Accuracy and Security of Fingerprint-Based Biometrics

Riyan Dubey

Abstract

Biometric systems are increasingly replacing traditional password- and token-based authentication systems. Security and recognition accuracy are the two most important aspects to consider in designing a biometric system. In this paper, a comprehensive review is presented to shed light on the latest developments in the study of fingerprint-based biometrics covering these two aspects with a view to improving system security and recognition accuracy. Based on a thorough analysis and discussion, limitations of existing research work are outlined and suggestions for future work are provided. It is shown in the paper that researchers continue to face challenges in tackling the two most critical attacks to biometric systems, namely, attacks to the user interface and template databases. How to design proper countermeasures to thwart these attacks, thereby providing strong security and yet at the same time maintaining high recognition accuracy, is a hot research topic currently, as well as in the foreseeable future. Moreover, recognition accuracy under non-ideal conditions is more likely to be unsatisfactory and thus needs particular attention in biometric system design. Related challenges and current research trends are also outlined in this paper.

Keywords: biometrics; security; template protection; recognition accuracy; latent fingerprint

Introduction

Biometrics is a technology that uses the unique patterns of physical or behavioral traits of users for authentication or identification. With biometric scanners on smartphones and other devices becoming more prevalent, as well as a growing number of services calling for high security and good customer experience, traditional methods of authentication (e.g., passwords and PINs) are increasingly being replaced by biometric technology. Passwords have some obvious drawbacks—they could be stolen, lost, or forgotten. In contrast, biometrics offer an alternative solution to the task of personalauthentication or identification based on biometric traits. To be forgotten or lost is impossible, and unlike passwords, they are hard to forge. There are some biometric traits that can be defined for an individual; for example, fingerprint, finger-vein, iris, voice, face, and so on.

Generally, a typical biometric system comprises four modules, namely, sensor module, feature extraction module, template database, and matching module. Specifically, the sensor module acquires the biometric image. A set of global or local features are extracted from the acquired biometric image by the feature extraction module. Structured feature representations are stored in the template database as template data. The matching module is responsible for comparing the query and template data to reach a match or non-match verdict. A typical biometric system carries out authentication in two stages
—the enrollment stage and verification stage—as shown in Figure 1. Take fingerprint recognition as an example. In the stage of enrollment, a user presents their finger to the fingerprint sensor and a fingerprint image is acquired by the sensor module. Certain features of the acquired fingerprint image are extracted, and further adapted or

transformed to generate template data for the purpose of comparison in the verification stage. In the verification stage, the fingerprint image of a query is collected by the sensor module. The feature representations of the query fingerprint image go through the same process as in the enrollment stage, so as to obtain query data. The query data are then compared with the template data so that a matching outcome is attained.

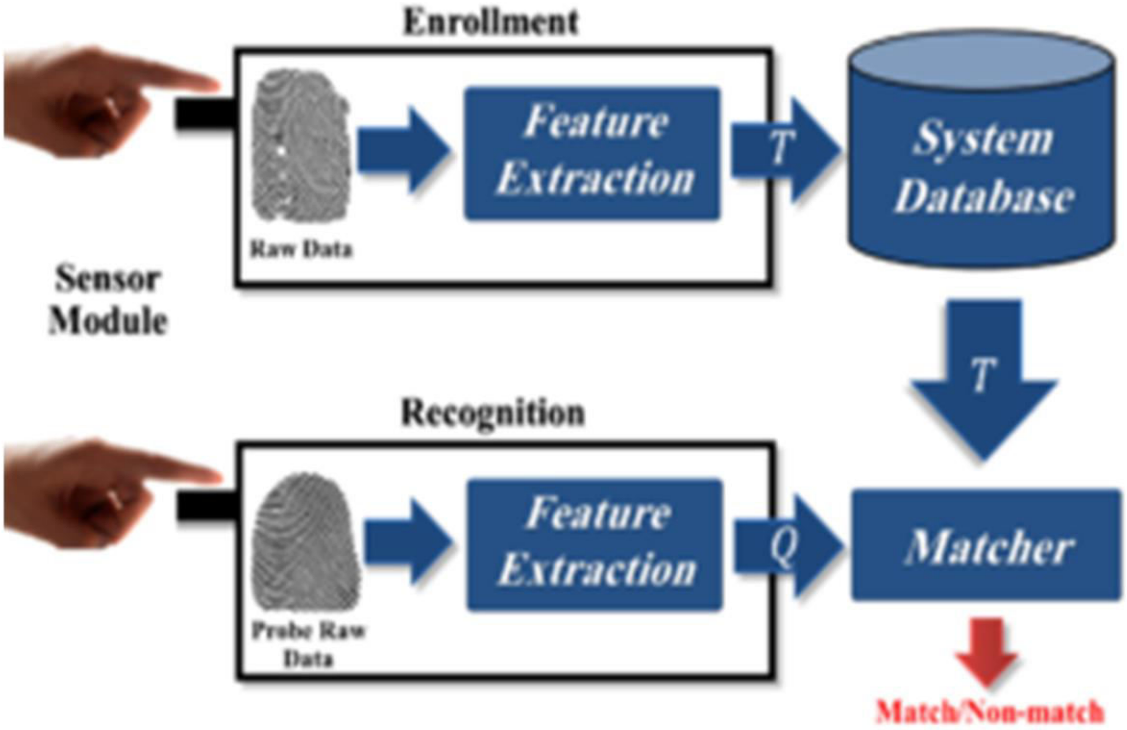

Figure 1. An example of two stages—enrollment and verification—in a biometric authentication system.

Due to some specific properties possessed by biometrics, biometric systems have been adopted in many civilian and military applications in the areas of law enforcement, border control, consumeror residential biometrics, and financial services.

(1) Law enforcement: Biometric technology has been embraced with open arms by law enforcement agencies across the world for its efficiency in security-oriented scenarios. In fact, biometrics is not a new tool in law enforcement. Fingerprint biometrics have been adopted by Argentinian criminologists for more than a century. Nowadays, with rapid technological development, biometrics have launched a worldwide revolution in law enforcement. Biometric recognition systems have now been utilized by law enforcement agencies of many countries, including the United States, United Kingdom, Australia, and China. For example, in 2011, the Department of Defense and the FBI started working on the United States' next generation biometric system, named Next Generation Identification (NGI), which is designed to include fingerprint, face, iris, and palm data, and their facial recognition program became fully operational in late 2014.

(2) Consumer biometrics: Consumer devices equipped with biometric systems are standalone products for the consumer market, such as door locks, surveillance systems, automotive, and especially mobile devices (smartphones, tablets, etc.). In the past, passwords were the only secure way of authentication, and fingerprint scanners were most likely used by law enforcement agencies and the military.

However, times have changed. In the last decade, biometric technology has developed in leaps and bounds and spread to every corner of our lives as a more secure method of authentication. With the popularity of smart phones, mobile phones utilizing biometrics is a winning combination in the consumer market, allowing biometric technology tobecome much more widely accepted.

(3) Financial services: Finance is the most mature biometrics market outside the domain of law enforcement for the logic that protecting money is the first priority for most people. Financial companies have been early adopters of biometrics. For example, cash machines with fingerprint readers are currently deployed at an increasing pace. Moreover, a new MasterCard, which includes an embedded fingerprint reader, attempts to introduce a biometric authentication layer for card payment, so as to enhance customers' comfort level in terms of security and convenience.

Compared with other biometric traits (e.g., face, iris, and voice), fingerprint-based recognition systems are studied most extensively and deployed most widely. For a fingerprint, the pattern of valleys and ridges is determined after birth, and different fingerprint patterns are owned by even identical twins. It has been reported that the recognition accuracy of fingerprint-based recognition systems is very high, with the general public showing medium acceptability to fingerprint acquisition. This is why fingerprint biometric systems occupy a large market share and have been adopted in various applications. Although fingerprint recognition shows substantial strength and a prosperous future, it has some unsolved issues, such as insufficient accuracy and security concerns.

In this paper, a comprehensive review is presented to shed light on the latest development in the study of fingerprint-based biometrics concerning two important aspects—security and recognition accuracy. The main contributions of this paper are highlighted as follows:

i. Security and recognition accuracy, despite being two most important aspects in biometric system design, have not been adequately studied simultaneously. Prior to this review paper, no research work has delivered a comprehensive review considering both of them. In this paper, up-to-date research and insights into security and recognition accuracy are thoroughly analyzed and discussed.

ii. Based on a thorough analysis, limitations of existing research are discussed and suggestions for future work to overcome those limitations are provided.

iii. The two most critical attacks to biometric systems are discussed in this paper. How to resolve the challenges, so as to defend biometric systems, is the focus of current and future biometricsecurity research.

iv. Most existing methods, either with or without template protection, were set forth in ideal situations. In this paper, we emphasize the importance of considering recognition accuracy under non-ideal conditions. Our analysis is backed by solid evidence and detailed comparison.

The rest of this paper is organized as follows. In Section 2, the security of biometrics is thoroughly analyzed from the perspective of attack points and countermeasures. In Section 3, system recognition accuracy under different conditions is discussed. The conclusion and future work is given in Section.

1. Security Analysis: Attacks and Countermeasures

Compared with password-based authentication systems, there are two major concerns over biometric systems. First, biometric traits cannot be revoked and reissued in the cases where they are compromised. For example, if a person’s fingerprint image is stolen, it is not possible to replace it like replacing a stolen password. Moreover, different applications might use the same biometric trait; if an adversary acquires an individual’s biometric trait in one application, they could also use it to gain access to other applications. Second, biometric traits are not secret. An individual could leave their fingerprint on any surface they touch. Ratha et al. identified eight different points of attacksin a biometric system, which is shown in Figure Attacks can be in various forms (e.g., phishing andfarming attacks, front- or back-end attacks), but they can generally be classified into four categories:

(a) Attacks at the interface, e.g., attacks at point 1;
(b) Attacks at the modules, e.g., attacks at points 3 and 5;
(c) Attacks to the channels between modules, e.g., attacks at points 2, 4, 7, and 8;
(d) Attacks to the template database, e.g., attacks at point 6.

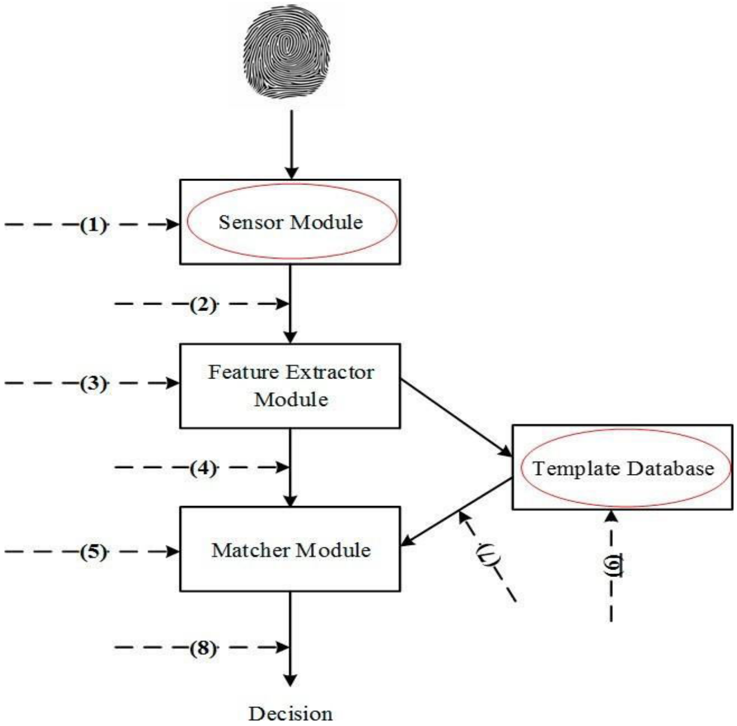

Figure 2. Eight possible attack points to a typical biometric authentication system (adapted from).

Here, threats and security issues related to those attack points in different stages of a generic biometric system are listed in Table. In light of the two major concerns mentioned above, in this paper we focus on the investigation of Attacks 1 and 11 (in Table) from attack categories a and d (labeled by the red circles in Figure, since they represent the most serious and critical threats to users' security and privacy.

2. Recognition Accuracy

Although biometric technology renders considerable benefits and is being used in many applications, it faces challenges, such as insufficient accuracy under non-ideal conditions or in the encrypted domain when template protection is implemented.

Biometric systems sometimes confront unrealistic expectations of achieving the matching accuracy of traditional password-based authentication systems. A password- based system always offers a crisp result—it grants access if the input password is a match, and vice versa. However, biometric matching cannot be 100% accurate. The accuracy of a biometric system can be evaluated by using well-known performance indicators, e.g., False Accept Rate (FAR), False Reject Rate (FRR), and Equal Error Rate (EER). Recognition accuracy generally depends on factors such as input image quality and matching algorithms. With decades of efforts from researchers, remarkable matching accuracy has been achieved and reported.

Conclusions

This paper gives a comprehensive review of two significant (and competing) measures for fingerprint-based biometric systems; that is, security and recognition accuracy. In regards to security, we have analyzed two categories of attacks: attacks to user interface and attacks to template databases. Countermeasures to defend against these attacks are also discussed. A total of 42 research articles in the area of biometric security (8 in liveness detection, 18 in cancelable biometrics, and 16 in biometric cryptography) are reviewed and discussed. In regards to recognition accuracy, in our opinion, although remarkable recognition accuracy has been attained, matching performance can still be unsatisfactory under some non-ideal conditions (e.g., latent fingerprint matching) or when the system security level is high. Since the requirements of system security impact recognition accuracy, it calls for the biometric system designers to carefully consider how to strike a good balance between recognition accuracy and security.

In view of the above issues, some latest research outcomes are analyzed and summarized in this paper. Despite the improvement in recognition accuracy under non- ideal conditions and recentadvances in biometric template protection, a number of open issues still exist, which call upon biometric researchers to resolve them. We highlight some research challenges and future directions in the following:

i. New developments in deep learning techniques have enhanced the performance of biometric systems across a wide range of biometric modalities, such as face recognition modality. We envisage that deep learning techniques will also be potential tools for latent fingerprint matching. However, the use of deep learning algorithms may bring potential threats to biometric systems because of the vulnerabilities of those deep learning algorithms themselves.

ii. The security issues (e.g., spoofing attacks, attacks to biometric templates) analyzed for a general biometric system are also valid to any biometric system on different platforms, for example, a mobile platform. Nowadays, smartphones are becoming more and more popular.