Robust Scheme for Iris Presentation Attack Detection Using Multiscale Binarized Statistical Image Features

R. Raghavendra and Christoph Busch

***Abstract*— Vulnerability of iris recognition systems remains a challenge due to diverse presentation attacks that fail to assure the reliability when adopting these systems in real-life scenarios. In this paper, we present an in-depth analysis of presentation attacks on iris recognition systems especially focusing on the photo print attacks and the electronic display (or screen) attack. To this extent, we introduce 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. We also propose a novel presentation attack detection (PAD) scheme based on multiscale binarized statistical image features and linear support vector machines. Extensive experiments are carried out on four different publicly available iris artefact databases that have revealed the outstanding performance of the proposed PAD scheme when benchmarked with various well-established state-of-the-art schemes.**

***Index Terms*— Biometrics, iris recognition, anti-spoofing, presentation attacks.**

I. Introduction

BIOMETRIC systems have witnessed a large scale deployment in a wide range of security applications. Among the available biometric modalities, iris recognition is one of the most promising and widely adopted modalities. Iris biometrics have been a core technology component in very large scale deployments such as the Indian UIDAI (Aadhaar) project [1]. However, despite many advantages including reliable identity recognition, iris biometric systems are highly vulnerable especially at the sensor level to various kinds of presentation attacks. The goal of a presentation attack is to subvert a biometric system by presenting a biometric artefact of the legitimate user to the sensor. With the evolving knowledge in creating a biometric artefact (or spoof), it is possible to generate a high quality attack instrument in a cost effective manner that can be used to subvert an iris system.

Among various ways one can perform a presentation attacks against an iris recognition system, the easiest way is by presenting an image of a legitimate enrollee either by printing a photo or by displaying a photo using electronic screens such as tablets or mobile phone displays. The feasibility of these attacks on both visible and near infrared (NIR) iris recognition systems are acknowledged by the number of recent publications in this field [2]–[8], the organization of competitions [9], [10] and the evolution of standards [11] that show the strong importance to develop a technique to successfully detect and mitigate the presentation attacks in real-life scenarios. Thus in this work, we address presentation attacks at the sensor level using cost effective attacks namely: photo print attack and electronic screen (or display) attack.

Manuscript received June 30, 2014; revised November 2, 2014; accepted January 7, 2015. Date of publication February 5, 2015; date of current version March 13, 2015. This work was supported by the European Union Seventh Framework Programme FP7/2007-2013 under Grant 284862 for the large-scale integrated Project FIDELITY. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Stan Z. Li. *(Corresponding author: R. Raghavendra.)*

The authors are with the Norwegian Biometric Laboratory, Gjøvik University College, Gjøvik 2815, Norway (e-mail: raghu07.mys@gmail.com; christoph.bush@hig.no).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2015.2400393

II. Related Work

In recent years several Presentation Attack Detection (PAD) (or counter measures or spoof detection or anti-spoofing) algorithms were proposed that include both hardware and software based solutions. The idea of a hardware based PAD solutions is to include additional hardware components with the sensor that can detect the properties of the normal (or real or live) presentation to the sensor. Even though hardware based schemes have shown a high chance of detecting presentation attacks, they appear to be more expensive when compared to software based techniques. The idea of the software based approaches is to identify an artefact (or spoof samples or fake samples) once after it is captured and processed using various techniques to analyze the statistical characteristics of the generated image sample. The use of software based approaches exhibit additional advantages when compared to hardware based approaches such as [4]: non-invasive, fast, robust, user friendly and low cost. Thus in this work, we follow the software based approach to accurately detect an iris presentation attack.

The iris artefact detection by measuring the reflectance ratio between iris and sclera region is presented in [6]. Here, the reflectance ratio between iris and sclera region is measured in various wavelength to capture the variation of the reflectance ratio. Then, the captured variation is processed further to check whether the presented sample is or is not an artefact. This method is based on the principle that the artefact generated using printing will have similar material present in iris and sclera region. Hence it will exhibit the constant reflectance ratio variation when compared to normal (or live) image. However this method will demand to use additional light source that can emit various wavelength of the light and

further appears to show limited performance when artefact are presented with electronic displays.

Statistical texture features to detect the artefact iris samples were proposed in [12]. Here, the Gray Level Co-occurrence Matrix (GLCM) and Support Vector Machine (SVM) is employed to identify an artefact iris sample. However, this method will show the limited performance not only against the micro-texture method but also on those very high quality iris artefacts that are generated using glossy papers and intjet printing.

An iris artefact detection using a purkinje image with collimated IR-LED illumination is presented in [13]. The idea of this method is to calculate the theoretical positions and distances between the Purkinje images based on model of the human eye. However, this method demands additional hardware and also requires subject cooperation.

In [14], the boosted Local Binary Pattern (LBP) are introduced to detect the presence of an artefact iris. Given the iris image, this method will first extract the feature descriptors using LBP. Then Adaboot learning is applied to identify the artefact iris sample. The experimental results show the improved performance over the GLCM scheme. However, the training process of Adaboost is time consuming and also tedious.

A general iris classification framework that can also be used for artefact detection based on a hierarchical visual codebook is presented in [15]. The hierarchical visual codebook is based on combining two existing bag-of-words schemes namely: Vocabulary Tree (VT), and Locality-constrained Linear Coding (LLC). The experimental validation shows that, this combination can achieve the state-of-the-art performance for iris presentation attack detection.

An iris PAD scheme based on analyzing well established Image Quality Measures (IQM) together with a Quadratic Discriminant Analysis (QDA) classifier was introduced in [4]. Here, 25 different well established image quality measures are adopted along with the QDA classifier to identify a presentation attacks on the biometric system. Experimental results carried out on the ATVS-Fake NIR iris Database show an acceptable performance. However the performance of the IQM-QDA approach strongly depends on the reference image used to estimate the IQM. Thus the method is not very suitable for generalization.

In [2] and [16], Image Frequency Analysis (IFA) using Fourier transform is proposed to detect the artefact iris patterns from photo print attacks on the NIR iris system. However the use of the IFA technique has shown a limited performance on high quality iris artefact samples especially with the print iris attack in which artefacts are obtained using high quality glossy paper.

In [8], both qualitative features that include frequency analysis, local contrast, global contrast, frequency distribution rates and statistical texture features using GLCM are explored. All these features are combined at feature level and a final decision is carried out using Support Vector Machine (SVM). Experiments carried out on four different publicly available database show the moderate performance of this scheme. Nevertheless, the main limitation of this scheme is the requirement of an accurate segmentation as it captures the features from iris sub-regions.

In [17], variation in the brightness of an iris pattern induced by a pupillary reflex is used to identify the artefact iris samples. However the use of pupillary information may change when different sensors are used and the approach may not be very robust when visible spectrum is employed.

Thus, based on the above reported works, it can be noted that the State-of-the-Art (SOTA) schemes are based either on an additional lighting components [6], [17] or by measuring the features that are too specific for the installed sensor [13] or the use of complicated feature representation and classification schemes [2], [8], [14], [15]. Furthermore, there is also a lack of analysis that can demonstrate the applicability of the existing SOTA schemes to work equally good on both visible and near infrared iris PAD. Finally, most of the SOTA schemes are limited to address only the iris print artefact. Therefore, in this work, we address the iris presentation attack detection especially for both photo print and electronic screen attack. In particular, (1) we present an in-depth analysis on the vulnerability of the iris recognition system for both photo print and electronic screen attacks and (2) we also present a novel algorithm to improve the performance of the iris recognition system by mitigating a various types of presentation attacks (or spoof attacks) in both visible and near infrared spectrum. Following are the main contributions of this work:

- *Novel Iris PAD Algorithm:* We present a novel PAD algorithm based on the Multi-scale Binarized Statistical Image Features (M-BSIF) and linear Support Vector Machines (SVM) that combines the micro-texture variations extracted from multiple scales at both feature and decision level to accurately identify the presentation attacks. To our knowledge this is the first work which address the presentation attack detection on iris recognition using M-BSIF features.
- *New Database:* We introduce a new Visible Spectrum Iris Artefact (VSIA) database with 110 unique eye patterns collected from 55 subjects that corresponds to $110 \times 5 = 550$ normal (or real or live) samples. We then generate 2750 artefact samples by simulating five different kind of attacks including photo print and electronic screen attacks. To our knowledge this is the largest visible iris artefact database available with five diverse attacks to study the vulnerability of the visible iris recognition system.
- *Vulnerability Analysis:* We present the extensive analysis on the newly constructed VSIA database to study the vulnerability of the baseline visible iris recognition system on five different presentation attacks.
- *Performance Evaluation:* We present an extensive experimental analysis of the proposed PAD scheme on our newly collected VSIA database. In addition to this, we also evaluate the proposed PAD scheme on three publicly available visible and NIR iris artefact databases namely: (1) Mobilive 2014 competition database [8] (2) ATVS Fake iris database [18] and (3) LivDet 2013 iris database [16]. Further, the proposed PAD scheme is

TABLE I
DETAILS OF VSIA DATABASE

Number of subjects eye instances	110
Number of attacks	5
Type of attacks	Photo print attack, Electronic display attack and Print-Electronic display attack
Visible iris sensor	Canon 550D DSLR camera with 18.1 MP
Number of samples per eye instance	5
Total number of images in database	3300
Download link:	http://www.nislab.no/biometrics_lab/vsia_db

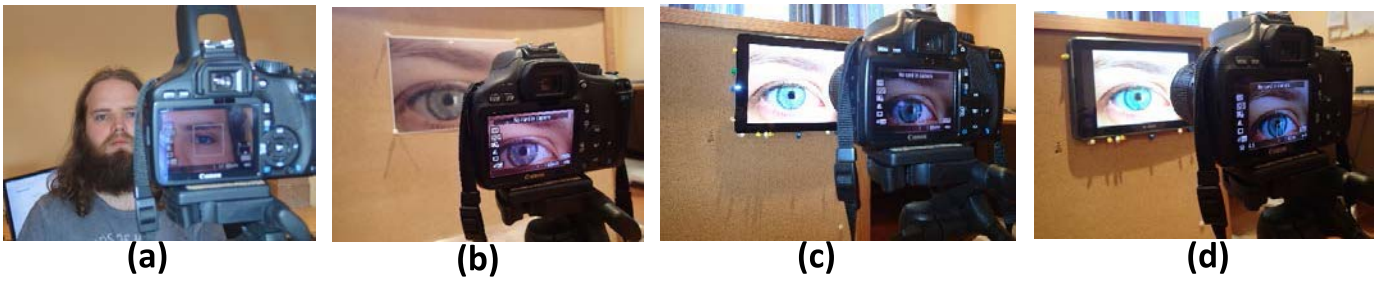

Fig. 1. Illustrating the VSIA data collection setup (a) normal image capture, (b) Attack 1 artefact capture, (c) Attack 2 artefact capture, (d) Attack 3 artefact capture.

compared with **17** (6 on VSIA database, 6 on MobiLive 2014 database, 3 on LiveDet 2013 and 2 on ATVS database) different well-established state-of-the-art schemes to provide the comprehensive comparison.

The rest of the paper is organized as follows: Section III describes the new artefact iris database construction and the associated protocols, Section IV presents the proposed PAD algorithm based on Multi-scale Binarized Statistical Image Features (M-BSIF) and linear Support Vector Machines (SVM), Section V will discuss the experimental results and conclusions are drawn in Section VI.

III. DATABASE CONSTRUCTION

The first major contribution of this work is pertaining to the construction of the new Visible Spectrum Iris Artefact (VSIA) database for analyzing the effect of presentation attacks on visible iris recognition systems. The new VSIA database is constructed by considering the following objectives: (1) To capture relatively large scale database with at least 100 unique eye samples. (2) To generate high quality visible iris artefact samples using both high definition electronic display screens and high quality printing. (3) To provide a performance assessment protocol to benchmark the results of various state-of-the-art presentation attack detection algorithms. To our knowledge, there exists only one public visible iris artefact database i.e. MobILive 2014 [8] that consists of only one attack (i.e. print attack). However, our VSIA database exhibits more unique features when compared to the MobILive 2014 database [8] such as: (1) High resolution image capture (2) Five different kinds of attacks that include electronic screen attacks which was introduced for the first time to evaluate the vulnerability of the visible iris presentation attacks. (3) High quality print attacks. Further, this is the relatively large scale database with highly diverse kind of attacks available to the research community.

Table I summarizes the characteristics of the VSIA database. The VSIA database is comprised of eye images captured from 55 subjects (29 males and 26 females) that will result in 110 unique eye patterns. Figure 1 (a) shows the normal (or real) image capturing setup adopted to capture the VSIA database. All eye images are captured using a Canon EOS 550D DSLR Camera with 18 Megapixel resolution by setting the camera focus on the eye region. Each subject was asked to stand at a distance of $0.5-1$ meter from the visible iris acquisition camera mounted on a tripod. The whole database collection is carried out in our laboratory under a mix of both natural (i.e. sun light) and artificial lighting (room lights). For each subject, we capture 5 samples for each eye instance in five different presentations that will result in $110 \times 5 = 550$ normal iris samples.

A. Artefact Iris Database Collection

In this work, we generated a high quality artefact of each eye image that can be used to attack an iris recognition system that is operating in the visible spectrum. All the artefacts are generated by considering the real-life attack scenarios that one can perform with visible iris recognition system. In this work, we generate the artefacts corresponding to 5 different kinds of static presentation attacks as follows:

1) Attack 1: Print Attack: The 2D print attack consists of displaying a high quality printout of the attacked eye instance to the sensor. The success of this kind of attack especially on the visible iris system depends on generating high quality photo prints. In this work we generated the artefact eye image by printing the normal (or real) eye image that was captured to enroll the subject to the visible iris system. We have used high quality photographic paper to print the artefact using a HP photosmart 5520 printer. We then fix these generated print artefacts on a grip board and presented to the visible

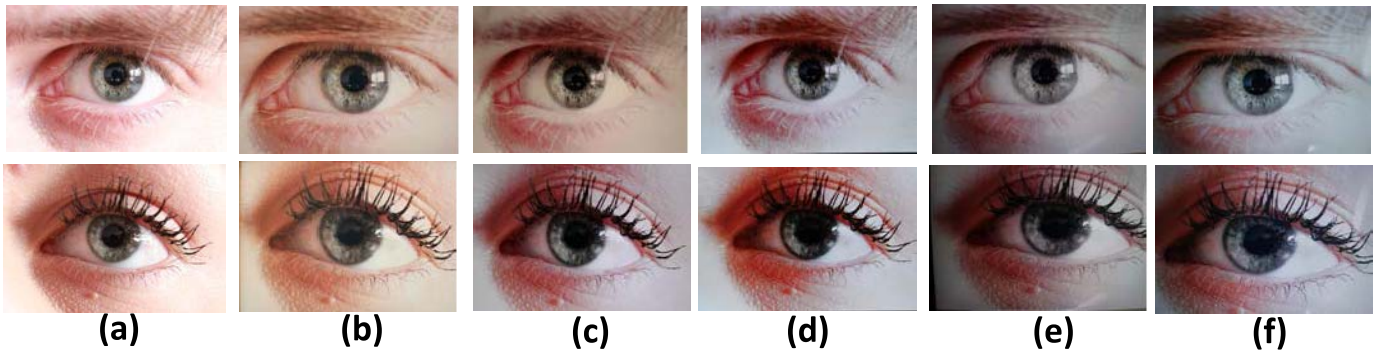

Fig. 2. VSIA Database samples (a) normal eye sample, (b) Attack 1 samples, (c) Attack 2 samples, (d) Attack 3 samples, (e) Attack 4 samples, (f) Attack 5 samples.

iris system in a similar lighting condition as the normal samples were captured. The Attack 1 dataset is comprised of $110 \times 5 = 550$ print artefact samples that corresponds to each of the normal sample. Figure 1 (b) shows the acquisition setup to generate the artefact samples to simulate the Attack 1. Figure 2 (b) shows the print artefacts of the normal (or real or live) eye image shown in the Figure 2 (a).

2) Attack 2: Electronic Screen Attack Using iPad: In attack 2, the artefacts are generated by displaying the normal samples captured earlier to enroll the subject by the aid of an electronic display using iPad (4th generation) with a retina display. This attack will simulate the scenario where an attacker can get access to the biometric samples stored in the visible iris system that in turn are presented using electronic screen to subvert the system. We stored all normal samples in the iPad which is then fixed on the holder and presented to the visible iris sensor in a similar lighting condition as the normal (or real or live) samples were captured. Thus, Attack 2 dataset is also comprised of $110 \times 5 = 550$ samples representing all normal (or real or live) samples. Figure 1 (c) shows the acquisition setup of attack 2 and Figure 2 (c) shows the generated artefact of the normal eye image shown in the Figure 2 (a).

3) Attack 3: Electronic Screen Attack Using Samsung Galaxy Pad: Attack 3 will also generate the artefact by presenting an electronic screen using the Samsung Galaxy Note 10.1. This database allows one to analyze the effectiveness of the presentation attack to yet another kind of electronic display attack on the visible iris recognition system. We first store all normal samples corresponding to each subject in the Samsung Galaxy Note 10.1 that in the turn will be presented to the visible iris recognition system. Thus the Attack 3 database is again comprised of $110 \times 5 = 550$ samples that represent all normal samples. Figure 1 (d) shows the acquisition setup of artefacts corresponding to Attack 3 and Figure 2 (d) shows the print artefacts of the normal eye images shown in the Figure 2 (a).

4) Attack 4: Combining Print and Electronic Screen Attack (iPad): In Attack 4, we generate the artefact by considering the situation in which the attacker will get the high quality printed photo of the enrolled subject which in turn is captured using an iPad and presented to the system. This kind of presentation attack can be easily performed since it is more convenient for the attacker to carry an electric device when compared to the print photo as the latter one demands good care in order to be successfully presented. To this extent, we construct the Attack 4 artefact database by capturing a high quality print photo that was generated in Attack 1 using iPad (4th generation) and then presented to the system. Thus, the Attack 4 database is also comprised of $110 \times 5 = 550$ representing all normal samples. Figure 2 (e) shows the example of the Attack 4 artefact data sample collected from the normal sample shown in the Figure 2 (a).

5) Attack 5: Combining Print and Electronic Screen Attack (Samsung Pad): The underlining idea of Attack 5 is similar to the Attack 4 with only difference that, in Attack 5 photo samples from Attack 1 are re-captured using Samsung Galaxy Note 10.1 that in turn is presented to the visible iris system. The Attack 5 artefact database also comprised of $110 \times 5 = 550$ representing all normal samples. Figure 2 (f) shows the example of the Attack 5 artefact data samples collected from the normal sample shown in the Figure 2 (a). Thus, the final VSIA database consist of 110 unique eye patterns $\times$ 5 samples $\times$ 5 different attacks $=$ 2750 visible eye artefact samples and $110 \times 5 = 550$ normal samples.

To our knowledge, this is unique (because it introduces electronic screen attacks on visible iris recognition system) and relatively large scale database contributed for analyzing the presentation attacks on visible iris recognition system so far.

B. Availability of VSIA Database

The complete VSIA database that includes both normal and artefact visible periocular and iris samples will be made available upon request through GUC database web page: http://www.nislab.no/biometrics_lab/vsia_db.

C. Performance Assessment Protocol

In order to effectively evaluate the VSIA database and to benchmark the presentation attack detection algorithms, we propose to divide the whole database of 110 unique eye patterns into three independent sets namely: Training set, Development set and Testing set. The training set is comprised of 30 unique eye patterns (i.e. $30 \times 5 = 150$ samples) that can be used only for training the classifiers. The development dataset is comprised of 6 unique eye patterns (i.e. $6 \times 5 = 30$ samples) that are used to tune any parameters associated

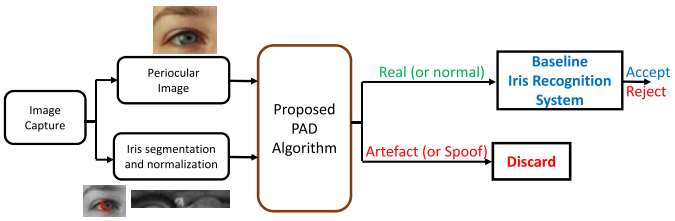

Fig. 3. Overview of the proposed visible iris presentation attack resistant system.

with the presentation attack detection algorithms. The testing dataset is comprised of 74 unique eye patterns (i.e. $74 \times 5 = 370$ samples) that are solely used to evaluate the presentation attack detection algorithm on the VSIA database. An additional protocol is used to analyze the vulnerability of the visible iris system that is involved in further dividing both development and testing dataset into two independent groups namely reference and probe set. To this extent, we use first four samples as the reference and last one sample as the probe with the baseline visible iris recognition algorithm.

IV. Proposed Scheme

Figure 3 shows the proposed scheme for a presentation attack (or spoof attack) resistant system for reliable iris recognition system. The proposed scheme is comprised of four important components explained as follows:

A. Iris Segmentation and Normalization

Given the captured image I, we perform the iris segmentation and normalization using OSIRIS V4.1 [19]. We adopt this scheme not only by considering its segmentation accuracy on both visible [20] and near infrared iris [19] but also by the fact that it is an open source software that is freely available. The OSIRIS V4.1 performs the iris segmentation based on tracing the optimal path of the contours using the Viterbi search algorithm [21]. Then, the segmented iris is normalized using Daugman's rubber sheet expansion technique [22] available within OSIRIS V4.1. The normalized iris image I_{IN} obtained using OSIRIS V1.4 is of dimension 512×64 pixels. For more information about OSIRIS readers can refer to [19]. Figure 4 shows the qualitative results of the IRIS segmentation and normalization obtained on our VSIA database using OSIRIS V1.4. The obtained results shows the effectiveness of the adopted OSIRIS V1.4. However, the images that are not properly segmented by the OSIRIS V1.4 are visually determined and manually rectified to improve the overall system performance.

B. Periocular Region Extraction

Since almost all captured samples have only an eye region, in this work we simply use the eye image captured by the sensors by resizing it to have a dimension of 120×120 pixels. Figure 5 shows the samples of periocular images from VSIA database that are employed in this work. Let the re-sized periocular image be represented as P.

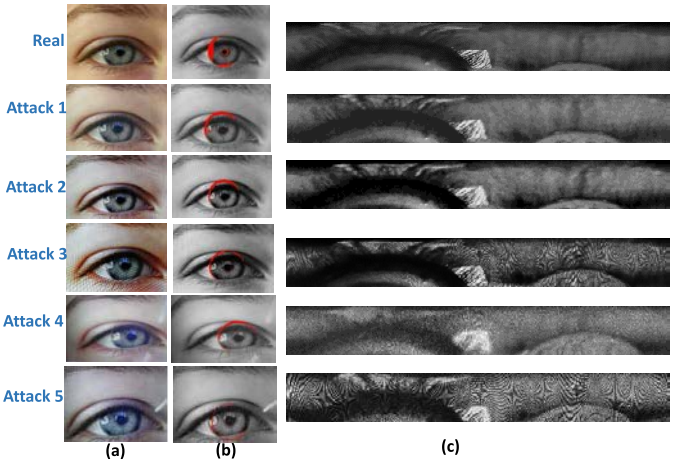

Fig. 4. Qualitative results of the OSIRIS V1.4 on VSIA Database. (a) Input image. (b) Iris segmentation. (3) Iris normalization.

Fig. 5. Examples of Periocular (or eye) images from VSIA database.

C. Proposed Presentation Attack Detection (PAD) Algorithm

Figure 6 shows the overview of the proposed PAD algorithm that explores both periocular (or eye region) and iris region to accurately identify the presentation attacks on the iris recognition system. The proposed scheme can be structured in the following two important components namely:

1) Multi-Scale Binarized Statistical Image Feature Extraction (M-BSIF): Unsupervised filter learning is widely used to learn a new filter by exploring the statistics from the natural images. These methods have emerged as a feasible alternative to the manually design filters, for instance like Local Binary Patterns (LBP). The most popular techniques of the unsupervised learning includes: Restricted Boltzmann Machines (RBMs) [23], [24], Auto-encoders [25], Sparse coding [26] and Independent Component Analysis (ICA) [27], [28]. Among these schemes, the use of ICA has proved to be a more appealing choice as it overcomes the tuning of large sets of hyper-parameters and can also provide a statistically independent basis that in turn can be utilized as the filter to extract the features from the given image.

The objective of the BSIF is to learn a set of filters from natural images using a ICA based unsupervised scheme. These learned filters can be used to represent each pixel of the given image as a binary string by simply computing its response to the learned filters. The binary code corresponding to the pixel can be considered as a local descriptor of the image intensity pattern in the neighborhood of pixel. Finally, the histogram of the pixels code values allow one to characterize the texture properties within the image sub-regions. Thus, the applicability of the BSIF especially for the visible iris presentation attack detection appears to be an elegant choice as it effectively capture the micro-texture information that can be used to detect the artefact.

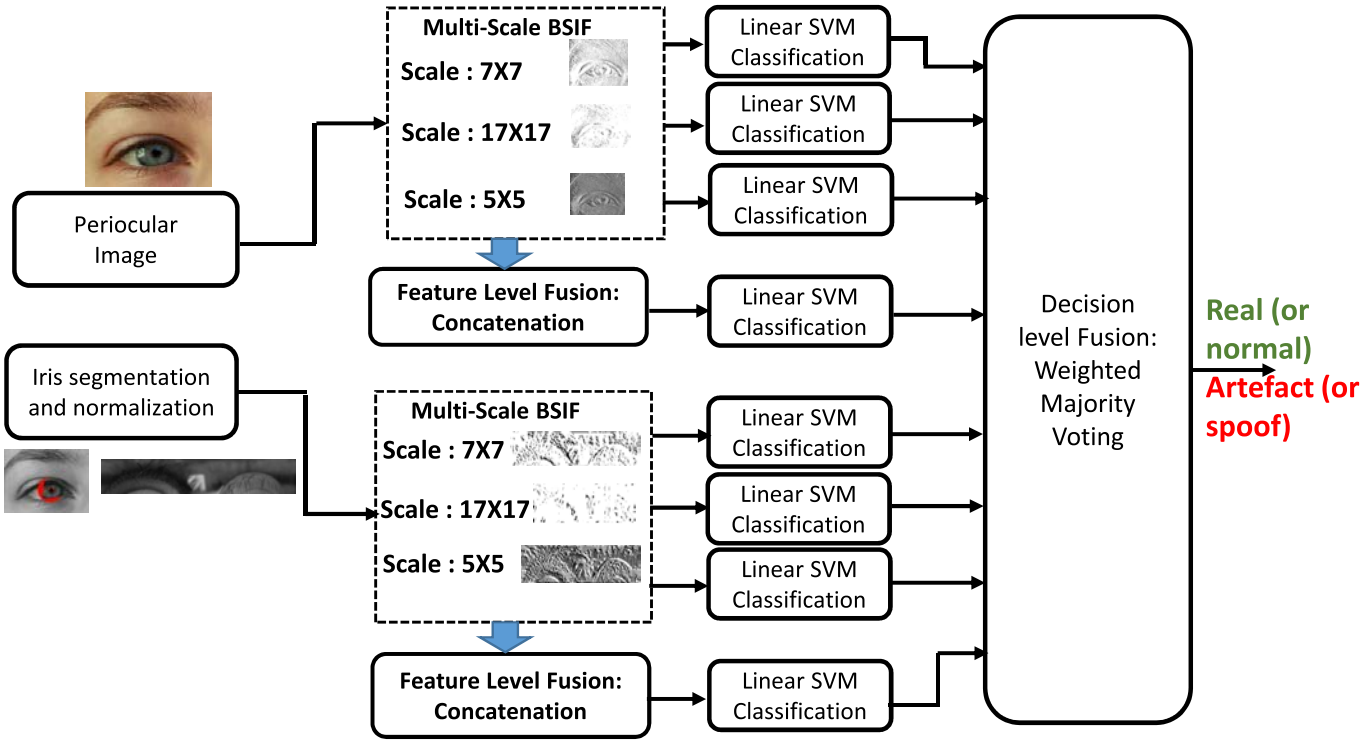

Fig. 6. Overview of the proposed iris presentation attack detection scheme.

In this work, we have employed the open-source filters [29] that are trained using 50000 image patches randomly sampled from 13 different natural scenic images [30]. The training process to construct BSIF filters involves three main steps [29], [31]: (1) Mean subtraction of each patches (2) Dimensionality reduction using Principle Component Analysis (PCA) (3) Estimation of statistically independent filters (or basis) using Independent Component Analysis (ICA). Thus, given a periocular (or iris) sample $P(m,n)$ and a filter F_i of same size then, filter response is obtained as follows [29]:

$$r_i = \sum_{m,n} P(m,n) F_i(m,n) \tag{1}$$

where m and n denotes the size of the periocular (or iris) sample and F_i, $\forall i = \{1,2,\ldots,n\}$ denotes the number of statistically independent filters whose response can be computed together and binarized to obtain the binary string as follows [29]:

$$b_i = \begin{cases} 1, & \text{if } r_i > 0 \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

Finally, the BSIF features are obtained as a normalized histogram of pixel's binary codes that can effectively characterize the texture components in the iris/periocular image. In order to accurately identify the presentation attacks on iris recognition system using BSIF one needs to consider two important factors namely: filter size and filter length. However, the use of single filter with a fixed length may not be capable of capturing sufficient information to identify the different kind of presentation attacks on iris system especially on both visible and NIR spectrum. Thus, in this work, we propose to use multiple filters with different scales to capture the prominent features and hence we call this as Multi-scale Binarized Statistical Image Feature Extraction (M-BSIF). Thus, the use of M-BSIF will allow one to combine various filter responses that in turn extract not only a rich set of information but also allows one to generalize the BSIF for presentation attack detection of iris on both visible and NIR spectrum.

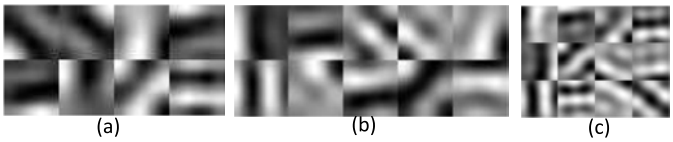

Fig. 7. M-SIF filters of size (a) 5×5, 8 bit, (b) 7×7, 10 bit, (c) 17×17, 12 bit learned from natural images.

In this work, we choose three different filters of size 17×17 with a length of 12 bits, 7×7 with a length of 10 bits and 5×5 with a length of 8 bits. These choices have been made by considering the overall performance in terms of accuracy and throughput of the proposed PAD system using M-BSIF. To this extent we have used the development dataset of VSIA dataset to select the filter size and length and these choices were kept constant throughout the experiments on the testing dataset of VSIA database and also on other three publicly available dataset namely: ATVS-Fir database [18], MobILive 2014 [8], [10] and LivDet-Iris 2013 database [9], [16] that are employed in this work.

Figure 7 shows the M-BSIF filters used in this work. The use of M-BSIF filters exhibits the following characteristics:

- *Generalization:* Since M-BSIF filters are designed using a set of natural image patches, it overcomes the need of

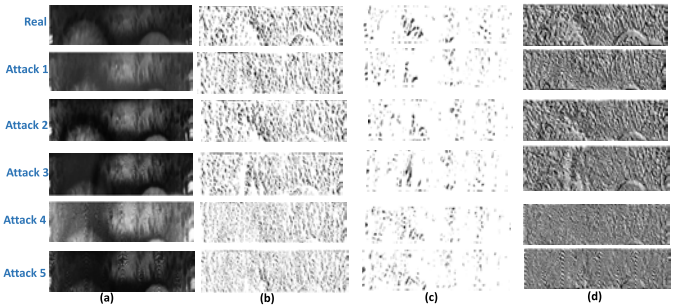

Fig. 8. Qualitative results of selected BSIF filters on both normal (or real) and artefact iris samples from VSIA database. (a) Input image. (b) BSIF features with 7×7 filter. (c) BSIF features with 17×17 filter. (d) BSIF features with 5×5 filter.

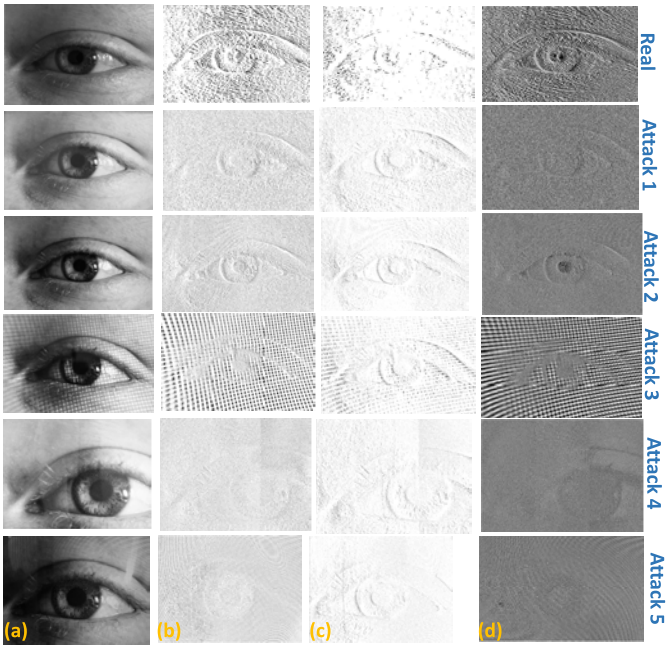

Fig. 9. Qualitative results of selected BSIF filters on both normal and artefact periocular samples from VSIA database. (a) Input image. (b) BSIF features with 7×7 filter. (c) BSIF features with 17×17 filter. (d) BSIF features with 5×5 filter.

manual tuning of filter parameters. Furthermore, the use of pre-learnt filter will overcome the need of application specific learning. Finally, the use of multiple scale filter further captures the prominent information from the given image and thus best suited for different kinds of artefact detection. Thus, the M-BSIF forms the generic representation to address different kinds of iris artefacts in real-life scenario.

- *Statistical Independence:* Since the filters are learned using ICA that can maximize the statistical independence between the learned filters and therefore ensures the effective information encoding.
- *Robustness:* The use of multiple scale improves the robustness of the proposed scheme to both visible and near infrared iris presentation attack detection (refer Section V and Appendix of the paper).

Figure 8 and 9 shows the qualitative results of the three different filters adopted in this work on both iris and periocular samples respectively. Here it can be observed that the use of large scale filter (17×17) will capture the coarse texture information (see Figure 9 (c) and Figure 8 (c)) while the small scale filters (7×7 and 5×5) will capture the micro-texture information (see Figure 9 (b) (d) and Figure 8 (b) (d)) from the presented iris/periocular sample. Further, it is also interesting to observe (from Figure 8 and 9) for the larger variation of the visual information between normal (or real) and artefact iris/periocular samples. Thus, combining these information in an effective manner will allow one to capture all distinctive information to identify the presentation attacks on the iris recognition system. For the comprehensive analysis on performance of individual filter in our proposed M-BSIF kindly refer Appendix of this paper.

Given a periocular sample P, we represent P using M-BSIF features that are extracted using three different filters to obtain three distinct feature set namely: $B_{I_{P1}}$, $B_{I_{P2}}$ and $B_{I_{P3}}$. We then combine these features by performing a feature level fusion by carrying out the feature concatenation to form a single feature vector $B_{I_P} = \{B_{P_1}||B_{P_2}||B_{P_3}\}$. The same procedure is also carried out on the iris samples I_{IN} to obtain the fused features $B_{I_{IN}} = \{B_{I_{IN1}}||B_{I_{IN2}}||B_{I_{IN3}}\}$.

2) Decision Level Fusion: In this work, we employed 8 independent linear Support Vector Machine (SVM) classifiers corresponding to both iris and periocular biometrics whose decisions are combined using weighted majority voting as illustrated in the Figure 6. Out of 8 different linear SVM classifiers, the first four are applied on periocular and the remaining four on the iris modality. Among four different linear SVM classifiers that are used on the periocular modality are distributed such that, one each is used on the three independent M-BSIF features and one on the feature level fusion of these M-BSIF features. Similarly, out of four linear SVM classifiers that were used on the iris modality, three classifiers are used on three independent M-BSIF features and one on the feature level fusion of M-BSIF features. The combination of all 8 SVM classifiers are illustrated in the Figure 6. Each of these linear SVM classifiers is first trained using a set of positive (either with normal (or real) iris or periocular samples) and negative (or artefact or spoof) samples according to the standard protocol described for each of the database used in this work.

Given a probe periocular sample P, we first extract M-BSIF features and perform the feature level fusion, which in turn is tested with their corresponding SVM classifier to obtain a decision as D_{P_k}, where $k = \{1, \ldots, 4\}$. A similar procedure is also carried out on the iris probe sample I_{IN} to obtain a decision D_{I_k}, where $k = \{1, \ldots, 4\}$. We then combine these 8 decisions using weighted majority voting as follows:

$$F_D = \max_{k=1}^{N_C} \sum_{r=1}^{N_E} w_r D_{rk} \tag{3}$$

where, F_D denotes the fused decision, D_{rk} denotes the decision of the rth expert (either periocular or iris), N_E denotes the number of experts, N_C denotes the number of class to be combined and w_r denotes the weights. In this work, weights w_r for the individual classifiers (or experts) are

computed according to their performance such that larger weights are assigned to the expert with high accuracy and vice-versa as mentioned in [32]. The weight assignment scheme will consider the individual performance of the expert and depending upon their performance the method will compute the weights such that $\sum_r w_r = 1$. These weights are assigned on the development dataset from VSIA database and kept constant throughout our experiments.

D. Baseline Iris Recognition System

In this work, we adopt the well-established baseline iris recognition system based on Gabor transform and Sparse Representation Classifier (SRC) [33]. The baseline system will accept only the iris (segmented and normalized) sample that was detected as a normal (or real) presentation as a probe sample. Then the probe iris sample is compared with the reference samples to make decision about accept or reject.

V. Experimental Results and Discussion

In this section, we present the results obtained by employing the proposed PAD scheme on the iris recognition system. The proposed schemes are evaluated not only on our newly constructed VSIA database but also on three publicly available large scale iris artefact databases namely: (1) Mobilive 2014 competition database [8]. (2) ATVS Fake iris database [18]. (3) LivDet 2013 iris database [16].

A. Results on VSIA Database

This section will present the results on our VSIA database that are obtained using our proposed PAD scheme. In order to present a comprehensive benchmark, we compare the proposed scheme with five different well-established state-of-the-art schemes namely: Image Quality Measures (IQM) and Quadratic Discriminant Analysis (QDA) [4], Image Frequency Analysis (IFA) [16], Local Binary Patterns ($LBP^{u2}_{8,2}$) with SVM [34], LBP-Pyramid of Histograms of Oriented Gradients (PHOG)-SVM [34] and modified-LBP (mLBP) and SVM [34]. The results of all the evaluated techniques are reported by following the performance assessment protocol as described in the Section III-C. In order to effectively analyze the performance of the proposed scheme we carry out the 10-fold cross validation method. For each fold, we randomly assign the unique eye pattern into any one of the data partition namely development, training and testing datasets. At the end the results are averaged over all 10 folds.

In this work, we present the performance of the presentation attack detection algorithms according to the ISO/IEC WD 30107-3 [11] in terms of: (1) Attack Presentation Classification Error Rate (APCER), which is defined as a proportion of attack presentation incorrectly classified as normal (or real) presentation (2) Normal Presentation Classification Error Rate (NPCER) which is defined as proportion of normal presentation incorrectly classified as attack presentation. Finally, the performance of the overall PAD algorithm is presented in terms of Average Classification Error Rate (ACER) such that, $ACER = \frac{(APCER+NPCER)}{2}$ thus, the lower the values of ACER the better is the PAD performance.

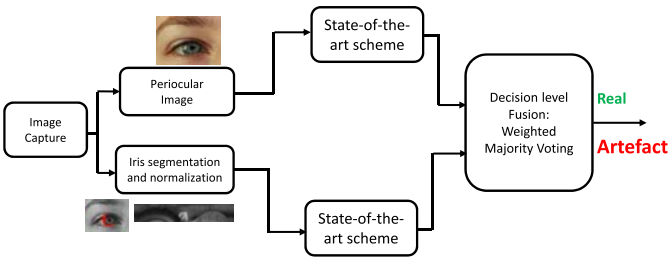

Fig. 10. General overview illustrating the evaluation of the State-of-the-art schemes adopted to evaluate VSIA database.

TABLE II
Performance of the Baseline Iris Recognition System to Five Different Attacks From VSIA Database

Probe samples	Reference samples	Baseline performance EER (%)
Normal (or real)	Normal (or Real)	**02.58**
Artefact from Attack 1	Normal (or Real)	02.18
Artefact from Attack 2	Normal (or Real)	02.74
Artefact from Attack 3	Normal (or Real)	05.71
Artefact from Attack 4	Normal (or Real)	05.22
Artefact from Attack 5	Normal (or Real)	12.73

In order to have a fair benchmark of the proposed PAD scheme with the 5 different state-of-the-art schemes, we carry out the state-of-the-art techniques on both periocular and iris independently and then combine them at the decision level using the weighted majority voting rule as shown in the Figure 10. For example, in order to compare the IQM-QDA technique with our proposed scheme, we carry out IQM-QDA technique independently on periocular and iris and then we combine the decision using weighted majority voting. For each technique the weights are fixed on the development dataset and then used on the testing dataset to obtain the final performance.

We first present the results on evaluating the vulnerability of the baseline iris recognition system to the five different kinds of artefacts that are available within our new VSIA database. In order to study this, we consider the iris recognition baseline system based on Gabor transform and Sparse Representation Classifier (SRC) [33]. We first obtain the baseline performance by considering both reference and probe samples from normal (or real or live) presentation. Then in order to evaluate the vulnerability of the baseline iris system, we use the artefact samples corresponding to five different attacks as the probe samples.

Table II shows the performance of the baseline with normal and artefact samples. Here, our idea is to analyze the performance of the baseline iris recognition system to the artefact samples from VSIA database. To this extent, we build the baseline visible iris recognition system that is enrolled with the live (or normal) samples from the VSIA database. Then, we use the probe samples as the artefact samples corresponding to five different attacks to evaluate the performance of the baseline system. Lastly, we compare the performance corresponding to different artefacts to the performance of

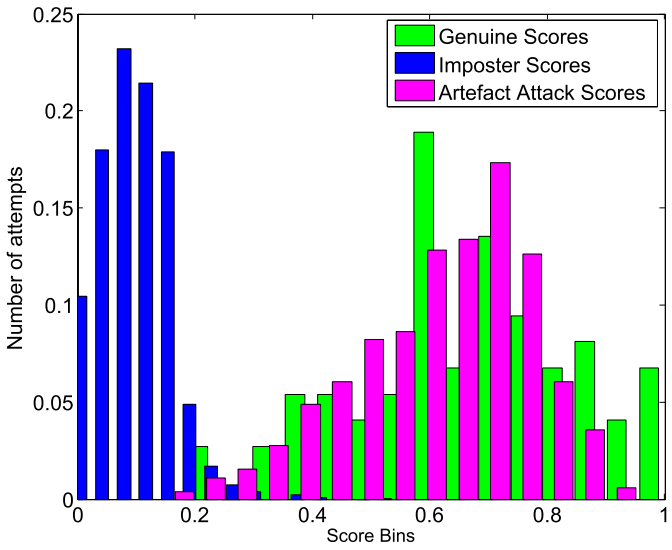

Fig. 11. Baseline system score distribution.

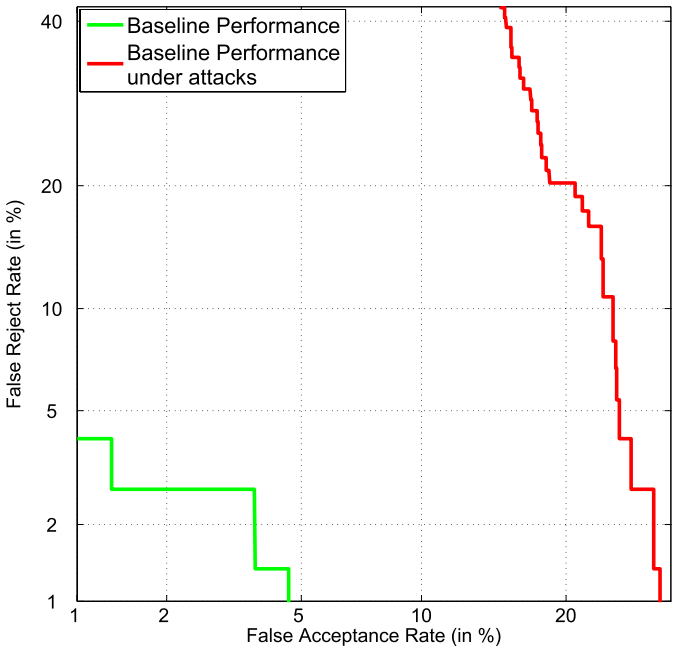

Fig. 12. DET Curve indicating system performance.

the live (or normal) probe sample to study the vulnerability of the baseline system. As noted from the Table II, the performance of the baseline visible iris system corresponding to the artefacts from attack 1 (with $EER = 2.18\%$) and attack 2 (with $EER = 2.74\%$) shows the similar performance to that of normal presentation (with $EER = 2.58\%$). This justifies the very high vulnerability of the baseline system to the artefact samples present in VSIA database.

Figure 11 shows the score distribution of the baseline with genuine, imposter and artefact scores stemming from the five different attack methods all obtained on the testing dataset from the VSIA database. Here one can observe the strong overlapping of artefact and genuine scores that strongly indicates the applicability of the VSIA database to study the vulnerability of the iris recognition system. Now, if we set a threshold value that corresponds to the EER on the development dataset, then 92.22% of the artefact samples can successfully intrude the system. This fact further justifies not only the quality of the generated artefacts but also the need of presentation attack detection techniques for the visible iris recognition system.

Figure 12 shows the DET curve of the verification performance of the baseline iris system with normal and artefact scores from all five attacks. As expected, due to the extreme overlapping of genuine and artefact scores the overall performance of the baseline iris system is highly deceived.

Table III shows the comparative performance of the proposed scheme for presentation attack detection with five well established state-of-the-art techniques on VSIA database. Here, it can be observed that, the proposed scheme emerges as the best algorithm to detect all five kinds of artefacts that are available in the VSIA database. The proposed scheme shows the outstanding performance with ACER $= 0.29\%$ on Attack 1 while achieved ACER $= 0\%$ on remaining four attacks.

Figure 13 shows the performance of the baseline iris system with the proposed PAD algorithm on Attack 1 and Attack 2 from the VSIA database. It can be observed that, the adoptability of the proposed PAD algorithm has mitigated the artefacts that are presented to the system and allowed only normal (or real or live) samples to the baseline system. As a consequence the performance of the baseline system together with our proposed PAD is more or less the same as the performance of the ideal baseline system. These results justifies the applicability of the proposed scheme for iris presentation attack detection. For simplicity, we have illustrated the performance of the baseline iris system on Attack 1 and Attack 2 however a similar performance can also be observed on the remaining attacks namely: Attack 3, Attack 4 and Attack 5 from the VSIA database.

B. Results on MobILive 2014 Database

In this section, we report the results of the proposed PAD scheme on 1st Mobile Iris Liveness detection competition (MobILive) [10] that was conducted during April 2014. The MobILive 2014 database consists of 1600 samples corresponding to both normal (or real or live) and artefact (or fake) iris captured in visible spectrum. Here presentation attacks are simulated by generating the artefact by printing the normal captured eye image using a high quality printer. In order to evaluate the proposed method, we followed the experimental protocol described for this database [10] and results are presented using the same PAD performance measures that were employed in the competition. The performance measure used in this competition are same as the one we used with our new VSIA database following the standards ISO/IEC WD 30107-3 [11]. But the terminology used to indicate the performance in MobILive 2014 is different. The term FAR used in MobILive 2014 corresponds to the APCER and FRR corresponds to NPCER and the Mean error rate corresponds to the ACER. However, in order to have a meaningful benchmark we retained the same convention used in the MobILive 2014 competition and

TABLE III
PERFORMANCE EVALUATION OF THE PROPOSED PAD SCHEME AND COMPARISON WITH STATE-OF-THE-ART SCHEMES ON VSIA DATABASE

Attack Scenario	Methods	APCER (%)	NPCER(%)	ACER(%)
Attack 1	IQM-QDA[4]	15.13	26.78	20.95
	IFA[16]	40.56	33.27	36.91
	$LBP^{u2}_{8,2}$-SVM [35]	0.18	1.08	0.94
	LBP-PHOG-SVM [34]	3.43	7.51	5.47
	mLBP-SVM [36]	1.48	1.24	1.36
	Boosted LBP [14]	0.69	3.94	2.31
	Proposed Scheme	0.59	0	**0.29**
Attack 2	IQM-QDA [4]	0.16	4.72	2.44
	IFA [16]	0.43	64.40	32.41
	$LBP^{u2}_{8,2}$-SVM [35]	2.27	3.05	2.66
	LBP-PHOG-SVM [34]	2.56	1.21	1.89
	mLBP-SVM [36]	2.21	1.59	1.90
	Boosted LBP [14]	2.42	4.74	3.58
	Proposed Scheme	0	0	**0**
Attack 3	IQM-QDA [4]	1.15	8.60	4.87
	IFA [16]	9.45	81.08	45.27
	$LBP^{u2}_{8,2}$-SVM [35]	0	0.59	0.29
	LBP-PHOG-SVM [34]	0.48	0.56	0.52
	mLBP-SVM [36]	0.48	0.16	0.32
	Boosted LBP [14]	1.10	1.42	1.26
	Proposed Scheme	0	0	**0**
Attack 4	IQM-QDA [4]	2.02	9.24	5.63
	IFA [16]	0.67	63.13	31.90
	$LBP^{u2}_{8,2}$-SVM [35]	4.16	7.75	5.95
	LBP-PHOG-SVM [34]	2.13	4.10	3.12
	mLBP-SVM [36]	1.37	0.21	0.79
	Boosted LBP [14]	5.74	7.17	6.45
	Proposed Scheme	0	0	**0**
Attack 5	IQM-QDA [4]	1.86	0	0.93
	IFA [16]	23.54	38.75	31.14
	$LBP^{u2}_{8,2}$-SVM [35]	0	0	0
	LBP-PHOG-SVM [34]	0.91	1.02	0.97
	mLBP-SVM [36]	0	0	0
	Boosted LBP [14]	0	0	0
	Proposed Scheme	0	0	**0**

included the corresponding standard terminology within brackets (in the Table IV) to preserve the consistency for the reader. Table IV shows the performance of the proposed PAD algorithm on the MobILive 2014 database. As indicated in the Table IV, the proposed scheme shows the outstanding performance with a Mean error rate (or ACER) of 0% and emerged as the best algorithm when compared with the six different existing schemes. These results dictates the efficacy of the proposed scheme on yet another publicly available visible iris database.

C. Results on LivDet Iris 2013 Warsaw Dataset

This section present the results on the Warsaw database [16] that was also used in LivDet 2013 competition [9]. This database is comprised of 1274 normal (or real) samples and 729 artefact samples. The artefacts are generated using both low and high resolution printers. Here also we follow the evaluation protocol suggested for this database [9] and report the results according to the terminology that have been used in the LivDet 2013 competition. However in order to avoid the confusion for the reader, we included the standard terminology according to the ISO/IEC WD 30107-3 [11] that has been adopted in this paper with in the brackets (of Table V) to get the better understanding on performance measures. Table V shows the performance of the proposed PAD algorithm in comparison with three different existing schemes that was evaluated during LiveDet 2013 competition. As indicated in the Table V, the proposed PAD scheme shows the best performance with an Average Error (or ACER) of 1.27% when compared with three different state-of-the-art schemes. This experiment indicate not only the efficiency but also the applicability of the proposed scheme on detecting the presentation attacks on NIR iris systems.

D. Results on ATVS Fake Iris Dataset

This section discuss the performance of the proposed scheme on the ATVS-Fake iris database [18]. This database is comprised of 800 normal and artefact iris samples captured in the NIR spectrum. In this database the artefact images are generated using high quality printing of normal (or real) samples. Here also we follow the recommended evaluation protocols and use the same PAD performance terminology that was adopted with this database to report the results of the proposed PAD algorithm. However similar to the earlier databases, here also we included the ISO/IEC WD 30107-3 [11] terminology in brackets (of Table V) to avoid confusion

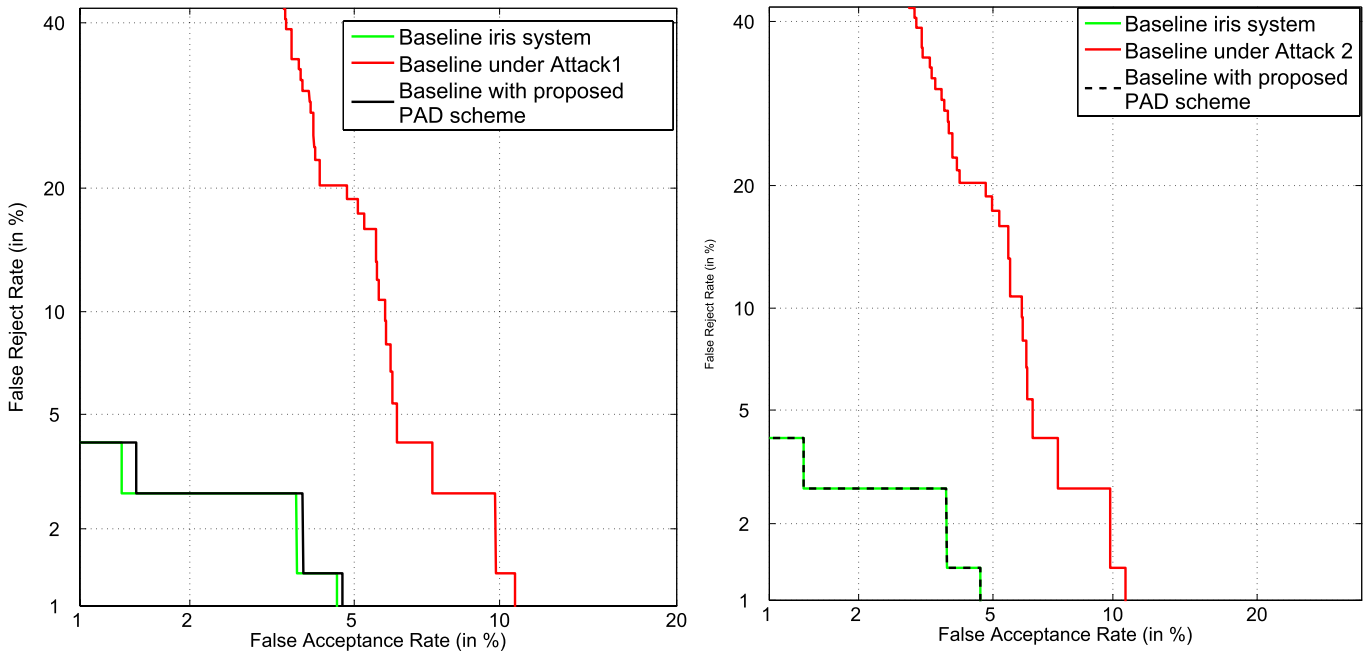

Fig. 13. Performance of the baseline iris system with proposed PAD scheme of VSIA database. (a) Performance with proposed PAD on Attack 1. (b) Performance with proposed PAD on Attack 2.

TABLE IV

PERFORMANCE OF THE PROPOSED SCHEME ON MOBILIVE 2014 DATASET

Techniques proposed by teams	FAR (or APCER) (%)	FRR (or NPCER) (%)	Mean Error Rate (or ACER) (%)
HH	29.25	7.00	18.13
IrisKent	0.25	3.75	2.00
Liv-IC-INICAMP	0.50	2.00	1.25
Federico II	1.25	0.00	0.63
GUC	0.75	0.00	0.38
IIT Indore	0.50	0.00	0.25
Proposed Scheme	0.00	0.00	**0.00**

TABLE V

PERFORMANCE OF THE PROPOSED SCHEME ON LIVDET IRIS 2013 WARSAW DATASET

Techniques proposed by teams	FerrFake (or APCER) (%)	FerrLive (or NPCER)(%)	Average Error (or ACER) (%)
ATVS	07.60	25.25	16.42
Federico	0.60	21.15	10.87
Porto	11.95	05.25	08.60
Proposed Scheme	02.14	0.40	**01.27**

TABLE VI

PERFORMANCE OF THE PROPOSED SCHEME ON ATVS FAKE IRIS DATASET

Algorithms	FGR (or APCER) (%)	FFR (or NPCER) (%)	HTER (or ACER) (%)
IQM-QDA [4]	0.25	4.20	2.20
Quality features [18]	4.90	1.30	3.10
Proposed scheme	0.00	0.00	**0.00**

to the reader. Table VI shows the performance of the proposed scheme along with two different state-of-the art schemes. Here it can be observed that, the proposed PAD algorithm shows outstanding performance with a HTER (or ACER) of 0%. This experiment provided yet another evidence on the efficacy of the proposed scheme for accurate presentation attack detection on both visible and NIR iris systems.

Thus based on the extensive experiments carried out on four different relatively large scale and publicly available databases with highly diverse artefacts not only revealed the accuracy of the proposed scheme but also its robustness to both visible and NIR iris presentation attack detection. The success of the proposed scheme can be attributed to the following reasons:

- The proposed M-BSIF that can accurately capture both micro-texture (with small scale size) as well as coarse texture (using large scale size) information from both periocular and iris region.
- The use of three different size filters will permit one to explore their complementary information by performing the fusion as they capture different level of texture information. Therefore, the proposed method will pertain the feature level fusion that has demonstrated the improved performance when compared with the individual performance of the different scale filters (Refer Appendix for detail analysis). This fact also contributed importantly to the success of the proposed system.
- Ultimately, the role of decision level fusion further explores the complementary information not merely between the scales, but also with iris and periocular region that results in accurate as well as robust PAD system.

VI. Conclusion

Iris biometric system are highly vulnerable to presentation attacks that can be carried out using either a photo print and electronic screen display. In this work, we explored the vulnerability of iris recognition systems to various presentation attacks. Further, we also proposed a novel algorithm to accurately detect and mitigate the presentation attacks on the iris recognition system. To this extent, we introduce a new relatively large scale visible iris artefact database that comprised of 550 normal and 2750 iris artefact samples. This is one of the important contribution of this work as the VSIA database will be made available to the research community. We then proposed a novel scheme based on M-BSIF and the linear SVM technique that emerged as the best iris presentation attack detection algorithm on both visible and NIR iris recognition system. Based on the extensive analysis carried out in this work the following are the main conclusions:

- Extensive experiments carried out on our 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. This indicates the high quality of the artefact iris samples that are available within VSIA database.
- The 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.
- Extensive evaluations of 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.

Acknowledgment

The authors are grateful to the anonymous reviewers for their constructive suggestions to improve the quality of the paper.

References

[1] *Unique Identification Authority of India*. [Online]. Available: http://uidai.gov.in//, accessed Jun. 2014.
[2] J. Daugman, "Iris recognition and anti-spoofing countermeasures," in *Proc. 7th Int. Biometrics Conf.*, 2004, pp. 1–6.
[3] X. He, Y. Lu, and P. Shi, "A fake iris detection method based on FFT and quality assessment," in *Proc. Chin. Conf. Pattern Recognit.*, Oct. 2008, pp. 1–4.
[4] J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," *IEEE Trans. Image Process.*, vol. 23, no. 2, pp. 710–724, Feb. 2014.
[5] X. He, Y. Lu, and P. Shi, "A new fake iris detection method," in *Advances in Biometrics*, vol. 5558, M. Tistarelli and M. S. Nixon, Eds. Berlin, Germany: Springer-Verlag, 2009, pp. 1132–1139.
[6] S. J. Lee, K. R. Park, and J. Kim, "Robust fake iris detection based on variation of the reflectance ratio between the iris and the sclera," in *Proc. Biometric Consortium Conf.*, Sep./Aug. 2006, pp. 1–6.
[7] K. Hughes and K. W. Bowyer, "Detection of contact-lens-based iris biometric spoofs using stereo imaging," in *Proc. 46th Hawaii Int. Conf. Syst. Sci.*, Jan. 2013, pp. 1763–1772.
[8] A. F. Sequeira, J. Murari, and J. S. Cardoso, "Iris liveness detection methods in mobile applications," in *Proc. 9th Int. Conf. Comput. Vis. Theory Appl.*, 2013, pp. 1–5.
[9] *Livdet-Iris Competition*. [Online]. Available: http://people.clarkson.edu/projects/biosal/iris/index.php, accessed Jul. 2014.
[10] *Mobilive-Iris Competition 2014*. [Online]. Available: http://mobilive2014.inescporto.pt/, accessed May 2014.
[11] *Information Technology—Biometrics—Presentation Attack Detection—Part 3: Testing, Reporting and Classification of Attacks*, International Organization for Standardization, ISO/IEC Standard WD 30107-3:2014, 2014.
[12] X. He, S. An, and P. Shi, "Statistical texture analysis-based approach for fake iris detection using support vector machines," in *Advances in Biometrics* (Lecture Notes in Computer Science), vol. 4642, S.-W. Lee and S. Z. Li, Eds. Berlin, Germany: Springer-Verlag, 2007, pp. 540–546.
[13] E. Lee, K. Park, and J. Kim, "Fake iris detection by using purkinje image," in *Advances in Biometrics* (Lecture Notes in Computer Science), vol. 3832, D. Zhang and A. K. Jain, Eds. Berlin, Germany: Springer-Verlag, 2005, pp. 397–403.
[14] Z. He, Z. Sun, T. Tan, and Z. Wei, "Efficient iris spoof detection via boosted local binary patterns," in *Advances in Biometrics*. Berlin, Germany: Springer-Verlag, 2009, pp. 1080–1090.
[15] Z. Sun, H. Zhang, T. Tan, and J. Wang, "Iris image classification based on hierarchical visual codebook," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 36, no. 6, pp. 1120–1133, Jun. 2014.
[16] A. Czajka, "Database of iris printouts and its application: Development of liveness detection method for iris recognition," in *Proc. 18th Int. Conf. Methods Models Autom. Robot. (MMAR)*, Aug. 2013, pp. 28–33.
[17] M. Kanematsu, H. Takano, and K. Nakamura, "Highly reliable liveness detection method for iris recognition," in *Proc. Annu. Conf. SICE*, Sep. 2007, pp. 361–364.
[18] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in *Proc. 5th IAPR Int. Conf. Biometrics (ICB)*, Mar./Apr. 2012, pp. 271–276.

[19] G. Sutra, B. Dorizzi, S. Garcia-Salicetti, and N. Othman, "A biometric reference system for iris OSIRIS version 4.1," Telecom SudParis, France, Tech. Rep., 2012.
[20] R. Raghavendra, K. B. Raja, B. Yang, and C. Busch, "Combining iris and periocular recognition using light field camera," in *Proc. 2nd IAPR Asian Conf. Pattern Recognit. (ACPR)*, Nov. 2013, pp. 155–159.
[21] G. D. Forney, Jr., "The Viterbi algorithm," *Proc. IEEE*, vol. 61, no. 3, pp. 268–278, Mar. 1973.
[22] J. Daugman, "How iris recognition works," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 21–30, Jan. 2004.
[23] H. Lee, C. Ekanadham, and A. Y. Ng, "Sparse deep belief net model for visual area V2," in *Advances in Neural Information Processing Systems 20*. Red Hook, NY, USA: Curran Associates, 2008, pp. 873–880.
[24] G. Hinton, S. Osindero, and Y. Teh, "A fast learning algorithm for deep belief nets," *Neural Comput.*, vol. 18, no. 7, pp. 1527–1554, Jul. 2006.
[25] P. Vincent, H. Larochelle, Y. Bengio, and P.-A. Manzagol, "Extracting and composing robust features with denoising autoencoders," in *Proc. 25th Int. Conf. Mach. Learn.*, 2008, pp. 1096–1103.
[26] B. A. Olshausen and D. J. Field, "Sparse coding with an overcomplete basis set: A strategy employed by V1?" *Vis. Res.*, vol. 37, no. 23, pp. 3311–3325, 1997.
[27] J. H. van Hateren and A. van der Schaaf, "Independent component filters of natural images compared with simple cells in primary visual cortex," *Proc. Roy. Soc. London, B, Biological Sci.*, vol. 265, no. 1394, pp. 359–366, 1998.
[28] A. J. Bell and T. J. Sejnowski, "The 'independent components' of natural scenes are edge filters," *Vis. Res.*, vol. 37, no. 23, pp. 3327–3338, 1997.
[29] J. Kannala and E. Rahtu, "BSIF: Binarized statistical image features," in *Proc. 21st Int. Conf. Pattern Recognit. (ICPR)*, Nov. 2012, pp. 1363–1366.
[30] A. Hyvèarinen, J. Hurri, and P. O. Hoyer, *Natural Image Statistics*, vol. 39. New York, NY, USA: Springer-Verlag, 2009.
[31] R. Raghavendra and C. Busch, "Robust palmprint verification using sparse representation of binarized statistical features: A comprehensive study," in *Proc. 2nd ACM Workshop Inf. Hiding Multimedia Secur. (IH&MMSEC)*, 2014, pp. 181–185.
[32] R. Raghavendra, G. H. Kumar, and A. Rao, "Qualitative weight assignment for multimodal biometric fusion," in *Proc. 7th Int. Conf. Adv. Pattern Recognit.*, Feb. 2009, pp. 193–196.
[33] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Secure and robust iris recognition using random projections and sparse representations," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 9, pp. 1877–1893, Sep. 2011.
[34] D. Yadav, N. Kohli, J. S. Doyle, R. Singh, M. Vatsa, and K. W. Bowyer, "Unraveling the effect of textured contact lenses on iris recognition," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 851–862, May 2014.
[35] J. Maatta, A. Hadid, and J. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in *Proc. Int. Joint Conf. Biometrics (IJCB)*, Oct. 2011, pp. 1–7.
[36] N. Erdogmus and S. Marcel, "Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect," in *Proc. IEEE 6th Int. Conf. Biometrics, Theory, Appl., Syst. (BTAS)*, Sep./Oct. 2013, pp. 1–6.

R. Raghavendra received the bachelor's degree in electronics and communication from the University of Mysore (UOM), Mysore, India, the master's degree from Visvesvaraya Technological University, Belgaum, India, and the Ph.D. degree in computer science and technology from UOM, the Institute Telecom, and Telecom Sudparis (carried out as a collaborative work). He was a Researcher with the Istituto Italiano di Tecnologia, Genoa, Italy. He is currently a Researcher with the Norwegian Biometric Laboratory, Gjøvik University College, Gjøvik, Norway. He is the author of several papers in the above subjects and a reviewer for several international conferences and journals. His main research interests include statistical pattern recognition, data fusion schemes, and random optimization, with applications to biometrics, multimodal biometric fusion, human behavior analysis, and crowd behavior analysis.

Christoph Busch received the Diploma degree from the Technical University of Darmstadt (TUD), Darmstadt, Germany, and the Ph.D. degree in computer graphics from TUD, in 1997. In 1997, he joined the Fraunhofer Institute for Computer Graphics, Darmstadt. Darmstadt. Furthermore, he lectures in biometric systems with the Technical University of Denmark, Kongens Lyngby, since 2007. He is currently a Faculty Member of computer science and media technology with Gjøvik University College, Gjøvik, Norway, and holds a joint appointment with the Computer Science Faculty, Hochschule Darmstadt. He coauthored over 230 technical papers, and has been a speaker at international conferences. His research includes in pattern recognition, multimodal, and mobile biometrics and privacy enhancing technologies for biometric systems. He is the Cofounder of the European Association for Biometrics and a Convener of WG3 in ISO/IEC JTC1 SC37 on Biometrics. He served for various program committees, and is an appointed member of the Editorial Board of the *IET Biometrics* journal.