Pattern Recognition Letters 37 (2014) 151–160

Contents lists available at SciVerse ScienceDirect

Pattern Recognition Letters

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

Analysis of unsupervised template update in biometric recognition systems

Luca Didaci *, Gian Luca Marcialis, Fabio Roli

Department of Electrical and Electronic Engineering, University of Cagliari, Piazza d'Armi, 09123 Cagliari, Italy

ARTICLE INFO

Article history:
Available online 1 June 2013

Keywords:
Biometrics recognition
Adaptive systems
Face
Fingerprint
Multi-modal biometrics
Path-based clustering

ABSTRACT

Performance of mono- and multi-modal biometric systems depends on the representativeness of enrolled templates. Unfortunately, error rate values estimated during the system design are subject to variations due to several aspects: intra-class variations arising on small-medium time-window, and ageing, which is the natural process involving any biometrics. This causes the increase of the False Rejection Rate (genuine users are no more recognized) or the False Acceptance Rate (impostors are misclassified as genuine users), or both. In fact, several vendors strongly suggest to repeat enrolment sessions in order to collect, over time, a set of templates representative enough. As alternative, automatic template update algorithms, which exploit the own-knowledge of the mono- or multi-modal biometric system, on a batch of samples collected during system operations without the human supervision, have been proposed.

Preliminary experimental results have shown that these algorithms are promising, but the motivation of their behaviour has not yet been explained. This paper is aimed to fill such gap, by showing that behaviour of self- and co-update may be explained by exploiting the concept of *path-based clustering*. Therefore, problems as 'intra-class' variations and ageing are dependent on the path-based cluster followed by each algorithm. Moreover, we show that the performance of co-update is superior than that of self-update, by a simulative model. The path-based clustering theory applied to self- and co-update algorithms, as well as the proposed model, are experimentally validated on the large DIEE Multimodal data set, the only one publicly available and explicitly conceived for comparing template update algorithms.

1. Introduction

In biometric verification systems, the identity of the user, also called 'client' or 'genuine user', is stored and associated to the related template(s).

Biometric templates are structural or statistical representations of the client's biometric obtained by image or signal processing techniques (Jain et al., 2008). The client's biometric is initially given by images or signals acquired by a certain sensor (face snapshot, voice registration, fingerprint image). The acquisition and computation phase is called 'enrolment'. Templates are stored into the system's data set, and used for comparison with novel input images or signals during system's operations.

Among open problems, updating of 'templates' is crucial (Jain et al., 2008; Infosecurity, 2008). In particular, an appropriate selection of template(s) may increase the system performance, in terms of False Rejection Rate (FRR: percentage of genuine users not recognized) or false acceptance rate (FAR: percentage of unknown users, also called impostors, misclassified as genuine users).

Beside additional enrolment sessions, recent works argued that the genuine/impostor labelling could be done by the matcher itself, thus avoiding human or semi-automatic supervision. Algorithms which perform such labelling, and, consequently, allow to add into the client gallery novel samples as templates, are called 'template update algorithms'. These approaches are inspired from machine learning methods called 'self-training' and 'co-training' (Zhu, 2006; Blum and Mitchell, 1998). In order to keep this link, authors have called them 'self updating' and 'co-updating', respectively (Roli et al., 2008). Therefore, the authors have proposed the application of self- and co-training to biometrics (Roli and Marcialis, 2006; Roli et al., 2007), for which an *ad hoc* analysis is necessary.

Main assumptions adopted by Blum and Mitchell (1998) are compatibility between classifiers, sufficiency of the views and independence between the views. Sufficiency and compatibility refers to the fact that, when provided with a *sufficient* number of training patterns, each view is sufficient for a correct classification (sufficiency) and classifiers agree on the label to be assigned (compatibility). Independence will be discussed in Section 2. In general, several authors have theoretically or empirically investigated a number of aspects of co-training, by focusing on how it works under different and less restrictive assumptions than those adopted by Blum and Mitchel. See, for example, Didaci and Roli (2012), Du et al. (2011), Zhou et al. (2007) and Didaci et al. (2012).

* Corresponding author. Tel.: +39 070 675 5844; fax: +39 070 675 5900.
E-mail addresses: luca.didaci@diee.unica.it (L. Didaci), marcialis@diee.unica.it (G.L. Marcialis), roli@diee.unica.it (F. Roli).

0167-8655/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.patrec.2013.05.021

The current state-of-the-art on self- and co-update is lacking of an analogous literature in biometric applications, that's means that there are no papers, to the best of our knowledge, where the self- and co-training algorithms were specifically adapted for the application, or an *ad hoc* theory has been developed. With regard to biometric applications, previous papers investigated the effect of the typology of enrolled clients on self-update in the sense of the Doddington's zoo (Doddington et al., 1998; Rattani et al., 2009), and benefits have been pointed out for clients intrinsically prone to low FRR. However, experiments were performed on a face data set made up of very low intra-class variations, thus conclusions were not definitive. Also, an experimental analysis of the self-update performance over time has been done in Marcialis et al. (2008) and Rattani et al. (2011), where this algorithm has shown to maintain the system EER stable over time, with respect to a non-adaptive biometric system. However, no specific theoretical study has gone in depth on the differences between self- and co-update. Although some preliminary papers (Didaci et al., 2008, 2009) have tried to model the co-update behaviour, whilst other ones (Roli et al., 2007; Rattani et al., 2008) have compared self-update and co-update experimentally on small data sets, none of them is able to give general insights about the motivation of their functioning. An *ad hoc* study is thus necessary to confirm previous achievements.

This is the aim of the present paper. First, contributions to the state-of-the-art are given in terms of a conceptual explanation of the behaviour of both algorithms according to the *path-based clustering* method. Second, an analytical model for the co-update algorithm, inspired from the above concepts, is proposed. Third, the model is used to analytically show that co-update algorithm is much more efficient than the self-update algorithm in terms of performance and number of acquired representative templates.

The conceptual explanation and the proposed model can be adapted to any self-update and co-update methods where classification systems are based on template matching, where each pattern admits two different representations (feature spaces), and the independence among matchers can be assumed. The experimental validation has been done on the case-study of bi-modal biometric verification systems, but without loss of generality.

Experimental evidences supporting our claims are carried out the data set collected at DIEE Laboratories, which, to the best of our knowledge, is the only one non-chimerical[1] multi-modal data set publicly available explicitly conceived for adaptive biometric systems.

Rest of the paper is organized as follows. Section 2 describes self-update and co-update algorithms. Section 3 performs a theoretical analysis of self and co-update performance by exploiting the path-based clustering approach. Experiments are presented in Section 4. Conclusions are drawn in Section 5.

2. Algorithms summary

In order to make better understandable the aims of this paper, we briefly describe self-update and co-update algorithms. They must be performed for each client stored in the system database.

For sake of clarity, we refer to face and fingerprint biometrics. In all cases, biometric verification systems are the focus of this work. When a person submit her/his biometric (e.g. face) and claims a certain identity, the system acquires the biometric signal and extracts a statistical or structured set of features. This set is compared to the template, an analogous set of features stored in the system memory after the registration process. These two feature sets are compared and a match score is computed. Match score is the similarity level among compared feature sets. It can be derived by evaluating the distance from two statistical feature sets (Turk and Pentland, 1991), or defining an appropriate metric from two structural representation (NIST, 2012; Jain et al., 1997; Wiskott et al., 1997). Good surveys on methods for evaluating the match score of fingerprint and face templates can be found in Maltoni et al. (2003) and Li and Jain (2005).

Self-update algorithm is based on uni-modal systems, that is, one view correspondent to the available biometric (e.g. fingerprint images). Co-update algorithm is base on bi-modal systems, where two views correspond to two biometrics. In this case, a sample is made up of a couple of biometric samples (fingerprint and face image of the client). Algorithms and conclusions remain valid even in other applications that admit two 'views', where the base classifier is a matcher and the independence assumptions hold true (e.g. camera and radar measurements for obstacles detection).

Self-update algorithm.

For each client stored in the system memory:

1. A batch of biometric samples B whose size is $|B| = N_{TOT}$ is collected during a certain time period.
2. A subset of k samples ($k \leqslant N_{TOT}$) is extracted with re-insertion from B and submitted to the system.
3. The system tries to verify the claimed identity for each of the k samples. The verified samples are added to the client's gallery.
4. Steps 2–3 are repeated until a certain stop criterion is met.[2]

Co-update algorithm.

The co-update algorithm works under the following hypothesis: two biometric traits are conditionally independent given the identity (Blum and Mitchell, 1998). For each couple of biometric samples $\{x^{(1)}, x^{(2)}\}$ from the same individual:

$$p\left(x^{(1)} = \hat{x}^{(1)} | x^{(2)} = \hat{x}^{(2)}\right) = p\left(x^{(1)} = \hat{x}^{(1)}\right) \tag{1}$$

$$p\left(x^{(2)} = \hat{x}^{(2)} | x^{(1)} = \hat{x}^{(1)}\right) = p\left(x^{(2)} = \hat{x}^{(2)}\right) \tag{2}$$

In other words, the probability that $x^{(1)}$ assumes a particular value $\hat{x}^{(1)}$ is independent on the value of $x^{(2)}$ (and vice versa). Eqs. (1) and (2) require that, for biometrics from the same individual, the appearance of the first and the second biometrics are independent each others. This assumption is met if there is no correlation among biometrics at hand.

The co-update algorithm description is given in the following. Let us call "master" the biometric that assumes the supervisors role, and "slave" the biometric whose gallery is augmented thanks to the master biometric, as suggested in Didaci et al. (2008, 2009, 2011)[3]:

1. A batch of biometric samples pairs B whose size is $|B| = N_{TOT}$ is collected during a certain time period.
2. A subset of k samples ($k \leqslant N_{TOT}$) is extracted with re-insertion from B and submitted to the system.
3. The system tries to verify the claimed identity for each of the k samples, using the master matcher. If the claimed identity is verified, the 'Slave' sample is added to the client's slave gallery.
4. Master and slave matchers roles are inverted.
5. Steps 2–4 are repeated until a certain stop criterion is met.[4]

[1] A chimerical biometric dataset is a dataset in which biometrics 1 came from a set of people, and biometrics 2 came from another, different, set.

[2] Usually, the adopted stop criterion refers to a certain number of iterations.

[3] In the following, the terms Master and Slave will be used for indicating: the biometric roles, and also related galleries, matchers and performance. For example: master gallery means the gallery of the master biometrics).

[4] Usually, the adopted stop criterion refers to a certain number of iterations.