Pre-print version

R. Donida Labati, F. Scotti, "Fingerprint", in Encyclopedia of Cryptography and Security (2nd ed.), H.C.A. van Tilborg, S. Jajodia (ed.), Springer, pp. 460 - 465, 2011.

DOI: 10.1007/978-1-4419-5906-5

Fingerprint

Ruggero Donida Labati and Fabio Scotti

December 2, 2010

1 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.

2 Background

Fingerprints are the most used and known biometric traits. Biometric systems based on the fingerprint trait estimate the identity of an individual by extracting and comparing information related to the characteristics of the ridge pattern.

Fingerprint recognition systems are used in different contexts [1]. Important applications of the fingerprint trait are the forensic investigation, and the public sector applications (e.g., border controls, police archives, national archives, and biometric documents). Also in the private sector, fingerprint biometric systems are commonly deployed to control the accesses to critical areas, consoles, data and electronic devices (e.g., personal computers, PDA, and mobile phones). Emerging sectors for the application of these technologies are e-government, e-commerce and banking.

Fingerprint recognition is the most mature biometric technology. In fact, fingerprint was introduced as a method for person identification before 1900, and the first automatic fingerprint recognition systems was introduced in the '70s.

Fingerprint is a biometric trait with high permanence and distinctiveness. The fingertip ridge structure is fully formed at about 7 months of fetus development, and this pattern configuration does not change for all the life unless serious accidents or diseases. Usually, cuts and bruises can only temporarily modify the fingerprint pattern.

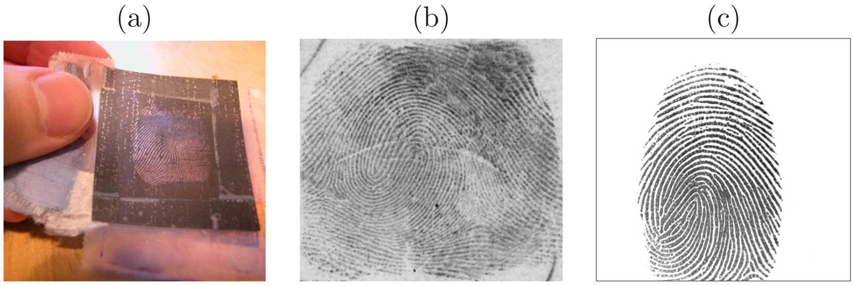

Figure 1: Examples of fingerprint images: (a) latent; (b) rolled and inked; (c) live-scan.

In general, fingerprints are a part of an individual's phenotype and are different for each individual. Also the fingerprints of the same person are different, and even in the case of the and fingerprints of identical twins are not equal. The social acceptability of the use of the fingerprint biometric trait can be considered as limited, since people perceive this biometric trait as related to police and investigative activities.

3 Theory

3.1 Fingerprint images

Three different classes of fingerprint images can be identified: latent fingerprints, inked fingerprints, and live-scan fingerprints.

Latent fingerprints are very important in forensics. This kind of fingerprints is produced by the transfer of the film of moisture and grease that is present on the surface of the finger when occur contacts to objects. Usually, latent fingerprint are not visible to naked eye and forensic investigators use proper substances for enhancing the visibility of the ridge pattern.

Inked fingerprints are typically obtained with the following procedure. The user's finger is spread with black/blue ink and then rolled on a paper card, secondly the card is converted into a digital form by means of a high-definition paper-scanner or by using a high-quality CCD camera.

Live-scan fingerprints are obtained by impressing a finger on the acquisition surface of a device. It is possible to distinguish three different types of live-scan sensor technologies: optical sensors; solid state sensors; ultrasound sensors. Fig. 1 shows an example of images obtained by the different fingerprint acquisition methods.

Only good quality images have to be stored in order to achieve subsequently accurate biometric recognitions by automatic systems. For example, the Federal Bureau of Investigation (FBI) of the USA defined a set of main parameters characterizing the acquisition of a digital fingerprint image encompassing minimum resolution, minimum size of the captured area, minimum number of pixels, maximum geometry distortion of the acquisition device, minimum number of gray-levels, maximum gray-level uniformity, minimum spatial frequency response of the device, and minimum signal to noise ratio.

In many law enforcement and government applications when Automatic Fingerprint Identification Systems (AFIS) are involved, the size of the fingerprint database is typically very large. For example, the FBI fingerprint card archive contains over 200 million of identities. In such cases, compressed formats are adopted. One of the most used compression algorithm had been proposed by the FBI and it is based on the Wavelet Scalar Quantization (WSQ) technique.

3.2 Fingerprint analysis

The analysis of the ridge details can be performed with three different level of accuracy.

- Level 1: the overall global ridge flow pattern is considered.
- Level 2: the analysis is based on distinctive points of the ridges, called minutiae points.
- Level 3: ultra-thin details, such as pores and local peculiarities of the ridge edges, are studied.

Examples of characteristics analyzed at Level 1 are the *local ridge orientation*, the *local ridge frequency*, the *singular regions* and the *ridge count*. The local ridge orientation is estimated as the angle of the ridges with respect to the horizontal axis. The ridge orientation map of the fingerprint can be computed by estimating the local ride orientation in areas centered in each pixel of the fingerprint images. In the literature, most of the methods for the computation of the ridge orientation map are based on the analysis of the gradient of the fingerprint image [2].

The local ridge frequency is the the number of ridges per unit length along a segment that is orthogonal to the ridge orientation. The ridge frequency map represents the local ridge frequency computed in each pixel of the fingerprint image.

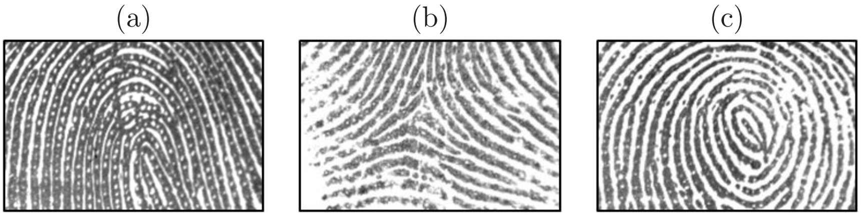

Figure 2: Examples of singular regions: (a) loop; (b) delta; (c) whorl.

An important Level 1 analysis consists of the estimation of the singular regions. A singular region represents an area of the finger with a distinctive shape of the ridges. Commonly, three different types of singular regions are considered: loop, delta, whorl. The distinctive shapes of these regions are $\cap$, Δ, and O respectively (Fig. 2). In the literature, the majority of the methods for the estimation of the singular methods uses the Poincaré technique [1] applied on the ridge orientation map. From the analysis of the singular regions, it is also possible to estimate a reference point in the fingerprint, which is called *core point*. Examples of other characteristics of Level 1 are the *ridge count* [3] and other global mapping information obtained by the application of Gabor filters on the input fingerprint images [4].

Level 2 analysis evaluates specific ridge discontinuities called *minutiae*. It is possible to distinguish many different classes of minutiae (Fig. 3), but most of the automatic biometric systems in the literature consider only terminations and bifurcations. Usually, the identification of the minutia can be achieved in four main steps [1]: (i) an adaptive binarization is applied in order to separate the ridges from the background in the fingerprint image; (ii) a thinning operation is achieved in order to reduce the thickness of the ridges to one single pixel; (iii) the coordinates of the minutiae are estimated by observing the specific local pattern of each single pixel of the ridges, typically in its 8-neighborhood; (iv) a post-processing method is applied in order to reduce the number of false minutiae detected in the previous step.

A different approach for the minutiae identification processes directly gray-scale images without the binarization step and it based on the capability to follow the ridges in the input image by observing the local orientation [5]. Another important information related to each minutia is its direction, considered as the value of the ridge orientation map in the minutia coordinates.

An additional step that can be present in the fingerprint analysis is the *image enhancement*. Different algorithms are available [1], for example pixel-

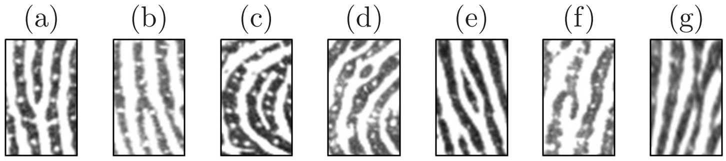

Figure 3: Examples of common minutiae types: (a) termination; (b) bifurcation; (c) lake; (d) point or island; (d) independent ridge; (f) spur; (g) crossover.

wise enhancement, contextual filtering and multi-resolution enhancement. One of the most famous enhancement method applies a set of Gabor filters to the fingerprint image according to to the ridge orientation map and the ridge frequency map [6].

Level 3 analysis requires high-resolution acquisition devices (with at least 800 dpi) and it is not commonly applied in commercial systems. Standard features extracted at this level of analysis consists in the spatial coordinates of the pores.

Captured fingerprint images can have an very different quality levels. In particular, low levels of the fingerprint quality can compromise the identity verification/recognition [7]. In order to control this factor, quality estimation methods are usually considered [8, 9]. Quality estimation is also useful to select unrecoverable image regions, to reduce the artifacts product by the enhancement algorithms, and to properly weight the extracted features according to the local quality level of the input fingerprint.

3.3 Fingerprint matching

Fingerprint matching algorithms compute a similarity index called *match-score* of two fingerprints used in the the verification/identification procedures. It is possible to divide the fingerprint matching algorithms in three different classes: correlation-based techniques; minutiae-based methods; methods based on other features.

The *correlation-based* techniques computes the match-score between two fingerprint images. The images are scaled, translated, rotated, equalized, and then, the match-score is obtained as the correlation between the two images. This approach is rather basic and not commonly present in automated fingerprint recognition system.

The *minutiae-based* methods are the most studied and applied in the literature [10]. Most of the methods perform an alignment of the minutiae extracted from two fingerprint images by shift and rotate operations, and then it is computed the match-score as the number of matched minutiae pairs divided by the mean number of minutiae in the two images. The alignment step is necessary for reducing problems related to difference of scale, rotation, translation, and non linear distortion caused by different pressures of the finger on the sensor. It is possible to distinguish global and local minutiae matching algorithms. Global algorithms consider all the minutiae points of the two fingerprint images and search the best match score by using different alignment strategies. For example, global minutiae matching methods can be based on algebraic geometry, Hough transform, relaxation, energy minimization. Local algorithms consider sets of minutiae divided in sub-portions, for example by adopting auxiliary graph structures (e.g., Delaunay triangles [11]). Local minutiae matching methods can be based on triangulation, multiple registration strategies, and warping techniques.

Other fingerprint matching methods can use features extracted at different levels as support information for processing a match score based on the minutiae set or directly process features extracted at Level 1 or Level 3 (e.g., the template creation technique processed at Level 1 called *Fingercode* [4]).

3.4 Fingerprint classification and indexing

The identification procedure requires to compare the captured biometric template with all the templates stored in a database. In the case of very large databases, the computational time required for a complete the full set of biometric comparisons can be unacceptable. A strategy used for reducing the required number of identity to be compared consists in the creation of partitions (called *bins*) containing only fingerprint that appertain to a defined class.

Usually, fingerprint are classified by the Galton-Henry classification scheme. This scheme is based on Level 1 features and is composed by 5 classes (arch, tented-arch, left loop, right loop, and whorl). Fig. 4 shows an example of the considered classes. Fingerprint classification can be achieved by different approaches, such as neural networks classifiers, statistical methods, syntactic methods, rule-based methods, support vector machines [12]. Further strategies can be applied for reducing the number of identity comparisons such as the use of a sub-classification [13] and the computation of continuous indexes related to different fingerprint features [11].

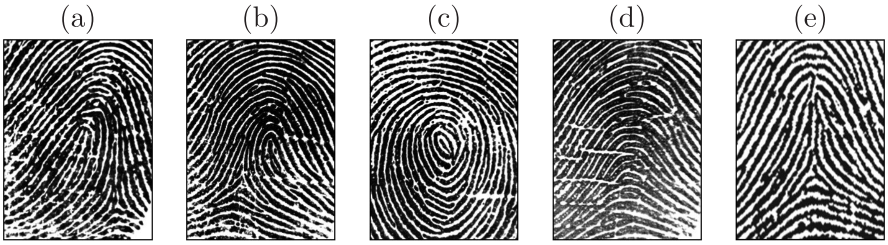

Figure 4: Galton-Henry classification scheme: (a) left loop; (b) right loop; (c) whorl; (d) arch; (e) tented arch.

3.5 Security and privacy in fingerprint recognition systems

All hardware and software modules composing a fingerprint recognition system can be subject to attacks. In the literature, the majority of techniques focuses on the injection of fingerprint data (e.g., fake fingers, injection of fingerprint data in the communication channel or in the storage system) and the replacement of software modules with a modified/malicious version in order to force/avoid the final match score.

The former approach of attacks can be countered by vitality controls [14]. It is possible to divide these methods in two categories: methods based on involuntary captured information by the biometric scanner, and methods that measure a voluntary response of the user. The first category evaluates directly physical characteristics (e.g., heartbeat, odor, arterial oxygen saturation of hemoglobin, pulse presence) or characteristics extracted from one single fingerprint images or frame sequences (e.g., fine movements of the fingertip surface, involuntary challenge-response, valley noise, pores presence). The second approach analyzes the voluntary behavior of the user, information related to other biometric traits as in multibiometrics [15], additional data provided by the user (e.g., password, smart-card, voluntary challenge-response, etc.) or surveillance.

The protection of the user privacy is an important issue to be considered when fingerprint recognition systems are deployed [16, 17]. Techniques based on biometric encryption are often considered to achieve the protection of the fingerprint template [18] [19, 20, 21]. The most known methods are the following: salting techniques, systems that non-invertible transforms, key-binding biometric cryptosystem, key generating biometric cryptosystem, and homomorphic cryptosystems.

Technologies for decentralizing fingerprint recognition computation are also available with specific reference to the match-on-card systems, system-on-device and system-on-a-chip technologies. An important advantage offered by these technologies is that the user keep the possession of her/his templates (mostly on a tamper resistant hardware). The main disadvantage of such approach is that the obtained performances in terms of accuracy and computational time tend to be inferior than the performances of dedicated and PC-based fingerprint systems.

4 Applications

The applications of fingerprint technology are heterogeneous and range from the public to private sector. In the market there are available fingerprint recognition systems with a great difference of sizes of sensors, costs, and accuracy [1, 22]. For example, there are systems integrated in electronic devices (e.g., PDA and mobile phones), on-card systems, systems based on a personal computers, and large distributed systems [23] such as the AFIS [24].

The main applicative contexts of fingerprint recognition systems are in forensics, governmental, and commercial sectors. In the forensic sector, the fingerprint trait is used for the identification of persons, the search of lost person and general investigative activities. In the governmental sector, important applications are border controls, biometric documents (for example passports and IDs). Examples of applications in the commercial sector are authentication systems integrated to ATM, terminal login, access control for on-line services (e.g. e-commerce and e-banking applications), and the protection of sensible data (e.g. in personal computers, PDA, mobile phones, and storage devices) and access control to restricted areas.

References

[1] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, 2nd Edition, Springer Publishing Company, Incorporated, 2009.

[2] Z. Hou, W.-Y. Yau, Y. Wang, A review on fingerprint orientation estimation, Security and Communication Networks.

[3] W.-C. Lin, R. C. Dubes, A review of ridge counting in dermatoglyphics, Pattern Recognition 16 (1) (1983) 1–8.

[4] A. Jain, S. Prabhakar, L. Hong, S. Pankanti, Filterbank-based fingerprint matching, IEEE Transactions on Image Processing 9 (5) (2000) 846–859.

[5] D. Maio, D. Maltoni, Direct gray-scale minutiae detection in fingerprints, IEEE Transaction o Pattern Analysis and Machine Intelligence 19 (1997) 27–40.

[6] L. Hong, Y. Wan, A. Jain, Fingerprint image enhancement: algorithm and performance evaluation, Pattern Analysis and Machine Intelligence, IEEE Transactions on 20 (8) (1998) 777–789.

[7] M. Gamassi, M. Lazzaroni, M. Misino, V. Piuri, D. Sana, F. Scotti, Quality assessment of biometric systems: a comprehensive perspective based on accuracy and performance measurement, IEEE Transactions on Instrumentation and Measurement 54 (4) (2005) 1489–1496.

[8] F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, J. Gonzalez-Rodriguez, H. Fronthaler, K. Kollreider, J. Bigun, A comparative study of fingerprint image-quality estimation methods, IEEE Transactions on Information Forensics and Security 2 (4) (2007) 734–743.

[9] F. S. R. Donida Labati, V. Piuri, Neural-based quality measurement of fingerprint images in contactless biometric systems, in: The 2010 International Joint Conference on Neural Networks (IJCNN), 2010, pp. 1–8.

[10] N. Yager, A. Amin, Fingerprint verification based on minutiae features: a review, Pattern Analysis & Applications 7 (2004) 94–113.

[11] X. Liang, A. Bishnu, T. Asano, A robust fingerprint indexing scheme using minutia neighborhood structure and low-order delaunay triangles, IEEE Transactions on Information Forensics and Security 2 (4) (2007) 721–733.

[12] R. Cappelli, D. Maio, The state of the art in fingerprint classification, in: N. Ratha, R. Bolle (Eds.), Automatic Fingerprint Recognition Systems, Springer New York, 2004, pp. 183–205.

[13] G. A. Drets, H. G. Liljenström, Intelligent biometric techniques in fingerprint and face recognition, CRC Press, Inc., Boca Raton, FL, USA, 1999, Ch. Fingerprint sub-classification: a neural network approach, pp. 107–134.

[14] P. Coli, G. Marcialis, F. Roli, Vitality detection from fingerprint images: A critical survey, in: S.-W. Lee, S. Li (Eds.), Advances in Biometrics, Vol. 4642 of Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 2007, pp. 722–731.

[15] A. Azzini, S. Marrara, R. Sassi, F. Scotti, A fuzzy approach to multimodal biometric continuous authentication, Fuzzy Optimization and Decision Making 7 (2008) 243–256.

[16] S. Cimato, M. Gamassi, V. Piuri, R. Sassi, F. Scotti, Biometrics: Theory, Methods, and Applications, Wiley-IEEE Press, 2008, Ch. Privacy in Biometrics.

[17] S. Cimato, M. Gamassi, V. Piuri, R. Sassi, F. Scotti, Privacy-aware biometrics: Design and implementation of a multimodal verification system, in: Annual Computer Security Applications Conference (ACSAC), 2008, pp. 130–139.

[18] A. K. Jain, K. Nandakumar, A. Nagar, Biometric template security, EURASIP Journal on Advances in Signal Processing 2008 (2008) 1–17.

[19] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. Donida Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, A. Piva, F. Scotti, A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates, in: Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), 2010, pp. 1–7.

[20] M. Barni, T. Bianchi, D. Catalano, M. D. Raimondo, R. Donida Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, F. Scotti, A. Piva, Privacy-preserving fingercode authentication, in: Proceedings of the 12th ACM workshop on Multimedia and security, ACM, New York, NY, USA, 2010, pp. 231–240.

[21] T. Bianchi, R. Donida Labati, V. Piuri, A. Piva, F. Scotti, S. Turchi, Implementing fingercode-based identity matching in the encrypted domain, in: 2010 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS), 2010, pp. 15–21.

[22] V. Piuri, F. Scotti, Fingerprint biometrics via low-cost sensors and webcams, in: 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2008, pp. 1–6.

[23] M. Gamassi, V. Piuri, D. Sana, F. Scotti, O. Scotti, Scalable distributed biometric systems - advanced techniques for security and safety, IEEE Instrumentation & Measurement Magazine 9 (2) (2006) 21–28.

[24] P. Komarinski, Automated Fingerprint Identification Systems (AFIS), Elsevier Academic Press, 2005.