Information Sciences 315 (2015) 67–87

Contents lists available at ScienceDirect

Information Sciences

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

A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation

Daniel Peralta [a], Mikel Galar [c], Isaac Triguero [d,a], Daniel Paternain [c], Salvador García [a,b,*], Edurne Barrenechea [c], José M. Benítez [a], Humberto Bustince [c], Francisco Herrera [a]

[a] Dept. of Computer Science and Artificial Intelligence, University of Granada, 18071 Granada, Spain
[b] Faculty of Computing and Information Technology – North Jeddah, King Abdulaziz University, 21589 Jeddah, Saudi Arabia
[c] Departamento de Automática y Computación, Universidad Pública de Navarra, Pamplona, Spain
[d] Inflammation Research Center, a VIB-UGent Dept. UGent Dept. of Internal Medicine, Respiratory Medicine (GE01), Technologiepark 927, B-9052 Zwijnaarde, Belgium

ARTICLE INFO

Article history:
Received 29 September 2014
Received in revised form 8 January 2015
Accepted 9 April 2015
Available online 16 April 2015

Keywords:
Biometrics
Fingerprint verification
Fingerprint identification
Local matching
Minutiae

ABSTRACT

Fingerprint recognition has found a reliable application for verification or identification of people in biometrics. Globally, fingerprints can be viewed as valuable traits due to several perceptions observed by the experts; such as the distinctiveness and the permanence on humans and the performance in real applications. Among the main stages of fingerprint recognition, the automated matching phase has received much attention from the early years up to nowadays. This paper is devoted to review and categorize the vast number of fingerprint matching methods proposed in the specialized literature. In particular, we focus on local minutiae-based matching algorithms, which provide good performance with an excellent trade-off between efficacy and efficiency. We identify the main properties and differences of existing methods. Then, we include an experimental evaluation involving the most representative local minutiae-based matching models in both verification and evaluation tasks. The results obtained will be discussed in detail, supporting the description of future directions.

1. Introduction

Automatic fingerprint recognition has been one of the most known and used biometric authentication systems during the last decades. It has been used for personal verification and identification with great achievements [76]. A vast number of applications incorporate fingerprint recognition as basics, such as forensics, building accessing, ATM authentication or secure payment [113]. There are some other human characteristics that can be used as traits of a biometric system, such as the person's face, the retina or iris [16] and the voice. There is no trait that highlights as the best one. However, on average, fingerprints offer good capabilities in all properties analyzed by the experts and excellent results in distinctiveness [126],

* Corresponding author at: Dept. of Computer Science and Artificial Intelligence, University of Granada, 18071 Granada, Spain. Tel.: +34 958 240598; fax: +34 958 243317.

E-mail addresses: dperalta@decsai.ugr.es (D. Peralta), mikel.galar@unavarra.es (M. Galar), Isaac.Triguero@irc.vib-UGent.be (I. Triguero), daniel.paternain@unavarra.es (D. Paternain), salvagl@decsai.ugr.es (S. García), edurne.barrenechea@unavarra.es (E. Barrenechea), J.M.Benitez@decsai.ugr.es (J.M. Benítez), bustince@unavarra.es (H. Bustince), herrera@decsai.ugr.es (F. Herrera).

http://dx.doi.org/10.1016/j.ins.2015.04.013
0020-0255/

permanence and global performance [113]. Although the recognition is not as accurate as with other traits, it provides a good balance between accuracy, speed, resource requirements and robustness.

Independent of the type of task, either verification [72] (one-to-one comparison) or identification (search for an input fingerprint in a database) [80], it is necessary to perform a sequence of operations to build a template database and later use the system. Assuming that there is a database and that proper enrollments have been previously taken, the order of the operations for both tasks is given by: a capture of the fingerprint, a feature extraction stage, a matching and a pre-selection or filtering [85] (which is associated to identification tasks only). The capture of the fingerprint obtains an image that is not usually stored as such in the database. Instead, a feature extraction process is applied to obtain up to three levels of features [60]: level 1 features provide, at the global level, information of singular points and ridge line flow or orientation; level 2 features, at a local level, refer to minutiae details which usually correspond to bifurcations and ridge endings; and level 3 features, at the very-fine level, include features inside the ridges such as width, shape, curvature and dots. These features are only observable in high resolution images.

Once a set of features is extracted from the fingerprint image, the final goal is to find (or confirm) the identity of a person whose fingerprint has been previously enrolled into the system. The matching mechanism is the responsible to provide a likeliness score between two fingerprints. Most of the efforts in matching are with the use of minutiae details, although there are other types of matching methods based on correlations of images, other types of features and even on level 3 features. Minutiae matching consists of finding the alignment between two templates that results in the maximum number of minutiae pairings. Furthermore, minutiae matching can be classified as local or global [81], aligned or not [189], etc.; all the categories will be detailed in this paper.

Many fingerprint matching algorithms have been proposed in the literature, and the operations with features they use are sometimes similar or even repeated. In spite of the existence of some reviews on the topic, such as [174,113,71], they are not explicitly focused on matching and the characteristics of the methods are not completely studied or categorized. This issue may lead to a lack of unification and even to propose very similar matching methods in the future. Moreover, there are few attempts to empirically compare them.

In this sense, the motivation of this paper can be segregated into three main objectives:

- To gather and briefly describe all the matching methods proposed in the specialized literature.
- To offer an entire taxonomy based on the main processes and properties observed in the matching methods. It allows us to understand the reasons to choose the most suitable matching algorithm depending on the circumstances.
- To conduct an empirical study analyzing the most important local minutiae-based matching algorithms in terms of accuracy and speed throughput when they are applied to both verification and identification tasks.

The rest of this paper is organized as follows. Section 2 provides the necessary background in fingerprint minutiae matching. In Section 3, we introduce the main properties and the taxonomy for the matching methods. Next, Section 4 overviews the current trends in fingerprint matching. In Section 5, experiments on several data sets compare some of the most important local minutiae-based matching methods. Finally, Section 6 concludes the paper, including some original opinions for instruction in theory and application and future research directions. Additional material to the paper can be found at http://sci2s.ugr.es/MatchingReview/.

2. Background in fingerprint minutiae matching

Fingerprint matching is a crucial step in both verification and identification problems. Roughly, a fingerprint matching algorithm compares two fingerprints and returns either a degree of similarity (a real number bounded into an interval) or a dichotomic output (matched or non-matched). Hereafter, we use the representation of the fingerprint acquired by enrollment as the template (T) and the representation of the input fingerprint (I). Two fingerprints are called *genuine* if they represent the same finger, and *impostor* when they are different.

Several factors make fingerprint matching a very challenging problem [113]: image noise, skin condition, distortions, rotations, displacement, etc. There are two well-known properties in fingerprints: large variability in different impressions of the same finger (large *intra-class* variations) and much similarity between two images from different fingers (small *inter-class* variations).

The most popular and used technique is the minutiae-based matching. Subsequent subsections will detail the main concepts of minutiae-based matching (Section 2.1), including the distinction between global and local matching (Section 2.2) and feature extraction techniques that are commonly used to obtain the minutiae for matching (SubSection 2.3).

2.1. Minutiae-based matching

The output of a minutiae extraction stage is, at least, a set of minutiae. Each minutia is represented by its location coordinates and orientation angles, forming a 3-tuple $M = (x, y, \theta)$. T and I fingerprints have m and n minutiae, respectively. A minutia M_j in I is considered matched with a minutia M_i in T when it falls within the tolerance box of M_i. The tolerance