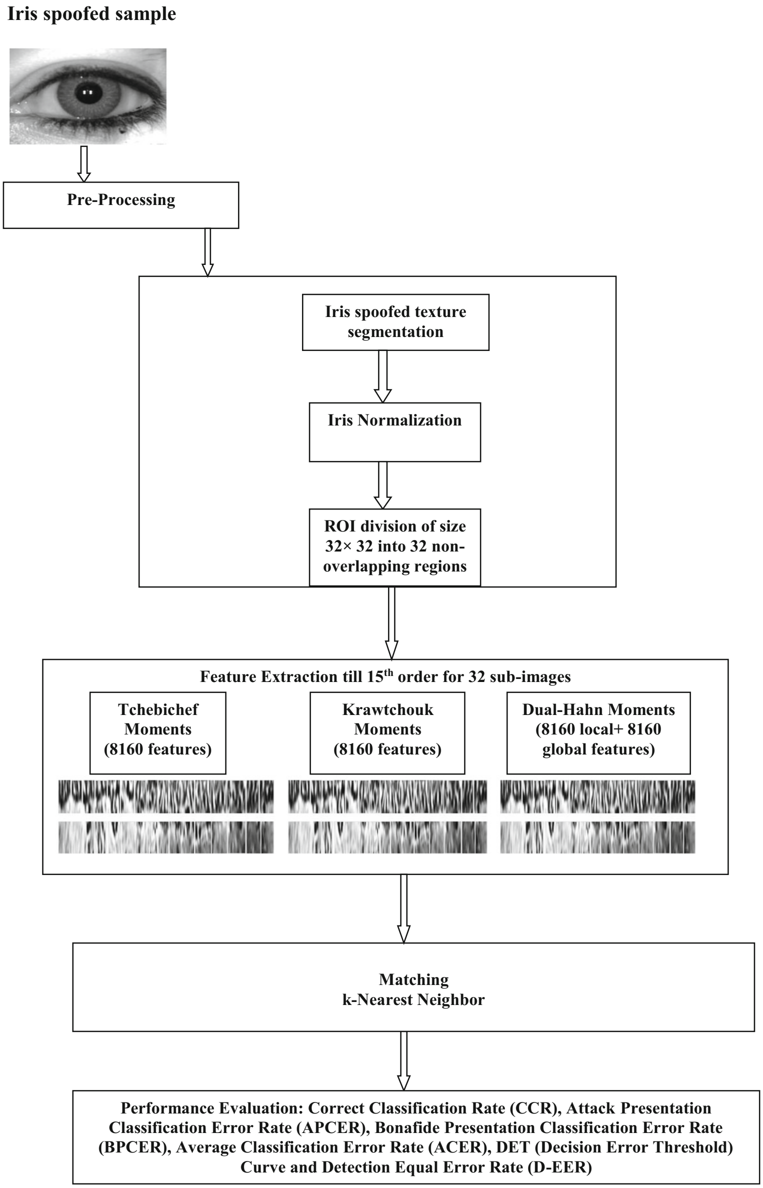

Iris spoofed sample
Pre-Processing
Iris spoofed texture segmentation
Iris Normalization
ROI division of size 32× 32 into 32 non-overlapping regions
Feature Extraction till 15th order for 32 sub-images
Tchebichef Moments (8160 features)
Krawtchouk Moments (8160 features)
Dual-Hahn Moments (8160 local+ 8160 global features)
Matching
k-Nearest Neighbor
Performance Evaluation: Correct Classification Rate (CCR), Attack Presentation Classification Error Rate (APCER), Bonafide Presentation Classification Error Rate (BPCER), Average Classification Error Rate (ACER), DET (Decision Error Threshold) Curve and Detection Equal Error Rate (D-EER)

Fig. 1 Proposed Iris spoofing detection algorithm

3.1 Iris segmentation

The first step of iris recognition is to detect iris-pupil and iris-sclera boundary. For this, Circular Hough Transform (CHT) has been deployed which detects circles in an image and is insensitive towards noise [33].

$$CHT\left(x_{c,}y_{c,}r\right) = \sum_{i=1}^{n} CHT\left(x_{i,}y_{i,}x_{c,}y_{c,}r\right) \tag{1}$$

where, (x_i, y_i), i = 1,2,3…..n are all edge points in an image. A binary edge map of the image is generated using Canny edge detector where each edge point is treated as the centre of the circle with varying radii. Iris being the largest circle with maximum number of edges is detected using CHT. The circumferential pixels are stored in an accumulator. CHT (x_c, y_c, r) = 1 is stored in accumulator, when CHT (x_i, y_i) lies on the perimeter of the circle else, CHT (x_c, y_c, r) = 0 is stored. The highest value stored in the accumulator corresponds to centre co-ordinates of iris.

3.2 Iris normalization

The segmented iris samples are transformed into fixed dimensions due to variations in illumination and acquisition of samples at varying distances. For normalizing segmented iris samples Daugman's homogeneous rubber sheet model [3] is employed which transforms iris segmented image F (x, y) into polar co-ordinates (r, θ), where r ϵ [0, 1] and θ ϵ [0,2π]:

$$F(x(r,\theta),y(r,\theta))\rightarrow F(r,\theta) \tag{2}$$

$$x(r,\theta) = (1-r)x_p(\theta) + rx_I(\theta) \tag{3}$$

$$y(r,\theta) = (1-r)\,y_p(\theta) + ry_I(\theta) \tag{4}$$

x_p,y_p and x_I, y_I are the pupil and iris co-ordinates, respectively. The normalized iris samples are shown in Fig. 2.

3.3 Feature extraction

Moments have been widely used by many researchers for applications like face recognition [43], gesture recognition [20–23, 40] and watermarking [48]. Hu for the first time proposed seven moment invariants for recognition [15]. Because of their non-orthogonal nature, there was maximum information redundancy which affected recognition performance. Teague introduced continuous orthogonal moments namely Zernike and Legendre which were rotation-invariant and orthogonal in nature but had numerical instabilities at higher orders [27, 28, 47]. To overcome this, discrete orthogonal moments like Tchebichef [23, 24, 26, 35] Krawtchouk [20–24, 26, 29, 53] and Dual-Hahn [23, 24, 26, 54] moments were introduced

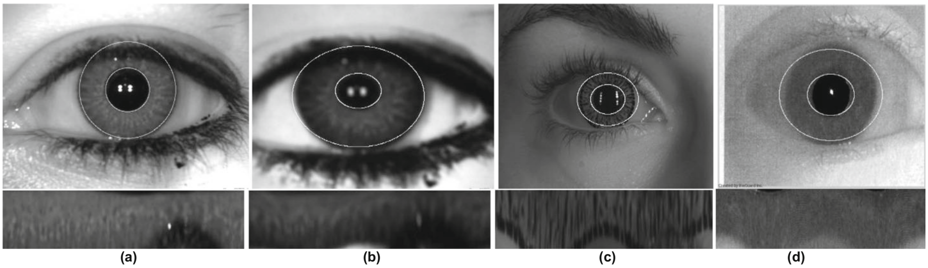


Fig. 2 Iris segmentation and normalization results of iris samples for **a** IIITD-CLI (Cogent) textured lens **b** IIS (Cogent) Print+Scan **c** Clarkson patterned lens **d** Warsaw fake printout

which worked in image co-ordinate space with no discretization errors and minimum information redundancy.

3.3.1 Tchebichef moments

These are derived from Tchebichef polynomials and can extract global features in an image by varying moment order. These are made translation and scale invariant [35].

The Tchebichef polynomial is defined as:

$$t_r(i) = (1-X)_{r3}F_2(-r,-i,1+r;1,1-r;1), \text{where}, r,i,j = 0,\ldots X-1 \tag{5}$$

To avoid numerical instabilities, normalized Tchebichef moments are derived [35]:

$$\bar{t}_r\ (i;X) = \frac{t_r\ (i)}{\rho(r;X)} \tag{6}$$

For an image intensity function f (i,j) of size X × Y, the Tchebichef moments of order (r, q) is [35]:

$$Trq = \textstyle\sum_0^{X-1}\sum_0^{Y-1}\bar{t}_r(i;X)\bar{t}_q(j;Y)f(i,j) \tag{7}$$

where, ${}_3F_2(m,m,o;p,q;r) = \sum_{k=0}^{\infty}\frac{(m)_k(n)_k(o)_k r^k}{(p)_k(q)_k(k!)}$ is a hypergeometric function.where, $(\mathrm{m})_\mathrm{k}$ is pochhammer symbol:

$$(m)_k = \mathrm{m}(\mathrm{m}+1)\ldots.(\mathrm{m}+\mathrm{k}-1) = \frac{\Gamma(m+k)}{\Gamma(m)} \tag{8}$$

where, $\rho(r;X)-(2r)!\begin{pmatrix} X+r \\ 2r+1 \end{pmatrix}$

3.3.2 Krawchouk moments

These are obtained from Krawtchouk polynomials associated with binomial functions. These are used to extract local features from a specific ROI in an image. These are made rotation, scale and translation invariant [53].

The r^{th} order classical Krawtchouk polynomial is given by [53]:

$$K_r(i;p,X) = \sum_{k=0}^{X}\left(a_{k,r,p}i^k\right) = {}_2F_1\left(-r,-i;-X;\frac{1}{p}\right) \tag{9}$$

where, i, $r = 0, 1, 2\ldots\ldots X$, $X \geq 0$, $p\epsilon(0, 1)$, $a_{k,\,r,\,p}$ are Krawtchouk polynomial coefficients.

Here, ${}_2F_1$ is a hypergeometric function which is given by:

$${}_2F_1(m,n;o;t) = \sum_{k=0}^{\infty}\frac{(m)_k(n)_k t^k}{(o)_k(k!)} \tag{10}$$

where $(\mathrm{m})_\mathrm{k}$ is a pochhammer symbol given by:

$$(m)_k = \mathrm{m}(\mathrm{m}+1)\ldots.(\mathrm{m}+\mathrm{k}-1) = \frac{\Gamma(m+k)}{\Gamma(m)} \tag{11}$$

The normalized Krawtchouk polynomials are given by [53]:

$$\acute{k}_r(i;p,X) = K_r(i;p,X)\sqrt{\frac{1}{\rho(r;p,X)}} \tag{12}$$

The weighted Krawtchouk polynomials are given by:

$$\acute{K}_r(i;p,X) = K_r(i;p,X)\sqrt{\frac{w(i;p,X)}{\rho(r;p,X)}} \tag{13}$$

The weight function is given by [53]:

$$\begin{gathered} w(i;p,X) = \binom{X}{i} p^i (1-p)^{X-i} \\ \rho(r;p,X) = (-1)^r \left(\frac{1-p}{p}\right)^r \frac{r!}{(-X)_r} \end{gathered} \tag{14}$$

The weighted Krawtchouk polynomials were derived in order to overcome numerical instabilities at higher orders.

The Krawtchouk moments of order (r + q) for an image intensity function f(i,j) is given by:

$$Q_{rq} = \sum_{i=0}^{X-1}\sum_{j=0}^{Y-1}\overline{K}_r\ (i;p_1,X-1)\overline{K}_q(j;p_2,Y-1)\,f(i,j) \tag{15}$$

where, f(i,j) is of size X × Y and these are substituted for X-1 and Y-1. p_1 and p_2 are used for varying ROI in an image [53].

'p_1' and 'p_2' are used for ROI variation in horizontal and vertical directions. For $p_1 > 0.5$, ROI shifts towards positive x-direction and for $p_1 < 0.5$, it shifts towards negative x-direction. With $p_2 > 0.5$, shifting occurs towards negative y-direction and with $p_2 < 0.5$ it takes place towards positive y-direction. In this paper, 'p_1' and 'p_2' have been taken to be 0.5 so that the focus of the moment invariants is towards the centre of the image.

3.3.3 Dual-Hahn moments

Dual-Hahn moments can extract global as well as local features with rotation, scale and translation invariance as opposed to Tchebichef moments that extract global features and Krawtchouk moments that extract local features from a specific ROI of the image [54].

$$h^{(v)}{}_r(p,a,b= \frac{(a-b+1)_r(a+v+1)}{r!}\,{}_3F_2(-r,a-p,a+p+1;a-b+1,+v+1;1) \tag{16}$$

where, $r = 0, 1, 2\ldots.\ R-1$, $p = a, a+1\ldots\ldots.\ b-1$

To avoid numerical fluctuations at higher orders, the Dual-Hahn polynomials are scaled using a weighted function which is given by [54]:

$$w(p) = \frac{\Gamma(a+p+1)\Gamma(v+p+1)}{\Gamma(p-a+1)\Gamma(b-p)\Gamma(b+p+1)\Gamma(p-v+1)} \tag{17}$$

$$h^{(v)}{}_r(p,a,b) = h^{(v)}{}_r(p,a,b)\sqrt{\frac{w(p)}{d2_r}} \tag{18}$$

where,

$$d2_r = \frac{\Gamma(a+v+r+1)}{r!(b-a-r-1)!\Gamma(b-v-r)} \tag{19}$$

For an image intensity function f (p,u) the Dual-Hahn moments with order (r,q) are calculated as [54]:

$$h_{rq} = \sum_{p=a}^{b-1}\sum_{u=a}^{b-1} h^{(v)}{}_r(p,a,b)\; h^{(v)}{}_q(u,a,b)\; f(p,u) \tag{20}$$

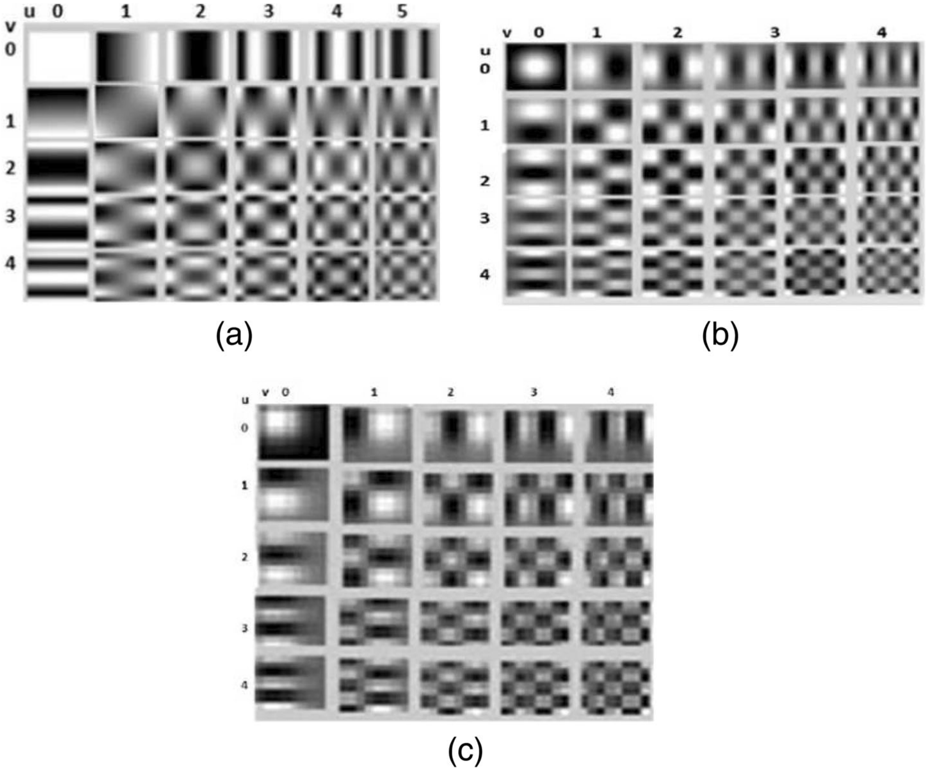
where,$-0.5 < a < b$, $|\ v\ | \ < 1 + a$, $b = a + R$, r, $q = 0$, $1\ldots\ldots.\ R-1$ and f(p,u) is R × R.

Feature Extraction is carried out using moment invariants which include discrete orthogonal moments i.e. Tchebichef (TM), Krawtchouk (KM) and Dual-Hahn moments (DM). In case of orthogonal moments, the image is projected onto a set of pair-wise orthogonal axes which minimize information redundancy and gives compact description of the image. The images are described in terms of moment-based orthogonal kernels which are real-values that represent features of a particular image. Based upon the moment order, different features are extracted for different orders. As the moment order increase, the features get added up which helps in discriminating between different classes.

3.3.4 Iris spoofed sample

Figure 3 shows the top views of discrete orthogonal basis polynomials for different moment orders. Visualization of the moment basis functions in the spatial domain. These basis functions are projected onto the image to give numerical values that represent features of an image. As the moment order increases, the number of zero-crossings increase which enhances the ability of the moments to represent the image. Dual-Hahn, Krawtchouk and Tchebichef polynomials behave as multi-frequency filter banks with polynomials having increased oscillations (zero-crossings) at higher orders. For both cases, horizontal and vertical edges are preserved at lower orders. However, Tchebichef moments have wider supports in terms of polynomial oscillations, thus capturing global information. But as the order increases, the polynomial oscillations become compact with local information capturing. In case of Krawtchouk moments the polynomials have wider supports at higher orders, thus capturing global information and compact support at lower orders, thus capturing local information. The Dual-Hahn moments act as Krawtchouk moments and Tchebichef moments, depending on its tuning parameters which are discussed in detail in this section. Further, it is seen that the enhancement is achieved up to a certain moment order, after which the recognition accuracy saturates. For discrete orthogonal feature-set, the recognition accuracy increases till 15th order after which it saturates. Also, to extract local information, the discrete orthogonal moment set is extracted for sub-images (32 equal sized (32 × 32 iris normalized sub-images).

The purpose is to extract sufficient number of features which can best represent different classes. Table 2 illustrates the feature-set based on moment-based methods. Tchebichef moments based on Tchebichef polynomials also act as global feature descriptors defined in the image co-ordinate space, are extracted till 15th order, thus representing details of the entire



(a)

(b)

(c)

Fig. 3 Representation of moments in spatial domain **a** Tchebichef **b** Krawtchouk **c** Dual-Hahn

image for further classification. In case of Krawtchouk moments, local description pertaining to a specific ROI is preserved in an image. For this, the ROI is localized at the centre of the image (using ‘p_1’ = ‘p_2’ = 0.5) and features are extracted till 15th order representing the image in terms of discrete Krawtchouk polynomials. Dual-Hahn moments extract both global and local features depending on tuning parameters ‘a’ and ‘v’ through which ROI can be varied using eq. (20). In order to accommodate for geometric transformation and scale changes in iris images during acquisition, the discrete orthogonal moment feature-set is made rotation, scale and translation invariant [6].

With ‘a’,‘v’ > 0, local information is captured from a specific ROI. As the values of ‘a’ and ‘v’ increase, the ROI starts shifting from top-right to bottom-right corner of the image. Thus, by tuning ‘a’ = ‘v’ = 18 at 15th order the ROI is focused to the centre of the image. However, for global feature extraction of the entire image, the parameters are set to ‘a’ = ‘v’ = 0.

The normalized iris samples of size 512 × 64 are partitioned into non-overlapping 32 equal sub-regions each of size 32 × 32. At each patch, the feature-set till 15th order comes out to be

Table 2 Moment-based feature-set

Order (r, q)	TM/KM/DM	No. of features	Accumulative features
1	$Q_{0,1}$; $Q_{1,0}$; $Q_{1,1}$	3	3
2	$Q_{2,0}$; $Q_{0,2}$; $Q_{2,1}$; $Q_{1,2}$; $Q_{2,2}$	5	8
…			
15	$Q_{15,0}$; $Q_{0,15}$;… $Q_{15,15}$	31	255

32 localized regions × 255 features till 15th order = 8160 features. However, in case of Dual-Hahn moments the feature-set is a fusion of 8160 local and 8160 global features [18, 19].

Pseudo code for calculation of Krawtchouk moments

```
Let f (i,j) be a binary image with size N×N after pre-processing
Wx = zeros (1, N);   % Initialize weight vector
Wy = zeros (1, N);
$p_1$ = 0.5;          %Initialize ROI by setting parameters $p_1$ and $p_2$
$p_2$ = 0.5;           % ROI fixed at centre
r=1;                 % Set orders
q=1;
K = [ ];              %Initialize Krawtchouk matrix
for  i = 0:N-1
  for  j=0:N-1
    %Calculation of weights
    Wx (i) =(factorial(N)/factorial(i).* factorial (N-i)).*($p_1$^(i)).*(1-$p_1$)^(N-i) ;
    Wy (j) =(factorial (N)/factorial (j).*factorial (N-j)).*($p_2$^(j)).*(1-$p_2$)^(N-j) ;
    %Calculation of Krawtchouk features
    K(i,j)= (hypergeom([-r,-i],-N,(1/$p_1$)).*sqrt(Wx)).*(hypergeom([-q,-j],-N,(1/$p_2$)).*sqrt(Wy)).*f(i,j);
  end
end
```

Pseudo code for calculation of Dual-Hahn moments

```
Let f (p,u) be a binary image with size R×R after pre-processing
Wx = zeros (1, R);   % Initialize weight vector
Wy = zeros (1, R);
a = 18; v = 18; b = 18;    % Set tuning parameters for local/global feature extraction
r=1;                 % Set orders
q=1;
h= [ ];              %Initialize Dual-Hahn matrix
for  p = 0:R-1
  for  u=0:R-1
    %Calculation of weights
    W(p) = (gamma(a+p+1)*gamma(v+p+1))/(gamma(p-a+1)*gamma(b-p)*gamma(b+p+1)*gamma(p-v+1));
    %Calculation of Dual-Hahn features
    h(p,u) = h(p,u)*sqrt(W(p))*f(p,u);
  end
end
end
```

3.4 Classification

For classification, k-Nearest Neighbor (k-NN) is used which works best with large databases. It is based on the principle that the instances belonging to the same class are closer to each other. Manhattan distance [12] is calculated between the training and the testing samples. Based on majority voting, the testing samples are classified into their respective classes. Moment-based techniques contain features which are highly correlated with the same class and uncorrelated with a different class. Thus, k-NN works best with moment-based features for discriminating between different classes. The best recognition accuracy results for all the databases are shown by Manhattan distance at ‘k’ = 1. Thus, experiments have been performed using these parameters.

4 Results and discussions

The experiments have been conducted on MATLAB R2014a using Intel(R) Pentium(R) laptop with windows 7, 32-bit operating system at 2GHz with 4GB RAM memory using four publicly available iris spoofing databases: IIITD Contact Lens Iris (IITD-CLI) (consists of

6570 images from 101 subjects captured using Cogent dual iris sensor (CIS 202) and VistaFA2E single iris sensor) [30, 51], IIITD Iris Spoofing (IIS) (contains 4848 images acquired from 101 subjects with two types of print attacks: print+scan and print+capture) [11, 31], Clarkson LivDet 2015 (consists of 828 genuine images for 45 subjects, 1152 fake images from 7 subjects using 20 contact lenses and 1746 printed iris images) [52] and Warsaw LivDet 2015 (The testing set contains 2002 genuine and 3890 fake printed samples while the training set consists of 852 genuine and 815 printed fake images) [52].

4.1 Performance evaluation of the proposed technique

The proposed technique is evaluated on four publicly available presentation attack databases using performance indices: APCER, BPCER, ACER and D-EER. APCER incorrectly classifies spoofed images as normal images and BPCER misclassifies normal images as spoofed images. ACER gives the average of APCER and BPCER. D-EER is a point where both BPCER and APCER are equal. The lower the D-EER value, better will be the performance of the system.

For fair comparative analysis of the proposed approach with other techniques available in the literature, the databases have been divided using the same training-testing protocol as done by existing approaches.

The problem of PAD via contact lenses and print attacks has been approached through 3-class classification i.e. no lens, soft lens and textured lens for contact lenses and original, print+capture and print+scan for print attacks. Correct classification rate has been evaluated on four publicly available presentation attack databases. These include inter-sensor, intra-sensor and multi-sensor classification also.

4.1.1 Intra-sensor

In this case, the training as well as testing sets have been evaluated using the same type of sensors. By fusing discrete moments best recognition accuracy is observed. For IIITD-Cogent, 89.20% normal, 100% textured and 99.99% soft lenses are correctly detected. In case of IIITD-Vista, 87.90% normal, 100% textured and 99.98% soft lenses are correctly classified. For IIS (Print+Scan) Cogent, 89.60% normal, 96.56% textured and 90.43% transparent lenses are correctly detected. In case of IIS (Print+Scan) Vista, 92.70% normal, 96.67% textured and 89.67% transparent lenses are correctly classified. For IIS (Print+Capture) Cogent, 56.98% normal, 98.50% textured and 99.32% transparent lenses are correctly detected. In case of IIS (Print+Capture) Vista, 85.89% normal, 92.60% textured and 89.78% transparent lenses are correctly classified. For Clarkson LG, the average CCR has resulted in 98.48% with patterned contact lens and printed detection rate of 100% and 98.56%, respectively. For Clarkson Dalsa, the average CCR is 99.39% with patterned contact lens and printed detection rate of 100% and 99.42%, respectively. In case of Warsaw, CCR obtained is 99.39% with fake iris printout detection rate of 100%. The results are summarized in Tables 3 and 5 with moment-based method achieving superior results in comparison to other approaches.

4.1.2 Inter-sensor

In this, database trained on one sensor is tested on another sensor to evaluate cross-sensor performance of the proposed system. Tables 4 and 6 show the proposed moment-based techniques outperform existing techniques for cross-sensor iris recognition problem. When

Table 3 Comparison of proposed method for intra-sensor lens detection (CCR in %); N-N: None-None T-T: Textured-Textured S-S Soft-Soft lens

Database	Class	Texture [50]	GLCM [13]	Weighted LBP [55]	LBP + SVM [51]	LBP + PHOG+SVM [51]	mLBP [51]	Deep Image [45]	Filters [41]	ContlensNet [42]	TM	KM	DM	Fusion
IIITD Cogent	N-N	33.28	32.76	45.39	65.53	59.73	66.83	35.50	64.16	66.68	72.45	73.67	75.89	89.20
	T-T	77.78	45.44	85.41	89.39	91.87	94.91	73.00	100	100	95.89	96.78	97.40	100
	S-S	42.73	33.34	54.43	42.73	52.84	56.66	98.21	66.45	93.62	63.56	67.90	69.30	99.99
	Total	51.63	37.31	62.06	66.40	68.57	73.01	69.05	76.87	86.73	79.40	81.45	83.56	98.40
IIITD Vista	N-N	79.75	53.99	43.15	53.37	49.49	76.21	60.80	68.89	74.50	78.50	78.92	80.40	87.90
	T-T	94.36	60.12	90.57	98.64	99.42	91.62	55.88	100	100	92.50	94.60	95.40	100
	S-S	16.43	0.00	56.11	50.90	59.32	67.52	98.30	75.63	87.50	70.34	72.60	74.75	99.98
	Total	63.73	32.69	63.72	68.04	69.84	80.04	72.08	81.50	87.33	82.46	84.06	86.57	97.95

Table 4 Comparison of proposed method with other approaches for inter-sensor and multi-sensor lens detection (CCR in %)

Database	Models	Classification	mLBP+Ensemble of classifier [51]	Statistically independent filters [41]	Deep Image Representation [45]	ContlensNet [42]	TM	KM	DM	Fusion
IIITD Cogent	IIITD Vista	N-N	65.99	57.67	48.67	87.75	85.84	86.36	89.30	95.69
		T-T	80.81	100	38.15	78.91	94.62	96.30	99.38	100
		S-S	48.31	66.06	42.25	87.75	83.50	88.78	90.80	95.69
		Total	65.29	74.57	43.08	84.80	90	92.40	95.20	99.20
IIITD Vista	IIITD Cogent	N-N	62.10	66.91	06.00	96.19	89.30	90.67	95.40	98.50
		T-T	92.95	97.09	89.61	100	92.60	95.70	97.62	100
		S-S	75.44	56.96	45.47	88.23	85.70	88.20	90.39	95.70
		Total	77.79	73.65	45.51	94.80	91.20	93.59	96.47	99.06
IIITD Combined	IIITD Combined	N-N	–	–	–	–	93.80	96.23	98.00	99.50
		T-T	–	–	–	–	94.80	97.70	99.00	100
		S-S	–	–	–	–	97.75	98.40	99.40	100
		Total	–	–	–	–	97.45	98.45	99.80	99.89

Table 5 Classification results of proposed method for intra-sensor iris spoofing (CCR in %); L-L: Live P-P: Patterned Contact Lens Pr-Pr: Printed

Database	Classification	Tchebichef Moments	Krawtchouk Moments	Dual-Hahn Moments	Fusion
IIS (Print+Scan) Cogent	N-N	72.70	74.60	77.56	89.60
	T-T	86.50	89.70	90.95	96.56
	Tr-Tr	84.45	85.35	86.67	90.43
	Total	83.22	85.22	87.08	94.20
IIS (Print+Scan) Vista	N-N	83.70	85.40	86.98	92.70
	T-T	92.99	93.78	95.68	96.67
	Tr-Tr	82.43	82.89	84.68	89.67
	Total	88.40	89.36	91.11	95.01
IIS (Print+Capture) Cogent	N-N	77.31	77.89	78.00	56.98
	T-T	89.30	92.67	95.90	98.50
	Tr-Tr	90.56	94.79	95.90	99.32
	Total	87.73	90.45	91.93	86.94
IIS (Print+Capture) Vista	N-N	73.69	74.89	75.23	85.89
	T-T	83.70	85.90	88.50	92.60
	Tr-Tr	83.56	84.70	85.87	89.78
	Total	82.32	83.83	85.20	91.43
Clarkson LG	L-L	88.79	93.42	94.40	96.60
	P-P	93.39	97.76	98.64	100
	Pr-Pr	90.54	95.84	97.63	98.56
	Total	92.90	97.67	97.89	98.48
Clarkson Dalsa	L-L	87.59	94.52	95.95	98.74
	P-P	95.89	96.74	97.84	100
	Pr-Pr	92.45	97.64	96.74	99.42
	Total	93.97	96.30	97.84	99.39
Warsaw	L-L	87.59	94.52	95.95	98.74
	Pr-Pr	95.89	96.74	97.84	100
	Total	93.97	96.30	97.84	99.39

models trained on IIITD Cogent were tested on IIITD Vista, the average CCR was observed to be 99.20% with 100% of textured contact lenses correctly detected. In case of models trained on IIITD Vista and tested on IIITD Cogent, the average CCR improved to 99.06% with contact lens detection accuracy of 100%. When models trained on IIS (Print+Scan) Cogent were tested on IIS (Print+Scan) Vista, the average CCR obtained is 93.60% with an accuracy of 93.60% contact lens detection. In case of models trained on IIS (Print+Scan) Vista and tested on IIS (Print+Scan) Cogent, the average CCR is 91.80% with contact lens detection accuracy of 93.78%. Similarly, in case of Print+Capture attack, models trained on Cogent and tested on Vista showed CCR of 93.35% with contact lens detection accuracy of 95.94%. When trained on Vista and tested on Cogent, the average CCR dropped to 92.57% with contact lens detection accuracy 93.89%. When models trained on Clarkson LG were tested on Clarkson Dalsa, the average CCR obtained is 99.81% with an accuracy of 100% of contact lens and print attack detection. In case of models trained on Clarkson Dalsa and tested on Clarkson LG, the average CCR is 99.98% with contact lens and print attack detection accuracy of 100%.

4.1.3 Multi-sensor

The inter-sensor and intra-sensor results indicate that the proposed system performs well for cross-sensor iris recognition system. In case of multi-sensor classification, the training dataset contains images from multiple sensors and the testing dataset contains images from the same set of multiple sensors. Tables 4 and 6 indicate that a high CCR is obtained even when database consists of images from multiple sensors. In case of IIITD combined database, fusion of discrete moments gives an average CCR of 99.89% and contact lens detection accuracy of 100%. For IIS combined database, average CCR of 95.45% with contact lens detection accuracy of 94.75% is obtained. For Clarkson combined database, the detection rate of patterned contact lenses and print attacks obtained is 99.74% and 98.46%, respectively. For a 3-class classification problem results of all the iris spoofing databases are summarized in Table 6. In case of IIITD and IIS combined databases, the textured contact lens can be easily detected with 98.90% and 96% accuracy, respectively. Both Print+Scan and Print+Capture attacks can be easily detected with 99% and 98.93% accuracy, respectively thus giving competent results. The patterned contact lenses and printed fake images in case of Clarkson database give recognition accuracy of 99.48% and 99.63%, respectively (Table 7).

Fake printouts of iris images in Warsaw dataset are detected with 98.89% accuracy. Tables 8 and 9 illustrate that the ACER value of 4.15% and 1.11% for Clarkson Dalsa and LG, respectively outperforms other algorithms submitted for LivDet-Iris 2015 competition. For

Table 6 Classification results of proposed method for inter-sensor and multi-sensor iris spoofing attacks (CCR in %)

Database	Models	Classification	Tchebichef Moments	Krawtchouk Moments	Dual-Hahn Moments	Fusion
IIS (Print+Scan) Cogent	IIS (Print+Scan) Vista	N-N	72.76	73.79	75.32	89.46
		T-T	84.75	85.40	86.32	93.60
		Tr-Tr	83.76	85.75	85.90	90.67
		Total	80.75	81.67	82.57	93.60
IIS (Print+Scan) Vista	IIS (Print+Scan) Cogent	N-N	75.48	76.54	77.69	83.89
		T-T	84.97	85.49	86.79	93.78
		Tr-Tr	82.89	83.30	85.77	91.74
		Total	81.78	82.74	83.47	91.80
IIS (Print+Capture) Cogent	IIS (Print+Capture) Vista	N-N	76.59	78.40	80.39	85.34
		T-T	86.54	87.39	87.60	95.94
		Tr-Tr	83.62	84.53	85.98	92.78
		Total	83.43	84.42	85.57	93.35
IIS (Print+Capture) Vista	IIS (Print+Capture) Cogent	N-N	74.89	75.48	76.40	83.86
		T-T	84.80	85.00	85.45	93.89
		Tr-Tr	85.40	86.44	87.00	93.98
		Total	81.69	82.78	83.00	92.57
IIS Combined	IIS Combined	N-N	76.54	77.45	79.34	85.98
		T-T	95.34	96.90	97.34	94.75
		Tr-Tr	92.56	93.75	94.00	99.53
		Total	88.68	89.85	90.95	95.45
Clarkson LG	Clarkson Dalsa	N-N	94.83	96.25	97.29	98.53
		P-P	95.76	98.20	98.25	100
		Pr-Pr	97.54	98.00	99.03	100
		Total	98.04	98.48	99.19	99.81
Clarkson Dalsa	Clarkson LG	N-N	93.47	97.38	98.29	99.05
		P-P	95.02	97.86	98.59	100
		Pr-Pr	97.85	98.74	99.34	100
		Total	97.46	98.99	99.74	99.98
Clarkson Combined	Clarkson Combined	N-N	95.67	96.84	98.62	99.42
		P-P	96.57	97.36	98.97	99.74
		Pr-Pr	97.74	98.33	99.25	98.46
		Total	98.66	99.51	99.94	99.21

Table 7 Classification results of proposed methods for iris spoofing detection (CCR in %)

Database	Class Type	Classes	Tchebichef Moments	Krawtchouk Moments	Dual-Hahn Moments	Fusion
IIITD CLD	3- class	Normal	86.80	88.00	89.00	94.89
		Textured	95.84	96.80	97.80	98.90
		Soft	87.43	88.30	89.80	95.97
		Total	90.02	91.56	92.64	98.56
IIS	3-class	Normal	86.74	87.40	89.00	93.90
		Textured	93.74	94.80	96.37	96.00
		Transparent	87.62	89.73	91.40	95.93
		Total	89.36	91.00	92.68	97.27
IIS	3-class	Original	96.74	97.40	99.00	99.90
		Print+Scan	97.74	97.80	98.37	99.00
		Print+Capture	97.62	99.73	98.40	98.93
		Total	98.36	98.31	98.59	99.28
Warsaw	2-class	Live	93.68	95.93	97.40	97.89
		Printed	95.43	96.40	98.52	98.89
		Total	96.55	98.17	98.96	99.39
Clarkson	3-class	Normal	95.70	96.38	97.00	98.56
		Patterned	96.58	97.47	98.68	99.48
		Printed	97.59	98.72	98.89	99.63
		Total	98.63	98.57	99.19	99.68

Warsaw dataset, ACER value of 0% is obtained. In case of IIITD and IIS databases, the results obtained are encouraging when compared to other approaches with ACER as low as 1.27% for IIITD Vista and 1.20% for IIS Vista. Table 10 compares D-EER values of presentation attack databases with other state-of-the-art techniques with proposed technique achieving lower D-EER values for all the databases. Figure 4 indicates the performance of the proposed system using DET curve by plotting APCER and BPCER with performance curves closer to lower left corner of the graph showing minimum errors for all the datasets. However, by fusing moment-based features, a superior performance is observed.

The results provided by existing research papers using SIFT, LBP and HOG do not provide invariant features and have redundant information involved in the features which results in poor accuracy. The redundancy in the feature-set results in overfitting thus, decreasing the accuracy performance. Also, these features have a large computation time.

However, in case of moment-based feature-set the image is projected onto a set of pair-wise orthogonal axes which minimize information redundancy and gives compact description of the image. This feature-set is further made invariant to rotation, scale and translation because of image scale variations and geometrical transformations that are embedded in iris images when acquired. Iris spoofed texture contains irregular and random patterns for which features capturing local intensity variations prove to be more effective than those which extract features from the entire image that work well with well-defined shape-based applications.

The orthogonal moment-based features provide compact description with invariance properties of rotation, scale and translation which are extracted from localized iris textural patterns emphasizing on local intensity distributions of the random and irregular iris spoofed texture. Table 11 compares the performance of the existing approaches which are applied using the proposed methodology with the proposed moment-based feature-set. Experimental results reveal that the proposed moment-based feature-set proves to be robust in presentation attack

Table 8 Classification Error Rates of proposed methods for IIITD CLI and IIS databases (in %)

Techniques	IIIT Cogent			IIIT Vista			IIS Cogent			IIS Vista		
	APCER	BPCER	ACER	APCER	BPCER	ACER	APCER	BPCER	ACER	APCER	BPCER	ACER
Triple Net [38]	–	–	5.5	–	–	0.7	–	–	–	–	–	–
SID [9]	–	–	6.2	–	–	3.5	–	–	–	–	–	–
Dense Sift [34]	–	–	13.9	–	–	2.5	–	–	–	–	–	–
Daisy [34]	–	–	17.2	–	–	8.8	–	–	–	–	–	–
LCPD [10]	–	–	11.0	–	–	3.1	–	–	–	–	–	–
Fusion (TM + KM + DM)	2.34	4.87	3.60	1.98	0.56	1.27	2.78	3.89	3.33	1.78	0.63	1.20

Table 9 Classification Error Rates of proposed methods for Clarkson and Warsaw databases (in %)

Database	Anon0 [52]			Anon1 [52]			Anon2 [52]			Federico [52]			Fusion (TM + KM + DM)		
	APCER	BPCER	ACER	APCER	BPCER	ACER	APCER	BPCER	ACER	APCER	BPCER	ACER	APCER	BPCER	ACER
Dalsa	31.48	13.23	22.35	0.96	11.9	6.43	1.65	10.85	6.25	13.85	3.18	8.51	0.85	7.45	4.15
LG	17.82	11.64	14.73	1.97	13.23	7.60	2.1	10.85	6.47	2.58	1.85	2.21	0.67	1.56	1.11
Warsaw	9.05	3.25	6.15	0.21	2.35	1.28	0.28	0.9	0.59	0	0	0	0	0	0
Average	19.45	9.37	14.41	1.05	9.16	5.10	1.34	7.53	4.44	5.48	1.68	3.57	0.51	3.00	1.75

Table 10 Detection-Equal Error Rates of proposed methods for iris spoofing detection (in %)

Database	SURF [36]	WPD(db4 + svd) [8]	Even symmetric Gabor [32]	1-D Log-gabor phase [39]	Real-valued Log-Gabor phase with DA-NBNN [36]	Fusion (TM + KM + DM)
IIIT Cogent	12.36	19.47	10.09	9.84	0.67	0.015
IIIT Vista	20.85	16.47	13.11	17.04	1.94	0.023
IIIT Cogent vs Vista	34.75	39.33	29.59	32.17	3.29	0.036
IIS Cogent	–	–	–	–	–	0.036
IIS Vista	–	–	–	–	–	0.025
IIS Cogent vs Vista	–	–	–	–	–	0.045
Clarkson	–	–	–	–	–	0.047
Warsaw	–	–	–	–	–	0.028

detection as it achieves superior performance results when compared with existing algorithms available in the literature.

5 Conclusions and future scope

The paper discusses iris spoofing attacks by which an imposter impersonates a genuine user. Thus, detection if iris spoofing attacks would make the system secure for practical applications. In this paper, discrete orthogonal moment-based invariant feature-set comprising of Tchebichef, Krawtchouk and Dual-Hahn moments is extracted at localized iris regions till 15th order. Results demonstrate that the features show textured contact lens detection rate of 100% for IIITD-CLI and 99.48% for Clarkson datasets, respectively. Similarly, print+scan and print+

Table 11 Accuracy results for iris spoofing detection (CCR in %) using different feature-sets

Training/Testing	Cogent	Vista	Cross-sensor
IIITD-CLI			
N-N	F1: 89.20 F2: 85.68	F1: 87.90 F2: 82.34	F1: 99.50 F2: 87.89
S-S	F1: 100 F2: 89.56	F1: 100 F2: 90.23	F1: 100 F2: 89.65
T-T	F1: 99.99 F2: 85.45	F1: 99.98 F2: 86.78	F1: 100 F2: 89.89
IIS (Print+Capture)			
N-N	F1: 56.98 F2: 56,34	F1: 85.89 F2: 81.56	F1: 85.98 F2: 82.35
T-T	F1: 98.50 F2: 67.89	F1: 92.60 F2: 87.45	F1: 94.75 F2: 87.89
Tr-Tr	F1: 99.32 F2: 75.89	F1: 89.78 F2: 84.57	F1: 99.53 F2: 89.78
IIS (Print+Scan)			
N-N	F1: 89.60 F2: 84.56	F1: 92.70 F2: 86.78	F1: 85.98 F2: 83.57
T-T	F1: 96.56 F2: 87.98	F1: 96.67 F2: 89.87	F1: 94.75 F2: 86.90
Tr-Tr	F1: 90.43 F2: 89.67	F1: 89.67 F2: 87.68	F1: 99.53 F2: 89.46
Clarkson LivDet-Iris 2015			
Training/Testing	LG	Dalsa	Cross-sensor
L-L	F1: 96.60 F2: 89.67	F1: 98.74 F2: 90.67	F1: 99.42 F2: 87.89
P-P	F1: 100 F2: 87.89	F1: 100 F2: 91.46	F1: 99.74 F2: 88.49
Pr-Pr	F1: 98.56 F2: 89.90	F1: 99.42 F2: 92.36	F1: 98.46 F2: 88.89
Warsaw LivDet-Iris 2015 (Iris Guard AD100)			
L-L	F1: 98.74 F2: 89.67	–	–
Pr-Pr	F1: 100 F2: 89.79	–	–

F1: KM + TM + DM F2: SIFT+LBP + HOG

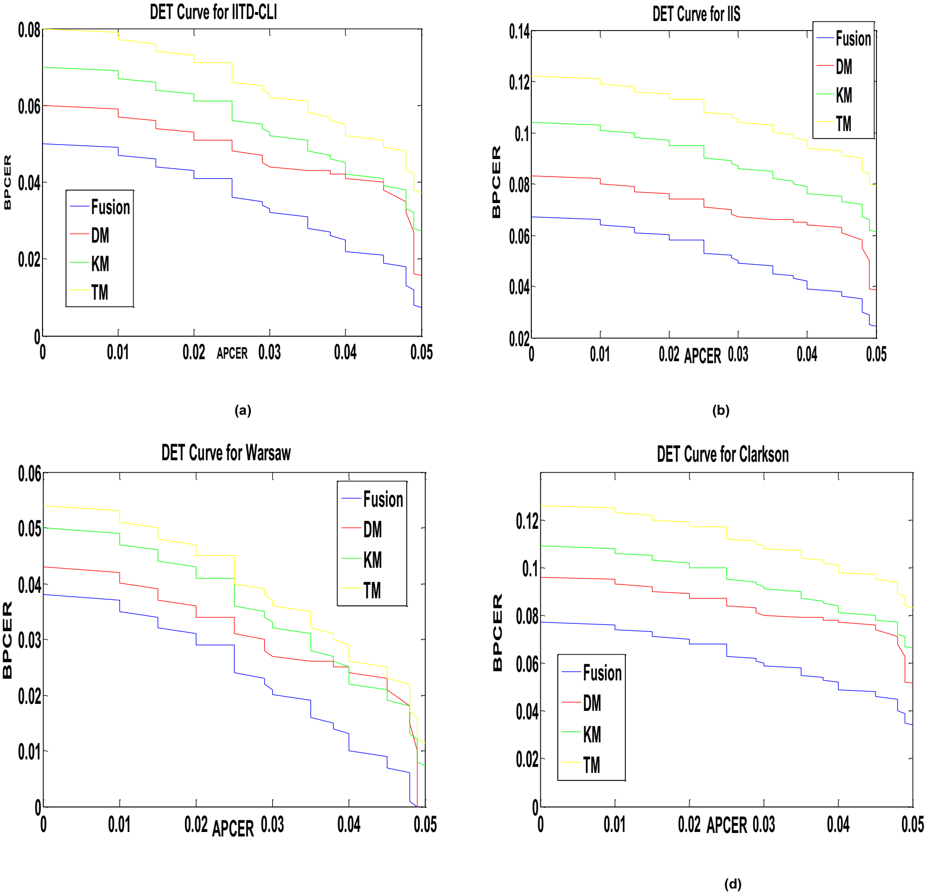


Fig. 4 DET Curves for **a** IIITD-CLI **b** IIS **c** Warsaw LivDet 2015 **d** Clarkson LivDet 2015

capture attacks are detected with 99% and 98.93% accuracy for IIS datasets, respectively. The print attacks were detected with 99.63% and 98.89% accuracy for Clarkson and Warsaw datasets, respectively. Experiments suggest that iris spoofing detection improves the reliability of the biometric system.

However, various possible future directions can be explored to make the system more secure and reliable. The performance of the iris spoof attack detection can be further improved by using deep convolutional neural networks for learning complex patterns more deeply when working on different spoofed samples. Also, the performance of the iris biometric system degrades when an unknown spoofing attack is encountered. This limits its application for real world when the nature of attacks is unpredictable. Therefore, effective and generalized algorithms need to be proposed that can detect unpredictable or unseen spoofing attacks by designing mathematical models of spoofs characterized by different materials and techniques like an artificial eye ball, a printed or video image and an eye removed from the authenticated user. Real world applications require a robust iris scanning system that uses surveillance cameras that can track the activities and identify individuals from a distance. Developing effective iris scanning systems that can scan multiple moving individuals at a distance of several feet is also an interesting future research direction. In addition to this, the biometric templates can be exploited to create synthetic spoofing databases. This threat can be addressed by using cancelable biometrics which means a non-invertible mathematical transformation is applied and only the transformed biometric template is stored through which biometric trait cannot be procured. Another solution could be using cryptographic keys for biometric templates to protect the user's privacy.

Acknowledgments The authors would like to acknowledge Indraprastha Institute of Information and Technology, Delhi (IIITD), Clarkson University, USA and Warsaw University of Technology, Poland for providing IIITD-CLI, IIS, Clarkson and Warsaw iris spoofing databases used in this work.

References

1. Arora SS, Vatsa M, Singh R, Jain A (2012) Iris recognition under alcohol influence: A preliminary study", 5th IEEE IAPR International Conference on Biometrics (ICB), pp. 336–341
2. Daugman J (2003) Demodulation by complex-valued wavelets for stochastic pattern recognition. Int J Wavelets Multiresolution Inf Process 1(1):1–17
3. Daugman J (2004) How iris recognition works. IEEE Transactions on Circuits and Systems for Video Technology 14(1):21–30
4. Doyle JS, Flynn PJ, Bowyer KW (2013) Automated classification of contact lens type in iris images. International Conference on Biometrics (ICB):1–6
5. Flom L, Safir A (1987) Iris recognition system. U.S. Patent 4 641 349
6. Flusser J, Suk T, Zitová B (2016) 3D Moment Invariants to translation, rotation, and scaling. 2D and 3D Image Analysis by Moments 96
7. Galbally J, Marcel S, Fierrez J, J. (2014) Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. IEEE Trans Image Process 23(2):710–724
8. Gan J, Liang Y (2005) Applications of wavelet packets decomposition in iris recognition. Advances in Biometrics. Berlin, Germany: Springer-Verlag:443–449
9. Gragnaniello D, Poggi G, Sansone C, Verdoliva L (2015) An investigation of local descriptors for biometric spoofing detection. IEEE Transactions on Information Forensics and Security 10(4):849–863
10. Gragnaniello D, Poggi G, Sansone C, Verdoliva L (2015) Local contrast phase descriptor for fingerprint liveness detection. Pattern Recogn 48(4):1050–1058
11. Gupta P, Behera S, Vatsa M, Singh R (2014) On iris spoofing using print attack. 22nd IEEE International Conference on Pattern Recognition:1681–1686
12. Han M, Pei J (2011) Data Mining: Concepts and Techniques, 3rd edn. Morgan Kaufmann Publishers, San Francisco
13. He X, An S, Shi P (2007) Statistical texture analysis-based approach for fake Iris detection using support vector machines. Proc IAPR Int Conf Biometrics:540–546
14. Hollingsworth K, Bowyer KW, Flynn PJ (2009) Pupil dilation degrades iris biometric performance. Comput Vis Image Underst 113(1):150–157
15. Hu MK (1962) Visual Pattern Recognition by Moment Invariants. IRE Transactions on Information Theory 8(2):179–187
16. Hu Y, Sirlantzis K, Howells G (2016) Iris liveness detection using regional features. Pattern Recogn Lett 82(2):242–250
17. Jain AK, Ross AA, Nandakumar K (2011) Introduction to biometrics. Springer Science & Business Media, Berlin
18. Kaur B (2019) Discrete Orthogonal Moments for iris recognition https://www.mathworks.com/matlabcentral/fileexchange/72412-discrete-orthogonal-moments-for-iris-recognition. MATLAB Central File Exchange. Retrieved August 15, 2019
19. Kaur B (2019). Dual-Hahn mOMENTS. https://www.mathworks.com/matlabcentral/fileexchange/72413-dual-hahn-moments. MATLAB Central File Exchange. Retrieved August 15, 2019
20. Kaur B, Joshi G (2016) Lower Order Krawtchouk Moment-Based Feature-Set for Hand Gesture Recognition. Advances in Human-Computer Interaction, Hindawi Publications 2016(2016):1–10
21. Kaur B, Joshi G, Vig R (2015) Analysis of shape recognition capability of Krawtchouk moments. IEEE International Conference on Computing, Communication and Automation:1085–1090

22. Kaur B, Joshi G, Vig R (2017) Indian sign language recognition using Krawtchouk moment-based local features. The Imaging Science Journal 65(3):171–179
23. Kaur B, Joshi G, Vig R (2017) Identification of ISL alphabets using discrete orthogonal moments. Wirel Pers Commun 95(4):4823–4845
24. Kaur B, Singh S, Kumar J (2018) Robust Iris Recognition using Moment Invariants. Wirel Pers Commun 99(2):799–828
25. Kaur B, Singh S, Kumar J (2018) A Study on Fake Iris Detection under Spoofing Attacks. J Eng Appl Sci 13(8):2049–2056
26. Kaur B, Singh S, Kumar J (2018) Fusing Iris and Periocular Recognition using Discrete Orthogonal Moment-based Invariant Feature-set. International Journal of Biometrics 10(4):352–367
27. Kaur B, Singh S, Kumar J (2018) Iris Recognition using Zernike Moments and Polar Harmonic Transforms. Arab J Sci Eng 43(12):7209–7218
28. Kaur B, Singh S, Kumar J (2019) Cross- Sensor Iris Spoofing Detection using Orthogonal Features. Comput Electr Eng 73:279–288
29. Kaur B, Singh S, Kumar J (2019) Orthogonal rotation invariant features for iris and periocular recognition. International Journal of Biometrics 11(2):160–176
30. Kohli N, Yadav D, Vatsa M, Singh R (2013) Revisiting Iris Recognition with Color Cosmetic Contact Lenses. Proc. 6th IAPR, pp. 1–5
31. Kohli N, Yadav D, Vatsa M, Singh R, Noore A (2016) Detecting medley of iris spoofing attacks using DESIST. IEEE 8th International Conference on Biometrics Theory, Applications and Systems:1–6
32. Ma L, Tan T, Wang Y, Zhang D (2003) Personal identification based on iris texture analysis. IEEE Trans Pattern Anal Mach Intell 25(12):1519–1533
33. Masek L (2003) Recognition of human iris patterns for biometric identification, pp. 1–7. http://www.csse.uwa.edu.au/opk/student projects/labor
34. Menotti D, Chiachia G, Pinto A, Schwartz WR, Pedrini H, Falcao AX, Rocha A (2015) Deep representations for iris, face, and fingerprint spoofing detection. IEEE Transactions on Information Forensics and Security 10(4):864–879
35. Mukundan R, Lee PA (2001) Image Analysis by Tchebichef Moments. IEEE Trans Image Process 10(9):1357–1364
36. Nalla PR, Kumar A (2017) Toward More Accurate Iris Recognition Using Cross-Spectral Matching. IEEE Trans Image Process 26(1):208–221
37. Nichols JJ (2012) Annual Report: Contact Lenses. Available:http://www.clspectrum.com/articleviewer.aspx?articleID=107853, accessed 26 June 2017
38. Pala F, Bhanu B (2017) Iris Liveness Detection by Relative Distance Comparisons. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops:162–169
39. Pillai JK, Puertas M, Chellappa R (2014) Cross-sensor iris recognition through kernel learning. IEEE Trans Pattern Anal Mach Intell 36(1):73–85
40. Priyal SP, Bora PK (2013) A Robust Static Hand Gesture Recognition System using Geometry based Normalizations and Krawtchouk Moments. Pattern Recogn Lett 46(8):2202–2219
41. Raghavendra R, Raja KB, Busch C (2014) Ensemble of statistically independent filters for robust contact lens detection in iris images. ACM Proceedings of the 2014 Indian Conference on Computer Vision Graphics and Image Processing, pp. 24:1–24:7
42. Raghavendra R, Raja KB, Busch C (2017) ContlensNet: Robust Iris Contact Lens Detection Using Deep Convolutional Neural Networks. IEEE Winter Conference on Applications of Computer Vision:1160–1167
43. Rahman SM, Howlader T, Hatzinakos D (2016) On the selection of 2D Krawtchouk moments for face recognition. Pattern Recogn 54:83–93
44. Sequeira AF, Murari J, Cardoso JS (2014) Iris liveness detection methods in the mobile biometrics scenario. International Joint Conference on Neural Networks (IJCNN):3002–3008
45. Silva P, Luz E, Baeta R, Pedrini H, Falcao AX, Menotti D (2015) An approach to iris contact lens detection based on deep image representations. 28th IEEEE SIBGRAPI Conference on Graphics, Patterns and Images:157–164
46. Tan CW, Kumar A (2013) Adaptive and localized iris weight map for accurate iris recognition under less constrained environments. Proc IEEE 6th Int Conf Biometrics, Theory Appl Syst (BTAS):1–7
47. Teague MR (1980) Image Analysis via the General Theory of Moments. J Opt Soc Am 70(8):920–930
48. Tsougenis ED, Papakostas GA, Koulouriotis DE, Tourassis VD (2012) Performance Evaluation of Moment-based Watermarking Methods: A Review. J Syst Softw 85(8):1864–1884
49. UID Authority of India (2012) Role of biometric technology in Aadhaar enrollments. Available : http://uidai.gov.in/images/FrontPageUpdates/role_of_biometric_technology_in_aadhaar_jan21_2012.pdf. accessed 26 June, 2017

50. Wei Z, Qiu X, Sun Z, Tan T (2008) Counterfeit Iris detection based on texture analysis. Proc 18th Int Conf Pattern Recognit:1–4
51. Yadav D, Kohli N, Doyle J, Singh R, Vatsa M, Bowyer K (2014) Unraveling the Effect of Textured Contact Lenses on Iris Recognition. IEEE Transaction on Information Forensics and Security 9(5):851–862
52. Yambay D, Walczak B, Schuckers S, Czajka A (2017) LivDet-Iris 2015 - Iris Liveness Detection. IEEE International Conference on Identity, Security and Behavior Analysis:1–6
53. Yap PT, Raveendran P, Ong SH (2003) Image analysis by Krawtchouk moments. IEEE Trans Image Process 12(11):1367–1377
54. Yap PT, Raveendran P, Ong SH (2007) Image analysis using Hahn moments. IEEE Trans Pattern Anal Mach Intell 29(11):2057–2062
55. Zhang H, Sun Z, Tan T (2010) Contact lens detection based on weighted LBP. Proc 20th Int Conf Pattern Recognit:4279–4282

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Er. Bineet Kaur is M.E. (Honors) in Electronics and Communication Engineering from University Institute of Engineering and Technology (UIET), Panjab University, Chandigarh, India. Her area of research includes image processing, gesture recognition, biometric systems and iris recognition. She has recently submitted her Ph.D. thesis (Punjab Engineering College (Deemed to be University), Chandigarh, India). Currently, she is working as Lecturer in National Institute of Technology (NIT), Hamirpur, Himachal Pradesh, India.