Information Fusion 33 (2017) 71–85

Contents lists available at ScienceDirect

Information Fusion

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

Overview of the combination of biometric matchers

Alessandra Lumini[a,*], Loris Nanni[b]

[a] Department of Computer Science and Engineering (DISI), University of Bologna, via Sacchi, 3 47521 Cesena (FC), Italy
[b] Department of Information Engineering of the University of Padua, Via Gradenigo 6/b 35131 - Padova, Italy

ARTICLE INFO

Article history:
Received 12 November 2015
Revised 9 May 2016
Accepted 16 May 2016
Available online 18 May 2016

Keywords:
Biometric matchers
Fusion at score level
Unimodal biometrics
Multimodal biometrics

ABSTRACT

Biometric identity verification refers to technologies used to measure human physical or behavioral characteristics, which offer a radical alternative to passports, ID cards, driving licenses or PIN numbers in authentication. Since biometric systems present several limitations in terms of accuracy, universality, distinctiveness, acceptability, methods for combining biometric matchers have attracted increasing attention of researchers with the aim of improving the ability of systems to handle poor quality and incomplete data, achieving scalability to manage huge databases of users, ensuring interoperability, and protecting user privacy against attacks. The combination of biometric systems, also known as "biometric fusion", can be classified into unimodal biometric if it is based on a single biometric trait and multimodal biometric if it uses several biometric traits for person authentication.

The main goal of this study is to analyze different techniques of information fusion applied in the biometric field. This paper overviews several systems and architectures related to the combination of biometric systems, both unimodal and multimodal, classifying them according to a given taxonomy. Moreover, we deal with the problem of biometric system evaluation, discussing both performance indicators and existing benchmarks.

As a case study about the combination of biometric matchers, we present an experimental comparison of many different approaches of fusion of matchers at score level, carried out on three very different benchmark databases of scores. Our experiments show that the most valuable performance is obtained by mixed approaches, based on the fusion of scores. The source code of all the method implemented for this research is freely available for future comparisons[1].

After a detailed analysis of pros and cons of several existing approaches for the combination of biometric matchers and after an experimental evaluation of some of them, we draw our conclusion and suggest some future directions of research, hoping that this work could be a useful start point for newer research.

1. Introduction

Biometrics refers to technologies used to measure human physical or behavioral characteristics such as iris, face, fingerprints, retina, hand geometry, voice or signatures and using such measures to detect and recognize individuals. Biometric identity verification offers a radical alternative to passports, ID cards, driving licenses or PIN numbers in authentication. Since biometrics authentication uses unique physical traits, the user is not required to carry any additional ID document. Moreover, unlike most traditional authorization systems such as personal identification numbers (PINs), passwords, or ID card, biometric credentials cannot be lost, forgotten, guessed, or easily cloned. Most common biometric systems include an enrollment and an identification/verification phase. Enrollment consists in the acquisition by a scanner of a "live sample" of the biometric of the person to be identified, followed by processing and storing as a template. Verification involves matching a captured biometric sample against the enrolled template that is stored in order to identify/verify user identity [1].

Since the first elementary fingerprint recognition system was proposed in early 20 century, the research community has spent energy to find out new biometric modalities, that is any physical or behavioral characteristic which satisfies the conditions of universality, discriminative amongst the population, invariance against time, easily collectible and difficult to reproduce/cheat. Based on the above criteria, several distinctive traits have been identified [2]: physiological (e.g. fingerprint, face, iris), behavioral (e.g. signature, gait, voice), medico-chemical (e.g. DNA, ECG) and soft (e.g. height, gender, ethnicity).

* Corresponding author.
E-mail addresses: alessandra.lumini@unibo.it (A. Lumini), loris.nanni@unipd.it (L. Nanni).

[1] www.dei.unipd.it/node/2357

http://dx.doi.org/10.1016/j.inffus.2016.05.003
1566-2535/

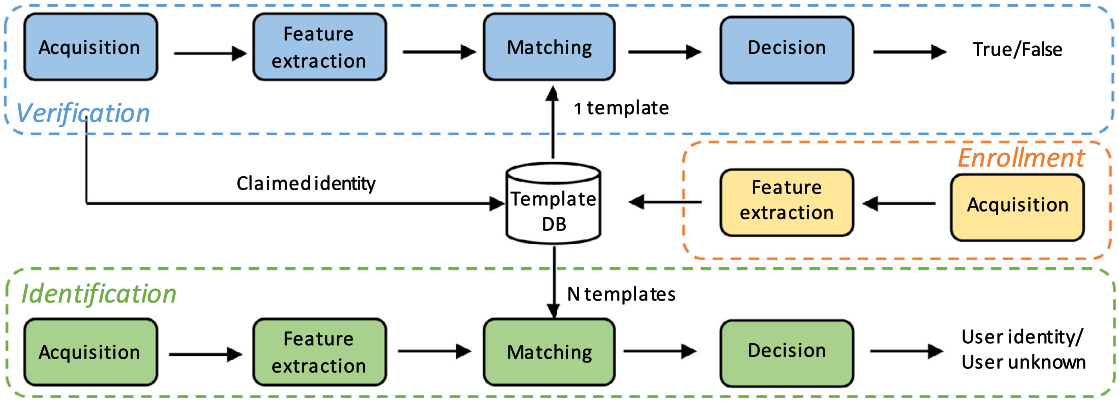

Fig. 1. General flow of a biometric system.

Biometric Identification is a One-to-Many matching of the captured biometric sample against all stored templates in order to determine a person's identity even without his/her knowledge or consent. For example, using a latent fingerprint to identify a criminal or scanning a crowd with a camera and using face recognition technology to find someone. In identification the user's biometric input is compared with the templates of all the persons enrolled in the database and the system outputs either the identity of the person whose template has the highest degree of similarity with the user's input or a rejection decision indicating that the user is not present in the DB. An extension to identification is *screening*, where the biometric system is called to guarantee that a particular individual does not belong to a watch list of identities.

Biometric Verification is a One-to-One matching of the captured biometric sample against the template of the person he/she claims to be, the identity claim is accepted as "genuine" if the degree of similarity is sufficiently high, as "impostor" otherwise. For example, fingerprint or retinal scans can be used to grant access to restricted areas or a bank account [1]. Many biometric applications (i.e. the FBI-IAFIS and US-VISIT IDENT program) work in the identification mode, and since the number of enrolled users can be very huge identification is significantly more challenging than verification.

Different biometric systems share a common general flow (Fig. 1), which is composed by four main components:

- *Acquisition module*: The first component of a biometric system is acquisition of the biometric data of an individual from a biometric sensor hardware. For face and iris images, the sensor is typically a camera, for fingerprints, the sensor is typically a scanner, for voice data, the sensor is a microphone. The quality of the acquisition module has a significant impact on the performance of the system which is sensitive to the environmental conditions (i.e. changes in brightness of an image), quality of sensor (i.e. dpi of the image), human factor (i.e. pose variations).
- *Feature extraction module*: The acquired data is pre-processed to remove noise or other abnormalities present and then subjected to the feature extraction process in order to extract biometrical values that ideally must describe uniquely an individual, so that biometric data collected from one individual, at different times, are "similar", while those collected from different individuals are "dissimilar". For example, the position and orientation of minutiae points in a fingerprint image are used in a fingerprint system. The features extracted during enrollment are stored in a template, which is a possibly small and easy to process. In order to improve interoperability among different biometric systems there exist proposals of standard format of templates, i.e. for fingerprint they are based only on minutiae points.
- *Matching module*: In this module, which is not used during enrollment, the feature values from an unknown individual are compared against those in the stored template by generating a matching score indicating the degree of similarity between a pair of biometrics data. The score should be high for features from the same individuals and low for those from different ones. For example in a fingerprint system, the number of matching minutiae points between the query and the template can be returned as a matching score. Usually matching is a difficult pattern-recognition problem due to large intra-class variations (caused by bad acquisition, noise, different environmental condition, distortions, etc.) and large inter-class similarity (i.e. differencing identical twins is very difficult in face recognition).
- *Decision component*: In this module the user's identity is established (identification) or a claimed identity is accepted/rejected (verification) based on the matching score. Usually the final decision is taken by comparing the matching score to a fixed threshold, which is selected according to consideration about the degree on security required by the application.

Unfortunately biometric systems also presents several limitations which in some cases make the performance of one single biometric modality insufficient for the related application in terms of accuracy, universality, distinctiveness, acceptability. Main limitations of biometric systems [3] are related to *(i)* variable environmental conditions (i.e. noise, changes in illumination, pose) which may heavily affect the accuracy of the system, in particular when acquisition is not performed in constrained conditions, *(ii)* large intra-class variations caused by acquisition in different conditions or aging effects, *(iii)* non-universality of some biometric credential due to illness or disabilities, *(iv)* spoof attacks that are performed by falsifying a biometric trait and then presenting this falsified information to the biometric system.

In order to overcome such limitations, methods for combining biometric matchers have attracted increasing attention of researchers [4] with the aim of improving the ability of systems to handle poor quality and incomplete data, achieve scalability to manage huge databases of users, ensure interoperability and protect user privacy against attacks. The combination of biometric systems, also known as "biometric fusion", can be classified into two groups [5]: unimodal biometric systems perform person recognition based on a single source of biometric information which is processed using different approaches, multimodal biometric systems acquire and use several biometric traits for person authentication. Some samples of possible sources of information, in a unimodal and a multimodal system, are depicted in Fig. 2.