Pattern Recognition Letters 57 (2015) 4–16

Contents lists available at ScienceDirect

Pattern Recognition Letters

journal homepage: www.elsevier.com/locate/patrec

Segmenting iris images in the visible spectrum with applications in mobile biometrics ☆

Raghavender Reddy Jillela [a,1], Arun Ross [b,*]

[a] Digital Signal Corporation, Chantilly, VA, USA
[b] Michigan State University, East Lansing, MI, USA

ARTICLE INFO

Article history:
Received 25 July 2014
Available online 31 October 2014

Keywords:
Iris
Segmentation
Mobile
Biometrics
Visible

ABSTRACT

The widespread use of mobile devices with Internet connectivity has resulted in the storage and transmission of sensitive data. This has heightened the need to perform reliable user authentication on mobile devices in order to prevent an adversary from accessing such data. Biometrics, the science of recognizing individuals based on their biological and behavioral traits, has the potential to be leveraged for this purpose. In this work, we briefly discuss the suitability of using the iris texture for biometric recognition in mobile devices. One of the critical components of an iris recognition system is the segmentation module which separates the iris from other ocular attributes. Since current mobile devices acquire color images of an object, we conduct a literature review for performing automated iris *segmentation* in the visible spectrum. The goal is to convey the possibility of successfully incorporating iris recognition in mobile devices.

1. Introduction

The degree of electronic connectivity in our society has increased tremendously over the past few years. According to the global statistics report compiled by the International Telecommunications Union, 2.7 billion people (i.e., almost 40% of the world's population) are currently connected through the Internet [1]. Such a staggering level of connectivity has been possible within just 25 years of the invention of the World Wide Web. An important factor driving these statistics is the growth of communication via mobile devices. Market research agencies indicate that 1.7 billion people around the world currently access the Internet via mobile devices [2]. In 2016, this number is projected to be close to 2.5 billion. As the advancements in communication technology become more accessible and affordable, mobile device connectivity is expected to rapidly increase. Examples of mobile devices include smartphones, tablet PCs, digital image and video recording devices, Personal Digital Assistants (PDAs), handheld and wearable computers, portable media, and game consoles (see Fig. 1). However, in this article we focus primarily on smartphones.

This explosion in the use of mobile devices for conducting private communication, financial transactions and business negotiations has heightened the need for reliably authenticating users accessing these devices. The authentication process is expected to be fast, automated, and preferably carried out remotely. Recent literature has explored the possibility of utilizing biometrics to authenticate mobile users. Biometrics is the science of recognizing individuals based on their physical or behavioral traits [3,4]. These traits include face [5], fingerprints [6], iris [7–10], periocular region [11], gait [12,13], voice, etc. While biometric solutions have been incorporated into a number of border security and access control applications, their use in mobile devices has only recently gained attention. The term *mobile biometrics* is now being used to refer to the process of utilizing biometric traits for authenticating users of mobile devices.[2] The *mobility* aspect of these devices refers to their high degree of portability and their ability to provide Internet connectivity on-the-move (e.g., cellular service, Wi-Fi, etc.). A vast majority of mobile devices are equipped with sophisticated audio, image, and video recording capabilities. Furthermore, due to the reduced size and cost of processing units and memory devices, additional sensors (e.g., accelerometer, fingerprint sensor, etc.) can be easily embedded into the mobile devices. This allows for the fast and reliable acquisition of various biometric traits for personal authentication. Examples of various biometric traits that can be acquired using mobile devices are shown in Fig. 2.

The past two decades have witnessed a significant growth in biometric technology (i.e., sensors, devices, algorithms, applications).

☆ This paper has been recommended for acceptance by G. Sanniti di Baja.

* Corresponding author. Fax: +1-517-432-1061.
E-mail addresses: Raghavender.Jillela@DigitalSignalCorp.com (R.R. Jillela), rossarun@cse.msu.edu (A. Ross).

[1] This work was performed when Raghavender Jillela was with West Virginia University, WV, USA

[2] In some instances, the term has also been used to refer to compact and portable standalone biometric devices (e.g., EyeLock Myris, Iritech IriShield, etc.).

http://dx.doi.org/10.1016/j.patrec.2014.09.014
0167-8655/

Fig. 1. Examples of mobile devices capable of capturing biometric data: (a) smartphones, (b) tablet computers, (c) digital cameras, (d) digital video recorders, (e) wearable activity trackers (e.g., Fitbit), (f) wearable head-mount displays (e.g., Google Glass), (g) 3D sensors (e.g., [14]), and (h) portable game consoles (e.g., XBOX Kinect).

Fig. 2. Examples of biometric traits that can be acquired using mobile devices: (a) face, (b) fingerprints, (c) iris, (d) handwriting, (e) voice, and (f) 3D structure, respectively.

However, a majority of this growth has been observed in the government (e.g. border crossing, law enforcement, national ID), forensics (e.g., criminal investigations, corpse identification), and commercial (e.g., access control) domains. In comparison, the usage of biometric technology in consumer electronics (e.g., mobile devices, computer login, etc.) has been limited. With the advent of mobile devices, this trend is likely to change in the near future. The Apple iPhone Touch ID and Google Nexus Face Unlock already utilize fingerprint and face recognition technologies, respectively, for personal authentication. Although still in the developmental stage, mobile biometric technology can potentially offer several advantages:

1. *Portability*: Owing to their compact footprint and high degree of portability, mobile devices are typically carried in person by their owners to different locations.
2. *Low operational cost*: The cost of performing biometric authentication on these devices is minimal due to decreasing size and increasing computational power of the processing units.
3. *Ease of multi-biometric data acquisition*: A number of mobile devices are equipped with sensors that can acquire multi-biometric data (e.g., high resolution cameras for face and iris recognition, voice recorders for speaker recognition, etc.). Fusion of biometric information can provide highly reliable authentication performance.
4. *Multi-factor authentication*: Mobile devices lend themselves to multi-factor authentication since the biometric data can be used in conjunction with graphical passwords (through touch screen) and geospatial data (from GPS) to harden the authentication process.
5. *Market penetration*: Due to the popularity and widespread use of mobile devices, they are better positioned to penetrate society thereby offering a broader customer base to the biometric industry.
6. *Data privacy:* Since a user's biometric template can be encrypted and retained within the mobile device, it is relatively difficult for an adversary to steal or modify the template of a user.
7. *Remote identification*: Mobile biometrics are more suitable for user verification, rather than identification. This is because of the higher computational cost of identification (1:*N* matching) compared to verification (1:1 matching). However, in cases where identification is required, mobile devices can also securely transfer the biometric data to a remote server (e.g., a cloud platform) to perform matching.

The focus of this paper is on the iris biometric trait. In particular, we focus on the segmentation module of the iris processing pipeline. The remainder of this paper is organized as follows: Section 2 discusses the significance of iris in the context of mobile biometric recognition. The various steps involved in an iris recognition system are outlined in Sections 3–7. Section 8 lists some of the major challenges in mobile iris recognition. A review of existing iris segmentation techniques that are suitable for mobile iris recognition is provided in Section 9. Section 10 concludes the article.

2. Mobile biometric recognition

A number of physical and behavioral traits have been studied as biometric indicators (e.g., face, fingerprints, iris, voice, gait, palm prints, ocular region, etc.). Amongst these traits, face, fingerprint, iris and voice have particularly received extensive coverage in the published literature. The potential of each of these four modalities in the context of mobile biometrics is reviewed below.

1. While a face image can be easily acquired using a mobile device, the degree of variability due to changes in facial pose and ambient illumination can severely impact the recognition performance.