Chapter 17
Secure Face Recognition for Mobile Applications

Brian C. Lovell
The University of Queensland, Australia

Daniel F. Smith
The University of Queensland, Australia

ABSTRACT
Biometric systems are generally restricted to specialist deployments and require expensive equipment. However, the world has recently experienced the widespread rollout of cheap biometric devices in the form of smart phones and tablets. One of the main drivers for mainstream adoption of biometric technologies is the need to address continuing problems with authenticating to online systems. These mobile devices may now be suitable to provide biometric-based authentication to a wide user population. This chapter discusses the different ways that face recognition can be used on smart mobile devices. The authors highlight the online authentication problem and show how three-factor authentication can address many pressing issues. They also discuss the ways that such a system could be attacked, and focus on replay attacks which have yet to be seriously addressed in the literature. The authors conclude with a brief examination of the current research into addressing replay attacks.

INTRODUCTION
Biometrics has been studied for several decades but widespread use is still yet to occur outside of specialist security deployments. Holding back the wider usage of biometrics is the lack of ubiquitous biometric sensors and systems, driven primarily by cost factors. Moreover, to date, there has been no compelling use case to motivate such a universal rollout.

What if, suddenly, every user had a biometric device available to them at no additional cost? Would this be enough to see the use of biometrics finally reach that elusive tipping point?

It appears that the world is indeed on the cusp of just such a tipping point. Biometric devices, in the form of hand-held smart mobile devices, are being purchased in increasingly large numbers. How could these now ubiquitous devices be leveraged into a gigantic biometric system?

DOI: 10.4018/978-1-4666-5966-7.ch017
This chapter examines the use of commodity smart mobile devices as biometric sensors. More specifically, we focus on using the video camera to support facial recognition applications. Mobile face recognition raises two important questions. What is the application driver that will ensure the widespread adoption of such a biometric system? What are the security issues that must still be resolved before smart mobile devices can successfully act as biometric sensors?

**BIOMETRICS**

Biometrics has been defined as “The automated use of physiological or behavioral characteristics to determine or verify identity” (International Biometric Group, 2013) and has been studied for over 100 years (Bertillon, 1893). Jain *et al.* (1999) is an excellent introduction to the field of Biometrics.

Examples of the many modes of biometric systems include fingerprints, face recognition, voice recognition, iris scanning, retina scanning, hand geometry, ear patterns, gait recognition, vein patterns, written signature, keystroke dynamics, and DNA.

Immigration and border protection services are among the early adopters of automated biometric systems. The USA originally used hand geometry in their INSPASS program, and then moved to face recognition and fingerprints in the upgraded US-VISIT program. This current system is manually driven, and very labour intensive. Australia and New Zealand use face recognition in their SmartGate system that is coupled to the passenger’s biometric enabled passport. This system uses automated booths, but there is still significant staff oversight to prevent security breaches and to facilitate passenger movement. Figure 1 shows examples of each of these biometric border protection systems.

Other uses for biometrics are personal identification of persons of interest (iris scanning), building/restricted space access control (face, voice, fingerprint), and crime scene investigation (DNA). More recently, biometrics have started to appear in laptop and desktop computers (face, fingerprint), but these are primarily used for local access to that computer system only.

Outside of such deployments, biometric systems are not commonly used by the general public. One of the primary challenges to widespread adoption is that the biometric sensor technology must be readily available in the location where it is expected to be used. An examination of the many different types of biometrics above shows that only a small subset of biometric modes could

*Figure 1. Border protection biometric systems - INSPASS, US-VISIT, and SmartGate*