Chapter 7
Biometric Spoofing and Anti-Spoofing

Zahid Akhtar
University of Udine, Italy

ABSTRACT

The demand for reliable and robust person recognition systems has expanded due to intense security requirements in today’s highly intertwined network society. The advantages of biometrics over traditional security systems have triggered large-scale deployment of biometrics as an authentic technique to determine the identity of an individual. The prime objective of such methods is to assure that the systems are only accessed by genuine users. Since, biometric traits are overt, leading thus to a threat of them being captured, copied, and forged. Numerous techniques have been developed over the years for biometric spoofing and anti-spoofing. The goal of this chapter is to provide a comprehensive overview on works in the field of spoofing and anti-spoofing with special attention to three mainly accepted biometric traits (i.e., fingerprint, face and iris) and multimodal biometric systems. We also present the key challenges, major issues and point out some of the salient and useful research directions.

INTRODUCTION

Due to exponential growth in digital information and communication technologies, the need and importance of robust user authentication is increasing day by day. Several efforts have been made to develop systems that can identify and authenticate genuine users. Authentication process validates the identity of user by utilizing one (or more) of the three-authentication factor - something user knows (the PIN or password), something user has (the card or keys), or something user is (the biometrics). Only biometrics among them exploits the distinct features associated with an individual, thus it could provide higher identification accuracy and security level (Jain, 2007).

Desirable properties of biometric characteristics are distinct for each user, temporal-invariance, and hard to be forged. But, recent research has demonstrated that biometric traits can be stolen, replicated and fake trait could be used to attack biometric systems (Matsumoto, 2002, Akhtar, 2012, Galbally, 2014). For instance, the Japanese border control fingerprint system was deceived in January 2009 by a woman,
who used tape-made fake fingerprints on her true fingerprints (Galbally, 2014, Akhtar, 2012). Similarly, just two days after the iPhone5s hit the market, it was fooled by a fingerprint spoof (Galbally, 2014). Unfortunately, one cannot change his or her biometric characteristics once it is stolen, unlike PIN’s and passwords. If someone’s biometric data is used illegally, they may face difficulty to prove their innocence.

Spoofing is a situation in which one person pretends as another by falsifying data and thereby gaining an illegal benefits. Biometric spoofing attack is a process by which individuals aim to compromise a biometric system by presenting a spoofed (fake) biometric sample of genuine user. Biometric spoofing attack is also referred as ‘direct attack’ as it is carried out directly on the biometric sensors. The most important point about biometric spoof attacks is that it does not require advanced technical skills and thus increases the number of potential attackers. Biometric spoof attacks also may be carried out in coordination with the genuine user to gain the delegate access rights or without user consent or knowledge (e.g., collected face images from surveillance cameras or latent fingerprints from objects or surfaces).

As we know that biometric traits are not secret. Everyone leaves their biometrics all over without being conscious that their biometrics can be captured, copied, and replicated, which later might possibly enable future acts of fraud. Therefore, to defeat spoofing attacks several countermeasure technologies and methods have been developed. In fact, the vulnerability of biometric systems to spoof attacks has generated a research trends to improve the robustness and reliability of biometrics such as anti-spoofing techniques or “liveness detection” (Li, 2009, Chingovska, 2013, Galbally, 2014) or multimodal biometric fusion (Jain, 2007, Akhtar, 2012).

Anti-spoofing method aims at automatically disambiguating real biometric traits presented to the sensor from synthetically produced artifacts imitating the genuine trait (Anjos, 2011, Lee, 2005, Chetty, 2005, Akhtar 2014). Anti-spoofing can be done in four different modes (see Figure 1.) (i) with available sensors detecting a pattern characteristic of attack in the signal; (ii) with dedicated sensors detecting an evidence of genuineness, which is not always feasible to deploy; (iii) with a challenge-response technique where an attack can be detected by asking user to interact with the system; or (iv) with recognition techniques intrinsically robust against presentation attacks if any. Anti-spoofing (liveness detection) methods may be software- or hardware-based. Software-based solutions are the most interesting and challenging ones, since they do not employ any additional and possibly invasive measurements such as blood pressure etc. Biometric anti-spoofing methods need to satisfy certain requirements: (i) non-invasive- neither harmful nor excessive contact with the user; (ii) user friendly- users are comfortable to use; (iii) fast- user interaction with system and computational time should be short; (v) performance- good spoof detection rate without drop in recognition performance (e.g., false rejection) of the biometric system. In this chapter, we present a comprehensive overview of the most representative techniques of spoof fabrications and their countermeasure for three widely used modalities (i.e., fingerprint, face and iris) and multimodal biometric systems.

Figure 1. Spoofing attacks are potentially detected by hardware/software-based anti-spoofing techniques.