IJCSC Volume 4 • Number 2 September 2013 pp.166-170 ISSN-0973-7391

Authenticity of Fingerprint as Biometric Traits

Dr. Chander Kant, Archana Toky
Assistant Professor, Deptt. of computer Science & Appl. K.U. Kurukshetra
Faculty, Deptt. Of Computer Science, Govt. College for women, Hisar
ckverma@rediffmail.com, archanatoky@gmail.com

Abstract: Biometric recognition or, simply, biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. By using biometrics, it is possible to confirm or establish an individual's identity based on "who he is," rather than by "what he possesses" (e.g., an ID card). Among all the biometric techniques, fingerprint-based identification is the oldest method, which has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points.
Keywords: Biometrics, identification, multimodal biometrics, recognition, verification.

1. Introduction

The problem of resolving the identity of a person can be categorized into two types [1]: (i) verification and (ii) identification, Verification (authentication) refers to the problem of confirming or denying a person's claimed. Identification refers to the problem of establishing a subject's identity. Typically, a person could be identified based on (i) a person's possession ("something that you possess"), e.g., permit physical access to a building to all persons whose identity could be authenticated by possession of a key; (ii) person's knowledge of a piece of information ("something that you know"), e.g., permit login access to a system to a person who knows the user-id and a password associated with it. Another approach to positive identification is based on identifying physical characteristics of the person. The characteristics could be either a person's physiological traits, e.g., fingerprints, hand geometry, etc. or her behavioral characteristics, e.g., voice and signature. This method of identification of a person based on his/her physiological/behavioral characteristics is called *biometrics* [2]. Since the biological characteristics can not be forgotten (like passwords) and can not be easily shared or misplaced (like keys), they are generally considered to be a more reliable approach to solving the personal identification problem [3].

Fingerprints as a Biometric

A smoothly flowing pattern formed by ridges and furrows on the hand is called a palmprint. A fingerprint is believed to be unique to each person. Fingerprints of even identical twins are different [4]. Fingerprints are one of the most mature biometric technologies and are considered legitimate proofs of evidence in courts of law all over the world. Fingerprints are, therefore, used in forensic divisions worldwide for criminal investigations. More recently, an increasing number of civilian and commercial applications are either using or actively considering to use fingerprint-based identification because of a better understanding of fingerprints as well as demonstrated matching performance than any other existing biometric technology.

Fingerprint Representation

Fingerprint representations are of two types [5]: local and global. Major representations of the local information in fingerprints are based on the entire image, finger ridges, pores on the ridges, or salient features derived from the ridges. Representations predominantly based on ridge endings or bifurcations (collectively known as minutiae (see Figure 1)) are the most common, primarily due to the following reasons: (i) minutiae capture much of the individual information, (ii) minutiae-based representations are storage efficient, and (iii) minutiae detection is relatively robust to various sources of fingerprint degradation. Typically, minutiae-based representations rely on locations of the minutiae and the directions of ridges at the minutiae location.

Figure 1: Ridge ending and ridge bifurcation.

Fingerprint Classification

Large volumes of fingerprints are collected and stored everyday in a wide range of applications, including forensics, access control, and driver license registration. Automatic identity recognition based on fingerprints requires that the input fingerprint be matched with a large number of fingerprints stored in a database [6]. To reduce the search time and computational complexity, it is desirable to classify these fingerprints in an accurate and consistent manner such that the input fingerprint needs to be matched only with a subset of the fingerprints in the database. Fingerprint classification is a technique used to assign a fingerprint into one of the several pre-specified types already established in the literature (and used in forensic applications), which can provide an indexing mechanism. Fingerprint classification can be viewed as a coarse level matching of the fingerprints.

To increase the search efficiency, the fingerprint classification algorithm can classify a fingerprint into five distinct classes, namely, *whorl* (*W*), *right loop* (*R*), *left loop* (*L*), *arch* (*A*), and *tented arch* (*T*) (Figure 1.5). The five classes are chosen based on the classes identified by the National Institute of Standards and Technology (NIST) to benchmark automatic fingerprint classification algorithms.

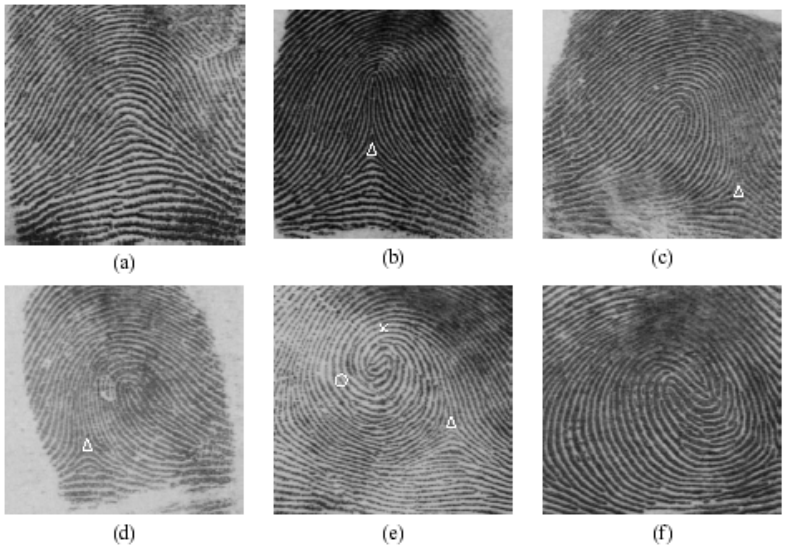


Figure 2: Fingerprints and a fingerprint classification schema involving six categories: (a) Arch, (b) tented arch, (c) right loop, (d) left loop, (e) whorl, and (f) twin loop.

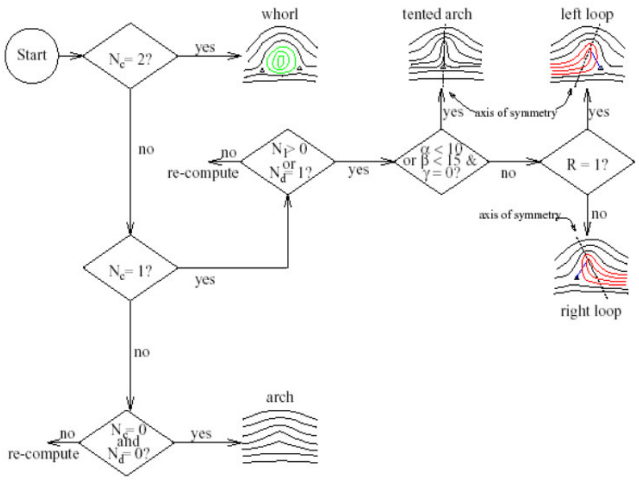


Figure 3: Flowchart of fingerprint classification algorithm.

Figure 2, shows one prevalent manual fingerprint classification scheme that has been the focus of many automatic fingerprint classification efforts. A fingerprint classification system should be invariant to rotation, translation, and elastic distortion of the frictional skin.
The classification algorithm summarized here in Figure 3, essentially devises a sequence of tests for determining the class of a fingerprint and conducts simpler tests earlier in the decision tree. For instance, two core points are typically detected for a whorl (see Figure 2), which is an easier condition to verify than detecting the number of Type-2 recurring ridges. Another highlight of the algorithm is that if does not detect the salient characteristics of any category from features detected in a fingerprint; it recomputes the features with a different pre-processing method. For instance, in the current implementation, the differential pre-processing consists of a different method/scale of smoothing. As can be observed from the flowchart that the algorithm detects (i) whorls based upon detection of either two core points or a sufficient number of Type-2 recurring ridges; (ii) arch based upon the inability to detect either delta or core points; (iii) left (right) loops based on the characteristic tilt of the symmetric axis, detection of a core point, and detection of either a delta point or a sufficient number of Type-1 recurring curves; and (iv) tented arch based on relatively upright symmetric axis, detection of a core point, and detection of either a delta point or a sufficient number of Type-1 recurring curves.

Feature Extraction
A feature extractor finds the ridge endings and ridge bifurcations from the input fingerprint images [8]. If ridges can be perfectly located in an input fingerprint image, then minutiae extraction is just a trivial task of extracting singular points in a thinned ridge map. However, in practice, it is not always possible to obtain a perfect ridge map. The performance of currently available minutiae extraction algorithms depends heavily on the quality of the input fingerprint images. Due to a number of factors (aberrant formations of epidermal ridges of fingerprints, postnatal marks, occupational marks, problems with acquisition devices, *etc.*), fingerprint images may not always have well-defined ridge structures. A reliable minutiae extraction algorithm is critical to the performance of an automatic identity authentication system using fingerprints. The overall flowchart of a typical algorithm [28, 18] is depicted in Figure 6. It mainly consists of three components: [9], Orientation field estimation, ridge extraction, and minutiae extraction and post processing.

1.**Orientation Estimation** The orientation field of a fingerprint image represents the directionality of ridges in the fingerprint image. It plays a very important role in fingerprint image analysis. A number of methods have been proposed to estimate the orientation field of fingerprint images.

2. Segmentation It is important to localize the portions of fingerprint image depicting the finger (foreground). The simplest approaches segment the foreground by global or adaptive thresholding.
3. **Ridge Detection** the approaches to ridge detection use either simple or adaptive thresholding. These approaches may not work for noisy and low contrast portions of the image. The extracted ridges may be thinned/cleaned using standard thinning and connected component algorithms.
4. **Minutiae Detection** once the thinned ridge map is available; the ridge pixels with three ridge pixel neighbors are identified as ridge bifurcations and those with one ridge pixel neighbor identified as ridge endings. However, all the minutia thus detected are not genuine due to image processing artifacts and the noise in the fingerprint image.

5. **Postprocessing** in this stage, typically, genuine minutiae are picked-up from the extracted minutiae using a number of heuristics. For instance, too many minutiae in a small neighborhood may indicate noise and they could be discarded. Very close ridge endings oriented anti-parallel to each other may indicate spurious minutia generated by a break in the ridge due either to poor contrast or a cut in the finger. Two very closely located bifurcations sharing a common short ridge often suggest extraneous minutia generated by bridging of adjacent ridges as a result of dirt or image processing artifacts.

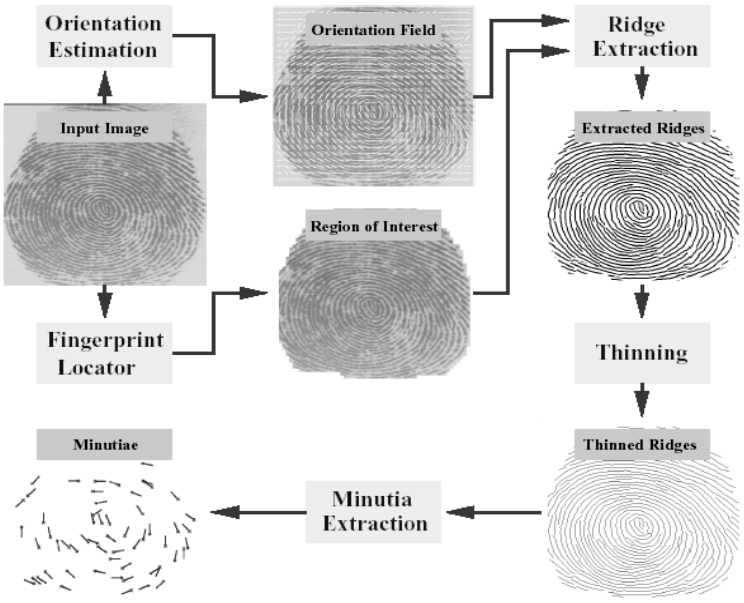


Figure 4: Flowchart of the minutiae extraction algorithm [18].

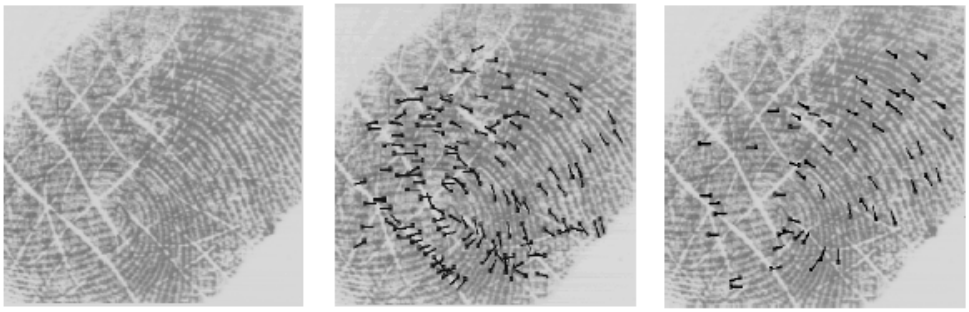
Fingerprint Enhancements

The performance of a fingerprint image-matching algorithm relies critically on the quality of the input fingerprint images. In practice, a significant percentage of acquired fingerprint images is of poor quality. The ridge structures in poor-quality fingerprint images are not always well defined and hence they cannot be correctly detected.

This leads to the following problems [9]:

- A significant number of spurious minutiae may be created
- A large percentage of genuine minutiae may be ignored
- Large errors in minutiae localization (position and orientation) may be introduced. In order to ensure that the performance of the minutiae extraction algorithm will be robust with respect to the quality of fingerprint images, an enhancement algorithm which can improve the clarity of the ridge structures is necessary.

The poor quality fingerprint image is processed using the filter to block the extraneous *noise* and pass the fingerprint *signal*. Some methods may estimate the orientation and/or frequency of ridge in each block in the fingerprint image and adaptively tune the filter characteristics to match the ridge characteristics. One typical variation of this theme segments the image into non-overlapping square blocks of widths larger than the average inter-ridge distance. A single block direction can never truly represent the directions of the ridges in the block and may consequently introduce filter artifacts.



(a) (b) (c)

Figure 5: Fingerprint Enhancement Results: (a) a poor quality fingerprint; (b) minutia extracted without image enhancement; and (c) minutiae extracted after image enhancement.

Summary
With recent advances in fingerprint sensing technology and improvements in the accuracy and matching speed of the fingerprint matching algorithms, automatic personal identification based on fingerprint is becoming an attractive alternative/complement to the traditional methods of identification. We have provided an overview of the fingerprint-based identification and summarized algorithms for fingerprint feature extraction, enhancement, matching, and classification. There will be a growing demand for faster and more accurate fingerprint matching algorithms, which can (particularly) handle poor quality images. It is too early to predict where, how, and which biometric technology would evolve and be mated with which applications. But it is certain that biometrics based identification will have a profound influence on the way we conduct our daily business. It is also certain that, as the most mature and well understood biometric, fingerprints will remain an integral part of the preferred biometric-based identification solutions in the years to come.

References
[1] Biometrics information resource, http://www.biometricsinfo.org.
[2] Bioinformatics by C.S.V. Murthy HPH.
[3] Anil K. Jain*, Fellow, Ieee*, Arun Ross*, Member, IEEE*, And Salil Prabhakar*, Member, IEEE* An Introduction To Biometric Recognition, *, IEEE* Transactions On Circuits And Systems For Video Technology, Vol. 14, No. 1, January 2004.
[4] Anil K. Jain, Sharath Pankanti, Salil Prabhakar, Lin Hong, and Arun Ross, *Michigan State University,* Biometrics: A Grand Challenge**,** *IBM T. J. Watson Research Center, DigitalPersona Inc., Siemens Corporate Research, West Virginia University.*
[5] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. New York: Springer-Verlag, 2005.
[6] *Salil Prabhakar* DISSERTATION, Fingerprint Classification and Matching Using a Filterbank By*, 200.*
[7] Anil Jain, S. Pankanti, Fingerprint Classification and Matching.
[8] Biometric Sensor Interoperability: A Case Study in Fingerprints, Arun Ross1 and Anil Jain2,] *LNCS Vol. 3087, pp. 134-145, Springer Publishers, May 2004.*
[9] S. Prabhakar and A. K. Jain, "Decision-level fusion in fingerprint verification," *Pattern Recognition,* vol. 35, no. 4, pp. 861–874, 2002.