



## Eye movement-driven defense against iris print-attacks

Ioannis Rigas<sup>a</sup>, Oleg V. Komogortsev<sup>a</sup>

<sup>a</sup> Texas State University, 601 University Drive, San Marcos, TX 78666, USA

### ABSTRACT

This paper proposes a methodology for the utilization of eye movement cues for the task of iris print-attack detection. We investigate the fundamental distortions arising in the eye movement signal during an iris print-attack, due to the structural and functional discrepancies between a paper-printed iris and a natural eye iris. The performed experiments involve the execution of practical print-attacks against an eye-tracking device, and the collection of the resulting eye movement signals. The developed methodology for the detection of print-attack signal distortions is evaluated on a large database collected from 200 subjects, which contains both the real ('live') eye movement signals and the print-attack ('spoof') eye movement signals. The suggested methodology provides a sufficiently high detection performance, with a maximum average classification rate (ACR) of 96.5% and a minimum equal error rate (EER) of 3.4%. Due to the hardware similarities between eye tracking and iris capturing systems, we hypothesize that the proposed methodology can be adopted into the existing iris recognition systems with minimal cost. To further support this hypothesis we experimentally investigate the robustness of our scheme by simulating conditions of reduced sampling resolution (temporal and spatial), and of limited duration of the eye movement signals.

2015 Elsevier Ltd. All rights reserved.

### 1. Introduction

Human iris is a widely endorsed biometric trait, due to the exceptional characteristics it provides in terms of accuracy, permanence, and processing speed. The systematic investigation of the iris in the field of biometric identification was founded by the research work of J. Daugman (Daugman, 1993), (Daugman, 1994). The subsequent efforts mainly focused on the development and optimization of techniques for the extraction and modeling of the iris, leading to the construction of reliable biometric schemes capable to exhibit very high identification rates (Daugman, 2007), (Phillips et al., 2010). As soon as the research on iris recognition reached a level of maturity and the technology became practically deployed, previously unaddressed challenges emerged. One of the major concerns regarded the vulnerability of iris recognition methods to image sensor attacks conducted by artificial representations of the iris.

The vulnerability of modern iris recognition systems to spoofing threats has been widely reported in various experimental studies. The work presented in (Ruiz-Albacete et al., 2008) investigated the behavior of an iris recognition system in the case of direct spoofing attacks. Using a set of printed iris images and a publicly available iris recognition system, researchers demonstrated the existence of security flaws in the absence of any effective anti-spoofing countermeasure. Another study which concerned the vulnerability assessment during direct counterfeit attacks (Ortiz-Lopez et al., 2011) exhibited a number of different image quality features which are present on fake iris imitations during such an attack. In (Tomeo-Reyes et al., 2011), an investigation was conducted to evaluate the intrusion success of artificial iris imitations of various types (paper printouts, contact lenses, prosthetic eyes) as well as the influence of noisy genuine samples on the recognition performance. Some studies explored the possibility of an attack by generating a spoof iris

image using an extracted iris template (Venugopalan and Savvides, 2011), (Galbally et al., 2013).

The findings of these studies demonstrated the security vulnerabilities of modern iris recognition systems to spoofing attacks. They also exposed a more alarming issue considering the easiness of performing such attacks even with relatively simple means (e.g. common printers and paper). As a result, there is an increased research focus on techniques for detecting direct spoofing attacks (sometimes referred as liveness detection techniques), and a more systematic evaluation of their potential. Recently, this necessity was further emphasized with the organization of two iris liveness detection competitions (Yambay et al., 2014), (Sequeira et al., 2014).

#### 1.1. Prior Art on Iris Anti-spoofing

Even before the comprehensive evaluation of the vulnerability of iris systems to direct counterfeit attacks, described earlier, there were initial ideas proposed for the protection from spoofing attacks. Some early anti-spoofing features were presented in the work of (Daugman, 2003). The work of (Li et al., 2003) practically explored the quality distortions in the texture of fake irises. Such distortions are usually generated due to focus, motion blur, and occlusion. A more systematic attempt to tackle the problem of iris aliveness detection was presented in (Pacut and Czajka, 2006). In the conducted research, the Fourier spectrum was employed for detecting spoof-indicative features of images coming from live and fake irises, and the experiments were performed using a variety of printing approaches. The same study investigated other anti-spoofing characteristics, such as the pupil size under controlled light intensity changes, and the iris reflection patterns induced by a preconfigured infrared light setting. The reflectance properties of human eye served as a source of inspiration for other methodologies as well. For example, in the method presented in (Lee et al., 2005) the

Purkinje images (light reflections from different eye areas) were employed for detecting fake irises. Also, in (Sung Joo et al., 2006), the reflectance ratio between the eye and the sclera was used as a trait for liveness. Pupil dynamics also served as a source of liveness detection characteristics in a number of subsequent studies. In (Bodade and Talbar, 2009), a scheme was developed for the calculation of variations during the localization of the inner iris boundary, whereas (Puhan et al., 2011) explored the iris pattern dissimilarities generated due to the pupil reflex in the case of semi-transparent contact lens spoofing attacks. In (Xinyu et al., 2013), pupil constriction was modeled by measuring iris patch differences and the ratio of iris and pupil diameters, in a scenario allowing free head movements.

A large category of methods for detecting fake irises is based on the analysis of image texture characteristics. In (He et al., 2007), the properties of the grey level co-occurrences matrices (GLCM) (Haralick et al., 1973) were proposed for the description of texture features of iris counterfeits, and the extracted features were incorporated into a classification scheme based on Support Vector Machines (SVM). Co-occurrence matrix features were also employed in the approach presented in (Zhuoshi et al., 2008), this time in conjunction with texture quality cues, specifically, iris edge sharpness and Iris-Texton (Xianchao et al., 2007) histograms. An investigation of iris textures printed on contact lenses was the main topic of research for the methodologies presented in (He et al., 2009) and (Hui et al., 2010). In both cases, the effective-proven texture descriptor of Local Binary Patterns (LBPs) (Ojala et al., 2002) was utilized for the analysis of captured iris samples. In (Galbally et al., 2012), a large ensemble of texture quality features was assessed for the detection of distortions arising during the image capturing procedure. More recently, the scheme presented in (Czajka, 2013) explored the existence of “alien” frequencies in the spectrum of the printed irises. Furthermore, a method for the analysis of texture features based on hierarchical visual codebooks was presented in (Sun et al., 2014).

Lately, the possibility to extract liveness indicative cues via eye movement biometrics in a simulated scenario of an attack by a mechanical replica of the human eye was examined in (Komogortsev et al., 2015). It should be mentioned that the use of eye movement cues has been also suggested as a mechanism for liveness detection in the domain of face recognition. In (Gang et al., 2007) and (Jiang-Wei, 2008), eye blink detection was proposed for the prevention of face photo presentation attacks. In (Ali et al., 2012), the extraction of gaze direction cues was suggested for the verification of liveness in a face recognition system. Their approach required the presentation of a specialized visual stimulus consisted of collinear points.

## 1.2. Motivation & Contribution

This paper presents a methodology for the detection of iris spoofing print-attacks based on the analysis of eye movement cues. The term print-attack is used to describe a counterfeit attempt performed with a paper-printed image of a live iris, fitted with a hole in place of the pupil. Given its simplicity, this attack is the most possible expected spoofing attack to be performed at an iris recognition system. Contemporary iris recognition devices are usually equipped with a mechanism for detecting pupil reflections in order to avoid spoofing attacks with printed iris images. However, this mechanism can be easily by-passed by making a hole that allows the light to be reflected from the cornea of the eye. The fact that the corneal reflection and the pupil are used from the eye tracking algorithms in order to capture the human eye movements gave us the motivation for

exploring the eye movement signal distortions arising during such a counterfeit attempt.

The detected artifacts in an eye movement signal during a print-attack are mainly generated by the structural inconsistencies of the printed iris with respect to the live functional iris characteristics. This differentiates our approach in comparison to most of the previous iris anti-spoofing methods which are based on image quality features (e.g. texture, blur etc.). In these techniques the images are directly inspected for the detection of image degrading characteristics. However, image quality can also be degraded by other reasons related to the recording procedure (e.g. noise). Our approach is based on a signal processing framework for the statistical modeling of distortions that arise mainly due to the structural differences of real and fake irises. There is no requirement for any complex analysis of the quality of specific image features like texture etc. Also, the proposed scheme analyzes the natural eye movement without the explicit requirement of any complex light pattern or any specialized eye stimulation process.

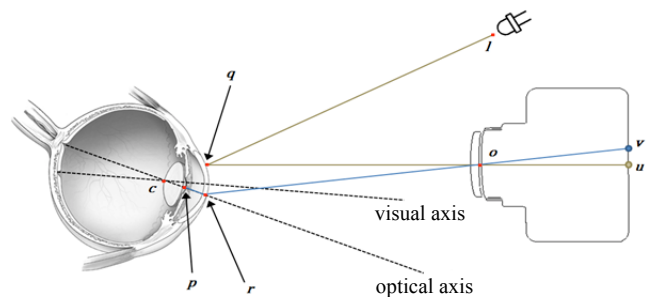
The method presented in this work improves significantly over the outcomes of the preliminary study presented in (Rigas and Komogortsev, 2014) in the following aspects:

- We present an enhanced feature set which can model additional sources of distortion. The provided detection rates are more accurate.
- We present results for experiments using a much larger database than our preliminary study. This allows for a more comprehensive analysis of the method’s large-scale potential.
- We perform an in-depth evaluation of the characteristics of the proposed method in case of different signal recording conditions (limited duration, temporal and spatial resolution). This analysis is crucial to support a possible incorporation of eye tracking capabilities to cotemporary iris scanners.

## 2. Characteristics of the captured eye movements during an iris print-attack

### 2.1. General Theory of Gaze Estimation

In this section, we present the basic theory describing the gaze estimation process based on the calculation of the relative positions of the pupil center and corneal reflection, generally known as the Pupil Center Corneal Reflection (PCCR) technique. This description will facilitate the understanding of the underlying sources that result in the appearance of artifacts in the eye movement signals in the case of an iris print-attack. Fig. 1 shows the basic components required in the eye-tracking configuration.



**Fig. 1.** Diagram of the eye-tracking configuration employed for estimating gaze based on PCCR technique.

The hardware elements of the configuration are: a) a light source  $I$  (usually infrared), generating the corneal reflection, and b) a high-speed camera capturing images of the pupil and the

corneal reflection. The exact point of a person’s fixation, the Point of Gaze (POG), is typically defined as the point where the visual axes of both eyes intersect in the space of visual stimulus. In order to find POG, we need to reconstruct the visual axis based on an initial estimation of the optical axis of the eye—due to eye anatomy these axes do not coincide.

The following description presents the basic steps followed during gaze estimation based on the general framework presented in (Guestrin and Eizenman, 2006), where additional details can be found. In order to estimate the optical axis we should find two points that it crosses, and calculate their position vectors. To this purpose, we can use the point that represents the pupil center  $\mathbf{p}$ , and the point that represents the center of curvature of a hypothetical spherical mirror modeling the eye cornea  $\mathbf{c}$ . The basic system of equations that needs to be solved for the estimation of optical axis is formed via the eye-tracking configuration geometry (Fig. 1), and can be summarized as follows:

$$\begin{aligned} \mathbf{p} - \mathbf{c} &= K & (1) \quad \mathbf{q} - \mathbf{c} &= R & (2) \quad \mathbf{r} - \mathbf{c} &= R & (3) \\ \mathbf{q} &= \mathbf{o} + k_q (\mathbf{o} - \mathbf{u}) & (4) \quad \mathbf{r} &= \mathbf{o} + k_r (\mathbf{o} - \mathbf{v}) & (5) \end{aligned}$$

Points  $\mathbf{p}$  and  $\mathbf{c}$  are connected through equation (1), where  $K$  symbolizes the distance between them. It can be observed from the configuration of Fig. 1 that the distance ( $K$ ) between  $\mathbf{p}$  and  $\mathbf{c}$  depends on the eye-structure. For this reason, the parameter  $K$  needs to be estimated using a calibration procedure (discussed in the next subsection), performed prior to the main gaze estimation process. We can employ equation (2) to connect the center of corneal curvature  $\mathbf{c}$  with the point where light is reflected on cornea’s surface, denoted with  $\mathbf{q}$ . Similarly, by using equation (3) we can connect  $\mathbf{c}$  to the point where a beam coming from the pupil center is refracted, denoted with  $\mathbf{r}$ . In both equations (2) and (3), parameter  $R$  represents the radius of the hypothetical spherical mirror modeling the cornea. This eye-structure related parameter is estimated via the same calibration procedure used for parameter  $K$ . The two last equations, (4) and (5), connect in a parametric form the points of reflection ( $\mathbf{q}$ ) and refraction ( $\mathbf{r}$ ) with the images of the corneal reflection ( $\mathbf{u}$ ) and the center of pupil ( $\mathbf{v}$ ), captured by the imaging element ( $k_q$  and  $k_r$  are parameters related only to the eye-tracking configuration). By further employing the laws of optics and the eye-tracking configuration geometry we can derive the auxiliary equations needed for completely solving the system of equations (1) to (5) (Guestrin and Eizenman, 2006). After computing the vectors for points  $\mathbf{p}$  and  $\mathbf{c}$ , we need to estimate the angle formed between the optical and the visual axis to complete gaze estimation. Again, this angle depends solely on the eye structure and may be estimated through the same calibration process used for parameters  $K$  and  $R$ . After calculating the direction of visual axis, we can use it along with a point that it crosses (e.g.  $\mathbf{c}$ ), to fully estimate POG.

#### Calibration Procedure

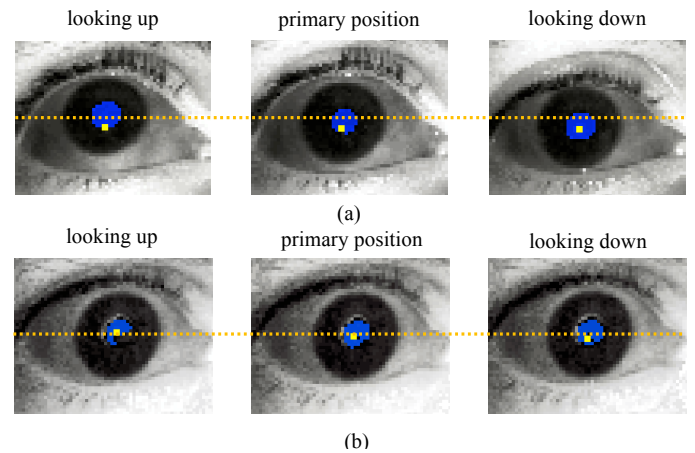
The goal of the calibration procedure is to train the eye-tracking algorithm prior to the main gaze recording procedure (described in previous subsection), by using the specific eye structure and experimental configuration characteristics. In a typical calibration process, the subject is instructed to fixate on a number of points (usually nine), positioned at predefined locations. The calibration errors, i.e. the disparity between the actual calibration points and the subject’s eye correspondences, can be represented in the form of a calibration map (Stampe, 1993). Using these errors, a number of parameters is calculated and then used to interpolate recorded eye positions to the respective places on visual stimulus space during the main

recording procedure. Additional information about the calibration process and its role during gaze estimation can be found in (Hansen and Qiang, 2010).

#### 2.2. Types of Generated Eye Movement Signal Distortions

From the above description it can be clearly understood that during an iris print-attack the structural and functional differences between the printed and a natural iris can affect the gaze estimation procedure based on equations (1) to (5). This may lead in the appearance of various artifacts in the eye tracking signals. In this section, we present the main generating sources of these signal artifacts along with the different forms of distortion that they cause.

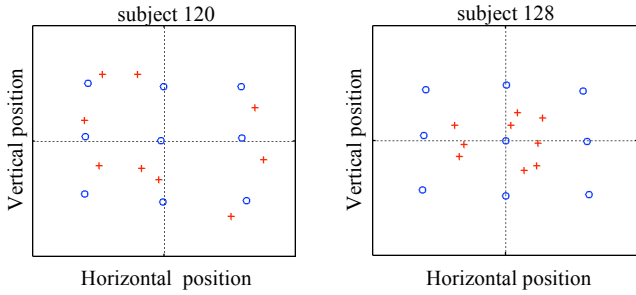
In Fig. 2, we practically demonstrate one of the main structural discrepancies between a printed iris and a real iris. In the case of a real iris (Fig. 2a), the pupil follows the natural movement of the eye and the iris. For example, when an upward eye movement is performed, the pupil center moves along with the iris in the upward direction. Simultaneously, the corneal reflection, marked as a bright (yellow) dot, appears to be close to the lower boundary of the pupil. An analogous process occurs in the event of a downward movement. Oppositely, in the case of a printed iris (Fig. 2b), the pupil center appears in a fixed position, but the corneal reflection is still moving. When the exact same movements—as previously—are performed, the relative captured positions of the pupil center and the corneal reflection diverge in an unnatural way. This inconsistent positioning of the pupil center and the corneal reflection is imprinted on the corresponding images  $\mathbf{v}$ ,  $\mathbf{u}$ , captured by the camera module of an eye tracking system (Fig. 1), and in turn transferred through equations (4), (5) to the rest equations used for the reconstruction of the optical axis, and the estimation of POG.



**Fig. 2.** Discrepancies appearing in the behavior of (a) a real iris and (b) a printed iris, while gaze focuses exactly at the same fixation points (pupil area marked with dark/blue color, corneal reflection marked as a light/yellow dot).

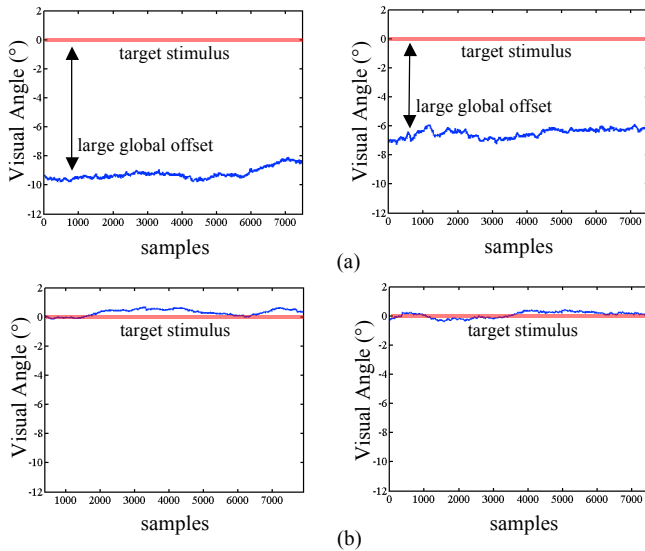
The observed discrepancies between a printed and a real iris are affecting the results of the calibration procedure as well. The structural inconsistencies of a printed iris result in the generation of calibration maps that substantially diverge from the typical pattern corresponding to a real eye. This leads on the calculation of erroneous values for the eye-structure related parameters estimated through the calibration procedure (e.g.  $K$ ,  $R$ ), and acts as an additional source of distortion in the eye movement signals. Fig. 3, shows some examples of the calibration maps that are generated from real eyes (denoted with blue circles), and their printed correspondences used to perform spoofing attacks (denoted with red crosses). We may observe that the maps corresponding to the real eyes, even if formed from different

subjects, follow a similar pattern, which corresponds to the fixed locations of the nine points used for calibration. In contrast, calibration maps corresponding to their printed iris counterparts strongly deviate from the typical patterns formed by natural eyes.



**Fig. 3.** Calibration maps generated from real eyes (blue circles) and their printed counterparts (red crosses).

There are various types of distortions that may arise in the eye-tracking signals due to the combined effect of discrepancies during the calibration procedure and the main gaze estimation process. The most prominent type of distortion in the eye tracking signal recorded during an iris print-attack is the global positional offset, i.e. a uniform translation of the recorded signal from its expected position with regard to the visual stimulus.

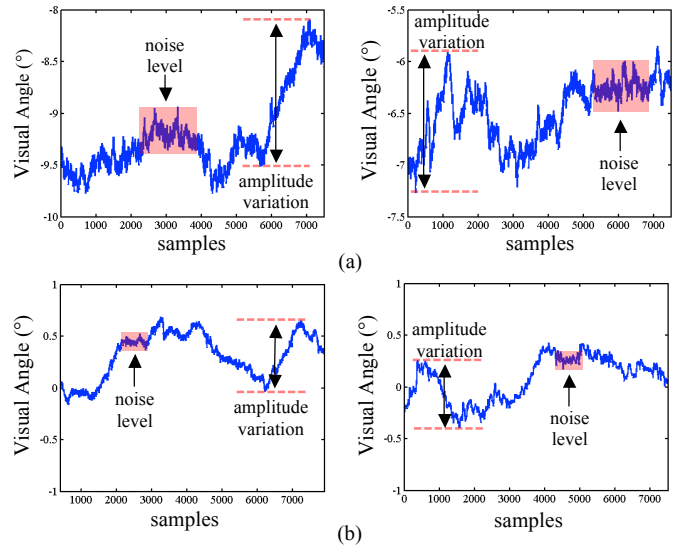


**Fig. 4.** Demonstration of eye movement positional signals captured in case of: (a) an iris print-attack, and (b) a real eye.

In Fig. 4, we present some example positional signals captured during our experiments in the case of an iris print-attack (Fig. 4a), and from a real eye (Fig. 4b). It can be easily observed that in the case of an iris print-attack large global positional offsets appear in the captured eye movement signals, when compared to the target stimulus position (marked with red solid line). Another observation is that the exact positioning (exact offset) of the signals generated for different print-attacks can vary considerably. Adversely, the positional signals captured from real eyes appear to be closely centered to the target stimulus position. In this case, the signals may present some natural variability caused by eye micro-movements (tremors, drifts, and micro-saccades), but in overall, their placement is consistent with the presented stimulus location.

A second category of signal distortions caused by print-attacks involves the appearance of abnormal local amplitude variations, i.e. irregular differences of amplitude levels in parts of the signal.

Examples of this kind of artifact are shown in Fig. 5. We magnified the eye movement signals depicted in Fig. 4 in order to inspect clearly the local amplitude variations of signals coming from iris print-attacks (Fig. 5a), and from real eyes (Fig. 5b). As it can be observed, there is a larger level of variation in local amplitudes for the signals generated during an iris print-attack compared to the real eye signals. The main cause for the appearance of these larger local amplitudes is again related to the functional discrepancies between the real eyes and their printed counterparts. Whereas the global positional offsets distortions are caused by erroneous estimations of the global gaze position of the eye, the local amplitude variations are inaccurate estimations of the micro-movements of the eye. Specifically, the source of these inaccuracies is the fixed pupil boundary of the printed iris and the captured corneal reflection micro-movements from the intruder's eye.



**Fig. 5.** Demonstration of local amplitude variations and noise levels for signals captured in the case of: (a) an iris print-attack, and (b) a real eye. Zooming in all cases corresponds to exactly the same range of 2° of visual angle.

A third class of signal distortions is caused by the finite quality and the shape of the pupil hole created on the printed irises. A directly observed result of these imperfections is the presence of enhanced levels of noise contaminating signals captured during an iris print-attack. Representative examples of the noise levels for signals captured from an iris print-attack and a real eye are marked with (red) rectangles in Fig. 5. Another phenomenon which occurs due to the finite quality and the shape of the pupil hole is the appearance of higher than usually percentages of invalid raw positional data, which happens when eye tracking equipment fails to determine gaze coordinates.

### 3. Proposed methodology for iris print-attack detection

In previous section, we described the different types of global and local distortions appearing in the eye movement signals recorded during an iris print-attack. In the current work, we present a methodology for modeling these signal distortions and detecting the print-attacks. In Fig. 6 we present a block diagram of the basic procedures followed during the suggested print-attack detection scenario. Following, we describe in detail the procedures for the implementation of the suggested method. It should be emphasized that the feature extraction algorithm is based on low complexity calculations, which is an important requirement for an anti-spoofing protection scenario.

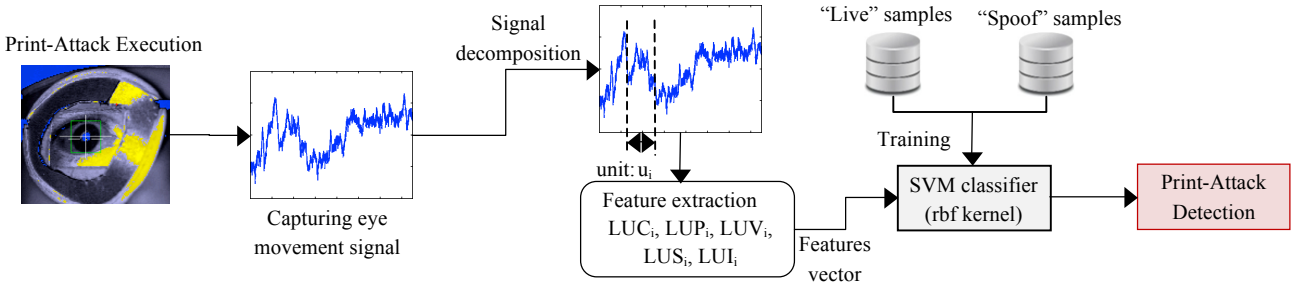


Fig. 6. Block diagram of the procedures followed in the proposed methodology.

### 3.1. Decomposition of Captured Eye Movement Signals

The first stage of the processing algorithm involves the decomposition of every eye movement recording into a set of elementary units representing the micro-movements of the eye. This initial decomposition of the eye movement signal into elementary units facilitates the dynamic statistical modeling both of the global and of the local distortions appearing in the signals captured during an iris print-attack. In order to perform the signal decomposition we employ the Velocity Threshold Identification (I-VT) technique (Salvucci and Goldberg, 2000). This method was originally developed for the extraction of the fixation and saccadic components from eye movement signals. In the current methodology, we need to obtain a fine-scaled decomposition of each signal into elementary units of eye micro-movements. Thus, we proceed to a carefully implemented parameterization of the I-VT algorithm based on the required signal characteristics, by utilizing a velocity threshold of  $5^\circ/\text{sec.}$  to filter out micro-saccades (and larger saccades if they are present in the signal) and leave fixational drift parts as the elementary units for subsequent analysis. Please note that fixational tremor cannot be reliably detected by the employed equipment (i.e., it requires scleral coil equipment (Robinson, 1963)), and thus the impact of tremor is not investigated in our work. The process is described by the following formulation:

$$EMr \rightarrow IVT(5^\circ/\text{sec.}) \rightarrow u_i, i = 1, \dots, N \quad (6)$$

In Eq. (6) we denote with  $u_i$  each of the  $N$  elementary units extracted from the decomposition of an eye movement recording ( $EMr$ ). The formation of the features used for the detection of iris print-attacks is implemented with the calculation of statistical measures on the extracted elementary eye movement signal units.

### 3.2. Statistical Modeling and Feature Extraction

During the second stage of the processing algorithm we proceed to the modeling of each elementary unit by calculating a set of statistical measures. The selection of the specific measures is directly connected to the analysis of the various print-attack signal distortions presented earlier. Thus, the calculated statistics encapsulate information related to the global and local amplitude properties of signals, the noise levels, and the invalidity.

**Local Unit Centroid.** The local centroid of each elementary unit ( $u_i$ ) provides an aggregated representation of samples positional information, and can be used to represent the global positioning properties of elementary units:

$$LUC_i = \sum_{m=1}^{M_{u_i}} u_i(m) / M_{u_i} \quad (7)$$

where  $M_{u_i}$  is the total number of samples of the elementary unit  $u_i$ . This number can vary due to different lengths of the units.

**Local Unit Power.** This measure is used to model the local signal energy per sample in every elementary unit ( $u_i$ ). It carries

information related both to the global offsets and the local amplitudes, and can be calculated as the signal power corresponding to every unit:

$$LUP_i = \sum_{m=1}^{M_{u_i}} |u_i(m)|^2 / M_{u_i} \quad (8)$$

**Local Unit Variance.** The signal variance is defined as the signal power for every elementary unit ( $u_i$ ) when subtracting the mean. Consequently, this specific statistical measure isolates the local amplitude variation characteristics, and thus provides robustness in cases where global offset information becomes insufficient. Local elementary unit variance can be calculated as:

$$LUV_i = \sum_{m=1}^{M_{u_i}} |u_i(m) - LUC_i|^2 / M_{u_i} \quad (9)$$

**Local Unit SNR.** We can express the Signal-to-Noise Ratio for every unit ( $u_i$ ), as the ratio of the mean amplitude of the samples to the corresponding standard deviation. This statistic can model noise artifacts appearing due to the finite quality of the iris paper-print and the artificial construction of the pupil hole.

$$LUS_i = LUC_i / \sqrt{LUV_i} \quad (10)$$

**Local Unit Invalidity.** As already mentioned, eye movement signals recorded during an iris print-attack usually appear to have enhanced levels of invalidity. The invalidity level of every unit ( $u_i$ ) can be expressed as:

$$LUI_i = M_{u_i}^{inval} / M_{u_i} \quad (11)$$

where  $M_{u_i}$  is the number of samples marked from the eye-tracker as invalid, i.e. not successfully captured.

### 3.3. Feature Vector Formation

The final feature vector is formed with the calculation of the average values and the standard deviations over the statistics extracted from all separate eye movement signal units, and the concatenation of values into a common representation:

$$f^{avg} = (LUC^{avg}, LUP^{avg}, LUV^{avg}, LUS^{avg}, LUI^{avg})_{x,y} \quad (12)$$

$$f^{std} = (LUC^{std}, LUP^{std}, LUV^{std}, LUS^{std}, LUI^{std})_{x,y} \quad (13)$$

$$f = (f^{avg}, f^{std}) \quad (14)$$

We denote with  $x, y$  the corresponding coefficients for the horizontal and vertical components of eye movement. It is important to mention that the procedure adopted for forming the final feature vectors allows for a hierarchical modeling of the signal distortions. The generated distortions can affect different parts of an eye movement signal in different degrees. For this reason, the statistics are initially calculated for every single elementary unit, and then, they are incorporated into a compact representation capable to represent both the global characteristics and the local amplitude variations in the signals.

## 4. Experimental methodology

The experiments for the collection of the real and the print-attack recordings were performed as two separate processes. Initially, we recorded the eye movements and the iris images from 200 subjects, thus forming the database of live recordings. Then, we used the iris images from the live subjects in order to create the fake iris printouts and attack the eye tracking device. The eye movement signals recorded during this procedure formed the database of print-attack recordings.

### 4.1. Apparatus

All eye movement recordings were performed using an EyeLink 1000 eye-tracker working at 1000 Hz (vendor reported spatial resolution of  $0.01^\circ$  RMS). In our experiments the eye-tracker operated in monocular mode collecting samples from the left eye. By employing very high grade commercial eye-tracking equipment we were able to conduct an analysis of our method's robustness by simulating scalable degradation of temporal and spatial resolution. The recordings of iris images were implemented via a CMITech BMT-20 system. This device captures images of both irises at resolution 640x480 pixels in a format conforming to standard ISO/IEC 19794-6:2011 for iris image data. For our experiments we used the left eye iris images.

The iris printouts used for conducting the attacks were printed on high quality matte paper, with the use of a HP Laserjet 4350dtn grayscale printer with resolution of 1200x1200 dpi. During our initial investigation we experimentally found that printing the iris patterns on a glossy paper using a laser color printer is not suitable for performing print-attacks at the eye-tracking device due to the reflectance properties of the resulting printout. In such case, the eye-tracking software fails to acquire any valid estimation for pupil boundary and corneal reflection, and the detection becomes trivial.

### 4.2. Experimental Stimulus

A single fixation point was employed as the visual stimulus. The point was positioned at a visual angle of  $3.5^\circ$  above the primary eye position (eye staring straight ahead). We carefully selected this type of stimulus (instead, for example, of a moving point) for the following reasons:

a) It is the most demanding scenario for the case of an iris print-attack and allows for an evaluation of the fundamental characteristics of our method. A visual stimulus that will provoke larger eye movements would result in even more pronounced distortions in the signals making thus the detection easier.

b) The overarching motivation of our work is to enable higher security in iris recognition devices by employing eye tracking capabilities. Iris recognition devices usually require a user to stare straight ahead and not make excessively large eye movements, for capturing a good quality iris image. The use of a stationary point stimulus during the experiments allows for the evaluation of our method under such a scenario.

### 4.3. Participants

A total of 200 subjects (99 male/101 female), ages 18-44 (average = 22, STD = 4.3) participated in the collection of data from real eyes. From the total number of participants, 96 had a normal (not-corrected) vision, and 104 had a corrected vision (46 glasses/58 contact lens). Each participant enrolled twice, forming thus a database of 400 eye movement recordings and the corresponding 400 real iris images. It should be noted that the large volume of subjects provides a sufficient diversity of eye/pupil shapes and sizes, allowing for a thorough evaluation of the proposed scheme. Texas State University institutional review

board approved the study, and participants provided informed consent.

The experiments for the collection of eye movements during the print-attacks were performed using the 400 printed iris images from the real eyes. Print-attacks were performed by a specific person that was not among the subjects employed in the database of real eyes. This decision was purposefully made in order to ensure that the differences between the real and print-attack eye movement signals were primarily the result of structural and functional inconsistencies of the iris printouts, rather than the result of inter-person eye movement differences. The person making the print-attacks did not have any reported eye movement disorders that could affect the captured signals.

The constructed datasets containing the eye movement recordings both for the real eyes and for their print-attack counterparts are publicly available via link<sup>1</sup>. The database contains also the iris images used to create the printouts. It should be noticed that our processing method uses only the eye tracking signals. However, we included also the real iris images in the database for any future techniques that might combine both.

### 4.4. Experimental Procedure

During the collection of eye movements from the real subjects, each participant's head was positioned at a distance of 550 millimeters from a 19" computer screen (474x297 millimeters, resolution 1680x1050 pixels), where the visual stimulus was presented. Each subject was instructed to fixate on the stationary point stimulus for a period of 15 seconds. During the implementation of the eye movement recordings with the corresponding iris printouts, each iris image was fastened to an eye patch, and was steadily adjusted on the head of the subject performing the attacks. Print-attacks were implemented against the same eye tracking device and recording setup as previously. A video demonstration of the implementation of an iris print-attack against the eye tracking device is provided in<sup>1</sup>.

We opted to perform two separate print-attack scenarios corresponding to the possible practical implementations of a spoofing attack against an eye-tracking system:

*Spoofing Attack Scenario I (SAS-I)*. In the first scenario the spoofing attack is conducted both during the calibration stage and during the stimulus presentation stage. It should be mentioned that during the calibration stage the subject performing the attack needs to make small head movements in order to bring the more distant points into the field of view, mimicking thus the natural eye movements. In the case of SAS-I, the distortions are generated both from the calibration stage and from the inconsistent positioning of pupil and corneal reflection during the stimulus presentation stage.

*Spoofing Attack Scenario II (SAS-II)*. In the second scenario the spoofing attack is conducted only during the stimulus presentation stage. In this case, the calibration stage is performed with the attacker's real eye. This scenario emulates the case when calibration is skipped. We decided to test this scenario since some eye trackers do not require re-calibration after the initial calibration is done. Signal distortions during this scenario are generated only from the inconsistent positioning of pupil and corneal reflection during the eye-tracking procedure.

## 5. Results

### 5.1. Distinctiveness of Single Features

---

<sup>1</sup> [http://cs.txstate.edu/~ok11/etpad\\_v2.html](http://cs.txstate.edu/~ok11/etpad_v2.html)

In order to investigate the relative contribution of each single feature in the overall performance, we calculate the decidability index  $d'$  ( $d'$ -prime value) (Daugman, 2003), which is a measure of the separation of genuine/impostor distributions for each feature. Table 1 presents the  $d'$  values for each of the extracted features.

**Table 1. Decidability index ( $d'$ ) for each single feature.**

Feature	Direction	$d'$	
		SAS-I	SAS-II
LUC <sub>AVG</sub>	Horizontal	0.17	1.34
	Vertical	0.04	0.95
LUP <sub>AVG</sub>	Horizontal	0.53	1.13
	Vertical	0.74	0.57
LUV <sub>AVG</sub>	Horizontal	0.32	0.31
	Vertical	0.33	0.28
LUS <sub>AVG</sub>	Horizontal	0.48	0.15
	Vertical	0.47	0.04
LUI <sub>AVG</sub>	Both	0.64	0.21
LUC <sub>STD</sub>	Horizontal	0.57	0.08
	Vertical	0.59	0.07
LUP <sub>STD</sub>	Horizontal	0.44	0.31
	Vertical	0.46	0.45
LUV <sub>STD</sub>	Horizontal	0.30	0.24
	Vertical	0.31	0.19
LUS <sub>STD</sub>	Horizontal	0.69	1.35
	Vertical	0.85	0.75
LUI <sub>STD</sub>	Both	0.37	0.27

## 5.2. Performance Evaluation Metrics

During the evaluation experiments we employ a SVM classifier<sup>2</sup> with a Gaussian Radial Basis Function kernel (SAS-I,  $\sigma = 1$ , SAS-II,  $\sigma = 2$ ). In all experiments we use a 50%-50% training-testing split for the SVM classifier, and the calculated rates are averaged over 100 iterations.

The used metrics (standard ISO/IEC 30107-3 for presentation attack detection) are presented below. In the definitions, the term “live” feature vectors refers to samples from real irises, and the term “spoof” feature vectors refers to samples from printed irises.

**Attack Presentation Classification Error Rate (APCER).** APCER is defined as the percentage of “spoof” test feature vectors that are incorrectly classified as “live”.

**Normal Presentation Classification Error Rate (NPCER).** NPCER is defined as the percentage of “live” test feature vectors that are incorrectly classified as “spoof”.

**Average Classification Rate (ACR).** ACR is defined as the average percentage of correctly classified test feature vectors (either “live” or “spoof”):

$$ACR = 100\% - APCER + NPCER / 2 \quad (15)$$

**Equal Error Rate (EER).** EER is the point of the Receiver Operating Characteristic (ROC) curve for which APCER equals NPCER. To construct the ROC curves we use the “soft-margin” implementation of the SVM classifier, and utilize the distances of the misclassified feature vectors from the optimum separating hyper-plane (slack variables) as “soft-scores”. By varying the acceptance threshold for these “soft-scores” we can build the ROC curve and determine the EER.

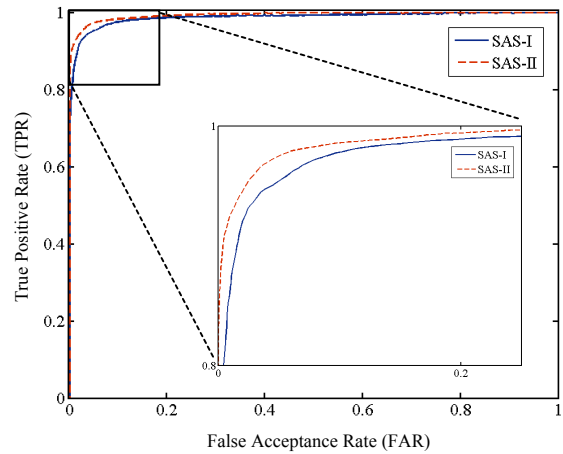
**Table 2. Performance results for print-attack detection.**

Performance Metric	Current Method (enhanced feature set)		Preliminary Method (Rigas and Komogortsev, 2014)	
	SAS-I	SAS-II	SAS-I	SAS-II
ACR (STD)	95.4 (1.0)%	96.5 (1.0)%	93.0 (1.1)%	95.7 (0.8)%
APCER (STD)	5.9 (1.5)%	3.4 (1.2)%	12.0 (2.4)%	6.7 (1.7)%
NPCER (STD)	3.4 (1.5)%	3.5 (1.6)%	2.7 (1.2)%	1.9 (1.0)%
EER (STD)	4.7 (0.8)%	3.4 (0.9)%	5.7 (1.1)%	3.9 (0.8)%

## 5.3. Print-Attack Detection Performance

In Table 2, we present the calculated print-attack detection rates along with the corresponding standard deviations (STD). Also, we show the corresponding print-attack detection rates for the 200-subject datasets achieved by the preliminary feature set presented in (Rigas and Komogortsev, 2014). The ACR for the case of the SAS-I peaks at a value of 95.4%, and for the case of the SAS-II at a value of 96.5%. It can be noticed that APCER for the SAS-I case is greater than NPCER, with values of 5.9% and 3.4% respectively. In the case of the SAS-II the situation is reversed, with APCER being 3.4% and NPCER 3.5%. A comparison with the results for the simple feature set used in (Rigas and Komogortsev, 2014) reveals an improvement both of the ACR and the EER. The APCER is considerably improved, whereas the NPCER is slightly increased. Also, the trade-off between APCER and NPCER appears to be more balanced.

In Fig. 7, we show the constructed ROC curves used for the calculation of the EER (note that  $TPR = 1 - FRR$ ). These curves describe the overall operational characteristics of the proposed method. The minimal EER values calculated for these curves are 4.7% for the SAS-I and 3.4% for the SAS-II respectively.



**Fig. 7. ROC curves for print-attacks of type SAS-I and SAS-II.**

## 5.4. Performance Analysis for Limited Recording Duration

We decided to conduct an experimental analysis regarding the behavior of performance when limiting the duration of the captured eye movement signal (input signal). As described in Section 4, the original recordings have duration of 15 seconds. However, for anti-spoofing modules embedded in more complex biometric recognition systems it is usually required to provide fast decisions, making it important to extract the print-attack decision from data captured within a relatively short recording duration.

<sup>2</sup> used MATLAB functions: svmtrain, svmclassify

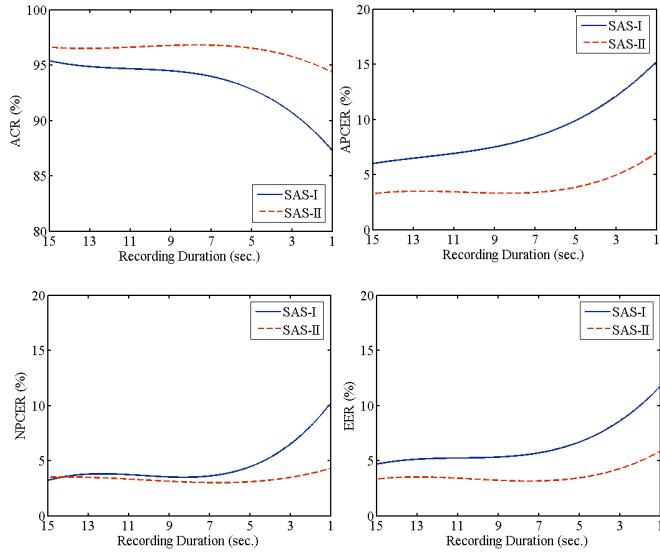


Fig. 8. Behavior of detection rates for limited duration of the input signal.<sup>3</sup>

Fig. 8 illustrates the performance of our method by artificially reducing the recording duration (cut-off initial part of the signal). For the ACR metric, the rates remain at the optimum levels about 96% for recording time over 7 seconds, for both types of attacks (SAS-I, SAS-II). For shorter recording time the performance starts decreasing, however not very drastically. Even for the lowest tested duration of 1 second, the ACR values for the SAS-I and SAS-II are 87.2% and 94.2%. A similar behavior is also mirrored by APCER and NPCER metrics, with their highest values being 15.1% and 10.5% for the case of SAS-I, and 7.2% and 4.4% for the case of SAS-II. For the EER metric, the optimum levels (3.5-4.5%) seem to persist also for a minimum recording time of 7 seconds. After that, the EER gradually increases to values of 11.9% for the SAS-I and 6.1% for the SAS-II, for recording duration of 1 second.

### 5.5. Performance Analysis for Temporal Resolution Degradation

We conducted experiments to evaluate the robustness of the proposed method by simulating recording conditions of lower sampling rate than the original frequency of 1000 Hz. To this purpose, we successively down-sample the original signals in lower temporal resolution and re-run the print-attack detection algorithm for the down-sampled signals. The frequencies used in our experiments are: 500 Hz, 250 Hz, 120 Hz, 75 Hz, 30 Hz, and 15 Hz, and the results are shown in Fig. 9. For the ACR metric, we observe a worst-case ACR of 89% for the SAS-I, and 94.8% for the SAS-II. The respective worst-case APCER and NPCER values are 11.2% and 10.9% for the SAS-I, and 6.1% and 5.4% for the SAS-II accordingly. The worst-case values for the EER metric are 11% for the SAS-I case, and 5.3% for the SAS-II case.

### 5.6. Performance Analysis for Spatial Resolution Degradation

We also decided to investigate the impact of spatial resolution degradation on the recorded eye movement signals, by dithering noise to the raw recorded signals captured with the eye-tracking device. Whereas in the case of temporal resolution degradation the rates behavior changed smoothly, the addition of noise to the samples is expected to affect the detection performance more dramatically, given the by-principle involvement of local amplitude variations and noise levels in the extracted feature set of the proposed algorithm.

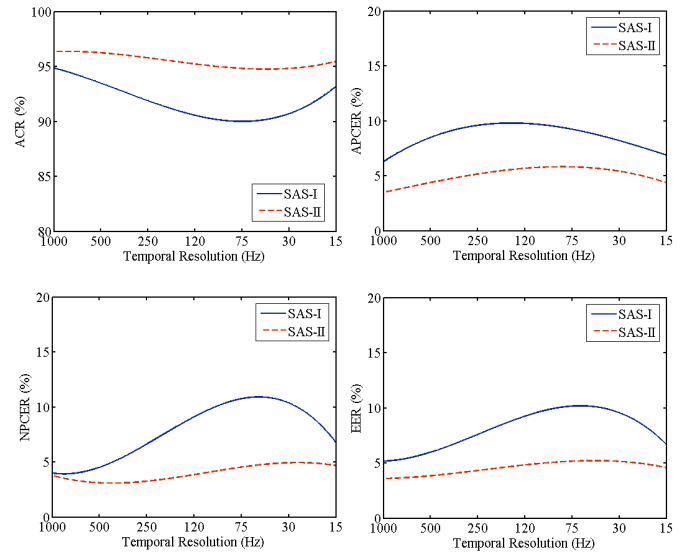


Fig. 9. Behavior of detection rates for temporal resolution degradation.<sup>3</sup>

As illustrated in Fig. 10, the detection rates remain in an acceptable range while the dithering noise does not exceed  $0.75^\circ$  of visual angle. In this case, the ACR metric decreases to a value of 90% for the SAS-I, and 95.5% for the SAS-II, whereas the EER metric increases to 9.3% and 4.6% accordingly. This behavior is also reflected from the values of the APCER and NPCER, which gradually increase to values of 11.3% and 8.6% for the SAS-I, and 5.4% and 3.6% for the SAS-II. For higher levels of dithering noise the decrease in performance is more drastic and reaches prohibitive levels for the task of print-attack detection.

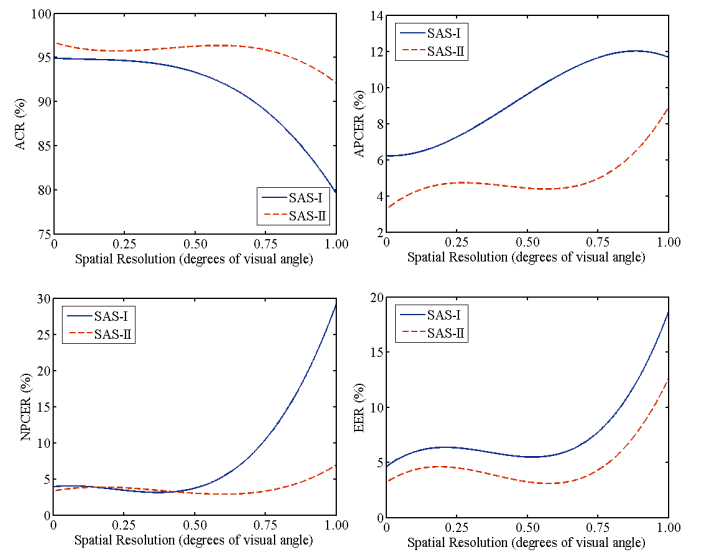


Fig. 10. Behavior of detection rates for spatial resolution degradation.<sup>3</sup>

## 6. Discussion

### 6.1. General Performance

The results demonstrated in Table 2 portray the satisfactory performance that can be achieved by the proposed method in the task of print-attack detection. The achieved ACR values are over 95% in both performed attack scenarios, and the EER values calculated from the ROC curves (shown in Fig. 7) are in the range of 3-5%. The use of a large database of eye movement signals allowed for an in-depth analysis of the proposed method, and the robustness assessment for various degrading conditions

<sup>3</sup> Data fitted in curves using MATLAB function: fit (3-order polynomial)



for the recorded signals. Furthermore, the overall rates are improved compared to our preliminary work in (Rigas and Komogortsev, 2014), due to the employed feature set used for modeling additional sources of signal distortion. The values of decidability index  $d'$  (Table 1) allow to infer the relative contribution of the extracted features. It is worth observing that whereas some features contribute highly on both the SAS-I and SAS-II, others seem to contribute differently due to the existing differences in the signal characteristics in the two scenarios.

Generally, our experimental findings show an optimistic perspective for the incorporation of eye movement-driven features in current iris recognition devices. The proposed method performs with moderate degradation in performance for signal durations as low as 1 second, however, the top performances are achieved for signal durations of about 7 seconds. During a practical implementation it is possible to adapt the required signal duration according to the system's requirements (trade-off between registration time and required detection accuracy). Another possible scenario involves the incorporation of the algorithm in a multi-modal system that fuses eye movement-driven biometrics and iris biometrics. In this case, the already available eye movement signal can be additionally used for performing liveness detection (single instance or continuous) of a subject with minimum additional cost. Furthermore, in the proposed scheme the feature extraction and vector formation steps can be computed via signal-processing procedures based on simple sum/product operations, which can be efficiently performed by digital signal processing (DSP) units.

It should be noticed that a direct comparison of our approach with any previous techniques based on image quality characteristics (e.g. texture, defocus distortions etc.) cannot happen due to the fact that the current database consists of eye movement signals and not from the images captured during the print-attack. Furthermore, none of the previously constructed databases provides eye movement signals. To provide an indirect assessment, we present the indicative performance levels that were obtained by some of the previously implemented methods. In (Pacut and Czajka, 2006), inspection of frequency spectrum in two different scenarios brought about rates ranging from null up to 11.1% for the APCER, and up to 2.8% for the NPCER. For the method presented in (Zhuoshi et al., 2008), where texture characteristics of images printed on contact lenses were examined, the reported ACR ranged from 97.8% to 100% for the first database they used, and from 76.8% to 95.8% for the second. In (Czajka, 2013), the inspection of "alien" frequencies in the image spectrum resulted in a performance of 5% APCER for null false rejection of valid samples. An experimental study of pupil constriction under different illumination scenarios (Xinyu et al., 2013), exhibited results for ACR ranging from 82% to 99.9%. The above rates give a general idea of the performance levels achieved in the field of iris anti-spoofing protection. It should be added, though, that in most of the previous efforts different and task-specific scenarios were used, and this partially explains the diversity in the reported detection accuracy ranges.

### 6.2. Robustness for Signal Recording Degradations

Our analysis regarding the robustness of the proposed method under different cases of signal degradation led to several useful findings. There is a relative smooth decrease of detection rates when the temporal resolution is degraded down to 15 Hz, as demonstrated by the results of Fig. 9. In addition, it can be observed that the rates in the case of SAS-II present a substantially milder variation than for the SAS-I. A possible explanation is that the smoothing effect on distortions, due to temporal down-sampling, is more important in the case of the

heavily distorted signals of the SAS-I than for the SAS-II. The significance of the obtained results can be further magnified given the fact that contemporary iris recognition devices typically operate with relatively low sampling rates. A phenomenon mostly observed in the case of temporal resolution degradation curves (Fig. 9), is that sometimes the results do not change monotonically. This effect can be attributed to the fine-scale influence of different down-sampling rates on the signal decomposition algorithm. The slightly different form of the smoothed signal leads in turn to slightly better (or worse) modeling of the elementary units, resulting in the observed behavior of the curves.

The degradation in the spatial resolution of the captured signal has also an impact on the detection rates (Fig. 10). In specific, the performance seems to be affected severely when dithering noise amplitude exceeds  $0.75^\circ$  of visual angle. It should be noticed though that this decrease in performance is expected, since after a specific level the noise starts absorbing important signal characteristics which are indicative of the print-attacks.

### 6.3. Limitations

The presented experimental study should be examined under the scope of certain limitations. Our experiments were performed in a controlled environment away from any external parameters, and the heads of the subjects were comfortably stabilized with the use of a headrest. It should be noticed, however, that the modern remote/head-mounted eye-tracking technologies can allow different degrees of head movement, and can provide thus additional robustness in the case of a practical scenario.

Another important issue involves the influence of several physical/behavioral states (e.g. fatigue, intoxication) and/or medical disorders on the recorded eye movement patterns. The optokinetic nystagmus (Leigh and Zee, 2006) (Ch. 10 - pp. 480-521) is an eye movement disorder that results in fixational signals presenting larger positional variability compared to the normal ones. The saccadic intrusions (Leigh and Zee, 2006) (Ch. 10 - pp. 521) are abrupt movements which appear in the form of artifacts contaminating the normal activity of an eye movement signal. The signal variations induced by these and other eye movement disorders can lead the detection algorithm to falsely correlate these distortions with a spoofing attack. This, in turn, may result in an increase of the falsely rejected biometric signals, thus increasing the NPCER. However, it is not expected to affect the APCER performance, since an attacker with an eye movement disorder is expected to have even less success in mimicking the normal eye movement behavior.

## 7. Conclusion

In this work, we presented a method based on eye movement traits for the extraction of features indicating an iris print-attack. We used a database containing real eye movements recorded from a large number of subjects, and the corresponding signals recorded during a spoofing attack performed with the printed iris images captured from the subjects. The developed scheme is capable to statistically model the eye movement signal distortions appearing due to the artificial nature of the iris paper-prints. The obtained rates demonstrate the effectiveness of the suggested method on the detection of spoofing print-attacks under different scenarios. We performed additional simulations for exploring the performance robustness in case of limited recording duration, and signal capturing quality degradation. Our analysis shows that the detection performance remains in reasonable levels for signal durations down to 1 second, sampling rates as low as 15 Hz, and dithering noise of amplitude less than  $0.75^\circ$  of visual angle.

In our future research we will examine the possibility of extracting additional eye movement features that could be incorporated with the current methodology in order to address more sophisticated attack scenarios, involving printed contact lenses and synthetic eye replicas.

## Acknowledgement

This work is supported in part by NSF CAREER Grant #CNS-1250718 and NIST Grants #60NANB10D213 and #60NANB12D234. Special gratitude is expressed to Dr. E. Abdulin, T. Miller, Ch. Heinrich for proctoring eye movement recordings.

## References

- Ali, A., Deravi, F., Hoque, S., 2012. Liveness Detection Using Gaze Collinearity, 3rd Int. Conference on Emerging Security Technologies (EST), pp. 62-65.
- Bodade, R., Talbar, S., 2009. Dynamic iris localisation: A novel approach suitable for fake iris detection, Int. Conference on Ultra Modern Telecommunications & Workshops (ICUMT '09) pp. 1-5.
- Czajka, A., 2013. Database of iris printouts and its application: Development of liveness detection method for iris recognition, 18th Int. Conference on Methods and Models in Automation and Robotics (MMAR), pp. 28-33.
- Daugman, J., 1993. High confidence visual recognition of persons by a test of statistical independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 15, 1148-1161.
- Daugman, J., 1994. Biometric Personal Identification System Based on Iris Analysis, U.S. Patent No. 5,291,560.
- Daugman, J., 2003. Demodulation by Complex-valued Wavelets for Stochastic Pattern Recognition. *Int. Journal of Wavelets, Multiresolution and Information Processing* 01, 1-17.
- Daugman, J., 2007. New Methods in Iris Recognition. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics* 37, 1167-1175.
- Galbally, J., Ortiz-Lopez, J., Fierrez, J., Ortega-Garcia, J., 2012. Iris liveness detection based on quality related features, 5th IAPR Int. Conference on Biometrics (ICB), pp. 271-276.
- Galbally, J., Ross, A., Gomez-Barrero, M., Fierrez, J., Ortega-Garcia, J., 2013. Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms. *Computer Vision and Image Understanding* 117, 1512-1525.
- Gang, P., Lin, S., Zhaohui, W., Shihong, L., 2007. Eyeblick-based Anti-Spoofing in Face Recognition from a Generic Webcam, 11th IEEE Int. Conference on Computer Vision (ICCV 2007), pp. 1-8.
- Guestin, E.D., Eizenman, E., 2006. General theory of remote gaze estimation using the pupil center and corneal reflections. *IEEE Transactions on Biomedical Engineering* 53, 1124-1133.
- Hansen, D.W., Qiang, J., 2010. In the Eye of the Beholder: A Survey of Models for Eyes and Gaze. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 32, 478-500.
- Haralick, R.M., Shanmugam, K., Dinstein, I.H., 1973. Textural Features for Image Classification. *IEEE Transactions on Systems, Man and Cybernetics SMC-3*, 610-621.
- He, X., An, S., Shi, P., 2007. Statistical texture analysis-based approach for fake iris detection using support vector machines, 2007 Int. Conference on Advances in Biometrics. Springer-Verlag, pp. 540-546.
- He, Z., Sun, Z., Tan, T., Wei, Z., 2009. Efficient Iris Spoof Detection via Boosted Local Binary Patterns, in: Tistarelli, M., Nixon, M.S. (Eds.), *Advances in Biometrics*. Springer Berlin Heidelberg, pp. 1080-1090.
- Hui, Z., Zhenan, S., Tieniu, T., 2010. Contact Lens Detection Based on Weighted LBP, 20th Int. Conference on Pattern Recognition (ICPR) pp. 4279-4282.
- Jiang-Wei, L., 2008. Eye blink detection based on multiple Gabor response waves, 2008 Int. Conference on Machine Learning and Cybernetics, pp. 2852-2856.
- Komogortsev, O.V., Karpov, A., Holland, C.D., 2015. Attack of Mechanical Replicas: Liveness Detection With Eye Movements. *IEEE Transactions on Information Forensics and Security* 10, 716-725.
- Lee, E.C., Park, K.R., Kim, J., 2005. Fake Iris Detection by Using Purkinje Image, in: Zhang, D., Jain, A.K. (Eds.), *Advances in Biometrics*. Springer Berlin Heidelberg, pp. 397-403.
- Leigh, R.J., Zee, D.S., 2006. *The Neurology of Eye Movements*.
- Li, M., Tieniu, T., Yunhong, W., Dexin, Z., 2003. Personal identification based on iris texture analysis. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 25, 1519-1533.
- Ojala, T., Pietikainen, M., Maenpaa, T., 2002. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 24, 971-987.
- Ortiz-Lopez, J., Galbally, J., Fierrez, J., Ortega-Garcia, J., 2011. Predicting iris vulnerability to direct attacks based on quality related features, 2011 IEEE Int. Carnahan Conference on Security Technology (ICST), pp. 1-6.
- Pacut, A., Czajka, A., 2006. Aliveness Detection for IRIS Biometrics, 40th IEEE Int. Carnahan Conferences Security Technology, pp. 122-129.
- Phillips, P.J., Scruggs, W.T., O'Toole, A.J., Flynn, P.J., Bowyer, K.W., Schott, C.L., Sharpe, M., 2010. FRVT 2006 and ICE 2006 Large-Scale Experimental Results. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 32, 831-846.
- Puhan, N.B., Sudha, N., Suhas Hegde, A., 2011. A new iris liveness detection method against contact lens spoofing, IEEE 15th Int. Symposium on Consumer Electronics (ISCE), pp. 71-74.
- Rigas, I., Komogortsev, O.V., 2014. Gaze estimation as a framework for iris liveness detection, 2014 IEEE Int. Joint Conference on Biometrics (IJCB), pp. 1-8.
- Robinson, D.A., 1963. A Method of Measuring Eye Movement Using a Scieral Search Coil in a Magnetic Field. *IEEE Transactions on Bio-medical Electronics* 10, 137-145.
- Ruiz-Albacete, V., Tome-Gonzalez, P., Alonso-Fernandez, F., Galbally, J., Fierrez, J., Ortega-Garcia, J., 2008. Direct Attacks Using Fake Images in Iris Verification, in: Schouten, B., Juul, N.C., Drygajlo, A., Tistarelli, M. (Eds.), *Biometrics and Identity Management*. Springer-Verlag, pp. 181-190.
- Salvucci, D.D., Goldberg, J.H., 2000. Identifying fixations and saccades in eye-tracking protocols, 2000 Symposium on Eye Tracking Research & Applications (ETRA). ACM, pp. 71-78.
- Sequeira, A.F., Oliveira, H.P., Monteiro, J.C., Monteiro, J.P., Cardoso, J.S., 2014. MobILive 2014 - Mobile Iris Liveness Detection Competition, 2014 IEEE Int. Joint Conference on Biometrics (IJCB), pp. 1-6.
- Stampe, D.M., 1993. Heuristic filtering and reliable calibration methods for video-based pupil-tracking systems. *Behavior Research Methods, Instruments, & Computers* 25, 137-142.
- Sun, Z., Zhang, H., Tan, T., Wang, J., 2014. Iris Image Classification Based on Hierarchical Visual Codebook. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 36, 1120-1133.
- Sung Joo, L., Kang Ryoung, P., Jaihie, K., 2006. Robust Fake Iris Detection Based on Variation of the Reflectance Ratio Between the IRIS and the Sclera, 2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference, pp. 1-6.
- Tomeo-Reyes, I., Liu-Jimenez, J., Rubio-Polo, I., Redondo-Justo, J., Sanchez-Reillo, R., 2011. Input images in iris recognition systems: A case study, 2011 IEEE Int. Systems Conference (SysCon), pp. 501-505.
- Venugopalan, S., Savvides, M., 2011. How to Generate Spoofed Irises From an Iris Code Template. *IEEE Transactions on Information Forensics and Security* 6, 385-395.
- Xianchao, Q., Zhenan, S., Tieniu, T., 2007. Learning Appearance Primitives of Iris Images for Ethnic Classification, 2007 IEEE Int. Conference on Image Processing (ICIP 2007), pp. II - 405-II - 408.
- Xinyu, H., Changpeng, T., Qi-zhen, H., Tokuta, A., Ruigang, Y., 2013. An experimental study of pupil constriction for liveness detection, 2013 IEEE Workshop on Applications of Computer Vision (WACV), pp. 252-258.
- Yambay, D., Doyle, J.S., Bowyer, K.W., Czajka, A., Schuckers, S., 2014. LivDet-iris 2013 - Iris Liveness Detection Competition 2013, 2014 IEEE Int. Joint Conference on Biometrics (IJCB), pp. 1-8.
- Zhuoshi, W., Xianchao, Q., Zhenan, S., Tieniu, T., 2008. Counterfeit iris detection based on texture analysis, 19th Int. Conference on Pattern Recognition (ICPR 2008), pp. 1-4.