



Iris recognition on consumer devices - challenges and progress

Title	Iris recognition on consumer devices - challenges and progress
Author(s)	Thavalengal, Shejin;Corcoran, Peter
Publication Date	2015-11-11
Publisher	IEEE
Repository DOI	10.1109/ISTAS.2015.7439440

Iris Recognition on Consumer Devices -Challenges and Progress

Shejin Thavalengal, Peter Corcoran

College of Engineering and Informatics,
National University of Ireland Galway, Ireland.

Email: s.thavalengal@nuigalway.ie, peter.corcoran@nuigalway.ie

Abstract— This article outlines various technical, social and ethical challenges in implementing and widely adopting iris recognition technology on consumer devices such as smartphone or tablets. Acquisition of sufficient quality iris images using today's consumer devices is noted to be the main challenge in implementing this technology. Current progress in this field is reviewed. A smartphone form factor camera is presented to be used as a front-facing camera. This device is modified to capture near infra-red iris images along with general purpose visible wavelength images. Analyses shows that such a device with improved optics and sensor could be used for implementing iris recognition in next generation hand held devices. The social impact of wider adoption of this technology is discussed. Iris pattern obfuscation is presented to address various security and privacy concerns which may arise when iris recognition will be a part of our daily life.

Keywords—consumer biometrics; iris recognition.

I. INTRODUCTION

Consumer devices such as smartphones play an important role in our day to day life. It is predicted that approximately 2 billion people will be using smartphones in 2016. This number is expected to grow to a third of the world's population in 2018 [1]. The majority of these devices are connected to internet all the time. 57% of the U.S. smartphone users are reported to carry out online banking through these devices [2]. As these devices are used to transmit such sensitive financial and personal information, reliable assessment of smartphone user's identity is crucial. PIN or passwords may not be sufficient for this purpose, but biometrics could be effectively used [3]. Biometrics is the process of recognizing individuals based on their physical or behavioral traits [4]. A detailed discussion by Corcoran [5] envisages the smartphone as a key appliance for authenticating its user. Face and fingerprint biometrics enabled smartphones are already available in today's consumer market. Other biometric traits are yet to make their way in to smartphones.

II. IRIS BIOMETRICS AND SMARTPHONES

Iris of the human eye is the annular region between the pupil and sclera. The iris pattern consist of complex and distinctive ligaments, furrows, ridges, rings, corona, freckles and collarette [6]. An example of an iris image is shown in

Fig.1. Also, iris is relatively stable over the lifetime of a person starting from eighth month of gestation and have high pattern variability, even for identical twins and between the left and right eye of the same person [6]. These characteristics make iris recognition a suitable candidate for user authentication in smartphones.

Even though the human iris is a near ideal biometric and the iris recognition technology is mature and widely deployed, iris recognition on smartphones is yet to be implemented. This is partly due to the market demand for an unconstrained and easy to use iris recognition system and the challenging nature of acquiring suitable high quality images using current smartphones. Some of the noted image acquisition challenges are – (i) the iris is a relatively small subject on a wet, curved and reflecting surface, (ii) the iris region could be occluded by eyelids, eyelashes and specular reflection, (iii) the iris is best captured in near infra-red (NIR) illumination, (iv) uncontrolled ambient illumination, (v) optical constraints introduced by miniature camera modules, (vi) pixel resolution limited by optical and cost consideration, (vii) an unstable hand-held platform which may introduce motion blur artefacts and (viii) limited processing power of the devices [7].

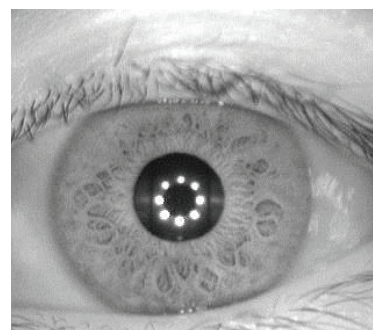


Fig. 1. Example of an Iris of the Human Eye. Image is from CASIA V4 iris database [8].

For smartphones, a typical use case is the user-authentication using the front-facing (user-facing) camera while holding the device at a comfortable arm's length. From the cost perspective, using the same sensor and optics to capture both visible (video call, selfie imaging etc.) and near infra-red (NIR) (iris image acquisition) image data favors a single user-facing camera.

The existing literature on smartphone iris recognition can be roughly classified in to two – (i) studies which use modified smartphones and constrained image acquisition conditions [9] or (ii) visible image iris recognition using existing smartphone cameras [10], [11]. The images captured in visible wavelength may not contain sufficient iris information, especially in dark colored irises [6]. This can be noticed in Fig. 2. Fig. 2(a) represents an eye image captured at visible wavelength.

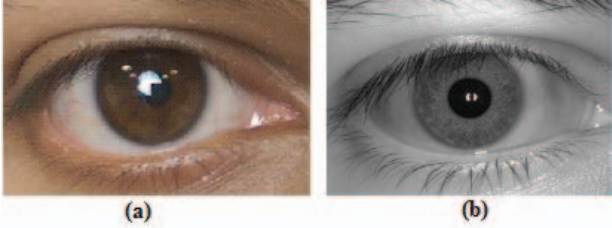


Fig. 2. Example of RGB (visible) and NIR iris image pairs: (a) RGB eye image, (b) the same eye image captured at NIR wavelength.

Fig. 2(b) shows the same image captured at NIR wavelength. The fine iris details can be visible in this image as opposed to the visible counterpart. Also, international standards recommends using NIR images for iris recognition [12].

III. SMARTPHONE IRIS IMAGE ACQUISITION

Corcoran, Bigioi and Thavalengal [13] carried out a feasibility study of iris recognition in smartphones. This work presented a detailed analysis of different image quality factors which may affect smartphone iris recognition. The authors concluded that iris images should ideally be acquired in near infrared illumination with a minimum 60-80 non-upsampled pixels across iris diameter to have an acceptable iris recognition performance in consumer devices. This iris image should have sufficient usable iris area, image sharpness, iris-pupil and iris-sclera contrast, gaze angle etc.

Previous researches presented various design strategies for implementing iris recognition on smartphones [13], [14]. The two main design considerations presented were (i) the use of a single hybrid camera with a single complementary metal-oxide-semiconductor sensor optimized for both visible and NIR wavelength use cases, (ii) dual-imaging system, where two dedicated user-facing cameras are present – one for video call which follows the existing commercial user-facing camera design and one for iris recognition which can capture NIR iris images. Even though the second design consideration comes with increased cost for an extra camera, the authors recommended it due the several advantages such as: (a) possibility of reducing the field of view of the infrared imaging system which will increase the pixel resolution in the iris region; (b) independent design of visible and infrared optical systems, and (c) no movable IR filter is needed.

A recent smartphone case study revealed that at least one model of contemporary smartphone is potentially capable of implementing visible iris authentication, although not with high reliability [14]. However visible wavelength authentication is limited to a segment of the population with a lightly-colored iris. A practical acquisition needs to employ NIR wavelengths, but could rely on established visible wavelength face and eye tracking techniques to determine suitable iris regions for NIR acquisition and subsequent segmentation.

Based on these studies [13], [14], a prototype of the smartphone form factor dual purpose RGB-NIR front facing camera has been engineered. This camera combines the functionality of a conventional front-camera, such as selfie imaging and video call, with the potential for iris authentication. Initial analysis shows that this device could be used as the user-facing camera in next generation smartphones for iris recognition [7]. An example of such a device is shown in Fig.3.

This prototype device is able to sense NIR information using the modified color filter array. Half of the green pixels from a standard Bayer color filter array are replaced with NIR sensitive pixels. The ‘hot mirror’ which is generally present in front of the image sensor is modified to pass a narrow band of NIR waves around 850nm wavelength. This camera is of 4 mega pixel spatial resolution with 4mm focal length [7], [15]. Example for iris images captured using this device is shown in Fig.4.

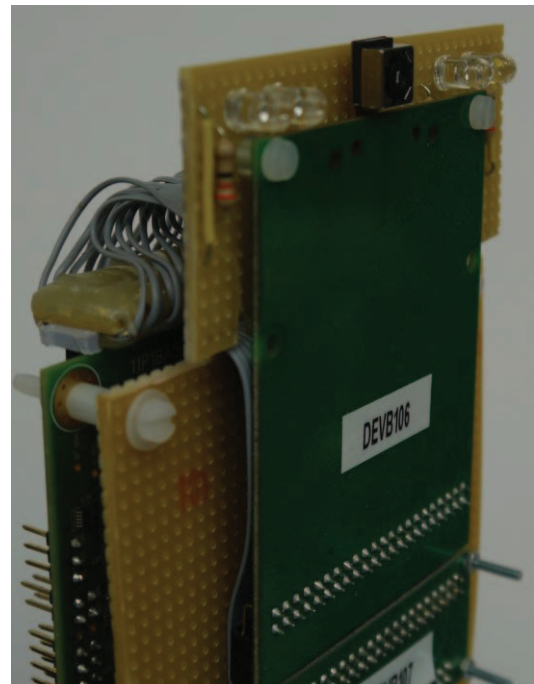


Fig. 3. Prototype device – Smartphone form factor optics and NIR light emitting diodes on both sides can be observed.

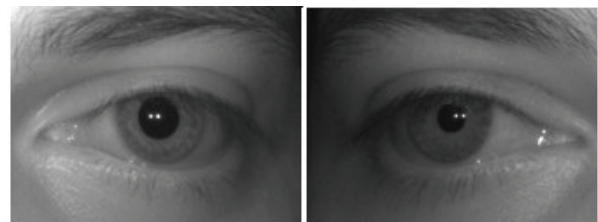


Fig. 4. Examples of iris images captured using the prototype device at 15cm standoff distance.

Images captured at 15cm away using this device are observed to have approximately 75 pixels across iris diameter. Even though this is below the minimum recommended level by international standard, Corcoran, Bigioi and Thavalengal [13] noted that this will be sufficient for acceptable iris recognition performance, especially in low security use cases such as device unlock as opposed to financial transactions. The optical resolution of these images are just above the minimum

acceptable threshold defined by international organization for standardization [12].

Experiments carried out using this device shows that iris biometrics can be implemented on smartphones devices using such a hybrid visible/NIR camera modules. But, a number of significant challenges remain in terms of image quality, recognition performance and user friendliness for this solution to meet the demands and expectations of the current consumer market.

IV. PRACTICAL CHALLENGES IN WIDER ADOPTIBILITY OF IRIS RECOGNITION

The brief discussion about iris recognition given in the previous section points the possibility of this powerful technology to be deployed in billions of consumer electronics devices such as smartphones and tablets in the near future. Iris recognition, like any other technology comes with inherent vulnerabilities such as data security, template protection issues, identity theft and spoofing attacks [16]. Face images of us are widely available from the social networks and other related websites in internet. But, a person's appearance can be easily changed. Also, face is not considered as a reliable biometric, on its own, for authentication purpose. The corresponding problem with iris could be more significant as iris is a reliable biometric and stable over time.

The biometric data is vulnerable to attack and theft if it is stored in the device or a central database. Instead, using the biometric data to generate an enrolment key, which is stored and used for comparison, can be a way to overcome this situation [5]. In this way, by restricting the biometrics analysis to the device and not storing any biometric data, we can counter the concerns related to biometric theft. This supposes a two-stage authentication where both person and device are required to complete the authentication procedure.

'A Life Revealed' by Cathy Newman tells how iris recognition is used to identify the 'Afghan Girl' from two face portrait photographs captured by National Geographic photographer Steve McCarthy [17], [18]. The first photo was captured in 1984 and the second photo was 18 years later. This shows a practical example of how face portrait images could be used to trace people using the iris information present.

The imaging subsystem of smartphones are improving day by day with the help of advanced optics and post processing systems. Some consumer devices even use NIR information to enhance the color images. Hence, usable iris data can be extracted from these images. This signals a new problem for people who capture the images of themselves, their friends and family and share it in internet. These information could be used not only to identify the person and invade his privacy, but also to use his identity for spoofing attacks against iris recognition systems [19].

A. Iris Pattern Obfuscation:

Hence, a solution to prevent the misuse of iris information in these images is crucial for wider adoption of iris recognition on consumer devices. Practically, such a solution is existing in current smartphones and other digital still cameras. Nowadays we cannot spot any 'red-eye' in the images captured using these devices. It is not because the red-eye doesn't occur, but it is detected and corrected in the camera itself. A similar technique, which could detect the iris region in the images and

replace them, could be used here. This should be done in such a way that the replaced images will look natural and similar to the subject's original eye, but the iris information should not match to the original iris. This technique is generally called iris pattern obfuscation [19]. Iris pattern obfuscation should be implemented within the camera before detailed iris data is transferred to permanent storage or transported over a network link.

Thavalengal *et al* introduced various iris pattern obfuscation techniques and analysed their efficiency and feasibility to be incorporated in next generation consumer devices [19]. Iris replacing technique, where the iris information present in the image is replaced with that of a standard iris is found to be highly effective. This standard iris could be an artificial iris pattern generated randomly. Examples of this technique are shown in Fig.5. It could be noted from Fig.5 that, the obfuscated iris has similar color and appearance as of the original one.

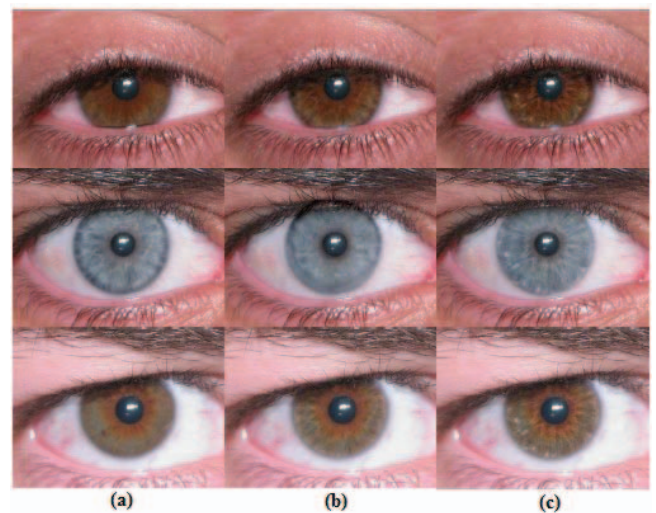


Fig. 5. Examples of iris pattern obfuscation – (a) Original image, (b) and (c) obfuscated images using different techniques.

Iris pattern obfuscation techniques face various challenges in implementation. First and foremost is the undetectable modification of the iris area. Even though human perception is more sensitive to the luminance variation and appearance than the underlying random pattern, large distortion in the eye region will be noticed. Obfuscation should not produce any visible artefacts for its acceptability by the consumers.

Another important challenge is the robust detection of 'at risk' iris region. If an eye image doesn't provide enough useful iris information (such as a closed eye), there is no need to obfuscate such images. Also, iris region should be detected and localized accurately for the obfuscation to look natural.

The real time implementation of this technology is crucial. This can be achieved with the existing hardware accelerators which are used for red-eye detection and removal. Hence, it can be concluded that, iris pattern obfuscation, if implemented and adopted widely, can address privacy concerns related to iris recognition technology.

V. SOCIAL IMPACT OF WIDER ADOPTION OF BIOMETRIC TECHNIQUES

Various social and ethical concerns will start to arise once biometrics becomes a common practice in our day to day life.

The first and foremost concern will be related to the privacy of the end users. Despite its advantages, one drawback of biometric recognition is related to the lack of secrecy of the data. Unlike passwords, biometrics cannot be replaced if the data is compromised. Considering that some of our biometric traits, particularly the face and the iris, are easily captured, stored and displayed in the internet by others, then one should question at what extent it is ethical to do something as common as publishing photos of other people in our social network accounts.

Another important impact will be on how and where the data is stored. With the help of the state of the art spoofing techniques, biometric data can be practically used for identity theft. If society is too dependent on biometrics for identity verification, identity theft will have severe social consequence. Also, the biometric data can be used for mass surveillance, law enforcement, targeted advertisements etc. This is of greater concern as we can obtain an estimate of age, gender and race from these biometric modalities such as iris [20],[21]. The current legal environment should be adapted to deal with such situations to avoid ‘function creep’ where these techniques introduced for a specific purpose is extended for other purposes which were not discussed or agreed up on the time of their implementation [22].

Examples like the Afghan Girl [17], [18] show how great the impact of these techniques can be in the lives it touches. If iris recognition is successfully implemented in smartphones the range of its impact is broaden significantly, due to the easiness of access to these devices. Therefore its ethical implications will also increase since the use of iris recognition will not only be confined to authorities who already have access to devices equipped with biometric recognition but also will be easily used by any common citizen.

VI. SUMMARY AND CONCLUSIONS

Biometrics is making its way in to smartphones. As a near ideal biometrics, iris recognition can provide the security demanded by next generation smartphones. Various challenges in implementing iris recognition on smartphones, different design strategies and practical solutions are presented. An analysis of a smartphone form factor prototype device is presented with analysis of its suitability for iris recognition. Practical challenges in adopting iris recognition on consumer devices are discussed and a potential solution – iris pattern obfuscation is presented. Various social and ethical impact of large scale adoption of biometric techniques such as the use in consumer devices is discussed.

ACKNOWLEDGMENT

This research is supported by the Employment based PhD program (EBP) of the Irish Research Council (www.research.ie) and part-funded by FotoNation Ltd. Authors would like to thank Professor Christopher Dainty and Ana Filipa for their valuable comments.

REFERENCES

[1] S. Curtis, “Quarter of the world will be using smartphones in 2016,” *The Telegraph*, 11 Dec. 2014. [Online]. Available: <http://www.telegraph.co.uk/technology/mobilephones/11287659/Quarter-of-the-world-will-be-using-smartphones-in-2016.html> [Last accessed: 13 Mar. 2015].

[2] Pew Research Center, “The Smartphone Difference.” [Online]. Available: <http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/> [Last accessed: 14 Jul. 2015].

[3] N. L. Clarke and S. M. Furnell, “Authentication of users on mobile telephones - A survey of attitudes and practices,” *Computers and Security*, vol. 24, no. 7, pp. 519–527, 2005.

[4] A. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, 2004.

[5] P. Corcoran, “Biometrics and Consumer Electronics: A Brave New World or the Road to Dystopia?” *IEEE Consumer Electronics Magazine*, vol. 2, no. 2, pp. 22–33, Apr. 2013.

[6] J. Daugman, “How Iris Recognition Works,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, Jan. 2004.

[7] The Institute of Automation of the Chinese Academy of Sciences, “CASIA iris database,” <http://biometrics.idealtest.org/>.

[8] S. Thavalengal, P. Bigioi, and P. Corcoran, “Evaluation of combined visible/nir camera for iris authentication on smartphones,” in *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, June 2015.

[9] K. Park, H.-A. Park, B. Kang, E. Lee, and D. Jeong, “A study on iris localization and recognition on mobile phones,” *EURASIP Journal on Advances in Signal Processing*, vol. 2008, no. 1, p. 281943, 2008.

[10] S. Barra, A. Casanova, F. Narducci, and S. Ricciardi, “Ubiquitous iris recognition by means of mobile devices,” *Pattern Recognition Letters*, vol. 57, pp.66–73, 2014.

[11] R. R. Jillela and A. Ross, “Segmenting iris images in the visible spectrum with applications in mobile biometrics,” *Pattern Recognition Letters*, vol. 57, pp. 4–16, 2015.

[12] Working Group 3, “ISO/IEC 19794-6 Information Technology - Biometric Data Interchange Formats - Part 6: Iris image,” *JTC1 :: SC37*, international standard edition, vol. 44, 2011.

[13] P. Corcoran, P. Bigioi, and S. Thavalengal, “Feasibility and design considerations for an iris acquisition system for smartphones,” in *IEEE Fourth International Conference on Consumer Electronics-Berlin*, pp. 164–167, Sep. 2014.

[14] S. Thavalengal, P. Bigioi, and P. Corcoran, “Iris authentication in handheld devices - considerations for constraint-free acquisition,” *IEEE Transactions on Consumer Electronics*, vol. 61, no. 2, pp. 245–253, May. 2015.

[15] S. Thavalengal, I. Andorko, A. Drimbarean, P. Bigioi, and P. Corcoran, “Proof-of-concept and evaluation of a dual function visible/nir camera for iris authentication in smartphones,” *IEEE Transactions on Consumer Electronics*, vol. 61, no. 2, pp. 137–143, May. 2015.

[16] B. Toth, “Liveness detection: Iris,” *Encyclopedia of Biometrics*, pp. 931–938, 2009.

[17] C. Newman, “A Life Revealed,” *National Geographic Magazine*, April 2002. [Online]. Available: <http://ngm.nationalgeographic.com/2002/04/afghan-girl/> [Last accessed: 14 Jul. 2015].

[18] J. Daugman, “How the Afghan Girl was Identified by Her Iris Patterns.” [Online]. Available: <http://www.cl.cam.ac.uk/jgd1000/afghan.html> [Last accessed: 14 Jul. 2015].

[19] S. Thavalengal, R. Vanceanu, R. Condorovici, and P. Corcoran, “Iris pattern obfuscation in digital images,” in *2014 IEEE International Joint Conference on Biometrics*, pp. 1–8, Sep. 2014.

[20] Lagree, S. Bowyer, K.W. Flynn, “Predicting ethnicity and gender from iris texture,” in *2011 IEEE International Conference on Technologies for Homeland Security*, pp.440-445, Nov. 2011.

[21] Sgroi, A. Bowyer, K.W. Flynn, P.J, “The prediction of old and young subjects from iris texture,” *2013 International Conference on Biometrics*, pp.1-5, Jun. 2013.

[22] The European Commission's Joint Research Centre, “Biometrics at the frontiers: assessing the impact on society,” *Executive Summary* [Online]. Available: <http://ftp.jrc.es/EURdoc/21585-ExeSumm.pdf> [Last accessed: 15 Jul. 2015].