Encyclopedia of Biometrics
DOI 10.1007/978-3-642-27733-7_9050-2

Anti-spoofing: Iris Databases

Javier Galbally[a*] and A. Bori Toth[b†]
[a]Joint Research Centre, European Commission, Ispra, Italy
[b]Cyberisk Limited, London, UK

Synonyms

Liveness detection; Presentation attack detection; Spoofing countermeasures; Spoof detection; Spoof resistance; Vitality tests

Definition

Anti-spoofing may be defined as the pattern recognition problem of automatically differentiating between real and fake biometric samples produced with a synthetically manufactured artifact (e.g., iris photograph or plastic eye). As with any other machine learning problem, the availability of data is a critical factor in order to successfully address this challenging task. Furthermore, such data should be public, so that the performance of different protection methods may be compared in a fully fair manner. This entry describes general concepts regarding spoofing dataset acquisition and particularizes them to the field of iris recognition. It also gives a summary of the most important features of the public iris spoofing databases currently available.

Introduction

One of the key challenges faced by the rapidly evolving biometric industry is the need for publicly available standard datasets that permit the objective and reproducible evaluation of biometric recognition systems (e.g., performance, security, interoperability, or privacy). This is particularly relevant for the assessment of spoofing attacks and their corresponding anti-spoofing protection methodologies.

In relation to spoofing, the biometric community has started only recently to devote some important efforts to the acquisition of large and statistically meaningful anti-spoofing databases. In most cases, these datasets have been generated in the framework of international evaluation competitions such as the recent Iris Liveness Detection Competition first held in 2013, the series of Fingerprint Liveness Detection Competitions, LivDet, held biannually since 2009, or the 2D Face Anti-Spoofing contests that started in 2011. Such initiatives provide public and common benchmarks for developers and researchers to objectively evaluate their proposed anti-spoofing solutions and compare them in a fair manner to other existing or future approaches. This way, the public availability of standardized datasets is fundamental for the evolution of state-of-the-art solutions.

[*]E-mail: javier.galbally@jrc.ec.europa.eu

[†]E-mail: aboritoth@gmail.com

DOI 10.1007/978-3-642-27733-7_9050-2

In spite of the increasing interest in the study of vulnerabilities to direct attacks, the availability of such spoofing databases is still scarce. This may be explained from both a technical and a legal point of view:

- From a technical perspective, the acquisition of spoofing-related data presents an added challenge to the usual difficulties encountered in the acquisition of standard biometric databases (i.e., time-consuming, expensive, human resources needed, cooperation from the donors, etc.): the generation of a large amount of fake artifacts which are in many cases tedious and slow to generate on large scale (e.g., printed iris lenses).
- The legal issues related to data protection are controversial and make the sharing and distribution of biometric databases among different research groups or industries very tedious and difficult. These legal restrictions have forced most laboratories working in the field of spoofing to acquire their own proprietary (and usually small) datasets on which to evaluate their protection methods. Although these are valuable efforts, they have a limited impact, since the results may not be compared or reproduced by other researchers.

Both public and proprietary datasets acquired for iris anti-spoofing evaluation have been constructed following one of these three approaches:

- **Different real/fake users**. The spoofing database is constructed using the real samples of a previously existing dataset. Then, fake samples of different new users are added. Anti-spoofing is a two-class classification problem; therefore, from a theoretic point of view, such an approach is valid for the evaluation of liveness detection techniques, as the database contains samples of both classes. However, this type of database is not advisable and should be avoided, as it presents two major problems: on the one hand, it has the fundamental limitation of not allowing vulnerability studies of spoofing attacks where the intruder tries to access the system using a fake biometric trait of a genuine user (as real and fake samples do not coincide) and, on the other hand, real and fake samples do not only correspond to different persons but may also have been acquired with a different sensor, at a different location, or following a different protocol, which could potentially lead to biased results. Examples of works using such databases are commonly found in iris spoofing-related literature [1, 12, 13].
- **Same real/fake users, but different acquisition conditions**. As in the previous case, the spoofing database is constructed based on the real samples of a previous standard dataset. However, in this case, those real samples are the ones used to produce the fake spoofs; consequently, both real and fake users coincide. This could be, for instance, the case of an iris spoofing database where the artifacts used to carry out the fraudulent access attempts are printed photographs of an already publicly available iris image database. Again, the problem in this case is that the results of an anti-spoofing evaluation may be biased due to changes in the acquisition environment (e.g., sensor, illumination, distance to the sensor, pose, size, resolution, etc.). In such conditions, the liveness detection algorithm may be detecting those contextual variations and not the intrinsic differences between real and fake samples. Examples of works using such databases in the iris domain include [2, 14].
- **Same real/fake users and same acquisition conditions**. This is the most advisable way to proceed in an anti-spoofing evaluation. In this case, the database is generated from scratch for the same real and fake users, under the same acquisition environment. All competitive anti-spoofing evaluation campaigns follow this approach.

This entry gives an overview of the current publicly available anti-spoofing databases that may be used for the development and evaluation of new protection measures against direct attacks in the field of iris recognition.

Before reviewing the most widely used fake iris databases which are publicly available, a brief summary of the most common spoofing techniques is presented. An overview on spoofing is provided to support the rationale behind the design of the datasets described later.

For a more comprehensive and detailed reading on iris spoofing and related countermeasures, please see the encyclopedia entry: "Anti-spoofing: Iris."

Iris Spoofing

While iris recognition is one of the most accurate biometric technologies, it is also a younger research field compared to, for instance, fingerprint or face. As a consequence, iris spoofing has also a somewhat shorter tradition than that of other long-studied modalities. Almost all iris spoofing attacks reported in the literature follow one of three trends:

- **Photo attacks**. From a chronological point of view, these were the first attacks to be reported in the literature and they still remain popular, probably due to their great simplicity and, in many cases, high success rate [8, 9]. They are carried out presenting a photograph of the genuine iris. In the vast majority of cases, this image is printed on paper (i.e., print attacks), although it could also be displayed on the screen of a digital device such as a mobile phone or a tablet (i.e., digital photo attacks). A slightly more evolved version of the basic print attacks, which has also been considered in specialized works, consists of cutting out the pupil from the printout and placing it in front of the attacker's real eye. This way, countermeasures based on features extracted from this part of the eye lose much of their efficiency [10].

  A more sophisticated variation of photo attacks is *video attacks*, which consist of the presentation of an eye video (or even a face video) replayed on a multimedia device such as a smartphone or a laptop. Although this type of attacks has been mentioned in different iris-related works [6, 14], up to date no practical vulnerability evaluation against video attacks has been publicly reported in the iris domain.
- **Contact-lens attacks**. These appeared as a further evolution of the classic photo attacks. In this case, the pattern of a genuine iris is printed on a contact lens that the attacker wears during the fraudulent access attempt [11]. Such attacks are very difficult to be recognized even by human operators and represent a real challenge for automatic protection methods as all the contextual and ancillary information of the iris corresponds to that of a living eye. In most cases, the impact analysis of this vulnerability has been carried out in the context of wider studies working on the development of appropriate anti-spoofing approaches for these artifacts [6, 12–14].
- **Artificial-eye attacks**. These are far less common than the previous two types and have just started to be systematically studied [3, 14]. Although some works may be found where very sophisticated spoofing artifacts are presented, such as the use of multilayered 3D artificial irises [7], in most cases, these attacks are carried out with artificial eyes made of plastic or glass. Anti-spoofing methods based on the analysis of depth properties of the eye are more prone to be deceived by such 3D reproductions.

DOI 10.1007/978-3-642-27733-7_9050-2

Iris Spoofing Databases

Compared to other modalities such as fingerprint or face, iris is still a step behind in terms of the organization of competitive liveness detection evaluations and also regarding the public availability of spoofing data. In this context of limited resources, several studies carried out in the field of iris security against direct attacks have been performed using samples from previously acquired real datasets, so that in some cases real and fake users do not coincide [1, 12, 13].

In fact, until 2013, only one public iris spoofing database, the ATVS-FIr DB, was available [9]. In addition, its practical use was limited as it only related to one type of attack (i.e., print attacks without cutting out the pupil) acquired with one sensor. The organization of the first Liveness Detection-Iris Competition of 2013 (LivDet-Iris 2013) that considered the submission of algorithms and systems [4] has notably improved iris data availability. The database used in the contest comprises three different subsets of print and contact-lens attacks and it is significantly larger than its predecessor.

ATVS-FIr DB

The ATVS-FIr DB [9] is publicly available at the ATVS-Biometric Recognition Group website (http://atvs.ii.uam.es/).

The database comprises real and fake iris images (printed on paper) of 50 users randomly selected from the BioSec baseline corpus. It follows the same structure as the original BioSec dataset; therefore, it comprises 50 users × 2 eyes × 4 images × 2 sessions = 800 fake iris images and its corresponding original samples. The acquisition of both real and fake samples was carried out using the LG IrisAccess EOU3000 sensor with infrared illumination which captures bmp grayscale images of 640 × 480 pixels.

The fake samples were acquired following a three-step process which is further detailed in [9]: (i) first, original images were processed to improve the final quality of the fake irises, (ii) then they were printed using a high-quality commercial printer, and lastly (iii) the printed images were handheld when presented to the iris sensor.

Although the database does not have an official protocol, in the experiments described in [5], the database was divided into a training set, comprising 400 real images and their corresponding fake samples of the first 50 eyes, and a test set with the remaining 400 real and fake samples captured from the other 50 eyes available in the dataset.

LivDet-Iris DB

The first Liveness Detection-Iris Competition (LivDet-Iris) was held in 2013 [4]. The LivDet-Iris 2013 DB used in the evaluation will be distributed from the competition website (http://people.clarkson.edu/projects/biosal/iris/index.php) once the official results are publicly released.

The database comprises over 4,000 samples acquired from around 500 different irises and is divided into three datasets captured at three different universities: University of Notre Dame, University of Warsaw, and Clarkson University. Each dataset was captured with a different sensor:

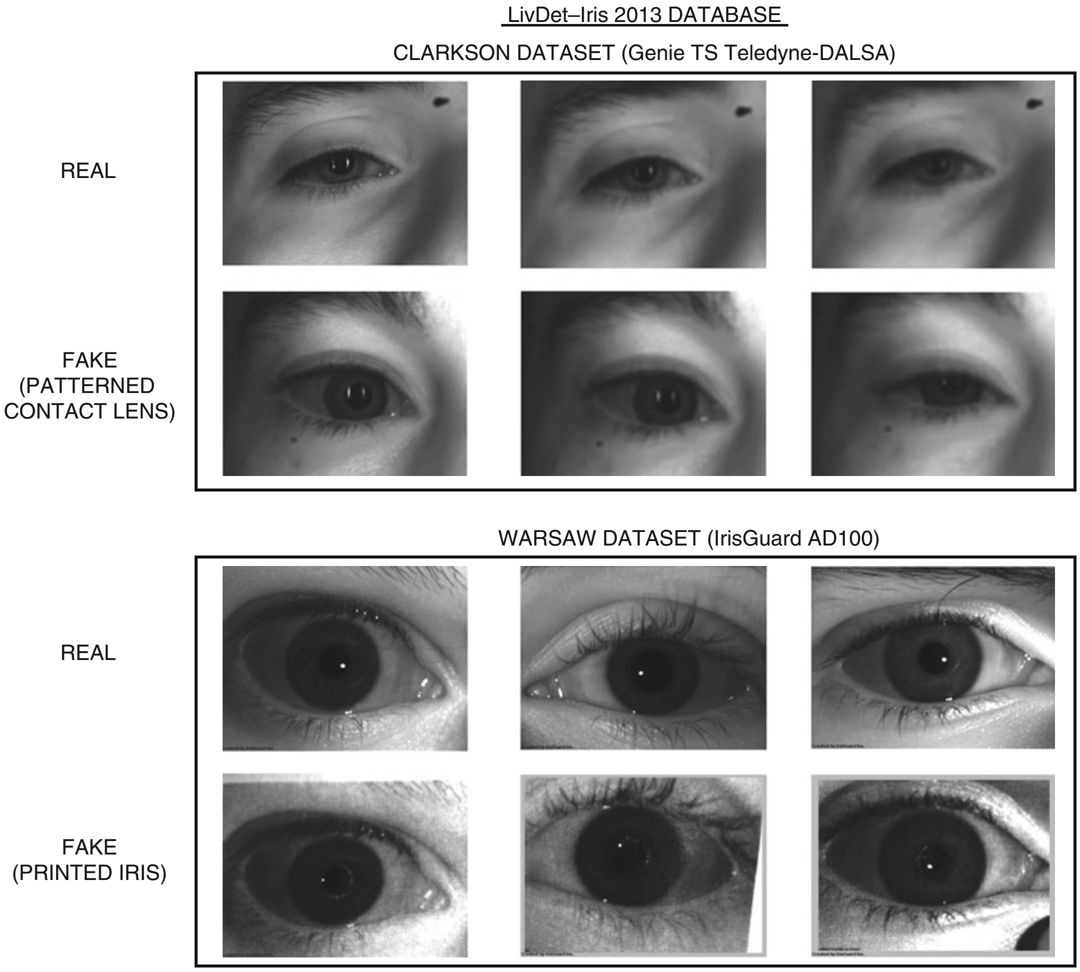
LivDet–Iris 2013 DATABASE
CLARKSON DATASET (Genie TS Teledyne-DALSA)
REAL
FAKE (PATTERNED CONTACT LENS)
WARSAW DATASET (IrisGuard AD100)
REAL
FAKE (PRINTED IRIS)

Fig. 1 Typical real iris images and fake samples from print and contact-lens attacks that may be found in the LivDet-Iris DB

- IrisAccess LG4000 for the University of Notre Dame dataset.
- EyeGuard AD100 for the University of Warsaw dataset.
- Genie TS from Teledyne DALSA for the Clarkson University dataset. This is the only sensor that captures video; however, in the dataset, only individual frames are included.

Two different types of spoof attacks are considered in the database: (i) print attacks, corresponding to the University of Warsaw dataset, and (ii) contact-lens attacks, contained in the Clarkson University and the University of Notre Dame datasets. In addition, the Clarkson University dataset, captured with a video camera, contains video frames that range from perfectly focused images to samples with a ±10 % focus deviation resulting in a varying level of blur (see Fig. 1 for graphical examples).

The training and test sets that will be released are the same as the ones used in the LivDet-Iris 2013 competition so that future results achieved using it may be directly compared to those obtained by the participants in the contest.

Table 1 Comparison of the most relevant features of the ATVS-FIr and LivDet iris spoofing databases

	Comparative summary: public iris spoofing DBs							
	Overall (real/fake)			Sensor	Attack (types)		Attack (focus)	
	# IDs	# Samples	Type	# Sens.	Ph	C-L	Reg.	Out
ATVS-FIr	100/100	800/800	Images	1	✓		✓	
LivDet	342/216	1,726/2,600	Images	3	✓	✓	✓	✓

# indicates number, *Ph* stands for photo, *C-L* stands for contact lens, *Reg* for regular focus, and *Out* for out of focus

Table 1 presents a comparison of the most important features of the two iris spoofing public databases currently available: ATVS-FIr DB and LivDet-Iris DB (described above). Examples of real and fake images that may be found in iris spoofing databases are shown in Fig. 1 (extracted from the LivDet-Iris DB).

Summary

The establishment of public evaluation benchmarks is fundamental for the development of efficient anti-spoofing countermeasures. The access to large databases permits a fair comparison between security protection methods and the evolution of state-of-the-art solutions. However, technical and legal difficulties associated with the collection of such data have slowed the development, and only two iris spoofing databases are publicly available today.

Although the organization of the 2013 LivDet-Iris competition was a significant step forward regarding the public availability of iris spoofing data, further efforts are still necessary before iris technology reaches the same level as other biometric modalities. In particular, the LivDet-Iris DB can still be complemented with data from additional subjects and/or collected under different conditions in order to increase its variability. In addition, a new subset containing samples of artificial-eye attacks (e.g., carried out with fake eyeballs) is yet to be generated.

Related Entries

▸ Anti-spoofing: Face Databases
▸ Anti-spoofing: Fingerprint Databases
▸ Anti-spoofing: Iris

References

1. R. Bodade, S. Talbar, Dynamic iris localisation: a novel approach suitable for fake iris detection. Int. J. Comput. Inf. Syst. Ind. Manage. Appl. **2**, 163–173 (2010)
2. R. Bodade, S. Talbar, Fake iris detection: a holistic approach. Int. J. Comput. Appl. **19**, 1–7 (2011)
3. R. Chen, X. Lin, T. Ding, Liveness detection for iris recognition using multispectral images. Pattern Recognit. Lett. **33**, 1513–1519 (2012)

DOI 10.1007/978-3-642-27733-7_9050-2

4. Clarkson University, LivDet-Iris 2013: liveness detection-iris competition (2013), Available online: http://people.clarkson.edu/projects/biosal/iris/
5. J. Galbally, J. Ortiz-Lopez, J. Fierrez, J. Ortega-Garcia, Iris liveness detection based on quality related features, in *Proceedings of the International Conference on Biometrics (ICB)*, New Delhi, 2012, pp. 271–276
6. X. He, Y. Lu, P. Shi, A new fake iris detection method, in *Proceedings of the IAPR/IEEE International Conference on Biometrics (ICB)*, Alghero. LNCS, vol. 5558 (Springer, 2009), pp. 1132–1139
7. A. Lefohn, B. Budge, P. Shirley, R. Caruso, E. Reinhard, An ocularist's approach to human iris synthesis. IEEE Trans. Comput. Graphics Appl. **23**, 70–75 (2003)
8. T. Matsumoto, Artificial irises: importance of vulnerability analysis, in *Proceedings of the Asian Biometrics Workshop (AWB)*, vol. 45, 2004
9. V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, J. Ortega-Garcia, Direct attacks using fake images in iris verification, in *Proceedings of the COST 2101 Workshop on Biometrics and Identity Management (BioID)*, Roskilde. LNCS, vol. 5372 (Springer, 2008), pp. 181–190
10. L. Thalheim, J. Krissler, Body check: biometric access protection devices and their programs put to the test, *c't Magazine*, Nov 2002, pp. 114–121
11. U.C. von Seelen, Countermeasures against iris spoofing with contact lenses, in *Proceedings of the Biometrics Consortium Conference*, Arlington, Virginia, 2005
12. Z. Wei, X. Qiu, Z. Sun, T. Tan, Counterfeit iris detection based on texture analysis, in *Proceedings of the IEEE International Conference on Pattern Recognition (ICPR)*, Tampa, 2008
13. H. Zhang, Z. Sun, T. Tan, Contact lens detection based on weighted LBP, in *Proceedings of the IEEE International Conference on Pattern Recognition (ICPR)*, Istanbul, 2010, pp. 4279–4282
14. H. Zhang, Z. Sun, T. Tan, J. Wang, Learning hierarchical visual codebook for iris liveness detection, in *International Joint Conference on Biometrics*, Washington DC, 2011