Expert Systems with Applications 39 (2012) 1837–1847

Contents lists available at SciVerse ScienceDirect

Expert Systems with Applications

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

Genetic programming for multibiometrics

Romain Giot *, Christophe Rosenberger

GREYC Laboratory, ENSICAEN, University of Caen, CNRS, 6 Boulevard Maréchal Juin, 14000 Caen Cedex, France

ARTICLE INFO

Keywords:
Multibiometrics
Genetic programming
Score fusion
Authentication

ABSTRACT

Biometric systems suffer from some drawbacks: a biometric system can provide in general good performances except with some individuals as its performance depends highly on the quality of the capture… One solution to solve some of these problems is to use multibiometrics where different biometric systems are combined together (multiple captures of the same biometric modality, multiple feature extraction algorithms, multiple biometric modalities…). In this paper, we are interested in score level fusion functions application (i.e., we use a multibiometric authentication scheme which accept or deny the claimant for using an application). In the state of the art, the weighted sum of scores (which is a linear classifier) and the use of an SVM (which is a non linear classifier) provided by different biometric systems provide one of the best performances. We present a new method based on the use of genetic programming giving similar or better performances (depending on the complexity of the database). We derive a score fusion function by assembling some classical primitives functions (+,∗,−,…). We have validated the proposed method on three significant biometric benchmark datasets from the state of the art.

1. Introduction

1.1. Objective

Every day, new evolutions are brought in the biometric field of research. These evolutions include the proposition of new algorithms with better performances, new approaches (cancelable biometrics, soft biometrics,…) and even new biometric modalities (like finger knuckle recognition (Kumar & Zhou, 2009), for example). There are many different biometric modalites, each classified among three main families (even if we can find a more precise topology in the literature):

- *biological*: recognition based on the analysis of biological data linked to an individual (e.g., DNA analysis Hashiyada, 2004, the odor Korotkaya, 2003, the analysis of the blood of different physiological signals, as well as heart beat or EEG Riera, Soria-Frisch, Caparrini, Grau, & Ruffini, 2008);
- *behavioural*: based on the analysis of an individual behaviour while he is performing a specific task (e.g., keystroke dynamics Gaines, Lisowski, Press, & Shapiro, 1980, online handwritten signature Fierrez & Ortega-Garcia, 2008, the way of using the mouse of the computer Weiss, Ramapanicker, Pranav, Noble, & Immohr, 2007, voice recognition Petrovska-Delacretaz, El Hannani, & Chollet, 2007, gait dynamics (way of walking) Nandini & Kumar, 2008 or way of driving Benli, Duzagac, & Eskil, 2008);
- *morphological*: based on the recognition of different particular physical patterns, which are, for most people, permanent and unique (e.g., face recognition Turk & Pentland, 1991, fingerprint recognition Maltoni, Jain, & Prabhakar, 2009, hand shape recognition Kumar & Zhang, 2006, or blood vessel Xu, Guo, Hu, & Cheng, 2005,…).

Nevertheless, there will always be some users for which a biometric modality (or method applied to this modality) gives bad results, whereas, they are better in average. These low performances can be implied by different facts: the quality of the capture, the instant of acquisition and the individual itself but they have the same implication (impostors can be accepted or user need to authenticate themselves several times on the system before being accepted). Multibiometrics allow to solve this problem while obtaining better performances (i.e., better security by accepting less impostors and better user acceptance by rejecting less genuine users) and by expecting that errors of the different modalities are not correlated. In this paper, we propose a generic approach for multibiometric systems.

We can find different types of biometric multimodalites (Ross, Nandakumar, & Jain, 2006). They use:

1. different sensors of the same biometric modality (i.e., capacitive or resistive sensors for fingerprint acquisition);

* Corresponding author.
E-mail addresses: romain.giot@ensicaen.fr (R. Giot), christophe.rosenberger@ensicaen.fr (C. Rosenberger).

0957-4174/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.eswa.2011.08.066

2. several different representations for the same capture (i.e., use of points of interest or texture for face or fingerprint recognition);
3. different biometric modalities (i.e., face and fingerprint recognition);
4. different instances of the same modality (i.e., left and right eye for iris recognition);
5. multiple captures (i.e., 25 images per second in a video used for face recognition);
6. an hybrid system composed of the association of the previous ones.

We are interested in the first four cases in this paper. Our objective is to automatically generate fusion functions which combine the scores provided by different biometric systems in order to obtain the most efficient multibiometrics authentication scheme.

1.2. Background

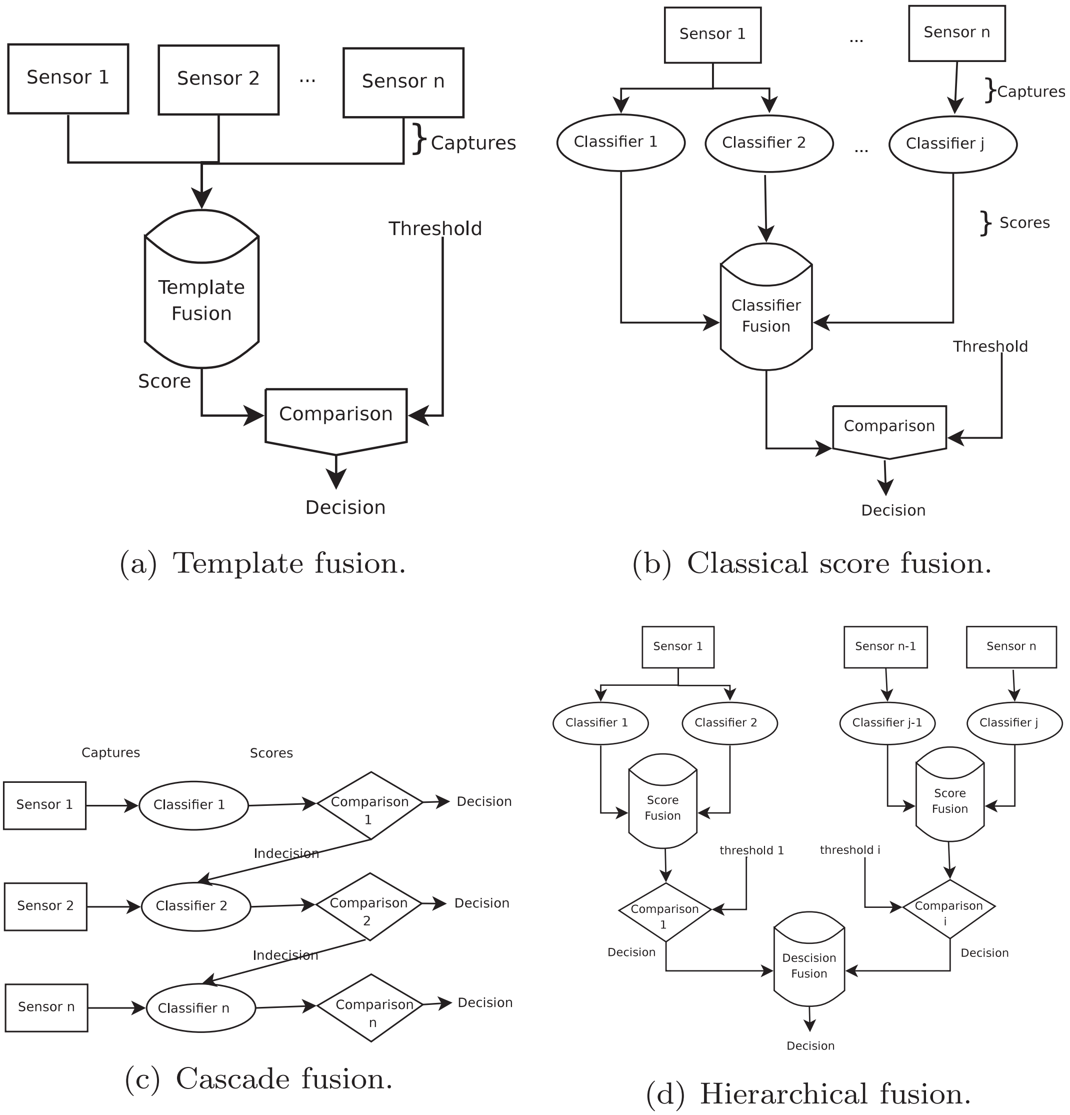
1.2.1. Performance evaluation

In order to compare different multibiometrics systems, we need to present the how to evaluate them. Several works have already done on the evaluation of biometric systems (Theofanos, Stanton, & Wolfson, 2008; ISO, 2006). Evaluation is generally realized within three aspects:

- *performance*: it has for objective to measure various statistical criteria on the performance of the system (*Capacity* Bhatnagar & Kumar, 2009, *EER*, *Failure To Enroll (FTE)*, *Failure To Acquire (FTA)*, computation time, *ROC* curves, etc. ISO, 2006);
- *acceptability*: it gives some information on the individuals' *perception*, *opinions* and *acceptance* regarding the system;
- *security*: it quantifies how well a biometric system (algorithms and devices) can resist to several types of logical and physical attacks such as Denial of Service (DoS) attack.

In this paper, we are only interested in performance evaluation (because the fusion approach is not modality dependant and perception and security depend on the used modalities). The main performance metrics are the following ones:

- *FAR (False Acceptance Rate)* which represents the ratio of impostors accepted by the system;
- *FRR (False Rejection Rate)* which represents the ratio of genuine users rejected by the system;



(a) Template fusion.

(b) Classical score fusion.

(c) Cascade fusion.

(d) Hierarchical fusion.

Fig. 1. Illustration of different fusion mechanisms.