Pre-print version

R. Donida Labati, F. Scotti, "Fingerprint", in Encyclopedia of Cryptography, Security and Privacy, S. Jajodia, P. Samarati, M. Yung (eds.), Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 1-6, January, 2021. ISBN: 978-3-642-27739-9.

[DOI: 10.1007/978-3-642-27739-9_740-2]

Fingerprint

Ruggero Donida Labati * and Fabio Scotti

Definition

Fingerprints are reproductions of the surface pattern of the fingertip epidermis. This pattern is a characteristic sequence of interleaved ridges and valleys, usually considered as unique for each individual.

Background

Fingerprint is the mostly used and known biometric trait. Fingerprint was introduced as a method for person identification before 1900, and the first automatic fingerprint recognition systems were introduced in the '70s.

Fingerprint is a biometric trait with high permanence and distinctiveness. In general, the fingertip ridge pattern is a part of the individual's phenotype and is different for each individual. The fingerprints of the same person are different, and even the ones of identical twins are not equal. Furthermore, the fingertip ridge structure is fully formed at about 7 months of the fetus development and this pattern configuration does not change for the entire life unless serious accidents or diseases. Usually, cuts and bruises can only temporarily modify the fingerprint pattern.

Fingerprint recognition technologies are diffused in heterogeneous applications, characterized by relevant differences in sensors, costs, and accuracy. There are systems integrated in electronic devices, on-card systems, systems based on a personal computers, mobile systems, and large distributed systems, such as Automatic Fingerprint Identification Systems (AFIS) and automated border controls. In many law enforcement and government applications, the size of the fingerprint database can be very large. For example, the FBI Next Generation Identification (NGI)

* corresponding author

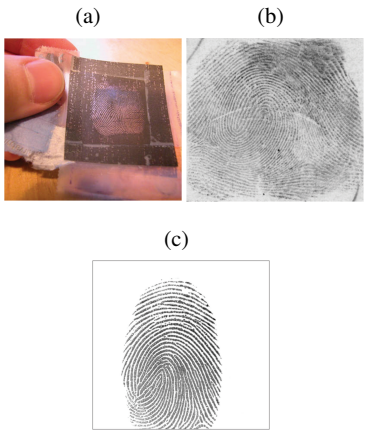

Fig. 1 Examples of fingerprint images: (a) latent; (b) rolled and inked; (c) live-scan.

System contains over 168 millions of fingerprints, as reported in Federal Bureau of Investigation (2019).

Most of the automatic biometric systems based on fingerprint characteristics perform identity recognitions by extracting and comparing information related to the ridge pattern present in fingerprint images.

Theory

Fingerprint images

It is possible to categorize the fingerprint images into three classes: latent fingerprints, inked fingerprints, and live-scan fingerprints. Fig. 1 shows an example of images obtained by the different fingerprint acquisition methods.

Latent fingerprints are widely used in forensic investigations. These fingerprints are involuntary produced by transferring on an object the film of moisture and grease present on the finger surface.

Inked fingerprints are typically used for governmental and police applications. The acquisition process requires user cooperation and can be divided in two tasks. First, the user rolls a finger spread with black / blue ink on a paper card. Second, the card is converted into a digital form.

Live-scan fingerprints are typically used to perform online biometric recognitions. The acquisition process requires user cooperation and consists of impressing a finger on the acquisition surface of a device. It is possible to distinguish three main types of live-scan technologies: optical, solid state, and ultrasound sensors.

To obtain accurate biometric recognitions, the fingerprint images should be of sufficient quality. To this purpose, the Federal Bureau of Investigation (FBI) defined a set of minimum parameters that should be guaranteed for the acquisition of digital fingerprint images.

The most commonly used algorithms used for image compression can significatively reduce the visibility of the distinctive characteristics of fingerprint images. Therefore, the image compression is frequently performed using specifically designed algorithms, as the Wavelet Scalar Quantization (WSQ), proposed by the FBI.

Fingerprint analysis

The analysis of fingerprint images can be performed using three levels of detail.

- *Level 1* considers the overall global ridge flow pattern.

- *Level 2* considers distinctive points of the ridges, called minutiae points.
- *Level 3* considers ultra-thin details, such as the pores, incipient ridges, and local peculiarities of the ridge edges.

Examples of Level 1 characteristics are the *local ridge orientation*, *local ridge frequency*, *ridge count*, *singular regions*, and techniques for mapping global information describing the ridge pattern. The local ridge orientation consists of the angle of the ridges with respect to the horizontal axis. The local ridge frequency consists of the number of ridges per unit length along a segment that is orthogonal to the ridge orientation. The ridge count consists of the number of ridges between two points in the fingerprint. Singular regions represent areas of the fingerprint with a distinctive shape of the ridges. There are three main types of singular regions: loop, delta, and whorl. The distinctive shapes of these regions are $\cap$, Δ, and O, respectively (Fig. 2). From the analysis of the singular regions, it is also possible to estimate a reference point in the fingerprint, called *core point*. Fruthermore, singular regions can be used to perform a classification of the samples, for example by using the Galton-Henry scheme, which is composed of 5 classes (arch, tented-arch, left loop, right loop, and whorl). Fig. 3 shows an example of the considered classes. There are also techniques for mapping global information describing the ridge pattern to extract distinctive features to be used by biometric matchers, for example by applying Gabor filters to local regions the fingerprint image.

Level 2 analysis evaluates specific ridge discontinuities called *minutiae*. It is possible to distinguish many classes of minutiae (Fig. 4), but most of the automatic biometric systems consider only terminations and bifurcations. The methods for estimating the minutiae coordinates are usually composed of four main tasks: (i) adaptive binarization of the ridges; (ii) reduction of the ridge thickness to one single pixel by performing a thinning operation; (iii) estimation of the minutiae coordinates by searching for specific local patterns of the ridges, typically in the 8-neighborhood; and (iv) post-processing for discarding erroneously estimated minutiae. Furthermore, most of the minutiae-based approaches estimate the orientation of the minutiae, considered as the value of the ridge orientation map in the coordinates of each minutia point.

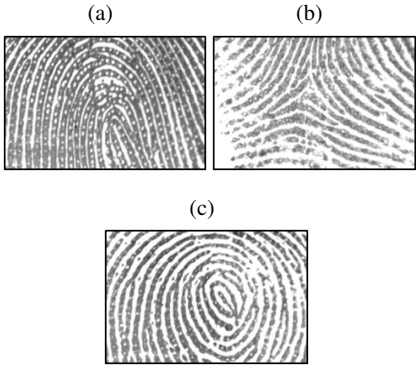

Fig. 2 Examples of singular regions: (a) loop; (b) delta; (c) whorl.

Level 3 analysis requires high-resolution acquisition devices (with at least 800 dpi) and it is not commonly applied in commercial systems. Methods for Level 3 analysis in the literature are heterogeneous and can be based on different techniques. As an example, the method presented in Donida Labati et al (2018) extracts the coordinates of

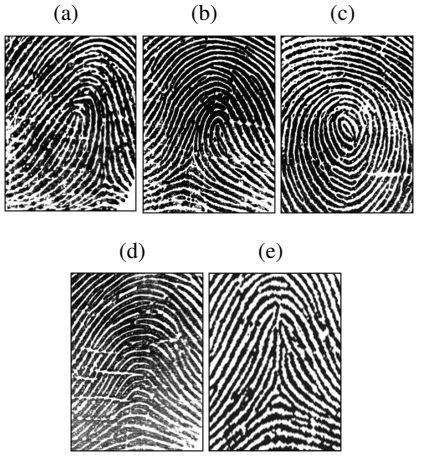

Fig. 3 Galton-Henry classification scheme: (a) left loop; (b) right loop; (c) whorl; (d) arch; (e) tented arch.

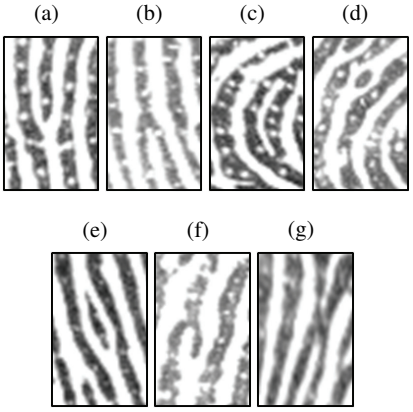

Fig. 4 Examples of common minutiae types: (a) termination; (b) bifurcation; (c) lake; (d) point or island; (d) independent ridge; (f) spur; (g) crossover.

the pores by using Convolutional Neural Networks (CNNs).

To obtain more discriminative features, most of the fingerprint recognition systems perform an *image enhancement* step before applying feature extraction algorithms. As described in Schuch et al (2018), different enhancement techniques are available, as pixel-wise enhancement, contextual filtering, and multi-resolution enhancement.

Another step that is frequently performed before the feature extraction consists of the *quality assessment*. As discussed in Yao et al (2016), quality assessment methods can be used to discard fingerprint images of insufficient quality, select only recoverable image regions, reduce the artifacts produced by the enhancement algorithms, and weight the features according to the local quality of the fingerprint image.

Fingerprint matching

Fingerprint matching algorithms compute a similarity index called *matching score* between two fingerprints. It is possible to divide the fingerprint matching algorithms into three classes: correlation-based techniques; minutiae-based methods; methods based on other features.

Correlation-based techniques compute the matching score directly from fingerprint images, without requiring a preliminary feature extraction step. This approach is rather basic and not commonly present in automated fingerprint recognition system.

Minutiae-based methods are the most studied and applied in the literature. As described in Peralta et al (2015), most of the methods can be divided in two tasks: alignment of the minutiae extracted from two fingerprint images, and matching score computation. It is possible to distinguish global and local

minutiae matching algorithms. Global algorithms compute the matching score by considering the full minutiae sets. Local algorithms consider sets of minutiae divided in sub-portions, for example by adopting auxiliary graph structures (e.g., Delaunay triangles).

Other fingerprint matching methods can use features extracted at different levels as support information for processing a matching score based on minutiae sets or can directly process features extracted at Level 1 or Level 3. Recent methods automatically learn feature extraction techniques directly from the input images by using deep learning strategies, as described in Sundararajan and Woodard (2018).

Security and privacy in fingerprint recognition systems

Security and privacy are two aspects of paramount importance for biometric systems.

Every hardware and software modules composing a fingerprint recognition system can be subject to attacks. One of the most common kinds of attacks to fingerprint recognition systems consists of presenting fake fingers to the sensor. As described in Marasco and Ross (2014), it is possible to use vitality detection methods to overcome this vulnerability. These methods can be divided in two categories: methods that do not require specific actions from the users (using additional physiological characteristics or analyzing only the input sample), and methods that measure voluntary responses of the users (presenting an additional biometric trait, password, or smart-card).

Privacy protection techniques for fingerprint recognition systems mainly aim at protecting the samples and templates by storing them using secured representations and by performing biometric recognitions in a secured domain. There are different methods in the literature for protecting fingerpint templates, as described in Donida Labati et al (2012). The most known methods are the following ones: salting, non-invertible transforms, key-binding biometric cryptosystem, key generating biometric cryptosystem, and homomorphic cryptosystems.

There are also technologies for decentralizing the computation of fingerprint recognition systems by increasing the privacy protection level with respect to centralized systems, as match-on-card, system-on-device, and system-on-a-chip. An important advantage offered by these technologies is that the user keep the possession of her / his templates (mostly on a tamper resistant hardware).

Open problems and Future directions

Although fingerprint recognition systems are one of the most mature biometric technologies, different open problems are still present. A relevant open problem consists of identifying people in large databases in a fast and accurate manner, for example in investigative applications. Another important problem is the limited capability to process latent fingerprint images using completely automatic systems. Since latent fingerprints are usually partial and affected by high level of noise

and distortions, automatic analysis techniques usually achieve poor results in this application scenario. Processing poor quality images acquired from manual workers and elder people is also an open problem since current biometric technologies frequently do not obtain satisfactory accuracy.

Feature research directions will consider the previously described open problems, as well as will improve different aspects of the current fingerprint recognition technologies. A research direction consists of improving the human-machine interaction by using touchless and / or three-dimensional systems, as described in Donida Labati et al (2016). Another direction consists of improving the accuracy, speed, and robustness of current technologies by using deep learning strategies for different steps of the biometric recognition process, as described in Sundararajan and Woodard (2018). Furthermore, the research community is focusing on novel and better performing strategies for privacy and security protection of biometrics, as described in Donida Labati et al (2012). Novel high-resolution sensors and processing techniques will also be studied to improve current technologies by using Level 3 feature, as described in Donida Labati et al (2018).

Summary

Fingerprint recognition systems are the most mature and diffused biometric technologies. Current biometric systems can process images acquired using heteregeneous procedures and compute different kinds of features, obtaining relevant recognition accuracy. Although the maturity of fingerprint recognition systems, the research community is still working on open problems and on improving the current technologies.

References

Donida Labati R, Piuri V, Scotti F (2012) Biometric privacy protection: Guidelines and technologies. In: Obaidat MS, Sevillano JL, Filipe J (eds) E-Business and Telecommunications, Springer Berlin Heidelberg, pp 3–19

Donida Labati R, Genovese A, Piuri V, Scotti F (2016) Toward unconstrained fingerprint recognition: A fully touchless 3-d system based on two views on the move. IEEE Transactions on Systems, Man, and Cybernetics: Systems 46(2):202–219

Donida Labati R, Genovese A, Muñoz E, Piuri V, Scotti F (2018) A novel pore extraction method for heterogeneous fingerprint images using convolutional neural networks. Pattern Recognition Letters 113:58 – 66

Federal Bureau of Investigation (2019) November 2019 Next Generation Identification (NGI) System Fact Sheet

Marasco E, Ross A (2014) A survey on anti-spoofing schemes for fingerprint recognition systems. ACM Computing Surveys 47(2)

Peralta D, Galar M, Triguero I, Paternain D, García S, Barrenechea E, Benítez JM, Bustince H, Herrera F (2015) A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation. Information Sciences 315:67 – 87

Schuch P, Schulz S, Busch C (2018) Survey on the impact of fingerprint image enhancement. IET Biometrics 7:102–115(13)

Sundararajan K, Woodard DL (2018) Deep learning for biometrics: A survey. ACM Computing Surveys 51(3)

Yao Z, Le Bars J, Charrier C, Rosenberger C (2016) Literature review of fingerprint quality assessment and its evaluation. IET Biometrics 5(3):243–251