Presentation Attack Detection (PAD) for Iris Recognition System on Mobile Devices-A Survey

Abdelwahed Motwakel[1,2] , Anwer Mustafa Hilal[1] , Manar Ahmed Hamza[1], Hesham E. Ghoneim[1]

a.ismaeil@psau.edu.sa a.hilal@psau.edu.sa ma.hamza@psau.edu.sa h.ghoneim@psau.edu.sa

[1]Department of Computer and Self Development, Preparatory Year Deanship,

Prince Sattam bin Abdulaziz University, AlKharj, Saudi Arabia

[2]Department of Computer Science, Faculty of Computer Science and Information Technology,

Omdurman Islamic University

Summary
The implementation of iris biometrics on smartphone devices has recently become an emerging research topic. As the use of iris biometrics on smartphone devices becomes more widely adopted, it is to be expected that there will be similar efforts in the research community to beat the biometric by exploring new spoofing methods and this will drive a corresponding requirement for new liveness detection methods. In this paper we addresses the problem of presentation attacks (Spoofing) against the Iris Recognition System on mobile devices and propose novel Presentation Attack Detection (PAD) method which suitable for mobile environment.

Keywords: *Presentation Attack Detection, Iris Recognition System.*

1. Introduction

Biometric system has authenticated and become using in many sensitive centers in government and border and for national and individual security[1]. Biometric is the ability of identifying the individuals by using their biological properties such as fingerprint, iris, face, voice, and gait. There are many types of biometrics (such as iris, vein pattern, gait, and touch dynamics) have been highlights in modern biometric research. Some recognition systems utilize a combination as multimodal biometrics. Long time ago the police using body measurements to identify the criminals. In modern society, the ability of dependably identifying individuals in real time is a main requirement in many applications including border crossing, forensics, mobile banking, and computer security[2][3].
The iris is a unique and it is more accuracy because the structure of iris. In 1994 John Daugman has designed the first algorithm for iris recognition [4]. Iris recognition's reputation as a highly-accurate biometric method is thus established in the context of using near-infrared illumination. According to the most recent IREX IX report [5], the best performance one-to-one iris matchers algorithms obtain a false non-match rate below one percent for a false match rate of 10-5 (1 in 100,000) [6]. Unfortunately, iris recognition system is still vulnerable against presentation (commonly spoofing) attack types such as printout, glasses, synthetic eye, Cadavers, cosmetic eyelashes, displays attack (video), Prosthetic Eyes, actual eye, and Coercion.
Biometric Recognition Systems are vulnerable against presentation attacks and lack of stability through time which has declined their usage and performance [7][8]. Their drawbacks have either overcome by adding human expert supervision or simply ignored. Even bio-electrical signals which were assumed to have fundamental liveness property, have been forged [9]. In [6] the author concluded that presentation attack detection for iris recognition is not yet a solved problem such as synthetic eye [10] and soft contact lens attack [11]. In addition, in [12] reported that printed iris attacks as well as patterned contacts lenses are still difficult for software-based systems to detect. Ironically, the presentation (spoofing) attacks equipment is very cheap an in hand.
The proposed PAD algorithms are designed to mitigate a specific kind of the presentation attacks and not all on the same time. As sequence the attacker may perform different presentation attacks which makes the IRS vulnerable. Unfortunately, the state-of-art unified PAD framework DESIS [13] fails to detect the new proposed presentation attack iDCGAN [10]. In other words, the presentation attacks are able to increase and create new unknown and unexpected attacks.
On other hand, the implementing the PAD on mobile devices has three challenges [14]. First, the visible-image camera of mobile has low resolution which leads to capture unclear iris [14]. Second, the processing power of the mobile devices is restricted. Last, the iris is best captured in near-infrared (NIR) illumination and that is not available with smartphone devices and it is difficult to connect a new hardware.
The paper is organized as follows: section II presents a survey of the literature on presentation attack detection for iris recognition system, section III presents a new

Manuscript received December 5, 2021
Manuscript revised December 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.12.57

proposed presentation attack detection method, and section IV presents the conclusion.

I. Related work

To meet the increasing security requirement of the current networked society, Biometric recognition system is becoming more and more important [15].

Biometric recognition system refers to the use of physiological (e.g., fingerprints, face, retina, iris) and behavioral (e.g., gait, signature) characteristics, called Biometrics for automatically recognizing individuals.

A. Iris Recognition System

The human iris is defined as a thin circular diaphragm lying between the cornea and the lens in the eye. Iris is one of the organs present internally in human body but also visible externally when the eye-lids are open [16].

Many papers in biometric literature address the problem of Presentation Attack Detection (PAD) for Iris Recognition System on Mobile Devices. But these methods still have some problems and can't be suitable for all the condition. The paper presents the literature of Iris Recognition System and then Presentation Attack Detection.

In [15] proposed pupil & iris segmentation method apt for the mobile environment. they find the pupil & iris at the same time, using both information of the pupil and iris. And they also use characteristic of the eye image. Experimental result shows that the algorithm has good performance in various images, which include motion or optical blurring, ghost, specular refection.

In [16] proposed a novel scheme to capture high quality iris samples by exploring new sensors based on light-field technology to address the limited depth-of-field exhibited by the conventional iris sensors. The idea stems out from the availability of multiple depth/focus images in a single exposure and use the best-focused iris image from the set of depth images rendered by the Light-field Camera (LFC).

In [17] iris recognition technology was applied in mobile phones, extracted the accurate iris code based on AGF (Adaptive Gabor Filter). The kernel size, frequency and amplitude of Gabor filter are determined by the amount of blurring and sunlight in input image, adaptively. Experimental results show that the Equal Error Rate (EER)by propose method is 0.14 %.

In [18] describes an approach to adapt iris recognition for resource-constrained mobile phones by reducing its computational complexity. The system was tested using a resource-constrained virtual machine to closely emulate the computational environment of a mobile phone. The system was implemented using C# running on .NET Compact Framework. The system was tested using CASIA iris image database. The system run time was consistently under three seconds.

In [19] proposed an enhanced iris segmentation method that allows iris recognition systems to be implemented in real-time applications by reducing segmentation time without scarifying accuracy. The method was implemented in two steps, Inner and outer boundary detection.

In [20] proposed a new segmentation scheme and adapt it to smartphone based visible iris images for approximating the radius of the iris to achieve robust segmentation. The scheme was tested by two public databases BIPLab and VSSIRIS.

In [21] proposed methods for iris edge detection, extraction of feature and matching whereas the important condition is that eye is partially closed or eye is blinked. Canny operator was used to separate edges of iris from non-iris part. To detect iris properties, K-out-of-n and Euclidian distance methods are used. The method was tested using CASIA v2.0 database.

In [22] proposed approach for feature extraction and encoding of noisy, off angled, at-a-distance, near infra red (NIR) imaged iris images with high accuracy. Were extract the features from both left and right irises, encode them separately and perform bit level fusion. The method was tested using benchmark databases namely, IITD, MMU v-2 and CASIA v-4 distance to exhibit the performance.

In [23] proposed a passive approach for sensing eye contact from a live camera or an existing still image or video recording and demonstrated several of the applications that it facilitates, such as human–object interaction and gaze triggered photography. And also performed a study on how accurately humans can perform the same task, finding several interesting results without calibration.

In [24] presented an approach for iris recognition based on the combination of three classifiers describing different aspects of the iris, namely the colour, the texture, and the features of the clusters (colour spots) characterizing the iris. The approach was assessed on a subset of the MICHE DB composed by pictures captured by two smartphones, namely the Apple i Phone 5 (IP5) and the Samsung Galaxy S4 (GS4).

In [25] proposed an application for scanning the iris through mobile devices without the need to use special cameras, using the resources of the device and its limitations with image processing techniques.

In [26] proposed a light version (LV) algorithm that can recognize iris images in smartphones and the algorithm capable of works faster when using the system in smartphones environment.

In [27] evaluated two trained image reconstruction algorithms in the context of smart-phone biometrics. They are based on the use of coupled dictionaries to learn the mapping relations between low and high resolution images. In addition, reconstruction is made in local overlapped image patches, where up scaling functions are modeled separately for each patch, allowing to better preserve local details. The testing was done in a database of 560 images captured with two different smart-phones, and two iris comparators employed for verification experiments.

In [28] proposed near-infrared iris dataset captured with a mobile device was evaluated to analyze, in particular, the rotation observed in images and its impact on segmentation and biometric recognition accuracy.

In [29] developed iris recognition system for smartphones. The system uses eye images that rely on visible wavelength; these images are acquired by the smartphone built-in camera. The development of the system passes through four main phases: the first phase is the iris segmentation phase, which is done in three steps to detect the iris region from the captured image, which contains the eye and part of the face using Haar Cascade Classifier training, pupil localization, and iris localization using a Circular Hough Transform. In the second phase, the system applies normalization using a Rubber Sheet model, which converts the iris image to a fixed size pattern. In the third phase, unique features are extracted from that pattern using a Deep Sparse Filtering algorithm. Finally, in the matching phase, seven different matching techniques are investigated. In [30] In this paper, we have proposed a deep feature fusion network that exploits the complementary information presented in iris and periocular regions to enhance the performance of mobile identification. Firstly, a convolutional neural networks (CNNs) model with maxout units has been exploited to extract robust, compact and discriminative features for the iris as well as the periocular region.

In [31] Proposed algorithm overcome captured iris images in non-uniform illumination as well as eye image with reflections .The method enhanced the performance of the segmentation and normalisation process in iris recognition systems to increase the overall accuracy. The algorithm was tested on UBIRIS V.1 database which includes 15 individuals from both Right and Left eyes resulting in 45 classes in total.

In [32] proposed approach to eliminate uncontrollable capturing conditions and limitations of computation power for iris recognition system in mobile devices.

Table I shows a summary of the Iris Recognition System techniques and their limitation.

TABLE I A BRIEF SURVEY OF IRIS RECOGNITION SYSTEM TECHNIQUES

Author(s) /year	Problem Statement	Proposed Solution (technique)	Measurements / Metrics/ dataset	Performance (Result)/ advantages	Notes (limitation) Disadvantages
Dae Sik Jeong (2005)	The optical and motion blurring occurs because of the mobile's user puts it by hands. In addition, the sunlight includes much amount of Infra-Red light which effects the accuracy of the captured image.	Their solution based on **AGF (Adaptive Gabor Filter)** for extracting the accurate iris code. Their method determines frequency and amplitude of Gabor filter by the rate of blurring and sunlight in input image.	EER (Equal Error Rate) **- They produce CASIA database**	- indoor images EER 0.09% - EER 0.10 % in outdoor image. - The EER is 0.14 %	More field tests are required to enhance the performance of AGF. In addition, the eyelash shade region made by sunlight should be detected and excluded to extract iris code for better performance.
Dal-ho Cho (2006)	Pupil segmentation hard to Locate in outdoor environment because wavelength of IR-LED light from the sun and outdoor light. in addition, the motion of mobile camera sensor effect on the captured images. Those factors make the outer boundary of iris blurry and the segmentation difficult	They propose a method for iris and pupil segmentation method in various environment using **Circular Edge Detection**. Their method detecting pupil and iris in same time by using mobile built-in camera.	**CASIA database**	A (M)	
Stan Kurkovsky (2010)	Mobile iris recognition methods are complex in term of performance and computational power.	They utilize **Hough transform** to find circles corresponding to the boundaries of the iris	EER (Equal Error Rate) **CASIA iris image database**	EER of approximately 3.5%, by the time less than 3 seconds	
Kiran B. Raja (2013)	Limited depth-of-field of the traditional iris imaging devices in the visible spectrum. In addition, bad focused images attained due to non-optimal focus reduce the identification rate.	They propose scheme to capture high quality iris samples using new sensors based on **Light-Field** technology under visible spectrum, they introduce **LIGHT-FIELD IRIS database**	Equal Error Rate (EER) **LIGHT-FIELD IRIS database**	Performance: the best-focus light-field camera has EER 2.38% whereas 8.53% for conventional camera. The overall improvement of the light-field iris image is 4.64% comparted to the conventional images.	
A.V. G.S.Sastry (2013)	Iris recognition is useless with high processing time. Iris segmentation is the most expensive process which consume time more than other processes. In addition, most iris processing implementations capture low resolution iris image to keep the segmentation process time within the limited time.	They reduce the segmentation time with no loss in accuracy. Their method using edge detection on thresholded image and a modified and improved Hough transform. Then it detects outer boundary with its center within a small window of pupil center and its perimeter outside the pupil circle within some range, using the robust circular Integro Differential Operator.	Accuracy. **CASIA 2 database**	The accuracy of detection is 99%. By adjusting the scale parameter and sector size of Integro Differential Operator, the accuracy could be increased to 99.5%. Out of 400 images with 0.9 – 1.03 sec average Computational time for inner and outer boundary detection.	
Brian A. Smith (2013)	Most of gaze-based interactive systems using gaze tracking technique that require infrared illumination, calibration standardization or sensitive to distance and pose.	They propose method based on gaze locking instead of gaze tracing, their solution sensing eye contact from a live camera or an existing still image, they present **data base (CAVE)**	Matthews correlation coefficient (MCC) **(CAVE)**	At long distance their result got MCC over 0.83 up 18 Metre and large pose variations (up to ±30 of head rotation.	
Kiran B.Raja (2014)	Unconstrained environment in visible image and unrestricted distance are led to unbeknown of radius between iris and pupil.	They introduce segmentation scheme adapted to smartphone based visible iris images (**Haar Cascade Eye Detection**) and propose feature extraction method based on **Deep Sparse Filtering.** They provide a new database for smart phone (**VSSIRIS**) and (BIPLab) database as compared.	Equal Error Rate (EER) VSSIRIS and BIPLab databases	EER is 1.62 % using iPhone 5S and 1.78 % using Nokia 1020.	
Ankita Satish Adhau (2015)	Due to occlusion effect present in an iris image, most images are incapable to maintain false rejection and acceptance ratio.	They used for segmentation **Canny edge operator,** they utilized **Gabor Filtering** for feature extraction and **K-out-of-n as a classifier** for pattern matching	FAR, FRR **CASIA v2.0 database**	FAR 3.01 and FRR 0.34 The K-out-of-n classifier gives better accuracy of 95% and 99% accuracy for the proposed system using Euclidean Distance classifier	
B.H. Shekar (2015)	Non-cooperative and noisy iris images may suffer from several noise sources like reflections, off angled images, defocus blur, and occlusion by eyelids, eyelashes, hair and glasses in addition extracting	They proposed technique for feature extraction and encoding purpose. Extracting the features are from both left and right iris, then encoding procedure be carried separately for both of them, and finally performing bit level fusion.	Recognition Rate (RR) **IITD, MMU v-2 and CASIA v-4 databases**	They get recognition rate 99%, 95.62% and 91.27% respectively for each database.	

	the significant features from these images which are having high imaging variations is a challenging task				
Kavita Joshi (2015)	Researchers have used same number of subjects for both training and testing without specifying any segregation of the dataset and thus not explicitly mentioning how FAR was calculated. Therefore the FAR cannot be taken as a reliable parameter of performance evaluation for an iris recognition system	They present a iris recognition system utilizing **Hamming Distance** as a classifier. They try to improve the FAR and FRR.	False Acceptance Rate (FAR) False Rejection Rate (FRR) **CASIA-Iris v-4 database**	-The result of Recognition accuracy with combination of Gabor and HAAR feature extraction technique for 50 subjects (In training Set) is FRR 0, FAR 0 and the accuracy 100 % -For 200 subjects the result is FRR 0.74 %, FAR 0 and the accuracy 99.26 %	
Chiara Galdi (2016)	Many application scenarios in which NIR illumination is not available or applicable. For example for continuous re-identification, i.e. when the system continuously verifies the user identity, in which case the user cannot be constantly exposed to NIR light, since the effects of a prolonged exposure to NIR light are still uncertain. Another example scenario in which NIR illumination cannot be available is for forensic, i.e. the process of analyzing images or videos to verify the identity of a person.	They present approach for iris recognition on Smartphones environment Euclidean distance to extract color descriptor between color histogram of the two images and different classifiers are used	They present **MICHE database** Area Under Receiver Operating Characteristic Curve (AUC)	They improved results on Apple I phone 5 (ip5) and Samsung galaxy-s4 (gs4) with AUC rate of 0.98 and 0.80 respectively.	
Rosales-Banderas (2016)	Low resolution camera in mobile devices and the computational power are challenge for iris recognition system.	They design a software for iris recognition on mobile phone without additional hardware and with mobile built in camera. They use **Hough Transform** for segmentation process and and use **Polar Coordinates Mapping** for normalization.	correct detections They use **L.Machala, Iris Database**	88.17% of correct detections.	
Syed Arslan (2017)	The challenges which facing iris recognition in mobile devices are many times everyday unlock the smart phone that need more required computational time in order to unlock it. In addition, the response time for authentication or verification process is large because of using complex recognition algorithm.	They propose **Light Version (LV)** Algorithm which recognizes iris images in mobile phone devices. They employ **Hough circle** and line cords procedure for segmentation process. for optimization they utilize **Gabor Filter.**	Response time in ms, Computing time in ms, CPU Usage in hz **CASIA-IrisV4 database**	The **CASIA-IrisV4 database contains** more than 50000 images. They experimented the algorithm on 2000 images. -The images (0-500) the Response Time is 876 ms, Computing time is 1290 ms and the CPU usage is 435 hz. -The images (501-1000) the Response Time is 790 ms, Computing Time is 1372 ms and the CPU usage is 489 hz. - The images (1001-1500) the Response Time is 908 ms, Computing Time is 1195 ms and the CPU usage is 580 hz. The images (1501-2000) the Response Time is 716 ms, Computing Time is 1417 ms and the CPU usage is 387 hz. They improve the Response time by 8.7 % ms, Computing time by 11.4 % and the CPU Usage by 5.20 % comparing with other existing systems.	Their algorithm did not work correctly with around 5 % of the images.
Fernando Alonso-Fernandez (2017)	The poor resolution image that captured with smart phone, the distance from iris rogation sensor, and application which using mobile biometric environment are still open problems which effect the iris recognition performance.	They apply two trained patch-based super-resolution approaches. They evaluate their approach based on PCA Eigen transformation (eigen-patches) and an implementation of the Locality-Constrained Iterative Neighbor Embedding (LINE) method for iris images.	Equal Error Rate (EER) **They use VSSIRIS database**	Their result show that the trained approaches are substantially superior to bilinear or bicubic interpolations at very low resolutions (images of 13×13 pixels) an EER of approx. 7% can be achieved using individual comparators, which is further pushed down to 4-6% after the fusion of the two systems.	
Heinz Hofbauer (2018)	Untrained users opened the door to sources of noise in mobile iris recognition such as larger extent of Rotation and off-angel in images captured by mobile phone effect on iris segmentation	They utilize the parameterized **CNN-based** iris segmentations and propose a way to use the resulting binary segmentation masks to generate normalised iris texture (applying the **Rubber Sheet Transform**).	The used databases: **IIT Delhi Iris Database version 1.0 (*iitd*), and the interval subset of the CASIA Iris Image Database version 4.0 (*casia4i*), and a subset of CASIA Iris Subject Ageing Version 1.0 Database (*casiaA*).**	This work has shown that CNN- based semantic segmentation together with a higher degree of explicit rotation compensation during matching significantly improves iris recognition performance for such datasets.	
Lamiaa A. Elrefaei (2018)	Many techniques for mobile recognition need extra hardware and it will be expensive and	they develop and test iris recognition system for mobile phones. Their system uses eye images that rely on visible wavelength capture by mobile phone built-in camera. The development of the system passes through four main phases: iris segmentation phase using Haar Cascade Classifier training, second phase is pupil localization using a Circular Hough Transform, third phase unique features are extracted using a Deep Sparse Filtering algorithm. Finally, matching phase using Cityblock, Euclidian, Chebyshev, Hamming, Canberra, Bhattacharyya and Correlation	Equal Error Rate (EER) **BIPLab database and their collected dataset**	For segmentation accuracy using is 86%., For normalization average accuracy 78.25% Equal Error Rate is 0.18 for system accuracy for BIPLab database and 0.26 for the collected dataset	**A (M)**
Qi Zhang (2018)	the quality of images capture by mobile devices is significantly degraded due to hardware limitations and various of environments. Traditional iris recognition methods do not possible to achieve high identification rate using these low-quality images	They develop a deep feature fusion network that exploits the complementary information presented in iris and periocular regions. Their method first applies maxout units into the convolutional neural networks (CNNs) to generate a compact representation for each modality They propose CASIAIris-Mobile-V1.0 and CASIA-CSIR2015 database	EER (Equal Error Rate)	EER 0.60% the proposed method achieves 0.60% EER and 2.32% FNMR@FMR=10 their proposed deep feature fusion with adaptive weights approach obtained results that the EER is 0.60% and FNMR@FMR=10^5 is 2.32%.	**A**
Bhagyashree Deshpande (2018)	Different illumination expected that captured image contains types of noise and eye image with reflections. In addition, many commercial iris biometric systems using Daugman's algorithm. It especially focuses on image segmentation and feature extraction for iris recognition process however Daugman's algorithm consumes more processing time.	They implement and propose algorithm for iris recognition process in term of segmentation and normalisation to increase the accuracy and reduces the complexity without compromising the accuracy of the system. For segmentation they use Daugman's Integro Differential Operator in unconstrained environments, for normalization they use Daugman's Rubber Sheet model, for feature extraction they use 1D log Gabor filter, and for matching they use Hamming Distance.	**UBIRIS V.1 database**	Their algorithm attains 95% overall accuracy in 0.467 seconds.	

B. Presentation Attack Detection

Liveness detection, also known as vitality detection, counterfeit detection, counter measure, fake detection, presentation attack detection, spoof detection, or anti-spoofing. A liveness detection method is usually accepted to be any technique that is able to automatically distinguish between real biometric traits presented to the sensor and synthetically produced artifacts imitating the genuine trait. Numerous Liveness detection methods have been presented in the literature[15].

In [6] presented a survey for Presentation Attack Detection for Iris Recognition. And different categories of presentation attack were described and placed in an application-relevant framework.

In [33] proposed a model-based method to generate iris images and evaluated the performance of synthetic irises by using a traditional Gabor filter-based iris recognition system. A comprehensive comparison of synthetic and real data is performed at three levels of processing: a) image level, b) texture level, and c) decision level.

In [34] proposed a real-time pupil and iris detection method appropriate for mobile phones. This method has three contributions. First, for users with glasses, there may be many noncorneal SRs on the surface of the glasses and it is very difficult to detect genuine SRs on the cornea. To overcome these problems, the method used the successive On/Off Scheme of the dual illuminators. Second, to detect SRs robustly, the method used a theoretical way of estimating the size, shape, and brightness of SRs based on eye, camera, and illuminator models. Third, the detected eye (iris) regions by using the SRs were verified again by using the AdaBoost eye detector.

In [35] presented a framework to synthesize large realistic iris databases, providing an alternative to iris database collection. Firstly, iris patch is used as a basic element to characterize visual primitive of iris texture, and patch-based sampling is applied to create an iris prototype. Then a set of pseudo irises with intra-class variations are derived from the prototype.

In [36] presented results of a study of 12,003 images from 87 contact-lens-wearing subjects and 9697 images from 124 non-contact-lens wearing subjects. They visually classified the contact lens images into four categories according to the type of lens effects observed in the image. The results show different degradations in performance for different types of contact lenses. Lenses that produce larger artifacts on the iris yield more degraded performance.

In [37] proposed a liveness iris detection method based on the eye's optical features. With the help of designing special imaging and infrared illumination module and image analysis, to implement the detection. The methods include finding the change of iris texture and light spot under different waveband and position of the infrared illumination, calculating the difference of the reflection property in different iris parts.

In [38] presented a novel liveness detection scheme for iris, based on quality related measures. The method was tested on an iris database which comprises 1,600 real and fake images.

In [39] presented method for classification three types of iris images as no lens, clear lens, or textured lens images for the iris recognition systems. The system has ability to automatically determine if a person is (a) wearing no contact lens, (b) wearing a clear prescription lens, or (c), wearing a textured cosmetic lens tackle.

In [40] presented analysis of the effect of contact lens on iris recognition performance. And also presented the IIIT-D Contact Lens Iris database with over 6500 images pertaining to 101 subjects. For each subject, images are captured without lens, transparent (prescription) lens, and color cosmetic lens (textured) using two different iris sensors.

In [41] highlight the sensitivity of textured contact lens detection to the composition of the training data. The method show that accuracy of textured lens detection can drop dramatically when tested on a manufacturer of lenses not seen in the training data, or when the iris sensor in use varies between the training and test data.

In [42] presented database of iris printout images with a controlled quality, and liveness detection method for iris recognition. The database gathers images of only those printouts that were accepted by an example commercial camera. The database consists of 729 printout images for 243 different eyes, and 1274 images of the authentic eyes, corresponding to imitations. And also presented an example application of this database.

In [43] show the Liveness Detection (LivDet) competitions to compare software-based iris liveness detection methodologies using a standardized testing protocol and large quantities of spoof and live images.

In [44] presented a method to detect the presence of fake iris patterns, such as designer contact lenses, during the image acquisition stage. Exploiting the anatomy and geometry of the human eye, they presented a structured light projection method to detect the presence of artificial items obscuring the real iris. The detection principle has been verified using an inexpensive experimental setup consisting of a miniature projector and an offset camera. And also presented an algorithm to process the acquired images to find patterned contact lenses.

In [45] proposed a more generalizing iris description by extracting binarized statistical image features from normalized iris images in the original Cartesian coordinate system in order to preserve the regular structure of printing signatures of cosmetic contact lenses.

In [46] proposed method to revisits iris recognition with spoofing attacks and analyzes their effect on the recognition performance. Specifically, print attack with contact lens variations is used as the spoofing mechanism. And also presents the IIITD iris spoofing database, which contains over 4800 iris images pertaining to over 100 individuals with variations due to contact lens, sensor, and print attack.

In [47] presented an analysis of the effect of contact lenses on iris recognition. Two databases, namely, the IIIT-D Iris Contact Lens database and the ND-Contact Lens database, are prepared to analyze the variations caused due to contact lenses. And also presented a lens detection algorithm used to reduce the effect of contact lenses.

In [48] presented a brief description of the methods and the results achieved by the participants in the Mobile Iris Liveness Detection Competition (MobILive). This competition covered the most common and simple spoofing attack in which printed images from an authorized user are presented to the sensor by a non-authorized user in order to obtain access.

In [49] proposed a novel software-based liveness detection method that can be used in multiple biometric systems. In particular, presented an approach for face, iris and fingerprint spoofing attack detection in mobile applications, by employing a real-time feature description based on order permutations, named Locally Uniform Comparison Image Descriptor (LUCID).

In [50] proposed method makes use of images captured in visible range with color (RGB) information. And employ Gray-Level Co-occurrence textural features and SVM classifiers for the task of fake iris detection. Used the Sequential Forward Floating Selection (SFFS) algorithm to select the best features.

In [51] proposed a technique to detect printed-iris attacks based on the local binary pattern (LBP) descriptor. In order to improve the discrimination ability of LBP and better explore the images statistics, LBP is performed on a high-pass version of the image with 3×3 integer kernel.

In [52] investigated three different issues that arise in the construction of a robust algorithm for detecting iris recognition images that contain textured contact lenses. The first issue is whether the accurate segmentation of the iris region is required in order to achieve the accurate detection of textured contact lenses. The second issue is whether an algorithm trained on the images acquired from one sensor will well generalize to the images acquired from a different sensor. The third issue is how well a detector generalizes to a brand of textured contact lenses, not seen in the training data.

In [53] proposed a technique to detect the artefact iris images by decomposing the images into Laplacian pyramids of various scales and obtain frequency responses in different orientations. The obtained features are classified using a support vector machine with a polynomial kernel. And used the same technique with majority voting rule to provide the decision on artefact detection for video based iris recognition in the visible spectrum.

In [54] proposed approach focus on a three-class detection problem: images with textured (colored) contact lenses, soft contact lenses, and no lenses. The approach uses a convolutional network to build a deep image representation and an additional fully-connected single layer with softmax regression for classification.

In [55] presented scheme for detecting video presentation attacks in visible spectrum iris recognition system by magnifying the phase information in the eye region of the subject. The proposed scheme employs modified Eulerian Video Magnification (EVM) to enhance the subtle phase information in eye region and novel decision module to classify it as artifact (spoof attack) or normal presentation. The proposed decision module is based on estimating the change of phase information obtained from EVM, specially tailored to detect presentation attacks on video based iris recognition systems in visible spectrum.

In [56] presented an analysis of presentation attacks on iris recognition systems especially focusing on the photo print attacks and the electronic display (or screen) attack. And introduced a new relatively large scale visible spectrum iris artefact database comprised of 3300 iris normal and artefact samples that are captured by simulating five different attacks on iris recognition system. And also proposed presentation attack detection (PAD) scheme based on multiscale binarized statistical image features and linear support vector machines.

In [57] presented detailed results of the second edition of international iris liveness competition, organized in 2015 (LivDet-Iris 2015). Four software-based approaches to Presentation Attack Detection were submitted. Results were tallied across three different iris datasets using a standardized testing protocol and large quantities of live and spoof iris images.

In [58] focused on a medley of iris spoofing attacks and present a unified framework for detecting such attacks. They proposed a novel structural and textural feature based iris spoofing detection framework (DESIST). Multi-order dense Zernike moments are calculated across the iris image which encodes variations in structure of the iris image. Local Binary Pattern with Variance (LBPV) is utilized for representing textural changes in a spoofed iris image.

In [59] proposed a framework, named as iDCGAN (iris deep convolutional generative adversarial network) for generating realistic appearing synthetic iris images. They demonstrate the effect of these synthetically generated iris images as presentation attack on iris recognition by using a commercial system.

In [60] presented results of the third international iris liveness competition, LivDet-Iris 2017. Three software-based approaches to Presentation Attack Detection were submitted. Four datasets of live and spoof images were tested with an additional cross-sensor test.

In [61] presented analysis of the effect of textured contact lenses on iris recognition in visible spectrum and contact lens database in visible spectrum, and Unconstrained Visible Contact Lens Iris (UVCLI) Database, containing samples from 70 classes with subjects wearing textured contact lenses in indoor and outdoor environments across multiple sessions.

In [62] presented a Mobile Uncontrolled Iris Presentation Attack Database (MUIPAD). The database contains more than 10,000 iris images that are acquired with and without textured contact lenses in indoor and outdoor environments using a mobile sensor. And also investigate the efficacy of textured contact lens in identity impersonation and obfuscation.

In [63] proposed a multi-task convolutional neural network learning approach that can simultaneously perform iris localization and presentation attack detection (PAD). The proposed multi-task PAD (MT-PAD) is inspired by an object detection method which directly regresses the parameters of the iris bounding box and computes the probability of presentation attack from the input ocular image.

In [64] presented a comparison of the performance of the participant methods by various Figures of Merit (FoMs). A particular attention is devoted to the identification of the image covariates that are likely to cause a decrease in the performance levels of the compared algorithms.

In [65] presented a dual-band spectral imaging system to capture an iridal image from a cosmetic-contact-lens-wearing subject. By using the independent component analysis to separate individual spectral primitives, where successfully distinguished the natural iris texture from the cosmetic contact lens (CCL) pattern, and restored the genuine iris patterns from the CCL-polluted image.

In [66] proposed a Hierarchical Multiclass Iris Classification (HMC) for liveness detection based on CNN. HMC mainly focuses on iris liveness detection of multipattern fake iris. The proposed method learns the features of different fake iris patterns by CNN and classifies the genuine or fake iris images by hierarchical multi-class classification. This classification takes various characteristics of different fake iris patterns into account. All kinds of fake iris patterns are divided into two categories by their fake areas. The process is designed as two steps to identify two categories of fake iris images respectively.

In [67] proposed an open source presentation attack detection (PAD) solution to distinguish between authentic iris images (possibly wearing clear contact lenses) and irises with textured contact lenses. This software can serve as a baseline in various PAD evaluations, and also as an open-source platform with an up-todate reference method for iris PAD.

In [68] presented a review of the recent progress in iris liveness detection. were categorize iris liveness detection approaches into sensor-level method, which add extra hardware to detect vital signal of subjects, and feature-level method, which use algorithm implemented in software to analysis liveness of the presentation.

Table 2 shows a summary of the Presentation Attack Detection techniques and their limitation.

TABLE II A BRIEF SURVEY OF PRESENTATION ATTACK DETECTION TECHNIQUES

Author (s) /year	Problem Statement	Proposed Solution (technique)	Measurements / Metrics/ dataset	Performance (Result)/ advantages	Notes (limitation) Disadvantages
Jinyu Zuo (2007)	Since there are not available large or medium size database, the designers claim high performance when they test their algorithm in small data.	They describe a model-based method to evaluate the performance and generate iris images using Gabor Filter-Based iris recognition system	FAR: False Accept Rate CASIA dataset, ICE-I datasets, UBATH database	The FAR 1% for identification performance (1:M).	
Kang Ryoung Park (2008)	It is difficult to recognize the real corneal specular reflections (SRs) and the noncorneal one which happened because of the eyeglasses. In order to capture a good iris image, it is needed to zoom the image and using a focus camera however that it is difficult to do with phones' camera.	They propose a new method to detect the genuine iris in corneas of subjects with glass. They employ Adaboost Eye Detector to detect SRs robustly and detect eye (iris) region.	- EER (Equal Error Rate) - Correct rate detection CASIA (version 1) database, CASIA (version 3) database	The rate of correct iris detection is 99.5% (for images without glasses) and 98.9% (for images with glasses or contact lenses) The EER 0.05% accuracy of iris authentication.	More field tests will be required.
Zhuoshi Wei (2008)	Developing new iris recognition algorithms evaluated on relatively small databases. The drawbacks of those database are none of the algorithms has gone through extensive testing, making the performance on large databases unpredictable and algorithms database is dependent and lacking of generalization	They present a framework to synthesize large realistic iris databases, providing an alternative to iris database collection. They use iris patch as basic element to characterize visual primitive of iris texture, and then patch-based sampling is applied to create an iris prototype. Then a set of pseudo irises with intra-class variations are derived from the prototype.	EER (Equal Error Rate) (CASIA DB, BATH DB, Syn1 DB, Syn2 DB)	Experimental results: real vs. synthetic databases CASIA DATABASE (0.7193% EER), BATH DB (0.0806% EER), Syn1DB (0.8204% EER), Syn2 (0.1138% EER)	
Sarah E. Baker (2010)	The assumption of non-cosmetic contact lenses has not or less effect on iris recognition system in term of performance and convenience.	They analyze 12,003 images from 87 subjects wearing contact lens and 9697 images from 124 subjects are not weaning contact lens. They utilize (irisBEE and VeriEye algorithms.), for evaluating.	False Rejection Rate (FRR) The dataset they used (contains a of 2953 iris images from 132 subjects)	VeriEye system is reported to perform better than other recognition systems. Matches involving images of soft contact lenses and ill-fitting artifacts obtain FRR about eighteen times than of matches between images with no contact lenses.	
Yuqing He (2010)	It is easy to frog the biometric treat by using the spoofing attacks, many types of liveness detection have limitation when implement in real recognition system.	They propose a liveness detection method by combining a special hardware structure and image texture analysis. Then they implement it using eye's optical features under different position of the infrared illumination.	FAR (False Accept Rate), FRR (False Reject Rate). (They produce dataset for their method)	They use 100 images for testing. Contain 20 classes and 5 images in each class. With the threshold of 2.35 they obtain False Accept Rate (FAR) as 0.03 and the False Reject Rate (FRR) as 0.06.	
Javier Galbally (2012)	Many researches have been conducted on spoofing attacks in sensor phase, those attacks difficult to detect because of using synthetic biometric traits such as print papers and synthetic traits.	They introduced database (ATVS-Fir). They propose PAD scheme based on quality and related measures on iris and test PAD method on their database using the best performing features are selected using the Sequential Floating Feature Selection (SFFS) algorithm	correctly classified (real or fake) samples, proving this (ATVS-Fir)	100% correctly classified (real or fake) samples	
James S. Doyle (2013)	The previous result shown a person wearing contact lenses (cosmetic, soft) the rate of false non-match increase compares with who does not wear, iris recognition system needs automatically distinguish between the person wearing (cosmetic, soft) contact lenses and who no wear	They present approach to classifying an iris image into one of three categories (textured contact lens, non-textured contact lens and no contact lens using Modified Local Binary Pattern analysis. In addition, they introduce Notre Dame Cosmetic Contact Lenses 2012 database (ND CCL 2012)	Accuracy detection rate Notre Dame Cosmetic Contact Lenses 2012 database (ND CCL 2012)	96.5% correct detection of iris images.	Their approach is able to detect 262 of 400 no-lens images. (the distinguish between real iris and soft lenses still open challenges)
Naman Kohli (2013)	Contact lenses, specially color cosmetic lens, obfuscate the iris pattern and hide features which leads to reduce the accuracy of the iris recognition system.	They analyze the effect of contact lenses on iris recognition system and provide a new database contained image with lenses (prescription and cosmetic lenses) They use (VeriEye commercial software) to understand the effect of contact lenses on iris verification.	(False Accept Rate) FAR IIIT-D Contact Lens Iris database (CLI)	Normal gallery-probe images yield 99.36% verification accuracy whereas with lens 0.01% false accept rate (FAR). When both gallery and probe images are with colored lenses, the verification accuracy reduces to only 50-60%. Other combinations of gallery probe pairs, the verification accuracy at 0.01% FAR is affected by cross sensor matching. With color gallery probe combination, the verification accuracy drops to 5%. VeriEye gives a score of zero for impostor matches and any score greater than zero denotes a genuine match. By applying lens detection algorithm, the accuracy improves to 94.41%.	
James S. Doyle (2013)	Available database for automatic detection on contact lenses for iris recognition in acquired phase contained one type of contact lenses from the same	They highlight a potential contact lens algorithm for detect texture lens. They employ Modified Local Binary Pattern Analysis to each region of each image at multiple scales to produce feature values.	Their database	the training data of one type of textured contact lens detection composition of the training data the classifier detect 100% of textured lenses and less than 60% when trained with two type and consider the third as	

	manufacture and Lack of diversity in sensor.			a new type, the performance degradation minimum of 4% to a maximum of 43%, other result shown degradation in performance when using different types of sensor.	
Czajka (2013)	There is no benchmark (reference) database of iris image printout which can be used for liveness detection and iris recognition assessments. Iris recognition system is vulnerable against presentation attacks.	Author presents a reference database of iris image printout (LivDet-Iris Warsaw 2013). Author proposes a liveness detection method for iris recognition based on Amplitude Frequency Analysis.	The lowest Equal Error Rate (EER), The lowest rate of living eyes rejection (i.e. false rejection rate – FRR) fake sample accepted, rate of imitation acceptance (i.e. false acceptance rate – FAR) with no rejections of authentic eyes, The amplitude frequency analysis, real iris image, fake iris image. LivDet-Iris Warsaw 2013	The winning approach accepts only 5% of imitations (with no authentic eyes rejection). In other words, his method is able to detect 95% of quality-controlled printouts, simultaneously not interfering with the existing iris recognition processes.	This approach does not apply on the patterned contact lenses.
David (2013)	It is necessary to get a guide reference for choosing the appropriate liveness detection techniques for iris recognition system	They conduct a competition between 3 algorithms in the same databases (ND Cosmetic Contact Lenses 2013 Dataset (NDCLD'13), LivDet 2013 Liveness Detection-Iris -- Warsaw Subset, and Iris Clarkson 2013.	False Reject Rate (FRR), False Accept Rate (FAR). NDCLD'13, LivDet 2013 Liveness Detection-Iris -- Warsaw Subset, and Iris Clarkson 2013 databases	The winner is Federico with a rate of falsely rejected live samples of 28.6% and the rate of falsely accepted fake samples of 5.7% across all three datasets.	Not all competitors accept to test their algorithms in the propose databases.
Jonathan Connell (2013)	The fashion industry of contact lenses developed with different patterns that lenses available and very affordable price, that uses for thwarting or spoofing iris	They propose a method for detect contact lenses using Structured Light Projection to produce contour changes in a stripe pattern to detect a contact lens.	Maximum Deviation,	maximum deviation for Naked eye 6.9 degrees and normal contact 6.4 degrees and they observe in the patterned contact case 9.1 degrees	They tasted their method on the blue eye contact lenses only, limit of pictures tested total images are 24 over 6 type of contact lenses
Jukka Komulainen (2014)	The generalization capability for detect iris contact lenses are not effective because they are detecting a specific type of texture lenses	They propose a method for PAD detection rely on Binarized Statistical Image Features (BSIF) for generalized cosmetic contact lens detection.	Equal Error Rate (EER) NDCLD DB	Their approach shown excellent ability for generalization 0.14% and 0.88% EER from across unseen printing signatures and different iris sensors	
Priyanshu Gupta (2014)	Presentation attacks techniques can be used for impersonation or change of identity and increase the rate of false acceptance or false rejection.	They use three descriptors in (Local Binary Pattern) LBP to encodes the texture feature of an image, GIST for providing a low-dimensional representation of an image, and Histogram of Oriented Gradients (HOG) uses to find the local object appearance and shape within an image by the distribution of local intensity gradients or edge directions. Then Support Vector Machine (SVM) used for matching.	Classification accuracy They introduce IIITD iris spoofing database	They use 50% training and 50% testing in database. Original vs Print+Scan (LBP+HOG) 92.32 Original vs Print+Capture (LBP+HOG) 72.38% Original (LBP+HOG) 45.09% Print+Scan (LBP+HOG) 84.64% Print+Capture (LBP+HOG) 99.67% Combined (LBP+HOG) 76.47%	
Daksha Yadav (2014)	Contact lens especially textured cosmetic lens is a challenge to iris recognition as obfuscates the natural iris patterns	They analyze the impact of contact lens on iris recognition. To evaluate the performance, they use VeriEye software and the databases (IIIT-D Iris Contact Lens) and (ND-Contact Lens). In addition, they present lens detection algorithm to detect contact lenses and improve iris recognition performance. They use for segmentation commercially available iris recognition SDK3 and Modified Local Binary Pattern (LBP) analysis for the three regions of each image pupil, iris, and sclera.	Accuracy (IIIT-D Iris Contact Lens) and (ND-Contact Lens) databases.	Their obtain the textured contact lenses can cause the false-non-match to exceed 90%. There for textured contact lenses could provide an effective way for someone on an iris recognition watch list to evade detection. Textured contact lenses can be automatically detected at a level of 95% accuracy or more for a wide range of sensors.	
Ana F. Sequeira (2014)	Iris recognition system in biometric attackable for many attacks specially spoofing iris attack on the sensor	They conduct six methods for liveness detection between 6 participants competition. The database they use for testing MobILive DB	False Acceptance Rate (FAR), False Rejection Rate (FRR) and Mean Error Rate (MER) (FAR AND FRR) MobILive DB	Best performance win (FedericoII) university, Result In term of (FAR, FRR, MER) the winner is IIT Indore (0.00, 0.50, 0.25) respectively and the worst HH university (29.25 ,7.00, 18.13)	

Zahid Akhtar (2014)	Extract features with low computational power still challenge. Furthermore, there are no liveness detection methods particularly concentrate on mobile applications.	They propose a method for detect a spoof attack in mobile devices for multiple biometric systems (face, fingerprint and iris) to detect spoofing attacks in mobile applications by using real-time feature description based on order permutations, named Locally Uniform Comparison Image Descriptor (LUCID). Then results are fed to Support Vector Machine (SVM) classifier.	Half Total Error Rate (HTER), (ATVS) iris database and (Notre Dame) dataset	Their performance result is 1.03±0:34 HTER in (ATVS) iris dataset and 0.07±0:67 HTER on Notre Dame database. Though the fake samples taken into account are high quality spoofed contact lenses for Iris (Notre Dame) dataset.	
Fernando Alonso (2014)	Iris detection methods depend on NIR sensor which provide grey-scale images that not found in new mobile devices such as smart phone.	They propose a new method for iris detection use of images captured in visible range with color (RGB) information. The utilize Gary-Level Co-Occurrence textural features and SVM classifiers for the task of fake iris detection.	correct classification rate (CCR) MobBIOfake database	Reaching a Correct Classification Rate (CCR) over 96%	
Diego Gragniello (2015)	Authentication systems vulnerable and easily to fool by attacks based on high quality printed	They propose a method fast and accurate technique to detect High quality print attack based on local binary pattern (LBP)descriptor MobBIOFake and MICHE databases	Half Total Error Rate (HTER)	Performance of LBP descriptors on MobBIOfake FFR 0.25 and HTER 4.38 on image and FFR 0.00 & HTER 0.25 On residual. The Performance of residual-based LBP descriptors on MICHE for HQ print Screen FFR 0.00, HTER 0.00 and the result on Screen FFR 0.16, HTER 0.23	
JAMES S. DOYLE (2015)	Three issues emerge consider while creating algorithms for presentation attack detection of contact lenses the first issue is segmentation accuracy and the second issue is the trained images different from sensor to sensor and the third one is how generalized a brand of the textured contact lenses in the training images not seen while training data.	They analyze all the three problems and prove that there is effect on the iris recognition system, they show a type of texture lenses significant impact on performance of texture lens detection. They employ the segmentation with (*Local binary patterns*) LBP. The dataset they used (Notre Dame Contact Lens Detection 2015 (NDCLD`15) Dataset) the dataset used tow sensors (LG400, AD100)	Correct classification cation rates (CCR) (Notre Dame Contact Lens Detection 2015 (NDCLD`15) Dataset) the dataset used tow sensors (LG400, AD100)	For the AD100 set, the CCR is 99.5%, for LG4000 the CCR is 99.67%, and combined the CCR is 99.75%. The CCR of the homogenous case is higher than the heterogeneous CCR. A drop is observed from 100% in the homogenous case to just over 95% in the heterogenous case. The accuracy degrades for novel lens type the CCR on novel lenses is about 86%. This increases dramatically to almost 98% when data from four manufacturers is used in training.	
Kiran B. Raja (2015)	The print screen and print paper are challenges for biometric in the sensor phase	They propose technique to detect the artefact iris images by decomposing the images into Laplacian pyramids of various scales and obtain frequency responses in different orientations. The obtained features are classified using a support vector machine with a polynomial kernel.	Classificiation Error Rate (ACER) (Presentation Attack Video Iris Database' (PAVID) and LiveDet Iris 2013)	The proposed technique has provided an (ACER) 0.64% on PAVID (They proposed database) and 1.37% ACER on LiveDet iris dataset	
Pedro Silva (2015)	Liveness detection methods for contact lenses may affect with different textures of lenses and type of sensor manufacture	they propose approach uses a convolutional network to build a deep image representation and an additional fully-connected single layer with softmax regression for classification to countermeasure issue of (three detection problem: images with textured (colored) contact lenses, soft contact lenses, and no lenses)	2013 Notre Dame and IIIT-Delhi database	Their method improve the performance 30% over the state-of-the-art approach, SOTA	C
Kiran B. Raja (2015)	In smart phone environment there has not earlier works for detect iris recognition in visible spectrum. And specially with video attack in smart phone platform that led to identity spoofing, presentation or direct attack	They first researcher's propose scheme for detect the presentation video attack in visible spectrum in smart phone, using phase information obtained from eye area, They proposed scheme employs modified Eulerian Video Magnification (EVM).	Average Classification Error Rate (ACER) They introduce database for Video Presentation Attack (VSSIRISV database)	They rustle is rebuts and get 0% ACER in the 11th frame	

R Ragha vendra (2015)	Vulnerability of iris recognition systems still a problem du the different presentation attacks that fail to ensure the reliability when adopting in real life scenario	They propose a novel Presentation Attack Detection (PAD) scheme based on Multi-scale Binarized Statistical Image Features (M-BSIF) and linear Support Vector Machines (SVM), they utilize for iris segmentation and normalization (OSIRIS V4.1)	Equal Error Rate (EER) They introduce (Visible Spectrum Iris Artefact (VSIA) database)	VSIA database indicate the strong vulnerability of the baseline iris recognition system. The overall performance of the proposed scheme is deceived to the greater extent as 92:22% of the artefact samples from VSIA database can successfully intrude the baseline system Their proposed presentation attack detection scheme based on M-BSIF and SVM has revealed the outstanding performance on VSIA database with a small ACER of 0:29% on the artefacts generated using Attack 1 and ACER of 0% on remaining four different kind of attacks available with-in VSIA database. the proposed scheme on three different relatively large scale publicly available databases corresponding to both visible and NIR iris have shown the best results with an outstanding performance with ACER of 0% on both MobILive 2014 and ATVS Fake iris database. While the proposed scheme has shown the best performance of ACER of 1:27% on LivDet Iris 2013 Warsaw dataset and emerged as the best PAD scheme for iris recognition system.	C , D
David Yamba y (2017)	spoofing attack such as printed paper and pattern contact lenses can be used to fool the iris recognition process. to detect this vulnerability different proposed solutions used, yet the independent evaluations and comparisons are rare	They conduct the second compotation LivDet-Iris 2015 after LivDet-Iris 2013 between four competitor	rate of rejected live samples and rate of accepted spoof samples (Clarkson LG Dataset, Clarkson Dalsa Dataset, Warsaw 2015 IrisGuard Dataset)	The winner is Federico Algorithm with a rate of rejected live samples of 1.68% and rate of accepted spoof samples of 5.48%.	
Naman Kohli (2016)	In PAD algorithms that detect a specific type of attack without detect various attacks in same time	they propose a framework to detect spoofed iris images attacks in real world scenarios. Their framework learns local structural changes by projecting the original image in the Zernike moment space. they also learn textural information through Local Binary Patterns (LBP) with Variance that accounts for contrast information. They propose a feature level fusion of these complementary features and finally they train a neural network classifier to detect among fake iris images and real images.	classification accuracy combined spoofing database (CSD)) collected from multi available databases	Their proposed DESIST framework detects spoofed iris images with a classification accuracy of 82.20%	
Naman Kohli (2017)	The author design a new presentation attack using synthetic iris images that attack that prove the iris recognition still able to attack	They present a presentation attack using deep learning based synthetic iris generation. Their attack applied on the state of art presentation attack detection framework DESIST	Equal Error Rate (EER) IIITD Contact Lens Database, IIT Delhi Iris Database and MultiSensor Iris Databases	Iris PAD accuracy on the synthetically generated iris images using the proposed iDCGAN framework is 85.95% with equal error rate (EER) of 14.19%. PAD performance of DESIST on SDB is 92.17% with an EER of 7.09%	C
David Yamba y (2017)	Spoofing attack using printed pattern or printouts of contact lenses can be used to effect on biometric security system	They conduct the result of - Iris Liveness Detection Competition 2017, between three competitors (Anonymous Anon1, Universita' degli Studi di Napoli UNINA and Chinese Academy of Sciences CASIA)	Bona Fide Presentation Classification Error Rate (BPCER) Attack Presentation Classification	Anon1 performed the best with a combined error rate of 9.03% with 14.71% APCER and 3.36% BPCER Result from cross sensor challenge UNINA saw a	C , D
			Error Rate (APCER) -The databases used (Clarkson dataset for LivDet-Iris 2017, Warsaw dataset used in LivDet-Iris 2017 competition, Notre Dame Contact Lens Detection 2015 (NDCLD15), IIITD-WVU dataset (they merge two of databases IIITD databases used for training and testing database captured at WVU using mobile iris sensor).	sharp decrease in BPCER but a stark increase their APCER with a combined error of 0.03% and 50.43%	
Daksh a Yadav (2017)	there are a few databases aiming iris recognition in visible spectrum which capture image in unconstrained environment. The visible spectrum recognition vulnerable same as NIR to different type of attacks	they analysis the effect of textured contact lenses in visible light on iris recognition process -they test 3 algorithms on their proposed database (DESIST- Weighted LBP- Multiscale BSIF)	they introduced UVCLI database.	They result led to the performance degrades over 25%. Then they evaluate three state-of-the-art PAD detecting multiple attacks but with (NIR ILLUMNATION) on their database (visible illumination) and highest PAD accuracy get 82.85%	C , D
Daksh a Yadav (2018)	There is not database contain most of spoofing attacks with indoor and outdoor environment and the images captured by mobile phone it's imperative to evaluate algorithms in detecting contact lenses in iris images captured in unconstrained scenarios	They first detailed analysis of the effect of textured contact lenses on iris recognition in visible spectrum. They evaluate three iris presentation attack detection (PAD) algorithms on their proposed database (DESIS, Weighted LBP and Multiscale BSIF) They introduce the first contact lens database in visible spectrum	equal error rates (EER) (Unconstrained Visible Contact Lens Iris (UVCLI))	they observe that textured contact lenses degrade the visible spectrum iris recognition performance by over 25% the evaluated PAD algorithms first the result for Unseen Subject Partition DESIS is the highest accuracy 82.85%, Weighted LBP 78.49% and Multiscale BSIF 63.30% second Unseen Subject Partition and Environment DESIST 74.60%, Weighted LBP 73.88% and Multiscale BSIF 56.29%	
ADA M CZAJ KA (2018)	Author mention to prestation attack detection for iris is still open problem	They conduct a review for the methods of presentation attack and their impacts.			C
Cunjia n Chen (2018)	Presentation attacks speared that lead to error in recognition system .	Their solution is first method that detect eye in term of iris and presentation attack detection, they employ CNN technique for localization and PAD in same time	Correct Classification Rate (CCR), Attack Presentation Classification Error Rate (APCER), Bonafide Presentation Classification Error Rate (BPCER) LivDet-Iris-2015-Warsaw,CASIA-Iris-Fake, ND-Contact, BERC-Iris-Fake and LivDet-Iris-2017-Clarkson datasets	The result for iris detection on two databases (LivDet-Iris-2015-Warsaw get Precision 100% and Recall 100%, for CASIA-Iris-Fake Precision 99.83% and Recall 99.67%) They proposed MT-PAD method results (for ND-Contact dataset CCR 99.58, APCER 0.25 and BPCER 0.5) and for (CASIA-Iris-Interval&Syn dataset CCR 100, APCER 0 and BPCER 0 For cross sensor result (in BERC-Iris-Fake CCR 97.75, APCER 3,25 and BPCER 20.44) and in (LivDet-Iris-2017-Clarkson dataset CCR 86.21, APCER 0.88 and BPCER 20.44)	C
Maria De Marsic o (2018)		they conduct the first international contest specifically devoted to iris/ocular recognition using data acquired of multiple handheld devices	Equal Error Rate (EER)		

Sheng-Hsun Hsieh (2018)	The PAD methods could detect spoofing attack but in case of contact lenses the system will reject recognition and need subject's cooperation to take off and then do the process again	They propose first method for iris recognition system that could detect contact lenses from hybrid (software and hardware) technique That can analysis the statically spectral domain (their assumption depend on iris texture and contact lenses separate on the statically spectral domain by removing contact lenses from mixed image without ask subject remove his contact lenses) for iris recognition they used (Daugman algorithm)	False Rejection Rate (FFR) Database containing 200 test image pairs from 20 CCL-wearing subjects	After conducting (Independent Component Analysis, ICA), and masking process for cosmetic contact lenses - wearing subjects, the authentic and impostor (Hamming Distance)HD distribution was separated farther, with moderate FRR (0.57%) and EER (0.26%). -The total of 200 enrolment images and 200 test naked eye image as the baseline test, the recognition system had performance as SI = 8.82, FRR = 0% when FAR was set to 0.1%, and the EER was 0%, - When the subjects wore (cosmetic contact lenses) CCLs, both FRR (10.52%) and EER (1.94%) increased dramatically in comparison with the naked eye, database containing 200 test image pairs from 20 CCL-wearing subjects as the proof of concept, the recognition accuracy (False Rejection Rate: FRR) was improved from FRR = 10.52% to FRR = 0.57% with the proposed ICA anti-spoofing scheme.	C
Zihui Yan (2018)	Algorithms using CNN network does not classify a multi type of spoofing iris pattern in specified category. -Unified training ignores the unique fake characteristics of each model. These uniqueness information can increase the accuracy of iris liveness detection with hybrid patterns.	They proposed a Hierarchical Multiclass Iris Classification (HMC) for liveness detection based on CNN. They choose Spoornet, Weighted LBP, HVC+SPM and MCNN for comparison with their algorithm	CCR (Correct Classification Rate) FAR (False Accept Rate) FRR (False Reject Rate) (NDContact, CASIA-Iris-Interval, CASIA-Iris-Syn and LivDet-Iris-2017-Warsaw) and hybrid dataset which consists of ND-Contact and LivDet-Iris-2017-Warsaw datasets	algorithm achieves 100% CCR on ND-Contact dataset, 99.91% CCR on CASIA-Iris-Interval & Syn datasets and 99.15% CCR on LivDet-Iris-2017-Warsaw Dataset For hyped dataset use 70% training. And the rest is used for testing. They achieve 100% CCR on ND-Contact dataset, 99.91% CCR on CASIA-Iris-Interval & Syn datasets and 99.15% CCR on LivDet-Iris-2017-Warsaw dataset respectively.	C
Joseph McGrath (2018)	The problem for many solutions of PAD detection because there isn't open source platform for PAD especially with unknown attacks to maintain the PAD for iris methodology for an improved and evlaoute solutions	they provide an open source PAD for detect textured contact lenses their method use Binary Statistical Image Features (BSIF) to extract PAD-related features, which are classified by an ensemble of SVM classifiers.	Correct Classification Rate (CCR) NDCLD'15 Database	SVM models trained with the NDCLD'15 Database correct classification rate exceeds 98%	C
Yangyu (2018)	The biometric system is vulnerable to the different type of attacks (Photo Attacks, Video Attacks, Contact-Lens Attacks, ficial-eye attacks	They conduct a survey for the techniques which used to resist presentation attacks and analyze its performance.			C

II. PROPOSED RESEARCH WORK

Biometric Iris Recognition System is now being used commonly as a perfect alternative to passwords on mobile devices. However, current Iris Recognition Systems are vulnerable against presentation attacks and lack of stability through time which has declined their usage and performance [69] and [8]. Many Presentation Attack Detection (PAD) (liveness detection methods) have been proposed to determine whether there is a live person or an artificial replica in front of the biometric sensor. Until now, the problem is unsolved due to hardship in finding discriminative and computationally inexpensive features for spoofing attacks [6][70][71]. Moreover, previous PAD approaches are not explicitly aimed for mobile biometric, thus principally unsuited for portable devices. In addition, the proposed PAD algorithms are designed to mitigate a specific kind of the presentation attacks and not all on the same time. As sequence the attacker may perform different presentation attacks which make the IRS vulnerable. Figures 1 and 2 shows the flowchart for the new proposed Presentation Attack Detection (PAD) for Iris Recognition System on Mobile Devices.

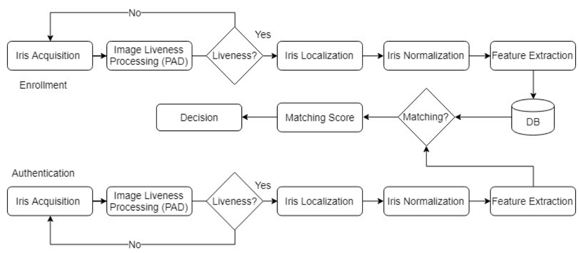

Figure 1. The flowchart of the proposed method

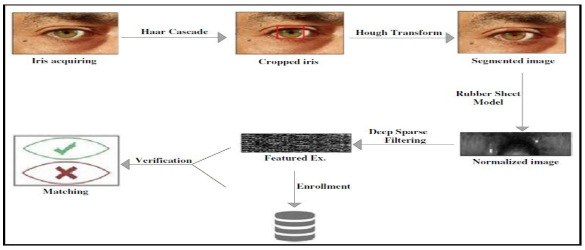

Figure 2. The flowchart of the proposed new algorithm.

III. CONCLUSION

With the increasing needs of security in our daily life, iris biometrics has become reliable identity, and it serve as the keystone for modern biometric system. In this paper we presented a survey of the different techniques used for Presentation Attack Detection (PAD) for Iris Recognition System on Mobile Devices. And also we are proposing a new Presentation Attack Detection (PAD) method which suitable for mobile environment. The proposed Iris Recognition with Presentation Attack Detection PAD technique Expected will provide a strong resistance against the presentation attacks type in iris recognition system on mobile devices.

Acknowledgments

The authors would like to thank the Deanship of Scientific Research at Prince Sattam Bin Abdulaziz University, Alkharj, Saudi Arabia for the assistance.

IV. REFERENCES

[1]. Jain, Anil K., Arun A. Ross, and Karthik Nandakumar. *Introduction to biometrics*. Springer Science & Business Media, 2011.

[2]. Jain, Anil K., Karthik Nandakumar, and Arun Ross. "50 years of biometric research: Accomplishments, challenges, and opportunities." *Pattern Recognition Letters* 79 (2016): 80-105.

[3]. Jiang, Richard, et al. *Biometric Security and Privacy*. Springer International Publishing AG, 2017.

[4]. Jan, J. Daugman. "How Iris Recognition works, IEEE Transactions on Circuits and systems for video Technology." (2004).

[5]. Quinn, George W., et al. *IREX IX Part One: Performance of Iris Recognition Algorithms*. US Department of Commerce, National Institute of Standards and Technology, 2018.

[6]. Czajka, Adam, and Kevin W. Bowyer. "Presentation attack detection for iris recognition: An assessment of the state-of-the-art." *ACM Computing Surveys (CSUR)* 51.4 (2018): 86.

[7]. El Baz, Didier, and Jerry Gao. "2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI 2017." *2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI 2017*(2017).

[8]. Gupta, Sandeep KS, Tridib Mukherjee, and Krishna Kumar Venkatasubramanian. *Body area networks: Safety, security, and sustainability*. Cambridge University Press, 2013.

[9]. Maiorana, Emanuele, et al. "On the vulnerability of an EEG-based biometric system to hill-climbing attacks algorithms' comparison and possible countermeasures." *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*. IEEE, 2013.

[10]. Kohli, Naman, et al. "Synthetic iris presentation attack using iDCGAN." *2017 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE, 2017.

[11]. Komulainen, Jukka, Abdenour Hadid, and Matti Pietikäinen. "Contact lens detection in iris images." Iris and Periocular Biometric Recognition, Christian Rathgeb and Christoph Busch (Eds.). IET, London, UK (2017): 265-290.

[12]. Yambay, David, et al. "LivDet iris 2017—Iris liveness detection competition 2017." *2017 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE, 2017.

[13]. Kohli, Naman, et al. "Detecting medley of iris spoofing attacks using DESIST." *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. IEEE, 2016.

[14]. Thavalengal, Shejin, and Peter Corcoran. "User authentication on smartphones: Focusing on iris biometrics." *IEEE Consumer Electronics Magazine* 5.2 (2016): 87-93.

[15]. Cho, Dal-ho, et al. "Pupil and iris localization for iris recognition in mobile phones." Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD'06). IEEE, 2006.

[16]. Raja, Kiran B., et al. "Robust iris recognition using light-field camera." 2013 Colour and Visual Computing Symposium (CVCS). IEEE, 2013.

[17]. Jeong, Dae Sik, et al. "Iris recognition in mobile phone based on adaptive gabor filter." International Conference on Biometrics. Springer, Berlin, Heidelberg, 2006.

[18]. Kurkovsky, Stan, Tommy Carpenter, and Caleb MacDonald. "Experiments with simple iris recognition for mobile phones." 2010 Seventh International Conference on Information Technology: New Generations. IEEE, 2010.

[19]. Sastry, A. V. G. S., and B. Durga Sri. "Enhanced Segmentation Method for Iris Recognition." International journal of computer trends and technology 4.2 (2013): 68-71.

[20]. Raja, Kiran B., et al. "Smartphone based visible iris recognition using deep sparse filtering." Pattern Recognition Letters 57 (2015): 33-42.

[21]. Adhau, Ankita Satish, and D. K. Shedge. "Iris recognition methods of a blinked eye in nonideal condition." 2015 International Conference on Information Processing (ICIP). IEEE, 2015.

[22]. Shekar, B. H., and Sharada S. Bhat. "Steerable riesz wavelet based approach for iris recognition." 2015 3rd IAPR Asian Conference on Pattern Recognition (ACPR). IEEE, 2015.

[23]. Smith, Brian A., et al. "Gaze locking: passive eye contact detection for human-object interaction." Proceedings of the 26th annual ACM symposium on User interface software and technology. ACM, 2013.

[24]. Galdi, Chiara, and Jean-Luc Dugelay. "Fusing iris colour and texture information for fast iris recognition on mobile devices." 2016 23rd International Conference on Pattern Recognition (ICPR). IEEE, 2016.

[25]. De Jesús, Rosales-Banderas José, et al. "Methodology for iris scanning through Smartphones." 2016 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, 2016.

[26]. Ali, Syed Arslan, et al. "Iris recognition system in smartphones using light version (LV) recognition algorithm." 2017 23rd International Conference on Automation and Computing (ICAC). IEEE, 2017.

[27]. Alonso-Fernandez, Fernando, Reuben A. Farrugia, and Josef Bigun. "Learning-based local-patch resolution reconstruction of iris smart-phone images." 2017 IEEE International Joint Conference on Biometrics (IJCB). IEEE, 2017.

[28]. Hofbauer, Heinz, et al. "Mobile NIR Iris Recognition: Identifying Problems and Solutions." 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS). IEEE, 2019.

[29]. Elrefaei, Lamiaa A., et al. "Developing Iris Recognition System for Smartphone Security." Multimedia Tools and Applications77.12 (2018): 14579-14603.

[30]. Zhang, Qi, et al. "Deep feature fusion for iris and periocular biometrics on mobile devices." IEEE Transactions on Information Forensics and Security 13.11 (2018): 2897-2912.

[31]. Deshpande, Bhagyashree, and Deepak Jayaswal. "Fast and Reliable Biometric Verification System Using Iris." 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT). IEEE, 2018.

[32]. Odinokikh, G. A., et al. "High-Performance Iris Recognition for Mobile Platforms." Pattern Recognition and Image Analysis28.3 (2018): 516-524.

[33]. Zuo, Jinyu, Natalia A. Schmid, and Xiaohan Chen. "On generation and analysis of synthetic iris images." IEEE Transactions on Information Forensics and Security 2.1 (2007): 77-90.

[34]. Park, Kang Ryoung, et al. "A study on iris localization and recognition on mobile phones." EURASIP Journal on Advances in Signal Processing 2008 (2008): 20.

[35]. Wei, Zhuoshi, Tieniu Tan, and Zhenan Sun. "Synthesis of large realistic iris databases using patch-based sampling." 2008 19th International Conference on Pattern Recognition. IEEE, 2008.

[36]. Baker, Sarah E., et al. "Degradation of iris recognition performance due to non-cosmetic prescription contact lenses." Computer Vision and Image Understanding 114.9 (2010): 1030-1044.

[37]. He, Yuqing, et al. "Liveness iris detection method based on the eye's optical features." Optics and Photonics for Counterterrorism and Crime Fighting VI and Optical Materials in Defence Systems Technology VII. Vol. 7838. International Society for Optics and Photonics, 2010.

[38]. Galbally, Javier, et al. "Iris liveness detection based on quality related features." 2012 5th IAPR International Conference on Biometrics (ICB). IEEE, 2012.

[39]. Doyle, James S., Patrick J. Flynn, and Kevin W. Bowyer. "Automated classification of contact lens type in iris images." 2013 International Conference on Biometrics (ICB). IEEE, 2013.

[40]. Kohli, Naman, et al. "Revisiting iris recognition with color cosmetic contact lenses." 2013 International Conference on Biometrics (ICB). IEEE, 2013.

[41]. Doyle, James S., Kevin W. Bowyer, and Patrick J. Flynn. "Variation in accuracy of textured contact lens detection based on sensor and lens pattern." 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS). IEEE, 2013.

[42]. Czajka, Adam. "Database of iris printouts and its application: Development of liveness detection method for iris recognition." 2013 18th International Conference on Methods & Models in Automation & Robotics (MMAR). IEEE, 2013.

[43]. Yambay, David, et al. "LivDet-Iris 2013–Iris Liveness Detection Competition 2013."

[44]. Connell, Jonathan, et al. "Fake iris detection using structured light." 2013 IEEE International Conference on Acoustics, Speech and Signal Processing. IEEE, 2013.

[45]. Komulainen, Jukka, Abdenour Hadid, and Matti Pietikäinen. "Generalized textured contact lens detection by extracting bsif description from cartesian iris images." IEEE International Joint Conference on Biometrics. IEEE, 2014.

[46]. Gupta, Priyanshu, et al. "On iris spoofing using print attack." 2014 22nd International Conference on Pattern Recognition. IEEE, 2014.

[47]. Yadav, Daksha, et al. "Unraveling the effect of textured contact lenses on iris recognition." IEEE Transactions on Information Forensics and Security 9.5 (2014): 851-862.

[48]. Sequeira, Ana F., et al. "Mobilive 2014-mobile iris liveness detection competition." IEEE International Joint Conference on Biometrics. IEEE, 2014.

[49]. Akhtar, Zahid, Christian Michelon, and Gian Luca Foresti. "Liveness detection for biometric authentication in mobile applications." 2014 International Carnahan Conference on Security Technology (ICCST). IEEE, 2014.

[50]. Alonso-Fernandez, Fernando, and Josef Bigun. "Exploting periocular and RGB information in fake iris detection." 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, 2014.

[51]. Gragnaniello, Diego, Carlo Sansone, and Luisa Verdoliva. "Iris liveness detection for mobile devices based on local descriptors." Pattern Recognition Letters 57 (2015): 81-87.

[52]. Doyle, James S., and Kevin W. Bowyer. "Robust detection of textured contact lenses in iris recognition using BSIF." IEEE Access 3 (2015): 1672-1683.

[53]. Raja, Kiran B., Ramachandra Raghavendra, and Christoph Busch. "Presentation attack detection using laplacian decomposed frequency response for visible spectrum and near-infra-red iris systems." 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS). IEEE, 2015.

[54]. Silva, Pedro, et al. "An approach to iris contact lens detection based on deep image representations." 2015 28th SIBGRAPI Conference on Graphics, Patterns and Images. IEEE, 2015.

[55]. Raja, Kiran B., Ramachandra Raghavendra, and Christoph Busch. "Video presentation attack detection in visible spectrum iris recognition using magnified phase information." IEEE Transactions on Information Forensics and Security10.10 (2015): 2048-2056.

[56]. Raghavendra, Ramachandra, and Christoph Busch. "Robust scheme for iris presentation attack detection using multiscale binarized statistical image features." IEEE Transactions on Information Forensics and Security 10.4 (2015): 703-715.

[57]. Yambay, David, et al. "LivDet-Iris 2015–Iris Liveness Detection Competition 2015."

[58]. Kohli, Naman, et al. "Detecting medley of iris spoofing attacks using DESIST." 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS). IEEE, 2016.

[59]. Kohli, Naman, et al. "Synthetic iris presentation attack using iDCGAN." 2017 IEEE International Joint Conference on Biometrics (IJCB). IEEE, 2017.

[60]. Yambay, David, et al. "LivDet iris 2017—Iris liveness detection competition 2017." 2017 IEEE International Joint Conference on Biometrics (IJCB). IEEE, 2017.

[61]. Yadav, Daksha, et al. "Unconstrained visible spectrum iris with textured contact lens variations: Database and benchmarking." 2017 IEEE International Joint Conference on Biometrics (IJCB). IEEE, 2017.

[62]. Yadav, Daksha, et al. "Iris Presentation Attack via Textured Contact Lens in Unconstrained Environment." 2018 IEEE Winter Conference on Applications of Computer Vision (WACV). IEEE, 2018.

[63]. Chen, Cunjian, and Arun Ross. "A multi-task convolutional neural network for joint iris detection and presentation attack detection." 2018 IEEE Winter Applications of Computer Vision Workshops (WACVW). IEEE, 2018.

[64]. De Marsico, Maria, et al. "Insights into the results of miche i-mobile iris challenge evaluation." Pattern Recognition 74 (2018): 286-304.

[65]. Hsieh, Sheng-Hsun, et al. "A novel anti-spoofing solution for iris recognition toward cosmetic contact lens attack using spectral ICA analysis." Sensors 18.3 (2018): 795.

[66]. Yan, Zihui, et al. "Hierarchical multi-class iris classification for liveness detection." 2018 International Conference on Biometrics (ICB). IEEE, 2018.

[67]. McGrath, Joseph, Kevin W. Bowyer, and Adam Czajka. "Open Source Presentation Attack Detection Baseline for Iris Recognition." arXiv preprint arXiv:1809.10172 (2018).

[68]. Chen, Yangyu, and Weigang Zhang. "Iris Liveness Detection: A Survey." 2018 IEEE Fourth International Conference on Multimedia Big Data (BigMM). IEEE, 2018.

[69]. Sohankar, Javad, et al. "Systematic analysis of liveness detection methods in biometrie security systems." 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). IEEE, 2017.

[70]. Akhtar, Zahid, et al. "MoBio_LivDet: Mobile biometric liveness detection." 2014 11th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS). IEEE, 2014.

[71]. Poster, Domenick, Nasser Nasrabadi, and Benjamin Riggan. "Deep Sparse Feature Selection and Fusion for Textured Contact Lens Detection." 2018 International Conference of the Biometrics Special Interest Group (BIOSIG). IEEE, 2018.