Database of Iris Printouts and its Application: Development of Liveness Detection Method for Iris Recognition

Adam Czajka[†,‡]
†Institute of Control and Computation Engineering
Warsaw University of Technology, ul. Nowowiejska 15/19, 00-665 Warsaw, Poland
‡Research and Academic Computer Network (NASK)
ul. Wawozowa 18, 02-796 Warsaw, Poland
Email: aczajka@elka.pw.edu.pl

***Abstract*— Liveness detection (often referred to as presentation attack detection) is the ability to detect artificial objects presented to a biometric device with an intention to subvert the recognition system. This paper presents the database of iris printout images with a controlled quality, and its fundamental application, namely development of liveness detection method for iris recognition. The database gathers images of only those printouts that were accepted by an example commercial camera, i.e. the iris template calculated for an artefact was matched to the corresponding iris reference of the living eye. This means that the quality of the employed imitations is not accidental and precisely controlled. The database consists of 729 printout images for 243 different eyes, and 1274 images of the authentic eyes, corresponding to imitations. It may thus serve as a good benchmark for at least two challenges: a) assessment of the liveness detection algorithms, and b) assessment of the eagerness of matching real and fake samples by iris recognition methods. To our best knowledge, the iris printout database of such properties is the first worldwide published as of today. In its second part, the paper presents an example application of this database, i.e. the development of liveness detection method based on iris image frequency analysis. We discuss how to select frequency windows and regions of interest to make the method sensitive to "alien frequencies" resulting from the printing process. The proposed method shows a very promising results, since it may be configured to achieve no false alarms when the rate of accepting the iris printouts is approximately 5% (i.e. 95% of presentation attack trials are correctly identified). This favorable compares to the results of commercial equipment used in the database development, as this device accepted all the printouts used. The method employs the same image as used in iris recognition process, hence no investments into the capture devices is required, and may be applied also to other carriers for printed iris patterns, e.g. contact lens.**

I. Introduction

Human iris is believed to present a lavish set of individual features, distinguishing even identical twins [1]. Iris recognition methodologies offer today a remarkable authentication accuracy and together with iris capture equipment constitute one of the best biometric systems protecting the most sensitive resources. Constant development of hardware platforms, as well as competition on the algorithms field, bring solutions ready to effectively recognize our irises on mobile devices, at the distance of a few meters or even when a subject moves. However, the implementation of a biometric method can be successful only when it processes *appropriate data*, i.e. those representing measurements of a living, human body or behavior. This is why liveness detection can be no longer separated from the biometric recognition process and becomes intrinsic capability of any biometric sensor, preventing the system from falsely accepting non-living or artificial objects.

The reliability of the liveness detection methods shall be assessed in a standardized manner, with the use of samples adequately simulating real spoofing attacks. We decided to build a reference database of iris printout images, with the intention to make it publicly available (starting from November 2013) as an element of the benchmarking environment related to liveness detection approaches. The quality of the prepared printouts is not accidental, as we photographed only these specimens which were not classified as a spoof by an example commercial system, and were matched to the biometric template calculated for an authentic, living eye (i.e. they were used in a typical, realistic and successful spoofing attacks). Usage of commercial equipment is definitely not for slandering a given product employed in tests, but solely for developing iris printouts of sufficient quality, corresponding to the quality of artefacts expected to be prepared by attackers. This database may thus serve as a good reference set of iris imitations in biometric security testing, and to our best knowledge this is the first such dataset with the printout quality verified by a commercial equipment.

Following this, we present a systematic approach to iris liveness detection methodology based on image frequency analysis, along with the evaluation results based on the collected database. Simple idea of detecting regularities within the image based on its amplitude spectrum was proposed early in the literature, yet this method still attracts engineers due to its simplicity, competing with more sophisticated approaches based on e.g. pupil dynamics or analysis of iris tissue characteristics. Frequency analysis for liveness detection may be regarded as an additional step of processing the same image as used for verification, and thus it does not call for

hardware investments. We achieved very encouraging results as the method may be configured to identify 95% of fake irises (note that all these printouts were accepted by an example commercial equipment), simultaneously introducing no false alarms.

II. Related work

Results published in the last decade revealed a lack of liveness detection mechanisms in iris commercial recognition systems, and the most important is the pioneering work by Thalheim *et al.* [2], presenting spoofing of example fingerprint, face and iris systems. On the one hand these experiments compromised selected devices (not necessarily regarding this as the main aim of the experiments). On the other hand the authors addressed an important issue of alarming lack of countermeasures, what today results in rich literature offering a range of iris anti-spoofing methods. In particular, identification of "alien frequencies" in iris images for detection of imitations was originally proposed by Daugman as early as in 1999 [1], and one of the first (known to us) methods of frequency-based liveness detection was described by Pacut *et al.*. This simple approach for attack detection still attracts developers, as it seriously limits the hardware investment costs when applied in the existing systems.

Increasing number of liveness detection methods results in a need of creating appropriate databases for method assessment. The only publicly available (known to us) database of printed irises was developed by Galbally *et al.* [3], collected in the framework of an earlier work by Ruiz-Albacete *et al.* [4]. The database consists of 800 images of iris printouts prepared for 100 different eyes (50 subjects), and the corresponding samples of authentic objects. However, the authors do not provide an information how the spoofing strength of printouts was assessed, in particular whether the prepared imitations were used to spoof any black-box biometric system.

III. Database of iris printouts

A. Rules of printouts preparation

Earlier experiments by Pacut *et al.* [5] suggest an ordinary matt paper as an optimal carrier, and a laser printing as the best process to produce artificial irises that are then eagerly accepted by example commercial systems. In this database collection we thus follow these rules, along with a simple gimmick of making a hole instead of a pupil, as originally suggested by Thalheim *et al.* [2]. This trick fools iris cameras as they typically search for a specular reflection from a cornea when detecting the iris.

Preparing the iris printout that imitates a given identity (i.e. allowing to impersonate a given subject) requires to put an actual iris pattern on a carrier, possible to be captured in an infrared light. Hence, a level of precision and sophistication of the imitation cannot be accidental, yet the precise rules how to prepare good printouts are difficult to be formally defined. To find this borderline we decided to employ an example commercial camera, implementing one of the most popular iris recognition method (Panasonic ET-100 with PrivateID® software), and prepared printouts of adequate quality to fool this example device. Only printouts that were accepted by this system (i.e. the iris pattern read from artifacts matched the corresponding iris templates based on authentic, living eyes) were then photographed by a separate commercial iris capture camera (IrisGuard AD100), as the ET-100 has no convenient iris capture capability. Such an approach increases the value of the database, as the accuracy of liveness detection methods developed with such images may better reflect the reliability expected in real attack scenarios.

B. Equipment used to prepare the printouts

1) Cameras: **a) Panasonic ET-100.** Commercial USB single-eye camera, implementing Daugman's methodology of iris coding, supplied with Iridian PrivateID®software, purchased by us in 2003 (currently out of production). Images are captured in near infrared light in non-standard resolution of 331×331 pixels, and of marginal quality according to ISO/IEC 29794-6 [6]. This camera was used to judge about the quality of each printout, i.e. the printout was added to the database when it was accepted by the camera (matched with a corresponding living eye template). **b) IrisGuard AD100.** Commercial two-eye camera with active zoom and focus adjustment and convenient iris capture SDK[1]. This device realizes a typical iris capture process in near infrared light. The iris size and central position within a frame are controlled to compensate for an eye placement and distance relative to the camera. The camera generates iris images in standard VGA resolution (640×480 pixels), and the image quality meets the ISO/IEC 29794-6 requirements. This camera was used to capture living eye images as well as images of the accepted printouts (for this purpose the liveness checks implemented by this camera were deactivated).

2) Printers: **a) HP LaserJet 1320.** Standard black and white laser printer. The device drivers allowed us to print the iris images of 600 dpi resolution. This printer was intentionally selected as an example of a low-cost and very popular printing device. **b) Lexmark c534dn.** Semi-professional color as well as black and white laser printer allowing to produce printouts of 1200 dpi resolution. This printer was intensionally used to make printouts of a higher resolution sufficient in spoofing.

C. Database collection

The data was collected for 237 volunteers from 2009 to 2012. We collected images for 426 distinct, authentic eyes (as not for every volunteer the images for both eyes were captured), ending up with 1274 images of living eyes, further referred to as *REAL subset*. Based on all authentic images we prepared the printouts and checked their fraudulent power in a commercial ET-100 camera. The verification was successful for images of 243 distinct eyes (i.e. approximately 57% of all classes) and all the accepted printouts were then photographed by the AD100 camera. That is, 243 distinct eyes

[1]Software Development Kit – the set of programming libraries convenient for programmers willing to develop own applications

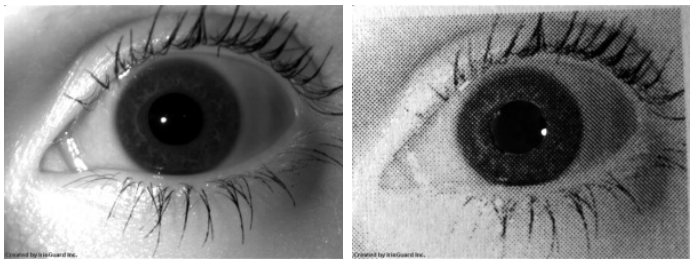

Fig. 1. Image of living eye (left) and the corresponding printout (right) of FAKE1 variant (i.e. prepared with HP LaserJet 1320 printer on a typical matt paper).

Fig. 2. Same as in Fig. 1, except the example of FAKE2 variant is shown on the right.

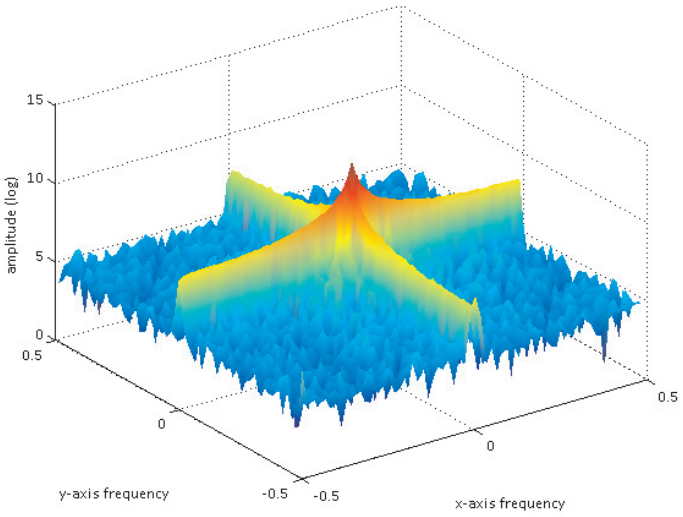

Fig. 3. Amplitude spectrum of the living iris image shown in Fig. 1 on the left. We may see a DC component, and a typical "cross" due to treating the image as periodical function (non-continuity of image borders) when calculating the spectrum. The remaining part of the spectrum is smooth, proving that there is no dominating frequency, i.e. no regular pattern exists within the image.

are represented by both the living and fake images (accepted by the commercial system) in the database. The total number of printout images is 729, and this constitutes the *FAKE subset* of the database.

D. Variants of the FAKE subset

The FAKE subset consists of two variants related to two different printers used: FAKE1 gathering "low resolution" printouts prepared with the HP LaserJet 1320, and FAKE2 collected with "high resolution" printouts, prepared with the Lexmark c534dn. Table I summarizes the number of samples for both variants. Pairs of authentic/fake samples of the example eyes are presented in Figs. 1 and 2.

TABLE I

NUMBER OF CLASSES (DIFFERENT EYES) THAT ARE REPRESENTED BY REAL AND FAKE SAMPLES (SIMULTANEOUSLY) IN THE DATABASES, ALONG WITH THE MINIMUM, MAXIMUM (PER CLASS) AND TOTAL (PER DATABASE VARIANT) NUMBERS OF PRINTOUT IMAGES.

Database variant	**Printout**	**Classes** (different eyes)	**Printout images** min, max (per class)	total
FAKE1	HP LJ 1320	92	1, 7	314
FAKE2	Lexmark c534dn	151	1, 7	415
Total		243		729

E. Metadata associated with images

All images of authentic and fake eyes are associated with the iris segmentation results. Following ISO recommendations [6] we approximate the iris by a circle, and for simplicity a circle modeling is done for pupil. That is, each image comes with six segmentation parameters. Due to unpredictability of segmentation algorithms when applied to non-living objects, the localization results were checked and corrected by an expert, what finally provides an accurate segmentation "ground truth". The latter feature allows for assessing how the available (and correct) segmentation may influence the method strength.

IV. Frequency analysis for printouts detection

A. Backgrounds of the method

The idea behind this liveness detection method lies in a fact that living, authentic irises do not reveal any regular pattern. This in particular results in a smooth frequency spectrum obtained by Fourier transform of an iris image, as shown in Fig. 3. In turn, a typical printing process introduces regularities within the image that disturb an original frequency spectrum, Fig. 4, producing characteristic peaks that correspond to the spatial frequencies of the artificial pattern. When these artefacts are identified within the frequency spectrum, a spoof is detected.

To speed up the calculation we decided to use Fast Fourier Transform (FFT) and analyze the frequency amplitudes only. To finally materialize this idea into an efficient and automatic method, we need to decide how to analyze the frequency information, and which areas of iris images should be engaged. Hence, in the following subsections we discuss:

- shape of the analysis windows (cf. subsection IV-B),
- number of analysis windows, their relations, and assessment of the amount of "alien frequencies" (cf. subsection IV-C),
- regions of interest within the analyzed images (cf. subsection IV-D).

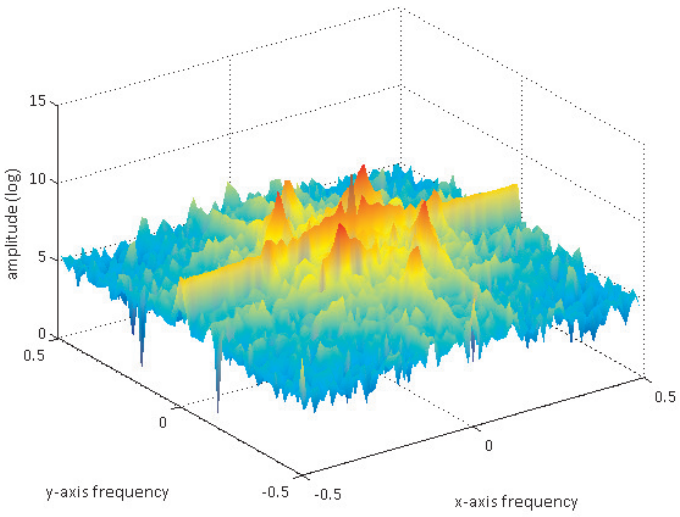

Fig. 4. Same as in Fig. 3, except that the amplitude spectrum for fake iris (shown in Fig. 1 on the right) is presented. Besides the DC component, we may clearly identify strong peaks related to "alien frequencies" being a result of a regular pattern in printed iris.

B. Relation between image and frequency spectrum rotation

Liveness detection method should be agnostic to the image properties resulting from printing process. In particular, the slope of the pattern (referenced to the image border) cannot be predicted due to unknown printer configuration. An attacker can also present the printout at different angles relative to the camera. That is, the proposed method should have a circular symmetry in the spatial domain to compensate for an image rotation.

As we use the FFT to analyze the image frequency, let's check how the image rotation influences the amplitude spectrum. Let $I(\mathbf{x}) : \mathbb{R}^2 \mapsto \mathbb{R}$, where $\mathbf{x} = [x_1, x_2]^T$ represents the image, $I'(\mathbf{x}) = f(\mathbf{R}^{-1}\mathbf{x})$ is a rotated version of image I, and $\mathbf{R}$ is the rotation matrix. Two dimensional Fourier Transform $\mathcal{I}'$ of the rotated image I' can be simply written as

$$\mathcal{I}'(u_1, u_2) = \int\int_{-\infty}^{\infty} I'(x_1, x_2) e^{-2\pi i(u_1 x_1 + u_2 x_2)} dx_1 dx_2$$

or, using vector notation

$$\mathcal{I}'(\mathbf{u}) = \int_{-\infty}^{\infty} I'(\mathbf{x}) e^{-2\pi i \mathbf{u}^T \mathbf{x}} d\mathbf{x}, \quad \text{where } \mathbf{u} = [u_1, u_2]^T$$

Replacing $I'(\mathbf{x})$ with $I(\mathbf{R}^{-1}\mathbf{x})$, letting $\mathbf{u} \to \mathbf{R}\mathbf{u}$ and using the property of rotation matrix, namely $\mathbf{R}^T = \mathbf{R}^{-1}$, yield:

$$\mathcal{I}'(\mathbf{R}\mathbf{u}) = \int_{-\infty}^{\infty} I(\mathbf{R}^{-1}\mathbf{x}) e^{-2\pi i (\mathbf{R}\mathbf{u})^T \mathbf{x}} d\mathbf{x} =$$

$$= \int_{-\infty}^{\infty} I(\mathbf{R}^{-1}\mathbf{x}) e^{-2\pi i \mathbf{u}^T \mathbf{R}^T \mathbf{x}} d\mathbf{x} =$$

$$= \int_{-\infty}^{\infty} I(\underbrace{\mathbf{R}^{-1}\mathbf{x}}_{\mathbf{y}}) e^{-2\pi i \mathbf{u}^T \underbrace{\mathbf{R}^{-1}\mathbf{x}}_{\mathbf{y}}} d\mathbf{x} = \mathcal{I}(\mathbf{u})$$

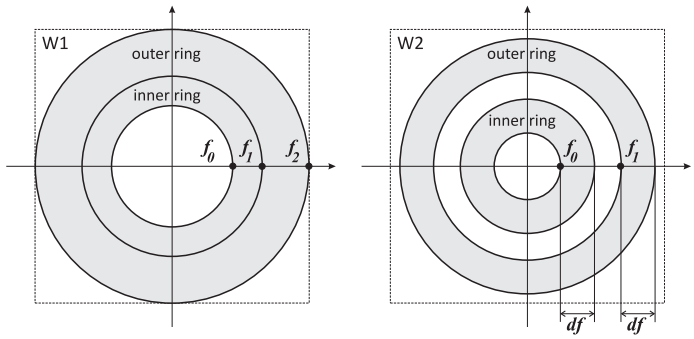

Fig. 5. Illustration of the frequency windows considered in this paper: W1) two windows fixed, and W2) one fixed and one moving window. Both methods have two degrees of freedom: f_0 and f_1 in W1 (as f_2 equals to maximum frequency in the image), f_0 and df in W2 (as f_1 is a variable assessed for every image separately).

Hence we finally obtain

$$\mathcal{I}'(\mathbf{R}\mathbf{u}) = \mathcal{I}(\mathbf{u}) \quad \text{or} \quad \mathcal{I}'(\mathbf{u}) = \mathcal{I}(\mathbf{R}^{-1}\mathbf{u})$$

what means that the rotation in image space results in identical rotation of the amplitude spectrum. This obvious property of Fourier transform significantly simplifies development of the method, as it is enough to take care about the method rotation invariance only in the frequency domain. We thus decided to analyze the amplitude spectra in circular-shaped frequency windows.

C. Frequency windows and the corresponding methods of calculating the liveness scores

To identify abnormalities in the amplitude spectrum, we set up two disjoint frequency windows. In the first window we expect to observe "alien frequencies", while the second window serves as a reference to the observed disturbances in the amplitude spectrum. There are certainly infinite number of possible, relative placements of these windows, thus we consider two scenarios (Fig. 5), and related with them methods of liveness score calculations.

a) Two fixed windows (W1): In this approach we use the collected database of real and fake images to estimate global (i.e. for all images) position of two, adjacent frequency windows, and use the following formula to calculate the liveness score q:

$$q_{W1} = \frac{h(f_1, f_2)}{h(f_0, f_1)} \tag{1}$$

where f_0, f_1 are parameters to be set experimentally, f_2 equals to the maximum frequency in the image (cf. Fig. 5), and h calculates maximum or average values within a given frequency window. Please note that we should maximize q_{W1} if "alien frequencies" are expected within the outer window, and we should minimize q_{W1} if we expect that the amplitude spectrum is disturbed within the inner window. Both these options are studied in this work.

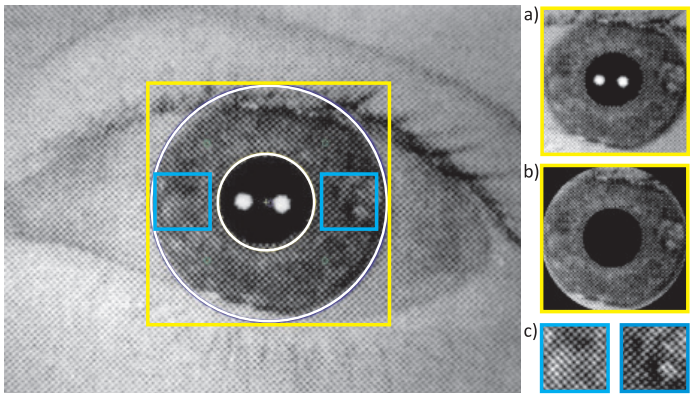

Fig. 6. Illustration of ROI variants considered in this paper: a) cropped iris, b) cropped and masked, and c) two segments found to be free from occlusions.

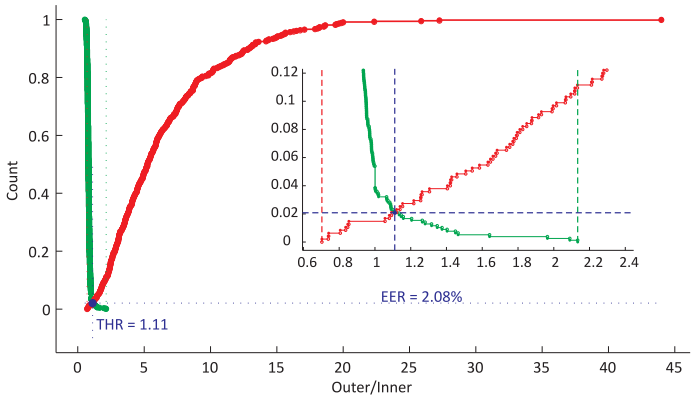

Fig. 7. Cumulative distributions of liveness score for imitations (right, in red color) and authentic samples (left, in green) for the winning variant guarantying the best EER. The winning solution is based on W1 window variant, CROPPED_AND_MASKED region of interest, h in (1) equivalent to the maximum function, and the assumption that "alien frequencies" are located in the outer window. The parameters $f_0 = 28$ and $f_1 = 33$.

b) One fixed and one moving window (W2): This approach is a slackened version of W1, as we allow the second window to move for every analyzed image, and the windows are not adjacent. Depending on the place where we expect to observe the "alien frequencies" (i.e. inner or outer window) we calculate the following liveness scores, respectively

$$q_{W2max} = \max_{f_1} \frac{h(f_1, f_1 + df)}{h(f_0, f_0 + df)} \tag{2}$$

$$q_{W2min} = \min_{f_1} \frac{h(f_1, f_1 + df)}{h(f_0, f_0 + df)} \tag{3}$$

where f_0, df are parameters, and h calculates maximum or average values within frequency window (as for q_{W1}). We investigate q_{W2max} and q_{W2min} indicators independently in this work.

D. Selection of region of interest

Calculating the liveness scores may be realized for the entire image, what does not require segmentation. This straightforward approach should deliver adequate discrepancy between authentic eyes and paper printouts, however may fail if printed contact lens are worn to spoof a system. In the latter case the amount of artificial pattern present within the image may insufficiently disturb the frequency spectrum, and the liveness scores may not exceed the required threshold.

We thus decided to employ the segmentation information (added to the database as a metadata, cf. Sec. III-E) and analyze only the area containing the iris tissue. This gives three possibilities of region of interest, Fig. 6:

- square crop of the iris (we call this variant CROPPED),
- square crop with simultaneous masking (zero-padding) of the areas outside the iris ring (we call this variant CROPPED_AND_MASKED),
- two square rectangular segments placed equidistantly to the iris center and in the middle of the pupil and iris boundaries (we call this variant TWO_SEGMENTS).

The aim of the second and the third variants is to process only the iris area, and omit any non-iris parts of the image (that may not reveal an artificial pattern in printout attacks). All three variants are evaluated in this work.

E. Results

Wrapping up all the above possibilities to adapt a frequency analysis for liveness detection, we have 24 variants to be investigated, i.e. 2 kind of windows (W1 and W2) $\times$ 2 possible locations of the "alien frequencies" (inner or outer window) $\times$ 2 variants of h in (1), (2) and (3) (maximum or average) $\times$ 3 regions of interest (CROPPED, CROPPED_AND_MASKED and TWO_SEGMENTS). Instead of selecting one winning solution, or to present the outcomes for all combinations, we present the optimal configuration and results for three, the most interesting scenarios described below.

a) The lowest Equal Error Rate (EER)[2]. This scenario simply looks for a method with the lowest numbers of false acceptances of fakes and false rejections of real samples. In this variant we obtained a very encouraging EER=2.08%, Fig. 7, what means that only two fake samples (out of 100) are falsely accepted as authentic eyes, and only two real samples (out of 100) are mistakenly rejected as fakes.

b) The lowest rate of living eyes rejection (i.e. false rejection rate – FRR) with no fake sample accepted. The second scenario corresponds with the highest system security requirements (as we do not accept any printout). Unfortunately, this demand yields 70% of authentic sample rejections for a winning variant (Fig. 8), what suggests that frequency analysis may offer a limited accuracy when is configured to meet such a high security demand.

c) The lowest rate of imitation acceptance (i.e. false acceptance rate – FAR) with no rejections of authentic eyes. The last scenario is probably the most important one, as it is focused on system usability. In this scenario we do not

[2]EER is the value of error at such an operating point of Receiver Operating Curve that yields equal values of false matches and false non-matches when testing a biometric system.

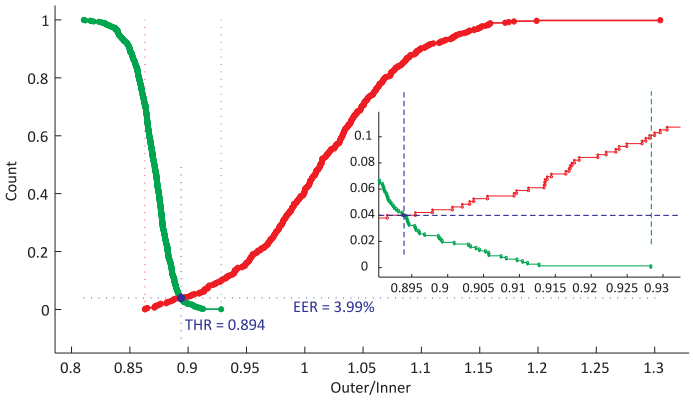

Fig. 8. Same as in Fig. 7, except that the solution optimal for the lowest FRR (at zero FAR) is shown. The best, yet discouraging result (FRR=70.7%) was obtained for W1 window variant, CROPPED region of interest, h in (1) equivalent to the maximum function, and the assumption that "alien frequencies" are located in the outer window. The parameters $f_0 = 10$ and $f_1 = 38$.

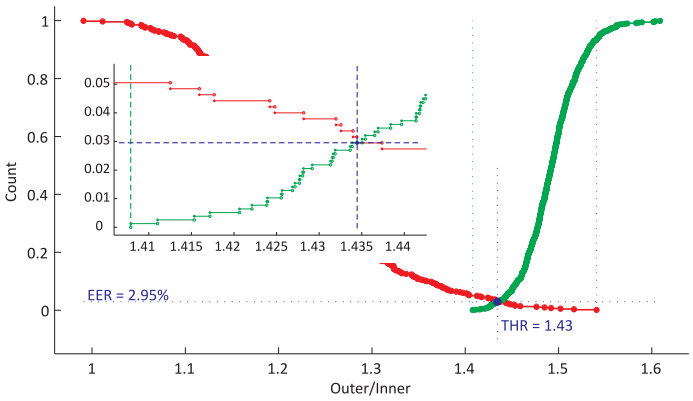

Fig. 9. Same as in Fig. 7, except that the solution optimal for the lowest FAR (at zero FRR) is shown. The best result (FAR=5%) was obtained for W1 window variant, CROPPED_AND_MASKED region of interest, h in (1) equivalent to the maximum function, and the assumption that "alien frequencies" are located in the inner window. The parameters $f_0 = 4$ and $f_1 = 52$.

introduce additional errors (related to liveness detection) to the iris recognition process, and find out how many fake samples are still (falsely) accepted. The winning approach accepts only 5% of imitations (with no authentic eyes rejection, Fig. 9), what very favorable compares to the example commercial system used in this work (remind that this camera accepted all the photographed printouts). In other words, we are able to detect 95% of quality controlled printouts, simultaneously not interfering with the existing iris recognition processes.

V. Conclusions

The paper proposes a database of iris printout images, and presents an example database deployment. The fake samples in the dataset were created with a special care to simulate real presentation attacks, and for this purpose each specimen was verified by a commercial system. This makes this database – to our best knowledge – unique worldwide.

We also present a complete procedure of an example liveness detection method development with the use of the collected database. The liveness detection rate obtained with this straightforward and low cost method may be used twofold. Firstly, observing decent accuracy (detection of 95% of printouts at zero false rejections of authentic samples) one may consider this method as an element of liveness detection system. Secondly, this may serve as an additional covariate when developing an iris image quality assessment methodology.

We believe that availability of the described database will allow for benchmarking of iris liveness detection methods, and the results presented in this paper will have an impact on faster development of countermeasures, still sluggishly implemented in the iris capture cameras.

Acknowledgment

This work was partially funded by The National Centre for Research and Development in Poland (NCBiR), grant No. OR0B002701: "Biometrics and PKI techniques for modern identity documents and protection of information systems – BIOPKI".

References

[1] J. Daugman, "Countermeasures against subterfuge," in *Biometrics: Personal Identication in Networked Society*, Jain, Bolle, and Pankanti, Eds. Amsterdam: Kluwer, 1999, pp. 103–121.

[2] L. Thalheim, J. Krissler, and P.-M. Ziegler. (2002, November) Biometric access protection devices and their programs put to the test. [Online]. Available: http://www.heise.de/ct/english/02/11/114/ (c't Magazine 11/2002)

[3] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in *Biometrics (ICB), 2012 5th IAPR International Conference on*, 2012, pp. 271–276.

[4] V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Direct attacks using fake images in iris verification," in *in: Proc. COST 2101 Workshop on Biometrics and Identity Management, BioID*, 2008.

[5] A. Pacut and A. Czajka, "Aliveness detection for iris biometrics," in *40th Annual IEEE International Carnahan Conference on Security Technology*, 2006, pp. 122–129.

[6] ISO/IEC 2nd CD 29794-6:201x, "Information technology – Biometric sample quality – Part 6: Iris image," 2011.