Mobile Iris Challenge Evaluation (MICHE)-I, biometric iris dataset and protocols ☆

Maria De Marsico [a], Michele Nappi [b], Daniel Riccio [c,*], Harry Wechsler [d]

[a] *Sapienza, University of Rome, via Salaria 113, 00198, Rome, Italy*
[b] *University of Salerno, via Giovanni Paolo II, 84084, Fisciano (SA), Italy*
[c] *University of Naples Federico II, via Claudio 21, 80125, Napoli, Italy*
[d] *University George Mason University, Fairfax, VA 22030-4444, USA*

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Iris biometric
Iris challenge
Mobile devices

ABSTRACT

We introduce and describe here MICHE-I, a new iris biometric dataset captured under uncontrolled settings using mobile devices. The key features of the MICHE-I dataset are a wide and diverse population of subjects, the use of different mobile devices for iris acquisition, realistic simulation of the acquisition process (including noise), several data capture sessions separated in time, and image annotation using metadata. The aim of MICHE-I dataset is to make up the starting core of a wider dataset that we plan to collect, with the further aim to address interoperability, both in the sense of matching samples acquired with different devices and of assessing the robustness of algorithms to the use of devices with different characteristics. We discuss throughout the merits of MICHE-I with regard to biometric dimensions of interest including uncontrolled settings, demographics, interoperability, and real-world applications. We also consider the potential for MICHE-I to assist with developing continuous authentication aimed to counter adversarial spoofing and impersonation, when the bar for uncontrolled settings raises even higher for proper and effective defensive measures.

1. Introduction

Mobile biometric technologies are nowadays the new frontier for secure use of data and services. We introduce and describe here Mobile Iris Challenge Evaluation (MICHE)-I, a new iris biometric dataset captured under uncontrolled settings using mobile devices (http://biplab.unisa.it/MICHE/database/). Mobile devices include phones, tablets, and similar smart devices, with smart standing for increasing power and equipment for information management, support for new apps, functions and gadgets, and incipient context awareness and personalization of services, all supported by Internet and cloud computing. We discuss throughout the merits of MICHE-I vis-à-vis biometric dimensions of interest including uncontrolled settings, interoperability, and real-world applications. The iris biometrics is today complementary to face and fingerprint biometrics for subject authentication. The applications are many and include mass screening for security, retail space (for advertising and data mining) and travel (for personal re-authentication), social networks, and most recently (continuous) authentication for mobile devices.

Iris biometrics is an alternative approach to reliable visual recognition of persons when imaging can be done at distances of less than a meter. In these conditions, this trait can provide a very good accuracy even with large galleries. As a matter of fact, notwithstanding the small size, which calls for a good capture resolution "the iris has the great mathematical advantage that its pattern variability among different persons is enormous" [2]. In addition, its structure is stable over time, for instance if compared with face. In controlled conditions it is well visible and easy to localize, following eye localization. Being internal to the eye, the iris is well protected from the environment, so that it is not subject to the kind of possible problems found with, e.g., degraded fingerprints of hard workers. The iris lacks the inherent 3D structure of face, therefore the angle of illumination does not cause distortions caused by self-occlusion. Off-angle variations can be addressed by affine transformations, while the distortion due to natural pupil dilation (due to light or pathological conditions), can be addressed quite easily too. Daugman [3] proposes some important suggestions on how to enhance iris recognition: "More disciplined methods for detecting and faithfully modeling the iris inner and outer boundaries with active contours, leading to more flexible embedded coordinate systems; Fourier-based methods for solving problems in iris trigonometry and projective geometry, allowing off-axis gaze to be handled by detecting it and 'rotating' the eye into orthographic perspective; statistical inference methods for detecting and excluding eyelashes; and exploration of score normalizations,

☆ This paper has been recommended for acceptance by Hugo Proença.

* Corresponding author. Tel.: +39 089 96 33 45; fax: +39 089 96 33 03.
E-mail addresses: demarsico@di.uniroma1.it (M. De Marsico), mnappi@unisa.it (M. Nappi), daniel.riccio@unina.it, driccio@unisa.it (D. Riccio), wechsler@gmu.edu (H. Wechsler).

http://dx.doi.org/10.1016/j.patrec.2015.02.009

depending on the amount of iris data that is available in images and the required scale of database search."

Proenca and Alexandre [16] report that the iris is often accepted as one of the most accurate traits and has been successfully applied in such distinct domains as airport check-in or refugee control. However, for the sake of accuracy, they emphasize that current iris recognition systems require that subjects stand close (less than 2 m) to the imaging device and look for a period of about 3 s until the data is captured. Some iris biometric evaluations have been conducted using images that fit these constraints, e.g., the Iris Challenge Evaluation (ICE) (http://iris.nist.gov/ICE/, [13]). Proenca and Alexandre [16] have engaged in noisy iris challenge evaluation (NICE I) as they simulate less constrained imaging environments and evaluate how noise bears on iris segmentation (http://nice1.di.ubi.pt). The challenging iris dataset UBIRIS.v2 ([15]) contains data captured in the visible wavelength, at-a-distance (between 4 and 8 m) and on the move (http://nice2.di.ubi.pt/). The results reported confirm the major impact that the levels of iris pigmentation have in the recognition feasibility. Most recently Proenca and Alexandre [17] organized a special issue dedicated to recognition of visible wavelength (VW) iris images captured at-a-distance and on the move with less controlled protocols, including the results of NICE II contest. Note that the VW usually has much higher level of detail than the more traditionally used near infrared (NIR) but also has many more noisy artifacts.

In this paper we move to issues related to iris acquisition by mobile devices, where it is assumed that the subject that needs to be recognized holds the capturing device by herself/himself. The aim of MICHE-I is to provide a dataset suitable to assess the performance of biometric applications related to this context. As it often happens, there are two faces of the same medal. On one face, capturing accuracy may be enhanced due to the usually short distance (in practice, equal to the length of a human arm) and quite natural frontal pose. On the other face, the lower resolution, possible motion blur and illumination distortions, caused respectively by the kind of device and by the lack of control on user capture action, require more robust detection as well as encoding procedures. Given its structure, the aim of MICHE-I dataset is to make up the starting core of a wider dataset that we plan to collect thanks to the contribution of data from participants to MICHE special issues. This should better support unbiased assessment of cross-demographic robustness and interoperability of recognition procedures. As for the latter, collecting more datasets in a single collection should allow to create a benchmark for a thorough assessment of interoperability characteristics of recognition algorithms. In particular we consider both the ability to match samples of the same subject acquired with different devices, and in general the ability to handle samples acquired by devices with different characteristics without a significant performance degradation.

The outline for paper is as follows. Uncontrolled settings and streaming video including image quality are the topic for Section 2. Mobile challenges and opportunities are discussed in Section 3. Dataset bias, and data fusion and interoperability, are addressed in Section 4. The new iris dataset MICHE-I is the topic for Section 5. Authentication protocols, mobile authentication using face and iris, and biometric vulnerabilities are addressed in Sections 6–8, respectively. Section 9 discusses the interplay between mobile devices and biometrics including iris and their impact on overall security. Section 10 summarizes the paper and charts venues for future development.

2. Uncontrolled settings and streaming video

The goal for MICHE-I, the new iris dataset introduced here, is to move iris recognition out of the current comfort zone to one framed by mobile devices with their inherent challenges. In analogy to face recognition we call the new medium "in the wild" and have it involved with real-world problems. Instead of relying on a "single best frame approach," one must now confront uncontrolled settings, which are all encompassing and include aging, pose, illumination, and expression (A-PIE), denial and deception characteristic of incomplete and uncertain information, uncooperative users, and last but not least unconstrained data collection, scenarios, and sensors. In particular, our setting addresses the typical cases of most mobile applications when, though being undoubtedly cooperative due to the aim to be positively identified, the user is rather non-expert or technically naïve. In other words, she/he may have little or no technical background to appreciate the capture result and/or improve its quality. As a consequence, she/he cannot effectively cooperate for improving the acquisition, and differently from assisted settings, nobody can suggest how to do that.

Characteristic of the move toward uncontrolled settings, the constraints on position and motion can be relaxed using high-resolution cameras, video synchronized using strobed illumination, and specularity based image segmentation [11]. The resulting Iris on the Move (IOM) system enable capture of iris images of sufficient quality for iris recognition while the subject is moving at a normal walking pace through a minimally confining portal. Moving even further toward uncontrolled settings involves capturing the iris biometrics using mobile devices, which are most prevalent in use today, with MICHE-I characteristic of such an effort.

2.1. Image quality

Image quality affects all biometrics and one has to contend with it either implicitly or explicitly. In particular, iris biometrics captured from partially cooperating subjects when using mobile devices suffer from blur, occlusion due to eyelids, and specular reflection. As a result, iris recognition performance degrades significantly. Pillai et al. [14] have recently addressed sparse representation-based classification (SRC) and dictionary learning (DL) while quantifying image quality in terms of sparsity concentration index (SCI). They show that low SCI images (from the University of Notre Dame ND-IRIS-0405 (ND) data set) [1] suffer from a high amount of distortion and that SRC provides the best recognition performance compared to that of a nearest neighbor based recognition algorithm (NN) that uses the Gabor features and Libor Masek's iris identification source code [10]. One can further expand SRC to multi-modal biometrics, e.g., iris, face, and fingerprints, using shared ("joint") sparse representations. The new MICHE-I iris data set introduced here is characteristic of mostly poorly cooperative (due to technical naiveness) subjects whose iris biometrics is captured by mobile devices. As the iris image quality is as expected quite challenging, there is much interest and opportunity to assess the extent to which SRC as stand-alone or as joint and multimodal can still help with recognition.

A comprehensive survey and assessment of iris image quality [8] helps with coupling specific metrics on image quality metrics (QM), authentication challenges for iris biometrics, benchmarks, and comparative contests and evaluations. Image quality critically affects observed performance. Iris image quality is "jointly determined by multiple factors such as de-focus, occlusion, motion blur, off-angle, and deformation." The authors further propose specific quality metrics (QM) and suggest that data fusion driven by discriminative methods, e.g., likelihood ratio, can inform on overall quality and improve on recognition.

2.2. Mobile challenges and opportunities

There has been an increase of viruses, worms, and malicious hacker software targeted at mobile devices. BullGuard has identified 2500 different types of mobile malware in 2010.[1] One can only expect that

[1] http://www.bullguard.com/bullguard-security-center/mobile-security/mobile-threats/mobile-security-what-you-need-to-know.aspx

this number has significantly increased since. As a matter of fact, just a few months later, IBM X-Force named 2011 "The year of the security breach," and predicted that "exploits targeting vulnerabilities that affect mobile operating systems will more than double from 2010".[2] More than 90% smartphones and tablets in 2011, however, were still lacking any robust security protection. The trade-off that needs to be addressed in light of increased penetration and subscription is that between pervasive usability and security, with the latter concerned with validation of credentials, and storage and power consumption. What makes mobile devices most appealing is their versatility including wide acceptance, intuitive operation, and ease of use, portability, and flexibility? As mobile devices come now endowed with expanded suites of sensors, additional opportunities for mobile devices involve all encompassing biometrics that include appearance, behavior, and physiological and cognitive state. Such applications require, often for legal reasons, continuous authentication.

2.3. How to exploit video

The degree of control that would be required during the acquisition phase is among the factors that may discourage the user of a biometric system. In addition, iris recognition generally requires maximum control: in an ideal (for the recognition system) setting, the user should stay immobile looking straight at the camera, at a distance possibly hindering a visual check of the actual image quality. For this reason a single acquired iris image might be not sufficient for a reliable recognition. On the other hand, repeated requests for new captures providing samples of better quality may be very disturbing for the user. A possible solution would involve, a fast strategy for best template selection, completely transparent to the user and requiring video instead of still image capture, including the ability to select the best samples from the video frames. The QMs listed earlier and additional measures can be used for such purposes. Toward that end, the QM used by De Marsico et al. [5] for face sample selection exploit a measure of entropy computed on the frames of the video [4].

3. Dataset bias

We note here the comments made by Torralba and Efros [20] on an "unbiased look at dataset bias," in particular the realization that "one major issue for many popular dataset competitions is "creeping over fitting, as algorithms over time become too adapted to the dataset, essentially memorizing all its idiosyncrasies, and losing ability to generalize". A further related consideration raised is that computer vision datasets, including biometric ones, which are [merely] supposed to be a representation of the world, "instead of helping us to train models that work in the real open world, have become closed worlds unto themselves." Methods should not become over-engineered for nuances of a dataset, with modest performance gains indicative of overfitting. The merits for MICHE-I are thus twofold. It is traced to a new medium not experienced so far but gaining in use and popularity, that of mobile devices, and is challenging as it is characteristic of the open world in-the-wild and not yet affected by creeping over fitting. Additional dataset biases one has to contend with include lack of cross-dataset generalization, or even of sufficient interoperability (training with one dataset and testing with a different dataset), and negative set bias. While the former is already raising interest in the research community [6], the latter one is more tricky to consider. In practice, it relates to the consideration that the space of all possible negatives in a classification problem "is astronomically large", therefore datasets can only include a small sample. The question is if this negative sample can be considered as sufficient to represent the variety of negative cases. The initial goal for MICHE-I is not to beat the latest benchmark numbers on the latest dataset but getting started and learning the in and outs of iris biometrics captured in the wild by mobile devices.

4. Data fusion and interoperability

Uncertainty and biometric decision-making are closely intertwined and their joint resolution depends on context and goals. No single model exists for all pattern recognition problems and no single method is applicable for all problems. Rather what one has access to are a bag of tools and a bag of problems. Toward that end, biometric authentication is at its best when it takes place using sequential ("cascade") aggregation of different components. This corresponds to an ensemble method ("mixtures of experts") and/or cascading ("stack") networks, in general, and data fusion, in particular. Data fusion is relevant to both generic multi-level and multi-layer fusion in terms of functionality and granularity. Multi-level fusion involves feature/parts, score ("match"), and detection ("decision"), while multi-layer fusion involves modality, quality, and method (algorithm). Multi-layer data fusion is of particular interest, with face, iris, and fingerprints the multi-modal suite of upmost interest, and with MICHE-I most appropriate for assessing mobile device applications. Image quality (see Section 2.1), uncontrolled settings, interoperability, and data fusion are all related.

Interoperability is the thread that links biometrics and forensics with distributed data collection and associated federated identity management systems. Interoperability is most important as it informs on operational performance and validation, on one side, and trustworthiness to reduce vulnerabilities, on the other side. The standard explanation provided for great discrepancies between observed training and test performance is the lack of interoperability, e.g., access to appropriate database pairs for training and testing to counter major covariate shifts, in particular those traced to uncontrolled settings. There is thus much need that datasets reflect on real-word variation with respect to data capture in terms of both sensors and geometry. It is here that MICHE-I plays a major role in terms of new sensor modalities and real-world biometric variation. The trade-off between security and privacy mediated by interoperability ultimately bears on surveillance and personalization.

One representative example for combining modalities such as face and iris is the Quality in Face and Iris Research Ensemble (Q-FIRE) dataset (see [19]). It contains the face and iris videos for 195 subjects over two visits. The datasets were collected at a distance of 5–25 ft. under less than ideal conditions in terms of illumination, blur, gaze angle, occlusion, and motion.[3] The MICHE-I iris dataset provides a way to take into consideration the novel and challenging medium of mobile devices. Coupling MICHE-I and face biometrics can establish both new performance benchmarks and compare them against those derived using Q-FIRE. Yet another worthwhile comparison across biometric mediums and modalities traced to mobile devices would be to compare iris (MICHE-I) and face biometrics against MOBIO, which combines face and speech (see Section 7).

5. MICHE

We describe here the current state of the new iris dataset MICHE-I and the diverse demographics and uncontrolled settings that define and frame its acquisition. Some representative samples from MICHE and the challenges they pose for iris recognition are illustrated below (see Fig. 1). It is worth underlining that, given its structure, the aim of MICHE-I dataset is to make up the starting core of a wider dataset that we plan to collect thanks to the contribution of data from participants to MICHE-I and MICHE-II special issues. Having more

2 http://www-03.ibm.com/security/landscape.html

3 http://www.citer.wvu.edu/quality_faceirisresearchensembleclarkson

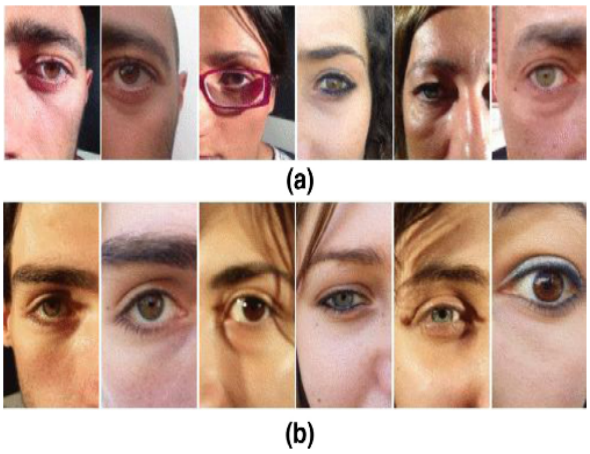

Fig. 1. Examples of images in MICHE: (a) captured from iPhone, (b) captured from Galaxy S4. In both rows odd positions correspond to indoor images and even positions to outdoor ones; the first two images belong to the same subject.

Fig. 2. Examples of images in MICHE captured from tablet: odd positions correspond to indoor images and even positions to outdoor ones; the first two images belong to the same subject.

sources of images from different countries and acquired in different settings should allow in the future to perform more extensive and less biased testing (in the sense of [20]) related to demographics and interoperability issues (different capture devices, different settings and different operating systems).

5.1. MICHE-I

Some popular datasets are provided to assess iris recognition. However, they differ from MICHE-I due to the kind of acquisition. One of the first group of datasets available dealing with iris images is CASIA Iris Image Database[4] (CASIA-Iris) that has been updated from CASIA-IrisV1 to CASIA-IrisV4 since 2002. Its images are collected under near infrared illumination or synthesized, therefore do not lend themselves to be used in investigations about mobile acquisition. The same holds for images used for ICE competitions.[5] UBIRIS datasets (see below) are captured in visible light and uncontrolled conditions, but with cameras with good resolution. As a consequence, they present a better resolution than average images acquired by mobile devices. MICHE-I is a dataset of iris images acquired in visible light by mobile devices. It was collected for the specific purpose of the Mobile Iris Challenge Evaluation (MICHE) competition (Part I). The aim of the competition is to assess the state of the art about iris recognition on mobile devices. The key features of the MICHE-I dataset (see below) are a wide and diverse population of users, the use of different mobile devices for the acquisition, realistic simulation of the acquisition process (including noise), several acquisition sessions separated in time, and image annotation using metadata. MICHE-I characteristics are thus consonant with the stated objective to further develop iris authentication for uncontrolled settings, interoperability, and real-world applications. Furthermore, we aim at providing a robust benchmark to assess interoperability of iris recognition algorithms. As a matter of fact, the way we have planned to collect more datasets from different sources (different devices, different operating systems, different countries) in a single bunch should allow creating such benchmark. In particular, we consider the ability of the algorithms to handle images captured by devices with different characteristics, without a significant decrease of recognition accuracy. This includes the possibility of reliably matching samples of the same person captured by different devices, and robustness to demographics (age, ethnicity, gender). The inspiring principle is the same underlying the creation of EGA [18], in order to avoid the dataset bias mentioned by Torralba and Efros.

The acquisition protocol used for MICHE-I aims to achieve a realistic simulation of the data capture process during user engagements in order to be identified by a mobile iris recognition system. Toward that end, the subjects involved in experiments were advised to behave similar to the way they would use a real system of this type; as an example, subjects wearing eyeglasses were allowed to remove or keep them according to what they would have done during a real engagement of such an application. The subjects were also asked to take self-images of their iris (by holding the mobile device by themselves), with a minimum of 4 shots for each device (or camera when using more than one per device) and acquisition mode (indoor, outdoor). During the indoor acquisition mode various sources of artificial light, sometimes combined with natural light sources, are used, while during the outdoor acquisition mode data capture takes place using natural light only. For each subject only one of the two irises was acquired.

Three kinds of devices were used for data acquisition purposes, with devices (smartphones and tablets) representative of the current top market category:

- iPhone5 (abbreviated IP5)
  - Operating System: Apple iOS;
  - Posterior Camera: *iSight* with 8 Megapixels (72 dpi);
  - Anterior Camera: *FaceTime HD Camera* with 1.2 Megapixels (72 dpi).
- Galaxy Samsung IV (abbreviated GS4)
  - Operating System: Google Android;
  - Posterior Camera: *CMOS* with 13 Megapixel (72 dpi);
  - Anterior Camera: *CMOS* with 2 Megapixel (72 dpi).
- Galaxy Tablet II (abbreviated GT2)
  - Operating System: Google Android;
  - Posterior Camera: N/A;
  - Anterior Camera: 0.3 Megapixels.

Fig. 1 shows examples of the images acquired by the two smartphones, while Fig. 2 shows examples of images captured by tablet. Notice that the three groups of images are at three different resolutions (1536×2048 for iPhone5, 2322×4128 for Galaxy S4, and 640×480 for the tablet).

It is possible to identify different sources ("factors") for noise in the MICHE-I dataset. This includes (a) reflexes: artificial light sources, natural light sources, people or objects in the scene during the acquisition; (b) focus; (c) blur: either due to an involuntary movement of the hand holding the device, or due to an involuntary movement of the head or of the eye during acquisition; (d) occlusions: eyelids, eyeglasses, eyelashes, hair, shadows; (e) device: artifacts due to the low resolution and/or to the specific noise of the device; (f) off-axis gaze; (g) variable illumination; and (h) different color dominants.

While these factors are also evident in UBIRIS.v2 (http://nice2.di.ubi.pt/), as shown in Fig. 3, we can observe the lack of precise localization and fixed distance in the capture (we can observe both well centered eyes and half faces), also resulting in variable sizes of the region useful for recognition. This is typical of mobile captures performed by the users, which are usually neither too close nor at arm-length. This introduces further difficulties, since eye localization must be performed in a pre-processing step, and

[4] http://biometrics.idealtest.org/
[5] http://www.nist.gov/itl/iad/ig/ice.cfm

Fig. 3. Example images from UBIRIS.v2.

Fig. 4. Images from MICHE Fake.

the resulting size of the iris region is smaller. On the other hand it provides further possibilities to possibly exploit a more extended periocular region. On the other hand, the recent CASIA-IrisV4 contains images collected under near infrared illumination, which is not the case with present mobile devices.[6]

MICHE-I dataset has been collected during several different data acquisition sessions separated in time. At present, only part of the original subjects have engaged in a second data acquisition session. The time elapsed between the first and second acquisition of a subject varies from a minimum of 2 months to a maximum of 9.

The metadata for the published dataset includes a reference XML file for each iris image, which contains metadata about the image itself, and the conditions under which the image was acquired. The XML file contains the following tags:

- *filename*: the name of the image to which the XML file refers; the name already contains a certain amount of information in order to quickly find the desired image;
- *img_type:* indicates the kind of image (in this case *iris*), but provision is made for face image as well;
- *iris*: indicates which iris was acquired (*right*, *left* or *both* when the image contains both irises);
- *distance_from_the_device*: distance of the user from the acquisition camera*;*
- *session_number*: the acquisition session when the image was captured*;*
- *image_number*: image ordinal number*;*
- *user*: identification number of the subject; moreover, for each subject further information is stored:
    - *age:* subject's age;
    - *gender:* subject's gender;
    - *ethnicity:* subject's ethnicity;
- *device*: contains all information about the capture device:
    - *type;*
    - *name;*
    - *camera (front* or *rear);*
        - *name;*
        - *resolution;*
        - *dpi;*
- *condition*: information about capture conditions:
    - *location;*
    - *illumination*;
- *author*: the XML file also contains the name of the laboratory/institution who made that acquisition.

The XML file structure allows a quick and reliable retrieval of any image as a function of any one of the above parameters.

Two further sets of images are included in MICHE-I.

- MICHE Fake

MICHE_fake.zip includes 80 photos of prints of iris images. For each person in a group of 20, 4 images were selected in indoor modality, 2 of which taken by Samsung Galaxy S4 – posterior camera, and the other two by a smartphone iPhone5 – posterior camera. These images were printed with a LaserJet printer and the prints were photographed by a Samsung Galaxy S4 – posterior camera. Fig. 4 shows some images in this subset.

- MICHE Video

MICHE_video.zip includes videos of irises of 10 persons, 4 of which are also present in the dataset of iris images. The 10 persons were acquired in two modalities, indoor and outdoor. Acquisition was performed by two devices: a smartphone Samsung Galaxy S4 and a tablet Samsung Galaxy Tab 2. Acquisitions by smartphone were performed by both anterior and posterior camera. Each video is about 15 s long. For each combination modality-device-camera, 2 videos were acquired. Therefore, the total is 120 videos.

5.2. Demographics

MICHE-I consists of 92 subjects, among them 66 male and 26 female, of age varying between 20 and 60 years, and all of Caucasian ethnicity. The second acquisition session has been attended by 22 persons so far. Currently MICHE-I consists of over 3732 images. The demographics are important in the following way. Similar to recent face recognition studies [7] one should leverage demographics ("cohort") as additional ancillary side ("helper") information for partitioning purposes leading to overall enhanced biometric authentication. It would be interesting to assess to what extent, if at all, the face recognition results carry over to the iris modality. In particular, the result of interest here is that face recognition performance was found to depend on the cohort used, with lower recognition accuracies observed on females, Blacks, and younger subjects (18–30 years old). Additional findings have shown that face recognition performance on race/ethnicity and age cohorts generally improves when training exclusively on the same cohort. The same authors finally suggest "the use of dynamic face matcher selection," where multiple biometric subsystems, trained on different demographic cohorts, are available for human operators to select from. The challenge that MICHE-I can answer for is the hypothesis that a dynamic iris matcher, driven by demographics (including gender and ethnicity but not age as iris is assumed to stay constant over the life span of the subject) can enhance ultimate iris authentication.

6. Authentication protocols

The biometric terminology used throughout this section is a standard one ([22]). Given a gallery with N subjects, the biometric tasks of interest are those of iris verification (1-1 matching) and identification (1-N matching). As for the latter we especially consider the open set and watch list modalities, when the probe subjects may not belong to the enrolled set, differently from closed set recognition where the top match is always accepted for the sought after identity. Assuming a hypothesis testing framework, we define the null hypothesis H0 that the unknown face belongs to a subject enrolled in the gallery, and the alternative hypothesis H1 that the face has never been enrolled before. When for a certain probe the null hypothesis H0 is rejected for each identity (class) enrolled, H1 is accepted and the answer for the

[6] http://biometrics.idealtest.org/dbDetailForUser.do?id=4

query is “unknown subject.” This corresponds to forensic exclusion with rejection.

The protocols associated with MICHE-I are iris specific and directly functional to cross-over, multi-level and multi-layer data and method fusion, and to interoperability. The MICHE protocols are specific of iris recognition and, in this sense, go beyond those used for the Iris Challenge Evaluation (ICE 2006) [13], which were the same used earlier in FERET for face recognition [12]. An extended and rich repertoire of performance indices is provided by multi-level and multi-layer performance evaluation. These include but are not limited to iris detection, iris segmentation and normalization, feature extraction for shape and texture characterization, iris authentication, and further extend to interoperability across sensors, OS, and device medium used for data capture, as well as dynamic determination of demographics (gender and ethnicity). MICHE-I composition is suitable to engage in the corresponding step-wise performance evaluation and to suggest ways and means to assembly/combine diverse methods into full-fledged iris biometric recognition systems for overall enhanced iris recognition performance. Recognition subtasks include learning the iris representation space, training for the purpose of encoding, and gallery enrollment including quality metrics (QM) assessment and signature generation. Furthermore, we can mention decision-making and smart identity management, e.g., de-duplication. Learning, training, and encoding can use the same/similar representation methods or not. The gallery can further consist of single or multiple images for each subject, or video clips (see MICHE Video). Different multi-set and video clip matching coupled to comprehensive metrics expand further on the performance indices made available earlier. Security, integrity, and privacy for biometric data are expected throughout despite vulnerabilities, deliberate or not, with MICHE Fake assisting in assessing this task.

We plan to devise additional performance indices that will bear on iris recognition performance and make our authentication protocols all-inclusive. Such indices would bear on (a) iris segmentation (pupil, eyelids, and eyelashes detection, location, and boxing) using for example Hough transform for circle detection and/or active contours (AC) and active shape models (ASM); (b) (linear and non-linear) normalization, registration, and unwrapping (including but not limited to Cartesian to polar coordinates mapping using pupil or limbus center); (c) feature extraction for shape and texture characterization; and (d) inpainting (reconstructing occluded, lost or deteriorated parts of images and video clips), e.g., iris occluded by eye lids and/or eye lashes and/or blurred by uneven illumination. For the time being we will continue using NICE I and NICE II performance indices,[7] which were found effective in assessing segmentation and classification of noisy irises.

7. Mobile biometric authentication

Modern smartphones can now store large amounts of sensitive data while providing access to significant amounts of personal data stored offline, e.g. on internet banking, e-mail and social networking sites. Though passwords provide some protection against unauthorized access to this data, an attractive alternative is to authenticate yourself using *biometrics* – physical characteristics, such as iris, that are unique to you but hard for you to lose [21]. One representative example for mobile biometric authentication is the Mobile Biometrics (MOBIO) project, which employs the camera and microphone on a mobile device to capture face and voice, and combine these two biometrics for secure yet rapid user verification to ensure that that someone who wants to access the data is entitled to do so (see Section 8.2). Marcel et al. [9] report on the 1st MOBIO face and speaker verification evaluation, with both modalities reporting similar levels of performance, respectively 10.9% and 10.6% of HTER.[8] The two modalities are complementary to each other and one can see “a clear gain in performance simply by fusing the individual face and speaker verification scores.” MOBIO also reports that segmentation (face detection and voice activity detection) is critical both for face and speaker verification. Toward bi-modal verification one can combine face and iris instead using the more challenging uncontrolled settings for iris data that MICHE-I provides.

Most recently De Marsico et al. [5] have reported on Face and Iris Recognition for Mobile Engagement (FIRME) implemented on the Android system. It is multimodal and can use one contactless sensor (“webcam”) rather than switching to an additional one if fingerprints were used instead of face. Accommodation of face samples (pose and illumination) is handled using best sample (“frame”) selection with the assumption that the biometric target usually occupies almost one whole frame, and that subjects are cooperative and aware of technical issues due to capture. FIRME matches for face and iris separately, is anti-spoof, and can perform continuous reidentification (see Section 8.2).

8. Biometric vulnerabilities

The range of vulnerabilities for mobile devices is wide open with many unknowns yet unknown. Vulnerabilities adversely affect among others security, privacy, data integrity, and anonymity, and resonate with fraud targeting sensitive information. We consider below the potential for MICHE-I to assist with developing and assessing continuous authentication aiming to counter spoofing and impersonation with uncontrolled setting raising the bar for defense.

8.1. Spoofing

Spoofing attacks occur when a biometric recognition system is bypassed by presenting counterfeit evidence of a legitimate user. All what spoofing needs is a simple photograph of the biometric used by the mobile device, e.g., iris. Alternatively, printed photographs, and photos and videos displayed on electronic screens, can easily serve for spoofing. Replay attacks using stored biometric data are yet another strategy available for spoofing. The challenge is to then ascertain if the biometric presented is live or not. When validation of credentials is monitored on a continuous basis it belongs to active authentication (see below). MICHE-I can help here with its MICHE Fake set of images.

8.2. Active authentication

Active authentication is responsible with confirming that the current user of the mobile device is a legitimate one at all times. The motivation and merit for such an application is straightforward as explained next. A mobile device gets unlocked and ready for use when its owner/legitimate user initiates a session using proper login ID and password for authentication. Once the mobile device is engaged/enabled, it remains available for use by any interested party. There is, however, no mechanism to verify on a continuous basis that the user originally authenticated is still the same user now in control of the mobile device rather than an imposter possibly impersonating the legitimate user. Unauthorized subjects may therefore improperly obtain (“hijack”) access to mobile devices and their (implicit and explicit) resources if adequate vigilance after initial authentication is not enforced. The purpose for active and continuous authentication is to counter such security vulnerabilities and their nefarious consequences. Biometric iris authentication can serve such a purpose. MICHE Video set from MICHE-I supports developing and assessing methods for continuous authentication.

9. Discussion

There is need to expand on the framework that MICHE-I and FIRME provide along several dimensions: (a) subject are not necessarily co-operative or even technically aware. (b1) Robust and reliable methods are needed to handle uncontrolled/unassisted settings (including human identification from distance HID) and diverse noise; (b2) the biometrics for reidentification is all encompassing rather than merely appearance and include behavior, e.g., motion and apparent stress; (c) active authentication needs to combine iris biometrics, user profiles, and adaptation, in order to counter spoofing and sophisticated impersonation; (d) the use of mobile devices requires resource optimization coupled to resolving the trade-offs between resolution, accuracy, speed, storage (local or on the cloud), mass readable identification (MRID) and mass readable travel documents (MRTD), and security; and (e) scalability and benchmark studies (see MICHE-I). Toward that end we plan to develop MICHE-II, which expands on MICHE-I along the mix of uncontrolled settings, authentication protocols, and applications.

10. Conclusions

The appeal for iris biometrics is obvious. It is complementary to face, on one side, and is contactless, not much intrusive, with iris codes among the less expensive and effective signatures from a storage and retrieval point of view, on the other side. Detection, segmentation, coding, and matching are still quite challenging for iris recognition, in general, and for their successful embedding on mobile devices, in particular. MICHE-I reflects on such challenges and promotes “reproducible research” so one can compare methods and assess progress. The protocols associated with MICHE-I are iris specific and directly functional to cross-over, multi-level and multi-layer data and method fusion, and interoperability. The protocols proposed go beyond those used for the Iris Challenge Evaluation (ICE) [13], which those used earlier for face (FERET) [12] rather than iris recognition. We are currently expanding on MICHE-I to obtain an extended version MICHE-II, which will contain a higher number of both grey level and color fake images. Furthermore, we will increase the number of available video clips, and provide baseline experiments and benchmark results for comparison. We also note here that most images in MICHE-I also include the periocular region, which allows one to test the joint use of iris and periocular region for recognition, an emerging trend in iris recognition. Experimental results in literature suggest that even in blurred or badly illuminated images, the shape of the eyebrows, and the shape and texture of the eye and other landmarks from the immediate neighborhood of the iris can provide additional discriminative information that helps with improving recognition accuracy. Such insights will bear on MICHE-II regarding both data capture and authentication protocols. The development of MICHE-II will also include and benefit from comparisons between machine (automatic) and human (manual) iris recognition to gain further insights and determine the possibly most effective and helpful factors for this task.

References

[1] K.W. Bowyer, P.J. Flynn, The ND-IRIS-0405 Iris Image Dataset, Notre Dame CVRL Technical Report. (2009).
[2] J.G. Daugman, How iris recognition works, IEEE Trans. Circuits Syst. Video Technol. 14 (1) (2004) 21–30.
[3] J.G. Daugman, New methods in iris recognition, IEEE Trans. Syst., Man, Cybern. B: Cybern. 37 (5) (2007) 1167–1175.
[4] M. De Marsico, M. Nappi, D. Riccio, ES-RU: an entropy based rule to select representative templates in face surveillance, MTAP, Special Issue on human vision and information theory, Springer J. 73 (1) (2014) 109–128.
[5] M. De Marsico, C. Galdi, M. Nappi, D. Riccio, FIRME: face iris recognition for mobile engagement, Image Vis. Comput. (2014) in press, Available at http://www.sciencedirect.com/science/article/pii/S0262885614000055, doi:10.1016/j.imavis.2013.12.014.
[6] H. El Khiyari, M. De Marsico, A.F. Abate, H. Wechsler, Biometric interoperability across training, enrollment, and testing for face authentication, in: Proceedings of 2012 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BioMS 2012), Salerno, Italy, 2012, pp. 1–8.
[7] B.F. Klare, M.J. Burge, J.C. Klontz, R.W. Vorder Bruegge, A.K. Jain, Face recognition performance: role of demographics information, IEEE Trans. Inf. Forensics Security 7 (6) (2012) 1789–1801.
[8] X. Li, Z. Sun, T. Tan, Comprehensive assessment of iris image quality, in: ICIP, 2011.
[9] S. Marcel, et al., On the results of the first mobile biometry (MOBIO) face and speaker verification evaluation, in: ICPR, 2010, pp. 210–225.
[10] L. Masek, P. Kovesi, MATLAB Source Code for a Biometric Identification System Based on Iris Patterns, The University of Western Australia, 2003.
[11] J.R. Matey, et al., Iris on the move: acquisition of images for iris recognition in less constrained environments, Proc. IEEE 94 (11) (2006) 1936–1947.
[12] P.J. Phillips, et al., The FERET evaluation methodology for face-recognition algorithms, IEEE Trans. Pattern Anal. Mach. Intell. 22 (10) (2000) 1090–1104.
[13] P.J. Phillips, et al., FRVT 2006 and ICE 2006 large-scale experimental results, IEEE Trans. Pattern Anal. Mach. Intell. 32 (5) (2010) 831–846.
[14] J.K. Pillai, V.M. Patel, R. Chellappa, N.K. Ratha, Secure and robust iris recognition using random projections and sparse representations, IEEE Trans. Pattern Anal. Mach. Intell. 33 (9) (2011) 1877–1893.
[15] H. Proenca, S. Filipe, R. Santos, J. Oliveira, L.A. Alexandre, The ubiris.v2: A database of visible wavelength iris images captured on-the-move and at-a-distance, IEEE Trans. Pattern Anal. Mach. Intell. 32 (8) (2010) 1529–1535.
[16] H. Proenca, L.A. Alexandre, The NICE.I: noisy iris challenge evaluation – Part I, in: Proc. IEEE First Int'l Conf. Biometrics: Theory, Applications, and Systems (BTAS), 2007, pp. 27–29.
[17] H. Proenca, L.A. Alexandre, Introduction to the special issue on the recognition of visible wavelength iris images captured at-a-distance and on the move, Pattern Recognit. Lett. 33 (2012) 963–964.
[18] D. Riccio, G. Tortora, M. De Marsico, H. Wechsler, EGA – Ethnicity, Gender and Age, a pre-annotated face database, in: Proceedings of 2012 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BioMS 2012), Salerno, Italy, 2012, pp. 38–45.
[19] S. Schuckers, P. Meyer Lopez, P. Johnson, N. Sazonova, F. Hua, R. Lazarick, C. Miles, E. Talbassi, E. Sazonov, A. Ross, L. Hornak, Quality–Face/Iris Research Ensemble (Q-FIRE) Dataset Overview, Technical Report, Clarkson University, Department of Electrical and Computer Engineering (2010).
[20] A. Torralba, A.A. Efros, Unbiased look at dataset bias, in: Proc. Computer Vision and Pattern Recognition (CVPR), Colorado Springs, CO, 2011.
[21] P.A. Tresadern, et al., Mobile biometrics (MoBio): combined face and voice verification for a mobile platform, Pervasive Comput. 12 (1) (2013) 79–87.
[22] H. Wechsler, Reliable Face Recognition Methods: System Design, Implementation and Evaluation, Springer, 2007.