Chapter 20
Cancellable Biometrics for On-Line Signature Recognition

Emanuele Maiorana
Università degli Studi Roma TRE, Italy

Patrizio Campisi
Università degli Studi Roma TRE, Italy

Alessandro Neri
Università degli Studi Roma TRE, Italy

ABSTRACT

With the widespread diffusion of biometrics-based recognition systems, there is an increasing awareness of the risks associated with the use of biometric data. Significant efforts are therefore being dedicated to the design of algorithms and architectures able to secure the biometric characteristics, and to guarantee the necessary privacy to their owners. In this work we discuss a protected on-line signature-based biometric recognition system, where the considered biometrics are secured by applying a set of non-invertible transformations, thus generating modified templates from which retrieving the original information is computationally as hard as random guessing it. The advantages of using a protection method based on non-invertible transforms are exploited by presenting three different strategies for the matching of the transformed templates, and by proposing a multi-biometrics approach based on score-level fusion to improve the performances of the considered system. The reported experimental results, evaluated on the public MCYT signature database, show that the achievable recognition rates are only slightly affected by the proposed protection scheme, which is able to guarantee the desired security and renewability for the considered biometrics.

INTRODUCTION

The recent widespread diffusion of biometrics-based recognition systems is mainly due to the greater convenience, comfort and security they offer with respect to traditional authentication methods based on passwords or tokens. In fact, being derived from who a person is or what a person does, instead of from what a person knows or what a person has, biometric data represent

DOI: 10.4018/978-1-60960-515-5.ch020

identifiers which cannot be lost or forgotten, and represent irrefutable evidences linking a user to his identity (Jain, 2007).

However, the use of biometric data in an automatic recognition system also involves serious risks for their owners: if a biometrics is somehow stolen or copied, it can be difficult to replace it. Moreover, biometric data can contain sensitive information regarding, for example, the users' health or genetic background, which can be used in an unauthorized manner for malicious or undesired intents (Prabhakar, 2003). Moreover the users' privacy can be compromised if cross-matching between different biometric databases is performed, in order to track the enrolled subjects using their personal biometric traits. The aforementioned security and privacy concerns need to be carefully considered when implementing a biometric recognition system, by providing appropriate countermeasures to the possible attacks which can be perpetrated at the vulnerable points of the system (Ratha, 2001). Therefore some measures should be adopted to enhance biometric data resilience against attacks, while allowing the matching to be performed efficiently, thus guaranteeing acceptable recognition performance.

In this contribution, a protected on-line signature based verification system is proposed. Specifically, non-invertible transformations are applied to signature templates represented by time sequences, in order to guarantee the necessary security and to allow the generation of multiple templates from the same original one. The present work stems from the papers by the authors in (Maiorana, 2008c) and (Maiorana, 2008b), and exploits the characteristics of the employed protection scheme by presenting a protected multi-biometrics approach based on score-level fusion, which provides a significant improvement for the performances of the considered system. Specifically, the paper is organized as follows: in Section II the solutions which have been investigated in the recent past to secure biometric templates are analyzed. The non-invertible transformations employed to provide protection to the considered signature templates are described in Section III, while the details regarding the proposed protected on-line signature recognition system, including the strategies employed to match the transformed templates, are given in Section IV. The experimental framework and the obtained results are shown in Section V, and some conclusions are drawn in Section VI.

BIOMETRIC TEMPLATE SECURITY

Among the possible threats regarding users' privacy and security which have to be considered when designing a biometrics-based recognition systems, the unauthorized acquisition of the stored biometric data is probably the most dangerous one (Ratha, 2001). Therefore, many solutions have been investigated in the recent past to secure biometric templates. Among them, *cancelable biometrics* approaches have been introduced in (Ratha, 2001). These techniques apply intentional non-invertible and repeatable modifications to the original biometric templates. Specifically, a properly defined cancelable biometrics should satisfy the following requirements:

- **Security:** it should be impossible or computationally unfeasible to obtain the original biometric template from the transformed one;
- **Revocability:** it should be possible to revoke a compromised template and issue a new one based on the same biometric data;
- **Diversity:** each template generated from a biometrics should not match with others previously generated from the same data;
- **Performance:** the recognition performance of the protected system, in terms of False Rejection Rate (FRR) or False Acceptance Rate (FAR), should not degrade significantly with respect to an unprotected system.