Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters

C. Rathgeb*, C. Busch

da/sec Biometrics and Internet Security Research Group, Hochschule Darmstadt, Germany

ARTICLE INFO

Article history:
Received 9 July 2013
Received in revised form
6 November 2013
Accepted 29 December 2013

Keywords:
Biometrics
Security
Template protection
Cancelable biometrics
Multi-biometrics

ABSTRACT

In this work adaptive Bloom filter-based transforms are applied in order to mix binary iris biometric templates at feature level, where iris-codes are obtained from both eyes of a single subject. The irreversible mixing transform, which generates alignment-free templates, obscures information present in different iris-codes. In addition, the transform is parameterized in order to achieve unlinkability, implementing cancelable multi-biometrics. Experiments which are carried out on the IITD Iris Database version 1.0 confirm the soundness of the proposed approach, (1) maintaining biometric performance at equal error rates below 0.5% for different feature extraction methods and fusion scenarios and (2) achieving a compression of mixed templates down to 10% of original size.

1. Introduction

Research confirms an extraordinarily high level of statistical reliability for iris recognition systems (Daugman, 1993; Bowyer et al., 2007). Daugman's algorithm (Daugman, 2004), which forms the basis of the vast majority of today's iris recognition systems comprises four stages: (1) image acquisition, in which an image of a subject's eye is captured; (2) preprocessing, which involves the detection of the iris and unrolling of the iris to a normalized texture (3) feature extraction, in which binary feature vectors, i.e. iris-codes, are generated; and (4) feature comparison, where iris-codes are aligned applying circular bit shifts, and dis-similarity scores are estimated based on the fractional Hamming distance. Biometric recognition represents the strongest form of personal identification, however, physiological biometric characteristics are not secret and cannot be revoked or reissued causing several vulnerabilities that violate individuals' privacy, e.g. tracking subjects without consent. In addition, it has been demonstrated that spoofed iris images can be reconstructed from stored iris-codes (Venugopalan and Savvides, 2011).

Biometric template protection schemes (Rathgeb and Uhl, 2011) which are categorized as biometric cryptosystems (Uludag et al., 2004) and cancelable biometrics (Ratha et al., 2001) offer solutions to privacy preserving biometric authentication. Cancelable biometrics consist of intentional, repeatable distortions of biometric signals based on transforms that provide a comparison of biometric templates in the transformed domain, i.e. biometric templates are permanently protected. In accordance with the ISO/IEC IS 24745 (ISO/IEC JTC1 SC27 Security Techniques ISO/IEC 24745:2011, 2011) on biometric information protection, technologies of cancelable biometrics meet the two major requirements of irreversibility and unlinkability. On the one hand knowledge of the

* Corresponding author.
E-mail addresses: christian.rathgeb@h-da.de, crathgeb@gmail.com (C. Rathgeb), christoph.busch@h-da.de (C. Busch).

0167-4048/$ – see front matter © 2014 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2013.12.005

protected template can not be used to determine any information about the original biometric sample, while it should be easy to generate the protected template (irreversibility). On the other hand different versions of protected biometric templates can be generated based on the same biometric data, while protected templates should not allow cross-matching (unlinkability). The majority of existing approaches to cancelable biometrics report a significant decrease in biometric performance which is caused by two issues: (1) local neighborhoods of feature elements are obscured and (2) transformed enrollment templates are not “seen”, i.e. alignment can not be performed properly at the time of comparison (Rathgeb and Uhl, 2011). This implies, that low intra-class variability at high inter-class variability is considered a fundamental premise for biometric template protection schemes which can only be achieved in case biometric traits are acquired under favorable environmental conditions. In order to overcome this restriction, multi-biometric template protection schemes (Nagar et al., 2012; Rathgeb and Busch, 2012) have been introduced, since a combination of different biometric characteristics generally leads to higher accuracy (Ross and Jain, 2003). Within a conventional biometric system a fusion of different biometric information can be performed at various stages yielding feature level, score level, and decision level fusion (Ross et al., 2006), as defined in the ISO/IEC TR 24722 (ISO/IEC JTC1 SC37 Biometrics ISO/IEC TR 24722:2007, 2007) on multimodal and other multi-biometric fusion. While preliminary scores are not available within the vast majority of biometric cryptosystems, cancelable multi-biometric systems based on score level fusion can be constructed analog to conventional biometric systems. For both technologies biometric fusion based on decision level can easily be implemented combining final decisions. However, score and decision level fusion require a separate storage of protected templates, i.e., with respect to template protection, feature level has been identified as the only suitable level of fusion (Kelkboom et al., 2009). Performing multi-biometric template protection at feature level represents a great challenge since it requires a generic framework in order to establish a common representation of biometric features (Nagar et al., 2012). In addition, feature alignment turns out to be a critical issue since protected templates, which comprise information of more than one biometric instance, are expected to require a complex alignment process. So far, hardly any alignment-free (multi-biometric) template protection schemes have been proposed.

1.1. *Contribution of work*

The proposed work builds upon the approach we proposed in Rathgeb et al. (2013) and the concept of mixing multiple instances of a single biometric characteristic, which has been introduced in Othman and Ross (2013) for fingerprints. In Rathgeb et al. (2013) the basic concept of Bloom filter-based cancelable iris biometrics has been introduced, however, within the presented work emphasis is put on cancelable multi-biometrics which represents a more challenging task (Rathgeb and Busch, 2012), i.e. we significantly exented existing work according to several aspects, tackling the aforementioned issues. We demonstrate the feasibility of multi-biometric Bloom filter-based template protection by introducing the recently proposed concept of mixing biometric features, which originate from different biometric characteristics, into a single protected template, to iris biometrics. For this purpose we asses multi-instance single-algorithm and multi-instance multi-algorithm fusion scenarios in order to obtain alignment-free mixed templates. Binary iris-biometric feature vectors extracted from both eyes of a subject are mixed to a single protected template at feature level, which highly increases security while at the same time biometric performance is maintained. Implementing cancelable biometrics the proposed technique exhibits the properties of irreversibility and unlinkability (ISO/IEC JTC1 SC27 Security Techniques ISO/IEC 24745:2011, 2011).

1.2. *Organization of article*

The remainder of this article is organized as follows: related work with respect cancelable iris biometrics and multi-biometric template protection is briefly summarized in Sect II. In Sect. III the proposed mixing approach is described in detail. Experimental results are presented in Sect. IV. Finally, conclusions are drawn in Sect. V.

2. Related work

Biometric template protection schemes (Rathgeb and Uhl, 2011) are commonly classified as biometric cryptosystems and cancelable biometrics. Since the presented approach represents an instance of cancelable multi-biometrics, in this section we will merely focus on these technologies. Ratha et al. (Ratha et al., 2001) were the first to introduced the concept of cancelable biometrics. In their work the authors apply image-based block permutations and surface-folding in order to obtain revocable biometric templates. In further work (Zuo et al., 2008) the authors propose different techniques to generate cancelable iris biometrics based on non-invertible transforms and biometric salting, which are applied in image and feature domain. In order to preserve a computational efficient alignment of resulting iris-codes based on circular bit-shifting, iris textures and iris-codes are obscured in a row-wise manner, which means adjacency of pixels and bits is maintained along *x*-axis in image and feature domain, respectively. In Hämmerle-Uhl et al. (2009) block re-mapping and image wraping have been applied to normalized iris textures. For both types of transforms a proper alignment of resulting iris-codes is infeasible causing a significant decrease of biometric performance. In Ouda et al. (2010) several enrollment templates are processed to obtain a vector of consistent bits. Revocability is provided by encoding the iris-code according to a subject-specific random seed. In case subject-specific transforms are applied in order to achieve cancelable biometrics, these transforms have to be considered compromised during inter-class comparisons (Kong et al., 2006). Subject-specific secrets, be it transform parameters, random numbers, or any kind of passwords are easily compromised, i.e. performance evaluations have to be performed under the “stolen-secret scenario”, where each impostor is in possession of valid secrets. In Pillai et al. (2011)