A Practical Challenge for Iris Authentication on Handheld Imaging Devices

Shejin THAVALENGAL, *Student Member, IEEE* and Peter CORCORAN, *Fellow, IEEE*
National University of Ireland Galway, Ireland.
{s.thavalengal1, peter.corcoran}@nuigalway.ie

***Abstract*-- Following on the introduction of fingerprint biometrics, iris authentication for handheld imaging devices has become a hot research topic. However widespread adoption of this technology faces a significant challenge as personal iris data for a significant proportion of the population can be extracted from high-quality images and the growth in image sharing and the creation of online personal photographic albums creates a significant security risk. In this paper we present an overview of the problem and a potential solution – iris obfuscation when images are acquired. Challenges to implementing a practical obfuscation technology are discussed and approaches to overcome these are explored.**

I. INTRODUCTION

Smartphones offer an excellent platform to introduce the use of biometrics for user authentication and as a key enabling technology for next generation online products & services [1]. Fingerprint sensing for smartphones is currently available, but the iris of the human eye has been shown to be a superior biometric [2], [3]. Moreover, iris recognition is known to be more robust to spoofing attacks as compared to many other biometric modalities such as fingerprints [4].

A feasibility study for an iris acquisition system for smartphones is presented in our previous work [5]. Acquisition system design strategies and the relevance of image quality parameters were analyzed in that work. Interestingly, recent smartphones have introduced user-facing cameras with high-resolution sensors providing sufficient pixel resolution for robust iris recognition, or multi-camera systems to support accurate depth/3D image acquisition. Such developments greatly enhance the quality of iris regions captured in regular smartphone self-portraits or 'selfies' – the most commonly shared personal images.

In parallel, there is significant industry research to improve the quality of smartphone imaging with the use of dual-aperture and employing IR spectral components to enhance visible images [6], [7]. It is very likely that we will see such dual-aperture imaging systems appear on the market within the next few years and these technologies enable hybrid iris acquisition as an alternative to NIR acquisition.

In summary, the introduction of smartphones and other hand-held devices equipped with iris recognition in consumer market seems imminent.

II. THE ELEPHANT IN THE ROOM – PERSONAL IMAGES

The All commercially deployed iris recognition algorithms use near infrared images, but significant work has also been carried out on iris recognition from images captured in visible wavelength [8]. A significant proportion of the human population possesses light to medium pigmented eyes and these eyes captured even in visible wavelength reveal sufficient iris pattern for person identification [8].

In addition, imaging subsystems on smart phones are becoming smarter, which enables enhanced, higher quality image capture including enhancement with NIR frequencies. A particular focus is enhancement of personal appearance and in particular eye regions [9]–[12]. Hence, it is likely in near future that images from cameras and smart-phones provide sufficient, enhanced eye-region quality to analyze and determine with some reliability the underlying features of an iris pattern [13]. This signals an emerging problem for people who capture images of themselves and their family, friends and acquaintances and share such images in social networks, or more widely on the Internet.

III. A POTENTIAL SOLUTION - IRIS OBFUSCATION

Iris pattern obfuscation as a measure to protect against obtaining iris data from personal images and use it for spoofing is introduced in our previous work [13]. Iris pattern obfuscation is the process of detecting and substituting the existing iris region with a similar region that has the same color and appearance but does not match the original iris pattern. Ideally, this should be implemented within the camera before the acquired image is transferred to permanent storage or transported over a network link. Iris pattern obfuscation will likely become a key enabling technology for the widespread adoption of iris biometrics on consumer imaging devices.

Various iris pattern obfuscation techniques were introduced in [13] and their feasibility was demonstrated. In this paper given that iris pattern replacement is feasible, some of the challenges to realize a more widespread adoption of obfuscation technology in today's consumer electronics devices are considered.

IV. CHALLENGES IN IMPLEMENTING IRIS OBFUSCATION

Having outlined the rationale for iris obfuscation, the next target is to address the challenges facing this proposed new technology. A more detailed explanation on how iris substitution is achieved and how the underlying eye region is restored to a natural appearance is presented in Thavalengal *et.al.* [13].

This research is supported by the Employment based PhD program of the Irish Research Council and part-funded by FotoNation Ltd.

A. Undetectable Modification of Eye-Regions

Meeting this first challenge relies on the iris pattern information being primarily stored as luminance variations. In contrast human perception of the eye region relies mainly on eye-color. Thus the generally random patterns of the iris are not distinguishable to most human observers. Some practical examples have been given in [13]. In addition well-known technologies such as the correction of flash-eye defects [11] and facial beautification [9] have introduced the underlying concepts of in-camera region substitution and enhancement to end-users.

Nevertheless these assumptions must be tested through more widespread studies across larger sets of images and across a significant population group. While most individuals will not notice changes in their own iris patterns or those of their loved ones, there are likely to be outlying examples where changes in the iris pattern prove disconcerting.

B. Robust Detection of 'At Risk' Eye Regions

This problem parallels that of the detection problem for red-eye (flash-eye) artifacts. As one might expect this is non-trivial as shown by the detailed analysis of related patents provided in [12]. At present the use of in-camera face detection and eye-gaze [14] technologies facilitates the location and determination of the properties of eye-regions in each image frame. This is sufficient to detect the location and the approximate orientation of each eye region. Frontal facing eye regions are the principle candidates for obfuscation and an additional check on the 'openness' of the eye [10] completes a determination if obfuscation is needed.

However the most challenging cases are those where the eye-gaze is at a non-frontal angle, or the eye is partially open. In these cases obfuscation is not straightforward to implement, but there is a risk that some of the iris pattern may be available, enabling a determined attacker to gather multiple complimentary iris region images and process these to reconstruct the original iris pattern. Some of these challenges will be discussed in detail in a future publication.

C. Real-Time Implementation

Real-time implementation of iris obfuscation is perhaps the key challenge – the above techniques must operate at full HD and be capable to scale to 4k video rates. For a practical in-camera system this demands a hardware implementation of key algorithmic primitives.

D. User Transparency

It goes without saying that any practical realization of obfuscation should be transparent to the end user. In fact it is likely to become a 'required' technology if iris authentication becomes commonplace.

V. Summary of Work

In this work, the main concepts of iris obfuscation are outlined, including a summary of recent results from Thavalengal *et.al.* [13]. More importantly, for the CE community some of the main challenges facing a practical in-camera realization of obfuscation technology are addressed, with emphasis on the requirement that obfuscation is a real-time process that must work at speeds compatible with the frame-to-frame data rates of consumer video systems.

Fortunately the availability of a range of existing in-camera hardware technologies makes certain aspects of this challenging engineering problem more realizable than might be expected and it is shown that practical realizations are within the capabilities of today's smartphone imaging systems.

References

[1] P. Corcoran, "Biometrics and Consumer Electronics: A Brave New World or the Road to Dystopia?," *IEEE Consum. Electron. Mag.*, vol. 2, no. 2, pp. 22–33, 2013.

[2] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, 2004.

[3] J. Daugman, "How Iris Recognition Works," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 21–30, Jan. 2004.

[4] B. Toth, "Liveness Detection: Iris," in *Encyclopedia of Biometrics*, S. Li and A. Jain, Eds. Springer US, pp. 931–938, 2009.

[5] P. Corcoran, P. Bigioi, and S. Thavalengal, "Feasibility and Design Considerations for an Iris Acquisition System for Smartphones," in *Proc. IEEE Fourth International Conference on Consumer Electronics - Berlin*, Sep. 2014.

[6] X. Zhang, T. Sim, and X. Miao, "Enhancing photographs with near infrared images," in *26th IEEE Conference on Computer Vision and Pattern Recognition,* 2008.

[7] Y. Lu, M. J. Higgins-Luthman, W. R. Livengood, and J. D. Harris, "Combined RGB and IR Imaging Sensor." US 8446470 B2, 2013.

[8] H. Proença, "Iris Recognition in the Visible Wavelength," in *Handbook of Iris Recognition*, M. J. Burge and K. W. Bowyer, Eds. Springer London, pp. 151–169, 2013.

[9] C. Florea, A. Capata, M. Ciuc, and P. Corcoran, "Facial enhancement and beautification for HD video cameras," in *Proc. IEEE International Conference on Consumer Electronics*, pp. 741–742, 2011.

[10] I. Bacivarov, M. Ionita, and P. Corcoran, "Statistical models of appearance for eye tracking and eye-blink detection and measurement," *IEEE Trans. Consum. Electron.*, vol. 54, pp. 1312–1328, 2008.

[11] P. Corcoran, P. Bigioi, E. Steinberg, and A. Pososin, "Automated in-camera detection of flash-eye defects," *IEEE Trans. Consum. Electron.*, vol. 51, no. 1, pp. 11–17, Feb. 2005.

[12] P. Corcoran, P. Bigioi, and F. Nanu, "Advances in the detection & repair of flash-eye defects in digital images-a review of recent patents," *Recent Patents Electr. Electron. Eng.*, vol. 5, no. 1, pp. 30–54., 2012.

[13] S. Thavalengal, R. Vranceanu, R. G. Condorovici, and P. Corcoran, "Iris Pattern Obfuscation in Digital Images," in *International Joint Conference on Biometrics*, Oct. 2014.

[14] P. M. Corcoran, F. Nanu, S. Petrescu, and P. Bigioi, "Real-time eye gaze tracking for gaming design and consumer electronics systems," *IEEE Trans.Consum. Electron.*, vol. 58, no. 2, pp. 347–355, 2012.